SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO

CARLOS HERNANDO SALAMANCA LOZANO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA

INGENIERIA DE TELECOMUNICACIONES
LETICIA-AMAZONAS
MAYO 2020

SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO

AUTOR

CARLOS HERNANDO SALAMANCA LOZANO

DIPLOMADO DE PROFUNDIZACIÓN PARA OPTAR POR EL TÍTULO DE INGENIERO DE TELECOMUNICACIONES

DIRECTOR DEL CURSO

ING. JUAN CARLOS VESGA FERREIRA

TUTOR

ING. DIEGO EDINSON RAMIREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
INGENIERIA DE TELECOMUNICACIONES
LETICIA-AMAZONAS

MAYO 2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Leticia, 27 de mayo (27, 05, 2020) (Mayo 27 de 2020)

EDICATORIA Y AGRADECIMIENTOS

Este trabajo de grado esta dedicado y enfocado como base teórica a todos los futuros estudiantes los cuales están iniciando su proceso formativo, espero sea de gran ayuda.

Agradezco a Dios, por las grandes oportunidades que me ha dado en la vida, Como es tener una familia que me ha apoyado siempre de manera incondicional, buscando siempre lo major.

Agradezco el apoyo y asesoría del tutor, director del curso y compañeros los cuales de una u otra manera me apoyaron durante este proceso formativo.

INDICE

Pag.

LISTA DE TABLAS

LISTA DE GRÁFICAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

DHCP: (Dynamic Host Configuration Protocol), protocolo de configuración de host dinámico) es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin una intervención especial).

LAN: son las siglas de Local Area Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada.
Packet Tracer: Programa de simulación de redes que permite a los estudiantes experimentar con el comportamiento de la red.

Cisco IOS: (originalmente Internetwork Operating System) es el software utilizado en la gran mayoría de routers (encaminadores) y switches (conmutadores) de Cisco Systems (algunos conmutadores obsoletos ejecutaban CatOS).
IPv4: es la versión actual del protocolo de Internet, el sistema de identificación que utiliza Internet para enviar información entre dispositivos.

OSPF: (Open Shortest Path First) Protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

CCNA: (Cisco Certified Network Associate) es una certificación entregada por la compañía Cisco Systems a las personas que hayan rendido satisfactoriamente el examen correspondiente sobre infraestructuras de red e Internet.

RESUMEN

Con el avance del presente trabajo, se desarrollará la evaluación final de habilidades Con el avance del presente trabajo, se desarrollará la evaluación final de habilidades prácticas del curso de profundización CISCO CCNA. En el que se pretende diseñar una topología de red y verificar la configuración predeterminada de los diferentes dispositivos, router, switch, computador y servidor configurar los parámetros básicos de los dispositivos de red, verificar y probar la conectividad de red y administrar direccionamiento ip dinamico y estático. Este diseño de red se realizara mediante el software de simulación cisco packet tracer, la conexión entre los router se hará mediante cable serial a cada puerto serial del mismo, para conexión entre los switch será con cable directo configurado de modo troncal y para los computadores por medio de cable directo asi mismo como para el servidor por medio del puerto Ethernet.

Por medio de este trabajo se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

PALABRAS CLAVE: Dhcp, dns, ospfv2, nat, enrutamiento dinamico y estatico, ripv2, troncal, vlan.

1. INTRODUCCIÓN

En el siguiente documento se pondrá en práctica todos los contenidos estudiados durante el diplomado de profundización Cisco, por consiguiente se pretenden demostrar la solución a los 2 escenarios, los cuales son problemáticas de un entorno real de una red de comunicaciones. Por lo tanto encontraremos diferentes protocolos tales como; enrutamiento, parámetros de seguridad y acceso en diferentes dispositivos en la red, además de las configuraciones OSPF, RIPv2, implementación DHCP, NAT, verificación de ACL, así mismo los comandos de configuraciones de estos protocolos.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Diseñar y configurar una red LAN y WAN, proponiendo commandos que evidencien el desarrollo de habilidades obtenidas en el desarrollo del curso teorico-practico Cisco ccna.

2.2 OBJETIVOS ESPECÍFICOS

- Proponer los comandos requeridos para poder efectuar los diferentes protocolos; DHCP, OSPFV2, RIP, NAT, RIP, VLAN.
- Configurar cada uno de los dispositivos activos de red; servidores, switch, pc y router.
- Diseñar e implementar las 2 topologias de red

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Se pretende solucionar el problema de los dos estudios de casos basados en problemáticas reales de networking, ya se en una red pequeña LAN o en una red área extendida entre las cuidades de Bogota y Medellin. En la cual se debe configurar dichas redes con politicas de seguridad de acceso y trafico de información.

3.2 JUSTIFICACIÓN

Debio a la problemática mencionada anteriormente descrita se hace necesario ofrecer una solución para cada situación, esto se solucionará mediante el uso del software de simulación de redes Cisco Packet Tracer, en el cual se programa todas las configuraciones y protocolos; DCHP, RIP, OSPFV2, IPV4, VLAN, NAT y TRONCALES. Así mismo como configuración local y global.

4. MARCO TEORICO

La pagina web El taller del bit la configuración del servicio dhcp explica:

> El Server creado de forma automática en Packet Tracer es muy simple, y aún así permite , entre otras cosas , crear un servidor web o servidor FTP, un servidor DNS, SMTP y algo más, pero en el caso del servidor dhcp. Por eso, mejor hacer esta práctica en Packet Tracer en un Router. (Barrio, 2012)

El blog Enrutamiento dinámico OSPF con Packet Tracer presenta:

> camino más corto primero, es un protocolo de red para encaminamiento jerárquico de pasarela interior o Interior Gateway Protocol (IGP), que usa el algoritmo SmoothWall Dijkstra enlace-estado (Link State Advertisement, LSA) para calcular la ruta idónea entre dos nodos cualesquiera de un sistema autónomo. (Prieto, 2020)

La pagina web Expone:

> Los comandos de configuración de dispositivos cisco. (Huertas, 2013)

5. MATERIALES Y MÉTODOS

MATERIALES

- Computador
- Internet
- Software de simulación de redes Cisco Packet Tracer

METODOLOGÍA

- Trabajo autónomo
- Trabajo por etapas de configuración
- Asesoria docente

6. DESCRIPCIÓN GENERAL DE LA PRUEBA DE HABILIDADES

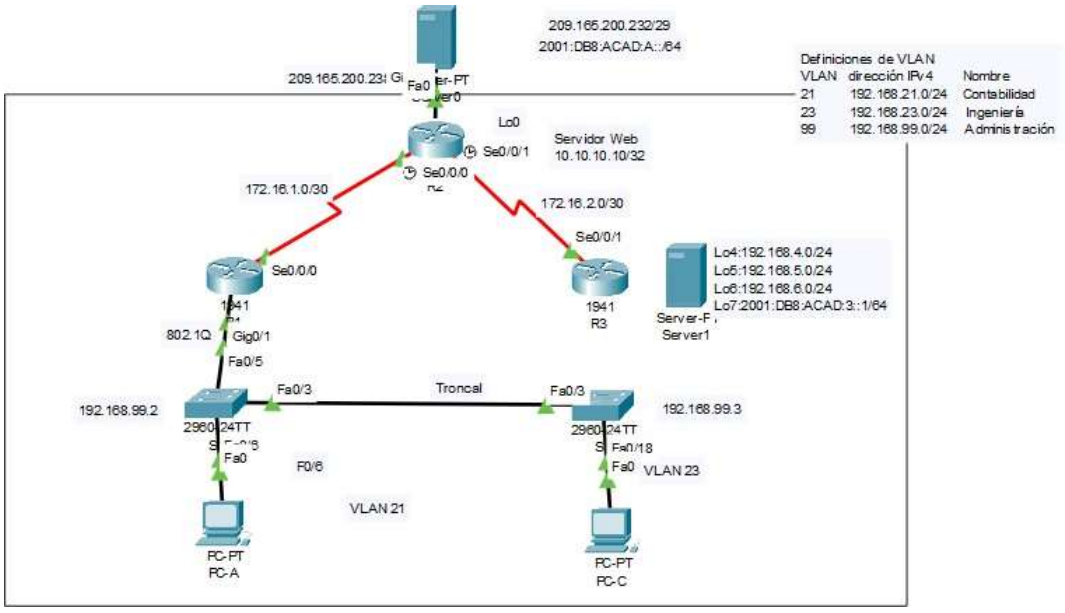
La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking. Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros. Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

7. DESARROLLO DE LOS ESCENARIOS

7.1 ESCENARIO 1

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

Gráfica 1. Topología – Escenario 1



Fuente: Simulador Cisco Packet Tracer 7.3, captura tomada por el autor.

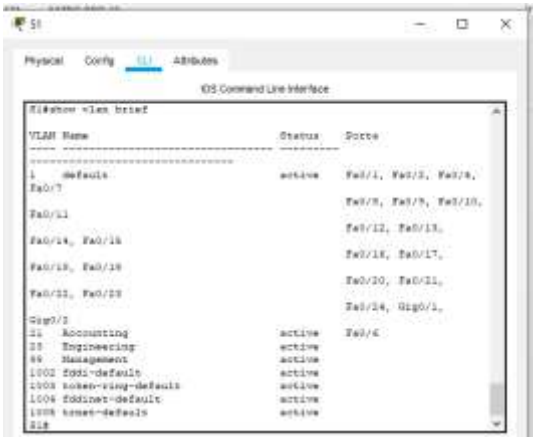
Parte 1. Inicializar dispositivos

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.

Tabla 1. Configuración básica del router y switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Se ejecuta el código: R1#Erase startup-config
Volver a cargar todos los routers	Digitamos el código: R1#reload System configuration has been modified. Save? [yes/no]:y Building configuration... [OK]Reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Para borrar el archivo el código: S1> enable S1#delete vlan.dat S1# delete flash:vlan.dat
Volver a cargar ambos switches	Comando: S1#Reload

Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Para verificar base de datos con el commando: S1#Show vlan brief Figura 1, Verificación de la base de datros de VLAN  **Fuente:** Simulador Cisco Packet Tracer 7.3, captura tomada por el autor.

Parte 2. Configurar los parámetros básicos de los dispositivos

Paso 1: Configuración del servidor de internet según la topología

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

Tabla 2. Configuración del servidor de Internet según topología

Elemento o tarea de configuración	Especifica
Dirección IPv4	Ingresamos al servidor, luego en la pestaña desktop, luego buscamos la pestaña o casilla de Ip configuration IPV4 Asignamos la ip 09.165.200.238
Máscara de subred para IPv4	En la siguiente casilla asignamos la mascara de subred Mask: 255.255.255.248

Gateway predeterminado	Por ultimo asignamos el Gateway o puerta de enlace: 209.165.200.225
Dirección IPv6/subred	Asignamos en casilla IPV6 Address: 2001:DB8:ACAD:A::38
Gateway predeterminado IPv6	Luego asignamos en la casilla Gateway de IPV6: 2001:DB8:ACAD:2::1

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente en partes posteriores de esta práctica de laboratorio.

Paso 2. Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3. Configuración del Router 1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Ingresamos en R1: Router(config)#no ip domain- lookup
Nombre del router	Se ingresa el código: Router(config)#hostname R1
Contraseña de exec privilegiado cifrada	R1(config)#Enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#password Cisco R1(config-line)#login 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)#exitLogin
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado. R1(config)#banner motd #se prohíbe el acceso no autorizado#

Interfaz S0/0/0	Establezca la descripción: comando: R1(config)#int S0/0/0 R1(config-if)#ip address 172.16.1.0 255.255.255.252 R1(config-if)#no shutdown Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones R1(config-if)int S0/0/0 R1(config-if)#ipv6 address 2001:db8:acad:1::1/64 R1(config-if)#ipv6 enable R1(config-if)#clock rate 128000 R1(config-if)#no shutdown R1(config-if)#exit R1(config)#ipv6 unicast-routing
Rutas predeterminadas	Configurar una ruta Ipv4 predeterminada de S0/0/0 R1(config)#int S0/0/0 R1(config-if)#ip address172.16.1.2 255.255.255.0 Configurar una ruta Ipv6 predeterminada de S0/0/0 interface Serial0/0/0 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Configuración del Router 2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	R2(config)#no ip domain-lookup
Nombre del router	Comando: Router(config)#hostname R2
Contraseña de exec Privilegiado cifrada	Comando: 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
Cifrar las contraseñas de texto no cifrado	R2(config)#service password- encryption
Habilitar el servidor HTTP	Comando: Para solucionar el servidor HTTP R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 Int f0/0 R2(config)#ip nat outside int f0/1 R2(config)#ip nat inside
Mensaje MOTD	R2(config)#Banner motd #unauthorized acces is strictly pohibited!# R2(config)#
Interfaz S0/0/0	Establezca la descripción interface serial 0/0/0 R2(config)#interface s0/0/0 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#no shutdown Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz int s0/0/0 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#ipv6 enable R2(config-if)#clock rate 128000 This command applies only to DCE interfaces R2(config-if)#no shutdown R2(config-if)#exit R2(config)#ipv6 unicast- routing ipv6 address 2001:DB8:ACAD:2::/64
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. int s0/0/1 ip address 172.16.2.1 255.255.255.0 R2(config)#interface s0/0/1

	R2(config-if)#ip address 172.16.2.1 255.255.255.0 R2(config-if)#no shutdown Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R2(config-if)#ipv6 address 2001:DB8:ACAD:3::/64 R2(config-if)#ipv6 enable R2(config-if)#clock rate 128000 This command applies only to DCE interfaces R2(config-if)#no shutdown
Interfaz G0/0 (simulación de Internet)	Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. ip address 209.165.200.236 255.255.255.250 Bad mask 0xFFFFFFFA for address 209.165.200.236 int g0/0 ip address 209.165.200.236 255.255.255.248 R2(config)#interface g0/0 R2(config-if)#ip address 209.165.200.236 255.255.255.250 R2(config-if)#no shutdown establezca la dirección IPv6. Utilizar la Primera dirección disponible en la subred. int G0/0 R2(config)#int G0/0 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown R2(config-if)#exit R2(config)#ipv6 unicast-routing

Interfaz loopback 0 (servidor web simulado)	Establecer la descripción. Establezca la direcciónPv4. R2#conf t R2(config)#interface loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#exit
Ruta predeterminada	Configure una ruta IPv4 predeterminada de G0/0. R2(config)# ip route 172.16.1.3 255.255.255.0 gigabitethernet 0/0 R2(config)#exit Configure una ruta IPv6 predeterminada de G0/0. R2(config)# ipv6 route ::/64 gigabiethernet 0/0 R2(config)#exit

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Configuración del Router 3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	Comando: R3(config)#no ip domain-lookup R3(config)#
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)# enable secret Class
Contraseña de acceso a la consola	R3(config)# line console 0 R3(config-line)#password Cisco R3(config-line)#login

Contraseña de acceso Telnet	R3(config)#line vty 0 4 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 # 'Unauthorized access is strictly prohibited!'#
Interfaz S0/0/1	Establecer la descripción interface serial 0/0/0 description 1 Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred: 172.16.2.0/30 R3(config)#interface s0/0/1 R3(config-if)#ip address 172.16.2.6 255.255.255.252 R3(config-if)#no shutdown Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. 2001:DB8:ACAD:2::/64 Activar la interfaz R3(config)#interface s0/0/1 R3(config-if)#ipv6 address 2001:db8:acad:2::3/64
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config)#interface lo4 R3(config-if)#ip address 192.168.4.2 255.255.255.0 R3(config-if)#no shutdown R3(config-if)#
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)#interface lo5 R3(config-if)#ip address 192.168.5.2 255.255.255.0 R3(config-if)#no shutdown

Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. R3(config-if)#interface lo6 R3(config-if)#ip address 192.168.6.2 255.255.255.0 R3(config-if)#no shutdown
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. R3(config-if)#interface lo7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64 R3(config-if)#no shutdown
Rutas predeterminadas	R3(config)#Ip route 0.0.0.0.0.0.0.0 s0/0/1 R3(config)#exit

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configuración swith 1

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	S1(config)#no ip domain-lookup S1(config)#
Nombre del switch	Switch(config)#hostname S1 S1(config)#
Contraseña de exec privilegiado cifrada	S1(config)#enable secret class S1(config)#
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 4 S1(config-line)#password cisco S1(config-line)#login

Cifrar las contraseñas de texto no cifrado	S1(config)#service password-encryption S1(config)#
Mensaje MOTD	S1(config)#banner motd #Se prohíbe el acceso no autorizado#

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7. Configuración swith 3

Elemento o tarea de configuración	**Especificación**
Desactivar la búsqueda DNS	S3#conf t S3(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3 S3(config)#
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 4 S3(config-line)#password cisco S3(config-line)#login S3(config-line)#end
Cifrar las contraseñas de texto no cifrado	Comando: S3(config)#service password-encryption

Mensaje MOTD	S3(config)#banner 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. Verificación de red

Desde	**A**	**Dirección IP**	**Resultados de ping**
R1	R2, S0/0/0	172.16.1.1	R1#ping 172,16,1,1
R2	R3, S0/0/1	172.16.2.2	R2#ping 172.16.2.2
PC de Internet	Gateway predeterminado	209.165.200.233	C:\>ping 209.165.200.233

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

Figura 2. Verificación de Ping en los R1 a R2

```
R1#ping 172.16.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/10 ms

R1#
```

Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Figura 3. Verificación de Ping de R2 a R3

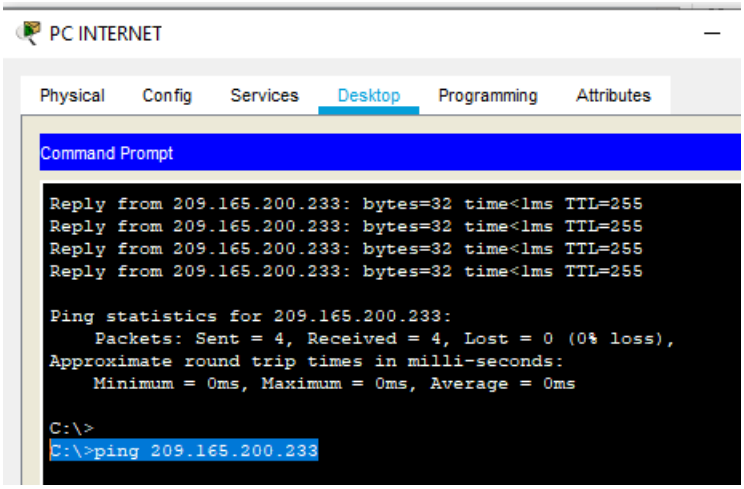
```
R2#ping 172.16.2.2

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 = 4/5/9 ms

R2#
```

Fuente: *Simulador Cisco Packet Tracer, captura tomada por el autor*

Figura 4. Verificación de Ping de PC INTERNET al Gateway Predeterminado



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

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. Seguridad del switches 1 de VLAN

Elemento o tarea de configuración	**Especificación**

Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indica. 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 ADMINISTRATIVO S1(config-vlan)#exit
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología Ingresamos el siguiente código S1(config)#int vlan 99 S1(config-if)#ip address 192.168.99.1 255.255.255.0 S1(config)#int vlan 21 S1(config-if)#ip address 192.168.21.1 255.255.255.0 S1(config)#int vlan 23 S1(config-if)#ip address 192.168.23.1 255.255.255.0
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. Comando: S1(config)#ip default-gateway 192.168.199.3 S1(config)#
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN native Comando: S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1

Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN native Comando: S1(config)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1 S1(config-if)#
Configurar el resto de los puertos como puertos de acceso	Comando: S1(config)#int range f0/2, f0/4, f0/6-23 switch mode access int f0/1 S1(config-if-range)#shutdown
Asignar F0/6 a la VLAN 21	S1(config)#interface f0/6 S1(config-if)#no shutdown S1(config-if)#switchport mode access S1(config-if)#switchport access vlan 21
Apagar todos los puertos sin usar	Ingresamos el siguiente código: S1(config)#int range f0/1-24 S1(config-if-range)#shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Seguridad del switch 3 de VLAN

Elemento o tarea de configuración	**Especificación**
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada 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 ADMINISTRATIVO S3(config-vlan)#exit

Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología S3(config)#int vlan 99 S3(config-if)#ip add 192.168.99.2 255.255.255.0 S3(config)#int vlan 21 S3(config-if)#ip add 192.168.21.2 255.255.255.0 S3(config)#int vlan 23 S3(config-if)#ip add 192.168.23.2 255.255.255.0
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado. S3(config)#ip default-gateway 192.168.199.2 S3(config)#
Forzar el enlace troncal en la interfaz F0/3	S3(config)# interface fastethernet0/3 S3(config-if)# switchport mode trunk S3(config-if)# switchport trunk native vlan 1 S3(config-if)# switchport trunk allowed vlan 21,23,99 S3(config-if)# end S3#
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range S3(config)#int range fa0/1-2, fa0/4-24 switchport mode access
Asignar F0/18 a la VLAN 23	Coamando: S3(config)#interface f0/18 S3(config-if)#no shutdown S3(config-if)#switchport mode access S3(config-if)#switchport access vlan 23 S3(config-if)#

Apagar todos los puertos sin usar	Comando: S3(config)#int range f0/1-2, f0/4-17, f0/19-24

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configuración del Router de la subinterfaz

Elemento o tarea de configuración	**Especificación**
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Comando: R1(config)#interface g0/1.21 R1(config-subif)#encapsulation dot1q 21 Asignar la primera dirección disponible a esta interfaz encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.4 255.255.255.0
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Comando R1(config-subif)#interface g0/1.23 R1(config-subif)#encapsulation dot1q 23 Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz encapsulation dot1Q 23 R1(config-subif)#iip add 192.168.23.4 255.255.255.0

Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración R1(config-subif)#interface g0/1.99 R1(config-subif)#encapsulation dot1q 99 description LAN de Administracion encapsulation dot1Q 99 Asignar la primera dirección disponible a esta interfaz R1(config-subif)#ip add 192.168.99.4 255.255.255.0
Activar la interfaz G0/1	R1(config-subif)# interface g0/1 R1(config-if)#no shutdown

Paso 4: Verificar la conectividad de la red

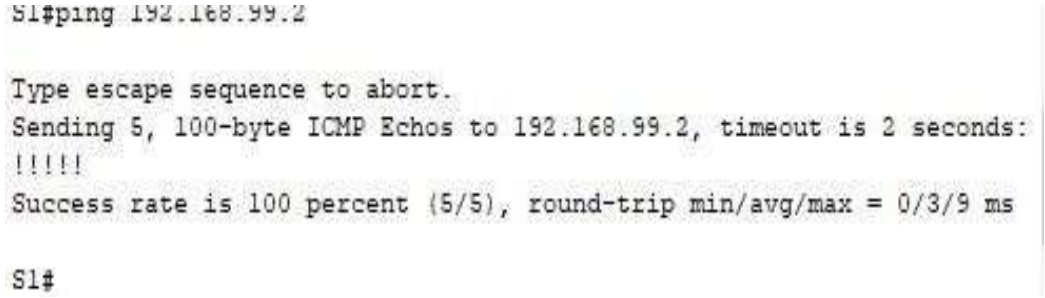
Utilice el comando **ping** para probar la conectividad entre los switches y el R1. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red.

Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Tabla 12. Verificación de la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.2	S1#Ping 192.168.99.2
S3	R1, dirección VLAN 99	192.168.99.2	S3#Ping 192.168.99.2
S1	R1, dirección VLAN 21	192.168.21.1	S1#Ping 192.168.21.1
S3	R1, dirección VLAN 23	192.168.23.2	S3#Ping 192.168.23.2

Figura 5. Verificación de conectividad en S1 al R1 del packet tracer



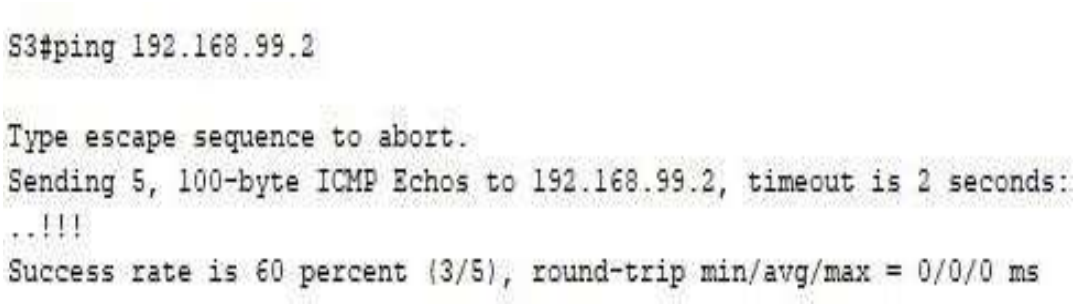
```
S1#ping 192.168.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/3/9 ms

S1#
```

Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor.

Figura 6. Verificación de conectividad en S3 al R1 del packet tracaer



```
S3#ping 192.168.99.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms
```

Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor.

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. Configuración el protocolo de routing 1, dinámico RIPv2

Elemento o tarea de	**Especificación**
Configurar RIP versión	Comando: router ospf 1

Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente. R1(config)#router ospf 10 R1(config-router)#router-id 2.2.2.2 R1(config-router)#network 192.168.21.0 0.0.0.255 area 0 R1(config-router)#network 192.168.23.0 0.0.0.255 area 0 R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
Establecer todas las interfaces LAN como pasivas	Comando: R1(config-router)# passive-interface g0/1
Desactive la sumarización automática	Utilizamos el código: R1(config-router)# no auto summary R1(config-router)#end

Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Configuración del protocolo de routing 2, dinámico RIPv2

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	R1(config)#router ospf 1
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.

Establecer la interfaz LAN (loopback) como pasiva	R2(config)#router ospf 2 R2(config-router)#router-id 2.2.2.2 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 R2(config-router)#network 172.16.2.0 0.0.0.3 area 0 R2(config-router)#network 10.10.10.10 0.0.0.255 area 0 R2(config-router)#passive-interface lo0
Desactive la sumarización automática.	R2(config-router)# no auto summary R2(config-router)#end

Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configuración del protocolo de routing 3, dinámico RIPv3

Elemento o tarea de configuración	**Especificación**
Configurar RIP versión 2	router ospf 1
Anunciar redes IPv4 conectadas directamente	R3(config-router)#network 172.16.3.0 0.0.0.3 area 0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#network 192.168.4.0 0.0.3.255 area 0 R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6 R3(config-router)#end
Desactive la sumarización automática.	R3(config-router)# no auto summary R3(config-router)#end

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?	R3#show ip ospf neig
¿Qué comando muestra solo las rutas RIP?	R3#show ip ospf interface
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	R3#Show ip protocols

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. Implementación DHCP y NAT para IPv4 en el router 1

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)#iip dhcp excluded-address 192.168.23.1 192.168.23.20

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 Comando: R1(config)#ip dhcp pool contabilidad R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com R1(config)#ip dhcp pool ACCT R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#exit
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 R1(config)#ip dhcp pool ENGR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#ip domain-name ccna-sa.com R1(config)#ip dhcp pool ingeniería R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0

Paso 2 Configurar la NAT estática y dinámica en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 18. Configuración de la NAT estática y dinámica en el R2

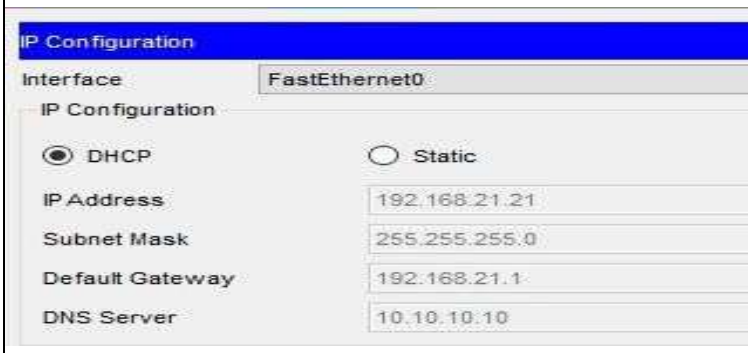
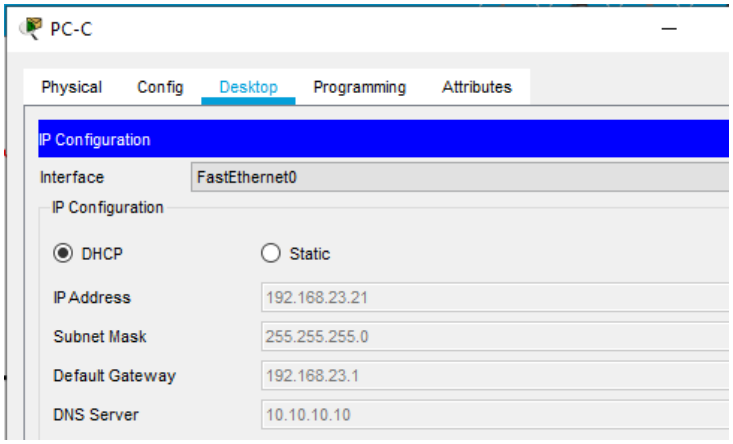
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15** R2(config)#User usuarioweb privilege 15 secret cisco12345 R2(config)#
Habilitar el servicio del servidor HTTP	R2(config)#ip http server (no se puede configurar en packet tracer)
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.99.0 0.0.0.255
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229** R2(config)#Ip nat inside source static 10.10.10.10 209.165.200.229
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 g0/0 R2(config-if)#ip nat inside R2(config-if)#end

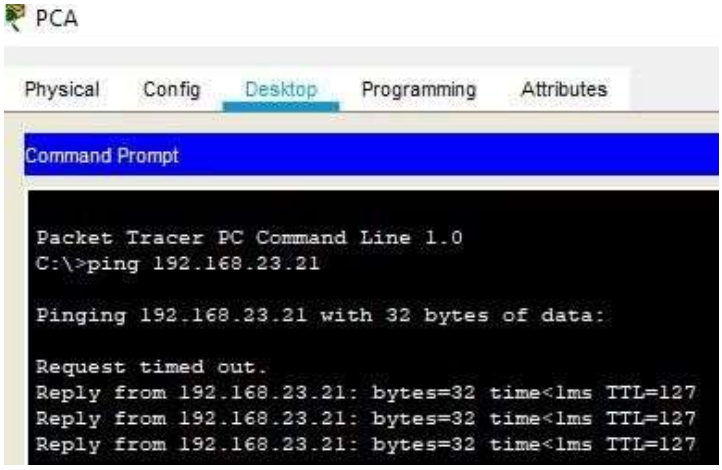
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3 R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: **INTERNET** El conjunto de direcciones incluye: **209.165.200.225** –**209.165.200.228** R2(config#Ip nat pool internet 209.165.200.225 209.165.200.228 netmask 255.255.255.248
Definir la traducción de NAT dinámica	R2(config)#Ip nat inside source list 1 pool internet ip nat pool Internet 209.165.200.229 209.165.200.228 netmask 255.255.255.248

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 el protocolo DHCP y la NAT estática

Prueba	**Resultado**
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	Figura 7. Verificación de la PC-A información de IP del servidor de DHCP  **Fuente:** Simulador Cisco Packet Tracer, captura tomada por el autor
Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	Figura 8. Verificación de la PC-A información de IP del servidor de DHCP  **Fuente:** Simulador Cisco Packet Tracer, captura tomada por el autor.

Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.	Figura 9. Verificación que la PC-A pueda hacer ping a la PC-C  **Fuente:** Simulador Cisco Packet Tracer, captura tomada por el autor.
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229), iniciar sesión con el nombre de ususario **webuser** y la contraseña **cisco12345**	Figura 10. Inicio de sesión desde el servicor web  **Fuente:** Simulador Cisco Packet Tracer, captura tomada por el autor

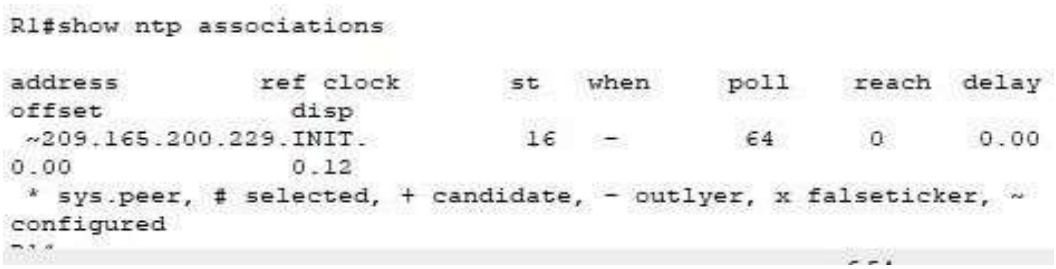
Parte 6: Configurar NTP

Tabla 20. Configuración NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	clock set 09:00:00 mar 05 2016
Configure R2 como un maestro NTP.	Nivel de estrato: **5**
Configurar R1 como un cliente NTP.	Servidor: **R2**

configure R1 para actualizaciones de calendario dicas con hora NTP.	ntp server 209.165.200.229
Verifique la configuración de NTP en R1.	R1#show ntp associations

Figura 11. Verifique la configuración de NTP en R1.



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Parte 7: Configurar y verificar las listas de control de acceso

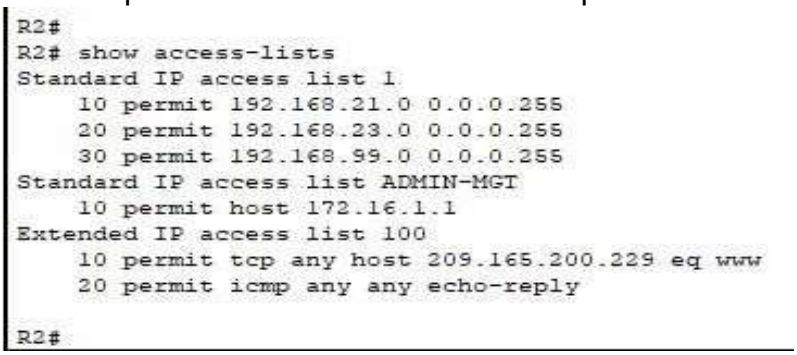
(ACL) Paso Restringir el acceso a las líneas VTY en el R2

Tabla 21. Configuración y verificación las listas de control de acceso (ACL)

Elemento o tarea de configuración	**Especificación**
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: **ADMIN-MGT** R2(config)#ip Access-list standard ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	R2(config-std-acl)#permit host 172.16.1.1 R2(config-std-acl)#exit
Permitir acceso por Telnet a las líneas de VTY	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in R2(config-line)#exit

Verificar que la ACL funcione como se espera	Comando: R2#show access-lists

Figura 12. Verificar que la ACL funcione Como se espera



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

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

Tabla 22. Comando de CLI

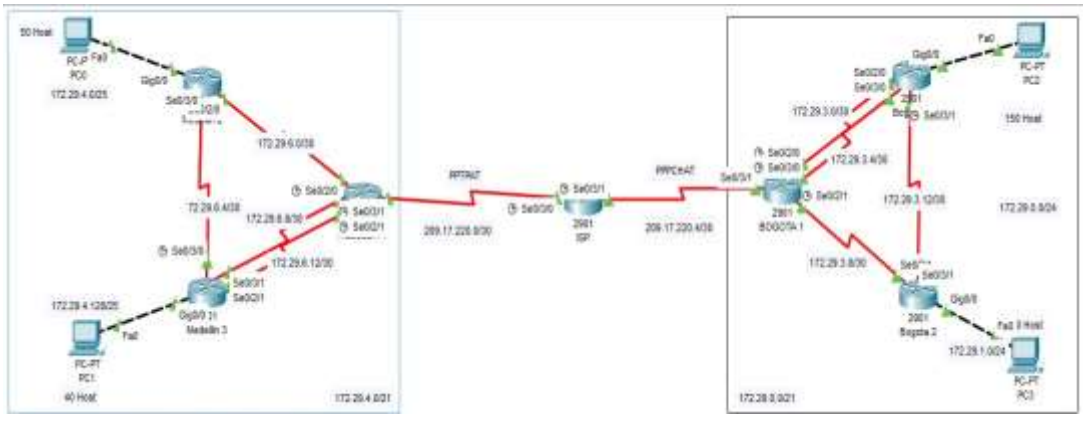
Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	R2#show access-list R2#show access-list Standard IP access list 1 10 permit 192.168.21.0 0.0.0.255 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 R2#
Restablecer los contadores de una lista de acceso	R2#clear 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 translations **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?	Comando R2#clear ip nat translation

7 . 2 ESCENARIO 2

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

Gráfica 2. Topología de red Escenario 2



Fuente: *Simulador Cisco Packet Tracer 7.3, captura tomada por el autor*

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.

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.

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.
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.
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.

Parte 2: Tabla de Enrutamiento.

a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
b. Verificar el balanceo de carga que presentan los routers.
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.

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.

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

Parte 4: Verificación del protocolo OSPF.

a. 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.

b. 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.

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

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.

Parte 7: Configuración del servicio DHCP.

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

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

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

d. Configure el router Bogotá1 para que habilite el paso de los mensajes
Broadcast hacia la IP del router Bogotá2.
Comenzamos con el desarrollo del escenario 2 de acuerdo a la problemática planteada.

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.

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.
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.

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.

Comandos ejecutados en el Router ISP:

```
Router>en
Router#conf t
Router(config)#hostna
me ISP
```

Configuramos interfaz

s0/0

```
ISP(config)#int s0/0
ISP(config-if)#description ISP-MEDELLIN1
ISP(config-if)#ip add 209.17.220.1 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shu
ISP(config-if)#exit
```

Configuramos la otra interfaz

s0/1

```
ISP(config)#int s0/1
ISP(config-if)#description ISP-BOGOTA1
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
```

ISP(config-if)#no shu
ISP(config-if)#exit

Configuramos el Protocolo OSPF V2

ISP(config-router)#router ospf
ISP(config-router)#version 2
ISP(config-router)#network 209.17.220.0

Desactivamos la Sumarización automática

ISP(config-router)#no auto-summary

Comandos ejecutados en el Router MEDELLIN1:

Router>en Router#conf t
Router(config)#hostname
MEDELLIN1

Configuramos interfaz s0/0 (Ruta por defecto
al ISP) MEDELLIN1(config)#interface Serial0/0
MEDELLIN1(config-if)#description MEDELLIN1-ISP
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#shutdown
MEDELLIN1(config-if)#exit

Configuramos interfaz s0/1

MEDELLIN1(config)#interface Serial0/1
MEDELLIN1(config-if)# description MEDELLIN1-
MEDELLIN MEDELLIN1(config-if)#ip address
172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shu
MEDELLIN1(config-if)#exit

Configuramos interfaz s0/2

MEDELLIN1(config)#interface Serial0/2
MEDELLIN1(config-if)# description MEDELLIN-MEDELLIN1
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252

MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shu
MEDELLIN1(config-if)#exit

Configuramos interfaz s0/3

MEDELLIN1(config)#interface Serial0/3
MEDELLIN1(config-if)# description MEDELLIN1-MEDELLIN2
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shu
MEDELLIN1(config-if)#exit

Configuramos el Protocolo OSPF V2

MEDELLIN1(config-router)#router ospf
MEDELLIN1(config-router)#version 2
MEDELLIN1(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática

MEDELLIN1(config-router)#no auto-summary

Comandos ejecutados en el Router MEDELLIN2:

Router>en Router#conf t
Router(config)#hostname
MEDELLIN2

Configuramos interfaz s0/0

MEDELLIN2(config)#interface Serial0/0
MEDELLIN2(config-if)#description MEDELLIN2-MEDELLIN1
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#shutdown
MEDELLIN2(config-if)#exit

Configuramos interfaz s0/1

MEDELLIN2(config)#interface Serial0/1
MEDELLIN2(config-if)# description MEDELLIN2-
MEDELLIN MEDELLIN2(config-if)#ip address
172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000

MEDELLIN2(config-if)#no shu
MEDELLIN2(config-if)#exit

Configuramos interfaz fa0/0

MEDELLIN2(config)#interface fa0/0
MEDELLIN2(config-if)# description MEDELLIN2-PC2
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shu
MEDELLIN2(config-if)#exit

Configuramos el Protocolo RIP V2

MEDELLIN2(config-router)#router rip
MEDELLIN2(config-router)#version 2
MEDELLIN2(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática

MEDELLIN2(config-router)#no auto-summary

Comandos ejecutados en el Router MEDELLIN:

Router>en Router#conf t
Router(config)#hostname
MEDELLIN

Configuramos interfaz s0/0

MEDELLIN(config)#interface Serial0/0
MEDELLIN(config-if)#description MEDELLIN-MEDELLIN1
MEDELLIN(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN(config-if)#clock rate 128000
MEDELLIN(config-if)#shutdown
MEDELLIN(config-if)#exit

Configuramos interfaz s0/1

MEDELLIN(config)#interface Serial0/1
MEDELLIN(config-if)#description MEDELLIN1-
MEDELLIN MEDELLIN(config-if)#ip address
172.29.6.10 255.255.255.252
MEDELLIN(config-if)#clock rate 128000

MEDELLIN(config-if)#no shu
MEDELLIN(config-if)#exit

Configuramos interfaz s0/2
MEDELLIN(config)#interface Serial0/2
MEDELLIN(config-if)#description MEDELLIN-MEDELLIN2
MEDELLIN(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN(config-if)#clock rate 128000
MEDELLIN(config-
if)#no shu
MEDELLIN(config-
if)#exit

Configuramos interfaz fa0/0
MEDELLIN(config)#interface fa0/0
MEDELLIN(config-if)#description MEDELLIN-PC3
MEDELLIN(config-if)#ip address 172.29.4.2 255.255.255.128
MEDELLIN(config-if)#clock rate 128000
MEDELLIN(config-if)#no shu
MEDELLIN(config-if)#exit

Configuramos el Protocolo OSPF V2
MEDELLIN(config-router)#router ospf
MEDELLIN(config-router)#version 2
MEDELLIN(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática
MEDELLIN(config-router)#no auto-summary

Comandos ejecutados en el Router BOGOTA1:

Router>en Router#conf t
Router(config)#hostname BOGOTA1

Configuramos interfaz s0/0 (Ruta por defecto
al ISP) BOGOTA1(config)#interface Serial0/0
BOGOTA1(config-if)#description BOGOTA1-ISP
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#shutdown

BOGOTA1(config-if)#exit

Configuramos interfaz s0/1
BOGOTA1(config)#interface Serial0/1
BOGOTA1(config-if)#description BOGOTA1-BOGOTA2
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shu
BOGOTA1(config-if)#exit

Configuramos interfaz s0/2
BOGOTA1(config)#interface Serial0/2
BOGOTA1(config-if)#description BOGOTA2-BOGOTA1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shu
BOGOTA1(config-if)#exit

Configuramos interfaz s0/3
BOGOTA1(config)#interface Serial0/3
BOGOTA1(config-if)#description BOGOTA1-BOGOTA
BOGOTA1(config-if)#ip address 172.29.3.9
255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shu
BOGOTA1(config-if)#exit

Configuramos el Protocolo RIP V2
BOGOTA1(config-router)#router rip
BOGOTA1(config-router)#version 2
BOGOTA1(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática
BOGOTA1(config-router)#no auto-summary

Comandos ejecutados en el Router BOGOTA2:
Router>en
Router#conf t
Router(config)#hostname BOGOTA2
Configuramos interfaz s0/0

BOGOTA2(config)#interface Serial0/0
BOGOTA2(config-if)#description BOGOTA2-BOGOTA1
BOGOTA2(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#shutdown
BOGOTA2(config-if)#exit

Configuramos interfaz s0/1
BOGOTA2(config)#interface Serial0/1
BOGOTA2(config-if)#description BOGOTA1-BOGOTA2
BOGOTA2(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shu
BOGOTA2(config-if)#exit

Configuramos interfaz s0/2
BOGOTA2(config)#interface Serial0/2
BOGOTA2(config-if)#description BOGOTA2-BOGOTA
BOGOTA2(config-if)#ip address 172.29.3.13
255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shu
BOGOTA2(config-if)#exit

Configuramos interfaz fa0/0
BOGOTA2(config)#interface fa0/0
BOGOTA2(config-if)#description BOGOTA2-PC0
BOGOTA2(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shu
BOGOTA2(config-if)#exit

Configuramos el Protocolo RIP V2
BOGOTA2(config-router)#router rip
BOGOTA2(config-router)#version 2
BOGOTA2(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática
BOGOTA2(config-router)#no auto-summary
Comandos ejecutados en el Router BOGOTA:

Router>en
Router#conf t Router(config)#hostname
BOGOTA

Configuramos interfaz s0/0
BOGOTA(config)#interface Serial0/0
BOGOTA(config-if)#description BOGOTA-BOGOTA1
BOGOTA(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA(config-if)#clock rate 128000
BOGOTA(config-if)#shutdown
BOGOTA(config-if)#exit

Configuramos interfaz s0/1
BOGOTA(config)#interface Serial0/1
BOGOTA(config-if)#description BOGOTA-BOGOTA2
BOGOTA(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA(config-if)#clock rate 128000
BOGOTA(config-if)#no shu
BOGOTA(config-if)#exit

Configuramos interfaz fa0/0
BOGOTA(config)#interface fa0/0
BOGOTA(config-if)#description BOGOTA-PC1
BOGOTA(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA(config-if)#clock rate 128000
BOGOTA(config-if)#no shu
BOGOTA(config-if)#exit

Configuramos el Protocolo OSPF V2
BOGOTA(config-router)#router ospf
BOGOTA(config-router)#version 2
BOGOTA(config-router)#network 172.29.0.0

Desactivamos la Sumarización automática
BOGOTA(config-router)#no auto-summary

Comandos usados para la ruta estática
en ISP: ISP>en
ISP#conf t
ISP(config)#ip route 172.29.4.0 255.255.252.0 s0/0
ISP(config)#ip route 172.29.0.0 255.255.252.0 s0/1

ISP(config)#ip route 172.29.4.128 255.255.255.128 s0/0
ISP(config)#ip route 172.29.1.0 255.255.255.0 s0/1
ISP(config)#exit

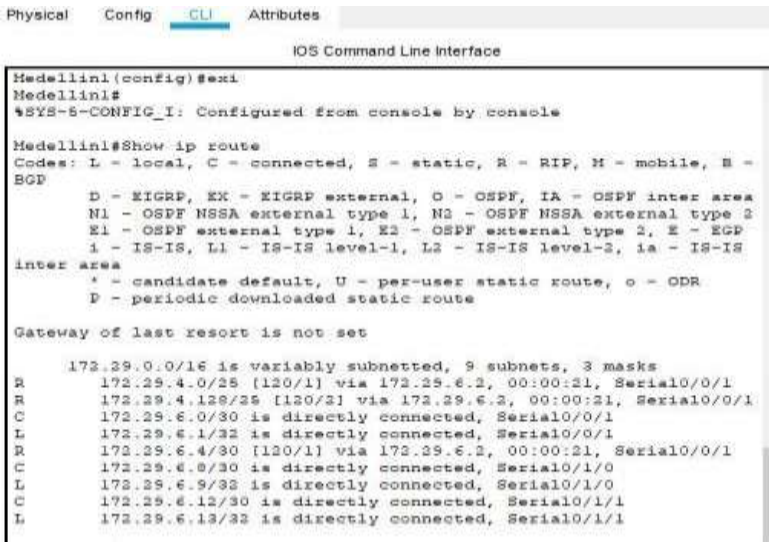
Comandos usados para la ruta estática predeterminada hace la red de MEDELLIN:

MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#exit

Parte 2.Tabla de enrutamiento

Enrutamiento de MEDELLIN: Desde PC2 a PC3

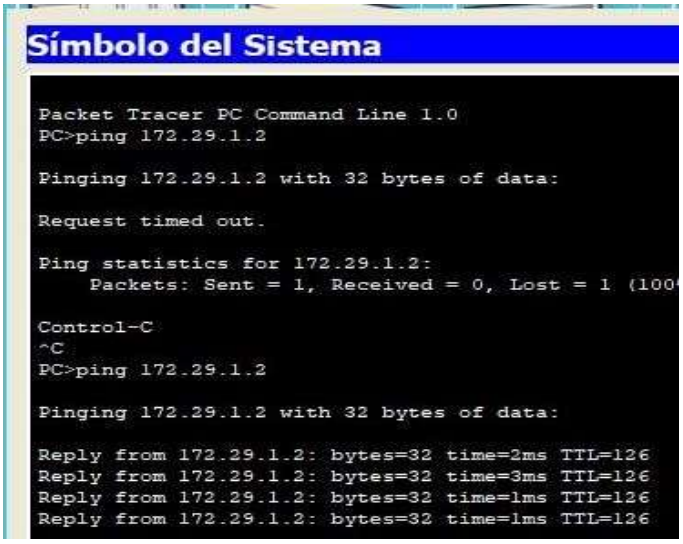
Figura 13. Enrrutamiento



Fuente: Simulador Cisco Packet Tracer, captura tomada del autor

Comandos usados para la ruta estática predeterminada hace la red de
BOGOTA:
BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#exit

Figura 14. Ping PC0 a PC1



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

Comandos de propagación de OSPF, para los router de MEDELLIN1, MEDELLIN 2, MEDELLIN 3, BOGOTÁ 1, BOGOTA 2 y BOGOTA 3, se debe tener en cuenta si es un puerto serial o FastEthernet.

Figura 15. Propagación de ospf

Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor.

Parte 4: Verificación del protocolo OSPF.

a. 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.

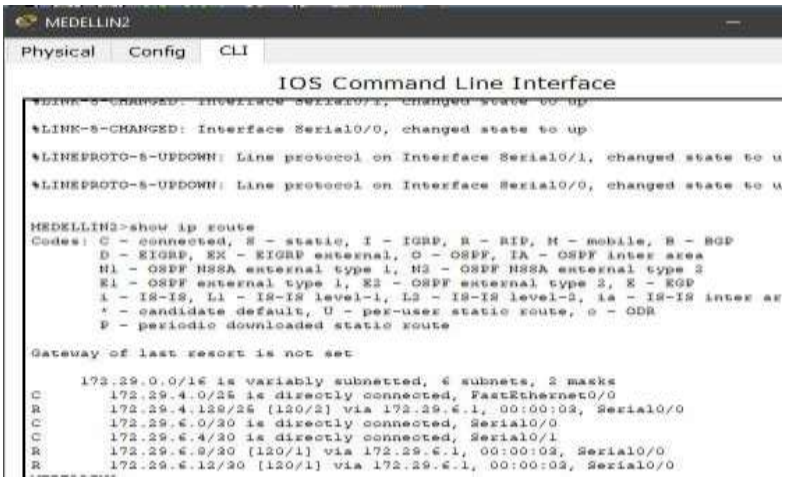
b. Verificar y documentar la base de datos de OSPF de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Verificación del commando show ip route en el router

Figura 16. MEDELLIN1#show ip route

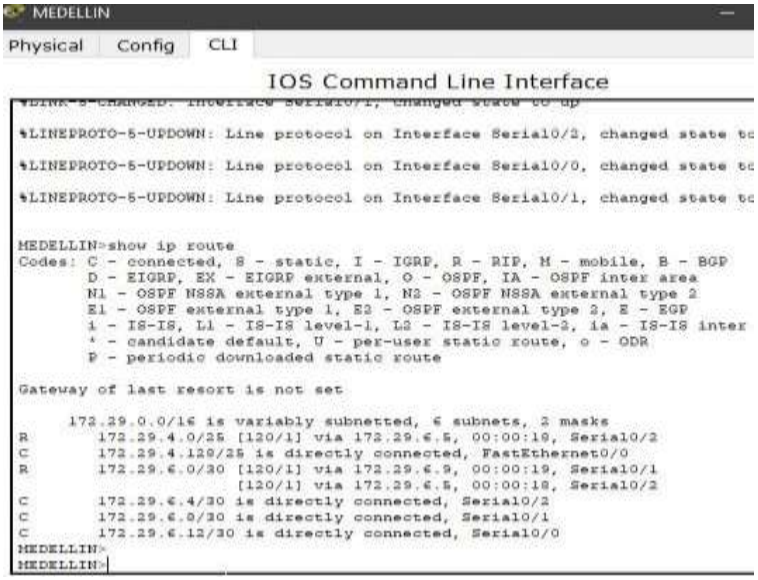
Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor.

Figura 17. MEDELLIN2#show ip route



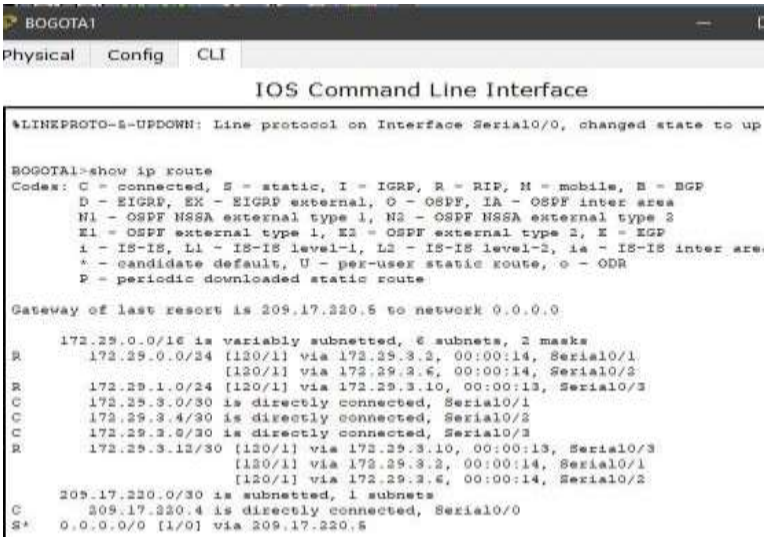
Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Figura 18. MEDELLIN#show ip route



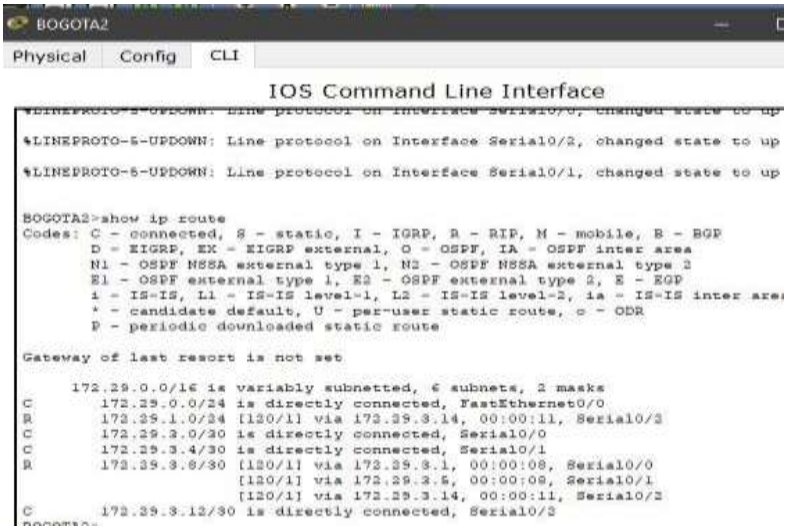
Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Figura 19. BOGOTA1# show ip route



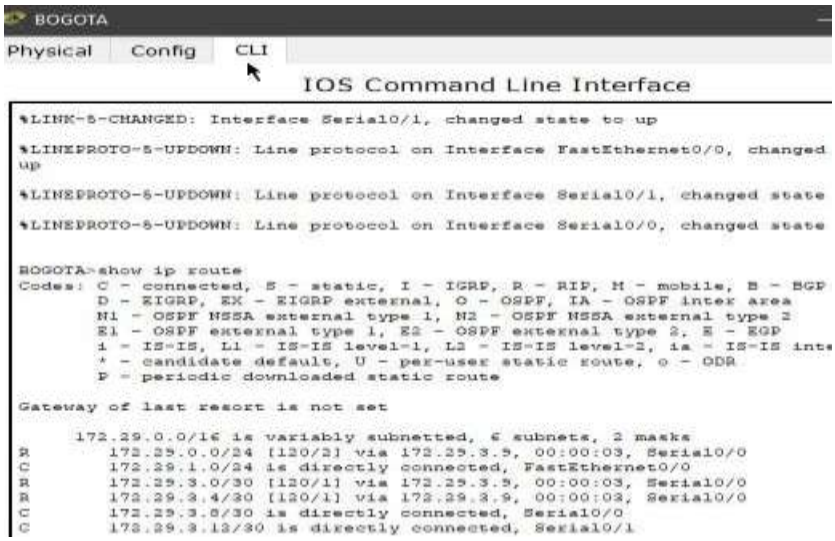
Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Figura 20. BOGOTA2#show ip route



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Figura 21. BOGOTA#show ip route



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Habilitación método encapsulamiento PPP:

MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#int
s0/0
MEDELLIN1(config-if)#encapsulation PPP
MEDELLIN1(config-if)#no shu
MEDELLIN1(config-if)#exit

BOGOTA1>en
BOGOTA1#conf t BOGOTA1(config)#int s0/0
BOGOTA1(config-if)#encapsulation
PPP BOGOTA1(config-if)#no shu
BOGOTA1(config-if)#exit

ISP>en ISP#conf t
ISP(config)#int s0/0

ISP(config-if)#encapsulation
PPP ISP(config-if)#no shu
ISP(config-if)#exit
ISP(config)#int s0/1
ISP(config-if)#encapsulation
PPP ISP(config-if)#no shu

Habilitación autenticación PAT DE PPP entre MEDELLIN1 Y EL

ISP: Configuración PAT DE PPP en ISP CON MEDELLIN1:

ISP>en ISP#conf t
ISP(config)#username

MEDELLIN1 secret
MEDELLIN ISP(config)#int se0/0

ISP(config-if)#PPP authentication PAT
ISP(config-if)#PPP PAT sent-username ISP
password ISP
ISP(config-if)#exit

Configuración PAT de PPP en MEDELLIN1 CON ISP:
MEDELLIN1>en
MEDELLIN1#conf t
MEDELLIN1(config)#username ISP
secret ISP MEDELLIN1(config)#int se0/0
MEDELLIN1(config-if)#PPP authentication PAT
MEDELLIN1(config-if)#PPP PAT sent-username
MEDELLIN1 password MEDELLIN
MEDELLIN1(config-if)#exit

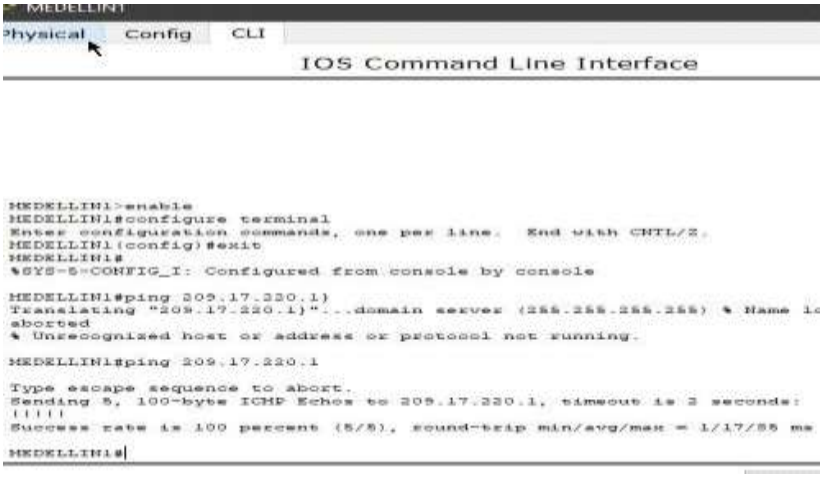
Habilitación autenticación CHAT DE PPP entre BOGOTA1 Y EL

ISP: Configuración CHAT DE PPP en ISP CON BOGOTA1:

ISP>en
ISP#conf t
ISP(config)#usernameBOGOTA1 secret BOGOTA1
ISP(config)#int se0/1
ISP(config-if)#PPP authentication
CHAT ISP(config-if)#exit
Configuración CHAT de PPP en BOGOTA1 CON ISP:

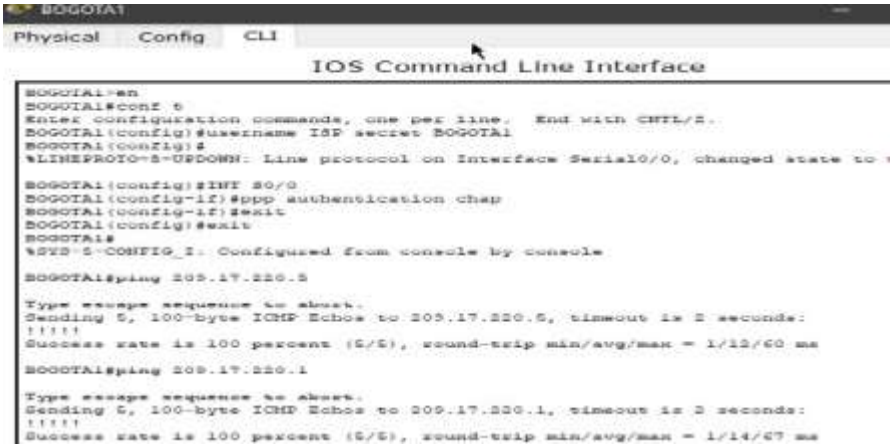
BOGOTA1>en
BOGOTA1#conf t
BOGOTA1(config)#username ISP secret BOGOTA1
BOGOTA1(config)#int se0/0
BOGOTA1(config-if)#PPP authentication
CHAT BOGOTA1(config-if)#exit

Figura 22. Verificación de autenticación PAT EN MEDELLIN Por ping hacia ISP



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Figura 23. Verificación de autenticación CHAP EN BOGOTA1 Por ping hacia ISP



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

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.

Configuración NAT en MEDELLIN1:

MEDELLIN1>en
MEDELLIN1#conf t

Con este comando definidos la red de los PC's que se desean que sean empleadas en el PAT"

MEDELLIN1(config)#ip access-list standard HOST
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
MEDELLIN1(config-std-nacl)#exit

Una vez creada la ACL, definimos la interfaz de salida del NAT, utilizando el método recargado que permite el PAT de muchos usuarios por la misma IP"

MEDELLIN1(config)#Ip nat inside source list HOST interface s0/0 overload
MEDELLIN1(config)#int s0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit

MEDELLIN1(config)#int s0/2
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/3
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#exit
MEDELLIN1#show ip nat translation

Iniciamos con la configuración NAT en BOGOTA1:

BOGOTA1>en
BOGOTA1#conf t

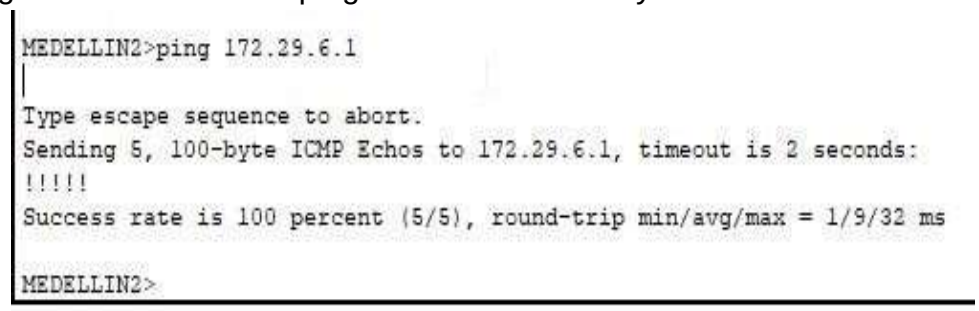
A continuación con el siguiente comando definidos la red de los PC's que se desean que sean empleadas en el PAT"

BOGOTA1(config)#ip access-list standard HOST BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config-std-nacl)#exit
Despues de crear la ACL, definimos la interfaz de salida del NAT, utilizando el método recargado que permite el PAT de muchos usuarios por la misma IP"

BOGOTA1(config)#Ip nat inside source list HOST interface s0/0 overload
BOGOTA1(config)#int s0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#exit
BOGOTA1|(config)#int s0/1

BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/2
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#exit
BOGOTA1(config)#int s0/3
BOGOTA1(config-if)#ip nat inside BOGOTA1
(config-if)#exit
BOGOTA1(config)#exit
BOGOTA1#show ip nat translation

Figura 24. Verificamos ping entre MEDELLIN2 y MEDELLIN1



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Parte 7: Configuración del servicio DHCP.

a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.
b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.
d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

Configurando en DHCP en el Router MEDELLIN2

MEDELLIN2>en
MEDELLIN2#conf t

Deficición del pool de direcciones ip del DHCP

MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.3
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132
MEDELLIN2(dhcp-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 8.8.4.4
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MEDELLIN

Definimos la red de IP's que serán arrendadas cuando el host solicite una IP.

MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128

Definimos la dirección del Gateway para los Host.

MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.4.4
MEDELLIN2(dhcp-config)#exit

Continuamos configurando el DHCP, como el router MEDELLIN tiene una red LAN conectada pero no realizara las veces de servidor DHCP, es necesario configurar "ip helper" el cual permitirá ser un router de tránsito para llegar al router con el roll de DHCP. Por lo anterior utilizamos el comando ip helper- addres para atrapar los broadcasts y redireccionarlos hacia la ip del router de MEDELLIN2:

MEDELLIN>en MEDELLIN#conf t
MEDELLIN(config)#Int fa0/0
MEDELLIN(config-if)#ip helper-addres 172.29.6.5
MEDELLIN(config-if)#exit

Iniciamos configurando en DHCP en el Router BOGOTA2

BOGOTA2>en
BOGOTA2#conf t

Definició del pool de direcciones ip del DHCP

BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.4
BOGOTA2(dhcp-config)#ip dhcp pool BOGOTA2
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 8.8.4.4
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#ip dhcp pool BOGOTA

-Definimos la red de IP's que serán arrendadas cuando el host solicite una IP.

BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0

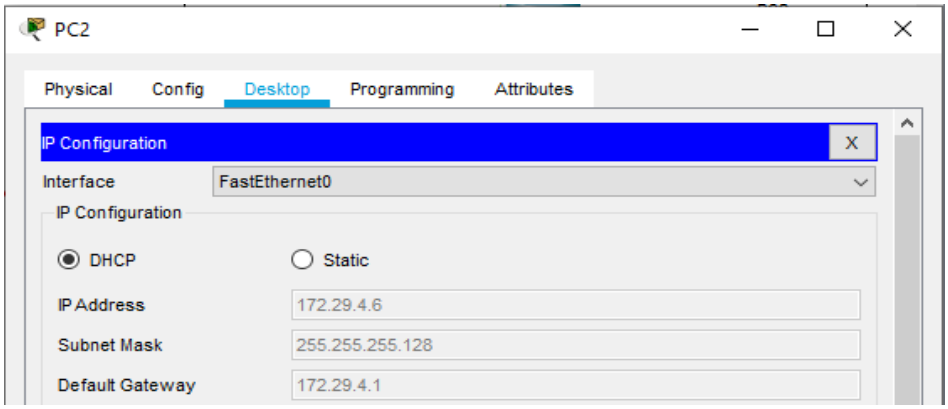
-Definimos la dirección del Gateway para los Host.

BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.4.4
BOGOTA2(dhcp-config)#exit

Continuamos configurando el DHCP, como el router BOGOTA tiene una red LAN conectada pero no realizara las veces de servidor DHCP, es necesario configurar “ip helper” el cual permitirá ser un router de tránsito para llegar al router con el roll de DHCP. Por lo anterior utilizamos el comando ip helper- addres para atrapar los broadcasts y redireccionarlos hacia la ip del router de BOGOTA2:

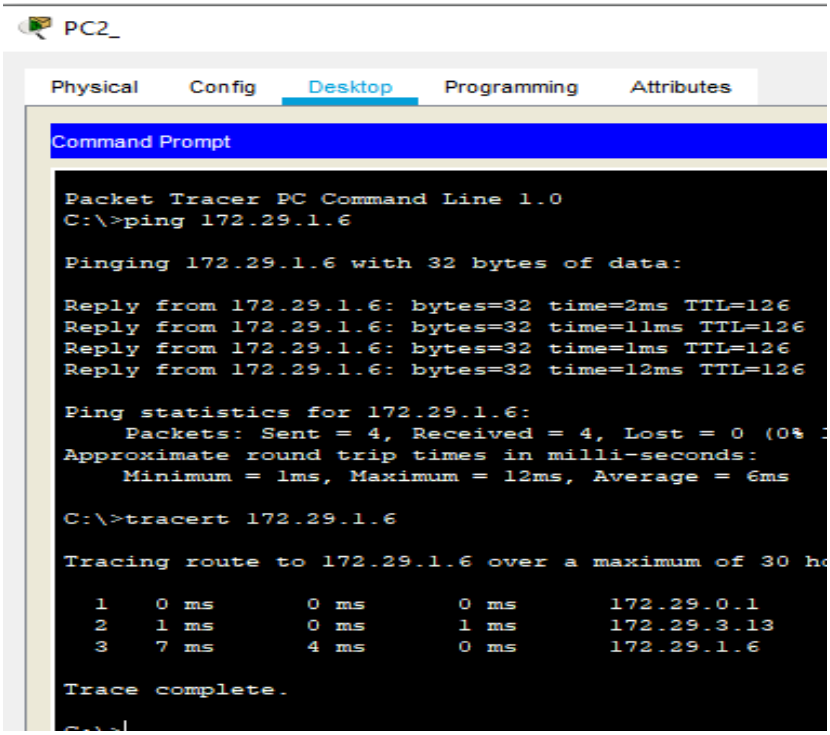
BOGOTA>en BOGOTA#conf t
BOGOTA(config)#Int fa0/0
BOGOTA(config-if)#ip helper-addres 172.29.3.13
BOGOTA(config-if)#exit

Figura 25. DHCP Medellín



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Figura 26. Ping PC2 a PC3



Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

Por ultimo se asignan claves de seguridad a cada router, este paso se realiza de ultimo para agilizar el acceso a los router mientras se hacían los demás puntos.

Configuración de claves de seguridad

Router ISP:
ISP>en
ISP#conf t
ISP(config)#enable secret ISP
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login ISP(config-
line)#exit ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#service password-encryption

ISP(config)#banner motd #Prohibido el acceso no autorizado!#
ISP(config)#exit

Router MEDELLIN1:

MEDELLIN1>en
MEDELLIN1#consf t MEDELLIN1(config)#enable secret MEDELLIN1
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login MEDELLIN1(config-line)#exit
MEDELLIN1(config)#line vty 0 4
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login MEDELLIN1(config-line)#exit
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#banner motd #Prohibido el acceso no autorizado!#
MEDELLIN1(config)#exit

Configuración MEDELLIN2>en
MEDELLIN2#conf t
MEDELLIN2(config)#enable secretMEDELLIN2
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login

MEDELLIN2(config-line)#exit
MEDELLIN2(config)#line vty 0 4
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#banner motd #Prohibido el acceso no autorizado!#
MEDELLIN2(config)#exit

Router MEDELLIN:

MEDELLIN>en
MEDELLIN#conf t
MEDELLIN(config)#enable secret MEDELLIN
MEDELLIN(config)#line console 0
MEDELLIN(config-line)#password cisco
MEDELLIN(config-line)#login MEDELLIN(config-line)#exit
MEDELLIN(config)#line vty 0 4
MEDELLIN(config-line)#password cisco

MEDELLIN(config-line)#login MEDELLIN(config-line)#exit
MEDELLIN(config)#service password-encryption
MEDELLIN(config)#banner motd #Prohibido el acceso no autorizado!#
MEDELLIN(config)#exit

Router BOGOTA1:

BOGOTA1>en BOGOTA1#conf t BOGOTA1(config)#enable secret BOGOTA1
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login BOGOTA1(config-line)#exit
BOGOTA1(config)#line vty 0 4
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login BOGOTA1(config-line)#exit
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#banner motd #Prohibido el acceso no autorizado!#
BOGOTA1(config)#exit

Router BOGOTA2:

BOGOTA2>en BOGOTA2#conf t
BOGOTA2(config)#enable secret BOGOTA2
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#exit
BOGOTA2(config)#line vty 0 4
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#exit
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#banner motd #Prohibido el acceso no autorizado!#
BOGOTA2(config)#exit

Router BOGOTA:

BOGOTA>en
BOGOTA#conf t
BOGOTA(config)#enable secret BOGOTA
BOGOTA(config)#line console 0
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#line vty 0 4
BOGOTA(config-line)#password cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit

BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd #Solo Personal autorizado!#
BOGOTA(config)#exit

Figura 27. Routing Bogotá

Fuente: Simulador Cisco Packet Tracer, captura tomada por el autor

CONCLUSIONES

Con el desarrollo de esta actividad practica se logró diseñar y configurar una red LAN de manera local y una red WAN o área extendiada desde la cuidad de Medellin hasta la cuidad de Bogota, esto fue posible por medio del uso del simulador packet tracer se realizó el montaje de las dos topologías de red de manera satisfactoria, plasmando los diferentes procedimientos de configuración para ambos escenarios, así mismo se aprendió a administrar una red de manera eficiente permitiendo y denegando diferentes tipos de privilegios según sea el caso.

A traves de esta propuesta se presentan una serie de posibles commandos para la configuración de los protocolos dhcp el cual nos permite entregar direccionamento ip de manera dinámica a cada uno de los dispositivos conectados a la red y adicionalmente permite reservar un rango de direcciones para que estas no sean asignadas.

Se empleo el protocolo de enrutamiento sin clase o escalabilidad ospf v2 para ipv4, el cual funcianan como estado de enlace en nuetra permitiendo la ruta mas fácil o la mas corta hacia el siguiente router. Adicionalmente se utilizó el protocolo nat el cual nos permite la tradcucción de direcciones ip es decir nos permite conectar la red de Medellin con la red Bogota, así, éstas tengan segmentos de red o estén en distintas redes, admitiendo la asignación de direcciones ip publicas de manera estatica o dinámica, Tambien se configuró el protocolo de seguridad ppp pat y chat para la autenticación de los dispositivos, accediendo a un enlace seguro entre las dos cuidades en ambos sentidos.

Por otra parte se confirugo las vlan para el ecesnario 1, las cuales se encargan de segmentar la red de acuerdo con las dependencias que tenga una empresa, y nos permite mayor velocidad y confiabilidad de la información.

De igual manera se realizó la configuración de: nombres, direcciones IP en los dispositivos e interfaces de los router, claves de acceso de cada uno de los dispositivos activos de red, servidores, switch, pc y router.

Con este diplomado se logró brindar solución a prueba de de habilidades prácticas ccna en ambos escenarios de una red LAN Y WAN partiendo desde una problemática de la vida cotidiana, y afianzando los conocimientos para la carrera ingeniería en telecomunicaciones.

8. BIBLIOGRAFIA

Calvo, A. C. (2015, 11 mayo). RIP Cisco, aprende a configurar este protocolo facilmente.. Recuperado 15 mayo, 2020, de https://aplicacionesysistemas.com/rip-cisco-version2-de-manera-facil-y-sencilla/

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

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

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

Huertas, S. (2013). Los comandos de configuración de dispositivos cisco. Recuperado de https://es.slideshare.net/samuelhuertasorjuela/comandos-de-configuracion-de-dispositivos-cisco

Juansa, J. (2008, 5 octubre). Solucionando errores TCP/IP. 4 – Uno de los blogs de Juansa. Recuperado 15 mayo, 2020, de https://geeks.ms/juansa/2008/10/05/solucionando-errores-tcpip-4/

Martinez E, (2015, 22 abril). Configuración de RIPv2 (protocolo dinámico). Recuperado 15 mayo, 2020, de http://theosnews.com/2013/02/configuracion-de-ripv2-protocolo-dinamico/

Martinez E,(2018, 16 agosto). Configuración de rutas estáticas (static route) Router Cisco. Recuperado 15 mayo, 2020, dehttp://theosnews.com/2013/02/configuracion-de-rutas-estaticas-static-route- router-cisco/

Prieto, R. (2020). Enrutamiento dinámico OSPF con Packet Tracer. Recuperado de https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ospf-con-packet-tracer