

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

DIEGO EDISON GALINDO MORENO

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD.
ESCUELA DE CIENCIAS BASICAS Y LA TECNOLOGIA
INGENIERIA ELECTRONICA
MOSQUERA CUNDINAMARCA
2020

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

DIEGO EDISON GALINDO MORENO

INFORME FINAL PARA OPTAR POR EL TITULO DE INGENIERÍA ELETRÓNICA

DIRECTOR
JUAN CARLOS VESGA

TUTOR
HECTOR JULIAN PARRA

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD.
ESCUELA DE CIENCIAS BASICAS Y LA TECNOLOGIA
INGENIERIA ELECTRONICA
MOSQUERA CUNDINAMARCA
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Mosquera Cundinamarca 15, 05, 2020

Dedico este trabajo a Dios a mi Madre, Esposa, hija y a las personas que siempre me han apoyado consiguiendo mis sueños

AGRADECIMIENTOS

Principalmente agradecimientos a mi familia a mi madre, Esposa, e hija que son el motor de mi vida dando cierre a las actividades y conclusión de un gran esfuerzo durante varios años a un sueño de superación personal, el cual se realizó paso a paso enfrentando cada obstáculo que surgió durante este proceso.

También agradezco a cada uno de los tutores de la UNAD que fueron fundamentales para lograr este propósito.

CONTENIDO

	Pág.
1. INTRODUCCIÓN	12
2. OBJETIVOS	13
2.1 OBJETIVO GENERAL	13
2.2 OBJETIVOS ESPECÍFICOS	13
3 PLANTEAMIENTO DEL PROBLEMA	14
3.1 DEFINICIÓN DEL PROBLEMA	14
3.2 JUSTIFICACIÓN	14
4. MARCO TEÓRICO	15
5.1 MATERIALES	16
5.2 METODOLOGÍA	16
6 DESARROLLO DEL PROYECTO	17
6.1 ESCENARIO 1	17
1.1.1 Parte 1 Inicializar dispositivos.	18
1.1.2 Parte 2 Configurar los parámetros básicos de los dispositivos.	18
1.1.3 Parte 3 Configurar la seguridad del switch, las VLAN y routing entre VLAN.	25
1.1.4 Parte 4 Configurar el protocolo de routing dinámico RIPv2.	30
1.1.5 Parte 5 Implementar DHCP y NAT para IPv4.	32
1.1.6 Parte 6 Configurar NTP.	36
1.1.7 Parte 7 Configurar y verificar las listas de control de acceso ACL.	37
6.2 ESCENARIO 2	40
1.1.1 Configuración del direccionamiento.	41
1.1.2 Parte 1 Configuración del enrutamiento.	44
1.1.3 Parte 2 Tabla del enrutamiento.	53
1.1.4 Parte 3 Deshabilitar la propagación el protocolo OSPF.	57
1.1.5 Parte 4 Verificación el protocolo OSPF..	58
1.1.6 Parte 5 Configuración encapsulamiento y autenticación PPP.	63
1.1.7 Parte 6 Configuración de PAT.	66
1.1.8 Parte 7 Configuración del servicio DHCP.	69
CONCLUSIONES	73
BIBLIOGRAFÍA	74

LISTA DE TABLAS

	Pág
Tabla 1. Inicializar dispositivos.	18
Tabla 2. Configurar PC – Diego Galindo	18
Tabla 3. Elementos de configuración.	19
Tabla 4. Configurar R1.	20
Tabla 5. Configurar R2.	21
Tabla 6. Configurar R3.	23
Tabla 7. Configurar S1.	24
Tabla 8. Configurar S3.	24
Tabla 9. Verificación de Red.	25
Tabla 10. Configurar la seguridad S1.	25
Tabla 11. Configurar la seguridad S3.	26
Tabla 12. Configurar la seguridad R1.	27
Tabla 13. Verificar la conectividad de la red.	28
Tabla 14. Configurar RIPv2 en el R1.	30
Tabla 15. Configurar RIPv2 en el R2.	30
Tabla 16. Configurar RIPv3 en el R3.	31
Tabla 17. Verificar RIP.	31
Tabla 18. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	33
Tabla 19. Configurar la NAT estática y dinámica en el R2.	34
Tabla 20. Sumarización Loop Back – Diego Galindo	35
Tabla 21. Verificar el protocolo DHCP y la NAT estática	36
Tabla 22. Configurar NPT	36
Tabla 23. Restringir el acceso a las líneas VTY en el R2	37
Tabla 24. Verificar lista de acceso CLI.	38
Tabla 25. Sumarización para Medellín– Diego Galindo.	52
Tabla 26. Sumarización para Bogotá – Diego Galindo.	52

LISTA DE FIGURAS

	Pág.
Figura 1. Topología escenario uno	17
Figura 2. Ping en S1 a R1	29
Figura 3. Ping en S3 a R1	29
Figura 4. Verificar RIP	32
Figura 5. Show ip interface	39
Figura 6. Show ip nat translations	39
Figura 7. Topología escenario dos	40
Figura 8. Show IP Route.	47
Figura 9. Ping desde BOGOTA3 a BOGOTA1	53
Figura 10. Ping desde BOGOTA3 a ESP	54
Figura 11. Ping desde BOGOTA1 a MEDELLIN2	54
Figura. 12 show ip route	56
Figura 13. Show Ip protocols	61
Figura 14. Show ip ospf neighbor	63
Figura 15. Ping desde ISP a 209.17.220.6	65
Figura 16. Ping desde HOTS 150 a ISP	67
Figura 17 ping desde HOTS 50 a ISP	68
Figura 18. Comprobación comando ping	69
Figura 19. Ping HOST 150 HOST 200	71

LISTA DE ANEXOS

Anexo A. Archivo PKT Ejercicio de habilidades Escenario 1 Diego Galindo

Anexo B. Archivo PKT Ejercicio de habilidades Escenario 2 Diego Galindo

GLOSARIO

RED: Se refiere al conjunto de elementos como cables, conductores que sirven para la comunicación entre computadores.

RED LAN: Red de computadoras que abarca un área reducida

Es RED WAN: Una red de área amplia, (Wide Area Network), es una que une varias redes locales, aunque sus miembros no estén todos en una misma ubicación física.

CISCO: Es una empresa de origen estadounidense fabricante de dispositivos para redes locales y externa.

ROUTER: Se conoce también como enrutador es un dispositivo que opera en capa tres de nivel tres. Así permite que varias redes u ordenadores conecten entre sí.

SWITCH: es el dispositivo analógico que permite interconectar redes operando en la capa 2 o de nivel de enlace de datos del modelo OSI.

RESUMEN

En el siguiente documento se encuentran dos casos propuestos los cuales se desarrollaron en torno a los conceptos básicos de la redes y de las nuevas tecnologías de la información, en los que se implementan los conocimientos adquiridos a lo largo del diplomado de profundización CISCO, de los cuales se aplicaron temas entre los que encontramos; Configuración de los parámetros básicos de los dispositivos, configuración la seguridad del switch, las VLAN y routing entre VLAN, implementación DHCP y NAT para IPv4 configuración NTP,PAT,DHCP configuración y verificación de las listas de control de acceso ACL, configuración de protocolos.

Lo anterior permite el diseño e implementación de redes de comunicación, conforme a los estándares y exigencias actuales llegando a desarrollar proyectos y soluciones integradas que sobresalgan en este auge de la revolución tecnológica, que sean útiles y propositivos en los ambiente laborales.

1. INTRODUCCIÓN

En la actualidad se está dando una revolución tecnológica, cada sector productivo de la sociedad y por donde quiera que lo observemos los avances tecnológicos se aplican, para las personas mayores un computador es una herramienta novedosa pero para los más jóvenes hace parte de su día a día y es muy normal la aplicación de ellos en los estudios y el trabajo, conceptos como ancho de banda son muy comunes hoy en día tener una llamada con video son avances que hace muy poco tiempo era difícil pensar en hacerlo realidad, todo se ha dado bajo la necesidad de comunicarnos, de llevar y traer información cada vez más rápido y de la forma más segura, para las empresas son indispensables las redes de comunicación para realizar su trabajo y sus negociaciones.

Teniendo en cuenta lo anterior y las necesidades individuales como las empresariales es muy importante establecer una comunicación efectiva y asertiva con las nuevas tecnologías las telecomunicaciones proponen las soluciones para estas exigencias de cobertura, infraestructura para cada sitio de trabajo teniendo en cuenta la calidad y el costo, lo que significa una alta competitividad y oportunidades en este sector.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Desarrollar los diferentes escenarios propuesto, aplicar los conocimientos adquiridos en el diplomado de profundización de CCNA en los cuales están los conceptos básicos y prácticos para aplicar en networking.

2.2 OBJETIVOS ESPECÍFICOS

- Verificar y desarrollar las topologías de cada escenario y desarrollarlas según lo solicitado por medio de herramientas de simulación, en este caso se trabajaran en Packet Tracer.
- Realizar las distribuciones y conexiones pertinentes para cada caso, Verificando el correcto funcionamiento de cada red y de sus elementos.
- Aplicar los conocimientos y habilidades adquiridas en el desarrollo del actual curso.
- Generar el informe y las evidencias del desarrollo de la actividad.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 PRUEBA DE HABILIDADES PRÁCTICAS CCNA

Escenario 1

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.

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.

3.2 JUSTIFICACIÓN

El planteamiento a la solución de los dos ejercicios anteriores se realiza con el fin de sustentar la prueba práctica del diplomado de profundización CCNA para ingeniería electrónica, el cual se desprende con el fin de finalizar los estudios de dicha carrera, se pretende implementar el desarrollo de las habilidades adquiridas a lo largo del diplomado, se utilizara la herramienta informática Packet Tracer como simulador, para realizar la topología y desarrollo de cada una de las partes solicitadas, al igual que el desarrollo de un informe en Word detallando cada uno de los pasos plateados a la solución de los dos casos.

4. MARCO TEÓRICO

Los ejercicios se desarrollan dentro de los conceptos básicos de las redes de telecomunicaciones implementación el uso y configuración de los elementos por medio de la herramienta de simulación Packet Tracer, se llevara a cabo el diplomado de profundización dando solución de dos estudios de caso bajo el uso de tecnología CISCO, los cuales se desarrollan con los conocimientos adquiridos durante proceso del curso, aplicando ejercicios que permiten la implementación de redes LAN y WAN.

LAN red de área local LAN (Local Area Network) es una red de computadoras que tiene un área pequeña. Por el contrario WAN es una red de área grande, (Wide Area Network), esta red interconecta varias redes locales, de modo que sus usuarios no están ubicados en la misma ubicación geográfica.

5. MATERIALES Y MÉTODOS

- Un computador con sistema operativo XP o superior.
- Herramienta de simulación Packet Tracer.
- Plataforma cisco.com

5.1 MATERIALES

Cisco Packet Tracer:

Esta es una poderosa herramienta de simulación de red diseñada por Cisco. Practique crear redes simples y complejas en una variedad de dispositivos y extiéndase más allá de los routers y los switches. Cree soluciones interconectadas para ciudades, hogares y empresas inteligentes.

Utilícelo junto con cursos de instrucción, capacitación profesional, planificación de trabajo. (<https://www.netacad.com/es/courses/packet-tracer>)

5.2 METODOLOGÍA

Se desarrolla mediante la solución a dos casos planteados de redes de comunicación LAN, por medio del simulador Packet Tracer.

6 DESARROLLO DE LOS ESCENARIOS

Se describe el procedimiento para darle solución a dos escenarios planteados.

6.1 ESCENARIO 1

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

Topología

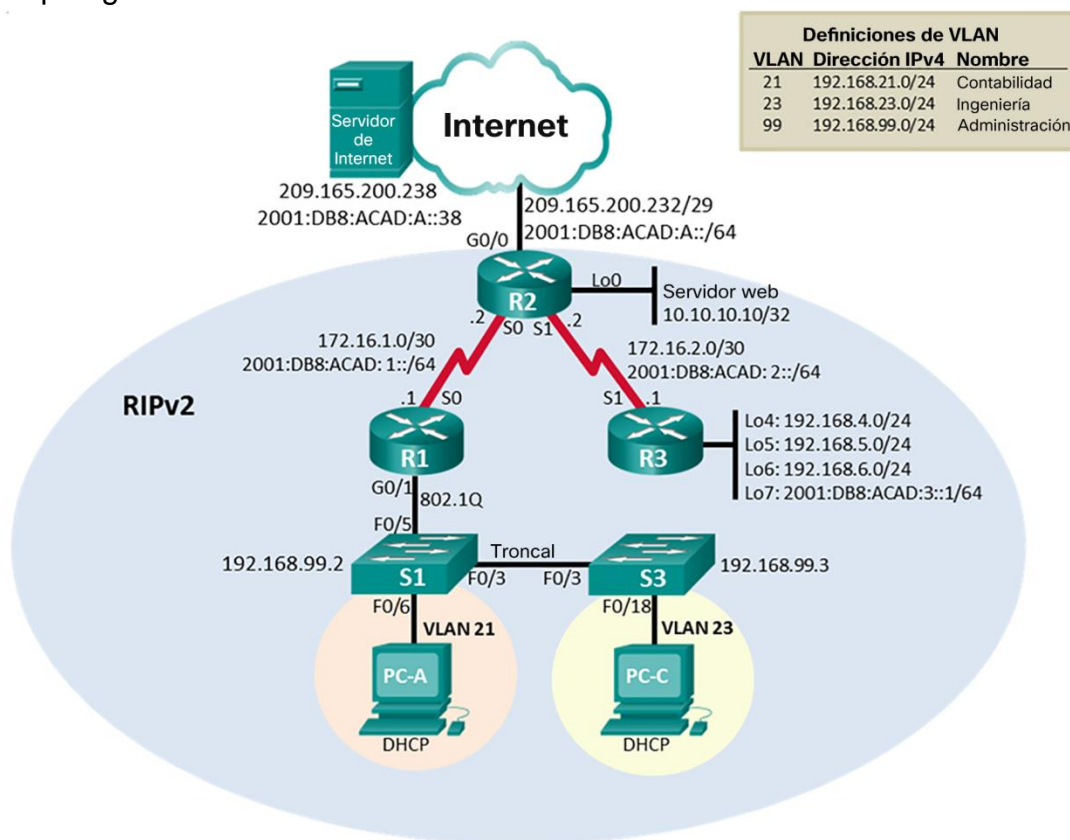


Figura 1. Topología escenario uno

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.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	<i>Router>enable</i> <i>Router#erase startup-config</i>
Volver a cargar todos los routers	<i>Router#reload</i>
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	<i>Switch#erase startup-config</i> <i>Switch#delete vlan.dat</i>
Volver a cargar ambos switches	<i>Switch#reload</i>
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	<i>Switch#show flash</i> <i>Directory of flash: /</i> <i>1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin</i>

Tabla 1. Inicializar dispositivos.

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

209	165	200	232	Red decimal
1 1 0 1 0 0 0 1	1 0 1 0 0 1 0 1	1 1 0 0 1 0 0 0	1 1 1 0 1 0 0 0	Red binario
255	255	255	248	Mascara de subred decimal
1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 1 1 1	1 1 1 1 1 0 0 0	Mascara de subred binario
209	165	200	239	Broadcast decimal
1 1 0 1 0 0 0 1	1 0 1 0 0 1 0 1	1 1 0 0 1 0 0 0	1 1 1 0 1 1 1 1	Broadcast binario
209	165	200	233	IP address primera
209	165	200	238	Ip address final

Tabla 2 Configurar PC

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

Tabla 3. Elementos de configuración.

Paso 2: Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<i>Router(config)#no ip domain-lookup</i>
Nombre del router	<i>R1 Router(config)#hostname R1</i>
Contraseña de exec privilegiado cifrada	<i>R1(config)#enable secret class</i>
Contraseña de acceso a la consola	<i>Cisco R1(config)#line console 0 R1(config-line)#password cisco R1(config-line)#login</i>
Contraseña de acceso Telnet	<i>Cisco R1(config-line)#line vty 0 15 R1(config-line)#password cisco R1(config-line)#login</i>
Cifrar las contraseñas de texto no cifrado	<i>R1(config-line)#service password-encryption</i>
Mensaje MOTD	<i>Se prohíbe el acceso no autorizado. R1(config)#banner motd &se prohíbe el acceso no autorizado&</i>

Interfaz S0/0/0	<p>Establezca la descripción</p> <p>Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones</p> <p>Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones</p> <p>Establecer la frecuencia de reloj en 128000</p> <p>Activar la interfaz</p> <pre>R1(config)#int s0/0/0 R1(config-if)#description connection 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</pre>
Rutas predeterminadas	<p>Configurar una ruta IPv4 predeterminada de S0/0/0</p> <p>Configurar una ruta IPv6 predeterminada de S0/0/0</p> <pre>R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#ipv6 route ::/0 s0/0/0</pre>

Tabla 4. Configurar R1.

Paso 3: Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<i>R2(config)#no ip domain-lookup</i>
Nombre del router	<i>R2</i> <i>R2(config)#enable secret class</i>
Contraseña de exec privilegiado cifrada	<i>Class</i> <i>Router(config)#hostname R2</i>
Contraseña de acceso a la consola	<i>Cisco</i> <i>R2(config-line)#login</i> <i>R2(config)#line console 0</i> <i>R2(config-line)#password cisco</i>
Contraseña de acceso Telnet	<i>Cisco</i> <i>R2(config-line)#line vty 0 15</i> <i>R2(config-line)#password cisco</i> <i>R2(config-line)#login</i>
Cifrar las contraseñas de texto no cifrado	<i>R2(config-line)#service passwor-encrytion</i> <i>R2(config-line)#service password-encryption</i>

Habilitar el servidor HTTP	<i>R2(config)#ip http server</i>
Mensaje MOTD	<i>Se prohíbe el acceso no autorizado. R2(config)#banner motd \$Se prohíbe el acceso no autorizado\$</i>
Interfaz S0/0/0	<i>Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz R2(config)#int s0/0/0 R2(config-if)#description Connection to R1 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:db8:acad:1::2/64 R2(config-if)#no shutdown</i>
Interfaz S0/0/1	<i>Establecer la descripción Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Establecer la frecuencia de reloj en 128000. Activar la interfaz R2(config-if)#int s0/0/1 R2(config-if)#description Connection 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</i>
Interfaz G0/0 (simulación de Internet)	<i>Establecer la descripción. Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred. Activar la interfaz R2(config-if)#int g0/0 R2(config-if)#description Connection to Internet R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:db8:acad:a::1/64 R2(config-if)#no shutdown</i>

Interfaz loopback 0 (servidor web simulado)	<i>Establecer la descripción. Establezca la dirección IPv4. R2(config-if)#int loopback 0 R2(config-if)#ip address 10.10.10.10 255.255.255.255 R2(config-if)#description Connection Web Server</i>
Ruta predeterminada	<i>Configure una ruta IPv4 predeterminada de G0/0. Configure una ruta IPv6 predeterminada de G0/0. R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0 R2(config)#ipv6 route ::/0 g0/0</i>

Tabla 5. Configurar R2.

Paso 4: Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<i>Router(config)#no ip domain-lookup</i>
Nombre del router	<i>R3 Router(config)#hostname R3</i>
Contraseña de exec privilegiado cifrada	<i>Class R3(config)#enable secret class</i>
Contraseña de acceso a la consola	<i>Cisco R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login</i>
Contraseña de acceso Telnet	<i>Cisco R3(config-line)#line vty 0 15 R3(config-line)#password cisco R3(config-line)#login</i>
Cifrar las contraseñas de texto no cifrado	<i>R3(config-line)#service password-encryption</i>
Mensaje MOTD	<i>Se prohíbe el acceso no autorizado. R3(config)#banner motd \$Se prohíbe el acceso no autorizado\$</i>

Interfaz S0/0/1	<p>Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz</p> <pre>R3(config)#int s0/0/1 R3(config-if)#description Connection 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</pre>
Interfaz loopback 4	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R3(config-if)#in loopback 4 R3(config-if)#ip address 192.168.4.1 255.255.255.0</pre>
Interfaz loopback 5	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R3(config-if)#in loopback 5 R3(config-if)#ip address 192.168.5.1 255.255.255.0</pre>
Interfaz loopback 6	<p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <pre>R3(config-if)#in loopback 6 R3(config-if)#ip address 192.168.6.1 255.255.255.0</pre>
Interfaz loopback 7	<p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <pre>R3(config-if)#in loopback 7 R3(config-if)#ipv6 address 2001:db8:acad:3::1/64</pre>
Rutas predeterminadas	<p>Ruta predeterminada IPv4 S0/0/1 Ruta predeterminada IPv6 S0/0/1</p> <pre>R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1 R3(config)#ipv6 route ::/0 s0/0/1</pre>

Tabla 6. Configurar R3.

Paso 5: Configurar S1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<pre>Switch(config)#no ip domain-lookup</pre>
Nombre del switch	<pre>S1 Switch(config)#hostname S1</pre>

Contraseña de exec privilegiado cifrada	<i>Class S1(config)#enable secret class</i>
Contraseña de acceso a la consola	<i>cisco S1(config)#line console 0 S1(config-line)#password cisco S1(config-line)#login</i>
Contraseña de acceso Telnet	<i>Cisco S1(config-line)#line vty 0 15 S1(config-line)#password cisco S1(config-line)#login</i>
Cifrar las contraseñas de texto no cifrado	<i>S1(config-line)#service password-encryption</i>
Mensaje MOTD	<i>Se prohíbe el acceso no autorizado. S1(config)#banner motd &Se prohíbe el acceso no autorizado&</i>

Tabla 7. Configurar S1.

Paso 6: Configurar el S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<i>Switch(config)#no ip domain-lookup</i>
Nombre del switch	<i>S3 Switch(config)#hostname S3</i>
Contraseña de exec privilegiado cifrada	<i>Class S3(config)#enable secret class</i>
Contraseña de acceso a la consola	<i>Cisco S3(config)#line console 0 S3(config-line)#password cisco S3(config-line)#login</i>
Contraseña de acceso Telnet	<i>Cisco S3(config-line)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login</i>
Cifrar las contraseñas de texto no cifrado	<i>S3(config-line)#service password-encryption</i>
Mensaje MOTD	<i>Se prohíbe el acceso no autorizado. S3(config)#banner motd \$Se prohíbe el acceso no autorizado\$</i>

Tabla 8. Configurar S3.

Paso 7: Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	<i>R1#ping 172.16.1.2</i>	<i>Success rate is 100 percent (5/5)</i>
R2	R3, S0/0/1	<i>R2#ping 172.16.2.1</i>	<i>Success rate is 100 percent (5/5)</i>
PC de Internet	Gateway predeterminado	<i>Ping 209.165.200.233</i>	<i>Satisfactorio</i>

Tabla 9. Verificación de Red.

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

Paso 1: Configurar S1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<i>Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name Ingenieria</i>
Asignar la dirección IP de administración.	<i>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion</i>
Asignar el gateway predeterminado	<i>Asigne la primera dirección IPv4 de la subred como el gateway predeterminado. S1(config)#ip default-gateway 192.168.99.1</i>
Forzar el enlace troncal en la interfaz F0/3	<i>Utilizar la red VLAN 1 como VLAN nativa S1(config)#int f0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1</i>

Forzar el enlace troncal en la interfaz F0/5	<i>Utilizar la red VLAN 1 como VLAN nativa</i> S1(config-if)#int f0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport trunk native vlan 1
Configurar el resto de los puertos como puertos de acceso	<i>Utilizar el comando interface range</i> 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-range)#shutdown

Tabla 10. Configurar la seguridad S1.

Paso 2: Configurar el S3

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<i>Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.</i> 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	<i>Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología</i> 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.	<i>Asignar la primera dirección IP en la subred como gateway predeterminado.</i> S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	<i>Utilizar la red VLAN 1 como VLAN nativa</i> S3(config)#int f0/3 S3(config-if)#switchport mode trunk S3(config-if)#switchport trunk native vlan 1

Configurar el resto de los puertos como puertos de acceso	<i>Utilizar el comando interface range</i> S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2 S3(config-if-range)#switchport mode access
Asignar F0/18 a la VLAN 21 Es incorrecto debe ser; Asignar F0/18 a la VLAN 23	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

Tabla 11. Configurar la seguridad S3.

Paso 3: Configurar R1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	<i>Descripción: LAN de Contabilidad</i> Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz R1(config)#int g0/1.21 R1(config-subif)#description VLAN 21 R1(config-subif)#encapsulation dot1 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	<i>Descripción: LAN de Ingeniería</i> Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz 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	<i>Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz</i> 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	R1(config-if)#no shutdown

Tabla 12. Configurar la seguridad R1.

Paso 4: Verificar la conectividad de la red

Se usa el comando ping para probar la conectividad entre los switches y el R1.

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	ping 192.168.99.1	Success rate is 100 percent (5/5)
S3	R1, dirección VLAN 99	ping 192.168.99.1	Success rate is 100 percent (5/5)
S1	R1, dirección VLAN 21	ping 192.168.21.1	Success rate is 100 percent (5/5)
S3	R1, dirección VLAN 23	ping 192.168.23.1	Success rate is 100 percent (5/5)

Tabla 13. Verificar la conectividad de la red

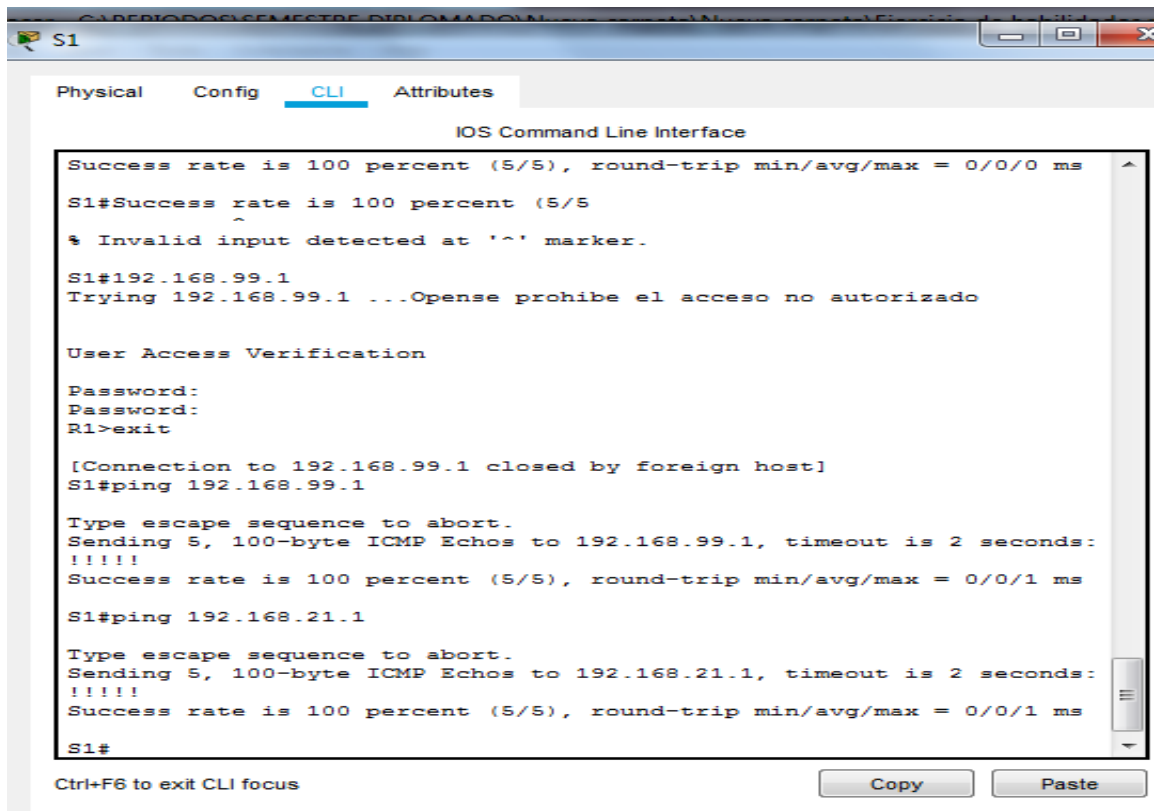


Figura 2. Ping en S1 a R1

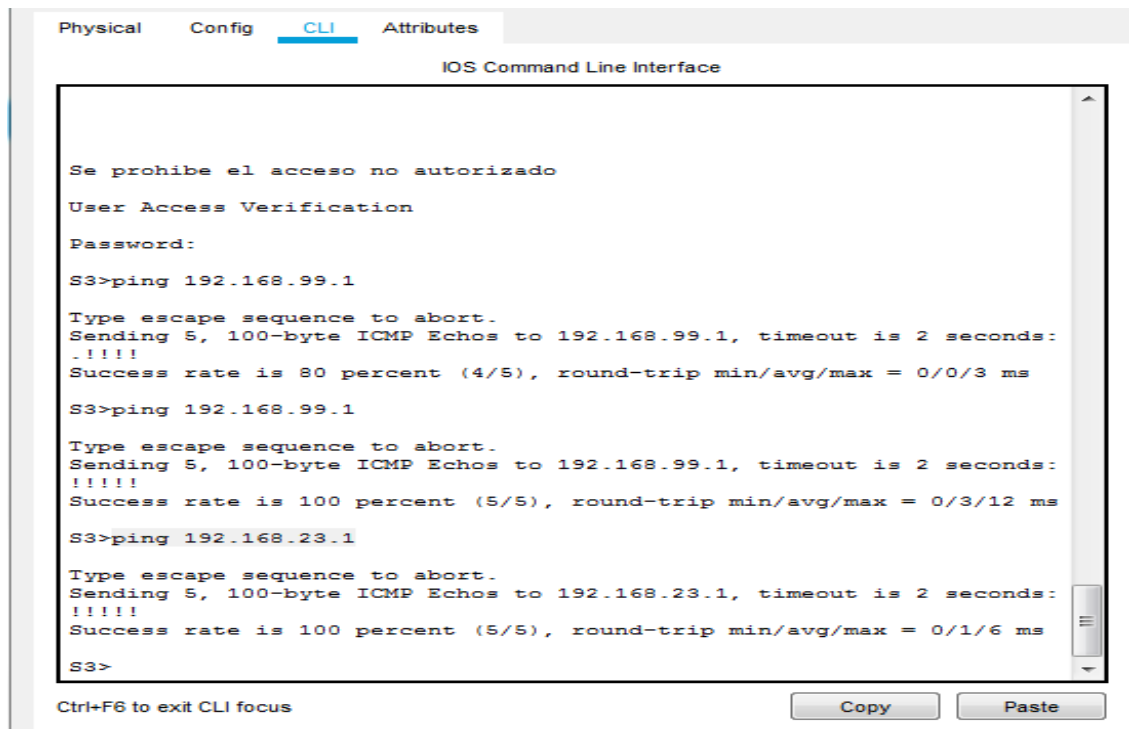


Figura 3. Ping en S3 a R1

Parte 3: Configurar el protocolo de routing dinámico RIPv2

Paso 1: Configurar RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	<i>R1(config)#router rip R1(config-router)#version 2</i>
Anunciar las redes conectadas directamente	<i>Asigne todas las redes conectadas directamente. R1(config-router)#do show ip route connected C 172.16.1.0/30 is directly connected, Serial0/0/0 C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99 R1(config-router)#network 172.16.1.0 R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0</i>
Establecer todas las interfaces LAN como pasivas	<i>R1(config-router)#passive-interface g0/1.21 R1(config-router)#passive-interface g0/1.23 R1(config-router)#passive-interface g0/1.99</i>
Desactive la sumarización automática	<i>R1(config-router)#no auto-summary</i>

Tabla 14. Configurar RIPv2 en el R1

Paso 2: Configurar RIPv2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	<i>R2(config)#router rip R2(config-router)#version 2</i>
Anunciar las redes conectadas directamente	<i>Nota: Omitir la red G0/0. R2(config-router)#network 10.10.10.10 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0</i>

Establecer la interfaz LAN (loopback) como pasiva	<i>R2(config-router)#passive-interface loopback 0</i>
Desactive la sumarización automática.	<i>R2(config-router)#no auto-summary</i>

Tabla 15. Configurar RIPv2 en el R2

Paso 3: Configurar RIPv3 en el R3

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	<i>R3(config)#router rip R3(config-router)#version 2</i>
Anunciar redes IPv4 conectadas directamente	<i>R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0</i>
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	<i>R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6</i>
Desactive la sumarización automática.	<i>R3(config-router)#no auto-summary</i>

Tabla 16. Configurar RIPv3 en el R3.

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:

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?	<i>R3#show ip protocols</i>
¿Qué comando muestra solo las rutas RIP?	<i>R3#show ip route rip</i>
¿Qué comando muestra la sección de RIP de la configuración en ejecución?	<i>Paket tracer no soporta el comando. se usa R3#show run</i>

Tabla 17. Verificar RIP.

```

User Access Verification

Password:

R3>en
Password:
R3#show ip route rip
      10.0.0.0/32 is subnetted, 1 subnets
R       10.10.10.10 [120/1] via 172.16.2.2, 00:00:03, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.16.1.0/30 [120/1] via 172.16.2.2, 00:00:03, Serial0/0/1
      192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
R       192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:03, Serial0/0/1
R       192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:03, Serial0/0/1
R       192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:03, Serial0/0/1

R3#

```

Figura 4. Verificar RIP

Parte 4: Implementar DHCP y NAT para IPv4

Paso 1: 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	<pre> R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.1.20 R1(config)#no ip dhcp excluded-address 192.168.21.1 192.168.1.20 R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20 </pre>
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	<pre> R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20 </pre>

<p>Crear un pool de DHCP para la VLAN 21.</p>	<p>Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com</p>
<p>Crear un pool de DHCP para la VLAN 23</p>	<p>Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado.</p> <p>R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com</p>

Tabla 18. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

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

<p>Elemento o tarea de configuración</p>	<p>Especificación</p>
<p>Crear una base de datos local con una cuenta de usuario</p>	<p>Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15</p> <p>R2(config)#username webuser privilege 15 secret cisco12345</p>
<p>Habilitar el servicio del servidor HTTP</p>	<p>R2(config)#ip http server ^ % Invalid input detected at '^' marker. Pakert Tracer no soporta este comando</p>
<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	<p>R2(config)#ip http server ^ % Invalid input detected at '^' marker. Pakert Tracer no soporta este comando</p>

Crear una NAT estática al servidor web.	<p><i>Dirección global interna: 209.165.200.229</i></p> <pre>R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229 1:11</pre>
Asignar la interfaz interna y externa para la NAT estática	<pre>R2(config)#int g0/0 R2(config-if)#ip nat outside R2(config-if)#int s0/0/0 R2(config-if)#ip nat inside R2(config-if)#int s0/0/1 R2(config-if)#ip nat inside</pre>
Configurar la NAT dinámica dentro de una ACL privada	<p><i>Lista de acceso: 1</i></p> <p><i>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1</i></p> <p><i>Permitir la traducción de un resumen de las redes LAN (loopback) en el R3</i></p> <pre>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</pre>
Defina el pool de direcciones IP públicas utilizables.	<p><i>Nombre del conjunto: INTERNET</i></p> <p><i>El conjunto de direcciones incluye:</i></p> <p><i>209.165.200.225 – 209.165.200.228</i></p> <pre>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248 1.17</pre>
Definir la traducción de NAT dinámica	<pre>R2(config)#ip nat inside source list 1 pool INTERNET</pre>

Tabla 19. Configurar la NAT estática y dinámica en el R2.

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	<i>Paker tracer no soporta este comando por lo tanto no se puede comprobar</i>
---	--

Tabla 21. Verificar el protocolo DHCP y la NAT estática

Parte 5: Configurar NTP

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	<i>5 de marzo de 2016, 9 a. m. R2#clock set 09:00:00 05 march 2016 R2#clock set 04:25:00 11 april 2020 lo configure con la hora actual</i>
Configure R2 como un maestro NTP.	<i>Nivel de estrato: 5 R2(config)#ntp master 5 ^ % Invalid input detected at '^' marker. Pakert Tracer no soporta este comando</i>
Configurar R1 como un cliente NTP.	<i>Servidor: R2 R1(config)#ntp server 172.16.1.2</i>
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	<i>R1(config)#ntp update-calendar</i>
Verifique la configuración de NTP en R1.	<i>R1#show ntp associations address ref clock st when poll reach delay offset disp ~172.16.1.2 .INIT. 16 - 64 0 0.00 0.00 0.48 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured</i>

Tabla 22. Configurar NPT

Parte 6: Configurar y verificar las listas de control de acceso (ACL)

Paso 1: 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	<p>Nombre de la ACL: ADMIN-MGT</p> <pre>R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1</pre>
Aplicar la ACL con nombre a las líneas VTY	<pre>R2(config)#line vty 0 15 R2(config-line)#access-class ADMIN-MGT in</pre>
Permitir acceso por Telnet a las líneas de VTY	<pre>R2(config-line)#transport input telnet</pre>
Verificar que la ACL funcione como se espera	<pre>R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohíbe el acceso no autorizado User Access Verification Password: R2>exit</pre>

Tabla 23. Restringir el acceso a las líneas VTY en el R2

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

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	<pre>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 (4 match(es)) R2#show ip 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 (4 match(es))</pre>

<p>Restablecer los contadores de una lista de acceso</p>	<pre>R2#clear ip access-list counters % Invalid input detected at '^' marker. R2#clear ip ? bgp Clear BGP connections dhcp Delete items from the DHCP database nat Clear NAT ospf OSPF clear commands route Delete route table entries</pre>
<p>¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?</p>	<pre>R2#show ip interface R2#show ip interface GigabitEthernet0/0 is up, line protocol is up (connection) Internet address is 209.165.200.233/29 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1500 bytes Helper address is not set Directed broadcast forwarding is disabled Outgoing access list is not set Inbound access list is not set</pre>
<p>¿Con qué comando se muestran las traducciones NAT?</p>	<p>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.</p> <pre>R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.229 10.10.10.10 --- --- tcp 209.165.200.229:80 10.10.10.10:80 209.165.200.238:1025209.165.200.238:1025 tcp 209.165.200.229:80 10.10.10.10:80 209.165.200.238:1026209.165.200.238:1026</pre>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<pre>R2#clear ip nat translation *</pre>

Tabla 24. Verificar lista de acceso CLI.

```

R2#
Password:
R2#show ip interface
GigabitEthernet0/0 is up, line protocol is up (connected)
  Internet address is 209.165.200.233/29
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  BGP Policy Mapping is disabled
  Input features: MCI Check
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
GigabitEthernet0/1 is administratively down, line protocol is down (disabled)
  Internet protocol processing disabled
Serial0/0/0 is up, line protocol is up (connected)

```

Figura 5. Show ip interface

```

R2#
R2#
R2#show ip nat translations

```

Pro	Inside global	Inside local	Outside local	Outside global
---	209.165.200.229	10.10.10.10	---	---

```

R2#

```

Figura 6. Show ip nat translations

6.2 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.

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

Topología

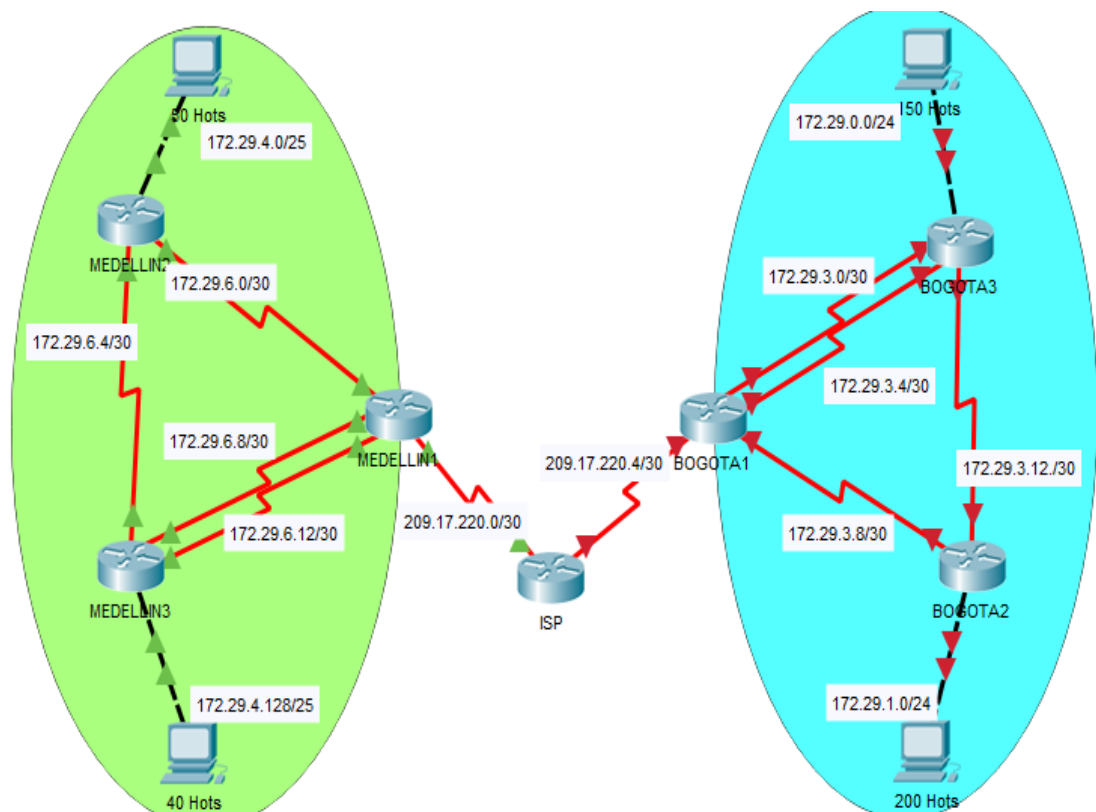


Figura 7. Topología escenario dos

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 física de los equipos con base en la topología de red
Configurar la topología de red, de acuerdo con las siguientes especificaciones.

Configuración del Direccinamineto:

- Para router ISP

```
Router>ENABLE
```

```
Router#configure terminal
```

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

```
Router(config)#hostname ISP
```

```
ISP(config)#int s0/0/0
```

```
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
```

```
ISP(config-if)#clock rate 4000000
```

```
ISP(config-if)#no shutdown
```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
```

```
ISP(config-if)#int s0/0/1
```

```
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
```

```
ISP(config-if)#clock rate 4000000
```

```
ISP(config-if)#no shutdown
```

- Para el router MEDELLIN1

```
MEDELLIN1(config)#int s0/0/0
```

```
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
```

```
MEDELLIN1(config-if)#no shutdown
```

```
MEDELLIN1(config-if)#int s0/0/1
```

```
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
```

```
MEDELLIN1(config-if)#clock rate 4000000
```

```
MEDELLIN1(config-if)#no shutdown
```

```
MEDELLIN1(config-if)#int s0/1/0
```

```
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
```

MEDELLIN1(config-if)#clock rate 4000000

MEDELLIN1(config-if)#no shutdown

MEDELLIN1(config-if)#int s0/1/1

MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252

MEDELLIN1(config-if)#clock rate 4000000

MEDELLIN1(config-if)#no shutdown

- Para router MEDELLIN2

MEDELLIN2(config)#int s0/0/0

MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252

MEDELLIN2(config-if)#no shutdown

MEDELLIN2(config-if)#int s0/0/1

MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252

MEDELLIN2(config-if)#clock rate 4000000

MEDELLIN2(config-if)#no shutdown

MEDELLIN2(config-if)#int g0/0

MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128

MEDELLIN2(config-if)#no shutdown

- Para router MEDELLIN3

MEDELLIN3(config)#int s0/0/0

MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252

MEDELLIN3(config-if)#no shutdown

MEDELLIN3(config)#int s0/0/1

MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252

MEDELLIN3(config-if)#no shutdown

MEDELLIN3(config-if)#int s0/1/0

MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252

MEDELLIN3(config-if)#no shutdown

MEDELLIN3(config-if)#int g0/0

MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128

MEDELLIN3(config-if)#no shutdown

- Para router BOGOTA1

```
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#no shutdown
```

```
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shutdown
```

```
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shutdown
```

```
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 4000000
BOGOTA1(config-if)#no shutdown
```

- Para router BOGOTA2

```
BOGOTA2(config)#int s0/0/0
BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#no shutdown
```

```
BOGOTA2(config-if)#int s0/0/1
BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#clock rate 4000000
BOGOTA2(config-if)#no shutdown
```

```
BOGOTA2(config-if)#int g0/0
BOGOTA2(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA2(config-if)#no shutdown
```

- Para router BOGOTA3

```
BOGOTA3(config)#int s0/0/0
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#no shutdown
```

```
BOGOTA3(config-if)#int s0/0/1
BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#no shutdown
```

```
BOGOTA3(config)#int s0/1/0
BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA3(config-if)#no shutdown
```

```
BOGOTA3(config-if)#int g0/0
BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA3(config-if)#no shutdown
```

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.

Se deben configurar las dos ciudades independientemente OSPF en Bogota y luego OSPF en Medellin.

Para router MEDELLIN1

En MEDELLIN1 hay cuatro interfaces conectadas, se notifican las primeras tres porque están en OSPF la cuarta (**C 209.17.220.0/30 is directly connected, Serial0/0/0**) La conexión a ISP se usara con otro protocolo de enrutamiento, es la conexión a internet que esta por fuera del alcance del administrador, se deja como pasiva, la cual se configura m'as adelante.

OSPF

- Para el router MEDELLIN1

```
MEDELLIN1(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
C 209.17.220.0/30 is directly connected, Serial0/0/0
```

```
MEDELLIN1(config)#router ospf 2
MEDELLIN1(config-router)#network 172.29.6.0 255.255.255.252 area 2
MEDELLIN1(config-router)#network 172.29.6.8 255.255.255.252 area 2
MEDELLIN1(config-router)#network 172.29.6.12 255.255.255.252 area 2
```

- Para router MEDELLIN2

```
MEDELLIN2(config)#do show ip route connected  
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0  
C 172.29.6.0/30 is directly connected, Serial0/0/0  
C 172.29.6.4/30 is directly connected, Serial0/0/1
```

```
MEDELLIN2(config)#router ospf 2  
MEDELLIN2(config-router)#network 172.29.4.0 255.255.255.128 area 2  
MEDELLIN2(config-router)#network 172.29.6.0 255.255.255.252 area 2  
MEDELLIN2(config-router)#network 172.29.6.4 255.255.255.252 area 2
```

- Para router MEDELLIN3

```
MEDELLIN3(config)#do show ip route connected  
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0  
C 172.29.6.4/30 is directly connected, Serial0/1/0  
C 172.29.6.8/30 is directly connected, Serial0/0/0  
C 172.29.6.12/30 is directly connected, Serial0/0/1
```

```
MEDELLIN3(config)#router ospf 2  
MEDELLIN3(config-router)#network 172.29.4.128 255.255.255.128 area 2  
MEDELLIN3(config-router)#network 172.29.6.4 255.255.255.252 area 2  
MEDELLIN3(config-router)#network 172.29.6.8 255.255.255.252 area 2  
MEDELLIN3(config-router)#network 172.29.6.12 255.255.255.252 area 2  
MEDELLIN3(config-router)#  
03:36:50: %OSPF-5-ADJCHG: Process 2, Nbr 209.17.220.2 on Serial0/0/1 from  
LOADING to FULL, Loading Done
```

- Para router BOGOTA1

```
BOGOTA1(config-router)#do show ip route connected  
C 172.29.3.0/30 is directly connected, Serial0/1/0  
C 172.29.3.4/30 is directly connected, Serial0/1/1  
C 172.29.3.8/30 is directly connected, Serial0/0/1  
C 209.17.220.4/30 is directly connected, Serial0/0/0
```

```
BOGOTA1(config-router)#network 172.29.3.0 255.255.255.252 area 1
```

```
BOGOTA1(config-router)#network 172.29.3.4 255.255.255.252 area 1
BOGOTA1(config-router)#network 172.29.3.8 255.255.255.252 area 1
BOGOTA1(config-router)#network 209.17.220.4 255.255.255.252 area 1
```

- Para router BOGOTA2

```
BOGOTA2(config)#route ospf 1
BOGOTA2(config-router)#do show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
```

```
BOGOTA2(config-router)#network 172.29.1.0 255.255.255.0 area 1
BOGOTA2(config-router)#network 172.29.3.8 255.255.255.252 area 1
BOGOTA2(config-router)#network 172.29.3.12 255.255.255.252 area 1
04:00:33: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/0/0 from
LOADING to FULL, Loading Done
BOGOTA2(config-router)#
```

- Para router BOGOTA3

```
BOGOTA3(config)#do show ip route connected
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/0/1
C 172.29.3.12/30 is directly connected, Serial0/1/0
```

```
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#network 172.29.0.0 255.255.255.0 area 1
BOGOTA3(config-router)#network 172.29.3.0 255.255.255.252 area 1
BOGOTA3(config-router)#network 172.29.3.4 255.255.255.252 area 1
BOGOTA3(config-router)#network 172.29.3.12 255.255.255.252 area 1
BOGOTA3(config-router)#
04:22:53: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.3.13 on Serial0/1/0 from
LOADING to FULL, Loading Done
```

Se verifica la conectividad con el comando Show ip route en el router BOGOTA1

```

BOGOTA1(config-router)#exit
BOGOTA1(config)#do show ip route connected
C   172.29.3.0/30   is directly connected, Serial0/1/0
C   172.29.3.4/30   is directly connected, Serial0/1/1
C   172.29.3.8/30   is directly connected, Serial0/0/1
C   209.17.220.4/30 is directly connected, Serial0/0/0
C   209.17.220.5/32 is directly connected, Serial0/0/0

BOGOTA1(config)#|

```

```

Password:
BOGOTA2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#do show ip route connected
C   172.29.1.0/24   is directly connected, GigabitEthernet0/0
C   172.29.3.8/30   is directly connected, Serial0/0/0
C   172.29.3.12/30  is directly connected, Serial0/0/1

BOGOTA2(config)#

```

```

BOGOTA3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#do show ip route connected
C   172.29.0.0/24   is directly connected, GigabitEthernet0/0
C   172.29.3.0/30   is directly connected, Serial0/0/0
C   172.29.3.4/30   is directly connected, Serial0/0/1
C   172.29.3.12/30  is directly connected, Serial0/1/0

BOGOTA3(config)#

```

Figura 8. Show IP Route.

- En BOGOTA1

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 not set

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O 172.29.0.0/24 [110/65] via 172.29.3.2, 00:29:15, Serial0/1/0
O 172.29.1.0/24 [110/65] via 172.29.3.10, 00:49:23, 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, 00:27:10, Serial0/1/0
[110/128] via 172.29.3.10, 00:27:10, Serial0/0/1
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks

Se verifica la conexión con el comando Show ip route en el router MEDELLIN1

- *En MEDELLIN1*

MEDELLIN1#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 not set

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O 172.29.4.0/25 [110/65] via 172.29.6.2, 01:35:08, Serial0/0/1
O 172.29.4.128/25 [110/65] via 172.29.6.10, 01:15:52, Serial0/1/0
C 172.29.6.0/30 is directly connected, Serial0/0/1
L 172.29.6.1/32 is directly connected, Serial0/0/1
O 172.29.6.4/30 [110/128] via 172.29.6.2, 01:15:52, Serial0/0/1
[110/128] via 172.29.6.10, 01:15:52, Serial0/1/0
C 172.29.6.8/30 is directly connected, Serial0/1/0

L 172.29.6.9/32 is directly connected, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
L 172.29.6.13/32 is directly connected, Serial0/1/1
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
 --More--

Las configuraciones basicas se realizaron al finalizar del ejercicio con el fin de evitar interrupciones en la configuración de los elementos durante el proceso.

no ip domain-lookup	Desactivar la búsqueda DNS
service password-encryption	Ocultar contraseñas y cifrarlas
enable secret class	Activar contraseña class
banner motd & Acceso negado-UNAD-Diego Edison Galindo Moreno&	Mensaje del día
ip domain-name UNAD.com	Dominio
line console 0	En la línea de consola contraseña cisco
password cisco	Contraseña
login	Activar la contraseña
line vty 0 15	En la línea vty de la 0 a la 15 contraseña cisco
password cisco	Contraseña
login	Activar la contraseña

BOGOTA1

BOGOTA1(config)#no ip domain-lookup
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#enable secret class
BOGOTA1(config)#banner motd & Acceso negado-UNAD-Diego Edison Galindo Moreno&
BOGOTA1(config)#ip domain-name UNAD.com
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#line vty 0 15
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#

BOGOTA2

BOGOTA2(config)#no ip domain-lookup
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#enable secret class
BOGOTA2(config)#banner motd & Acceso negado-UNAD-Diego Edison Galindo Moreno&
BOGOTA2(config)#ip domain-name UNAD.com

```
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#line vty 0 15
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
```

BOGOTA3

```
BOGOTA3(config)#
BOGOTA3(config)#no ip domain-lookup
BOGOTA3(config)#service password-encryption
BOGOTA3(config)#enable secret class
BOGOTA3(config)#banner motd & Acceso negado-UNAD-Diego Edison Galindo
Moreno&
BOGOTA3(config)#ip domain-name UNAD.com
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#line vty 0 15
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
```

MEDELLIN1

```
MEDELLIN1(config)#no ip domain-lookup
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#banner motd & Acceso negado-UNAD-Diego Edison Galindo
Moreno&
MEDELLIN1(config)#ip domain-name UNAD.com
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#line vty 0 15
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#end
MEDELLIN1#
```

MEDELLIN2

```
MEDELLIN2(config)#no ip domain-lookup
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#banner motd & Acceso negado-UNAD-Diego Edison Galindo
Moreno&
```

```
MEDELLIN2(config)#ip domain-name UNAD.com
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#line vty 0 15
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#
```

MEDELLIN3

```
MEDELLIN3(config)#no ip domain-lookup
MEDELLIN3(config)#service password-encryption
MEDELLIN3(config)#enable secret class
MEDELLIN3(config)#banner motd & Acceso negado-UNAD-Diego Edison Galindo
Moreno&
MEDELLIN3(config)#ip domain-name UNAD.com
MEDELLIN3(config)#line console 0
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#line vty 0 15
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#
MEDELLIN3#
```

ISP

```
ISP(config)#no ip domain-lookup
ISP(config)#service password-encryption
ISP(config)#enable secret class
ISP(config)#banner motd & Acceso negado-UNAD-Diego Edison Galindo Moreno&
ISP(config)#ip domain-name UNAD.com
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#end
```

- 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

MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1

MEDELLIN1(config)#router ospf 2

MEDELLIN1(config-router)#default-information originate

BOGOTA 1

BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5

BOGOTA1(config)#router ospf 2

BOGOTA1(config-router)#default-information originate

- 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.

Tabla 3. Sumarización para MEDELLIN

MEDELLIN 1																		
DECIMAL		BINARIO																
172	29	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	<div style="border: 1px solid black; padding: 5px;"> 172.29.4.0/25 172.29.4.128/25 172.29.6.4/30 172.29.6.8/30 172.29.6.12/30 172.29.6.0/30 </div>
172	29	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0		
172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	0	0		
172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0		
172	29	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0		
172	29	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0		
172	29	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	<div style="border: 1px solid black; padding: 5px; background-color: #008000; color: white;"> 172.29.4.0/22 </div>	Red sumarizada

172.29.4.0 255.255.252.0

Tabla 4. Sumarización para BOGOTA

BOGOTA 1																		
DECIMAL		BINARIO																
172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	<div style="border: 1px solid black; padding: 5px;"> 172.29.0.0/24 172.29.1.0/24 172.29.3.12/30 172.29.3.8/30 172.29.3.0/30 172.29.3.4/30 </div>	
172	29	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0		
172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	1	0		
172	29	0	0	0	0	0	0	1	1	0	0	0	0	1	0	0		
172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0		
172	29	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0		
172	29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	<div style="border: 1px solid black; padding: 5px; background-color: #008000; color: white;"> 172.29.0.0/22 </div>	Red sumarizada

172.29.0.0 255.255.252.0

- Se declaran las rutas estaticas en el router ISP

```
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
ISP(config)#
```

Parte 2: Tabla de Enrutamiento.

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

- Ping desde BOGOTA3 a BOGOTA1

```
BOGOTA3#ping 172.29.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 m
```

El ping fue satisfactorio

```
BOGOTA3#ping 172.29.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/13 ms

BOGOTA3#
```

Figura 9. Ping desde BOGOTA3 a BOGOTA1

- Ping desde BOGOTA3 a ESP

```
BOGOTA3#ping 209.17.220.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/5 ms
```

El ping fue satisfactorio

```
Password:

BOGOTA3>en
Password:
BOGOTA3#ping 209.17.220.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms

BOGOTA3#
```

Figura 10. Ping desde BOGOTA3 a ESP

- Ping desde BOGOTA1 a MEDELLI2

```
BOGOTA1#ping 172.29.6.0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.0, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/5 ms
```

El ping fue satisfactorio

```
Password:

BOGOTA1>en
Password:
BOGOTA1#ping 172.29.6.0

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.0, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms

BOGOTA1#
```

Figura 11. desde BOGOTA1 a MEDELLIN2

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

El balanceo de carga se hace en los routers donde hay dos seriales para una misma conexión en un route.

Ejemplo BOGOTA3 A BOGOTA1

BOGOTA3#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 not set

172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
L 172.29.0.1/32 is directly connected, GigabitEthernet0/0
O 172.29.1.0/24 [110/65] via 172.29.3.13, 03:35:13, Serial0/1/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
L 172.29.3.2/32 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/0/1
L 172.29.3.6/32 is directly connected, Serial0/0/1
O 172.29.3.8/30 [110/128] via 172.29.3.1, 03:35:13, Serial0/0/0
[110/128] via 172.29.3.13, 03:35:13, Serial0/1/0
C 172.29.3.12/30 is directly connected, Serial0/1/0
L 172.29.3.14/32 is directly connected, Serial0/1/0
209.17.220.0/30 is subnetted, 1 subnets
O 209.17.220.4/30 [110/128] via 172.29.3.1, 03:37:28, Serial0/0/0

```

BOGOTA3>en
Password:
BOGOTA3#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 not set

      172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
C       172.29.0.0/24 is directly connected, GigabitEthernet0/0
L       172.29.0.1/32 is directly connected, GigabitEthernet0/0
O       172.29.1.0/24 [110/65] via 172.29.3.13, 00:02:37, Serial0/1/0
C       172.29.3.0/30 is directly connected, Serial0/0/0
L       172.29.3.2/32 is directly connected, Serial0/0/0
C       172.29.3.4/30 is directly connected, Serial0/0/1
L       172.29.3.6/32 is directly connected, Serial0/0/1
O       172.29.3.8/30 [110/128] via 172.29.3.5, 00:02:37, Serial0/0/1
           [110/128] via 172.29.3.13, 00:02:37, Serial0/1/0
C       172.29.3.12/30 is directly connected, Serial0/1/0
L       172.29.3.14/32 is directly connected, Serial0/1/0
--More--

```

Figura. 12 show ip route

- 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.

Los routers tiene similitud en su ubicación y sus enlaces y la red a la que pertenecen.

- 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.

Son rutas con más de un camino llamadas rutas redundantes, ejemplo

MEDELLIN1 Y MEDELLIN2 o BOGOTA1 Y BOGOTA2

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

```
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
```

```
ISP(config)#ip route 172.29.0.0 255.255.252.0 209.17.220.6
```

```
ISP(config)#
```

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.

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

Para ospf 2

```
MEDELLIN1(config)#router ospf 2
MEDELLIN1(config-router)#do show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
C 209.17.220.0/30 is directly connected, Serial0/0/0
```

```
MEDELLIN1(config-router)#passive-interface s0/0/0
```

```
MEDELLIN2(config)#router ospf 2
MEDELLIN2(config-router)#do show ip route connected
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.4/30 is directly connected, Serial0/0/1
```

```
MEDELLIN2(config-router)#passive-interface g0/0
MEDELLIN2(config-router)#
```

```
MEDELLIN3(config)#router ospf 2
MEDELLIN3(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#do show ip route connected
C 172.29.4.128/25 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/1/0
C 172.29.6.8/30 is directly connected, Serial0/0/0
C 172.29.6.12/30 is directly connected, Serial0/0/1
```

```
MEDELLIN3(config-router)#passive-interface g0/0
MEDELLIN3(config-router)#
```

Para ospf 1

```
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#do show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/1/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/0/1
C 209.17.220.4/30 is directly connected, Serial0/0/0
```

```
BOGOTA1(config-router)#passive-interface s0/0/0
BOGOTA1(config-router)#
```

```
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#do show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
```

```
BOGOTA2(config-router)#passive-interface g0/0
BOGOTA2(config-router)#
```

```
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#do show ip route connected
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
```

C 172.29.3.4/30 is directly connected, Serial0/0/1
C 172.29.3.12/30 is directly connected, Serial0/1/0

BOGOTA3(config-router)#passive-interface g0/0
BOGOTA3(config-router)#

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.

- Se verifica la red en la ruta del lado de la ciudad de Medellín.

Routing Protocol is "ospf 2"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 209.17.220.2
It is an autonomous system boundary router
Redistributing External Routes from,
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.6.0 0.0.0.3 area 2
172.29.6.8 0.0.0.3 area 2
172.29.6.12 0.0.0.3 area 2
Passive Interface(s):
Serial0/0/0
Routing Information Sources:
Gateway Distance Last Update
172.29.6.5 110 00:20:42
172.29.6.14 110 00:20:43
209.17.220.2 110 00:20:42
Distance: (default is 110)

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 172.29.6.13
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Maximum path: 4

Routing for Networks:
Routing Information Sources:
Gateway Distance Last Update
Distance: (default is 110)

- Se verifica la red en la ruta del lado de la ciudad de Bogotá.

BOGOTA1#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 209.17.220.6
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.3.0 0.0.0.3 area 1
172.29.3.4 0.0.0.3 area 1
172.29.3.8 0.0.0.3 area 1
209.17.220.4 0.0.0.3 area 1
Passive Interface(s):
Serial0/0/0
Routing Information Sources:
Gateway Distance Last Update
172.29.3.13 110 00:25:17
172.29.3.14 110 00:25:16
209.17.220.6 110 00:25:15
Distance: (default is 110)

Routing Protocol is "ospf 2"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 172.29.3.9
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:

Routing Information Sources:
 Gateway Distance Last Update
 Distance: (default is 110)

```

BOGOTA1
Physical Config CLI Attributes
IOS Command Line Interface

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 209.17.220.6
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.0 0.0.0.3 area 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
    209.17.220.4 0.0.0.3 area 1
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway          Distance      Last Update
    172.29.3.13      110          00:25:17
    172.29.3.14      110          00:25:16
    209.17.220.6     110          00:25:15
  Distance: (default is 110)

Routing Protocol is "ospf 2"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 172.29.3.9
  Number of areas in this router is 0. 0 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing Information Sources:
    Gateway          Distance      Last Update
  Distance: (default is 110)

BOGOTA1#
  
```

Figura 13. Show Ip protocols

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.

```

MEDELLIN1#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
172.29.6.5 0 FULL/ - 00:00:32 172.29.6.2 Serial0/0/1
172.29.6.14 0 FULL/ - 00:00:30 172.29.6.10 Serial0/1/0
172.29.6.14 0 FULL/ - 00:00:30 172.29.6.14 Serial0/1/1
MEDELLIN1#
  
```

```

MEDELLIN2#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
  
```

```
209.17.220.2 0 FULL/ - 00:00:30 172.29.6.1 Serial0/0/0
172.29.6.14 0 FULL/ - 00:00:30 172.29.6.6 Serial0/0/1
MEDELLIN2#
```

```
MEDELLIN3#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
209.17.220.2 0 FULL/ - 00:00:30 172.29.6.9 Serial0/0/0
209.17.220.2 0 FULL/ - 00:00:31 172.29.6.13 Serial0/0/1
172.29.6.5 0 FULL/ - 00:00:39 172.29.6.5 Serial0/1/0
MEDELLIN3#
```

```
BOGOTA1#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
172.29.3.13 0 FULL/ - 00:00:37 172.29.3.10 Serial0/0/1
172.29.3.14 0 FULL/ - 00:00:35 172.29.3.2 Serial0/1/0
172.29.3.14 0 FULL/ - 00:00:34 172.29.3.6 Serial0/1/1
BOGOTA1#
```

```
BOGOTA2#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
209.17.220.6 0 FULL/ - 00:00:33 172.29.3.9 Serial0/0/0
172.29.3.14 0 FULL/ - 00:00:31 172.29.3.14 Serial0/0/1
BOGOTA2#
```

```
BOGOTA3#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
209.17.220.6 0 FULL/ - 00:00:31 172.29.3.1 Serial0/0/0
209.17.220.6 0 FULL/ - 00:00:31 172.29.3.5 Serial0/0/1
172.29.3.13 0 FULL/ - 00:00:33 172.29.3.13 Serial0/1/0
BOGOTA3#
```

```

Password:
MEDELLIN1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address      Interface
172.29.6.5       0     FULL/ -         00:00:36   172.29.6.2   Serial0/0/1
172.29.6.14     0     FULL/ -         00:00:35   172.29.6.10  Serial0/1/0
172.29.6.14     0     FULL/ -         00:00:36   172.29.6.14  Serial0/1/1
MEDELLIN1#

```

```

BOGOTA1#en
BOGOTA1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address      Interface
172.29.3.13     0     FULL/ -         00:00:35   172.29.3.10  Serial0/0/1
172.29.3.14     0     FULL/ -         00:00:35   172.29.3.2   Serial0/1/0
172.29.3.14     0     FULL/ -         00:00:35   172.29.3.6   Serial0/1/1
BOGOTA1#

```

Figura 14. show ip ospf neighbor

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>EN

ISP#config t

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

ISP(config)#username MEDELLIN1 password cisco

ISP(config)#int s0/0/0

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

ISP(config-if)#encapsulation ppp

ISP(config-if)#ppp authentication pap

ISP(config-if)#ppp pap sent-username ISP password cisco

ISP(config-if)#

EN MEDELLIN1

MEDELLIN1(config)#int s0/0/0

MEDELLIN1(config-if)#encapsulation ppp

MEDELLIN1(config-if)#ppp authentication pap

MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco

MEDELLIN1(config-if)#

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

```
MEDELLIN1(config-if)#end
MEDELLIN1#
%SYS-5-CONFIG_I: Configured from console by console
```

Para comprobar la conexión hacemos ping al otro extremo en este caso a ISP que tiene la ip 209.17.220.1

```
MEDELLIN1#ping 209.17.220.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/7/35 ms
MEDELLIN1#
```

Fue satisfactorio el ping esto quiere decir que hay conexión

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

En BOGOTA1

```
BOGOTA1(config)#username ISP password cisco
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
BOGOTA1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state
to up
```

En ISP

```
ISP(config)#int s 0/0/1
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)#  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state  
to up
```

```
ISP(config-if)#end  
ISP#  
%SYS-5-CONFIG_I: Configured from console by console
```

- Para comprobar la conexión hacemos un ping al otro extremo en este caso a BOGOTA1 209.17.220.6

```
ISP#ping 209.17.220.6
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/8/37 ms
```

```
ISP>en  
Password:  
ISP#ping 209.17.220.6  
  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms  
  
ISP#
```

Figura 15 ping desde ISP a 209.17.220.6

```
ISP#
```

El ping fue satisfactorio comprobando que hay conexión

Se configura DHCP

```
MEDELLIN2(config)#ip dhcp pool MEDELLIN2  
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128  
MEDELLIN2(dhcp-config)#default-router 172.29.4.1  
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8  
MEDELLIN2(dhcp-config)#exit
```

```
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#
```

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.

```
MEDELLIN1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/0 overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#int s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int s0/1/1
MEDELLIN1(config-if)#ip nar inside
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#
```

```
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-if)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip nat inside
```

```
BOGOTA1(config-if)#int s0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#
```

Se comprueba con ping desde HOTS 150 a ISP

```
C:\>ping 209.17.220.5
```

Ping 209.17.220.5 with 32 bytes of data:

```
Reply from 209.17.220.5: bytes=32 time=2ms TTL=253
Reply from 209.17.220.5: bytes=32 time=4ms TTL=253
Reply from 209.17.220.5: bytes=32 time=2ms TTL=253
Reply from 209.17.220.5: bytes=32 time=2ms TTL=253
```

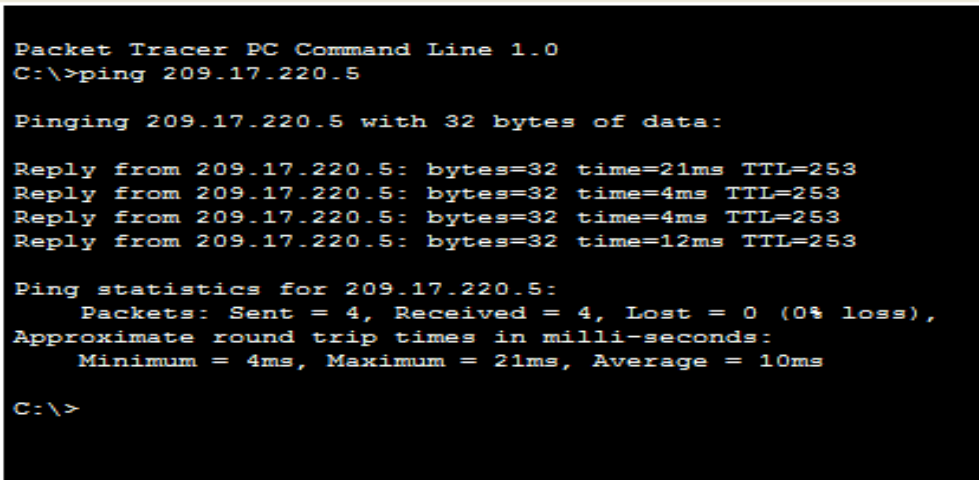
Ping statistics for 209.17.220.5:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 4ms, Average = 2ms

Es satisfactorio



```
Packet Tracer PC Command Line 1.0
C:\>ping 209.17.220.5

Pinging 209.17.220.5 with 32 bytes of data:

Reply from 209.17.220.5: bytes=32 time=21ms TTL=253
Reply from 209.17.220.5: bytes=32 time=4ms TTL=253
Reply from 209.17.220.5: bytes=32 time=4ms TTL=253
Reply from 209.17.220.5: bytes=32 time=12ms TTL=253

Ping statistics for 209.17.220.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 21ms, Average = 10ms

C:\>
```

Figura 16 Ping desde HOTS 150 a ISP

Y con ping desde HOTS 50 a ISP

```
C:\>ping 209.17.220.5
```

Pinging 209.17.220.5 with 32 bytes of data:

Reply from 209.17.220.5: bytes=32 time=39ms TTL=253
Reply from 209.17.220.5: bytes=32 time=3ms TTL=253
Reply from 209.17.220.5: bytes=32 time=2ms TTL=253
Reply from 209.17.220.5: bytes=32 time=2ms TTL=253

Ping statistics for 209.17.220.5:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 2ms, Maximum = 39ms, Average = 11ms

```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 209.17.220.5

Pinging 209.17.220.5 with 32 bytes of data:

Reply from 209.17.220.5: bytes=32 time=3ms TTL=253
Reply from 209.17.220.5: bytes=32 time=4ms TTL=253
Reply from 209.17.220.5: bytes=32 time=2ms TTL=253
Reply from 209.17.220.5: bytes=32 time=11ms TTL=253

Ping statistics for 209.17.220.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 5ms

C:\>
```

Figura 17 ping desde HOTS 50 a ISP

Es satisfactorio

Sin embargo con ping desde HOTS 150 al HOTS 50 no debe ser satisfactorio debido a que nat bloquea la traducción de afuera hacia adentro.

Si se borra NAT Y PAT el ping va a funcionar normalmente.

C:\>ping 172.29.4.6

Pinging 172.29.4.6 with 32 bytes of data:

Reply from 172.29.0.1: Destination host unreachable.

Request timed out.

*Reply from 172.29.0.1: Destination host unreachable.
Request timed out.*

*Ping statistics for 172.29.4.6:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),*

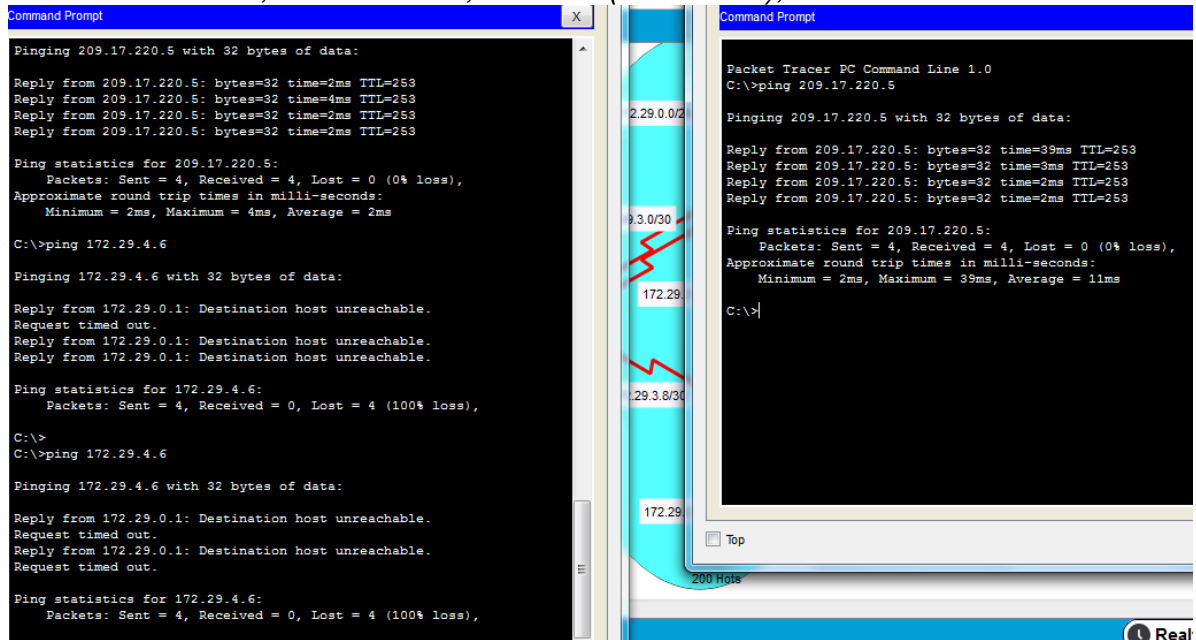


Figura18. Comprobación comando ping

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.

Se excluyen algunas direcciones ip que no serán utilizadas en DHCP

```
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)#
```

El pc Host 40 aun no puede ingresar a MEDELLIN2 primero se debe configurar en MEDELLIN3 un redireccionamiento para que se puedan conectar MEDELLIN2 con DHCP

```
MEDELLIN3(config)#int g0/0  
MEDELLIN3(config-if)#ip helper-address 172.29.6.5  
MEDELLIN3(config-if)#
```

```
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#
```

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

```
MEDELLIN1(config)#interface g0/0
MEDELLIN1(config-if)#ip helper-address 172.29.4.1
MEDELLIN1(config-if)#
```

- c. Configurar red Bogota2 y Bogota3 donde el router Medellin2 debe ser el servidor DHCP para ambas redes Lan.

Se excluyen algunas direcciones IP que no serán utilizadas en DHCP

```
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
```

```
BOGOTA2(config)#ip dhcp pool BOGOTA2
BOGOTA2(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 8.8.8.8
BOGOTA2(dhcp-config)#ip dhcp pool BOGOTA3
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#
```

```
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
BOGOTA3(config-if)#
```

- Se activa DHCP en ambas computadoras

Se puede comprobar la conexión haciendo un ping de HOST 150 HOST 200
Que está en otra red pero dentro del mismo Bogotá.

```
C:\>ping 172.29.1.6
```

Ping 172.29.1.6 with 32 bytes of data:

Reply from 172.29.1.6: bytes=32 time=1ms TTL=126

Reply from 172.29.1.6: bytes=32 time=1ms TTL=126

Reply from 172.29.1.6: bytes=32 time=1ms TTL=126

Reply from 172.29.1.6: bytes=32 time=1ms TTL=126

Ping statistics for 172.29.1.6:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

Fue satisfactorio el ping

```
Pinging 172.29.1.6 with 32 bytes of data:

Reply from 172.29.1.6: bytes=32 time=2ms TTL=126
Reply from 172.29.1.6: bytes=32 time=1ms TTL=126
Reply from 172.29.1.6: bytes=32 time=1ms TTL=126
Reply from 172.29.1.6: bytes=32 time=3ms TTL=126

Ping statistics for 172.29.1.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 1ms

C:\>
```

Figura 19 ping HOST 150 HOST 200

Los demás ping entre Bogotá y Medellín no funcionan se debe reiniciar los tres router isp bogota1 y medellin1 surgieron problemas de conectividad en el momento que se configuro PPP PAT CHAT.

BOGOTA1#copy run start

Destination filename [startup-config]?

*Building configuration...
[OK]
BOGOTA1#reload
Proceed with reload? [confirm]*

*ISP#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
ISP#reload
Proceed with reload? [confirm]*

*MEDELLIN1#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
MEDELLIN1#reload
Proceed with reload? [confirm]*

CONCLUSIONES

- Se Desarrollaron los dos escenarios propuesto aplicando los conocimientos adquiridos en el diplomado de profundización de CCNA en los cuales están los conceptos básicos y prácticos para aplicar en networking.
- En el escenario uno se utilizó el protocolo de enrutamiento RIP es sencillo y tiene compatibilidad, una desventaja es el límite de saltos, es un protocolo de enrutamiento por vector.
- En el escenario dos se utilizó el protocolo de enrutamiento OSPF el cual mejora algunas limitaciones de RIP ofrece escalabilidad en redes mayores y converge más rápido.
- Se verificaron y desarrollaron las topologías de cada escenario y se trabajaron según lo solicitado por medio de herramientas de simulación, en este caso se trabajó en Packet Tracer.
- Se aplican los conocimientos y habilidades adquiridas en el desarrollo del actual curso.
- Se reconoce e identifica la necesidad y utilización practica de las redes LAN y WAN.
- Los protocolos de enrutamiento OSPF y RIPv2 son esenciales para el desarrollo de las topologías los cuales permiten intercomunicar computadoras para diseñar redes según la necesidad del usuario.
- Los datos fluyen a través de las redes desde un origen a un destino, utilizando los routers de manera dinámica con protocolos de enrutamiento manual, usando rutas estáticas.
- El progreso de las actividades permitieron visualizar los retos a los que nos enfrentaremos en nuestra futura vida laboral, los laboratorios las prácticas el desarrollo del diplomado, las tutorías son una herramienta indispensables para adquirir conocimiento.

BIBLIOGRAFÍA

CISCO. (2017). Exploración de la red. Fundamentos de Networking. Recuperado de

<https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>

CISCO. (2017). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de [https://static-course-](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1)

[assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1)

CISCO. (2017). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de [https://static-course-](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1)

[assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1)

CISCO. (2017). Ethernet. Fundamentos de Networking. Recuperado de [https://static-course-](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1)

[assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1)

CISCO. (2017). Capa de red. Fundamentos de Networking. Recuperado de [https://static-course-](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1)

[assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1](https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1)

UNAD (2017). Diseño y configuración de redes con Packet Tracer [OVA].

Recuperado de https://1drv.ms/u/s!AmIJYei-NT1lhgCT9VCtl_pLtPD9

Vesga, J. (2019). Introducción al Laboratorio Remoto SmartLab [OVI]. Recuperado de <http://hdl.handle.net/10596/24167>

[http://www.unipamplona.edu.co/unipamplona/portallG/home_15/recursos/01_gene](http://www.unipamplona.edu.co/unipamplona/portallG/home_15/recursos/01_general/09062014/n_icontec.pdf)

[ral/09062014/n_icontec.pdf](http://www.unipamplona.edu.co/unipamplona/portallG/home_15/recursos/01_general/09062014/n_icontec.pdf)

<https://1314297.netacad.com/courses/973101>

<https://www.netacad.com/>

<https://campus113.unad.edu.co/ecbti63/course/view.php?id=23>

<https://www.definicionabc.com/tecnologia/router.php>

