

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

ALEXANDER HERRERA GUTIÉRREZ

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS**

BOGOTÁ D.C.

2020

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

ALEXANDER HERRERA GUTIÉRREZ

Evaluación – Prueba de Habilidades Prácticas CCNA

Tutor: JOSE IGNACIO CARDONA

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERÍA DE SISTEMAS
BOGOTÁ D.C.**

2020

Nota de aceptación

Presidente del jurado

Jurado

Jurado

Bogotá D.C., 15/05/2020

AGRADECIMIENTOS

Agradezco a Dios en primer lugar por darme la oportunidad de terminar este ciclo académico de la mejor manera.

En segundo lugar, agradezco a todos y a cada uno de los tutores y directores de curso de la Universidad Nacional Abierta y a Distancia - UNAD quienes estuvieron presentes en mi formación académica contribuyendo con su experiencia en la construcción de mi proyecto profesional.

Agradezco especialmente a mi esposa Viviana Andrea Castillo y a mi familia por su apoyo incondicional y motivacional en este proceso formativo en el cual estoy siendo partícipe.

TABLA DE CONTENIDO

LISTADO DE TABLAS.....	6
LISTADO DE GRÁFICOS.....	7
INTRODUCCIÓN.....	8
OBJETIVO GENERAL.....	9
OBJETIVOS ESPECÍFICOS.....	9
ESCENARIO 1.....	10
Parte 1. Inicializar dispositivos.....	11
Parte 2. Configurar los parámetros básicos de los dispositivos.....	12
Parte 3. Configurar la seguridad del switch, las VLAN y el routing entre VLAN.....	23
Parte 4. Configurar el protocolo de routing dinámico RIPv2.....	30
Parte 5. Implementar DHCP y NAT para IPv4.....	35
Parte 6. Configurar NTP.....	39
Parte 7. Configurar y verificar las listas de control de acceso (ACL).....	40
ESCENARIO 2.....	43
Parte 1. Configuración del enrutamiento.....	44
Parte 2. Tabla de Enrutamiento.....	52
Parte 3. Deshabilitar la propagación del protocolo OSPF.....	56
Parte 4. Verificación del protocolo OSPF.....	58
Parte 5. Configurar encapsulamiento y autenticación PPP.....	60
Parte 6. Configuración de PAT.....	62
Parte 7. Configuración del servicio DHCP.....	64
CONCLUSIONES.....	66
REFERENCIAS BIBLIOGRÁFICAS.....	67

LISTADO DE TABLAS

Tabla 1 Inicialización y cargue de los dispositivos	11
Tabla 2 Direccionamiento IP de la computadora de Internet.....	12
Tabla 3 Configuración básica del Router 1	14
Tabla 4 Configuración básica del Router 2	17
Tabla 5 Configuración básica del Router 3	19
Tabla 6 Configuración básica del Switch 1.....	19
Tabla 7 Configuración básica del Switch 3.....	20
Tabla 8 Ping entre los dispositivos de la red.....	22
Tabla 9 Configuración IP y VLANs de Switch 1	24
Tabla 10 Configuración IP y VLANs de Switch 3	26
Tabla 11 Configuración de interface GigaEthernet de Router 1.....	27
Tabla 12 Evidencia de Ping entre dispositivos.....	29
Tabla 13 Configuración de RIPv2 en Router 1.....	30
Tabla 14 Configuración de RIPv2 en Router 2.....	31
Tabla 15 Configuración de RIPv2 en Router 3.....	32
Tabla 16 Verificación de información de RIP	34
Tabla 17 Configuración DHCP para las VLAN 21 y 23 en Router 1.....	35
Tabla 18 Configuración NAT estática y dinámica en Router 2.....	37
Tabla 19 Verificación del protocolo DHCP y la NAT estática	38
Tabla 20 Configuración NTP en Router 1 y Router 2.....	39
Tabla 21 Restricción del acceso a las líneas VTY en Router 2.....	40
Tabla 22 Descripción de comandos en CLI	42
Tabla 23 Interfaces que no requieren desactivación.....	57

LISTADO DE GRÁFICOS

Gráfico 1 Primer estudio de caso. Prueba de Habilidades Practicas	10
Gráfico 2 Topología realizada en Packet Tracer. Imagen propia	10
Gráfico 3 Ping de Router 1 a Router 2. Imagen propia	21
Gráfico 4 Ping de R2 a R3. Imagen propia	21
Gráfico 5 Ping de Switch1 a Router1 (VLAN 99). Imagen propia.....	28
Gráfico 6 Ping de Switch3 a Router1 (VLAN 99). Imagen propia.....	28
Gráfico 7 Ping de Switch1 a Router1 (VLAN 21). Imagen propia.....	28
Gráfico 8 Ping de Switch3 a Router1 (VLAN23). Imagen propia.....	29
Gráfico 9 Dirección IP DHCP de PC-A. Imagen propia.....	37
Gráfico 10 Dirección IP DHCP de PC-C. Imagen propia.....	38
Gráfico 11 Ping de PC-A a PC-C. Imagen propia	38
Gráfico 12 Evidencia de navegación de computadora de Internet. Imagen propia	38
Gráfico 13 Segundo estudio de caso. Prueba de Habilidades Practicas.....	43
Gráfico 14 Tabla de enrutamiento. Imagen propia	53
Gráfico 15 Comando show ip route en Bogotá2. Imagen propia.....	53
Gráfico 16 Comando show ip route en ISP. Imagen propia	54
Gráfico 17 Comando show ip route en Bogota3. Imagen propia.....	54
Gráfico 18 Comando show ip route en Medellin1. Imagen propia.....	55
Gráfico 19 Comando show ip route en Medellin2. Imagen propia.....	55
Gráfico 20 Comando show ip route en Medellin3. Imagen propia.....	56
Gráfico 21 Base de datos OSPF de Router Bogota1. Imagen propia	59
Gráfico 22 Base de datos OSPF de Router Bogota2. Imagen propia	59
Gráfico 23 Base de datos OSPF de Router Bogota3. Imagen propia	60
Gráfico 24 Base de datos OSPF de Router Medellin1. Imagen propia	60
Gráfico 25 Base de datos OSPF de Router Medellin2. Imagen propia	60
Gráfico 26 Base de datos OSPF de Router Medellin3. Imagen propia	61
Gráfico 27 Configuración DHCP en PCs en la red de Bogotá. Imagen propia.....	65

INTRODUCCIÓN

Desde el inicio y/o nacimiento de las redes de computadoras por allá en los años 50's, éstas se han convertido en una herramienta que facilita la vida del ser humano en cuanto a procesos en las que éstas sean utilizadas, dando a su vez flexibilidad, rapidez y dinamismo a las tareas que se estén desempeñando. Desde los años 50's que fue el inicio de las redes de computadoras hasta la fecha de hoy y a través de todo el tiempo que ha transcurrido, las redes han transformado el diario vivir de las personas gracias a sus innumerables cambios que incluyen técnicas y métodos para la comunicación de las mismas haciendo de esto una parte fundamental para la existencia.

En este trabajo escrito se pretende dar a entender los nuevos conocimientos adquiridos en el Diplomado de Profundización Cisco (Diseño e Implementación de Soluciones Integradas LAN / WAN) correspondiente a la opción de grado del periodo 2020-I. En este estudio se da a conocer la aplicación de enrutamientos en una red de datos con sus respectivos parámetros de seguridad y acceso en los diferentes dispositivos en la red. De igual manera, se dan a conocer las configuraciones de RIP, NAT, OSPF y la verificación de listas ACL. Todo lo anterior se realiza en los dispositivos enrutadores (Router) con el fin de dar mayor solidez y estabilidad a una red o también puede aplicar para otorgar transferencia de paquetes según las políticas adecuadas para los dispositivos. Teniendo en cuenta las distintas formas de conexión existente entre redes, también se da a conocer uno de los protocolos más utilizados: el protocolo DHCP; es un sistema de reglas que permiten que dos o más dispositivos de un sistema de comunicación se comuniquen entre ellas.

OBJETIVO GENERAL

Analizar y resolver detalladamente los dos estudios de caso establecidos en el Diplomado de Profundización Cisco mediante el uso de aplicativos de simulación Packet Tracer / GNS3.

OBJETIVOS ESPECÍFICOS

- Diseñar la topología en el software de simulación Packet Tracer / GNS3 según la parametrización entregada en el estudio de caso.
- Configurar de forma detallada los direccionamientos de conexión de los routers y switches de la topología entregada en el estudio de caso.
- Configurar de forma detallada las VLANs, los puertos troncales, los puertos de acceso, el encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red entregada.
- Comprobar la conectividad entre los dispositivos de la topología entregada una vez se haya terminado el trabajo.

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

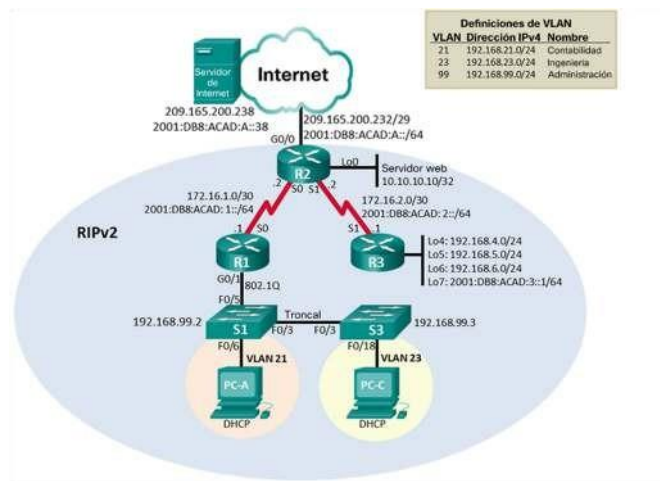


Gráfico 1 Primer estudio de caso. Prueba de Habilidades Practicas

Topología realizada en Packet Tracer

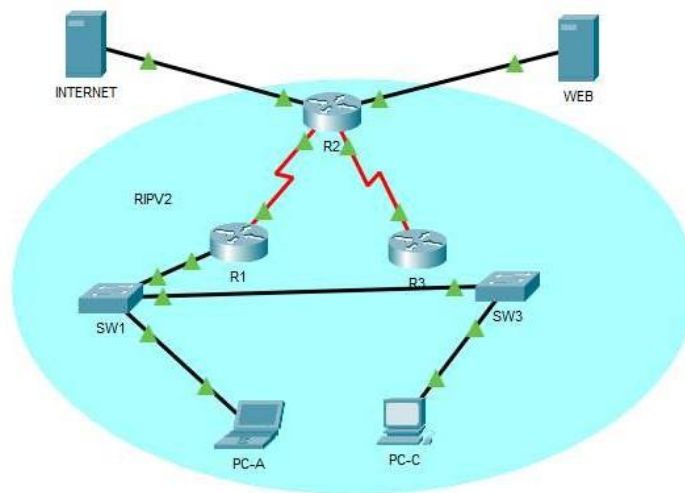


Gráfico 2 Topología realizada en Packet Tracer. Imagen propia

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.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Se digita el comando: Router#erase startup-config
Volver a cargar todos los routers	Se introduce el comando: Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Para hacer el borrado del archivo en mención se ingresa el comando: Switch#erase startup-config Para hacer el borrado de la base de datos de VLAN se ingresa el comando: Switch#delete flash:vlan.dat
Volver a cargar ambos switches	Se digita el comando: Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Se utiliza el comando: Switch#show vlan brief

Tabla 1 Inicialización y cargue de los dispositivos

Parte 2. Configurar los parámetros básicos de los dispositivos.

Paso 1: Configurar la computadora de Internet.

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	Se ingresa al servidor de Internet, se ubica la pestaña "Desktop" y se configura la dirección IPv4: 209.165.200.238
Máscara de subred para IPv4	Se ingresa al servidor de Internet, se ubica la pestaña "Desktop" y se configura la máscara de subred IPv4: 255.255.255.248
Gateway predeterminado	Se ingresa al servidor de Internet, se ubica la pestaña "Desktop" y se configura la Puerta de enlace predeterminada o Default Gateway: 209.165.200.233
Dirección IPv6/subred	Se ingresa al servidor de Internet, se ubica la pestaña "Desktop" y se registra la dirección IPv6: 2001:DB8:ACAD:A::1/64
Gateway predeterminado IPv6	Se ingresa al servidor de Internet, se ubica la pestaña "Desktop" y se configura la Puerta de enlace predeterminada o Default Gateway: 2001:DB8:ACAD:A::2/64

Tabla 2 Direcciónamiento IP de la computadora de Internet

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:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para desactivar la búsqueda DNS Se digita el comando: Router(config)#no ip domain-lookup

Nombre del router	Se Utiliza el comando: Router (config) #hostname R1 R1 (config) #
Contraseña de exec privilegiado cifrada	Se introduce el comando: R1 (config) #enable secret class
Contraseña de acceso a la consola	Se digita la siguiente línea de comando: R1 (config) #line console 0 R1 (config-line) #password cisco R1 (config-line) #login
Contraseña de acceso Telnet	Se digita la siguiente línea de comando: R1 (config) #line vty 0 4 R1 (config-line) #password cisco R1 (config-line) #login
Cifrar las contraseñas de texto no cifrado	Se Utiliza el comando: R1 (config) #service password-encryption
Mensaje MOTD	Se configura con el commando: R1 (config) #banner motd # Se prohíbe el acceso no autorizado. #

<p>Interfaz S0/0/0</p>	<p>Se configura la interface serial 0/0/0 con el siguiente comando:</p> <pre>R1(config)#int s0/0/0 R1(config-if)#description Trunk R1 to R2s0/0/0</pre> <p>Establecer la dirección Ipv4 Consultar el diagrama de topología para conocer la información de direcciones es: 172.16.1.0/30</p> <p>Establecer la dirección Ipv6 Consultar el diagrama de topología para conocer la información de direcciones es:</p> <pre>2001:DB8:ACAD:1::/64</pre> <p>Con el siguiente comando se establece la frecuencia de reloj: R1(config-if)#clock rate 128000</p> <pre>R1(config-if)#no shutdown R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64</pre>
<p>Rutas predeterminadas</p>	<p>Se digita el siguiente comando con la respectiva ruta predeterminada IPv4 para que coincida con cualquier dirección: R1(config)# ip route 0.0.0.0 0.0.0.0 Serial0/0/0</p> <p>Se digita el siguiente comando con la respectiva ruta predeterminada IPv6 para que coincida con cualquier dirección: R1(config)#ipv6 route ::/0 serial 0/0/0 2001:DB8:ACAD:1::1</p>

Tabla 3 Configuración básica del Router 1

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2.

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para desactivar la búsqueda DNS Se digita el comando: Router(config)#no ip domain-lookup
Nombre del router	Se Utiliza el comando: Router (config) #hostname R2 R2 (config) #
Contraseña de exec privilegiado cifrada	Se utiliza el comando: R2 (config) #enable secret class
Contraseña de acceso a la consola	Se digita la siguiente línea de comandos: R2 (config) #line console 0 R2 (config-line) #password cisco R2 (config-line) #login
Contraseña de acceso Telnet	Se digita la siguiente línea de comandos: R2 (config) #line vty 0 4 R2 (config-line) #password cisco R2 (config-line) #login
Cifrar las contraseñas de texto no cifrado	Se Utiliza el comando: R2 (config) #service password-encryption
Habilitar el servidor HTTP	Los siguientes comandos no son soportados en packet tracer: R2 (config) #ip http server R2 (config) #ip http secure-server R2 (config) #ip http autenticación local
Mensaje MOTD	Se configura con el comando: R2 (config) #banner motd # Se prohíbe el acceso no autorizado #

<p>Interfaz S0/0/0</p>	<p>Se configura la interface serial 0/0/0 con el siguiente comando:</p> <pre>R2(config)#int s0/0/0 R2(config-if)#description Trunk R2 to R1s0/0/0 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</pre>
<p>Interfaz S0/0/1</p>	<p>Se configura la interface serial 0/0/1 con el siguiente comando:</p> <pre>R2(config-if)#int s0/0/1 R2(config-if)#description Trunk R2 to R3s0/0/1 R2(config-if)#clock rate 128000 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R2(config-if)#no shutdown</pre>
<p>Interfaz G0/0 (simulación de Internet)</p>	<p>Se configura la interface gigaEthernet G0/0 con el siguiente comando:</p> <pre>R2(config-if)#interface gigabitEthernet 0/0</pre> <p>Descripción de la interface G0/0 que indica hacía donde va conectada:</p> <pre>R2(config-if)#description Servidor de Internet f0/0</pre> <p>Se configura la dirección IPv4 con su respectiva mascara de subred:</p> <p>Se configura la dirección IPv4:</p> <pre>R2(config-if)#ip address 209.165.200.233 255.255.255.248</pre> <p>Se configura la dirección IPv6 con su respectiva mascara de subred:</p> <pre>R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64</pre>

Interfaz loopback 0 (servidor web simulado)	<p>Se digita el comando:</p> <pre>R2(config-if)#interface loopback 0 R2(config-if)#description Servidor web simulado R2(config-if)#ip address 10.10.10.10 255.255.255.255</pre>
Ruta predeterminada	<p>Se digita el siguiente comando con la respectiva ruta predeterminada IPv4 para que coincida con cualquier dirección:</p> <pre>R2(config)#ip route 0.0.0.0 0.0.0.0 gigabitEthernet 0/0 1</pre> <p>Se digita el siguiente comando con la respectiva ruta predeterminada IPv6 para que coincida con cualquier dirección:</p> <pre>R2(config)#ipv6 route ::/0 gigabitEthernet 0/0 2001:DB8:ACAD:A::1</pre>

Tabla 4 Configuración básica del Router 2

Paso 4: Configurar R3.

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para desactivar la búsqueda DNS Se digita el comando: R3(config)#no ip domain-lookup
Nombre del router	Se Utiliza el comando: R3(config)#hostname R3
Contraseña de exec privilegiado cifrada	Se digita el comando: R3(config)#enable secret class
Contraseña de acceso a la consola	Se digita la siguiente línea de comandos: R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	Se digita la siguiente línea de comandos: R3(config-line)#line vty 0 4 R3(config-line)#password cisco R3(config-line)#login

Cifrar las contraseñas de texto no cifrado	<p>Se introduce el comando: R3(config-line)#service password-encryption</p>
Mensaje MOTD	<p>Se digita el comando: R3(config)#banner motd # Se prohíbe el acceso no autorizado #</p>
Interfaz S0/0/1	<p>Se configura la interface serial 0/0/1 con el siguiente comando: R3(config)#int s0/0/1 R3(config-if)#description Trunk R3 to R2s0/0/1 R3(config-if)#clock rate 128000 This command applies only to DCE interfaces R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64 R3(config-if)#no shutdown</p>
Interfaz loopback 4	<p>Se digita el comando: R3(config-if)#interface loopback 4</p> <p>R3(config-if)#description Servidor web simulado R3(config-if)#ip address 192.168.4.1 255.255.255.0</p>
Interfaz loopback 5	<p>Se utiliza el comando: R3(config-if)#interface loopback 5</p> <p>R3(config-if)#description Servidor web simulado R3(config-if)#ip address 192.168.5.1 255.255.255.0</p>
Interfaz loopback 6	<p>Se introduce el comando: R3(config-if)#interface loopback 6</p> <p>R3(config-if)#description Servidor web simulado R3(config-if)#ip address 192.168.6.1 255.255.255.0</p>

Interfaz loopback 7	<p>Se digita el comando: R3(config-if)#interface loopback 7</p> <p>R3(config-if)#description Servidor web simulado R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64</p>
Rutas predeterminadas	

Tabla 5 Configuración básica del Router 3

Paso 5: Configurar S1.

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<p>Se introduce el comando: SW1(config)#no ip domain-lookup</p>
Nombre del switch	<p>Se utiliza el comando: SW1(config)#hostname SW1</p>
Contraseña de exec privilegiado cifrada	<p>Se usa el comando: SW1(config)#enable secret class</p>
Contraseña de acceso a la consola	<p>Se digita la siguiente línea de comandos: SW1(config)#line console 0 SW1(config-line)#password cisco SW1(config-line)#login</p>
Contraseña de acceso Telnet	<p>Se digita la siguiente línea de comandos: SW1(config-line)#line vty 0 4 SW1(config-line)#password cisco SW1(config-line)#login</p>
Cifrar las contraseñas de texto no cifrado	<p>Se digita el comando: SW1(config-line)#service password-encryption</p>
Mensaje MOTD	<p>Se configura con el comando: SW1(config)#banner motd # Se prohíbe el acceso no autorizado #</p>

Tabla 6 Configuración básica del Switch 1

Paso 6: Configurar el S3.

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Para desactivar la búsqueda DNS se digita el comando: Switch(config)#no ip domain-lookup
Nombre del switch	Se introduce el comando: Switch(config)#hostname SW3
Contraseña de exec privilegiado cifrada	Se usa el comando: SW3(config)#enable secret class
Contraseña de acceso a la consola	Se digita la siguiente línea de comandos: SW3(config)#line console 0 SW3(config-line)#password cisco SW3(config-line)#login
Contraseña de acceso Telnet	Se digita la siguiente línea de comandos: SW3(config-line)#line vty 0 4 SW3(config-line)#password cisco SW3(config-line)#login
Cifrar las contraseñas de texto no cifrado	Se introduce el comando: SW3(config-line)#service password-encryption
Mensaje MOTD	Se configura con el comando: SW3(config)#banner motd # Se prohíbe el acceso no autorizado #

Tabla 7 Configuración básica del Switch 3

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:

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2	<pre> R1# R1#ping 172.16.1.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/16 ms </pre> <p style="text-align: center;"><i>Gráfico 3 Ping de Router 1 a Router 2. Imagen propia</i></p>
R2	R3, S0/0/1	172.16.2.1	<pre> R3#ping 172.16.2.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms R3# </pre> <p style="text-align: center;"><i>Gráfico 4 Ping de R2 a R3. Imagen propia</i></p>
PC de Internet	Gateway predeterminado	200.165.200.233	<pre> C:\>ping 200.165.200.233 Pinging 200.165.200.233 with 32 bytes of data: Reply from 200.165.200.233: bytes=32 time=10ms TTL=128 </pre>

			<pre> Reply from 200.165.200.238: bytes=32 time=20ms TTL=128 Reply from 200.165.200.233: bytes=32 time=13ms TTL=128 Reply from 200.165.200.233: bytes=32 time=2ms TTL=128 Ping statistics for 200.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 2ms, Maximum = 20ms, Average = 11ms </pre>
--	--	--	--

Tabla 8 Ping entre los dispositivos de la red

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

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:

Elemento o tarea de configuración	Especificación
<p>Crear la base de datos de VLAN</p>	<p>Se configuran las siguientes VLANs con los comandos:</p> <pre>SW1(config)#vlan 21 SW1(config-vlan)#name Contabilidad SW1(config-vlan)#vlan 26 SW1(config-vlan)#name Ingenieria SW1(config-vlan)#vlan 99 SW1(config-vlan)# %LINK-5-CHANGED: Interface Vlan99, changed state to up SW1(config-vlan)#name Administracion SW1(config-vlan)#</pre>
<p>Asignar la dirección IP de administración.</p>	<p>Se configura la dirección IPv4 de la VLAN 99 :</p> <pre>SW1(config)#interface vlan 99 SW1(config-if)#description Administracion SW1(config-if)#ip address 192.168.99.2 255.255.255.0</pre>
<p>Asignar el gateway predeterminado</p>	<p>Se configura la dirección IPv4 del Default Gateway:</p> <pre>SW1(config)#ip default-gateway 192.168.99.2</pre>
<p>Forzar el enlace troncal en la interfaz F0/3</p>	<p>Se fuerza el enlace troncal con el comando:</p> <pre>SW1(config-if)#interface F0/3 SW1(config-if)#switchport mode trunk SW1(config-if)#switchport trunk native vlan 1</pre>

<p>Forzar el enlace troncal en la interfaz F0/5</p>	<p>Se fuerza el enlace troncal con el comando: SW1(config-if)#interface F0/5 SW1(config-if)#switchport mode trunk SW1(config-if)#switchport trunk native vlan 1</p>
<p>Configurar el resto de los puertos como puertos de acceso</p>	<p>Se configuran los puertos de acceso con los comandos: SW1(config-if-range)#interface range fastEthernet 0/1 -2 SW1(config-if-range)#switchport mode Access SW1(config)#interface r fastEthernet 0/4 SW1(config-if)#switchport mode Access SW1(config-if-range)#interface range fastEthernet 0/7 - 24 SW1(config-if-range)#switchport mode access</p>
<p>Asignar F0/6 a la VLAN 21</p>	<p>Se configura la VLAN 21 en la interface F0/6: SW1(config)#interface fastethernet 0/6 SW1(config-if)#switchport mode access SW1(config-if)#switchport access vlan 21</p>
<p>Apagar todos los puertos sin usar</p>	<p>Se introduce las siguientes líneas de comandos: SW1(config)#interface range fastEthernet 0/1 -4 SW1(config-if-range)#shutdown SW1(config-if-range)#interface range fastEthernet 0/7 -24 SW1(config-if-range)#shutdown</p>

Tabla 9 Configuración IP y VLANs de Switch 1

Paso 2: Configurar el S3.

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Se configuran las siguientes VLANs con los comandos: SW3 (config-vlan) #vlan 21 SW3 (config-vlan) #name Contabilidad SW3 (config-vlan) #vlan 23 SW3 (config-vlan) #name Ingenieria SW3 (config-vlan) #vlan 99 SW3 (config-vlan) #name Administracion
Asignar la dirección IP de administración	Se configura la dirección IPv4 de la VLAN 99: SW3 (config) #inter vlan 99 SW3 (config-if) #ip address 192.168.99.3 255.255.255.0
Asignar el gateway predeterminado.	Se configura la dirección IPv4 del Default Gateway: SW3 (config) #ip default-gateway 192.168.99.3
Forzar el enlace troncal en la interfaz F0/3	Se fuerza el enlace troncal con el comando: SW3 (config) #interface F0/3 SW3 (config-if) #switchport mode trunk
Configurar el resto de los puertos como puertos de acceso	Se configuran los puertos de acceso con los comandos: SW3 (config) #interface range fastEthernet 0/1 -2 SW3 (config-if-range) #switchport mode Access SW3 (config-if-range) #interface range fastEthernet 0/4 -17 SW3 (config-if-range) #switchport mode Access SW3 (config-if-range) #interface range fastEthernet 0/19 -24 SW3 (config-if-range) #switchport mode Access

Asignar F0/18 a la VLAN 21	<p>Se configura la VLAN 21 en la interface F0/18:</p> <pre>SW3(config-if)#interface F0/18 SW3(config-if)#switchport mode access SW3(config-if)#switchport access vlan 21</pre>
Apagar todos los puertos sin usar	<p>Se introduce las siguientes líneas de comandos:</p> <pre>SW3(config-if-range)#interface range fastEthernet 0/1 -2 SW3(config-if-range)#shut SW3(config-if-range)#interface range fastEthernet 0/4 -17 SW3(config-if-range)#shut SW3(config-if-range)#interface range fastEthernet 0/19 -24 SW3(config-if-range)#shut SW3(config-if-range)#</pre>

Tabla 10 Configuración IP y VLANs de Switch 3

Paso 3: Configurar R1.

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	<p>Se configura con la siguiente línea de comandos para la LAN Contabilidad:</p> <pre>R1(config)#interface GigabitEthernet0/1.21 R1(config-subif)#description Contabilidad - S1 F0/5</pre> <p>Se configura la encapsulación:</p> <pre>R1(config-subif)#encapsulation dot1Q 21 R1(config-subif)#ip address 192.168.21.2 255.255.255.0</pre>

<p>Configurar la subinterfaz 802.1Q .23 en G0/1</p>	<p>Se configura con la siguiente línea de comandos para la LAN Ingeniería: R1 (config-subif) #interface GigabitEthernet0/1.23 R1 (config-subif) #description Ingenieria - S1 F0/5</p> <p>Se configura la encapsulación: R1 (config-subif) #encapsulation dot1Q 23 R1 (config-subif) #ip address 192.168.23.2 255.255.255.0</p>
<p>Configurar la subinterfaz 802.1Q .99 en G0/1</p>	<p>Se configura con la siguiente línea de comandos para la LAN Administración: R1 (config-subif) #interface GigabitEthernet0/1.99 R1 (config-subif) #description Administracion - S1 F0/5</p> <p>Se configura la encapsulación: R1 (config-subif) #encapsulation dot1Q 99 R1 (config-subif) #ip address 192.168.99.5 255.255.255.0</p>
<p>Activar la interfaz G0/1</p>	<p>Se utiliza el comando: R1 (config) #interface GigabitEthernet0/1 R1 (config-if) #no shutdown</p>

Tabla 11 Configuración de interface GigaEthernet de Router 1

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:

Desde	A	Dirección IP	Resultados de ping
S1	R1, dirección VLAN 99	192.168.99.1	<pre> --* S1#ping 192.168.99.1 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/4/17 ms </pre> <p><i>Gráfico 5 Ping de Switch1 a Router1 (VLAN 99). Imagen propia</i></p>
S3	R1, dirección VLAN 99	192.168.99.3	<pre> R1#ping 192.168.99.3 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.99.3, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/11 ms R1# </pre> <p><i>Gráfico 6 Ping de Switch3 a Router1 (VLAN 99). Imagen propia</i></p>
S1	R1, dirección VLAN 21	192.168.21.2	<pre> SW1#ping 192.168.21.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms SW1# </pre> <p><i>Gráfico 7 Ping de Switch1 a Router1 (VLAN 21). Imagen propia</i></p>

S3	R1, dirección VLAN 23	192.168.23.2	<pre> SW3#ping 192.168.23.2 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.23.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/5/14 ms SW3# </pre> <p style="text-align: right;"><i>Gráfico 8 Ping de Switch3 a Router1 (VLAN23). Imagen propia</i></p>
----	-----------------------------	--------------	--

Tabla 12 Evidencia de Ping entre dispositivos

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:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Se digita el comando: R1(config)#router rip R1(config-router)#version 2
Anunciar las redes conectadas directamente	Redes conectadas directamente: R1(config-router)#network 192.168.21.0 R1(config-router)#network 192.168.23.0 R1(config-router)#network 192.168.99.0 R1(config-router)#network 172.16.1.0
Establecer todas las interfaces LAN como pasivas	Se introduce las siguientes líneas de comandos: R1(config-router)#passive-interface GigabitEthernet0/1 R1(config-router)#passive-interface GigabitEthernet0/1.21 R1(config-router)#passive-interface GigabitEthernet0/1.23 R1(config-router)#passive-interface GigabitEthernet0/1.99
Desactive la sumarización automática	Se utiliza el comando: R1(config-router)# default-information originate

Tabla 13 Configuración de RIPv2 en Router 1

Paso 2: Configurar RIPv2 en el R2.

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Se digita el comando: R2 (config)#router rip R2 (config-router)#version 2
Anunciar las redes conectadas directamente	Redes conectadas directamente: R2 (config-router)#network 172.16.1.0 R2 (config-router)#network 172.16.2.0 R2 (config-router)#network 209.165.200.232 R2 (config-router)#network 10.10.10.10
Establecer la interfaz LAN (loopback) como pasiva	Se ingresan las siguientes líneas de comandos: R2 (config-router)# R2 (config-router)#passive-interface loopback 0 R2 (config-router)#passive-interface s0/0/1 R2 (config-router)#passive-interface s0/0/0
Desactive la sumarización automática.	Se utiliza el comando: R2 (config-router)# default-information originate

Tabla 14 Configuración de RIPv2 en Router 2

Paso 3: Configurar RIPv2 en el R3.

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	Se introduce el comando: R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	Se ingresan las siguientes líneas de comandos: R3(config-router)#network 172.16.2.0 R3(config-router)#network 192.168.4.0 R3(config-router)#network 192.168.5.0 R3(config-router)#network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	Se digitan las siguientes líneas de comandos: R3(config-router)#passive-interface s0/0/1 R3(config-router)#passive-interface loopback 4 R3(config-router)#passive-interface loopback 5 R3(config-router)#passive-interface loopback 6 R3(config-router)#passive-interface loopback 7
Desactive la sumarización automática.	Se usa el comando: R3(config-router)# default-information originate

Tabla 15 Configuración de RIPv2 en Router 3

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	Se usa el comando: R1#Show ip protocols Routing Protocol is "rip"

<p>de routing y las interfaces pasivas configuradas en un router?</p>	<pre> Sending updates every 30 seconds, next due in 25 seconds Invalid after 180 seconds, hold down 180, flushed after 240 Outgoing update filter list for all interfaces is not set Incoming update filter list for all interfaces is not set Redistributing: rip Default version control: send version 2, receive 2 Interface Send Recv Triggered RIP Key- chain Serial0/0/0 2 2 Automatic network summarization is in effect Maximum path: 4 Routing for Networks: 172.16.0.0 192.168.21.0 192.168.23.0 192.168.99.0 Passive Interface(s): GigabitEthernet0/1 GigabitEthernet0/1.21 GigabitEthernet0/1.23 GigabitEthernet0/1.99 Routing Information Sources: Gateway Distance Last Update Distance: (default is 120) </pre>
<p>¿Qué comando muestra solo las rutas RIP?</p>	<p>Se utiliza el comando:</p> <pre> R1#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 </pre>

	<pre> Gateway of last resort is 0.0.0.0 to network 0.0.0.0 172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks C 172.16.1.0/30 is directly connected, Serial0/0/0 L 172.16.1.1/32 is directly connected, Serial0/0/0 192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.21.0/24 is directly connected, GigabitEthernet0/1.21 L 192.168.21.2/32 is directly connected, GigabitEthernet0/1.21 192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.23.0/24 is directly connected, GigabitEthernet0/1.23 L 192.168.23.2/32 is directly connected, GigabitEthernet0/1.23 192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks C 192.168.99.0/24 is directly connected, GigabitEthernet0/1.99 L 192.168.99.5/32 is directly connected, GigabitEthernet0/1.99 S* 0.0.0.0/0 is directly connected, Serial0/0/0 R1# </pre>
<p>¿Qué comando muestra la sección de RIP de la configuración en ejecución?</p>	<p>Se usa el comando: Show ip protocols</p>

Tabla 16 Verificación de información de RIP

Parte 5. Implementar DHCP y NAT para IPv4.

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

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	Se digita el comando: 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	Se introduce el comando: R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Se configura bajo las líneas de comandos para la VLAN 21: R1(dhcp-config)#ip dhcp pool ACCT R1(dhcp-config)# R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#network 192.168.21.0 255.255.255.0
Crear un pool de DHCP para la VLAN 23	Se configura bajo las líneas de comandos para la VLAN 23: R1(dhcp-config)#ip dhcp pool ENGNR R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#network 192.168.23.0 255.255.255.0

Tabla 17 Configuración DHCP para las VLAN 21 y 23 en Router 1

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

La configuración del R2 incluye las siguientes tareas:

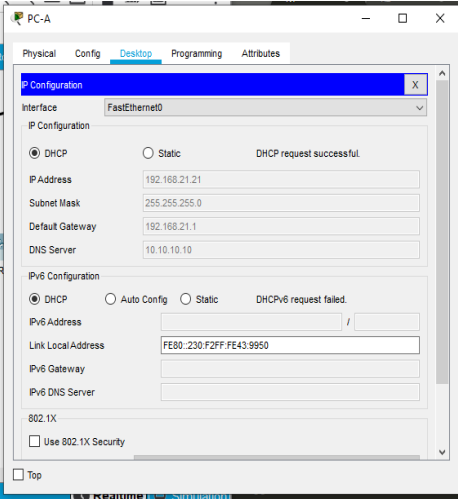
Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Se digita el comando: R2(config)#user webuser privilege 15 secret Cisco12345
Habilitar el servicio del servidor HTTP	No soporta protocolo HTTP
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	Se introducen las siguientes líneas de códigos: 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.	Se digita el comando respectivo con la dirección IPv4 correspondiente: 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	Se usa el comando: R2(config-if)#interface gigabitEthernet 0/0 R2(config-if)#ip nat inside R2(config-if)#interface gigabitEthernet 0/1 R2(config-if)#ip nat outside
Configurar la NAT dinámica dentro de una ACL privada	Se utiliza el comando: 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 R2(config)#access-list 1 permit 192.168.5.0 0.0.0.255 R2(config)#access-list 1 permit 192.168.6.0 0.0.0.255

Defina el pool de direcciones IP públicas utilizables.	Se define el pool de direcciones IP públicas utilizables: R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.238 netmask 255.255.255.248
Definir la traducción de NAT dinámica	Se digita el comando: R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.238 netmask 255.255.255.248

Tabla 18 Configuración NAT estática y dinámica en Router 2

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.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 <p>Gráfico 9 Dirección IP DHCP de PC-A. Imagen propia</p>

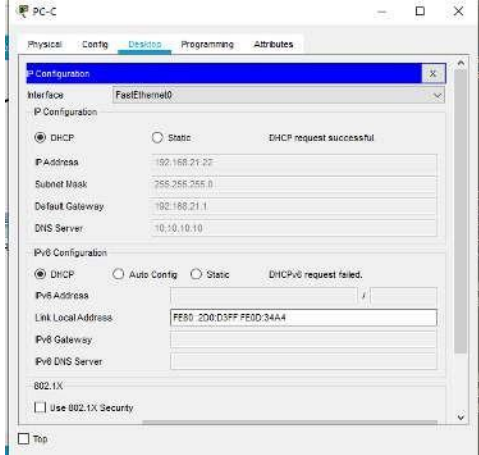
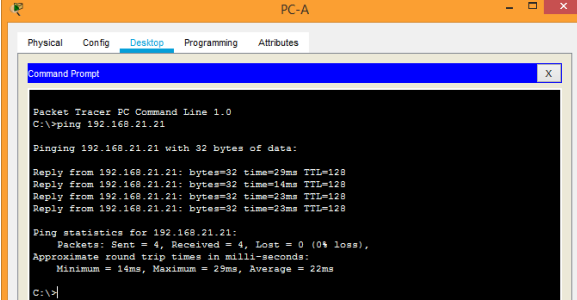
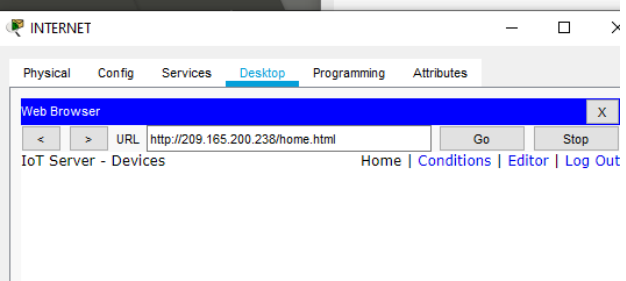
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	 <p>Gráfico 10 Dirección IP DHCP de PC-C. Imagen propia</p>
<p>Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	 <p>Gráfico 11 Ping de PC-A a PC-C. Imagen propia</p>
<p>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</p>	 <p>Gráfico 12 Evidencia de navegación de computadora de Internet. Imagen propia</p>

Tabla 19 Verificación del protocolo DHCP y la NAT estática

Parte 6. Configurar NTP.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	Se digita el comando: R2#clock set 09:00:00 05 MAR 2016
Configure R2 como un maestro NTP.	Se configura con el comando: R2(config)#ntp master 5
Configurar R1 como un cliente NTP.	Se configura con el comando: R2(config)#ntp server 172.16.1.1
Configure R1 para actualizaciones de calendario periódicas con hora NTP.	Se utiliza el comando: R2(config)#ntp server 172.16.1.1
Verifique la configuración de NTP en R1.	<p>Se verifica la configuración NTP con el comando:</p> <pre>R1#show ntp status Clock is synchronized, stratum 6, reference is 172.16.1.2 nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**24 reference time is 0C6D67FA.000002CE (9:8:10.718 UTC sáb. mar. 5 2016) clock offset is 2.00 msec, root delay is 2.00 msec root dispersion is 10.06 msec, peer dispersion is 0.12 msec. loopfilter state is 'CTRL' (Normal Controlled Loop), drift is - 0.000001193 s/s system poll interval is 4, last update was 16 sec ago. R1# R1#show ntp associations address ref clock st when poll reach delay offset disp *~172.16.1.2 127.127.1.1 5 3 16 177 2.00 2.00 0.12 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured</pre>

Tabla 20 Configuración NTP en Router 1 y Router 2

Parte 7. 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	Se introduce el comando: R2(config)#ip access-list standard ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	Se digita el comando: R2(config-std-nacl)#permit host 172.16.1.1
Permitir acceso por Telnet a las líneas de VTY	Se usa el comando: R2(config)#ip access-list standard ADMIN-MGT
Verificar que la ACL funcione como se espera	Se verifica que la ACL funcione con el comando: R2#show access-lists 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 192.168.99.0 0.0.0.255 40 permit 192.168.5.0 0.0.0.255 50 permit 192.168.6.0 0.0.0.255 Standard IP access list 2 10 permit host 172.16.1.1 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1

Tabla 21 Restricción del acceso a las líneas VTY en Router 2

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	<p>Se digita el comando: 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 192.168.99.0 0.0.0.255 40 permit 192.168.5.0 0.0.0.255 50 permit 192.168.6.0 0.0.0.255 Standard IP access list 2 10 permit host 172.16.1.1 Standard IP access list ADMIN-MGT 10 permit host 172.16.1.1 (34 match(es))</p>
Restablecer los contadores de una lista de acceso	<p>Se utiliza el comando: R2#Clear access-list counters ADMIN-MGT R2#</p>
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	<p>Se introduce el comando: R2#show ip interface serial 0/0/0 Serial0/0/0 is up, line protocol is up (connected) Internet address is 172.16.1.2/30 Broadcast address is 255.255.255.255 Address determined by setup command MTU is 1500 Helper address is not set Directed broadcast forwarding is disabled Outgoing access list is not set Inbound access list is ADMIN-MGT</p> <p>R2#show access-lists ADMIN-MGT Standard IP access list ADMIN-MGT permit host 172.16.1.1 (42 match(es))</p>

<p>¿Con qué comando se muestran las traducciones NAT?</p>	<p>Se digita el comando: R2#show ip nat translations Pro Inside global Inside local Outside local Outside global --- 209.165.200.233 10.10.10.10 -- - ---- R2#</p>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<p>R2#clear ip nat translation *</p>

Tabla 22 Descripción de comandos en 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.

Topología

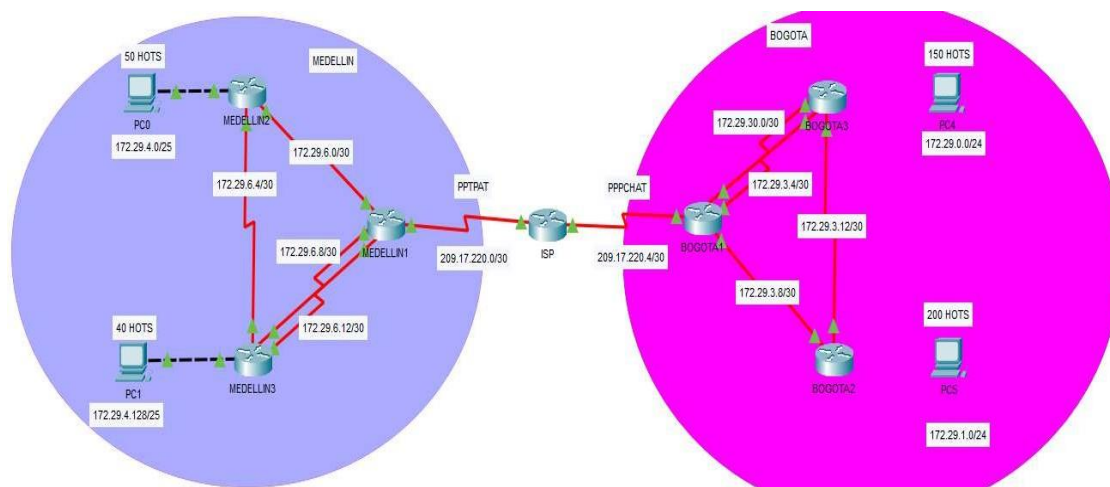


Gráfico 13 Segundo estudio de caso. Prueba de Habilidades Practicas

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

Los routers Bogota2 y medellin2 proporcionan el servicio DHCP a su propia red LAN y a los routers 3 de cada ciudad.

Debe configurar PPP en los enlaces hacia el ISP, con autenticación.

Debe habilitar NAT de sobrecarga en los routers Bogota1 y medellin1.

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.

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 suman las subredes de cada uno a /22.

```
Router(config)#hostname BOGOTA1
BOGOTA1(config)#no ip domain-lookup
BOGOTA1(config)#enable secret class
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#line vty 0 4
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#service password-encryption
BOGOTA1(config)#banner motd # Se prohíbe el acceso no
autorizado #
BOGOTA1(config)#router ospf 1
OSPF process 1 cannot start. There must be at least one "up"
IP interface
BOGOTA1(config-router)# router-id 1.1.1.1
BOGOTA1(config-router)# log-adjacency-changes
BOGOTA1(config-router)# network 172.29.3.0 0.0.0.3 area 0
BOGOTA1(config-router)# network 172.29.4.0 0.0.0.3 area 0
BOGOTA1(config-router)# network 172.29.3.8 0.0.0.3 area 0
BOGOTA1(config-router)# network 172.29.3.4 0.0.0.3 area 0
BOGOTA1(config-router)# network 172.29.1.0 0.0.0.3 area 0
BOGOTA1(config-router)# network 172.29.3.12 0.0.0.3 area 0
BOGOTA1(config-router)# network 172.29.0.0 0.0.0.3 area 0
BOGOTA1(config-router)#
BOGOTA1(config-router)# router rip
BOGOTA1(config-router)# no auto-summary

Router(config)#hostname BOGOTA2
BOGOTA2(config)#no ip domain-lookup
BOGOTA2(config)#enable secret class
BOGOTA2(config)#line console 0
```

```

BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#line vty 0 4
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#service password-encryption
BOGOTA2(config)#banner motd # Se prohíbe el acceso no
autorizado #
BOGOTA2(config)# router ospf 1
OSPF process 1 cannot start. There must be at least one "up"
IP interface
BOGOTA2(config-router)# router-id 2.2.2.2
BOGOTA2(config-router)# log-adjacency-changes
BOGOTA2(config-router)# network 172.29.3.8 0.0.0.3 area 0
BOGOTA2(config-router)# network 172.29.3.12 0.0.0.3 area 0
BOGOTA2(config-router)# network 172.29.1.0 0.0.0.3 area 0
BOGOTA2(config-router)#
BOGOTA2(config-router)# router rip
BOGOTA2(config-router)# no auto-summary

Router(config)#hostname BOGOTA3
BOGOTA3(config)#no ip domain-lookup
BOGOTA3(config)#enable secret class
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#line vty 0 4
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#service password-encryption
BOGOTA3(config)#banner motd # Se prohíbe el acceso no
autorizado #
BOGOTA3(config)#
BOGOTA3(config)#router ospf 1
OSPF process 1 cannot start. There must be at least one "up"
IP interface
BOGOTA3(config-router)# router-id 3.3.3.3
BOGOTA3(config-router)# log-adjacency-changes
BOGOTA3(config-router)# network 172.29.0.0 0.0.0.255 area 0
BOGOTA3(config-router)# network 172.29.3.0 0.0.0.3 area 0
BOGOTA3(config-router)# network 172.29.3.4 0.0.0.3 area 0
BOGOTA3(config-router)# network 172.29.3.12 0.0.0.3 area 0
BOGOTA3(config-router)#
BOGOTA3(config-router)# router rip

```

```

BOGOTA3(config-router)# no auto-summary

Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#no ip domain-lookup
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#line vty 0 4
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#service password-encryption
MEDELLIN1(config)#banner motd # Se prohíbe el acceso no
autorizado #
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)# router-id 4.4.4.4
MEDELLIN1(config-router)# log-adjacency-changes
MEDELLIN1(config-router)# network 172.29.6.12 0.0.0.2 area 0
OSPF: Invalid address/mask combination (discontiguous mask)
MEDELLIN1(config-router)# network 172.29.6.8 0.0.0.3 area 0
MEDELLIN1(config-router)# network 172.29.6.0 0.0.0.3 area 0
MEDELLIN1(config-router)# network 172.29.3.12 0.0.0.3 area 0
MEDELLIN1(config-router)# router rip
MEDELLIN1(config-router)# no auto-summary
MEDELLIN1(config-router)#

Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#no ip domain-lookup
MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#line vty 0 4
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#service password-encryption
MEDELLIN2(config)#banner motd # Se prohíbe el acceso no
autorizado #
MEDELLIN2(config)# router ospf 1
OSPF process 1 cannot start. There must be at least one "up"
IP interface
MEDELLIN2(config-router)# router-id 5.5.5.5

```

```

MEDELLIN2 (config-router)# log-adjacency-changes
MEDELLIN2 (config-router)# network 172.29.4.0 0.0.0.255 area
0
MEDELLIN2 (config-router)# network 172.29.6.4 0.0.0.3 area 0
MEDELLIN2 (config-router)# network 172.29.6.0 0.0.0.3 area 0
MEDELLIN2 (config-router)#
MEDELLIN2 (config-router)# router rip
MEDELLIN2 (config-router)# no auto-summary

Router (config)#hostname MEDELLIN3
MEDELLIN3 (config)#no ip domain-lookup
MEDELLIN3 (config)#enable secret class
MEDELLIN3 (config)#line console 0
MEDELLIN3 (config-line)#password cisco
MEDELLIN3 (config-line)#login
MEDELLIN3 (config-line)#line vty 0 4
MEDELLIN3 (config-line)#password cisco
MEDELLIN3 (config-line)#login
MEDELLIN3 (config-line)#service password-encryption
MEDELLIN3 (config)#banner motd # Se prohíbe el acceso no
autorizado #
MEDELLIN3 (config)# router ospf 1
OSPF process 1 cannot start. There must be at least one "up"
IP interface
MEDELLIN3 (config-router)# router-id 6.6.6.6
MEDELLIN3 (config-router)# log-adjacency-changes
MEDELLIN3 (config-router)# network 172.29.4.128 0.0.0.255
area 0
MEDELLIN3 (config-router)# network 172.29.6.4 0.0.0.3 area 0
MEDELLIN3 (config-router)# network 172.29.6.8 0.0.0.3 area 0
MEDELLIN3 (config-router)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN3 (config-router)# router rip
MEDELLIN3 (config-router)# no auto-summary

Router (config)#hostname ISP
ISP (config)#no ip domain-lookup
ISP (config)#enable secret class
ISP (config)#line console 0
ISP (config-line)#password cisco
ISP (config-line)#login
ISP (config-line)#line vty 0 4
ISP (config-line)#password cisco
ISP (config-line)#login
ISP (config-line)#service password-encryption

```

```

ISP(config)#banner motd # Se prohíbe el acceso no autorizado
#
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)#int s0/0/0
ISP(config-if)#description ISP-MEDELLIN1s0/1/0
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
ISP(config)#
ISP(config)#int s0/0/1
ISP(config-if)#description TRUNK ISP-BOGOTA1s0/0/0
ISP(config-if)#ip add 209.17.220.5 255.255.255.252
ISP(config-if)#clock rate 128000
ISP(config-if)#no shut
ISP(config-if)#exit

MEDELLIN1(config)#interface Serial0/1/0
MEDELLIN1(config-if)#description MEDELLIN1-ISP S0/0/0
MEDELLIN1(config-if)#ip address 209.17.220.2 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown

MEDELLIN1(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up

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

MEDELLIN1(config-if)#
%LINK-5-CHANGED: Interface Serial0/1/1, changed state to up

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

MEDELLIN1(config-if)#
MEDELLIN1(config-if)#interface Serial0/0/1
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 shutdown

MEDELLIN1(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
ip address 172.29.6.9 255.255.255.252
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up

MEDELLIN1(config-if)#
MEDELLIN1(config-if)#
MEDELLIN1(config-if)#interface Serial0/0/0
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 shutdown

MEDELLIN2(config)#interface Serial0/0/0
MEDELLIN2(config-if)#description MEDELLIN2-
MEDELLIN1Serial0/0/0
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#
MEDELLIN2(config-if)#interface Serial0/0/1
MEDELLIN2(config-if)# description MEDELLIN2-
MEDELLIN3Serial0/0/0
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#
MEDELLIN2(config-if)#interface GI0/0
MEDELLIN2(config-if)# description MEDELLIN2-PC2fa0
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#no shutdown

MEDELLIN3(config)#
MEDELLIN3(config)#interface Serial0/1/0
MEDELLIN3(config-if)#description MEDELLIN-
MEDELLIN1Serial0/1/1
MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#

```

```

MEDELLIN3(config-if)#interface Serial0/0/1
MEDELLIN3(config-if)#description MEDELLIN1-
MEDELLINSerial0/0/1
MEDELLIN3(config-if)#ip address 172.29.6.10 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#
MEDELLIN3(config-if)#interface Serial0/0/0
MEDELLIN3(config-if)#description MEDELLIN-
MEDELLIN2Serial0/0/1
MEDELLIN3(config-if)#ip address 172.29.6.6 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
This command applies only to DCE interfaces
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#
MEDELLIN3(config-if)#interface Gi0/0
MEDELLIN3(config-if)#description MEDELLIN-PC3fa0
MEDELLIN3(config-if)#ip address 172.29.4.2 255.255.255.128
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#

BOGOTA1(config)#
BOGOTA1(config)#interface Serial0/0/0
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
This command applies only to DCE interfaces
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#
BOGOTA1(config-if)#interface Serial0/0/1
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 shutdown
BOGOTA1(config-if)#
BOGOTA1(config-if)#interface Serial0/1/0
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 shutdown
BOGOTA1(config-if)#
BOGOTA1(config-if)#interface Serial0/1/1
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 shutdown

BOGOTA2(config)#interface Serial0/0/1
BOGOTA2(config-if)#interface Serial0/0/1
BOGOTA2(config-if)#description BOGOTA-BOGOTA1
BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#exit
BOGOTA2(config)#interface Serial0/0/0
BOGOTA2(config-if)#description BOGOTA-BOGOTA2Serial0/0/0
BOGOTA2(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shutdown
03:42:00: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on
Serial0/0/0 from LOADING to FULL, Loading Done

BOGOTA2(config-if)#
03:42:03: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on
Serial0/0/1 from LOADING to FULL, Loading Done

BOGOTA2(config-if)#
BOGOTA2(config-if)#
BOGOTA2(config-if)#interface gi0/0
BOGOTA2(config-if)#description BOGOTA-PC1fa0/0
BOGOTA2(config-if)#ip address 172.29.1.1 255.255.255.0
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#

BOGOTA3(config)#
BOGOTA3(config)#interface Serial0/0/1
BOGOTA3(config-if)#description BOGOTA2-BOGOTA1Serial0/0/1
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#
BOGOTA3(config-if)#interface Serial0/1/0

```

```

BOGOTA3(config-if)#description BOGOTA2-BOGOTA1Serial0/1/0
BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#
BOGOTA3(config-if)#interface Serial0/0/0
BOGOTA3(config-if)#description BOGOTA2-BOGOTA3Serial0/0/0
BOGOTA3(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
This command applies only to DCE interfaces
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#
BOGOTA3(config-if)#interface gi0/0
BOGOTA3(config-if)#description BOGOTA2-PC0fa0/0
BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.0
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#

```

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.

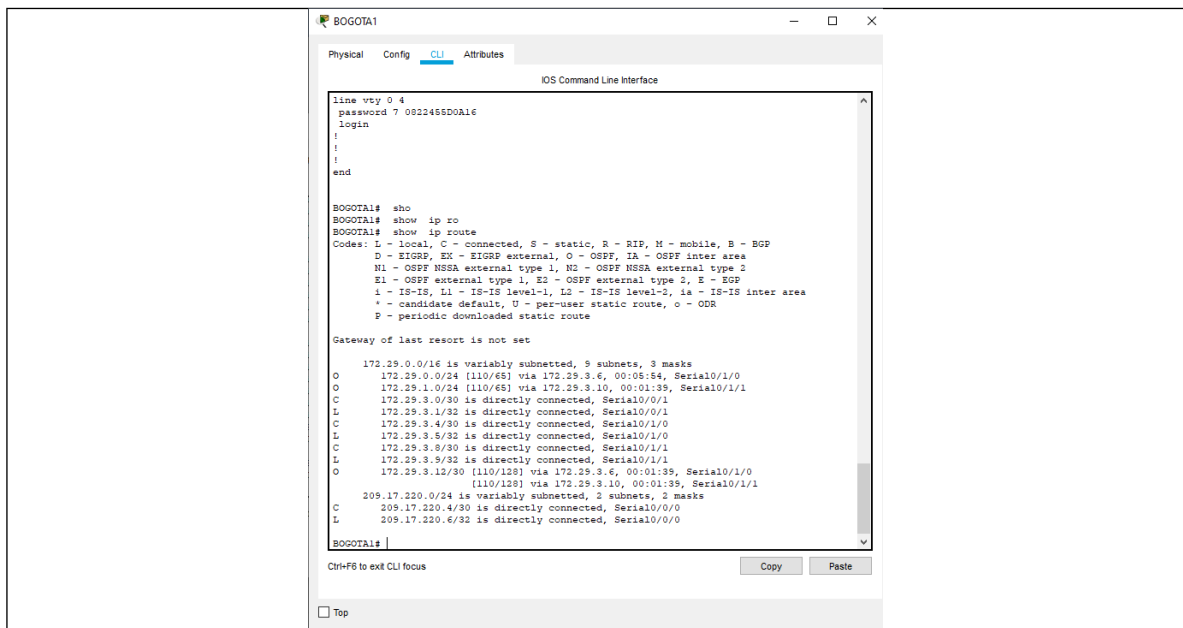


Gráfico 14 Tabla de enrutamiento. Imagen propia

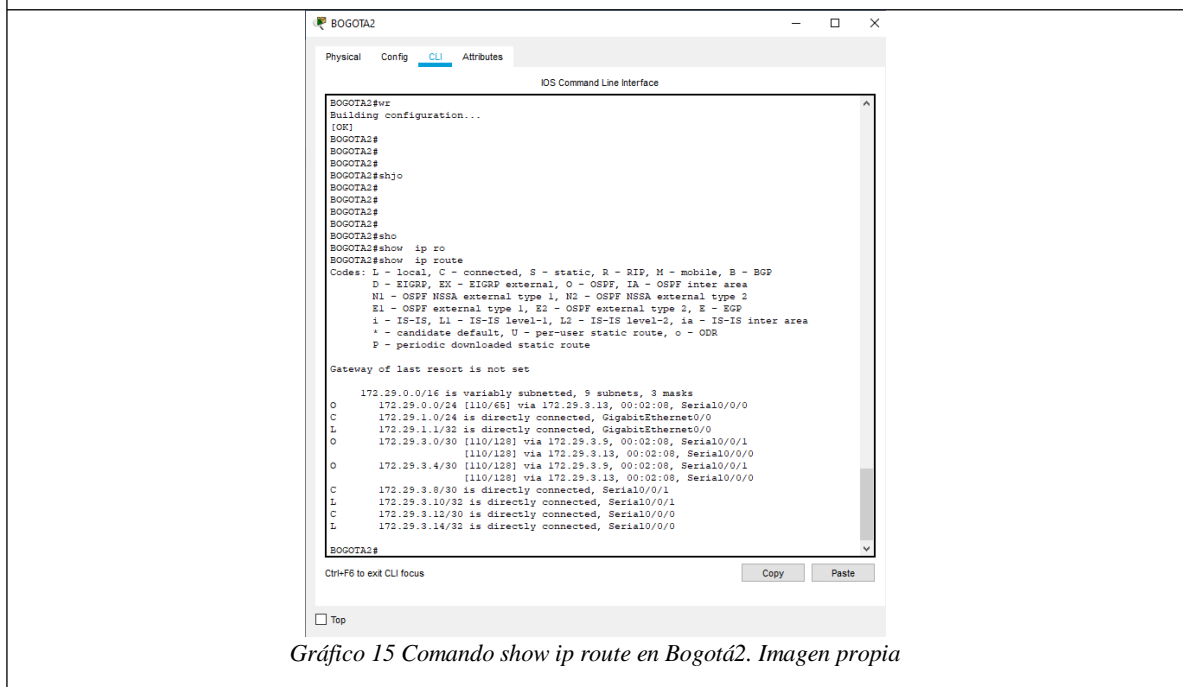


Gráfico 15 Comando show ip route en Bogotá2. Imagen propia

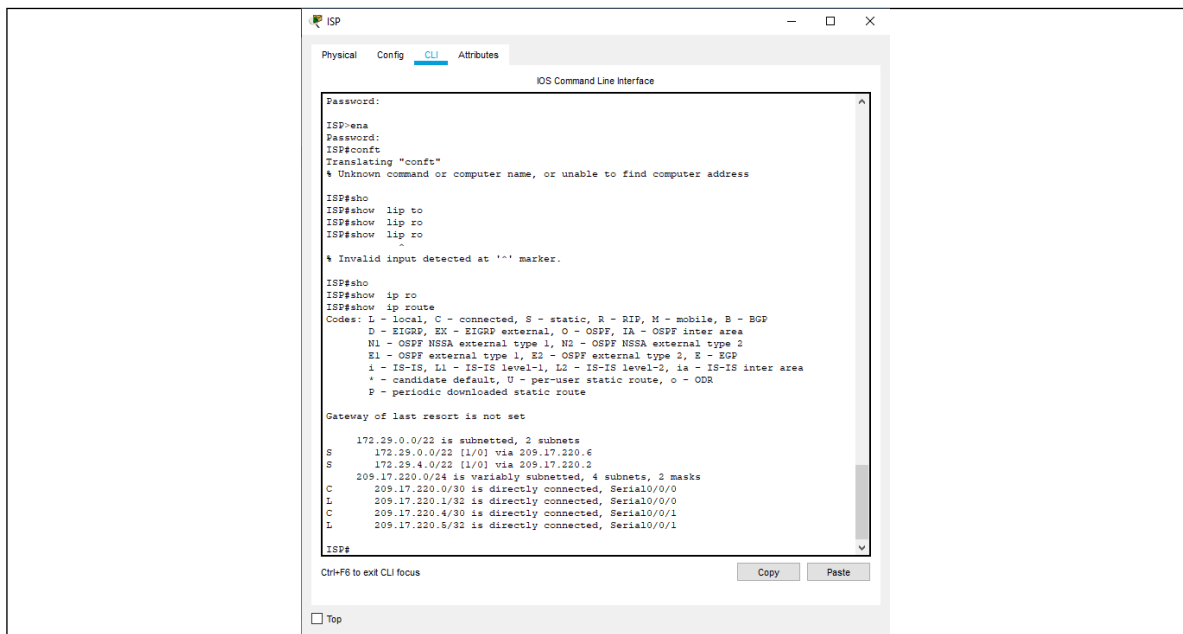


Gráfico 16 Comando show ip route en ISP. Imagen propia



Gráfico 17 Comando show ip route en Bogota3. Imagen propia

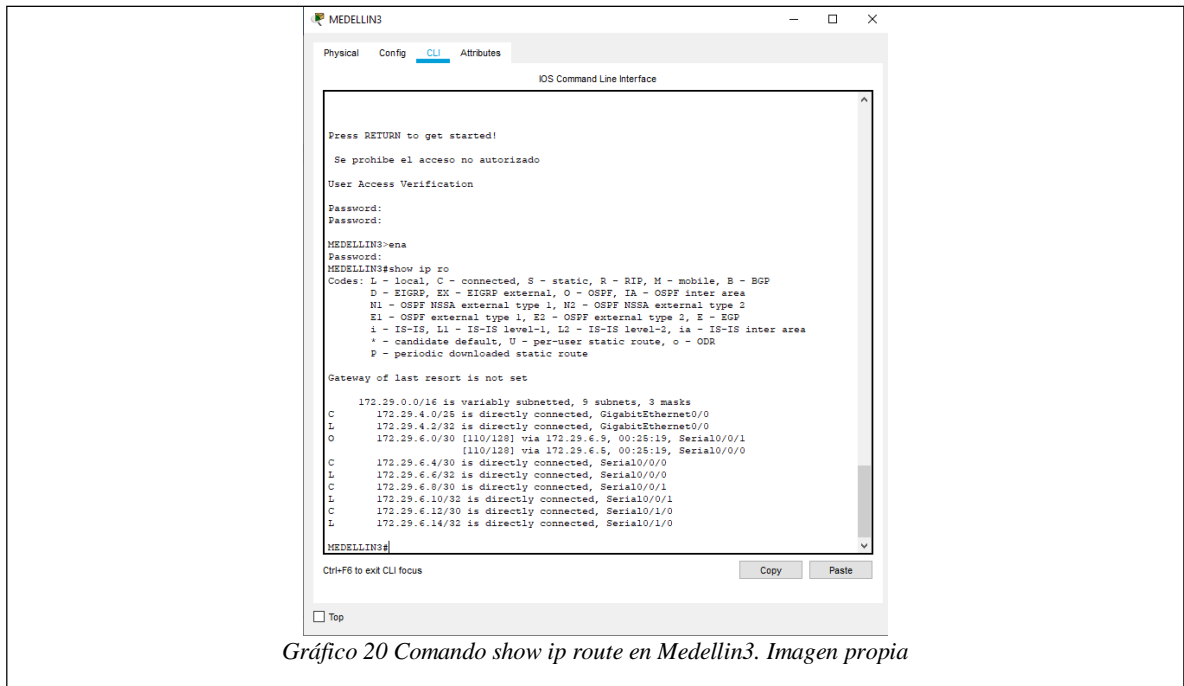


Gráfico 20 Comando show ip route en Medellin3. Imagen propia

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.

```

BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)# router-id 1.1.1.1
BOGOTA1(config-router)# log-adjacency-changes
BOGOTA1(config-router)#passive-interface SERIAL0/0/1
BOGOTA1(config-router)#passive-interface SERIAL0/1/0
BOGOTA1(config-router)#passive-interface SERIAL0/1/1

BOGOTA2(config)# router ospf 1
BOGOTA2(config-router)# router-id 2.2.2.2
BOGOTA2(config-router)# log-adjacency-changes
BOGOTA2(config-router)#passive-interface SERIAL0/0/0
BOGOTA2(config-router)#passive-interface SERIAL0/0/1

BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)# router-id 3.3.3.3
BOGOTA3(config-router)# log-adjacency-changes
BOGOTA3(config-router)#passive-interface SERIAL0/0/0
BOGOTA3(config-router)#passive-interface SERIAL0/0/1
  
```



```

BOGOTA3(config-router)#passive-interface SERIAL0/1/0

MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)# router-id 4.4.4.4
MEDELLIN1(config-router)# log-adjacency-changes
MEDELLIN1(config-router)# passive-interface SERIAL0/0/0
MEDELLIN1(config-router)#passive-interface SERIAL0/0/1
MEDELLIN1(config-router)#passive-interface SERIAL0/1/1

MEDELLIN2(config)# router ospf 1
MEDELLIN2(config-router)# router-id 5.5.5.5
MEDELLIN2(config-router)# log-adjacency-changes
MEDELLIN2(config-router)# passive-interface SERIAL0/0/0
MEDELLIN2(config-router)# passive-interface SERIAL0/0/1

MEDELLIN3(config)# router ospf 1
MEDELLIN3(config-router)# router-id 6.6.6.6
MEDELLIN3(config-router)# log-adjacency-changes
MEDELLIN3(config-router)# passive-interface SERIAL0/0/0
MEDELLIN3(config-router)# passive-interface SERIAL0/0/1
MEDELLIN3(config-router)# passive-interface SERIAL0/1/0

```

Interfaces que no requieren 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

Tabla 23 Interfaces que no requieren desactivación

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 digita el comando router ospf 1:

```
BOGOTA1 (config)#router ospf 1
BOGOTA1 (config-router)# router-id 1.1.1.1
BOGOTA1 (config-router)# log-adjacency-changes
BOGOTA1 (config-router)#passive-interface SERIAL0/0/1
BOGOTA1 (config-router)#passive-interface SERIAL0/1/0
BOGOTA1 (config-router)#passive-interface SERIAL0/1/1

BOGOTA2 (config)# router ospf 1
BOGOTA2 (config-router)# router-id 2.2.2.2
BOGOTA2 (config-router)# log-adjacency-changes
BOGOTA2 (config-router)#passive-interface SERIAL0/0/0
BOGOTA2 (config-router)#passive-interface SERIAL0/0/1

BOGOTA3 (config)#router ospf 1
BOGOTA3 (config-router)# router-id 3.3.3.3
BOGOTA3 (config-router)# log-adjacency-changes
BOGOTA3 (config-router)#passive-interface SERIAL0/0/0
BOGOTA3 (config-router)#passive-interface SERIAL0/0/1
BOGOTA3 (config-router)#passive-interface SERIAL0/1/0

MEDELLIN1 (config)#router ospf 1
MEDELLIN1 (config-router)# router-id 4.4.4.4
MEDELLIN1 (config-router)# log-adjacency-changes
MEDELLIN1 (config-router)# passive-interface SERIAL0/0/0
MEDELLIN1 (config-router)#passive-interface SERIAL0/0/1
MEDELLIN1 (config-router)#passive-interface SERIAL0/1/1

MEDELLIN2 (config)# router ospf 1
MEDELLIN2 (config-router)# router-id 5.5.5.5
MEDELLIN2 (config-router)# log-adjacency-changes
MEDELLIN2 (config-router)# passive-interface SERIAL0/0/0
MEDELLIN2 (config-router)# passive-interface SERIAL0/0/1
```

```

MEDELLIN3(config)# router ospf 1
MEDELLIN3(config-router)# router-id 6.6.6.6
MEDELLIN3(config-router)# log-adjacency-changes
MEDELLIN3(config-router)# passive-interface SERIAL0/0/0
MEDELLIN3(config-router)# passive-interface SERIAL0/0/1
MEDELLIN3(config-router)# passive-interface SERIAL0/1/0

```

- 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.

```

BOGOTA1#show ip ospf database
          OSPF Router with ID (1.1.1.1) (Process ID 1)

          Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum Link
count
1.1.1.1      1.1.1.1      564        0x80000004  0x00b24d 3
BOGOTA1#show ip route connected
C 172.29.3.0/30 is directly connected, Serial0/0/1
C 172.29.3.4/30 is directly connected, Serial0/1/0
C 172.29.3.8/30 is directly connected, Serial0/1/1
C 209.17.220.4/30 is directly connected, Serial0/0/0

BOGOTA1#|

```

Gráfico 21 Base de datos OSPF de Router Bogota1. Imagen propia

```

BOGOTA2#show ip ospf database
          OSPF Router with ID (2.2.2.2) (Process ID 1)

          Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum Link
count
2.2.2.2      2.2.2.2      773        0x80000004  0x00bb72 3
BOGOTA2#show ip ro
BOGOTA2#show ip route co
BOGOTA2#show ip route connected
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.8/30 is directly connected, Serial0/0/1
C 172.29.3.12/30 is directly connected, Serial0/0/0

BOGOTA2#|

```

Gráfico 22 Base de datos OSPF de Router Bogota2. Imagen propia

```

BOGOTA3#show ip ospf database
      OSPF Router with ID (3.3.3.3) (Process ID 1)

      Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum L:
count
3.3.3.3      3.3.3.3      1024        0x80000005  0x0014fb 4
BOGOTA3#sh
BOGOTA3#show ip route con
BOGOTA3#show ip route connected
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/1
C 172.29.3.4/30 is directly connected, Serial0/1/0
C 172.29.3.12/30 is directly connected, Serial0/0/0

BOGOTA3#|

```

Gráfico 23 Base de datos OSPF de Router Bogota3. Imagen propia

```

MEDELLIN1#show ip ospf database
      OSPF Router with ID (4.4.4.4) (Process ID 1)

      Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum Link
count
4.4.4.4      4.4.4.4      1215        0x80000003  0x00d42c 2
MEDELLIN1#show ip route c
MEDELLIN1#show ip route connected
C 172.29.6.0/30 is directly connected, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/0/1
C 172.29.6.12/30 is directly connected, Serial0/1/1
C 209.17.220.0/30 is directly connected, Serial0/1/0

MEDELLIN1#|

```

Gráfico 24 Base de datos OSPF de Router Medellin1. Imagen propia

```

MEDELLIN2#show ip ospf database
      OSPF Router with ID (5.5.5.5) (Process ID 1)

      Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum Link
count
5.5.5.5      5.5.5.5      1345        0x80000004  0x00d9c2 3
MEDELLIN2#ip route c
MEDELLIN2#show ip route co
MEDELLIN2#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#|

```

Gráfico 25 Base de datos OSPF de Router Medellin2. Imagen propia

```

MEDELLIN3#show ip ospf database
      OSPF Router with ID (6.6.6.6) (Process ID 1)

      Router Link States (Area 0)

Link ID          ADV Router      Age           Seq#           Checksum Link
count
6.6.6.6         6.6.6.6        1495         0x80000005 0x00f56c 4
MEDELLIN3#show ip route co
MEDELLIN3#show ip route connected
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
C 172.29.6.4/30 is directly connected, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/0/1
C 172.29.6.12/30 is directly connected, Serial0/1/0

MEDELLIN3#

```

Gráfico 26 Base de datos OSPF de Router Medellin3. Imagen propia

Parte 5. Configurar encapsulamiento y autenticación PPP.

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

Se realiza una secuencia para encapsular la información y poder conectar los res route Medellin y Bogota, ISP:

```

ISP(config)#int se0/0/0
ISP(config-if)#PPP authentication PAP
Must set encapsulation to PPP before using PPP subcommands
ISP(config-if)#PPP PAP sent-username ISP password ISP
Must set encapsulation to PPP before using PPP subcommands
ISP(config-if)#

MEDELLIN1(config)#username MEDELLIN1 secret MEDELLIN
MEDELLIN1(config)#int Serial0/1/0
MEDELLIN1(config-if)#PPP authentication PAP
Must set encapsulation to PPP before using PPP subcommands
MEDELLIN1(config-if)#PPP PAP sent-username ISP password ISP
Must set encapsulation to PPP before using PPP subcommands
MEDELLIN1(config-if)#

```

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

Se configura el enlace Bogotá1 con autenticación CHAT, en los router de ISP Y MEDELLIN:

```
ISP(config-if)#
ISP(config-if)#username BOGOTA1 secret BOGOTA1
ISP(config)#int se0/0/1
ISP(config-if)#PPP authentication CHAP
Must set encapsulation to PPP before using PPP subcommands
ISP(config-if)#

BOGOTA1(config)#int se0/0/0
BOGOTA1(config-if)#PPP authentication CHAP
Must set encapsulation to PPP before using PPP subcommands
BOGOTA1(config-if)#exit
BOGOTA1(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(config)#ip access-list standard HOST
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.0.255
MEDELLIN1(config-std-nacl)#

BOGOTA1(config)#ip access-list standard HOST
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.0.255
BOGOTA1(config-std-nacl)#
```

- 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.

```
MEDELLIN1(config)#interface Serial0/0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#!
```

```
MEDELLIN1(config-if)#interface Serial0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#!
MEDELLIN1(config-if)#interface Serial0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#!
MEDELLIN1(config-if)#interface Serial0/1/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#
```

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.

```
BOGOTA1(config)#interface Serial0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#!
BOGOTA1(config-if)#interface Serial0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#!
BOGOTA1(config-if)#interface Serial0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#!
BOGOTA1(config-if)#interface Serial0/1/1
BOGOTA1(config-if)#ip nat inside
```

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.

```
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1
172.29.4.5
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129
172.29.4.133
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-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
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
```

- c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.
- d. Configure el router Bogotá1 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.

```
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)#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
```

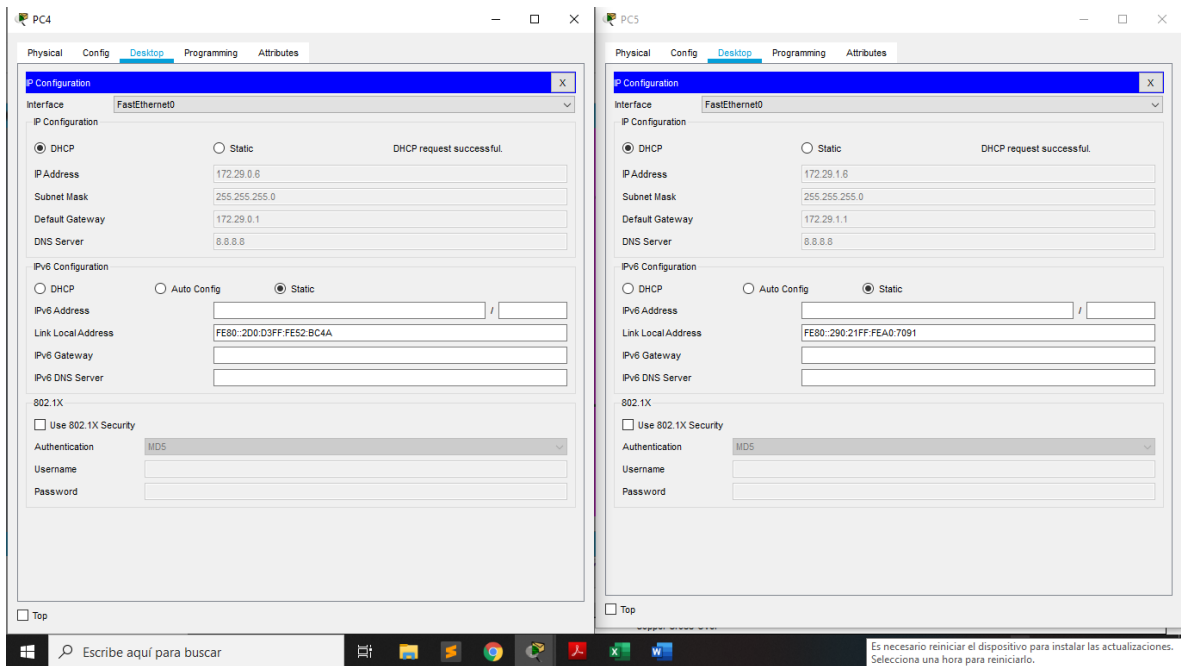



Gráfico 27 Configuración DHCP en PCs en la red de Bogotá. Imagen propia

CONCLUSIONES

- Para una correcta identificación de todos y cada uno de los dispositivos presentes en la topología entregada para cada uno de los escenarios es necesario nombrar cada equipo y solidificar sus estructuras configurando su respectiva seguridad.
- Configurando las direcciones IP de los dispositivos (Routers y Switches) conforme a la topología de red entregada en los escenarios 1 y 2, se tuvo especial cuidado al momento de establecer las direcciones IP y conjugarlas con sus respectivas máscaras de subred teniendo en cuenta que de la correcta configuración depende del éxito de las diferentes conexiones entre los equipos solicitados.
- El protocolo OSPF es muy importante al momento de poner en marcha una red de datos ya que gracias a ella las grandes y medianas redes son más eficientes y de rápida convergencia. La principal ventaja de este protocolo es la de brindar diversas opciones de configuración lo que permite adaptarlo a requerimientos muy específicos dentro de una red.
- Para que la red que se esté implementando pueda conectarse con redes exteriores, es de vital importancia activar el mecanismo de traducción de dirección de red (NAT). Con este mecanismo, hay un ahorro significativo en direcciones IP ya que se pueden conectar múltiples dispositivos con una única IP pública. En cuanto a seguridad de las redes, NAT ofrece protección a dispositivos locales de los distintos ataques que puedan sufrir desde redes externas.
- El protocolo de configuración dinámica de host (DHCP), es un protocolo que ofrece facilidades y ahorro de tiempo en cuanto a configuración ya que los dispositivos que implementen este protocolo acogen automáticamente el direccionamiento IP en una red determinada.

REFERENCIAS BIBLIOGRÁFICAS

- Bonet, E. (2014). Servicios avanzados II: Configuración dinámica de IPs (DHCP). Recuperado de <http://informatica.uv.es/it3guia/AGR/apuntes/teoria/documentos/DHCP.pdf>. (13/05/2020)
- Chimento, J. (2015). Comunicaciones NAT. Recuperado de <https://dcc.fceia.unr.edu.ar/sites/default/files/uploads/materias/nat.pdf>. (13/05/2020)
- Coto, A. (2008). Capítulo 8: Direccionamiento IP. Recuperado de http://www.ie.tec.ac.cr/acotoc/CISCO/R&S%20CCNA1/R&S_CCNA1_ITN_Chapter8_Direccionamiento%20IP.pdf. (10/05/2020)
- Ochoa, V. (2015). Uso del Packet Tracer y Aplicaciones Resueltas. Recuperado de <https://vochoa84.files.wordpress.com/2010/08/tutorial-uso-packet-tracer-y-aplicaciones-resueltas-corpocides-2010.pdf>. (11/05/2020)
- Prieto, R. (2016). Enrutamiento dinámico OSPF con Packet Tracer. Recuperado de <https://www.raulprietofernandez.net/blog/packet-tracer/enrutamiento-dinamico-ospf-con-packet-tracer>. (13/05/2020)
- Villagómez, C. (2017). El protocolo DHCP. Recuperado de <https://es.ccm.net/contents/261-el-protocolo-dhcp>. (13/05/2020)