

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

LEIDY MARCELA MANRIQUE OBREGON

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERIA DE SISTEMAS

BOGOTÁ D.C.

MAYO DE 2020

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

PRESENTADO POR  
LEIDY MARCELA MANRIQUE OBREGON

TRABAJO DE GRADO PARA ADQUIRIR TITULO  
DE INGENIERA DE SISTEMAS

PRESENTADO A  
JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA  
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA  
INGENIERIA DE SISTEMAS

BOGOTÁ D.C.

MAYO DE 2020

INGENIERIA DE SISTEMAS  
BOGOTÁ D.C.  
MAYO DE 2020

## **DEDICATORIA**

A mi familia, mi madre, mis hermanas, a mi pareja son las personas con las que he podido contar y su apoyo incondicional siempre, sus palabras y actos de amor día a día me impulsaron a finalizar una de mis metas.

## **AGRADECIMIENTOS**

Agradecimientos a Dios y a mi familia la cual me han apoyado en esta etapa de crecimiento personal.

A cada uno de los tutores de la universidad nacional abierta y a distancia (UNAD) quienes me guiaron en el proceso de aprendizaje y formación académica.

## LISTA DE CONTENIDO

INTRODUCCIÓN .....	10
DESARROLLO DE LAS TAREAS PROPUESTAS .....	11
<i>Escenario 1</i> .....	11
1    Figura 1.Topología de red escenario 1 .....	11
Parte 2:    Configurar los parámetros básicos de los dispositivos.....	17
Parte 3:    Configurar la seguridad del switch, las VLAN y el routing entre VLAN 34	
Parte 4:    Configurar el protocolo de routing dinámico RIPv2 .....	44
Parte 5:    Implementar DHCP y NAT para IPv4.....	50
Parte 6:    Configurar NTP .....	60
Parte 7:    Configurar y verificar las listas de control de acceso (ACL) Paso 1: Restringir el acceso a las líneas VTY en el R2.....	63
<i>Escenario 2</i> .....	65
Parte 1: Configuración del enrutamiento.....	70
parte 2: Tabla de Enrutamiento.....	76
Parte 3: Deshabilitar la propagación del protocolo OSPF .....	86
Parte 4: Verificación del protocolo OSPF .....	89
Parte 5: Configurar encapsulamiento y autenticación PPP .....	104
Parte 6: Configuración de PAT .....	107
Parte 7: Configuración del servicio DHCP .....	111
CONCLUSIONES .....	115
BIBLIOGRAFÍA.....	116

## LISTA DE FIGURAS

Figura 1.Topología de red escenario 1 1.....	11
Figura 2Ping a R1 1 1 .....	32
Figura 3Ping a R2 1 1 .....	32
Figura 4 .Ping 209.165.200.233 1 .....	33
Figura 5. Ping a S1 desde 192.168.99.1 1 .....	42
Figura 6.. Ping a S3 desde 192.168.99.1 1 .....	43
Figura 7. Ping a S1 desde 192.168.21.1 1 .....	43
Figura 8. Ping a S3 desde 192.168.23.1 1 1 .....	43
Figura 9. Ipconfig/all 1 1 .....	57
Figura 10. Ping 209.165.200.229 1 .....	58
Figura 11. Ping 192.168.23.21 1 1 .....	58
Figura 12. Topología de red escenario 2 1.....	66
Figura 13. Ping a 172.29.6.6 1 .....	107
Figura 14. Ip nat translations 1 1 .....	109
Figura 15. Ip nat translationsBOGOTA1 1 1.....	110
Figura 16. fastEthernet0 172.29.4.155 1 .....	112
Figura 17. fastEthernet0 172.29.1.6 1 .....	114

## LISTA DE TABLAS

Tabla 1 Inicializar y volver a cargar los routers y los switches .....	12
Tabla 2 Configurar la computadora de Internet.....	17
Tabla 3 Configurar R1.....	17
Tabla 4 Configurar R2.....	19
Tabla 5 Configurar R3 1.....	22
Tabla 6 Configurar S1 1 .....	25
Tabla 7 Configurar el S3 1 .....	25
Tabla 8 Verificar la conectividad de pc 1.....	27
Tabla 9 Configurar S1 1 .....	34
Tabla 10 Configurar el S3 1 .....	36
Tabla 11 Configurar R1 1.....	38
Tabla 12 Verificar la conectividad 1 .....	40
Tabla 13 Configurar RIPv2 en el R1 1 .....	44
Tabla 14 Configurar RIPv2 en el R2 1 .....	45
Tabla 15 Configurar RIPv3 en el R2 1 .....	46
Tabla 16 Verificar la información de RIP 1 .....	47
Tabla 17 Implementar DHCP y NAT para IPv4 1 .....	50



Tabla 18 Configurar la NAT estática 1 .....	51
Tabla 19 Verificar el protocolo DHCP 1 .....	54
Tabla 20 Configurar NTP 1 .....	60
Tabla 21 Restringir el acceso líneaVTY 1 .....	63
Tabla 22 Introducir el comando de CLI 1 .....	64
Tabla 23 Deshabilitar propagación OSPF 1 .....	86

## GLOSARIO

**DHCP:** El protocolo de configuración de host dinámico simplifica y mejora la precisión del direccionamiento IP, pero puede generar inquietudes de seguridad.

**NTP:** Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del enrutamiento de paquetes en redes con latencia variable.

**SWITCHES:** Los dispositivos de interconexión tienen dos ámbitos de actuación en las redes telemáticas. En un primer nivel se encuentran los más conocidos, los Router, que se encargan de la interconexión de las redes.

**OSPF:** Es un Interna Gateway Protocolo (IGP) que se usa para distribuir la información de ruteo dentro de un solo sistema autónomo.

**VLAN:** Red física está basada principalmente en uno o más switch. Se trata de dispositivos que regulan el tráfico de datos entre los participantes.

**PING:** es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión o host local

**TOPOLOGIAS:** e define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como «conjunto de nodos interconectados». Un nodo es el punto en el que una curva se intercepta a sí misma. Lo que un nodo es concretamente depende del tipo de red en cuestión.

**TRACERT:** una utilidad de línea de comandos que se usa para determinar la ruta que toma un paquete de protocolo de Internet (IP) para alcanzar su destino.

## INTRODUCCIÓN

En el siguiente informe se abarcarán todas las configuraciones existentes a nivel de red, este laboratorio incluirá la configuración de distintos protocolos como los son DHCP, PPP, NTP, Enrutamientos OSPF y RIP, entre otros; también las técnicas y conceptos de enrutamiento y conmutación, aplicados para los distintos segmentos de red dentro de una vlan independiente. Se estudiarán las formas de establecer una conexión a internet actuando desde una red privada, aplicando los conceptos conocidos como traductores de red.

Evaluaremos el ámbito de seguridad como el cifrado por PPP, las directivas de seguridad en switches, configuración y restricción de acceso tanto por usuarios para administrar equipos, como por segmentos para conectar otros segmentos.

Estudiaremos a profundidad los conceptos del enrutamiento OSPF, evaluaremos los distintos tipos de encapsulamiento serial PPP, y la diferencia de configurarlo con cifrado o texto claro, adicional experimentaremos las configuraciones que se deben realizar para permitir tráfico Broadcast en una sesión DHCP.

Con estos escenarios abarcaremos gran parte esencial de los conceptos y políticas establecidas en el mundo de las redes

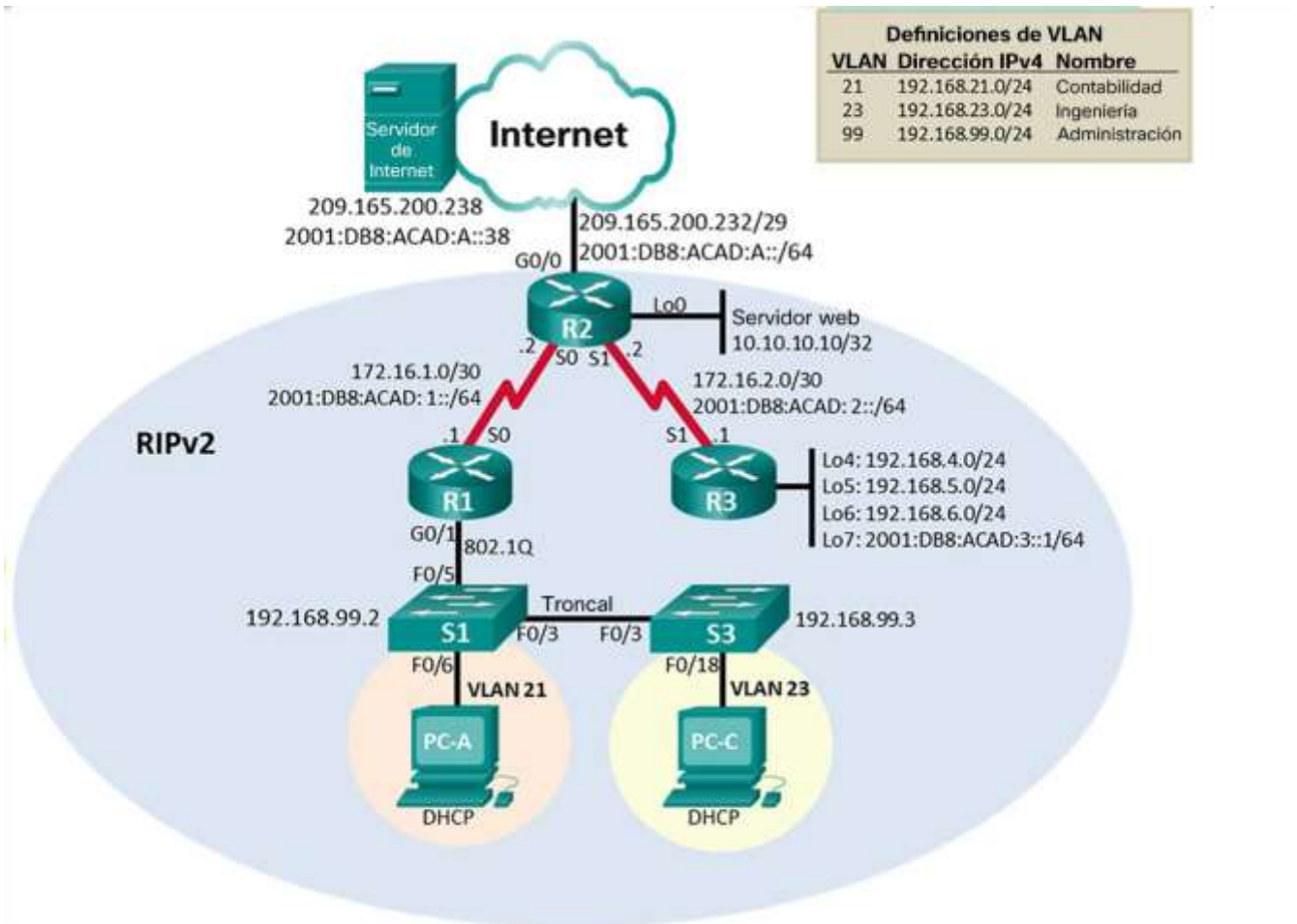
## DESARROLLO DE LAS TAREAS PROPUESTAS

### 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 de red escenario 1 1



Parte 1: Inicializar dispositivos

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

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.

Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tabla 1 Inicializar y volver a cargar los routers y los switches

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router1#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Router2# erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Router3# erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

<p>Volver a cargar todos los routers</p>	<pre>Router1#reload Proceed with reload? [confirm] Router2#reload Proceed with reload? [confirm] Router3#reload Proceed with reload? [confirm]</pre>
--	--

<p>Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior</p>	<pre>Switch1#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch3# Switch1#erase startup-config Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [OK] Erase of nvram: complete %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram Switch3# Switch1# Switch1#delete flash:vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm] %Error deleting flash:/vlan.dat (No such file or directory)  Switch1# Switch3#delete flash:vlan.dat Delete filename [vlan.dat]? Delete flash:/vlan.dat? [confirm]</pre>
--	---

%Error deleting flash:/vlan.dat (No such file or directory)

Switch2#

<p>Volver a cargar ambos switches</p>	<pre> Switch1#reload Proceed with reload? [confirm] C2950 Boot Loader (C2950-HBOOT-M) Version 12.1(11r)EA1,  RELEASE SOFTWARE (fc1)  Compiled Mon 22-Jul-02 18:57 by miwang Cisco WS-C2950T-24 (RC32300) processor (revision C0) with 21039K bytes of memory. 2950T-24 starting...  Base ethernet MAC Address: 0006.2A3D.BA24  Xmodem file system is available. Initializing Flash...  flashfs[0]: 1 files, 0 directories  flashfs[0]: 0 orphaned files, 0 orphaned directories  flashfs[0]: Total bytes: 64016384 flashfs[0]: Bytes used: 3058048 flashfs[0]: Bytes available: 60958336 flashfs[0]: flashfs fsck took 1 seconds.  ...done Initializing Flash.  Boot Sector Filesystem (bs:) installed, fsid: 3 Parameter Block Filesystem (pb:) installed, fsid: 4  Loading "flash:/c2950-i6q4l2-mz.121- 22.EA4.bin"...  ##### [OK]  Switch3#reload Proceed with reload? [confirm] </pre>
---------------------------------------	--



<p>Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches</p>	<pre> Switch1#dir Directory of flash:/  1 -rw- 3058048 &lt;no date&gt; c2950-i6q4l2- mz.121-22.EA4.bin  64016384 bytes total (60958336 bytes free) Switch1#  Switch3#dir Directory of flash:/  1 -rw- 3058048 &lt;no date&gt; c2950-i6q4l2- mz.121-22.EA4.bin  64016384 bytes total (60958336 bytes free) Switch3# </pre>
---	---

En la primera parte pide borrar la configuración esto se realiza por medio del comando `erase startup-config`, este código borra el contenido de la NVRAM”, Este es un tipo de memoria que no pierde la información almacenada así exista un daño eléctrico”, luego se carga el Router esto se realizado mediante el comando `reload`, se eliminan las configuraciones de todos los switch y VLAN se dejan los swicth a la configuración de fábrica.

## Parte 2: Configurar los parámetros básicos de los dispositivos

### Paso 1: Configurar la computadora de Internet

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

Tabla 2 Configurar la computadora de Internet

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

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

### Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 3 Configurar R1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain-lookup Router(config)#
Nombre del router	Router(config)#hostname R1 R1(config)#
Contraseña de exec privilegiado cifrada	R1(config)#enable secret 5 class R1(config)#

<p>Contraseña de acceso a la consola</p>	<pre>R1(config)#line console 0 R1(config-line)#password ?  7 Specifies a HIDDEN password will follow LINE The UNENCRYPTED (cleartext) line password  R1(config-line)#password cisco R1(config-line)#password cisco? LINE  R1(config-line)#password cisco  R1(config-line)#</pre>
<p>Contraseña de acceso Telnet</p>	<pre>R1(config)#line vty 0 4 R1(config-line)#password cisco R1(config-line)#</pre>
<p>Cifrar las contraseñas de texto no cifrado</p>	<pre>R1(config)#service password-encryption R1(config)#</pre>
<p>Mensaje MOTD</p>	<p>Se prohíbe el acceso no autorizado.</p>
<p>Interfaz S0/0/0</p>	<pre>R1(config)#int s0/0/0 R1(config-if)# ip add 172.16.1.1 255.255.255.252 R1(config-if)#no shu %LINK-5-CHANGED: Interface Serial0/0/0, changed state to down R1(config-if)#description link-R1-R2 R1(config-if)#clock rate 128000 R1(config-if)#  R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#</pre>
<p>Rutas predeterminadas</p>	<pre>R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.1.2 R1(config)#  R1(config)#ipv6 route ::/0 2001:DB8:ACAD:1::2 R1(config)#^Z</pre>

Nota: Todavía no configure G0/1.

- En esta configuración procedemos a realizar la desactivación de la búsqueda de DNS, con el fin de iniciar la asignación de nombre, contraseñas, y encriptación, esto con el fin de tener la seguridad requerida, implementamos la interfaz S/0/0/0 para interconectar los routers entre sí.

### Paso3 Configurar R2

Tabla 4 Configurar R2

<p><b>La configuración del R2 incluye las siguientes tareas:</b></p> <p><b>Elemento o tarea de configuración</b></p>	<p><b>Especificación</b></p>
Desactivar la búsqueda DNS	<pre>Router#conf t Enter configuration commands, one per line. End with CNTL/Z. Router(config)#no ip domain-lookup</pre>
Nombre del router	<pre>Router(config)#hostname R2 R2(config)#</pre>
Contraseña de exec privilegiado cifrada	<pre>R2(config)#enable secret 5 class</pre>
Contraseña de acceso a la consola	<pre>R2(config)#line console 0 R2(config-line)#password cisco</pre>
Contraseña de acceso Telnet	<pre>R2(config-line)#line vty 0 4 R2(config-line)#password cisco R2(config-line)#exi</pre>
Cifrar las contraseñas de texto no cifrado	<pre>R2(config)#service password-encryption R2(config)#</pre>

Habilitar el servidor HTTP	<pre> R2(config)#configure terminal Enter configuration commands, one per line. End with CNTL/Z. R2(config)#ip http server R2(config)# </pre>
Mensaje MOTD	<pre> R2#conf t Enter configuration commands, one per line. End with CNTL/Z. R2(config)#banner motd #Se prohbe el acceso no autorizado.# R2(config)# </pre>
Interfaz S0/0/0	<pre> R2(config)#int s0/0/0 R2(config-if)#ip add 172.16.1.2 255.255.255.252 R2(config-if)#no shu R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64 %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up  R2(config-if)#no shu %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state description link-R1-R2 R2(config-if)#description link-R2-R1 R2(config-if)#^Z </pre>

<p>Interfaz S0/0/1</p>	<pre>R2(config)#int          s0/0/1 R2(config-if)#ip add 172.16.2.2 255.255.255.252 R2(config-if)#no shu  %LINK-5-CHANGED:   Interface Serial0/0/1, changed state to down R2(config-if)#clock rate 128000 R2(config-if)#ipv6      address 2001:DB8:ACAD:2::2/64  R2(config-if)#description link-R2-R3 R2(config-if)#</pre>
<p>Interfaz G0/0 (simulación de Internet)</p>	<pre>R2(config)#int g0/0 R2(config-if)#ip add  R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#no shu  R2(config-if)#  %LINK-5-CHANGED:   Interface GigabitEthernet0/0, changed state to up  R2(config-if)# R2(config-if)#ipv6 add 2001:DB8:ACAD:A::1/64 R2(config-if)#</pre>

<p>Interfaz loopback 0 (servidor web simulado)</p>	<pre>R2(config)#int lo0  R2(config-if)# %LINK-5-CHANGED: Interface Loopback0, changed state to up  %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up  R2(config-if)#ip add 10.10.10.10 255.255.255.255 R2(config-if)#</pre>
<p>Ruta predeterminada</p>	<pre>R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.238  R2(config)#^Z  R2(config)#ipv6 route ::/0 2001:DB8:ACAD:A::38  R2(config)#</pre>

En esta configuración procedemos a realizar la desactivación de la búsqueda de DNS, con el fin de iniciar la asignación de nombre, contraseñas, y encriptación, esto con el fin de tener la seguridad requerida, implementamos

la interfaz S/0/0/0 para interconectar los routers entre si.

Configurando la Interfaz G0/0 realizamos la simulación de internet al router, cuando realizamos la configuración de interfaz loopback la cual nos sirve para tener latente el protocolo de enrutamiento OSPF.

### Paso 3: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5 Configurar R3 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	
Nombre del router	Router(config)#no ip domain-lookup Router(config)#hostname R3
Contraseña de exec privilegiado cifrada	R3(config)#enable secret class R3(config)#line console 0
Contraseña de acceso a la consola	R3(config-line)#password cisco R3(config-line)#line vty 0 4 R3(config-line)#password cisco
Contraseña de acceso Telnet	R3(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R3(config)#service password-encryption R3(config)#
Mensaje MOTD	R3(config)#banner motd #Se prohíbe el acceso no autorizado.# R3(config)#
Interfaz S0/0/1	R3(config)#int s0/0/1 R3(config-if)#ip add 172.16.2.1 255.255.255.252 R3(config-if)#no shu  R3(config-if)#description link-R2-R3 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64  %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up  R3(config-if)#
Interfaz loopback 4	R3(config-if)#int lo4 R3(config-if)#ip add 192.168.4.1 255.255.255.0
Interfaz loopback 5	R3(config-if)#int lo5 R3(config-if)#ip add 192.168.5.1 255.255.255.0



Interfaz loopback 6	R3(config-if)#int lo6 R3(config-if)#ip add 192.168.6.1 255.255.255.0
Interfaz loopback 7	R3(config-if)#int lo7  R3(config-if)#
	%LINK-5-CHANGED: Interface Loopback7, changed state to up  %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up  R3(config-if)#ip add 192.168.7.1 255.255.255.0
Rutas predeterminadas	R3(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2 R3(config)#ipv6 route ::/0 s0/0/1 R3(config)#

En esta configuración procedemos a realizar la desactivación de la búsqueda de DNS, con el fin de iniciar la asignación de nombre, contraseñas, y encriptación, esto con el fin de tener la seguridad requerida, implementamos la interfaz S/0/0/0 para interconectar los routers entre sí.

Configurando la Interfaz G0/0 realizamos la simulación de internet al router, cuando realizamos la configuración de interfaz loopback la cual nos sirve para tener latente el protocolo de enrutamiento OSPF.

### Paso 3: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6 Configurar S1 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch#conf t
Nombre del switch	Enter configuration commands, one per line. End with CNTL/Z
Contraseña de exec privilegiado cifrada	Switch(config)#no ip domain-lookup Switch(config)#hostname S1
Contraseña de acceso a la consola	S1(config)#enable secret class S1(config)#line console 0
Contraseña de acceso Telnet	S1(config-line)#password cisco S1(config-line)#line vty 0 4
Cifrar las contraseñas de texto no cifrado	S1(config-line)#password cisco S1(config-line)#exit  S1(config)#service password-encryption S1(config)#
Mensaje MOTD	S1(config)#banner motd S1(config)#banner motd #Se prohbe el acceso no autorizado.#  S1(config)#

En esta configuración procedemos a realizar la desactivación de la búsqueda de DNS, con el fin de iniciar la asignación de nombre, contraseñas las cuales se estipulan para cada uno de los protocolos las cuales también van cifradas.

Paso 4: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7 Configurar el S3 1

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	S3#conf t
Nombre del switch	Enter configuration commands, one per

Contraseña de exec privilegiado cifrada	line. End with CNTL/Z
Contraseña de acceso a la consola	S3(config)#no ip domain-lookup
Contraseña de acceso Telnet	S3(config)#hostname S3
Cifrar las contraseñas de texto no cifrado	S3(config)#enable secret class
Mensaje MOTD	S3(config)#line console 0
	S3(config-line)#password cisco
	S3(config-line)#line vty 0 4
	S3(config-line)#password cisco
	S3(config-line)#exit
	S3(config)#service password-encryption
	S3(config)#banner motd #Se prohbe el acceso no autorizado.#

En esta configuración procedemos a realizar la desactivación de la búsqueda de DNS, con el fin de iniciar la asignación de nombre, contraseñas las cuales se estipulan para cada uno de los protocolos las cuales también van cifradas, y se estipula un mensaje en dado caso de que la contraseña sea incorrecta.

Paso 5: Verificar la conectividad de la red

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

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

Tabla 8 Verificar la conectividad de pc 1

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.1.2 2001:DB8:ACAD:1::2	<p>R1#ping 172.16.1.2</p> <p>Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!</p> <p>Success rate is 100 percent (5/5), round- trip min/avg/max = 1/6/16 ms</p> <p>R1# R1#ping 2001:DB8:ACAD:1::2</p> <p>Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::2, timeout is 2 seconds: !!!!</p> <p>Success rate is 100 percent (5/5), round- trip min/avg/max = 1/5/24 ms</p> <p>R1#</p>

R2	R3, S0/0/1	172.16.2.1 2001:DB8:ACAD:2::1	<p>R2#ping 172.16.2.1</p> <p>Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds: !!!!</p> <p>Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms</p> <p>R2#</p> <p>R2(config)#do ping 2001:DB8:ACAD:2::1</p> <p>Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::1, timeout is 2 seconds: !!!!</p> <p>Success rate is 100 percent (5/5), round-trip min/avg/max = 2/7/15 ms</p> <p>R2(config)#</p>
----	------------	----------------------------------	--

PC de Internet	Gateway predeterminado	209.165.200.233 2001:DB8:ACAD:A::1	<pre> SERVER&gt;ping 209.165.200.233  Pinging 209.165.200.233 with 32 bytes of data:  Reply                from 209.165.200.233: bytes=32 time=1ms TTL=255  Reply                from 209.165.200.233: bytes=32 time=10ms TTL=255  Reply                from 209.165.200.233: bytes=32 time=0ms TTL=255  Reply                from 209.165.200.233: bytes=32 time=0ms TTL=255  Ping statistics for 209.165.200.233:     Packets: Sent = 4,     Received = 4, Lost =     0 (0% loss),     Approximate round     trip times in milli-     seconds:         Minimum = 0ms,         Maximum = 10ms,         Average = 2ms  SERVER&gt; </pre>
----------------	------------------------	---------------------------------------	--

			<pre>SERVER&gt;ping 2001:DB8:ACAD:A::1  Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data:</pre>
--	--	--	---

			<p>Reply from 2001:DB8:ACAD:A::1: bytes=32 time=1ms TTL=255</p> <p>Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255</p> <p>Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255</p> <p>Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255</p> <p>Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli- seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms</p> <p>SERVER&gt;</p>
--	--	--	---



### Figura 2 Ping a R1 1 1

```
-----
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 = 1/6/13 ms

R1#ping 2001:DB8:ACAD:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:1::2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/9 ms

R1#
```

---

### Figura 3 Ping a R2 1 1

```
R2#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 = 1/3/8 ms

R2#ping 2001:DB8:ACAD:2::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/6/11 ms

R2#
```

---

Figura 4 .Ping 209.165.200.233 1

```
Pinging 209.165.200.233 with 32 bytes of data:
Reply from 209.165.200.233: bytes=32 time=0ms TTL=255
Reply from 209.165.200.233: bytes=32 time=0ms TTL=255
Reply from 209.165.200.233: bytes=32 time=0ms TTL=255
Reply from 209.165.200.233: bytes=32 time=0ms TTL=255

Ping statistics for 209.165.200.233:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

SERVER>ping 2001:DB8:ACAD:A::1

Pinging 2001:DB8:ACAD:A::1 with 32 bytes of data:

Reply from 2001:DB8:ACAD:A::1: bytes=32 time=57ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255
Reply from 2001:DB8:ACAD:A::1: bytes=32 time=0ms TTL=255

Ping statistics for 2001:DB8:ACAD:A::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 57ms, Average = 14ms

SERVER>
```

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

Se realiza las pruebas de conexión por medio del comando ping de r1 a r2 s0/0/0, en la cual se evidencia que hay conexión, luego se realiza ping de r2 a r3 s0/0/1, en la que también se evidencia que hay conexión, por ultimo se realiza ping al pc de internet 209.165.200.223, la cual indica que establece conexión con el host.

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

#### Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9 Configurar S1 1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>S1(config)#vlan 21 S1(config-vlan)#name Contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#nam Ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name Administracion S1(config-vlan)#</pre>
Asignar la dirección IP de administración.	<pre>S1(config)#int vlan 99 S1(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up  S1(config-if)#ip add 192.168.99.2 255.255.255.0 S1(config-if)#no shu</pre>
Asignar el gateway predeterminado	<pre>S1(config)#ip default-gateway 192.168.99.1 S1(config)#</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>S1(config)#int fa0/3 S1(config-if)#switchport mode trunk S1(config-if)#switchport native vlan 1 S1(config-if)#</pre>
Forzar el enlace troncal en la interfaz F0/5	<pre>S1(config-if)#int fa0/5 S1(config-if)#switchport mode trunk S1(config-if)#switchport native vlan 1 S1(config-if)#</pre>

Configurar el resto de los puertos como puertos de acceso	<pre>S1(config-if)#int range fa0/1-2,fa0/4,fa0/6-24 S1(config-if-range)#sw S1(config-if-range)#switchport mode acces S1(config-if-range)#</pre>
Asignar F0/6 a la VLAN 21	<pre>S1(config-if-range)#int fa0/6 S1(config-if)#sw S1(config-if)#switchport acc S1(config-if)#switchport access vlan 21 S1(config-if)#</pre>
Apagar todos los puertos sin usar	<pre>S1(config-if)#int range fa0/1-2,fa0/4,fa0/7-24 S1(config-if-range)#shu  %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down  %LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down  %LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down  ...  %LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down  S1(config-if-range)#</pre>

Se procede a crear la base de datos de la VLAN para posteriormente asignar la dirección Ip de administración, se configura el gateway en este caso se deja predeterminado, forzamos el enlace trocal para configurar el resto de los puertos como puertos de acceso y asignar F0/6 a la VLAN 21 y apagar los puertos sin usar.

### **Paso 2: Configurar el S3**

La configuración del S3 incluye las siguientes tareas:

Tabla 10 Configurar el S3 1

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	<pre>S3(config-vlan)#vlan 21 S3(config-vlan)#name Contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#nam Ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name Administracion S3(config-vlan)#</pre>
Asignar la dirección IP de administración	<pre>S3(config)#int vlan 99 S3(config-if)# %LINK-5-CHANGED: Interface Vlan99, changed state to up  S3(config-if)#ip add 192.168.99.3 255.255.255.0 S3(config-if)#no shu S3(config-if)#</pre>
Asignar el gateway predeterminado.	<pre>S3(config)#ip default-gateway 192.168.99.1 S3(config)#</pre>
Forzar el enlace troncal en la interfaz F0/3	<pre>S3(config)#int fa0/3 S3(config-if)#sw S3(config-if)#switchport mode trunk S3(config-if)#swit S3(config-if)#switchport          nat S3(config-if)#switchport native vlan 1 S3(config-if)#</pre>
Configurar el resto de los puertos como puertos de acceso	<pre>S3(config-if)#int range fa0/1-2,fa0/4-24 S3(config-if-range)#switch mode acce S3(config-if-range)#</pre>

Asignar F0/18 a la VLAN 21	<pre>S3(config-if-range)#exi S3(config)#int f0/18 S3(config-if)#swi S3(config-if)#switchport acc vlan 21 S3(config-if)#</pre>
Apagar todos los puertos sin usar	<pre>S3(config-if)#int range fa0/1-2,fa0/4-17,fa0/19-24 S3(config-if-range)#shu</pre> <p>%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down</p> <p>%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to administratively down</p>

Se procede a crear la base de datos de la VLAN para posteriormente asignar la dirección Ip de administración, se configura el gateway en este caso se deja predeterminado, forzamos el enlace trocal para configurar el resto de los puertos como puertos de acceso y asignar F0/6 a la VLAN 21 y apagar los puertos sin usar.

**Paso 3: Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11 Configurar R1 1

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/1.99 R1(config-subif)#enca
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config-subif)#encapsulation dot1q 99 R1(config-subif)#ip add 192.168.99.1 255.255.255.0
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config-subif)#int g0/1.21 R1(config-subif)#encapsulation dot1q 21
Activar la interfaz G0/1	R1(config-subif)#ip add 192.168.21.1 255.255.255.0 R1(config-subif)#int g0/1.23 R1(config-subif)#encapsulation dot1q 23 R1(config-subif)#ip add 192.168.23.1 255.255.255.0 R1(config-subif)#descr LAN_INGENIERIA R1(config-subif)#int g0/1.21 R1(config-subif)#descr LAN_CONTABILIDAD R1(config-subif)#int g0/1.99 R1(config-subif)#descr LAN_ADMINISTRACION R1(config-subif)#int g0/1 R1(config-if)#no shu  R1(config-if)# %LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up  %LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up  %LINK-5-CHANGED: Interface GigabitEthernet0/1.23, changed state to up

```
%LINK-5-CHANGED: Interface  
GigabitEthernet0/1.99, changed state to up
```

```
R1(config-if)#
```



Procedemos a configurar las subinterfaces según la configuración planteada para proceder a activar la interfaz.

**Paso 4: Verificar la conectividad de la red**

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

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

Tabla 12 Verificar la conectividad 1

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    = 0/0/1 ms  S1# </pre>

S3	R1, dirección VLAN 99	192.168.99.1	<p>S3#ping 192.168.99.1</p> <p>Type       escape sequence to abort. Sending 5, 100- byte ICMP Echos to 192.168.99.1,  timeout is 2 seconds:  !!!!</p> <p>Success rate is 100 percent (5/5), round-trip min/avg/max     = 0/1/6 ms</p> <p>S3#</p>
----	-----------------------	--------------	--

S1	R1, dirección VLAN 21	192.168.21.1	<p>S1#ping 192.168.21.1</p> <p>Type       escape sequence to abort. Sending 5, 100- byte ICMP Echos to 192.168.21.1,  timeout is 2 seconds:  !!!!</p> <p>Success rate is 100 percent (5/5), round-trip min/avg/max     = 0/0/1 ms</p> <p>S1#</p>
----	-----------------------	--------------	--

S3	R1, dirección VLAN 23	192.168.23.1	<pre> S3#ping 192.168.23.1  Type      escape sequence to abort. Sending 5, 100- byte ICMP Echos to 192.168.23.1, timeout is 2 seconds: !!!!  Success rate is 100 percent (5/5), round-trip min/avg/max    = 0/0/2 ms  S3# </pre>
----	-----------------------	--------------	--

Procedemos a verificar la conectividad de red de cada una de las VLAN, hacemos ping para verificar que respondan de manera adecuada.

Figura 5. Ping a S1 desde 192.168.99.1

```

S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#

```

---

Figura 5.. Ping a S3 desde 192.168.99.1

Figura 6.. Ping a S3 desde 192.168.99.1 1

```
S3#ping 192.168.99.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

```
S3#
```

---

Figura 7. Ping a S1 desde 192.168.21.1 1

```
S1#ping 192.168.21.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

```
S1#
```

---

Figura 8. Ping a S3 desde 192.168.23.1 1 1

```
S3#ping 192.168.23.1
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

```
S3#
```

---

## Parte 4: Configurar el protocolo de routing dinámico RIPv2

### Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13 Configurar RIPv2 en el R1 1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R1(config)#router rip R1(config-router)#version 2
Anunciar las 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 mask ? % Unrecognized command R1(config-router)#network 172.16.1.0
Establecer todas las interfaces LAN como pasivas	R1(config-router)#passive- interface g0/1 R1(config-router)#
Desactive la sumarización automática	R1(config-router)#no auto- summary R1(config-router)#

En este paso se configura la RIP versión 2 para el r1, este protocolo permite la configuración de varias subredes, se configuran todas las interfaces como LAN pasivas, para evitar que se envíen mensajes de routing por la interfaz g0/1, se desactiva la sumarización automática para que esta no de

permisos al Router para agrupar redes.

**Paso 2: Configurar RIPv2 en el R2**

La configuración del R2 incluye las siguientes tareas:

Tabla 14 Configurar RIPv2 en el R2 1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#router rip R2(config-router)#version 2
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.0 R2(config-router)#network 172.16.1.0 R2(config-router)#network 172.16.2.0
Establecer la interfaz LAN (loopback) como pasiva	R2(config-router)#passive-interface loopback 0 R2(config-router)#
Desactive la sumarización automática.	R2(config-router)#no auto-summary R2(config-router)#

En este paso se configura la RIP versión 2 para el r2, este protocolo permite la configuración de varias subredes, se configuran todas las interfaces como LAN pasivas, para evitar que se envíen mensajes de routing por la interfaz loopback, se desactiva la sumarización automática para que esta no de permisos al Router para agrupar redes.

**Paso 3: Configurar RIPv3 en el R2**

La configuración del R3 incluye las siguientes tareas:

Tabla 15 Configurar RIPv3 en el R2 1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R3(config)#router rip R3(config-router)#version 2
Anunciar redes IPv4 conectadas directamente	R3(config-router)#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 R3(config-router)#network 192.168.7.0 R3(config-router)#
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R3(config-router)#passive-interface lo4 R3(config-router)#passive-interface lo5 R3(config-router)#passive-interface lo6 R3(config-router)#passive-interface lo7 R3(config-router)#
Desactive la sumarización automática.	R3(config-router)#no auto-summary R3(config-router)#

En este paso se configura la RIP versión 2 para el r3, este protocolo permite la configuración de varias subredes, se configuran todas las interfaces como LAN IPV4 pasivas, para evitar que se envíen mensajes de routing por la interfaz loopback, se desactiva la sumarizacion automática para que esta

no de permisos al Router para agrupar redes.

**Paso 4: Verificar la información de RIP**

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

Tabla 16 Verificar la información de RIP 1

Pregunta	Respuesta
<p>¿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?</p>	<pre>R3#sh ip protocols Routing Protocol is "rip" Sending updates every 30 seconds, next due in 6 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 Serial0/0/1 2 2 Automatic network summarization is not in effect  Maximum path: 4 Routing for Networks: 172.16.0.0 192.168.4.0 192.168.5.0 192.168.6.0 192.168.7.0  Passive Interface(s): Loopback4 Loopback5 Loopback6 Loopback7</pre>



	<p>Routing Information Sources:</p> <p>Gateway Distance Last Update</p> <p>172.16.2.2 120 00:00:01</p> <p>Distance: (default is 120)</p> <p>R3#</p>
--	---

<p>¿Qué comando muestra solo las rutas RIP?</p>	<pre>R3#sh ip route rip 10.0.0.0/32 is subnetted, 1 subnets R 10.10.10.10 [120/1] via 172.16.2.2, 00:00:27, 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, 00:00:27, Serial0/0/1 192.168.7.0/24 is variably subnetted, 2 subnets, 2 masks R 192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:27, Serial0/0/1 R 192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:27, Serial0/0/1 R 192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:27, Serial0/0/1</pre> <p>R3#</p>
---	---

<p>¿Qué comando muestra la sección de RIP de la configuración en ejecución?</p>	<pre>Sh run   sec rip router rip version 2  passive-interface Loopback0 network 10.0.0.0  network 172.16.0.0  no auto-summary</pre>
---	---

El comando `sh ip protocols` me muestra varios parámetros sobre la configuración activa que esta sobre el protocolo de routing IPV4, me indica que sobre `s0/0/1` tiene como ruta máxima 4 enrutamientos para redes 172.16.0.0, 192.168.4.0, 192.168.5.0, 192.168.6.0, 192.168.7.0. Las Interfaces pasivas son: Loopback4 Loopback5 Loopback6 Loopback7, la Distancia de puerta de enlace es 172.16.2.2 120 00:00:0, tiene desactivada la sumarizacion automática para que esta no de permisos al Router para agrupar redes.

## Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17 Implementar DHCP y NAT para IPv4 1

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 192.168.21.1 192.168.21.20 R1(config)#</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 R1(config)#</pre>
Crear un pool de DHCP para la VLAN 21.	<pre>R1(config)# ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 ? A.B.C.D Network mask R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#default-router ? A.B.C.D Router's IP address R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#dom  R1(dhcp-config)#ip R1(dhcp-config)#?  default-router Default routers dns-server Set name server  exit Exit from DHCP pool configuration mode network Network number and mask  no Negate a command or set its defaults  option Raw DHCP options</pre>

<p>Crear un pool de DHCP para la VLAN 23</p>	<pre> R1(config)# ip dhcp pool ENGR R1(dhcp-config)#net R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#defa R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#dns 10.10.10.10 R1(dhcp-config)#? default-router Default routers dns-server Set name server exit Exit from DHCP pool configuration mode network Network number and mask no Negate a command or set its defaults option Raw DHCP options R1(dhcp-config)# </pre>
--	---

En esta parte de la configuración se asignan las ip utilizables DHCP de la 192.168.21.1 a la 192.168.21.20 sobre la VLAN21, luego se reservan ip de la 192.168.23.1 a 192.168.23.20 para la VLAN23

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

La configuración del R2 incluye las siguientes tareas:

Tabla 18 Configurar la NAT estática 1

Elemento o tarea de configuración	Especificación
<p>Crear una base de datos local con una cuenta de usuario</p>	<pre> R2(config)#username webuser privilege 15 password cisco12345 R2(config)# </pre>
<p>Habilitar el servicio del servidor HTTP</p>	<p>Habilitado</p>

<p>Configurar el servidor HTTP para utilizar la base de datos local para la autenticación</p>	<p>R2(config)#ip ?  access-list Named access-list  cef Cisco Express Forwarding  default-gateway Specify default gateway (if not routing IP)  default-network Flags networks as candidates for default routes  dhcp Configure DHCP server and relay parameters  domain IP DNS Resolver  domain-lookup Enable IP Domain Name System hostname translation  domain-name Define the default domain name  flow-export Specify host/port to send flow statistics  forward-protocol Controls forwarding of physical and directed IP broadcasts  ftp FTP configuration commands  host Add an entry to the ip hostname table  local Specify local options  name-server Specify address of name server to use  nat NAT configuration commands  route Establish static routes  routing Enable IP routing  ssh Configure ssh options  tcp Global TCP parameters</p> <p>R2(config)#ip  No da la opción para habilitar el http sobre los routers</p>
<p>Crear una NAT estática al servidor web.</p>	<p>R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229  R2(config)#</p>

Asignar la interfaz interna y externa para la NAT estática	<pre>R2(config)#int      g0/0 R2(config-if)#ip   nat   o R2(config-if)#ip nat outside  R2(config-if)#  R2(config)#int      lo0 R2(config-if)#ip nat inside</pre>
Configurar la NAT dinámica dentro de una ACL privada	<pre>R2#sh ip access-lists Standard IP access list 1 10 permit 192.168.23.0 0.0.0.255 20 permit 192.168.21.0 0.0.0.255 30 permit 192.168.4.0 0.0.3.255</pre>
Defina el pool de direcciones IP públicas utilizables.	<pre>R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netma 255.255.25.248 R2(config)#</pre>
Definir la traducción de NAT dinámica	<pre>R2(config)#ip nat inside source list 1 pool INTERNET overload R2(config)#</pre>

En este paso se creó una base de datos local con usuario y password, se configura un servidor HTTP para el acceder a la base de datos solicitando usuario password, se crea una NAT 10.10.10.10 209.165.200.229, estática al servidor web lo que permite que cualquier host que este en la misma dirección ip pueda consultar sobre esta, se asigna una interfaz interna y externa para la NAT estática, se configura la NAT dinámica esto se realiza para que cada que una dirección ip privada este consultando en la internet, el router asigne una ip pública que no se esté utilizando, lo que aumenta la seguridad, porque las ip públicas van cambiando a medida que se conecte un host externo.

### **Paso 3: Verificar el protocolo DHCP y la NAT estática**

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

Tabla 19 Verificar el protocolo DHCP 1

Prueba	Resultados
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	<pre> PC&gt;ipconfig /all  FastEthernet0 Connection:(default port)  Connection-specific DNS Suffix...: Physical Address..... 0001.42EA.1C2C Link-local IPv6 Address.....: FE80::201:42FF:FEEA:1C2C IP Address..... : 192.168.21.21 Subnet Mask ..... : 255.255.255.0 Default Gateway..... : 192.168.21.1 DNS Servers.....: 10.10.10.10 DHCP Servers..... : 192.168.21.1 DHCPv6 IAID. ....15105 DHCPv6 Client DUID.....: 00-01-00-01- 2B-54-06-04-00-01-42-EA-1C-2C  PC&gt; </pre>

<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	<pre> PC&gt;ipconfig /all  FastEthernet0 Connection:(default port)  Connection-specific DNS Suffix...: Physical Address..... 0060.3E82.7C18 Link-local IPv6 Address.....: FE80::260:3EFF:FE82:7C18 IP Address..... : 192.168.23.21 Subnet Mask .....: 255.255.255.0 Default Gateway ..... : 192.168.23.1 DNS Servers.....: 10.10.10.10 DHCP Servers..... : 192.168.23.1 DHCPv6 Client DUID.....: 00-01-00-01- 5D-1C-1D-BC-00-60-3E-82-7C-18  PC&gt; </pre>
--	--



<p>Verificar que la PC-A pueda hacer ping a la PC-C</p> <p>Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	<pre>PC&gt;ping 192.168.23.21  Pinging 192.168.23.21 with 32 bytes of data:  Request timed out. Reply from 192.168.23.21: bytes=32 time=0ms TTL=127 Reply from 192.168.23.21: bytes=32 time=0ms TTL=127 Reply from 192.168.23.21: bytes=32 time=0ms TTL=127  Ping statistics for 192.168.23.21: Packets: Sent = 4, Received = 3, Lost = 1 (25% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms  PC&gt;</pre>
---	--

<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>Se prueba acceso desde el servidor externo a la loopbak por ping:</p> <p>SERVER&gt;ping 209.165.200.229</p> <p>Pinging 209.165.200.229 with 32 bytes of data:</p> <p>Reply from 209.165.200.229: bytes=32 time=0ms TTL=255</p> <p>Reply from 209.165.200.229: bytes=32 time=0ms TTL=255</p> <p>Reply from 209.165.200.229: bytes=32 time=0ms TTL=255</p> <p>Reply from 209.165.200.229: bytes=32 time=0ms TTL=255</p> <p>Ping statistics for 209.165.200.229:</p> <p>Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),</p> <p>Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 0ms, Average = 0ms</p> <p>SERVER&gt;</p>
--	--

Figura 9. Ipconfig/all 1 1

```

PC>ipconfig /all

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Physical Address.....: 0060.3E82.7C18
    Link-local IPv6 Address.....: FE80::260:3EFF:FE82:7C18
    IP Address.....: 192.168.23.21
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 192.168.23.1
    DNS Servers.....: 10.10.10.10
    DHCP Servers.....: 192.168.23.1
    DHCPv6 Client DUID.....: 00-01-00-01-5D-1C-1D-BC-00-60-3E-82-7C-18

PC>

```

Figura 10. Ping 209.165.200.229 1

```
SERVER>ping 209.165.200.229

Pinging 209.165.200.229 with 32 bytes of data:

Reply from 209.165.200.229: bytes=32 time=0ms TTL=255
Reply from 209.165.200.229: bytes=32 time=1ms TTL=255
Reply from 209.165.200.229: bytes=32 time=0ms TTL=255
Reply from 209.165.200.229: bytes=32 time=0ms TTL=255

Ping statistics for 209.165.200.229:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

SERVER>
```

Figura 11. Ping 192.168.23.21 1 1

```
FastEthernet0 Connection:(default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0001.42EA.1C2C
Link-local IPv6 Address.....: FE80::201:42FF:FEEA:1C2C
IP Address.....: 192.168.21.21
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.21.1
DNS Servers.....: 10.10.10.10
DHCP Servers.....: 192.168.21.1
DHCPv6 Client DUID.....: 00-01-00-01-2B-54-06-04-00-01-42-EA-1C-2C

PC>ping 192.168.23.21

Pinging 192.168.23.21 with 32 bytes of data:

Reply from 192.168.23.21: bytes=32 time=0ms TTL=127
Reply from 192.168.23.21: bytes=32 time=0ms TTL=127
Reply from 192.168.23.21: bytes=32 time=0ms TTL=127
Reply from 192.168.23.21: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.23.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

- Se verifica que las PC-A, PC-C adquirieron protocolos de ip del servidor

DHCP realiza ping verificando las conexiones de la PC-A a la PC-C, se evidencia conexión entre el pc.

## Parte 6: Configurar NTP

Tabla 20 Configurar NTP 1

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2.	<pre>R2#clock set 9:00 5 MAR 2016 R2#.</pre>
Configure R2 como un maestro NTP.	<pre>R2#sh ntp status Clock is synchronized, stratum 2, reference is 209.165.200.238  nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19 reference time is E2343007.000002FE (10:23:03.766 UTC Tue May 5 2020)  clock offset is 0.00 msec, root delay is 0.00 msec  root dispersion is 0.02 msec, peer dispersion is 0.02 msec.  R2#</pre>

Configurar R1 como un cliente NTP.

```
R1#sh ntp status
Clock is synchronized,
stratum 2, reference is
209.165.200.238

nominal freq is
250.0000 Hz, actual
freq is 249.9990 Hz,
precision is 2**19
reference time is
E2343084.0000013B
(10:25:08.315 UTC Tue
May 5 2020)

clock offset is 0.00
msec, root delay is 0.00
msec

root dispersion is 0.02
msec, peer dispersion
is 0.02 msec.

R1#
```

<p>Verifique la configuración de NTP en R1.</p>	<pre> R2#sh ntp status Clock is synchronized, stratum 2, reference is 209.165.200.238  nominal freq is 250.0000 Hz, actual freq is 249.9990 Hz, precision is 2**19 reference time is E2343007.000002FE (10:23:03.766 UTC Tue May 5 2020)  clock offset is 0.00 msec, root delay is 0.00 msec  root dispersion is 0.02 msec, peer dispersion is 0.02 msec.  R2# </pre>
---	---

- Se ajusta la hora y fecha a R2, se configura a r2 como un maestro NTP, este protocolo es usado para sincronizar los relojes de los sistemas de conmutación, se configura r1 como cliente de NTP, esto se realiza para tener datos en fecha y hora real así su configuración será más coherente.

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

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

Tabla 21 Restringir el acceso líneaVTY 1

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	<pre>R2(config)#ip access- list extended ADMIN- MGT R2(config-ext- nacl)#permit tcp host 172.16.1.1 host 172.16.1.2 eq 23 R2(config-ext-nacl)#</pre>
Aplicar la ACL con nombre a las líneas VTY	<pre>R2(config-line)#access- class ADMIN-MGT in</pre>
Permitir acceso por Telnet a las líneas de VTY	<pre>R2(config-line)# R2(config- line)#transport input telnet R2(config-line)#</pre>
Verificar que la ACL funcione como se espera	<pre>R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenSe prohbe el acceso no autorizado.  User Access Verification Password:</pre>

Se configura una lista de accesos como administrador, para que R1 establezca conexiones telnet con R2, mediante parametro ACL el cual limita la conexiones de salida entre dispositivos entre esta listas de direcciones, restringiendo que cualquier acceso no autorizado.



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

Tabla 22 Introducir el comando de CLI 1

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#sh ip access-lists Standard IP access list 1 10 permit host 192.168.21.0 20 permit host 192.168.23.0 30 permit 192.168.4.0 0.0.3.255 Extended IP access list ADMIN-MGT 10 permit tcp any host 172.16.1.2 eq telnet 20 permit tcp any host 172.16.2.2 eq telnet (3 match(es)) 30 permit tcp any host 10.10.10.10 eq telnet</pre>
Restablecer los contadores de una lista de acceso	<pre>R2#clear access-list counters R2#</pre>
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	<pre>R2#sh ip interface s0/0/0 Serial0/0/0 is up, line protocol is up (connection)  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</pre>

<p>¿Con qué comando se muestran las traducciones NAT?</p>	<pre>R2#sh ip nat translations Pro Inside global Inside local Outside local Outside global icmp 209.165.200.225:43192.168.21.21:43 209.165.200.238:43 209.165.200.238:43 icmp 209.165.200.225:44192.168.21.21:44 209.165.200.238:44 209.165.200.238:44 icmp 209.165.200.225:45192.168.21.21:45 209.165.200.238:45 209.165.200.238:45 icmp 209.165.200.225:46192.168.21.21:46 209.165.200.238:46 209.165.200.238:46 --- 209.165.200.229 10.10.10.10 --- ---</pre>
<p>¿Qué comando se utiliza para eliminar las traducciones de NAT dinámicas?</p>	<pre>R2#clear ip nat translation * R2#</pre>

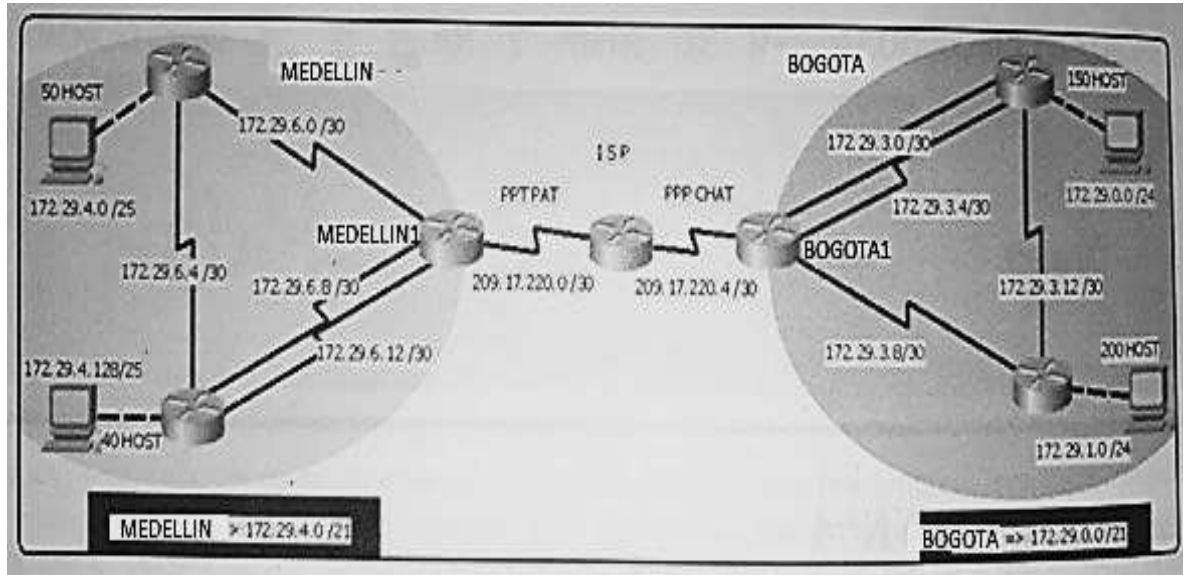
En este paso se revisa mediante comando `sh ip access-lists`, permite ver la lista de accesos de las ip estándar y el acceso de las Lista de acceso IP extendida ADMIN-MGT, identificamos las direcciones ip que tiene permisos, luego ejecutamos el comando `sh ip nat translations` en r2, para verificar que la traducción de existe en la table de traducción de la NAT, luego se utiliza le ,comando `clear ip nat translation` para eliminar las traducciones de la NAT dinámicas.

## 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 de red

Figura 12. Topología de red escenario 2 1



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).**

```

hostname MEDELLIN1
hostname MEDELLIN2
hostname MEDELLIN3
hostname BOGOTA1
hostname BOGOTA2
hostname BOGOTA3
hostname ISP
!
enable secret class
!
service password-encryption
!
line con 0
password 7 cisco login
!
line aux 0
!
line vty 0 4
password 7 cisco login
line vty 5 15
password 7 cisco
login

```

Realizar la conexión física de los equipos con base en la topología de red BOGOTA1(config)#int s0/0/1  
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252

```

BOGOTA1(config
-if)#no      shu
BOGOTA1(config
)#int s0/1/1

```

```

BOGOTA1(config-if)#ip  address  172.29.3.5
255.255.255.252 BOGOTA1(config-if)#no shu

```

```

BOGOTA1(config-if)#int s0/1/0

```

```

BOGOTA1(config-if)#ip  address  172.29.3.9
255.255.255.252 BOGOTA1(config-if)#no shu

```

```

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

```

```

MEDELLIN1(config-if)#ip  address  172.29.6.1
255.255.255.252 MEDELLIN1(config-if)#no shu

```

```

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

```

```

MEDELLIN1(config-if)#ip  address  172.29.6.9

```

```
255.255.255.252 MEDELLIN1(config-if)#no shu
MEDELLIN1(config)#int s0/0/0
```

```
MEDELLIN1(config-if)#ip address 172.29.6.13
255.255.255.252 MEDELLIN1(config-if)#no shu
```

```
MEDELLIN1#sh ip int brief
```

```
Interface IP-Address OK? Method Status Protocol
```

```
GigabitEthernet0/0 unassigned YES unset administratively
down down GigabitEthernet0/1 unassigned YES unset
administratively down down Serial0/0/0 172.29.6.13 YES
manual up up
```

```
Serial0/0/1 172.29.6.1 YES
manual up up Serial0/1/0
172.29.6.9 YES manual up up
Serial0/1/1 209.17.220.2 YES
manual up up
```

```
Vlan1 unassigned YES unset administratively
down down MEDELLIN1#
```

```
BOGOTA1#sh ip int bri
```

```
Interface IP-Address OK? Method Status Protocol
```

```
GigabitEthernet0/0 unassigned YES unset administratively
down down GigabitEthernet0/1 unassigned YES unset
administratively down down Serial0/0/0 209.17.220.6 YES
manual up up
```

```
Serial0/0/1 172.29.3.1 YES
manual up up Serial0/1/0
172.29.3.9 YES manual up up
Serial0/1/1 172.29.3.5 YES
manual up up
```

```
Vlan1 unassigned YES unset administratively
down down BOGOTA1#
```

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

En esta configuración procedo a realizar la desactivación de la búsqueda de DNS, con el fin de iniciar la asignación de nombre, contraseñas, y encriptación, esto con el fin de tener la seguridad requerida, implementamos las interfaces S/0/0/0, S/0/0/0, S/0/1/0 para interconectar los routers entre sí, Configuro las Interfaces G0/0, G0/1.

,

## 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.

```
BOGOTA1(config)#router ospf 100
BOGOTA1(config-router)#network 209.17.220.6 ?
A.B.C.D OSPF wild card bits
BOGOTA1(config-router)#network 209.17.220.6 0.0.0.3
% Incomplete command.
BOGOTA1(config-router)#network 209.17.220.6 0.0.0.3 ar
BOGOTA1(config-router)#network 209.17.220.6 0.0.0.3 area 1
BOGOTA1(config-router)#no network 209.17.220.6 0.0.0.3 area 1
BOGOTA1(config-router)# network 172.29.3.0 0.0.0.3 area 1
BOGOTA1(config-router)# network 172.29.3.4 0.0.0.3 area 1
BOGOTA1(config-router)#          network
172.29.3.8 0.0.0.3 area 1 BOGOTA1(config-
router)#no au
BOGOTA1(conf
ig-router)#suma
BOGOTA1(conf
ig-router)#nei

BOGOTA1(config-router)#neighbor ?
A.B.C.D Neighbor address
BOGOTA1(config-router)#neighbor 172.17.3.2 ?
<cr>
BOGOTA1(config-router)#neighbor 172.17.3.2
BOGOTA1(config-router)#neighbor 172.17.3.9
BOGOTA1(config-router)#neighbor 172.17.3.5
BOGOTA1(config-router)#no neighbor 172.17.3.5
BOGOTA1(config-router)#no neighbor 172.17.3.9
BOGOTA1(config-router)#neighbor 172.17.3.6
```

```
BOGOTA1(config-  
router)#neighbor 172.17.3.10  
BOGOTA1(config-router)#^Z
```

### **BOGOTA2#conf t**

```
Enter configuration commands, one per line.  
End with CNTL/Z. BOGOTA2(config)#router  
ospf 100
```

```
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3
```

```
% Incomplete command.
```

```
BOGOTA2(config-router)#network 172.29.3.4 0.0.0.3
```

```
% Incomplete command.
```

```
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 1
```

```
BOGOTA2(config-router)#network 172.29.3.4 0.0.0.3 area 1
```

```
BOGOTA2(config-router)#network  
172.29.3.0 0.0.0.3 area 1 BOGOTA2(config-  
router)#ne
```

```
BOGOTA2(config-router)#nei  
BOGOTA2(config-  
router)#neighbor 172.29.3.
```

```
00:53:03: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.6 on  
Serial0/0/0 from LOADING to FULL, Loading Done
```

```
14
```

```
BOGOTA2(config-router)#neighbor 172.29.3.14 ?
```

```
<cr>
```

```
BOGOTA2(config-  
router)#neighbor 172.29.3.14  
BOGOTA2(config-router)#
```

```
% OSPF: Configured Nbr 172.29.3.14 is incompatible with OSPF  
network type on Serial0/0/0
```

```
00:53:09: %OSPF-4-CFG_NBR_INVALID_NET_TYPE: Can not  
use configured neighbor 172.29.3.14 on Serial0/0/0. Neighbor  
command only allowed on NBMA and P2MP networks
```



00:53:09: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.6 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Neighbor configuration invalid

00:53:13: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.6 on Serial0/0/0 from LOADING to FULL, Loading Done

```
BOGOTA2(config-  
router)#neighbor 172.29.3.5  
BOGOTA2(config-router)#
```

% OSPF: Configured Nbr 172.29.3.5 is incompatible with OSPF network type on Serial0/0/0

00:53:23: %OSPF-4-CFG\_NBR\_INVALID\_NET\_TYPE: Can not use configured neighbor 172.29.3.5 on Serial0/0/0. Neighbor command only allowed on NBMA and P2MP networks

00:53:23: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.6 on Serial0/0/0 from FULL to DOWN, Neighbor Down: Neighbor configuration invalid

00:53:23: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.6 on Serial0/0/0 from LOADING to FULL, Loading Done

```
BOGOTA2(config-  
router)#neighbor 172.29.3.1  
BOGOTA2(config-router)#
```

% OSPF: Configured Nbr 172.29.3.1 is incompatible with OSPF network type on Serial0/0/0

00:53:27: %OSPF-4-CFG\_NBR\_INVALID\_NET\_TYPE: Can not use configured neighbor 172.29.3.1 on Serial0/0/0. Neighbor command only allowed on NBMA and P2MP networks

00:53:27: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.6 on

Serial0/0/0 from FULL to DOWN, Neighbor Down: Neighbor configuration invalid

BOGOTA2(config-router)#neighbor 172.29.3.1

00:53:33: %OSPF-5-ADJCHG: Process 100, Nbr 209.17.220.6 on Serial0/0/0 from LOADING to FULL, Loading Done

BOGOTA2#sh ip ospf neighbor

Neighbor Address	ID	Pri	State	Dead Time	Interface
209.17.220.6	0	FULL/			Serial0/0/0
172.29.3.1	0	FULL/		00:00:34	Serial0/0/0
209.17.220.6	0	FULL/		00:00:39	Serial0/0/1
172.29.3.14	0	FULL/		00:00:34	Serial0/1/0

BOGOTA3(config)#router ospf 100

BOGOTA3(config-router)#network 172.29.3.8 0.0.0.3

% Incomplete command.

BOGOTA3(config-router)#network 172.29.3.8 0.0.0.3 area 1

BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 1

BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 1

00:55:36: %OSPF-5-ADJCHG: Process 100, Nbr 172.29.3.13 on Serial0/0/1 from LOADING to FULL, Loading Done

MEDELLIN2(config)  
)#router ospf 50  
MEDELLIN2(config  
-router)#net

MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3

% Incomplete command.

MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 2

MEDELLIN2(config-router)#network 172.29.6.8 0.0.0.3 area 2

```
MEDELLIN2(config-router)#no network 172.29.6.8 0.0.0.3 area 2
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 2
MEDELLIN2(config-router)#network 172.29.4.0
0.0.0.255 area 2 MEDELLIN2(config-router)#
```

```
MEDELLIN3(config)#router ospf 50
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 2
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 2
MEDELLIN3(config-router)#network
172.29.6.4 0.0.0.3 area 2 MEDELLIN3(config-
router)#
```

```
MEDELLIN3#sh ip ospf neighbor
Neighbor ID Pri State Dead Time
Address Interface 172.29.6.6 0 FULL/
- 00:00:38 172.29.6.6 Serial0/0/0
209.17.220.2 0 FULL/ - 00:00:31 172.29.6.9 Serial0/0/1
209.17.220.2 0 FULL/ - 00:00:35
172.29.6.13 Serial0/1/0 MEDELLIN3#
```

Se procede a configura el enrutamiento en la red utilizando los protocolos (OSPF), para proceder a declarar los enrutamientos para la sucursal de Bogotá se le asigna el id 100 y para el protocolo OSPF de la sucursal de Medellín se le asigna el id 50 se les asigna el id 1 para las áreas se desactiva la sumarizacion automática para que esta no de permisos al Router para agrupar redes.

- b. Los routers Bogota1 y Medellín1 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.

```
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
```

```
BOGOTA1(config)#router ospf  
100 BOGOTA1(config-  
router)#redistribute static
```

```
BOGOTA1(config-router)#default-  
information originate BOGOTA1(config-  
router)#
```

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
```

```
MEDELLIN1(config)#router ospf 50  
MEDELLIN1(config-router)#info  
MEDELLIN1(config-router)#de  
MEDELLIN1(config-router)#default-  
information or
```

```
MEDELLIN1(config-router)#default-  
information originate MEDELLIN1(config-  
router)#red
```

```
MEDELLIN1(config-  
router)#redistribute st  
MEDELLIN1(config-  
router)#redistribute static
```

```
% Only classful networks will be  
redistributed MEDELLIN1(config-  
router)#
```

Se configuran los routers de bogota1 y medellin1 con su respectivo direccionamiento, para que tengan accesos a la ISP, "servicio de internet".

- 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.

```
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)#
```

- Se realiza el respectivo direccionamiento del Router hacia el ISP se segmentan las subredes de cada sucursal se sumarizan.

## parte 2: Tabla de Enrutamiento.

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

Gateway of last resort is 209.17.220.5 to

network 0.0.0.0 172.29.0.0/16 is variably

subnetted, 8 subnets, 3 masks

O 172.29.1.0/24 [110/65] via 172.29.3.10, 00:14:31, Serial0/1/1

C 172.29.3.0/30 is directly  
connected, Serial0/0/1 L

172.29.3.1/32 is directly  
connected, Serial0/0/1 C

172.29.3.4/30 is directly  
connected, Serial0/1/0 L

172.29.3.5/32 is directly  
connected, Serial0/1/0 C

172.29.3.8/30 is directly  
connected, Serial0/1/1 L

172.29.3.9/32 is directly  
connected, Serial0/1/1

O 172.29.3.12/30 [110/128] via 172.29.3.6, 00:14:11,  
Serial0/1/0 [110/128] via 172.29.3.10, 00:14:11,  
Serial0/1/1

209.17.220.0/24 is variably subnetted, 2  
subnets, 2 masks C 209.17.220.4/30 is  
directly connected, Serial0/0/0

L 209.17.220.6/32 is directly  
connected, Serial0/0/0 S\* 0.0.0.0/0  
[1/0] via 209.17.220.5

BOGOTA1#

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 172.29.3.14, 00:29:38, 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 172.29.3.14, 00:14:56, Serial0/1/0

[110/128] via 172.29.3.1, 00:14:56, Serial0/0/0

C 172.29.3.12/30 is directly  
connected, Serial0/1/0 L  
172.29.3.13/32 is directly  
connected, Serial0/1/0

O\*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:09:06, Serial0/0/0

BOGOTA2#

172.29.0.0/16 is variably subnetted, 8  
subnets, 3 masks C 172.29.1.0/24 is  
directly connected, GigabitEthernet0/0 L  
172.29.1.1/32 is directly connected,  
GigabitEthernet0/0

O 172.29.3.0/30 [110/128] via 172.29.3.9, 00:15:40,  
Serial0/0/0 [110/128] via 172.29.3.13, 00:15:40,  
Serial0/0/1

O 172.29.3.4/30 [110/128] via 172.29.3.9, 00:15:30,  
Serial0/0/0 [110/128] via 172.29.3.13, 00:15:30,  
Serial0/0/1

C 172.29.3.8/30 is directly  
connected, Serial0/0/0 L  
172.29.3.10/32 is directly  
connected, Serial0/0/0 C  
172.29.3.12/30 is directly  
connected, Serial0/0/1 L  
172.29.3.14/32 is directly  
connected, Serial0/0/1

O\*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:09:50, Serial0/0/0  
BOGOTA3#

172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks

O 172.29.4.0/25 [110/65] via 172.29.6.2, 00:27:24, Serial0/0/1

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, 00:20:17,  
Serial0/0/1 [110/128] via 172.29.6.14, 00:20:17,  
Serial0/1/0

C 172.29.6.8/30 is directly  
connected, Serial0/0/0 L  
172.29.6.9/32 is directly  
connected, Serial0/0/0 C  
172.29.6.12/30 is directly  
connected, Serial0/1/0 L  
172.29.6.13/32 is directly  
connected, Serial0/1/0

209.17.220.0/24 is variably subnetted, 2  
subnets, 2 masks C 209.17.220.0/30 is  
directly connected, Serial0/1/1

L 209.17.220.2/32 is directly  
connected, Serial0/1/1 S\* 0.0.0.0/0  
[1/0] via 209.17.220.1

MEDELLIN1#

Gateway of last resort is 172.29.6.1 to network 0.0.0.0

172.29.0.0/16 is variably subnetted, 8  
subnets, 3 masks C 172.29.4.0/25 is  
directly connected, GigabitEthernet0/1 L  
172.29.4.1/32 is directly connected,  
GigabitEthernet0/1 C 172.29.6.0/30 is  
directly connected, Serial0/0/1

L 172.29.6.2/32 is directly

connected, Serial0/0/1 C  
172.29.6.4/30 is directly  
connected, Serial0/0/0

L 172.29.6.6/32 is directly connected, Serial0/0/0

O 172.29.6.8/30 [110/128] via 172.29.6.1, 00:20:28,  
Serial0/0/1 [110/128] via 172.29.6.5, 00:20:28,  
Serial0/0/0

O 172.29.6.12/30 [110/128] via 172.29.6.1, 00:20:41,  
Serial0/0/1 [110/128] via 172.29.6.5, 00:20:41,  
Serial0/0/0

O\*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:08:21, Serial0/0/1

MEDELLIN2#

Gateway of last resort is 172.29.6.13 to

network 0.0.0.0 172.29.0.0/16 is variably

subnetted, 10 subnets, 3 masks

O 172.29.4.0/25 [110/65] via 172.29.6.6, 00:28:55, Serial0/0/0

C 172.29.4.128/25 is directly connected,  
GigabitEthernet0/0 L 172.29.4.129/32 is  
directly connected, GigabitEthernet0/0

O 172.29.6.0/30 [110/128] via 172.29.6.13, 00:21:02,  
Serial0/1/0 [110/128] via 172.29.6.6, 00:21:02,  
Serial0/0/0

C 172.29.6.4/30 is directly  
connected, Serial0/0/0 L  
172.29.6.5/32 is directly  
connected, Serial0/0/0 C  
172.29.6.8/30 is directly  
connected, Serial0/0/1 L  
172.29.6.10/32 is directly  
connected, Serial0/0/1 C  
172.29.6.12/30 is directly  
connected, Serial0/1/0 L  
172.29.6.14/32 is directly  
connected, Serial0/1/0



O\*E2 0.0.0.0/0 [110/1] via 172.29.6.13, 00:08:42, Serial0/1/0  
MEDELLIN3#

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

BOGOTA2#

O 172.29.3.8/30 [110/128] via 172.29.3.14, 00:14:56,  
Serial0/1/0 [110/128] via 172.29.3.1, 00:14:56,  
Serial0/0/0

MEDELLIN3#

O 172.29.6.0/30 [110/128] via 172.29.6.13, 00:21:02,  
Serial0/1/0 [110/128] via 172.29.6.6, 00:21:02,  
Serial0/0/0

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.

Gateway of last resort is 209.17.220.5 to  
network 0.0.0.0 172.29.0.0/16 is variably  
subnetted, 8 subnets, 3 masks

O 172.29.1.0/24

[110/65]via172.29.3.10,00:14:31,Serial0/1/1

C 172.29.3.0/30 is directly  
connected, Serial0/0/1 L  
172.29.3.1/32 is directly  
connected, Serial0/0/1 C  
172.29.3.4/30 is directly  
connected, Serial0/1/0 L  
172.29.3.5/32 is directly  
connected, Serial0/1/0 C  
172.29.3.8/30 is directly

connected, Serial0/1/1 L  
172.29.3.9/32 is directly  
connected, Serial0/1/1  
O 172.29.3.12/30 [110/128] via 172.29.3.6,  
00:14:11, Serial0/1/0 [110/128] via 172.29.3.10,  
00:14:11, Serial0/1/1  
209.17.220.0/24 is variably subnetted, 2  
subnets, 2 masks C 209.17.220.4/30 is  
directly connected, Serial0/0/0  
L 209.17.220.6/32 is directly  
connected, Serial0/0/0  
S\* 0.0.0.0/0 [1/0] via 209.17.220.5  
BOGOTA1#

172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks  
O 172.29.4.0/25 [110/65] via 172.29.6.2, 00:27:24, Serial0/0/1  
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,  
00:20:17, Serial0/0/1 [110/128] via 172.29.6.14,  
00:20:17, Serial0/1/0  
C 172.29.6.8/30 is directly  
connected, Serial0/0/0 L  
172.29.6.9/32 is directly  
connected, Serial0/0/0 C  
172.29.6.12/30 is directly  
connected, Serial0/1/0 L  
172.29.6.13/32 is directly  
connected, Serial0/1/0  
209.17.220.0/24 is variably subnetted, 2  
subnets, 2 masks C 209.17.220.0/30 is  
directly connected, Serial0/1/1  
L 209.17.220.2/32 is directly  
connected, Serial0/1/1  
S\* 0.0.0.0/0 [1/0] via 209.17.220.1  
MEDELLIN1#

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

172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks C 172.29.4.0/25 is directly connected, GigabitEthernet0/1 L 172.29.4.1/32 is directly connected, GigabitEthernet0/1 C 172.29.6.0/30 is directly connected, Serial0/0/1

L 172.29.6.2/32 is directly connected, Serial0/0/1 C 172.29.6.4/30 is directly connected, Serial0/0/0 L 172.29.6.6/32 is directly connected, Serial0/0/0

O 172.29.6.8/30 [110/128] via 172.29.6.1, 00:20:28, Serial0/0/1 [110/128] via 172.29.6.5, 00:20:28, Serial0/0/0

O 172.29.6.12/30 [110/128] via 172.29.6.1, 00:20:41, Serial0/0/1 [110/128] via 172.29.6.5, 00:20:41, Serial0/0/0

O\*E2 0.0.0.0/0 [110/1] via 172.29.6.1, 00:08:21, Serial0/0/1

## MEDELLIN2#

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 172.29.3.14, 00:29:38, 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 172.29.3.14, 00:14:56, Serial0/1/0  
[110/128] via 172.29.3.1, 00:14:56, Serial0/0/0

C 172.29.3.12/30 is directly  
connected, Serial0/1/0 L  
172.29.3.13/32 is directly  
connected, Serial0/1/0

O\*E2 0.0.0.0/0 [110/1] via 172.29.3.1, 00:09:06, Serial0/0/0

## BOGOTA2#

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

172.29.0.0/16 is variably subnetted, 8  
subnets, 3 masks C 172.29.1.0/24 is  
directly connected, GigabitEthernet0/0 L  
172.29.1.1/32 is directly connected,  
GigabitEthernet0/0

O 172.29.3.0/30 [110/128] via 172.29.3.9, 00:15:40, Serial0/0/0  
[110/128] via 172.29.3.13, 00:15:40, Serial0/0/1

O 172.29.3.4/30 [110/128] via 172.29.3.9, 00:15:30, Serial0/0/0  
[110/128] via 172.29.3.13, 00:15:30, Serial0/0/1

C 172.29.3.8/30 is directly  
connected, Serial0/0/0 L  
172.29.3.10/32 is directly  
connected, Serial0/0/0 C  
172.29.3.12/30 is directly  
connected, Serial0/0/1 L  
172.29.3.14/32 is directly  
connected, Serial0/0/1

O\*E2 0.0.0.0/0 [110/1] via 172.29.3.9, 00:09:50, Serial0/0/0

## BOGOTA3#

172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks

O 172.29.4.0/25 [110/65] via 172.29.6.6, 00:28:55, Serial0/0/0

C 172.29.4.128/25 is directly connected,  
GigabitEthernet0/0 L 172.29.4.129/32 is  
directly connected, GigabitEthernet0/0

O 172.29.6.0/30 [110/128] via 172.29.6.13, 00:21:02, Serial0/1/0

[110/128] via 172.29.6.6, 00:21:02, Serial0/0/0

C 172.29.6.4/30 is directly  
connected, Serial0/0/0 L  
172.29.6.5/32 is directly  
connected, Serial0/0/0 C  
172.29.6.8/30 is directly  
connected, Serial0/0/1 L  
172.29.6.10/32 is directly  
connected, Serial0/0/1

C 172.29.6.12/30 is directly  
connected, Serial0/1/0 L  
172.29.6.14/32 is directly  
connected, Serial0/1/0

O\*E2 0.0.0.0/0 [110/1] via 172.29.6.13, 00:08:42, Serial0/1/0

MEDELLIN3#

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

Gateway of last resort is not set

172.29.0.0/22 is  
subnetted, 2 subnets  
S 172.29.0.0/22 [1/0]  
via 209.17.220.6 S

172.29.4.0/22 [1/0] via  
209.17.220.2

209.17.220.0/24 is variably subnetted, 4  
subnets, 2 masks C 209.17.220.0/30 is  
directly connected, Serial0/0/0

L 209.17.220.1/32 is directly  
connected, Serial0/0/0 C  
209.17.220.4/30 is directly  
connected, Serial0/0/1 L  
209.17.220.5/32 is directly  
connected, Serial0/0/1 ISP#

Al realizar la revisión de la carga que presentan los routers encuentro, que los routers bogota1 y medellin1 tienen ciertas similitudes por la ubicación y por tener ciertas características como lo son los enlaces de conexión hacia el otro Router y por la ruta por defecto que manejan, encuentro que los routers bogota2 y medellin2 presentan redes conectadas directamente y recibidas mediante la RIP, para los routers bogota3 y medellin3, encuentro que tienen dos interfaces para acceso a la internet, las tablas de los demás routers deben permitir visualizar las rutas por defecto asignadas en el punto b donde se halla más de una ruta para acceder a internet.

### Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

Tabla 23 Deshabilitar propagación OSPF 1

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

```

BOGOTA1(config)
#router ospf 100
BOGOTA1(config-
router)#pas

BOGOTA1(config-
router)#passive-interface s0/0/0
BOGOTA1(config-router)#
BOGOTA2(config)#router ospf
100 BOGOTA2(config-router)#pas

BOGOTA2(config-
router)#passive-interface in
BOGOTA2(config-
router)#passive-interface gi0/0
BOGOTA2(config-router)#

```

```
BOGOTA3(config)
#router osp
BOGOTA3(config)
#router ospf 100
BOGOTA3(config-
router)#pas
BOGOTA3(config-
router)#passive-interface g0/0
BOGOTA3(config-router)#
```

```
MEDELLIN1(config
)#router osp
MEDELLIN1(config
)#router ospf 50
MEDELLIN1(config
-router)#pas
MEDELLIN1(config-router)#passive-interface s/0/1/1
```

```
MEDELLIN2#conf t
Enter configuration commands, one per line. End with
CNTL/Z. MEDELLIN2(config)#router os
MEDELLIN2(config)#router ospf
50 MEDELLIN2(config-
router)#pas MEDELLIN2(config-
router)#passive-interface g0/1
MEDELLIN2(config-router)#
```

```
MEDELLIN3#conf t
Enter configuration commands, one per line. End with
CNTL/Z. MEDELLIN3(config)#router ospf 100
MEDELLIN3(config-router)#pas
MEDELLIN3(config-
router)#passive-interface g0/0
MEDELLIN3(config-router)#
```

En este paso nos piden deshabilitar los protocolos OSPF según la tabla y esto se realiza mediante el comando passibe-interface,



este comando nos permite restringir los mensajes de salida entre los routers pero en este caso se utilizó para restringir el intercambio de paquetes de saludos entre los routers, lo que ocasiona pérdida de relación con los vecinos no permite ninguna actualización de ruteo de salida o de entrada.

#### **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.

```
BOGOTA1#sh ip ospf interface
```

```
Serial0/0/1 is up, line  
protocol is up Internet  
address is 172.29.3.1/30,  
Area 1
```

Process ID 100, Router ID 209.17.220.6, Network Type POINT-TO-POINT, Cost: 64

Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
Hello due in 00:00:05

Index 1/1, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1 , Adjacent neighbor count is 1

Adjacent with neighbor 172.29.3.13

Suppress hello for 0 neighbor(s)

Serial0/1/0 is up, line protocol is up

Internet address is 172.29.3.5/30, Area 1

Process ID 100, Router ID 209.17.220.6, Network Type POINT-TO-POINT, Cost: 64

Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
Hello due in 00:00:00

Index 2/2, flood queue length 0

Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 1 , Adjacent neighbor count is 1

Adjacent with neighbor 172.29.3.13

Suppress hello for 0 neighbor(s)

Serial0/1/1 is up, line protocol is up

Internet address is 172.29.3.9/30, Area 1

Process ID 100, Router ID 209.17.220.6, Network Type POINT-TO-POINT, Cost: 64

Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:00

Index 3/3, flood queue length 0  
Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 1 , Adjacent neighbor count is 1  
Adjacent with neighbor 172.29.3.14

Suppress hello for 0 neighbor(s)

```
Neighbor ID Pri State Dead Time Address Interface
172.29.3.13 0 FULL/ - 00:00:38 172.29.3.2 Serial0/0/1
172.29.3.13 0 FULL/ - 00:00:32 172.29.3.6 Serial0/1/0
172.29.3.14 0 FULL/ - 00:00:30 172.29.3.10 Serial0/1/1
BOGOTA1#
```

BOGOTA2#sh ip ospf interface

Serial0/1/0 is up, line protocol is up Internet  
address is 172.29.3.13/30, Area 1

Process ID 100, Router ID 172.29.3.13, Network Type POINT-TO-POINT, Cost: 64  
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
Hello due in 00:00:04

Index 1/1, flood queue length 0  
Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 1 , Adjacent neighbor count is 1  
Adjacent with neighbor 172.29.3.14

Suppress hello for 0 neighbor(s)  
Serial0/0/1 is up, line protocol is up  
Internet address is 172.29.3.6/30, Area 1

Process ID 100, Router ID 172.29.3.13, Network Type POINT-TO-POINT, Cost: 64  
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
Hello due in 00:00:06

Index 2/2, flood queue length 0  
Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 1 , Adjacent neighbor count is 1  
Adjacent with neighbor 209.17.220.6

Suppress hello for 0 neighbor(s)  
Serial0/0/0 is up, line protocol is up  
Internet address is 172.29.3.2/30, Area 1

Process ID 100, Router ID 172.29.3.13, Network Type POINT-TO-POINT, Cost: 64  
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5

Hello due in 00:00:02

Index 3/3, flood queue length 0  
Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 1 , Adjacent neighbor count is 1  
Adjacent with neighbor 209.17.220.6

Suppress hello for 0 neighbor(s)  
BOGOTA2#sh ip ospf nei

```
Neighbor ID Pri State Dead Time Address Interface
209.17.220.6 0 FULL/ - 00:00:30 172.29.3.1 Serial0/0/0
209.17.220.6 0 FULL/ - 00:00:36 172.29.3.5 Serial0/0/1
172.29.3.14 0 FULL/ - 00:00:30 172.29.3.14 Serial0/1/0
BOGOTA2#
```

BOGOTA3#sh ip ospf interface

Serial0/0/1 is up, line protocol is up Internet  
address is 172.29.3.14/30, Area 1

Process ID 100, Router ID 172.29.3.14, Network Type POINT-TO-POINT, Cost: 64  
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
Hello due in 00:00:01

Index 1/1, flood queue length 0  
Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 1 , Adjacent neighbor count is 1  
Adjacent with neighbor 172.29.3.13

Suppress hello for 0 neighbor(s)  
GigabitEthernet0/0 is up, line protocol is up  
Internet address is 172.29.1.1/24, Area 1

Process ID 100, Router ID 172.29.3.14, Network Type BROADCAST, Cost: 1  
Transmit Delay is 1 sec, State WAITING, Priority 1

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
No Hellos (Passive interface)

Index 2/2, flood queue length 0  
Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec

Neighbor Count is 0, Adjacent neighbor count is 0  
Suppress hello for 0 neighbor(s)

Serial0/0/0 is up, line protocol is up Internet  
address is 172.29.3.10/30, Area 1

Process ID 100, Router ID 172.29.3.14, Network Type POINT-TO-POINT, Cost: 64  
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
Hello due in 00:00:03

Index 3/3, flood queue length 0  
Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 1 , Adjacent neighbor count is 1  
Adjacent with neighbor 209.17.220.6

Suppress hello for 0 neighbor(s)  
BOGOTA3#sh ip ospf nei

```
Neighbor ID Pri State Dead Time Address Interface
209.17.220.6 0 FULL/ - 00:00:31 172.29.3.9 Serial0/0/0
172.29.3.13 0 FULL/ - 00:00:39 172.29.3.13 Serial0/0/1
BOGOTA3#
```

MEDELLIN1#sh ip ospf interface

Serial0/0/1 is up, line protocol is up  
Internet address is 172.29.6.1/30, Area 2

Process ID 50, Router ID 209.17.220.2, Network Type POINT-TO-POINT, Cost: 64  
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
Hello due in 00:00:04

Index 1/1, flood queue length 0  
Next 0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 1 , Adjacent neighbor count is 1  
Adjacent with neighbor 172.29.6.6

Suppress hello for 0 neighbor(s)  
Serial0/1/0 is up, line protocol is up Internet  
address is 172.29.6.13/30, Area 2

Process ID 50, Router ID 209.17.220.2, Network Type POINT-TO-POINT, Cost: 64

```

Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 172.29.6.14
Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
Internet address is 172.29.6.9/30, Area 2
Process ID 50, Router ID 209.17.220.2, Network Type POINT-TO-POINT, Cost: 64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:03
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 172.29.6.14
Suppress hello for 0 neighbor(s)
MEDELLIN1#sh ip ospf nei

Neighbor ID Pri State Dead Time Address Interface
172.29.6.14 0 FULL/ - 00:00:30 172.29.6.10 Serial0/0/0
172.29.6.6 0 FULL/ - 00:00:32 172.29.6.2 Serial0/0/1
172.29.6.14 0 FULL/ - 00:00:37 172.29.6.14 Serial0/1/0
MEDELLIN1#
MEDELLIN1#

```



```
MEDELLIN2#sh ip ospf int
```

```
Serial0/0/1 is up, line protocol is up
```

```
Internet address is 172.29.6.2/30, Area 2
```

```
Process ID 50, Router ID 172.29.6.6, Network Type POINT-TO-POINT, Cost: 64  
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
```

```
No designated router on this network
```

```
No backup designated router on this network
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
Hello due in 00:00:09
```

```
Index 1/1, flood queue length 0
```

```
Next 0x0(0)/0x0(0)
```

```
Last flood scan length is 1, maximum is 1
```

```
Last flood scan time is 0 msec, maximum is 0 msec
```

```
Neighbor Count is 1 , Adjacent neighbor count is 1
```

```
Adjacent with neighbor 209.17.220.2
```

```
Suppress hello for 0 neighbor(s)
```

```
Serial0/0/0 is up, line protocol is up
```

```
Internet address is 172.29.6.6/30, Area 2
```

```
Process ID 50, Router ID 172.29.6.6, Network Type POINT-TO-POINT, Cost: 64  
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
```

```
No designated router on this network
```

```
No backup designated router on this network
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
Hello due in 00:00:03
```

```
Index 2/2, flood queue length 0
```

```
Next 0x0(0)/0x0(0)
```

```
Last flood scan length is 1, maximum is 1
```

```
Last flood scan time is 0 msec, maximum is 0 msec
```

```
Neighbor Count is 1 , Adjacent neighbor count is 1
```

```
Adjacent with neighbor 172.29.6.14
```

```
Suppress hello for 0 neighbor(s)
```

```
GigabitEthernet0/1 is up, line protocol is up
```

```
Internet address is 172.29.4.1/25, Area 2
```

```
Process ID 50, Router ID 172.29.6.6, Network Type BROADCAST, Cost: 1  
Transmit Delay is 1 sec, State WAITING, Priority 1
```

No designated router on this network  
No backup designated router on this network  
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5  
No Hellos (Passive interface)  
Index 3/3, flood queue length 0  
Next 0x0(0)/0x0(0)  
Last flood scan length is 1, maximum is 1  
Last flood scan time is 0 msec, maximum is 0 msec  
Neighbor Count is 0, Adjacent neighbor count is 0  
Suppress hello for 0 neighbor(s)  
MEDELLIN2#sh ip ospf nei

```
Neighbor ID Pri State Dead Time Address Interface  
172.29.6.14 0 FULL/ - 00:00:37 172.29.6.5 Serial0/0/0  
209.17.220.2 0 FULL/ - 00:00:34 172.29.6.1 Serial0/0/1  
MEDELLIN2#
```

```
MEDELLIN3#sh ip ospf int
```

```
Serial0/1/0 is up, line protocol is up
```

Internet address is 172.29.6.14/30, Area 2  
Process ID 50, Router ID 172.29.6.14, Network Type POINT-TO-POINT, Cost: 64 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0  
No designated router on this network  
No backup designated router on this network  
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:05  
Index 1/1, flood  
queue length 0  
Next  
0x0(0)/0x0(0)  
Last flood scan length is 1, maximum is 1  
Last flood scan time is 0 msec,  
maximum is 0 msec Neighbor Count  
is 1 , Adjacent neighbor count is 1  
Adjacent with neighbor  
209.17.220.2  
Suppress hello for 0  
neighbor(s) Serial0/0/1 is  
up, line protocol is up  
Internet address is  
172.29.6.10/30, Area 2  
Process ID 50, Router ID 172.29.6.14, Network Type POINT-TO-POINT, Cost: 64 Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0  
No designated router on this network  
No backup designated router on this network  
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5 Hello due in 00:00:08  
Index 2/2, flood  
queue length 0  
Next  
0x0(0)/0x0(0)  
Last flood scan length is 1, maximum is 1  
Last flood scan time is 0 msec,  
maximum is 0 msec Neighbor Count

is 1 , Adjacent neighbor count is 1  
Adjacent with neighbor  
209.17.220.2

Suppress hello for 0  
neighbor(s) Serial0/0/0 is  
up, line protocol is up  
Internet address is  
172.29.6.5/30, Area 2

Process ID 50, Router ID 172.29.6.14, Network Type POINT-TO-  
POINT, Cost: 64 Transmit Delay is 1 sec, State POINT-TO-POINT,  
Priority 0

No designated router on this network

No backup designated router on this network

Timer intervals configured, Hello 10, Dead 40, Wait  
40, Retransmit 5 Hello due in 00:00:00

Index 3/3, flood  
queue length 0  
Next  
0x0(0)/0x0(0)

Last flood scan length is 1, maximum is 1

Last flood scan time is 0 msec,  
maximum is 0 msec Neighbor Count  
is 1 , Adjacent neighbor count is 1  
Adjacent with neighbor 172.29.6.6

Suppress hello for 0  
neighbor(s) MEDELLIN3#sh  
ip ospf nei

Neighbor ID Pri State Dead Time  
Address Interface 172.29.6.6 0 FULL/  
- 00:00:39 172.29.6.6 Serial0/0/0  
209.17.220.2 0 FULL/ - 00:00:32 172.29.6.9 Serial0/0/1  
209.17.220.2 0 FULL/ - 00:00:37  
172.29.6.13 Serial0/1/0 MEDELLIN3#

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.

```
MEDELLIN3#sh ip ospf database
OSPF Router with ID (172.29.6.14)
```

```
(Process ID 50) Router Link States (Area
2)
```

```
Link ID ADV Router Age Seq#
Checksum Link count 172.29.6.14
172.29.6.14 1781 0x80000007
0x002b38 6
209.17.220.2 209.17.220.2 1057 0x8000000c 0x00bca9 6
172.29.6.6 172.29.6.6 416 0x80000007 0x0072bf 5
```

```
Type-5 AS External Link States
```

```
Link ID ADV Router Age Seq#
Checksum Tag 0.0.0.0
209.17.220.2 1057 0x80000002
0x001cf3 1 MEDELLIN3#
```

```
MEDELLIN2#sh ip ospf database
OSPF Router with ID (172.29.6.6)
```

```
(Process ID 50) Router Link States (Area
2)
```

```
Link ID ADV Router Age Seq#
Checksum Link count 172.29.6.6
172.29.6.6 435 0x80000007 0x0072bf 5
172.29.6.14 172.29.6.14 1801 0x80000007 0x002b38 6
209.17.220.2 209.17.220.2 1077 0x8000000c 0x00bca9 6
```

Type-5 AS External Link States

```
Link ID ADV Router Age Seq#  
Checksum      Tag      0.0.0.0  
209.17.220.2 1077 0x80000002  
0x001cf3 1 MEDELLIN2#
```

MEDELLIN1#sh ip ospf database

OSPF Router with ID (209.17.220.2)

(Process ID 50) Router Link States

(Area 2)

```
Link ID ADV Router Age Seq# Checksum  
Link count 209.17.220.2 209.17.220.2 1090  
0x8000000c 0x00bca9 6
```

172.29.6.6 172.29 6.6 449 0x80000007 0x0072bf 5

172.29.6.14 172.29 6.14 14 0x80000008 0x002939 6

Type-5 AS External Link States

```
Link ID ADV Router Age Seq#  
Checksum      Tag      0.0.0.0  
209.17.220.2 1090 0x80000002  
0x001cf3 1 MEDELLIN1#
```

BOGOTA1#sh ip ospf data

OSPF Router with ID (209.17.220.6)

(Process ID 100) Router Link States

(Area 1)

```
Link ID ADV Router Age Seq#  
Checksum Link count 172.29.3.13  
172.29.3.13 1628 0x8000000d  
0x00304a 6
```

209.17.220.6 209.17 220.6 1146 0x80000017 0x00d89f 6

172.29.3.14 172.29 3.14 1146 0x80000009 0x00bfd5 5

Type-5 AS External Link States

```
Link ID ADV Router Age Seq#  
Checksum Tag 0.0.0.0 209.17.220.6  
1296 0x80000002 0x000408 1  
BOGOTA1#
```

BOGOTA2#sh ip ospf data

OSPF Router with ID (172.29.3.13)

(Process ID 100) Router Link States

(Area 1)

```
Link ID ADV Router Age Seq#  
Checksum Link count 172.29.3.13  
172.29.3.13 1643 0x8000000d  
0x00304a 6  
172.29.3.14 172.29.3.14 1161 0x80000009 0x00bfd5 5  
209.17.220.6 209.17.220.6 1161 0x80000017 0x00d89f 6
```

Type-5 AS External Link States

```
Link ID ADV Router Age Seq#  
Checksum Tag 0.0.0.0 209.17.220.6  
1312 0x80000002 0x000408 1  
BOGOTA2#
```

BOGOTA3#sh ip ospf data

OSPF Router with ID (172.29.3.14)

(Process ID 100) Router Link States

(Area 1)

```
Link ID ADV Router Age Seq#  
Checksum Link count 172.29.3.13  
172.29.3.13 1655 0x8000000d  
0x00304a 6  
172.29.3.14 172.29.3.14 1172 0x80000009 0x00bfd5 5
```

```
209.17.220.6 209.17.220.6 1172 0x80000017 0x00d89f 6
```

#### Type-5 AS External Link States

```
Link ID ADV Router Age Seq#  
Checksum Tag 0.0.0.0 209.17.220.6  
1323 0x80000002 0x000408 1  
BOGOTA3#
```

- En estos pasos se utiliza comandos `sh ip ospf database`, este realiza la consulta a la base de datos de los routers mostrando las configuraciones, restricciones que tiene los routers de los unos a los otros.



## Parte 5: Configurar encapsulamiento y autenticación PPP.

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

```
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username
MEDELLIN1 pas
```

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

```
MEDELLIN1(config)#username ISP
secret cisco 2 MEDELLIN1(config)#
```

```
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1
password 0 cisco MEDELLIN1(config-if)#
```

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

```
MEDEN1(config-if)# interface Serial0/0/0
ip address 209.17.220.1 255.255.255.252
encapsulation ppp
```

```
ppp authentication pap
```

```
ISP(config-if)#ppp pap sent-username ISP password 0 cisco ISP(config-if)#
```

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

El enlace Bogotá1 con ISP se debe configurar con autenticación CHAP. BOGOTA1(config)#username ISP

```
secret cisco
```

```
BOGOTA1(config)#int
Serial0/0/0
BOGOTA1(config-if)#en
BOGOTA1(config-
if)#encapsulation ppp
BOGOTA1(config-if)#pp
```

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

```
BOGOTA1(config-if)#ppp au
BOGOTA1(config-if)#ppp
authentication          ch
BOGOTA1(config-if)#ppp
authentication          chap
BOGOTA1(config-if)#
```

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

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

```
BOGOTA1(config-if)#
```

```
ISP(config)#username BOGOTA1 secret cisco
```

```
ISP(config)#int interface Serial0/0/1
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
ISP(config)#interface Serial0/0/1
```

```
ISP(config-if)#enc
```

```
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 ISP(config-if)#ppp chap sen
```

```
ISP(config-if)#ppp au
```

```
ISP(config-if)#ppp authentication cha ISP(config-if)#ppp authentication chap
```

```
ISP(config-if)#
```

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

En este paso nos piden configurar el encapsulamiento ppp, esto nos

Permite levantar la interfaz y verificar la negociacion, establece conexion

Con el enlace para medellin1y la ISP, pare como pide que la ISP solicite autenticacion de PAP, las interfases tendran protocolos de autenticacion diferente y los paquetes se descartaran por lo que el router pone en abajo

la intefaz

## 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.

Figura 13. Ping a 172.29.6.6 1

```
BOGOTA2#ping 172.29.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.6, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)

BOGOTA2#
```

- 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)#ip access-list standard 1
MEDELLIN1(config-std-nacl)#per
MEDELLIN1(config-std-nacl)#permit 172.29.4.0 0.0.3.255
MEDELLIN1(config-std-nacl)#^Z
MEDELLIN1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
MEDELLIN1#
MEDELLIN1#
MEDELLIN1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#ip na
MEDELLIN1(config)#ip nat
MEDELLIN1(config)#ip nat st
MEDELLIN1(config)#ip nat ? inside Inside address translation
outside Outside address translation pool Define pool of addresses
MEDELLIN1(config)#ip nat in
  MEDELLIN1(config)#ip nat inside so
MEDELLIN1(config)#ip nat inside source li
MEDELLIN1(config)#ip nat inside source list 1 ? interface Specify interface for
global address pool Name pool of global addresses
  MEDELLIN1(config)#ip nat inside source list 1 in
MEDELLIN1(config)#ip nat inside source list 1 interface Serial0/1/1 ov
MEDELLIN1(config)#ip nat inside source list 1 interface Serial0/1/1 overload
MEDELLIN1(config)#int Serial0/0/0
MEDELLIN1(config-if)#ip nat in
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int Serial0/0/1
MEDELLIN1(config-if)#ip nat inside

MEDELLIN1(config-if)#int Serial0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#int Serial0/1/1
MEDELLIN1(config-if)#ip nat o
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#
```

Figura 14. Ip nat translations 1 1

```
MEDELLINI#sh ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
icmp 209.17.220.2:1     172.29.6.2:1     209.17.220.1:1   209.17.220.1:1
icmp 209.17.220.2:2     172.29.6.2:2     209.17.220.1:2   209.17.220.1:2
icmp 209.17.220.2:3     172.29.6.2:3     209.17.220.1:3   209.17.220.1:3
icmp 209.17.220.2:4     172.29.6.2:4     209.17.220.1:4   209.17.220.1:4
icmp 209.17.220.2:5     172.29.6.2:5     209.17.220.1:5   209.17.220.1:5
MEDELLINI#
```

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)#ip access-list standard 1
BOGOTA1(config-std-nacl)#permi
BOGOTA1(config-std-nacl)#permit 172.29.0.0 0.0.3.255
BOGOTA1(config-std-nacl)#exi
BOGOTA1(config)#
BOGOTA1(config)#
BOGOTA1(config)#ip na
BOGOTA1(config)#ip nat
BOGOTA1(config)#ip nat in
BOGOTA1(config)#ip nat inside so
BOGOTA1(config)#ip nat inside source li
BOGOTA1(config)#ip nat inside source list 1 in
BOGOTA1(config)#ip nat inside source list 1 interface Serial0/0/0 ov
BOGOTA1(config)#ip nat inside source list 1 interface Serial0/0/0 overload
BOGOTA1(config)#int Serial0/0/1
```

```

BOGOTA1(config-if)#ip nat i
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int Serial0/1/0
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int Serial0/1/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int Serial0/0/0
BOGOTA1(config-if)#ip nat ou
BOGOTA1(config-if)#ip nat outside

BOGOTA1(config-if)#^Z
BOGOTA1#

```

Figura 15. Ip nat translationsBOGOTA1 1 1

```

BOGOTA1#sh ip nat translations
Pro  Inside global      Inside local          Outside local          Outside global
icmp 209.17.220.6:11    172.29.3.2:11        209.17.220.5:11      209.17.220.5:11
icmp 209.17.220.6:12    172.29.3.2:12        209.17.220.5:12      209.17.220.5:12
icmp 209.17.220.6:13    172.29.3.2:13        209.17.220.5:13      209.17.220.5:13
icmp 209.17.220.6:14    172.29.3.2:14        209.17.220.5:14      209.17.220.5:14
icmp 209.17.220.6:15    172.29.3.2:15        209.17.220.5:15      209.17.220.5:15
BOGOTA1#

```

En este paso nos piden revisar conexiones mediante el comando ping, esto para verificar que ningún Router distinto a bogota1, medellin1 y la ISP, establezca conexión entre ellos, se configuran las NAT para las sucursales según indicaciones y se pueden observar la data de entrada y salida.

## Parte 7: Configuración del servicio DHCP.

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

```
MEDELLIN2(config)#ip dhcp excluded-address
172.29.4.1 172.29.4.5
MEDELLIN2(config)#ip de
MEDELLIN2(config)#ip
dh
MEDELLIN2(config)#ip
dhcp po
MEDELLIN2(config)#ip
dhcp pool LAN50
MEDELLIN2(dhcp-
config)#net
MEDELLIN2(dhcp-config)#network 172.29.4.0
255.255.255.128
MEDELLIN2(dhcp-config)#def
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#ip dhcp excluded-address
172.29.4.129 172.29.4.134
MEDELLIN2(config)#ip dhcp pool LAN40
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-
router 172.29.4.129
MEDELLIN2(dhcp-config)#
```

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

```
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip hel
MEDELLIN3(config-if)#ip helpe
```



```
MEDELLIN3(config-if)#ip helper-address 172.29.6.6
MEDELLIN3(config-if)#^Z
MEDELLIN3#
%SYS-5-CONFIG_I: Configured from console by console

MEDELLIN3#
MEDELLIN3(config-router)#network 172.29.4.128 0.0.0.128 area 2
```

Figura 16. fastEthernet0 172.29.4.155 1

FastEthernet0	
Port Status	<input checked="" type="checkbox"/> On
Bandwidth	<input type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
Duplex	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
MAC Address	00D0.D3AB.1D3B
IP Configuration	
<input checked="" type="radio"/> DHCP	
<input type="radio"/> Static	
IP Address	172.29.4.155
Subnet Mask	255.255.255.128
IPv6 Configuration	
<input type="radio"/> DHCP	
<input type="radio"/> Auto Config	
<input checked="" type="radio"/> Static	
IPv6 Address	
Link Local Address:	FE80::2D0:D3FF:FEAB:1D3B

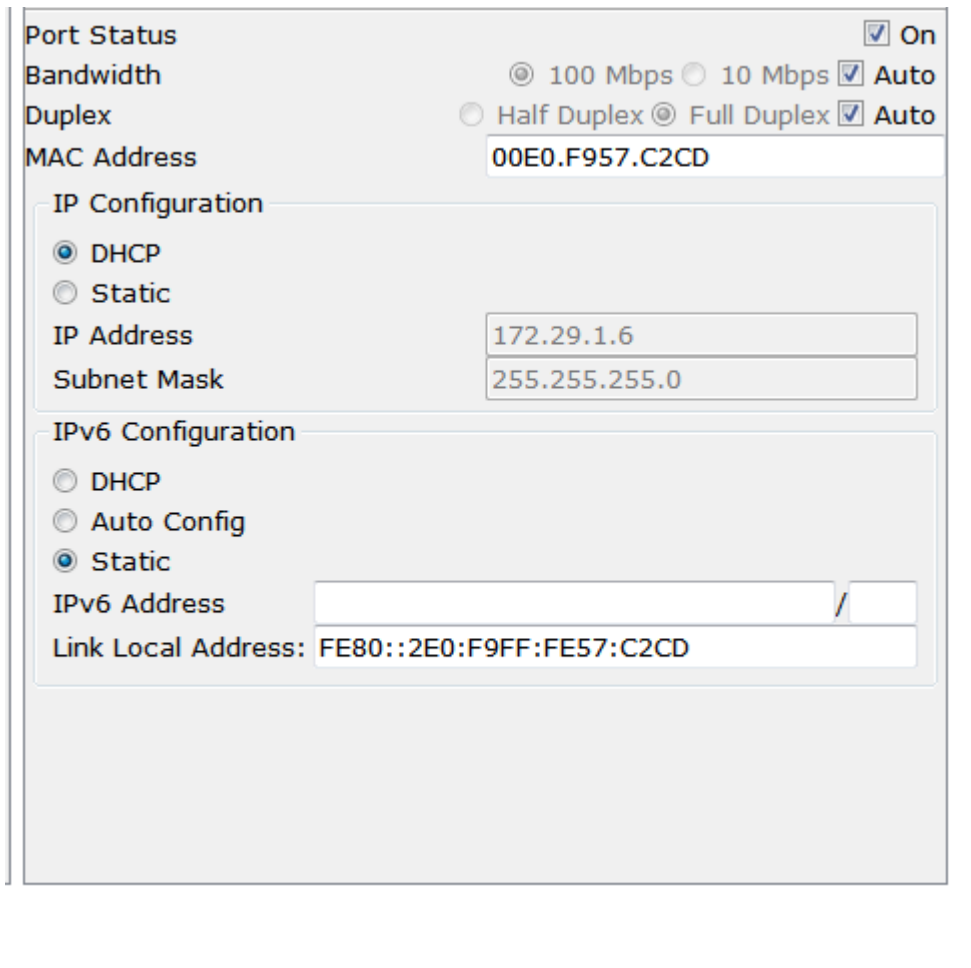
c. Configurar la red Bogotá2 y Bogotá3 donde el router Bogota2 debe ser el servidor DHCP para ambas redes LAN.

```
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOGOTA2(config)#ip dhcp po
BOGOTA2(config)#ip dhcp pool LAN150
BOGOTA2(dhcp-config)#net
BOGOTA2(dhcp-config)#network 172.29.0.0 mas
BOGOTA2(dhcp-config)#network 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#def
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#
BOGOTA2(dhcp-config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOGOTA2(config)#ip dhcp pool LAN200
BOGOTA2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#
```

**d. Configure el router Bogotá3 para que habilite el paso de los mensajes Broadcast hacia la IP del router Bogotá2.**

```
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.0.1
BOGOTA3(config-if)#
```

Figura 17. fastEthernet0 172.29.1.6 1



Port Status  On

Bandwidth  100 Mbps  10 Mbps  Auto

Duplex  Half Duplex  Full Duplex  Auto

MAC Address 00E0.F957.C2CD

IP Configuration

DHCP

Static

IP Address 172.29.1.6

Subnet Mask 255.255.255.0

IPv6 Configuration

DHCP

Auto Config

Static

IPv6 Address /

Link Local Address: FE80::2E0:F9FF:FE57:C2CD

Se realizan las configuraciones de los routers medellin2 y medellin3, bogota2 y bogota3, donde el medellin2 y Bogotá 2 deben quedar como servidor DHCP para las redes LAN, lo que indica que siempre que el medellin3 y bogota3 se conecten con medellin2 y bogota2 lo van hacer bajo la dirección asignada la cual se guarda en la base de datos junto con la MAC, estas direcciones no estarán disponibles si no para estos routers.

## CONCLUSIONES

Dada la red configurada en el escenario 1, se puede deducir que existe una topología de acceso a internet desde una red LAN interna aplicándose un nateo para poder conectar a los servicios externos y viceversa, ya que el servidor externo se le es posible conectar con el servidor interno web según las pruebas indicadas, por la facilidad de la comunicación entre los routers de la WAN se puede establecer un protocolo de enrutamiento rip, donde se especifica la no auto-sumarización dado que existen redes del segmento 172.16.0.0 que puede tornarse ambigua para el router R2, he ahí la importancia del comando. Adicional se establece la configuración de subinterfaces donde se observa como el router R1 es el router Gateway en la conexión LAN- WAN, se verifica el establecimiento de los protocolos DHCP, para el protocolo NTP, no es posible realizar la configuración sobre el router R2 como master (por la versión del IOS aplicado en el laboratorio), pero se establece el servidor externo como un sincronizador y se observan las configuraciones del mismo, y sincronización exitosa.

En el segundo ejercicio vemos como se abarca todo el tema a profundidad de un enrutamiento OSPF, con interáreas en este panorama probamos la redundancia de contar con un respaldo en la ruta default para los routers de BOGOTA2 y 3 / MEDELLIN2 y 3, adicional probamos y configuramos el encapsulado en los enlaces seriales por PPP tanto con cifrado como en texto claro, viendo sus principales diferencias.

Se realizó la configuración del DHCP-Relay donde observe algunas fallas en la configuración del enrutamiento OSPF en el router MEDELLIN3 dado que no contaba con la propagación del segmento LAN, y por ende no era posible establecer la solicitud de broadcas

## BIBLIOGRAFÍA

CISCO. (2017). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO. (2017). Capa de Aplicación. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1>

CISCO. (2017). Capa de Transporte. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>

CISCO. (2017). Como borrar los datos de la vlan en switches cisco. Recuperado de [https://community.spiceworks.com/how\\_to/47462-erase-vlan-data-on-cisco-switches](https://community.spiceworks.com/how_to/47462-erase-vlan-data-on-cisco-switches)

CISCO. (2017). SubNetting. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>