

CURSO DE PROFUNDIZACION CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN – WAN)

JHON FRANKLIN DOMINGUEZ BONILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
BARRANCABERMEJA
15-05-2020

CURSO DE PROFUNDIZACION CISCO (DISEÑO E IMPLEMENTACIÓN DE
SOLUCIONES INTEGRADAS LAN – WAN)

JHON FRANKLIN DOMINGUEZ BONILLA

TUTOR:
JUAN CARLOS VESGA
INGENIERO.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
BARRANCABERMEJA
15-05-2020.

CONTENIDO

	Pág.
1. INTRODUCCION	4
1.1 Prueba de habilidades practicas CCNA	
2. OBJETIVOS GENERALES	5
3. OBJETIVOS ESPECIFICOS	5
4. LISTA DE TABLAS	6-7
5. LISTA DE FIGURAS	8
6. CONLCUCIONES	63
7. BIBLIOGRAFIA, WEBGRAFICA	64

INTRODUCCION

En el trabajo que se presenta se desarrolla 2 topologías de acuerdo a unas especificaciones claras que se nos entrega y gracias a los cuales profundizaremos en los temas tratados a lo largo del diplomado de CCNA.

El presente trabajo tal como lo vamos a ver se desarrolla desde cero, vamos a ver cada uno de los dispositivos y sus interfaces con el fin de poder adecuar cada uno de ellos a nuestras necesidades. Las guías son claras y nos muestran exactamente qué es lo que necesitamos de cada una de las 2 topologías. El desarrollo y la implementación lo hare paso a paso y documentando cada uno de ellos con el fin de ser lo más explicativos posible y de esta manera poder tomar las medidas necesarias de acuerdo a las necesidades que setiene.

Dentro de la guía se nos entregan una serie de necesidades bien claras, y cada una de ellas la debemos satisfacer indicando el proceso que se hace para poderlo culminar, debemos tener en cuenta que en cada caso se hace una proyección con el fin de poder ampliar nuestra red hacia futuro.

OBJETIVOS GENERAL

- Realizar el diseño, montaje de cada una de las 2 redes que se nos solicita dentro de la guía para la prueba de habilidades.

OBJETIVOS ESPECIFICOS

- Debemos aplicar los conocimientos adquiridos a lo largo de los 2 módulos de CCNA vistos.
- Aplicar VLSM en cada uno de los diseños.
- Profundizar en la aplicación y el funcionamiento de los protocolos de enrutamiento.
- Realizar el montaje de las topologías dentro del Simulador de Packet-Tracer herramienta que va a favorecer nuestro proceso de aprendizaje.
- Debemos realizar la configuración de cada uno de los dispositivos que hará parte de las redes aplicando los diferentes comandos para tal fin.
- Algo supremamente importante a la hora de diseñar una red es la documentación que debemos hacer de cada una de ellas, esto lo haremos con el fin de poder realizar las correcciones de una manera más sencilla.
- Siempre realizaremos la verificación de cada uno de los pasos desarrollados, esto con el fin de observar el correcto funcionamiento de lo elaborado.

LISTA DE TABLAS

	Pág.
Tabla 1. Dispositivos	9
Tabla 2. Parámetros básicos	11
Tabla 3. Configurar R1	12
Tabla 4. Configurar R2	13
Tabla 5. Configurar R3	15
Tabla 6. Configurar S1	16
Tabla 7. Configurar S3	17
Tabla 8. Verificar la conectividad de la red	17
Tabla 9. Configurar la seguridad del switch, las VLAN y el routing entre VLAN (Configurar S1)	18
Tabla 10. Configurar la seguridad del switch, las VLAN y el routing entre VLAN (Configurar S3)	19
Tabla 11. Configurar la seguridad del switch, las VLAN y el routing entre VLAN (Configurar R1)	20
Tabla 12. Verificar la conectividad de la red	21
Tabla 13. Configurar RIPv2 en el R1	22
Tabla 14. Configurar RIPv2 en el R2	23
Tabla 15. Configurar RIPv3 en el R2	24
Tabla 16. Verificar la información de RIP	25
Tabla 17. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23	26
Tabla 18. Configurar la NAT estática y dinámica en el R2	27

Tabla 19. Verificar el protocolo DHCP y la NAT estática	28
Tabla 20. Configurar NTP	30
Tabla 21. Restringir el acceso a las líneas VTY en el R2	31
Tabla 22. Introducir el comando de CLI	32
Tabla 23. Deshabilitar la propagación del protocolo RIP	35
Tabla 24. Direccionamiento	39-44
Tabla 25. Configuración del enrutamiento	45
Tabla 26. Deshabilitar la propagación del protocolo RIP	49
Tabla 27. Configurar encapsulamiento y autenticación PPP	53
Tabla 28. configuración de los ROUTERS	56

LISTA DE FIGURAS

	Pág.
FIGURA 1: Topología	9
FIGURA 2: Configuración de internet	12
FIGURA 3: Conectividad de red	21
FIGURA 4: Configurar RIPv2 en el R1	22
FIGURA 5: Configurar RIPv2 en el R2	23
FIGURA 6: Configurar RIPv3 en el R2	24
FIGURA 7: Verificar la información de RIP	25
FIGURA 8: Implementar DHCP y NAT para IPv4	27
FIGURA 9: Verificar el protocolo DHCP y la NAT estática	30
FIGURA 10: Introducir el comando de CLI	32
FIGURA 11: Topología de red	44
FIGURA 12: Tipo de Interfaces	37-38
FIGURA 13: Enrutamiento	46/48
FIGURA 14: Verificación de protocolo RIP	50-52
FIGURA 15: Configuración de NAT	54
FIGURA 16: Verificación de configuración de Routers	56

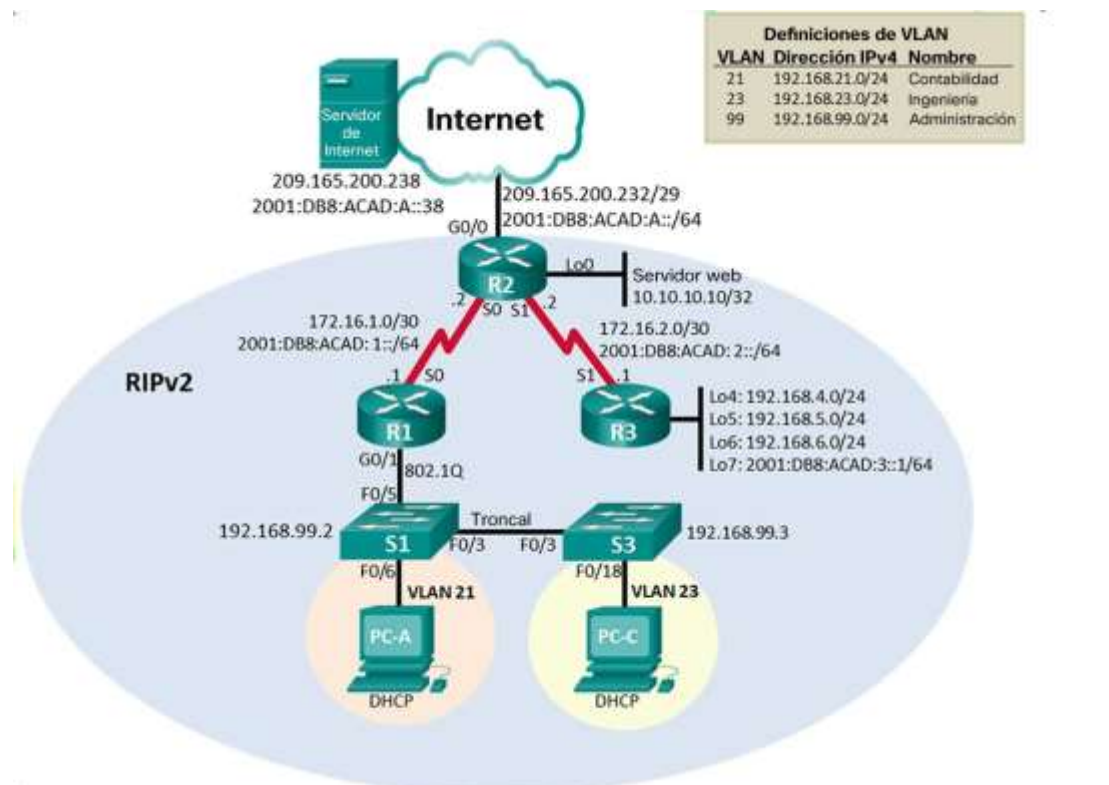
Descripción de escenarios propuestos para la prueba de habilidades

Escenario 1

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

Topología

Figura 1. topología



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. Dispositivos

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Para eliminar la configuración en los dispositivos debemos aplicar el comando: “erase startup-config”
Volver a cargar todos los routers	En este caso debemos aplicar el siguiente comando: “reload”
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Para poder eliminar la totalidad de la configuración debemos aplicar estos 2 comandos en los switches: <ul style="list-style-type: none">- erase startup-config- delete vlan.dat
Volver a cargar ambos switches	Igualmente que en los routers en este caso aplicamos el comando: “Reload”
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Para mirar en la memoria debemos aplicar el siguiente comando: “show flash”

Parte 2: Configurar los parámetros básicos de los dispositivos

Paso 1: Configurar la computadora de Internet

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

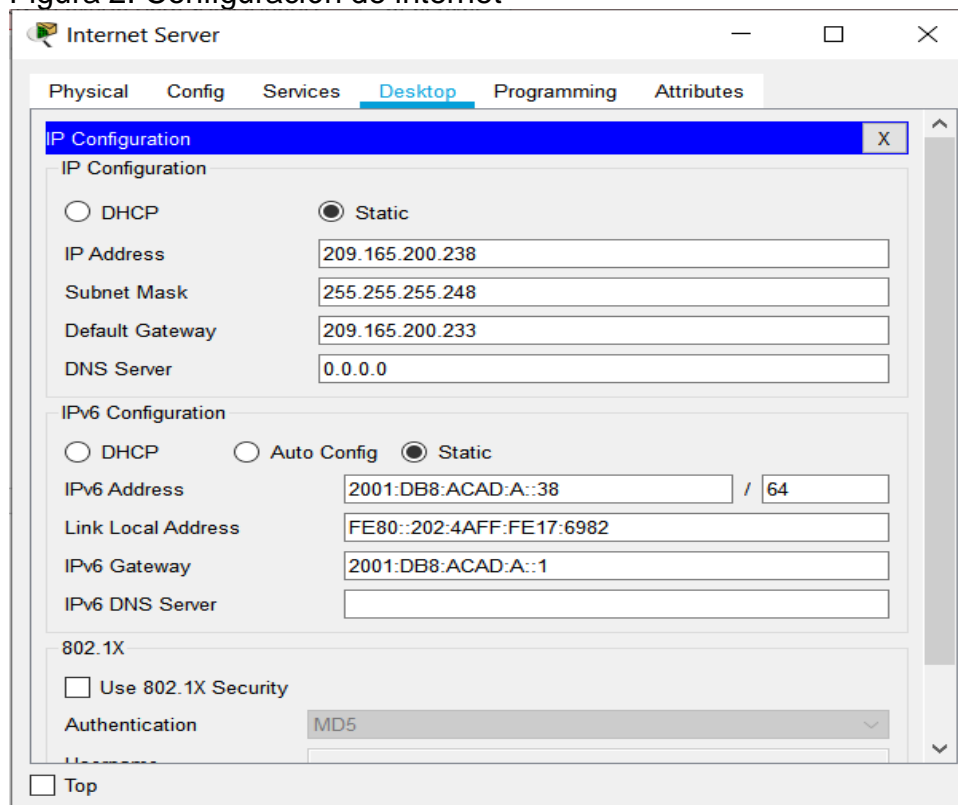
Recordemos que esta parte la debemos configurar de acuerdo a la información que nos suministra en la TOPOLOGÍA:

Tabla 2. Parámetros básicos

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.230
Máscara de subred para IPv4	255.255.255.248
Gateway predeterminado	209.165.200.225
Dirección IPv6/subred	2001:DB8:ACAD:2::30/64
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.

Figura 2. Configuración de internet



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	Para desactivar la búsqueda debemos aplicar el siguiente comando: “ No ip domain lookup”
Nombre del router	R1
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco
Cifrar las contraseñas de texto no cifrado	“ Service password-encryption “
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones Establecer la frecuencia de reloj en 128000 Activar la interfaz
Rutas predeterminadas	Configurar una ruta IPv4 predeterminada de S0/0/0 Configurar una ruta IPv6 predeterminada de S0/0/0

Nota: Todavía no configure G0/1.

Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

Tabla 4. Configurar R2

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	" No ip domain lookup "
Nombre del router	R2
Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Para activar este servicio debemos aplicar el siguiente comando dentro del dispositivo: " Service password-encryption "
Habilitar el servidor HTTP	En este caso se aplica el comando: "ip http server"
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/0	Establezca la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz

Interfaz S0/0/1	<p>Establecer la descripción</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.</p> <p>Establecer la frecuencia de reloj en 128000.</p> <p>Activar la interfaz</p>
Interfaz G0/0 (simulación de Internet)	<p>Establecer la descripción.</p> <p>Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.</p> <p>Establezca la dirección IPv6. Utilizar la primera dirección disponible en la subred.</p> <p>Activar la interfaz</p>
Interfaz loopback 0 (servidor web simulado)	<p>Establecer la descripción.</p> <p>Establezca la dirección IPv4.</p>
Ruta predeterminada	<p>Configure una ruta IPv4 predeterminada de G0/0.</p> <p>Configure una ruta IPv6 predeterminada de G0/0.</p>

Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Tabla 5. Configurar R3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	<p>Debemos aplicar el siguiente comando:</p> <p>“No ip domain lookup”</p>
Nombre del router	R3

Contraseña de exec privilegiado cifrada	class
Contraseña de acceso a la consola	cisco
Contraseña de acceso Telnet	cisco
Cifrar las contraseñas de texto no cifrado	Debemos aplicar el siguiente comando: "Service password-encryption"
Mensaje MOTD	Se prohíbe el acceso no autorizado.
Interfaz S0/0/1	Establecer la descripción Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred. Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. Activar la interfaz
Interfaz loopback 4	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 5	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 6	Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred.
Interfaz loopback 7	Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.
Rutas predeterminadas	

Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 6. Configurar S1

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

Paso 6: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 7. Configurar S3

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	En este caso aplicamos el comando: No ip domain lookup
Nombre del switch	S3
Contraseña de exec privilegiado cifrada	Class
Contraseña de acceso a la consola	Cisco
Contraseña de acceso Telnet	Cisco

Cifrar las contraseñas de texto no cifrado	En este caso debemos aplicar el comando: Service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado.

Paso 7: Verificar la conectividad de la red

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

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

Tabla 8. Verificar la conectividad de la red

Desde	A	Dirección IP	Resultados de ping
R1	R2, S0/0/0	172.16.12.2	Exitoso
R2	R3, S0/0/1	172.16.23.2	Exitoso
PC de Internet	Gateway predeterminado	209.165.200.225	Exitoso

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

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

Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Tabla 9. Configurar la seguridad del switch, las VLAN y el routing entre VLAN (Configurar S1)

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear y nombrar cada una de las VLAN que se indican
Asignar la dirección IP de administración.	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S1 en el diagrama de topología
Asignar el gateway predeterminado	Asigne la primera dirección IPv4 de la subred como el gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Forzar el enlace troncal en la interfaz F0/5	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/6 a la VLAN 21	Debemos asignar la vlan 21 y darle acceso a las interfaz f0/6 interface F0/6 switchport access vlan 21
Apagar todos los puertos sin usar	Con el fin de no hacer el proceso interfaz por interfaz debemos aplicar el comando RANGE: interface range F0/1-2, F0/4, F0/7-24, G0/1-2 shutdown

Paso 2: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Tabla 10. Configurar la seguridad del switch, las VLAN y el routing entre VLAN (Configurar S3)

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	Utilizar la tabla de equivalencias de VLAN para topología para crear cada una de las VLAN que se indican Dé nombre a cada VLAN.
Asignar la dirección IP de administración	Asigne la dirección IPv4 a la VLAN de administración. Utilizar la dirección IP asignada al S3 en el diagrama de topología
Asignar el gateway predeterminado.	Asignar la primera dirección IP en la subred como gateway predeterminado.
Forzar el enlace troncal en la interfaz F0/3	Utilizar la red VLAN 1 como VLAN nativa
Configurar el resto de los puertos como puertos de acceso	Utilizar el comando interface range
Asignar F0/18 a la VLAN 21	Igualmente que en el caso anterior debemos crear la VLAN y además asignarla a una interfaz: interface F0/18 switchport access vlan 23
Apagar todos los puertos sin usar	En este caso empleamos el comando RANGE junto con SHUTDOWN. interface range F0/1-2, F0/4, F0/6-17, F0/19-24, G0/1-2 shutdown

Paso 3: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 11. Configurar la seguridad del switch, las VLAN y el routing entre VLAN (Configurar R1)

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	Descripción: LAN de Contabilidad Asignar la VLAN 21 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .23 en G0/1	Descripción: LAN de Ingeniería Asignar la VLAN 23 Asignar la primera dirección disponible a esta interfaz
Configurar la subinterfaz 802.1Q .99 en G0/1	Descripción: LAN de Administración Asignar la VLAN 99 Asignar la primera dirección disponible a esta interfaz
Activar la interfaz G0/1	interface g0/1 no shutdown

Paso 4: Verificar la conectividad de la red

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

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

Tabla 12. Verificar la conectividad de la red

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

Figura 3. Conectividad de red

```

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#
    
```

```

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#
    
```

Configurar el protocolo de routing dinámico RIPv2

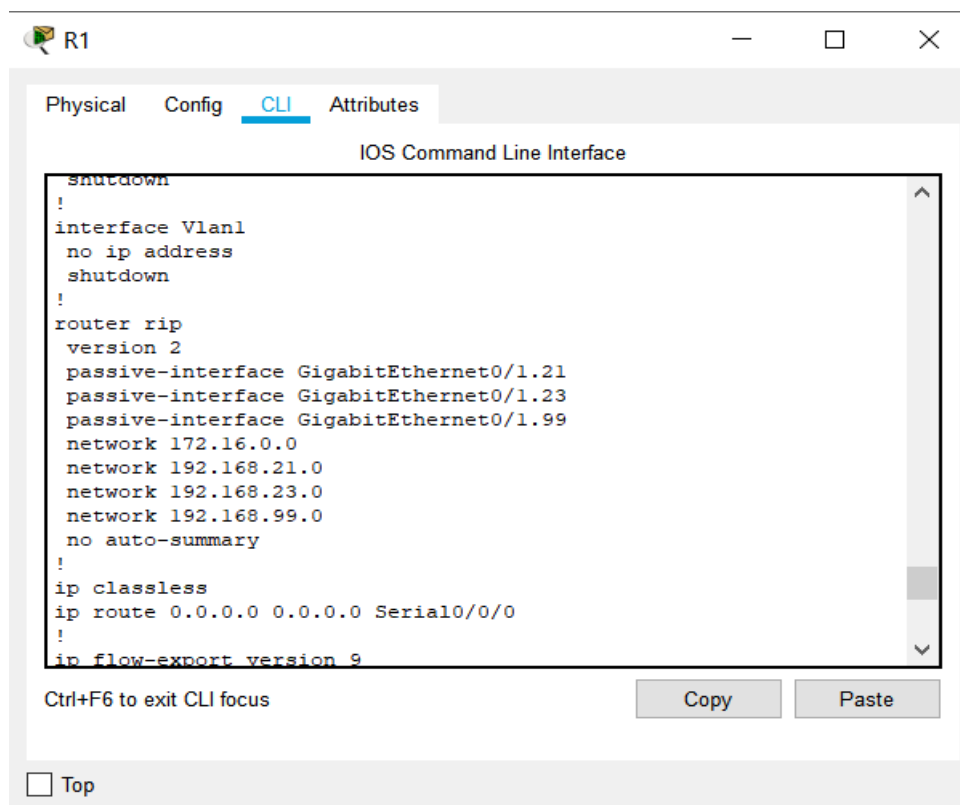
Paso 5: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 13. Configurar RIPv2 en el R1

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router rip version 2
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	passive-interface g0/1.21 passive-interface g0/1.23 passive-interface g0/1.99
Desactive la sumarización automática	no auto-summary

Figura 4. Configurar RIPv2 en el R1



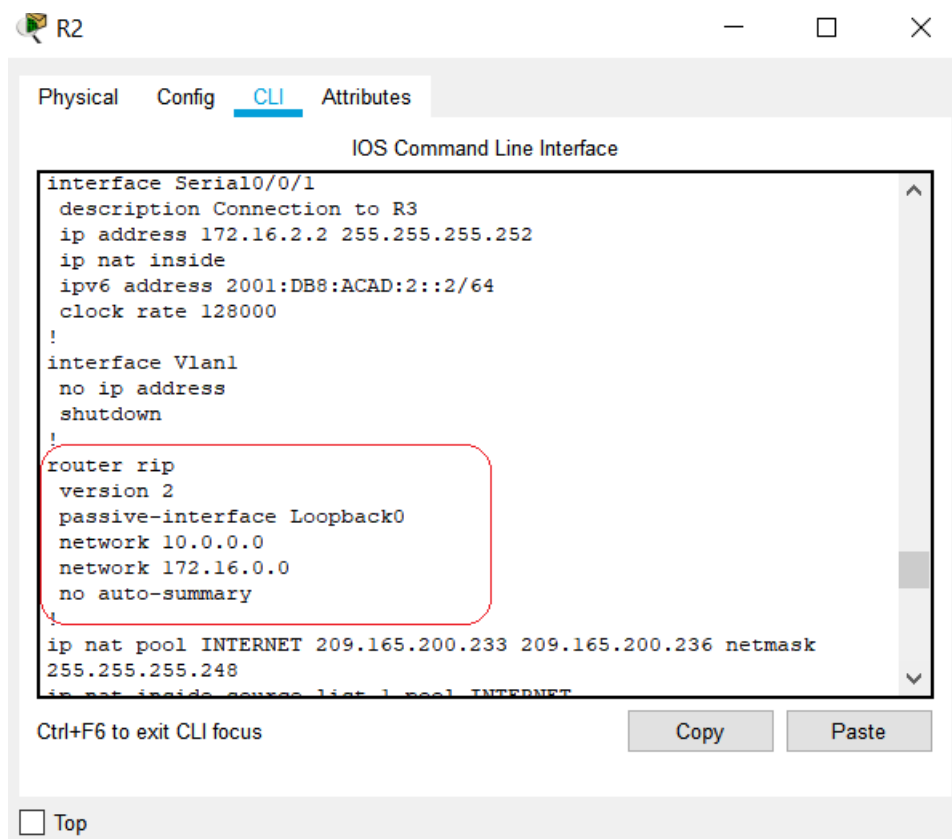
Paso 6: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Tabla 14. Configurar RIPv2 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router rip version 2
Anunciar las redes conectadas directamente	Nota: Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	passive-interface lo0
Desactive la sumarización automática.	no auto-summary

Figura 5. Configurar RIPv2 en el R2



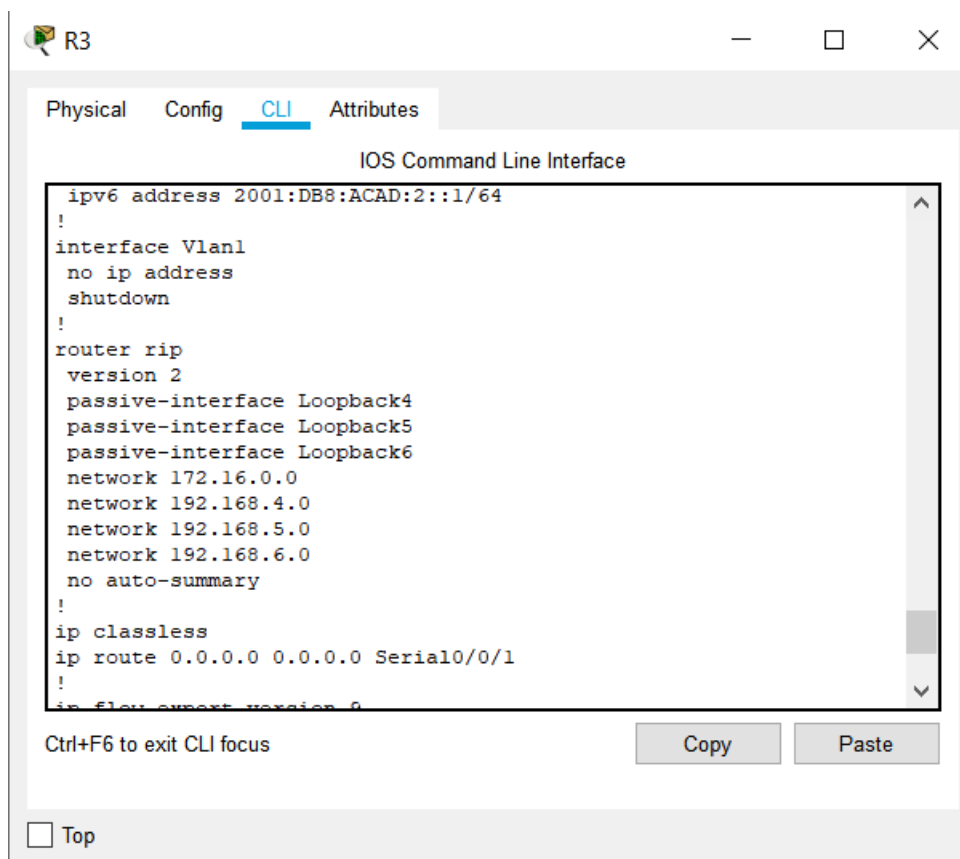
Paso 7: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Tabla 15. Configurar RIPv3 en el R2

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	router rip version 2
Anunciar redes IPv4 conectadas directamente	network 172.16.0.0 network 192.168.4.0 network 192.168.5.0 network 192.168.6.0
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	passive-interface lo4 passive-interface lo5 passive-interface lo6
Desactive la sumarización automática.	no auto-summary

Figura 6. Configurar RIPv3 en el R2



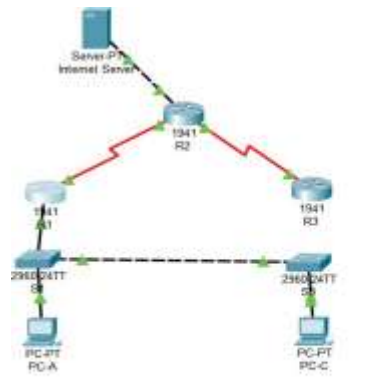
Paso 8: Verificar la información de RIP

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

Tabla 16. Verificar la información de RIP

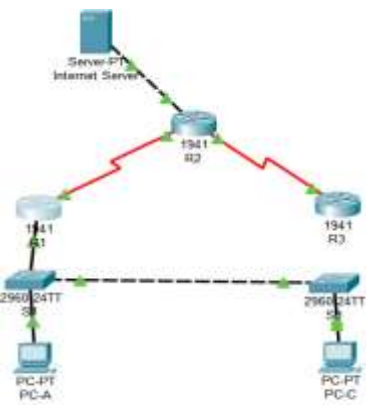
Pregunta	Respuesta
¿Con qué comando se muestran la ID del proceso RIP, la ID del router, las redes de routing y las interfaces pasivas configuradas en un router?	show ip protocols
¿Qué comando muestra solo las rutas RIP?	show ip route rip
¿Qué comando muestra la sección de RIP de la configuración en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

Figura 7. Verificar la información de RIP



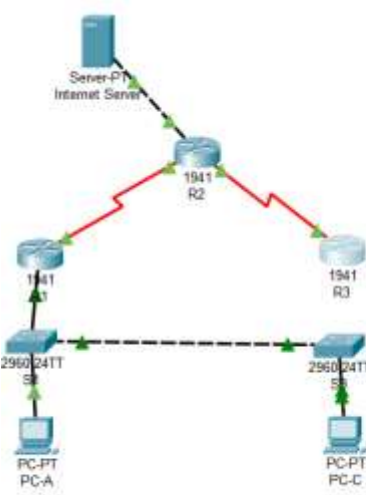
```

R1#show ip route rip
10.0.0.0/32 is subnetted, 1 subnets
R   10.10.10.10 [120/1] via 172.16.1.2, 00:00:20, Serial0/0/0
R   172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R   172.16.2.0/30 [120/2] via 172.16.1.2, 00:00:20, Serial0/0/0
R   192.168.4.0/24 [120/2] via 172.16.1.2, 00:00:20, Serial0/0/0
R   192.168.6.0/24 [120/2] via 172.16.1.2, 00:00:20, Serial0/0/0
R   192.168.8.0/24 [120/2] via 172.16.1.2, 00:00:20, Serial0/0/0
R   192.168.99.0/24 is variably subnetted, 1 subnets, 2 masks
  
```



```

R2#show ip route rip
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
R   192.168.4.0/24 [120/1] via 172.16.2.1, 00:00:04, Serial0/0/1
R   192.168.6.0/24 [120/1] via 172.16.2.1, 00:00:04, Serial0/0/1
R   192.168.8.0/24 [120/1] via 172.16.2.1, 00:00:04, Serial0/0/1
R   192.168.21.0/24 [120/1] via 172.16.1.1, 00:00:04, Serial0/0/0
R   192.168.23.0/24 [120/1] via 172.16.1.1, 00:00:04, Serial0/0/0
R   192.168.99.0/24 [120/1] via 172.16.1.1, 00:00:04, Serial0/0/0
R   209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
  
```



```

R3#show ip route rip
10.0.0.0/32 is subnetted, 1 subnets
R   10.10.10.10 [120/1] via 172.16.2.2, 00:00:23, Serial0/0/1
R   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, 00:00:23, Serial0/0/1
R   192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
R   192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:23, Serial0/0/1
R   192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:23, Serial0/0/1
R   192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:23, Serial0/0/1
  
```

Parte 4: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

Tabla 17. Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21.	Nombre: ACCT Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado
Crear un pool de DHCP para la VLAN 23	Nombre: ENGNR Servidor DNS: 10.10.10.10 Nombre de dominio: ccna-sa.com Establecer el gateway predeterminado

Figura 8. Implementar DHCP y NAT para IPv4

```
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!  
!  
ip dhcp excluded-address 192.168.21.1 192.168.21.20  
ip dhcp excluded-address 192.168.23.1 192.168.23.20  
!
```

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

La configuración del R2 incluye las siguientes tareas:

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

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: webuser Contraseña: cisco12345 Nivel de privilegio: 15
Habilitar el servicio del servidor HTTP	ip http server
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	ip http authentication local
Crear una NAT estática al servidor web.	Dirección global interna: 209.165.200.229
Asignar la interfaz interna y externa para la NAT estática	interface lo0 ip nat inside interface g0/0 ip nat outside
Configurar la NAT dinámica dentro de una ACL privada	Lista de acceso: 1 Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1 Permitir la traducción de un resumen de las redes LAN (loopback) en el R3
Defina el pool de direcciones IP públicas utilizables.	Nombre del conjunto: INTERNET El conjunto de direcciones incluye: 209.165.200.225 – 209.165.200.228
Definir la traducción de NAT dinámica	ip nat inside source list 1 pool INTERNET

Paso 3: Verificar el protocolo DHCP y la NAT estática

Utilice las siguientes tareas para verificar que las configuraciones de DHCP y NAT estática funcionen de forma correcta. Quizá sea necesario

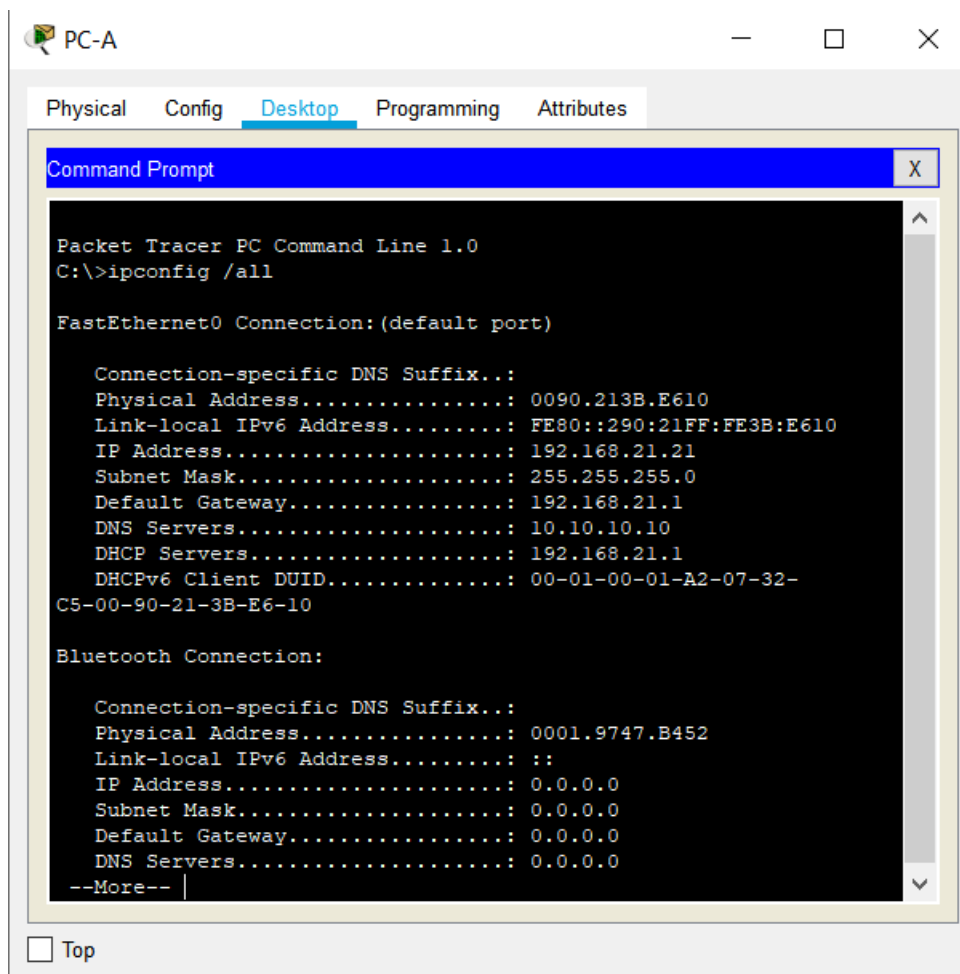
deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

Tabla 19. Verificar el protocolo DHCP y la NAT estática

Prueba	Resultados
<p>Verificar que la PC-A haya adquirido información de IP del servidor de DHCP</p>	<pre>C:\>ipconfig /all FastEthernet0 Connection:(default port) Connection-specific DNS Suffix.: Physical Address.0090.213B.E610 Link-local IPv6 Address.....: FE80::290:21FF:FE3B:E610 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-A2- 07-32-C5-00-90-21-3B-E6-10</pre>
<p>Verificar que la PC-C haya adquirido información de IP del servidor de DHCP</p>	<pre>C:\>ipconfig /all FastEthernet0 Connection:(default port) Connection-specific DNS Suffix.: Physical Address.0004.9A32.A8C5 Link-local IPv6 Address.....: FE80::204:9AFF:FE32:A8C5 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- CE-16-91-9B-00-04-9A-32-A8-C5</pre>

<p>Verificar que la PC-A pueda hacer ping a la PC-C Nota: Quizá sea necesario deshabilitar el firewall de la PC.</p>	<pre>C:\>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=1 ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1 ms TTL=127 Reply from 192.168.23.21: bytes=32 time<1 ms 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 = 1 ms, Average = 0ms</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>El navegador debe mostrar a ventana de inicio de sesión que solicita usuario y contraseña, packet tracer no soporta este procedimiento.</p>

Figura 9. Verificar el protocolo DHCP y la NAT estática



Configurar NTP

Tabla 20. Configurar NTP

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

Verifique la configuración de NTP en R1.	<pre>R1#show ntp associations address ref clock st when poll reach delay offset disp *~172.16.1.2 127.127.1.1 5 2 64 1 4.00 1.00 0.00 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured</pre>
--	---

Parte 5: Configurar y verificar las listas de control de acceso (ACL)

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

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

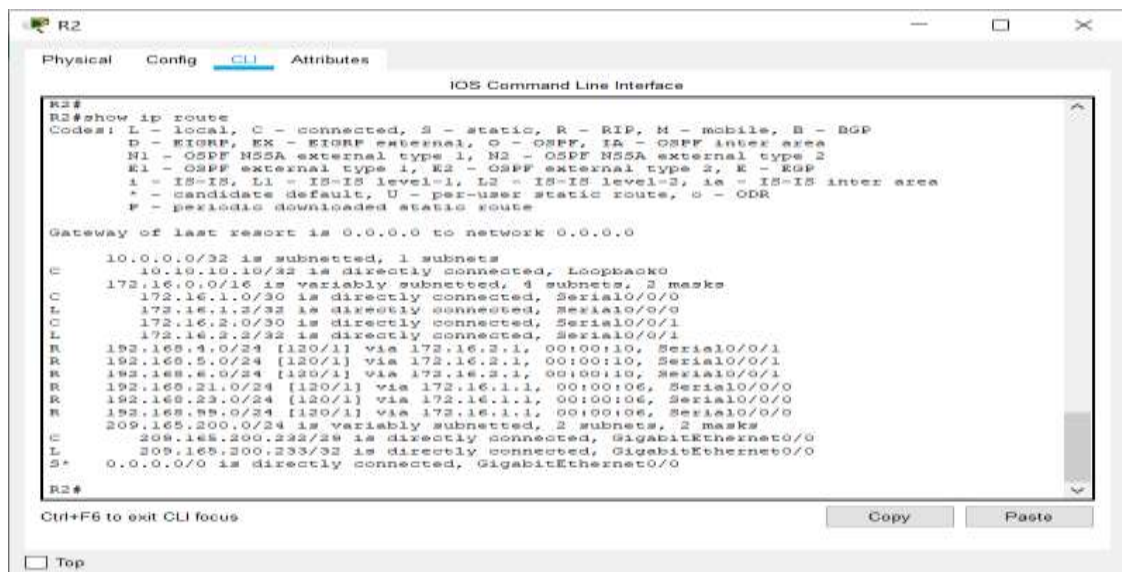
Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión Telnet con R2	Nombre de la ACL: ADMIN-MGT
Aplicar la ACL con nombre a las líneas VTY	line vty 0 4 access-class ADMIN-MGT in
Permitir acceso por Telnet a las líneas de VTY	transport input telnet
Verificar que la ACL funcione como se espera	<pre>R1#telnet 172.16.1.2 Trying 172.16.1.2 ...OpenUnauthorized Access is Prohibited!^ User Access Verification Password: R2>en Password: R2#</pre>

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

Tabla 22. Introducir el comando de CLI

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

Figura 10. : Introducir el comando de CLI



R1

Physical Config CLI Attributes

IOS Command Line Interface

```

R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
       area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

 10.0.0.0/32 is subnetted, 1 subnets
R   10.10.10.10/32 [120/1] via 172.16.1.2, 00:00:12, Serial0/0/0
C   172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
C   172.16.1.0/30 is directly connected, Serial0/0/0
L   172.16.1.1/32 is directly connected, Serial0/0/0
R   172.16.2.0/30 [120/1] via 172.16.1.2, 00:00:12, Serial0/0/0
R   192.168.4.0/24 [120/2] via 172.16.1.2, 00:00:12, Serial0/0/0
R   192.168.5.0/24 [120/2] via 172.16.1.2, 00:00:12, Serial0/0/0
R   192.168.6.0/24 [120/2] via 172.16.1.2, 00:00:12, Serial0/0/0
 192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
L   192.168.21.1/32 is directly connected, GigabitEthernet0/1.21
 192.168.23.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
L   192.168.23.1/32 is directly connected, GigabitEthernet0/1.23
 192.168.99.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.99.0/24 is directly connected, GigabitEthernet0/1.99
L   192.168.99.1/32 is directly connected, GigabitEthernet0/1.99
S*  0.0.0.0/0 is directly connected, Serial0/0/0

```

R1#

Ctrl+F6 to exit CLI focus

Copy Paste

Top

R3

Physical Config CLI Attributes

IOS Command Line Interface

```

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

 10.0.0.0/32 is subnetted, 1 subnets
R   10.10.10.10/32 [120/1] via 172.16.2.2, 00:00:22, 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, 00:00:22, Serial0/0/1
C   172.16.2.0/30 is directly connected, Serial0/0/1
L   172.16.2.1/32 is directly connected, Serial0/0/1
 192.168.4.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.4.0/24 is directly connected, Loopback4
L   192.168.4.1/32 is directly connected, Loopback4
 192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.5.0/24 is directly connected, Loopback5
L   192.168.5.1/32 is directly connected, Loopback5
 192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.6.0/24 is directly connected, Loopback6
L   192.168.6.1/32 is directly connected, Loopback6
R   192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:22, Serial0/0/1
R   192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:22, Serial0/0/1
R   192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:22, Serial0/0/1
S*  0.0.0.0/0 is directly connected, Serial0/0/1

```

R3#

Ctrl+F6 to exit CLI focus

Copy Paste

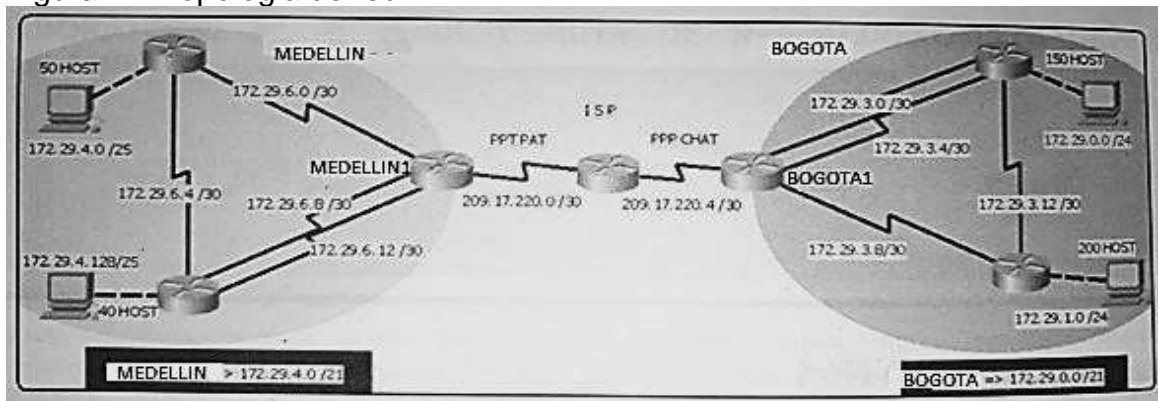
Top

Descripción de escenarios propuestos para la prueba de habilidades

Escenario 2

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

Figura 11. Topología de red



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

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

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

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

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

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

Parte 1: Configuración del enrutamiento

- a. Configurar el enrutamiento en la red usando el protocolo RIP versión 2, declare la red principal, desactive la sumarización automática.
- b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de RIP.
- c. El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se sumarian las subredes de cada uno a /22.

Parte 2: Tabla de Enrutamiento.

- a. Verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.
- b. Verificar el balanceo de carga que presentan los routers.
- c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.
- d. Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante RIP.
- e. Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.
- f. El router ISP solo debe indicar sus rutas estáticas adicionales a las directamente conectadas.

Parte 3: Deshabilitar la propagación del protocolo RIP.

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

Tabla 23. Deshabilitar la propagación del protocolo RIP

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

Parte 4: Verificación del protocolo RIP.

- 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 RIP y las interfaces que participan de la publicación entre otros datos.
- b. Verificar y documentar la base de datos de RIP de cada router, donde se informa de manera detallada de todas las rutas hacia cada red.

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Parte 6: Configuración de PAT.

- a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
- b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.
- c. Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

Parte 7: Configuración del servicio DHCP.

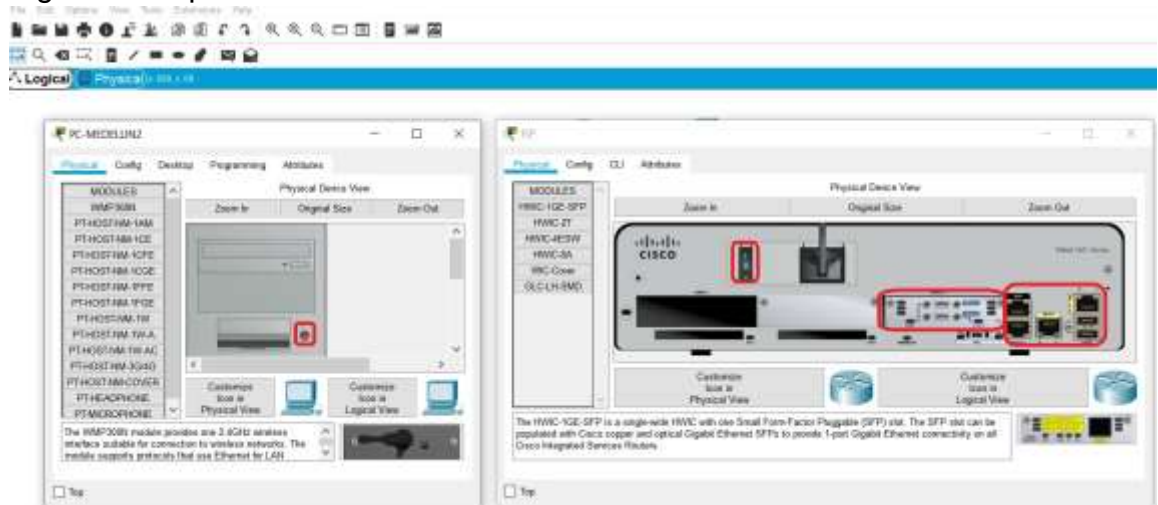
- a. Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes Lan.
- b. El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2.
- c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe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

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

DESARROLLO DEL ESCENARIO 2.

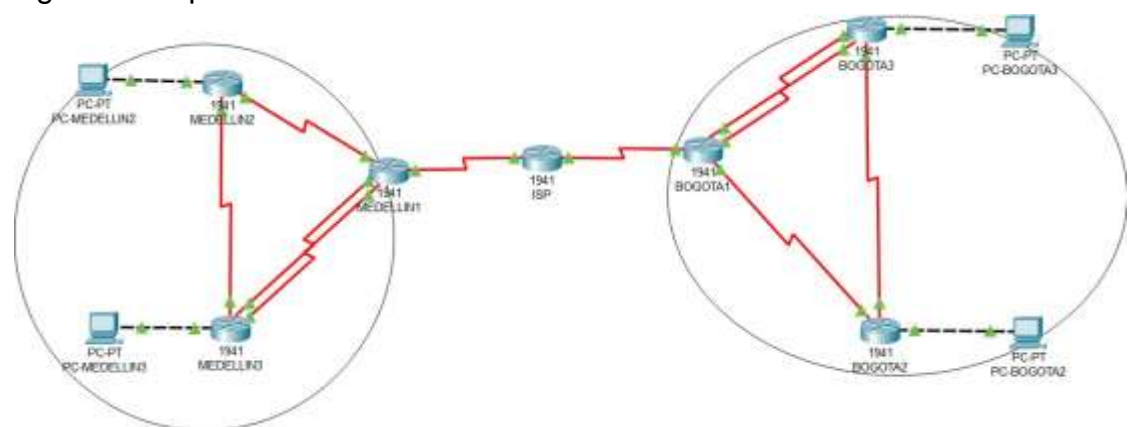
Observamos los requerimientos de cada uno de los dispositivos sabiendo la cantidad de interfaces y el tipo de interfaces que necesitamos dentro de cada dispositivo.

Figura 12. Tipo de interfaces



Como conocemos el diagrama de la TOPOLIGIA procedemos a realizar la distribución y conexión de los mismos.

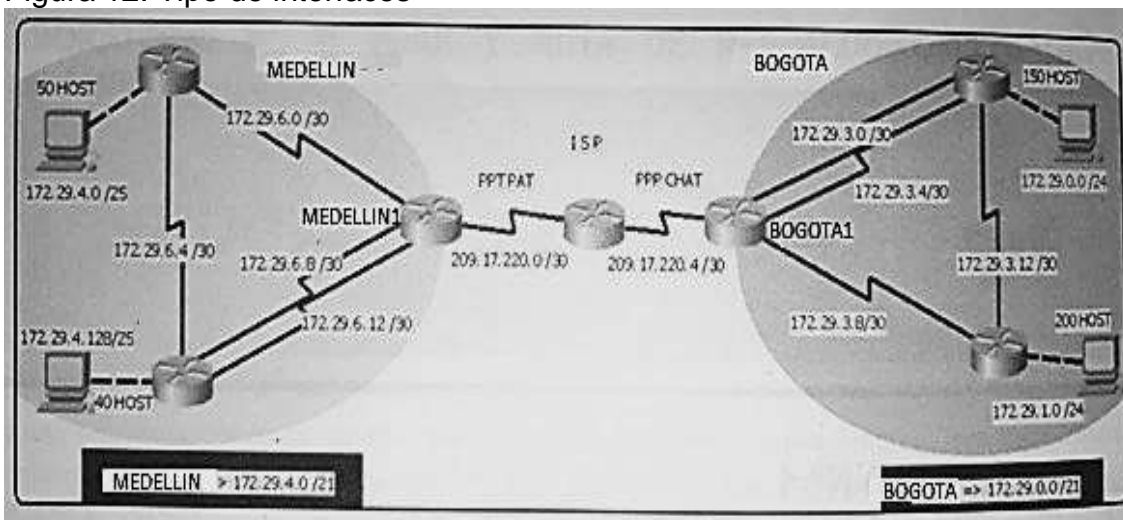
Figura 12. Tipo de interfaces



De cada uno de los pasos que se hacen debemos tener una documentación con el fin de poder corregir problemas posteriores o con el fin de poder realizar los cambios pertinentes.

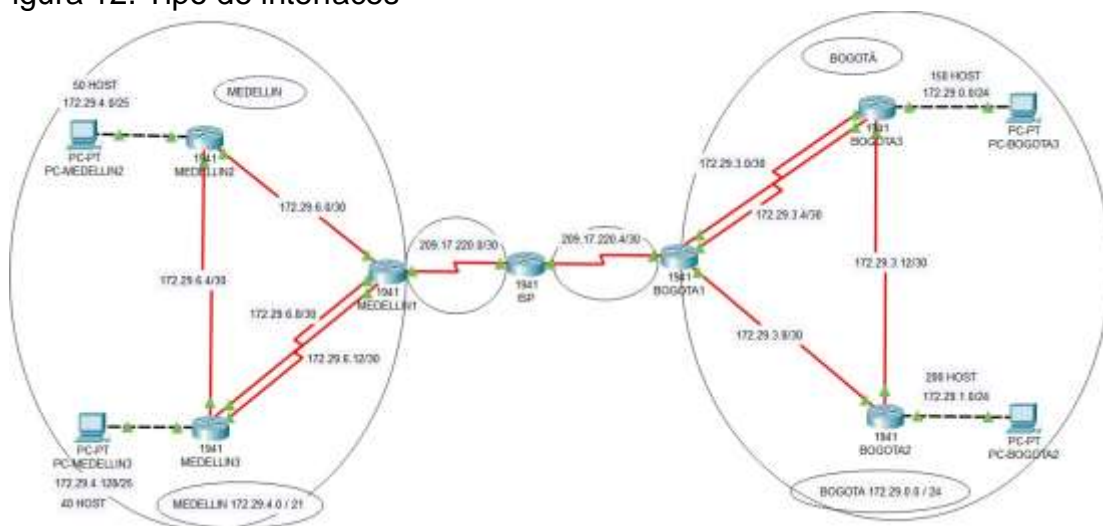
- Recordemos ante que nada que el ejercicio nos suministra las direcciones de red que vamos a emplear en cada uno de los rangos a configurar:

Figura 12. Tipo de interfaces



Con la información que se nos entrega en el diagrama de la topología procedemos a armar nuestra red etiquetando igualmente cada una de estas subredes.

Figura 12. Tipo de interfaces



El ejercicio nos suministra la información de direccionamiento, es por esto que podemos proceder a realizar las tablas de direccionamiento con el fin de conocer el rango de cada uno de ellos y así poder configurar los dispositivos que hacen parte de cada uno.

Tabla de Direccionamiento

Procedemos entonces a formular nuestra tabla de direccionamiento:

Comenzamos identificando cada uno de los rangos de las diferentes SUBREDES.

Tabla 24. Direccionamiento

Dir. red	Primera IP	Ultma IP	Broadcast.	Mascara.
172.29.4.0/25	172.29.4.1	172.29.4.126	172.29.4.0	255.255.255.128
172.29.4.128/25	172.29.4.129	172.29.4.254	172.29.4.255	255.255.255.128
172.29.6.0/30	172.29.6.1	172.29.6.2	172.29.6.3	255.255.255.252
172.29.6.4/30	172.29.6.5	172.29.6.6	172.29.6.7	255.255.255.252
172.29.6.8/30	172.29.6.9	172.29.6.10	172.29.6.11	255.255.255.252
172.29.6.12/30	172.29.6.13	172.29.6.14	172.29.6.15	255.255.255.252
172.29.0.0/24	172.29.0.1	172.29.0.254	172.29.0.255	255.255.255.0
172.29.1.0/24	172.29.1.1	172.29.1.254	172.29.1.255	255.255.255.0
172.29.3.0/30	172.29.3.1	172.29.3.2	172.29.3.3	255.255.255.252
172.29.3.4/30	172.29.3.5	172.29.3.6	172.29.3.7	255.255.255.252
172.29.3.8/30	172.29.3.9	172.29.3.10	172.29.3.11	255.255.255.252
172.29.3.12/30	172.29.3.13	172.29.3.14	172.29.3.15	255.255.255.252
209.17.220.0/30	209.17.220.1	209.17.220.2	209.17.220.3	255.255.255.252
209.17.220.4/30	209.17.220.5	209.17.220.6	209.17.220.7	255.255.255.252

Ya conocemos el rango que le corresponde a cada una de las SUBREDES, es por esto que podemos proceder a asignar la dirección exacta a cada dispositivo:

Tabla 24. Direccionamiento

Dispositivo	Interface	Dirección IP	Máscara Subred	de	Puerta de Enlace
-------------	-----------	--------------	----------------	----	------------------

BOGOTA1	S0/0/0	209.165.200.6	255.255.255.252	
	S0/0/1	172.29.3.9	255.255.255.252	
	S0/1/0	172.29.3.1	255.255.255.252	
	S0/1/1	172.29.3.5	255.255.255.252	
BOGOTA2	S0/0/0	172.29.3.10	255.255.255.252	
	S0/0/1	172.29.3.13	255.255.255.252	
	G0/0	172.29.1.1	255.255.255.0	
BOGOTA3	S0/0/0	172.29.3.2	255.255.255.252	
	S0/0/1	172.29.3.6	255.255.255.252	
	S0/1/0	172.29.3.14	255.255.255.252	
	G0/0	172.29.0.1	255.255.255.0	
ISP	S0/0/0	209.165.200.1	255.255.255.252	
	S0/0/1	209.165.200.5	255.255.255.252	
MEDELLIN1	S0/0/0	209.165.200.2	255.255.255.252	
	S0/0/1	172.29.6.1	255.255.255.252	
	S0/1/0	172.29.6.9	255.255.255.252	
	S0/1/1	172.29.6.13	255.255.255.252	
MEDELLIN2	S0/0/0	172.29.6.2	255.255.255.252	
	S0/0/1	172.29.6.5	255.255.255.252	
	G0/0	172.29.4.1	255.255.255.128	
MEDELLIN3	S0/0/0	172.29.6.10	255.255.255.252	
	S0/0/1	172.29.6.14	255.255.255.252	
	S0/1/0	172.29.6.6	255.255.255.252	
	G0/0	172.29.4.129	255.255.255.128	
PC- MEDELLIN2	F0/0	DHCP	DHCP	DHCP
PC- MEDELLIN3	F0/0	DHCP	DHCP	DHCP
PC- BOGOTA2	F0/0	DHCP	DHCP	DHCP
PC- BOGOTA3	F0/0	DHCP	DHCP	DHCP

Podemos proceder a configurar, este proceso se lo detalla a continuación:

- Realizar las rutinas de diagnóstico y dejar los equipos listos para su configuración (asignar nombres de equipos, asignar claves de seguridad, etc).

Tabla 24. Direccionamiento

<p>BOGOTA1</p> <pre>hostname BOGOTA1 no ip domain-lookup service password-encryption enable secret class banner motd %Acceso Restringido%</pre>	<p>BOGOTA2</p> <pre>hostname BOGOTA2 no ip domain-lookup service password-encryption enable secret class banner motd %Acceso Restringido%</pre>
---	---

<pre>ip domain-name cisco.com line console 0 password cisco login line vty 0 15 password cisco login</pre>	<pre>ip domain-name cisco.com line console 0 password cisco login line vty 0 15 password cisco login</pre>
<p>BOGOTA 3</p> <pre>hostname BOGOTA3 no ip domain-lookup service password-encryption enable secret class banner motd %Acceso Restringido% ip domain-name cisco.com line console 0 password cisco login line vty 0 15 password cisco login</pre>	<p>Router ISP:</p> <pre>hostname ISP no ip domain-lookup service password-encryption enable secret class banner motd %Acceso Restringido% ip domain-name cisco.com line console 0 password cisco login line vty 0 15 password cisco login</pre>
<p>MEDELLIN1</p> <pre>hostname MEDELLIN1 no ip domain-lookup service password-encryption enable secret class banner motd %Acceso Restringido% ip domain-name cisco.com line console 0 password cisco login line vty 0 15 password cisco login</pre>	<p>MEDELLIN2</p> <pre>hostname MEDELLIN2 no ip domain-lookup service password-encryption enable secret class banner motd %Acceso Restringido% ip domain-name cisco.com line console 0 password cisco login line vty 0 15 password cisco login</pre>
<p>MEDELLIN3</p> <pre>hostname MEDELLIN3 no ip domain-lookup service password-encryption enable secret class</pre>	

<pre> banner motd %Acceso Restringido% ip domain-name cisco.com line console 0 password cisco login line vty 0 15 password cisco login </pre>	
---	--

- Configuración de direcciones IP de cada una de las interfaces de cada uno de los routers:

Tabla 24. Direcccionamiento

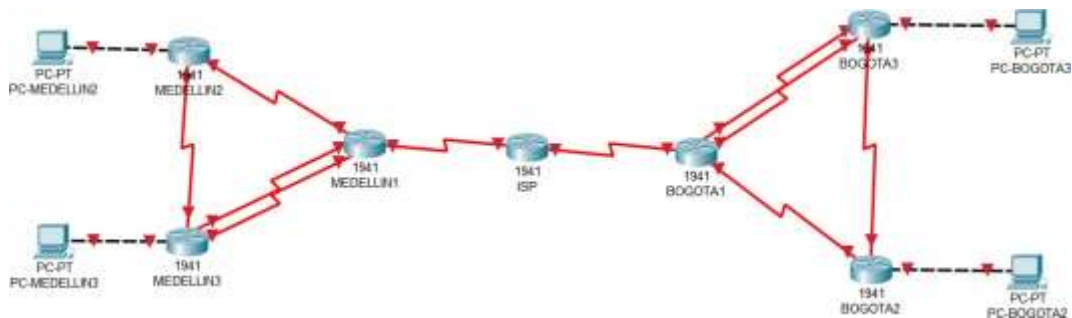
<pre> Interface seriales ISP interface Serial0/0/0 ip address 209.17.220.1 255.255.255.252 clock rate 4000000 no shutdown interface Serial0/0/1 ip address 209.17.220.5 255.255.255.252 clock rate 4000000 no shutdown </pre>	<pre> Interfaces seriales MEDELLIN 1: interface Serial0/0/0 ip address 209.17.220.2 255.255.255.252 no shutdown interface Serial0/0/1 ip address 172.29.6.1 255.255.255.252 clock rate 4000000 no shutdown interface Serial0/1/0 ip address 172.29.6.9 255.255.255.252 clock rate 4000000 no shutdown interface Serial0/1/1 ip address 172.29.6.13 255.255.255.252 clock rate 4000000 no shutdown </pre>
<pre> Interface seriales MEDELLIN 2: interface GigabitEthernet0/0 ip address 172.29.4.1 255.255.255.128 no shutdown </pre>	<pre> Interface bseriales MEDELLÍN 2: interface GigabitEthernet0/0 ip address 172.29.4.129 255.255.255.128 no shutdown </pre>

<pre> interface Serial0/0/0 ip address 172.29.6.2 255.255.255.252 no shutdown interface Serial0/0/1 ip address 172.29.6.5 255.255.255.252 clock rate 4000000 no shutdown </pre>	<pre> interface Serial0/0/0 ip address 172.29.6.10 255.255.255.252 no shutdown interface Serial0/0/1 ip address 172.29.6.14 255.255.255.252 no shutdown interface Serial0/1/0 ip address 172.29.6.6 255.255.255.252 no shutdown </pre>
<p>Interafce seriales BOGOTA 1:</p> <pre> interface Serial0/0/0 ip address 209.17.220.6 255.255.255.252 no shutdown interface Serial0/0/1 ip address 172.29.3.9 255.255.255.252 no shutdown interface Serial0/1/0 ip address 172.29.3.1 255.255.255.252 clock rate 4000000 no shutdown interface Serial0/1/1 ip address 172.29.3.5 255.255.255.252 no shutdown </pre>	<p>Interface seriales BOGOTA 2:</p> <pre> interface GigabitEthernet0/0 ip address 172.29.1.1 255.255.255.0 no shutdown interface Serial0/0/0 ip address 172.29.3.10 255.255.255.252 no shutdown interface Serial0/0/1 ip address 172.29.3.13 255.255.255.252 clock rate 4000000 no shutdown </pre>
<p>Intrefaces seriales BOGOTA 3:</p> <pre> interface GigabitEthernet0/0 ip address 172.29.0.1 255.255.255.0 no shutdown interface Serial0/0/0 </pre>	

<pre> ip address 172.29.3.2 255.255.255.252 no shutdown interface Serial0/0/1 ip address 172.29.3.6 255.255.255.252 no shutdown interface Serial0/1/0 ip address 172.29.3.14 255.255.255.252 no shutdown </pre>	
---	--

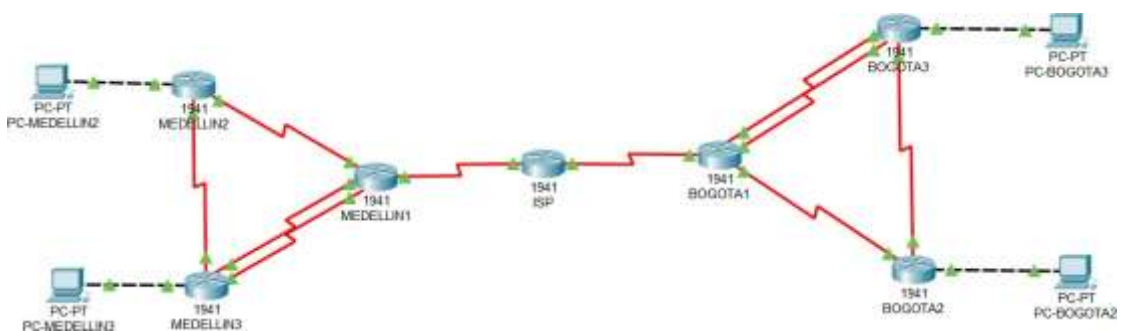
- Realizar la conexión física de los equipos con base en la topología de red

Figura 11. Topología de red



Luego de configurar las diferentes interfaces cada uno de los indicadores de los dispositivos cambia de color:

Figura 11. Topología de red



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

Configuración del enrutamiento

Configuramos el protocolo de enrutamiento RIP V2, el cual posibilita el intercambio de paquetes entre las diferentes subredes.

- Debeos activar el protocolo RIP V2 en cada uno de los routers, indicando cuales son las subredes que se van a intercambiar y ademas debemos aplicar el comando “no auto sumary” CON EL FIN de que estas sean publicadas de manera individual.

Tabla 25. Configuración del enrutamiento

MEDELLIN1 router rip version 2 network 172.29.0.0 no auto-summary	MEDELLIN2 router rip version 2 network 172.29.0.0 no auto-summary
MEDELLIN3 router rip version 2 network 172.29.0.0 no auto-summary	BOGOTA1 router rip version 2 network 172.29.0.0 no auto-summary
BOGOTA2 router rip version 2 network 172.29.0.0 no auto-summary	BOGOTA3 router rip version 2 network 172.29.0.0 no auto-summary

Debemos agregar rutas estáticas en los routers de MEDELLIN y de BOGOTA y ademas las debemos propagar hacia los demas dispositivos empleando RIP.

Tabla 25. Configuración del enrutamiento

MEDELLIN1 ip route 0.0.0.0 0.0.0.0 209.17.220.1 router rip default-information originate	BOGOTA1 ip route 0.0.0.0 0.0.0.0 209.17.220.5 router rip default-information originate
---	---

- Desde el router ISP debemos crear 2 rutas estáticas dirigidas hacia cada una de las redes internas de Bogotá y Medellín para el caso se sumarizan las subredes de cada uno a /22.

ISP

ip route 172.29.4.0 255.255.252.0 209.17.220.2

```
ip route 172.29.0.0 255.255.252.0 209.17.220.6
```

Parte 2: Tabla de Enrutamiento.

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

Figura 13. Enrutamiento

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

Gateway of last resort is not set

 172.29.0.0/22 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, 6 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    209.17.220.2/32 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
C    209.17.220.6/32 is directly connected, Serial0/0/1

ISP#

MEDELLIN2#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.29.6.1 to network 0.0.0.0

 172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C    172.29.4.0/25 is directly connected, GigabitEthernet0/0
L    172.29.4.1/32 is directly connected, GigabitEthernet0/0
R    172.29.4.128/25 [120/1] via 172.29.6.6, 00:00:18, Serial0/0/1
C    172.29.6.0/30 is directly connected, Serial0/0/0
L    172.29.6.2/32 is directly connected, Serial0/0/0
C    172.29.6.4/30 is directly connected, Serial0/0/1
L    172.29.6.5/32 is directly connected, Serial0/0/1
R    172.29.6.8/30 [120/1] via 172.29.6.1, 00:00:17, Serial0/0/0
    [120/1] via 172.29.6.6, 00:00:18, Serial0/0/1
R    172.29.6.12/30 [120/1] via 172.29.6.1, 00:00:17, Serial0/0/0
    [120/1] via 172.29.6.6, 00:00:18, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.29.6.1, 00:00:17, Serial0/0/0

MEDELLIN2#
```

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

Gateway of last resort is 172.29.6.13 to network 0.0.0.0

```
172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
R    172.29.4.0/25 [120/1] via 172.29.6.5, 00:00:20, Serial0/1/0
C    172.29.4.128/25 is directly connected, GigabitEthernet0/0
L    172.29.4.129/32 is directly connected, GigabitEthernet0/0
R    172.29.6.0/30 [120/1] via 172.29.6.13, 00:00:24, Serial0/0/1
        [120/1] via 172.29.6.9, 00:00:24, Serial0/0/0
        [120/1] via 172.29.6.5, 00:00:20, Serial0/1/0
C    172.29.6.4/30 is directly connected, Serial0/1/0
L    172.29.6.6/32 is directly connected, Serial0/1/0
C    172.29.6.8/30 is directly connected, Serial0/0/0
L    172.29.6.10/32 is directly connected, Serial0/0/0
C    172.29.6.12/30 is directly connected, Serial0/0/1
L    172.29.6.14/32 is directly connected, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.29.6.13, 00:00:24, Serial0/0/1
        [120/1] via 172.29.6.9, 00:00:24, Serial0/0/0
```

MEDELLIN3#

IOS Command Line Interface

```
BOGOTA2# show ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
```

Gateway of last resort is 172.29.3.9 to network 0.0.0.0

```
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R    172.29.0.0/24 [120/1] via 172.29.3.14, 00:00:20, Serial0/0/1
C    172.29.1.0/24 is directly connected, GigabitEthernet0/0
L    172.29.1.1/32 is directly connected, GigabitEthernet0/0
R    172.29.3.0/30 [120/1] via 172.29.3.14, 00:00:20, Serial0/0/1
        [120/1] via 172.29.3.9, 00:00:14, Serial0/0/0
R    172.29.3.4/30 [120/1] via 172.29.3.14, 00:00:20, Serial0/0/1
        [120/1] via 172.29.3.9, 00:00:14, Serial0/0/0
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    172.29.3.13/32 is directly connected, Serial0/0/1
R*   0.0.0.0/0 [120/1] via 172.29.3.9, 00:00:14, Serial0/0/0
```

BOGOTA2#

IOS Command Line Interface

```
BOGOTA3#show ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route
```

Gateway of last resort is 172.29.3.1 to network 0.0.0.0

```
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
R    172.29.1.0/24 [120/1] via 172.29.3.13, 00:00:20, 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
R    172.29.3.8/30 [120/1] via 172.29.3.1, 00:00:17, Serial0/0/0
        [120/1] via 172.29.3.5, 00:00:17, Serial0/0/1
        [120/1] via 172.29.3.13, 00:00:20, Serial0/1/0
C    172.29.3.12/30 is directly connected, Serial0/1/0
L    172.29.3.14/32 is directly connected, Serial0/1/0
R*   0.0.0.0/0 [120/1] via 172.29.3.1, 00:00:17, Serial0/0/0
        [120/1] via 172.29.3.5, 00:00:17, Serial0/0/1
```

BOGOTA3#

- En este caso luego de aplicar el comando SHOW IP ROUTE vemos que cada uno de los routers cuenta con una ruta independiente para cada una de las subredes de nuestra topología.
 - a) Verificar el balanceo de carga que presentan los routers.
 - b) 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.
 - c) Los routers Medellín2 y Bogotá2 también presentan redes conectadas directamente y recibidas mediante RIP.
 - d) Las tablas de los routers restantes deben permitir visualizar rutas redundantes para el caso de la ruta por defecto.

Figura 13. Enrutamiento

```

IOS Command Line Interface

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 172.29.3.5 to network 0.0.0.0

 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
R   172.29.1.0/24 [120/1] via 172.29.3.13, 00:00:18, 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
R   172.29.3.8/30 [120/1] via 172.29.3.13, 00:00:18, Serial0/1/0
    [120/1] via 172.29.3.5, 00:00:21, Serial0/0/1
    [120/1] via 172.29.3.1, 00:00:21, Serial0/0/0
C   172.29.3.12/30 is directly connected, Serial0/1/0
L   172.29.3.14/32 is directly connected, Serial0/1/0
R*  0.0.0.0/0 [120/1] via 172.29.3.5, 00:00:21, Serial0/0/1
    [120/1] via 172.29.3.1, 00:00:21, Serial0/0/0

BOGOTA3#
  
```

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

```

ISP

Physical  Config  CLI  Attributes

IOS Command Line Interface

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

Gateway of last resort is not set

 172.29.0.0/22 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, 6 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   209.17.220.2/32 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
C   209.17.220.6/32 is directly connected, Serial0/0/1

ISP#
  
```


Parte 3: Deshabilitar la propagación del protocolo RIP.

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

- Desactivamos las interfaces que no necesitan que se propague las actualizaciones de RIP, aplicando el comando `PASSIVE INTERFACE`.

Tabla 26. Deshabilitar la propagación del protocolo RIP

MEDELLIN1 router rip passive-interface Serial0/0/0	MEDELLIN2 router rip passive-interface GigabitEthernet0/0
MEDELLIN3 router rip passive-interface GigabitEthernet0/0	BOGOTA1 router rip passive-interface Serial0/0/0
BOGOTA2 router rip passive-interface GigabitEthernet0/0	BOGOTA3 router rip passive-interface GigabitEthernet0/0

Parte 4: Verificación del protocolo RIP.

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 RIP y las interfaces que participan de la publicación entre otros datos.

Figura 14. Verificación de protocolo RIP

```

S* 0.0.0.0/0 [1/0] via 209.17.220.1
MEDELLIN1# show 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
Serial0/1/0        2     2
Serial0/1/1        2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
 172.29.0.0
Passive Interface(s):
 Serial0/0/0
Routing Information Sources:
 Gateway          Distance      Last Update
 172.29.6.2       120           00:00:19
 172.29.6.14      120           00:00:18
 172.29.6.10      120           00:00:18
Distance: (default is 120)
MEDELLIN1#

```

```

[120/1] via 172.29.6.6, 00:00:18, Serial0/0/1
R* 0.0.0.0/0 [120/1] via 172.29.6.1, 00:00:17, Serial0/0/0
MEDELLIN2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 4 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
Serial0/0/0        2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
 172.29.0.0
Passive Interface(s):
 GigabitEthernet0/0
Routing Information Sources:
 Gateway          Distance      Last Update
 172.29.6.1       120           00:00:01
 172.29.6.6       120           00:00:01
Distance: (default is 120)
MEDELLIN2#

```

```

MEDELLIN3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 7 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
Serial0/0/0        2     2
Serial0/1/0        2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
 172.29.0.0
Passive Interface(s):
 GigabitEthernet0/0
Routing Information Sources:
 Gateway          Distance      Last Update
 172.29.6.13      120           00:00:19
 172.29.6.9       120           00:00:19
 172.29.6.5       120           00:00:14
Distance: (default is 120)
MEDELLIN3#

```

```

L* 209.17.220.0/32 is directly connected, Serial0/0/0
S* 0.0.0.0/0 [1/0] via 209.17.220.5

BOGOTA1#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 14 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
  Serial0/1/0         2     2
  Serial0/1/1         2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.29.0.0
Passive Interface(s):
  Serial0/0/0
Routing Information Sources:
  Gateway            Distance    Last Update
  172.29.3.2         120        00:00:17
  172.29.3.6         120        00:00:17
  172.29.3.10        120        00:00:21
Distance: (default is 120)
BOGOTA1#

R* 0.0.0.0/0 [120/1] via 172.29.3.9, 00:00:14, Serial0/0/0

BOGOTA2#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 13 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
  Serial0/0/0         2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.29.0.0
Passive Interface(s):
  GigabitEthernet0/0
Routing Information Sources:
  Gateway            Distance    Last Update
  172.29.3.9         120        00:00:06
  172.29.3.14        120        00:00:08
Distance: (default is 120)
BOGOTA2#

[120/1] via 172.29.3.5, 00:00:17, Serial0/0/1

BOGOTA3#show ip protocols
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 0 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip
Default version control: send version 2, receive 2
  Interface          Send Recv Triggered RIP Key-chain
  Serial0/0/0         2     2
  Serial0/0/1         2     2
  Serial0/1/0         2     2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
  172.29.0.0
Passive Interface(s):
  GigabitEthernet0/0
Routing Information Sources:
  Gateway            Distance    Last Update
  172.29.3.1         120        00:00:26
  172.29.3.5         120        00:00:26
  172.29.3.13        120        00:00:07
Distance: (default is 120)
BOGOTA3#

```

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

Figura 14. Verificación de protocolo RIP

```

172.29.6.10      120      00:00:18
Distance: (default is 120)
MEDELLIN1#show ip route rip
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R   172.29.4.0/25 [120/1] via 172.29.6.2, 00:00:10, Serial0/0/1
R   172.29.4.128/25 [120/1] via 172.29.6.14, 00:00:21, Serial0/1/1
    [120/1] via 172.29.6.10, 00:00:21, Serial0/1/0
R   172.29.6.4/30 [120/1] via 172.29.6.2, 00:00:10, Serial0/0/1
    [120/1] via 172.29.6.14, 00:00:21, Serial0/1/1
    [120/1] via 172.29.6.10, 00:00:21, Serial0/1/0
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
MEDELLIN1#

172.29.6.1      120      00:00:10
172.29.6.6      120      00:00:10
Distance: (default is 120)
MEDELLIN2#show ip route rip
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R   172.29.4.128/25 [120/1] via 172.29.6.6, 00:00:17, Serial0/0/1
R   172.29.6.8/30 [120/1] via 172.29.6.1, 00:00:16, Serial0/0/0
    [120/1] via 172.29.6.6, 00:00:17, Serial0/0/1
R   172.29.6.12/30 [120/1] via 172.29.6.1, 00:00:16, Serial0/0/0
    [120/1] via 172.29.6.6, 00:00:17, Serial0/0/1
R*  0.0.0.0/0 [120/1] via 172.29.6.1, 00:00:16, Serial0/0/0
MEDELLIN2#

172.29.6.9      120      00:00:19
172.29.6.5      120      00:00:14
Distance: (default is 120)
MEDELLIN3#show ip route rip
172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
R   172.29.4.0/25 [120/1] via 172.29.6.5, 00:00:23, Serial0/1/0
R   172.29.4.0/30 [120/1] via 172.29.6.13, 00:00:08, Serial0/0/1
    [120/1] via 172.29.6.9, 00:00:08, Serial0/0/0
    [120/1] via 172.29.6.5, 00:00:23, Serial0/1/0
R*  0.0.0.0/0 [120/1] via 172.29.6.13, 00:00:08, Serial0/0/1
R*  0.0.0.0/0 [120/1] via 172.29.6.9, 00:00:08, Serial0/0/0
MEDELLIN3#

172.29.3.10     120      00:00:21
Distance: (default is 120)
BOGOTA1#show ip route rip
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R   172.29.0.0/24 [120/1] via 172.29.3.2, 00:00:18, Serial0/1/0
    [120/1] via 172.29.3.6, 00:00:18, Serial0/1/1
R   172.29.1.0/24 [120/1] via 172.29.3.10, 00:00:26, Serial0/0/1
R   172.29.3.12/30 [120/1] via 172.29.3.2, 00:00:18, Serial0/1/0
    [120/1] via 172.29.3.6, 00:00:18, Serial0/1/1
    [120/1] via 172.29.3.10, 00:00:26, Serial0/0/1
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
BOGOTA1#

172.29.3.9      120      00:00:06
172.29.3.14     120      00:00:08
Distance: (default is 120)
BOGOTA2#show ip route rip
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R   172.29.0.0/24 [120/1] via 172.29.3.14, 00:00:11, Serial0/0/1
R   172.29.3.0/30 [120/1] via 172.29.3.14, 00:00:11, Serial0/0/1
    [120/1] via 172.29.3.9, 00:00:10, Serial0/0/0
R   172.29.3.4/30 [120/1] via 172.29.3.14, 00:00:11, Serial0/0/1
    [120/1] via 172.29.3.9, 00:00:10, Serial0/0/0
R*  0.0.0.0/0 [120/1] via 172.29.3.9, 00:00:10, Serial0/0/0
BOGOTA2#

172.29.3.5      120      00:00:07
172.29.3.13     120      00:00:07
Distance: (default is 120)
BOGOTA3#show ip route rip
172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
R   172.29.1.0/24 [120/1] via 172.29.3.13, 00:00:14, Serial0/1/0
R   172.29.3.8/30 [120/1] via 172.29.3.1, 00:00:07, Serial0/0/0
    [120/1] via 172.29.3.5, 00:00:07, Serial0/0/1
    [120/1] via 172.29.3.13, 00:00:14, Serial0/1/0
R*  0.0.0.0/0 [120/1] via 172.29.3.1, 00:00:07, Serial0/0/0
R*  0.0.0.0/0 [120/1] via 172.29.3.5, 00:00:07, Serial0/0/1
BOGOTA3#

```

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

Tabla 27. Configurar encapsulamiento y autenticación PPP

ISP	MEDELLIN1
username MEDELLIN password cisco	username ISP password cisco
interface Serial0/0/0 encapsulation ppp ppp authentication pap ppp pap sent-username ISP password cisco	interface Serial0/0/0 encapsulation ppp ppp authentication pap ppp pap sent-username MEDELLIN password cisco

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

Tabla 27. Configurar encapsulamiento y autenticación PPP

ISP	BOGOTA1
username BOGOTA password cisco	username ISP password cisco
interface Serial0/0/1 encapsulation ppp ppp authentication chap	interface Serial0/0/0 encapsulation ppp ppp authentication chap

Parte 6: Configuración de NAT.

- a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.
- b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

MEDELLIN1

```
ip nat inside source list 1 interface Serial0/0/0 overload
access-list 1 permit 172.29.4.0 0.0.3.255
```

```
interface Serial0/0/0
ip nat outside
interface Serial0/0/1
ip nat inside
```

```

interface Serial0/1/0
ip nat inside
interface Serial0/1/1
ip nat inside

```

Figura 15. Configuración de NAT

```

Password:
MEDELLINI>en
Password:
MEDELLINI#show ip nat translation
Pro Inside global      Inside local      Outside local     Outside global
icmp 209.17.220.2:1    172.29.4.6:1     209.17.220.1:1   209.17.220.1:1
icmp 209.17.220.2:2    172.29.4.6:2     209.17.220.1:2   209.17.220.1:2
icmp 209.17.220.2:3    172.29.4.6:3     209.17.220.1:3   209.17.220.1:3
icmp 209.17.220.2:4    172.29.4.6:4     209.17.220.1:4   209.17.220.1:4
MEDELLINI#

```

a. 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, como diferente puerto.

BOGOTA1

```

ip nat inside source list 1 interface Serial0/0/0 overload
access-list 1 permit 172.29.0.0 0.0.3.255

```

```

interface Serial0/0/0
ip nat outside
interface Serial0/0/1
ip nat inside
interface Serial0/1/0
ip nat inside
interface Serial0/1/1
ip nat inside

```

Figura 15. Configuración de NAT

```

Password:
BOGOTA1>en
Password:
BOGOTA1#show ip nat translation
Pro Inside global      Inside local      Outside local     Outside global
icmp 209.17.220.6:1    172.29.0.6:1     209.17.220.1:1   209.17.220.1:1
icmp 209.17.220.6:2    172.29.0.6:2     209.17.220.1:2   209.17.220.1:2
icmp 209.17.220.6:3    172.29.0.6:3     209.17.220.1:3   209.17.220.1:3
icmp 209.17.220.6:4    172.29.0.6:4     209.17.220.1:4   209.17.220.1:4
BOGOTA1#

```

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

```
ip dhcp excluded-address 172.29.4.1 172.29.4.5
ip dhcp excluded-address 172.29.4.129 172.29.4.133
ip dhcp pool MED2
network 172.29.4.0 255.255.255.128
default-router 172.29.4.1
dns-server 8.8.8.8
ip dhcp pool MED3
network 172.29.4.128 255.255.255.128
default-router 172.29.4.129
dns-server 8.8.8.8
```

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

MEDELLIN3

```
interface GigabitEthernet0/0
ip helper-address 172.29.6.5
```

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

BOGOTA2

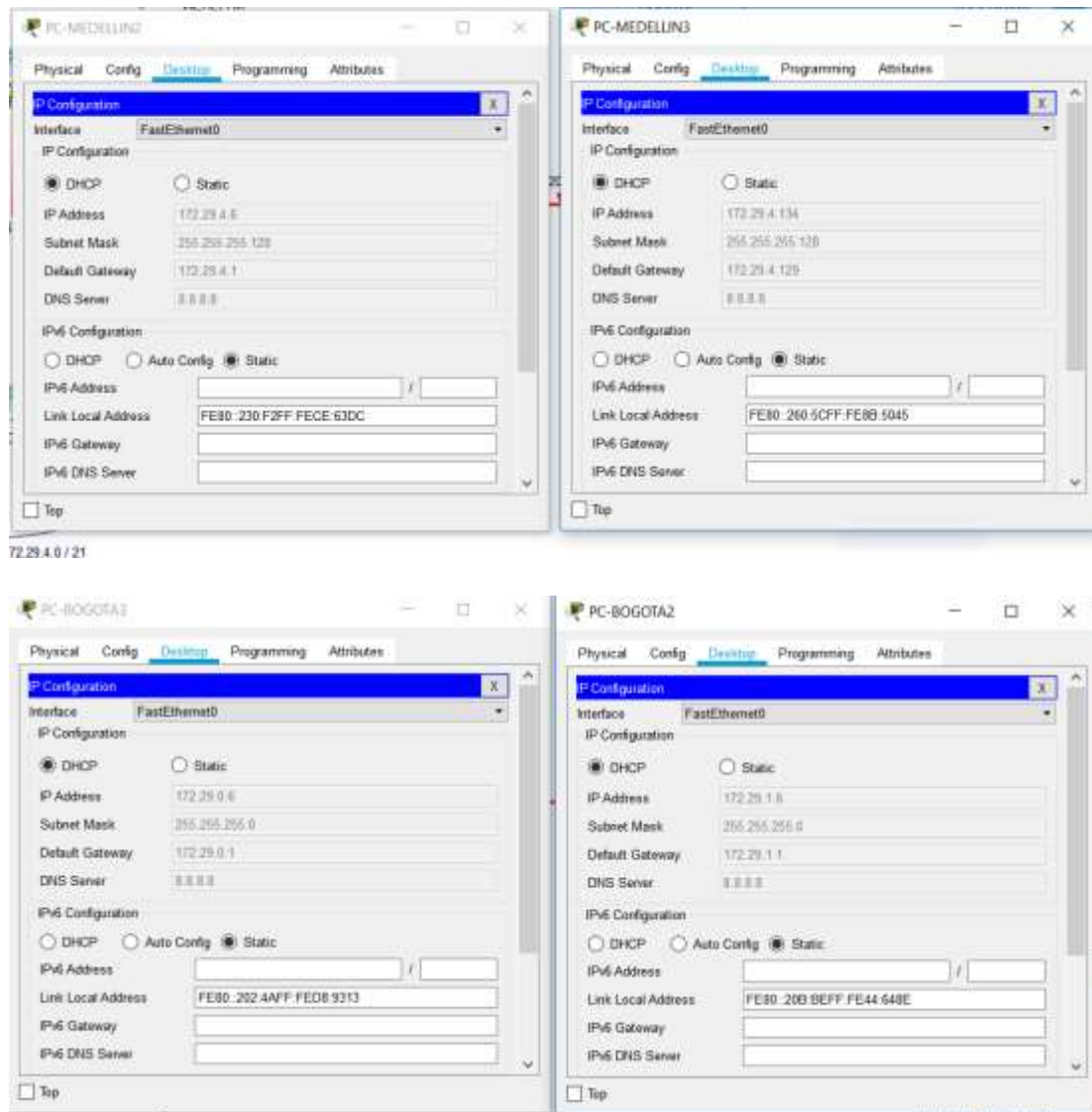
```
ip dhcp excluded-address 172.29.1.1 172.29.1.5
ip dhcp excluded-address 172.29.0.1 172.29.0.5
ip dhcp pool BOG2
network 172.29.1.0 255.255.255.0
default-router 172.29.1.1
dns-server 8.8.8.8
ip dhcp pool BOG3
network 172.29.0.0 255.255.255.0
default-router 172.29.0.1
dns-server 8.8.8.8
```

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

BOGOTA3

interface GigabitEthernet0/0
 ip helper-address 172.29.3.13

Figura 16. Verificación de configuración de Routers



Verificación de configuración de los ROUTERS:

Tabla 28. configuración de los ROUTERS

<pre>ISP#show running-config Building configuration... Current configuration : 1318 bytes</pre>	<pre>MEDELLIN1#show running-config Building configuration... Current configuration : 1613 bytes</pre>
--	--

<pre> ! version 15.1 no service timestamps log datetime msec no service timestamps debug datetime msec service password-encryption ! hostname ISP ! ! ! enable secret 5 \$1\$mERr\$9cTjUIEqNGurQiFU.ZeCi1 ! ! ! ! ! no ip cef no ipv6 cef ! ! ! username BOGOTA password 7 0822455D0A16 username MEDELLIN password 7 0822455D0A16 ! ! license udi pid CISCO1941/K9 sn FTX1524V670- ! ! ! ! ! ! ! ! ! no ip domain-lookup ip domain-name cisco.com ! ! spanning-tree mode pvst ! </pre>	<pre> ! version 15.1 no service timestamps log datetime msec no service timestamps debug datetime msec service password-encryption ! hostname MEDELLIN1 ! ! ! enable secret 5 \$1\$mERr\$9cTjUIEqNGurQiFU.ZeCi1 ! ! ! ! ! no ip cef no ipv6 cef ! ! ! username ISP password 7 0822455D0A16 ! ! license udi pid CISCO1941/K9 sn FTX1524QB89- ! ! ! ! ! ! ! ! ! no ip domain-lookup ip domain-name cisco.com ! ! spanning-tree mode pvst ! ! </pre>
--	---

<pre> ! ! ! ! ! interface GigabitEthernet0/0 no ip address duplex auto speed auto shutdown ! interface GigabitEthernet0/1 no ip address duplex auto speed auto shutdown ! interface Serial0/0/0 ip address 209.17.220.1 255.255.255.252 encapsulation ppp ppp authentication pap ppp pap sent-username ISP password 0 cisco clock rate 4000000 ! interface Serial0/0/1 ip address 209.17.220.5 255.255.255.252 encapsulation ppp ppp authentication chap clock rate 4000000 ! interface Vlan1 no ip address shutdown ! ip classless ip route 172.29.4.0 255.255.252.0 209.17.220.2 ip route 172.29.0.0 255.255.252.0 209.17.220.6 ! ip flow-export version 9 ! ! ! </pre>	<pre> ! ! ! interface GigabitEthernet0/0 no ip address duplex auto speed auto shutdown ! interface GigabitEthernet0/1 no ip address duplex auto speed auto shutdown ! interface Serial0/0/0 ip address 209.17.220.2 255.255.255.252 encapsulation ppp ppp authentication pap ppp pap sent-username MEDELLIN password 0 cisco ip nat outside ! interface Serial0/0/1 ip address 172.29.6.1 255.255.255.252 ip nat inside clock rate 4000000 ! interface Serial0/1/0 ip address 172.29.6.9 255.255.255.252 ip nat inside clock rate 4000000 ! interface Serial0/1/1 ip address 172.29.6.13 255.255.255.252 ip nat inside clock rate 4000000 ! interface Vlan1 no ip address shutdown ! router rip version 2 </pre>
---	--

<pre> banner motd ^CAcceso Restringido^C ! ! ! ! ! line con 0 password 7 0822455D0A16 login ! line aux 0 ! line vty 0 4 password 7 0822455D0A16 login line vty 5 15 password 7 0822455D0A16 login ! ! ! ! end ISP# </pre>	<pre> passive-interface Serial0/0/0 network 172.29.0.0 default-information originate no auto-summary ! ip nat inside source list 1 interface Serial0/0/0 overload ip classless ip route 0.0.0.0 0.0.0.0 209.17.220.1 ! ip flow-export version 9 ! ! access-list 1 permit 172.29.4.0 0.0.3.255 ! banner motd ^CAcceso Restringido^C ! ! ! ! ! line con 0 password 7 0822455D0A16 login ! line aux 0 ! line vty 0 4 password 7 0822455D0A16 login line vty 5 15 password 7 0822455D0A16 login ! ! ! end MEDELLIN1# </pre>
<pre> BOGOTA#show running-config Building configuration... Current configuration : 1186 bytes </pre>	

```
!  
version 15.1  
no service timestamps log datetime  
msec  
no service timestamps debug  
datetime msec  
no service password-encryption  
!  
hostname BOGOTA  
!  
!  
!  
!  
!  
!  
!  
no ip cef  
no ipv6 cef  
!  
!  
!  
username ISP password 0 cisco  
!  
!  
license udi pid CISCO1941/K9 sn  
FTX15245EE2-  
!  
!  
!  
!  
!  
!  
!  
!  
spanning-tree mode pvst  
!  
!  
!  
!  
!  
interface GigabitEthernet0/0  
no ip address  
duplex auto
```

```

speed auto
shutdown
!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/0/0
ip address 209.17.220.6
255.255.255.252
encapsulation ppp
ppp authentication chap
!
interface Serial0/0/1
ip address 172.29.3.9
255.255.255.252
clock rate 4000000
!
interface Serial0/1/0
ip address 172.29.3.1
255.255.255.252
clock rate 4000000
!
interface Serial0/1/1
ip address 172.29.3.5
255.255.255.252
clock rate 4000000
!
interface Vlan1
no ip address
shutdown
!
router rip
version 2
passive-interface Serial0/0/0
network 172.29.0.0
default-information originate
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 209.17.220.5
!
ip flow-export version 9
!
!
!

```

```
!  
!  
!  
!  
!  
line con 0  
!  
line aux 0  
!  
line vty 0 4  
login  
line vty 5 15  
login  
!  
!  
!  
end  
  
BOGOTA#
```

CONCLUSIONES

Cuando realizamos el direccionamiento IP aplicando VLSM ajustamos nuestro diseño a las necesidades reales de la red.

El proceso seguido para configurar cada una de las 2 topologías nos mostró el grado de asimilación del conocimiento hecho hasta el momento a lo largo de los 2 módulos.

Luego de realizar el proceso de análisis de las redes, se procedió a montar cada topología en el simulador, gracias a este programa podemos practicar cada uno de los comandos y verificar el correcto funcionamiento.

Documentamos cada uno de los pasos con el fin de corregir posibles inconvenientes que se nos presentaron y gracias a esta etapa los pudimos solucionar empleando el tiempo adecuado.

Siento seguridad a la hora de desarrollar proyectos de este tipo y de mediana envergadura.

Packet Tracer es una herramienta excelente a la hora de ayudarnos a realizar la configuración de redes como las indicadas, podemos practicar y practicar.

Videos de sustentación: <https://youtu.be/dDvqkZ7UP9A>

BIBLIOGRAFÍA

Andrew s. Tanenbaum (2003). Redes de Computadoras (Cuarta Edición). México. PEARSON Prentice Hall.

Asociación americana de Psicólogos. Referencias Bibliográficas según normas A.P.A [En Línea] Disponible en:

<http://www.slideshare.net/anafenech/modelo-apa-bibliografia> [2014, 22 de junio].

Cisco Systems Inc. Módulo de estudio CCNA Exploration 4.0. Conceptos y protocolos de enrutamiento. [Documento PDF en línea]. Disponible en: http://www.mediafire.com/view/5y052miul2vezhj/MODULO_DE_ESTUDIO_CCNA_2_EXPLORATION.pdf [2014, 19 de Junio]

Comunicación a través de la Red. [En Línea] Disponible en:

<http://www.utp.edu.co/~fgallego/claseXcapitulo/clase02.pdf> [2014, 21 de junio].

Cisco Packet Tracer [En Línea] Disponible en:

<https://www.netacad.com/web/about-us/cisco-packet-tracer> [2014, 19 de junio].

CP CCNA 1 I-2014. CCNA Exploration: Aspectos Básicos de Networking [En Línea] Disponible en: <https://1314297.netacad.com/courses/125408> [2014, 4 de febrero].

CP CCNA 2 I-2014. CCNA Exploration: Conceptos y Protocolos de Enrutamiento [En Línea] Disponible en:

<https://1314297.netacad.com/courses/144284> [2014, 26 de abril].

Ejemplo de Monografía. Fundamentos de Investigación [En Línea]

Publicación Manual Preparación de Una Monografía Según APA (5° Edición) [En Línea] Disponible en:

<http://www.slideshare.net/craupru/monografia-apa-1012210> [2014, 19 de junio].