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

LIRIA MARITZA RINCON ANTONIO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
BOGOTÁ D.C.
JUNIO DE 2020

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

LIRIA MARITZA RINCON ANTONIO

TRABAJO DE GRADO PARA OBTENER
EL TITULO DE INGENIERA DE SISTEMAS

PRESENTADO A
TUTOR
JOSE IGNACIO CARDONA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
INGENIERIA DE SISTEMAS
BOGOTÁ D.C.
JUNIO DE 2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Bogotá D.C, 01 de junio del 2020

DEDICATORIA

El presente trabajo está dedicado a mi hija Isabella Perilla a mi esposo Iddinael Perilla por haber sido mi apoyo a lo largo de toda mi carrera universitaria y a lo largo de mi vida. A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y como ser humano

AGRADECIMIENTOS

A mi esposo, por haberme dado la oportunidad de formarme en esta prestigiosa universidad y haber sido mi apoyo durante todo este tiempo.

De manera especial a los tutores, por haberme guiado, no solo en la elaboración de este trabajo de titulación, sino a lo largo de mi carrera universitaria y haberme brindado el apoyo para desarrollarme profesionalmente y seguir cultivando mis valores.

A la Universidad Nacional Abierta y a Distancia, por haberme brindado tantas oportunidades y enriquecerme en conocimiento

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

LISTADO DE TABLAS

INTRODUCCIÓN

El constante avance en la tecnología de la información y la comunicación ha provocado grandes cambios en las redes de comunicaciones, produciendo un incremento tanto en los volúmenes de información entre voz, datos y video que se transmiten, como en el número de destinatarios.

Este crecimiento del tráfico en redes exige el desarrollo de técnicas que permitan un consumo de menor cantidad de recursos, aumentando la velocidad, capacidad, rendimiento y tasa de envío de paquetes.

Las aplicaciones modernas y servicios de comunicaciones exigen funcionalidades mayores y más versátiles en las redes, y los usuarios días son más exigentes en cuanto a servicios de comunicación interactiva.

Las tecnologías de hoy ofrecen una opción viable para la difusión masiva, ya que promueven la disminución del tráfico en la red en la medida que permiten el envío de la información a múltiples destinos simultáneamente (realizando la transmisión una sola vez), de esta forma se reduce sustancialmente el consumo de recursos de ancho de banda y se emplea un menor tiempo para hacer llegar los contenidos a todas las ubicaciones.

En este documento se hace una referencia de los fundamentos y protocolos de enrutamiento utilizados, se desarrollan dos prácticas en el simuladores de redes Packet Tracer donde en una de ellas realizamos la conectividad de IPv4 e IPv6 utilizamos el protocolo de routing dinámico RIPv2 se hace la configuración de hosts dinámicos (DHCP) listas de control de acceso (ACL) también se realiza la configuración de protocolos de enrutamiento, OSPF y se realiza configuración de PAT ,Configuración del servicio DHCP.

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.

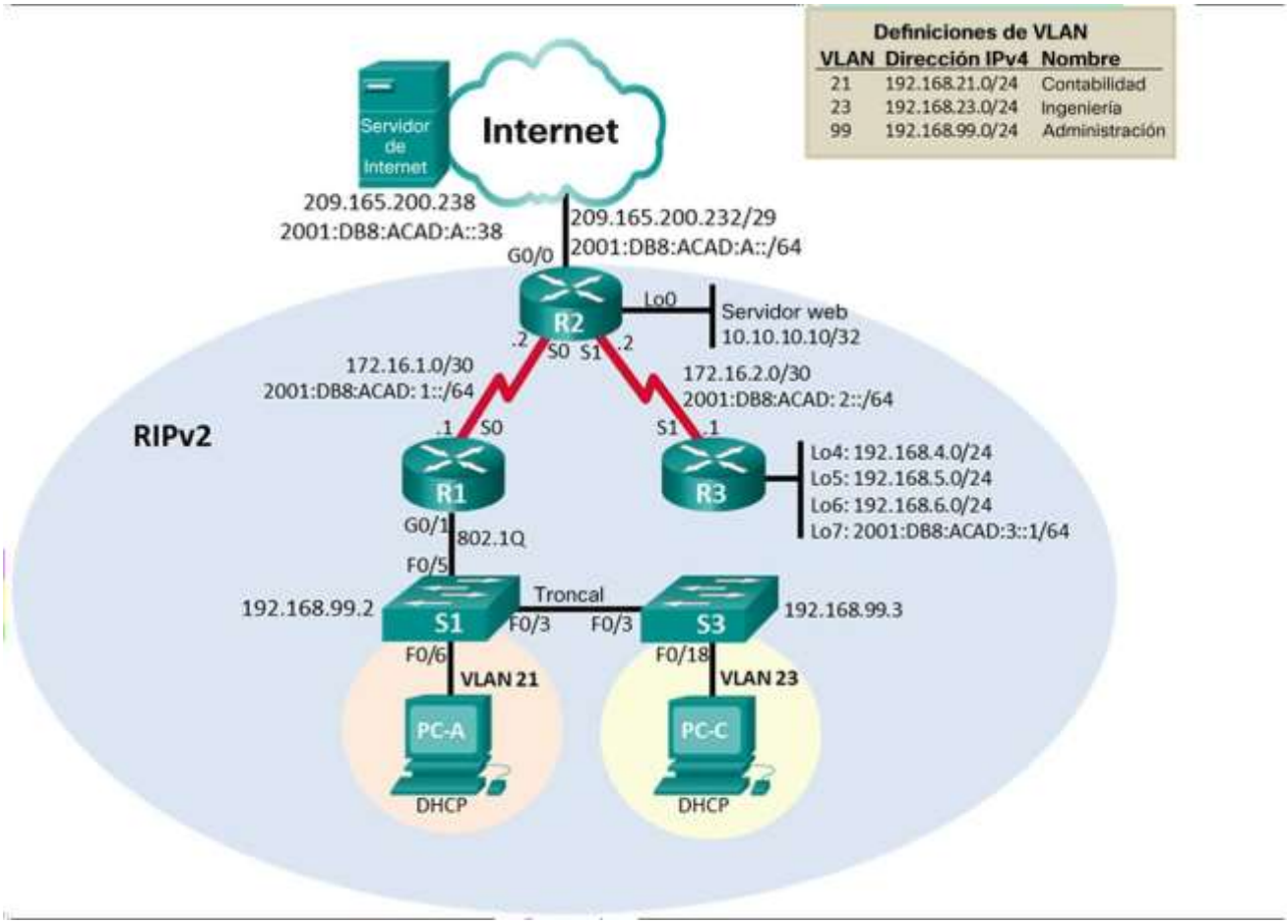


Ilustración 1.Topología Escenario 1

Parte1 Inicializar y volver a cargar los routers y los switches

Elimine las configuraciones de inicio y vuelva a cargar los dispositivos.
Antes de continuar, solicite al instructor que verifique la inicialización de los dispositivos.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router>enable Router#erase startup-config
Volver a cargar todos los routers	Router#reload
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup-config Switch#delete vlan.dat
Volver a cargar ambos switches	Switch#reload
Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches	Switch>enable Switch#show flash

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

Nota. Al inicia los equipos automáticamente carga la memoria y al borrar este archivo en los equipos pueden volver a su configuración básica después de una recarga.

Step 1: Configurar los parámetros básicos de los dispositivos

Step 2: Configurar la computadora de Internet

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

Elemento o tarea de configuración	Especificación
Dirección IPv4	209.165.200.238
Máscara de subred para IPv4	255.255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección IPv6/subred	201:db8:acad:a::38/64
Gateway predeterminado IPv6	2001:DB8:ACAD:2::1

Tabla 2.Configurar la computadora de Internet

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

Paso 1: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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

Tabla 3.Configurar R1

Nota: Todavía no configure G0/1.

R1

```
R1(config)#no ip domain-lookup
R1(config)#hostname R1
```

```
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd $Unauthorized Access is Prohibited!$
R1(config)#int s0/0/0
R1(config-if)#description connection R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64
R1(config-if)#clock rate 128000
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
R1(config)#ipv6 route ::/0 s0/0/0
```

Paso 2: Configurar R2

La configuración del R2 incluye las siguientes tareas:

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	service password-encryption
Habilitar el servidor HTTP	ip http server(código no aceptado en packet tracer)
Mensaje MOTD	banner motd $Unauthorized Access is Prohibited!$

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

Tabla 4.Configurar R2

R2:

```
Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#password cisco
R2(config-line)#login
```

```
R2(config-line)#line vty 0 15
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#ip http server
 ^

% Invalid input detected at '^' marker.
R2(config)#banner motd $Unauthorized Access is Prohibited!$
R2(config)#int s0/0/0
R2(config-if)#description connection R1
R2(config-if)#ip address 172.16.1.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
R2(config-if)#no shutdown
R2(config-if)#

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

R2(config-if)#int s0/0/1
R2(config-if)#description connection R3
R2(config-if)#ip address 172.16.2.2 255.255.255.252
R2(config-if)#ipv6 address 2001:DB8:ACAD:2::2/64
R2(config-if)#clock rate 128000
R2(config-if)#no shut
R2(config-if)#no shutdown

R2(config-if)#int g0/0
R2(config-if)#description connection to internet
R2(config-if)#ip address 209.165.200.233 255.255.255.248
R2(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
R2(config-if)#no shutdow
R2(config-if)#int loopback 0
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#description connection to simulated web server
R2(config-if)#exit

R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0
%Default route without gateway, if not a point-to-point interface, may impact
performance
R2(config)#ipv6 route ::/0 g0/0
```

Paso 3: Configurar R3

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	no ip domain-lookup
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	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	

Tabla 5. Configurar R3

R3

```
Router>enable
Router#conf
Router#configure t
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#line vty 0 15
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd $Unauthorized Access is Prohibited!$
R3(config)#int s0/0/1
R3(config-if)#description connection to R2
R3(config-if)#ip address 172.16.2.1 255.255.255.252
R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64
R3(config-if)#no shutdown
R3(config-if)#int loopback 4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#int loopback 7
R3(config-if)#ip address 2001:DB8:ACAD:3::1/64
R3(config-if)#int loopback 7
R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#exit
```

Paso 4: Configurar S1

La configuración del S1 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	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	
Mensaje MOTD	Se prohíbe el acceso no autorizado

Tabla 6.Configurar S1

S1

```
S1(config)#
S1(config)#no ip domain-lookup
S1(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd $Unauthorized Access is Prohibited!$
```

Paso 5: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	

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	service password-encryption
Mensaje MOTD	Se prohíbe el acceso no autorizado

Tabla 7.Configurar el S3

S3

```
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd $Unauthorized Access is Prohibited!$
```

Paso 6: Verificar la conectividad de la red

Utilice el comando **ping** para probar la conectividad entre los dispositivos de red. Utilice la siguiente tabla para verificar metódicamente la conectividad con cada dispositivo de red. Tome medidas correctivas para establecer la conectividad si alguna de las pruebas falla:

Desde	A	Dirección IP		Resultados de ping
R1	R2, S0/0/0	172.16.1.2		Success rate is 100 percent (5/5)

R2	R3, S0/0/1	172.16.2.1		Success rate is 100 percent (5/5)
PC de Internet	Gateway predeterminado	209.165.200.233		Ping statistics for 209.165.200.233

Tabla 8.Verificar la conectividad de la red

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

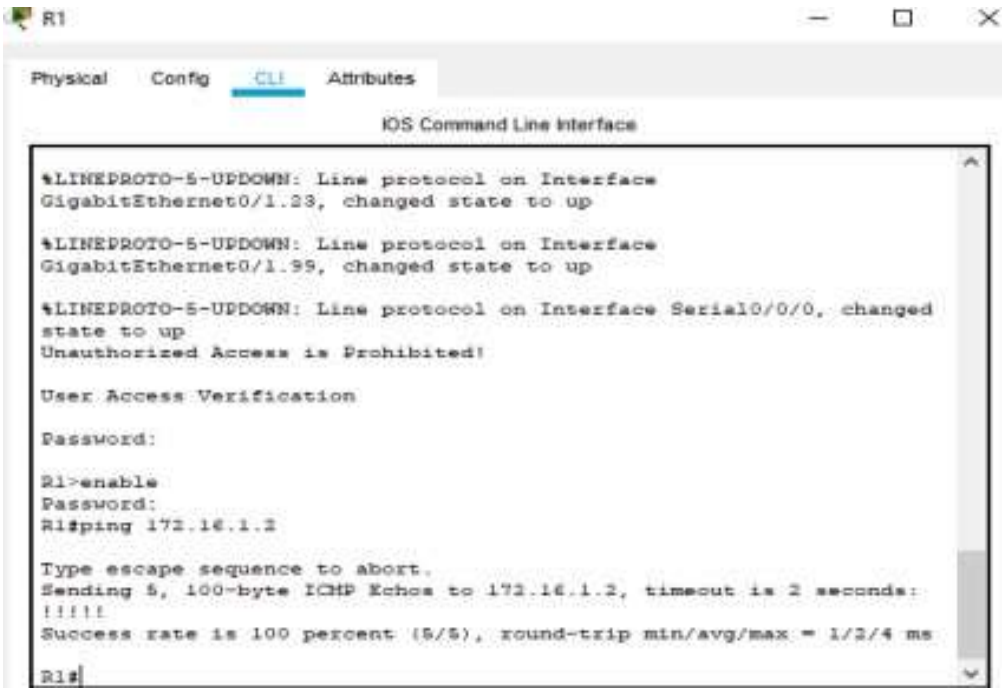


Ilustración 2.Ping R1

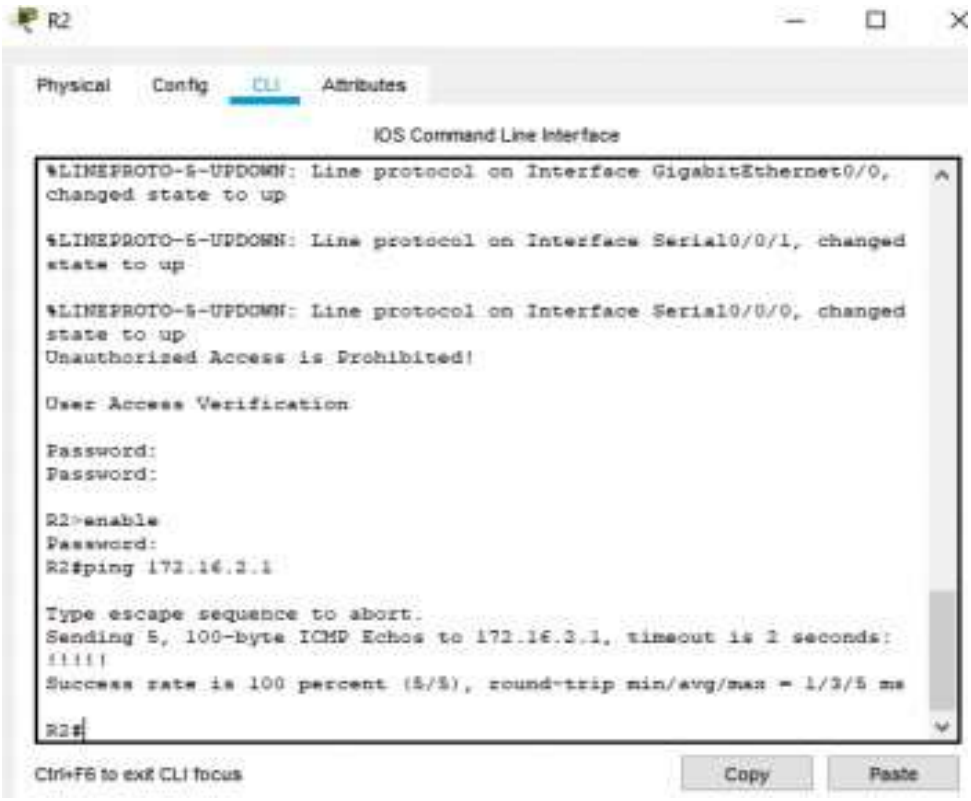


Ilustración 3 Ping R2

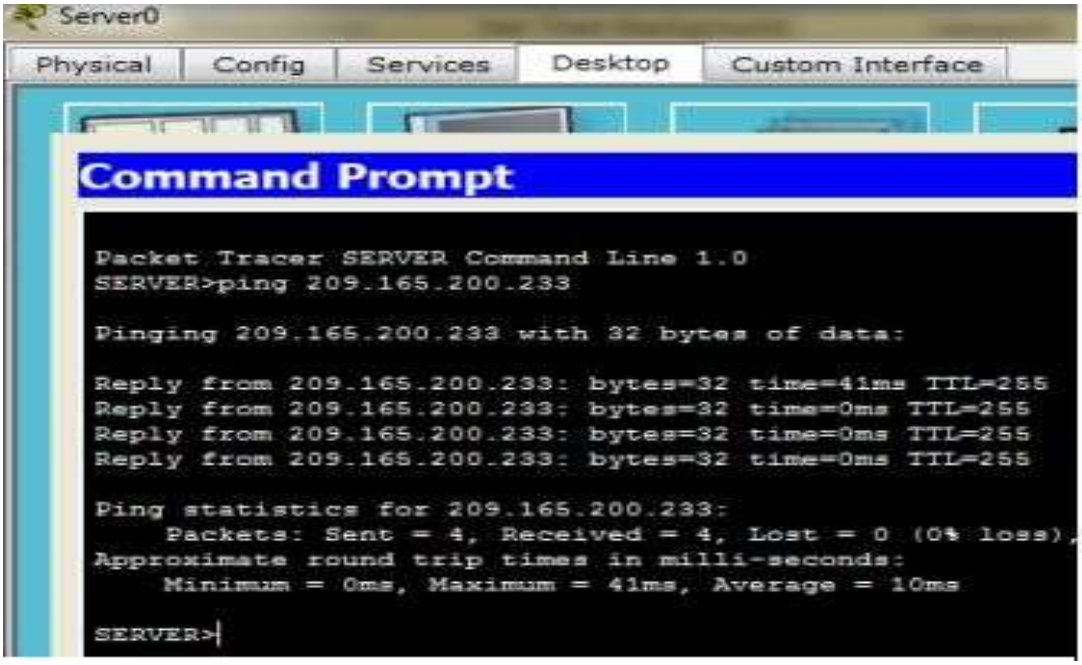


Ilustración 4.ping Web Server

Se inicializan los 3 routers y 2 switches con su configuración básica y se configura nombre, contraseñas de exec privilegiado, acceso de consola, acceso telnet, interfaces, rutas predeterminadas IPv4 y Ipv6 y mensaje MOTD. También se configuro el protocolo TCP/IP v4 en las computadoras para verificar la conectividad de la red

Parte2 Configurar la seguridad del switch, las VLAN y el routing entre VLAN

Paso 7: Configurar S1

La configuración del S1 incluye las siguientes tareas:

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	
Apagar todos los puertos sin usar	

Tabla 9.Configurar S1

S1

```
S1(config)#vlan 21
S1(config-vlan)#name contabilidad
S1(config-vlan)#vlan 23
S1(config-vlan)#vlan 21
S1(config-vlan)#name Contabilidad
```

```
S1(config-vlan)#vlan 23
S1(config-vlan)#name Ingenieria
S1(config-vlan)#vlan 99
S1(config-vlan)#name Administracion
S1(config-if)#exit
S1(config-if)#int vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#int range f0/1-2, f0/4, f0/7-24, g0/1-2
S1(config-if-range)#shutdown
```

Paso 8: Configurar el S3

La configuración del S3 incluye las siguientes tareas:

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	
Apagar todos los puertos sin usar	

Tabla 10.Configurar el S3

S3

```
S3(config)#vlan 21
S3(config-vlan)#name  contabilidad
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown
```

Paso 9: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	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	

Tabla 11.Configurar R1

R1

```
R1(config)#int g0/1.21
R1(config-subif)#description vlan 21
R1(config-subif)#encapsulation dot1Q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/1.23
R1(config-subif)#description vlan 23
R1(config-subif)#encapsulation dot1Q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#int g0/1.99
R1(config-subif)#description vlan 99
R1(config-subif)#encapsulation dot1Q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#int g0/1
R1(config-subif)#no shutdown
```

Paso 10: Verificar la conectividad de la red

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

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

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

Tabla 12.Verificar la conectividad de la red

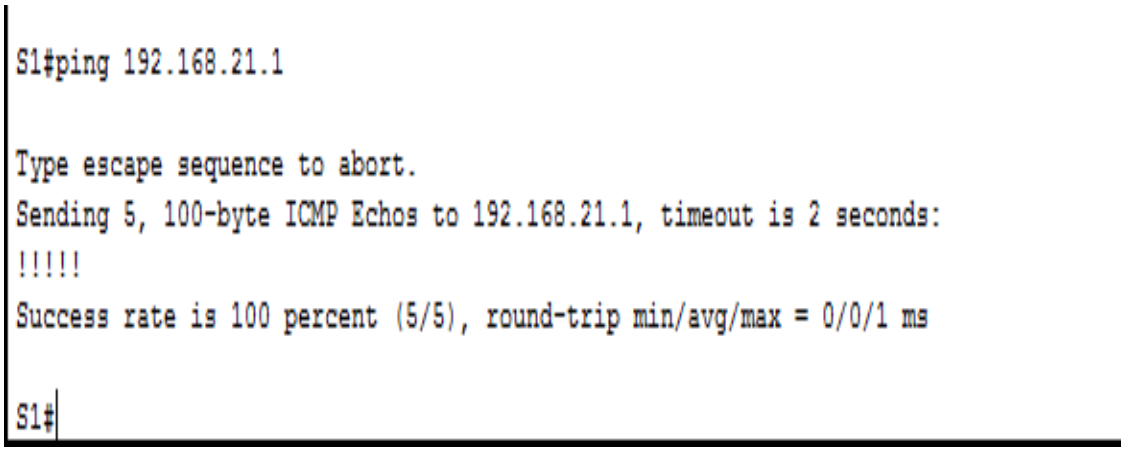


Ilustración 5.Ping S1

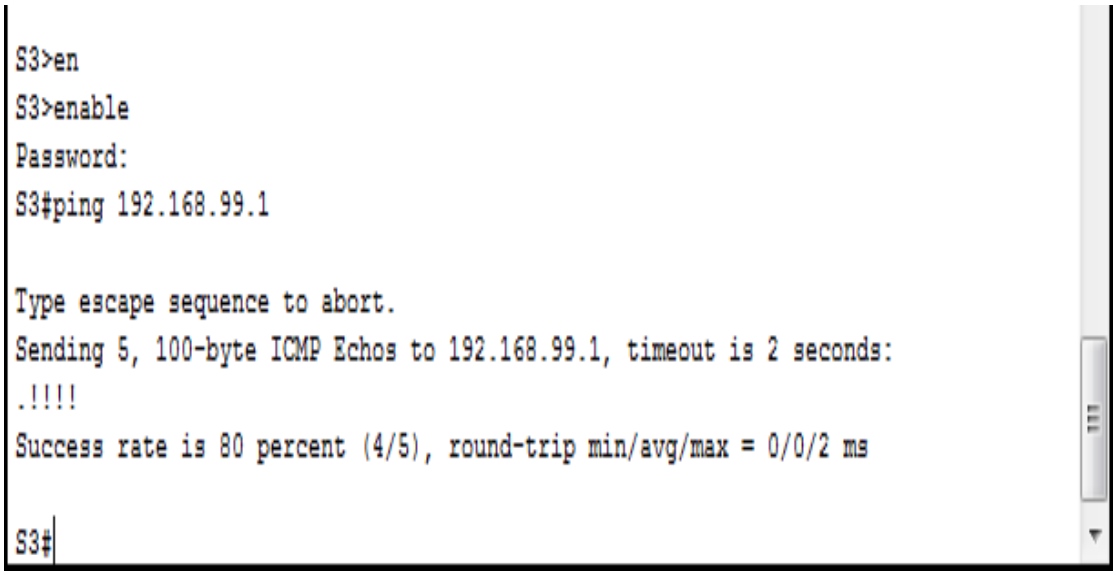


Ilustración 6.Ping.S3

En los 2 switches se crearon la base de datos de VLAN, se asignó la dirección IP de administración, Gateway, se forzó el enlace troncal en la interfaz, se apagan los puertos sin usar y los demás puertos se configuran como puertos de acceso. Se configura y se asignan las VLAN21, VLAN23 y VLAN99 en G0/1 en el router No. 1 y se verifico la conectividad entre los switches y el router 1 a través del comando ping

Parte3 Configurar el protocolo de routing dinámico RIPv2

Paso 11: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	Asigne todas las redes conectadas directamente.
Establecer todas las interfaces LAN como pasivas	
Desactive la sumarización automática	no auto-summary

Tabla 13.Configurar RIPv2 en el R1

R1

```
R1(config-router)#exit
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#do show ip route connected
 C   172.16.1.0/30 is directly connected, Serial0/0/0
 C   192.168.21.0/24  is directly connected, GigabitEthernet0/1.21
 C   192.168.23.0/24  is directly connected, GigabitEthernet0/1.23
 C   192.168.99.0/24  is directly connected, GigabitEthernet0/1.99

R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary
```

Paso 12: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	
Anunciar las redes conectadas directamente	**Nota:** Omitir la red G0/0.
Establecer la interfaz LAN (loopback) como pasiva	
Desactive la sumarización automática.	

Tabla 14.Configurar RIPv2 en el R2

R2

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#do show ip route connected
 C   10.10.10.10/32 is directly connected, Loopback0
 C   172.16.1.0/30 is directly connected, Serial0/0/0
 C   172.16.2.0/30 is directly connected, Serial0/0/1
 C   209.165.200.232/29 is directly connected, GigabitEthernet0/0
R2(config-router)#network 10.10.10.10
```

R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#passive-interface loopback 0
R2(config-router)#no auto-sumary

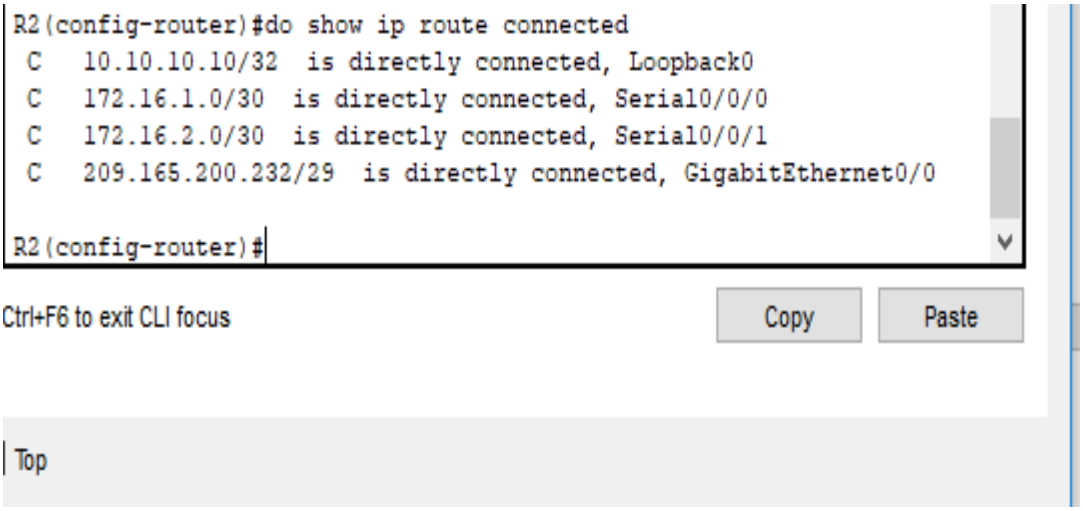


Ilustración 7.Comando show ip route R2

Paso 13: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Configurar RIP versión 2	R2(config)#ip access-list standard ADMIN-MGT R2(config-std-nacl)#permit host 172.16.1.1
Anunciar redes IPv4 conectadas directamente	R2(config)#line vty 0 4 R2(config-line)#access-class ADMIN-MGT in
Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas	R2(config-line)#transport input telnet
Desactive la sumarización automática.	

Tabla 15.Configurar RIPv3 en el R2

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#do show ip route connected
 C   172.16.2.0/30 is directly connected, Serial0/0/1
C   192.168.4.0/24 is directly connected, Loopback4
C   192.168.5.0/24 is directly connected, Loopback5
C   192.168.6.0/24 is directly connected, Loopback6
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)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary
```

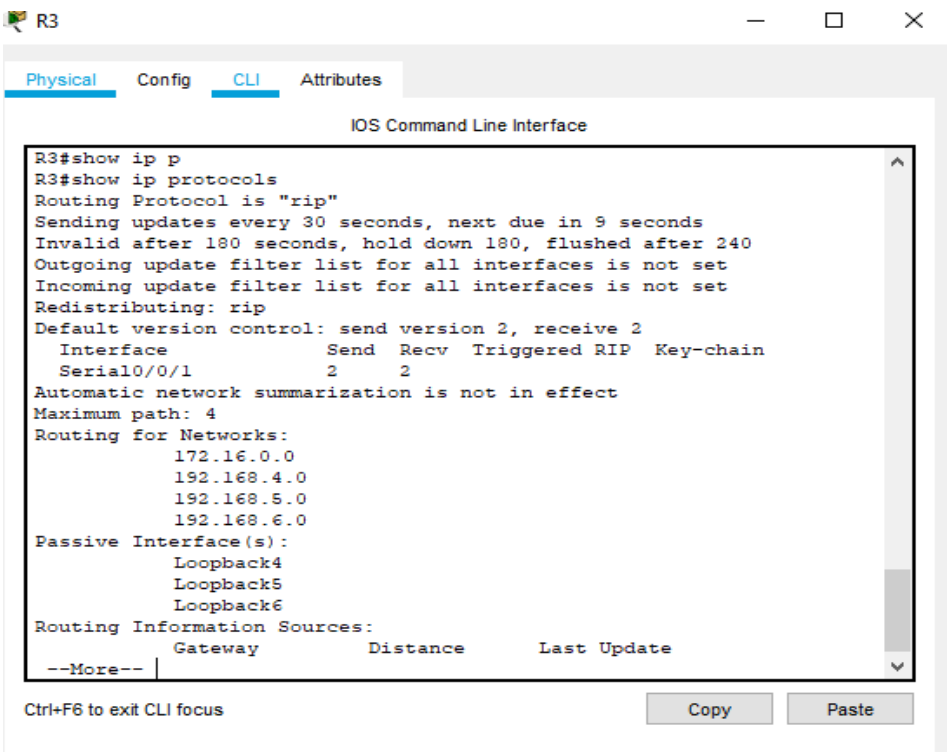


Ilustración 8.Show protocols

Paso 14: Verificar la información de RIP

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

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

Tabla 16.Verificar la información de RIP

Se realizo la configuración del Protocolo de enrutamiento vector distancia RIPv2 en cada uno de los 3 routers permitiendo él envió de información de la máscara de subred con la actualización de la ruta.

Parte4 Implementar DHCP y NAT para IPv4

Paso 15: Configurar el R1 como servidor de DHCP para las VLAN 21 y 23

Las tareas de configuración para R1 incluyen las siguientes:

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas	
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas	
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

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

R1

```
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
```

```
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
R1(dhcp-config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#domain-name ccna-sa.com
```

Paso 16: CONFIGURAR LA NAT ESTÁTICA Y DINÁMICA EN EL R2

La configuración del R2 incluye las siguientes tareas:

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Nombre de usuario: **webuser** Contraseña: **cisco12345** Nivel de privilegio: **15**
Habilitar el servicio del servidor HTTP	No lo acepta el packet tracer
Configurar el servidor HTTP para utilizar la base de datos local para la autenticación	
Crear una NAT estática al servidor web.	Dirección global interna: **209.165.200.229**
Asignar la interfaz interna y externa para la NAT estática	
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	

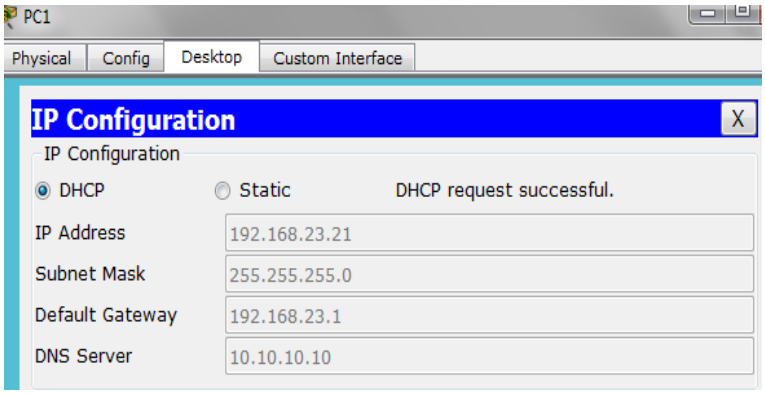
Tabla 18.Configurar la NAT estática y dinámica en el R2

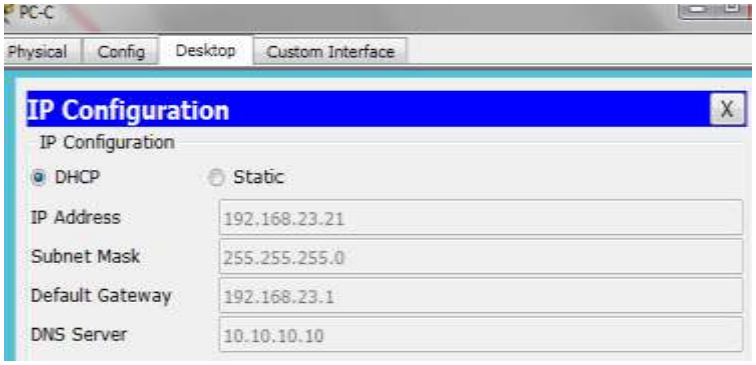
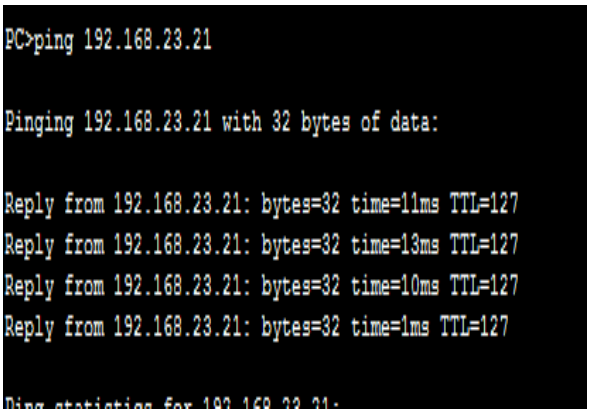
R2

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
```

Paso 17: Verificar el protocolo DHCP y la NAT estática

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

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor de DHCP	 Ilustración 9.PC-A _DHCP

Verificar que la PC-C haya adquirido información de IP del servidor de DHCP	 Ilustración 10.PC-C –DHCP
Verificar que la PC-A pueda hacer ping a la PC-C .	 Ilustración 11.Ping PC-A a PC-C

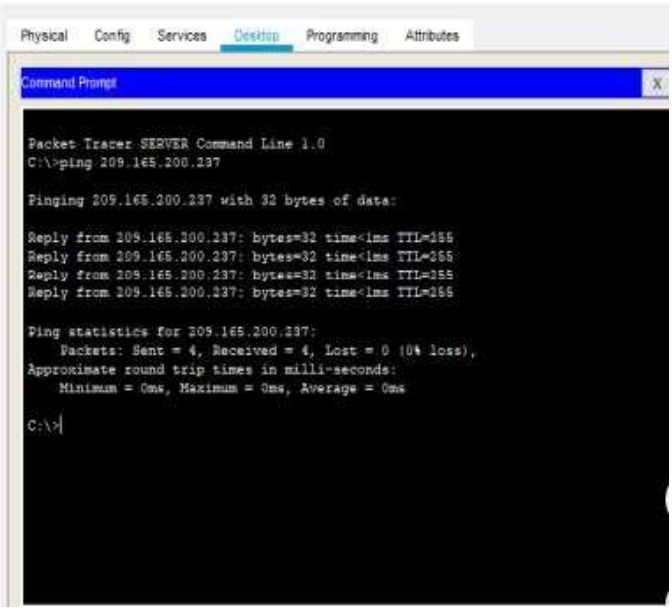
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.229) Iniciar sesión con el nombre de usuario: webuser y la contraseña: cisco12345	 Ilustración 12.Navegador web  Ilustración 13.Ping de ip server

Tabla 19.Verificar el protocolo DHCP y la NAT estática

Se implemento en el router 1 como servidor DHCP reservando las primeras 20 direcciones IP de las VLAN 21 y VLAN 23 para configuraciones estáticas y en el router 2 se asignó la interfaz interna y externa para la NAT estática y se configura la NAT dinámica dentro de una ACL privada.

Parte5 Configurar NTP

Elemento o tarea deconfiguración	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.	
Verifique la configuración de NTP en R1.	

Tabla 20.Configurar NTP

R2

R2#clock set 9:00:00 5 march 2016
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ntp master 5
R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R1(config)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#show ntp associations
address ref clock st when poll reach delay offset disp
~172.16.1.2 127.127.1.1 5 1 16 17 6.00
726184533724.00 0.12
* sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
Utilizando el protocolo NTP se configuro el router 2 como maestro y el router 1 como cliente con el fin de sincronizar los dispositivos que funcionan en una red en la cual se sincroniza la fecha y hora del servidor

Parte6 Configurar y verificar las listas de control de acceso (ACL)

Paso 18: Restringir el acceso a las líneas VTY en el R2

Elemento o tarea deconfiguración	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	
Permitir acceso por Telnet a las líneas de VTY	

Verificar que la ACL funcione como se espera	

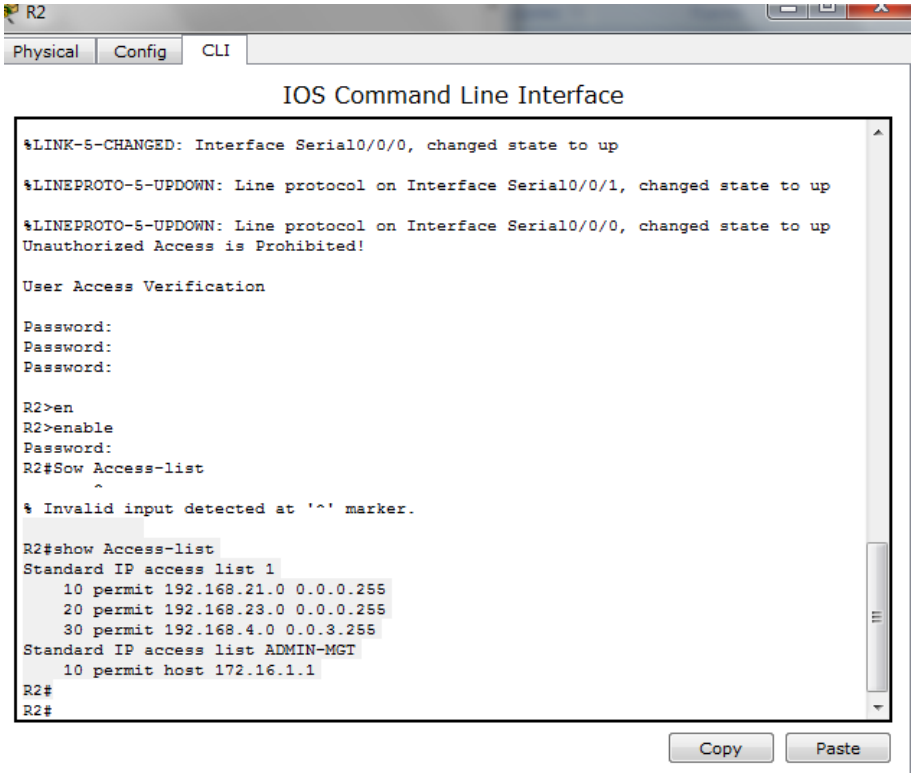
Tabla 21.Restringir el acceso a las líneas VTY en el R2

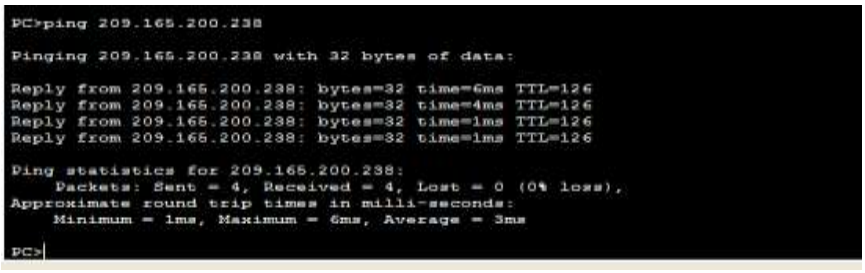
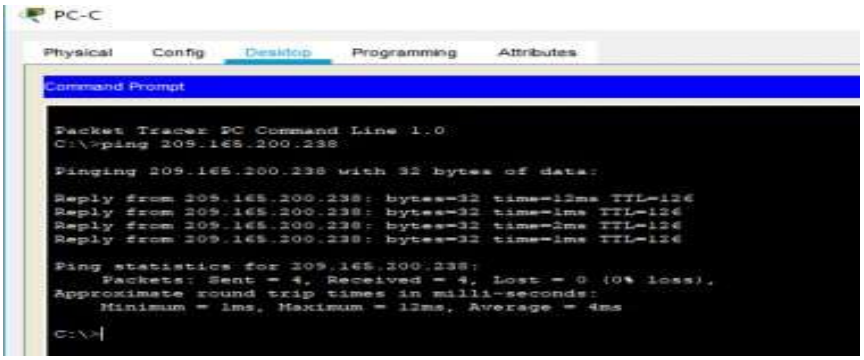
R2

```
R2(config)#ip access-list standard ADMIN-MGT
R2(config-std-nacl)#permit host 172.16.1.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 15
R2(config-line)#access-class ADMIN-MGT in
R2(config-line)#transport input telnet
```

R1

```
R1>enable
Password:
R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenUnauthorized Access is Prohibited!
User Access Verification
Password:
R2>exit
[Connection to 172.16.1.2 closed by foreign host]
R1#
R3>enable
Password:
R3#telnet 172.16.1.2
Trying 172.16.1.2 ...
% Connection refused by remote host
R3#Introducir el comando de CLI adecuado que se necesita para mostrar lo
siguiente
```

Descripción del comando	Entrada del estudiante (comando)
Mostrar las coincidencias recibidas por una lista de acceso desde la última vez que se restableció	Acceso CLI R2#show ip access-lists  Ilustración 14.Show Access-list
Restablecer los contadores de una lista de acceso	R2#clear access-list counters ip
¿Qué comando se usa para mostrar qué ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface

¿Con qué comando se muestran las traducciones NAT?	R2#show ip nat translations  Ilustración 15.Ping PC-A o la PC-C  Ilustración 16.Ping-209.165.200.238  Ilustración 17.Navegador **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?	R2#clear ip nat translation *

Tabla 22.comando de CLI

Utilizando la lista de control de acceso se logró configurar el tráfico de red que entra y sale de la interfaz del router 1 y 2, logrando que esta lista le diga al router 1 y 2 que paquetes son permitidos, denegados y se verifico su funcionamiento correcto

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.

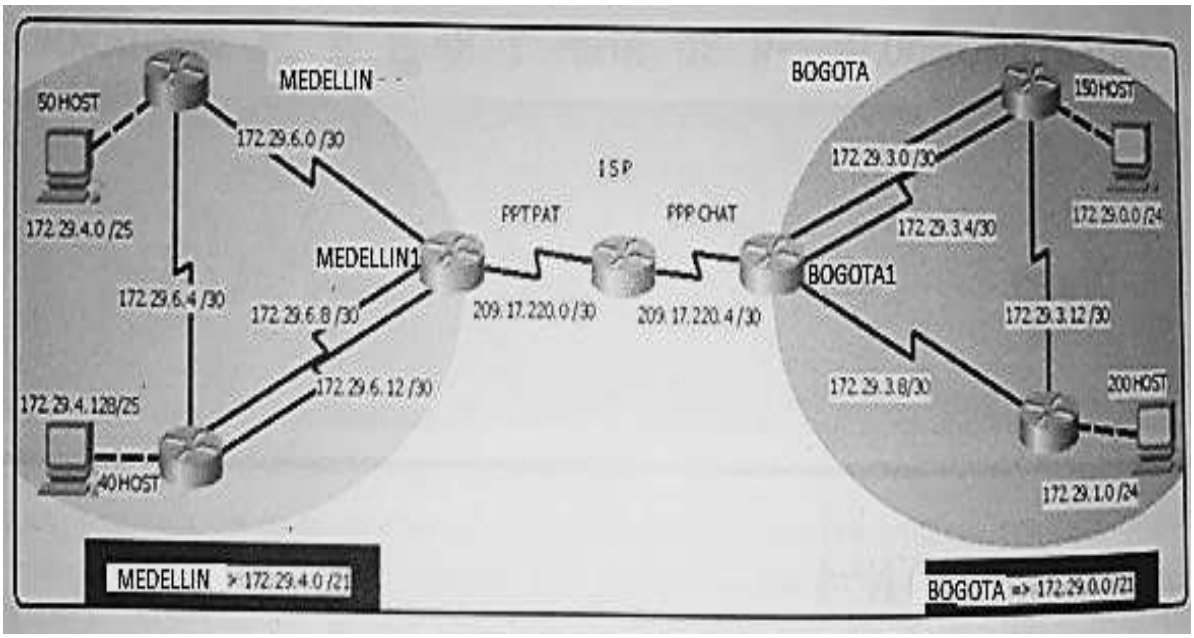


Ilustración 18.Escenario 2. Topología Red

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

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

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

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

Realizar 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.

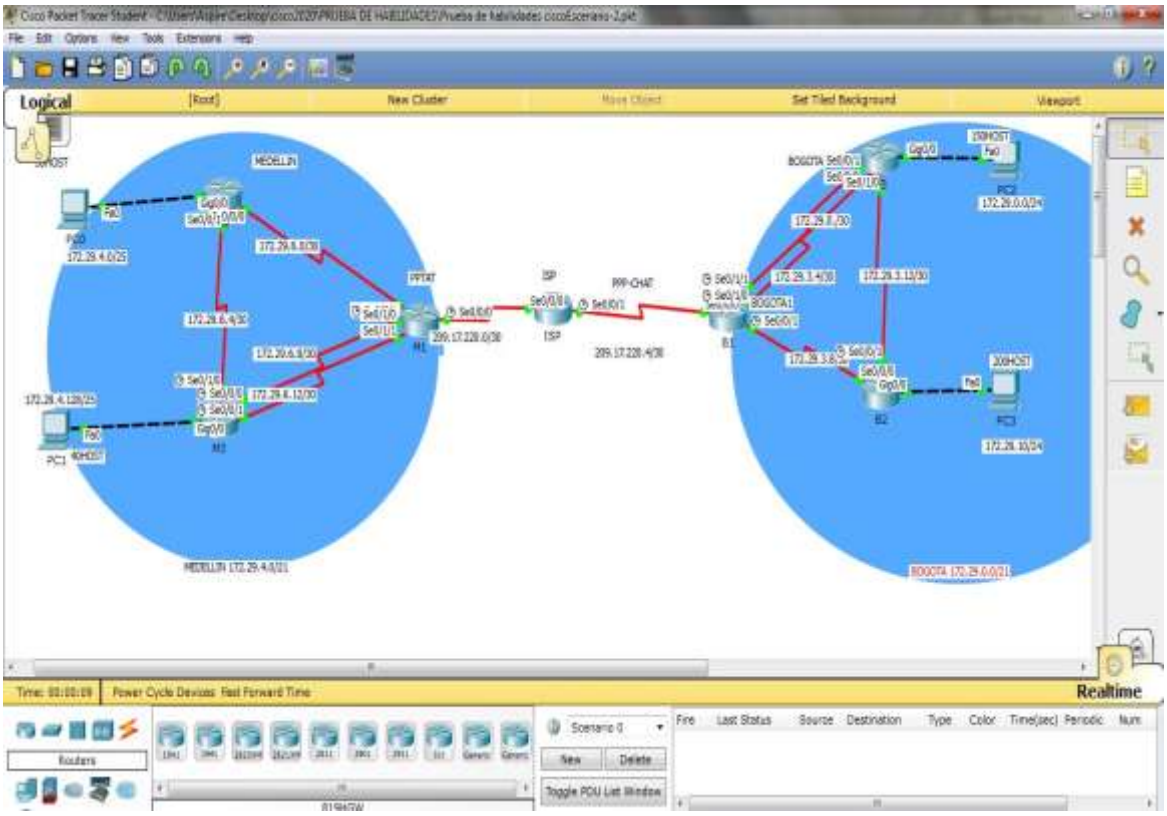


Ilustración 19.conexión física de los equipos con base en la topología

EQUIPOS	SERIAL	DIRECCIONES IP
MEDELLIN1 MEDELLIN2	0/0/1 0/0/0	172.29.6.1/30 172.29.6.2/30
MEDELLIN1 MEDELLIN3	0/1/1 0/0/1	172.29.6.13/30 172.29.6.14/30
MEDELLIN1 MEDELLIN3	0/1/0 0/0/0	172.29.6.9/30 172.29.6.10/30
MEDELLIN1 ISP	0/0/0 0/0/0	209.17.220.1/30 209.17.220.2/30
BOGOTA 1 BOGOTA2	0/0/1 0/0/0	172.29.3.9/30 172.29.3.10/30
BOGOTA 1 BOGOTA3	0/1/1 0/0/1	172.29.3.1/30 172.29.3.2/30
BOGOTA 1	0/0/1	172.29.3.13/30

BOGOTA3	0/1/0	172.29.3.14/30
BOGOTA 1 ISP	0/0/0 0/0/1	209.17.220.5/30 209.17.220.6/30

Tabla 23.conexión física de equipos con base en la topología

Configuración basica para cada uno de los router ISP

```
ISP>ENABLE
ISP#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#hostname ISP
ISP(config)#no ip domain-lookup
ISP(config)#service password-encryption
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#LINE VTY 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
```

MEDELLIN1

```
MEDELLIN>ENABLE
MEDELLIN#CONF T
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN(config)#hostname MEDELLIN1
MEDELLIN1(config)#no ip domain-lookup
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#LINE VTY 0 15
MEDELLIN1(config-line)#password cisco
      MEDELLIN1(config-line)#login
```

MEDELLIN2

```
MEDELLIN>enable
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#hostname MEDELLIN2
MEDELLIN2(config)#no ip domain-lookup
MEDELLIN2(config)#service password-encryption
```

MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#LINE VTY 0 15
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login

MEDELLIN3

MEDELLIN>enable
MEDELLIN#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#hostname MEDELLIN3
MEDELLIN3(config)#no ip domain-lookup
MEDELLIN3(config)#service password-encryption
MEDELLIN3(config)#enable secret class
MEDELLIN3(config)#line console 0
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#LINE VTY 0 15
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login

BOGOTA1

BOGOTA>ENABLE
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA1
BOGOTA1(config)#no ip domain-lookup
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#enable secret class
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#LINE VTY 0 15
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login

BOGOTA2

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#hostname BOGOTA2
BOGOTA2(config)#no ip domain-lookup
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#enable secret class
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#LINE VTY 0 15
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login

BOGOTA3

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA3
BOGOTA3(config)#no ip domain-lookup
BOGOTA3(config)#service password-encryption
BOGOTA3(config)#enable secret class
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#LINE VTY 0 15
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login

CONEXIÓN

MEDELLIN1

MEDELLIN1(config)#interface s0/1/1
MEDELLIN1(config-if)#ip address 172.29.6.13 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#interface s0/1/0
MEDELLIN1(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#interface s0/0/1
MEDELLIN1(config-if)#ip address 172.29.6.1 255.255.255.252
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown
MEDELLIN1(config-if)#interface s0/0/0
MEDELLIN1(config-if)#ip address 209.17.220.1 255.255.255.252

```
MEDELLIN1(config-if)#clock rate 128000
MEDELLIN1(config-if)#no shutdown
```

MEDELLIN 2

```
MEDELLIN2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#interface g0/0
MEDELLIN2(config-if)#ip address 172.29.4.1 255.255.255.128
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#interface s0/0/0
MEDELLIN2(config-if)#ip address 172.29.6.2 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shutdown
MEDELLIN2(config-if)#interface s0/0/1
MEDELLIN2(config-if)#ip address 172.29.6.5 255.255.255.252
MEDELLIN2(config-if)#clock rate 128000
MEDELLIN2(config-if)#no shutdown
```

MEDELLIN3

```
MEDELLIN3(config)#interface g 0/0
MEDELLIN3(config-if)#ip address 172.29.4.129 255.255.255.128
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#interface serial 0/1/0
MEDELLIN3(config-if)#ip address 172.29.6.6  255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#interface serial 0/0/0
MEDELLIN3(config-if)#ip address 172.29.6.9 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#interface serial 0/0/1
MEDELLIN3(config-if)#ip address 172.29.6.14 255.255.255.252
MEDELLIN3(config-if)#clock rate 128000
MEDELLIN3(config-if)#no shutdown
MEDELLIN3(config-if)#
```

ISP

```
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#interface s0/0/0
```

```
ISP(config-if)#ip address 209.17.220.1 255.255.255.252
ISP(config-if)#no shutdown
ISP(config-if)#interface s0/0/1
ISP(config-if)#ip address 209.17.220.5 255.255.255.252
ISP(config-if)#no shutdown
```

BOGOTA 1

```
BOGOTA1#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA1(config)#interface s0/0/0
BOGOTA1(config-if)#ip address 209.17.220.6 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#interface s0/1/1
BOGOTA1(config-if)#ip address 172.29.3.5 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#interface s0/1/0
BOGOTA1(config-if)#ip address 172.29.3.1 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#interface s0/0/1
BOGOTA1(config-if)#ip address 172.29.3.9 255.255.255.252
BOGOTA1(config-if)#clock rate 128000
BOGOTA1(config-if)#no shutdown
BOGOTA1(config-if)#
```

BOGOTA 2

```
BOGOTA2#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#interface s0/0/0
BOGOTA2(config-if)#ip address 172.29.3.10 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#interface s0/0/1
BOGOTA2(config-if)#ip address 172.29.3.13 255.255.255.252
BOGOTA2(config-if)#clock rate 128000
BOGOTA2(config-if)#no shutdown
BOGOTA2(config-if)#interface g0/0
BOGOTA2(config-if)#ip address 172.29.1.1 255.255.255.128
BOGOTA2(config-if)#no shutdown
```

BOGOTA 3

```
BOGOTA3(config)#interface g0/0
BOGOTA3(config-if)#ip address 172.29.0.1 255.255.255.218
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#interface s0/0/0
BOGOTA3(config-if)#ip address 172.29.3.2 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#interface s0/0/1
BOGOTA3(config-if)#ip address 172.29.3.6 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#interface s0/1/0
BOGOTA3(config-if)#ip address 172.29.3.14 255.255.255.252
BOGOTA3(config-if)#clock rate 128000
BOGOTA3(config-if)#no shutdown
BOGOTA3(config-if)#
```

Parte 1: Configuración del enrutamiento

Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

MEDELLIN1

```
Medellin1(config)#router ospf 1
Medellin1(config-router)#router-id 1.1.1.1
Medellin1(config-router)#no auto-summary
Medellin1(config-router)#network 209.17.220.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.0 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.8 0.0.0.3 area 0
Medellin1(config-router)#network 172.29.6.12 0.0.0.3 area 0
Medellin1(config-router)#passive-interface gigabitEthernet 0/0
```

MEDELLIN 2

```
MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#router-id 2.2.2.2
MEDELLIN2(config-router)#no auto-summary
MEDELLIN2(config-router)#network 172.29.6.0 0.0.0.3 area 0
MEDELLIN2(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN2(config-router)#passive-interface GigabitEthernet0/0
```

MEDELLIN 3

```
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#router-id 3.3.3.3
MEDELLIN3 (config-router)#no auto-summary
MEDELLIN3(config-router)#network 172.29.6.8 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.12 0.0.0.3 area 0
MEDELLIN3(config-router)#network 172.29.6.4 0.0.0.3 area 0
MEDELLIN3(config-router)#passive-interface GigabitEthernet0/0
```

ISP

```
ISP#config t
Enter configuration commands, one per line. End with CNTL/Z.
ISP(config)#router ospf 1
ISP(config)# router-id 2.2.2.2
ISP(config-router)#no auto-summary
ISP(config-router)#network 209.17.220.1 0.0.0.3 area 0
ISP(config-router)#network 209.17.220.5 0.0.0.3 area 0
ISP(config-router)#exit
```

BOGOTA 1

```
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#router-id 1.1.1.1
BOGOTA1(config-router)#no auto-summary
BOGOTA1(config-router)#network 172.28.3.8 0.0.0.3 area 0
BOGOTA1(config-router)#network 209.17.220.4 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.28.3.0 0.0.0.3 area 0
BOGOTA1(config-router)#network 172.28.3.4 0.0.0.3 area 0
Bogota1(config-router)#passive-interface gigabitEthernet 0/0
```

BOGOTA 2

```
BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#router-id 2.2.2.2
BOGOTA2 (config-router)#no auto-summary
BOGOTA2(config-router)#network 172.29.3.8 0.0.0.3 area 0
BOGOTA2(config-router)#network 172.29.3.12 0.0.0.3 area 0
BOGOTA2(config-router)#passive-interface GigabitEthernet0/0
```

BOGOTA 3

```
BOGOTA3(config)#router ospf 1
```

```
BOGOTA3(config-router)#router-id 3.3.3.3
BOGOTA3 (config-router)#no auto-summary
BOGOTA3(config-router)#network 172.29.3.12 0.0.0.3 area 0
BOGOTA3(config-router)#network 172.29.3.4 0.0.0.3 area 0
BOGOTA3(config-router)#network 172.29.3.0 0.0.0.3 area 0
BOGOTA3(config-router)#passive-interface GigabitEthernet0/0
BOGOTA3(config-router)#
```

Los routers Bogota1 y Medellín 1 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

```
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
```

MEDELLIN 1

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
```

a. 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

```
ISP(config)#ip route 172.29.4.0 255.255.252.0 209.17.220.2
ISP(config)#ip route 172.29.0.0 255.255.255.0 209.17.220.6
```

Se utilizo el protocolo de enrutamiento del estado de enlace OSPF para que varias áreas se conecten a un área de distribución y además los routers mantendrán la tabla de enrutamiento, una base de datos de adyacencia y una base de datos topológica

Parte 2: Tabla de Enrutamiento.

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

MEDELLIN1

```
MEDELLIN1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

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

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 7 subnets, 2 masks
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] vía 172.29.6.2, 00:04:30, Serial0/0/1
[110/128] vía 172.29.6.9, 00:04:30, Serial0/1/0
C 172.29.6.8/30 is directly connected, Serial0/1/0
L 172.29.6.9/32 is directly connected, Serial0/1/0
C 172.29.6.12/30 is directly connected, Serial0/1/1
L 172.29.6.13/32 is directly connected, Serial0/1/1
209.17.220.0/24 is variably subnetted, 2 subnets, 2 masks
C 209.17.220.0/30 is directly connected, Serial0/0/0
L 209.17.220.1/32 is directly connected, Serial0/0/0
MEDELLIN1#
MEDELLIN2
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 not set

172.29.0.0/16 is variably subnetted, 8 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
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
O 172.29.6.8/30 [110/128] vía 172.29.6.6, 00:04:26, Serial0/0/1
O 172.29.6.12/30 [110/128] vía 172.29.6.6, 00:04:26, Serial0/0/1
MEDELLIN2#
MEDELLIN3

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 not set

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
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] vía 172.29.6.9, 00:05:05, Serial0/0/0
[110/128] vía 172.29.6.5, 00:05:05, 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 172.29.6.9/32 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
209.17.220.0/30 is subnetted, 1 subnets
O 209.17.220.0/30 [110/128] via 172.29.6.9, 00:05:15, Serial0/0/0
MEDELLIN3#
MEDELLIN3#
ISP
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

172.29.0.0/16 is variably subnetted, 4 subnets, 3 masks
S 172.29.0.0/24 [1/0] via 209.17.220.6
S 172.29.4.0/22 [1/0] vía 209.17.220.2
O 172.29.6.8/30 [110/128] vía 209.17.220.1, 00:03:22, Serial0/0/0
O 172.29.6.12/30 [110/128] via 209.17.220.1, 00:03:22, Serial0/0/0
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#
BOGOTA1
BOGOTA1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C 172.29.3.0/30 is directly connected, Serial0/1/0
L 172.29.3.1/32 is directly connected, Serial0/1/0
C 172.29.3.4/30 is directly connected, Serial0/1/1
L 172.29.3.5/32 is directly connected, Serial0/1/1
C 172.29.3.8/30 is directly connected, Serial0/0/1
L 172.29.3.9/32 is directly connected, Serial0/0/1
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
BOGOTA1#
BOGOTA2

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

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks
C 172.29.1.0/25 is directly connected, GigabitEthernet0/0
L 172.29.1.1/32 is directly connected, GigabitEthernet0/0
O 172.29.3.0/30 [110/128] vía 172.29.3.14, 00:04:04, Serial0/0/1
O 172.29.3.4/30 [110/128] vía 172.29.3.14, 00:04:04, 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 172.29.3.13/32 is directly connected, Serial0/0/1
BOGOTA2#

BOGOTA3

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

Gateway of last resort is not set

172.29.0.0/16 is variably subnetted, 7 subnets, 2 masks
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 172.29.3.13, 00:04:39, 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
BOGOTA3#

Verificar el balanceo de carga que presentan los routers.

MEDELLIN1

MEDELLIN1#show ip route ospf
    172.29.0.0/16 is variably subnetted, 7 subnets, 2 masks
O   172.29.6.4 [110/128] via 172.29.6.2, 00:07:47, Serial0/0/1
                [110/128] via 172.29.6.9, 00:07:47, Serial0/1/0

MEDELIN2

MEDELLIN2#show ip route ospf
    172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks
O   172.29.6.8 [110/128] via 172.29.6.6, 00:07:56, Serial0/0/1
172.29.6.12 [110/128] via 172.29.6.6, 00:07:56, Serial0/0/1

MEDELLIN3

MEDELLIN3#show ip route ospf

```
    172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
O       172.29.6.0 [110/128] via 172.29.6.9, 00:08:29, Serial0/0/0
                   [110/128] via 172.29.6.5, 00:08:29, Serial0/1/0
209.17.220.0/30 is subnetted, 1 subnets
O       209.17.220.0 [110/128] via 172.29.6.9, 00:08:39, Serial0/0/0
MEDELLIN3#
```

BOGOTA2

```
BOGOTA2#show ip route ospf
    172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks
O       172.29.3.0 [110/128] via 172.29.3.14, 00:07:38, Serial0/0/1
O       172.29.3.4 [110/128] vía 172.29.3.14, 00:07:38, Serial0/0/1
BOGOTA2#
```

BOGOTA3

```
BOGOTA3#show ip route OSPF
172.29.0.0/16 is variably subnetted, 7 subnets, 2 masks
O       172.29.3.8 [110/128] via 172.29.3.13, 00:07:59, Serial0/1/0
BOGOTA3#
```

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.

MEDELLIN1

```
MEDELLIN1#show ip route ospf
    172.29.0.0/16 is variably subnetted, 7 subnets, 2 masks
O       172.29.6.4 [110/128] via 172.29.6.2, 00:07:47, Serial0/0/1
                   [110/128] via 172.29.6.9, 00:07:47, Serial0/1/0
```

BOGOTA1

```
BOGOTA1#show ip route ospf
 172.29.0.0/16 is variably subnetted, 7 subnets, 2 masks
O 172.29.3.12 [110/128] via 172.29.3.10, 03:42:44, Serial0/1/1
 [110/128] via 172.29.3.2, 03:42:44, Serial0/0/1
```

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

.

MEDELLIN 2

172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks
O 172.29.6.8 [110/128] via 172.29.6.6, 00:07:56, Serial0/0/1
O 172.29.6.12 [110/128] via 172.29.6.6, 00:07:56, Serial0/0/1
BOGOTA2
172.29.0.0/16 is variably subnetted, 8 subnets, 3 masks
O 172.29.3.0 [110/128] via 172.29.3.14, 00:07:38, Serial0/0/1
O 172.29.3.4 [110/128] via 172.29.3.14, 00:07:38, Serial0/0/1
BOGOTA2#

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

ISP

172.29.0.0 /16 is variably subnetted, 4 subnets, 3 masks
O 172.29.6.8 [110/128] via 209.17.220.1, 00:14:25, Serial0/0/0
O 172.29.6.12 [110/128] via 209.17.220.1, 00:14:25, Serial0/0/0
ISP#

Cuando un router inicia un proceso de enrutamiento OSPF en una interfaz envía un paquete y continúa enviándolos en intervalos regulares de tiempo y cuando los router son adyacentes deben estar en su estado completo antes de crear tablas de enrutamiento y enrutar el trafico

Parte 3: Deshabilitar la propagación del protocolo OSPF.

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

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

Tabla 24.Deshabilitar la propagación del protocolo OSPF

MEDELLIN1

MEDELLIN1#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#passive-interface serial 0/0/0
MEDELLIN1(config-router)#passive-interface serial 0/0/1
MEDELLIN1(config-router)#passive-interface serial 0/1/1

MEDELLIN 2

MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#passive-interface s0/0/0
MEDELLIN2(config-router)#
MEDELLIN2(config-router)#passive-interface s0/0/1
MEDELLIN2(config-router)#

MEDELLIN 3

MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#passive-interface serial 0/0/0
MEDELLIN3(config-router)#passive-interface serial 0/0/1
MEDELLIN3(config-router)#passive-interface serial 0/1/0

BOGOTA 1

BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#passive-interface serial 0/0/1
BOGOTA1(config-router)#passive-interface serial 0/1/1
BOGOTA1(config-router)#passive-interface serial 0/1/0

BOGOTA 2

BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#passive-interface SERIAL0/0/0
BOGOTA2(config-router)#passive-interface SERIAL0/0/1
BOGOTA3
BOGOTA3(config)#router ospf 1
BOGOTA3(config-router)#passive-interface serial 0/0/0
BOGOTA3(config-router)#passive-interface serial 0/1/0
Bogota3(config-router)#passive-interface serial 0/0/0

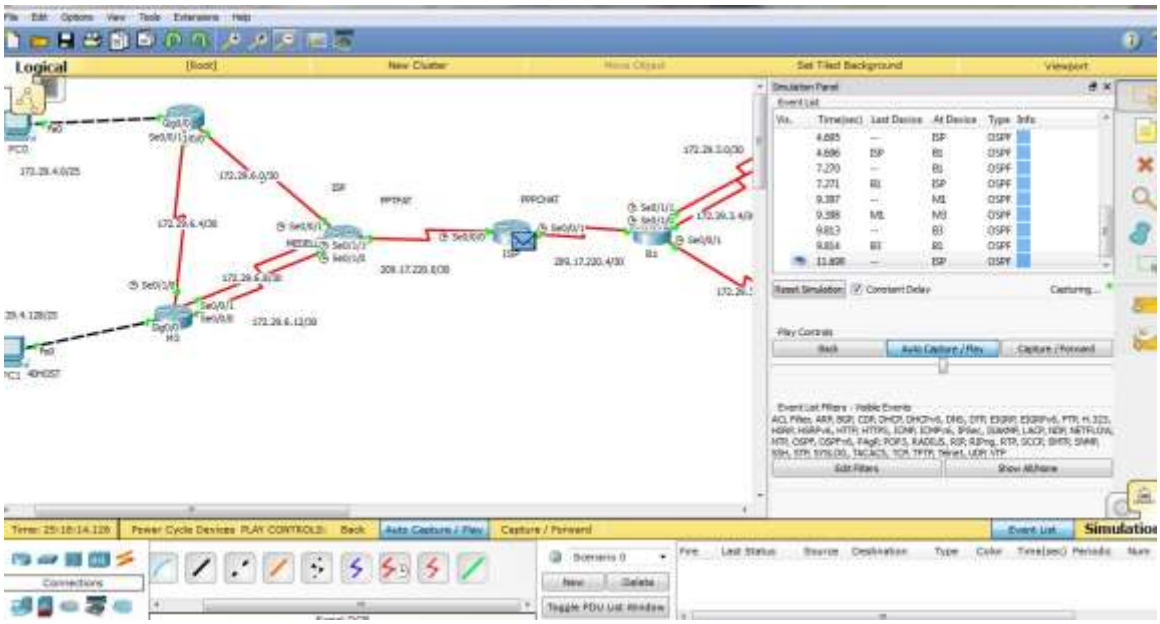


Ilustración 20.OSPF Deshabilitado

Se deshabilita la propagación del protocolo OSPF utilizando el modo de pasivado de interfaces con el propósito de optimizar el uso del ancho de banda de nuestros enlaces y reduciendo el uso de la CPU de nuestros dispositivos

Parte 4: Verificación del protocolo OSPF.

Verificar y documentar las opciones de enrutamiento configuradas en los routers,

-**show ip protocols**

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

MEDELLIN1

MEDELLIN1#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
209.17.220.0 0.0.0.3 area 0
172.29.6.0 0.0.0.3 area 0

172.29.6.8 0.0.0.3 area 0
172.29.6.12 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Serial0/0/0
Serial0/0/1
Serial0/1/1
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:07:30
2.2.2.2 110 00:08:59
3.3.3.3 110 00:08:12
Distance: (default is 110)

MEDELLIN2

MEDELLIN2#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 2.2.2.2
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.6.0 0.0.0.3 area 0
172.29.6.4 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Serial0/0/0
Serial0/0/1
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:09:49
2.2.2.2 110 00:09:19
3.3.3.3 110 00:25:43
Distance: (default is 110)

MEDELLIN 3

MEDELLIN3#show ip protocols

Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set

Router ID 3.3.3.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.6.8 0.0.0.3 area 0
172.29.6.12 0.0.0.3 area 0
172.29.6.4 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Serial0/0/0
Serial0/0/1
Serial0/1/0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:10:13
2.2.2.2 110 00:09:59
3.3.3.3 110 00:09:08
Distance: (default is 110)

BOGOTA 1

BOGOTA1#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.28.3.8 0.0.0.3 area 0
209.17.220.4 0.0.0.3 area 0
172.28.3.0 0.0.0.3 area 0
172.28.3.4 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:26:07
2.2.2.2 110 00:10:33
3.3.3.3 110 00:26:26
Distance: (default is 110)

BOGOTA 2

BOGOTA2#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 2.2.2.2
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.3.8 0.0.0.3 area 0
172.29.3.12 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Serial0/0/0
Serial0/0/1
Serial0/1/0
Routing Information Sources:
Gateway Distance Last Update
2.2.2.2 110 00:07:47
3.3.3.3 110 00:25:05
Distance: (default is 110)

BOGOTA 3

BOGOTA3#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 3.3.3.3
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.29.3.12 0.0.0.3 area 0
172.29.3.4 0.0.0.3 area 0
172.29.3.0 0.0.0.3 area 0
Passive Interface(s):
GigabitEthernet0/0
Serial0/0/0
Serial0/1/0
Routing Information Sources:
Gateway Distance Last Update
2.2.2.2 110 00:25:26
3.3.3.3 110 00:07:24
Distance: (default is 110)

Mediante el comando show ip protocols podemos observar la información del protocolo, como el identificador ID del proceso OSPF, el Identificador del router y las redes que publica.

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

ISP

ISP(config)#Int s0/0/0
ISP(config-if)#Encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#Ppp pap sent-username ISP password 12345

MEDELLIN1

MEDELLIN1(config)#Int s0/0/0
MEDELLIN1(config-if)#Encapsulation ppp
MEDELLIN1(config-if)#Ppp authentication pap
MEDELLIN1(config-if)#Ppp pap sent-username ISP password 12345

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

BOGOTA1

BOGOTA1(config)#Username ISP password cisco
BOGOTA1(config)#Int s0/0/0
BOGOTA1(config-if)#Encapsulation ppp
BOGOTA1(config-if)#Ppp authentication chap

ISP

ISP(config)#Username BOGOTA1 password cisco
ISP(config)#Int s0/0/1
ISP(config-if)#Encapsulation ppp
ISP(config-if)#Ppp authentication chap
ISP (config-if)#
Los routers intercambian mensajes de autenticación utilizando el protocolo de autenticación por contraseña PAP y el protocolo de autenticación de intercambio de señales CHAP

Parte 6: Configuración de PAT.

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. 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.
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.

MEDELLIN 1

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

BOGOTA 1

```
BOGOTA1(config-if)#exit
BOGOTA1(config)#Ip nat inside source list 1 interface s0/0/0 overload
BOGOTA1(config)#Access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#Int s0/0/0
BOGOTA1(config-if)#Ip nat outside
BOGOTA1(config-if)#Int s0/0/1
BOGOTA1(config-if)#Ip nat inside
BOGOTA1(config-if)#Int s0/1/0
BOGOTA1(config-if)#Ip nat inside
BOGOTA1(config-if)#Int s0/1/1
BOGOTA1(config-if)#Ip nat inside
```

BOGOTA1(config-if) #

Mediante la configuración PAT protegemos la seguridad de la red ya que las redes externas no conocen las direcciones privadas de los host de la red interna y los host internos pueden compartir una sola dirección IP publica para toda la comunicación externa.

Parte 7: Configuración del servicio DHCP.

Configurar la red Medellín2 y Medellín3 donde el router Medellín 2 debe ser el servidor DHCP para ambas redes LAN.
El router Medellín3 deberá habilitar el paso de los mensajes broadcast hacia la IP del router Medellín2

MEDELLIN2

```
MEDELLIN2#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.6
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.134
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
MEDELLIN2(dhcp-config)#network 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 8.8.8.8
MEDELLIN2(dhcp-config)#exit
MEDELLIN2(config)#
```

MEDELLIN3

```
MEDELLIN3#config t
Enter configuration commands, one per line. End with CNTL/Z.
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
MEDELLIN3(config-if)#
```

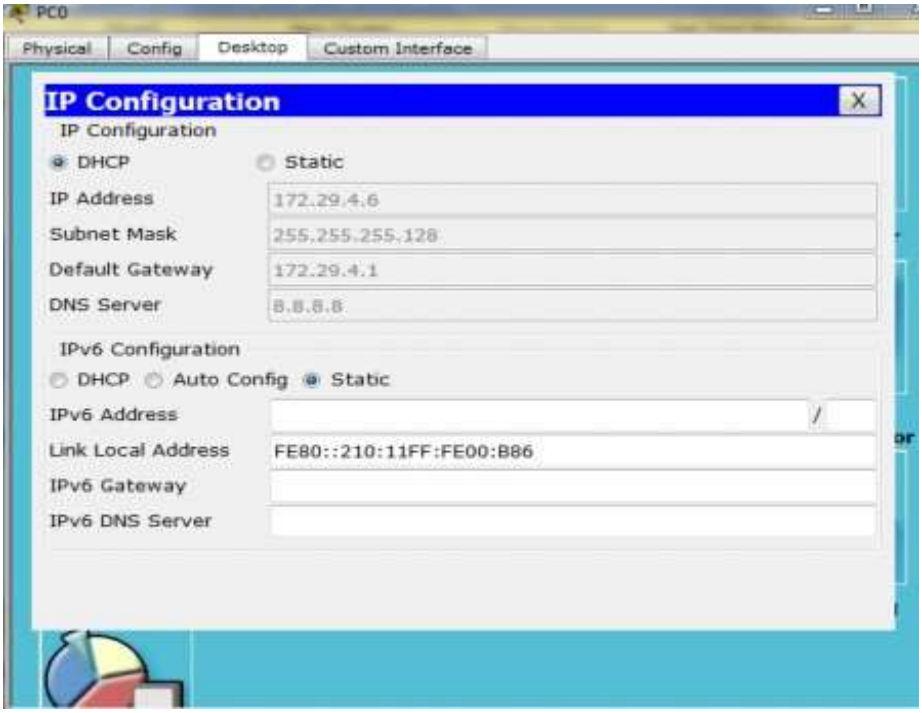


Ilustración 21.Configuración DHCP

BOGOTA 2

BOGOTA2#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.6
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.6
BOGOTA2(config)#ip dhcp pool BOGOTA2
BOGOTA2(dhcp-config)#NETWORK 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#DEFAULT-ROUTER 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#ip dhcp pool BOGOTA3
BOGOTA2(dhcp-config)#NETWORK 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#DEFAULT-ROUTER 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 8.8.8.8
BOGOTA2(dhcp-config)#exit
BOGOTA2(config)#

BOGOTA3

BOGOTA3#config t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13

BOGOTA3(config-if)#exit
BOGOTA3(config)#

El protocolo de configuración dinámica de host DHCP se diseñó para asignar direcciones IP y toda información de configuración de red importante de forma dinámica y los routers de Cisco pueden utilizar un conjunto de funciones Cisco IOS para ofrecer un servidor DHCP

CONCLUSIONES

El protocolo de enrutamiento de vector distancia RIP v2 es una versión mejorada de RIP donde ofrece el enrutamiento por prefijo, lo que le permite enviar información de la máscara de subred con la actualización de la ruta además admite el uso de enrutamiento sin clase en el cual diferentes subredes dentro de una misma red pueden utilizar distintas máscaras de subred, como lo hace VLSM y usa el número de saltos como métrica

Los protocolos de enrutamiento del estado de enlace difieren de los protocolos de vector distancia porque los routers mantienen una visión completa de la topología de red, permitiendo el uso eficiente del ancho de banda y una convergencia más rápida

Cuando se produce una falla en la red, el protocolo de estado de enlace OSPF inundan el área con publicaciones de estado de enlace (LSA) mediante una dirección multicast, cada router de estado de enlace toma una copia de la LSA y usa esta información para actualizar su base de datos del estado de enlace o topológica y vuelve a calcular las rutas

La recopilación de estado de enlaces forma una base de datos del estado de enlace la cual se denomina base de datos topológica y se utiliza para calcular las mejores rutas para la red

REFERENCIAS BIBLIOGRÁFICAS

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

CISCO. (2017). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2017). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-courseassets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

UNAD (2017). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmlJYei-NT1IhgL9QChD1m9EuGqC