

**PRUEBA DE HABILIDADES PRACTICAS CCNA
ESCENARIOS 1 Y 2**

DIPLOMADO CISCO

**Por
JORGE ELIECER ESCOBAR**

**UNAD UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ANTIOQUIA - MEDELLÍN
MAYO 2019**

**PASO 11: PRUEBA DE HABILIDADES PRACTICAS CCNA
ESCENARIOS 1 Y 2**

**For
JORGE ELIECER ESCOBAR**

**Diplomado de profundización CISCO como opción de grado en
Ingeniería en Telecomunicaciones**

**Director del curso
Juan Carlos Vesga**

**UNAD UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
ANTIOQUIA - MEDELLÍN**

MAYO 2019

NOTA DE ACEPTACIÓN

.....
.....

Juan Carlos Vesga

Director del curso

EFRAIN ALEJANDRO PEREZ

Tutor

AGRADECIMIENTO Y DEDICATORIA

Este trabajo y proceso está dedicado a mi hermana que ha sido la única persona incondicional en mi vida, siempre me ha brindado de su apoyo y ha confiado en mis capacidades para lograr los objetivos propuestos en todo este proceso, brindándome palabras motivantes, dándome sus consejos y su conocimiento.

También quiero agradecer mis compañeros de curso que siempre tuvieron la mejor disposición para trabajar en equipo y atentos para realizar el mejor trabajo posible.



TABLA DE CONTENIDO

INTRODUCCIÓN	11
OBJETIVOS	12
ESCENARIO 1	13
ESCENARIO 2	34
CONCLUSIONES	55
REFERENCIAS BIBLIOGRAFICAS	56

LISTA DE TABLAS

Tabla 1 Direccionamiento IP	14
Tabla 2 Interfaces que no requieren desactivación	25
Tabla 3 OSPF Area 0.....	37
Tabla 4 Vlan y direccionamiento.....	44
Tabla 5 Datos para DHCP	48

LISTA DE FIGURAS

Figura 1 Topología escenario 1	13
Figura 2 Pruebas ping del enrutamiento creado.....	20
Figura 3 Tabla de enrutamiento router MEDELLIN1	21
Figura 4 Tabla de enrutamiento router MEDELLIN2	21
Figura 5 Tabla de enrutamiento router MEDELLIN3 y balanceo de carga.....	21
Figura 6 Tabla de enrutamiento router ISP	22
Figura 7 Tabla de enrutamiento router BOGOTA1	22
Figura 8 Tabla de enrutamiento router BOGOTA2	22
Figura 9 Tabla de enrutamiento router BOGOTA3 y balanceo de carga	23
Figura 10 Similitudes entre routers Bogotá1 y Medellín1	23
Figura 11 Rutas redundantes en routers Medellín3 y Bogotá3.....	24
Figura 12 Rutas en router ISP.....	24
Figura 13 PING DE MEDELLIN1 Y BOGOTA1 AL ROUTER ISP.....	26
Figura 14 PING DESDE PC2 Y SOLO ES EXITOSO HASTA BOGOTA1	28
Figura 15 REVISION DE LA TRADUCCION DEL NAT.....	29
Figura 16 ping desde PC4 y solo es exitoso hasta MEDELLIN1	30
Figura 17 Validacion DHCP dinamico	31
Figura 18 Validación conectividad entre los host.....	33
Figura 19 TOPOLOGÍA ESCENARIO 2	34
Figura 20 Se valida DHCP en los host de vlan 30 y 40 ESCENARIO 2	47
Figura 21 PING A IP INTERNET RECHAZADA.....	50
Figura 22 PING A IP INTERNET RECHAZADA.....	50
Figura 23 TELNET DESDE VLAN 30 Y LUEGO DESDE VLAN 40	52
Figura 24 Ping entre las redes	53
Figura 25 VALIDACION DE TRACERT.....	53

RESUMEN

A continuación veremos dos escenarios con sus respectivas soluciones de conectividad, en el primer escenario presentamos una topología en la que un Router de borde conecta a internet y posee dos sedes Medellín y Bogotá y cada una de estas integra otras subredes. Los host de cada red debe tener comunicación con demás redes y tener salida hacia internet, esto se logra con la configuración de enrutamiento RIPv2 implementada en los Router, con la configuración del servicio de NAT, DHCP y demás parámetros necesarios.

En el segundo escenario se presenta una topología con dos sedes también, se aplica la configuración de enrutamiento OSPF, se configura Nat, DHCP en uno de los Routers, listas de acceso, configuración y encapsulamiento de vlans por medio de puerto troncal, también se realiza configuración necesaria para que las dos sedes Bogotá y Buenos Aires tengan salida a internet. Al completar las configuraciones se realizan las pruebas necesarias como validación la conectividad como la asignación de DHCP en los host, las tablas de enrutamiento en los Router, ejecución ping a las otras redes y hacia internet cuales son completadas con éxito, además se realiza la ejecución del comando tracert y se valida las rutas que toma el ping sean las configuradas.

ABSTRACT

Then we will see two scenarios with their respective connectivity solutions, in the first scenario we present a topology in which an edge router connects to the internet and has two Medellin and Bogota offices and each of these integrates other subnets. The hosts of each network must have communication with other networks and have an internet connection, this is achieved with the RIPv2 routing configuration implemented in the Routers, with the configuration of the NAT, DHCP service and other necessary parameters.

In the second scenario, a topology with two sites is also presented, the OSPF routing configuration is applied, Nat is configured, DHCP in one of the Routers, access lists, configuration and encapsulation of vlans by means of trunk port, it is also performed necessary configuration for the two Bogota and Buenos Aires sites to have Internet access. When completing the configurations, the necessary tests are performed, such as connectivity validation, such as DHCP assignment in the host, routing tables in the Routers, ping execution to the other networks and to the Internet, which are completed successfully. of the tracert command and the routes that the ping takes are configured.

GLOSARIO

DHCP: Protocolo de asignación de direccionamiento IP dinámico de tipo cliente/servidor que consiste en asignar parámetros de dirección IP a los host de una red

HOST: Computador o dispositivo que se puede conectar a una red y ofrece servicios de transferencia de datos, almacenamiento, conexión remota, etc.

IP: Numero Identificación única y jerárquica que se puede asignar a una interfaz

IPV4: Es la cuarta versión del protocolo de internet IP, usa direcciones de 32 bits y será reemplazado en el futuro por IPV6.

LAN: Es una red de área local pequeña comúnmente es una red de oficina u hogar en la cual se permite enviar y recibir archivos.

NAT: Es una traducciones de direcciones de red, permite la comunicación de una red privada con una red pública generando ahorro de direcciones IP, hay varios tipos como Nat estático, dinámico, sobrecarga y solapamiento.

OSPF: Es un protocolo de red para el encaminamiento jerarquico, este usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos. Su medida de métrica se denomina costo, también tiene en cuenta parámetros como el ancho de banda y congestión en los enlaces.

RIPV2: Es un Protocolo de Información de Encaminamiento, es un protocolo de puerta de enlace interna o interior usado en los routers con los que se intercambia información acerca de redes a las que se encuentran conectados.

ROUTER: Dispositivo que se encarga de encaminar los datos por los diferentes caminos disponibles o configurados dentro de la red. Además se encarga de interconectar las diferentes redes.

SWITCH: Es un dispositivo conmutador que permite interconectar muchos dispositivos para formar una red LAN.

VLAN: Es una red de área local virtual, la cual se configura para crear redes lógicas independientes dentro de una red física. Pueden configurarse varias redes vlan dentro de un mismo escenario físico.

INTRODUCCIÓN

En el presente trabajo solucionaremos el planteamiento de dos escenarios diferentes en el software Packet tracer, los cuales exigen diferentes habilidades., conceptos y configuraciones de las 4 unidades estudiadas durante el diplomado de cisco, donde se deben realizar una serie de pasos como las conexiones con su tipo de cableado y configuraciones en los equipos Switch, router y PC, para establecer las conectividades propuestas por medio de los distintos protocolos de enrutamiento como RIP V2, OSPF V2, autenticación PPP, configuración de servicios como DHCP, encapsulamiento de vlans, validación y asignación de direccionamiento IP en las interfaces, configuración de listas de acceso y servicio de NAT. Se realizan las pruebas y la validación de los datos arrojados en los diferentes equipos.

Realizando todas las configuraciones y diseños de la red pertinentes brindaremos una solución segura y eficaz para aprovechar los recursos y generar un funcionamiento adecuado de la red.

OBJETIVOS

Generales

Desarrollar las habilidades y competencias necesarias para brindar soluciones de conectividad en diferentes escenarios y situaciones, por medio del conocimiento adquirido de las 4 unidades estudiadas en el diplomado de cisco.

Específicos

Escenario 1

Realizar las configuraciones del direccionamiento IP de acuerdo a los lineamientos propuestos en el escenario a los diferentes equipos host, interfaces físicas e interfaces vlan.

Realizar configuración de enrutamiento con tipo RIP versión 2 en los Routers.

Configurar Routers para realizar servicio DHCP a los host.

Configurar el protocolo de autenticación PPP para los enlaces seriales con el Router ISP.

Realizar configuración de NAT (PAT) en Router.

Validar y realizar pruebas con la información del enrutamiento Rip v2, Realizar pruebas de conectividad en toda la solución o escenario 1

Escenario 2

Aplicar los conceptos estudiados de enrutamiento de vlans, configuración de puertos troncales en los switch.

Realizar configuración de enrutamiento OSPF v2, configurar el servicio de DHCP en el Router para la asignación del direccionamiento IP a los host

Configuración de servicio de NAT en el Router de borde con salida a internet

Creación de listas de acceso para permitir o restringir el tráfico desde o hacia el Router de borde (hacia internet).

ESCENARIO 1

FIGURA 1 TOPOLOGÍA ESCENARIO 1

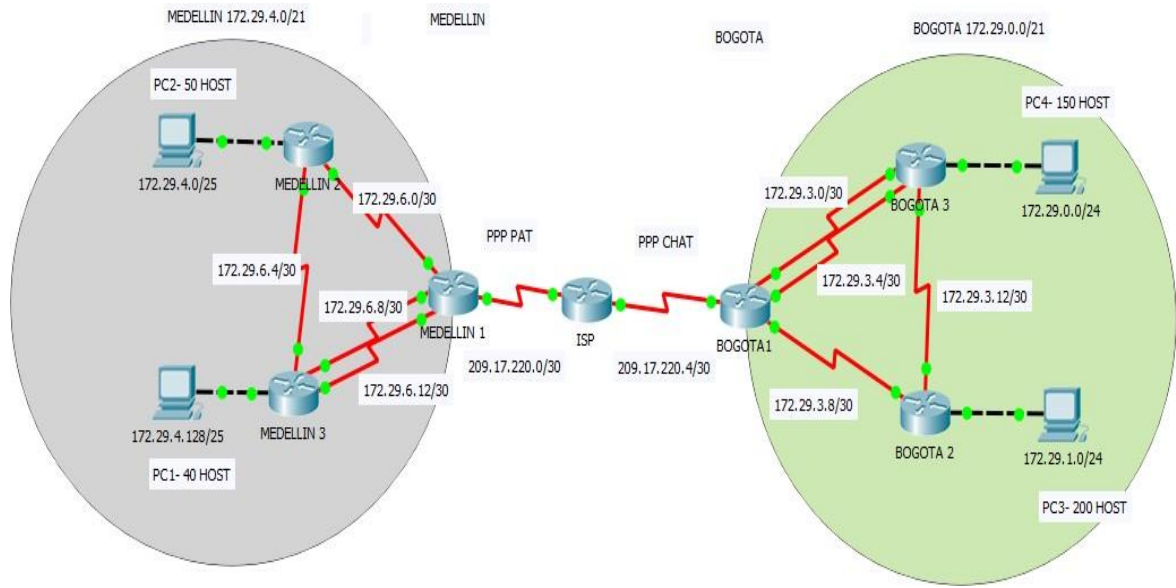


TABLA 1 DIRECCIONAMIENTO IP

Equipo	Interfaz	Dirección IP	Mascara de subred	Gateway
MEDELLIN1	Serial 0/0/0	172.29.6.2	255.255.255.252	N/A
	Serial 0/0/1	172.29.6.13	255.255.255.252	N/A
	Serial 0/1/0	172.29.6.10	255.255.255.252	N/A
	Serial 0/1/1	209.17.220.1	255.255.255.252	N/A
MEDELLIN2	FastEthernet 0/0	172.29.4.1	255.255.255.128	N/A
	Serial 0/0/0	172.29.6.1	255.255.255.252	N/A
	Serial 0/0/1	172.29.6.5	255.255.255.252	N/A
MEDELLIN3	FastEthernet 0/0	172.29.4.129	255.255.255.128	N/A
	Serial 0/0/0	172.29.6.14	255.255.255.252	N/A
	Serial 0/0/1	172.29.6.6	255.255.255.252	N/A
	Serial 0/1/0	172.29.6.9	255.255.255.252	N/A
BOGOTA1	Serial 0/0/0	172.29.3.6	255.255.255.252	N/A
	Serial 0/0/1	172.29.3.10	255.255.255.252	N/A
	Serial 0/1/0	172.29.3.2	255.255.255.252	N/A
	Serial 0/1/1	209.17.220.5	255.255.255.252	N/A
BOGOTA2	FastEthernet 0/0	172.29.1.1	255.255.255.0	N/A
	Serial 0/0/0	172.29.3.13	255.255.255.252	N/A
	Serial 0/0/1	172.29.3.9	255.255.255.252	N/A
BOGOTA3	FastEthernet 0/0	172.29.0.1	255.255.255.0	N/A
	Serial 0/0/0	172.29.3.5	255.255.255.252	N/A
	Serial 0/0/1	172.29.3.14	255.255.255.252	N/A
	Serial 0/1/0	172.29.3.1	255.255.255.252	N/A
ISP	Serial 0/0/0	209.17.220.2	255.255.255.252	N/A
	Serial 0/0/1	209.17.220.6	255.255.255.252	N/A
PC1	FastEthernet 0	DHCP	DHCP	DHCP
PC2	FastEthernet 0	DHCP	DHCP	DHCP
PC3	FastEthernet 0	DHCP	DHCP	DHCP
PC4	FastEthernet 0	DHCP	DHCP	DHCP

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

```
Router>enable
Router(config)#hostname MEDELLIN1
MEDELLIN1(config)#No ip domain lookup
MEDELLIN1(config)#enable secret class
MEDELLIN1(config)#line console 0
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#line vty 0 15
MEDELLIN1(config-line)#password cisco
MEDELLIN1(config-line)#login
MEDELLIN1(config-line)#exit
MEDELLIN1(config)#service password-encryption
MEDELLIN1(config)#banner motd #***** Prohibido el acceso no
autorizado a este equipo***** #
MEDELLIN1(config)#
```

```
Router>enable
Router(config)#hostname MEDELLIN2
MEDELLIN2(config)#No ip domain lookup
MEDELLIN2(config)#enable secret class
MEDELLIN2(config)#line console 0
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#line vty 0 15
MEDELLIN2(config-line)#password cisco
MEDELLIN2(config-line)#login
MEDELLIN2(config-line)#exit
MEDELLIN2(config)#service password-encryption
MEDELLIN2(config)#banner motd #***** Prohibido el acceso no
autorizado a este equipo***** #
MEDELLIN2(config)#
```

```
Router>enable
Router(config)#hostname MEDELLIN3
```

```
MEDELLIN3(config)#No ip domain lookup
MEDELLIN3(config)#enable secret class
MEDELLIN3(config)#line console 0
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#exit
MEDELLIN3(config)#line vty 0 15
MEDELLIN3(config-line)#password cisco
MEDELLIN3(config-line)#login
MEDELLIN3(config-line)#exit
MEDELLIN3(config)#service password-encryption
MEDELLIN3(config)#banner motd #***** Prohibido el acceso no
autorizado a este equipo***** #
```

```
Router>enable
Router(config)#hostname BOGOTA1
BOGOTA1(config)#No ip domain lookup
BOGOTA1(config)#enable secret class
BOGOTA1(config)#line console 0
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#exit
BOGOTA1(config)#line vty 0 15
BOGOTA1(config-line)#password cisco
BOGOTA1(config-line)#login
BOGOTA1(config-line)#exit
BOGOTA1(config)#service password-encryption
BOGOTA1(config)#banner motd #***** Prohibido el acceso no
autorizado a este equipo***** #
```

```
Router>enable
Router(config)#hostname BOGOTA2
BOGOTA2(config)#No ip domain lookup
BOGOTA2(config)#enable secret class
BOGOTA2(config)#line console 0
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
```



```
BOGOTA2(config-line)#exit
BOGOTA2(config)#line vty 0 15
BOGOTA2(config-line)#password cisco
BOGOTA2(config-line)#login
BOGOTA2(config-line)#exit
BOGOTA2(config)#service password-encryption
BOGOTA2(config)#banner motd #***** Prohibido el acceso no
autorizado a este equipo***** #
```

```
Router>enable
Router(config)#hostname BOGOTA3
BOGOTA3(config)#No ip domain lookup
BOGOTA3(config)#enable secret class
BOGOTA3(config)#line console 0
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#exit
BOGOTA3(config)#line vty 0 15
BOGOTA3(config-line)#password cisco
BOGOTA3(config-line)#login
BOGOTA3(config-line)#exit
BOGOTA3(config)#service password-encryption
BOGOTA3(config)#banner motd #***** Prohibido el acceso no
autorizado a este equipo***** #
```

```
Router>enable
Router(config)#hostname ISP
ISP(config)#No ip domain lookup
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#line vty 0 15
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
```

```
ISP(config)#service password-encryption
ISP(config)#banner motd #***** Prohibido el acceso no autorizado a
este equipo***** #
```

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

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

Configuración RIP2

```
MEDELLIN1(config)#router rip
MEDELLIN1(config-router)#version 2
MEDELLIN1(config-router)#network 172.29.6.0
MEDELLIN1(config-router)#network 172.29.6.8
MEDELLIN1(config-router)#network 172.29.6.12
MEDELLIN1(config-router)#no auto-summary
MEDELLIN1(config-router)#passive-interface serial 0/1/1
```

```
MEDELLIN2(config)#router rip
MEDELLIN2(config-router)#version 2
MEDELLIN2(config-router)#network 172.29.4.0
MEDELLIN2(config-router)#network 172.29.6.4
MEDELLIN2(config-router)#network 172.29.6.0
MEDELLIN2(config-router)#passive-interface fa 0/0
MEDELLIN2(config-router)#no auto-summary
```

```
MEDELLIN3(config)#router rip
MEDELLIN3(config-router)#version 2
MEDELLIN3(config-router)#network 172.29.4.128
MEDELLIN3(config-router)#network 172.29.6.4
MEDELLIN3(config-router)#network 172.29.6.8
MEDELLIN3(config-router)#network 172.29.6.12
MEDELLIN3(config-router)#no auto-summary
MEDELLIN3(config-router)#passive-interface fa 0/0
```

```
BOGOTA1(config)#router rip
BOGOTA1(config-router)#version 2
BOGOTA1(config-router)#network 172.29.3.0
BOGOTA1(config-router)#network 172.29.3.4
BOGOTA1(config-router)#network 172.29.3.8
BOGOTA1(config-router)#no auto-summary
BOGOTA1(config-router)#passive-interface serial 0/1/1
```

```
BOGOTA2(config)#router rip
BOGOTA2(config-router)#version 2
BOGOTA2(config-router)#network 172.29.1.0
BOGOTA2(config-router)#network 172.29.3.8
BOGOTA2(config-router)#network 172.29.3.12
BOGOTA2(config-router)#no auto-summary
BOGOTA2(config-router)#passive-interface fa 0/0
```

```
BOGOTA3(config)#router rip
BOGOTA3(config-router)#version 2
BOGOTA3(config-router)#network 172.29.0.0
BOGOTA3(config-router)#network 172.29.3.0
BOGOTA3(config-router)#network 172.29.3.4
BOGOTA3(config-router)#network 172.29.3.12
BOGOTA3(config-router)#no auto-summary
BOGOTA3(config-router)#passive-interface fa 0/0
```

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.

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 serial0/1/1
MEDELLIN1(config-router)#default-information originate
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 serial0/1/1
BOGOTA1(config-router)#default-information originate
```

El router ISP deberá tener una ruta estática dirigida hacia cada red interna de Bogotá y Medellín para el caso se suman las subredes de cada uno a /22.

```
ISP(config)#ip route 172.29.4.0 255.255.252.0 serial 0/0/0
ISP(config)#ip route 172.29.0.0 255.255.252.0 serial 0/0/1
```

Parte 2: Tabla de Enrutamiento.

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

FIGURA 2 PRUEBAS PING DEL ENRUTAMIENTO CREADO

```
BOGOTA3#ping 172.29.3.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.3.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms

BOGOTA3#ping 209.17.220.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/4/14 ms

BOGOTA3#ping 209.17.220.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/5/11 ms

BOGOTA3#ping 172.29.6.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/17/31 ms

BOGOTA3#ping 172.29.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.29.6.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/11/16 ms

BOGOTA3#
```

FIGURA 3 TABLA DE ENRUTAMIENTO ROUTER MEDELLIN1

```

172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R   172.29.4.0/25 [120/1] via 172.29.6.1, 00:00:05, Serial0/0/0
R   172.29.4.128/25 [120/1] via 172.29.6.14, 00:00:16, Serial0/0/1
    [120/1] via 172.29.6.9, 00:00:16, Serial0/1/0
C   172.29.6.0/30 is directly connected, Serial0/0/0
R   172.29.6.4/30 [120/1] via 172.29.6.1, 00:00:05, Serial0/0/0
    [120/1] via 172.29.6.14, 00:00:16, Serial0/0/1
    [120/1] via 172.29.6.9, 00:00:16, Serial0/1/0
C   172.29.6.8/30 is directly connected, Serial0/1/0
C   172.29.6.12/30 is directly connected, Serial0/0/1
209.17.220.0/30 is subnetted, 1 subnets
C   209.17.220.0 is directly connected, Serial0/1/1
S*  0.0.0.0/0 is directly connected, Serial0/1/1

```

MEDELLIN1#

FIGURA 4 TABLA DE ENRUTAMIENTO ROUTER MEDELLIN2

```

172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C   172.29.4.0/25 is directly connected, FastEthernet0/0
R   172.29.4.128/25 [120/1] via 172.29.6.6, 00:00:20, Serial0/0/1
C   172.29.6.0/30 is directly connected, Serial0/0/0
C   172.29.6.4/30 is directly connected, Serial0/0/1
R   172.29.6.8/30 [120/1] via 172.29.6.6, 00:00:20, Serial0/0/1
    [120/1] via 172.29.6.2, 00:00:24, Serial0/0/0
R   172.29.6.12/30 [120/1] via 172.29.6.6, 00:00:20, Serial0/0/1
    [120/1] via 172.29.6.2, 00:00:24, Serial0/0/0
R*  0.0.0.0/0 [120/1] via 172.29.6.2, 00:00:24, Serial0/0/0

```

MEDELLIN2#

FIGURA 5 TABLA DE ENRUTAMIENTO ROUTER MEDELLIN3 Y BALANCEO DE CARGA

```

172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R   172.29.4.0/25 [120/1] via 172.29.6.5, 00:00:14, Serial0/0/1
C   172.29.4.128/25 is directly connected, FastEthernet0/0
R   172.29.6.0/30 [120/1] via 172.29.6.5, 00:00:14, Serial0/0/1
    [120/1] via 172.29.6.13, 00:00:10, Serial0/0/0
    [120/1] via 172.29.6.10, 00:00:10, Serial0/1/0
C   172.29.6.4/30 is directly connected, Serial0/0/1
C   172.29.6.8/30 is directly connected, Serial0/1/0
C   172.29.6.12/30 is directly connected, Serial0/0/0
R*  0.0.0.0/0 [120/1] via 172.29.6.13, 00:00:10, Serial0/0/0
    [120/1] via 172.29.6.10, 00:00:10, Serial0/1/0

```

MEDELLIN3#

FIGURA 6 TABLA DE ENRUTAMIENTO ROUTER ISP

```

172.29.0.0/22 is subnetted, 2 subnets
S    172.29.0.0 is directly connected, Serial0/0/1
S    172.29.4.0 is directly connected, Serial0/0/0
209.17.220.0/30 is subnetted, 2 subnets
C    209.17.220.0 is directly connected, Serial0/0/0
C    209.17.220.4 is directly connected, Serial0/0/1

ISP#|

```

FIGURA 7 TABLA DE ENRUTAMIENTO ROUTER BOGOTA 1

```

172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R    172.29.0.0/24 [120/1] via 172.29.3.1, 00:00:16, Serial0/1/0
      [120/1] via 172.29.3.5, 00:00:16, Serial0/0/0
R    172.29.1.0/24 [120/1] via 172.29.3.9, 00:00:02, Serial0/0/1
C    172.29.3.0/30 is directly connected, Serial0/1/0
C    172.29.3.4/30 is directly connected, Serial0/0/0
C    172.29.3.8/30 is directly connected, Serial0/0/1
R    172.29.3.12/30 [120/1] via 172.29.3.9, 00:00:02, Serial0/0/1
      [120/1] via 172.29.3.1, 00:00:16, Serial0/1/0
      [120/1] via 172.29.3.5, 00:00:16, Serial0/0/0
209.17.220.0/30 is subnetted, 1 subnets
C    209.17.220.4 is directly connected, Serial0/1/1
S*  0.0.0.0/0 is directly connected, Serial0/1/1

BOGOTA1# |

```

FIGURA 8 TABLA DE ENRUTAMIENTO ROUTER BOGOTA 2

```

172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
R    172.29.0.0/24 [120/1] via 172.29.3.14, 00:00:26, Serial0/0/0
C    172.29.1.0/24 is directly connected, FastEthernet0/0
R    172.29.3.0/30 [120/1] via 172.29.3.14, 00:00:26, Serial0/0/0
      [120/1] via 172.29.3.10, 00:00:01, Serial0/0/1
R    172.29.3.4/30 [120/1] via 172.29.3.10, 00:00:01, Serial0/0/1
      [120/1] via 172.29.3.14, 00:00:26, Serial0/0/0
C    172.29.3.8/30 is directly connected, Serial0/0/1
C    172.29.3.12/30 is directly connected, Serial0/0/0
R*  0.0.0.0/0 [120/1] via 172.29.3.10, 00:00:01, Serial0/0/1

BOGOTA2#|

```


FIGURA 9 TABLA DE ENRUTAMIENTO ROUTER BOGOTA3 Y BALANCEO DE CARGA

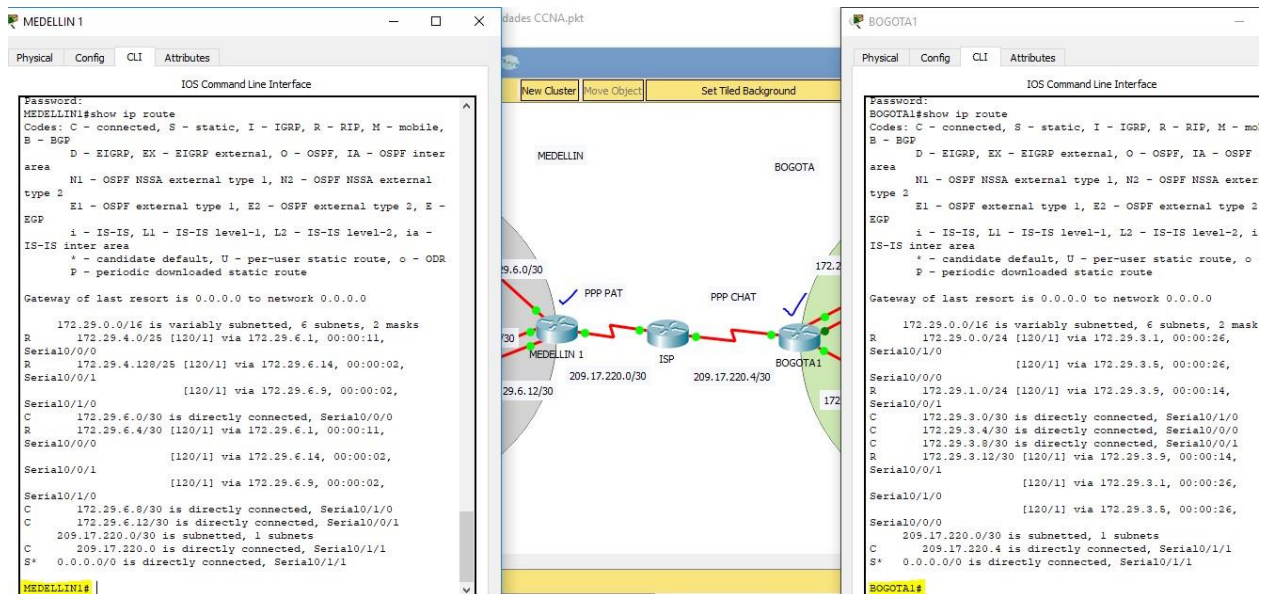
```

172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks
C    172.29.0.0/24 is directly connected, FastEthernet0/0
R    172.29.1.0/24 [120/1] via 172.29.3.13, 00:00:24, Serial0/0/1
C    172.29.3.0/30 is directly connected, Serial0/1/0
C    172.29.3.4/30 is directly connected, Serial0/0/0
R    172.29.3.8/30 [120/1] via 172.29.3.13, 00:00:24, Serial0/0/1
    [120/1] via 172.29.3.6, 00:00:11, Serial0/0/0
    [120/1] via 172.29.3.2, 00:00:11, Serial0/1/0
C    172.29.3.12/30 is directly connected, Serial0/0/1
R*  0.0.0.0/0 [120/1] via 172.29.3.6, 00:00:11, Serial0/0/0
    [120/1] via 172.29.3.2, 00:00:11, 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.

FIGURA 10 SIMILITUDES ENTRE ROUTERS BOGOTÁ1 Y MEDELLÍN1



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

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

FIGURA 11 RUTAS REDUNDANTES EN ROUTERS MEDELLÍN3 Y BOGOTÁ3

<pre>MEDELLIN3#show ip route Codes: C - connected, S - static, I - IGRP, 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, 6 subnets, 2 masks R 172.29.4.0/25 [120/1] via 172.29.6.5, 00:00:10, Serial0/0/1 C 172.29.4.128/25 is directly connected, FastEthernet0/0 R 172.29.6.0/30 [120/1] via 172.29.6.5, 00:00:10, Serial0/0/1 [120/1] via 172.29.6.13, 00:00:05, Serial0/0/0 [120/1] via 172.29.6.10, 00:00:05, Serial0/1/0 C 172.29.6.4/30 is directly connected, Serial0/0/1 C 172.29.6.8/30 is directly connected, Serial0/1/0 C 172.29.6.12/30 is directly connected, Serial0/0/0 R* 0.0.0.0/0 [120/1] via 172.29.6.13, 00:00:05, Serial0/0/0 [120/1] via 172.29.6.10, 00:00:05, Serial0/1/0 MEDELLIN3#</pre>	<pre>BOGOTA3#show ip route Codes: C - connected, S - static, I - IGRP, 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 172.29.3.6 to network 0.0.0.0 172.29.0.0/16 is variably subnetted, 6 subnets, 2 masks C 172.29.0.0/24 is directly connected, FastEthernet0/0 R 172.29.1.0/24 [120/1] via 172.29.3.13, 00:00:01, Serial0/0/1 C 172.29.3.0/30 is directly connected, Serial0/1/0 C 172.29.3.4/30 is directly connected, Serial0/0/0 R 172.29.3.8/30 [120/1] via 172.29.3.13, 00:00:01, Serial0/0/1 [120/1] via 172.29.3.6, 00:00:10, Serial0/0/0 [120/1] via 172.29.3.2, 00:00:10, Serial0/1/0 C 172.29.3.12/30 is directly connected, Serial0/0/1 R* 0.0.0.0/0 [120/1] via 172.29.3.6, 00:00:10, Serial0/0/0 [120/1] via 172.29.3.2, 00:00:10, Serial0/1/0 BOGOTA3#</pre>
--	---

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

FIGURA 12 RUTAS EN ROUTER ISP

```
172.29.0.0/22 is subnetted, 2 subnets
S 172.29.0.0 is directly connected, Serial0/0/1
S 172.29.4.0 is directly connected, Serial0/0/0
209.17.220.0/30 is subnetted, 2 subnets
C 209.17.220.0 is directly connected, Serial0/0/0
C 209.17.220.4 is directly connected, Serial0/0/1

ISP#
ISP#
ISP#
```

Parte 3: Deshabilitar la propagación del protocolo RIP.

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 2 INTERFACES QUE NO REQUIEREN DESACTIVACIÓN

Equipo	Interfaz
BOGOTA1	Serial 0/0/0, Serial 0/0/1, Serial 0/1/0
BOGOTA2	Serial 0/0/0, Serial 0/0/1
BOGOTA3	Serial 0/0/0, Serial 0/0/1, Serial 0/1/0
MEDELLIN1	Serial 0/0/0, Serial 0/0/1, Serial 0/1/0
MEDELLIN2	Serial 0/0/0, Serial 0/0/1
MEDELLIN3	Serial 0/0/0, Serial 0/0/1, Serial 0/1/0
ISP	N/A

Parte 4: Verificación del protocolo RIP.

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.

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.

Se realiza desactivación de propagación de publicaciones en las siguientes interfaces de cada uno de los routers:

Para los Routers que conectan las LAN:

```
MEDELLIN2(config-router)#passive-interface fa 0/0
MEDELLIN3(config-router)#passive-interface fa 0/0
BOGOTA2(config-router)#passive-interface fa 0/0
BOGOTA3(config-router)#passive-interface fa 0/0
```

Para los Routers que conectan con el ISP:

```
MEDELLIN1(config-router)#passive-interface serial 0/1/1
BOGOTA1(config-router)#passive-interface serial 0/1/1
```

Parte 5: Configurar encapsulamiento y autenticación PPP.

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

```
MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config)#inter serial 0/1/1
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco
```

```
ISP(config)#username MEDELLIN1 password cisco
ISP(config)#interface serial 0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication pap
ISP(config-if)#ppp pap sent-username ISP password cisco
```

FIGURA 13 PING DE MEDELLIN1 Y BOGOTA1 AL ROUTER ISP

```
MEDELLIN1#ping 209.17.220.2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.2, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/4/11 ms
```

```
MEDELLIN1#
```

```
BOGOTA1#ping 209.17.220.6
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.6, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/8
ms
```

```
BOGOTA1#
```

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

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

```
BOGOTA1(config)#interface serial 0/1/1
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
```

```
ISP(config)#username BOGOTA1 password cisco
ISP(config)#interface serial 0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication 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.

Configuración de PAT (NAT con sobrecarga) en Routers Bogotá1 y Medellín1

Se realizan pruebas de conectividad y se evidencia que sólo existe 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.

```
MEDELLIN1(config)#ip nat inside source list 1 interface s0/1/1 overload
MEDELLIN1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MEDELLIN1(config)#interface serial 0/1/1
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#inter s0/0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#inter s0/1/0
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#inter s0/0/0
MEDELLIN1(config-if)#ip nat inside
```

FIGURA 14 PING DESDE PC2 Y SOLO ES EXITOSO HASTA BOGOTA1

```
Command Prompt
^C
C:\>ping 209.17.220.5 ✓

Pinging 209.17.220.5 with 32 bytes of data:

Reply from 209.17.220.5: bytes=32 time=4ms TTL=252
Reply from 209.17.220.5: bytes=32 time=12ms TTL=252
Reply from 209.17.220.5: bytes=32 time=10ms TTL=252
Reply from 209.17.220.5: bytes=32 time=3ms TTL=252

Ping statistics for 209.17.220.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 12ms, Average = 7ms

C:\>ping 172.29.0.5 ✗

Pinging 172.29.0.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.29.0.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.29.1.5 ✗

Pinging 172.29.1.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.29.1.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>|
```

FIGURA 15 REVISION DE LA TRADUCCION DEL NAT

```
MEDELLIN1#show ip nat translations
Pro  Inside global      Inside local        Outside local       Outside global
icmp 209.17.220.1:14    172.29.4.5:14      209.17.220.5:14    209.17.220.5:14
icmp 209.17.220.1:15    172.29.4.5:15      209.17.220.5:15    209.17.220.5:15
icmp 209.17.220.1:16    172.29.4.5:16      209.17.220.5:16    209.17.220.5:16
icmp 209.17.220.1:17    172.29.4.5:17      209.17.220.5:17    209.17.220.5:17

MEDELLIN1#

BOGOTA1#show ip nat translations
Pro  Inside global      Inside local        Outside local       Outside global
icmp 209.17.220.5:64    172.29.0.5:64      209.17.220.1:64    209.17.220.1:64
icmp 209.17.220.5:65    172.29.0.5:65      209.17.220.1:65    209.17.220.1:65
icmp 209.17.220.5:66    172.29.0.5:66      209.17.220.1:66    209.17.220.1:66
icmp 209.17.220.5:67    172.29.0.5:67      209.17.220.1:67    209.17.220.1:67

BOGOTA1#
```

Proceda a configurar el NAT en el router Bogotá1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Bogotá1, cómo diferente puerto.

```
BOGOTA1(config)#ip nat inside source list 1 interface s0/1/1 overload
BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#exi
BOGOTA1(config)#int s0/1/1
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/0/0
BOGOTA1(config-if)#ip nat inside
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)#
```

FIGURA 16 PING DESDE PC4 Y SOLO ES EXITOSO HASTA MEDELLIN1

```

C:\>ping 209.17.220.1 ✓

Pinging 209.17.220.1 with 32 bytes of data:

Reply from 209.17.220.1: bytes=32 time=4ms TTL=252
Reply from 209.17.220.1: bytes=32 time=7ms TTL=252
Reply from 209.17.220.1: bytes=32 time=13ms TTL=252
Reply from 209.17.220.1: bytes=32 time=3ms TTL=252

Ping statistics for 209.17.220.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 13ms, Average = 6ms

C:\>ping 172.29.4.5 ✗

Pinging 172.29.4.5 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.29.4.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
C:\>ping 172.29.4.133 ✗

Pinging 172.29.4.133 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.29.4.133:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

Parte 7: Configuración del servicio DHCP.

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

```

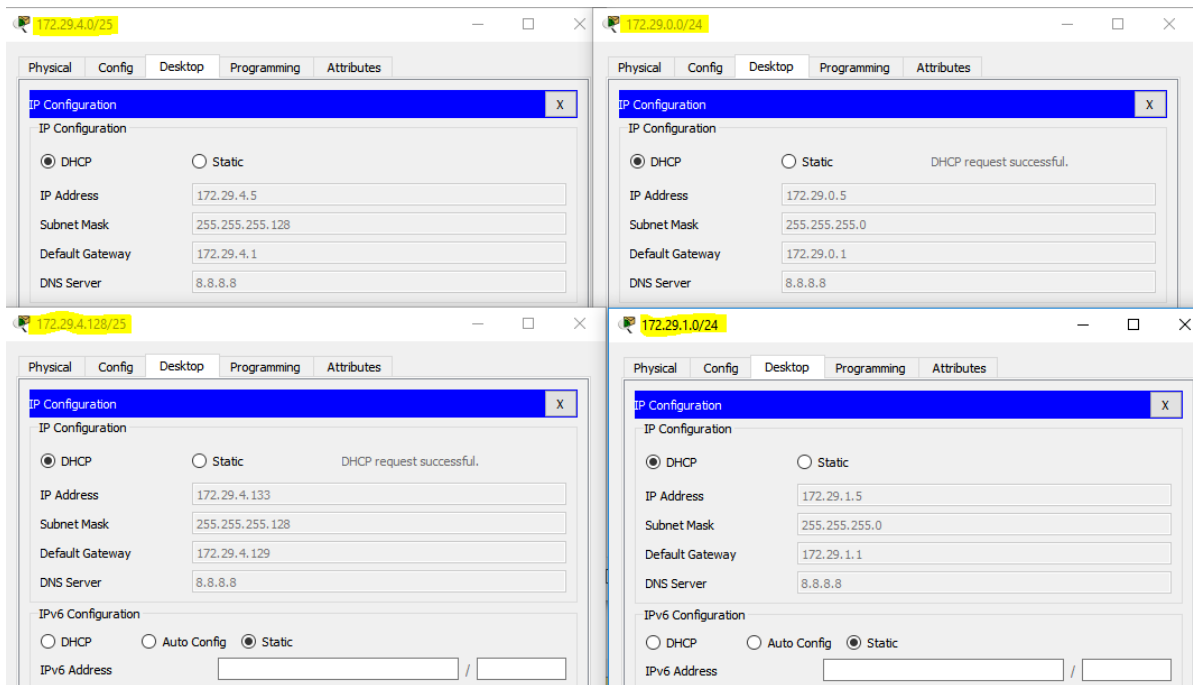
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.4
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.132
MEDELLIN2(config)#ip dhcp pool Medellin2
MEDELLIN2(dhcp-config)#network 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 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)#exi
MEDELLIN2(config)#
  
```

FIGURA 17 VALIDACION DHCP DINAMICO



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

```

MEDELLIN3(config)#interface fa0/0
MEDELLIN3(config-if)#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(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.4
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.0 172.29.1.4
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)#
```

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

```
BOGOTA3(config)#interface fa0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
```

Se realiza verificación de conectividad desde equipo PC4 en red Bogotá y hay conectividad exitosa a todos los otros PC1, PC2 y PC3 luego de la asignación de direccionamiento IP por DHCP

FIGURA 18 VALIDACIÓN CONECTIVIDAD ENTRE LOS HOST

```
Command Prompt

C:\>ping 172.29.1.5

Pinging 172.29.1.5 with 32 bytes of data:

Reply from 172.29.1.5: bytes=32 time=1ms TTL=126
Reply from 172.29.1.5: bytes=32 time=1ms TTL=126
Reply from 172.29.1.5: bytes=32 time=1ms TTL=126
Reply from 172.29.1.5: bytes=32 time=1ms TTL=126

Ping statistics for 172.29.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 172.29.4.5

Pinging 172.29.4.5 with 32 bytes of data:

Reply from 172.29.4.5: bytes=32 time=5ms TTL=123
Reply from 172.29.4.5: bytes=32 time=4ms TTL=123
Reply from 172.29.4.5: bytes=32 time=10ms TTL=123
Reply from 172.29.4.5: bytes=32 time=20ms TTL=123

Ping statistics for 172.29.4.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 20ms, Average = 9ms

C:\>ping 172.29.4.133

Pinging 172.29.4.133 with 32 bytes of data:

Reply from 172.29.4.133: bytes=32 time=11ms TTL=123
Reply from 172.29.4.133: bytes=32 time=4ms TTL=123
Reply from 172.29.4.133: bytes=32 time=9ms TTL=123
Reply from 172.29.4.133: bytes=32 time=13ms TTL=123

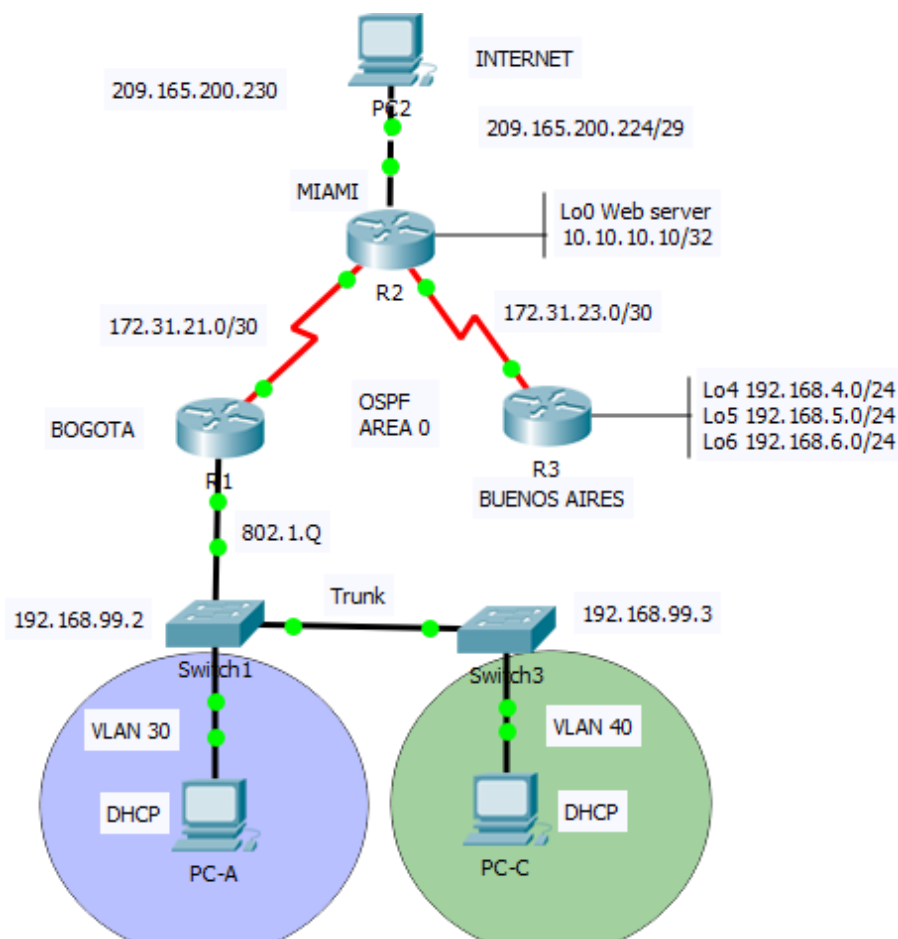
Ping statistics for 172.29.4.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
```

ESCENARIO 2

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, 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

FIGURA 19 TOPOLOGÍA ESCENARIO 2



Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario

```
Router(config)#hostname Bogotá
Bogotá(config)#No ip domain lookup
Bogotá(config)#enable secret class
Bogotá(config)#line con 0
Bogotá(config-line)#password cisco
Bogotá(config-line)#login
Bogotá(config-line)#line vty 0 4
Bogotá(config-line)#password cisco
Bogotá(config-line)#login
Bogotá(config-line)#exit
Bogotá(config)#service password-encryption
Bogotá(config)#banner motd #***** Prohibido el acceso no autorizado a
este equipo***** #
Bogotá(config)#interface serial 0/0/0
Bogotá(config-if)#ip address 172.31.21.1 255.255.255.252
Bogotá(config-if)#clock rate 64000
Bogotá(config-if)#no shutdown
```

```
Router#conf ter
Router(config)#hostname MIAMI
MIAMI(config)#No ip domain lookup
MIAMI(config)#enable secret class
MIAMI(config)#line con 0
MIAMI(config-line)#password cisco
MIAMI(config-line)#login
MIAMI(config-line)#line vty 0 4
MIAMI(config-line)#password cisco
MIAMI(config-line)#login
MIAMI(config-line)#exit
MIAMI(config)#service password-encryption
MIAMI(config)#banner motd #***** Prohibido el acceso no autorizado a
este equipo***** #
MIAMI(config)#interface serial 0/0/0
MIAMI(config-if)#ip address 172.31.23.1 255.255.255.252
MIAMI(config-if)#clock rate 64000
MIAMI(config-if)#no shutdown
MIAMI(config)#interface serial 0/0/1
MIAMI(config-if)#ip address 172.31.22.2 255.255.255.252
MIAMI(config-if)#no shutdown
MIAMI(config)#interface fa 0/0
```

```
MIAMI(config-if)#ip address 209.165.200.225 255.255.255.248
MIAMI(config-if)#no shutdown
MIAMI(config)#interface loopback 0
MIAMI(config-if)#ip address 10.10.10.10 255.255.255.255
```

```
Router(config)#hostname BuenosAires
BuenosAires(config)#No ip domain lookup
BuenosAires(config)#enable secret class
BuenosAires(config)#line con 0
BuenosAires(config-line)#password cisco
BuenosAires(config-line)#login
BuenosAires(config-line)#line vty 0 4
BuenosAires(config-line)#password cisco
BuenosAires(config-line)#login
BuenosAires(config-line)#exit
BuenosAires(config)#service password-encryption
BuenosAires(config)#banner motd #***** Prohibido el acceso no
autorizado a este equipo***** #
BuenosAires(config)#inter serial 0/0/1
BuenosAires(config-if)#ip address 172.31.23.2 255.255.255.252
BuenosAires(config-if)#no shutdown
BuenosAires(config)#interface loopback 4
BuenosAires(config-if)#ip address 192.168.4.1 255.255.255.0
BuenosAires(config-if)#no shutdown
BuenosAires(config)#interface loopback 5
BuenosAires(config-if)#ip address 192.168.5.1 255.255.255.0
BuenosAires(config-if)#no shutdown
BuenosAires(config)#interface loopback 6
BuenosAires(config-if)#ip address 192.168.6.1 255.255.255.0
BuenosAires(config-if)#no shutdown
```

```
Switch(config)#hostname S1
S1(config)#No ip domain lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #***** Prohibido el acceso no autorizado a este
equipo***** #
```

```
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #***** Prohibido el acceso no autorizado a este
equipo***** #
```

1. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

TABLA 3 OSPF AREA 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

```
Bogotá(config)#router ospf 1
Bogotá(config-router)#router-id 1.1.1.1
Bogotá(config-router)#passive-interface f0/0.30
Bogotá(config-router)#passive-interface f0/0.40
Bogotá(config-router)#passive-interface f0/0.200
Bogotá(config-router)#network 172.31.21.0 0.0.0.3 área 0
Bogotá(config-router)#network 192.168.30.0 0.0.0.255 área 0
Bogotá(config-router)#network 192.168.40.0 0.0.0.255 área 0
Bogotá(config-router)#network 192.168.200.0 0.0.0.255 área 0
Bogotá(config-router)#
20:50:48: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/0 from
LOADING to FULL, Loading Done
Bogotá(config-router)#
```

```

MIAMI(config)#router ospf 1
MIAMI(config-router)#router-id 5.5.5.5
MIAMI(config-router)#passive-interface f0/0
MIAMI(config-router)#default-information originate
MIAMI(config-router)#network 172.31.21.0 0.0.0.3 área 0
20:50:48: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from
LOADING to FULL, Loading Done
MIAMI(config-router)#network 172.31.23.0 0.0.0.3 área 0
MIAMI(config-router)#network 10.10.10.10 0.0.0.0 área 0
MIAMI(config-router)#
20:54:21: %OSPF-5-ADJCHG: Process 1, Nbr 8.8.8.8 on Serial0/0/0 from
LOADING to FULL, Loading Done
MIAMI(config-router)#

```

```

BuenosAires(config)#router ospf 1
BuenosAires(config-router)#router-id 8.8.8.8
BuenosAires(config-router)#network 172.31.23.0 0.0.0.3 área 0
20:54:21: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from
LOADING to FULL, Loading Done
BuenosAires(config-router)#network 192.168.4.0 0.0.0.255 área 0
BuenosAires(config-router)#network 192.168.5.0 0.0.0.255 área 0
BuenosAires(config-router)#network 192.168.6.0 0.0.0.255 área 0
BuenosAires(config-router)#

```

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

```

Bogota#show ip 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
O    10.10.10.10 [110/65] via 172.31.21.2, 00:50:08, Serial0/0/0
  172.31.0.0/30 is subnetted, 2 subnets
C    172.31.21.0 is directly connected, Serial0/0/0
O    172.31.23.0 [110/128] via 172.31.21.2, 00:51:59, Serial0/0/0
  192.168.4.0/32 is subnetted, 1 subnets
O    192.168.4.1 [110/129] via 172.31.21.2, 00:48:17, Serial0/0/0
  192.168.5.0/32 is subnetted, 1 subnets

```

```
O 192.168.5.1 [110/129] via 172.31.21.2, 00:48:04, Serial0/0/0
  192.168.6.0/32 is subnetted, 1 subnets
O 192.168.6.1 [110/129] via 172.31.21.2, 00:48:04, Serial0/0/0
C 192.168.30.0/24 is directly connected, FastEthernet0/0.30
C 192.168.40.0/24 is directly connected, FastEthernet0/0.40
C 192.168.200.0/24 is directly connected, FastEthernet0/0.200
S* 0.0.0.0/0 is directly connected, Serial0/0/0
```

Bogota#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
5.5.5.5	0	FULL/ -	00:00:39	172.31.21.2	Serial0/0/0

Bogotá#

MIAMI#show ip route

```
10.0.0.0/32 is subnetted, 1 subnets
C 10.10.10.10 is directly connected, Loopback0
172.31.0.0/30 is subnetted, 2 subnets
C 172.31.21.0 is directly connected, Serial0/0/1
C 172.31.23.0 is directly connected, Serial0/0/0
192.168.4.0/32 is subnetted, 1 subnets
O 192.168.4.1 [110/65] via 172.31.23.2, 00:25:15, Serial0/0/0
  192.168.5.0/32 is subnetted, 1 subnets
O 192.168.5.1 [110/65] via 172.31.23.2, 00:25:15, Serial0/0/0
  192.168.6.0/32 is subnetted, 1 subnets
O 192.168.6.1 [110/65] via 172.31.23.2, 00:25:15, Serial0/0/0
O 192.168.30.0/24 [110/65] via 172.31.21.1, 00:25:15, Serial0/0/1
O 192.168.40.0/24 [110/65] via 172.31.21.1, 00:25:15, Serial0/0/1
O 192.168.200.0/24 [110/65] via 172.31.21.1, 00:25:15, Serial0/0/1
  209.165.200.0/29 is subnetted, 1 subnets
C 209.165.200.224 is directly connected, FastEthernet0/0
```

MIAMI#show ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
8.8.8.8	0	FULL/ -	00:00:32	172.31.23.2	Serial0/0/0
1.1.1.1	0	FULL/ -	00:00:32	172.31.21.1	Serial0/0/1

MIAMI#

BuenosAires#show ip route

```
10.0.0.0/32 is subnetted, 1 subnets
O 10.10.10.10 [110/65] via 172.31.23.1, 00:46:10, Serial0/0/1
  172.31.0.0/30 is subnetted, 2 subnets
O 172.31.21.0 [110/128] via 172.31.23.1, 00:46:10, Serial0/0/1
C 172.31.23.0 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
O 192.168.30.0/24 [110/129] via 172.31.23.1, 00:46:10, Serial0/0/1
O 192.168.40.0/24 [110/129] via 172.31.23.1, 00:46:10, Serial0/0/1
O 192.168.200.0/24 [110/129] via 172.31.23.1, 00:46:10, Serial0/0/1
S* 0.0.0.0/0 is directly connected, Serial0/0/1
BuenosAires#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
5.5.5.5 0 FULL/ - 00:00:33 172.31.23.1 Serial0/0/1
BuenosAires#

```

- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface.

```

Bogota#show ip ospf interface se0/0/0
Serial0/0/0 is up, line protocol is up
Internet address is 172.31.21.1/30, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type POINT-TO-POINT, Cost:
64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:05
Index 4/4, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 5.5.5.5
Suppress hello for 0 neighbor(s)

```

```

MIAMI#show ip ospf interface se0/0/1
Serial0/0/1 is up, line protocol is up
Internet address is 172.31.21.2/30, Area 0
Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT, Cost:
64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:09
Index 2/2, flood queue length 0

```



```
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 1.1.1.1
Suppress hello for 0 neighbor(s)
```

```
MIAMI#show ip ospf interface se0/0/0
Serial0/0/0 is up, line protocol is up
Internet address is 172.31.23.1/30, Area 0
Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT, Cost:
64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:09
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 8.8.8.8
Suppress hello for 0 neighbor(s)
```

```
BuenosAires#show ip ospf interface se0/0/1
Serial0/0/1 is up, line protocol is up
Internet address is 172.31.23.2/30, Area 0
Process ID 1, Router ID 8.8.8.8, Network Type POINT-TO-POINT, Cost:
64
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:07
Index 4/4, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 1 , Adjacent neighbor count is 1
Adjacent with neighbor 5.5.5.5
Suppress hello for 0 neighbor(s)
```

- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

```
Bogota#show ip ospf
Routing Process "ospf 1" with ID 1.1.1.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 4
    Area has no authentication
    SPF algorithm executed 36 times
    Area ranges are
    Number of LSA 5. Checksum Sum 0x030dd3
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

```
Bogota#sh run
!
router ospf 1
router-id 1.1.1.1
log-adjacency-changes
passive-interface FastEthernet0/0.30
passive-interface FastEthernet0/0.40
passive-interface FastEthernet0/0.200
network 172.31.21.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
```

```
MIAMI#show ip ospf
Routing Process "ospf 1" with ID 5.5.5.5
Supports only single TOS(TOS0) routes
```

```
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm executed 30 times
    Area ranges are
    Number of LSA 5. Checksum Sum 0x0303d8
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

MIAMI#

MIAMI#show run

```
!
router ospf 1
router-id 5.5.5.5
log-adjacency-changes
passive-interface FastEthernet0/0
passive-interface loopback 0
network 172.31.21.0 0.0.0.3 area 0
network 172.31.23.0 0.0.0.3 area 0
network 10.10.10.10 0.0.0.0 area 0
default-information originate
```

BuenosAires#show ip ospf

```
Routing Process "ospf 1" with ID 8.8.8.8
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
```

```

Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
Area BACKBONE(0)
  Number of interfaces in this area is 4
  Area has no authentication
  SPF algorithm executed 28 times
  Area ranges are
  Number of LSA 5. Checksum Sum 0x0303d8
  Number of opaque link LSA 0. Checksum Sum 0x000000
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
  
```

BuenosAires#

BuenosAires#show run

```

!
router ospf 1
  router-id 8.8.8.8
  log-adjacency-changes
  passive-interface loopback 4
  passive-interface loopback 5
  passive-interface loopback 6
  network 172.31.23.0 0.0.0.3 area 0
  network 192.168.4.0 0.0.0.255 area 0
  network 192.168.5.0 0.0.0.255 area 0
  network 192.168.6.0 0.0.0.255 area 0
  
```

2. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a **la topología de red establecida.**

TABLA 4 VLAN Y DIRECCIONAMIENTO

VLAN	Dirección MAC	Src MAC
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

Se marcan las Vlans

```
S1 (config)#vlan 30
S1 (config-vlan)#name Administración
S1 (config)#vlan 40
S1 (config-vlan)#name Mercadeo
S1 (config)#vlan 200
S1 (config-vlan)#name Mantenimiento
configuración puerto F0/3 modo troncal con S3
S1 (config)#int f0/3
S1 (config-if)#switchport mode trunk
S1 (config-if)#switchport trunk native vlan 1
```

```
configuración puerto F0/24 hacia Bogotá
S1 (config-if)#int f0/24
S1 (config-if)#switchport mode trunk
S1 (config-if)#switchport trunk native vlan 1
S1 (config-if)#no shutdown
```

Configuración modo acceso de puertos

```
S1 (config-if)#int range fa0/1-2, fa0/4-23, g0/1-2
S1 (config-if-range)#switchport mode access
```

```
S3#conf t
S3 (config)#vlan 30
S3 (config-vlan)#name Administración
S3 (config)#vlan 40
S3 (config-vlan)#name Mercadeo
S3 (config)#vlan 200
S3 (config-vlan)#name Mantenimiento
S3 (config-vlan)#
```

```
configuración puerto F0/3 modo troncal con S3
S3 (config)#int F0/3
S3 (config-if)#switchport mode trunk
S3 (config-if)#switchport trunk native vlan 1
```

```
Puerto de enlace S3 VLAN Mantenimiento
S3 (config)#ip default-gateway 192.168.99.1
```

```
Configuración modo acceso de puertos
S3(config)#int range fa0/1-2, fa0/4-23, g0/1-2
S3(config-if-range)#switchport mode Access
```

Se configura ruta por defecto

```
Bogotá(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
```

```
Bogotá(config)#int f0/0.30
```

```
Bogotá(config-subif)#description accouting LAN
```

```
Bogotá(config-subif)#encapsulation dot1q 30
```

```
Bogotá(config-subif)#ip address 192.168.30.1 255.255.255.0
```

```
Bogotá(config-subif)#int f0/0.40
```

```
Bogotá(config-subif)#description accouting LAN
```

```
Bogotá(config-subif)#encapsulation dot1q 40
```

```
Bogotá(config-subif)#ip address 192.168.40.1 255.255.255.0
```

```
Bogotá(config-subif)#int f0/0.200
```

```
Bogotá(config-subif)#description accouting LAN
```

```
Bogotá(config-subif)#encapsulation dot1q 200
```

```
Bogotá(config-subif)#ip address 192.168.200.1 255.255.255.0
```

```
Bogotá(config)#inter fa0/0
```

```
Bogotá(config-if)#no shutdown
```

3. En el Switch 3 deshabilitar DNS lookup

```
S3(config)#No ip domain lookup
```

4. Asignar direcciones IP a los Switches acorde a los lineamientos.

Vlan Mantenimiento

```
S1(config)#int vlan 200
```

```
S1 (config-if)#ip address 192.168.99.2 255.255.255.0
```

Puerto de enlace S3 VLAN Mantenimiento

```
S3 (config)#int vlan 200
```

```
S3 (config-if)#ip address 192.168.99.3 255.255.255.0
```

5. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

Puerto F0/1 y desactivacion demas puertos

```
S1 (config)#int f0/1
```

```
S1(config-if)#switchport mode access
```

```
S1(config-if)#switchport access vlan 30
```

```
S1(config-if)#int range fa0/2, fa0/4-23, g0/1-2
```

```
S1(config-range)#shutdown
```

Puerto F0/1 y desactivacion demas puertos

S3 (config)#int f0/1

S3 (config-if)#switchport mode access

S3 (config-if)#switchport access vlan 40

S3 (config-if)#int range fa0/2, fa0/4-23, g0/1-2

S3(config-range)#shutdown

6. Implement DHCP and NAT for IPv4

7. Configurar R1 como servidor DHCP para las VLANs 30 y 40.

Bogotá(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30

Bogotá(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30

Bogotá(config)#ip dhcp pool ADMINISTRACION

Bogotá(dhcp-config)#network 192.168.30.0 255.255.255.0

Bogotá(dhcp-config)#default-router 192.168.30.1

Bogotá(dhcp-config)#dns-server 10.10.10.11

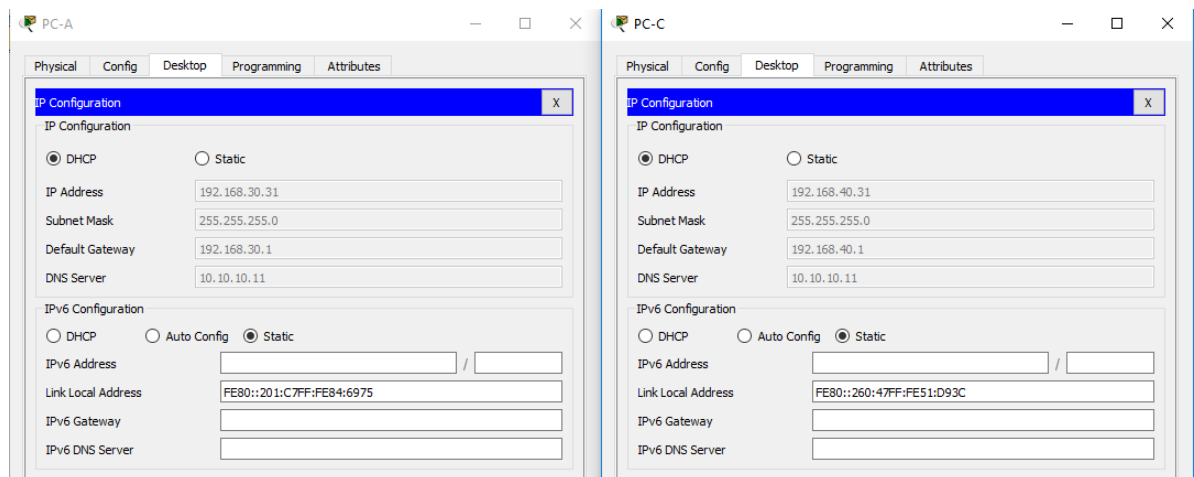
Bogotá(config)#ip dhcp pool MERCADEO

Bogotá(dhcp-config)#network 192.168.40.0 255.255.255.0

Bogotá(dhcp-config)#default-router 192.168.40.1

Bogotá(dhcp-config)#dns-server 10.10.10.11

FIGURA 20 SE VALIDA DHCP EN LOS HOST DE VLAN 30 Y 40 ESCENARIO 2



8. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

TABLA 5 DATOS PARA DHCP

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

9. Configurar NAT en R2 para permitir que los host puedan salir a internet.

```

MIAMI(config)#access-list 1 permit 192.168.30.0 0.0.0.255
MIAMI(config)#access-list 1 permit 192.168.40.0 0.0.0.255
MIAMI(config)#ip nat pool public_access 209.165.200.225 209.165.200.230
netmask 255.255.255.248
MIAMI(config)#ip nat inside source list 1 pool public_access overload
MIAMI(config)#interface serial 0/0/1
MIAMI(config-if)#ip nat inside
MIAMI(config-if)#interface serial 0/0/0
MIAMI(config-if)#ip nat inside
MIAMI(config-if)#inter fa0/0
MIAMI(config-if)#ip nat outside
MIAMI(config-if)#ex

```

```

MIAMI#sh ip nat translations
Pro Inside global   Inside local   Outside local   Outside global
icmp 209.165.200.225:18 192.168.30.31:18 209.165.200.230:18
209.165.200.230:18
icmp 209.165.200.225:19 192.168.30.31:19 209.165.200.230:19
209.165.200.230:19
icmp 209.165.200.225:20 192.168.30.31:20 209.165.200.230:20
209.165.200.230:20
icmp 209.165.200.225:21 192.168.30.31:21 209.165.200.230:21
209.165.200.230:21
icmp 209.165.200.225:26 192.168.30.31:26 172.16.30.30:26
172.16.30.30:26
icmp 209.165.200.225:27 192.168.30.31:27 172.16.30.30:27
172.16.30.30:27
MIAMI#

```


10. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

- Lista para denegar acceso hacia la interfaz(internet)
209.165.200.230 desde el host 192.168.40.31
- Lista para denegar acceso hacia la interfaz (internet)
209.165.200.230 desde la red 192.168.4.0 del router Buenos aires.

```
!  
interface FastEthernet0/0  
ip address 209.165.200.225 255.255.255.248  
ip access-group 1 out  
ip nat outside  
duplex auto  
speed auto  
!  
access-list 1 deny host 192.168.40.31  
access-list 1 deny 192.168.4.0 0.0.3.255  
access-list 1 permit 192.168.30.0 0.0.0.255  
access-list 1 permit 192.168.40.0 0.0.0.255  
access-list 1 permit any  
!  
MIAMI#
```

FIGURA 21 PING A IP INTERNET RECHAZADA

```

C:\>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Reply from 172.31.21.2: Destination host unreachable.
Reply from 172.31.21.2: Destination host unreachable.
Reply from 172.31.21.2: Destination host unreachable.
Reply from 172.31.21.2: Destination host unreachable.

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=4ms TTL=254
Reply from 209.165.200.225: bytes=32 time=11ms TTL=254
Reply from 209.165.200.225: bytes=32 time=28ms TTL=254
Reply from 209.165.200.225: bytes=32 time=11ms TTL=254

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 28ms, Average = 13ms
  
```

FIGURA 22 PING A IP INTERNET RECHAZADA

```

BuenosAires#ping
Protocol [ip]:
Target IP address: 209.165.200.230
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.4.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2
seconds:
Packet sent with a source address of 192.168.4.1
UUUUU
Success rate is 0 percent (0/5)
  
```

11. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

- Permitir telnet desde la vlan 30 hacia interfaz 172.31.21.2
 - Denegar telnet desde la vlan 40 hacia interfaz 172.31.21.2
- ```
!
interface FastEthernet0/0.30
description accounting LAN
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0
ip access-group 101 in
!
interface FastEthernet0/0.40
description accounting LAN
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0
ip access-group 101 in
!
!!
access-list 101 permit tcp 192.168.30.0 0.0.0.255 172.31.21.0 0.0.0.3
eq telnet
access-list 101 deny tcp 192.168.40.0 0.0.0.255 172.31.21.0 0.0.0.3
eq telnet
access-list 101 permit ip any any
!
Bogota#
```

FIGURA 23 TELNET DESDE VLAN 30 Y LUEGO DESDE VLAN 40

```
C:\>telnet 172.31.21.2 ✓
Trying 172.31.21.2 ...Open***** Prohibido el acceso no autorizado a este equipo*****

User Access Verification

Password:
MIAMI>

Top

C:\>telnet 172.31.21.2 ✗
Trying 172.31.21.2 ...
% Connection timed out; remote host not responding
C:\>
```

12. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

Se realizan pruebas de ping desde PC-A hacia todas las redes y responde bien, se realiza ping a internet ok, prueba a loopback4, 5 y 6 responde ok, prueba a servidor web responde ok.

FIGURA 24 PING ENTRE LAS REDES

```
C:\>ping 192.168.4.1

Pinging 192.168.4.1 with 32 bytes of data:

Reply from 192.168.4.1: bytes=32 time=4ms TTL=253
Reply from 192.168.4.1: bytes=32 time=12ms TTL=253
Reply from 192.168.4.1: bytes=32 time=29ms TTL=253
Reply from 192.168.4.1: bytes=32 time=13ms TTL=253

Ping statistics for 192.168.4.1:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 4ms, Maximum = 29ms, Average = 14ms

C:\>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:

Reply from 10.10.10.10: bytes=32 time=2ms TTL=254
Reply from 10.10.10.10: bytes=32 time=12ms TTL=254
Reply from 10.10.10.10: bytes=32 time=1ms TTL=254
Reply from 10.10.10.10: bytes=32 time=1ms TTL=254

Ping statistics for 10.10.10.10:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 1ms, Maximum = 12ms, Average = 4ms

C:\>ping 192.168.30.31

Pinging 192.168.30.31 with 32 bytes of data:

Reply from 192.168.30.31: bytes=32 time=3ms TTL=128
Reply from 192.168.30.31: bytes=32 time=10ms TTL=128
Reply from 192.168.30.31: bytes=32 time=14ms TTL=128
Reply from 192.168.30.31: bytes=32 time=18ms TTL=128

Ping statistics for 192.168.30.31:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 3ms, Maximum = 18ms, Average = 11ms
```

Se realiza prueba de tracert hacia las redes mencionadas anteriormente y son completadas exitosamente.

FIGURA 25 VALIDACION DE TRACERT

```
C:\>tracert 192.168.4.1

Tracing route to 192.168.4.1 over a maximum of 30 hops:

 1 0 ms 0 ms 15 ms 192.168.40.1
 2 13 ms 10 ms 11 ms 172.31.21.2
 3 13 ms 12 ms 12 ms 192.168.4.1

Trace complete.

C:\>tracert 192.168.6.1

Tracing route to 192.168.6.1 over a maximum of 30 hops:

 1 0 ms 0 ms 2 ms 192.168.40.1
 2 13 ms 12 ms 11 ms 172.31.21.2
 3 2 ms 13 ms 4 ms 192.168.6.1

Trace complete.

C:\>tracert 10.10.10.10

Tracing route to 10.10.10.10 over a maximum of 30 hops:

 1 0 ms 0 ms 0 ms 192.168.40.1
 2 4 ms 16 ms 0 ms 10.10.10.10

Trace complete.
```

## CONCLUSIONES

Al solucionar cada escenario se logran comprender los diferentes conceptos y habilidades de la necesidad de realizar una configuración básica con sus diferentes parámetros de acceso para tener una conexión y seguridad inicial.

Con el desarrollo de los escenarios se mejoran las habilidades de solución y diseño para una necesidad con seguridad, conectividad y acceso entre diferentes redes privadas y acceso a internet.

Al integrar las diferentes configuraciones se desarrollan las habilidades y se comprende mejor las funcionalidades de cada configuración.

## REFERENCIAS BIBLIOGRAFICAS

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1>

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1>

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1>