# SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO

MARLIO ANDRES ORTIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA (ECBTI)
INGENIERIA DE SISTEMAS
2020

# SOLUCION DE DOS ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGIA CISCO

MARLIO ANDRES ORTIZ

INFORME FINAL
PRESENTADO PARA OBTENER EL TÍTULO DE
INGENIERO DE SISTEMAS

DOCENTE
HÉCTOR JULIÁN PARRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA (ECBTI)
INGENIERIA DE SISTEMAS
2020

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

17 de mayo de 2020

**Dedicatoria**

Dedico este proyecto final a mi familia, quienes fueron una base fundamental para que fuera capaz de llevar esta actividad a su culminación, mis ganas por salir adelante y lograr cada una de las metas que me he propuesto, mis sueños, que gracias al apoyo que me brindaron cada día fui capaz de conseguir este logro.

## AGRADECIMIENTOS

Quiero darle primero que todo gracias a Dios por ser mi guía en este proceso, a mi familia y un agradecimiento profundo a la Universidad Nacional Abierta y a Distancia de Florencia, a sus tutores, directores, puesto que gracias a sus conocimientos aportaron para lograr hoy este nuevo título.

## CONTENIDO

## LISTA DE TABLAS

Pág.

## LISTA DE FIGURAS

Pág.

## RESUMEN

Se realizan dos escenarios de pruebas de habilidades cada uno con tematicas diferentes las cuales traen consigo su topologia, las conexiones y configuracion de dispositivos desarrollados con la herramienta de simulacion Cisco Packet Tracer.

A la hora de llevar a cabo la solucion de dichos modulos de CCNA, se obtiene consigo los pilares que seran de mucha ayuda para el desarrollo de dichas pruebas de habilidades puesto que con el conocimiento que obtenemos en estos modulos se da la capacidad de comprender tematicas como IPv4 e IPv6, seguridad de switches, Protocolo OSPF, configuracion de host dinamicos DHCP, control de acceso ACL, encapsulamiento PPP y su autenticacion.



**Palabras claves:**

-Enrutamiento
-Protocolos
-Dispositivos
-Conexiones

# 1. INTRODUCCIÓN

El presente trabajo está construido con las actividades evaluativas propuestas en el Diplomado de profundización CCNA, desarrollando en estos ejercicios con aspectos de networking que se han ido manejando a lo largo del curso. En este se hace referencia a las pruebas de habilidades las cuales contienen dos escenarios que tienen como finalidad poner a prueba todos los conocimientos que han sido aprendidos en el curso.

Este proceso es realizado en la herramienta Packet Tracer, en la cual podremos observar el manejo de configuración básica del router, configuraciones de seguridad, implementación DHCP y NAT, enrutamiento, configuración de PAT, etc. En el primer escenario para ser más específico se manejan temas der red con conectividad IPv4 y IPv6 con protocolos dinámicos, y en el segundo escenario se ve la comunicación entre router y servicio ISP.

# 2. PLANTEAMIENTO DEL PROBLEMA

## 2.1 DEFINICION DEL PROBLEMA

El diplomado Cisco es una de las opciones que ofrece la universidad como opciones de grado, la cual se base en proponer pruebas de habilidades prácticas la cual está construida por dos escenarios con topología distinta, que pondrá a prueba todo lo aprendido a lo largo del curso.

## 2.3 JUSTIFICACIÓN

La comprensión y desarrollo de las pruebas de habilidades prácticas propuestas en el diplomado permite el fortalecimiento de todos los conocimientos y bases teóricas necesarias para el diseño de redes y configuración de las mismas. Para este se contó con una metodología de carácter virtual, basada en exámenes, trabajos y acompañamiento del tutor para la comprensión del mismo, a su vez la implementación de la herramienta de simulación Cisco Packet Tracer.

# 3. OBJETIVOS

## 3.1 OBJETIVO GENERAL

Analizar los procedimientos para el desarrollo de competencias y habilidades adquiridas en el trascurso del diplomado.

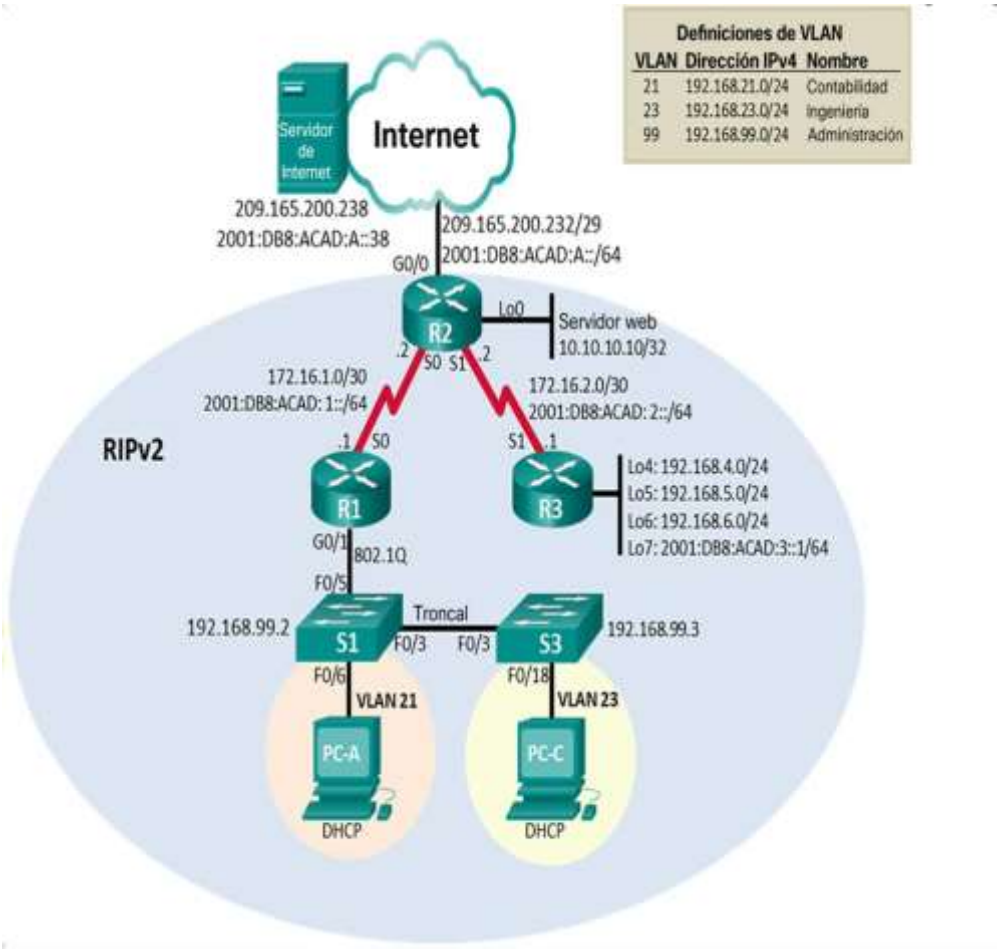
## 3.2 OBJETIVOS ESPECÍFICOS

- Implementar la herramienta Packet Tracer como gestora en la configuración de redes que permitan la conectividad IPV5 e IPV6, configuración de seguridad, protocolos de configuración de host dinámico.
- Configurar dispositivos conectados en ciudades distintas implementando el protocolo OSPF, brindando servicios DHCP.

## 4. ESCENARIO 1

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

**Topología**



## Parte 1: Inicializar dispositivos

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

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

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

| Tarea | Comando de IOS |
|---|---|
| Eliminar el archivo startup-config de todos los routers | Erase startup-config |
| Volver a cargar todos los routers | Reload |
| Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior | Erase startup-config Delete vlan.dat |
| Volver a cargar ambos switches | Reload |
| Verificar que la base de datos de VLAN no esté en la memoria flash en ambos switches | Show flash |

```
Router>enable
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]

Switch>enable
Switch#erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete

Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:/vlan.dat? [confirm]
%Error deleting flash:/vlan.dat (No such file or directory)

Switch#reload
Proceed with reload? [confirm]

Switch#show flash
Directory of flash:/

    1  -rw-     4414921          <no date>  c2960-lanbase-mz.
122-25.FX.bin
```

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

### Paso 1: Configurar la computadora de Internet

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

| Elemento o tarea de configuración | Especificación |
|---|---|
| Dirección IPv4 | 209.165.200.238 |
| Máscara de subred para IPv4 | 255.255.255.248 |
| Gateway predeterminado | 209.165.200.233 |
| Dirección IPv6/subred | 2001:DB8:ACAD:A::38/64 |
| Gateway predeterminado IPv6 | 2001:DB8:ACAD:A::1 |

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

### Paso 2: Configurar R1

Las tareas de configuración para R1 incluyen las siguientes:

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

| | |
|---|---|
| Interfaz S0/0/0 | Establezca la descripción<br>Establecer la dirección IPv4 Consultar el diagrama de topología para conocer la información de direcciones<br>Establecer la dirección IPv6 Consultar el diagrama de topología para conocer la información de direcciones<br>Establecer la frecuencia de reloj en 128000 Activar la interfaz |
| Rutas predeterminadas | Configurar una ruta IPv4 predeterminada de S0/0/0<br>Configurar una ruta IPv6 predeterminada de S0/0/0 |

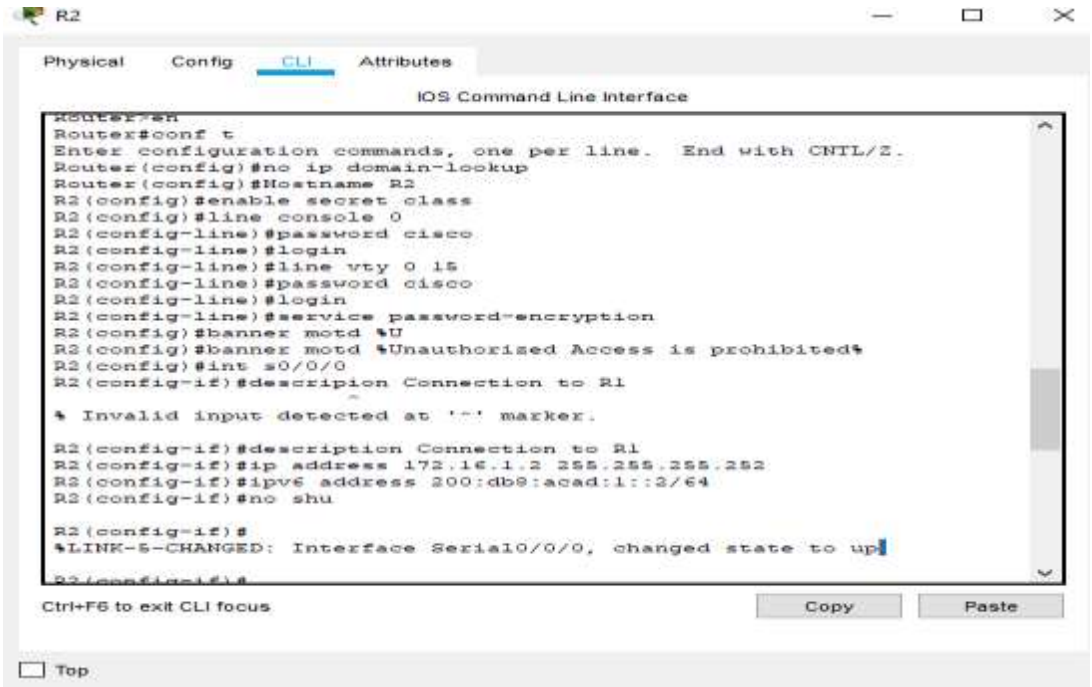
**Nota:** Todavía no configure G0/1.

### Paso 3: Configurar R2

La configuración del R2 incluye las siguientes tareas:

| **Elemento o tarea de configuración** | **Especificación** |
|---|---|
| Desactivar la búsqueda DNS | |
| 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 | |
| Habilitar el servidor HTTP | |
| Mensaje MOTD | Se prohíbe el acceso no autorizado. |
| Interfaz S0/0/0 | Establezca la descripción<br>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.<br>Activar la interfaz |

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



### Paso 4: Configurar R3

La configuración del R3 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | |
| 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 | |
| Mensaje MOTD | Se prohíbe el acceso no autorizado. |
| Interfaz S0/0/1 | Establecer la descripción<br>Establezca la dirección IPv4. Utilizar la siguiente dirección disponible en la subred.<br>Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones.<br>Activar la interfaz |
| Interfaz loopback 4 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. |
| Interfaz loopback 5 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. |
| Interfaz loopback 6 | Establezca la dirección IPv4. Utilizar la primera dirección disponible en la subred. |
| Interfaz loopback 7 | Establezca la dirección IPv6. Consulte el diagrama de topología para conocer la información de direcciones. |
| Rutas predeterminadas | |

### Paso 5: Configurar S1

La configuración del S1 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Desactivar la búsqueda DNS | |
| 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. |

### Paso 6: 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 | |
| Mensaje MOTD | Se prohíbe el acceso no autorizado. |

### Paso 7: Verificar la conectividad de la red

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

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

| 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 | Success |

```
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/5 ms


R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/7 ms
```

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

### Paso 1: Configurar S1

La configuración del S1 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| 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 | |

**Paso 2: Configurar el S3**

La configuración del S3 incluye las siguientes tareas:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear la base de datos de VLAN | 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 | |

**Paso 3: Configurar R1**

Las tareas de configuración para R1 incluyen las siguientes:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar la subinterfaz 802.1Q .21 en G0/1 | Descripción: LAN de Contabilidad<br>Asignar la VLAN 21<br>Asignar la primera dirección disponible a esta interfaz |
| Configurar la subinterfaz 802.1Q .23 en G0/1 | Descripción: LAN de Ingeniería<br>Asignar la VLAN 23<br>Asignar la primera dirección disponible a esta interfaz |
| Configurar la subinterfaz 802.1Q .99 en G0/1 | Descripción: LAN de Administración<br>Asignar la VLAN 99<br>Asignar la primera dirección disponible a esta interfaz |
| Activar la interfaz G0/1 | |

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

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

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

| Desde | A | Dirección IP | Resultados de ping |
|---|---|---|---|
| S1 | R1, dirección VLAN 99 | 192.168.99.1 | 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) |

```
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

S3#ping 192.168.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.23.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.168.21.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.21.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms
```

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

### Paso 1: Configurar RIPv2 en el R1

Las tareas de configuración para R1 incluyen las siguientes:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar RIP versión 2 | |
| Anunciar las redes conectadas directamente | Asigne todas las redes conectadas directamente. |
| Establecer todas las interfaces LAN como pasivas | |
| Desactive la sumarización automática | |

```
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
```

### Paso 2: Configurar RIPv2 en el R2

La configuración del R2 incluye las siguientes tareas:

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

```
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
```

### Paso 3: Configurar RIPv3 en el R2

La configuración del R3 incluye las siguientes tareas:

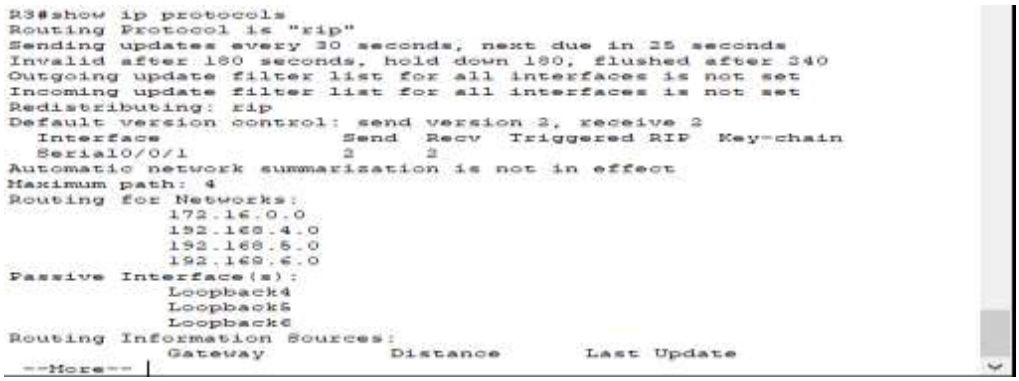
| Elemento o tarea de configuración | Especificación |
|---|---|
| Configurar RIP versión 2 | |
| Anunciar redes IPv4 conectadas directamente | |
| Establecer todas las interfaces de LAN IPv4 (Loopback) como pasivas | |
| Desactive la sumarización automática. | |

```
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
```

### Paso 4: Verificar la información de RIP

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

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




```
R3#show ip route rip
     10.0.0.0/32 is subnetted, 1 subnets
R       10.10.10.10 [120/1] via 172.16.2.2, 00:00:26, Serial0/0/1
     172.16.0.0/16 is variably subnetted, 3 subnets, 2 masks
R       172.16.1.0/30 [120/1] via 172.16.2.2, 00:00:26, Serial0/0/1
     192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
R    192.168.21.0/24 [120/2] via 172.16.2.2, 00:00:26, Serial0/0/1
R    192.168.23.0/24 [120/2] via 172.16.2.2, 00:00:26, Serial0/0/1
R    192.168.99.0/24 [120/2] via 172.16.2.2, 00:00:26, Serial0/0/1
```

```
R3#show run
Building configuration...

Current configuration : 1530 bytes
!
version 15.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
```

## Parte 5: Implementar DHCP y NAT para IPv4

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

Las tareas de configuración para R1 incluyen las siguientes:

| Elemento o tarea de configuración | Especificación |
|---|---|
| Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas | |
| Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas | |
| Crear un pool de DHCP para la VLAN 21. | Nombre: ACCT<br>Servidor DNS: 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>Establecer el gateway predeterminado |
| Crear un pool de DHCP para la VLAN 23 | Nombre: ENGNR<br>Servidor DNS: 10.10.10.10<br>Nombre de dominio: ccna-sa.com<br>Establecer el gateway predeterminado |

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

La configuración del R2 incluye las siguientes tareas:

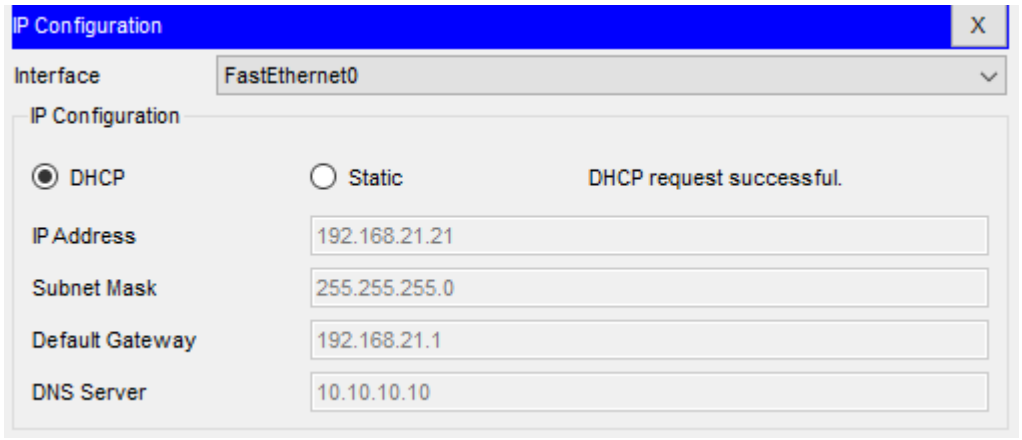
| Elemento o tarea de configuración | Especificación |
|---|---|
| Crear una base de datos local con una cuenta de usuario | Nombre de usuario: **webuser**<br>Contraseña: **cisco12345**<br>Nivel de privilegio: **15** |
| Habilitar el servicio del servidor HTTP | |
| Configurar el servidor HTTP para utilizar 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 | |

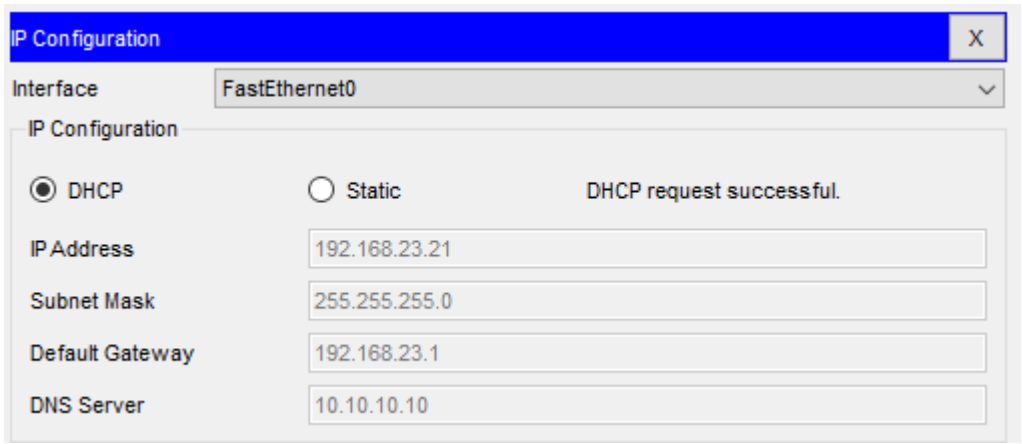
| | |
|---|---|
| Configurar la NAT dinámica dentro de una ACL privada | Lista de acceso: 1<br>Permitir la traducción de las redes de Contabilidad y de Ingeniería en el R1<br>Permitir la traducción de un resumen de las<br>redes LAN (loopback) en el R3 |
| Defina el pool de direcciones IP públicas utilizables. | Nombre del conjunto: **INTERNET**<br>El conjunto de direcciones incluye:<br>**209.165.200.225** – **209.165.200.228** |
| Definir la traducción de NAT dinámica | |

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

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

| Prueba | Resultados |
|---|---|
| Verificar que la PC-A haya adquirido información de IP del servidor de DHCP | DHCP request successful. |
| Verificar que la PC-C haya adquirido información de IP del servidor de DHCP | DHCP request successful. |
| Verificar que la PC-A pueda hacer ping a la PC-C<br>**Nota:** Quizá sea necesario deshabilitar el firewall de la PC. | Successful. |
| 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** | Successful. |




```
C:\>ping 192.168.23.21

Pinging 192.168.23.21 with 32 bytes of data:

Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time<1ms TTL=127
Reply from 192.168.23.21: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.23.21:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms
```

## Parte 6: Configurar NTP

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

```
R1#show ntp associations

address         ref clock       st   when     poll    reach  delay
offset            disp
 ~172.16.1.2    .INIT.          16   -        64      0      0.00
0.00              0.12
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~
configured
```

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

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

```
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]
```

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

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

```
R2#show ip access-list
Standard IP access list 1
    10 permit 192.168.21.0 0.0.0.255
    20 permit 192.168.23.0 0.0.0.255
    30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN-MGT
    10 permit host 172.16.1.1 (2 match(es))
```

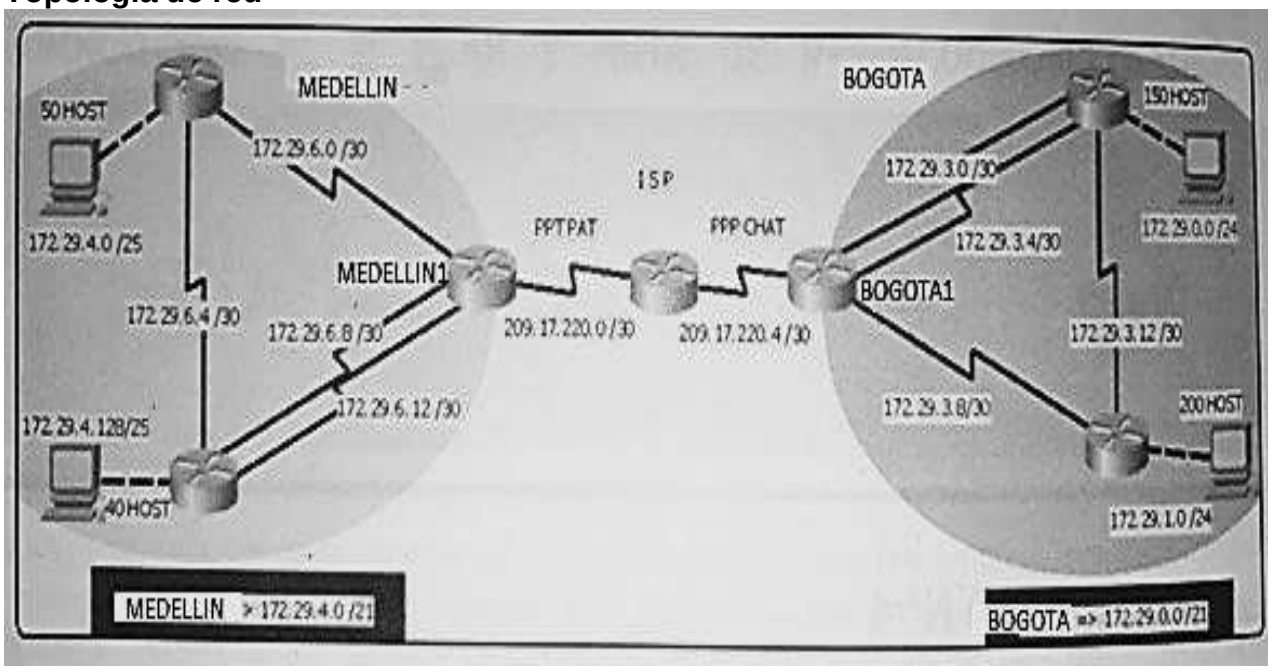
```
R2#clear ip ?
  bgp    Clear BGP connections
  dhcp   Delete items from the DHCP database
  nat    Clear NAT
  ospf   OSPF clear commands
  route  Delete route table entries
```

```
R2#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside
global
---  209.165.200.237   10.10.10.10        ---                ---
```

## 5. ESCENARIO 2

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

**Topología de red**



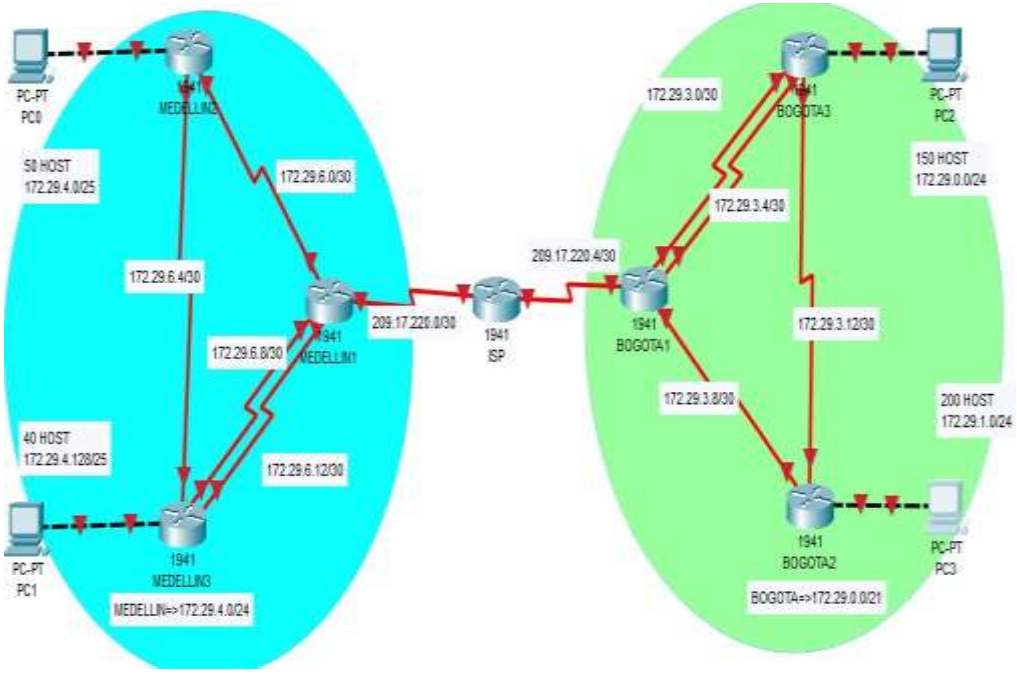
Este escenario plantea el uso de OSPF como protocolo de enrutamiento, considerando que se tendran rutas por defecto redistribuidas; asimismo, habilitar el encapsulamiento PPP y su autenticación.

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.

**Desarrollo**

Como trabajo inicial se debe realizar lo siguiente.

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



**Parte 1: Configuración del enrutamiento**

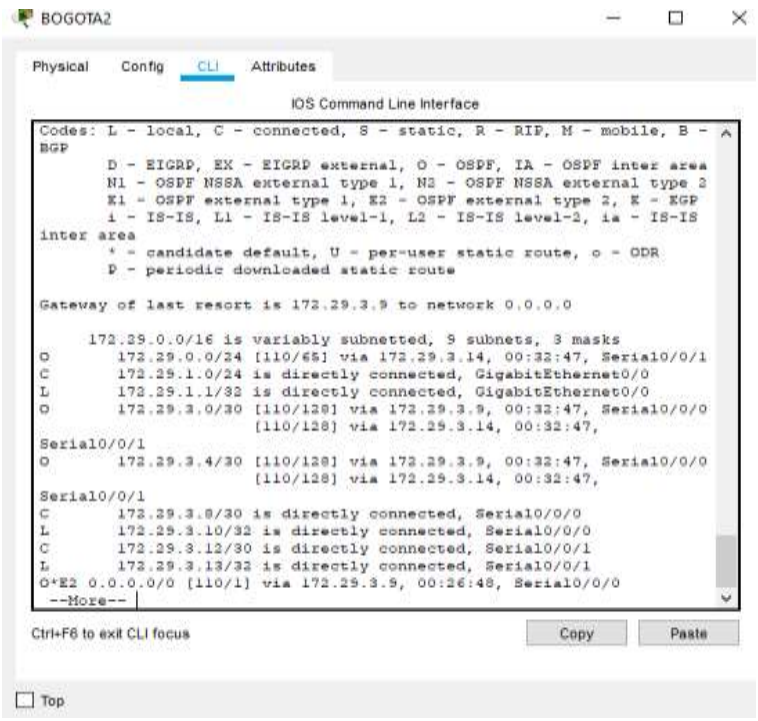
a. Configurar el enrutamiento en la red usando el protocolo OSPF versión 2, declare la red principal, desactive la sumarización automática.

```
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#net 172.29.6.0 0.0.0.3 area 0
MEDELLIN1(config-router)#net 172.29.6.8 0.0.0.3 area 0
MEDELLIN1(config-router)#net 172.29.6.12 0.0.0.3 area 0
MEDELLIN1(config-router)#

MEDELLIN2(config)#router ospf 1
MEDELLIN2(config-router)#net 172.29.4.0 0.0.0.255 area 0
MEDELLIN2(config-router)#net 172.29.6.0 0.0.0.3 area 0
MEDELLIN2(config-router)#net 172.29.6.4 0.0.0.3 area 0
MEDELLIN2(config-router)#
01:41:32: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.10 on Serial0/
from LOADING to FULL, Loading Done
MEDELLIN3(config)#router ospf 1
MEDELLIN3(config-router)#net 172.29.4.128 0.0.0.255 area 0
MEDELLIN3(config-router)#net 172.29.6.4 0.0.0.3 area 0
MEDELLIN3(config-router)#net 172.29.6.8 0.0.0.3 area 0
01:41:37: %OSPF-5-ADJCHG: Process 1, Nbr 172.29.6.5 on Serial0/1/0
from LOADING to FULL, Loading Done

MEDELLIN3(config-router)#net 172.29.6.8 0.0.0.3 area 0
MEDELLIN3(config-router)#net 172.29.6.12 0.0.0.3 area 0
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#net 172.29.3.0 0.0.0.3 area 1
BOGOTA1(config-router)#net 172.29.3.4 0.0.0.3 area 1
BOGOTA1(config-router)#net 172.29.3.8 0.0.0.3 area 1

BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#net 172.29.1.0 0.0.0.255 area 1
BOGOTA2(config-router)#net 172.29.3.8 0.0.0.3 area 1
BOGOTA2(config-router)#
01:45:15: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/0/0
from LOADING to FULL, Loading Done

BOGOTA2(config-router)#net 172.29.3.8 0.0.0.3 area 1
BOGOTA2(config-router)#net 172.29.3.12 0.0.0.3 area 1

BOGOTA2(config)#router ospf 1
BOGOTA2(config-router)#net 172.29.1.0 0.0.0.255 area 1
BOGOTA2(config-router)#net 172.29.3.8 0.0.0.3 area 1
BOGOTA2(config-router)#
01:45:15: %OSPF-5-ADJCHG: Process 1, Nbr 209.17.220.6 on Serial0/0/0
from LOADING to FULL, Loading Done

BOGOTA2(config-router)#net 172.29.3.8 0.0.0.3 area 1
BOGOTA2(config-router)#net 172.29.3.12 0.0.0.3 area 1
```

b. Los routers Bogota1 y Medellín deberán añadir a su configuración de enrutamiento una ruta por defecto hacia el ISP y, a su vez, redistribuirla dentro de las publicaciones de OSPF.

```
MEDELLIN1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.1
MEDELLIN1(config)#router ospf 1
MEDELLIN1(config-router)#default-information originate
MEDELLIN1(config-router)#exit
```

```
BOGOTA1(config)#ip route 0.0.0.0 0.0.0.0 209.17.220.5
BOGOTA1(config)#router ospf 1
BOGOTA1(config-router)#default-information originate
BOGOTA1(config-router)#exit
```




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

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

```
BOGOTA2#ping 209.17.220.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.17.220.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/8/35 ms

BOGOTA2#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 = 3/7/19 ms
```

**Parte 2: Tabla de Enrutamiento.**

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

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

c. Obsérvese en los routers Bogotá1 y Medellín1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

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

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

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

```
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, 10 subnets, 3 masks
C       172.29.2.12/30 is directly connected, Serial0/0/1
L       172.29.2.14/32 is directly connected, Serial0/0/1
O       172.29.4.0/25 [110/65] via 172.29.6.5, 00:03:35, Serial0/1/0
C       172.29.4.128/25 is directly connected, GigabitEthernet0/0
L       172.29.4.129/32 is directly connected, GigabitEthernet0/0
O       172.29.6.0/30 [110/128] via 172.29.6.5, 00:03:35, Serial0/1/0
C       172.29.6.4/30 is directly connected, Serial0/1/0
L       172.29.6.6/32 is directly connected, Serial0/1/0
C       172.29.6.8/30 is directly connected, Serial0/0/0
L       172.29.6.10/32 is directly connected, Serial0/0/0
```

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

Gateway of last resort is not set

     172.29.0.0/22 is subnetted, 2 subnets
S       172.29.0.0/22 [1/0] via 209.17.220.6
S       172.29.4.0/22 [1/0] via 209.17.220.2
     209.17.220.0/24 is variably subnetted, 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
```

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

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

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

**Parte 4: Verificación del protocolo OSPF.**

a. Verificar y documentar las opciones de enrutamiento configuradas en los routers, como el **passive interface** para la conexión hacia el ISP, la versión de OSPF y las interfaces que participan de la publicación entre otros datos.

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

```
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 209.29.6.13
  It is an autonomous system boundary router
  Redistributing External Routes from,
  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
    172.29.6.8 0.0.0.3 area 0
    172.29.6.12 0.0.0.3 area 0
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    209.29.6.13           110      00:26:18
  Distance: (default is 110)
```

```
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 209.17.220.6
  It is an autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.29.3.0 0.0.0.3 area 1
    172.29.3.4 0.0.0.3 area 1
    172.29.3.8 0.0.0.3 area 1
  Passive Interface(s):
    Serial0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    172.29.3.13           110      00:25:52
    172.29.3.14           110      00:25:57
    209.17.220.6          110      00:25:57
  Distance: (default is 110)
```

```
BOGOTA3#show ip ospf interface

GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.29.0.1/24, Area 1
  Process ID 1, Router ID 172.29.3.14, Network Type BROADCAST, Cost:
1
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
    No Hellos (Passive interface)
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 172.29.3.6/30, Area 1
  Process ID 1, Router ID 172.29.3.14, Network Type POINT-TO-POINT,
Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit
5
```

## Parte 5: Configurar encapsulamiento y autenticación PPP.

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

```
ISP(config)#username MEDELLIN1 password cisco
ISP(config)#int s0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed
state to down

ISP(config-if)#ppp authentication ppp
                                  ^
% Invalid input detected at '^' marker.

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

```
MEDELLIN1(config)#username ISP password cisco
MEDELLIN1(config)#int s0/0/0
MEDELLIN1(config-if)#encapsulation ppp
MEDELLIN1(config-if)#ppp authentication pap
MEDELLIN1(config-if)#ppp pap sent-username MEDELLIN1 password cisco
```

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

```
ISP(config)#username BOGOTA1 password cisco
ISP(config)#int s0/0/1
ISP(config-if)#encapsulation ppp
ISP(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed
state to down

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

```
BOGOTA1(config)#username ISP password cisco
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#encapsulation ppp
BOGOTA1(config-if)#ppp authentication chap
```

### Parte 6: Configuración de PAT.

a. En la topología, si se activa NAT en cada equipo de salida (Bogotá1 y Medellín1), los routers internos de una ciudad no podrán llegar hasta los routers internos en el otro extremo, sólo existirá comunicación hasta los routers Bogotá1, ISP y Medellín1.

b. Después de verificar lo indicado en el paso anterior proceda a configurar el NAT en el router Medellín1. Compruebe que la traducción de direcciones indique las interfaces de entrada y de salida. Al realizar una prueba de ping, la dirección debe ser traducida automáticamente a la dirección de la interfaz serial 0/1/0 del router Medellín1, cómo diferente puerto.

```
MEDELLIN1(config)#ip nat inside source list 1 interface s0/0/0
overload
MEDELLIN1(config)#acces-list 1 permit 172.29.4.0 0.0.3.255
                  ^
% Invalid input detected at '^' marker.

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
```

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

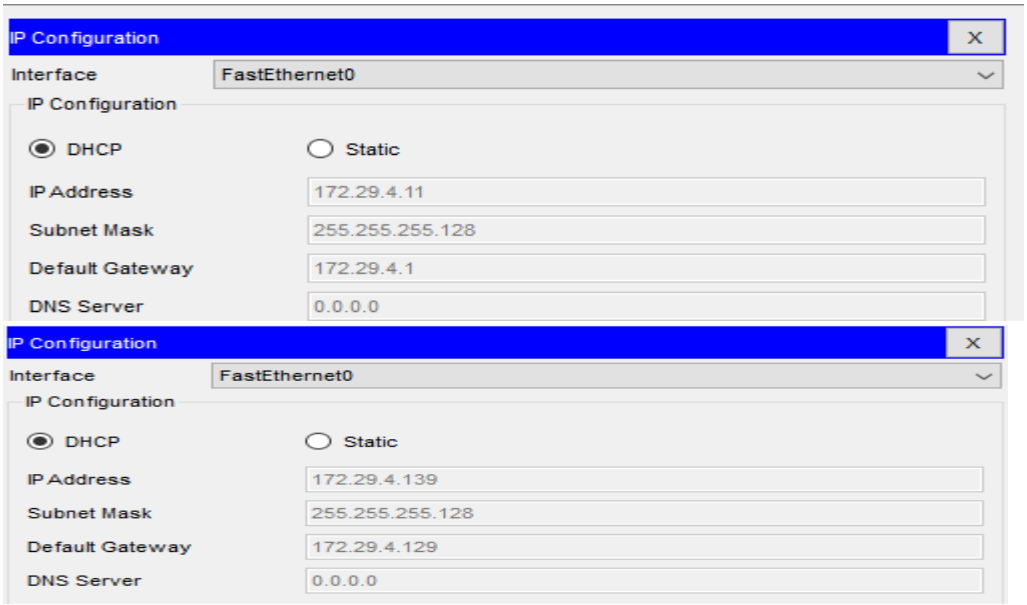
```
BOGOTA1(config)#ip nat inside source list 1 interface s0/0/0 overload
BOGOTA1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
BOGOTA1(config)#int s0/0/0
BOGOTA1(config-if)#ip nat outside
BOGOTA1(config-if)#int s0/0/1
BOGOTA1(config-if)#ip nat inside
BOGOTA1(config-if)#int s0/1/0
BOGOTA1(config-if)#ip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

### Parte 7: Configuración del servicio DHCP.

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

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

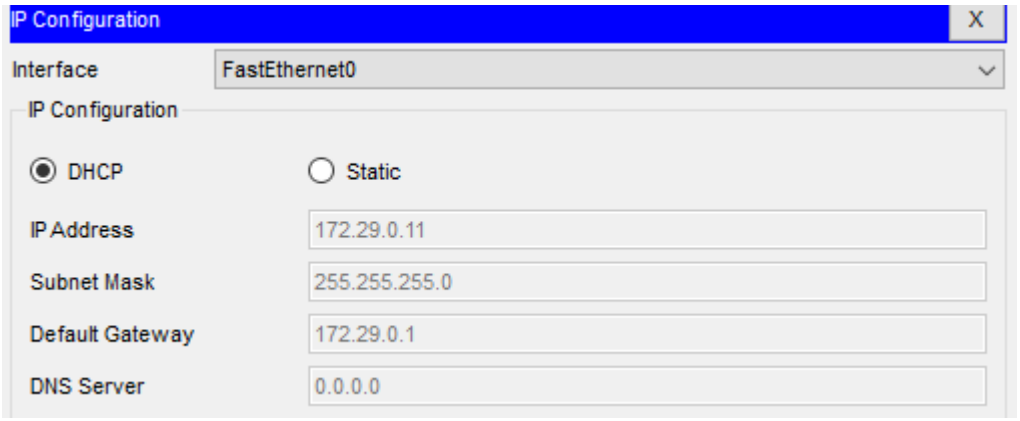
```
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.1 172.29.4.10
MEDELLIN2(config)#ip dhcp excluded-address 172.29.4.129 172.29.4.138
MEDELLIN2(config)#ip dhcp pool MEDELLIN2
MEDELLIN2(dhcp-config)#net 172.29.4.0 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.1
MEDELLIN2(dhcp-config)#dns-server 0.0.0.0
MEDELLIN2(dhcp-config)#ex
MEDELLIN2(config)#ip dhcp pool MEDELLIN3
MEDELLIN2(dhcp-config)#net 172.29.4.128 255.255.255.128
MEDELLIN2(dhcp-config)#default-router 172.29.4.129
MEDELLIN2(dhcp-config)#dns-server 0.0.0.0
MEDELLIN3(config)#int g0/0
MEDELLIN3(config-if)#ip helper-address 172.29.6.5
```

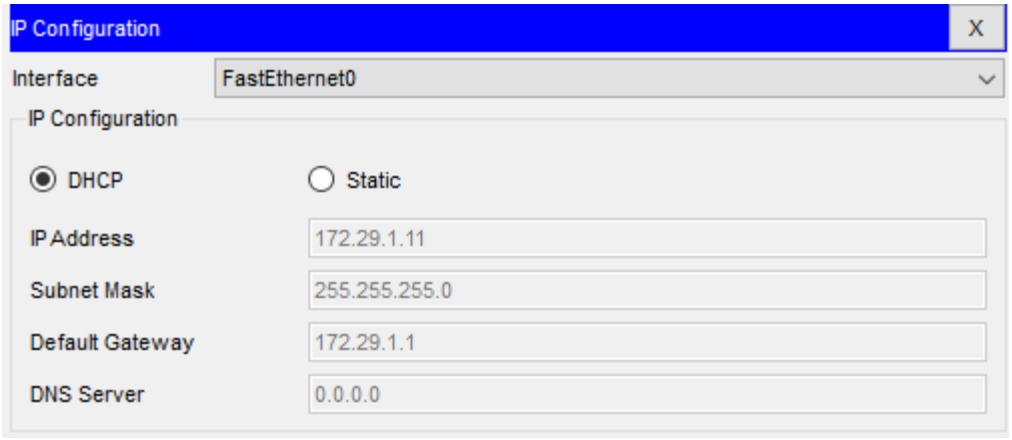



c. Configurar la red Bogotá2 y Bogotá3 donde el router Medellín2 debe ser el servidor DHCP para ambas redes Lan.

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

```
BOGOTA2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.10
BOGOTA2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.10
BOGOTA2(config)#ip dhcp pool BOGOTA2
BOGOTA2(dhcp-config)#net 172.29.1.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.1.1
BOGOTA2(dhcp-config)#dns-server 0.0.0.0
BOGOTA2(dhcp-config)#ex
BOGOTA2(config)#ip dhcp pool BOGOTA3
BOGOTA2(dhcp-config)#net 172.29.0.0 255.255.255.0
BOGOTA2(dhcp-config)#default-router 172.29.0.1
BOGOTA2(dhcp-config)#dns-server 0.0.0.0

BOGOTA3(config)#int g0/0
BOGOTA3(config-if)#ip helper-address 172.29.3.13
```


IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
172.29.0.11
Subnet Mask
255.255.255.0
Default Gateway
172.29.0.1
DNS Server
0.0.0.0


IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IP Address
172.29.1.11
Subnet Mask
255.255.255.0
Default Gateway
172.29.1.1
DNS Server
0.0.0.0

# 6. CONCLUSIONES

En el desarrollo del primer escenario se logra configurar una red en la cual se implementa la conectividad IPv4 e IPv6 y en el segundo escenario configuración de PAT, DHCP, entre otros.

Basados en las temáticas que se trabajaron a lo largo del curso, las distintas actividades y exámenes CCNA, se desarrollan competencias para lograr dar solución a las pruebas de habilidades prácticas propuestas basadas en escenarios que constituyen la creación de topologías de una red.

En los escenarios se deben de implementar comandos con el fin de configurar la seguridad de los switches, entre otras cosas, a su vez configurar por medio de protocolos NAT, NTP, ACL y PPP.

Con la culminación de esta actividad pude lograr la configuración de redes, implementación de protocolos routing dinámicos, protocolo de hosts dinámicos DHCP, a su vez en la configuración de las conexiones de distintas ciudades se obtiene una ventaja al utilizar el protocolo OSPF.

# 7. BIBLIOGRAFÍA

Academy, Cisco Networking. (2020). Servidores de DHCP y servidores DNS. Obtenido de https://www.netacad.com/es

Cisco Networking Academy. (2020). Configuring Basic Single-Area OSPFv2. Obtenido de https://www.netacad.com/es