

PRUEBA DE HABILIDADES PRÁCTICAS

AUTOR:LISSET JANETH SILVA GONZALEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

DIPLOMADO CISCO CCNA

INGENIERA DE TELECOMUNICACIONES

BOGOTA

2019

PRUEBA DE HABILIDADES PRÁCTICAS

AUTOR:LISSET JANETH SILVA GONZALEZ

Proyecto de grado presentado para obtener el título de:
INGENIERIA DE TELECOMUNICACIONES

TUTOR

ING. IVAN GUSTVO PENA

DIRECTOR DIPLOMADO CCNA

ING. JUAN VESGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

DIPLOMADO CISCO CCNA

INGENIERA DE TELECOMUNICACIONES

BOGOTA

2019

CONTENIDO

GLOSARIO.....	7
INTRODUCCION	8
OBJETIVO.....	9
OBJETIVO GENERAL	9
OBJETIVO ESPECIFICO	9
1. ESCENARIO 1	10
1.1. TOPOLOGÍA DE RED	10
1.2. CONFIGURACIÓN INICIAL ROUTER	11
1.3. DIRECCIONAMIENTO IP.....	12
1.4. CONFIGURACION PROTOCOLO RIP V2.....	13
1.5. BALANCEO DE CARGA DE LOS ROUTERS.....	19
1.6. DESHABILITAR RIP EN DETERMINADAS INTERFACES	21
1.7. VERIFICACIÓN DEL PROTOCOLO RIP	22
AUTENTICACIÓN PPP.....	24
1.8. CONFIGURACIÓN DE PAT	25
1.9. CONFIGURACIÓN DHCP	27
2. ESCENARIO 2	31
2.1. CONFIGURACION INICIAL DE LOS DISPOSITIVOS	32
2.2. DIRECCIONAMIENTO IP.....	34
2.3. CONFIGURACIÓN PROTOCOLO OSPFV2	37
2.4. COSTOS DE INTERFACES DEL PROTOCOLO OSPF	42
2.5. CONFIGURACION SWITCHES	44
2.6. CONFIGURACIÓN DHCP	49
2.7. CONFIGURAR NAT	51
2.8. CONFIGURACION LISTA DE ACCESO	51
CONCLUSIONES.....	55
BIBLIOGRAFÍA	56
ANEXO.....	58

LISTA DE TABLAS

Tabla 1. Direccionamiento IP del caso 1	12
Tabla 2 Puertos habilitados para los router	21
Tabla 3 Direccionamiento IP del caso 2	34
Tabla 4 Especificacion configuracion OSPF	37

TABLA DE ILUSTRACIONES

Ilustración 1 Topología de red caso 1	10
Ilustración 2 Configuración DHCP para 40 host	27
Ilustración 3 Configuración DHCP para 50 host	28
Ilustración 4 Configuración DHCP para 200 host	29
Ilustración 5 Configuración DHCP para 150 host	30
Ilustración 6 Topológica caso 2	31
Ilustración 7 Ping desde Internet hacia R2	36
Ilustración 8 Ping desde el Servidor hacia internet	37
Ilustración 9 Verificación DHCP para PC VLAN 30	50
Ilustración 10 Verificación DHCP para PC VLAN 40	50
Ilustración 11 Configuración lista de acceso	52
Ilustración 12 Prueba de conectividad entre el PC VLAN 30 y PC VLAN 40	52
Ilustración 13 Prueba de conectividad entre el PC VLAN 40 y PC VLAN 30	53
Ilustración 14 Prueba de navegación PC Internet	53
Ilustración 15 Prueba de conectividad del PC VLAN 40 hacia PC Internet	54
Ilustración 16 Prueba de conectividad del PC VLAN 30 hacia PC Internet	54

LISTA DE ANEXOS

Anexo 1. Link Cisco Packet Tracer del caso 1 y caso 2.....	58
--	----

GLOSARIO

DHCP: Es un protocolo de red de tipo cliente/servidor mediante el cual asigna dinámicamente una dirección IP y otros parámetros de configuración de red a cada dispositivo.

IP: Es un número que identifica, de manera lógica y jerárquica, a una Interfaz en la red de un dispositivo (computadora, tableta, portátil, teléfono inteligente).

ISP: Proveedor de servicios de Internet

LAN: Es una red de área local que conecta diferentes ordenadores en un área pequeña

LISTA DE ACCESO: Una **Lista** de Control de **Acceso** o **ACL**) es un concepto de seguridad informática usado para fomentar la separación de privilegios

OSPF: Open Shortest Path First (**OSPF**), es un protocolo de red para encaminamiento jerárquico de pasarela interior), que usa el algoritmo Dijkstra, para calcular la ruta más corta entre dos nodos.

PAT: Es una característica de un dispositivo de red que traduce las comunicaciones TCP o UDP realizadas entre hosts en una red privada y hosts en una red pública.

PING: Es una utilidad de diagnóstico en redes de computadoras que comprueba el estado de la comunicación del anfitrión local con uno o varios equipos remotos de una red que ejecuten IP

PPP; Protocolo punto a punto del nivel de enlace de datos, utilizado para establecer una conexión directa entre dos nodos de una **red**.

RIP: Es un protocolo de enrutamiento del tipo **vector distancia**.(numero de saltos)

TRACEROUTE: Es una herramienta de diagnóstico que permite seguir la pista de los paquetes que vienen desde un host (punto de *red*). Se obtiene además una estadística del RTT o latencia de *red*

INTRODUCCION

En el siguiente informe se pondrá en práctica los módulos estudiados CCNA1-2 con la actividad propuesta "Pruebas de habilidades prácticas", el cual se desarrollan dos escenarios donde debemos configurar e interconectar los diferentes dispositivos de acuerdo con los lineamientos establecidos,

En el primer escenario se configurarán dos redes LAN cuya comunicación se realiza mediante un ISP, según los lineamientos el enrutamiento debe ser configurado con el protocolo RIP V2, los Pc's se configurarán con direccionamiento DHCP y las redes privadas de cada segmento LAN deben tener NAT.

En el segundo escenario contamos con tres LAN el cual son Bogotá, Miami, Buenos Aires , cuyo enrutamiento se configurará con OSPF , se debe configurar DHCP, VLAN's , NAT.

Para los dos escenarios se deben realizar las respectivas validaciones mediante comandos ping, tracert y show.

OBJETIVO

OBJETIVO GENERAL

En la prueba de habilidades prácticas estudiaremos dos escenarios, donde configuraremos cada dispositivo de red y ejecutaremos los protocolos de enrutamiento RIPv2 y OSPF para cada escenario propuesto, entre otras configuraciones vistas durante el Diplomado de profundización cisco (diseño e implementación de soluciones integradas lan / wan).

OBJETIVO ESPECIFICO

Para cada dispositivo se configurara el acceso seguro.

Se asignara a cada dispositivo una dirección ip.

Se analizara el comportamiento de los protocolos de enrutamiento RIPv2 y OSPF de acuerdo al escenario que corresponda.

Se configurara DHCP, PPP NAT y lista de acceso.

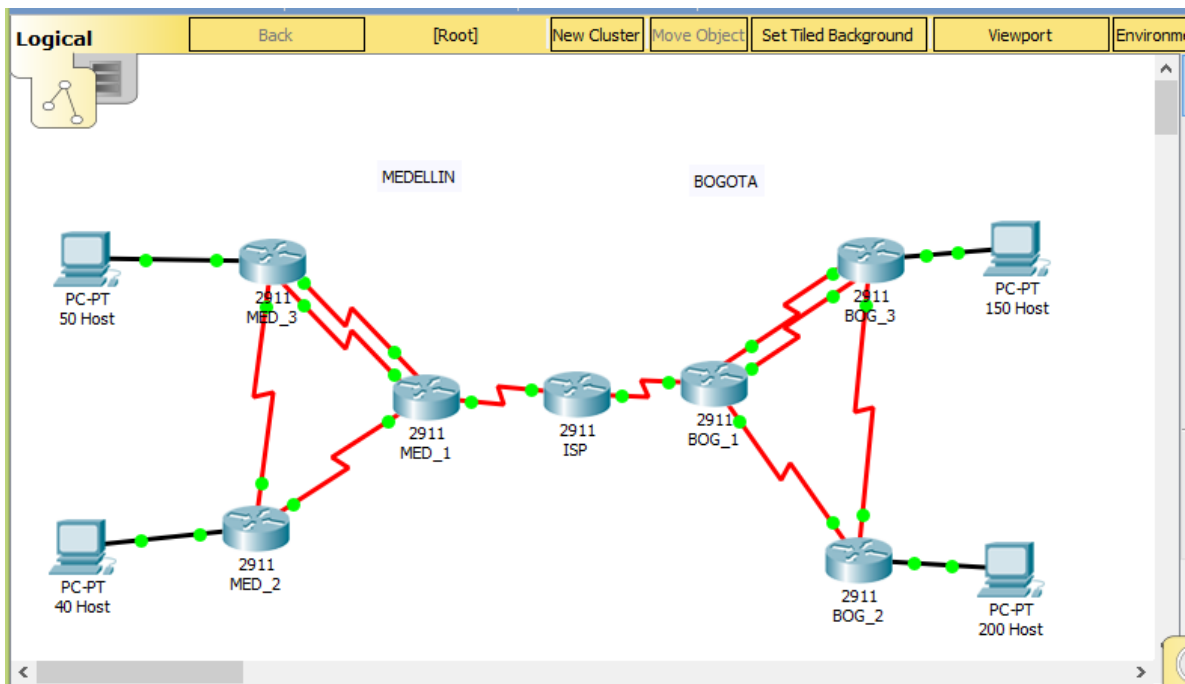
Observare la importancia de los comandos "Show".

1. ESCENARIO 1

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.

1.1. TOPOLOGÍA DE RED

Ilustración 1 Topología de red caso 1



Fuente: información proporcionada en la topología del caso 1

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

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

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

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

1.2. CONFIGURACIÓN INICIAL ROUTER

Se aplica la configuración inicial para cada router BOG_1, 2, 3 y MED_1, 2, 3.

Para proteger el acceso a modo privilegiado se debe configurar la contraseña de acceso al modo EXEC privilegiado utilizando el comando de configuración global "enable secret password".

Para proteger el acceso remoto a los routers se debe configurar las líneas VTY

```
router(config)#hostname BOG_1
```

```
BOG_1(config)#enable secret class
```

Para proteger el acceso al puerto de consola se debe configurar "line console 0".

```
BOG_1(config)#line console 0
```

```
BOG_1(config-line)#password cisco
```

```
BOG_1(config-line)#exec-timeout 5 0
```

```
BOG_1(config-line)#login
```

```
BOG_1(config-line)#logging synchronous
```

```
BOG_1(config-line)#exit
```

Para proteger el acceso remoto a los routers se debe configurar las líneas VTY

```
BOG_1(config)#line vty 0 4
```

```
BOG_1(config-line)#password cisco
```

```
BOG_1(config-line)#exec-timeout 5 0
```

```
BOG_1(config-line)#login
```

```
BOG_1(config-line)#logging synchronous
```

```
BOG_1(config-line)#exit
```

Se usa el siguiente comando para cifrar las contraseñas

BOG_1(config)#service password-encryption

Se crea un mensaje de aviso el cual se mostrara al ingresar al router

BOG_1(config)#banner motd #Unauthorized access prohibited!#

1.3. DIRECCIONAMIENTO IP

Se relaciona en la siguiente tabla la configuración ip que debe tener cada dispositivo de red, el cual incluye dirección ip, mascara de subred e interfaz de cada dispositivo:

Tabla 1. Direccionamiento IP del caso 1

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Bog_1	SERIAL0/0/1	172.29.3.1	255.255.255.252	N/A
	SERIAL0/1/0	172.29.3.5	255.255.255.252	N/A
	SERIAL0/1/1	172.29.3.9	255.255.255.252	N/A
	SERIAL0/0/0	209.17.220.6	255.255.255.252	N/A
Bog_2	SERIAL0/0/0	172.29.3.10	255.255.255.252	N/A
	SERIAL0/0/1	172.29.3.13	255.255.255.252	N/A
	Gi0/0	172.29.0.1	255.255.255.0	N/A
Bog_3	SERIAL0/0/0	172.29.3.2	255.255.255.252	N/A
	SERIAL0/0/1	172.29.3.6	255.255.255.252	N/A
	SERIAL0/1/1	172.29.3.14	255.255.255.252	N/A
	Gi0/0	172.29.1.1	255.255.255.0	N/A
Med_1	SERIAL0/0/0	172.29.6.1	255.255.255.252	N/A
	SERIAL0/0/1	172.29.6.9	255.255.255.252	N/A
	SERIAL0/1/1	172.29.6.13	255.255.255.252	N/A
	SERIAL0/1/0	209.17.220.2	255.255.255.252	N/A
Med_2	SERIAL0/0/0	172.29.6.2	255.255.255.252	N/A
	SERIAL0/0/1	172.29.6.5	255.255.255.252	N/A
	Gi0/0	172.29.128.1	255.255.255.128	
Med_3	SERIAL0/0/0	172.29.6.10	255.255.255.252	N/A
	SERIAL0/0/1	172.29.6.6	255.255.255.252	N/A
	SERIAL0/1/0	172.29.6.14	255.255.255.252	N/A
	Gi0/0	172.29.4.1	255.255.255.128	
ISP	SERIAL0/0/0	209.17.220.5	255.255.255.252	N/A
	SERIAL0/1/0	209.17.220.1	255.255.255.252	N/A

150 Host	NIC	172.29.0.2	255.255.255.0	172.29.2.1
200 Host	NIC	172.29.1.2	255.255.255.0	172.29.1.1
50 Host	NIC	172.29.4.2	255.255.255.128	172.29.4.1
40 Host	NIC	172.29.128.2	255.255.255.128	172.29.128.1

Fuente: información proporcionada en la topología del caso 1

1.4. CONFIGURACION PROTOCOLO RIP V2

Se configura el enrutamiento en la red usando el protocolo RIP versión 2, donde declaramos la red principal y desactivamos la sumarización automática para cada dispositivo:

BOG_1

```
BOG_1(config)#router rip
BOG_1(config-router)#version 2
BOG_1(config-router)#network 172.29.3.0
BOG_1(config-router)#network 172.29.3.4
BOG_1(config-router)#network 172.29.3.8
BOG_1(config-router)#network 209.17.220.4
BOG_1(config-router)#no auto-summary
```

BOG_2

```
BOG_2(config)#router rip
BOG_2(config-router)#version 2
BOG_2(config-router)#network 172.29.0.0
BOG_2(config-router)#network 172.29.3.8
BOG_2(config-router)#network 172.29.3.12
BOG_2(config-router)#no auto-summary
```

BOG_3

```
BOG_3(config)#router rip
BOG_3(config-router)#version 2
BOG_3(config-router)#network 172.29.1.0
BOG_3(config-router)#network 172.29.3.0
BOG_3(config-router)#network 172.29.3.4
BOG_3(config-router)#network 172.29.3.12
BOG_3(config-router)#no auto-summary
```

MED_1

```
MED_1(config)#router rip
MED_1(config-router)#version 2
MED_1(config-router)#network 172.29.6.0
MED_1(config-router)#network 172.29.6.8
MED_1(config-router)#network 172.29.6.12
MED_1(config-router)#network 209.17.220.0
MED_1(config-router)#no auto-summary
MED_2
```

```
MED_2(config)#router rip
MED_2(config-router)#version 2
MED_2(config-router)#network 172.29.6.0
MED_2(config-router)#network 172.29.6.4
MED_2(config-router)#network 172.29.128.0
MED_2(config-router)#no auto-summary
```

MED_3

```
MED_3(config)#router rip
MED_3(config-router)#version 2
MED_3(config-router)#network 172.29.4.0
MED_3(config-router)#network 172.29.6.4
MED_3(config-router)#network 172.29.6.8
MED_3(config-router)#network 172.29.6.12
MED_3(config-router)#no auto-summary
```

Los routers Bogota1 y Medellín 1 tienen una ruta por defecto hacia el ISP y se redistribuye dentro de las publicaciones de RIP.

BOG_1

```
BOG_1(config)#ip route 0.0.0.0 0.0.0.0 Serial0/0/0
BOG_1(config)#router rip
BOG_1(config-router)#version 2
BOG_1(config-router)#redistribute static
BOG_1(config-router)#passive-interface Serial0/0/0
BOG_1(config-router)#no auto-summary
```

MED_1

```
MED_1(config)#ip route 0.0.0.0 0.0.0.0 Serial0/1/0
MED_1(config)#router rip
MED_1(config-router)#version 2
MED_1(config-router)#redistribute static
MED_1(config-router)#passive-interface Serial0/1/0
MED_1(config-router)#no auto-summary
```

Los router ISP tienen una ruta estática dirigida hacia cada red interna de Bogotá y Medellín y se suman las subredes de cada uno a /22.

```
ISP(config)#ip route 172.29.0.0 255.255.252.0 Serial0/0/0
ISP(config)#ip route 172.29.4.0 255.255.252.0 Serial0/1/0
```

Con el comando “show ip route” podemos observar la tabla de enrutamiento de los routers ISP, BOG_1, 2, 3 Y MED_1, 2, 3, el cual nos suministra información de las redes conectadas directamente y las redes remotas.

Podemos identificar en la tabla de enrutamiento la letra “C” el cual indica que la red está conectada directamente, la letra “L” indica una red de la interfaz local, la letra “S” indica que conoce una red de forma estática

ISP

El router ISP solo indica sus rutas estáticas adicionales a las directamente conectadas

```
Gateway of last resort is not set
172.29.0.0/22 is subnetted, 2 subnets
S 172.29.0.0/22 is directly connected, Serial0/0/0
S 172.29.4.0/22 is directly connected, Serial0/1/0
209.17.220.0/24 is variably subnetted, 6 subnets, 2 masks
C 209.17.220.0/30 is directly connected, Serial0/1/0
L 209.17.220.1/32 is directly connected, Serial0/1/0
C 209.17.220.2/32 is directly connected, Serial0/1/0
C 209.17.220.4/30 is directly connected, Serial0/0/0
L 209.17.220.5/32 is directly connected, Serial0/0/0
C 209.17.220.6/32 is directly connected, Serial0/0/0
```

BOG_1

En la tabla de enrutamiento de BOG_1 podemos observar la letra "R" el cual indica que conoce la red a través del protocolo RIP v2

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R 172.29.0.0/24 [120/1] via 172.29.3.10, 00:00:23, Serial0/1/1
R 172.29.1.0/24 [120/1] via 172.29.3.2, 00:00:19, Serial0/0/1
[120/1] via 172.29.3.6, 00:00:19, Serial0/1/0
C 172.29.3.0/30 is directly connected, Serial0/0/1
L 172.29.3.1/32 is directly connected, Serial0/0/1
C 172.29.3.4/30 is directly connected, Serial0/1/0
L 172.29.3.5/32 is directly connected, Serial0/1/0
C 172.29.3.8/30 is directly connected, Serial0/1/1
L 172.29.3.9/32 is directly connected, Serial0/1/1
R 172.29.3.12/30 [120/1] via 172.29.3.2, 00:00:19, Serial0/0/1
[120/1] via 172.29.3.6, 00:00:19, Serial0/1/0
[120/1] via 172.29.3.10, 00:00:23, Serial0/1/1
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C 209.17.220.4/30 is directly connected, Serial0/0/0
C 209.17.220.5/32 is directly connected, Serial0/0/0
L 209.17.220.6/32 is directly connected, Serial0/0/0
S* 0.0.0.0/0 is directly connected, Serial0/0/0
```

BOG_2

```
Gateway of last resort is 172.29.3.9 to network 0.0.0.0
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
C 172.29.0.0/24 is directly connected, GigabitEthernet0/0
L 172.29.0.1/32 is directly connected, GigabitEthernet0/0
R 172.29.1.0/24 [120/1] via 172.29.3.14, 00:00:23, Serial0/0/1
R 172.29.3.0/30 [120/1] via 172.29.3.14, 00:00:23, Serial0/0/1
[120/1] via 172.29.3.9, 00:00:01, Serial0/0/0
R 172.29.3.4/30 [120/1] via 172.29.3.14, 00:00:23, Serial0/0/1
[120/1] via 172.29.3.9, 00:00:01, Serial0/0/0
C 172.29.3.8/30 is directly connected, Serial0/0/0
L 172.29.3.10/32 is directly connected, Serial0/0/0
C 172.29.3.12/30 is directly connected, Serial0/0/1
L 172.29.3.13/32 is directly connected, Serial0/0/1
209.17.220.0/30 is subnetted, 1 subnets
R 209.17.220.4/30 [120/1] via 172.29.3.9, 00:00:01, Serial0/0/0
R* 0.0.0.0/0 [120/1] via 172.29.3.9, 00:00:01, Serial0/0/0
```


BOG_3

Gateway of last resort is 172.29.3.1 to network 0.0.0.0
172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
R 172.29.0.0/24 [120/1] via 172.29.3.13, 00:00:25, Serial0/1/1
C 172.29.1.0/24 is directly connected, GigabitEthernet0/0
L 172.29.1.1/32 is directly connected, GigabitEthernet0/0
C 172.29.3.0/30 is directly connected, Serial0/0/0
L 172.29.3.2/32 is directly connected, Serial0/0/0
C 172.29.3.4/30 is directly connected, Serial0/0/1
L 172.29.3.6/32 is directly connected, Serial0/0/1
R 172.29.3.8/30 [120/1] via 172.29.3.1, 00:00:24, Serial0/0/0
[120/1] via 172.29.3.5, 00:00:24, Serial0/0/1
[120/1] via 172.29.3.13, 00:00:25, Serial0/1/1
C 172.29.3.12/30 is directly connected, Serial0/1/1
L 172.29.3.14/32 is directly connected, Serial0/1/1
209.17.220.0/30 is subnetted, 1 subnets
R 209.17.220.4/30 [120/1] via 172.29.3.1, 00:00:24, Serial0/0/0
[120/1] via 172.29.3.5, 00:00:24, Serial0/0/1
R* 0.0.0.0/0 [120/1] via 172.29.3.1, 00:00:24, Serial0/0/0
[120/1] via 172.29.3.5, 00:00:24, Serial0/0/1

MED_1

172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R 172.29.4.0/25 [120/1] via 172.29.6.10, 00:00:09, Serial0/0/1
[120/1] via 172.29.6.14, 00:00:09, Serial0/1/1
C 172.29.6.0/30 is directly connected, Serial0/0/0
L 172.29.6.1/32 is directly connected, Serial0/0/0
R 172.29.6.4/30 [120/1] via 172.29.6.10, 00:00:09, Serial0/0/1
[120/1] via 172.29.6.14, 00:00:09, Serial0/1/1
[120/1] via 172.29.6.2, 00:00:06, Serial0/0/0
C 172.29.6.8/30 is directly connected, Serial0/0/1
L 172.29.6.9/32 is directly connected, Serial0/0/1
C 172.29.6.12/30 is directly connected, Serial0/1/1
L 172.29.6.13/32 is directly connected, Serial0/1/1
R 172.29.128.0/25 [120/1] via 172.29.6.2, 00:00:06, Serial0/0/0
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
C 209.17.220.0/30 is directly connected, Serial0/1/0
C 209.17.220.1/32 is directly connected, Serial0/1/0
L 209.17.220.2/32 is directly connected, Serial0/1/0
S* 0.0.0.0/0 is directly connected, Serial0/1/0

MED_2

Gateway of last resort is 172.29.6.1 to network 0.0.0.0
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R 172.29.4.0/25 [120/1] via 172.29.6.6, 00:00:26, Serial0/0/1
C 172.29.6.0/30 is directly connected, Serial0/0/0
L 172.29.6.2/32 is directly connected, Serial0/0/0
C 172.29.6.4/30 is directly connected, Serial0/0/1
L 172.29.6.5/32 is directly connected, Serial0/0/1
R 172.29.6.8/30 [120/1] via 172.29.6.6, 00:00:26, Serial0/0/1
[120/1] via 172.29.6.1, 00:00:08, Serial0/0/0
R 172.29.6.12/30 [120/1] via 172.29.6.6, 00:00:26, Serial0/0/1
[120/1] via 172.29.6.1, 00:00:08, Serial0/0/0
C 172.29.128.0/25 is directly connected, GigabitEthernet0/0
L 172.29.128.1/32 is directly connected, GigabitEthernet0/0
209.17.220.0/30 is subnetted, 1 subnets
R 209.17.220.0/30 [120/1] via 172.29.6.1, 00:00:08, Serial0/0/0

R* 0.0.0.0/0 [120/1] via 172.29.6.1, 00:00:08, Serial0/0/0

MED_3

Gateway of last resort is 172.29.6.9 to network 0.0.0.0
172.29.0.0/16 is variably subnetted, 10 subnets, 3 masks
C 172.29.4.0/25 is directly connected, GigabitEthernet0/0
L 172.29.4.1/32 is directly connected, GigabitEthernet0/0
R 172.29.6.0/30 [120/1] via 172.29.6.9, 00:00:04, Serial0/0/0
[120/1] via 172.29.6.13, 00:00:04, Serial0/1/0
[120/1] via 172.29.6.5, 00:00:10, Serial0/0/1
C 172.29.6.4/30 is directly connected, Serial0/0/1
L 172.29.6.6/32 is directly connected, Serial0/0/1
C 172.29.6.8/30 is directly connected, Serial0/0/0
L 172.29.6.10/32 is directly connected, Serial0/0/0
C 172.29.6.12/30 is directly connected, Serial0/1/0
L 172.29.6.14/32 is directly connected, Serial0/1/0
R 172.29.128.0/25 [120/1] via 172.29.6.5, 00:00:10, Serial0/0/1
209.17.220.0/30 is subnetted, 1 subnets
R 209.17.220.0/30 [120/1] via 172.29.6.9, 00:00:04, Serial0/0/0
[120/1] via 172.29.6.13, 00:00:04, Serial0/1/0
R* 0.0.0.0/0 [120/1] via 172.29.6.9, 00:00:04, Serial0/0/0
[120/1] via 172.29.6.13, 00:00:04, Serial0/1/0

1.5. BALANCEO DE CARGA DE LOS ROUTERS.

Podemos observar el balanceo de cargas mediante el comando "show ip route", en este caso seremos más específicos y preguntaremos al router con ip's específicas.

El asterisco (*) que se observa en el resultado del comando nos indica la trayectoria que tomaran los paquetes.

Router's Bogota

```
BOG_1#sho ip route 172.29.3.12
Routing entry for 172.29.3.12/30
Known via "rip", distance 120, metric 1
Redistributing via rip
Last update from 172.29.3.10 on Serial0/1/1, 00:00:09 ago
Routing Descriptor Blocks:
* 172.29.3.2, from 172.29.3.2, 00:00:19 ago, via Serial0/0/1
  Route metric is 1, traffic share count is 1
172.29.3.6, from 172.29.3.6, 00:00:19 ago, via Serial0/1/0
  Route metric is 1, traffic share count is 1
172.29.3.10, from 172.29.3.10, 00:00:09 ago, via Serial0/1/1
  Route metric is 1, traffic share count is 1
```

```
BOG_2#sho ip route 172.29.3.0
Routing entry for 172.29.3.0/30
Known via "rip", distance 120, metric 1
Redistributing via rip
Last update from 172.29.3.9 on Serial0/0/0, 00:00:03 ago
Routing Descriptor Blocks:
* 172.29.3.9, from 172.29.3.9, 00:00:03 ago, via Serial0/0/0
  Route metric is 1, traffic share count is 1
```

```
BOG_3#sho ip route 172.29.3.0
Routing entry for 172.29.3.0/30
Known via "connected", distance 0, metric 0 (connected, via interface)
Redistributing via rip
Advertised by rip
Routing Descriptor Blocks:
* directly connected, via Serial0/0/0
  Route metric is 0, traffic share count is 1
```

Router's Medellin

```
MED_1#sho ip route 172.29.6.4
Routing entry for 172.29.6.4/30
Known via "rip", distance 120, metric 1
Redistributing via rip
Last update from 172.29.6.2 on Serial0/0/0, 00:00:22 ago
Routing Descriptor Blocks:
* 172.29.6.10, from 172.29.6.10, 00:00:23 ago, via Serial0/0/1
  Route metric is 1, traffic share count is 1
172.29.6.14, from 172.29.6.14, 00:00:23 ago, via Serial0/1/1
  Route metric is 1, traffic share count is 1
172.29.6.2, from 172.29.6.2, 00:00:22 ago, via Serial0/0/0
  Route metric is 1, traffic share count is 1
```

```
MED_2#sho ip route 172.29.6.8
Routing entry for 172.29.6.8/30
Known via "rip", distance 120, metric 1
Redistributing via rip
Last update from 172.29.6.6 on Serial0/0/1, 00:00:15 ago
Routing Descriptor Blocks:
* 172.29.6.6, from 172.29.6.6, 00:00:15 ago, via Serial0/0/1
  Route metric is 1, traffic share count is 1
172.29.6.1, from 172.29.6.1, 00:00:28 ago, via Serial0/0/0
  Route metric is 1, traffic share count is 1
```

```
MED_3#sho ip route 172.29.6.0
Routing entry for 172.29.6.0/30
Known via "rip", distance 120, metric 1
Redistributing via rip
Last update from 172.29.6.9 on Serial0/0/0, 00:00:01 ago
Routing Descriptor Blocks:
* 172.29.6.9, from 172.29.6.9, 00:00:01 ago, via Serial0/0/0
  Route metric is 1, traffic share count is 1
172.29.6.13, from 172.29.6.13, 00:00:01 ago, via Serial0/1/0
  Route metric is 1, traffic share count is 1
172.29.6.5, from 172.29.6.5, 00:00:11 ago, via Serial0/0/1
  Route metric is 1, traffic share count is 1
```

Se puede observar en los routers BOG_1 y MED_1 cierta similitud por su ubicación, por tener dos enlaces de conexión hacia otro router y por la ruta por defecto que manejan.

Los routers MED_2 y BOG_2 también presentan redes conectadas directamente y recibidas mediante RIP.

1.6.DESHABILITAR RIP EN DETERMINADAS INTERFACES

Para no propagar las publicaciones por interfaces que no lo requieran se deshabilita la propagación del protocolo RIP con el comando “no passive-interface interface”, en la siguiente tabla se indican las interfaces de cada router que no necesitan desactivación.

Tabla 2 Puertos habilitados para los router

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

Fuente: información proporcionada en la topología del caso 1

```
BOG_1(config)#router rip
BOG_1(config-router)#no passive-interface Serial0/0/0
```

```
BOG_2(config)#router rip
BOG_2(config-router)#no passive-interface Serial0/1/0
BOG_2(config-router)#no passive-interface Serial0/1/1
```

```
BOG_3(config)#router rip
BOG_3(config-router)#no passive-interface Serial0/1/0
```

```
MED_1(config)#router rip
MED_1(config-router)#no passive-interface Serial0/1/0
```

```
MED_2(config)#router rip
MED_2(config-router)#no passive-interface Serial0/1/0
MED_2(config-router)#no passive-interface Serial0/1/1
```

```
MED_3(config)#route rip
MED_3(config-router)#no passive-interface Serial0/1/1
```

1.7. VERIFICACIÓN DEL PROTOCOLO RIP.

Los siguientes comandos pueden ser comprobados en todos los router's configurados en el caso 1, a continuación una explicación de la funcionalidad de cada uno de estos:

El comando "show ip route rip" identificamos específicamente las rutas que se conocen mediante el protocolo RIPv2

BOG_1#show ip route rip

```
172.29.0.0/16 is variably subnetted, 9 subnets, 3 masks
R 172.29.0.0/24 [120/1] via 172.29.3.10, 00:00:01, Serial0/1/1
R 172.29.1.0/24 [120/1] via 172.29.3.6, 00:00:11, Serial0/1/0
[120/1] via 172.29.3.2, 00:00:11, Serial0/0/1
R 172.29.3.12/30 [120/1] via 172.29.3.10, 00:00:01, Serial0/1/1
[120/1] via 172.29.3.6, 00:00:11, Serial0/1/0
[120/1] via 172.29.3.2, 00:00:11, Serial0/0/1
209.17.220.0/24 is variably subnetted, 3 subnets, 2 masks
```

El comando "show ip protocol" nos muestra el protocolo de enrutamiento configurado en este caso RIPv2, podemos identificar las interfaces el cual recibe y envía RIPv2, la trayectoria máxima y las redes que se conocen.

BOG_1#show ip protocol

```
Routing Protocol is "rip"
Sending updates every 30 seconds, next due in 24 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip, static
Default version control: send version 2, receive 2
Interface Send Recv Triggered RIP Key-chain
Serial0/1/0 2 2
Serial0/0/1 2 2
Serial0/1/1 2 2
Serial0/0/0 2 2
Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
172.29.0.0
209.17.220.0
```

Passive Interface(s):
Routing Information Sources:
Gateway Distance Last Update
172.29.3.10 120 00:00:29
172.29.3.6 120 00:00:13
172.29.3.2 120 00:00:13
Distance: (default is 120)

El comando “show ip rip database” nos muestra el contenido de la base de datos de la información de enrutamiento de RIPv2.

172.29.0.0/24 auto-summary; Muestra la sumarización automática de rutas y su clase.

209.17.220.4/30 directly connected, Serial0/0/0, Indica la red directamente conectada a una interfaz que se encuentra configurada bajo RIP v2.

BOG_1#show ip rip database

```
0.0.0.0/0 auto-summary
0.0.0.0/0
    [1] via 0.0.0.0, 00:11:56, Serial0/0/0
172.29.0.0/24 auto-summary
172.29.0.0/24
    [1] via 172.29.3.10, 00:00:24, Serial0/1/1
172.29.1.0/24 auto-summary
172.29.1.0/24
    [1] via 172.29.3.6, 00:00:07, Serial0/1/0 [1] via 172.29.3.2, 00:00:07,
Serial0/0/1
172.29.3.0/30 auto-summary
172.29.3.0/30 directly connected, Serial0/0/1
172.29.3.4/30 auto-summary
172.29.3.4/30 directly connected, Serial0/1/0
172.29.3.8/30 auto-summary
172.29.3.8/30 directly connected, Serial0/1/1
172.29.3.12/30 auto-summary
172.29.3.12/30
    [1] via 172.29.3.10, 00:00:24, Serial0/1/1
    [1] via 172.29.3.6, 00:00:07, Serial0/1/0
    [1] via 172.29.3.2, 00:00:07, Serial0/0/1
209.17.220.4/30 auto-summary
209.17.220.4/30 directly connected, Serial0/0/0
```

AUTENTICACIÓN PPP

La autenticación PPP (Punto a punto) permite la comunicación entre dos equipos en este caso los router's MED_1 e ISP son configurados con el Protocolo de Autenticación por Clave (PAP, Password Authentication Protocol)

```
ISP(config)#interface Serial0/1/0
ISP(config-if)#encap ppp
ISP(config-if)#ppp auth pap
ISP(config-if)#ppp pap sent-username ISP pass 1234
```

```
MED_1(config)#interface Serial0/1/0
MED_1(config-if)#encapsulation ppp
MED_1(config-if)#ppp authentication pap
MED_1(config-if)#ppp pap sent-username MED_1 password 1234
MED_1(config-if)#
```

El enlace BOG_1 con ISP son configurar con el protocolo de autenticación de intercambio de señales (CHAP, Challenge Handshake Authentication Protocol).

```
BOG_1(config)#username ISP password 1234
BOG_1(config)#interface Serial0/0/0
BOG_1(config-if)#encapsulation ppp
BOG_1(config-if)#ppp authentication chap
BOG_1(config-if)#
```

```
ISP(config)#username BOG_1 password 1234
ISP(config)#interface Serial0/0/0
ISP(config-if)#encapsulation ppp
ISP(config-if)#ppp authentication chap
ISP(config-if)#
```


1.8.CONFIGURACIÓN DE PAT

PAT es conocida también como NAT con sobre carga, esta configuración consiste en asignar varias direcciones IPv4 privadas a una única dirección IPv4 pública. Se activa NAT en cada interfaz de entrada y salida del router MED_1

```
MED_1(config)#ip nat inside source list 1 interface Serial0/1/0 overload
MED_1(config)#access-list 1 permit 172.29.4.0 0.0.3.255
MED_1(config)#interface Serial0/0/0
MED_1(config-if)#ip nat inside
MED_1(config-if)#exit
MED_1(config)#interface Serial0/0/1
MED_1(config-if)#ip nat inside
MED_1(config-if)#exit
MED_1(config)#interface Serial0/1/1
MED_1(config-if)#ip nat inside
MED_1(config-if)#exit
MED_1(config)#interface Serial0/1/0
MED_1(config-if)#ip nat outside
```

Después de verificar mediante el comando “show ip nat translations” se comprueba la traducción de direcciones y los respectivos puertos.

También identificamos que se usa un número de puerto TCP distinto para cada sesión:

```
MED_1#show ip nat translations
Pro Inside global Inside local Outside local Outside global
icmp 209.17.220.2:10 172.29.6.2:10 209.17.220.1:10 209.17.220.1:10
icmp 209.17.220.2:11 172.29.6.2:11 209.17.220.1:11 209.17.220.1:11
icmp 209.17.220.2:7 172.29.6.2:7 209.17.220.1:7 209.17.220.1:7
icmp 209.17.220.2:8 172.29.6.2:8 209.17.220.1:8 209.17.220.1:8
icmp 209.17.220.2:9 172.29.6.2:9 209.17.220.1:9 209.17.220.1:9
```

El comando “show ip nat statistics” indica las interfaces de entrada y de salida:

```
MED_1#show ip nat statistics
Total translations: 5 (0 static, 5 dynamic, 5 extended)
Outside Interfaces: Serial0/1/0
Inside Interfaces: Serial0/0/0 , Serial0/0/1 , Serial0/1/1
Hits: 6 Misses: 638
Expired translations: 0
Dynamic mappings:
Configuración NAT
```

Se ejecuta la misma configurar NAT en el router BOG_1.

```
BOG_1(config)#ip nat inside source list 1 interface Serial0/0/0 overload  
BOG_1(config)#access-list 1 permit 172.29.0.0 0.0.3.255
```

```
BOG_1(config)#inter SERIAL0/0/1BOG_1(config-if)#ip nat inside
```

```
BOG_1(config-if)#exi  
BOG_1(config)#int SERIAL0/1/0  
BOG_1(config-if)#ip nat inside  
BOG_1(config-if)#exit  
BOG_1(config)# int SERIAL0/1/1  
BOG_1(config-if)#ip nat inside  
BOG_1(config-if)#exit  
BOG_1(config)#int SERIAL0/0/0  
BOG_1(config-if)#ip nat outside
```

```
BOG_1#show ip nat translations
```

```
Pro Inside global Inside local Outside local Outside global  
icmp 209.17.220.6:5 172.29.3.10:5 209.17.220.5:5 209.17.220.5:5  
icmp 209.17.220.6:6 172.29.3.10:6 209.17.220.5:6 209.17.220.5:6  
icmp 209.17.220.6:7 172.29.3.10:7 209.17.220.5:7 209.17.220.5:7  
icmp 209.17.220.6:8 172.29.3.10:8 209.17.220.5:8 209.17.220.5:8  
icmp 209.17.220.6:9 172.29.3.10:9 209.17.220.5:9 209.17.220.5:9
```

```
BOG_1#sho ip nat statistics
```

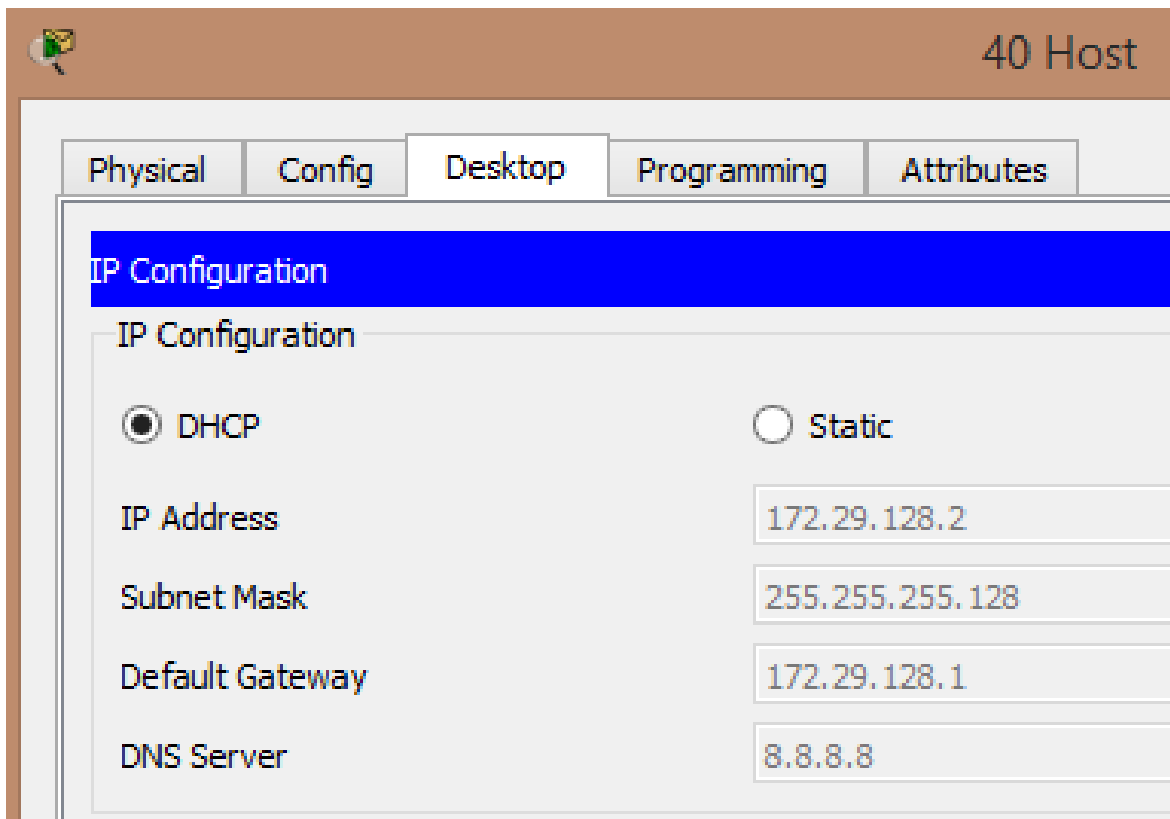
```
Total translations: 5 (0 static, 5 dynamic, 5 extended)  
Outside Interfaces: Serial0/0/0  
Inside Interfaces: Serial0/0/1 , Serial0/1/0 , Serial0/1/1  
Hits: 6 Misses: 675  
Expired translations: 0  
Dynamic mappings:
```

1.9.CONFIGURACIÓN DHCP.

MED_2 se configura como servidor DHCP para las redes Lan de Medellin

```
MED_2(config)#ip dhcp pool DHCP_MED2
MED_2(dhcp-config)#network 172.29.128.0 255.255.255.128
MED_2(dhcp-config)#default-router 172.29.128.1
MED_2(dhcp-config)#dns-server 8.8.8.8
MED_2(dhcp-config)#exit
MED_2(config)#ip dhcp pool DHCP_MED3
MED_2(dhcp-config)# network 172.29.4.0 255.255.255.128
MED_2(dhcp-config)# default-router 172.29.4.1
MED_2(dhcp-config)# dns-server 8.8.8.8
```

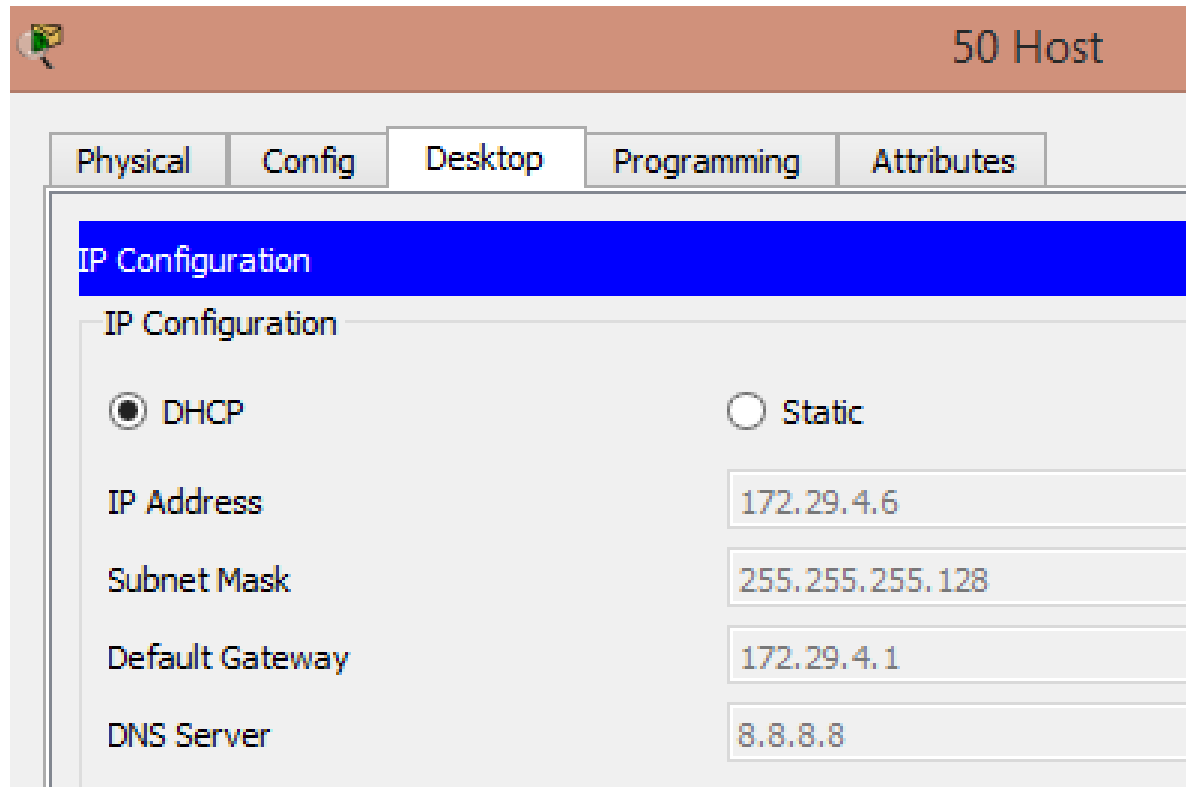
Ilustración 2 Configuración DHCP para 40 host



Fuente: Cisco Packet tracer, diseño de red.

```
MED_3(config)#interface GigabitEthernet0/0
MED_3(config-if)#ip helper-address 172.29.6.5
```

Ilustración 3 Configuración DHCP para 50 host

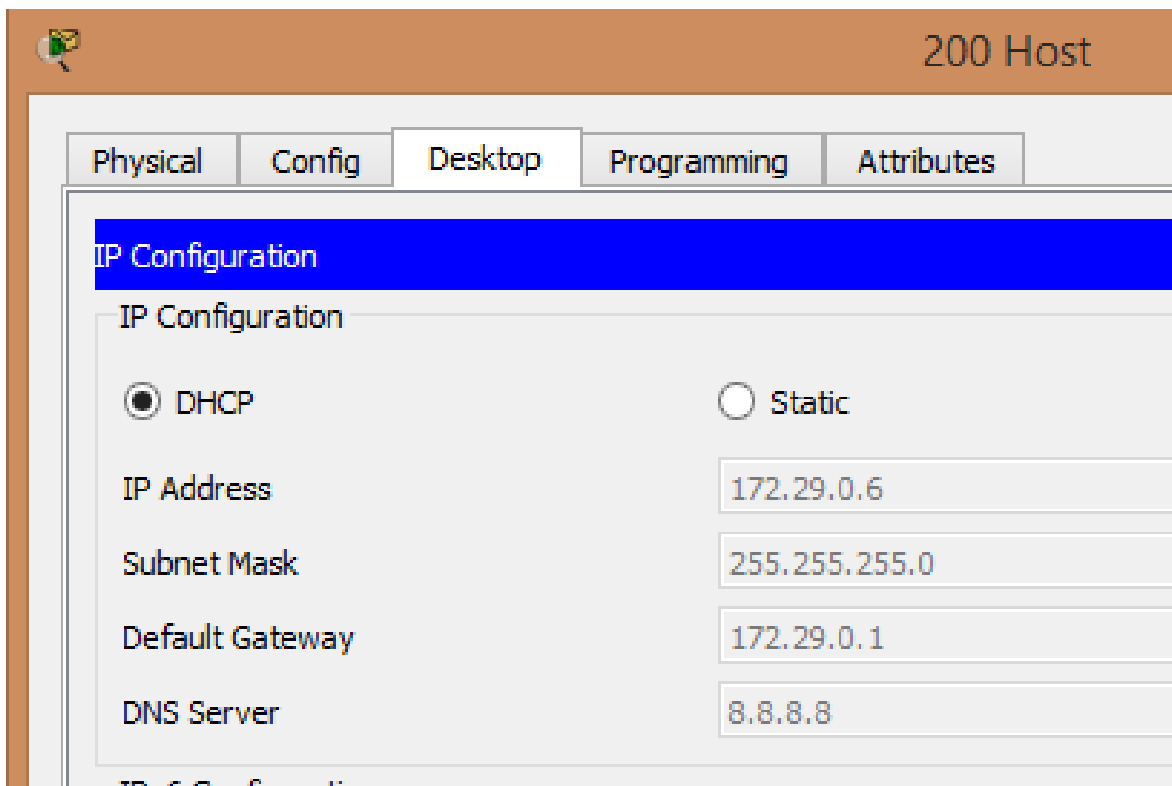


Fuente: Cisco Packet tracer, diseño de red.

BOG_2 se configura como servidor DHCP para ambas redes Lan de Bogota

```
BOG_2(config)#ip dhcp excluded-address 172.29.1.1 172.29.1.5
BOG_2(config)#ip dhcp excluded-address 172.29.0.1 172.29.0.5
BOG_2(config)#ip dhcp pool DHCP_BOG3
BOG_2(dhcp-config)#network 172.29.1.0 255.255.255.0
BOG_2(dhcp-config)#default-router 172.29.1.1
BOG_2(dhcp-config)#dns-server 8.8.8.8
BOG_2(dhcp-config)#exit
BOG_2(config)#ip dhcp pool DHCP_BOG2
BOG_2(dhcp-config)# network 172.29.0.0 255.255.255.0
BOG_2(dhcp-config)# default-router 172.29.0.1
BOG_2(dhcp-config)# dns-server 8.8.8.8
```

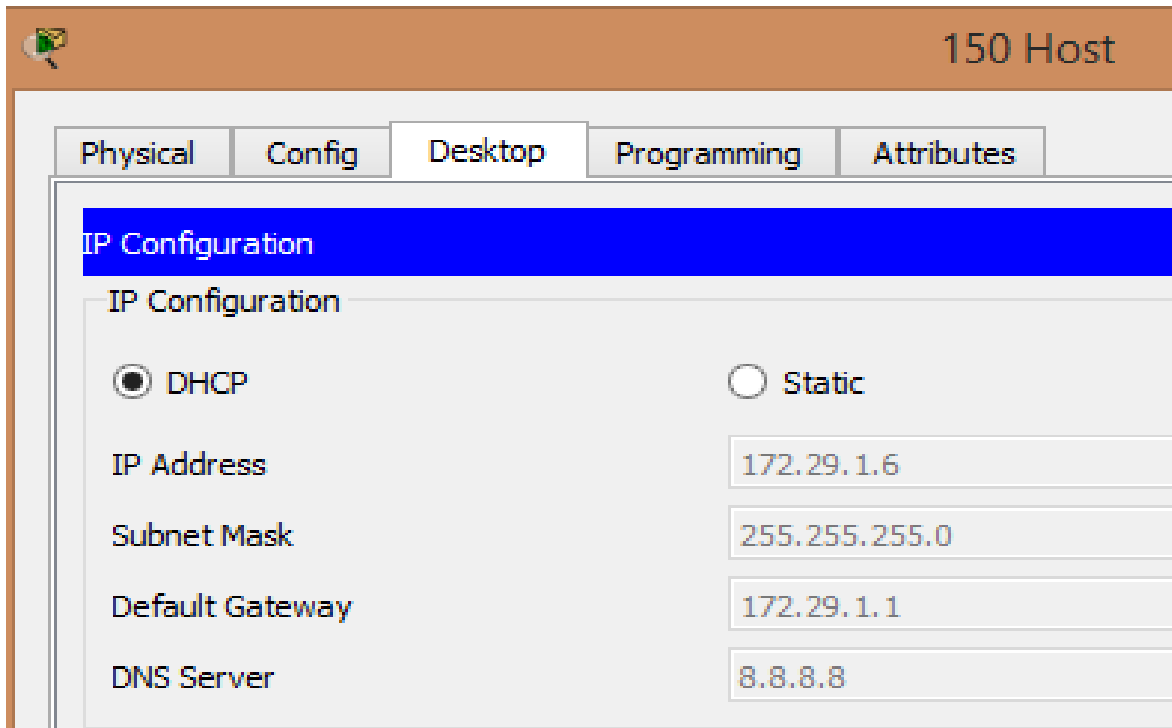
Ilustración 4 Configuración DHCP para 200 host



Fuente: Cisco Packet Tracer, diseño de red.

```
BOG_3(config)#interface GigabitEthernet0/0
BOG_3(config-if)#ip helper-address 172.29.3.13
```

Ilustración 5 Configuración DHCP para 150 host

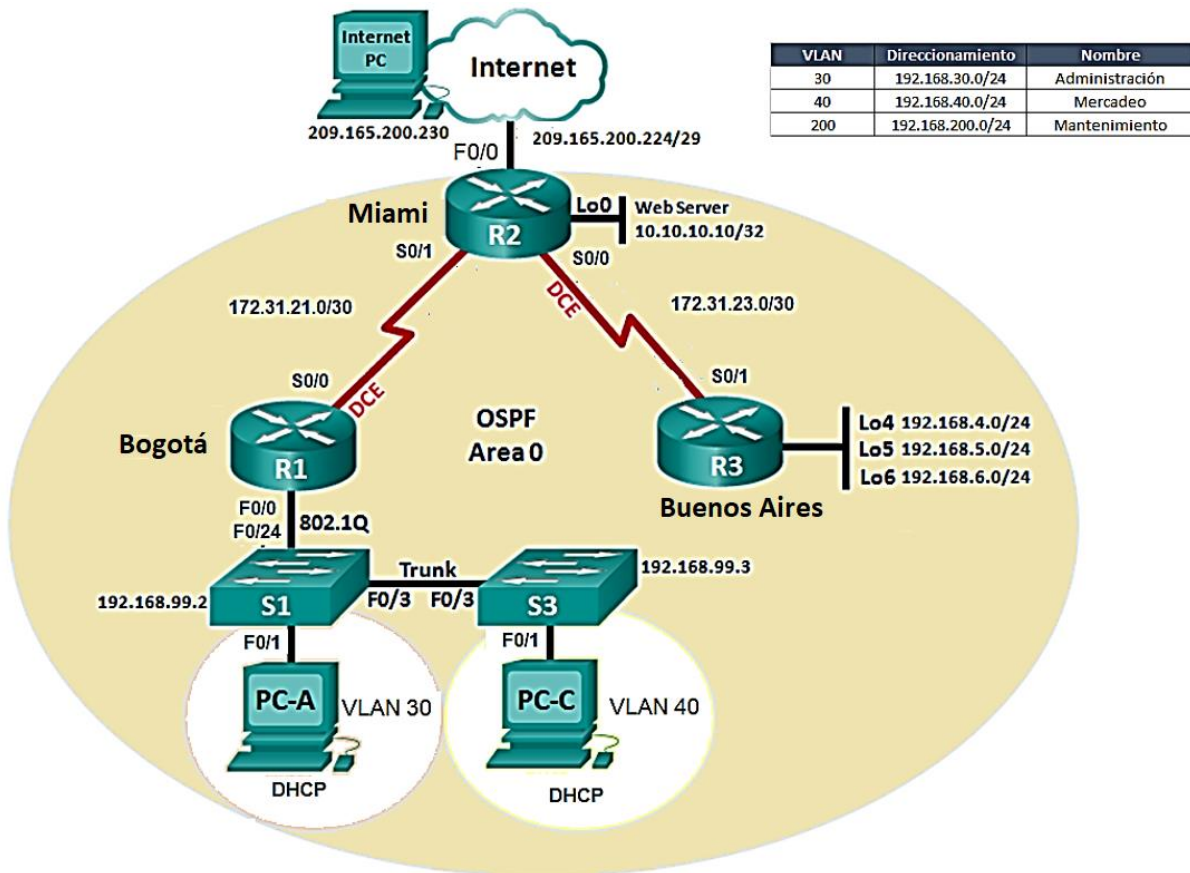


Fuente: Cisco Packet tracer, diseño de red.

2. 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.

Ilustración 6 Topologica caso 2



Fuente: información proporcionada en la topología del caso 2

2.1. CONFIGURACION INICIAL DE LOS DISPOSITIVOS

Se aplica la configuración inicial para cada router Bogota, Buenos_Aires, Miami y los respectivos switches

Para proteger el acceso a modo privilegiado se debe configurar la contraseña de acceso al modo EXEC privilegiado utilizando el comando de configuración global "enable secret password".

Para proteger el acceso remoto a los routers se debe configurar las líneas VTY.

Para proteger el acceso al puerto de consola se debe configurar line console 0.

Bogota

```
Bogota(config)#
Bogota(config)#enable secret class
Bogota(config)#line con 0
Bogota(config-line)#password cisco
Bogota(config-line)#exec-timeout 5 0
Bogota(config-line)#login
Bogota(config-line)#logging synchronous
Bogota(config-line)#exit
Bogota(config)#line vty 0 4
Bogota(config-line)#password cisco
Bogota(config-line)#exec-timeout 5 0
Bogota(config-line)#login
Bogota(config-line)#logging synchronous
Bogota(config-line)#exit
Bogota(config)#line vty 0 4
Bogota(config-line)#password cisco
Bogota(config-line)#exec-timeout 5 0
Bogota(config-line)#login
Bogota(config-line)#logging synchronous
Bogota(config-line)#exit
Bogota(config)#service password-encryption
Bogota(config)#banner motd #Unauthorized access prohibited!#
```

Miami

```
Miami#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
Miami(config)#
Miami(config)#enable secret class
Miami(config)#line con 0
Miami(config-line)#password cisco
Miami(config-line)#exec-timeout 5 0
Miami(config-line)#login
```



```
Miami(config-line)#logging synchronous
Miami(config-line)#exit
Miami(config)#line vty 0 4
Miami(config-line)#password cisco
Miami(config-line)#exec-timeout 5 0
Miami(config-line)#login
Miami(config-line)#logging synchronous
Miami(config-line)#exit
Miami(config)#service password-encryption
Miami(config)#banner motd #Unauthorized access prohibited!#
```

Buenos Aires

```
Buenos_Aires#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
Buenos_Aires(config)#
Buenos_Aires(config)#enable secret class
Buenos_Aires(config)#line con 0
Buenos_Aires(config-line)#password cisco
Buenos_Aires(config-line)#exec-timeout 5 0
Buenos_Aires(config-line)#login
Buenos_Aires(config-line)#logging synchronous
Buenos_Aires(config-line)#exit
Buenos_Aires(config)#line vty 0 4
Buenos_Aires(config-line)#password cisco
Buenos_Aires(config-line)#exec-timeout 5 0
Buenos_Aires(config-line)#login
Buenos_Aires(config-line)#logging synchronous
Buenos_Aires(config-line)#exit
Buenos_Aires(config)#service password-encryption
Buenos_Aires(config)#banner motd #Unauthorized access prohibited!#
```

S1

```
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#exec-timeout 5 0
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#exec-timeout 5 0
S1(config-line)#login
S1(config-line)#logging synchronous
```

```
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #Unauthorized access prohibited!#
```

S3

```
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#exec-timeout 5 0
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#exec-timeout 5 0
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #Unauthorized access prohibited!#
```

2.2. DIRECCIONAMIENTO IP

Se relaciona en la siguiente tabla la configuración ip que debe tener cada dispositivo de red, el cual incluye dirección ip, máscara de subred e interfaz de cada dispositivo:

Tabla 3 Direccionamiento IP del caso 2

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
Bogota	Serial0/1/0	172.31.21.1	255.255.255.252	N/A
	Vlan 30	192.168.30.1	255.255.255.0	N/A
	Vlan 40	192.168.40.1	255.255.255.0	N/A
	Vlan 200	192.168.200.1	255.255.255.0	N/A
Miami	Serial0/1/1	172.31.21.2	255.255.255.252	N/A
	Serial0/1/0	172.31.23.1	255.255.255.252	N/A
	Giga0/0	209.165.200.225	255.255.255.248	N/A
	Giga0/1	10.10.10.1	255.255.255.0	N/A
Servidor	Nic	10.10.10.10	255.255.255.0	10.10.10.1
Buenos Aires	Serial0/1/1	172.31.23.2	255.255.255.252	N/A
	loopback 4	192.168.4.1	255.255.255.0	N/A
	loopback 5	192.168.5.1	255.255.255.0	N/A

	loopback 6	192.168.6.1	255.255.255.0	N/A
Sw1		192.168.200.2	255.255.255.0	192.168.200.1
Sw2		192.168.200.3	255.255.255.0	192.168.200.1
internet		209.165.200.230	255.255.255.248	209.165.200.225

Fuente: información proporcionada en la topología del caso 2

Bogota

```
Bogota(config-if)#ip address 172.31.21.1 255.255.255.252
Bogota(config-if)#no shutdown
Bogota(config-if)#exit
```

Miami

```
Miami(config)#int Serial0/1/1
Miami(config-if)#ip address 172.31.21.2 255.255.255.252
Miami(config-if)#no shutdown
Miami(config)#int Serial0/1/0
Miami(config-if)#ip address 172.31.23.1 255.255.255.252
Miami(config-if)#no shut
Miami(config)#int GigabitEthernet0/0
Miami(config-if)#ip address 209.165.200.225 255.255.255.248
Miami(config-if)#no shut
Miami(config)#int gi0/1
Miami(config-if)#ip address 10.10.10.1
Miami(config-if)#no shut
Miami(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/1
```

Buenos Aires

```
Router(config)#hostname Buenos_Aires
Buenos_Aires(config)#int Serial0/1/1
Buenos_Aires(config-if)#ip address 172.31.23.2 255.255.255.252
Buenos_Aires(config-if)#no shut

Buenos_Aires(config)#interface loopback 4
Buenos_Aires(config-if)#ip address 192.168.4.1 255.255.255.0
Buenos_Aires(config-if)#no shutdown
Buenos_Aires(config-if)#exit
Buenos_Aires(config)#interface loopback 5
Buenos_Aires(config-if)#ip address 192.168.5.1 255.255.255.0
Buenos_Aires(config-if)#no shut
```

```
Buenos_Aires(config-if)#exit
Buenos_Aires(config)#interface loopback 6
Buenos_Aires(config-if)#ip address 192.168.6.1 255.255.255.0
Buenos_Aires(config-if)#no shut
```

Verificación conectividad

Ping desde Bogota hacia Miami

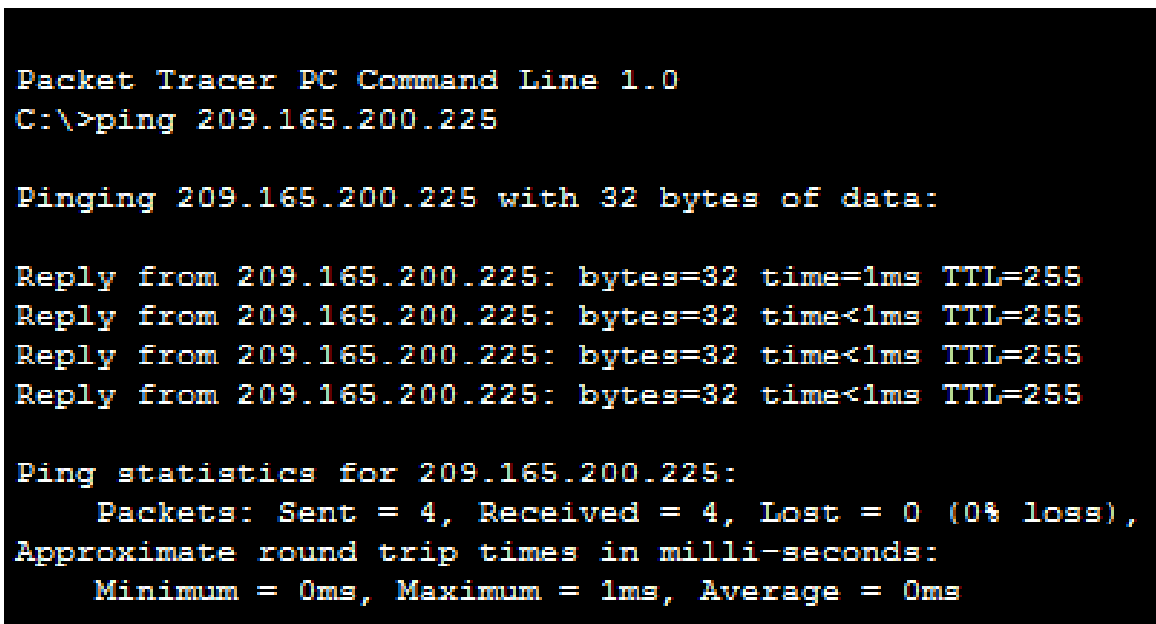
```
Bogota#ping 172.31.21.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/14 ms
```

Ping desde Miami hacia Buenos Aires

```
Miami#ping 172.31.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms
```

Ping desde Internet hacia R2

Ilustración 7 Ping desde Internet hacia R2



```
Packet Tracer PC Command Line 1.0
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=1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Cisco Packet tracer, prueba de conectividad.

Ping desde el Servidor hacia internet

Ilustración 8 Ping desde el Servidor hacia internet

```
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=1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255
Reply from 209.165.200.225: bytes=32 time<1ms TTL=255

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Fuente: Cisco Packet tracer, prueba de conectividad.

2.3. CONFIGURACIÓN PROTOCOLO OSPFV2

Se realiza la configuración del protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 area 0

Tabla 4 Especificacion configuracion OSPF

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

Fuente: información proporcionada en la topología del caso 2

Router 1 Bogota

```
Bogota(config)#router ospf 1
Bogota(config-router)#router-id 1.1.1.1
Bogota(config-router)#network 172.31.21.0 0.0.0.3 area 0
Bogota(config-router)#network 192.168.200.0 0.0.0.255 area 0
Bogota(config-router)#network 192.168.30.0 0.0.0.255 area 0
Bogota(config-router)#network 192.168.40.0 0.0.0.255 area 0
Bogota(config-router)#passive-interface GigabitEthernet0/0
```

```
Bogota(config)#interface Serial0/1/0
Bogota(config-if)#bandwidth 256
Bogota(config-if)#ip ospf cost 9500
```

Router 2 Miami

```
Miami(config)#router ospf 1
Miami(config-router)#router-id 5.5.5.5
Miami(config-router)#log-adjacency-changes
Miami(config-router)#passive-interface GigabitEthernet0/0
Miami(config-router)#network 172.31.21.0 0.0.0.3 area 0
Miami(config-router)#network 10.10.10.0 0.0.0.255 area 0
Miami(config-router)#network 172.31.23.0 0.0.0.3 area 0
Miami(config)#int Serial0/1/0
Miami(config-if)#bandwidth 256
Miami(config-if)#ip ospf cost 9500
Miami(config-if)#exit
Miami(config)#int Serial0/1/1
Miami(config-if)#bandwidth 256
Miami(config-if)#ip ospf cost 9500
```

Router 3 Buenos_Aires

```
Buenos_Aires(config)#router ospf 1
Buenos_Aires(config-router)#router-id 8.8.8.8
Buenos_Aires(config-router)#log-adjacency-changes
Buenos_Aires(config-router)#network 192.168.4.0 0.0.0.255 area 0
Buenos_Aires(config-router)#network 192.168.5.0 0.0.0.255 area 0
Buenos_Aires(config-router)#network 192.168.6.0 0.0.0.255 area 0
Buenos_Aires(config-router)#network 172.31.23.0 0.0.0.3 area 0
Buenos_Aires(config-router)#passive-interface lo4
Buenos_Aires(config-router)#passive-interface lo5
Buenos_Aires(config-router)#passive-interface lo6
Buenos_Aires(config-router)#exit
```

```
Buenos_Aires(config)#int Serial0/1/1
Buenos_Aires(config-if)#bandwidth 256
Buenos_Aires(config-if)#ip ospf cost 9500
Buenos_Aires(config-if)#exit
```

Para verificar información de OSPF utilizamos los siguientes comandos:

El comando "Show ip ospf neighbor", nos indica información del router vecino el cual podemos identificarlo por el ID en este caso es 5.5.5.5 (Miami), la prioridad es 0 , lo que significa que no está configurado para hacer DR o backup:

```
Bogota#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
5.5.5.5 0 FULL/ - 00:00:36 172.31.21.2 Serial0/1/0
```

El comando "Show ip protocols" nos indica el protocolo de enrutamiento configurado en el router, se puede identificar el ID asignado en este caso es 1.1.1.1 para Bogotá , las redes conocidas, el tiempo de interacción y la distancia administrativa que para OSPF es 110:

```
Bogota#show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 1.1.1.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.31.21.0 0.0.0.3 area 0
192.168.200.0 0.0.0.255 area 0
192.168.30.0 0.0.0.255 area 0
192.168.40.0 0.0.0.255 area 0
Passive Interface(s):
GigabitEthernet0/0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:09:18
5.5.5.5 110 00:09:18
8.8.8.8 110 00:09:20
Distance: (default is 110)
```

El comando "Show ip route ospf" nos muestra las redes que se conocen a través del protocolo OSPF:

```
Bogota#show ip route ospf
10.0.0.0/24 is subnetted, 1 subnets
O 10.10.10.0 [110/9501] via 172.31.21.2, 00:40:09, Serial0/1/0
172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
O 172.31.23.0 [110/19000] via 172.31.21.2, 00:40:09, Serial0/1/0
192.168.4.0/32 is subnetted, 1 subnets
O 192.168.4.1 [110/19001] via 172.31.21.2, 00:40:09, Serial0/1/0
192.168.5.0/32 is subnetted, 1 subnets
O 192.168.5.1 [110/19001] via 172.31.21.2, 00:40:09, Serial0/1/0
192.168.6.0/32 is subnetted, 1 subnets
O 192.168.6.1 [110/19001] via 172.31.21.2, 00:40:09, Serial0/1/0
```

Miami

El comando "Show ip protocols" nos indica el protocolo de enrutamiento configurado en el router, se puede identificar el ID asignado en este caso es 5.5.5.5 para Miami, las redes conocidas, el tiempo de interacción y la distancia administrativa que para OSPF es 110:

```
Miami#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 5.5.5.5
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
172.31.21.0 0.0.0.3 area 0
172.31.23.0 0.0.0.3 area 0
10.10.10.0 0.0.0.255 area 0
Passive Interface(s):
GigabitEthernet0/0
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:02:02
5.5.5.5 110 00:02:02
8.8.8.8 110 00:02:02
Distance: (default is 110)
```


El comando "Show ip route ospf" nos muestra las redes que se conocen a través del protocolo OSPF:

```
Miami#sho ip route ospf
192.168.4.0/32 is subnetted, 1 subnets
O 192.168.4.1 [110/9501] via 172.31.23.2, 00:04:28, Serial0/1/0
192.168.5.0/32 is subnetted, 1 subnets
O 192.168.5.1 [110/9501] via 172.31.23.2, 00:04:28, Serial0/1/0
192.168.6.0/32 is subnetted, 1 subnets
O 192.168.6.1 [110/9501] via 172.31.23.2, 00:04:28, Serial0/1/0
O 192.168.30.0 [110/9501] via 172.31.21.1, 00:04:28, Serial0/1/1
O 192.168.40.0 [110/9501] via 172.31.21.1, 00:04:28, Serial0/1/1
O 192.168.200.0 [110/9501] via 172.31.21.1, 00:04:28, Serial0/1/1
```

Buenos Aires

El comando "Show ip ospf neighbor", nos indica información del router vecino el cual podemos identificarlo por el ID en este caso es 5.5.5.5 (Miami), la prioridad es 0, lo que significa que no está configurado para hacer DR o backup:

```
Buenos_Aires#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
 5.5.5.5 0 FULL/ - 00:00:34 172.31.23.1 Serial0/1/1
```

El comando "Show ip protocols" nos indica el protocolo de enrutamiento configurado en el router, se puede identificar el ID asignado en este caso es 8.8.8.8 para Buenos_Aires, las redes conocidas, el tiempo de interacción y la distancia administrativa que para OSPF es 110:

```
Buenos_Aires#sho 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 8.8.8.8
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
192.168.4.0 0.0.0.255 area 0
192.168.5.0 0.0.0.255 area 0
192.168.6.0 0.0.0.255 area 0
```

```
172.31.23.0 0.0.0.3 area 0
Passive Interface(s):
Loopback4
Loopback5
Loopback6
Routing Information Sources:
Gateway Distance Last Update
1.1.1.1 110 00:11:10
5.5.5.5 110 00:11:10
8.8.8.8 110 00:11:10
Distance: (default is 110)
```

2.4. COSTOS DE INTERFACES DEL PROTOCOLO OSPF

Con el comando “Show ip ospf interface” podemos visualizar una lista resumida de interfaces por OSPF en donde se ilustra el costo de cada interface, por ejemplo en Bogota en la interface GigabitEthernet0/0.30 se encuentra en estado operativo (UP). La Dirección IP de la interfaz es 192.168.30, la máscara de subred /24 y dirección de área es 0. El retardo de transmisión es 1 segundo, el estado de la interfaz es DR y la prioridad del enrutador ES 1. El ID de enrutador designado es 1.1.1.1 y la dirección IP de la interfaz es 192.168.30.1. Se muestra también Información de configuración de intervalos de temporizador:

Bogota

```
Bogota#sho ip ospf interface
```

```
GigabitEthernet0/0.30 is up, line protocol is up
Internet address is 192.168.30.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, Interface address 192.168.30.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Index 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)
GigabitEthernet0/0.40 is up, line protocol is up
Internet address is 192.168.40.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
```

Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, Interface address 192.168.40.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Index 2/2, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
GigabitEthernet0/0.200 is up, line protocol is up
Internet address is 192.168.200.1/24, Area 0
Process ID 1, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 1.1.1.1, Interface address 192.168.200.1
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Index 3/3, flood queue length 0
Next 0x0(0)/0x0(0)
Last flood scan length is 1, maximum is 1
Last flood scan time is 0 msec, maximum is 0 msec
Neighbor Count is 0, Adjacent neighbor count is 0
Suppress hello for 0 neighbor(s)
Serial0/1/0 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: 9500
Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
No designated router on this network
No backup designated router on this network
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:08
Index 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)

2.5. CONFIGURACION SWITCHES

La configuración de un switch tiene las siguientes especificaciones, Configuración de VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida:

Configuración Vlan's:

SWITCH S1

Switch#configure ter
Enter configuration commands, one per line. End with CNTL/Z.

```
S1 (config)#int vlan 30
S1 (config-vlan)# description Administracion
S1 (config-vlan)#exit
S1 (config)#int vlan 40
S1 (config-vlan)# description Mercadeo
S1 (config-vlan)#ex
S1 (config)#int vlan 200
S1 (config-vlan)# description Mantenimiento
```

```
S1(config)#int vlan 200
S1(config-if)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.200.1
```

```
S1(config)#int fastEthernet 0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#exit
```

Con el comando "show vlan brief" podemos identificar las vlan activas y los puertos asignados para cada vlan:

```
S1#show vlan brief
```

```
VLAN Name Status Ports
```

```
-----
1 default active Fa0/4, Fa0/5, Fa0/6, Fa0/7
Fa0/8, Fa0/9, Fa0/10, Fa0/11
Fa0/12, Fa0/13, Fa0/14, Fa0/15
Fa0/16, Fa0/17, Fa0/18, Fa0/19
Fa0/20, Fa0/21, Fa0/22, Fa0/23
Gig0/1, Gig0/2
30 administracion active Fa0/1, Fa0/2
40 Mercadeo active
```

```
200 Mantenimiento active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

SWITCH S3

```
Switch(config)#hostname S3
S3(config)#
S3(config)#int vlan 30
S3(config-vlan)# description Administracion
S3(config-vlan)#exit
S3(config)#int vlan 40
S3(config-vlan)# description Mercadeo
S3(config-vlan)#exit
S3(config)#int vlan 200
S3(config-vlan)# description Mantenimiento
```

```
S3(config)#int vlan 200
S3(config-if)#ip address 192.168.200.3 255.255.255.0
S3(config)#ip default-gateway 192.168.200.1
```

Aplicamos “show vlan brief” para identificar las vlan activas y los puertos asignados para cada vlan, asi validamos que la configuración cumpla con lo exigido:

```
S3#show vlan brief
```

```
VLAN Name Status Ports
```

```
-----
1 default active Fa0/2, Fa0/4, Fa0/5, Fa0/6
Fa0/7, Fa0/8, Fa0/9, Fa0/10
Fa0/11, Fa0/12, Fa0/13, Fa0/14
Fa0/15, Fa0/16, Fa0/17, Fa0/18
Fa0/19, Fa0/20, Fa0/21, Fa0/22
Fa0/23, Fa0/24, Gig0/1, Gig0/2
30 Administracion active
40 Mercadeo active Fa0/1
200 Mantenimiento active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

Configuración de Encapsulamiento

Para tener conectividad se configura en el router de Bogota las vlan's que se asignaron para cada área:

```
Bogota(config)#int GigabitEthernet0/0.30
Bogota(config-subif)#description Administracion
Bogota(config-subif)#encapsulation dot1q 30
Bogota(config-subif)#ip address 192.168.30.1 255.255.255.0
Bogota(config-subif)#no shutdown
```

```
Bogota(config)#int GigabitEthernet0/0.40
Bogota(config-subif)#description Mercadeo
Bogota(config-subif)#encapsulation dot1q 40
Bogota(config-subif)#ip address 192.168.40.1 255.255.255.0
Bogota(config-subif)#no shutdown
```

```
Bogota(config)#interface GigabitEthernet0/0.200
Bogota(config-subif)#description Mantenimiento
Bogota(config-subif)# ip address 192.168.200.1 255.255.255.0
Bogota(config-subif)#encapsulation dot1Q 200
Bogota(config-subif)#no shutdown
```

En el S1 configuramos en los puertos fastEthernet 0/24 y 0/3 , en "mode trunk" ya que pasan varias vlan's

S1

```
S1(config)#int fastEthernet 0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int fastEthernet 0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#no shutdown
```

```
S3(config)#interface fastEthernet 0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk nativ vlan 1
S3(config-if)#no shutdown
```

Puertos de acceso

Los puertos de acceso son configurados para conectar las maquinas terminales, pueden ser PC, portatiles, impresoras, etc:

S1

```
S1(config)#int fastEthernet 0/1
S1(config-if)#switchport mode acces
S1(config-if)#switchport acces vlan 30
S1(config-if)#exit
```

S3

```
S3(config)#interface fastEthernet 0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#^Z
```

En el Switch 3 deshabilitar DNS lookup

```
S3(config)#no ip domain-lookup
```

Asignacion direcciones IP

Con el fin de tener conectividad asignamos direccionamiento ip a los Switches en la interfaz vlan 1:

S1

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
```

S3

```
S3(config)#interface vlan 1
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
```

Para evitar ataques a la red o ingreso a la red no autorizado se desactivan todas las interfaces que no sean utilizadas en el esquema de red.

```
S1(config)#interface range fastEthernet 0/4-24
```

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

```
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
```

```
-----EDITADO-----
```

```
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
```

```
S3(config)#interface range fastEthernet 0/4-24
```

```
S3(config-if-range)#shutdown
```

```
%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to administratively down
```

```
-----EDITADO-----
```

```
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
```

Verificación conectividad

S1 to S3

```
S1#ping 192.168.200.3
```

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

```
Sending 5, 100-byte ICMP Echos to 192.168.200.3, timeout is 2 seconds:
```

```
!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms
```

S1 to R1

```
S1#ping 192.168.200.1
```

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

```
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
```

```
!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/13 ms
```

S3 to S1

```
S3#ping 192.168.200.2
```

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

```
Sending 5, 100-byte ICMP Echos to 192.168.200.2, timeout is 2 seconds:
```

```
!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/7 ms
```

S3 to R1

```
S3#ping 192.168.200.1
```

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

```
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
```

```
!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/10 ms
```


2.6. CONFIGURACIÓN DHCP

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

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

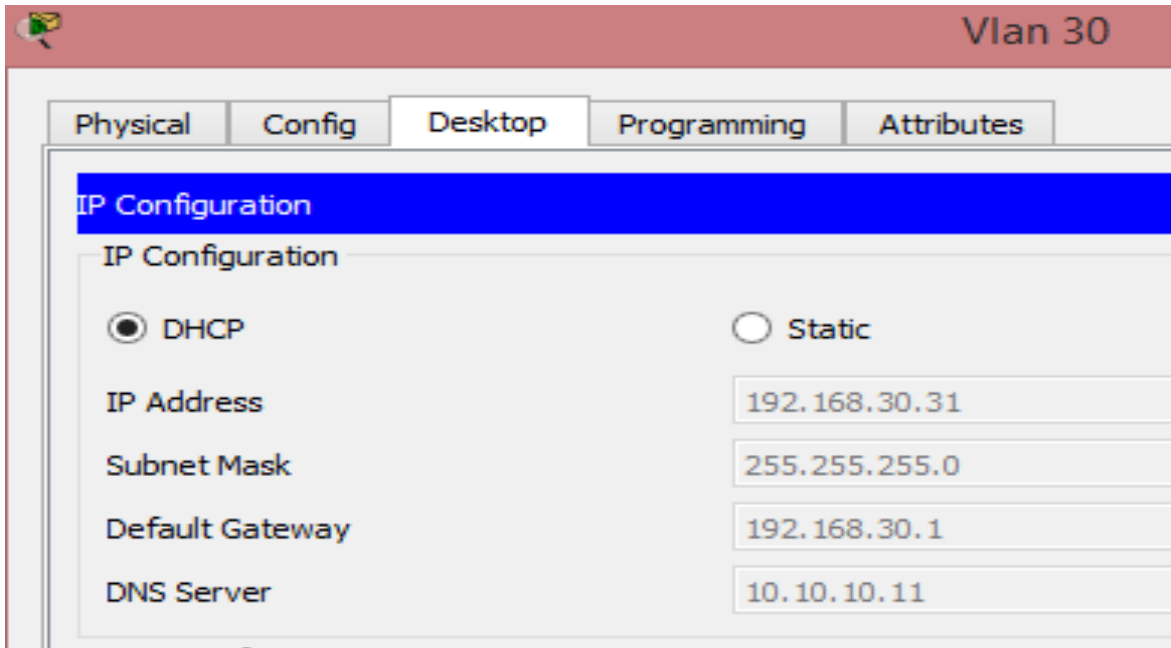
```
Bogota#configure ter
Enter configuration commands, one per line. End with CNTL/Z.
Bogota(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
Bogota(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
Bogota(config)#ip dhcp pool Admin_V30
Bogota(dhcp-config)#network 192.168.30.0 255.255.255.0
Bogota(dhcp-config)#default-router 192.168.30.1
Bogota(dhcp-config)#dns-server 10.10.10.11
```

```
Bogota(config)#no ip dhcp pool Merca_V40network
Bogota(config)#ip dhcp pool Merca_V40
Bogota(dhcp-config)#network 192.168.40.0 255.255.255.0
Bogota(dhcp-config)#default-router 192.168.40.1
Bogota(dhcp-config)#dns-server 10.10.10.11
```

```
S1(config-if)#ip helper-address 192.168.30.1
```

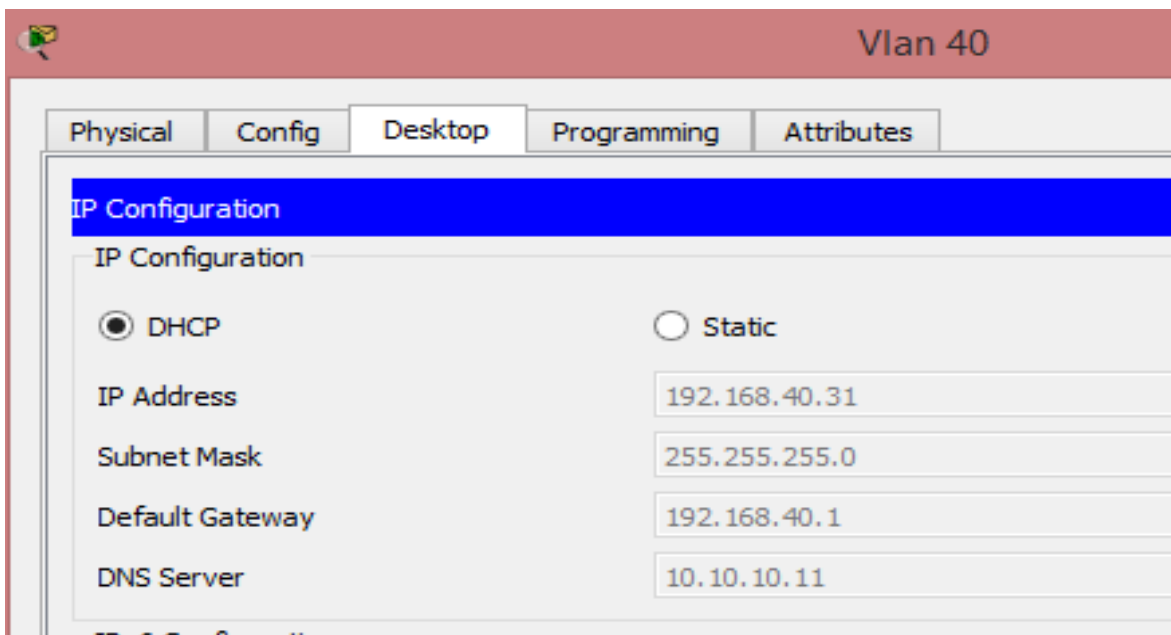
Verificacion DHCP

Ilustración 9 Verificacion DHCP para PC VLAN 30



Fuente: Cisco Packet tracer, diseño de red.

Ilustración 10 Verificacion DHCP para PC VLAN 40



Fuente: Cisco Packet tracer, diseño de red.

2.7. CONFIGURAR NAT

Configurar NAT en R2 para permitir que los hosts puedan salir a internet

```
Miami(config)#ip nat inside source static 10.10.10.10 209.165.200.225  
Miami(config)#int GigabitEthernet0/1
```

```
Miami(config-if)#ip nat inside
```

```
Miami(config)#ip nat pool Internet 209.165.200.226 209.165.200.230 netmask  
255.255.255.248
```

```
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)#access-list 1 permit 192.168.4.0 0.0.3.255
```

```
Miami(config)#ip nat inside source list 1 pool Internet
```

```
Miami(config)#int Serial0/1/1
```

```
Miami(config-if)#ip nat inside
```

```
Miami(config-if)#exit
```

```
Miami(config)#int GigabitEthernet0/0
```

```
Miami(config-if)#ip nat outside
```

2.8. CONFIGURACION LISTA DE ACCESO

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

```
Miami(config)#ip access-list standard Admin_Mtto
```

```
Miami(config-std-nacl)#permit host 172.31.21.1
```

```
Miami(config-std-nacl)#
```

```
Miami(config-std-nacl)#exit
```

```
Miami(config)#line vty 0 4
```

```
Miami(config-line)#acce
```

```
Miami(config-line)#access-class Admin_Mtto in
```

```
Miami(config-line)#
```

Verificación

Ilustración 11 Configuración lista de acceso

```
Bogota#telnet 172.31.21.2
Trying 172.31.21.2 ...OpenUnauthorized access prohibited!

User Access Verification

Password:
Miami>en
Password:
Miami#exit

[Connection to 172.31.21.2 closed by foreign host]
Bogota#
```

Fuente: Cisco Packet tracer, diseño de red.

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

Ilustración 12 Prueba de conectividad entre el PC VLAN 30 y PC VLAN 40

The image shows two windows from Cisco Packet Tracer. The left window is titled 'Vlan 40' and shows the 'IP Configuration' tab. It displays the following settings: IP Configuration is set to 'Static' (selected), IP Address is 192.168.40.31, Subnet Mask is 255.255.255.0, Default Gateway is 192.168.40.1, and DNS Server is 10.10.10.11. The right window is titled 'Vlan 30' and shows a 'Command Prompt' window. The command prompt displays the following output for a ping test to 192.168.40.31:

```
C:\>ping 192.168.40.31

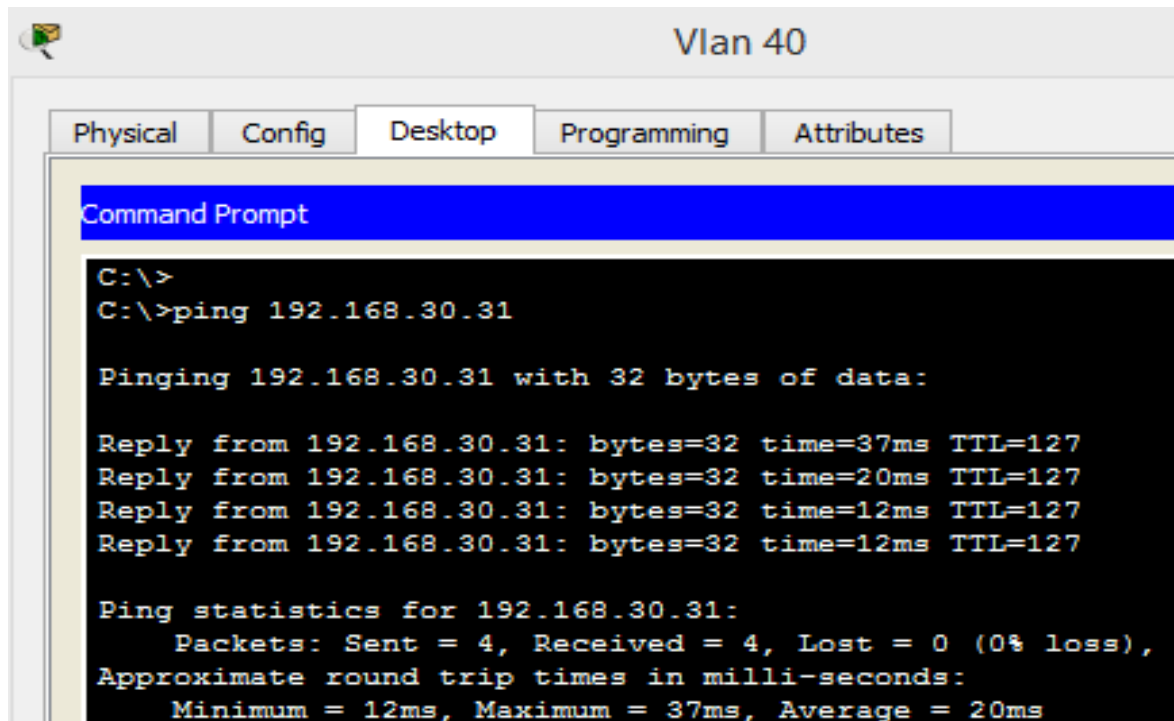
Pinging 192.168.40.31 with 32 bytes of data:

Reply from 192.168.40.31: bytes=32 time=21ms TTL=127
Reply from 192.168.40.31: bytes=32 time=16ms TTL=127
Reply from 192.168.40.31: bytes=32 time=12ms TTL=127
Reply from 192.168.40.31: bytes=32 time=12ms TTL=127

Ping statistics for 192.168.40.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 21ms, Average = 15ms
```

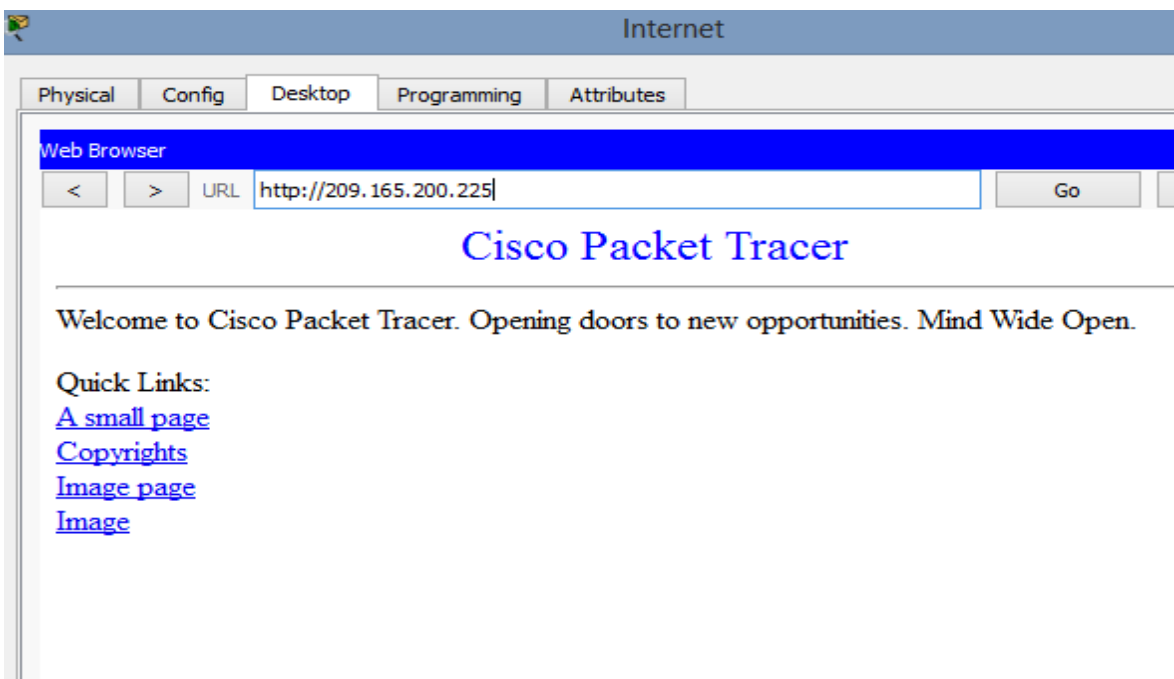
Fuente: Cisco Packet tracer, diseño de red.

Ilustración 13 Prueba de conectividad entre el PC VLAN 40 y PC VLAN 30



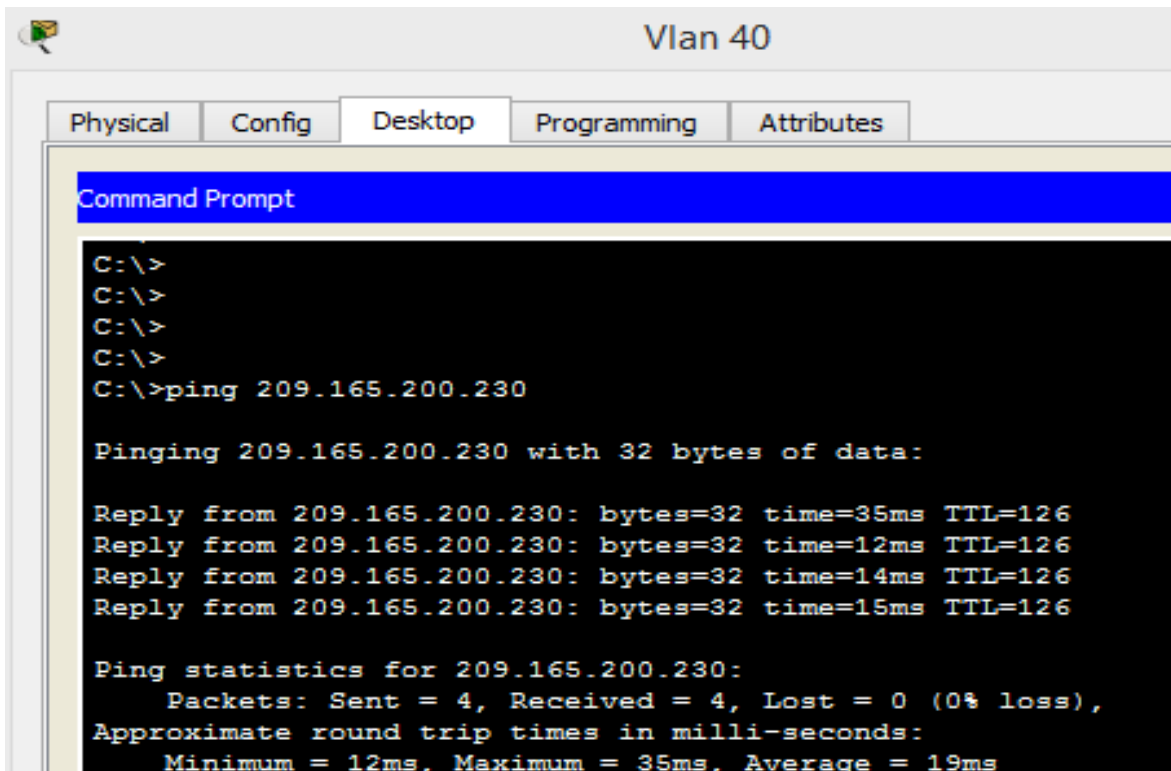
Fuente: Cisco Packet tracer, diseño de red.

Ilustración 14 Prueba de navegación PC Internet



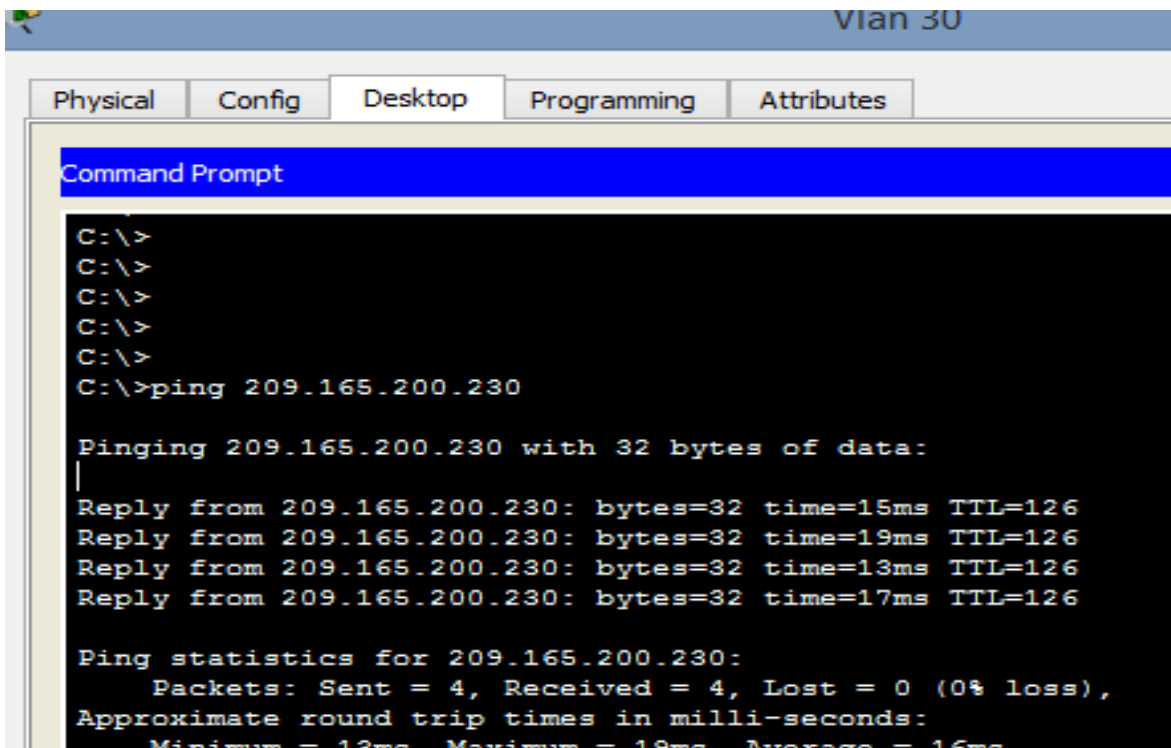
Fuente: Cisco Packet tracer, diseño de red.

Ilustración 15 Prueba de conectividad del PC VLAN 40 hacia PC Internet



Fuente: Cisco Packet tracer, diseño de red.

Ilustración 16 Prueba de conectividad del PC VLAN 30 hacia PC Internet



Fuente: Cisco Packet tracer, diseño de red.

CONCLUSIONES

En el informe realizado “Pruebas de habilidades prácticas”, podemos observar el comportamiento de las redes LAN y WAN según lineamientos requeridos.

En el primer escenario aprendí sobre el comportamiento del protocolo de enrutamiento RIP que según pruebas ejecutadas evidencie que este protocolo calcula la mejor ruta para enviar los paquetes IP hacia el destino utilizando como métrica el número de saltos.

En el segundo escenario configure tres redes LAN; Bogotá, Miami, Buenos Aires , en el análisis del protocolo de enrutamiento OSPF evidencie que la prioridad para envío de paquetes depende del menor costo, teniendo en cuenta que a mayor ancho de banda menor es el costo, también ejecute configuración de DHCP VLAN's , NAT. Y listas de acceso.

Esta prueba de habilidad práctica de Cisco reúne todos los temas vistos en los módulos.

BIBLIOGRAFÍA

¿Cómo funciona el balanceo de cargas? - Cisco. (s. f.). Recuperado 13 de julio de 2019, de https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/5212-46.html

Protocolo RIP [Sistemas Operativos]. (s. f.). Recuperado 13 de julio de 2019, de http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicacion/es/protocolo_rip#compatibilidad_ripv1ripv21

(4) en RSE Skills Assessment Student Exam - YouTube. (s. f.). Recuperado 13 de julio de 2019, de <https://www.youtube.com/watch?v=HWC2bHCjIAA>

ANEXO

ANEXO 1 LINK CISCO PACKET TRACERT DEL CASO 1 Y CASO 2

<https://drive.google.com/open?id=1C6BuFpPbWvnTr08r7alyGRj6oT7LoI-R>

