

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

HELMUT HOLGUIN VEGA

**Diplomado CCNA
como opción de grado**

Instructor: Iván Gustavo Peña

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
BOGOTA D.C.**

2019

Contenido

Introducción	3
1. Escenario 1	4
2. Desarrollo de las actividades Escenario 1	5
2.1. Configuración RIPv2 en R1, R2 Y R3.....	5
2.2. Consulta tabla de enrutamiento R1, R2 y R3.....	6
2.3. Pruebas de conectividad.....	10
3. Escenario 2	13
3.1. Direccionamiento IP	14
3.2. Configuración OSPFv2	17
3.3. Verificación información OSPF	19
3.4. Configuración switches	25
3.5. Deshabilitar DNS lookup.....	28
3.6. Asignación de direcciones IP a los switches.....	28
3.7. Desactivación Puertos	29
3.8. Implementación DHCP y NAT para IPv4	30
3.9. Configuración NAT	31
3.10. Listas de Acceso	31
3.11. Verificación comunicación	33
Conclusiones	36
Bibliografía.....	37

Introducción

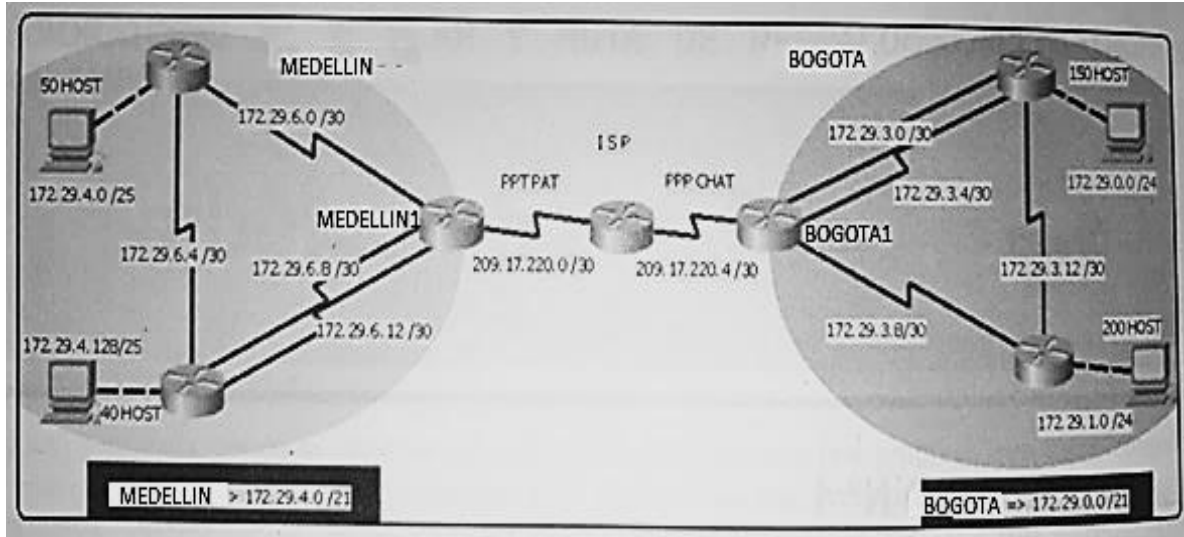
El mundo de hoy, tal como lo conocemos, se mantiene en un intercambio constante de información en medios digitales, las redes de cómputo hacen posible esta tarea, cada día aumenta de forma exponencial, ya que se agregan nuevos dispositivos, tales como celulares, televisores, lavadoras y todo lo que comprende el IoT o internet de las cosas, nuevas granjas de servidores más pc's entre otros. Entendiendo dichos requerimientos, surge una necesidad en el ámbito de las tecnologías de la información y es el de ingenieros que puedan realizar las implementaciones que contribuyan a la integración del mundo cibernético.

El siguiente trabajo escrito, en el cual se desarrollan las habilidades prácticas del diplomado CCNA, plasma el conocimiento adquirido, se puede apreciar, como todas y cada una de las actividades están enfocadas a la solución de problemas de la vida cotidiana de las empresas, las cuales dependen en gran medida de las tecnologías de la información.

Para ello, tenemos dos escenarios, en el primero hacemos uso del enrutamiento dinámico RIPv2 empleando NAT con sobrecarga y servicio de DHCP sobre el mismo router, para el segundo caso usamos el enrutamiento OSPFv2, servidor de DHCP y listas de acceso estándar y extendida, entre otros.

1. Escenario 1

Ilustración 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.

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

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

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

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

Desarrollo

Como trabajo inicial se debe realizar lo siguiente.

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

2. Desarrollo de las actividades Escenario 1

Para el desarrollo de este escenario, lo primero hacemos es armar la topología solicitada en la guía, con un router haciendo de ISP y 3 router adicionales interconectados, luego colocamos dos switches, uno en R2 y el otro en R3, dos PC y dos laptops, asignamos nombres y según la tabla realizamos el direccionamiento respectivo, recordemos que eso es lo básico, para poder identificar cada uno de los elementos en la red, posteriormente realizamos el NAT, no sin antes hacer una lista de acceso, requerida para poder hacer traducción de direcciones, igualmente, si no hacemos enrutamiento, no podemos tampoco alcanzar al ISP, también realizamos la configuración de DHCP server tanto en R2 como en R3, no hay que olvidar, que en este debemos además configurar el dual-stack, para poder darle direccionamiento en IPv4 e IPv6.

2.1. Configuración RIPv2 en R1, R2 Y R3

- R1, R2 y R3 intercambian información de routing mediante RIP versión 2.

Como necesitamos intercambiar rutas con los vecinos, implementamos RIPv2, con eso no tendremos que escribir las rutas una a una, solo declaramos las redes que ve el router a través de sus interfaces.

El script:

Para R1:

```
ena
conf ter
router rip
version 2
network 10.0.0.0
network 200.123.211.0
end
copy running-config startup-config
```

Para R2:

```
ena
conf ter
```

```
router rip
version 2
network 10.0.0.0
network 192.168.20.0
network 192.168.21.0
network 200.123.211.0
end
copy running-config startup-config
```

Para R3:

```
ena
conf ter
router rip
version 2
network 10.0.0.0
network 192.168.30.0
network 200.123.211.0
end
copy running-config startup-config
```

2.2. Consulta tabla de enrutamiento R1, R2 y R3

- R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.

Para dar cumplimiento a este punto, solo debemos ejecutar el comando `show ip route`, en donde se muestran todas y cada una de las rutas y su carácter o protocolo, por ejemplo, si la letra al principio de la línea, es C, entonces quiere decir que está directamente conectada, si, por el contrario, es R, es una ruta obtenida mediante RIP, S en cambio, es una ruta estática o configurada manualmente:

Ilustración 2: Tabla de enrutamiento R1

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

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 3 subnets
C       10.0.0.0 is directly connected, Serial0/1/0
C       10.0.0.4 is directly connected, Serial0/1/1
R       10.0.0.8 [120/1] via 10.0.0.6, 00:00:20, Serial0/1/1
         [120/1] via 10.0.0.2, 00:00:01, Serial0/1/0
R      192.168.20.0/24 [120/1] via 10.0.0.2, 00:00:01, Serial0/1/0
R      192.168.21.0/24 [120/1] via 10.0.0.2, 00:00:01, Serial0/1/0
R      192.168.30.0/24 [120/1] via 10.0.0.6, 00:00:20, Serial0/1/1
C      200.123.211.0/24 is directly connected, Serial0/0/0
S*     0.0.0.0/0 is directly connected, Serial0/0/0

R1#
```

Acá podemos apreciar lo anteriormente dicho, mediante el comando show ip route solicitamos al router la tabla de enrutamiento y esto es lo que nos muestra, 3 subredes sumariadas en 10.0.0.0/30, 3 directamente conectadas y 4 vistas por el router a través del protocolo RIP.

Ilustración 3: Tabla de enrutamiento R2

```
R2>ena
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

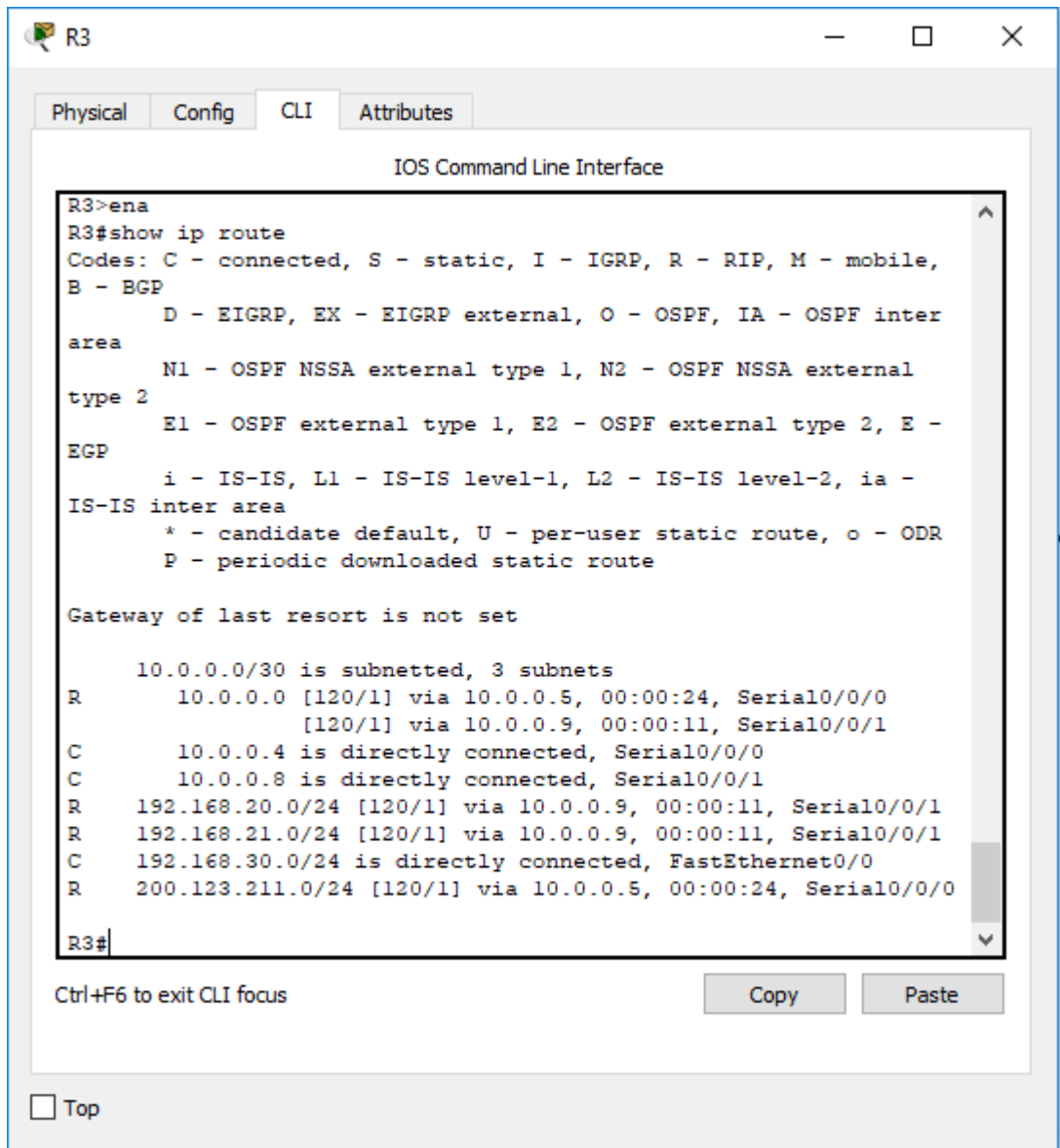
Gateway of last resort is not set

10.0.0.0/30 is subnetted, 3 subnets
C      10.0.0.0 is directly connected, Serial0/0/0
R      10.0.0.4 [120/1] via 10.0.0.10, 00:00:13, Serial0/0/1
       [120/1] via 10.0.0.1, 00:00:03, Serial0/0/0
C      10.0.0.8 is directly connected, Serial0/0/1
C      192.168.20.0/24 is directly connected, FastEthernet0/0.100
C      192.168.21.0/24 is directly connected, FastEthernet0/0.200
R      192.168.30.0/24 [120/1] via 10.0.0.10, 00:00:13, Serial0/0/1
R      200.123.211.0/24 [120/1] via 10.0.0.1, 00:00:03, Serial0/0/0

R2#
```

En esta imagen, la información de enrutamiento que nos arroja es: 3 subredes sumariadas en 10.0.0.0/30, 4 directamente conectadas y 3 vistas por el router a través del protocolo RIP, no hay estáticas.

Ilustración 4: Tabla de enrutamiento R3



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

Gateway of last resort is not set

      10.0.0.0/30 is subnetted, 3 subnets
R       10.0.0.0 [120/1] via 10.0.0.5, 00:00:24, Serial0/0/0
         [120/1] via 10.0.0.9, 00:00:11, Serial0/0/1
C       10.0.0.4 is directly connected, Serial0/0/0
C       10.0.0.8 is directly connected, Serial0/0/1
R       192.168.20.0/24 [120/1] via 10.0.0.9, 00:00:11, Serial0/0/1
R       192.168.21.0/24 [120/1] via 10.0.0.9, 00:00:11, Serial0/0/1
C       192.168.30.0/24 is directly connected, FastEthernet0/0
R       200.123.211.0/24 [120/1] via 10.0.0.5, 00:00:24, Serial0/0/0
R3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Aquí, la información de enrutamiento que nos arroja es: 3 subredes sumariadas en 10.0.0.0/30, 3 directamente conectadas y 4 vistas por el router a través del protocolo RIP, no hay estáticas.

2.3. Pruebas de conectividad

Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre ellos y el servidor.

Para hacer pruebas de conectividad, usamos la interfaz gráfica, aunque también lo podemos hacer directamente desde el terminal, entonces, arrastramos un mensaje simple PDU, lo soltamos primero en el origen y luego en el destino:

Ilustración 5: Haciendo ping en IPv4

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC20	Laptop21	ICMP	Black	0.000	N	0	(edit)	(delete)
	Successful	PC20	ISP	ICMP	Purple	0.000	N	1	(edit)	(delete)
	Successful	PC20	PC31	ICMP	Yellow	0.000	N	2	(edit)	(delete)
	Successful	Lapto...	Laptop20	ICMP	Pink	0.000	N	3	(edit)	(delete)

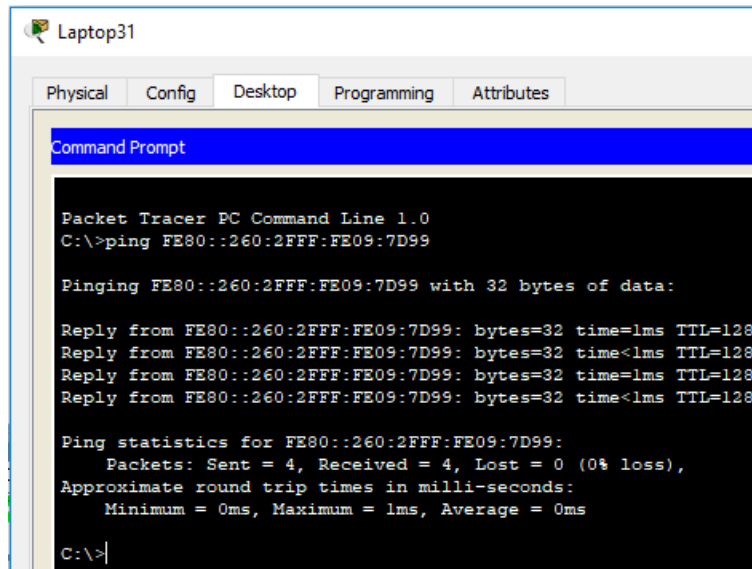
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC31	ISP	ICMP	Green	0.000	N	4	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP	Teal	0.000	N	5	(edit)	(delete)
	Successful	PC20	ISP	ICMP	Light Green	0.000	N	6	(edit)	(delete)
	Successful	PC21	ISP	ICMP	Blue	0.000	N	7	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Lapto...	ISP	ICMP	Purple	0.000	N	8	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP	Green	0.000	N	9	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP	Brown	0.000	N	10	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP	Olive	0.000	N	11	(edit)	(delete)
	Successful	PC31	ISP	ICMP	Blue	0.000	N	12	(edit)	(delete)
	Successful	PC30	ISP	ICMP	Dark Blue	0.000	N	13	(edit)	(delete)

Se observa que las pruebas fueron satisfactorias, lo que nos indica que la implementación nos ha quedado según lo solicitado en la guía para el desarrollo de las habilidades prácticas.

La interfaz gráfica no nos es útil cuando deseamos hacer pruebas de ping en IPv6, por eso usamos el CMD o command prompt, para realizar dichas pruebas:

Ilustración 18: ping IPv6 de Laptop31 a Servidor0



```
Packet Tracer PC Command Line 1.0
C:\>ping FE80::260:2FFF:FE09:7D99

Pinging FE80::260:2FFF:FE09:7D99 with 32 bytes of data:

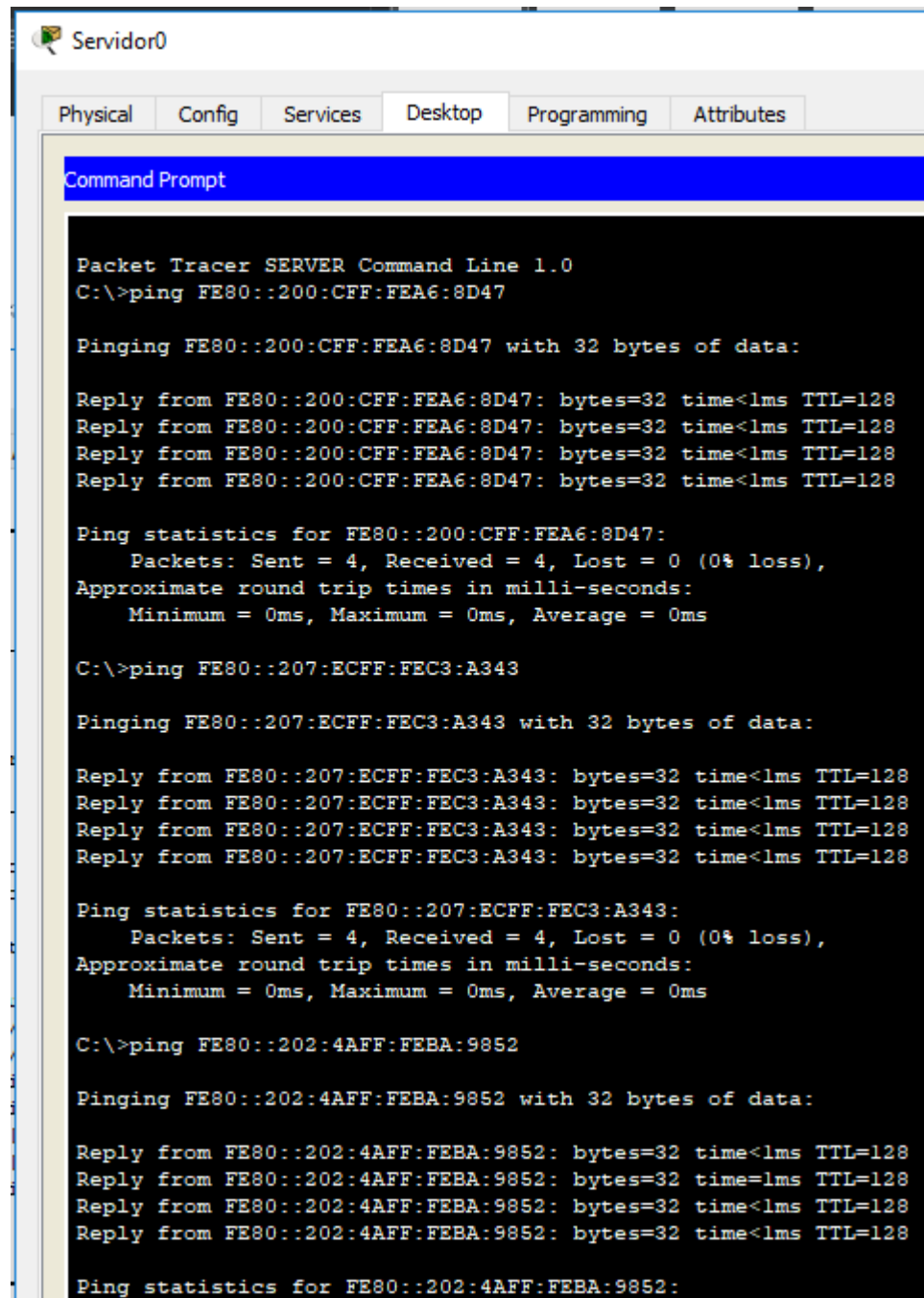
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time=1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time=1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128

Ping statistics for FE80::260:2FFF:FE09:7D99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Aquí estamos haciendo ping al servidor desde Laptop31 y esta es satisfactoria. Ahora, desde el servidor hacia los PC:

Ilustración 69: ping IPv6 desde Servidor0 a PCs



The screenshot shows a Packet Tracer interface for 'Servidor0'. The 'Command Prompt' window is active, displaying the results of three IPv6 ping tests. Each test shows four successful replies with 32 bytes of data, a time of less than 1ms, and a TTL of 128. The statistics for each test indicate that all four packets were sent and received, with 0% loss and 0ms round trip times.

```
Packet Tracer SERVER Command Line 1.0
C:\>ping FE80::200:CFF:FEA6:8D47

Pinging FE80::200:CFF:FEA6:8D47 with 32 bytes of data:

Reply from FE80::200:CFF:FEA6:8D47: bytes=32 time<1ms TTL=128
Reply from FE80::200:CFF:FEA6:8D47: bytes=32 time<1ms TTL=128
Reply from FE80::200:CFF:FEA6:8D47: bytes=32 time<1ms TTL=128
Reply from FE80::200:CFF:FEA6:8D47: bytes=32 time<1ms TTL=128

Ping statistics for FE80::200:CFF:FEA6:8D47:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping FE80::207:ECFF:FEC3:A343

Pinging FE80::207:ECFF:FEC3:A343 with 32 bytes of data:

Reply from FE80::207:ECFF:FEC3:A343: bytes=32 time<1ms TTL=128
Reply from FE80::207:ECFF:FEC3:A343: bytes=32 time<1ms TTL=128
Reply from FE80::207:ECFF:FEC3:A343: bytes=32 time<1ms TTL=128
Reply from FE80::207:ECFF:FEC3:A343: bytes=32 time<1ms TTL=128

Ping statistics for FE80::207:ECFF:FEC3:A343:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping FE80::202:4AFF:FEBA:9852

Pinging FE80::202:4AFF:FEBA:9852 with 32 bytes of data:

Reply from FE80::202:4AFF:FEBA:9852: bytes=32 time<1ms TTL=128
Reply from FE80::202:4AFF:FEBA:9852: bytes=32 time<1ms TTL=128
Reply from FE80::202:4AFF:FEBA:9852: bytes=32 time<1ms TTL=128
Reply from FE80::202:4AFF:FEBA:9852: bytes=32 time<1ms TTL=128

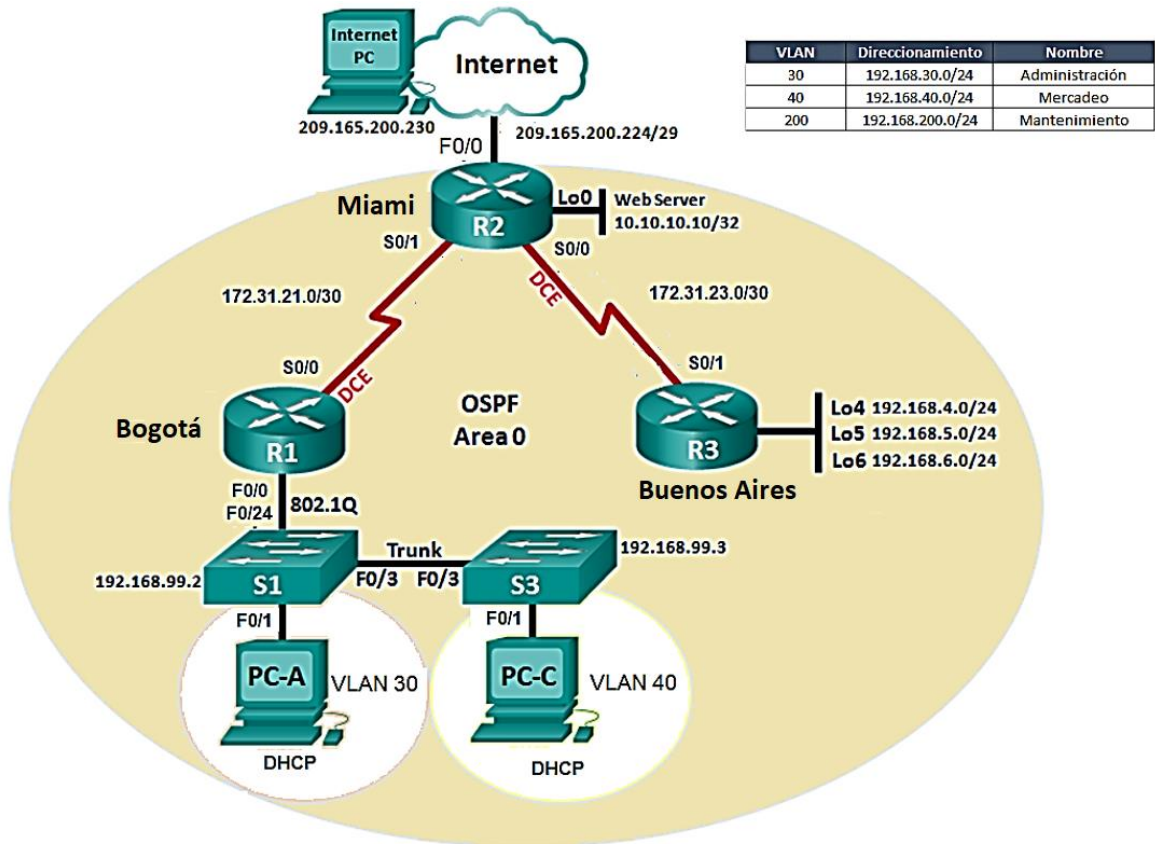
Ping statistics for FE80::202:4AFF:FEBA:9852:
```

Igualmente es satisfactoria la prueba de conectividad por el protocolo IPv6 desde el Servidor0 hacia los PC y Laptops conectados en SW3.

3. 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 20: Escenario 2



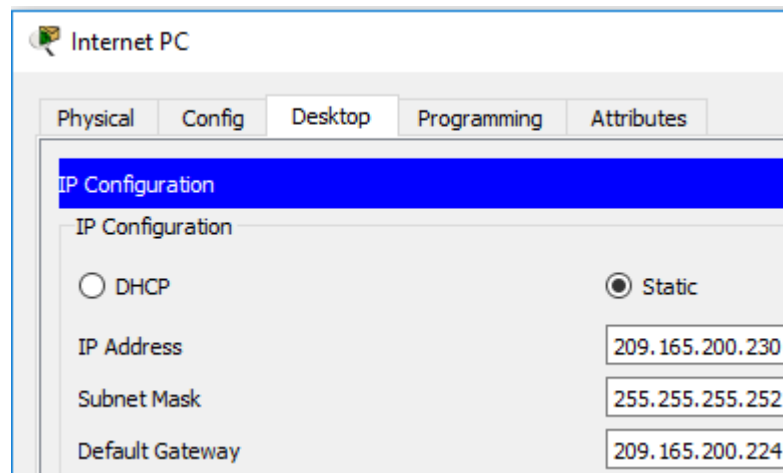
Para este escenario, lo primero que debemos hacer, es montar la topología según indica el gráfico, en el, observamos que la red de mantenimiento, es decir, la red que usan los switches para ser administrados, tiene una vlan asignada, la cual es la 200, con un direccionamiento 192.168.200.0/24, pero algo diferente es lo que observamos al lado switches y es que no concuerda el gráfico con la tabla, por ejemplo, el S1 lleva direccionamiento 192.168.99.2, pero debería ser 200.2 según la tabla, por tal motivo he escogido usar el direccionamiento de la tabla, que en términos de la práctica se cumple con lo solicitado.

3.1. Direccionamiento IP

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

Para este punto, lo que debemos hacer, como siempre, luego de montar la topología, es asignar las direcciones, subir interfaces en los routers y en los switches, apagar las que no se vayan a utilizar:

Ilustración 71: Direccionamiento Internet PC



El internet PC debemos configurarlo mediante la interfaz gráfica, en la pestaña Desktop, luego hacemos click en el ícono de **IP Configuration**, damos click en checkbox Static y colocamos los números de rigor, la IP, la máscara y la salida por defecto, además, ponemos una descripción a cada una de las interfaces, importante, al momento de revisar después de un tiempo nuestro equipo configurado y saber cuál es el carácter de la misma.

A continuación, digitamos el script necesario para cada uno de los routers de la topología y los switches:

El script:

Para R1

ena

conf ter

host Bogota

```
inter f0/0
no shut
inter f0/30
description Administracion
ip addr 192.168.30.1 255.255.255.0
inter f0/40
description Mercadeo
ip addr 192.168.40.1 255.255.255.0
inter f0/200
description Mantenimiento
ip addr 192.168.200.1 255.255.255.0
inter s0/0/0
ip address 172.31.21.2 255.255.255.252
no shut
end
copy running-config startup-config
```

Para R2

```
ena
conf ter
host Miami
inter lo0
description WebServer
ip addr 10.10.10.10 255.255.255.255
inter f0/0
ip addr 209.165.200.229 255.255.255.248
no shut
inter s0/0/0
ip addr 172.31.23.1 255.255.255.252
no shut
inter s0/0/1
```

```
ip addr 172.31.21.1 255.255.255.252
no shut
end
copy running-config startup-config
```

Para R3

```
ena
conf ter
host Buenos_Aires
inter lo4
ip addr 192.168.4.1 255.255.255.0
inter lo5
ip addr 192.168.5.1 255.255.255.0
inter lo6
ip addr 192.168.6.1 255.255.255.0
inter s0/0/1
ip address 172.31.23.2 255.255.255.252
no shut
end
copy running-config startup-config
```

Para SW1

```
ena
conf ter
host S1
vlan 200
inter vlan 200
ip addr 192.168.200.2 255.255.255.0
end
copy running-config startup-config
```


Para SW3

```
ena
conf ter
host S3
vlan 200
inter vlan 200
ip addr 192.168.200.3 255.255.255.0
end
copy running-config startup-config
```

3.2. Configuración OSPFv2

Configurar el protocolo de enrutamiento OSPFv2 bajo los criterios de la tabla 3:

Tabla 3: parámetros OSPFv2

OSPFv2 area 0

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

A diferencia del escenario anterior, acá usaremos otro tipo de enrutamiento dinámico, este es el más usado en redes grandes y es OSPF, en su versión 2, lo primero es darle un id al router, para poderlo identificar cuando hagamos una consulta para troubleshooting, luego, declaramos las interfaces pasivas, son aquellas que no se utilizan en el proceso de OSPF, esto ahorrará poder de procesamiento y memoria en el router, ya sabemos que son recursos preciados, luego declaramos las redes que se encuentran en cada interface que participa en el proceso de OSPF, de esta manera, mediante mensajes publicados a través de estas, conoce a sus vecinos y comparten las rutas para poder a llegar a todas las redes interconectadas, evitando así, el arduo trabajo administrativo de digitar las rutas.

Luego nos vamos a la interfaz involucrada y le damos el ancho de nada máximo a usar, con esto manejamos también el consumo de recursos en la red, luego

configuramos el costo, recordemos que, según el costo, OSPF va a escoger la mejor ruta, la que le cueste menos enviar un paquete.

Todo esto se configura así:

El script

Para R1

```
ena
conf ter
router ospf 1
router-id 1.1.1.1
passive-interface FastEthernet0/0
network 172.31.21.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
interface Serial0/0/0
bandwidth 256
ip ospf cost 9500
end
copy running-config startup-config
```

Para R2

```
ena
conf ter
router ospf 1
router-id 5.5.5.5
passive-interface FastEthernet0/0
passive-interface Loopback0
network 209.165.200.224 0.0.0.7 area 0
network 172.31.21.0 0.0.0.3 area 0
network 172.31.23.0 0.0.0.3 area 0
network 10.10.10.10 0.0.0.0 area 0
interface Serial0/0/0
```

```
bandwidth 256
ip ospf cost 9500
interface Serial0/0/1
bandwidth 256
end
copy running-config startup-config
```

Para R3

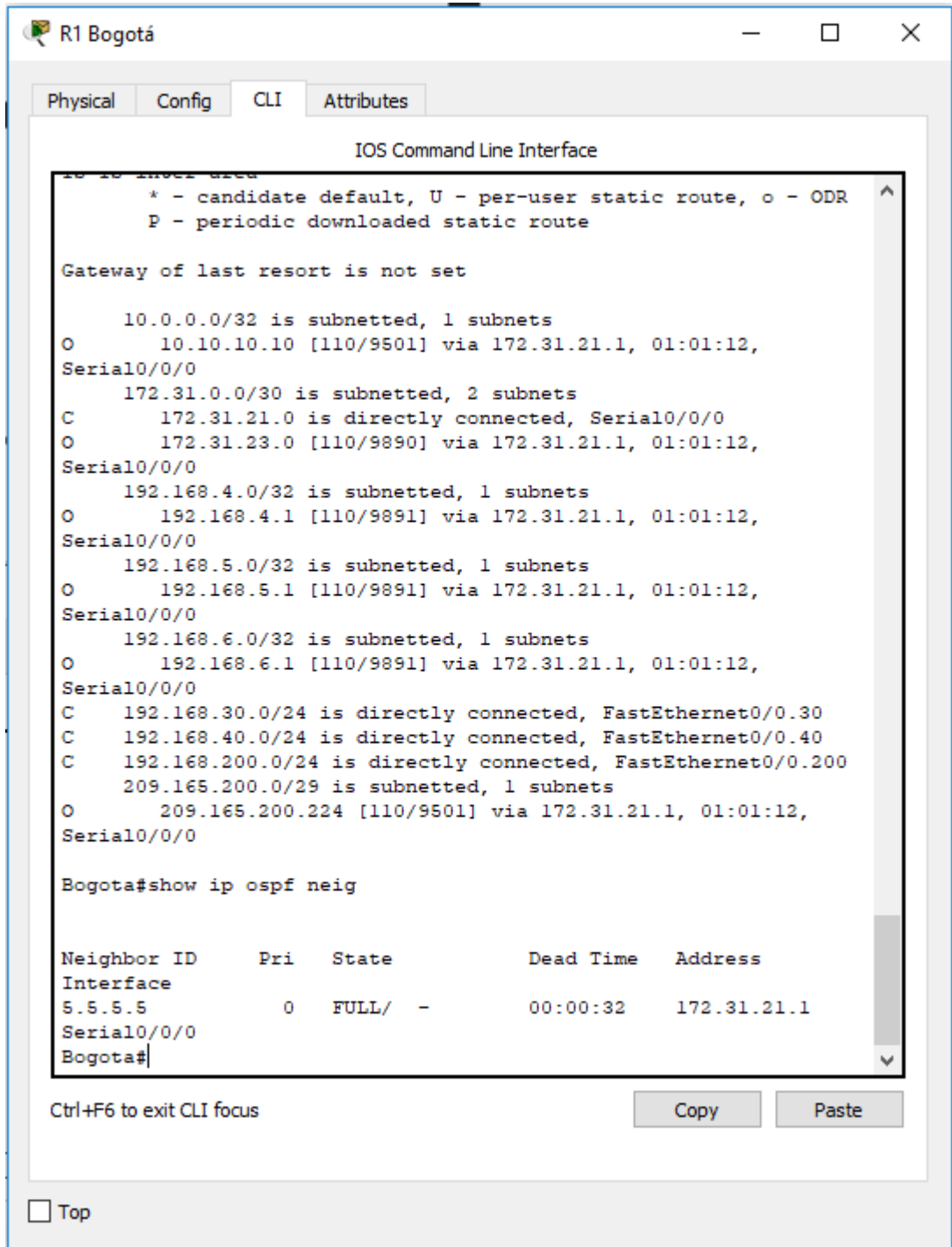
```
ena
conf ter
router ospf 1
router-id 8.8.8.8
passive-interface Loopback4
passive-interface Loopback5
passive-interface Loopback6
network 172.31.23.0 0.0.0.3 area 0
network 192.168.4.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
interface Serial0/0/1
bandwidth 256
end
copy running-config startup-config
```

3.3. Verificación información OSPF

Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Con las redes declaradas en cada switch, inmediatamente comienzan a intercambiar información, el protocolo hace lo que debe y a los segundos ya los router se encuentran en comunicación. Allí es donde nosotros podemos hacer una consulta con los diferentes comandos que nos lo permiten:

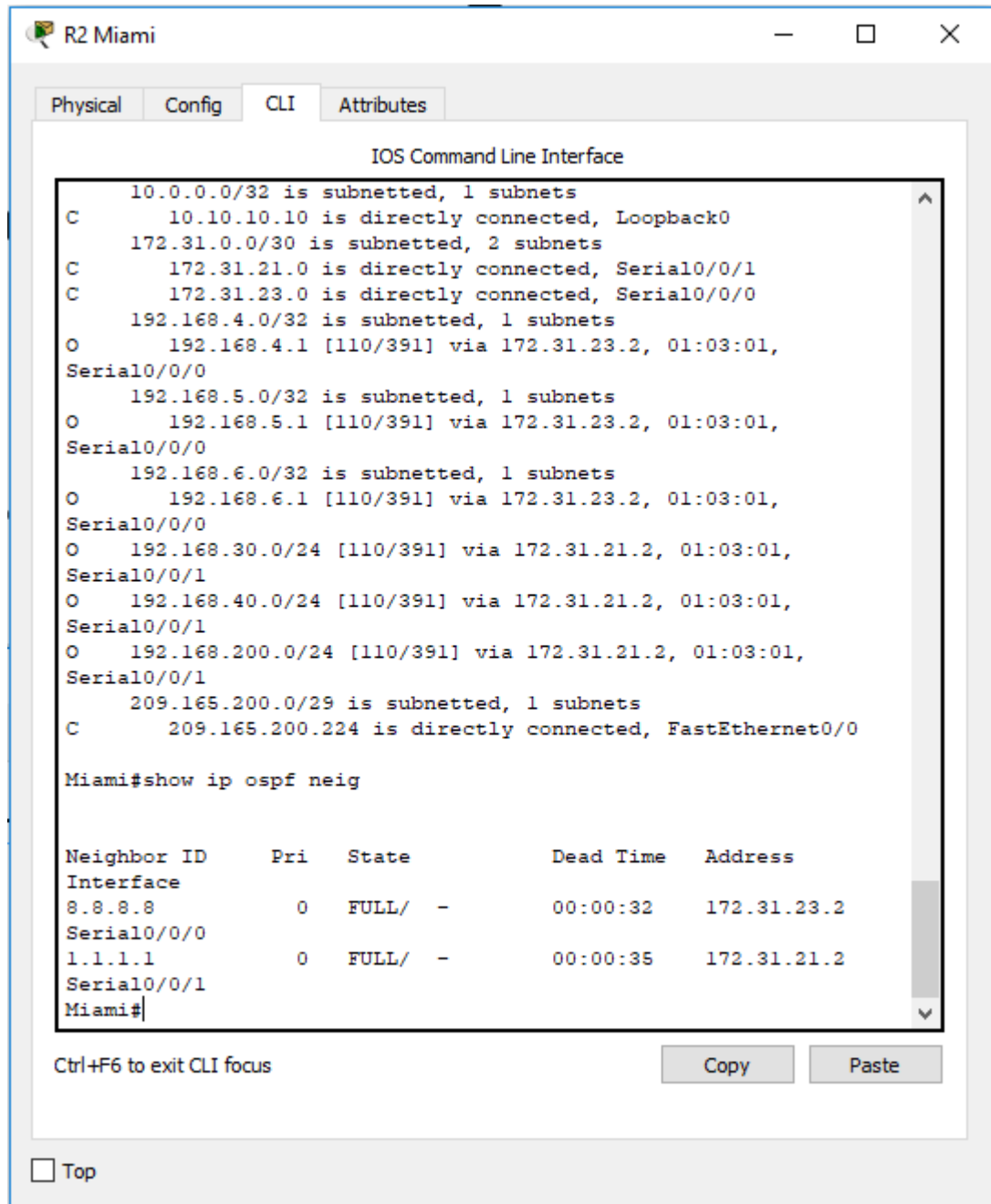
Ilustración 82: Tabla de enrutamiento R1



En esta imagen observa, cuales con las rutas obtenidas por OSPF y las que están directamente conectadas, el comando empleado es show ip router, seguidamente

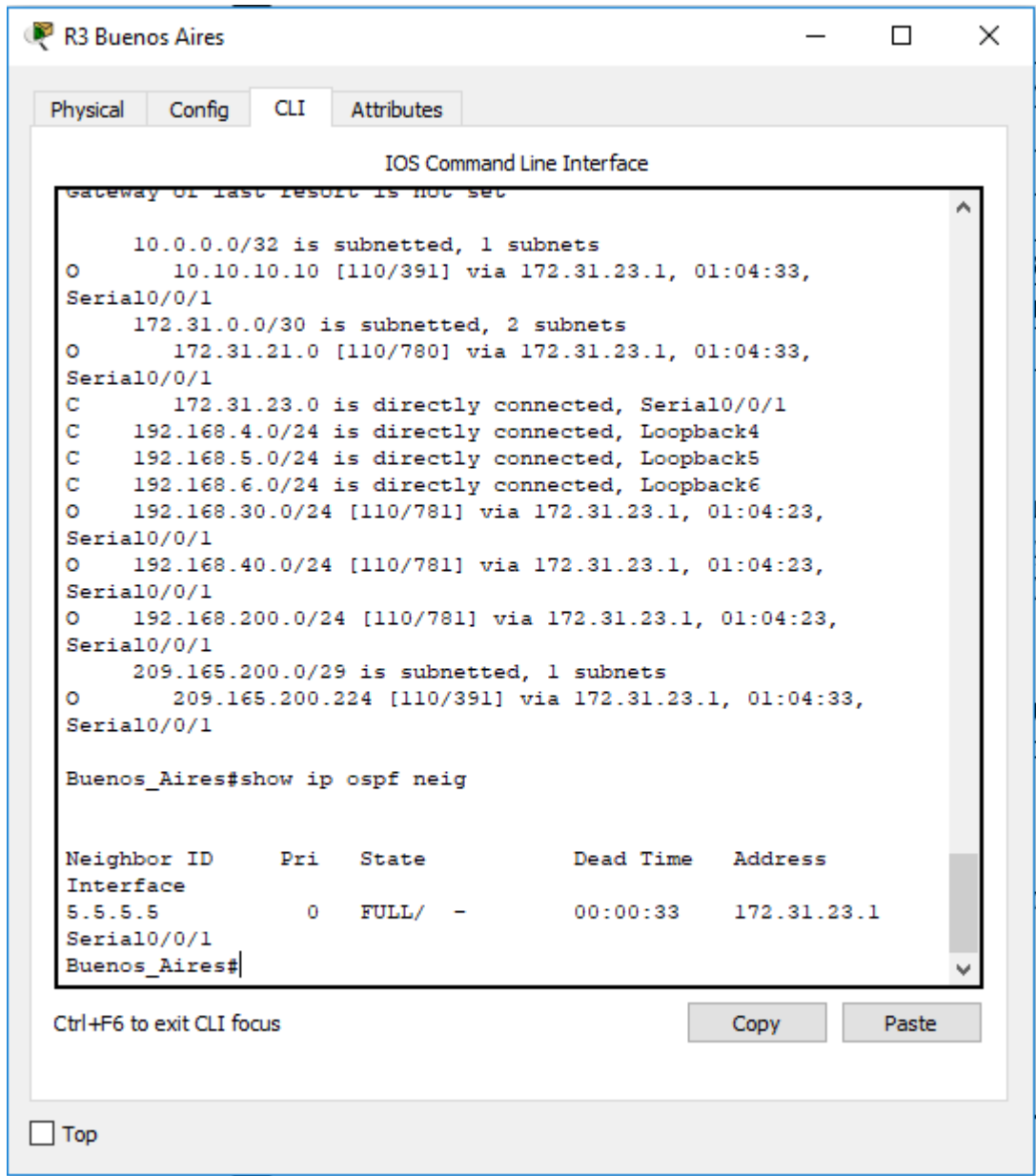
digitamos el comando show ip ospf neighbor, es decir, consultar cuales son los vecinos.

Ilustración 23: Tabla de enrutamiento R2



En esta gráfica observamos la misma consulta, pero realizada a R2, como podemos ver, en el R1 solo había 1 vecino, pero R2 tiene 2 vecinos, uno por cada interfaz serial.

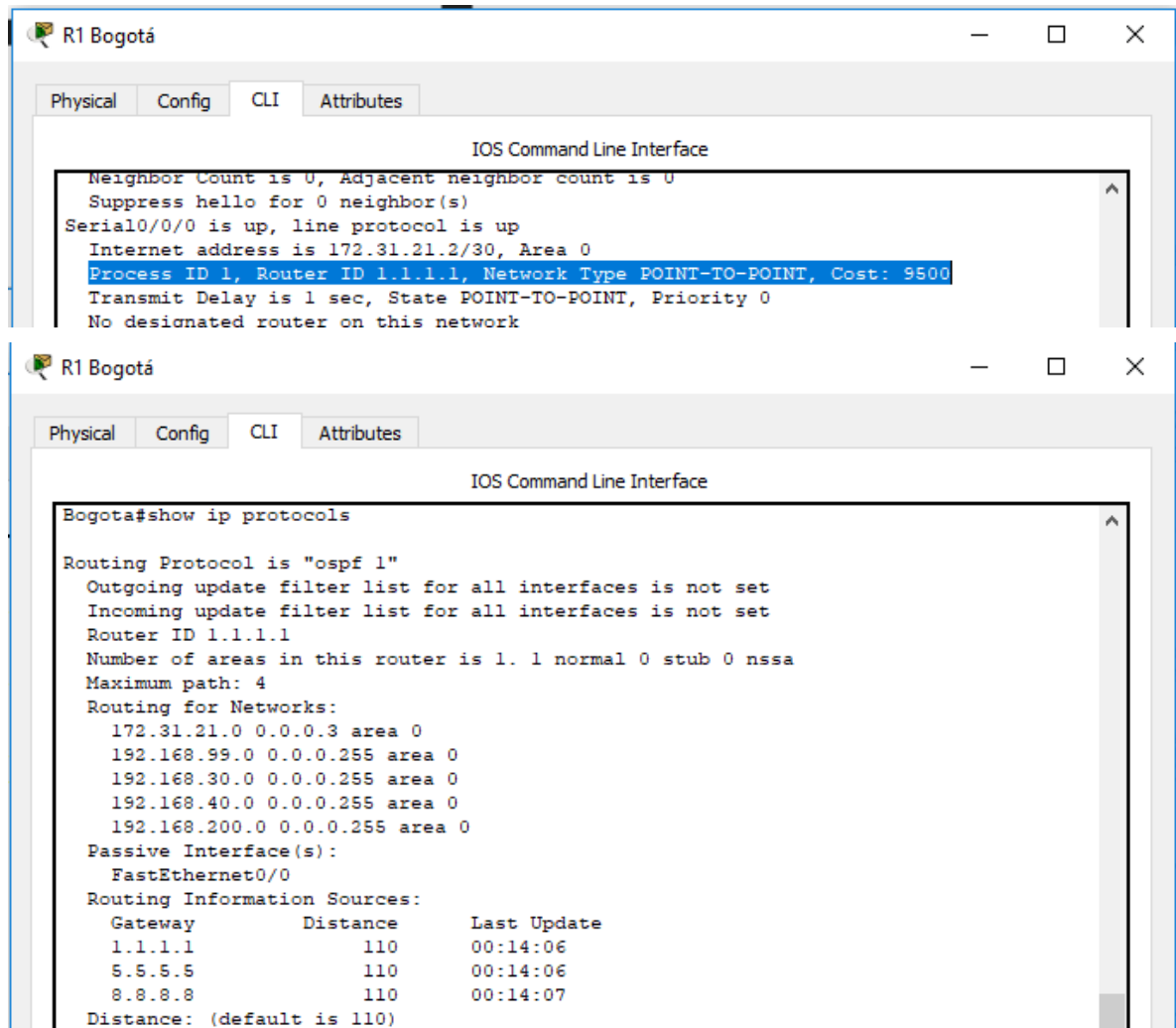
Ilustración 24: Tabla de enrutamiento R3



Finalmente, vemos a R3, el cual tiene un solo vecino conectado en la interfaz s0/0/1. Cada uno de los router, tiene en su tabla de enrutamiento las rutas que sus router vecinos le proporcionan mediante el protocolo de OSPF, por ejemplo, en R3 está la ruta 192.168.200.0/24 red que se encuentra en el R1, pero que es posible alcanzarla, al salir por la 172.31.23.1 y de esta manera evitamos el trabajo asministrativo, que implicaría estar ingresando manualmente las rutas.

- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Ilustración 95: Verificación en R1

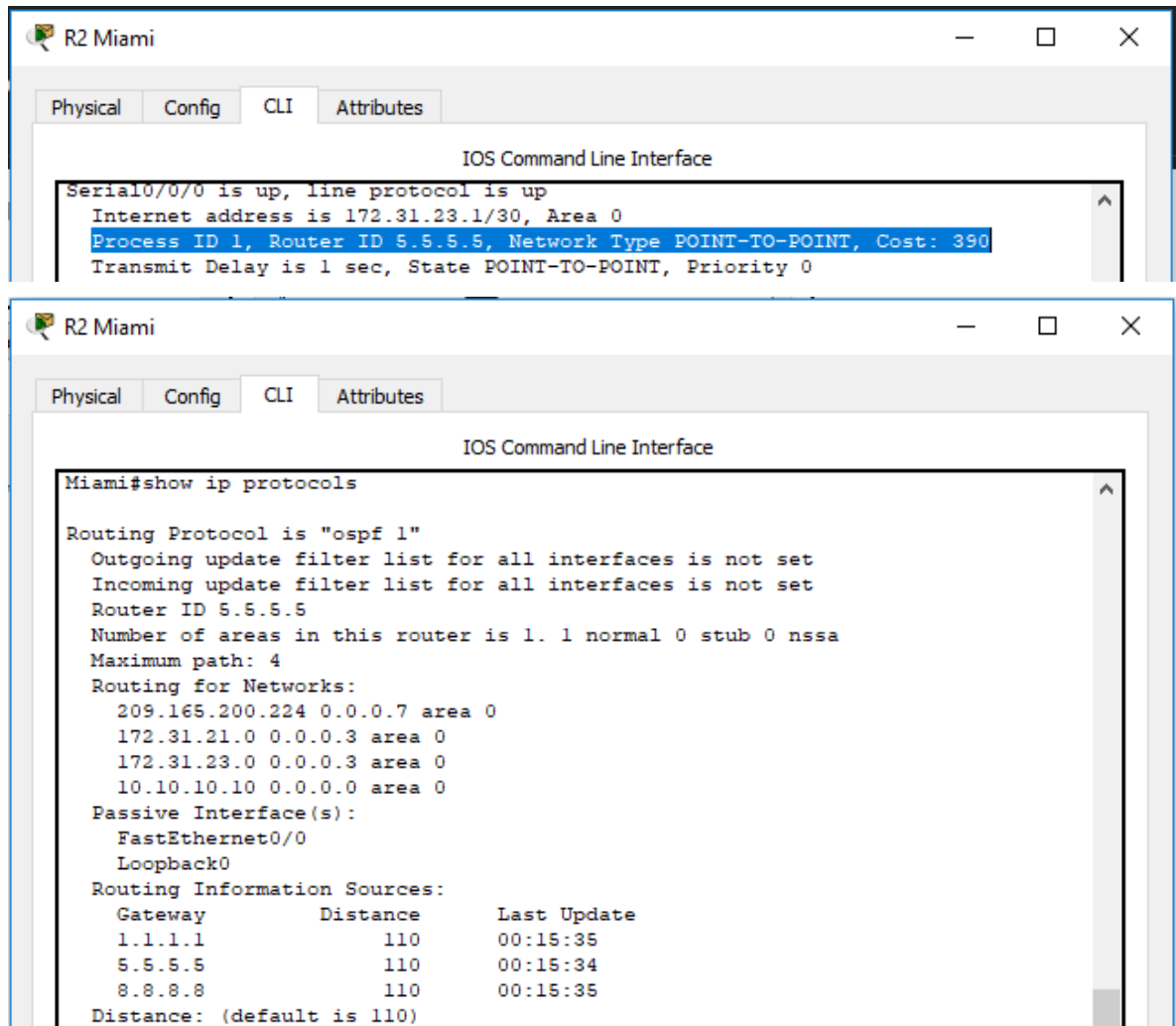


En la gráfica anterior, podemos apreciar el costo de las interfaces, al final de la línea resaltada en azul, y su valor es 9500. Información obtenida mediante el comando **show ip ospf interface**

También podemos visualizar cual es el id de proceso, este es 1, el id del router, el cual configuramos como 1.1.1.1.

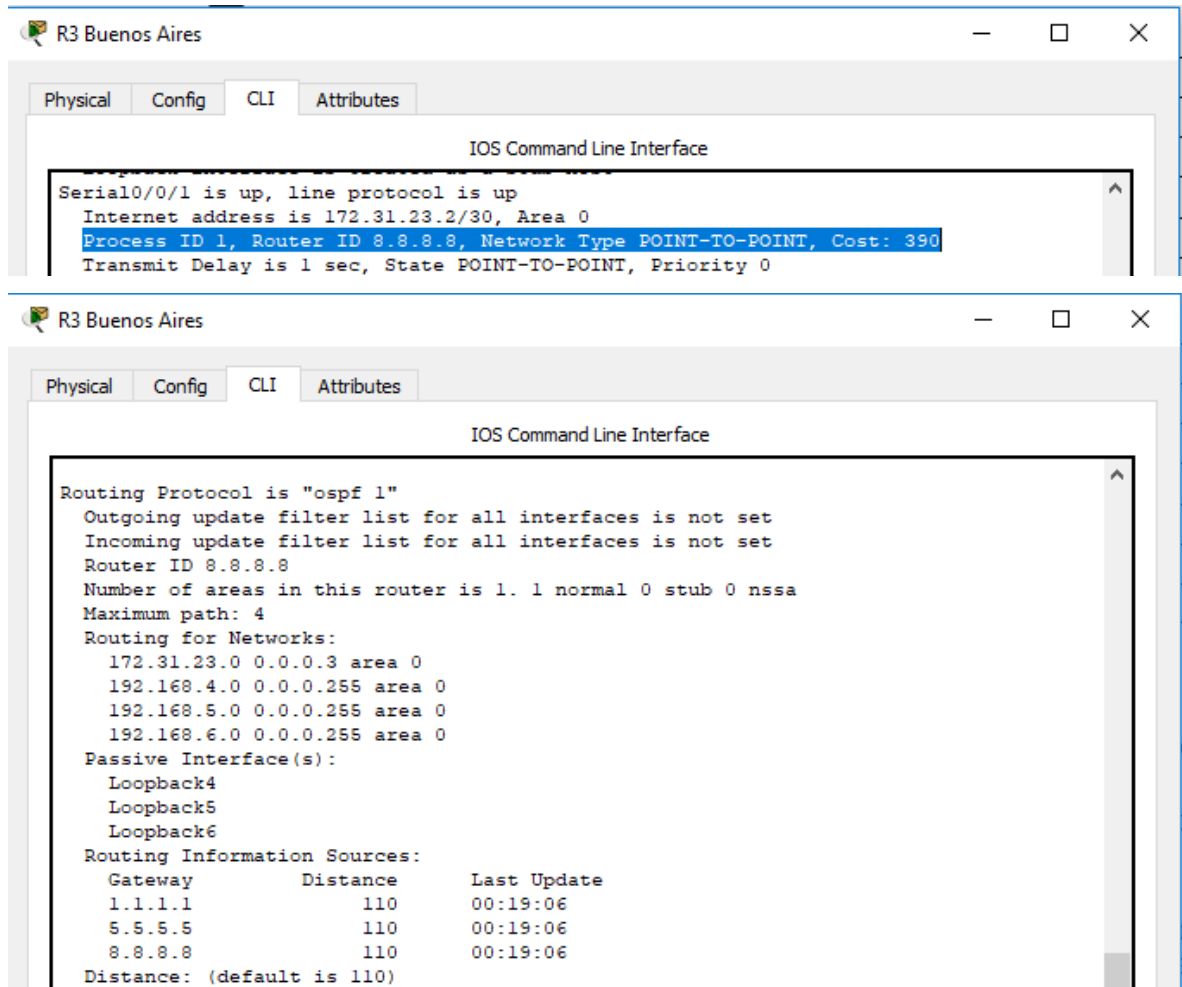
Por último, con el comando **show ip protocols**, podemos conocer cuales son las interfaces pasivas y la redes enrutadas,

Ilustración 106: Verificación en R2



Información obtenida con los comandos anteriormente explicados, para R2

Ilustración 117: Verificación en R3



Información obtenida con los comandos anteriormente explicados, para R3

3.4. Configuración switches

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

Para este punto, en el cual configuraremos los switches, debemos tener en cuenta que también se nos pide configurar la seguridad, lo primero es darle nombre al dispositivo, luego digitar las vlan, configurar los enlaces troncales, recordemos que, por defecto, el solo digitar en el enlace destinado por nosotros a ser troncal, en un switch 2960 el comando switchport mode trunk, automáticamente queda en vlan all,

es decir, pasando todas las vlan que se encuentran configuradas en él, así las cosas:

El script:

Para SW1

```
ena
conf ter
vlan 30
vlan 40
inter f0/3
switchport mode trunk
inter f0/24
switchport mode trunk
interface FastEthernet0/1
switchport access vlan 30
switchport mode access
exit
enable secret C0l0mb14
enable password C0l0mb14_1
line console 0
password C0l0mb14
login
line vty 0 4
password C0l0mb14
login
banner motd x Prohibido el Acceso no Autorizado! x
service password-encryption
end
copy running-config startup-config
```

Para SW3

```
ena
conf ter
```

```
vlan 40
inter f0/3
switchport mode trunk
interface FastEthernet0/1
switchport access vlan 40
switchport mode access
exit
enable secret C0l0mb14
enable password C0l0mb14_1
line console 0
password C0l0mb14
login
line vty 0 4
password C0l0mb14
login
banner motd x Prohibido el Acceso no Autorizado! x
service password-encryption
end
copy running-config startup-config
```

las configuraciones de seguridad es otro ítem muy importante, ya que la integridad de la red depende de ello, en ese orden de ideas, para el enable, podemos configurar un secret o un password, para la consola, es decir para out of band, configuramos igualmente, un password y por ultimo debemos digitar la palabra login, que nos habilita el uso del password, lo mismo hacemos para las conexiones virtuales, es decir, vty, por recomendación de seguridad, habilitamos 5, pero podemos habilitar hasta 16, donde 0 es el mínimo y 15 el máximo.

3.5. Deshabilitar DNS lookup

El comando no ip domain-lookup desactiva la traducción de nombres a dirección del dispositivo, ya sea éste un Router o Switch. Después de agregar esa instrucción, cualquier error de digitación en el dispositivo, simplemente enviará el mensaje indicando que el comando es desconocido o que no ha podido localizar el nombre de host, ahorrándonos segundos valiosos especialmente si estamos realizando un examen práctico.

En el Switch 3 deshabilitar DNS lookup

```
ena
conf ter
no ip domain-lookup
end
copy running-config startup-config
```

3.6. Asignación de direcciones IP a los switches

Asignar direcciones IP a los Switches acorde a los lineamientos.

Cuando tenemos una red que administrar, resulta muy práctico tener los switches gestionados a través de una red administrativa, acá se llama red de mantenimiento y como se manifestó anteriormente, se tomó la expresada en la tabla que presenta en el diagrama:

El script:

Para SW1:

```
ena
conf ter
vlan 200
inter vlan 200
ip addr 192.168.200.2 255.255.255.0
end
copy running-config startup-config
```

Para SW3:

```
ena
conf ter
vlan 200
inter vlan 200
ip addr 192.168.200.3 255.255.255.0
end
copy running-config startup-config
```

3.7. Desactivación Puertos

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

Las interfaces que no se usan, siempre deben quedar desactivadas, para evitar el inadecuado uso, por personal no calificado:

El script:

Para SW1:

```
ena
conf ter
inter range f0/2 , f0/4-23
shut
end
copy running-config startup-config
```

Para SW3:

```
ena
conf ter
inter range f0/2 , f0/4-24
shut
end
copy running-config startup-config
```

3.8. Implementación DHCP y NAT para IPv4

- 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.

Así como en el anterior escenario, debemos activar el NAT con sobrecarga, también llamado PAT, para que los terminales puedan salir a internet, en nuestro caso, poder comunicarse con el InternetPC, además, se nos pide que configuremos el DHCP para que tanto PC-A como PC-C obtengan su dirección de manera automática y así se puedan comunicar

Comenzaremos con la configuración de DHCP, para esto, excluirémos 30 direcciones IP para que no sean asignables dentro del pool, y las podamos usar en direccionamiento estático, nombramos los pools, ponemos la ruta por defecto, el dns y el dominio, esto aparecerá en las configuraciones de los pc de manera automática.

El script:

Configuración DHCP IPv4

```
ena
conf ter
ip dhcp excluded-address 192.168.30.2 192.168.30.32
ip dhcp excluded-address 192.168.40.2 192.168.40.32
ip dhcp pool ADMINISTRACION
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 10.10.10.11
ip dhcp pool MERCADEO
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1
dns-server 10.10.10.11
ip domain-name ccna-unad.com
end
copy running-config startup-config
```

3.9. Configuración NAT

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

La lista de acceso se configura primero, luego se ejecuta el comando de overload y por último las interfaces de entrada y de salida.

```
ena
conf ter
ip access-list standard INTERNET
permit 192.168.0.0 0.0.255.255
permit 172.31.0.0 0.0.255.255
ip nat inside source list INTERNET interface FastEthernet0/0 overload
inter f0/0
ip nat outside
inter s0/0/0
ip nat inside
inter s0/0/1
ip nat inside
end
copy running-config startup-config
```

Con lo anterior, ya tenemos salida a internet, lo cual se demostrará en las pruebas de conectividad más adelante.

3.10. Listas de Acceso

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

Las listas de acceso se hacen muy necesarias, a la hora de restringir el tráfico a determinados usuarios, o impedir ataques a la infraestructura, en la guía se nos piden 2 ACL estándar y extendida, las primeras solo tenemos que especificar una dirección de origen, en las últimas, debemos especificar origen y destino, a continuación, se expone el script necesario para realizar estas ACL:

El script:

```
ena
conf ter
ip access-list standard list_1
permit 192.168.30.0 0.0.0.255
deny 192.168.40.0 0.0.0.255
ip access-list standard list_2
deny 192.168.30.0 0.0.0.255
permit 192.168.40.0 0.0.0.255
ip access-list extended list_3
permit ip 192.168.30.0 0.0.0.255 host 209.165.200.230
deny ip 192.168.40.0 0.0.0.255 host 209.165.200.230
ip access-list extended list_4
permit ip 192.168.40.0 0.0.0.255 host 209.165.200.230
deny ip 192.168.30.0 0.0.0.255 host 209.165.200.230
end
copy running-config startup-config
```





Luego, debemos aplicar estas ACL en las interfaces de las cuales deseamos bloquear el tráfico.

El script:

```
ena
conf ter
inter f0/0.40
ip access-group list_1 in
end
copy running-config startup-config
```

si realizamos una prueba, encontraremos que hay comunicación permitida desde la red 192.168.30.0/24 pero no desde 192.168.40.0/24

verifiquemos:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-A	Internet PC	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC-C	Internet PC	ICMP		0.000	N	1	(edit)	(delete)





Efectivamente, el ping falló por haber aplicado esas reglas ACL.

Ahora hagámoslo con una extendida:

El script:

```
ena
conf ter
inter f0/0.40
ip access-group list_3 in
end
copy running-config startup-config
```

verifiquemos:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC-A	Internet PC	ICMP		0.000	N	0	(edit)	(delete)
	Failed	PC-C	Internet PC	ICMP		0.000	N	1	(edit)	(delete)

3.11. Verificación comunicación

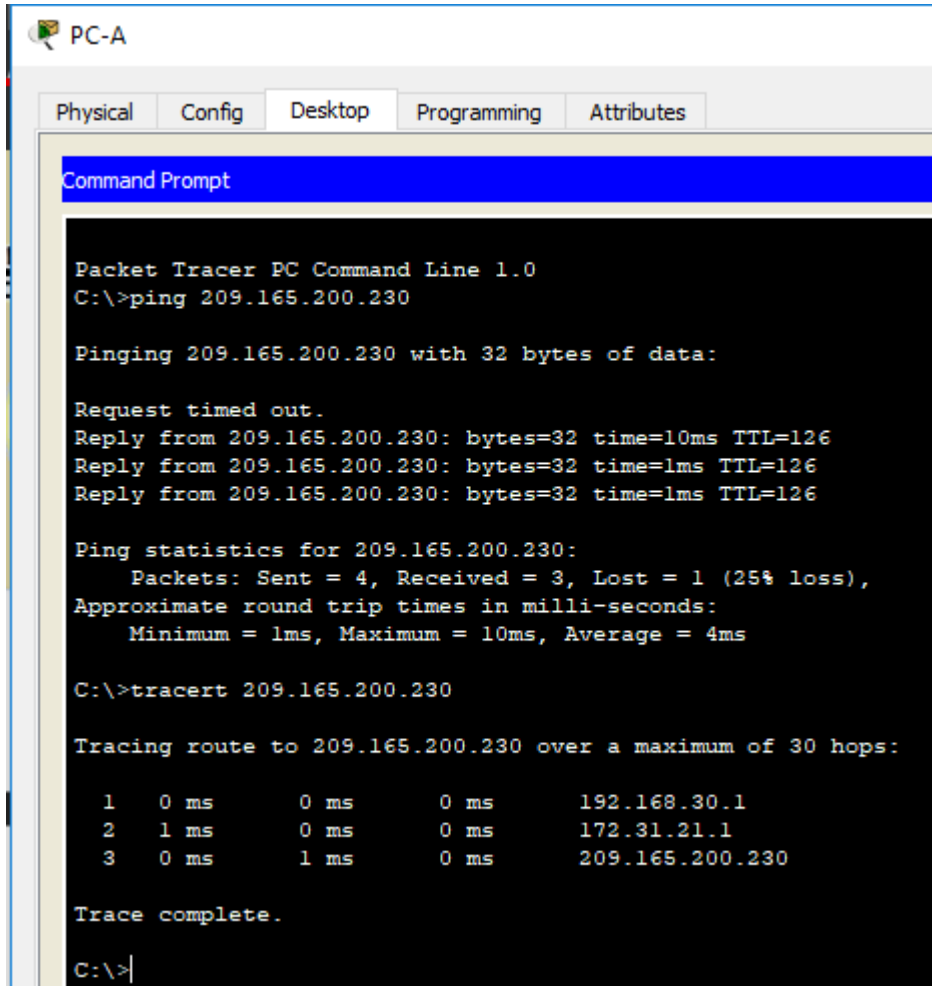
Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

Finalmente, realizamos verificaciones con el comando ping y tracert, con el primero, nos damos cuenta si alcanzamos al InternetPC y con el segundo, nos damos cuenta, cuales son los saltos que debe dar el paquete antes de llegar a destino, por ejemplo, si hacemos tracert desde PC-A hacia InternetPC, el cual tiene una dirección 209.165.200.230, el primero salto lo dará hacia su puerta de enlace 192.168.30.1, de ahí hacia la ruta indicada por OSPF, que nos indica que todas las solicitudes que se hagan a la red 209.165.200.224 se pueden hacer a 172.31.21.1 que se encuentra configurado en la interfaz s0/0/1 de R2.

Así las cosas:

Desde PC-A:

Ilustración 12: PC-A pruebas de conectividad



```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Request timed out.
Reply from 209.165.200.230: bytes=32 time=10ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 4ms

C:\>tracert 209.165.200.230

Tracing route to 209.165.200.230 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    192.168.30.1
  1  1 ms    0 ms    0 ms    172.31.21.1
  2  0 ms    1 ms    0 ms    209.165.200.230

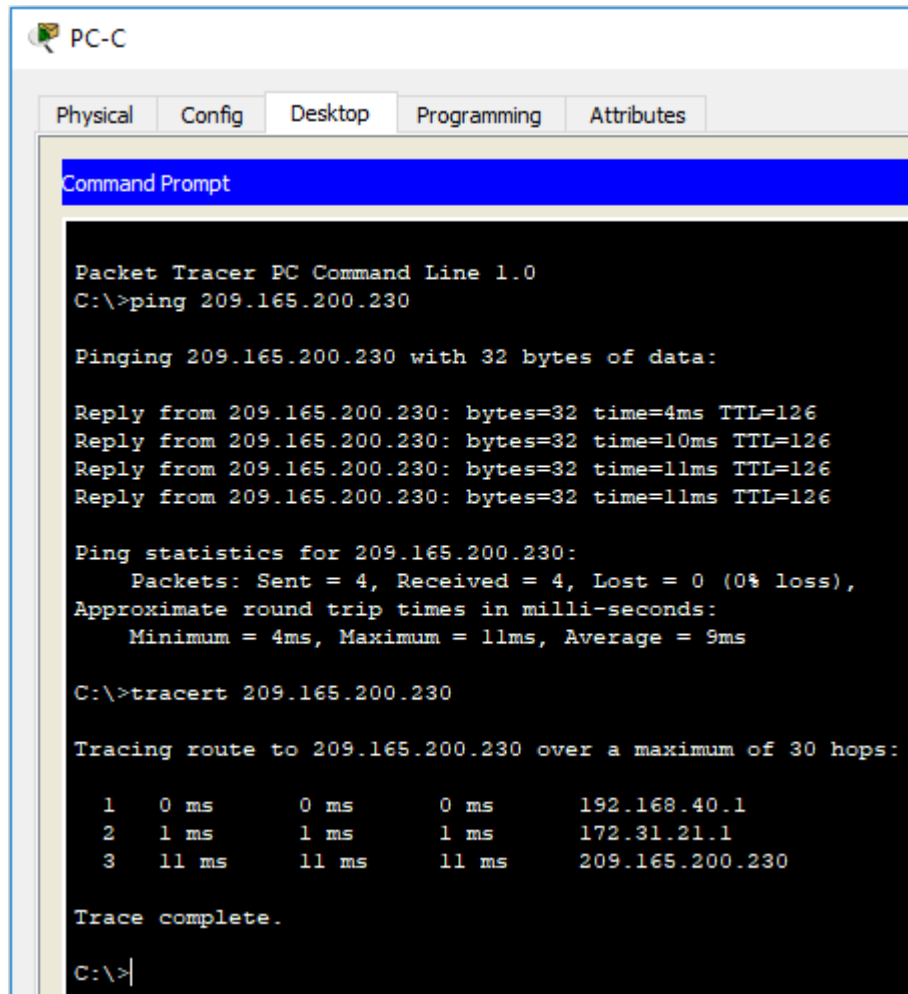
Trace complete.

C:\>
```

Como lo podemos apreciar, se alcanzó el destino en el tercer salto, es decir, del pc, saltó a R1 de ahí a R2y finalmente llegó al host llamado InternetPC

Desde PC-B:

Ilustración 13: PC-C pruebas de conectividad



The screenshot shows a Packet Tracer PC Command Line window for PC-C. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, displaying a Command Prompt. The Command Prompt shows the following output:

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Reply from 209.165.200.230: bytes=32 time=4ms TTL=126
Reply from 209.165.200.230: bytes=32 time=10ms TTL=126
Reply from 209.165.200.230: bytes=32 time=11ms TTL=126
Reply from 209.165.200.230: bytes=32 time=11ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 11ms, Average = 9ms

C:\>tracert 209.165.200.230

Tracing route to 209.165.200.230 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    192.168.40.1
  1  1 ms    1 ms    1 ms    172.31.21.1
  2  11 ms   11 ms   11 ms   209.165.200.230

Trace complete.

C:\>
```

En esta prueba, nos pasa lo mismo, alcanzamos el InternetPC en el tercer salto.

Conclusiones

- Esta práctica ha servido para poder afianzar los conocimientos adquiridos a lo largo del curso, temas como enrutamiento, troncalización, configuración de vlan, son temas que se usan en el día a día del ingeniero de telecomunicaciones sistemas o electrónico.
- La mínima configuración básica del switch debe incluir desde el nombre del dispositivo, es decir el nombre con el cuál se va a referir en la configuración, la forma detallada de la estructura de interfaces que lo componen, la asignación de contraseñas, el mensaje de alerta (MOTD), la tabla de direccionamiento en donde se señala la asignación de las IP, las direcciones MAC, dinámicas o estática y administración remota del switch.

Bibliografía

- CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>. (s.f.).
- CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>. (s.f.).
- CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>. (s.f.).
- CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>. (s.f.).