EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

RONALD STEVEN TIQUE RANGEL

Diplomado CCNA
opción de grado

Instructor: Efraín Alejandro Pérez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA
INGENIERIA DE TELECOMUNICACIONES
BOGOTA D.C.
2019

Contenido

Introducción 3
1. Escenario 1 4
2. Desarrollo de las actividades Escenario 1 6
2.1. Configuración puertos y VLAN's 6
2.2. Direccionamiento IP para los router ISP, R1, R2 y R3 7
2.3. Configuración de DHCP en host 9
2.4. Configuración de NAT o PAT 13
2.5. Configuración de la ruta estática 14
2.6. Configuración del servicio DHCP en R2 15
2.7. Pruebas de conectividad al Servidor0 15
2.8. Configuración doble stack 19
2.9. Configuración doble stack en FastEthernet 0/0 de R3 21
2.10. Configuración RIPv2 en R1, R2 Y R3 22
2.11. Verificación tabla de enrutamiento R1, R2 y R3 23
2.12. Pruebas de conectividad entre terminales 27
3. Escenario 2 30
3.1. Direccionamiento IP según esquema del escenario 31
3.2. Configuración OSPFv2 34
3.3. Verificación de la información OSPF 36
3.4. Configuración switches 42
3.5. Deshabilitar del DNS lookup 43
3.6. Configuración de direcciones IP a los switches 44
3.7. Desactivación Puertos 45
3.8. Implementación DHCP y NAT para IPv4 45
3.9. Configuración Network Address Translation o NAT 46
3.10. Listas de Acceso estándar y extendidas 47
3.11. Verificación de la comunicación 48
CONCLUSIONES 50
BIBLIOGRAFÍA 51

Introducción

El mundo de las telecomunicaciones es un mundo apasionante, teniendo en cuenta el valor que tiene hoy en día para el ser humano, nuestra supervivencia, depende en gran medida de ellos, cada día se crean más y mejores redes, que se van añadiendo a las ya existentes o las reemplazan, diferentes compañías dedicadas a esta labor ofrecen soluciones sobre lo ya inventado o diseñan tecnologías propietarias, que a la larga, podría ser lo mismo que lo ya existente, solo que con algunas mejoras.

Con el desarrollo de las habilidades prácticas del diplomado de profundización, se ha querido dar un repaso con las tecnologías más relevantes para la industria del IT, pues masivamente, es lo que se utiliza en cada hogar, empresa, persona, por ejemplo, en cualquier vivienda que usen internet, ya sea para ver Netflix, descargar música, hacer la tarea del colegio, se necesita que el computador alcance internet y eso se hace posible gracias a varias tecnología, como por ejemplo, el NAT, para poder tener una dirección, la cual sale con un número de puerto, por lo tanto se le llama PAT en algunos casos, también usaremos OSFP y RIP protocolos de enrutamiento dinámico que nos hacen el trabajo administrativo de configuración de rutas mucho más fácil.

Finalmente, el trabajo expuesto es la consumación de lo que aprendimos en el curso de profundización CCNA, que aun que, a lo largo de la carrera, aprendimos variada información, Este diplomado nos mete a la esencia misma de las telecomunicaciones.

1. Escenario 1

El escenario 1 nos propone una topología de 3 routers con conexiones redundantes y un router adicional que nos da salida al ISP, mediante el uso de enrutamiento RIPv2, NAT o mejor PAT, también usaremos DHCP para obtener las direcciones que requieren los terminales, a continuación, la imagen del primer escenario:

Ilustración 1: Escenario 1

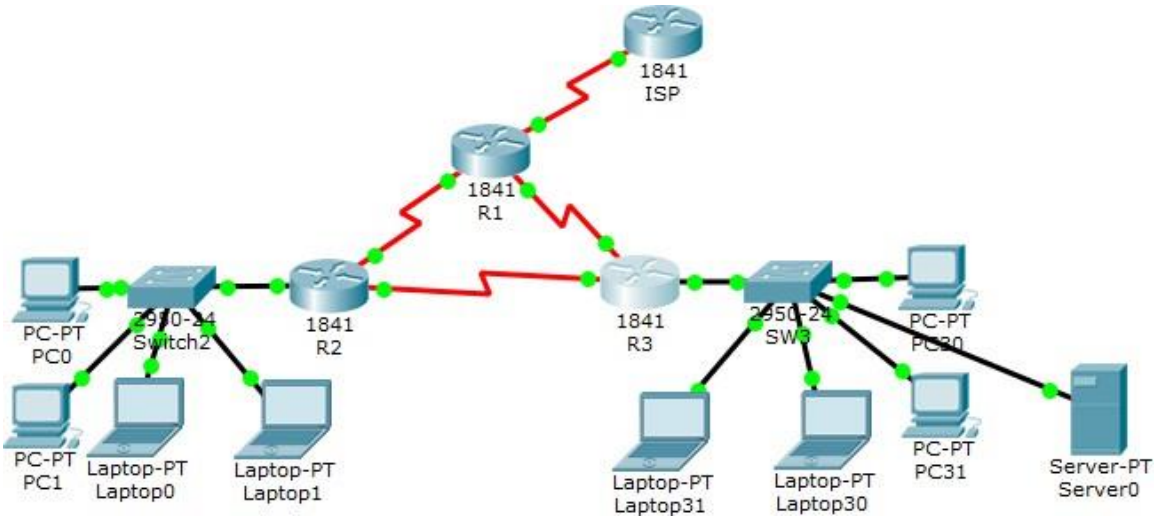


Tabla 1: Tabla de direccionamiento

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
ISP	S0/0/0	200.123.211.1	255.255.255.0	N/D
R1	Se0/0/0	200.123.211.2	255.255.255.0	N/D
	Se0/1/0	10.0.0.1	255.255.255.252	N/D
	Se0/1/1	10.0.0.5	255.255.255.252	N/D
R2	Fa0/0,100	192.168.20.1	255.255.255.0	N/D
	Fa0/0,200	192.168.21.1	255.255.255.0	N/D
	Se0/0/0	10.0.0.2	255.255.255.252	N/D
	Se0/0/1	10.0.0.9	255.255.255.252	N/D
R3	Fa0/0	192.168.30.1	255.255.255.0	N/D
		2001:db8:130::9C0:80F:301	/64	N/D
	Se0/0/0	10.0.0.6	255.255.255.252	N/D
	Se0/0/1	10.0.0.10	255.255.255.252	N/D
SW2	VLAN 100	N/D	N/D	N/D
	VLAN 200	N/D	N/D	N/D
SW3	VLAN1	N/D	N/D	N/D

Continuación Tabla 1

PC20	NIC	DHCP	DHCP	DHCP
PC21	NIC	DHCP	DHCP	DHCP
PC30	NIC	DHCP	DHCP	DHCP
PC31	NIC	DHCP	DHCP	DHCP
Laptop20	NIC	DHCP	DHCP	DHCP
Laptop21	NIC	DHCP	DHCP	DHCP
Laptop30	NIC	DHCP	DHCP	DHCP
Laptop31	NIC	DHCP	DHCP	DHCP

Tabla 2: asignación de puertos a VLAN

Dispositivo	VLAN	Nombre	Interfaz
SW2	100	LAPTOPS	Fa0/2-3
SW2	200	DESTOPS	Fa0/4-5
SW3	1	-	Todas las interfaces

Las tablas anteriores, nos muestran el direccionamiento que llevan los elementos que conforman la red, la segunda, la VLAN a la que pertenecerán luego de las configuraciones respectivas

Situación

En esta actividad, demostrará y reforzará su capacidad para implementar NAT, servidor de DHCP, RIPV2 y el routing entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces. Todas las pruebas de alcance deben realizarse a través de ping únicamente.

Para su solución debemos crear la topología en el simulador, tal como aparece en la ilustración 1, posteriormente, configuramos el direccionamiento propuesto en sus interfaces, las que no usemos las apagamos, los switches tienen por defecto encendidas las interfaces, los routers por el contrario, las traen apagadas, así que cuando estemos configurando no debemos olvidar encenderlas o de lo contrario no funcionará la implementación, seguimos con el ruteo, la configuración DHCP y el NAT, por último realizaremos las pruebas de rigor.

2. Desarrollo de las actividades Escenario 1

2.1. Configuración puertos y VLAN's

SW2 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1:

Los puertos de red que no se utilizan se deben deshabilitar.

En esta parte, luego de montar la topología, escribimos la configuración según lo requiera cada elemento, no olvidemos apagar las interfaces no utilizadas y grabar la información, usaremos el comando write.

El script requerido, lo escribimos a continuación:

```
enable
configure terminal
hostname SW2
interface fast0/1
switchport mode trunk
vlan 100
vlan 200
interface fast0/2
switchport access vlan 100
switchport mode access
interface fast0/3
switchport access vlan 100
switchport mode access
interface fast0/4
switchport access vlan 200
switchport mode access
interface fast0/5
switchport access vlan 200
switchport mode access
interface range f0/6-24
shutdown
end
write
```

2.2. Direccionamiento IP para los router ISP, R1, R2 y R3

La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.

Empezamos configurando la dirección ip del router que nos sirve de ISP eso significa (Internet Service Provider) no olvidamos levantar la interfaz y guardamos, esto mismo hacemos para R1, R2 y R3 siguiendo la tabla 1.

Utilizaremos el siguiente es el script:

Para ISP

```
enable
configure terminal
hostname ISP
interface serial0/0/0
ip address 200.123.211.1 255.255.255.0
end
write
```

Para R1:

```
enable
configure terminal
host R1
inter s0/0/0
ip address 200.123.211.2 255.255.255.0
no shutdown
inter s0/1/0
ip address 10.0.0.1 255.255.255.252
no shutdown
inter s0/1/1
ip address 10.0.0.5 255.255.255.252
no shutdown
end
write
```

Para R2:

```
enable
configure terminal
host R2
interface fast0/0
no shutdown
interface fast0/0.100
encapsulation dot1Q 100
ip address 192.168.20.1 255.255.255.0
interface fast0/0.200
encapsulation dot1Q 200
ip address 192.168.21.1 255.255.255.0
inter serial0/0/0
ip address 10.0.0.2 255.255.255.252
no shutdown
inter serial0/0/1
ip address 10.0.0.9 255.255.255.252
no shutdown
end
write
```

Para R3:

```
enable
configure terminal
host R3
interface fast0/0
ip address 192.168.30.1 255.255.255.0
ipv6 address 2001:DB8:130::9C0:80F:301/64
ipv6 enable
no shutdown
interface serial0/0/0
```

ip address 10.0.0.6 255.255.255.252

inter s0/0/1

ip address 10.0.0.10 255.255.255.252

no shutdown

end

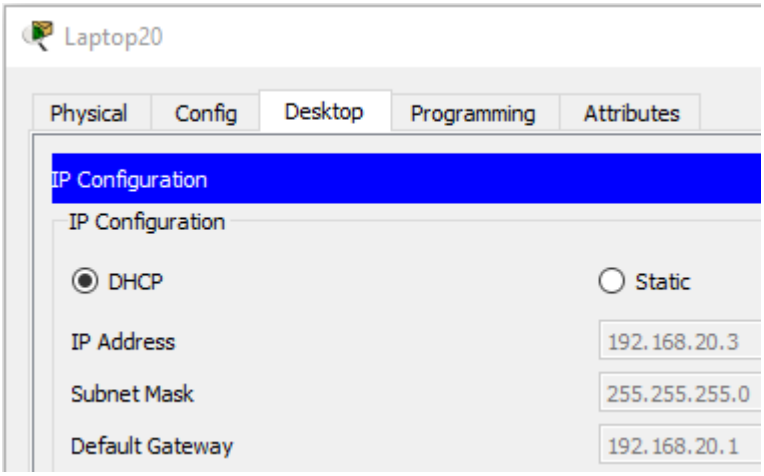
write

2.3. Configuración de DHCP en host

Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP.

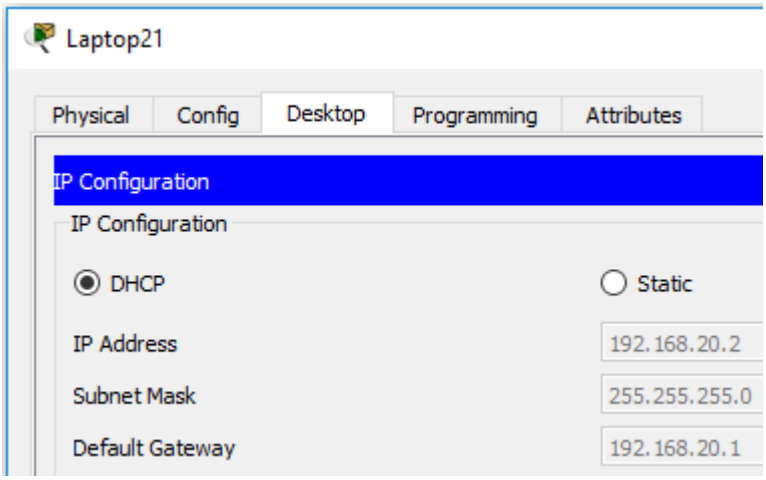
El siguiente paso, sería configurar el servicio de DCHP en los terminales, eso lo logramos, haciendo click en el PC o Laptop a configurar, luego pasamos a la pestaña Desktop y hacemos click en IP Configuration, seleccionamos DHCP y eso es todo.

Ilustración 2: Laptop20



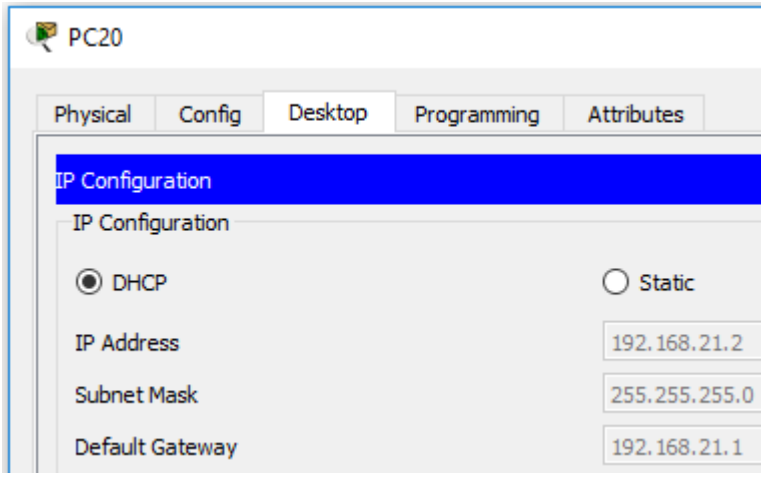
Podemos observar en la ilustración que a la Laptop20 se le seleccionó la opción DHCP y le dio una dirección 192.168.20.3/24 y gateway 192.168.20.1 ya que el servicio se encuentra activo en el router al cual se encuentra conectado.

Ilustración 3: Laptop21



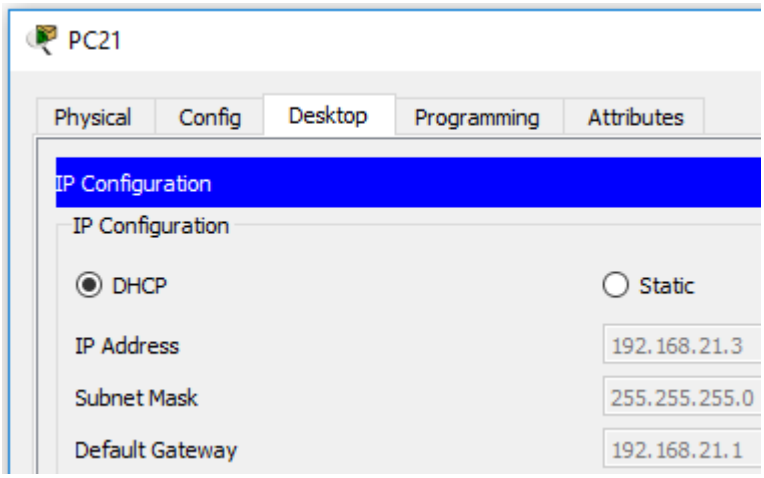
Pasa lo mismo con Laptop21 se le seleccionó DHCP y la dirección obtenida es 192.168.20.2/24 y gateway 192.168.20.1

Ilustración 4: PC20



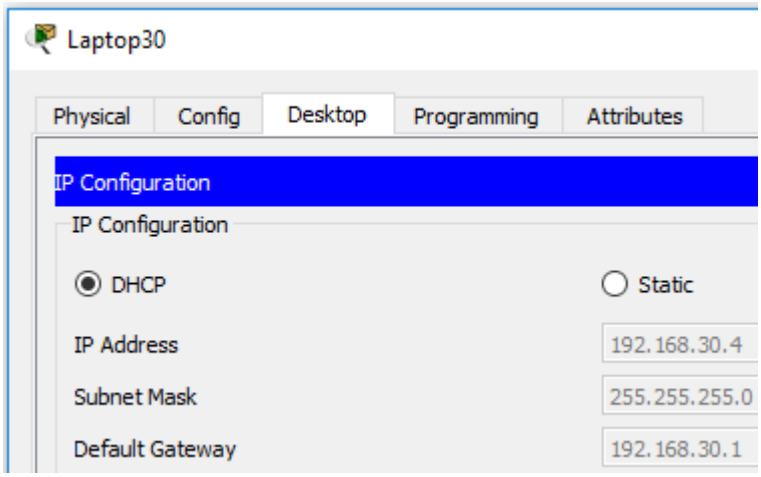
Posteriormente en la PC20 se realizó la misma operación y el resultado es: 192.168.21.2/24 con gateway 192.168.21.1

Ilustración 5: PC21



Así se hizo con todos los terminales de esta red, como se puede observar, todos obtuvieron dirección IP:

Ilustración 6: Laptop30



Estos equipos que siguen, pertenecen a la red que está conectada al router 3

Ilustración 7: Laptop31

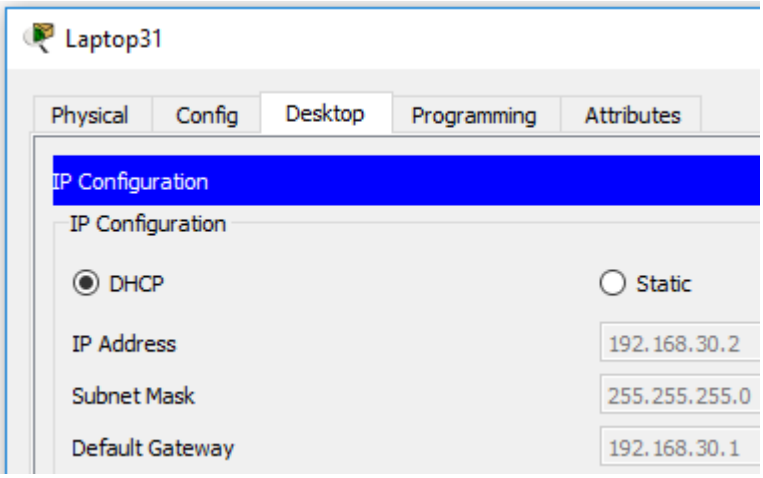
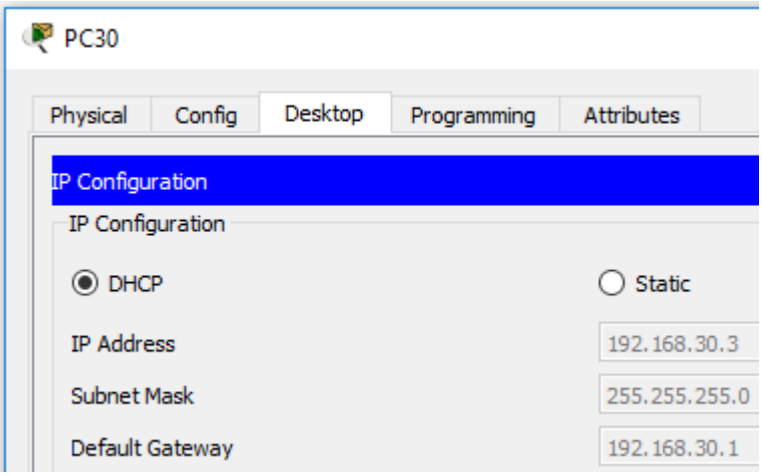
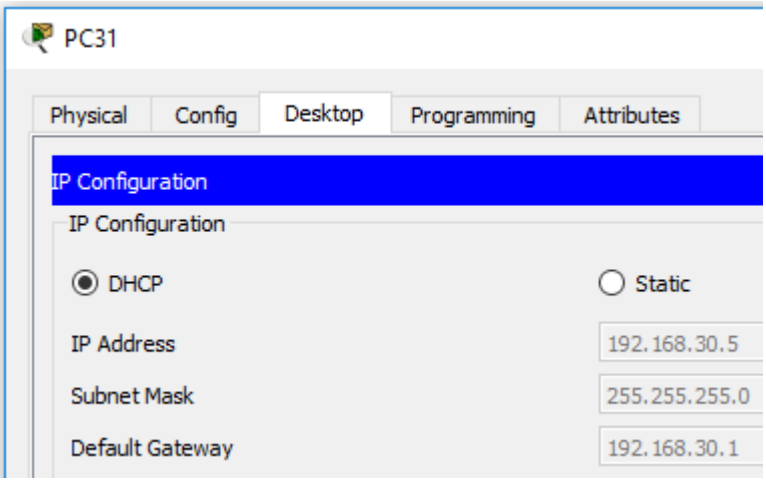


Ilustración 8: PC30



Si no se configura el servicio de DHCP previamente, nuestros terminales hubieran obtenido una dirección IP que comienza en su primer octeto con 169, señal de que no hay servicio, si queremos interconectar los terminales, debemos configurar direcciones estáticas.

Ilustración 9: PC31



Respuesta de DHCP satisfactoria en PC31

2.4. Configuración de NAT o PAT

R1 debe realizar una NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se **llama INSIDE-DEVS**.

El NAT hace posible que se traduzcan direcciones IP en otras para alcanzar ciertos destinos, como es el caso del PAT o NAT con sobrecarga para ello, debemos crear una ACL con las redes o hosts que se les permitirá salida hacia ISP, a continuación, el cli para esa configuración:

enable

configure terminal

ip access-list standard INSIDE-DEVS

permit 192.168.0.0 0.0.255.255

ip nat inside source list INSIDE-DEVS inter s0/0/0 overload

interface serial0/0/0

ip nat outside

interface serial0/1/0

ip nat inside

inter s0/1/1

ip nat inside

end

write

Ahora hacemos las pruebas:

Ilustración 10: ping a ISP

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC20	ISP	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC21	ISP	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Laptop20	ISP	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Laptop21	ISP	ICMP		0.000	N	3	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Laptop31	ISP	ICMP		0.000	N	4	(edit)	(delete)
	Successful	Laptop30	ISP	ICMP		0.000	N	5	(edit)	(delete)
	Successful	PC30	ISP	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC31	ISP	ICMP		0.000	N	7	(edit)	(delete)

Observamos que las pruebas de conectividad con ICMP son satisfactorias

2.5. Configuración de la ruta estática

R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en **el dominio** RIPv2.

Hacemos la configuración estática de la ruta predeterminada, es decir los paquetes que no encuentren el destino dentro de la implementación que estamos haciendo, buscarán salida por s0/0/0:

La configuración:

enable

configure terminal

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

end

write

2.6. Configuración del servicio DHCP en R2

R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.

Ahora configuramos los pools de DHCP según la tabla, para que den direccionamiento a los terminales conectados al router 2 en vlan 100 y en la 200:

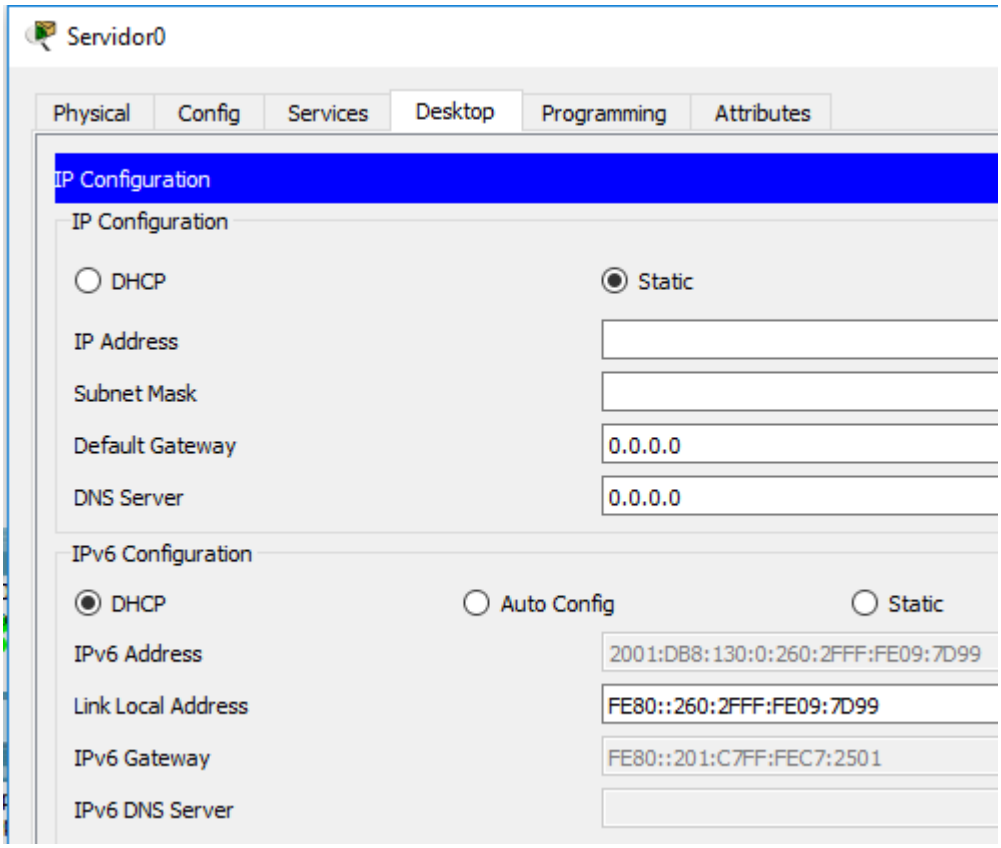
```
enable
configure terminal
ip dhcp pool vlan_100
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
ip dhcp pool vlan_200
network 192.168.21.0 255.255.255.0
default-router 192.168.21.1
end
write
```

2.7. Pruebas de conectividad al Servidor0

El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).

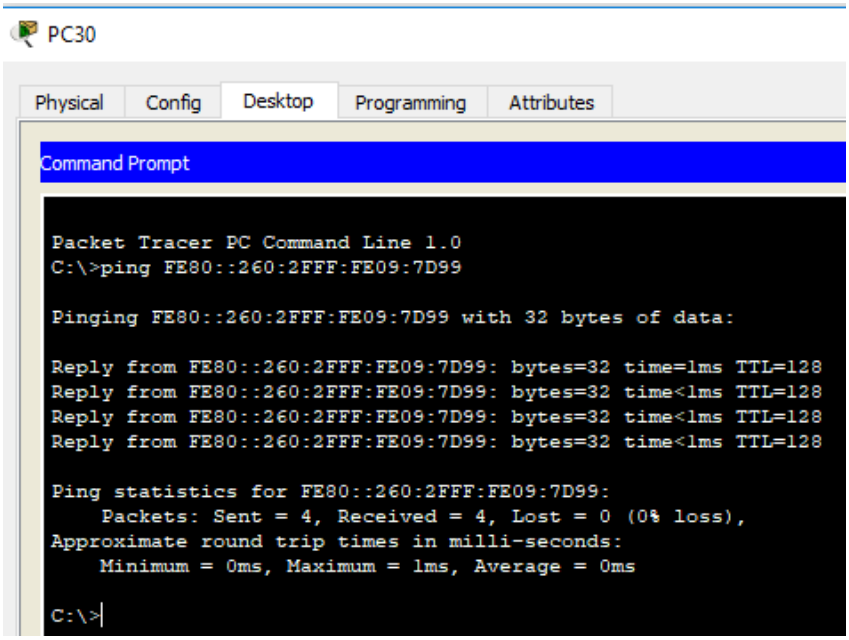
Ahora realizamos pruebas de conectividad en IPv6 no sin antes configurar esto según lo explicamos anteriormente para tomar direccionamiento por DHCP, en el Servidor0:

Ilustración 11: Dirección IPv6 Servidor0 tomada por DHCPv6



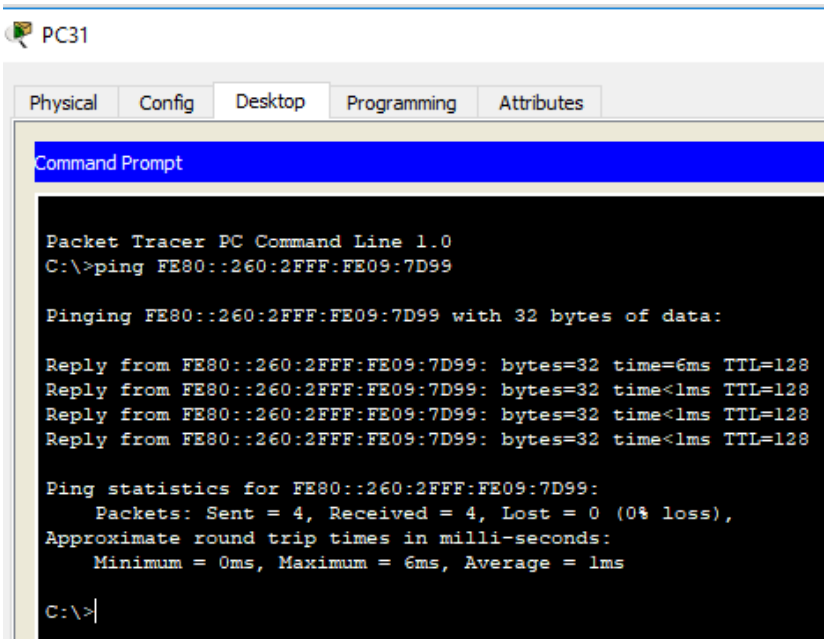
Observamos en la ilustración que hemos cambiado la configuración estática a la configuración por DHCP en versión IPv6, ya que el router se encuentra en doble stack, explicaremos esto adelante, ahora realizaremos las pruebas de conectividad en IPv6:

Ilustración 12: ping IPv6 de PC30 a Servidor0



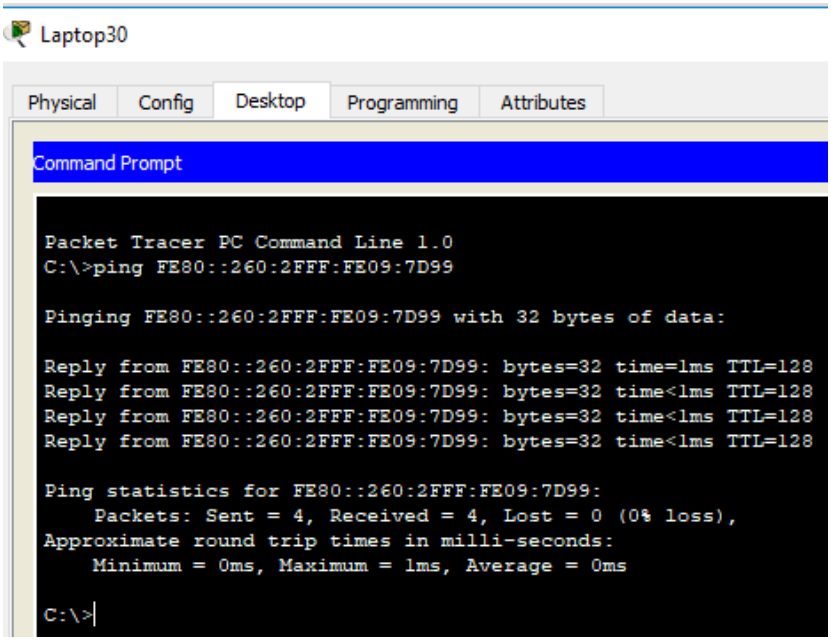
Realizaremos las pruebas en orden, primero desde PC30 hacia él servidor.

Ilustración 13: ping IPv6 de PC31 a Servidor0



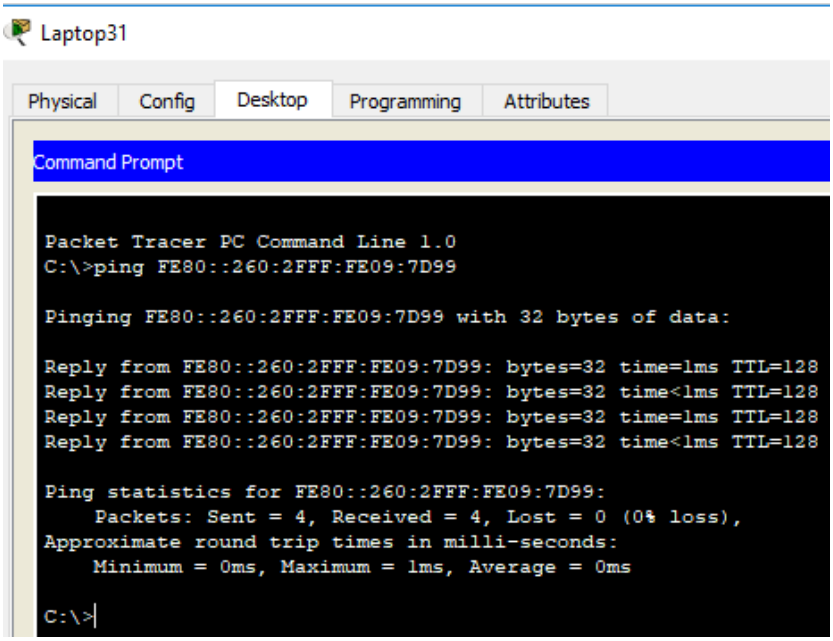
Ahora desde PC31 se hace lo mismo, la prueba es satisfactoria.

Ilustración 14: ping IPv6 de Laptop30 a Servidor0



Todos los terminales tienen conectividad por IPv6 según se observa

Ilustración 15: ping IPv6 de Laptop31 a Servidor0



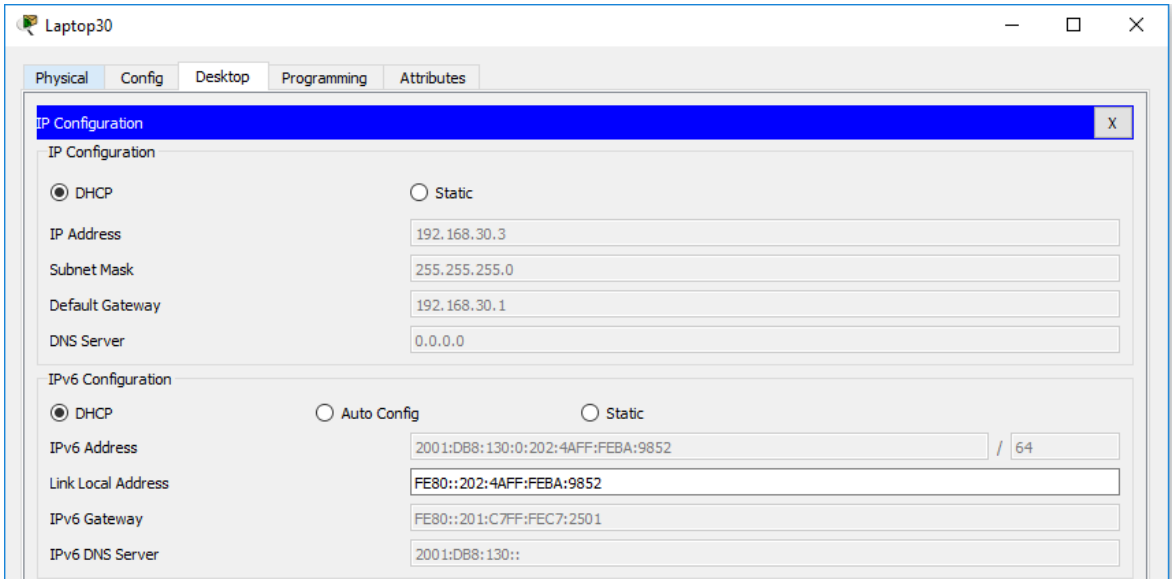
Se comprueba que la configuración DHCPv6 es correcta.

2.8. Configuración doble stack

La NIC instalado en direcciones IPv4 e IPv6 de Laptop30, de Laptop31, de PC30 y obligación de configurados PC31 simultáneas (dual-stack). Las direcciones se deben configurar mediante DHCP y DHCPv6.

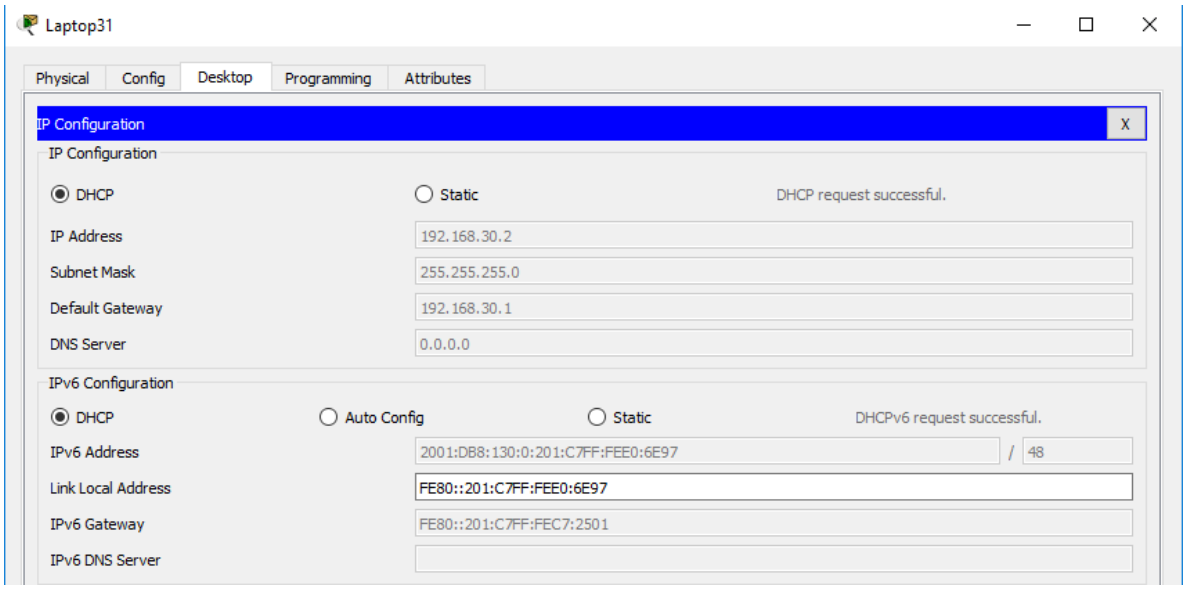
Ya habíamos explicado la configuración DHCP en las dos versiones, y acá la volvemos a explicar, solo, nos vamos al equipo que deseamos dejar configurado para las dos pilas, luego la pestaña Desktop y por último seleccionamos DHCP, y así queda en doble stack

Ilustración 16: dual-stack Laptop30



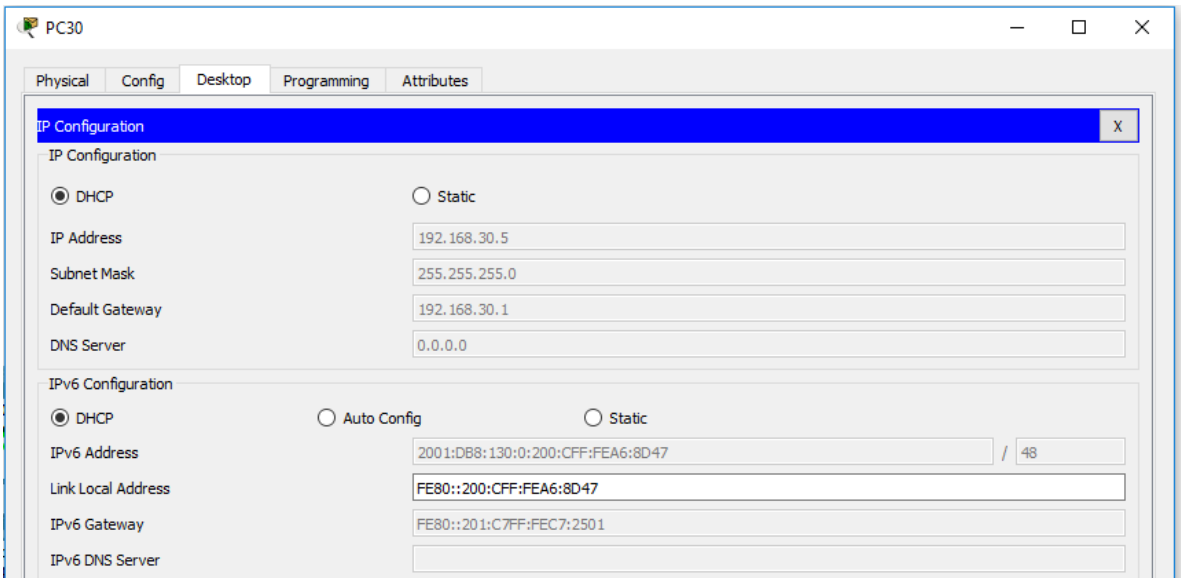
Se observa como ambos tipos de IP tomaron direccionamiento con la numeración correspondiente, decimal para IPv4 y hexadecimal para IPv6.

Ilustración 17: dual-stack Laptop31



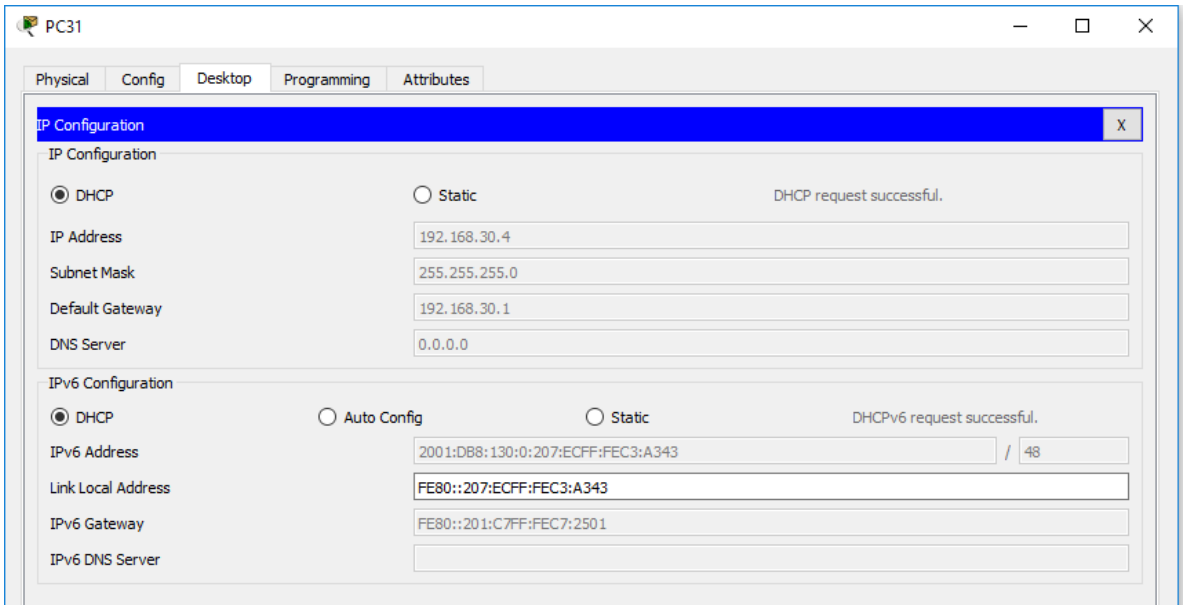
Vamos a cada uno de los terminales conectados a router 5, acá observamos que la respuesta del servidor DHCP fue satisfactoria.

Ilustración 18: dual-stack PC30



Hacemos lo mismo en cada terminal, seguimos entonces el mismo procedimiento que en el resto de equipos.

Ilustración 19: dual-stack PC31



Observamos que ya terminamos lo que sería la configuración a doble stack en la parte cliente.

2.9. Configuración doble stack en FastEthernet 0/0 de R3

La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).

Seguidamente configuramos el router para que nos funcione el doble stack, para ello, lo principal es entrar a la interfaz involucrada y habilitar el unicast-routing en IPv6, crear el pool, darle la dirección IPv6 que deseemos ponerle, en este caso, la que tenemos en la tabla 1 para ello. Finalmente, habilitamos en la interfaz el IPv6 y declaramos el pool DHCP creado, El cli necesario:

enable

ipv6 unicast-routing

ipv6 dhcp pool dhcpv6

prefix-delegation pool dhcpv6-pool1 lifetime 1800 600

exit

ipv6 local pool dhcpv6-pool1 2001:DB8:130::9C0:80F:301/40 48

inter f0/0

ip addr 192.168.30.1 255.255.255.0

ipv6 address 2001:DB8:130::9C0:80F:301/64

ipv6 enable

ipv6 dhcp server dhcpv6

end

write

2.10. Configuración RIPv2 en R1, R2 Y R3

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

Para que todas las redes se vean, así como en lo solicitado, implementamos el RIPv2, declaramos las redes que el router tiene conectados directamente y guardamos:

El Script necesario:

Para R1:

enable

configure terminal

router rip

version 2

network 10.0.0.0

network 200.123.211.0

end

write

Para R2:

enable

configure terminal

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

write

Para R3:

enable

configure terminal

router rip

version 2

network 10.0.0.0

network 192.168.30.0

network 200.123.211.0

end

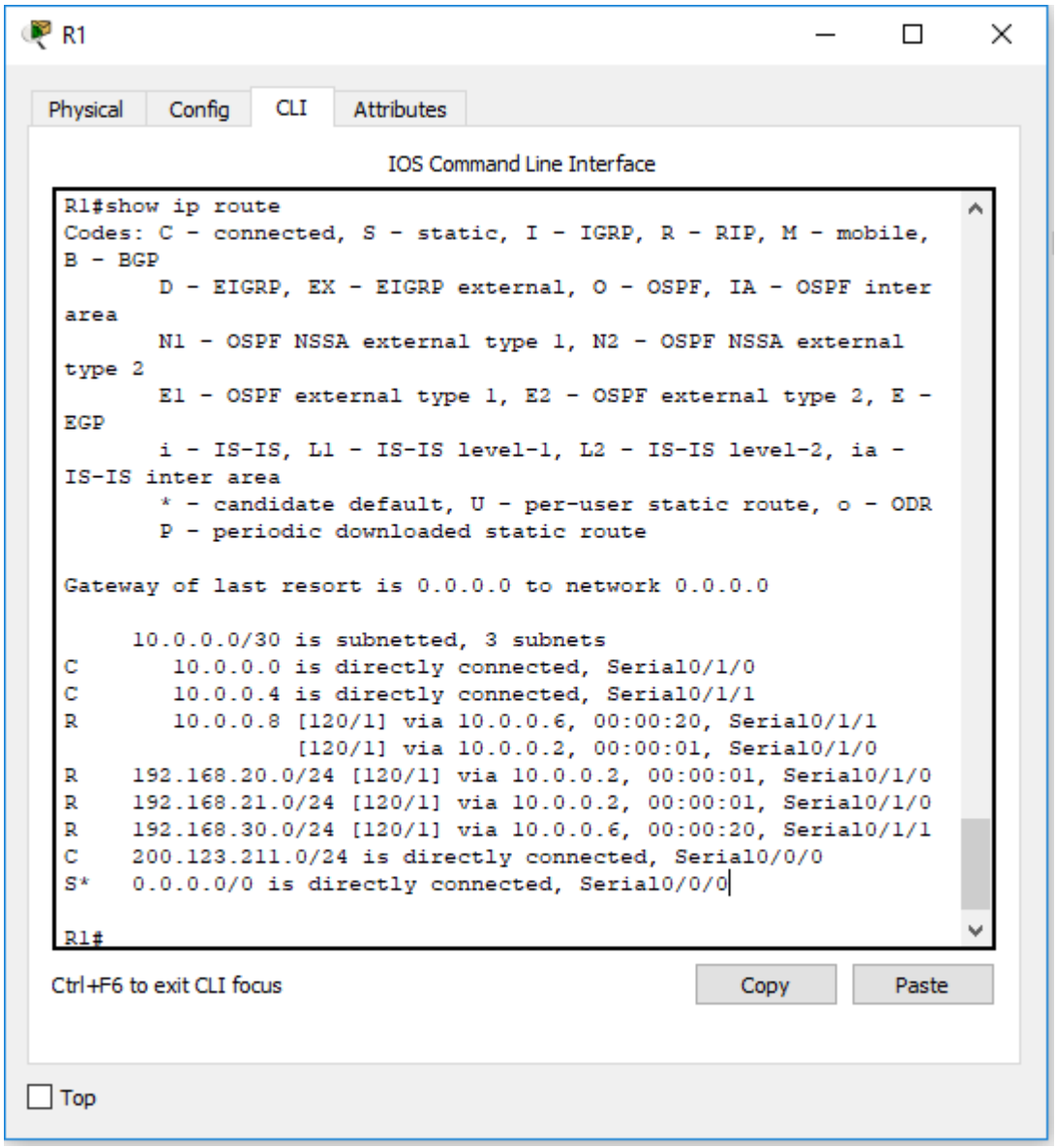
write

2.11. Verificación 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.

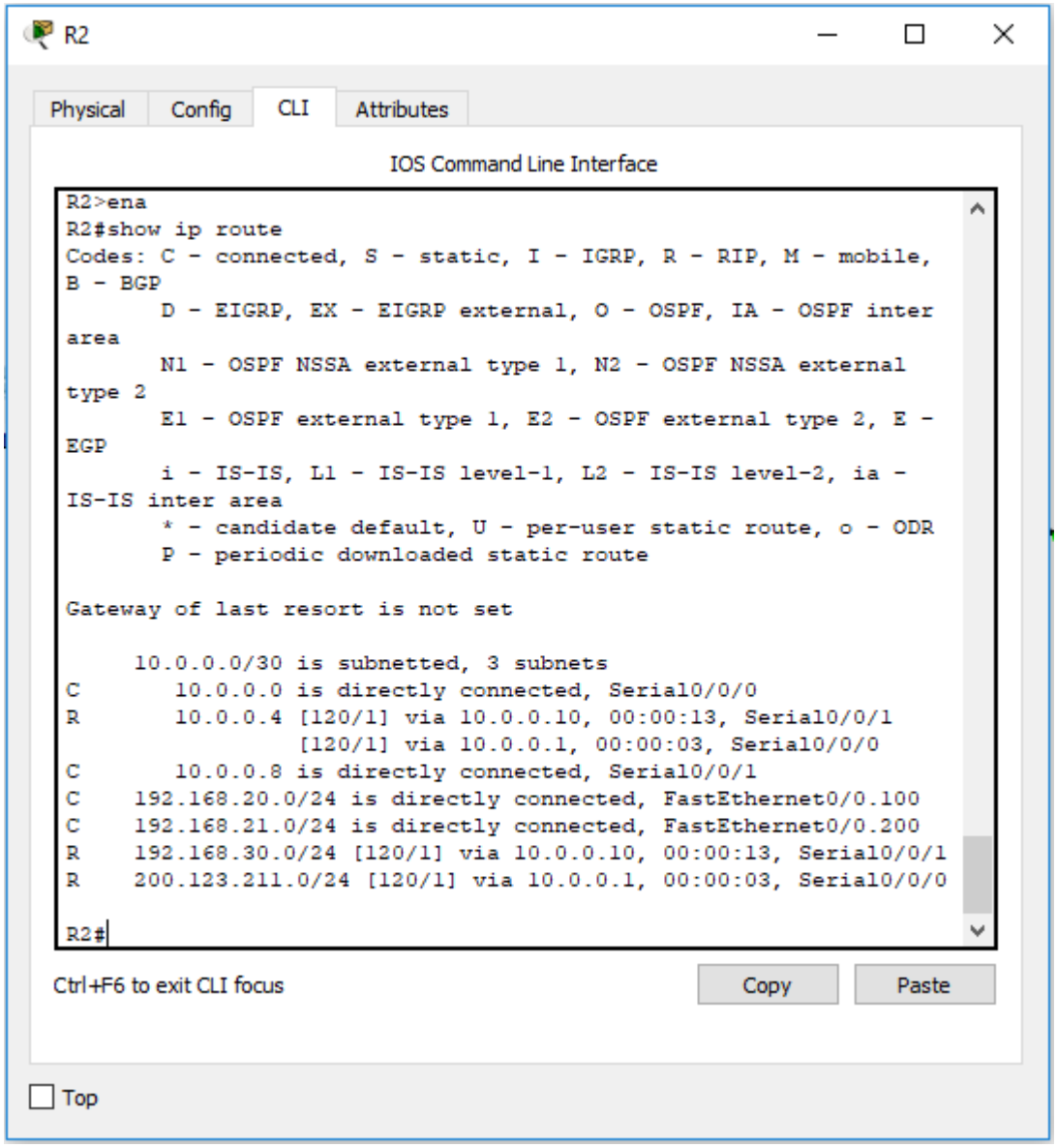
Habiendo hecho la configuración, ya podemos consultar las tablas de enrutamiento en cada uno de los router, eso lo hacemos mediante el comando show ip route, debemos además conocer que significa cada letra que encabeza la ruta, ya que así sabemos como la obtuvo, y la precede una O es de OSPF si la precede R se obtuvo por RIP si la precede C está directamente conectada, si S es una ruta estática.

Ilustración 20: Tabla de enrutamiento R1



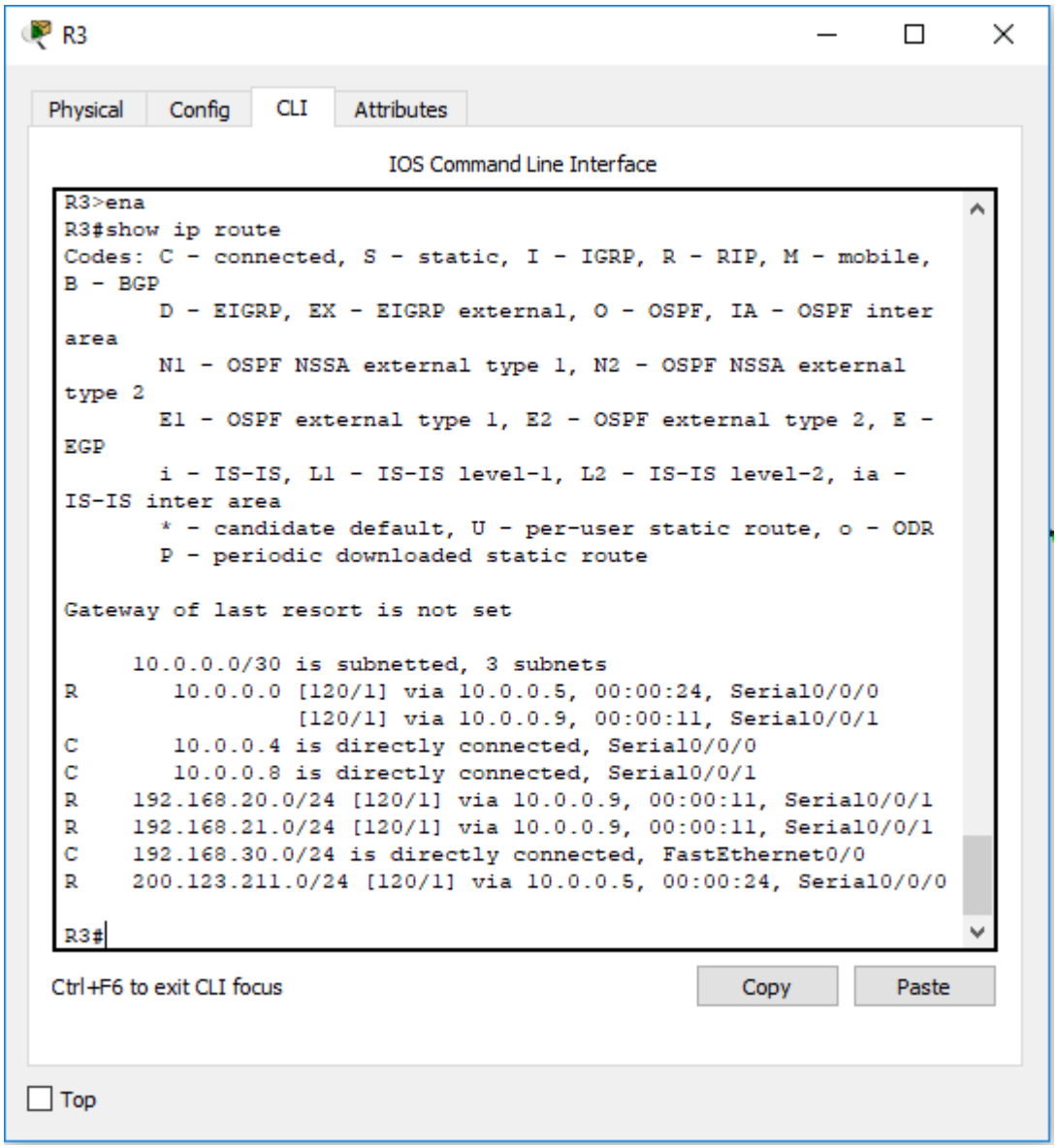
La ilustración nos enseña lo descrito anteriormente, y podemos ver, primero, que la tabla nos muestra 3 subredes sumarizadas en 10.0.0.0/30, 3 conectadas directamente, 4 obtenidas por RIP y hay una estática que además es nuestra salida por defecto, es lo que está configurado en R1.

Ilustración 21: Tabla de enrutamiento R2



En R2 visualizamos que son 4 las rutas directamente conectadas y 3 las obtenidas por RIP, además la ruta por defecto para salir a ISP es s0/0/0

Ilustración 22: Tabla de enrutamiento R3



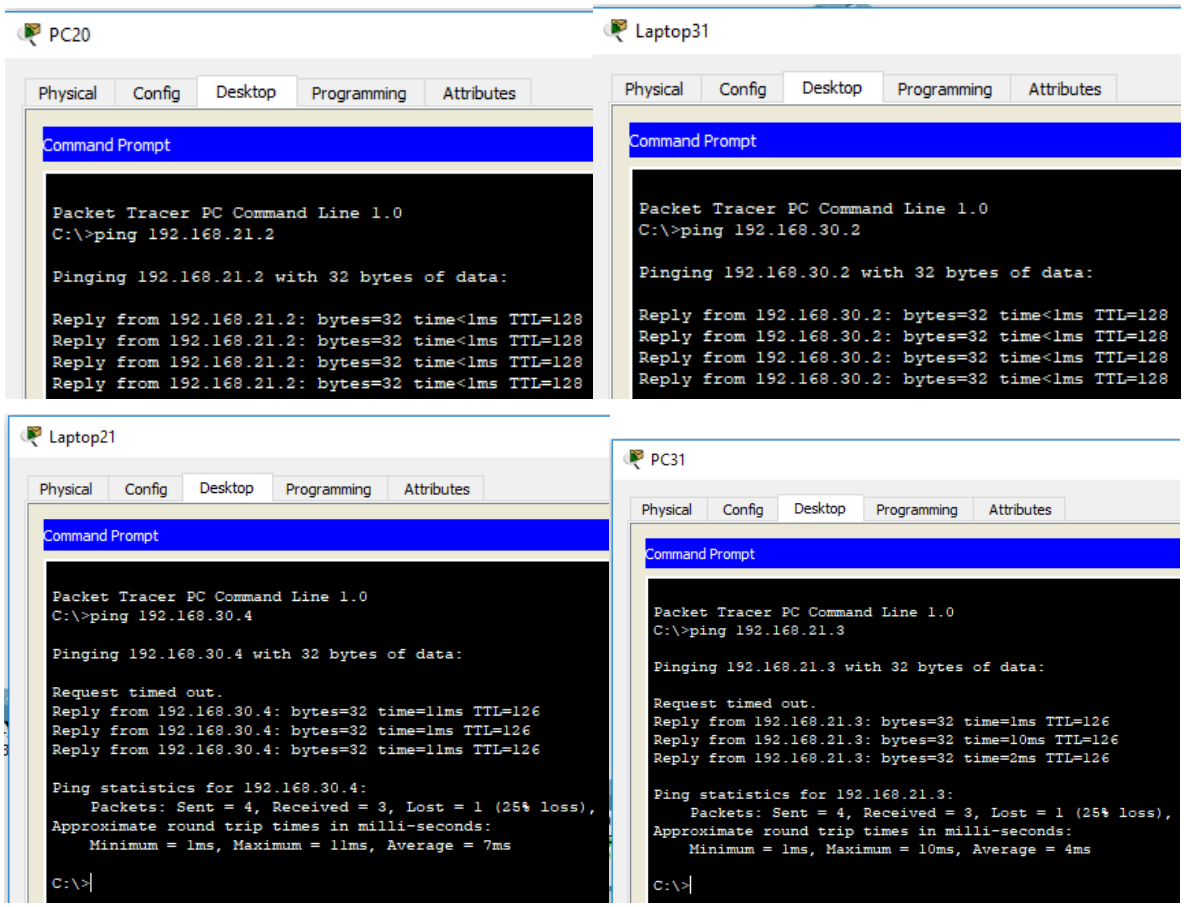
De esta forma, verificamos que todos los routers están compartiendo las rutas y se pueden intercomunicar.

2.12. Pruebas de conectividad entre terminales

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.

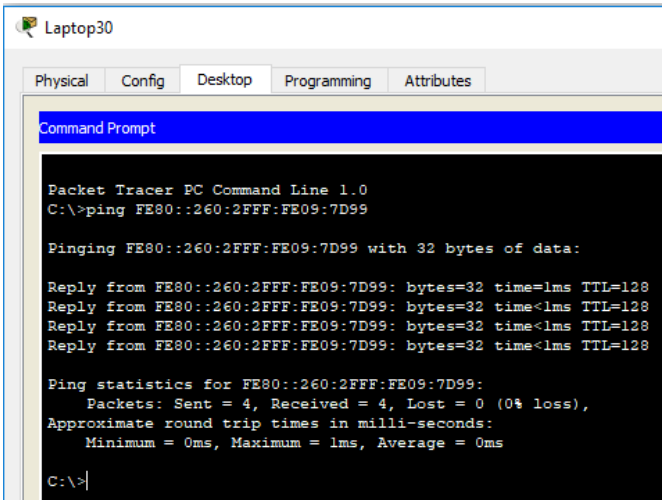
Ahora realizamos las pruebas de conectividad, podemos hacerlas gráficamente o por cmd:

Ilustración 23:algunas pruebas IPv4-ping



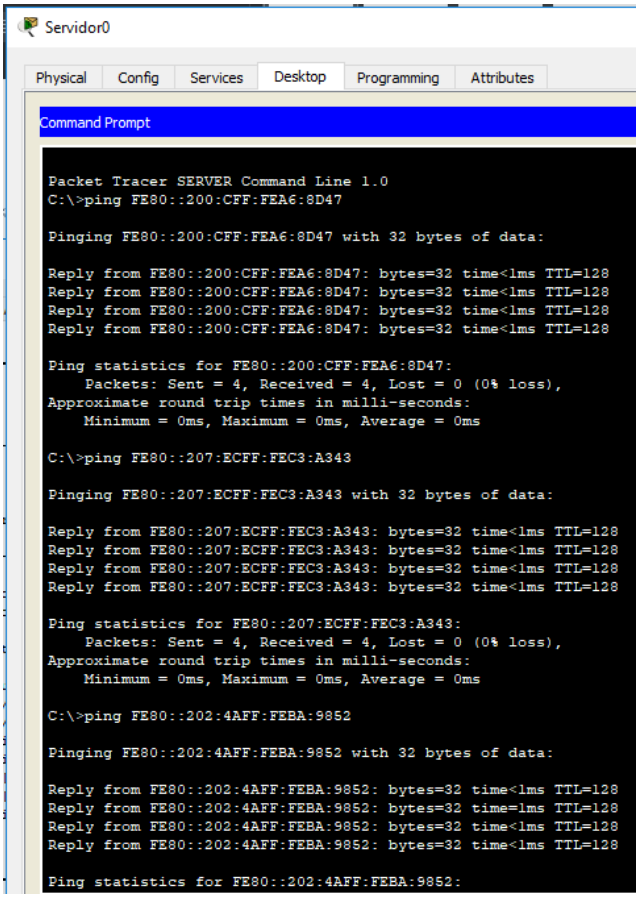
Se observa que las pruebas realizadas fueron satisfactorias hacia cualquiera de los terminales participantes de este escenario.

Ilustración 24: ping IPv6 de Laptop30 a Servidor0



La prueba bajo IPv6 también fue exitosa según se observa.

Ilustración 25: ping IPv6 desde Servidor0 a PCs

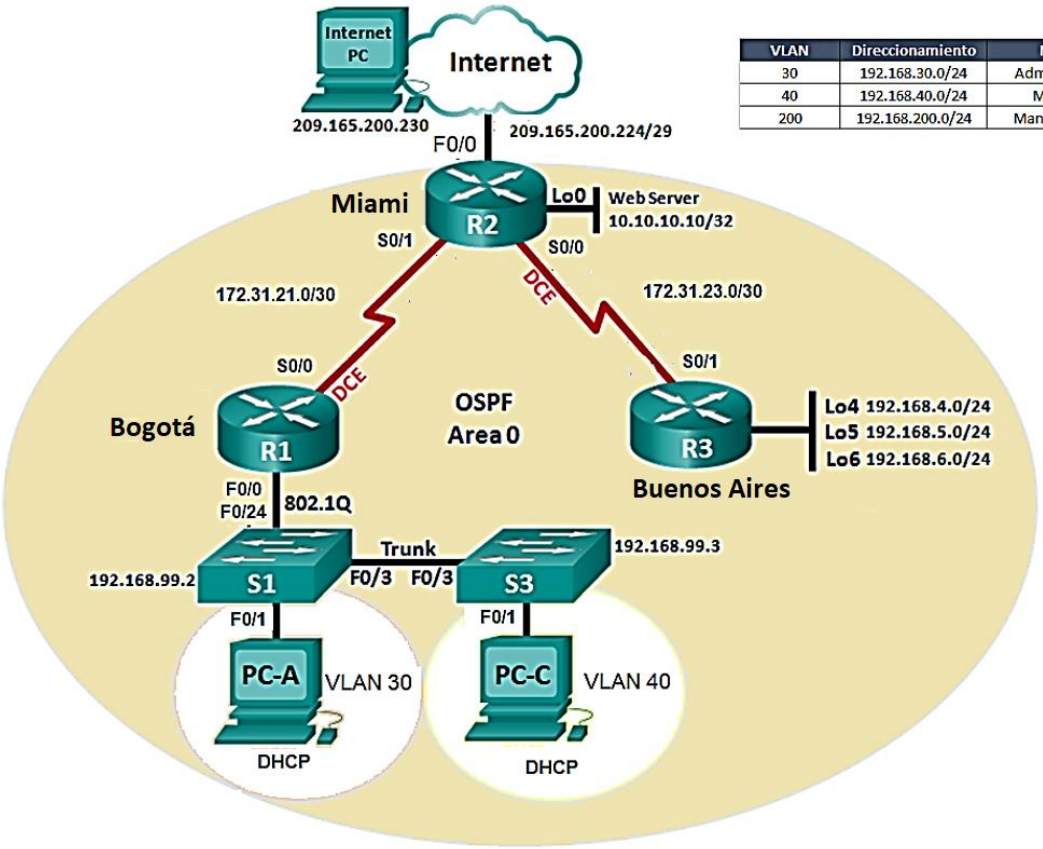


Se realizaron pruebas de conectividad desde el Servidor0 hacia el resto de los terminales resultando satisfactorias según se observa en la gráfica.

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 26: Escenario 2



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

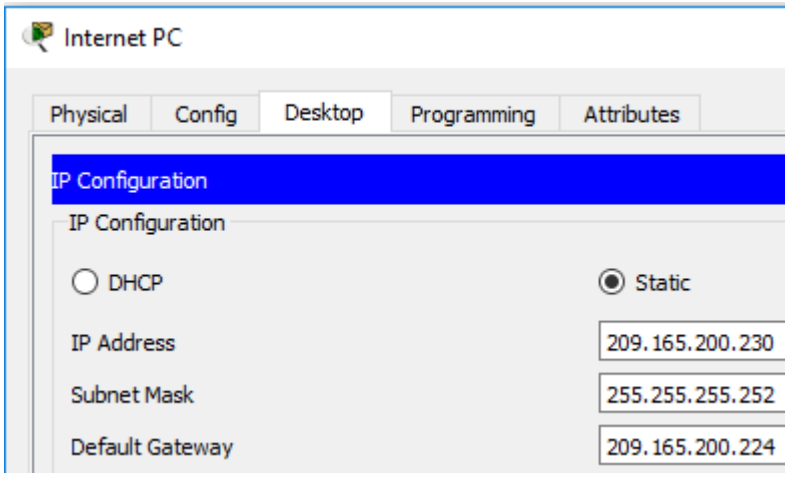
Este escenario nos pide utilizar el protocolo OSPFv2 el más usado por los proveedores de internet, posee una rápida convergencia, entre otras ventajas, comenzaremos montando la topología solicitada y configurando el direccionamiento solicitado, el tercer octeto para la red de mantenimiento, no coincide la tabla exhibida con el direccionamiento de los switches, de acuerdo a esto se usará el direccionamiento terminado en 99.2 y 99.3, y como la práctica consiste en tener 3 redes independientes, se cumple igual si configuramos la 200 o la 99.

3.1. Direccionamiento IP según esquema del escenario

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

Empezamos con el direccionamiento en cada uno de los equipos, en orden de arriba abajo, por ejmeplo, el InternetPC, tiene una IP pública con máscara 30 en la cual solo puede tener 2 direcciones asignables, una dirección de red y una de broadcast:

Ilustración 27: Direccionamiento Internet PC



La selección estática está por defecto así que colocamos el direccionamiento indicado, dado que el límite de la red es máscara 30, eso quiere decir que quedan 2 bit y 2^2 es igual a 4, 2 direcciones asignables y una para broadcast y la otra para la red.

Para R1, nombramos R1, levantamos la interfaz f0/0, creamos las subinterfaces 0.30 y 0.40 para las vlan respectivas, les damos una descripción y le damos direccionamiento según la ilustración del escenario.

Este es el script:

Para R1

enable

configure terminal

host Bogota

interface fast0/0

no shutdown

interface fast/0.30

description Administracion

ip addr 192.168.30.1 255.255.255.0

interface fast0/0.40

```
description Mercadeo
ip addr 192.168.40.1 255.255.255.0
interface fast0/0.99
description Mantenimiento
ip addr 192.168.99.1 255.255.255.0
inter s0/0/0
ip address 172.31.21.2 255.255.255.252
no shutdown
end
write
```

Para R2

```
enable
configure terminal
host Miami
inter lo0
description WebServer
ip addr 10.10.10.10 255.255.255.255
interface fast0/0
ip addr 209.165.200.229 255.255.255.248
no shutdown
inter s0/0/0
ip addr 172.31.23.1 255.255.255.252
no shutdown
inter s0/0/1
ip addr 172.31.21.1 255.255.255.252
no shutdown
end
write
```

Para R3

```
enable
```

```
configure terminal
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 shutdown
end
write
```

En los switches configuramos la dirección de mantenimiento:

Para SW1

```
enable
configure terminal
host S1
vlan 99
inter vlan 99
ip addr 192.168.99.2 255.255.255.0
end
write
```

Para SW3

```
enable
configure terminal
host S3
vlan 99
inter vlan 99
```

ip addr 192.168.99.3 255.255.255.0

end

write

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

Ahora, configuramos el OSPFv2 para poder compartir tablas de enrutamiento, bajo los parámetros de la tabla 3, comenzamos en R1, iniciamos digitando el protocolo con un número de identificación, en este caso el 1, luego le damos el id de acuerdo con la tabla, nombramos las interfaces que no participan de OSPF como interfaces pasivas, luego nombramos las redes que el router puede alcanzar a través de las interfaces que participan en el proceso, posteriormente entramos en la interfaz que la tabla indica para colocar el ancho de banda, de último aplicamos el costo del enlace, a continuación se indica el script para configurar en cada router:

Para R1

enable

configure terminal

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
write
```

Para R2

```
enable
configure terminal
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
write
```

Para R3

```
enable
configure terminal
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

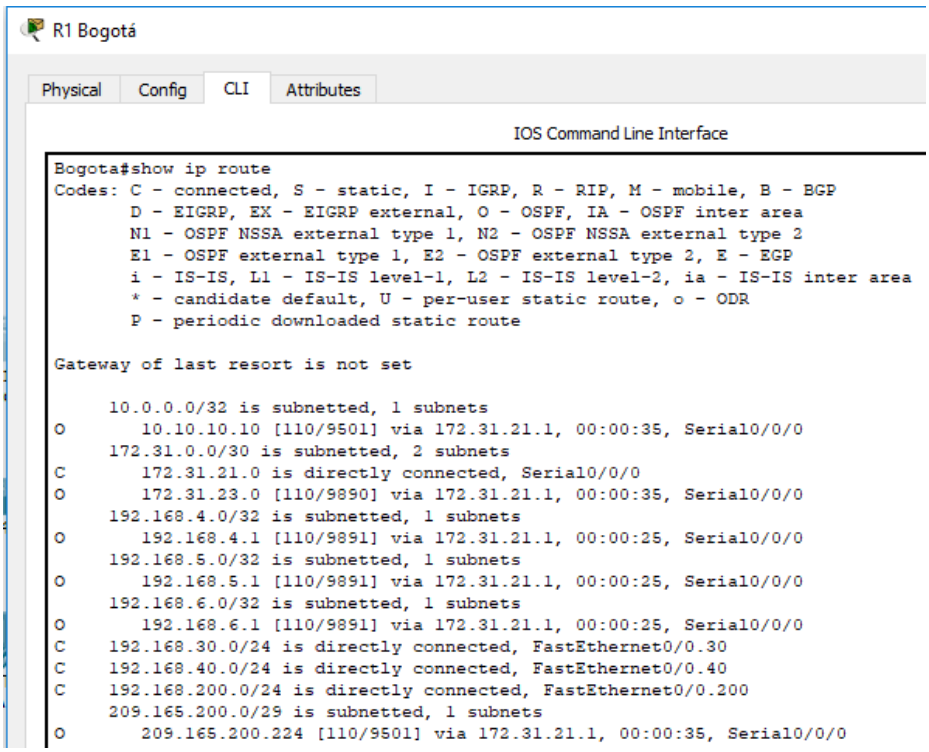
write

3.3. Verificación de la información OSPF

Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Tan pronto realizamos la configuración anterior, podemos consultar las tablas de enrutamiento, verificando como se obtuvo dicho direccionamiento:

Ilustración 248: Verificación routing table R1



Si la letra precedente es O, la ruta fue obtenida por OSPF, si está conectada directamente, es C, así las cosas: 6 se obtuvieron por OSPF, cuatro de ellas son las que están directamente conectadas al router.

Ilustración 29: Verificación routing table R2

R2 Miami

Physical | Config | CLI | Attributes

IOS Command Line Interface

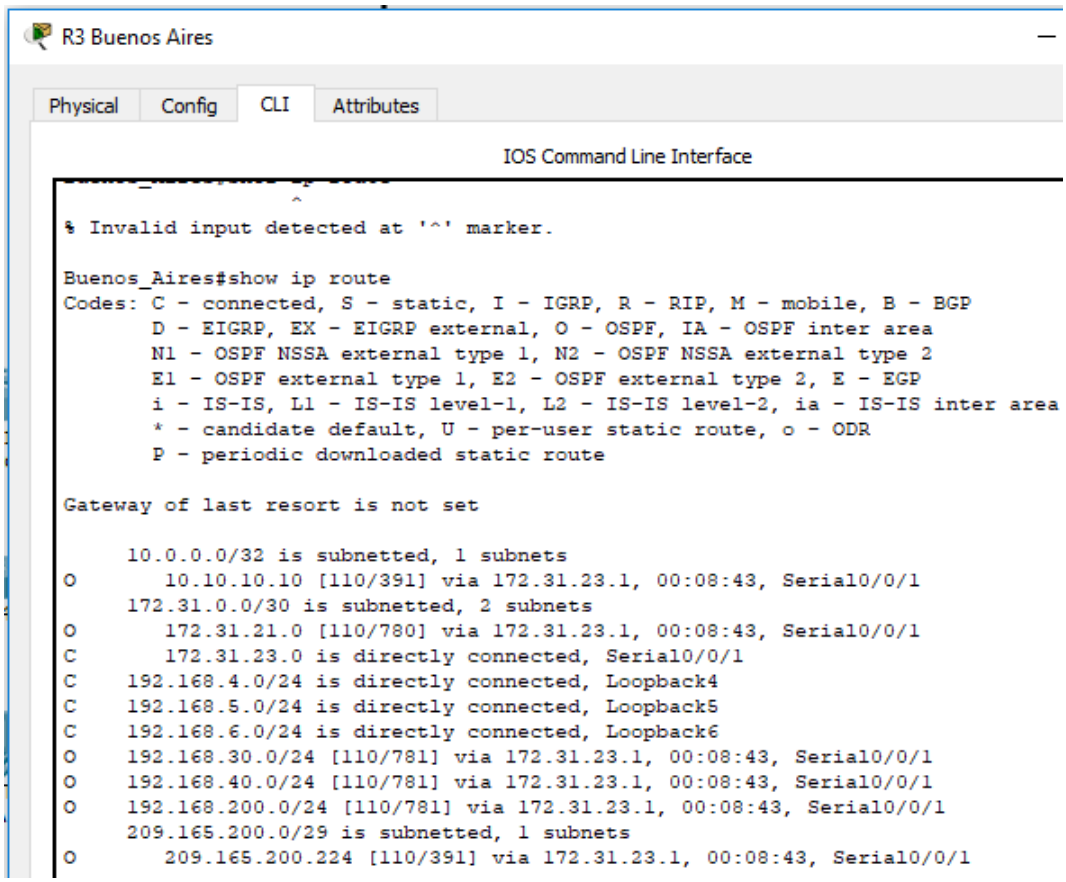
```
Miami#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - 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

     10.0.0.0/32 is subnetted, 1 subnets
C       10.10.10.10 is directly connected, Loopback0
     172.31.0.0/30 is subnetted, 2 subnets
C       172.31.21.0 is directly connected, Serial0/0/1
C       172.31.23.0 is directly connected, Serial0/0/0
     192.168.4.0/32 is subnetted, 1 subnets
O       192.168.4.1 [110/391] via 172.31.23.2, 00:04:08, Serial0/0/0
     192.168.5.0/32 is subnetted, 1 subnets
O       192.168.5.1 [110/391] via 172.31.23.2, 00:04:08, Serial0/0/0
     192.168.6.0/32 is subnetted, 1 subnets
O       192.168.6.1 [110/391] via 172.31.23.2, 00:04:08, Serial0/0/0
O    192.168.30.0/24 [110/391] via 172.31.21.2, 00:04:08, Serial0/0/1
O    192.168.40.0/24 [110/391] via 172.31.21.2, 00:04:08, Serial0/0/1
O    192.168.200.0/24 [110/391] via 172.31.21.2, 00:04:08, Serial0/0/1
     209.165.200.0/29 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, FastEthernet0/0
```

En esta parte encontramos que el router encontró seis redes a través de OSPF y tiene 4 conectadas directamente.

Ilustración 30: Verificación routing table R3

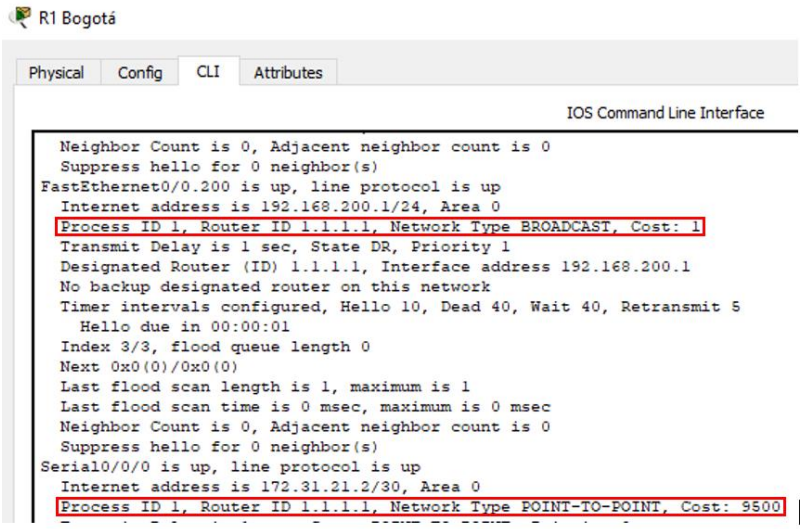


En esta última figura se observa que el router 3 obtiene igualmente 6 redes por OSPF.

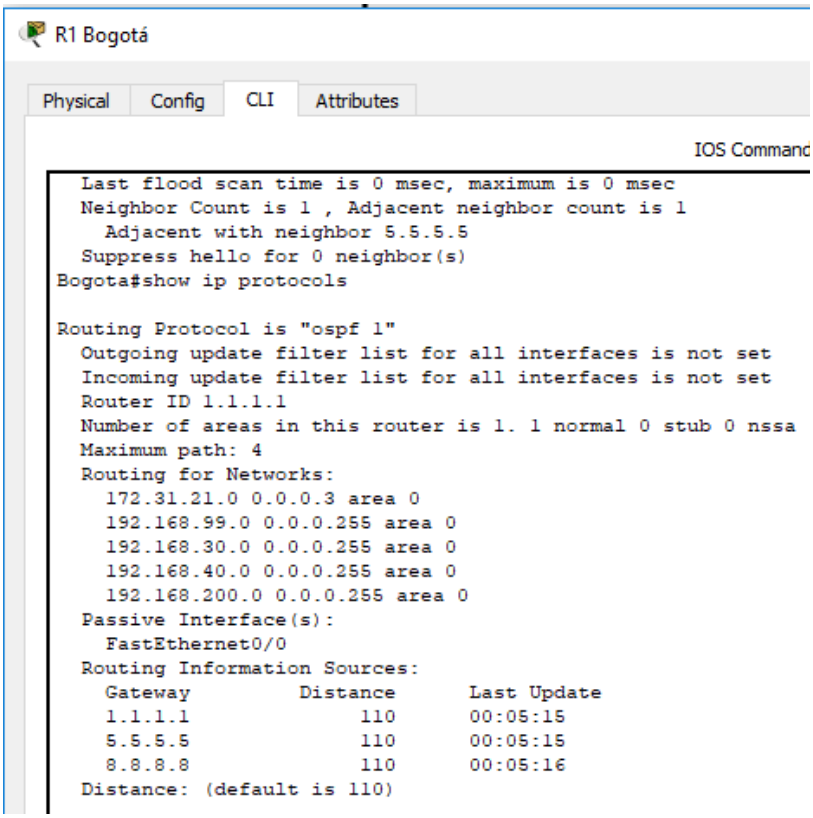
- Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface
- Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Visualizamos lo solicitado, aplicando los comandos **show ip ospf interface** y **show ip protocols**, a continuación, los pantallazos de demostración de la información solicitada al router:

Ilustración 31: Verificación en R1

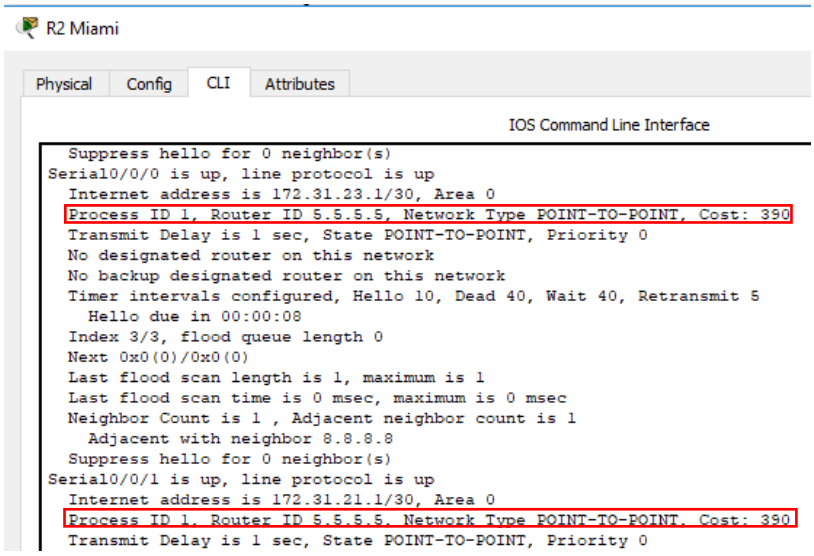


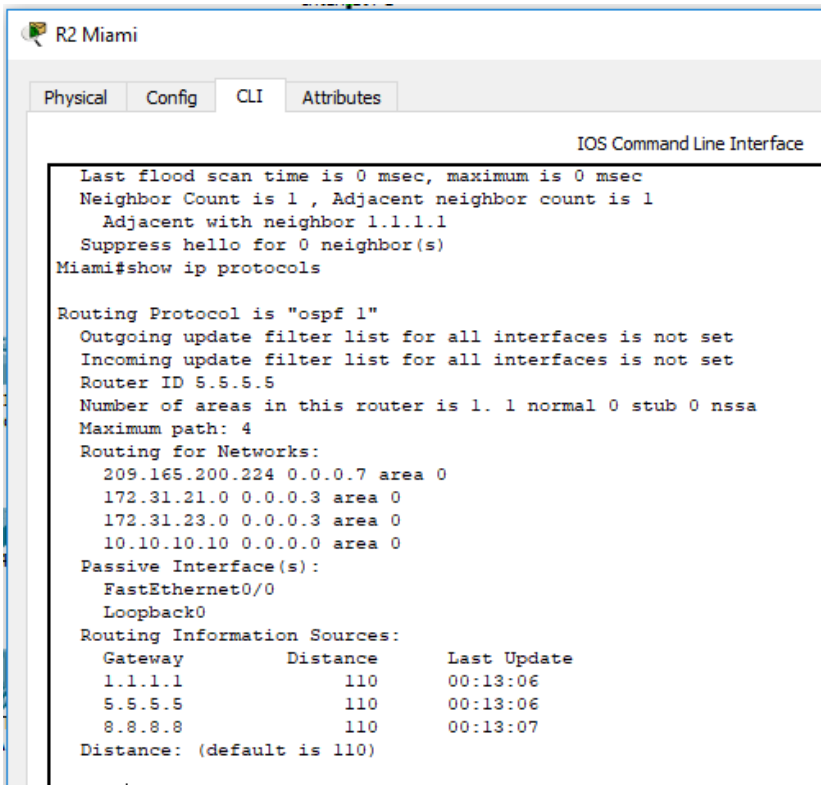
Esta ilustración muestra los costos de cada interface, también muestra el Process ID, Router ID,



En esta apreciamos el Routing Networks, and passive interfaces configuradas en cada router

Ilustración 32: Verificación en R2





Seguimos con la verificación en cada router, aplicando los mismos comandos indicados

Ilustración 33: Verificación en R3

R3 Buenos Aires

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
Loopback4 is up, line protocol is up
  Internet address is 192.168.4.1/24, Area 0
  Process ID 1, Router ID 8.8.8.8, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Loopback5 is up, line protocol is up
  Internet address is 192.168.5.1/24, Area 0
  Process ID 1, Router ID 8.8.8.8, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Loopback6 is up, line protocol is up
  Internet address is 192.168.6.1/24, Area 0
  Process ID 1, Router ID 8.8.8.8, Network Type LOOPBACK, Cost: 1
  Loopback interface is treated as a stub Host
Serial0/0/1 is up, line protocol is up
  Internet address is 172.31.23.2/30, Area 0
  Process ID 1, Router ID 8.8.8.8, Network Type POINT-TO-POINT, Cost: 390
  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
```

R3 Buenos Aires

Physical | Config | CLI | Attributes

IOS Command Line Interface

```
  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)
Buenos_Aires# 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 8.8.8.8
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.23.0 0.0.0.3 area 0
    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
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1              110      00:16:27
    5.5.5.5              110      00:16:27
    8.8.8.8              110      00:16:27
  Distance: (default is 110)
```

Finalmente, llegamos a router 3, en donde hay 3 interfaces pasivas, las cuales son Lo4 a Lo6

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.

Seguidamente configuramos las vlan, los puertos que son troncales en los switches además la seguridad en cada switch según se nos indica en el escenario, debemos implementar password para el ingreso al switch y password para el enable, con eso evitamos configuraciones por parte de personas no autorizadas que podrían hacer que la red se caiga.

El script para su configuración:

Para SW1

```
enable
configure terminal
vlan 30
vlan 40
interface fast0/3
switchport mode trunk
interface fast0/24
switchport mode trunk
interface FastEthernet0/1
switchport access vlan 30
switchport mode access
exit
enable secret villamil
enable password villamil
line console 0
password villamil
login
line vty 0 4
password villamil
login
banner motd x Prohibido el Acceso no Autorizado! x
service password-encryption
```

end

write

Para SW3

enable

configure terminal

vlan 40

interface fast0/3

switchport mode trunk

interface FastEthernet0/1

switchport access vlan 40

switchport mode access

exit

enable secret villamil

enable password villamil

line console 0

password villamil

login

line vty 0 4

password villamil

login

banner motd x Prohibido el Acceso no Autorizado! x

service password-encryption

end

write

3.5. Deshabilitar del DNS lookup

En el Switch 3 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.

A continuación, el script:

```
enable
configure terminal
no ip domain-lookup
end
write
```

3.6. Configuración de direcciones IP a los switches

Asignar direcciones IP a los Switches acorde a los lineamientos.

El direccionamiento de los switches es muy necesario para poder realizar ajustes posteriores a la configuración incial, como, por ejemplo, levantar un puerto o apagarlo según sea la necesidad entre otras, este es el cli:

Para SW1:

```
enable
configure terminal
vlan 99
inter vlan 99
ip addr 192.168.99.2 255.255.255.0
end
write
```

Para SW3:

```
enable
configure terminal
vlan 200
inter vlan 200
ip addr 192.168.200.3 255.255.255.0
end
write
```

3.7. Desactivación Puertos

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

Por seguridad de la red esto debe ser configurado, así evitamos fallas provocadas por personas no capacitadas en la ingeniería de networking, a continuación, el script:

Para SW1:

```
enable
configure terminal
inter range f0/2 , f0/4-23
shutdown
end
write
```

Para SW3:

```
enable
configure terminal
inter range f0/2 , f0/4-24
shutdown
end
write
```

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.

Seguimos con la configuración del servicio de DHCP para las VLAN 30 y 40, primero reservamos 30 direcciones para configuraciones estáticas, a continuación, el script para esto:

Configuración DHCP IPv4

```
enable
configure terminal
```

```
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
write
```

3.9. Configuración Network Address Translation o NAT

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

El NAT es lo que nos permite salir a internet, por lo tanto, debemos realizar PAT o mejor dicho, NAT con sobrecarga, ya que esta es la manera que tienen los terminales para alcanzar la red internet, para ello implementamos los parámetros necesarios, una lista de acceso que indique que redes o hosts pueden salir a internet, luego la aplicamos en el comando de NAT con sobrecarga, nombramos las interfaces que entran y las que salen y ya queda funcionando NAT para salir a internet. El cli:

```
enable
configure terminal
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
interface fast0/0
ip nat outside
inter s0/0/0
ip nat inside
```

inter s0/0/1

ip nat inside

end

write

3.10. Listas de Acceso estándar y extendidas

- 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.

Configuraremos listas de acceso para permitir o bloquear el paso de paquetes de un host a otro, esto lo hacemos con las siguientes líneas de configuración:

enable

configure terminal

ip access-list standard ACL_1

permit 192.168.30.0 0.0.0.255

deny 192.168.40.0 0.0.0.255

ip access-list standard ACL_2

deny 192.168.30.0 0.0.0.255

permit 192.168.40.0 0.0.0.255

ip access-list extended ACL_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 ACL_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

write

Seguidamente, estas listas se aplican en la interfaz requerida con el comando **ip access-group lista_uno in** y esto impediría direcciones que no concuerden con la lista de acceso implementada.

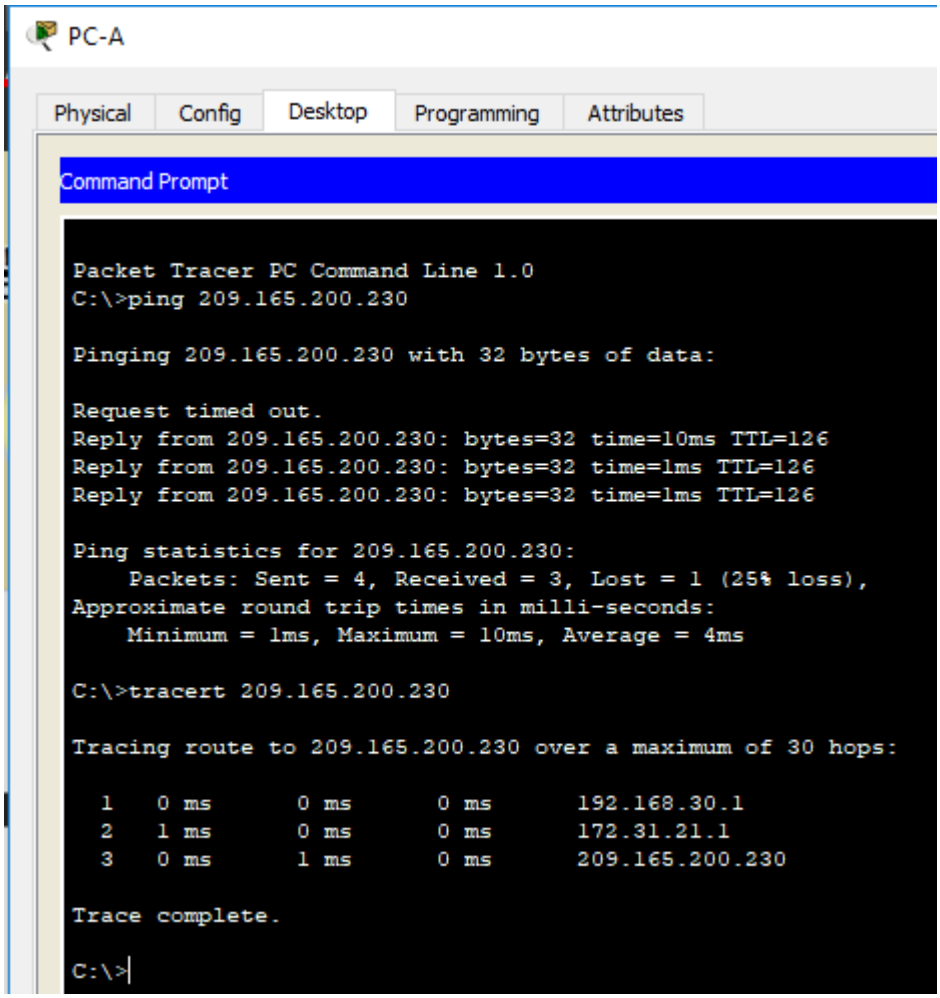
3.11. Verificación de la comunicación

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

Con el comando ping podemos hacer pruebas de conectividad, también, podemos usar el comando tracert para comprobar en cual salto se quedó el ping y así tomar decisiones sobre que hacer para solucionar problemas de conectividad.

Desde PC-A:

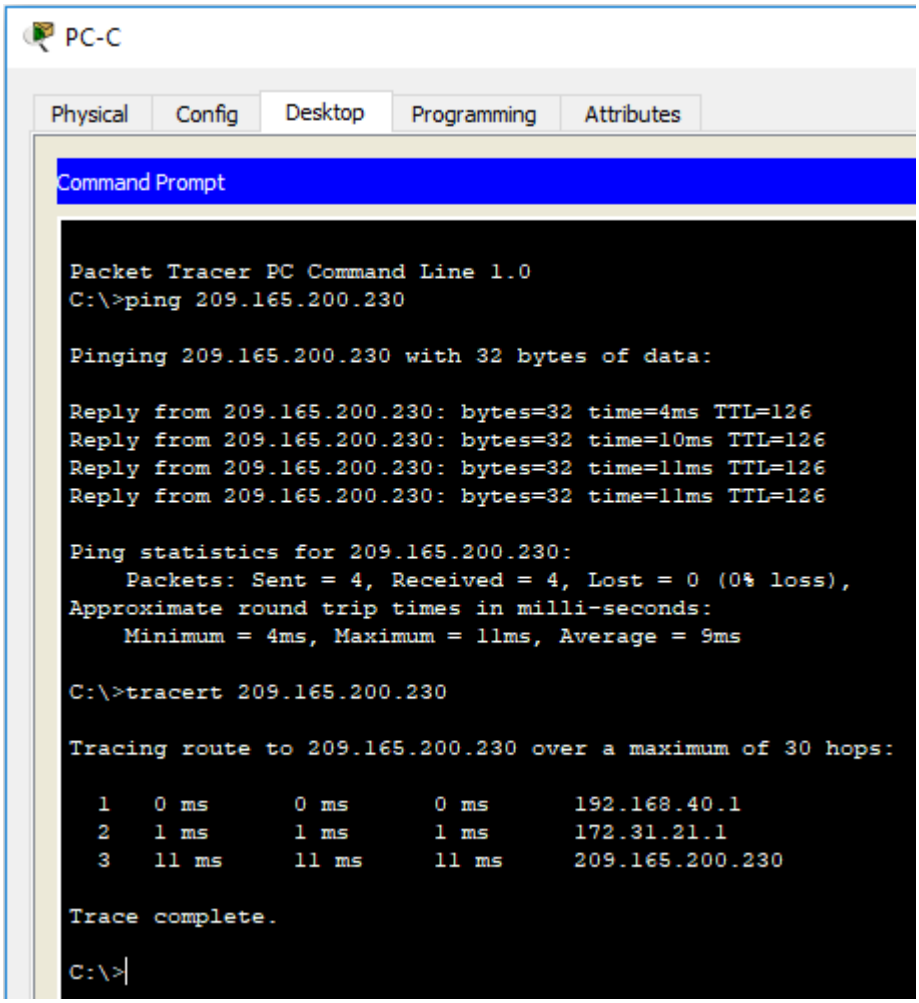
Ilustración 3254: PC-A pruebas de conectividad



Observamos que el ping fue exitoso, y mediante tracert, nos damos cuenta cuantos saltos fueron necesarios para que el paquete alcanzara el destino.

Desde PC-B:

Ilustración 35: PC-C pruebas de conectividad



Pasó lo mismo con PC-C tuvo 3 saltos antes de llegar a destino.

Todo lo anterior fue posible, gracias a las configuraciones realizadas para tal fin.

CONCLUSIONES

Para poder implementar grandes redes, este curso resultó ser muy útil, pues pudimos ampliar el conocimiento sobre las mismas y no es simplemente creer que por que un pc dio “link” ya tiene conectividad, puede tener conectividad, física talvez, pero la física sin la lógica, no son nada.

Realmente fue una profundización, porque el tema de redes, para que funcione todo sin problemas, y sea muy veloz el intercambio de datos, se necesitan ciertas configuraciones sencillas o complejas, además de que las direcciones IP deben ser únicas para que el proceso de comunicación pueda llevarse a cabo.

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.).