EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ALEXANDER VILLAMIL POVEDA

Diplomado CCNA
opción de grado

Instructor: Iván Gustavo Peña

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

Contenido

Introducción

El siguiente trabajo es el resultado del examen práctico del diplomado de CISCO, el cual plantea desde un caso práctico, la aplicación de lo aprendido durante el desarrollo del diplomado de profundización CCNA.

El desarrollo de la práctica es desarrollado mediante el software Packet Tracer, en donde se simula la red del caso y se resuelven cada uno de los escenarios.

El desarrollo es de carácter práctico y con él se desarrolló de este, se plasmará los conocimientos adquiridos durante todo el diplomado.

1. Escenario 1

Ilustración 1: Escenario 1

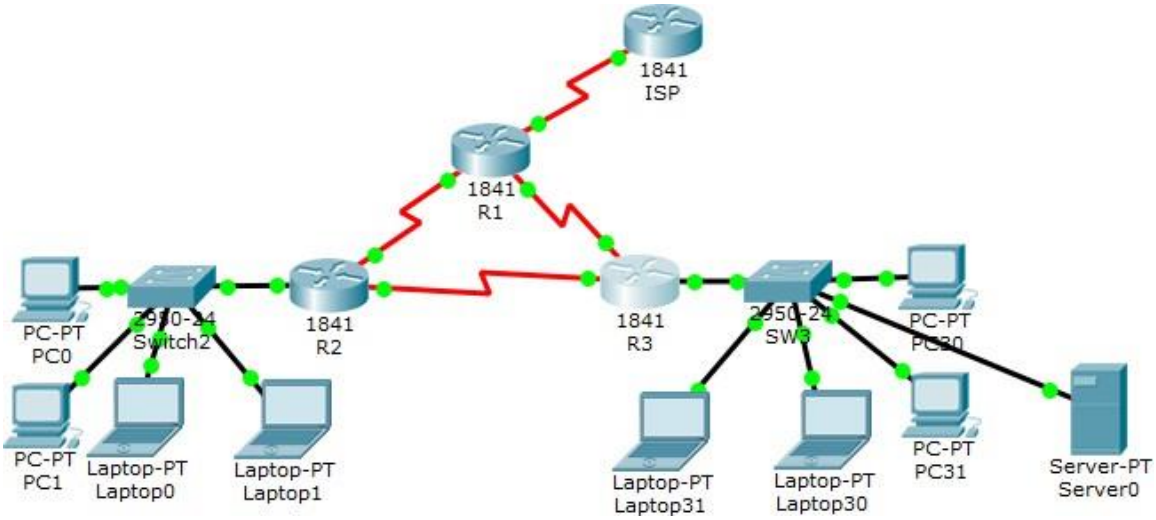


Tabla 1: Tabla de direccionamiento

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

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 la solución de este escenario, en primer lugar, debemos realizar las configuraciones de direccionamiento que solicita la tabla 1, ya que dependiendo de eso es que vamos a obtener la conectividad que requiere el problema, en ese orden, entramos primero al ISP y le configuramos la IP solicitada en la interfaz s0/0/0, por último levantamos la misma, ya que como lo sabemos, en un router, contrario de lo que sucede en un switch, viene down, al R1 debemos instalarle una tarjeta adicional con 2 interfaces seriales, ya que el router 1841, que es el que estamos usando, viene con 2 únicas interfaces seriales, podríamos utilizar otro router, pero por seguir los lineamientos de la guía, ponemos el mencionado router y luego, lo apagamos y le insertamos una tarjeta de interfaces seriales, la cual viene con dos puertos y así, montamos la topología observada y configuramos todos los elementos de la red, como vamos a ver a continuación.

2. Desarrollo de las actividades Escenario 1

2.1. Asignaciones de puertos y configuración de VLAN

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.

La solución de este punto, consiste, primero que nada, en darle un nombre al switch, seguidamente, darle el carácter que requiere la interfaz 0/1, el cual debe ser troncal, para permitir el paso de todas las vlan que creemos en el switch, luego, damos acceso a las vlan indicadas, los puertos asignados a terminales, por último, apagamos las interfaces que no sean utilizadas, esta acción agrega seguridad a la implementación, guardamos la configuración usando los comandos copy running-config startup-config o 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 en ISP, R1, R2 y R3

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

Comenzamos configurando la dirección ip del router que nos sirve de ISP (Internet Service Provider) no olvidamos encender la interfaz y grabamos, así hacemos para R1, R2 y R3 siguiendo la tabla 1.

El siguiente es el script que utilizaremos:

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

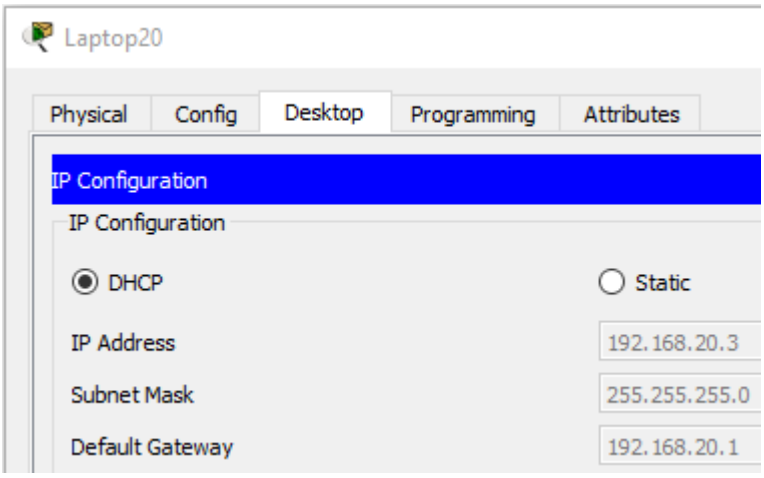
write

2.3. Configuración de DHCP en host

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

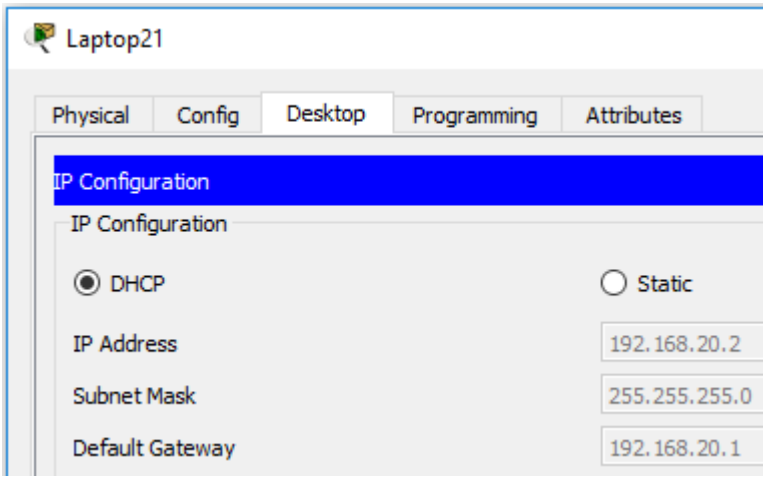
Luego de hacer las configuraciones de hacer las configuraciones en los routers sobre direccionamientos, pasamos a realizar lo mismo en los PC conectados, pero acá usamos la interfaz gráfica, para ello damos click sobre el terminal a modificar y luego en la pestaña Desktop, por último hacemos click en la opción DHCP.

Ilustración 2: Laptop20



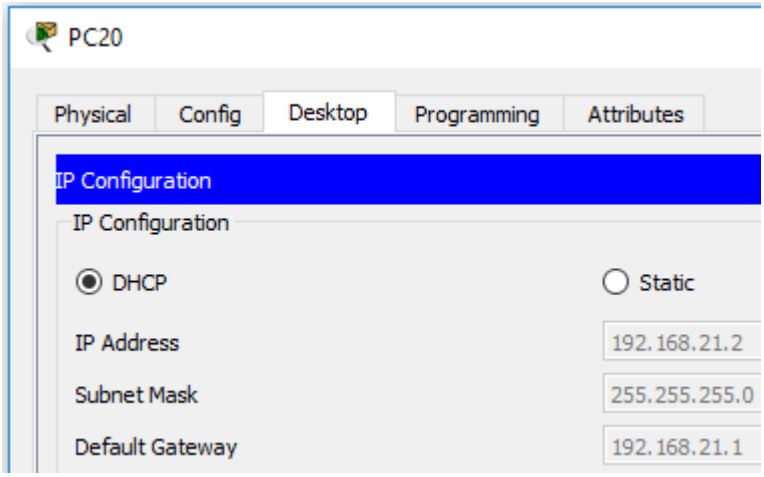
En esta parte podemos ver que a la Laptop20 se le seleccionó la opción DHCP y le dio una dirección 192.168.20.3/24 y gateway 192.168.20.1

Ilustración 3: Laptop21



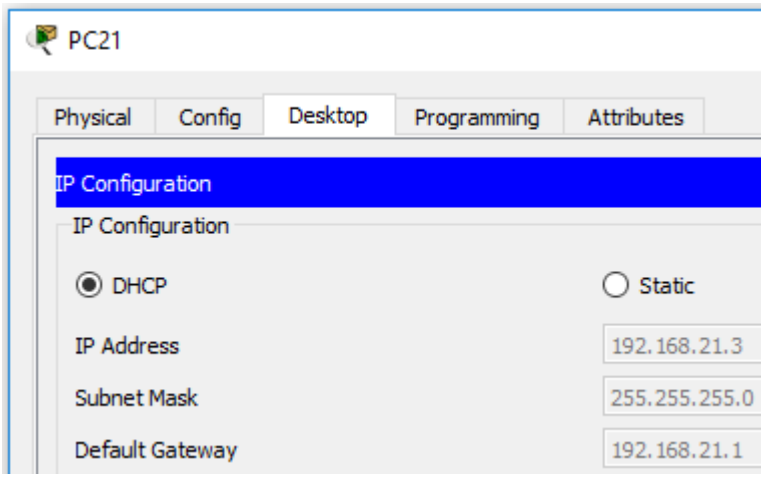
Acá observamos a la Laptop21 se le seleccionó DHCP y la dirección obtenida es 192.168.20.2/24 y gateway 192.168.20.1

Ilustración 4: PC20



Seguidamente en la PC 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

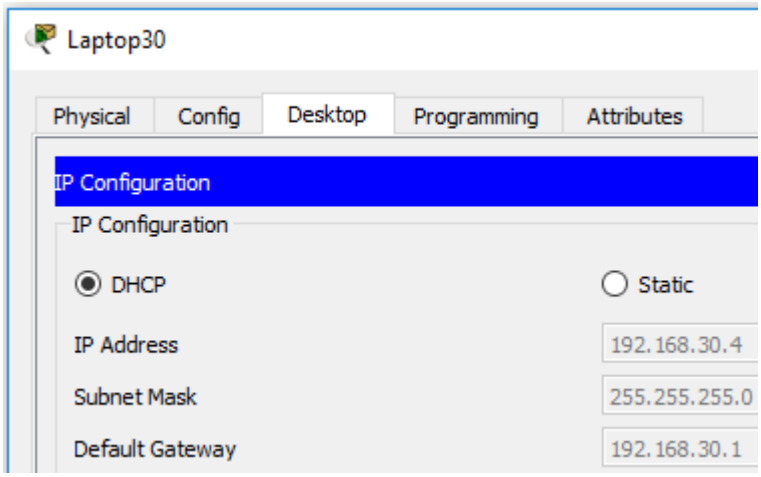


Ilustración 7: Laptop31

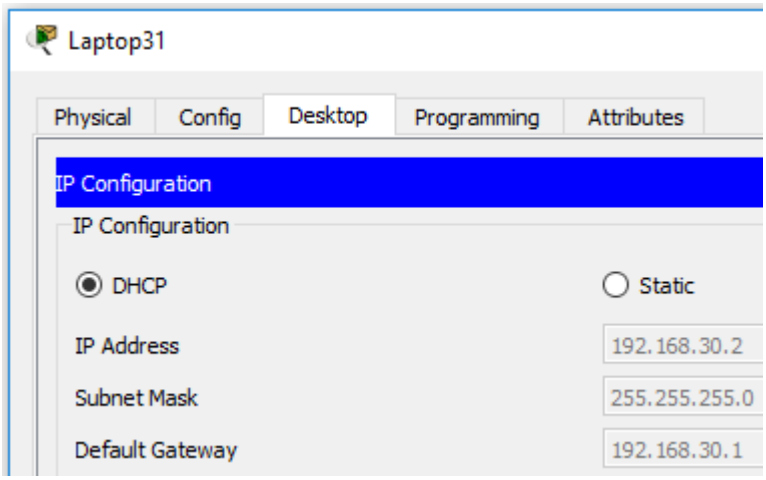
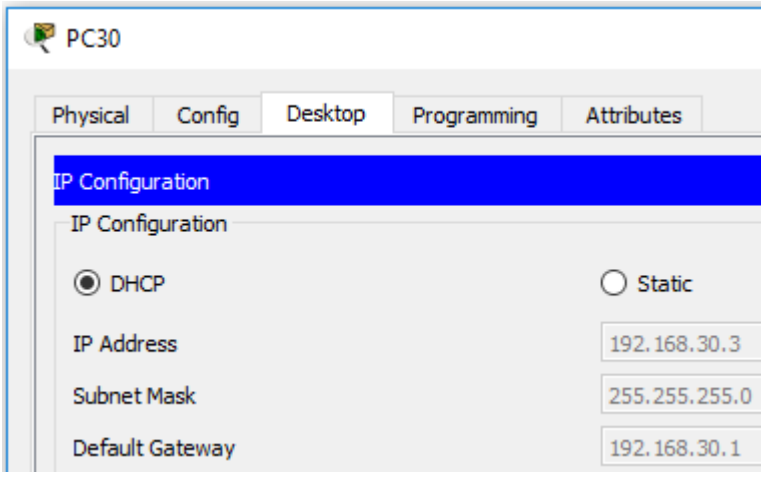
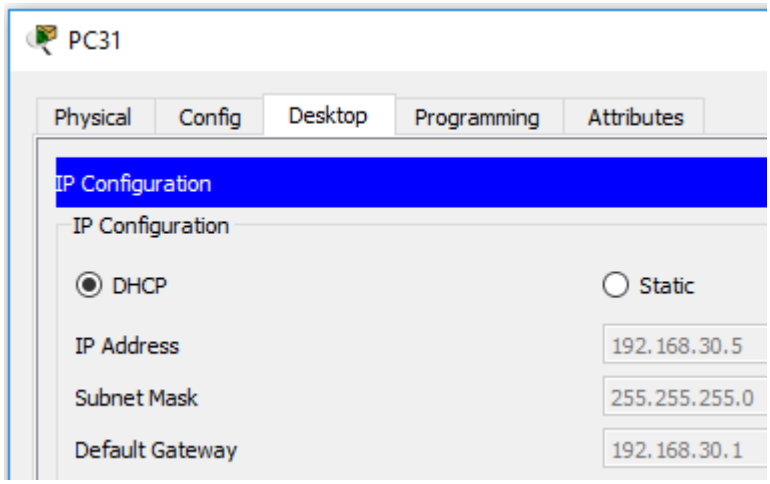


Ilustración 8: PC30



Es claro que todo ese proceso no hubiera sido posible si no se configura previamente el servicio de DHCP en router a la cual están conectados los terminales. La configuración de dicho servicio se explicará más adelante.

Ilustración 9: PC31



Respuesta de DHCP satisfactoria en PC31

2.4. Configuración de NAT

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**.

Algo muy importante para que nuestros terminales alcancen a ISP y que, en la práctica en la vida real, se emplea esto a diario, ya que ayuda a alargar el tiempo de vida de las IPv4.

A continuación, el cli para que este proceso se ponga en función, debemos crear una lista de acceso, para indicar que terminales dentro de nuestra red pueden alcanzar ISP, posteriormente, escribimos la línea que indica como se hará NAT o mejor dicho PAT que es como se le conoce al NAT con sobrecarga, se indican las interfaces de entrada y salida y ya está:

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

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)

Esta gráfica nos muestra que las pruebas de conectividad con ICMP son satisfactorias

2.5. Configuración ruta estática

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

La configuración de una ruta estática predeterminada, significa que, si la dirección solicitada por un host no se encuentra dentro de las redes que conoce el router, él la envía la solicitud por dicha ruta para que la resuelva el dispositivo conectado en esa interfaz y haga su “best effort” en caso de que no se encuentre el destino, el paquete es descartado, a continuación, el script:

enable

configure terminal

ip route 0.0.0.0 0.0.0.0 Serial0/0/0

end

write

2.6. Configuración de DHCP en R2

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

De acuerdo a la solicitud de la guía, debemos configurar un servicio de DHCP en el router 2, entonces, el paso a seguir, es crear el vlan pool, podemos colocarle el nombre que deseemos, pero para que tengamos en cuenta a que red pertenece, la nombraremos vlan_100, a continuación, el script:

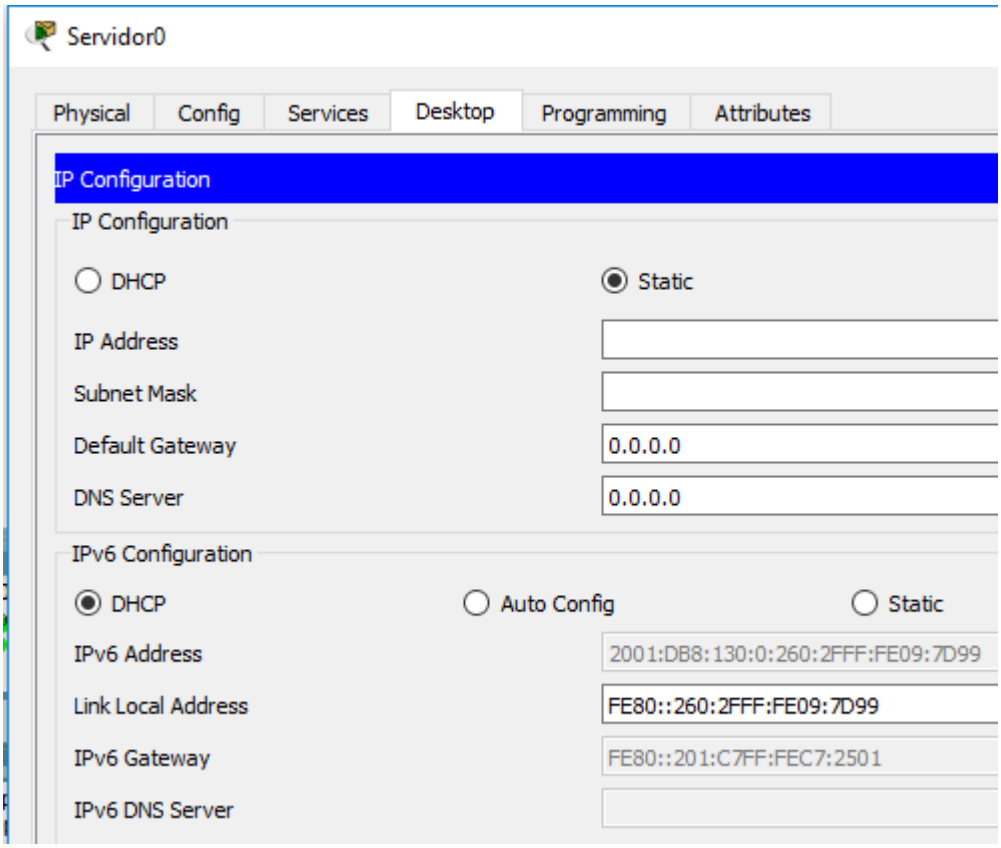
```
enable
configure terminal
ip dhcp pool vlan_100
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
ip dhcp pool vlan_200
network 192.168.21.0 255.255.255.0
default-router 192.168.21.1
end
write
```

2.7. Pruebas de ping al Servidor0

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

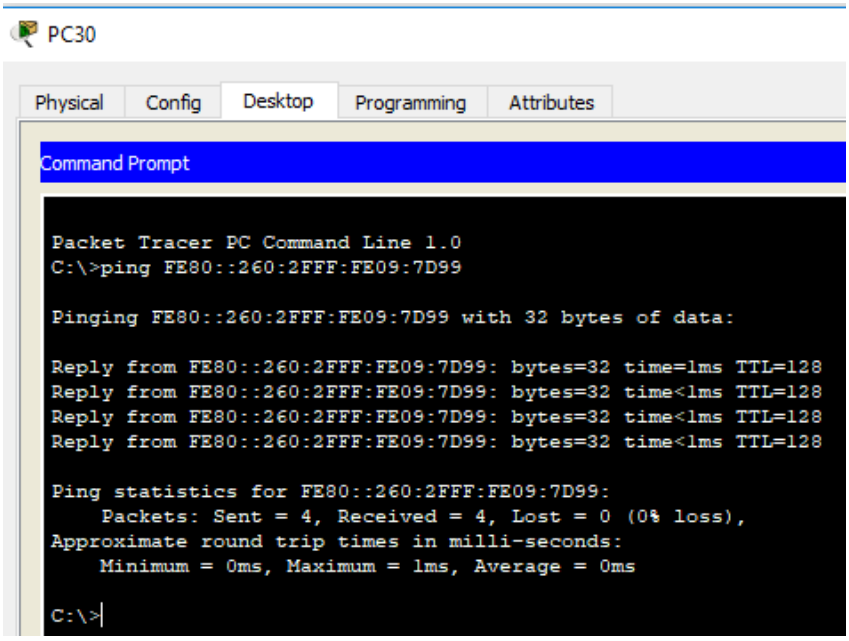
Ya realizado el paso anterior y con las direcciones obtenidas, podemos realizar las pruebas de conectividad, haciendo ping desde Servidor0, pero en protocolo IPv6, a continuación, las pruebas:

Ilustración 11: Dirección IPv6 Servidor0 tomada por DHCPv6



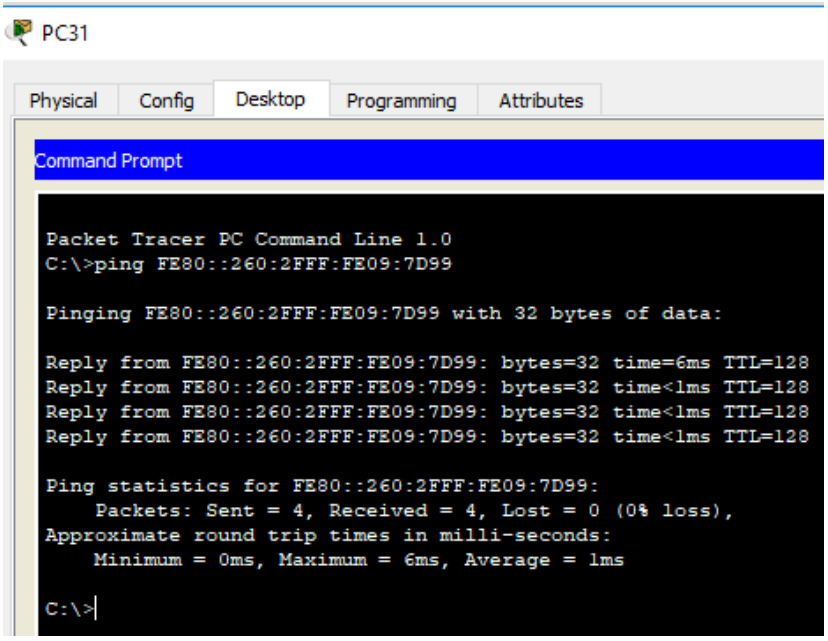
En esta parte podemos ver como hemos cambiado la configuración estática a la configuración por DHCP en versión IPv6, ya que el router se encuentra en doble stack, lo que explicaremos más adelante, por lo pronto haremos las pruebas de conectividad:

Ilustración 12: ping IPv6 de PC30 a Servidor0



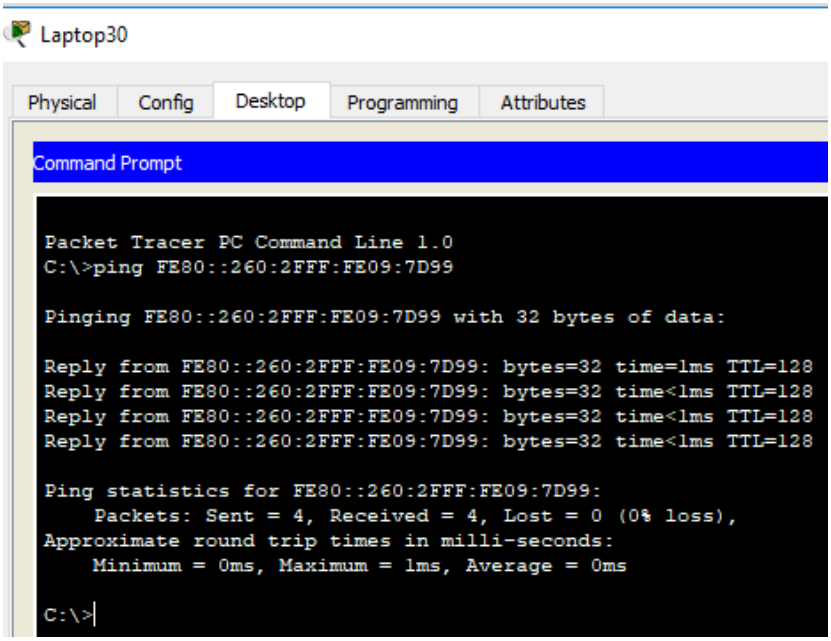
Los terminales conectados a R3 son los únicos que pueden tener esta configuración según la guía, el PC30, por lo tanto, se hace ping desde ellos a el Servidor0, en la ilustración, se puede apreciar que el ping fue satisfactorio.

Ilustración 13: ping IPv6 de PC31 a Servidor0



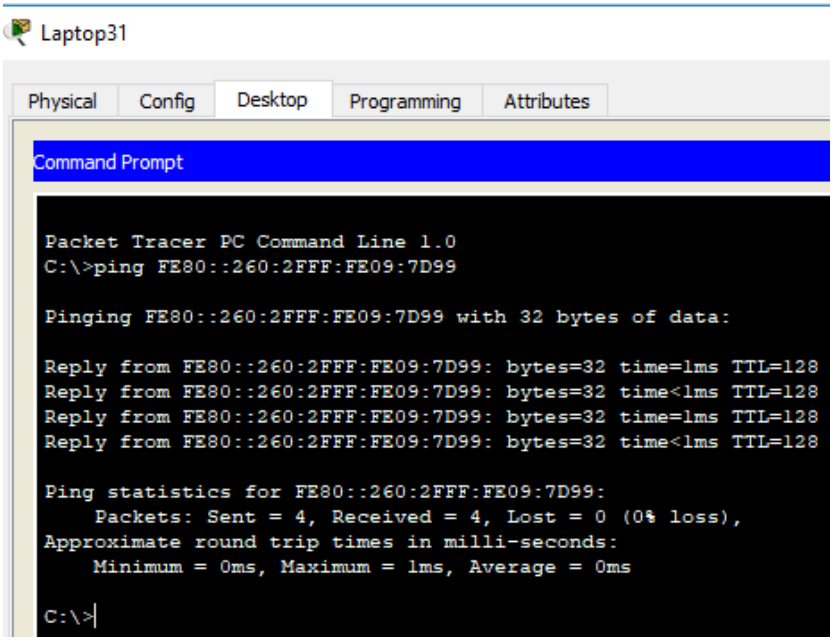
Desde PC31 se hace lo mismo y se obtiene el mismo resultado.

Ilustración 14: ping IPv6 de Laptop30 a Servidor0



Desde las Laptop también

Ilustración 15: ping IPv6 de Laptop31 a Servidor0



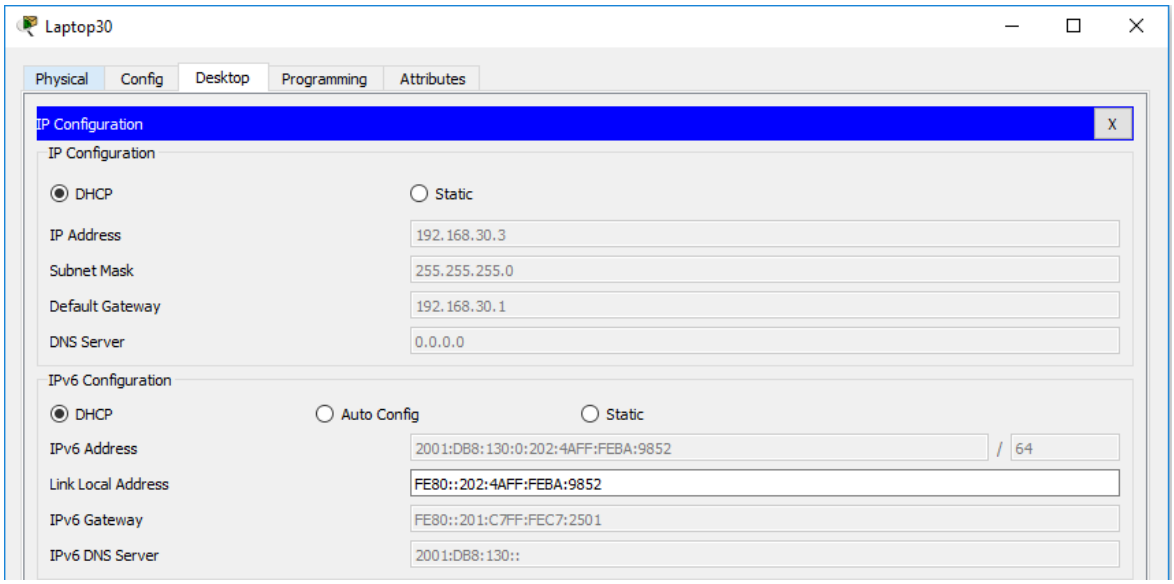
Y así todos son probados, lo que nos indica que la configuración para DHCPv6 es correcta.

2.8. Configuración dual-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.

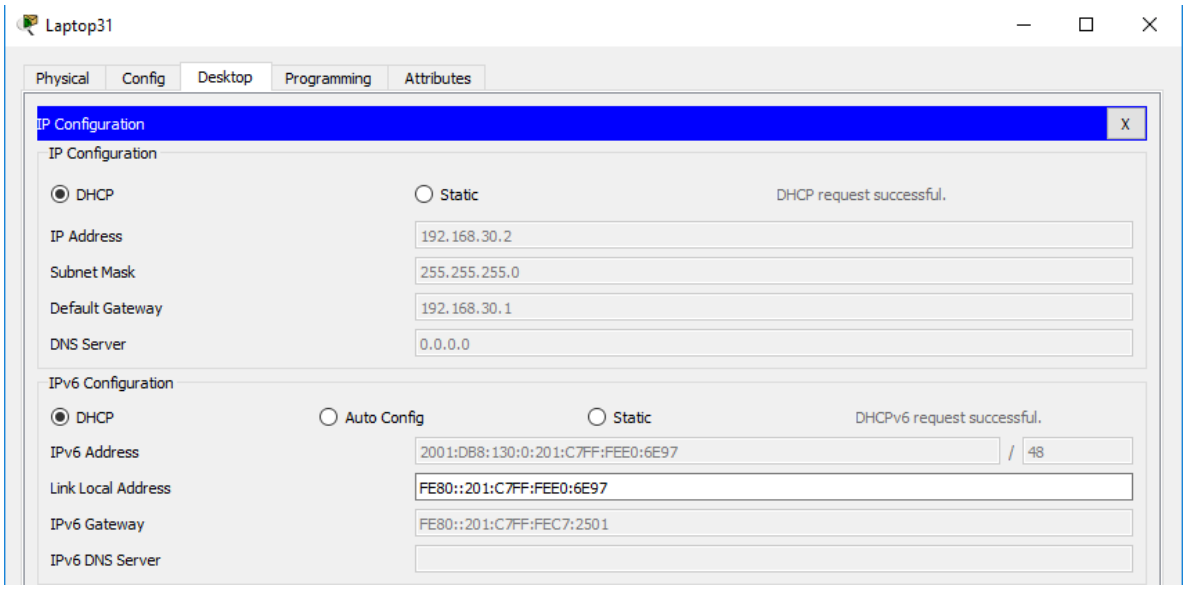
Para configurar esta cualidad, es decir, que los equipos obtengan direccionamiento de las dos pilas disponibles, solo debemos hacer click en el equipo a modificar, luego en la pestaña Desktop, IP Configuration, y selecciona en ambos apartados DHCP ya que por defecto viene estático:

Ilustración 16: dual-stack Laptop30



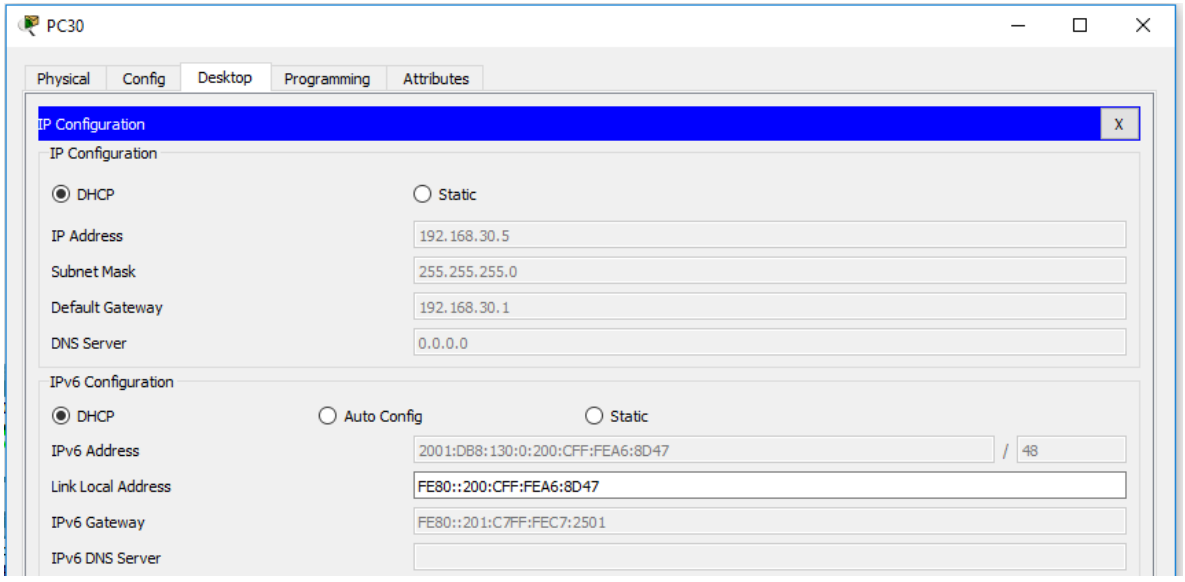
Se aprecia entonces como ambas pilas tomaron direccionamiento con la numeración correspondiente, decimal para IPv4 y hexadecimal para IPv6.

Ilustración 17: dual-stack Laptop31



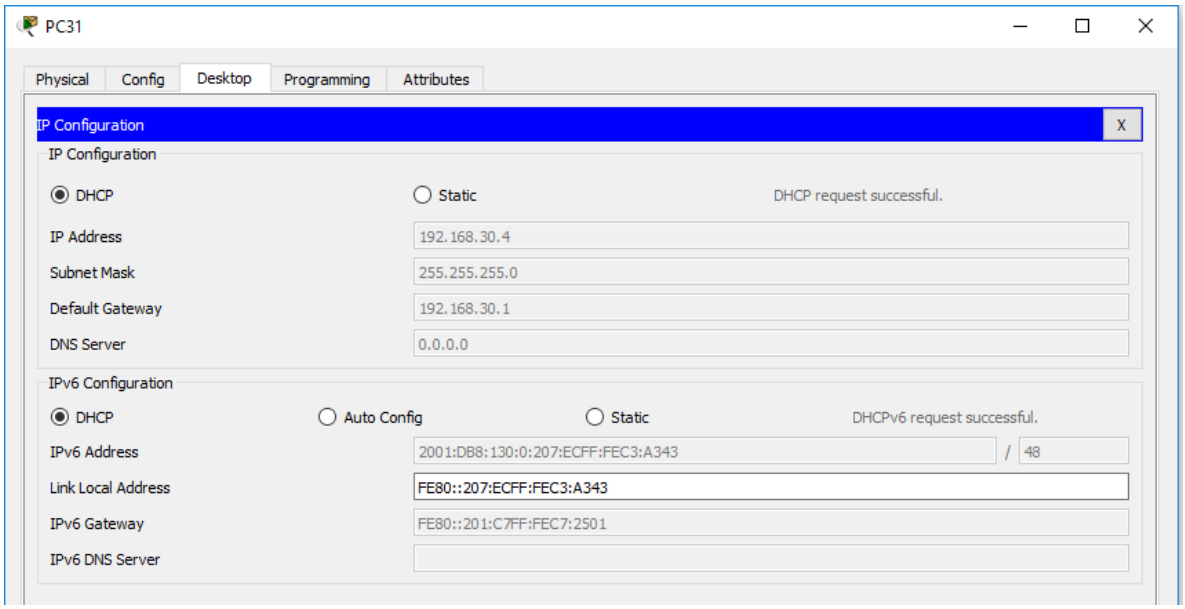
Hacemos lo propio para cada uno de los terminales conectados a esa red, acá observamos que la respuesta del servidor DHCP fue satisfactoria.

Ilustración 18: dual-stack PC30



En los PC no funciona diferente, seguimos entonces el mismo procedimiento que en el resto de equipos.

Ilustración 19: dual-stack PC31



Con esta gráfica, ya terminamos lo que sería la configuración a doble stack en la parte cliente.

2.9. Configuración dual-stack FastEthernet 0/0 de R3

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

Ahora, indicaremos cual es la configuración necesaria a realizar en 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. Por último habilitamos en la interfaz el IPv6 y declaramos el pool DHCP creado, a continuación el script:

```
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.

En este punto configuraremos los routers para que intercambien información de rutas y así los paquetes enviados desde los terminales, encuentren su destino, para ello, debemos habilitar el RIPv2 en el router y seguidamente, declarar las redes que puede ver directamente el router, no olvidamos guardar lo que configuramos con el comando write o copy running-config startup-config, para que la configuración almacenada suba nuevamente en caso de reinicio. A continuación, el script:

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

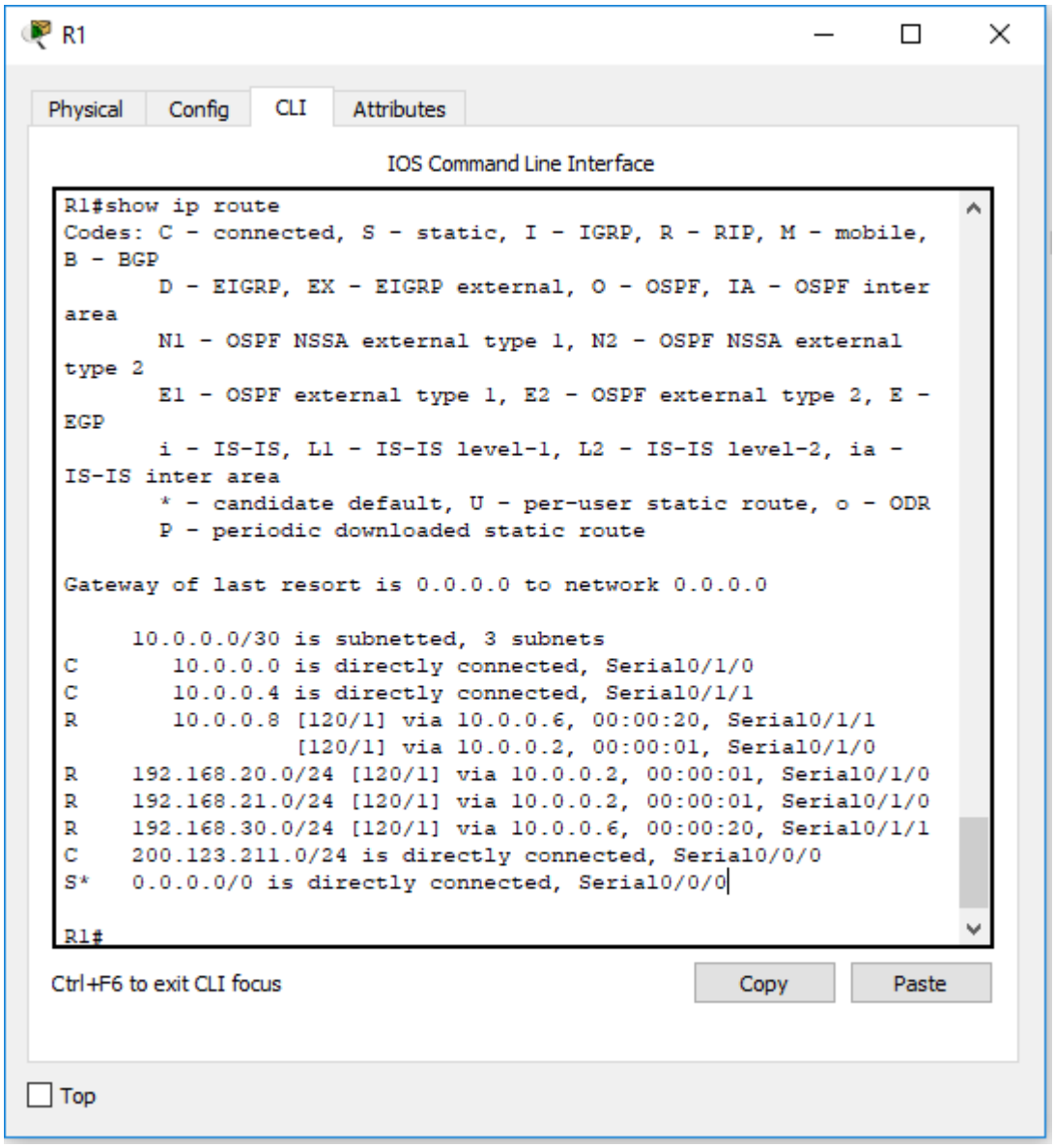
2.11. Consulta tabla de enrutamiento R1, R2 y R3

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

Ahora verificaremos que en las tablas de enrutamiento estén todas las redes que hemos configurado en cada uno de los routers, esto con el objetivo de tener la certeza que los paquetes van a llegar a destino sin necesidad de estar escribiendo las rutas una a una.

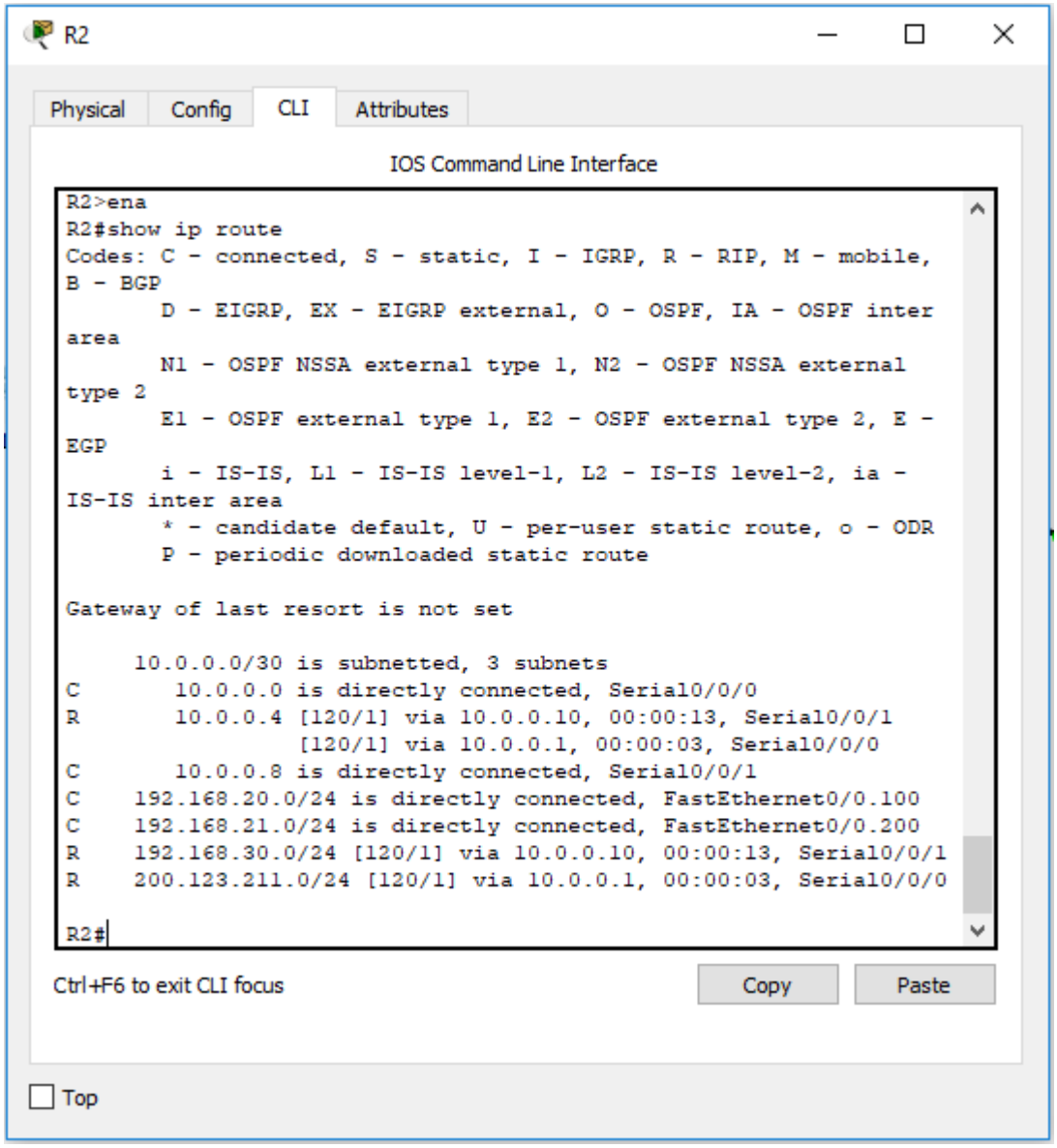
Cabe destacar que en RIPv1 y RIPv2 se utilizan saltos como métricas para determinar qué camino tomar para enrutar datos, ambos tienen un límite de 15 saltos (en pocas palabras 15 routers que pueden usar para llegar a un destino) al salto 16 el paquete es descartado. Su convergencia es lenta, donde las actualizaciones pueden tardar un poco en recibirse. Este protocolo es poco utilizado y se puede decir que se puede aplicar en empresas muy pequeñas.

Ilustración 20: Tabla de enrutamiento R1



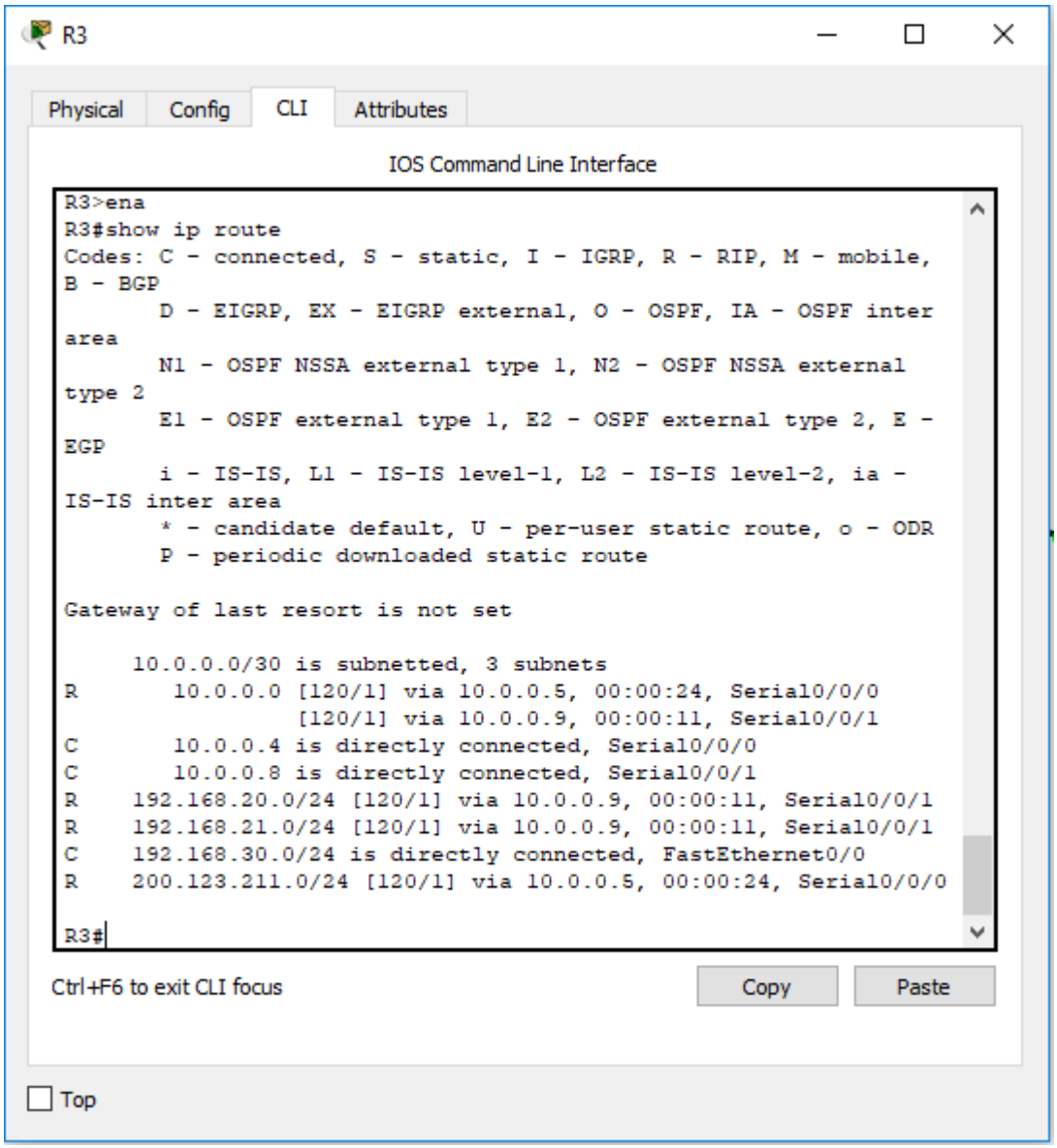
En esta ilustración visualizamos la tabla de enrutamiento de R1, y de como el router conoce las rutas directamente conectadas, pues son las que declaramos en el propio router, y las se adquirieron por RIP, para ello, al comienzo de cada línea hay una letra en mayúsculas, que indica cómo se adquirieron esas rutas, por ejemplo, si se obtuvo por RIP, la letra que le precede es R, si por el contrario es una ruta directamente conectada, le precede una C. Las rutas estáticas son las precedidas por la letra S y el asterisco, corresponde a una indicación que es la ruta candidata a ser la ruta por defecto.

Ilustración 21: Tabla de enrutamiento R2



En R2 observamos que son cuatro las rutas directamente conectadas y 3 las obtenidas por RIP.

Ilustración 22: Tabla de enrutamiento R3



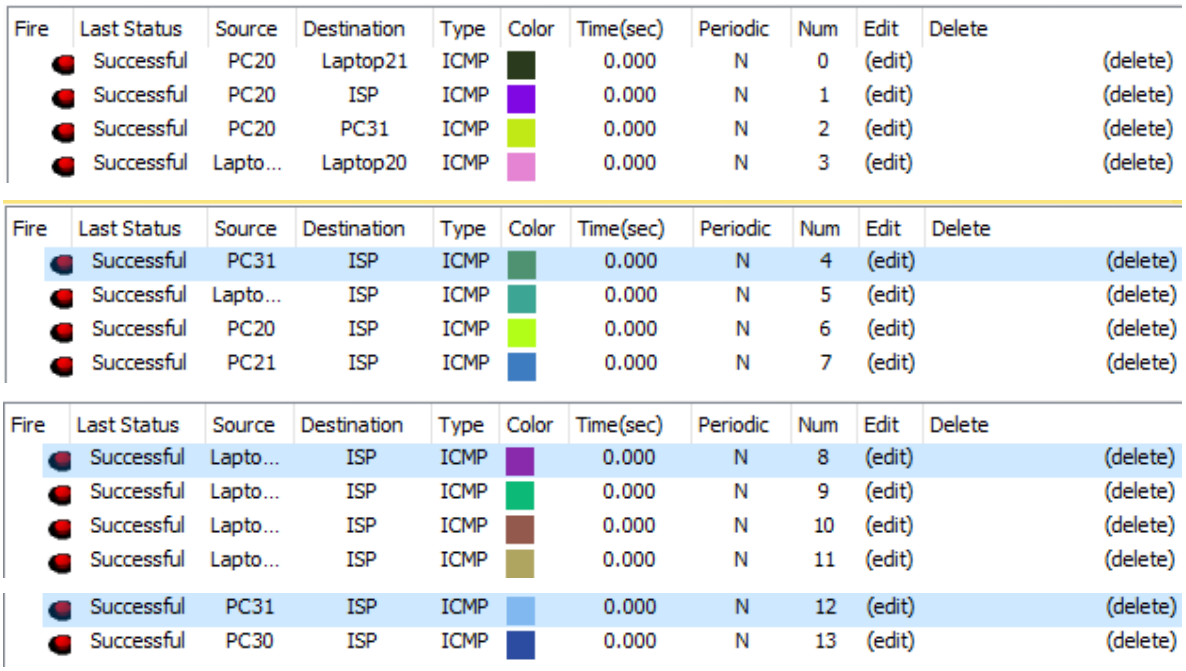
Así, nos damos cuenta que los routers involucrados en la topología implementadas, conocen las rutas necesarias para poder intercomunicar los diferentes terminales con el ISP o viceversa.

2.12. 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.

Finalmente hacemos pruebas de conectividad, entre los hosts y también entre los hosts y el ISP, para ello usamos el ambiente gráfico del propio Packet Tracert, aunque también se puede hacer desde el prompt en la pestaña Desktop de la ventana de configuración de cualquier pc o servidor.

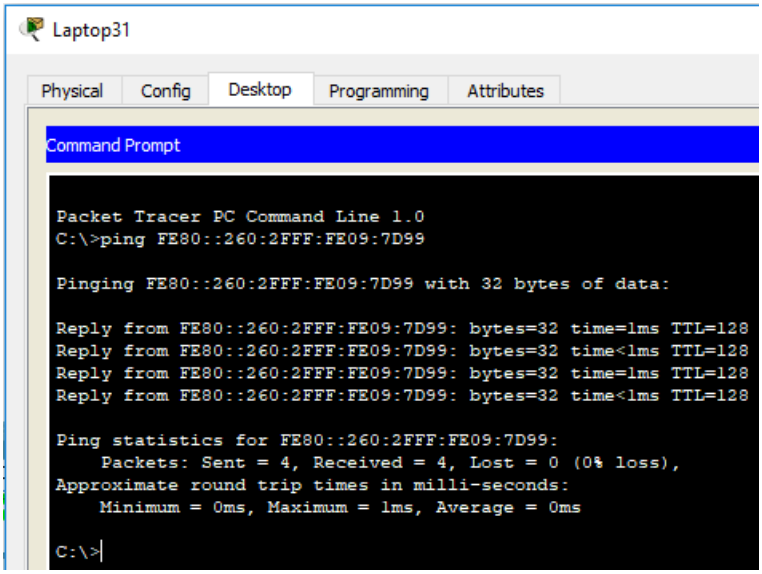
Ilustración 23: IPv4-ping



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC20	Laptop21	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC20	ISP	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC20	PC31	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Lapto...	Laptop20	ICMP		0.000	N	3	(edit)	(delete)
	Successful	PC31	ISP	ICMP		0.000	N	4	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP		0.000	N	5	(edit)	(delete)
	Successful	PC20	ISP	ICMP		0.000	N	6	(edit)	(delete)
	Successful	PC21	ISP	ICMP		0.000	N	7	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP		0.000	N	8	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP		0.000	N	9	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP		0.000	N	10	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP		0.000	N	11	(edit)	(delete)
	Successful	PC31	ISP	ICMP		0.000	N	12	(edit)	(delete)
	Successful	PC30	ISP	ICMP		0.000	N	13	(edit)	(delete)

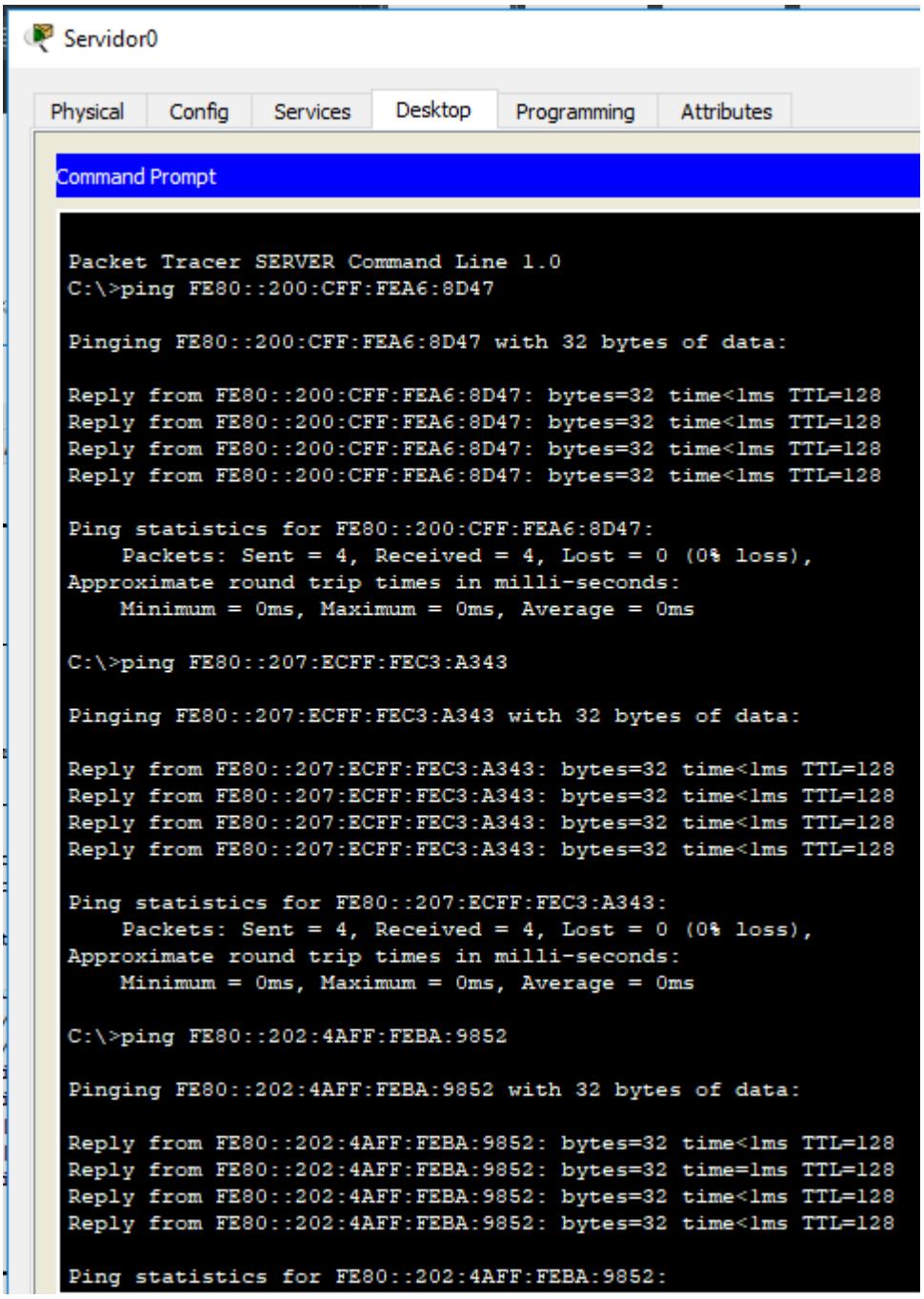
Las pruebas realizadas, nos demuestran que fue satisfactorio el ping hacia cualquiera de los terminales participantes de este escenario.

Ilustración 24: ping IPv6 de Laptop31 a Servidor0



Las pruebas de conectividad bajo IPv6, se deben hacer en el CMD ya que no es posible desde el ambiente gráfico, aunque, una vez más, fue satisfactoria la prueba, como lo observamos en la ilustración 24.

Ilustración 25: ping IPv6 desde Servidor0 a PCs

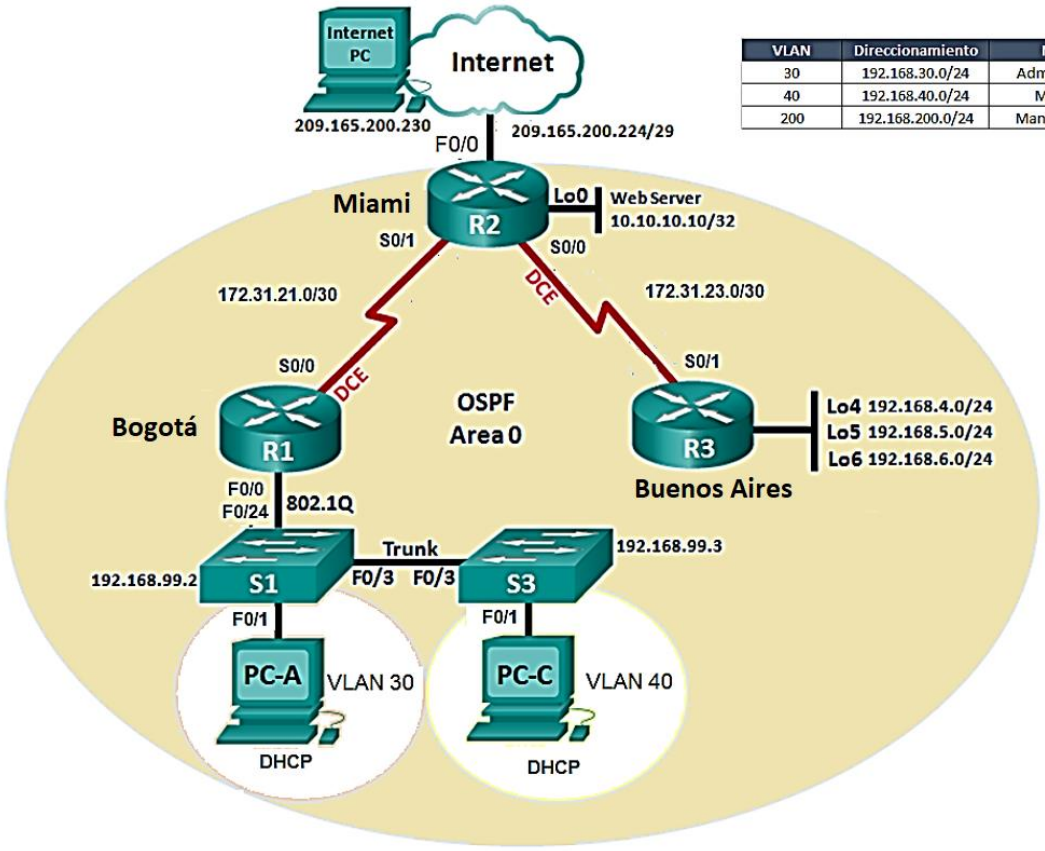


También realizamos pruebas desde el servidor y los terminales que pertenecen a su red, respondiendo satisfactoriamente con un TTL de 128, enviando un paquete de 32 bytes.

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 246: 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

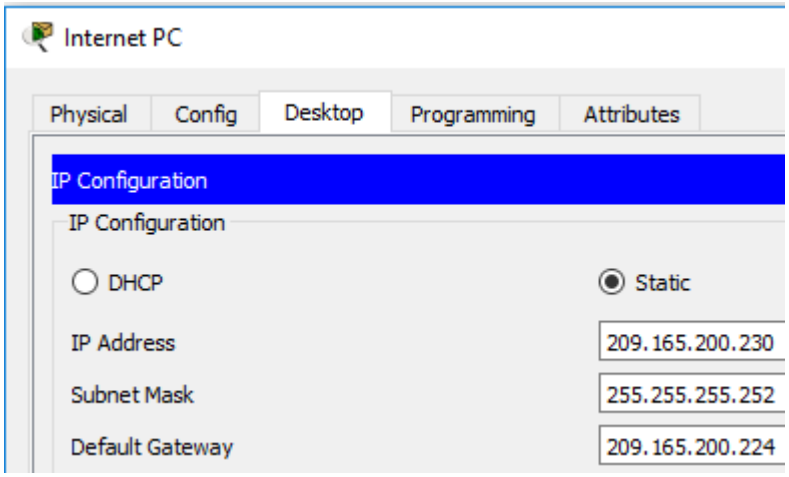
Para este escenario utilizaremos el protocolo OSPFv2 el más usado por los proveedores de internet, posee una rápida convergencia, entre otras ventajas, comenzaremos montando la topología solicitada y configurando el direccionamiento solicitado, para la red de mantenimiento, el tercer octeto, no coincide la tabla exhibida con el direccionamiento de los switches, por lo tanto realizaremos el direccionamiento basados en lo que se debe configurar en los switches el cual es 99.2 y 99.3, y como la práctica consiste en tener 3 redes separadas, se cumple igual si configuramos la 200 o la 99.

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.

Comenzamos acá con el direccionamiento en cada uno de los equipos, en orden de arriba abajo, se tiene el InternetPC, el cual 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 257: Direccionamiento Internet PC



Recordemos que debemos ponerla de manera estática, por defecto esa es la opción que viene seleccionada.

Seguimos con 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.

A continuación, 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 gestión:

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

Siguiendo con la implementación del escenario, configuramos el OSPFv2 para poder compartir tablas de enrutamiento, bajo los parámetros de la tabla 3, comenzamos en R1, iniciamos declarando 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 vera través de las interfaces que participan en el proceso, posteriormente entramos en la interfaz que la tabla indica para colocar el ancho de banda, finalmente aplicamos el costo del enlace, a continuación se indica el CLI para implementar 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

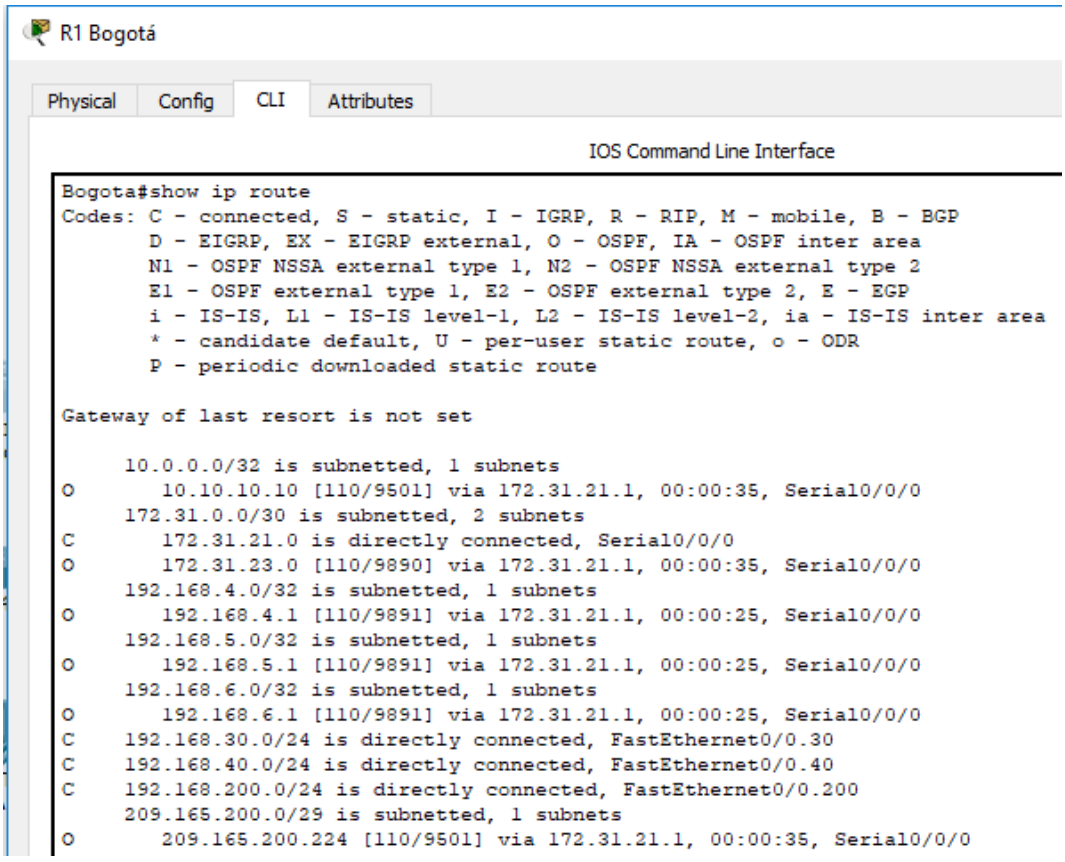
write

3.3. Verificación información OSPF

Visualizar tablas de enrutamiento y routers conectados por OSPFv2

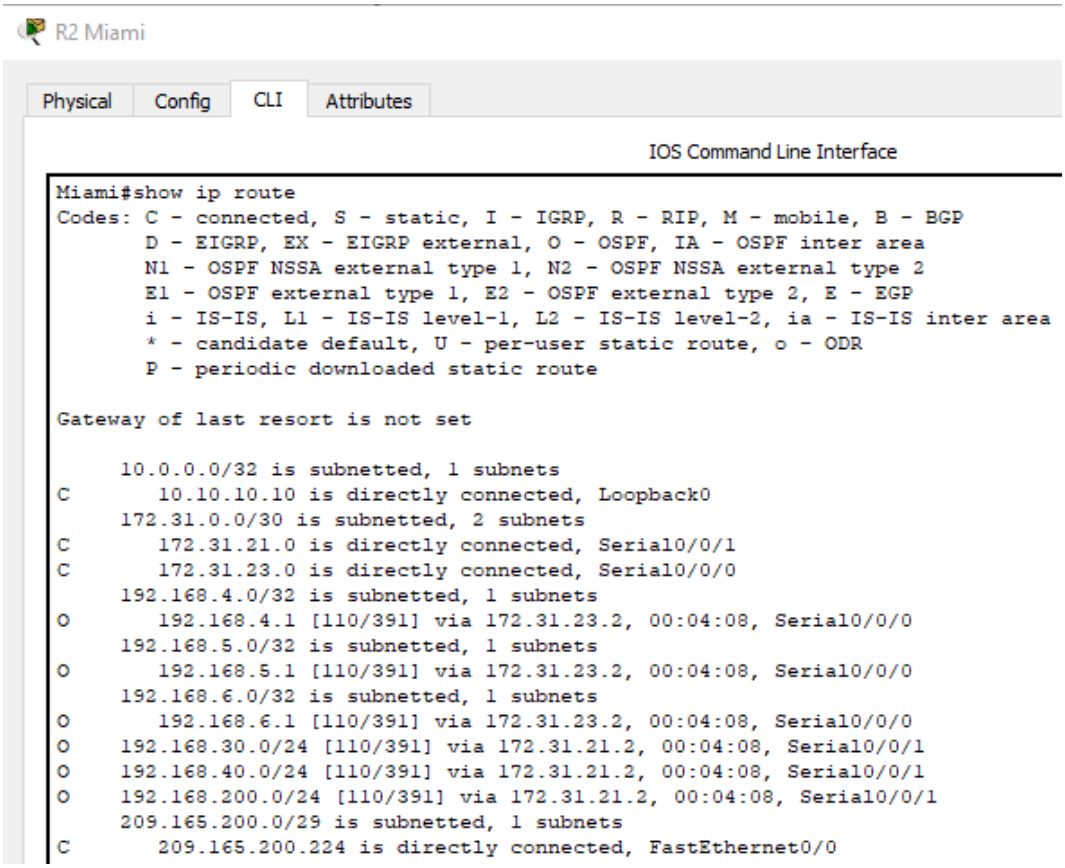
Una vez realizado el punto anterior, podemos verificar las tablas de enrutamiento de cada router, para confirmar que los equipos involucrados estén compartiendo las tablas:

Ilustración 268: Verificación routing table R1



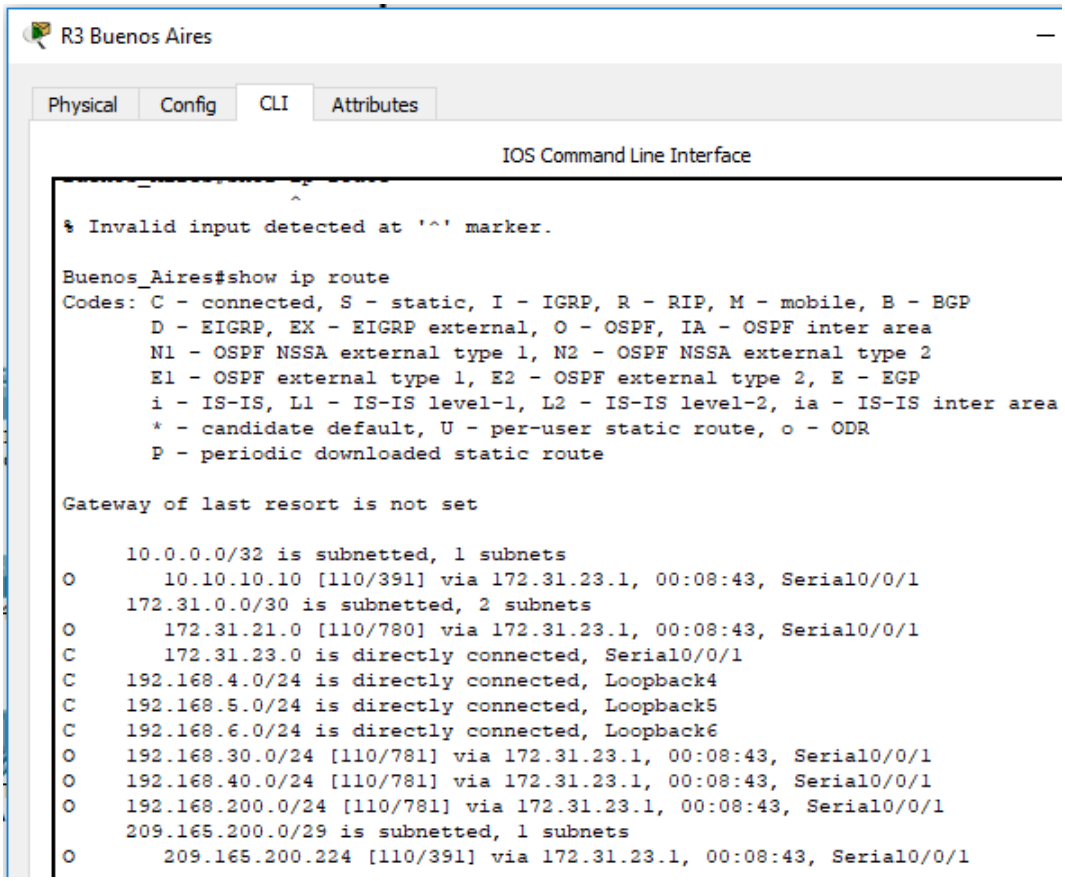
En esta imagen, empleando el comando show ip route, se observan cada una de las rutas utilizadas por el router, y de las cuales 6 se obtuvieron por OSPF, cuatro de ellas con las que están directamente conectadas al router.

Ilustración 29: Verificación routing table R2



En esta parte encontramos que el router encontró 6 redes a través de OSPF y tiene 4 conectadas directamente.

Ilustración 30: Verificación routing table R3

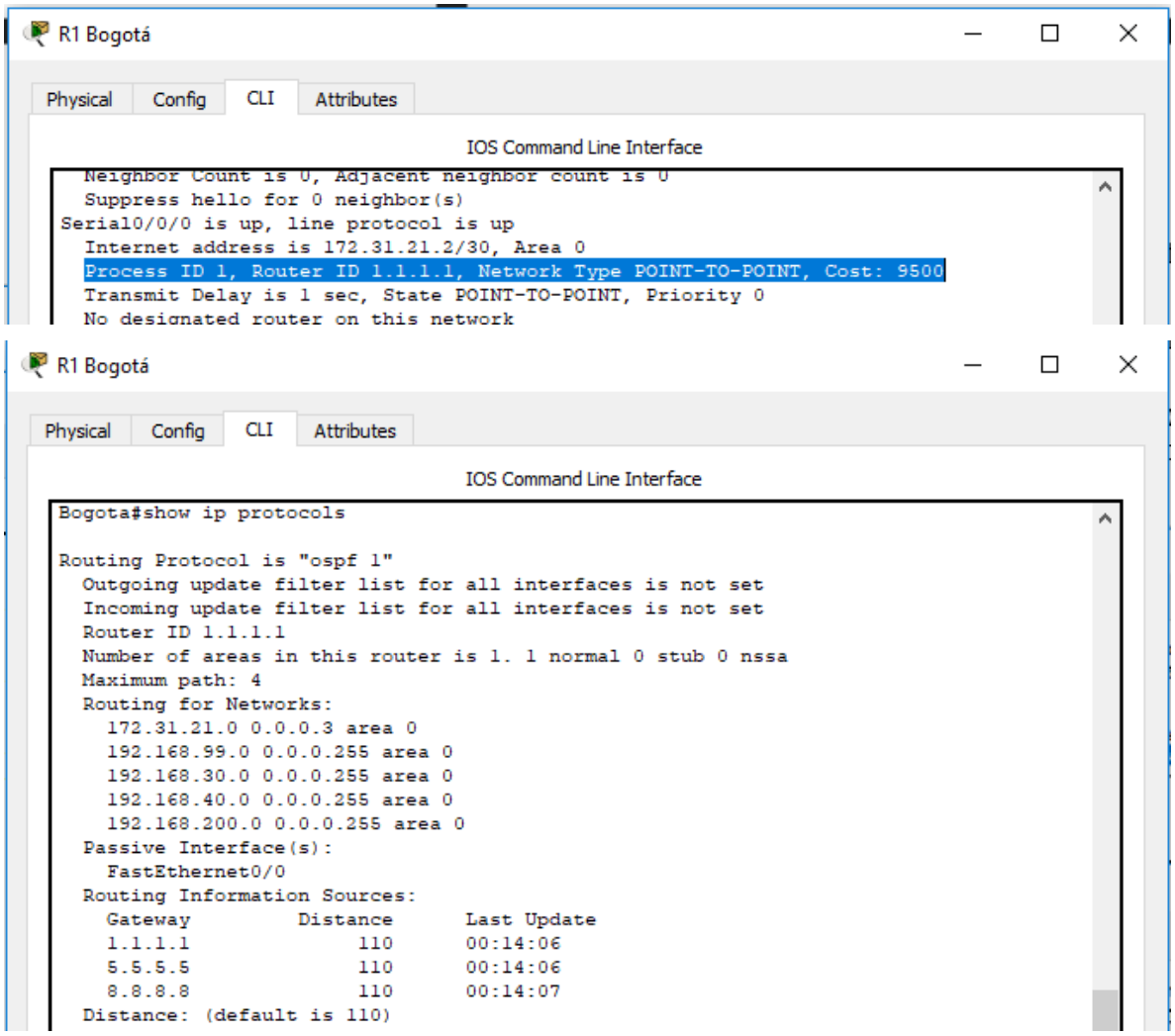


En esta última figura se observa que el router 3 obtiene igualmente 6 redes por OSPF.

- 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.

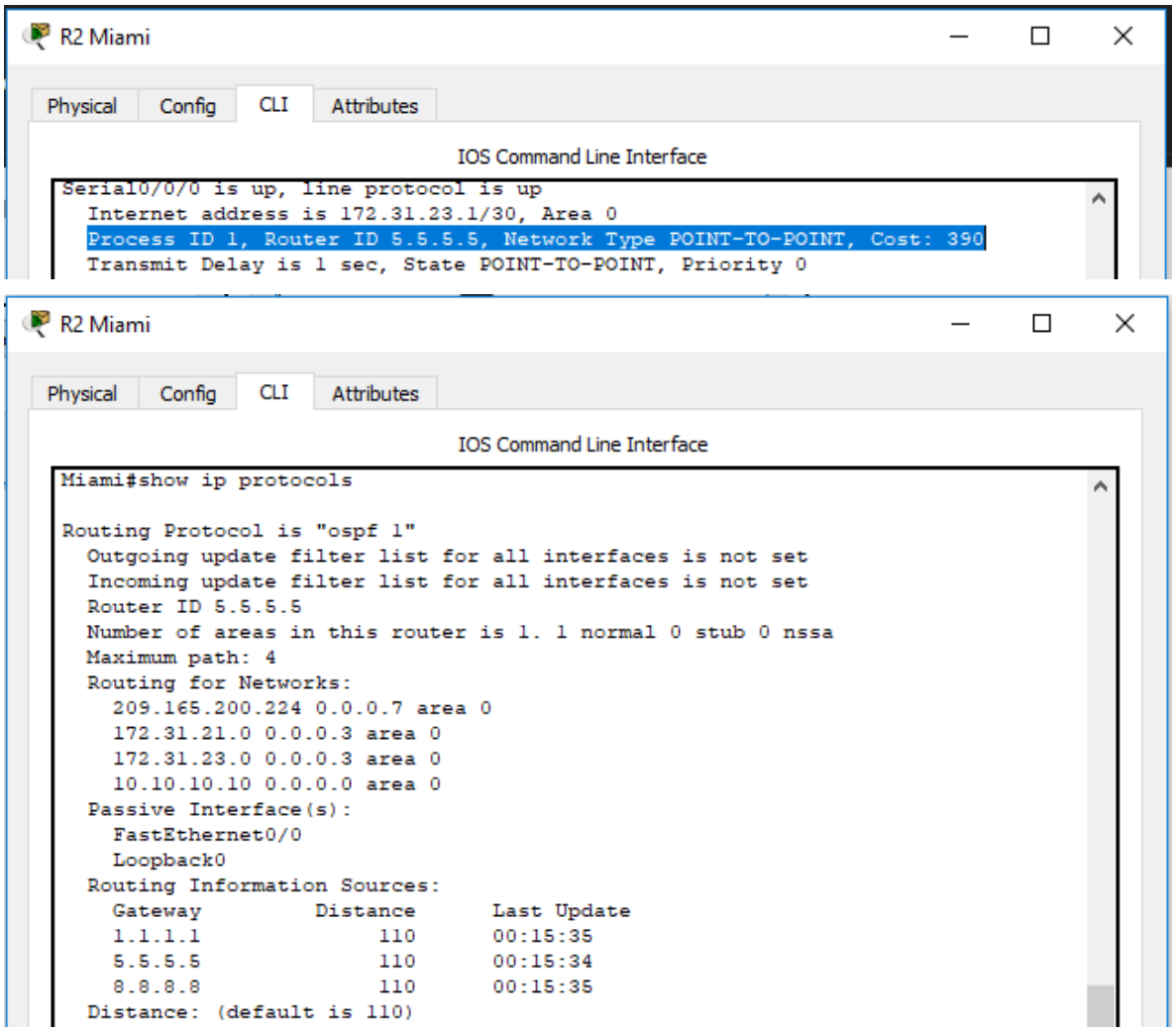
Para poder visualizar lo solicitado, aplicamos los comandos **show ip ospf interface** y **show ip protocols**, a continuación, los pantallazos de demostración de la información solicitada al router:

Ilustración 31: Verificación en R1



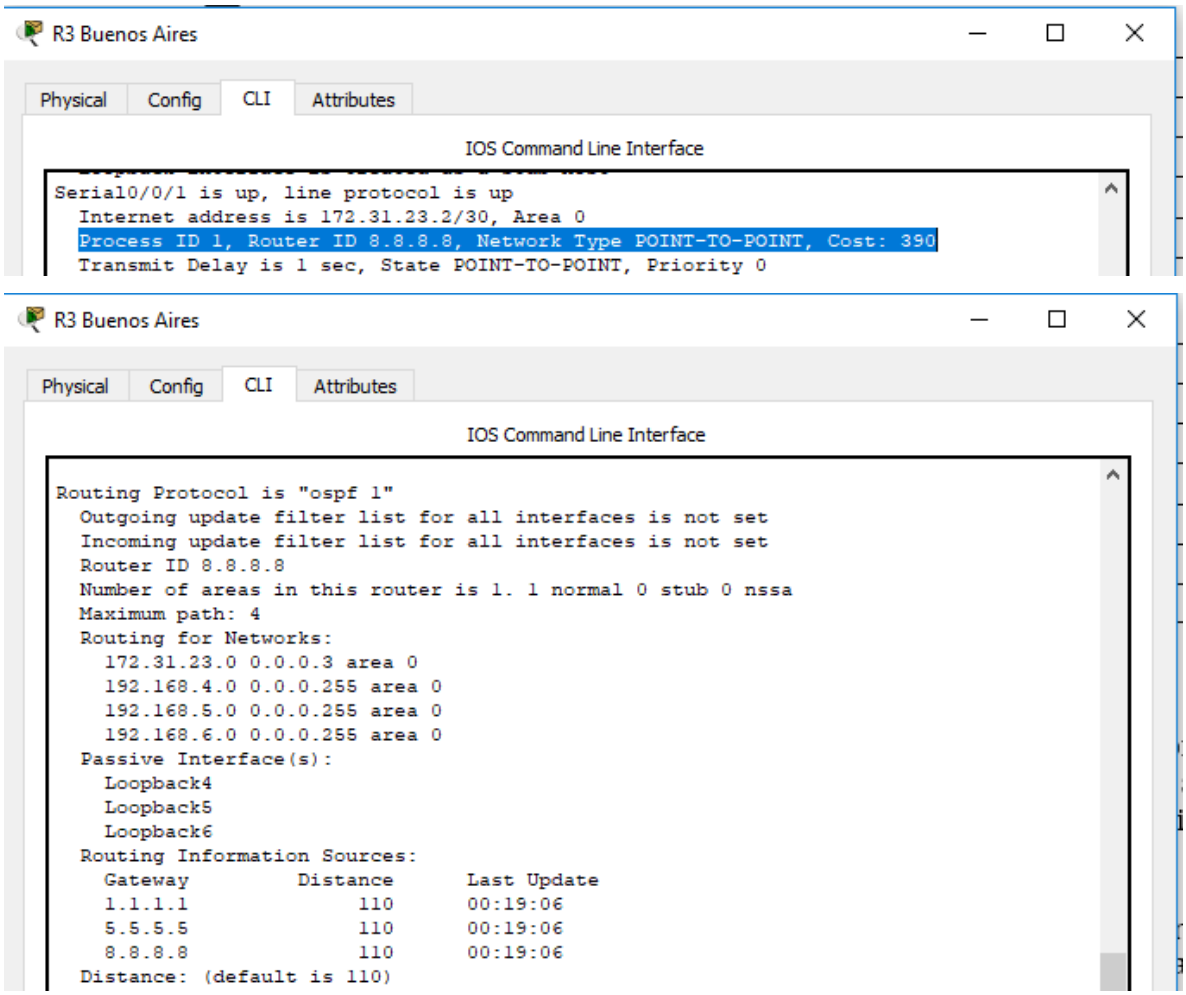
En esta imagen visualizamos el costo, el ID del router, el ID del proceso, las interfaces pasivas y las redes enrutadas.

Ilustración 32: Verificación en R2



Hacemos los mismo en cada router para comprobar que todo esté según lo solicitado en la guía.

Ilustración 273: Verificación en R3



Por último completamos la tarea con el 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, debemos nombrar las vlan, no es necesario el InterVLAN en el switch, ya que en el router se lleva a cabo ese proceso, luego entramos en las interfaces troncales, las declaramos como tal, asignamos los puertos a las vlan indicadas y las que queden libres las apagamos, por último, configuramos la seguridad del switch, a continuación, el script para eso:

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 DNS lookup

En el Switch 3 deshabilitar DNS lookup

Como sabemos, 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. Asignación de direcciones IP a los switches

Asignar direcciones IP a los Switches acorde a los lineamientos.

En los puntos anteriores ya habíamos explicado la configuración del direccionamiento de los switch, esto es requerido, ya que a través de conexiones virtuales podemos acceder de manera remota, a continuación, el script:

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, este lineamiento debe ser configurado, así evitamos fallas provocadas por personas no entrenadas en la ingeniería de redes, 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.

Seguidamente, configuraremos el servicio de DHCP para las VLAN 30 y 40, sin olvidar antes reservar 30 direcciones para configuraciones estáticas, a continuación, el script:

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 NAT

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

Unas vez más, como en la implementación anterior, 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 de siempre, 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 nuestro NAT para salir a internet. A continuación, el script:

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

- 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.

Como sabemos, las listas de acceso, las podemos comparar a una lista de compras, en la cual se indica quien puede pasar y quien no, en las de tipo estándar se indica el host al que se permite o se le niega el acceso y en las listas extendidas se da un origen y un destino, a continuación el script:

enable

configure terminal

ip access-list standard lista_uno

permit 192.168.30.0 0.0.0.255

deny 192.168.40.0 0.0.0.255

ip access-list standard lista_dos

deny 192.168.30.0 0.0.0.255

permit 192.168.40.0 0.0.0.255

ip access-list extended lista_tres

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 lista_cuatro

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

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

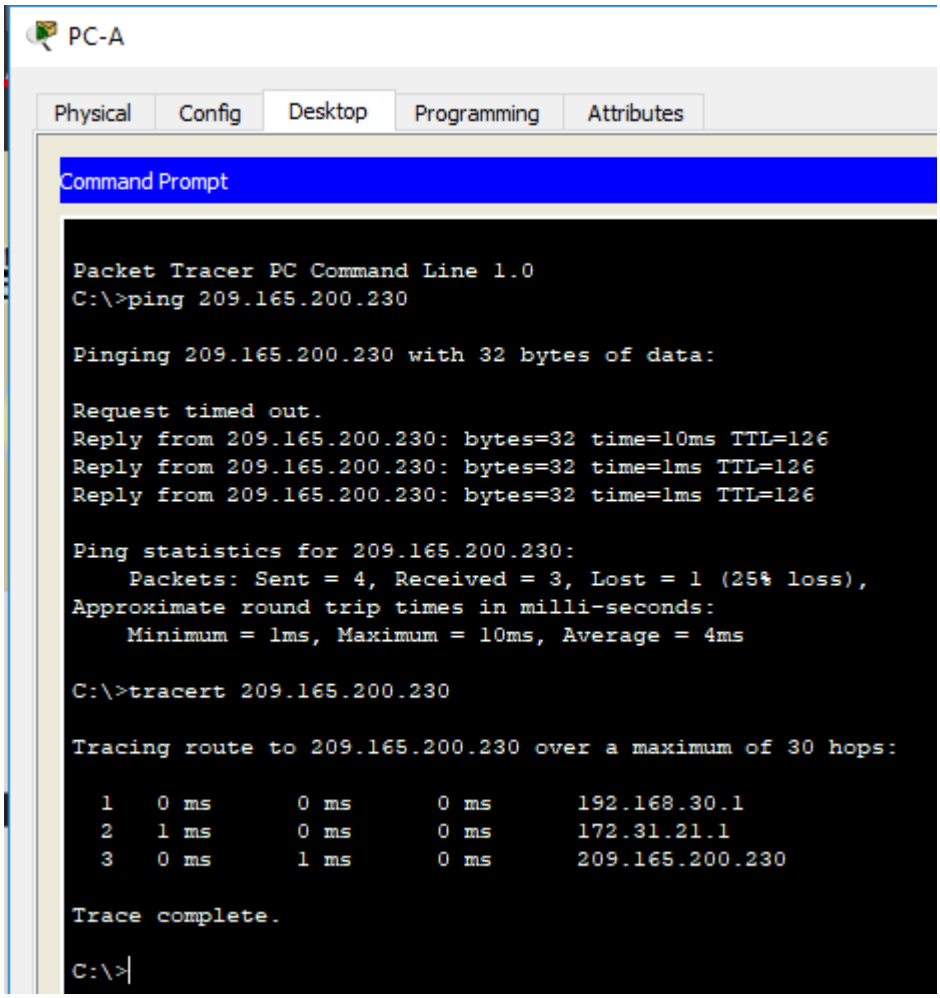
3.11. Verificación comunicación

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, pero si por alguna razón, el ping no alcanza el destino, podemos usar tracert para comprobar en cual salto se quedó y así tomar decisiones sobre que hacer para solucionar el problema.

Desde PC-A:

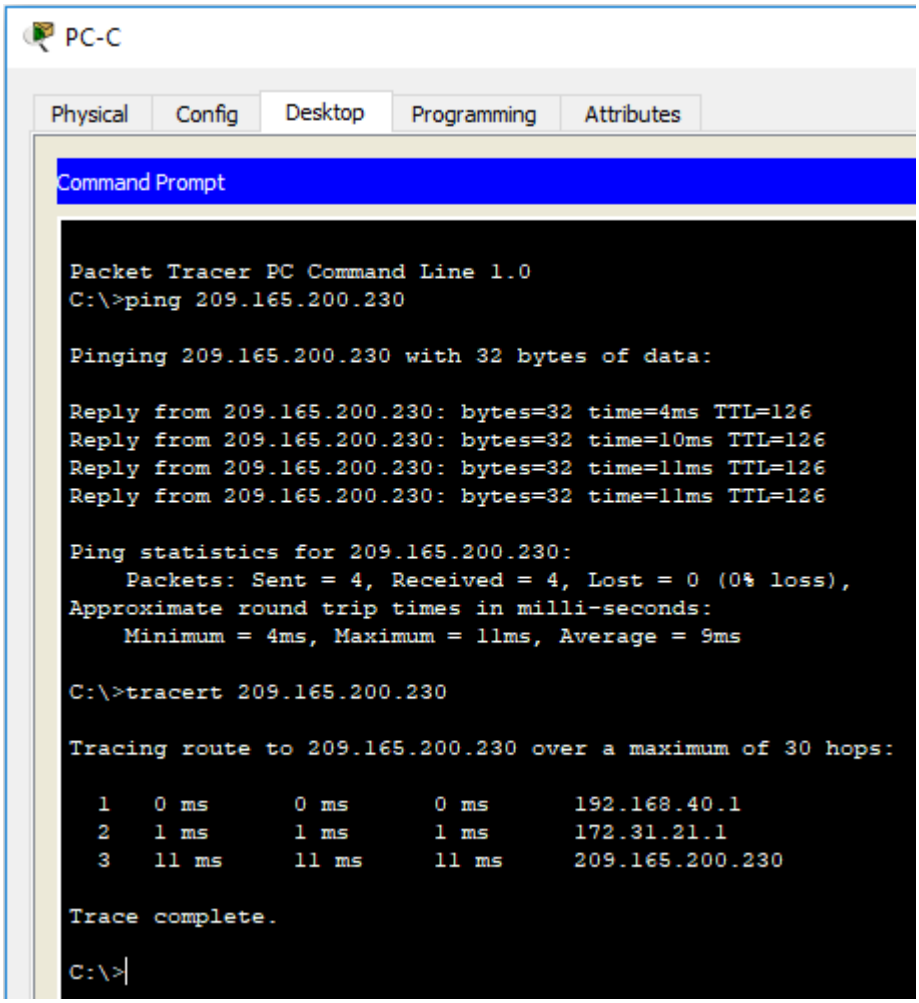
Ilustración 284: PC-A pruebas de conectividad



Como podemos apreciar en esta imagen, 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 295: PC-C pruebas de conectividad



Los mismo realizamos con el PC-C y funcionó de la misma forma, lo que confirma que la implementación está realizada de forma adecuada para permitir que haya comunicación fluida en la misma.

CONCLUSIONES

Este documento consolida la actividad de la prueba de habilidades práctica final, en el desarrollo de acuerdo al caso de estudio dado, se ha aplicado los conocimientos proporcionados en el material de apoyo emanado por la empresa CISCO en el desarrollo del aprendizaje autónomo promovido para este tipo de ambientes virtuales.

Se logró una satisfactoria conexión, configuración y simulación de los dispositivos de la red en el correspondiente caso de estudio.

En general se expresa satisfacción por el aprendizaje adquirido durante el desarrollo del curso y la aplicación de la teoría vista en la plataforma cisco, obteniendo grandes conocimientos en mi desarrollo profesional.

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.).