EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

FRANKLIN JOAN PUENTES MORALES

Diplomado CCNA
como opción de grado

Instructor: EFRAIN ALEJANDRO PEREZ

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

Contenido

Introducción

Las comunicaciones forman parte del apasionante mundo de las tecnologías de la información, sin ellas no existiría la información “al alcance de la mano” han hecho posible que el mundo entero se vuelva muy pequeño, no es necesario estar físicamente en ningún lado, solo, con ingresar en un terminal, ya tenemos acceso al más recóndito de los lugares, ese es el poder que nos otorgan los las redes de comunicación.

El presente trabajo, nos pone a prueba para hacer dos implementaciones, sobre 2 escenarios, en el primero realizaremos prácticas sobre nateo, enrutamiento dinámico con RIP versión 2, además servicio de DHCP en versión IPv4 e IPv6, para el escenario 2, haremos enrutamiento dinámico con OSPFv2 DHCP v4, listas de acceso y nateo entre otros.

1. Escenario 1

Ilustración 1: Escenario 1

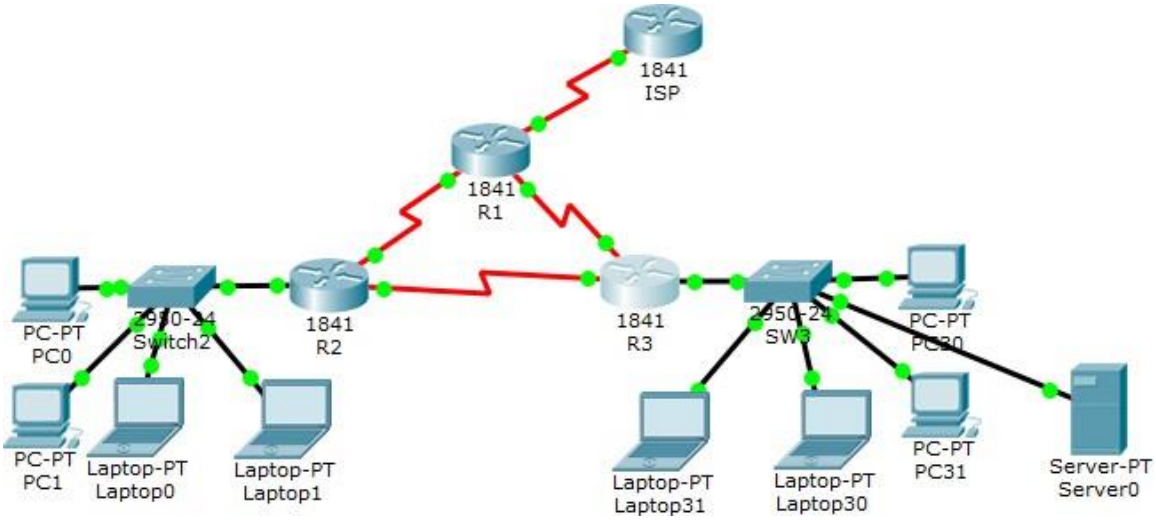


Tabla 1: Tabla de direccionamiento

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 VLAN y de puertos

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 este primer escenario, comenzaremos realizando el montaje de la topología como aparece en la ilustración 1, luego, configuraremos el direccionamiento según indica la tabla 1, se usará protocolo de enrutamiento RIPv2 para compartir tablas de enrutamiento, y para dar direccionamiento, en los routers de los extremos se configurará el servicio de DHCP en versión 4 y 6.

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.

El primer paso en esta línea de configuración es realizar las configuraciones iniciales como son darle un nombre a cada equipo de los que pertenecen a la red, luego, ingresar a la interface requerida y darle el carácter que le corresponde, por ejemplo, si es troncal, ya que el switch utilizado es un 2960, es solo declararla como “mode trunk” e inmediatamente esa interfaz dejará pasar todas las VLAN, creamos las VLAN 100 y la 200, luego, ingresamos a las interfaces indicadas en la topología, dedicadas a los terminales y las asignamos a las VLAN respectivas, las interfaces que no se usen, las apagamos mediante el comando shutdown, para todo lo anterior, usaremos la siguiente línea de comandos:

```
ena
config ter
host SW2
inter f0/1
switchport mode trunk
vlan 100
vlan 200
inter f0/2
switchport access vlan 100
switchport mode access
inter f0/3
switchport access vlan 100
switchport mode access
inter f0/4
switchport access vlan 200
switchport mode access
inter f0/5
switchport access vlan 200
switchport mode access
```

inter range f0/6-24

shutdown

end

copy running-config startup-config

2.2. Direccionamiento IP ISP, R1, R2 y R3

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

Ahora realizaremos el direccionamiento, según la tabla 1, como sabemos, en los routers las interfaces por defecto, está apagadas, no hay que olvidar levantarlas con el comando “no shutdown” y luego de configura, usaremos la siguiente línea de comandos:

Para ISP

ena

config ter

hostname ISP

inter s0/0/0

ip addr 200.123.211.1 255.255.255.0

end

copy running-config startup-config

Para R1:

ena

conf ter

host R1

inter s0/0/0

ip addr 200.123.211.2 255.255.255.0

no shut

inter s0/1/0

ip addr 10.0.0.1 255.255.255.252

no shut

inter s0/1/1

ip addr 10.0.0.5 255.255.255.252
no shut
end
copy running-config startup-config

Para R2:

ena
conf ter
host R2
inter f0/0
no shut
inter f0/0.100
encapsulation dot1Q 100
ip addr 192.168.20.1 255.255.255.0
inter f0/0.200
encapsulation dot1Q 200
ip address 192.168.21.1 255.255.255.0
inter s0/0/0
ip addr 10.0.0.2 255.255.255.252
no shut
inter Serial0/0/1
ip address 10.0.0.9 255.255.255.252
no shut
end
copy running-config startup-config

Para R3:

ena
conf ter
host R3
inter f0/0

ip addr 192.168.30.1 255.255.255.0

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

ipv6 enable

no shut

inter s0/0/0

ip addr 10.0.0.6 255.255.255.252

inter s0/0/1

ip addr 10.0.0.10 255.255.255.252

no shut

end

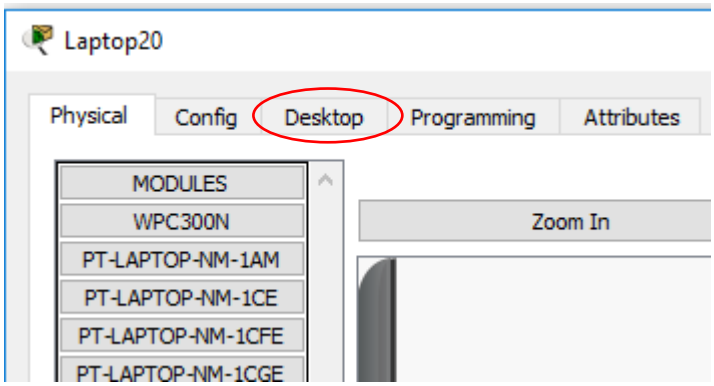
copy running-config startup-config

2.3. Configuración DHCP en host

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

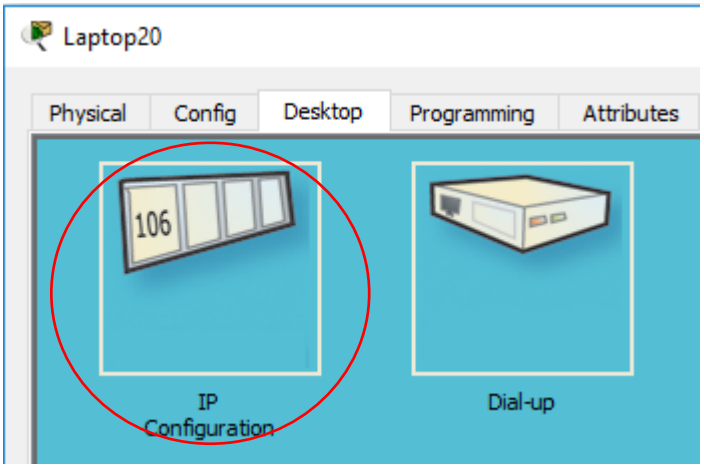
Las configuraciones para esta parte se realizan de la siguiente forma:

Ilustración 2: Ventana de configuración Laptop20



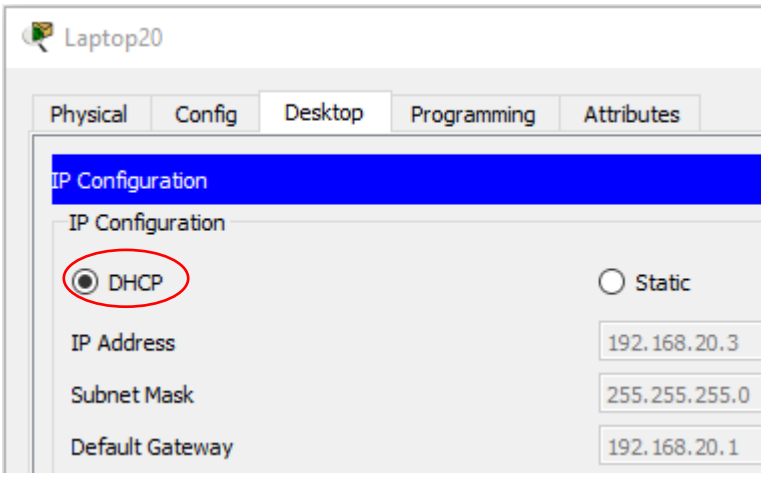
Hacemos click en la pestaña Desktop del cuadro de configuración del PC.

Ilustración 3: ícono IP Configuration



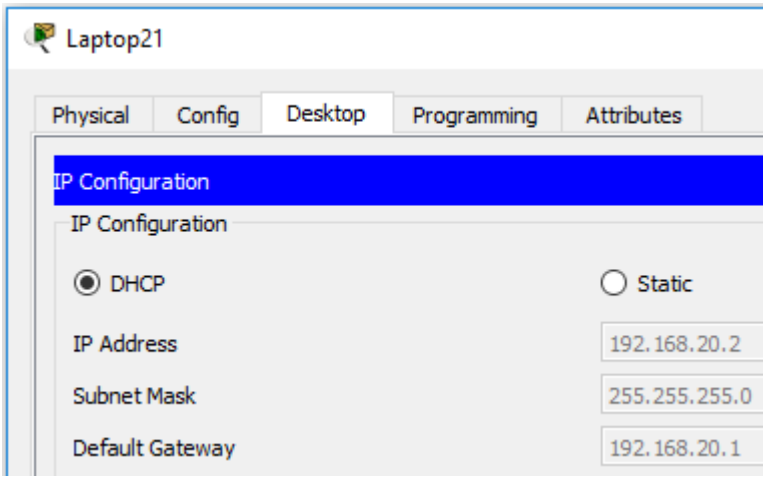
Seleccionamos el ícono de configuración de IP.

Ilustración 4: Laptop20 selección opción DHCP



Finalmente hacemos click en la opción DHCP, si hay un servidor recibiendo peticiones, le devolverá el direccionamiento, tal como ocurre en la gráfica.

Ilustración 5: Laptop21



Realizamos el mismo procedimiento para todos los host.

Ilustración 6: PC20

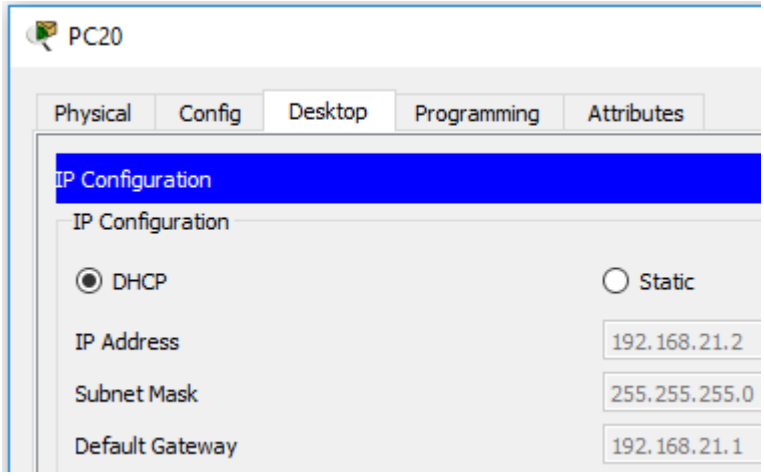


Ilustración 7: PC21

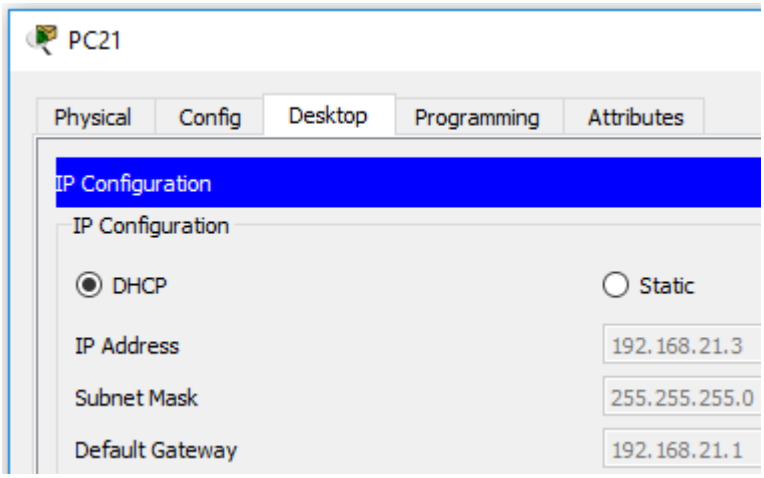


Ilustración 8: Laptop30

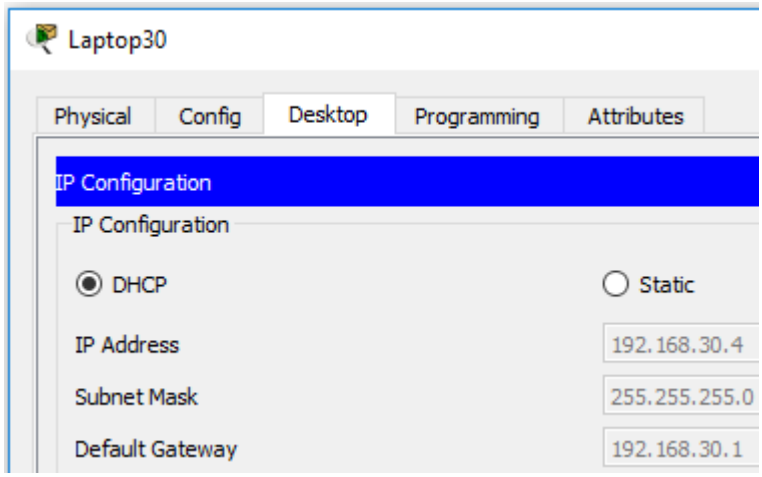


Ilustración 9: Laptop31

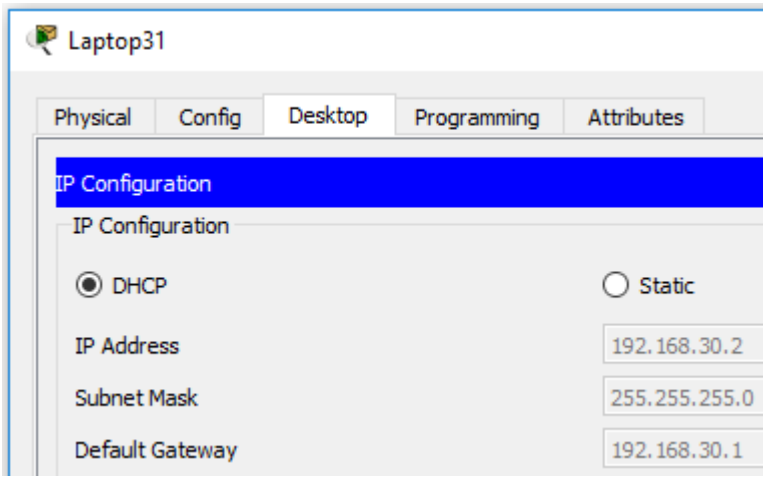


Ilustración 10: PC30

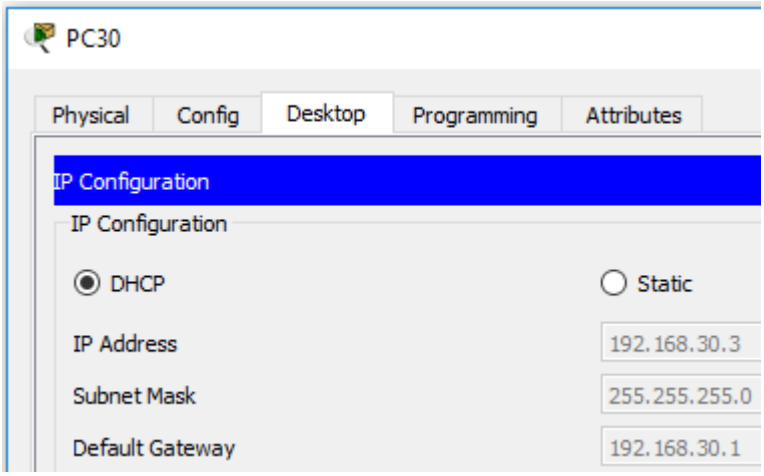
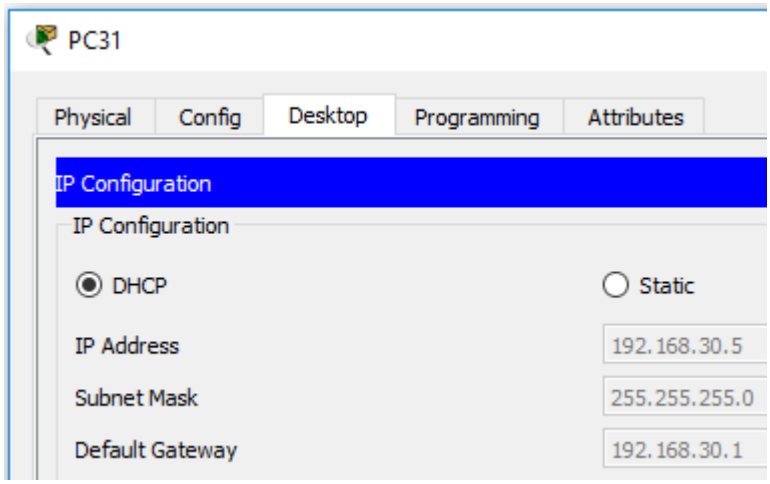


Ilustración 11: PC31



Todos recibieron direccionamiento, porque el servicio de DHCP solicitado por la guía ya se encuentra operando, más adelante realizaremos la explicación de esa configuración.

2.4. Configuración 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**.

El NAT que realizaremos a continuación es comúnmente llamado PAT, es el NAT con sobrecarga que se usa para salir a internet por lo general, aunque existen otros tipos de NAT como por ejemplo el NAT 1:1 es usado para servidores u otros dispositivos que deben quedar de cara a internet, es decir, la dirección pública, debe llegar a la red interna a un host específico. Para configurarlo, debemos, primero que nada, crear una lista de acceso, en la cual se indique cuales redes van a salir a internet, luego se indica la línea de NAT la cual lleva el origen, la lista y la interfaz por la cual saldrá, seguidamente, se declaran las interfaces de entra y salida, y de esta manera la red queda con acceso a internet.

Para realizar esta configuración, esta es la línea de comandos:

```
ena
config ter
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

inter s0/0/0

ip nat outside

inter s0/1/0

ip nat inside

inter s0/1/1

ip nat inside

end

copy running-config startup-config

Ahora hacemos pruebas de conectividad mediante el uso del ping o el ambiente gráfico de PT.

Ilustración 12: 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	PC30	ISP	ICMP		0.000	N	4	(edit)	(delete)
	Successful	PC31	ISP	ICMP		0.000	N	5	(edit)	(delete)
	Successful	Laptop30	ISP	ICMP		0.000	N	6	(edit)	(delete)
	Successful	Laptop31	ISP	ICMP		0.000	N	7	(edit)	(delete)

Tal como lo observamos, gracias al NAT con sobrecarga, fue posible alcanzar al ISP.

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.

Configuramos la ruta estática, ya que, con ella, podemos alcanzar direccionamiento que no se encuentre en nuestra red, por eso, todo lo que no esté en la tabla de enrutamiento, va a salir por la interfaz s0/0/0 de R1, digitamos la siguiente línea de comando:

ena

conf ter

```
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
end
copy running-config startup-config
```

2.6. Configuración de DHCP en R2

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

Con el DHCP en R2, damos direccionamiento a los equipos que dependen de él, realizamos la configuración router on stick, para poder pasar a través de una misma interfaz del router, 2 VLAN, las cuales son, las VLAN 100 y 200, a continuación, la línea de comandos que se aplica para ese servicio:

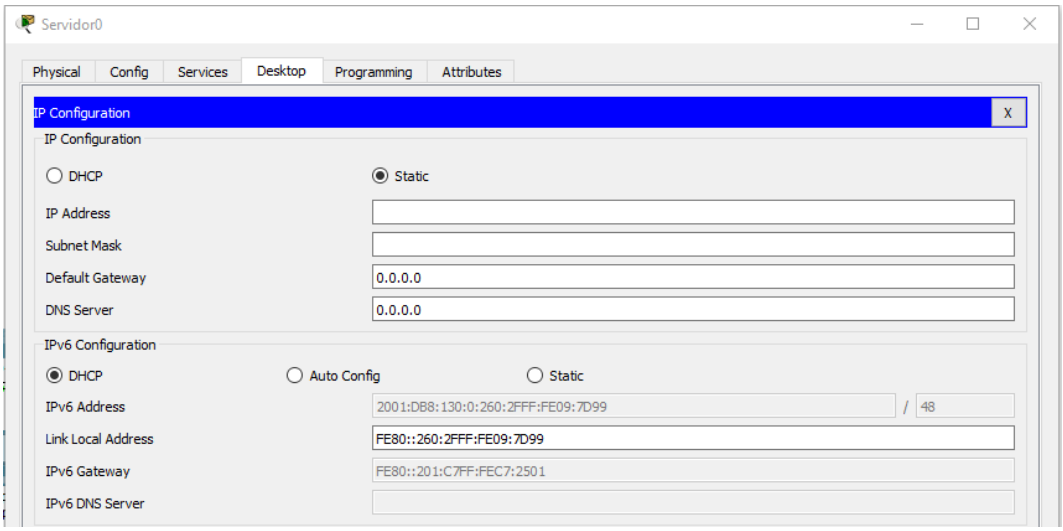
```
ena
conf ter
ip dhcp pool vlan_100
network 192.168.20.0 255.255.255.0
default-router 192.168.20.1
ip dhcp pool vlan_200
network 192.168.21.0 255.255.255.0
default-router 192.168.21.1
end
copy running-config startup-config
```

2.7. Pruebas de ping Servidor0

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

De la misma manera que realizamos la configuración para DHCP, ahora lo hacemos para versión 6:

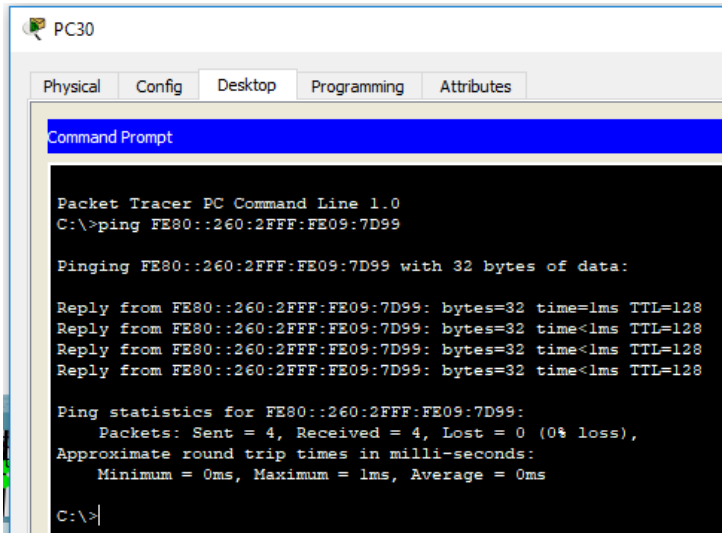
Ilustración 13: Dirección IPv6 Servidor0 tomada por DHCPv6



De esta forma, obtenemos el DHCPv6 ya que la guía indica que debe ser tomada por este medio la configuración de direccionamiento para este servidor.

Ahora realizamos pruebas de conectividad en IPv6:

Ilustración 14: ping IPv6 de PC30 a Servidor0



La prueba es satisfactoria, así, seguimos realizando pruebas a todos los hosts que dependen de ese router:

Ilustración 15: ping IPv6 de PC31 a Servidor0

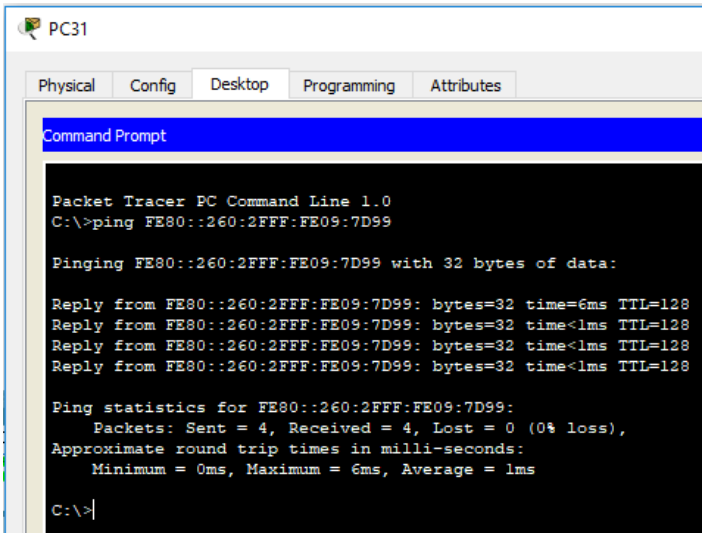


Ilustración 16: ping IPv6 de Laptop30 a Servidor0

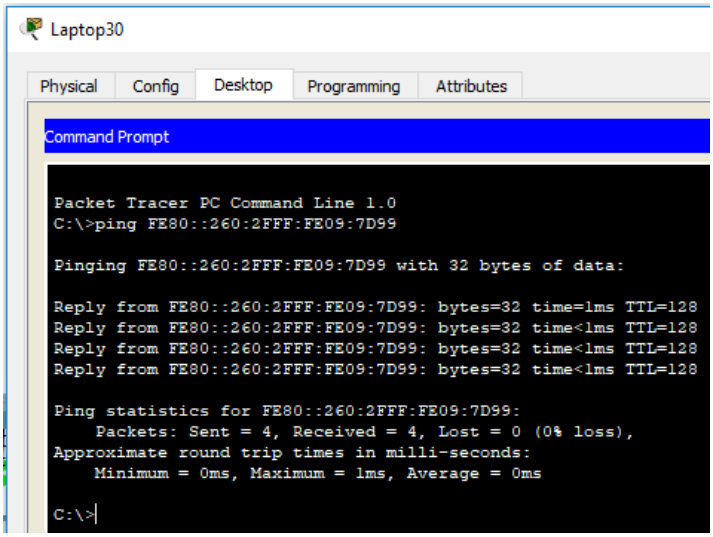
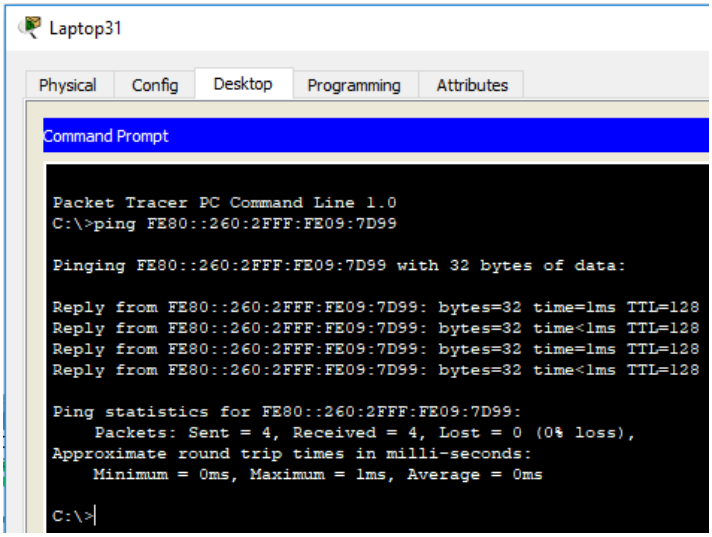


Ilustración 17: ping IPv6 de Laptop31 a Servidor0

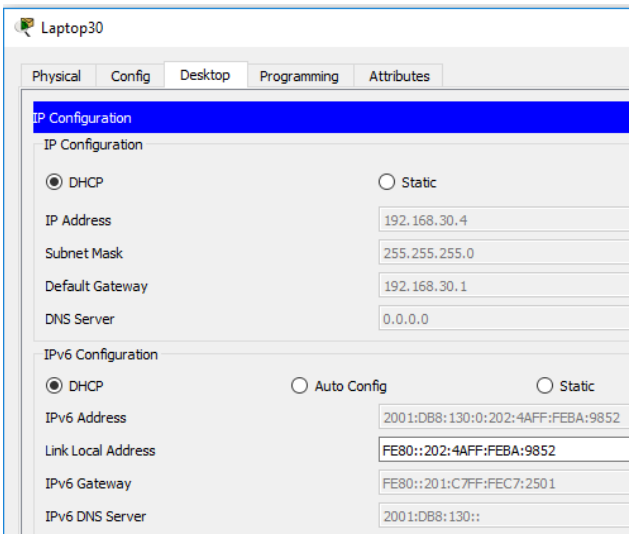


2.8. Configuración dual-stack en las NIC de los terminales red 30

- 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.

Configuramos ahora el doble stack en las tarjetas de red de los Laptops y PC pertenecientes a esa red:

Ilustración 18: dual-stack Laptop30



Se observa que ya ha tomado el direccionamiento requerido, ya que hay un servicio de DHCP arriba en ese router.

Ilustración 19: dual-stack Laptop31

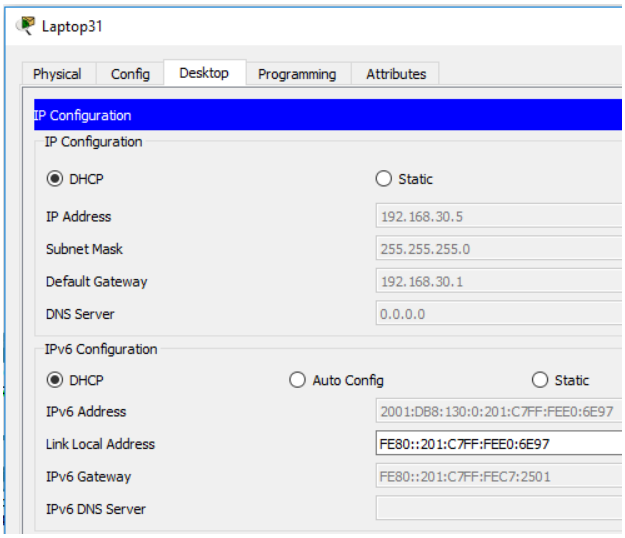
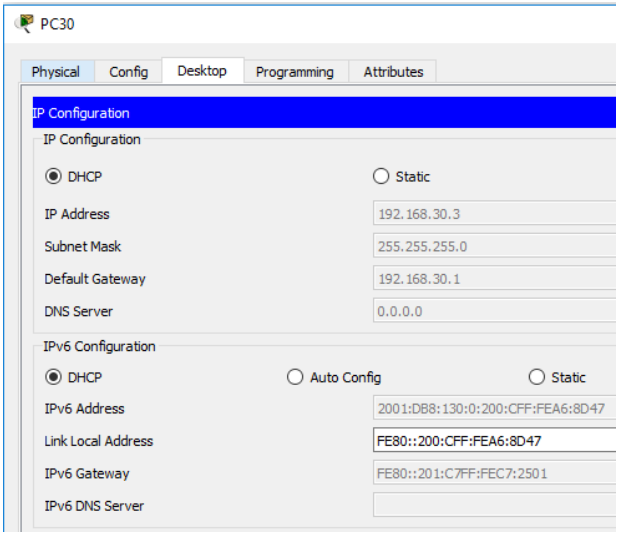
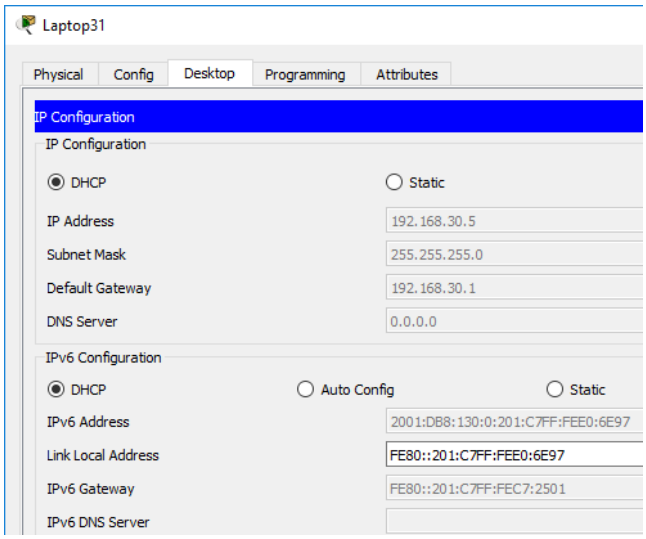


Ilustración 20: dual-stack PC30



Todos los equipos han tomado el double-stack

Ilustración 21: dual-stack PC31



Y así finalizamos la configuración requerida.

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).

Para que funcione nuestro direccionamiento, debemos implementar un servicio de este tipo, primero nos vamos a la interfaz que va intervenir en ese proceso y le damos direccionamiento, esta es la línea de comando empleada para tal fin:

```
ena
conf ter
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

copy running-config startup-config

2.10. Configuración RIPv2 en R1, R2 Y R3

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

Ahora, lo que necesitamos para que todas las redes del escenario se comuniquen, es el enrutamiento, puede ser estático o dinámico, par este caso usaremos RIPv2, el cual es un protocolo de enrutamiento vector distancia, más empleado para redes pequeñas, para realizar esta configuración, debemos habilitar el protocolo y luego declarar la redes que el router puede ver a través de sus interfaces, a continuación la línea de comandos empleada para esta tarea:

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

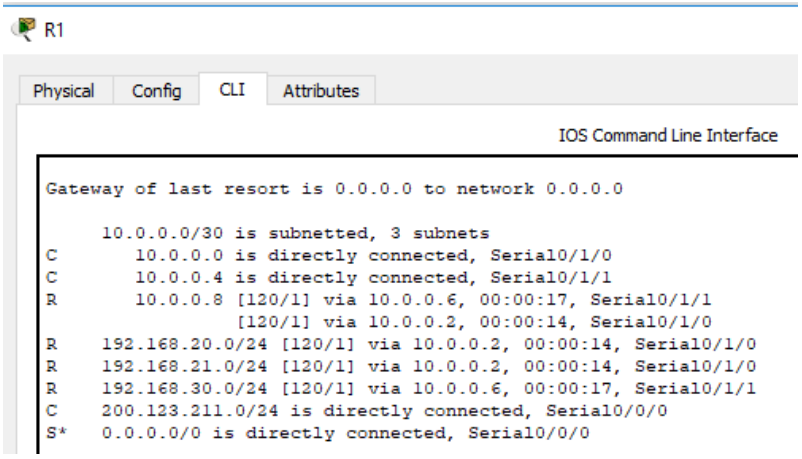
copy running-config startup-config

2.11. 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.

Seguidamente, consultaremos la tabla de enrutamiento, que es la que nos indica que si la configuración ha funcionado, nos mostrará las rutas existentes y de como se obtuvieron, por ejemplo, si la letra que está al comienzo de la línea, es R significa que la ruta se obtuvo por RIP, si tiene una S, significa que se obtuvo por configuración manual, si además tiene un asterisco, significa que es la ruta por defecto, seguidamente, se muestran los pantallazos de esta consulta:

Ilustración 22: consulta tabla de enrutamiento R1



Así realizamos la consulta de las tablas en cada router:

Ilustración 23: Tabla de enrutamiento R2

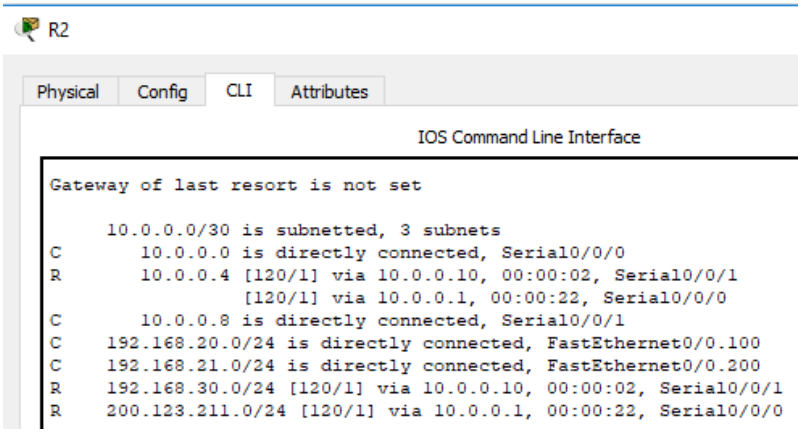
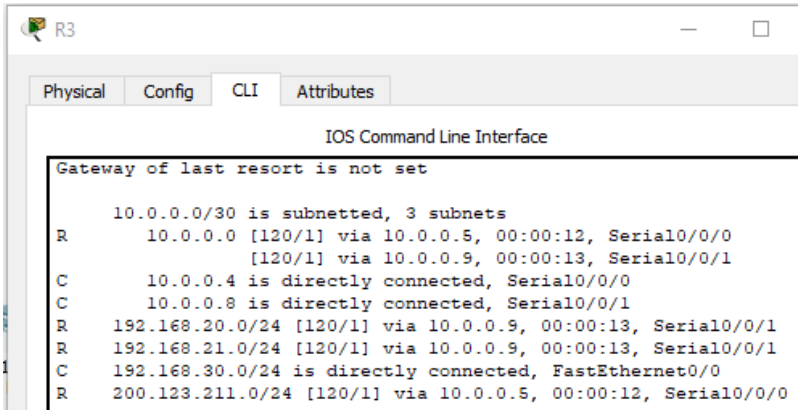


Ilustración 24: Tabla de enrutamiento R3

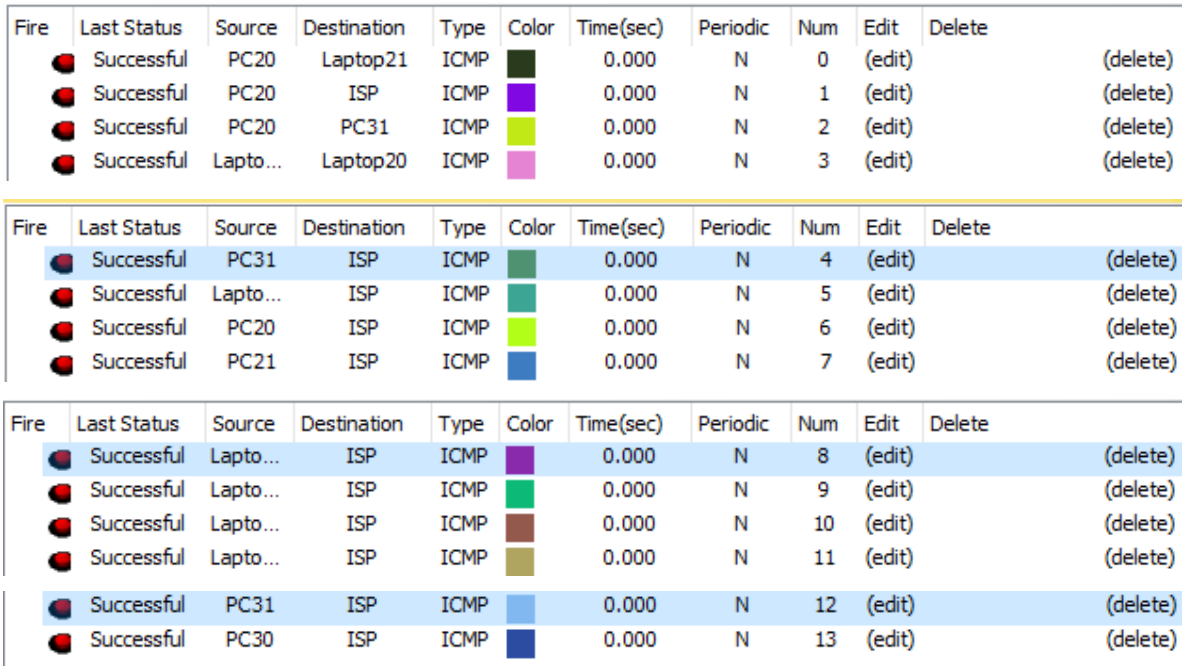


2.12. Pruebas de conectividad

- 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.

Ahora hacemos pruebas de conectividad de cualquier host a cualquier destino, y luego al ISP:

Ilustración 25: IPv4-ping

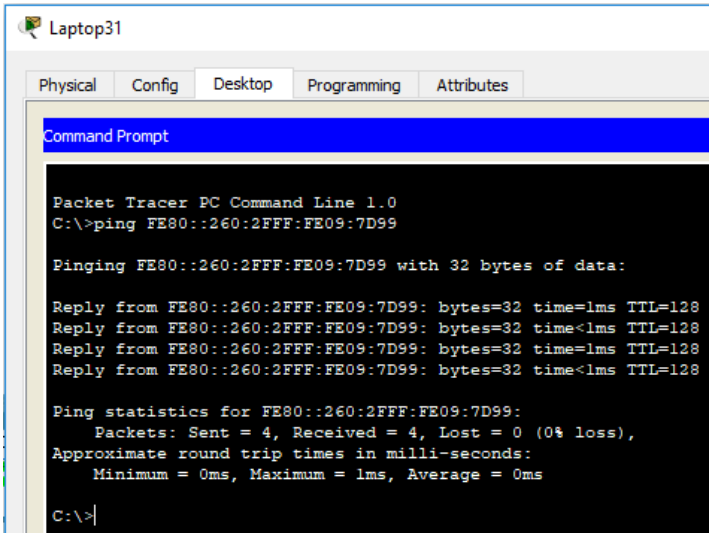


Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC20	Laptop21	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC20	ISP	ICMP		0.000	N	1	(edit)	(delete)
	Successful	PC20	PC31	ICMP		0.000	N	2	(edit)	(delete)
	Successful	Lapto...	Laptop20	ICMP		0.000	N	3	(edit)	(delete)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

Observamos que todas dicen sucessful, es decir pruebas satisfactorias.

Seguidamente realizamos las pruebas de ping en la versión 6:

Ilustración 24: ping IPv6 de Laptop31 a Servidor0



Prueba satisfactoria desde Laptop31

Ilustración 26: ping IPv6 de Servidor0 a Laptop31

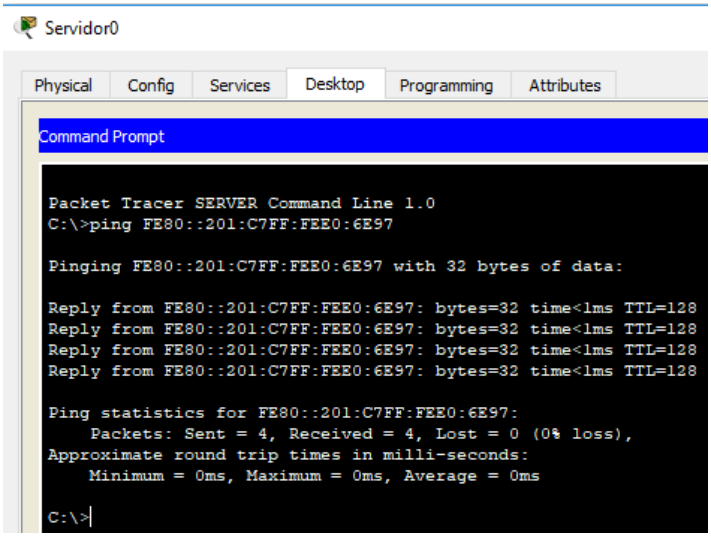


Ilustración 27: ping IPv6 de Servidor0 a Laptop30

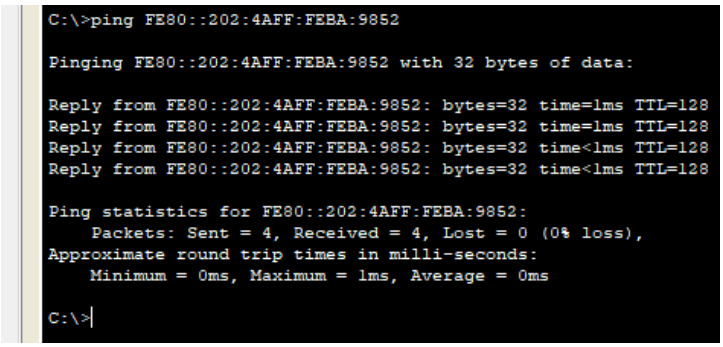


Ilustración 28: ping IPv6 de Servidor0 a PC30

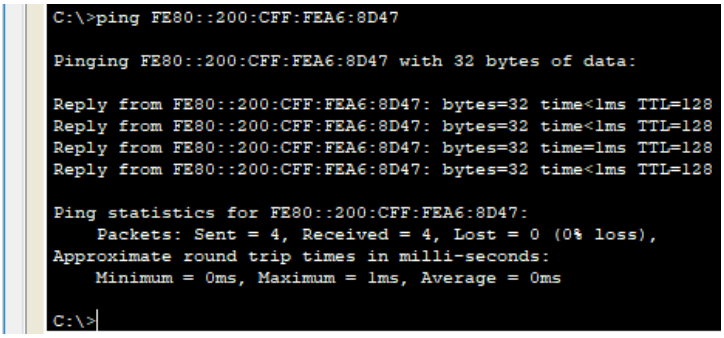
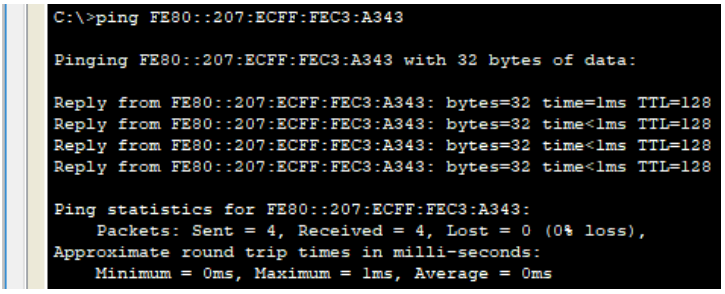


Ilustración 29: ping IPv6 de Servidor0 a PC31

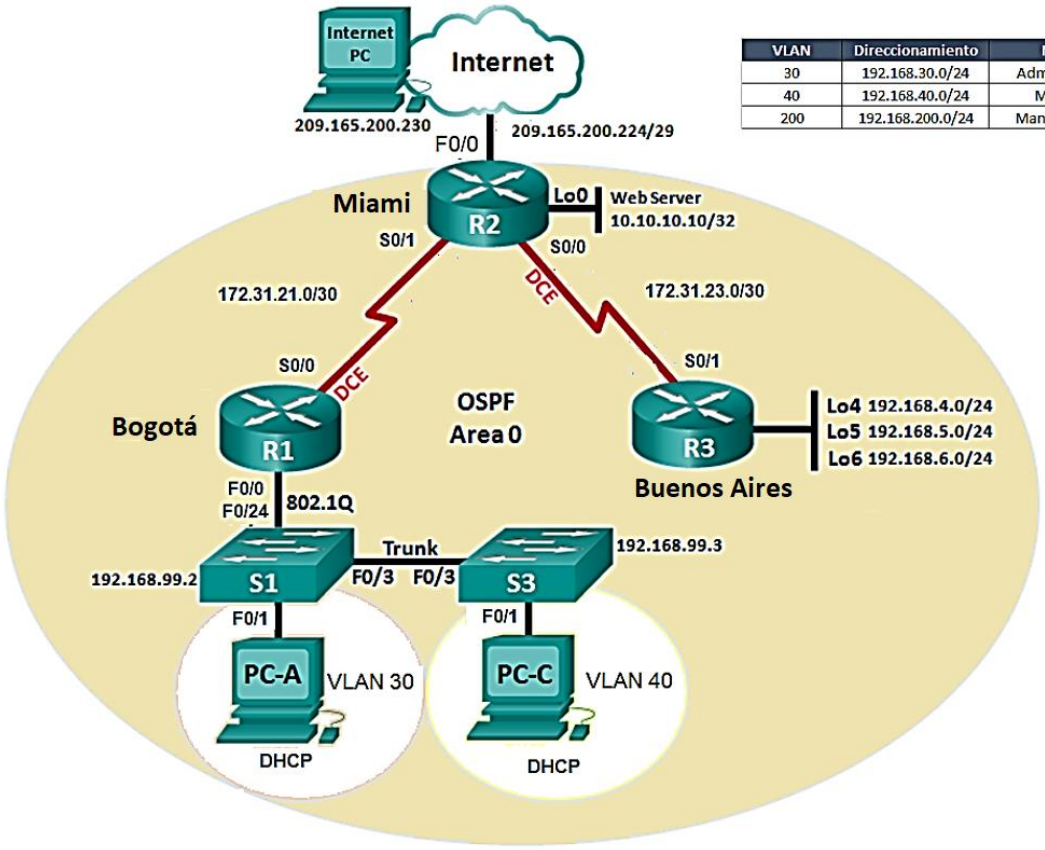


Observamos que todas las pruebas fueron satisfactorias, gracias a las configuraciones realizadas y siguiendo los pasos indicados en la guía de actividades para este escenario.

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 30: 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

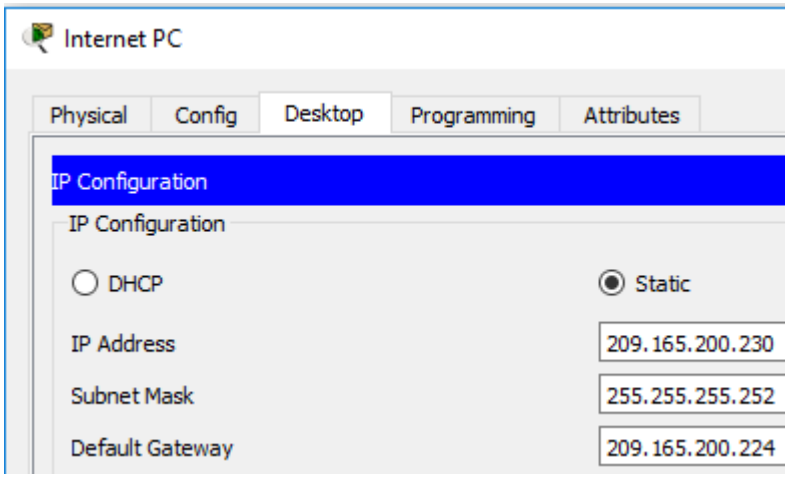
Para este escenario, se nos solicita que montemos la topología siguiendo la gráfica, debemos de hacer la aclaración de que la red de mantenimiento, indicada en la tabla es diferente a la indicada en los switches, por lo tanto tomaremos lo indicado en la tabla, es decir, los switches no tendrán direccionamiento 99.2 y 99.3 , si no, 200.2 y 200.3, de igual manera se está cumpliendo con el objetivo de la implementación.

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.

Siguiendo la imagen, comenzamos por el Internet PC, como lo explicábamos anteriormente, vamos a la pestaña Desktop y seleccionamos el ícono del direccionamiento IP, allí por defecto la opción es estático e ingresamos los parámetros que requiere el Internet PC para pode comunicarse con lo hosts en la red.

Ilustración 31: Direccionamiento Internet PC



Seguidamente ingresamos en los routers y le damos el direccionamiento necesario según el esquema, recordemos que tenemos en R1 dos redes la 30 y la 40, que configuramos mediante un router on stick, a continuación, el CLI para esta configuración:

Para R1

ena

conf ter

host Bogota

inter f0/0

no shut

inter f/0.30

description Administracion

ip addr 192.168.30.1 255.255.255.0
inter f0/0.40
description Mercadeo
ip addr 192.168.40.1 255.255.255.0
inter f0/0.200
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

Dado que debemos comunicarnos con los diferentes hosts en la red, empleamos el protocolo de enrutamiento OSPFv2 el cual es un protocolo tipo enlace de estado, muy empleado actualmente por los operadores de internet, para esta configuración, ingresamos en el router y declaramos el id de ospf, luego el id del router, seguidamente las interfaces que son pasivas para este proceso, y por último las redes que el router puede ver a través de sus interfaces, le damos además los parámetros ordenados en la tabla 3, a continuación, la línea de comandos para ejecutar esta tarea:

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

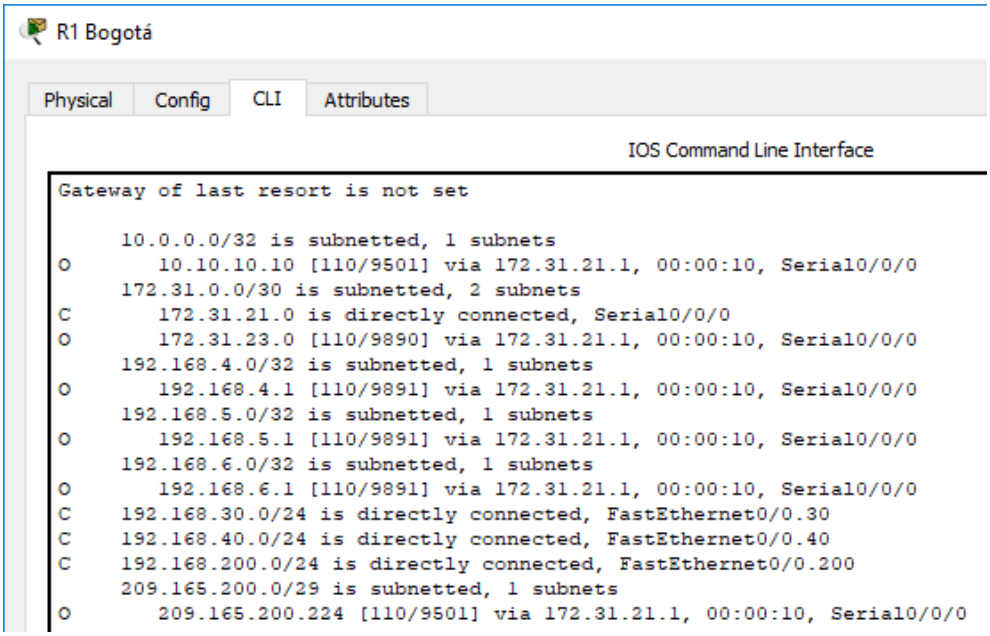
router-id 8.8.8.8
passive-interface Loopback4
passive-interface Loopback5
passive-interface Loopback6
network 172.31.23.0 0.0.0.3 area 0
network 192.168.4.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
interface Serial0/0/1
bandwidth 256
end
copy running-config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

3.3. Verificación información OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

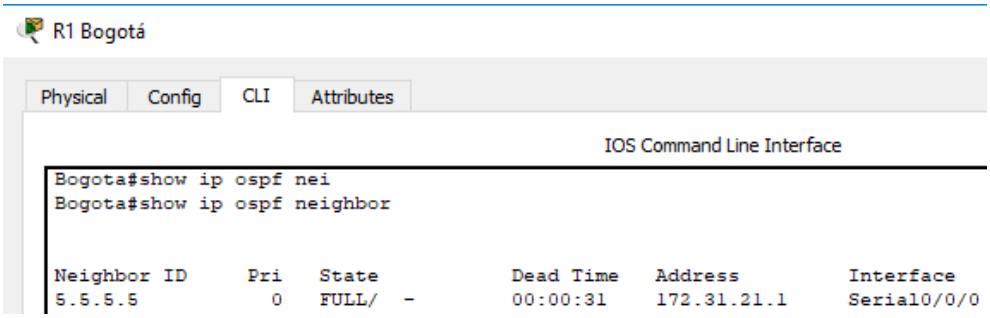
Ahora verificamos mediante el comando show ip route y show ip ospf neighbor:

Ilustración 32: show ip route R1



Observamos que las rutas que aparecen son las que configuramos en los otros router, si lo precede la letra O, significa que fue adquirido por el protocolo OSPF.

Ilustración 33: comando show ip ospf neighbor R1



Con el anterior comando verificamos los vecinos que están conectados al router.

Ahora realizamos lo mismo para los otros routers que participan de la implementación:

Ilustración 34: comando show ip route R2

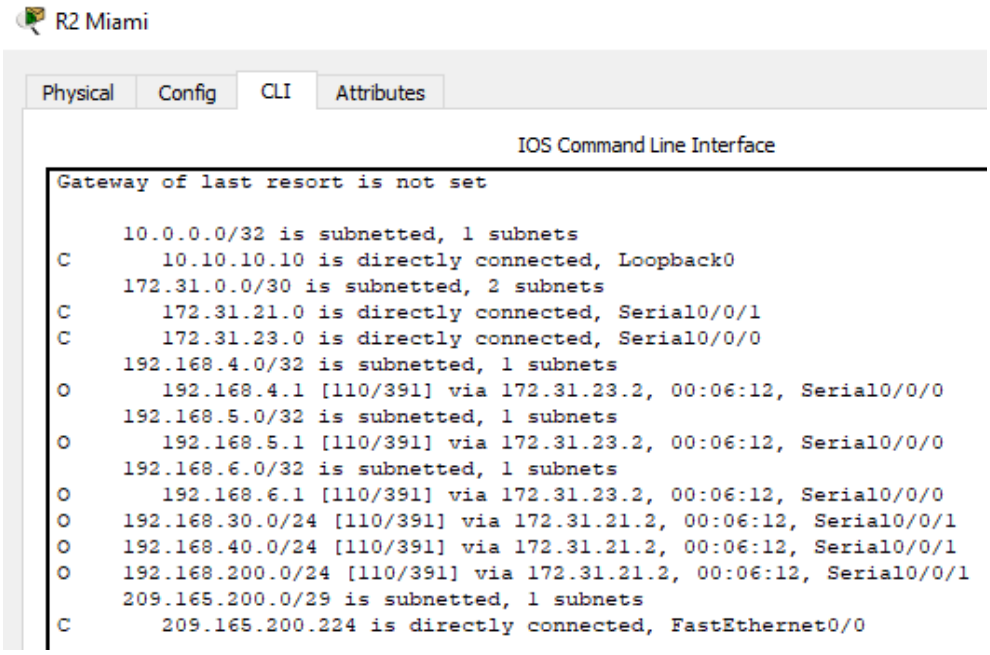


Ilustración 35: comando show ip ospf neighbor R2

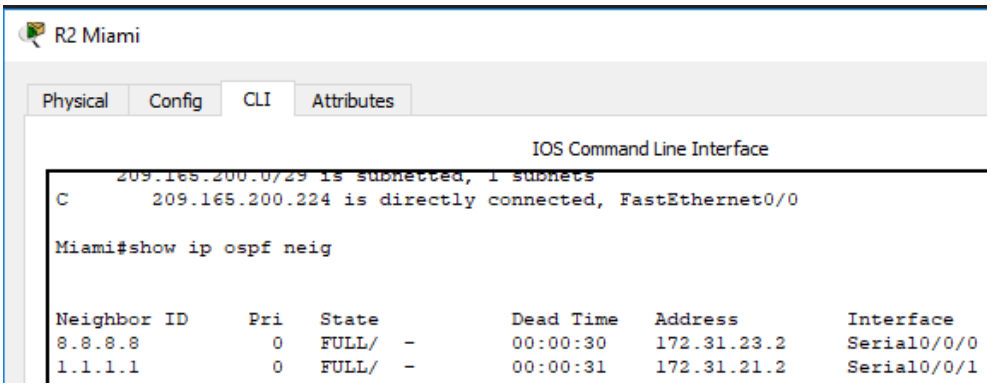


Ilustración 36: : comando show ip route R3

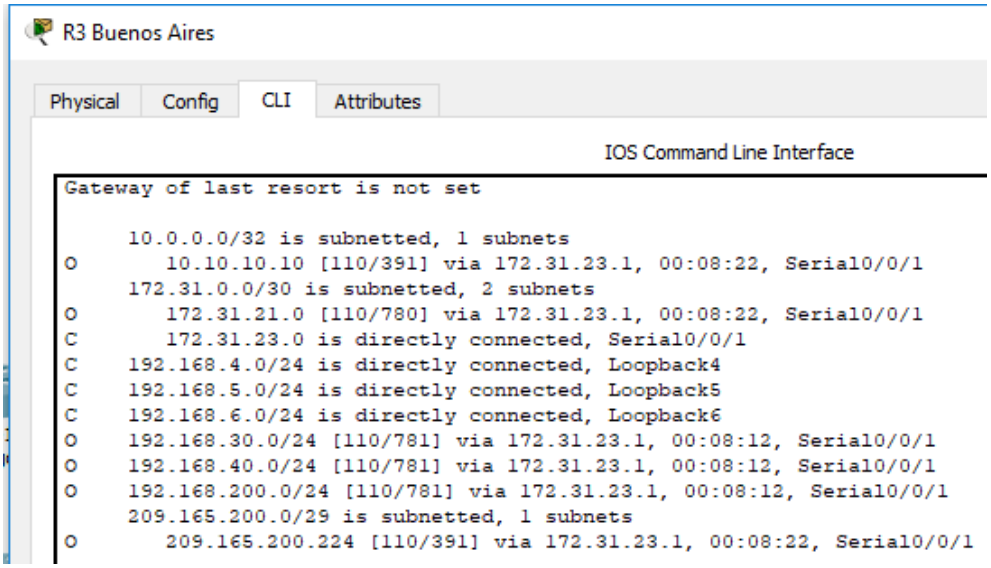
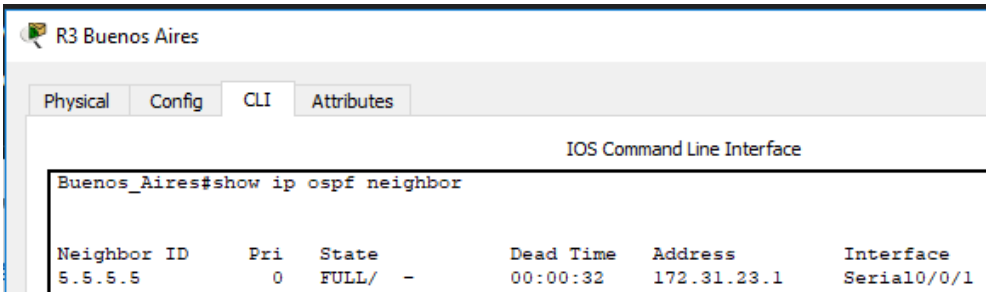
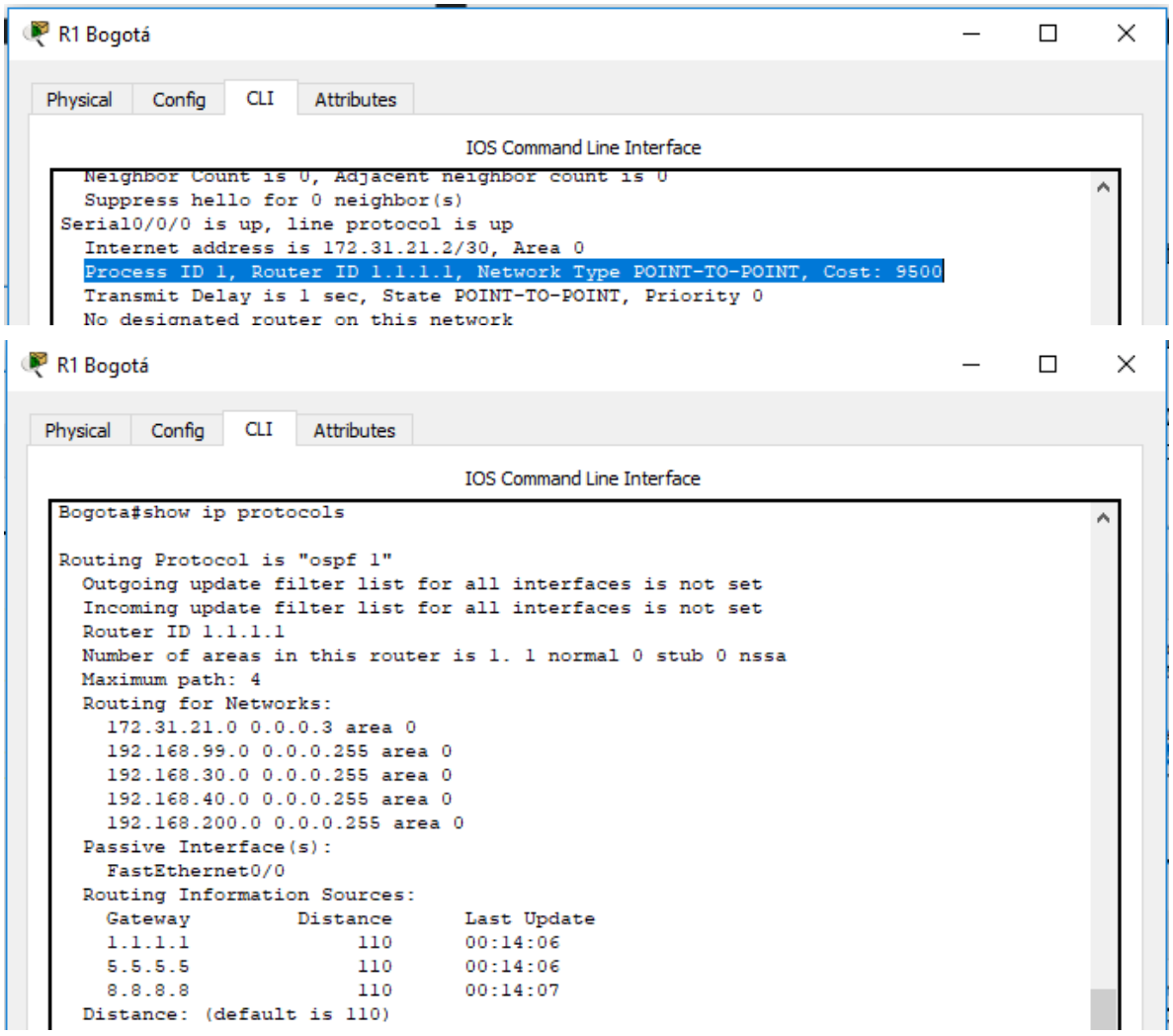


Ilustración 37: comando show ip ospf neighbor R3



- 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 38: Verificación en R1

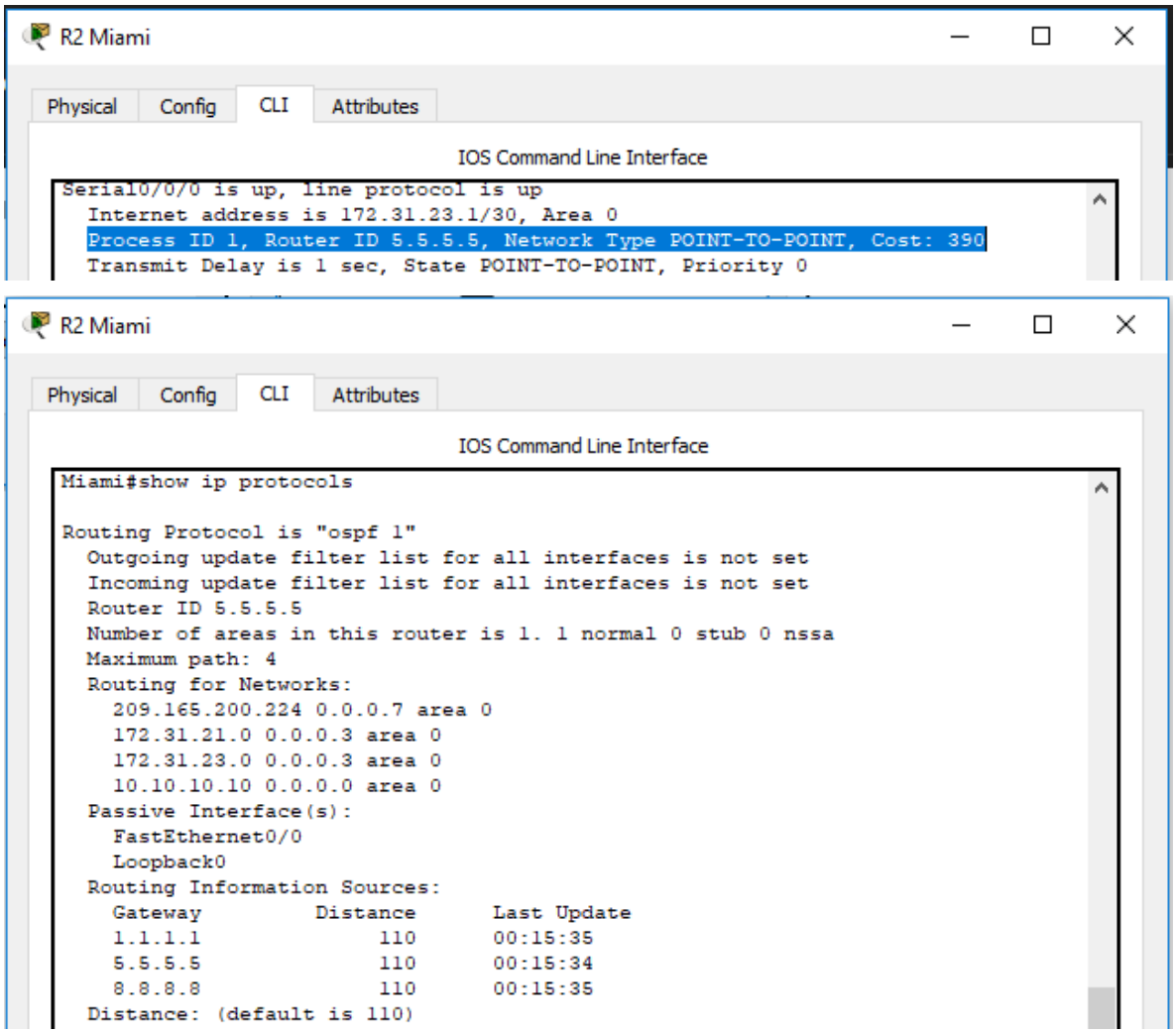


En la gráfica anterior, podemos apreciar el costo de las interfaces, al final de la línea resaltada en azul, y su valor es 9500. Información obtenida mediante el comando **show ip ospf interface**

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

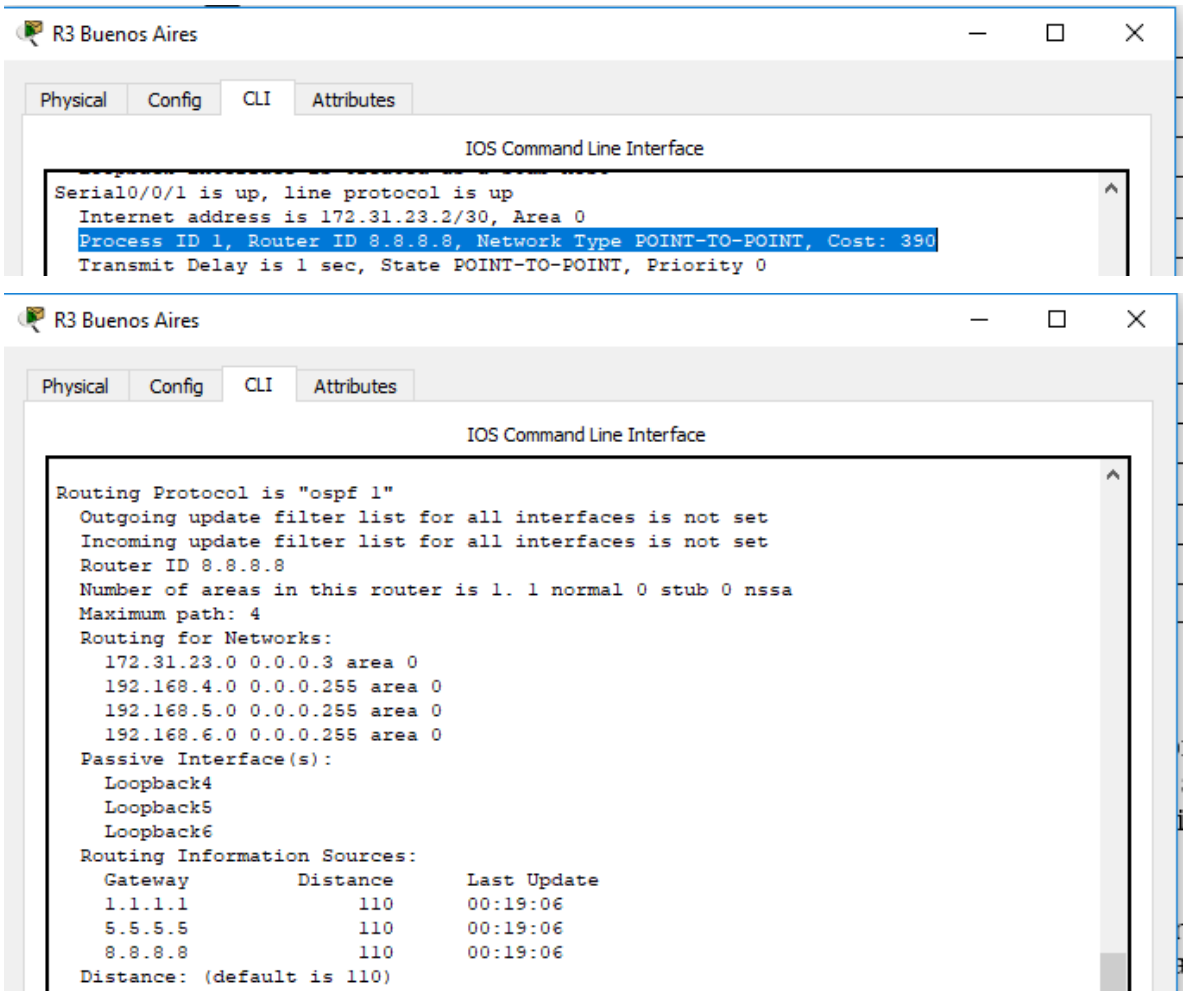
Por último, con el comando **show ip protocols**, podemos conocer cuáles son las interfaces pasivas y las redes enrutadas,

Ilustración 39: Verificación en R2



Información obtenida mediante los comandos anteriormente explicados, para R2

Ilustración 40: Verificación en R3



Información obtenida mediante 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.

La configuración en los switches, primero que nada, debemos configurar las vlan, es decir, nombrarlas, la vlan 30 y la vlan 40, luego ingresamos en la configuración de la interfaz que va a tener esas vlan y configuramos el modo troncal, asignamos los puertos, también implementamos la seguridad al switch, tanto para el ingreso a este como para el enable, también un mensaje de advertencia, no olvidamos grabar la configuración. A continuación, la línea de comandos para este fin:

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

3.5. Deshabilitar 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, la línea de comandos para este fin:

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: A continuación, la línea de comandos para esta tarea:

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.

Para tener aún más seguridad de que nuestra red no sea atacada, debemos apagar los puertos que no se usan en el switch, de la siguiente manera:

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.

Iniciamos con la configuración de DHCP, para esto, excluiremos 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.

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

Ahora implementaremos NAT, como en el escenario anterior, en necesario el NAT ya que mediante esta implementación los terminales pueden salir a internet, solo les tenemos que decir por donde van a salir, así las cosas, lo primero que debemos a hace es crear la lista de acceso que vamos a usar para saber cuáles son las redes que podrán salir, luego indicar en la línea de nat cuál es el origen y la interfaz por la cual va a salir, por último, vamos a indicar las entradas y las salidas para este nat, finalmente escribimos “overload” que habilita a este NAT a que sea PAT o port address translation, a continuación la línea de comandos:

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

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:

```
ena
conf ter
ip access-list standard lista1
permit 192.168.30.0 0.0.0.255
deny 192.168.40.0 0.0.0.255
ip access-list standard lista2
deny 192.168.30.0 0.0.0.255
permit 192.168.40.0 0.0.0.255
ip access-list extended lista3
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 lista4
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
```

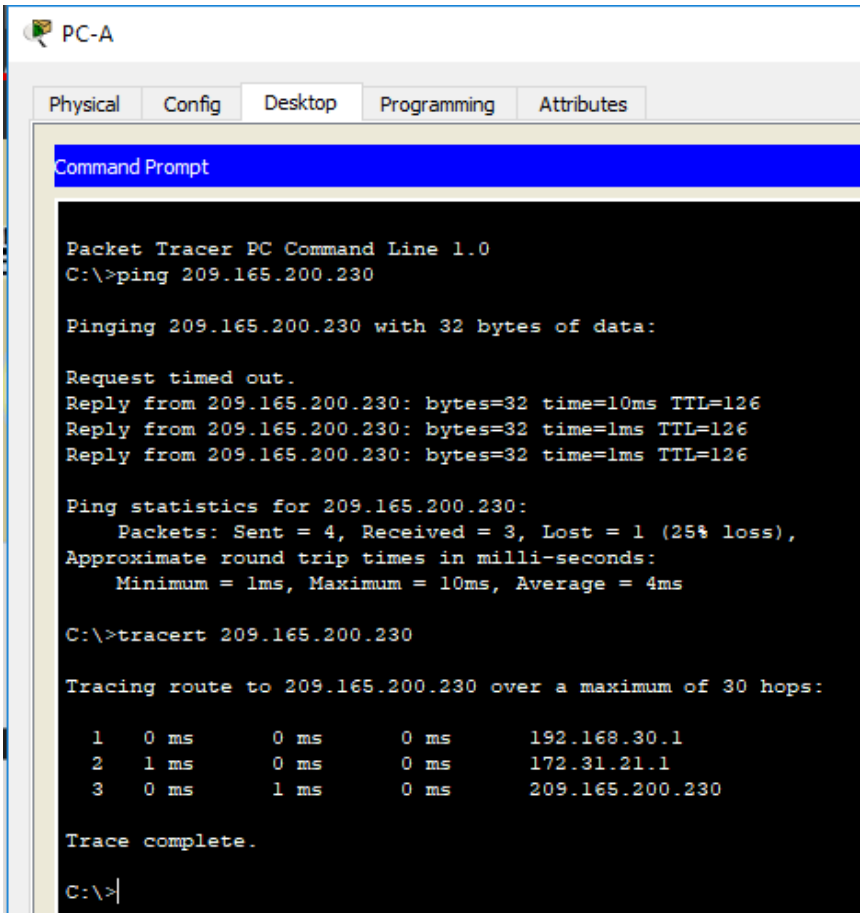
3.11. Verificación comunicación

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

Ahora realizaremos verificaciones con el comando ping y tracert, con el primero, nos damos cuenta si alcanzamos al InternetPC y con el segundo, nos damos cuenta, cuáles son los saltos que debe dar el paquete antes de llegar a destino, por ejemplo, si hacemos tracert desde PC-A hacia 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.

Desde PC-A:

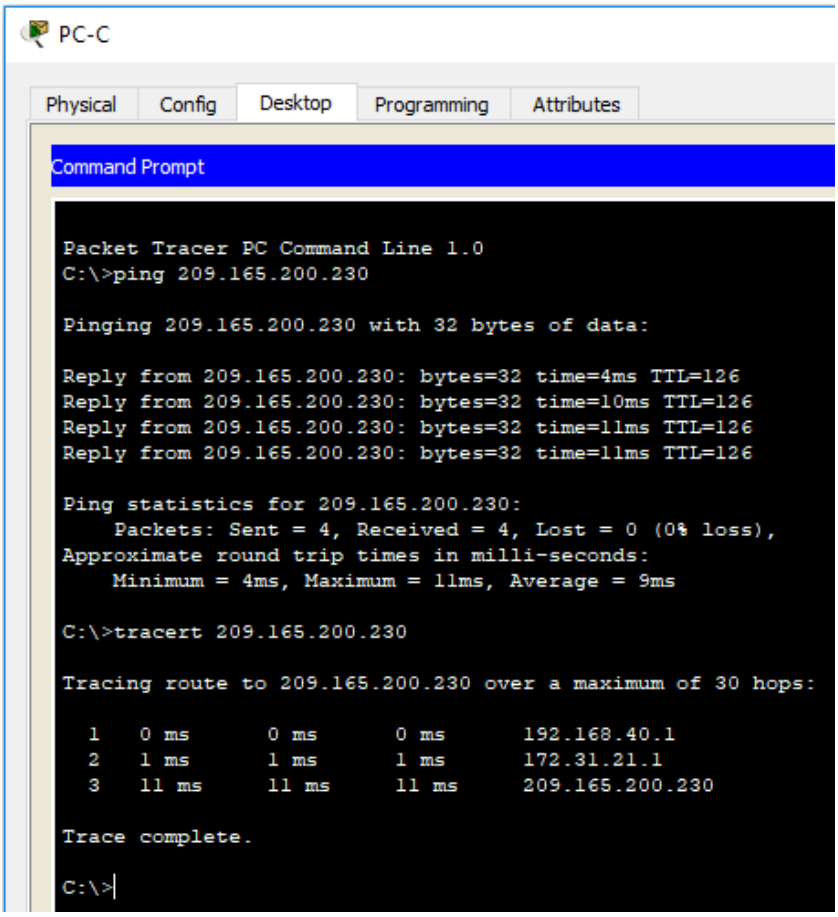
Ilustración 41: PC-A pruebas de conectividad



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 42: PC-C pruebas de conectividad



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

CONCLUSIONES

- Esta práctica ha servido para aplicar varios aspectos de lo aprendido a lo largo del curso de profundización y ya que gracias a que la práctica es la que hace al maestro, cada vez que realizamos una implementación, se va haciendo más fluido el tema.
- Las configuraciones de seguridad en un switch son extremadamente necesarias, ya que de ellas depende la estabilidad de la red.
- Entendimos que los routers y los switches pertenecen a dos capas diferentes del modelo osi, el primero a la capa 3, capa de red y el segundo a la capa 2 o enlace de datos.

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.).