EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

DWIGHT FITZGERALD CHOW

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 redes de computadoras, también conocida como red ordenadores o red informática en el siglo XIX, son una unión de técnicas, dispositivos y sistemas de comunicación los cuales nacieron desde la invención del teléfono, a partir de ahí han nacido diferentes tipos de redes. Las redes se han convertido en la base más importante del ser humano ya que permite consultar y compartir información, permite la comunicación mediamente audio o video.

Al existir diferentes tipos de redes de comunicación como los son las redes LAN, WAN WLAN, WMAN, PAN, SAN lo visto en este curso sobre redes LAN y WAN, permite poder realizar la configuración de dichas redes mediante programas para su simulación como los son packet tracer o GNS3.

1. Primer escenario

Ilustración 1: Escenario 1

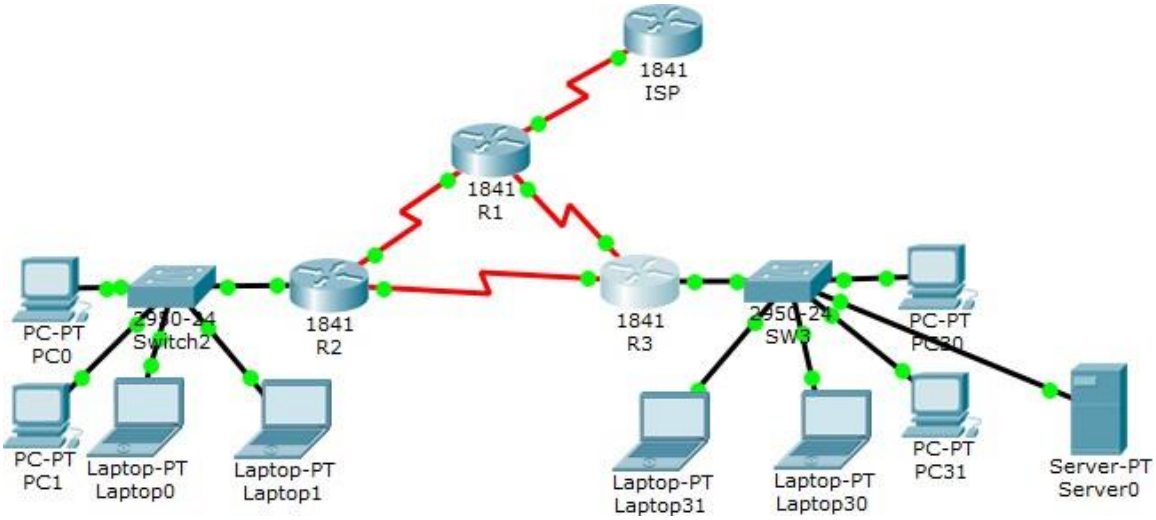


Tabla 1: Tabla de direccionamiento

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 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.

El plan para hacer el desarrollo de este trabajo práctico, consiste en hacer el montaje de la topología en PT, de acuerdo a la ilustración y a la tabla, en la que se nos indica el direccionamiento y las interfaces que se deben configurar para que las pruebas solicitadas sean satisfactorias, usaremos la tecnología de NAT para poder alcanzar el ISP, DHCP para que los terminales obtengan el direccionamiento y RIP, protocolo de enrutamiento, el cual hace posible que los routers obtengan la ruta requerida para entregar un paquete.

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.

En primera instancia, vamos a configurar las vlan en el switch 2 para que cumpla con la tabla, ya que este debe tener las 2 vlan, 1 puerto troncal y puertos asignados a los PC y a las Laptops, las interfaces que no se usen deben ser apagadas, en este caso usamos el comando “shutdown”. para implementar lo anterior, la línea de comandos necesaria es la siguiente:

```
enable
configure terminal
host SW2
interface fa0/1
switchport mode trunk
vlan 100
vlan 200
interface fa0/2
switchport access vlan 100
switchport mode access
interace fa0/3
switchport access vlan 100
switchport mode access
interface fa0/4
switchport access vlan 200
switchport mode access
interface fa0/5
switchport access vlan 200
switchport mode access
interface range fa0/6-24
```

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.

Como ya lo habíamos dicho anteriormente, cumpliendo con la tabla 1, encendemos las interfaces solicitadas en la tabla 1 y le damos direccionamiento.

Para esta parte de la configuración, entramos primero a configurar el router ISP, es decir el destino de internet para nuestro escenario, para el router 1 que es el que recibe al ISP, le configuramos el direccionamiento indicado en la tabla, sin olvidar levantar la interface para que el escenario funcione, para pasar las vlan del router 2, configuramos las subinterfaces 0.100 y 0.200 y le configuramos el direccionamiento indicado en la tabla, sin más que decir, procedemos a realizar la configuración mediante 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

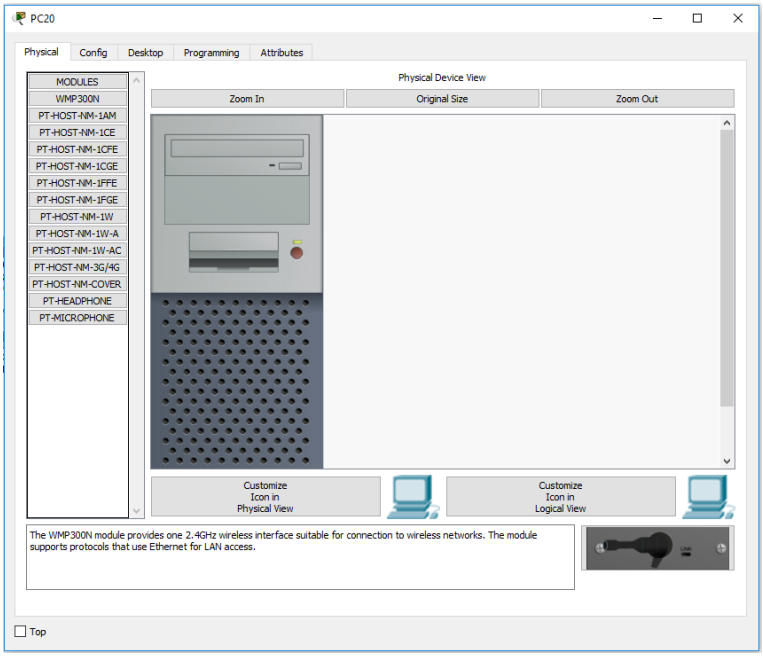
copy running-config startup-config

2.3. Configuración DHCP en host

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

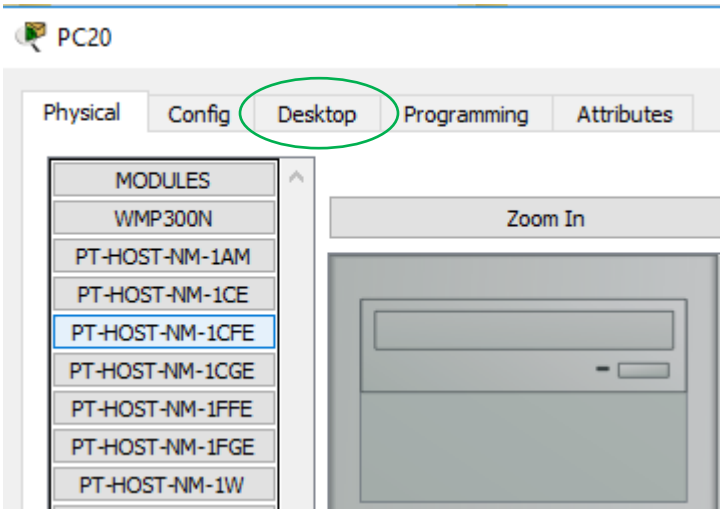
Entramos ahora a configurar los terminales, para que tomen direccionamiento DHCP, con esto ahorramos mucho en trabajo administrativo, pues los PC toman los datos de IP, máscara, puerta de enlace, DNS y dominio, todo esto en PT lo debemos hacer mediante ambiente gráfico, a continuación las imágenes:

Ilustración 2: Configuración DHCP en los terminales



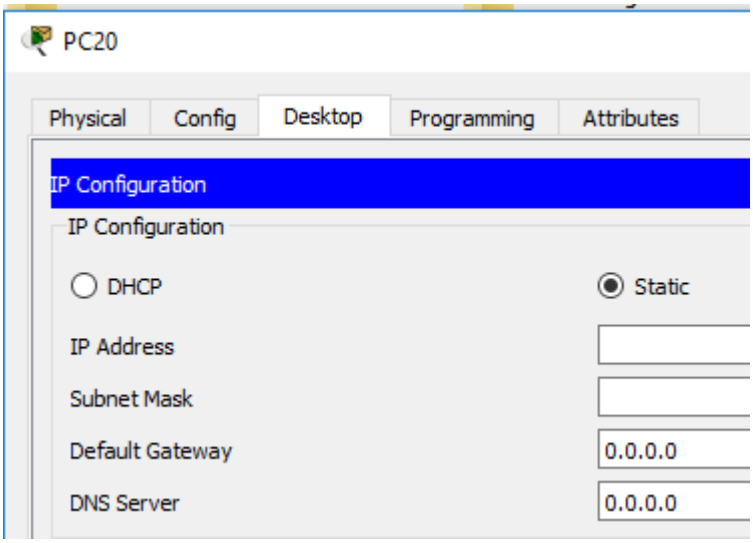
Damos click en el terminal a modificar, con solo darle un click, ya se abre la ventana.

Ilustración 3: Configuración DHCP en los terminales



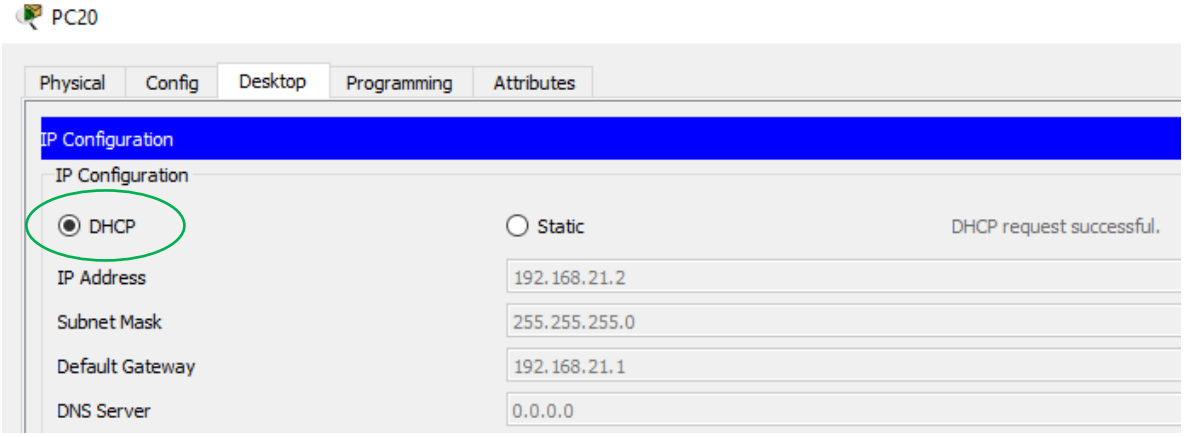
Seguidamente damos click en la ficha Desktop.

Ilustración 4: Configuración DHCP en los terminales



Por default es estático, es allí donde seleccionamos la opción de DHCP.

Ilustración 5: PC20



Como ya tenemos el servicio de DHCP activo, la respuesta del servidor de DHCP fue satisfactoria.

Esa operación la realizamos para todos los terminales de la red implementada.

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**.

Los pasos que debemos seguir para la configuración del NAT lo primero es crear una lista de acceso, en la cual vamos a colocar cuales son esas redes que pueden pasar hasta el ISP, luego, en la línea de configuración de NAT, incluimos la lista precisamente creada y al final, la interfaz por la cual va a salir el tráfico y escribir sobrecarga, es decir “overload”, por último, indicamos las interfaces que entran, “inside” y la que sale “outside” que es la que nos comunica con internet.

El script:

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

inter s0/0/0

ip nat outside

interface serial0/1/0

ip nat inside

inter serial0/1/1

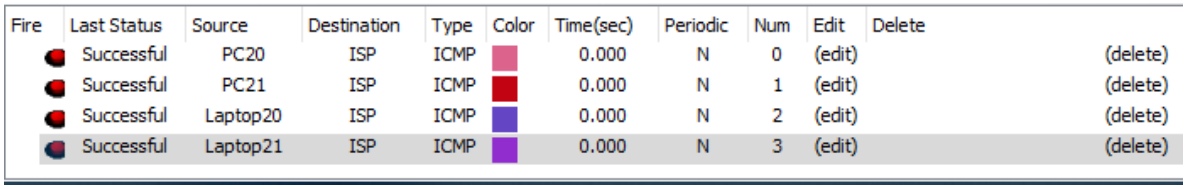
ip nat inside

end

copy running-config startup-config

Realizamos las pruebas de ping en IPv4 que es la prueba que podemos hacer en el ambiente gráfico de PT.

Ilustración 6: 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)

Ilustración 7: ping a ISP

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)

Las pruebas fueron exitosas, esto quiere decir que por el momento todo el deployment está en orden, estamos explicando esto en orden, pero es de anotar que antes de hacer este documento, montamos el escenario, por eso nos entrega DHCP y las pruebas de conectividad son exitosas.

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.

Si el destino que solicita un host de nuestra red, no concuerda con la tabla de rutas, este paquete sale por la ruta por defecto, para este escenario, se nos pide que la ruta sea Serial0/0/0, esta es la línea de comandos que usaremos para configurarla:

El script:

```
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.

La configuración del pool dhcp, lo hacemos en el router 2 como lo indica esta guía, para ello, lo primero es nombrar el pool, lo llamaremos vlan_100, damos la red que tendrá y la salida por defecto, por buenas prácticas en una red de máscara 24, esa ruta es la dirección 1 o la 254, para esta implementación usaremos la 20.1 1 la 21.1.

El script:

La línea de comandos para esta configuración es la siguiente:

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

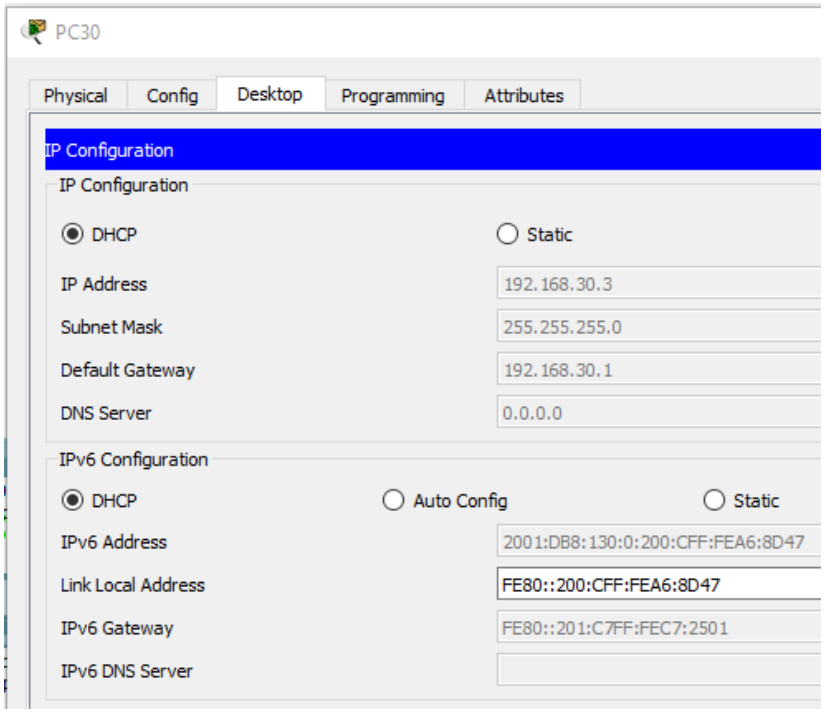
copy running-config startup-config

2.7. Pruebas de conectividad Servidor0

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

Habíamos dicho que teníamos montada toda la implementación requerida, por eso ahora, explicaremos como se obtiene el direccionamiento IPv6, vamos nuevamente al equipo que vamos a configurar, le damos click, luego en la pestaña Desktop, seguidamente seleccionamos DHCP en la sección IPv6, y así toma el direccionamiento:

Ilustración 8: Configuración DHCPv6 en PC30



Observamos la doble pila, es decir, la pila IPv4 y la IPv6.

Realizamos pruebas de conectividad solicitadas, haciendo ping desde los PC hacia el Servidor0:

Ilustración 9: ping IPv6 de PC30 a Servidor0

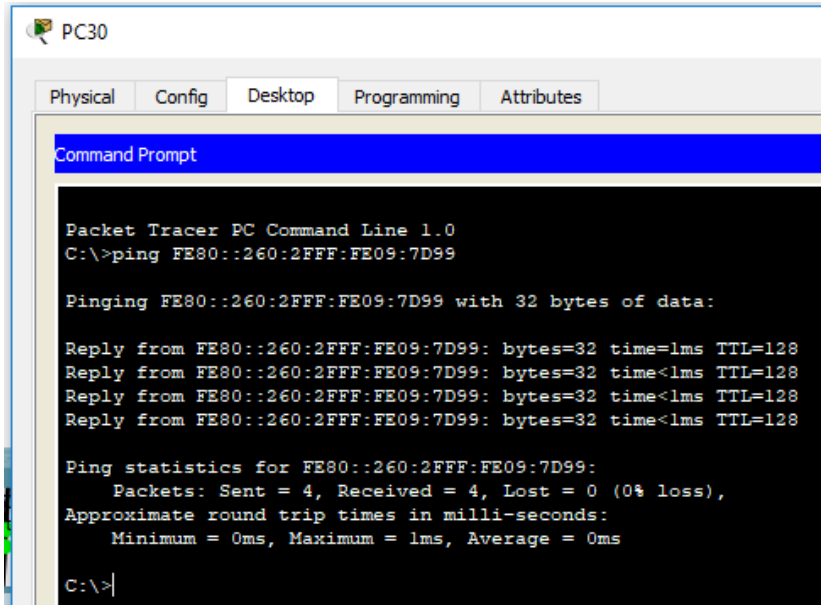


Ilustración 10: ping IPv6 de PC31 a Servidor0

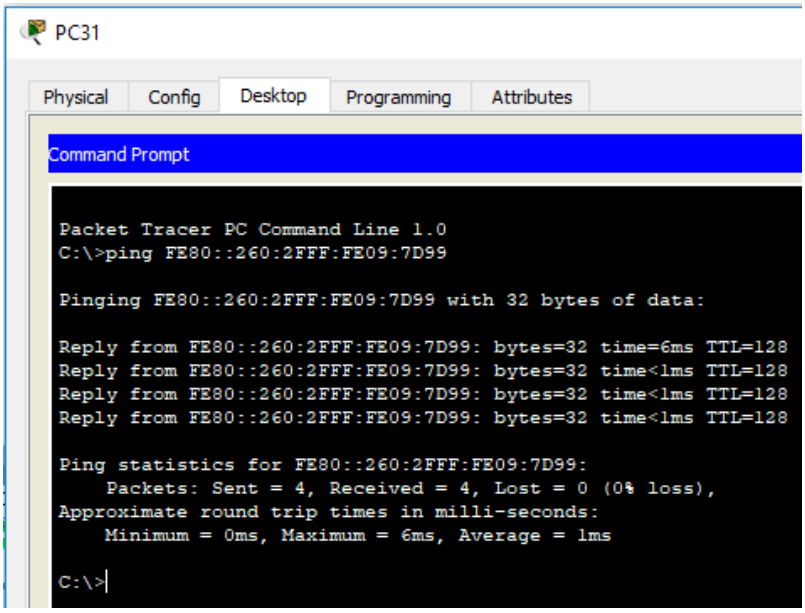


Ilustración 11: ping IPv6 de Laptop30 a Servidor0

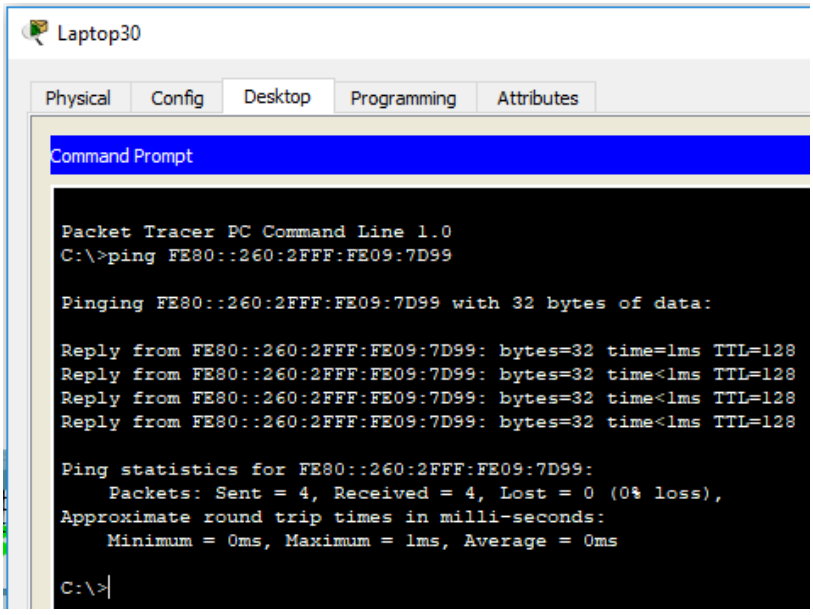
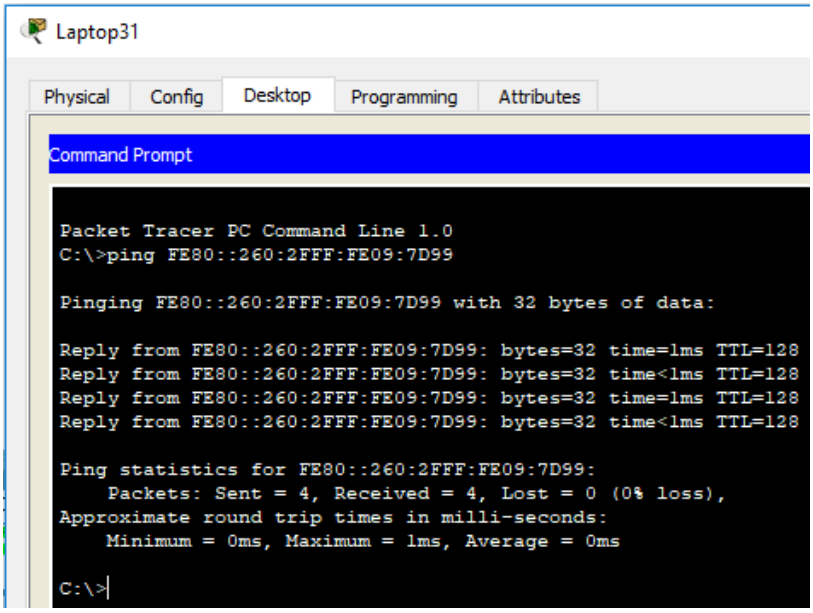


Ilustración 12: ping IPv6 de Laptop31 a Servidor0



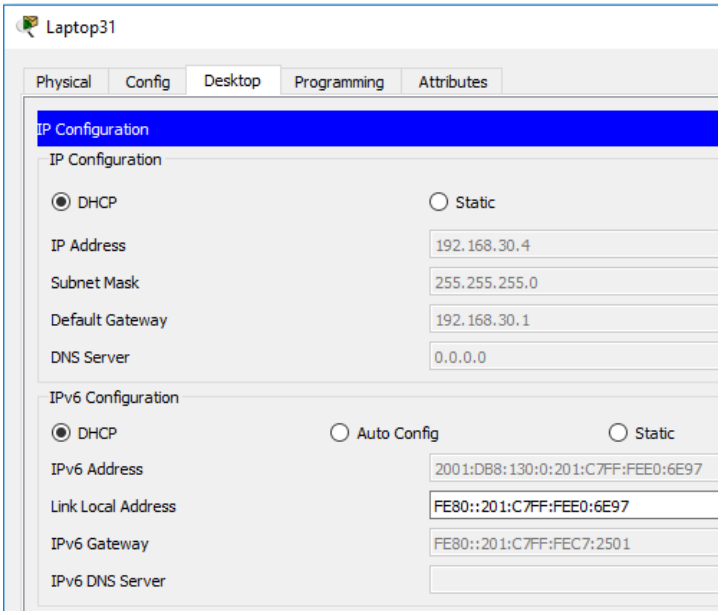
2.8. Configuración dual-stack en las NIC

- 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 este punto en la pestaña Desktop de cada Laptop y PC se ha configurado doble pila, debido a esto, se puede hacer pruebas de conectividad entre los dispositivos IPv6 y entre los IPv4,

Acá la configuración dual de Laptop31:

Ilustración 13: Configuración dual-stack en Laptop31



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).

Por último, las líneas de comando que debemos ingresar y que hacen posible la doble pila son:

enable

configure terminal

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

interface fa0/0

ip address 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.

Para intercambiar rutas con los vecinos, implementamos RIPv2, evita mucho trabajo administrativo y, por ende, tiempo, tan solo declaramos las redes que ve el router a través de sus interfaces.

Esta es la configuración que debemos realizar en cada router que interviene en esta operación:

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

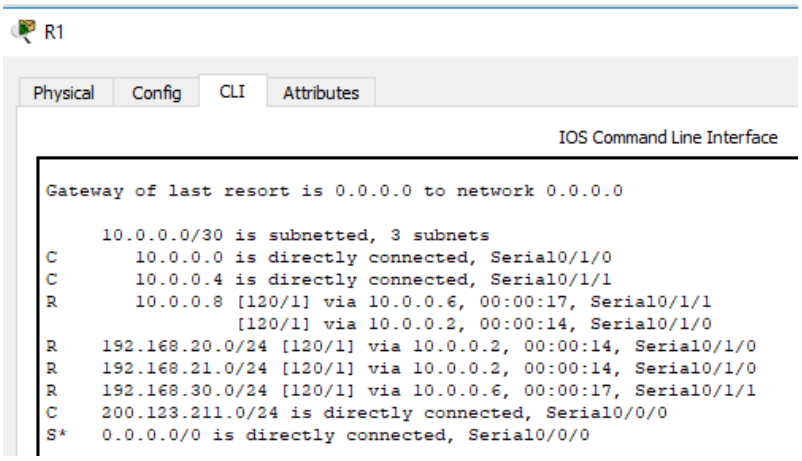
copy running-config startup-config

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.

La consulta de los router sobre que rutas tiene, se realiza mediante el comando “show ip route”, de esta manera podemos conocer y hacer “troubleshooting” en el caso que no haya comunicación entre terminales de diferentes redes:

Ilustración 14: consulta tabla de enrutamiento R1



Observamos de esta forma como se obtuvieron las tablas, unas por configuración estática, en este caso, lleva una S, si es por RIP lleva una R y si es por directamente conectada, aparecerá una C, el asterísco indica que es la ruta pñor defecto como es el caso del Serial0/0/0

Ilustración 15: Tabla de enrutamiento R2

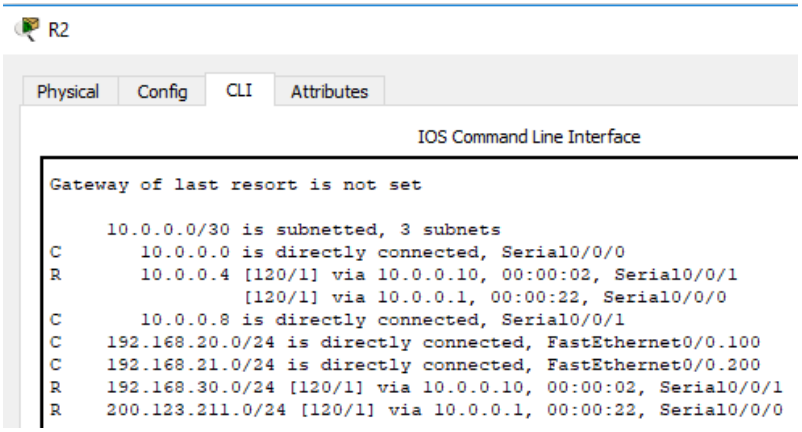
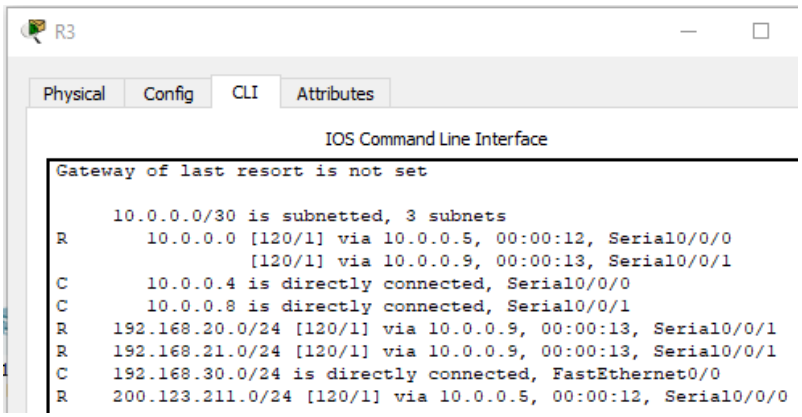


Ilustración 16: Tabla de enrutamiento R3



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.

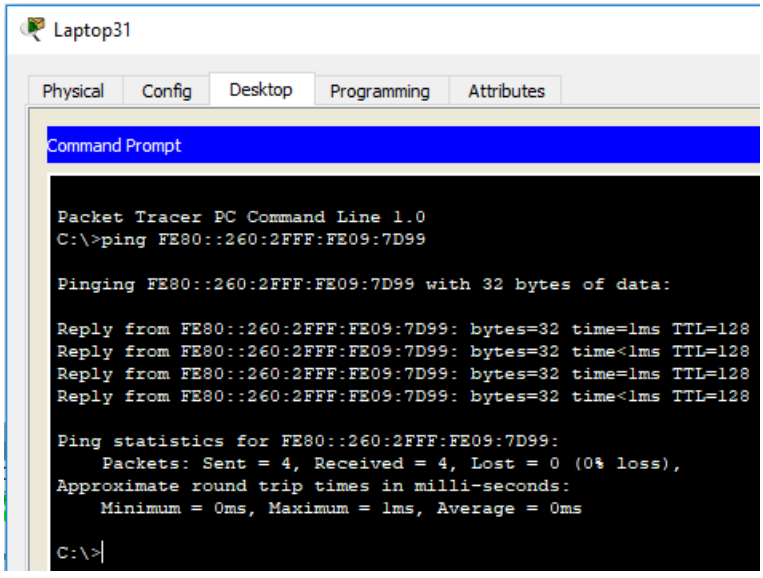
Ya que hemos realizado la configuración de todos y cada uno de los elementos de la red, significa que ya podemos hacer prueba de conectividad según se requiera, procedemos a hacerla en IPv4 con la herramienta gráfica de PT.

Ilustración 17: Haciendo ping en IPv4

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)

Podemos ver, que todos los paquetes llegaron a destino satisfactoriamente, ahora vamos a hacer lo mismo con IPv6, pero en esta parte si debemos hacerlo por el command prompt el cual se encuentra en la pestaña Desktop de la configuración de cada equipo de cómputo, esto solo lo vamos a hacer con los equipos conectados en la red del extremo derecho, es decir los terminales conectados por medio del switch en R3:

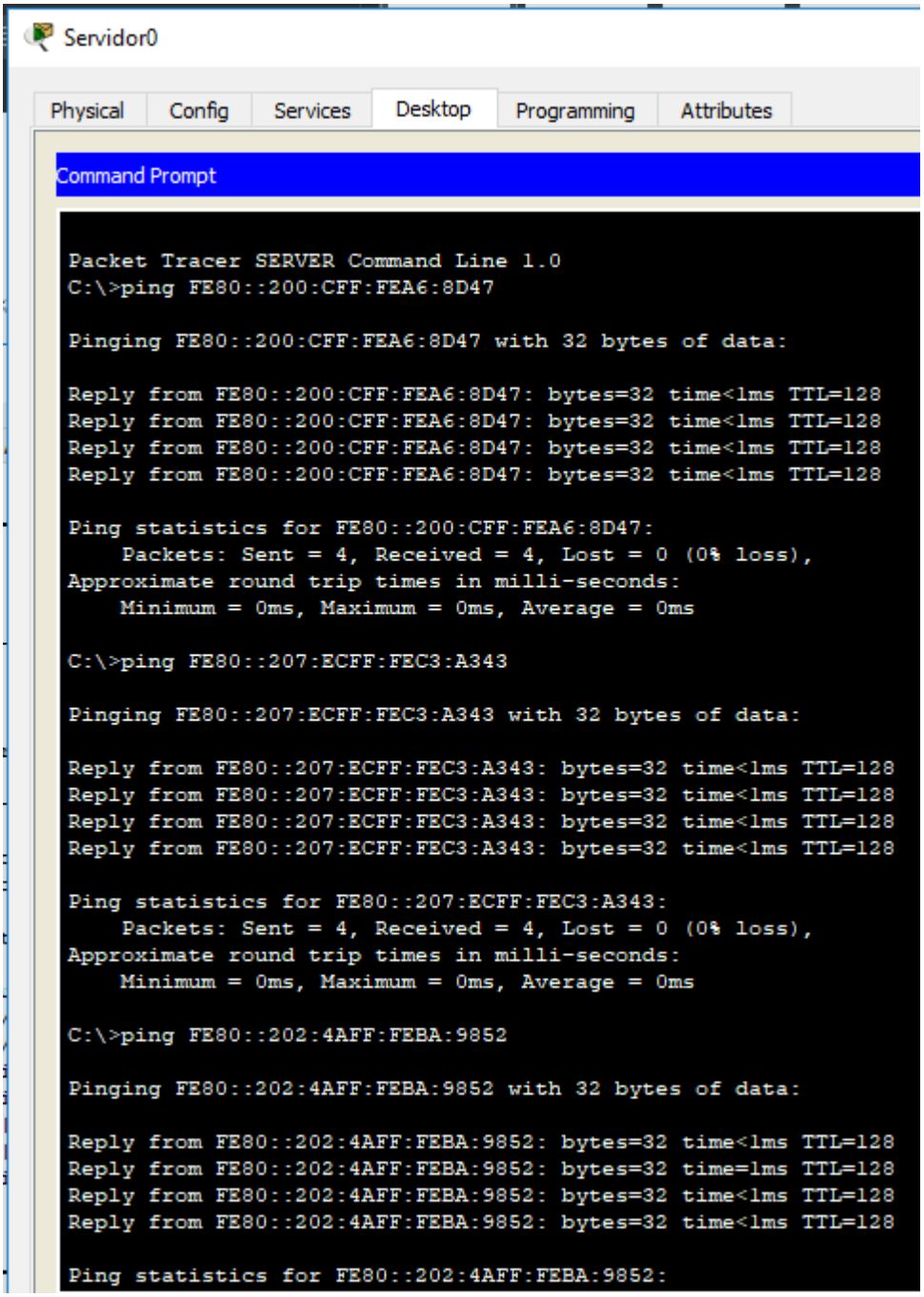
Ilustración 18: ping IPv6 de Laptop31 a Servidor0



Como podemos ver, estamos haciendo ping al servidor desde Laptop31 y llega perfecto a destino.

Ahora, desde el servidor hacia los PC de esa red:

Ilustración 189: ping IPv6 desde Servidor0 a PCs

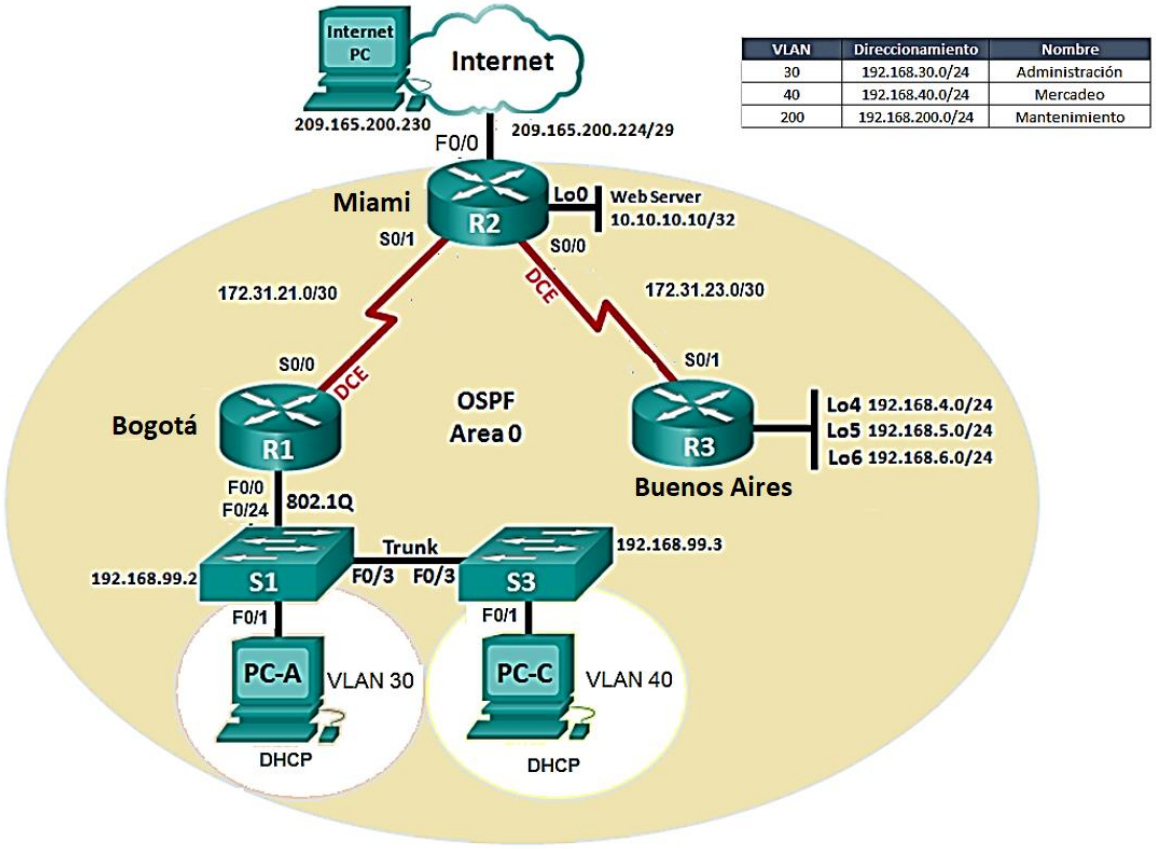


Las pruebas de conectividad fueron satisfactorias por el protocolo IPv6 desde el Servidor0 hacia los PC y Laptops conectados en SW3.

3. Segundo escenario

Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

Ilustración 20: Escenario 2



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

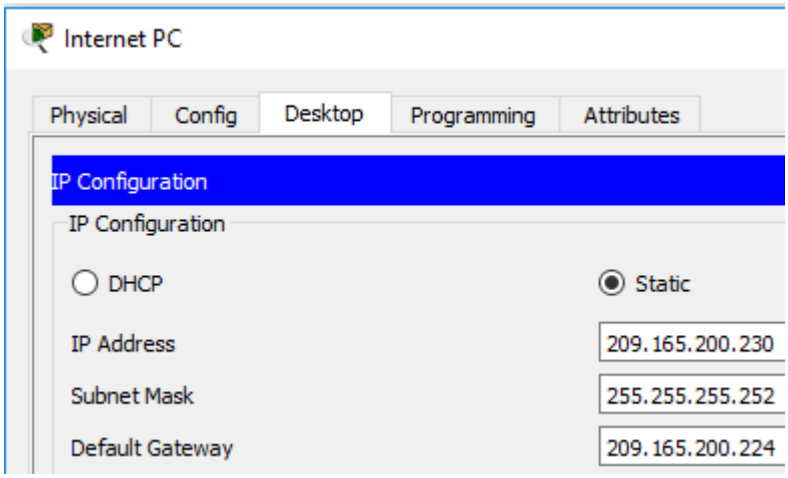
Para este escenario, el protocolo de enrutamiento que emplearemos es el OSPF, recordemos que el RIPv2 solo soporta 15 saltos, por lo que no es tan utilizado por los ISP. En la gráfica de arriba, podemos ver que el direccionamiento de los switches, es diferente al de la tabla, por lo que, para este ejercicio, solo haremos el que corresponde a la tabla, entonces, lo switches, en la red de gestión tendrán un direccionamiento 200.2 y 200.3. también, para este escenario, haremos prácticas de NAT que en la práctica se conoce como PAT, y listas de acceso que nos ayudarán a bloquear el acceso o permitirlo, desde redes o host que deseemos aplicarle esta opción, a continuación, el desarrollo de este escenario.

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.

Luego de montar la topología que nos indica el punto, procedemos a configurar el direccionamiento solicitado, en el Internet PC, solo se nos entrega el direccionamiento y la máscara, y nosotros debemos calcular que gateway emplea, para ello podemos apoyarnos en las calculadoras de red o, entender que teniendo en cuenta la máscara, podemos saber que número forman parte de ella, en este caso, la máscara es 30, lo cual nos indica, que hay 4 direcciones disponibles, 2 asignables y una para red y la otra para el boradcast, de acuerdo a eso, esta es la configuración:

Ilustración 191: Direccionamiento Internet PC



Para el internet PC mediante la interfaz gráfica, en la pestaña Desktop, hacemos click en el ícono de **IP Configuration**, por defecto ya está en Static y colocamos los números decimales que requiere, la IP, la máscara y la salida por defecto.

Seguimos con los switches, digitamos el script necesario para cada uno de los routers de la topología y los switches, a continuación, la línea de comandos necesaria, en R1 hay una configuración especial, y es crear subinterfaces, las cuales serán nombradas de acuerdo a la vlan que vamos a crear en los switches: 0.30 y 0.40, así en los switches serán vlan 30 y vlan 40:

Para R1

enable

configure terminal

host Bogota
interface fa0/0
no shutdown
interface fa/0.30
description Administracion
ip address 192.168.30.1 255.255.255.0
interface fa0/0.40
description Mercadeo
ip address 192.168.40.1 255.255.255.0
interface fa0/0.200
description Mantenimiento
ip address 192.168.200.1 255.255.255.0
interface serial0/0/0
ip address 172.31.21.2 255.255.255.252
no shutdown
end
copy running-config startup-config

Para R2

enable
configure terminal
host Miami
interface lo0
description WebServer
ip address 10.10.10.10 255.255.255.255
interface fa0/0
ip address 209.165.200.229 255.255.255.248
no shutdown
interface serial0/0/0
ip address 172.31.23.1 255.255.255.252
no shutdown

interface serial0/0/1
ip address 172.31.21.1 255.255.255.252
no shutdown
end
copy running-config startup-config

Para R3

enable
configure terminal
host Buenos_Aires
interface lo4
ip address 192.168.4.1 255.255.255.0
interface lo5
ip address 192.168.5.1 255.255.255.0
interface lo6
ip address 192.168.6.1 255.255.255.0
interface serial0/0/1
ip address 172.31.23.2 255.255.255.252
no shutdown
end
copy running-config startup-config

Para SW1

enable
configure terminal
host S1
vlan 200
inter vlan 200
ip address 192.168.200.2 255.255.255.0
end
copy running-config startup-config

Para SW3

ena

configure terminal

host S3

vlan 200

inter vlan 200

ip address 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

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

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

La línea de comandos, es la siguiente:

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

copy running-config startup-config

Para R2

ena

conf ter

router ospf 1

router-id 5.5.5.5

passive-interface FastEthernet0/0

passive-interface Loopback0

network 209.165.200.224 0.0.0.7 area 0

network 172.31.21.0 0.0.0.3 area 0

network 172.31.23.0 0.0.0.3 area 0

network 10.10.10.10 0.0.0.0 area 0

interface Serial0/0/0

bandwidth 256

ip ospf cost 9500

interface Serial0/0/1

bandwidth 256

end

copy running-config startup-config

Para R3

ena

conf ter

router ospf 1

router-id 8.8.8.8

passive-interface Loopback4

passive-interface Loopback5

passive-interface Loopback6

network 172.31.23.0 0.0.0.3 area 0

network 192.168.4.0 0.0.0.255 area 0

network 192.168.5.0 0.0.0.255 area 0

network 192.168.6.0 0.0.0.255 area 0

interface Serial0/0/1

bandwidth 256

end

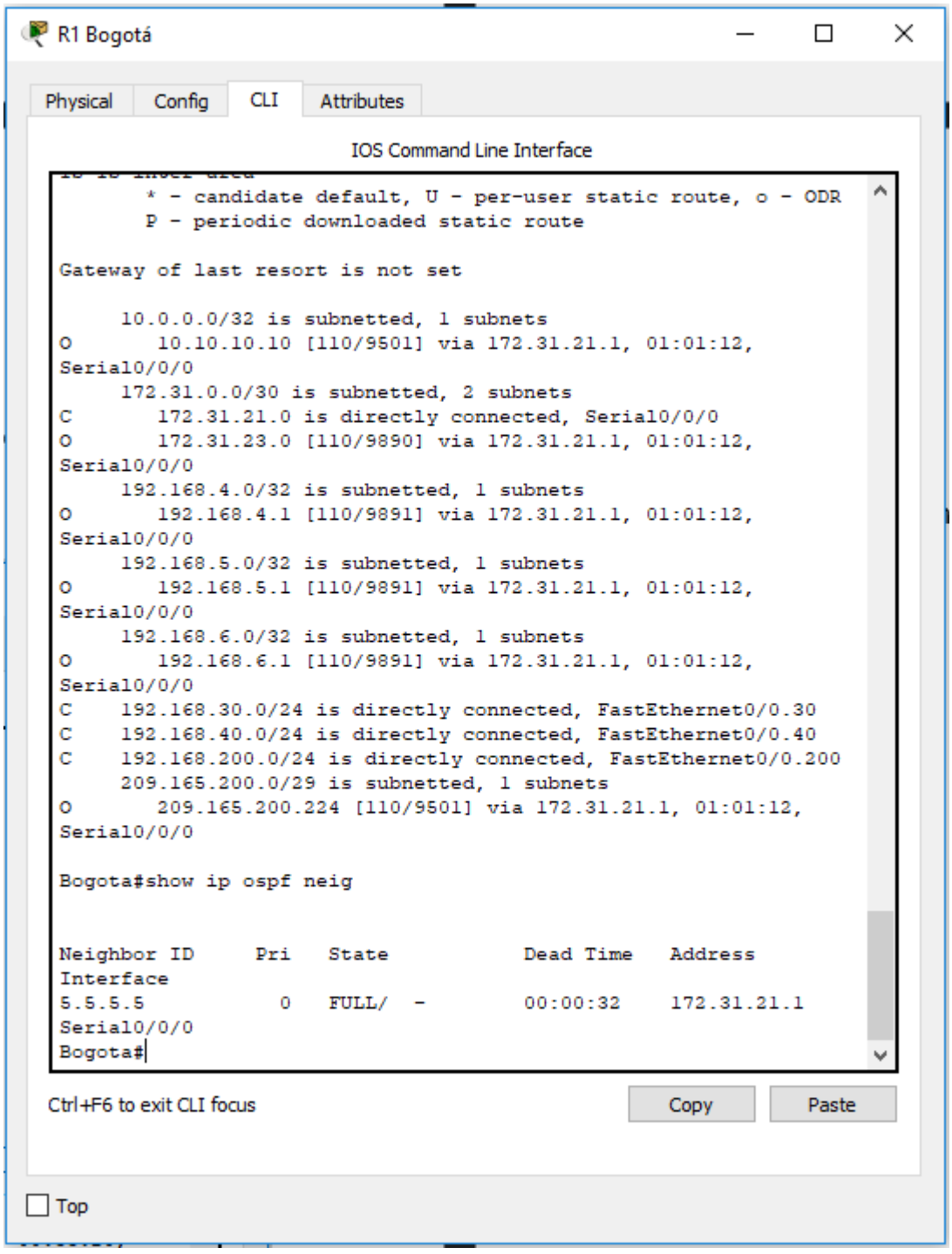
copy running-config startup-config

3.3. Verificación información OSPF

Visualizar tablas de enrutamiento y routers conectados por OSPFv2

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

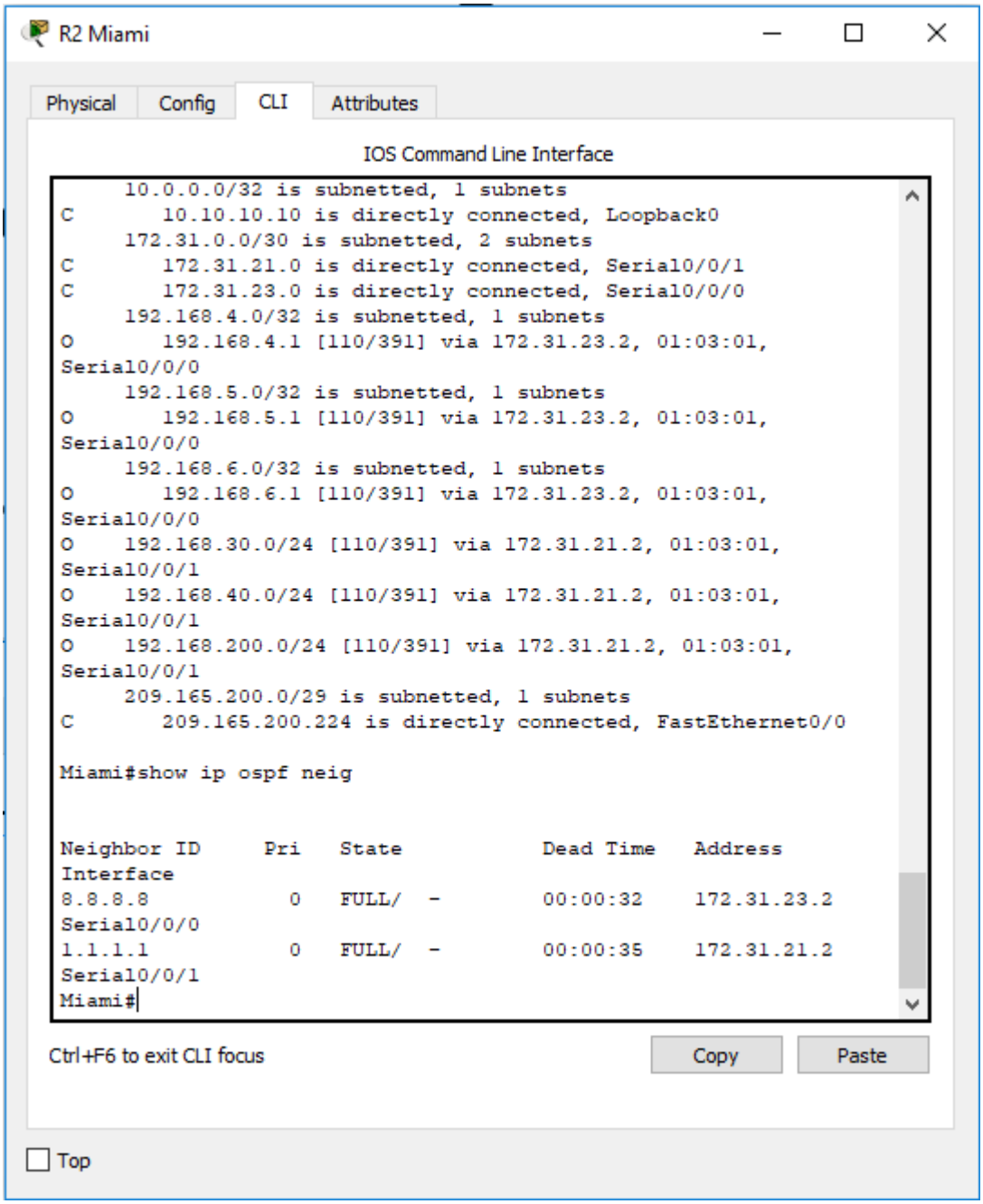
Ilustración 202: Tabla de enrutamiento R1



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

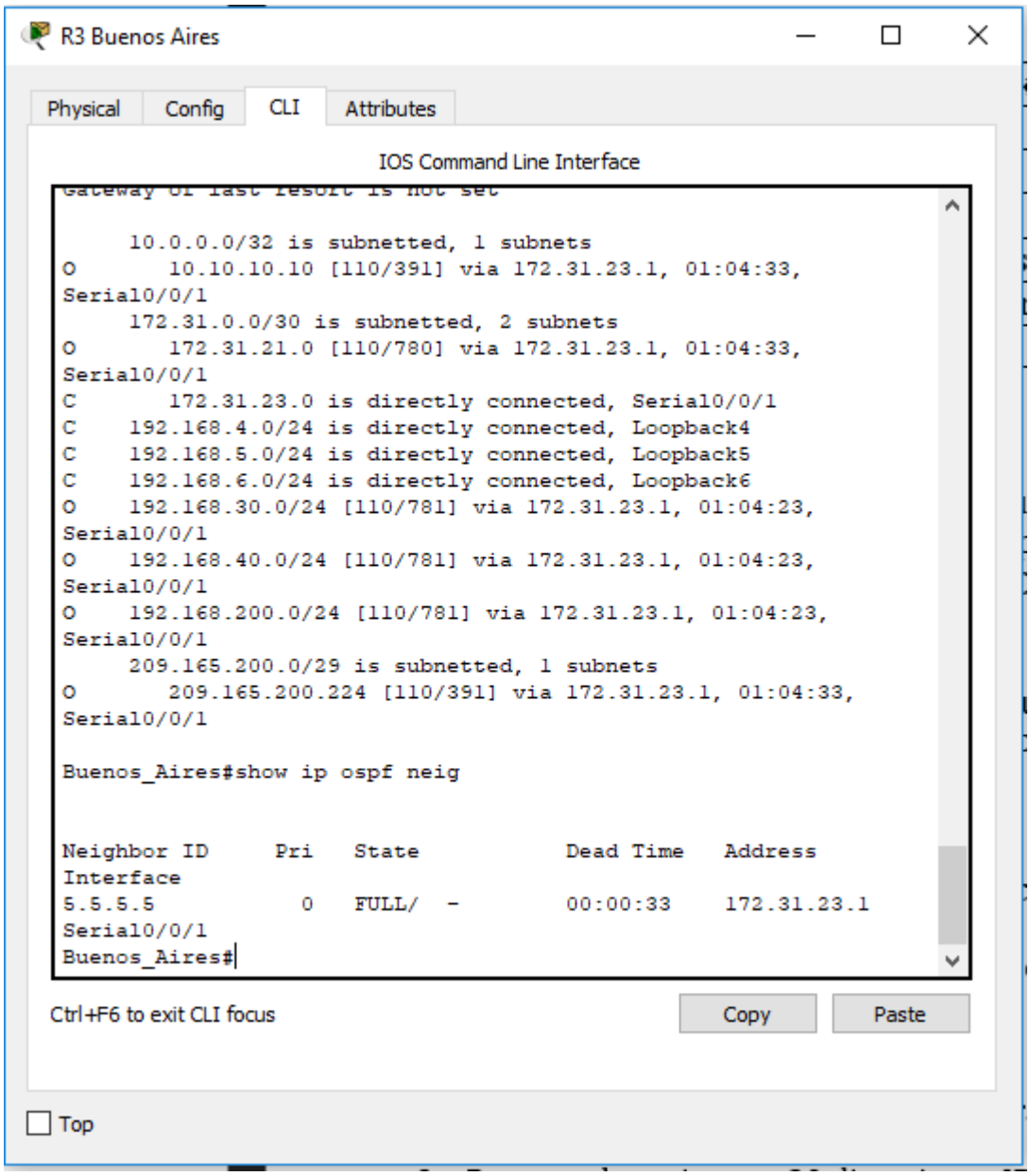
ingresamos el comando show ip ospf neighbor, es decir, consultar cuales son los vecinos.

Ilustración 23: Tabla de enrutamiento R2



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

Ilustración 24: Tabla de enrutamiento R3

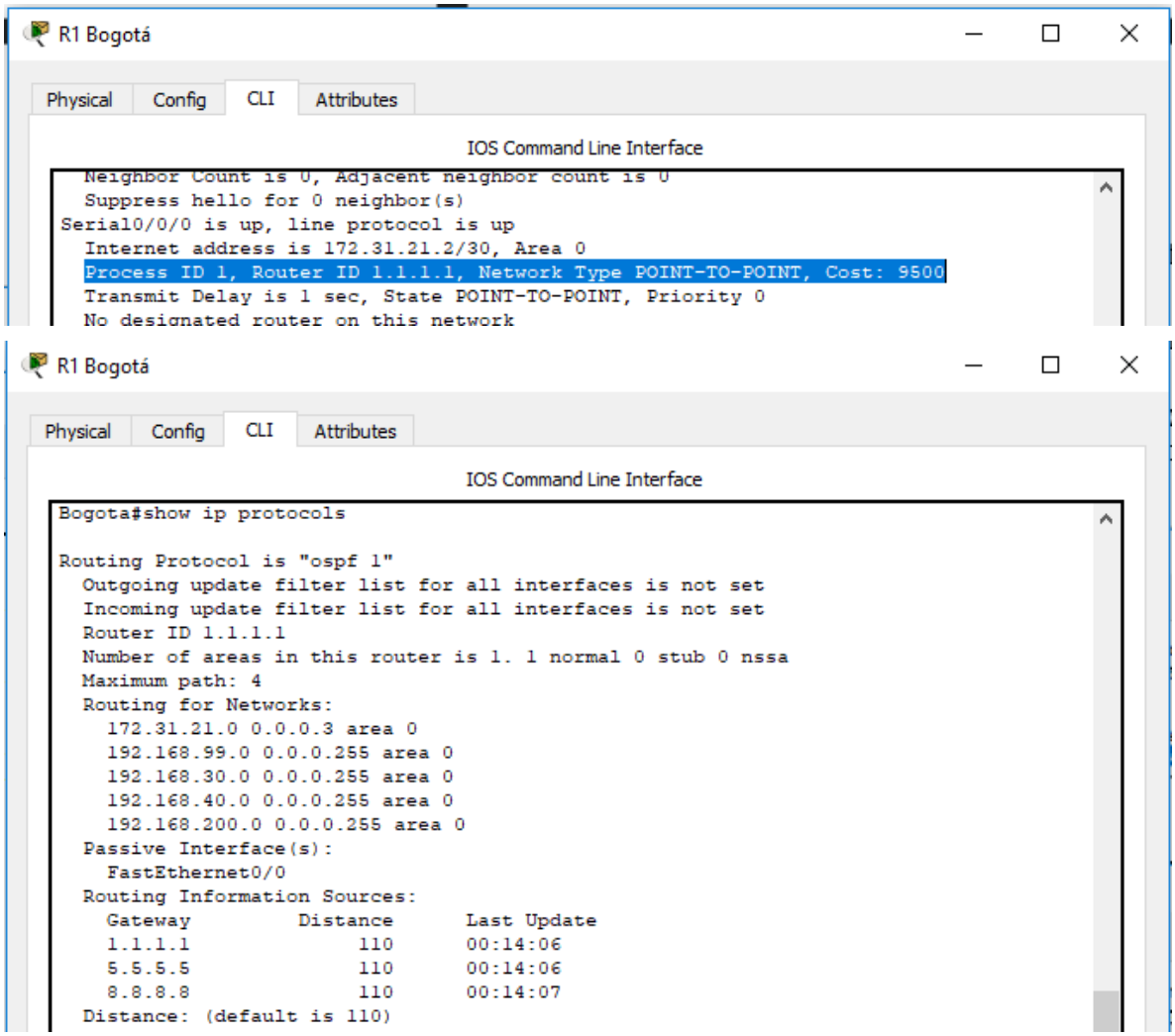


En esta imagen, vemos a R3, el cual tiene un solo vecino conectado en la interfaz s0/0/1.

Cada uno de los router, tiene en su tabla de enrutamiento las rutas que sus router vecinos le proporcionan mediante el protocolo de OSPF, por ejemplo, en R3 está la ruta 192.168.200.0/24 red que se encuentra en el R1, pero que es posible alcanzarla, al salir por la 172.31.23.1 y de esta manera evitamos la complicación que implicaría estar ingresando manualmente las rutas.

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

Ilustración 215: Verificación en R1

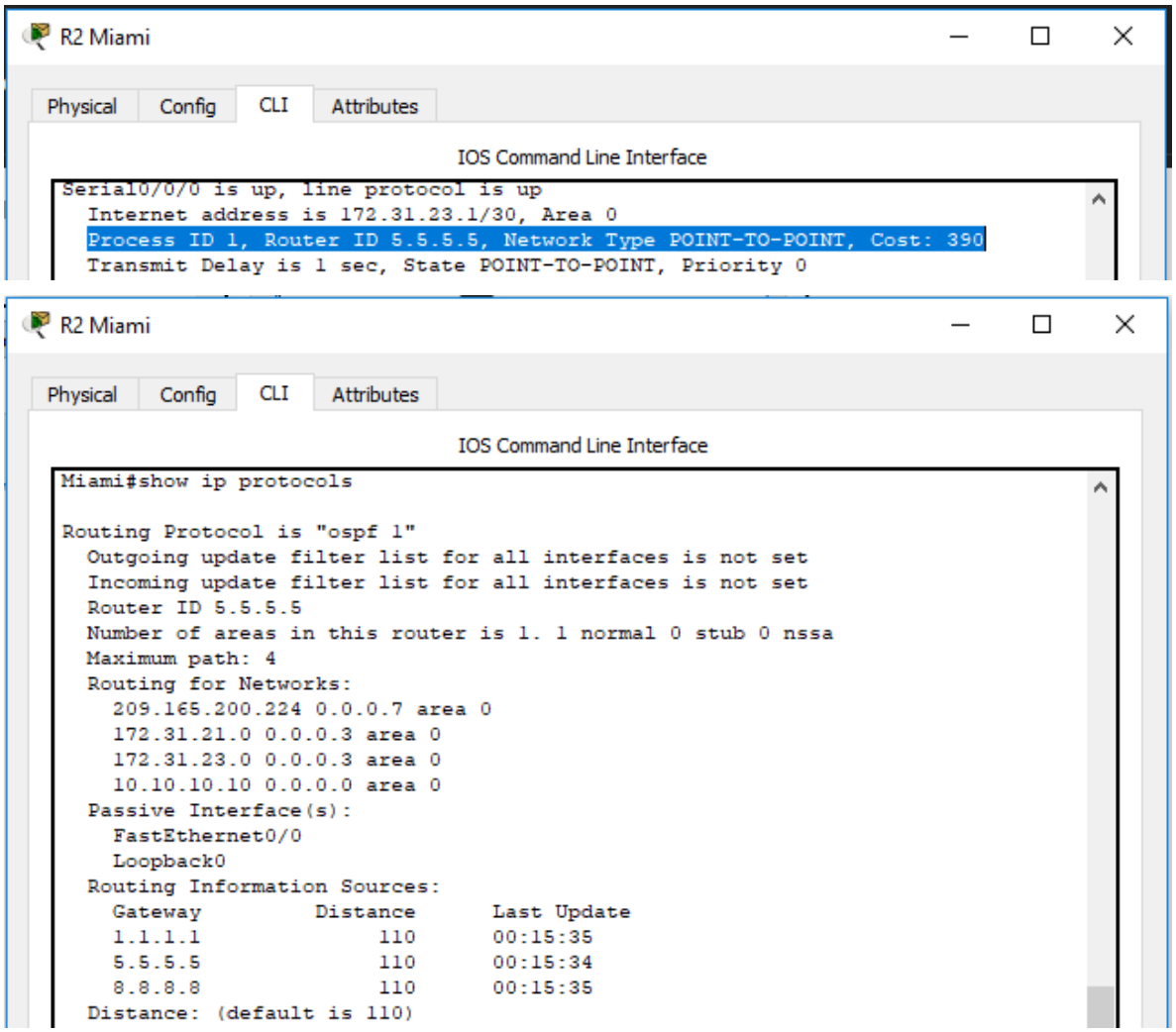


En esta gráfica, podemos apreciar el costo de las interfaces, al final de la línea resaltada y su valor es 9500. Información obtenida mediante el comando “show ip ospf interface”

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

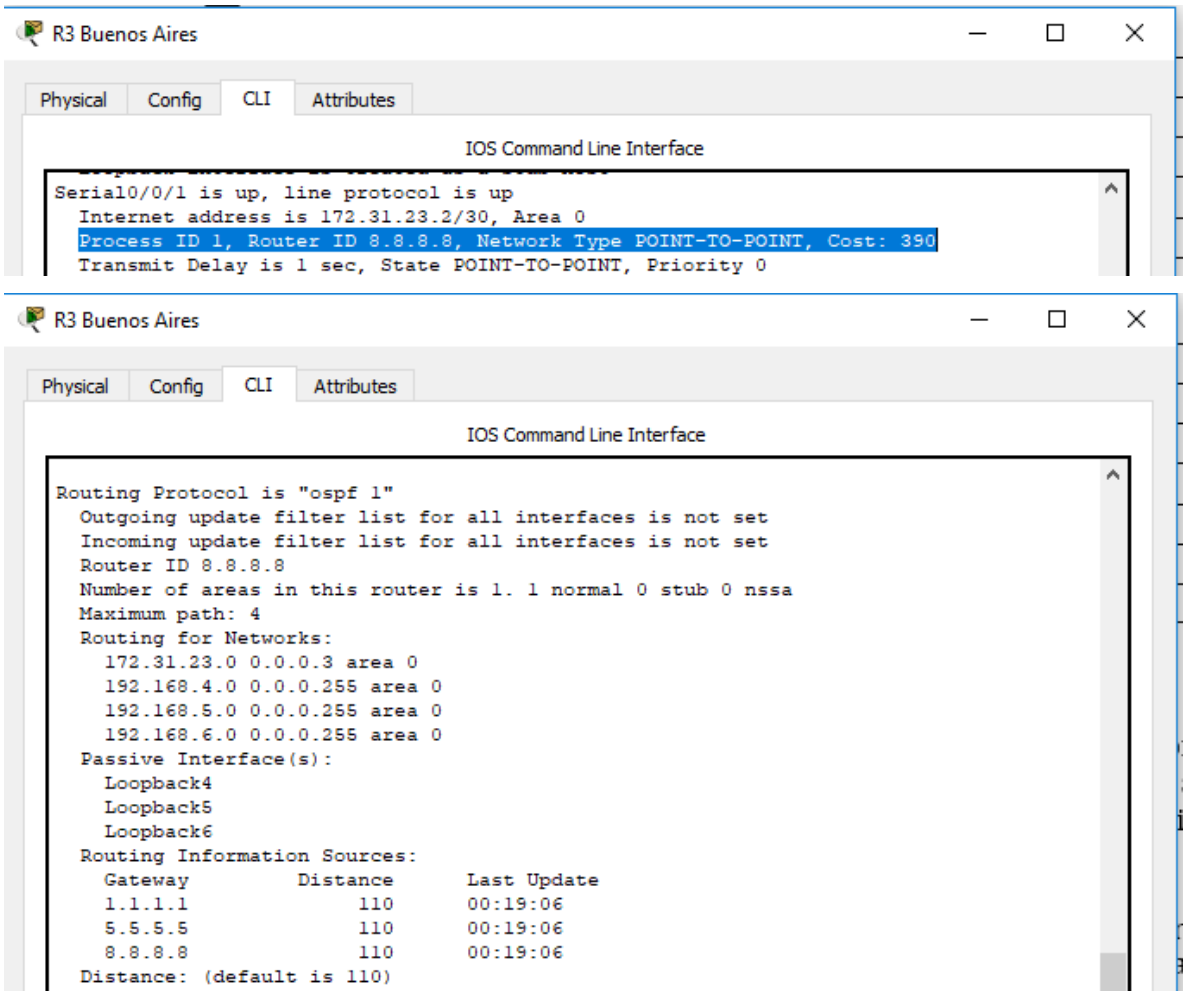
Por último, con el comando “show ip protocols”, podemos conocer cuales son las interfaces pasivas y las redes enrutadas,

Ilustración 226: Verificación en R2



La imagen nos muestra Información obtenida con los comandos anteriormente explicados, para R2.

Ilustración 237: Verificación en R3



Información obtenida con los comandos anteriormente explicados, para R3

3.4. Configuración switches

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

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

Para SW1

enable
configure terminal
vlan 30
vlan 40
interface fa0/3
switchport mode trunk
interface fa0/24
switchport mode trunk
interface FastEthernet0/1
switchport access vlan 30
switchport mode access
exit
enable secret dwaight
enable password DWIGHT_1
line console 0
password DWIGHT
login
line vty 0 4
password DWIGHT
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
interface fa0/3

```
switchport mode trunk
interface FastEthernet0/1
switchport access vlan 40
switchport mode access
exit
enable secret DWIGHT
enable password DWIGHT _1
line console 0
password DWIGHT
login
line vty 0 4
password DWIGHT
login
banner motd x Prohibido el Acceso no Autorizado! x
service password-encryption
end
copy running-config startup-config
```

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

3.5. Deshabilitar DNS lookup

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

En el Switch 3 deshabilitar DNS lookup

ena

conf ter

no ip domain-lookup

end

copy running-config startup-config

3.6. Asignación de direcciones IP a los switches

Asignar direcciones IP a los Switches acorde a los lineamientos.

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

El script:

Para SW1:

ena

conf ter

vlan 200

inter vlan 200

ip addr 192.168.200.2 255.255.255.0

end

copy running-config startup-config

Para SW3:

enable

configure terminal

vlan 200

inter vlan 200

ip addr 192.168.200.3 255.255.255.0

end

copy running-config startup-config

3.7. Desactivación Puertos

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

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

El script:

Para SW1:

ena

conf ter

inter range f0/2 , f0/4-23

shut

end

copy running-config startup-config

Para SW3:

ena

conf ter

inter range f0/2 , f0/4-24

shut

end

copy running-config startup-config

3.8. Implementación DHCP y NAT para IPv4

- Configurar R1 como servidor DHCP para las VLANs 30 y 40.
- Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

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

Comenzaremos con la configuración de DHCP, para esto, 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.

La línea de comandos:

Configuración DHCP IPv4

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

3.9. Configuración NAT

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

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

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

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

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:

La línea de comandos:

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

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

El script:

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

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

verifiquemos:

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

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

Ahora hagámoslo con una extendida:

El script:

ena

conf ter

inter f0/0.40

ip access-group list_3 in

end

copy running-config startup-config

verifiquemos:

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

3.11. Verificación comunicación

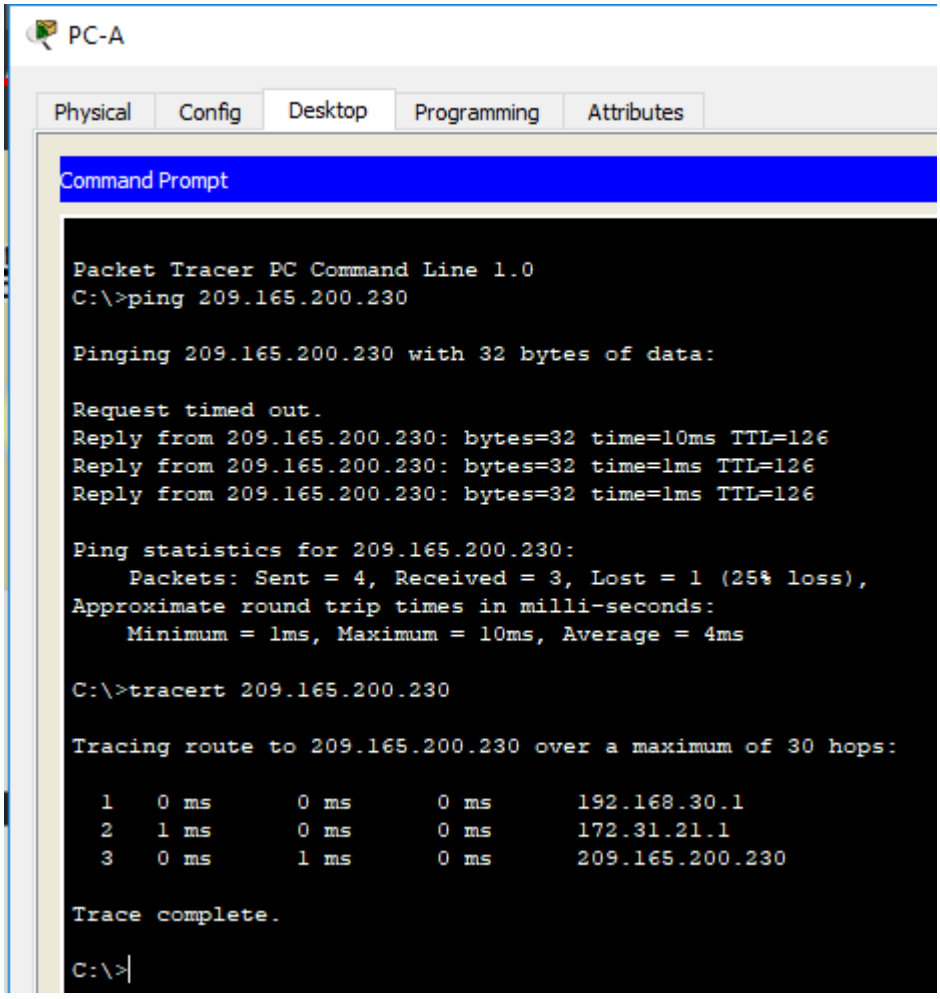
Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

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

Así las cosas:

Desde PC-A:

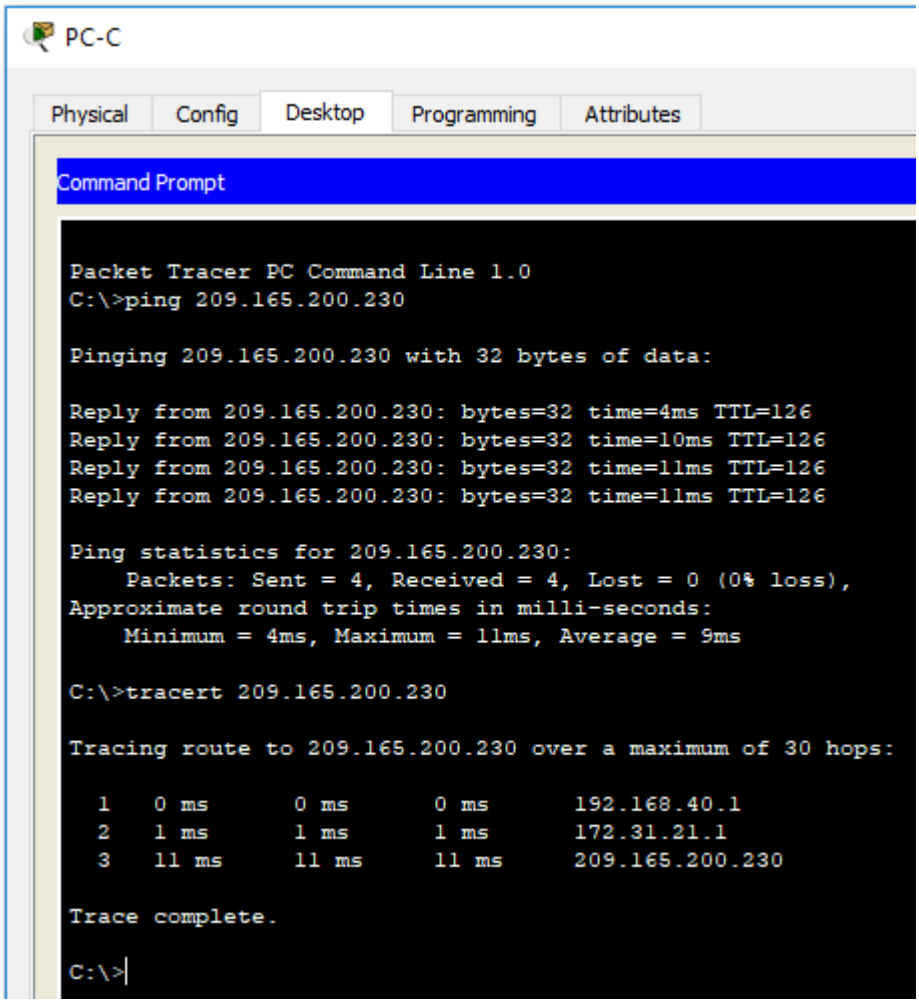
Ilustración 24: PC-A pruebas de conectividad



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 25: PC-C pruebas de conectividad



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

CONCLUSIONES

- Esta práctica, pone sobre la mesa, lo importante que es para el ingeniero dedicado a las redes conocer al detalle estas tecnologías, NAT, enrutamiento, DHCP ya que esto es implementado todo el tiempo en redes, ya sean pequeñas o grandes,

- La mínima configuración básica del switch debe incluir desde el nombre del dispositivo, es decir el nombre con el cuál se va a referir en la configuración, la forma detallada de la estructura de interfaces que lo componen, la asignación de contraseñas, el mensaje de alerta (MOTD), la tabla de direccionamiento en donde se señala la asignación de las IP, las direcciones MAC, dinámicas o estática y administración remota del switch.

BIBLIOGRAFÍA

CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1. (s.f.).

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1. (s.f.).

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1. (s.f.).

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. recuperado de https://static-course assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1. (s.f.).