INFORME PRUEBAS DE HABILIDADES PRÁCTICAS CCNA

YANETH MARCELA RODRÍGUEZ VINASCO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTÓNICA
MEDELLÍN
2018

INFORME PRUEBAS DE HABILIDADES PRÁCTICAS CCNA

YANETH MARCELA RODRÍGUEZ VINASCO

CÓDIGO: 1.088.248.071

Informe presentado para optar por el título de ingeniera electrónica.

Asesor
Nilson Albeiro Ferreira Manzanares
Docente de la facultad de ciencias básicas e ingeniería

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
FACULTAD DE CIENCIAS BÁSICAS E INGENIERÍA
PROGRAMA DE INGENIERÍA ELECTÓNICA
MEDELLÍN
2018

TABLA DE CONTENIDO

LISTA DE FIGURAS

INTRODUCCIÓN

Desde hace tres décadas que la comunidad científica comenzó a buscar la forma de compartir información de forma rápida y efectiva, el internet ha evolucionado a pasos agigantados. La primera red que permitió la comunicación entre muchas universidades desarrolló la conmutación de paquetes los cuáles podían tomar diversos caminos dependiendo de la saturación de la red.

Con la expansión de las redes fue necesario implementar protocolos y estándares que permitieran la comunicación entre diversos dispositivos. El protocolo TCP/IP define cuidadosamente como se mueve la información desde el remitente hasta el usuario, mediante la aplicación de capas.

El routing consiste en mover paquetes o información a nivel de una red de internet hasta otra, buscando un camino entre todos los posibles por diferentes topologías que poseen gran conectividad. Se consideran parámetros como el número de saltos (los equipos por donde pasa el paquete de un punto a otro de la red), el tiempo de retardo, y el coste de comunicación de un paquete transmitido.

También es importante tener en cuenta la seguridad de la información, por lo que se deben implementar soluciones en varias capas puesto que no existe una solución única y el conocer como parametrizar los routers y suiches permite mejorar la seguridad de la red.

En el presente trabajo se encuentra el desarrollo de dos escenarios que hacen parte del diplomado de profundización de Switching and Routing (CCNA 1 y CCNA 2) de CISCO de la Universidad Nacional Abierta y a Distancia UNAD del programa ingeniería electrónica. Mediante el análisis de los dos escenarios se pretende validar los conceptos y destrezas del software de simulación y de la solución de problemas en los elementos que componen las redes de datos.

1. DESARROLLO DE LOS ESCENARIOS

1.1 Escenario 1.

Topología:

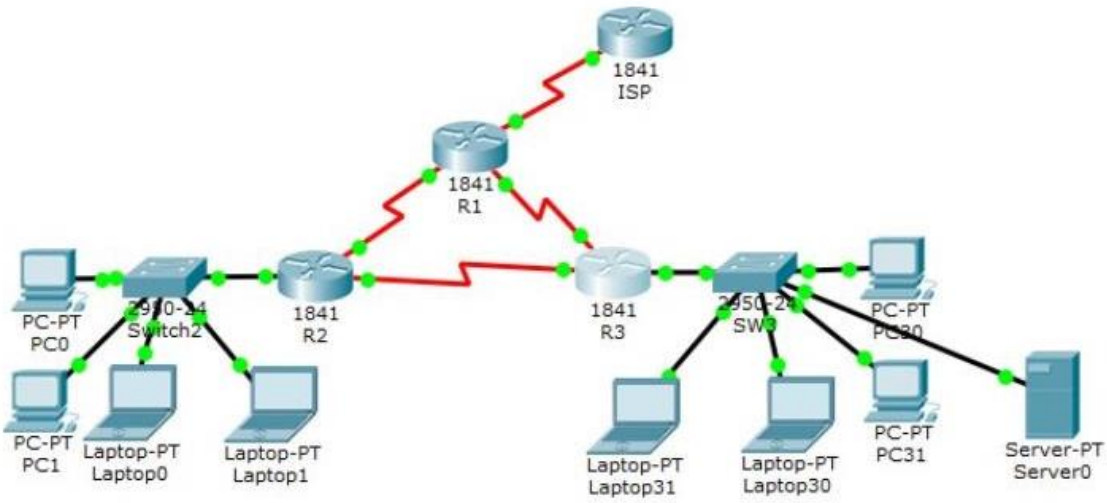

Figura 1 Topología

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
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

Figura 2 Tabla de direcciones

Tabla de asignación de VLAN's y puertos

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

Figura 3 Asignación de VLAN's

Tabla de enlaces troncales:

Dispositivo local	Interfaz local	Dispositivo remoto
SW2	Fa0/2-3	100

Figura 4 Enlaces

Descripción de la actividad:

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

```
SW2(config)#vlan 100
SW2(config-vlan)#name LAPTOPS
SW2(config-vlan)#EXIT
SW2(config)#vlan 200
SW2(config-vlan)#name DESTOPS
SW2(config-vlan)#EXIT
SW2(config)#interface range fa0/2-3
SW2(config-if-range)#switchport access vlan 100
SW2(config-if-range)#exit
SW2(config)#interface range fa0/4-5
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 200
SW2(config-if-range)#exit
SW2(config)#interface range fa0/4-5
SW2(config-if-range)#switchport mode trunk
SW2(config-if-range)#exit
```

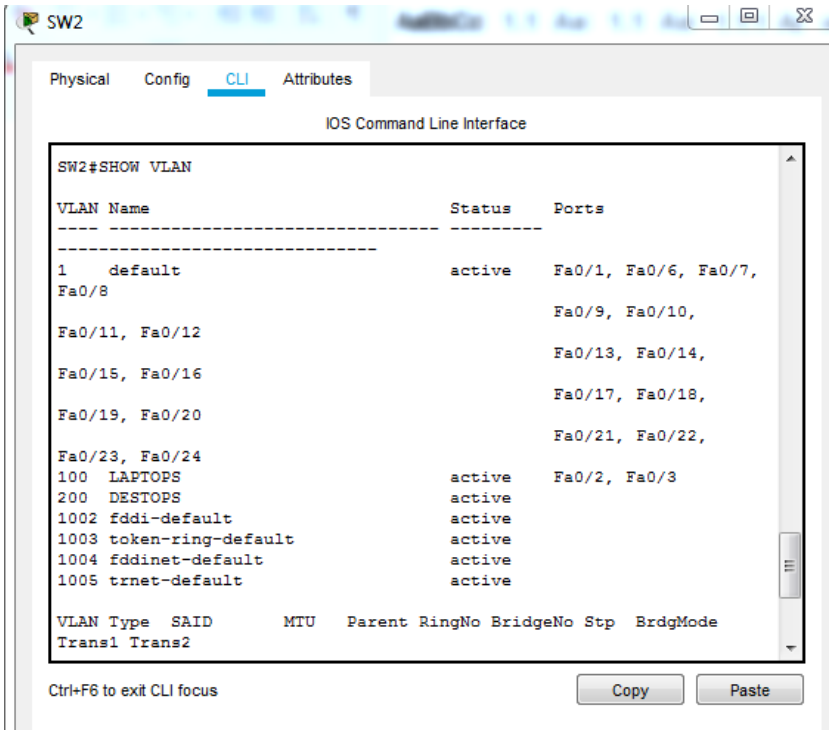

Figura 5 Configuración de interfaces SW2

SW3(config)#interface range fa0/1-24
SW3(config-if-range)#switchport mode acces
SW3(config-if-range)#switchport access vlan 1

Verificación:

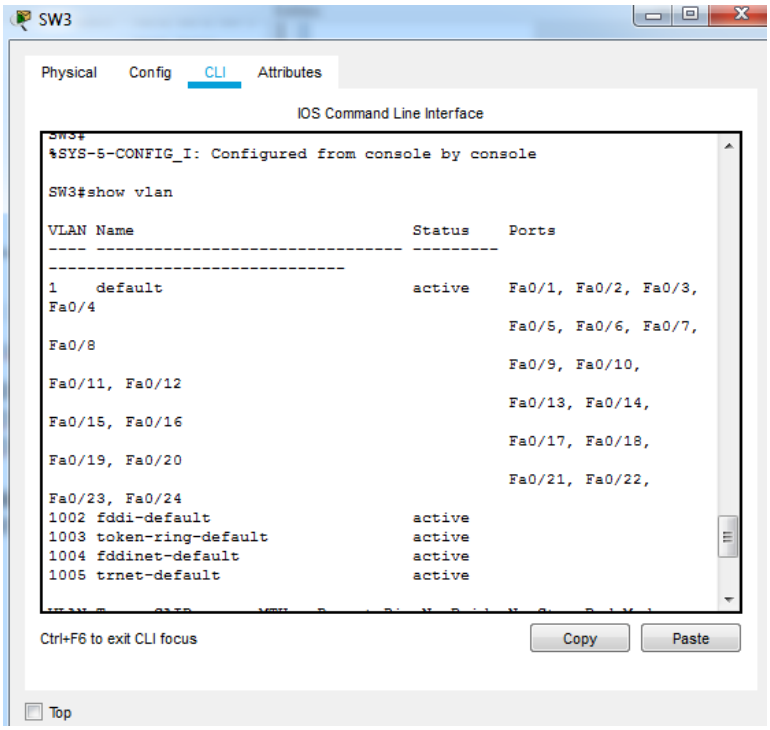

Figura 6 Configuración de interfaces SW3

1.1.2 Deshabilitar los puertos de red que no se utilizan.

Para el suiche 2:

SW2(config)#interface range fa0/6-24
SW2(config-if-range)#shutdown

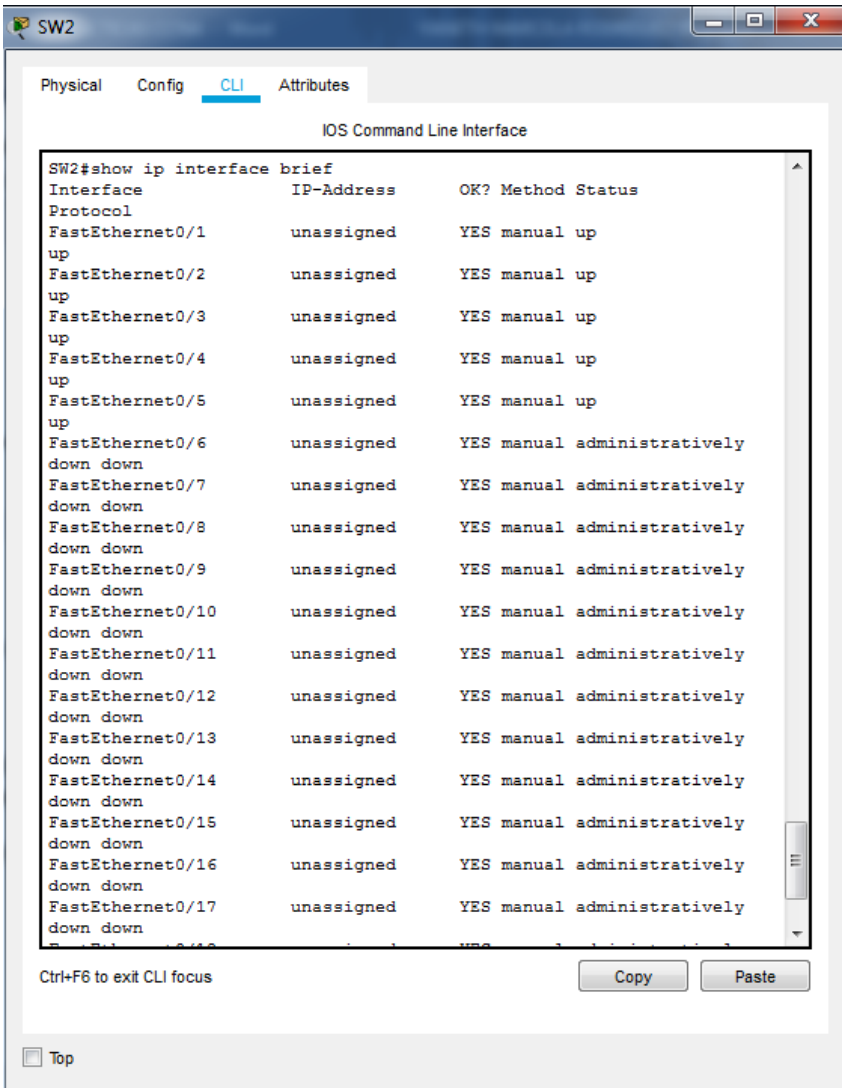

Figura 7 Puertos deshabilitados SW2

Para el suiche 3:
SW3(config)#interface range fa0/7-24
SW3(config-if-range)#shutdown

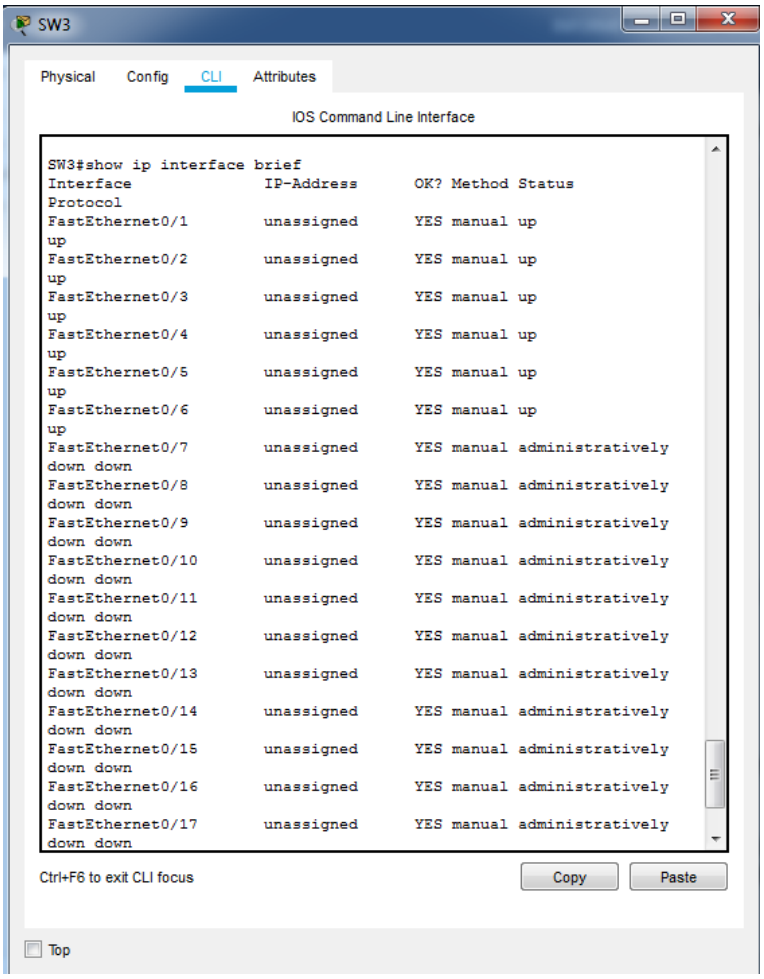

Figura 8 Puertos deshabilitados SW3

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

Configuración del router 1:
Router>enable
Router#configure terminal
Router(config)#hostname R1

R1(config)#interface s0/0/0
R1(config-if)#ip address 200.123.211.2 255.255.255.0
R1(config-if)#clock rate 19200
R1(config-if)#no shutdown

R1(config)#interface s0/1/0

R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#no shutdown

R1(config)#interface s0/1/1
R1(config-if)#ip address 10.0.0.5 255.255.255.252
R1(config-if)#clock rate 19200
R1(config-if)#no shutdown

Para el router 2:

R2(config)#interface s0/0/0
R2(config-if)#ip address 10.0.0.2 255.255.255.252
R2(config-if)#clock rate 19200
R2(config-if)#no shutdown

R2(config)#interface s0/0/1
R2(config-if)#ip address 10.0.0.9 255.255.255.252
R2(config-if)#clock rate 19200
R2(config-if)#no shutdown
R2#configure terminal
R2(config)#interface fa0/0.100
R2(config-subif)#encapsulation dot1Q 100
R2(config-subif)#ip address 192.168.20.1 255.255.255.0
R2(config-subif)#interface fa0/0.200
R2(config-subif)#encapsulation dot1Q 200
R2(config-subif)#ip address 192.168.21.1 255.255.255.0

Activación del Puerto:

R2(config)#interface fa0/0
R2(config-if)#no shutdown

Verificación:

```
R2#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        unassigned      YES NVRAM  up
up
FastEthernet0/0.100    192.168.20.1    YES manual up
up
FastEthernet0/0.200    192.168.21.1    YES manual up
up
FastEthernet0/1        unassigned      YES NVRAM  administratively
down down
Serial0/0/0            10.0.0.2        YES NVRAM  up
down
Serial0/0/1            10.0.0.9        YES NVRAM  up
up
```

Figura 9 Verificación de puertos R2

Para el router 3:

Router>enable
Router#configure terminal
Router(config)#hostname R3

Para la IPv4
R3(config)#interface fa0/0
R3(config-if)#ip address 192.168.30.1 255.255.255.0
R3(config-if)#no shutdown

Para la IPv6
R3(config)#ipv6 unicast-routing
R3(config)#interface fa0/0
R3(config-if)#ipv6 address 2001:db8:130::9c0:80f:301/64
R3(config-if)#no shutdown

R3(config)#interface s0/0/0
R3(config-if)#ip address 10.0.0.6 255.255.255.252
R3(config-if)#no shutdown

R3(config)#interface s0/0/1
R3(config-if)#ip address 10.0.0.10 255.255.255.252
R3(config-if)#clock rate 19200
R3(config-if)#no shutdown

Verificación de las interfaces IPv4:

```
R3#show ip interface brie
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        192.168.30.1    YES manual up
up
FastEthernet0/1        unassigned      YES unset  administratively
down down
Serial0/0/0            10.0.0.6        YES manual up
up
Serial0/0/1            10.0.0.10       YES manual down
```

Figura 10 Verificación de puertos R2

Verificación de las interfaces IPv6:

```
R3#show ipv6 interface brief
FastEthernet0/0            [up/up]
    FE80::202:4AFF:FE9E:5301
    2001:DB8:130::9C0:80F:301
```

Figura 11 Verificación de puertos R3

Router>enable
Router#configure terminal
Router(config)#hostname ISP

ISP(config)#interface s0/0/0
ISP(config-if)#ip address 200.123.211.1 255.255.255.0
ISP(config-if)#no shutdown
Verificación:

```
ISP#show ip interface brief
Interface              IP-Address      OK? Method Status
Protocol
FastEthernet0/0        unassigned      YES unset  administratively
down down
FastEthernet0/1        unassigned      YES unset  administratively
down down
Serial0/0/0            200.123.211.1   YES manual up
up
```

Figura 12 Configuración puerto ISP

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

A continuación, se muestra la configuración realizad a cada host:

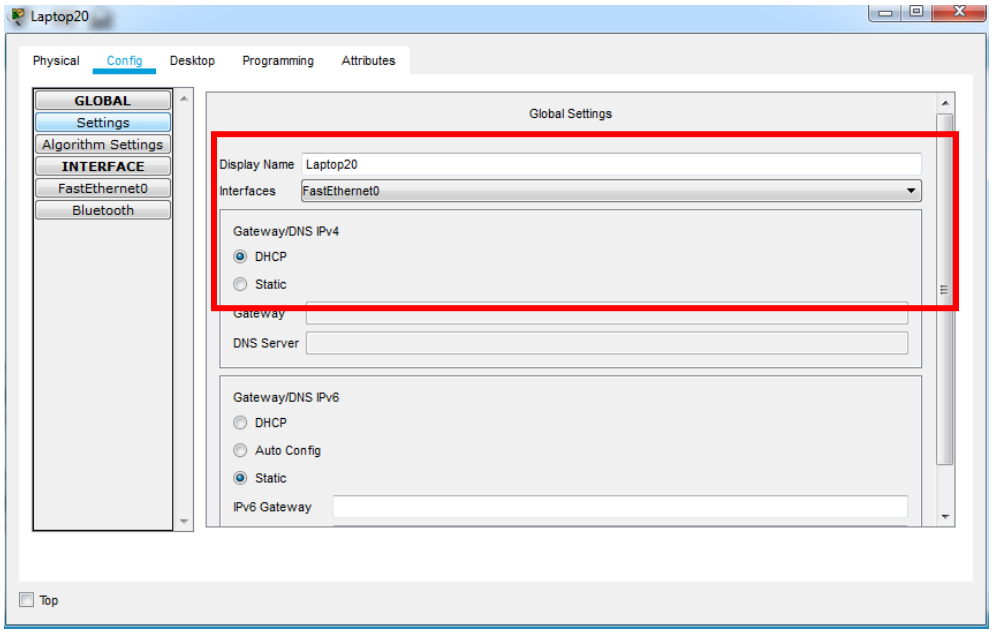

Figura 13 Configuración de puerto Laptop20

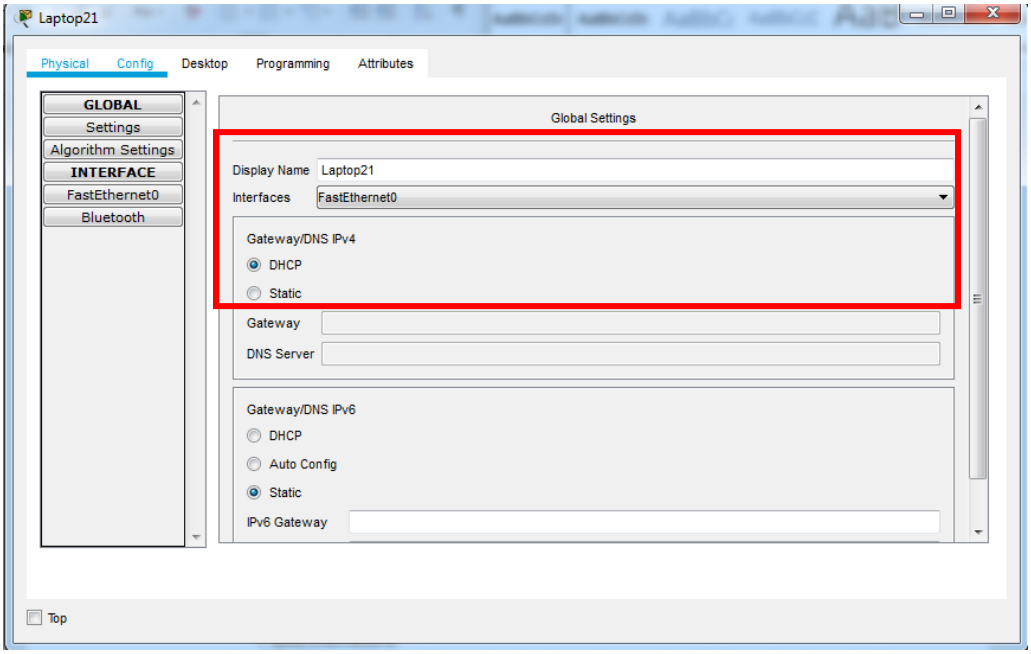

Figura 14 Configuración de puerto Laptop 21

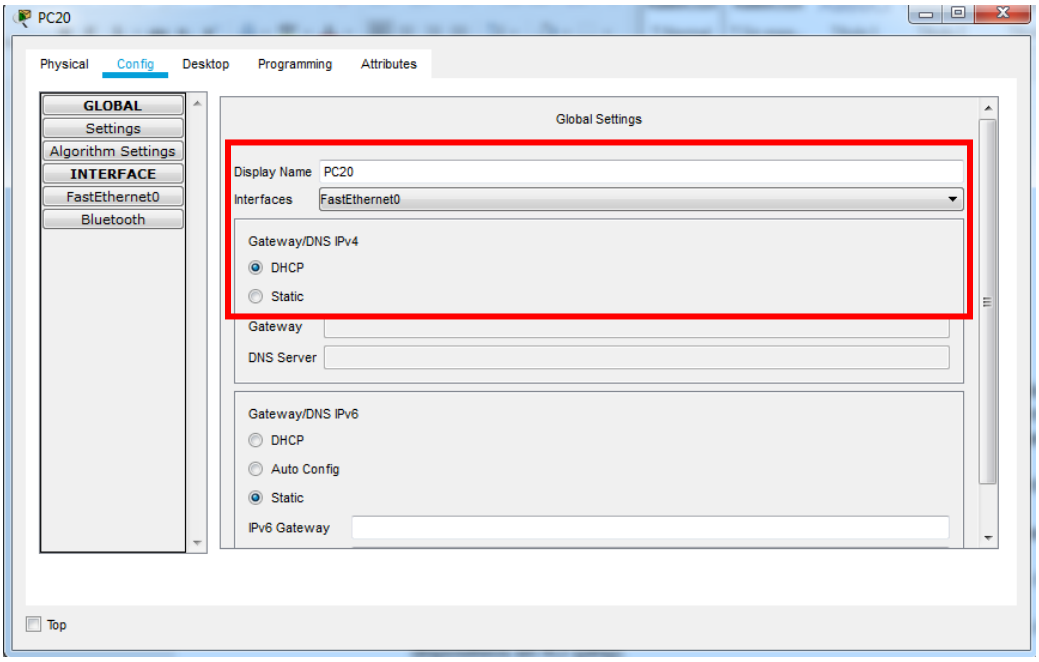

Figura 15 Configuración DHCP PC20

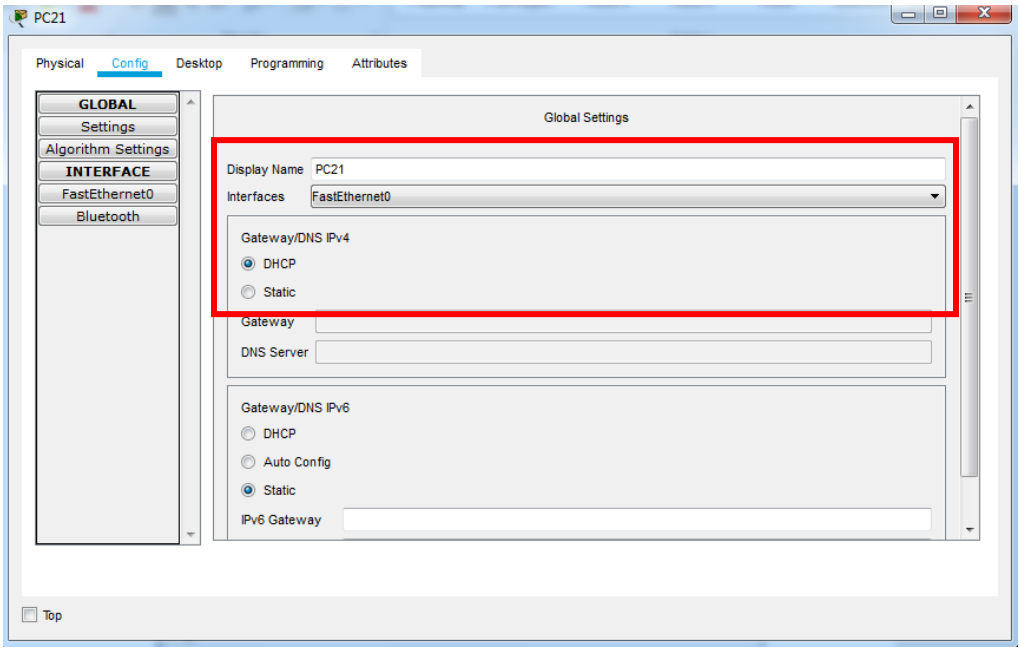

Figura 16 Configuración DHCP PC21

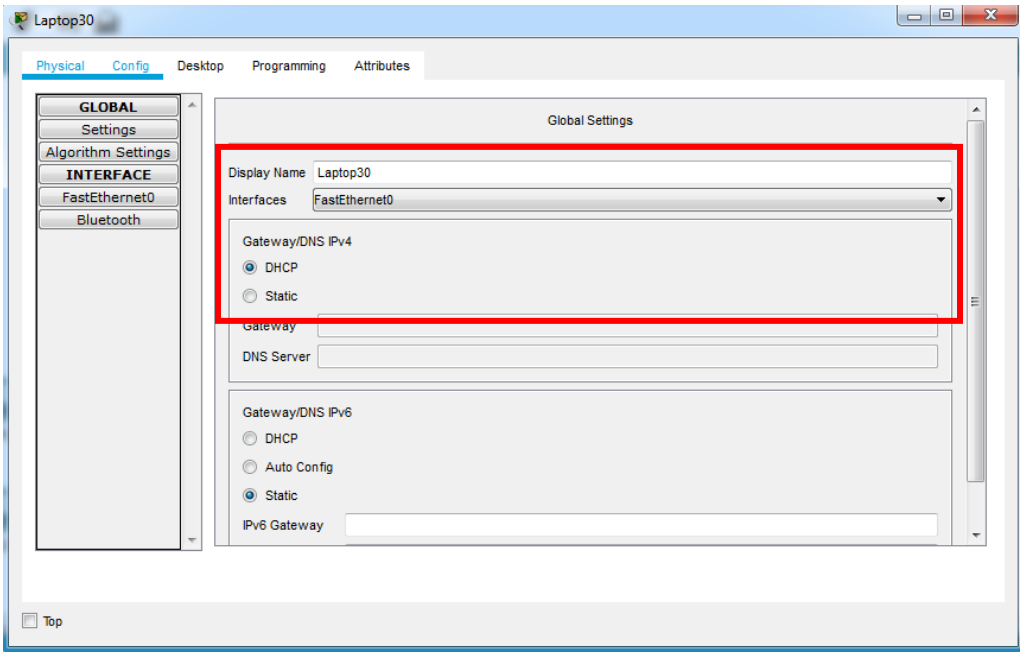

Figura 17 Configuración DHCP Laptop 30

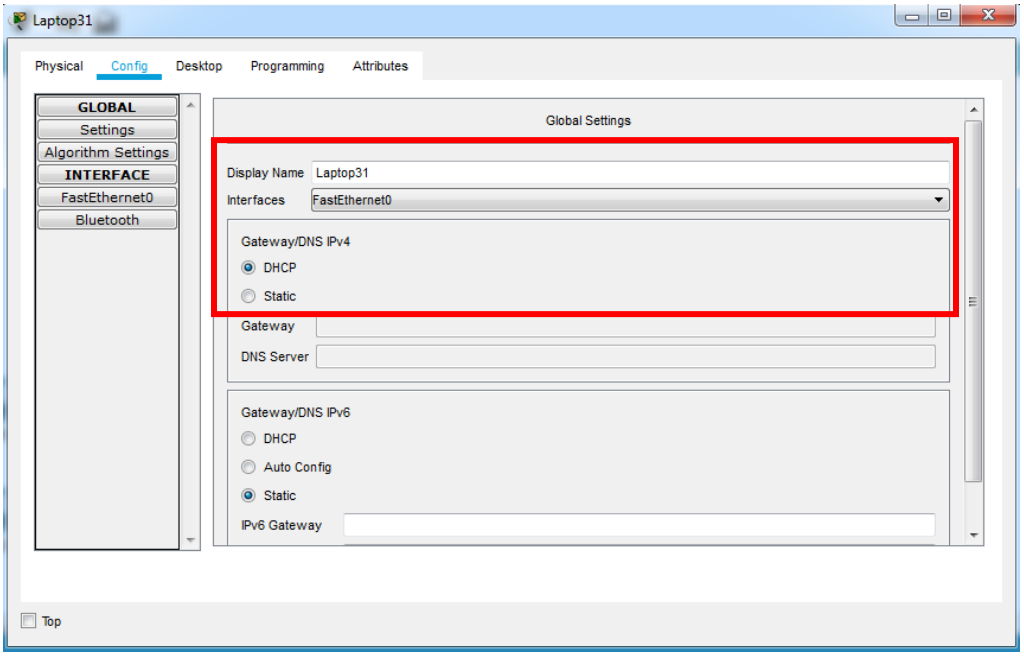

Figura 18 Configuración DHCP Laptop31

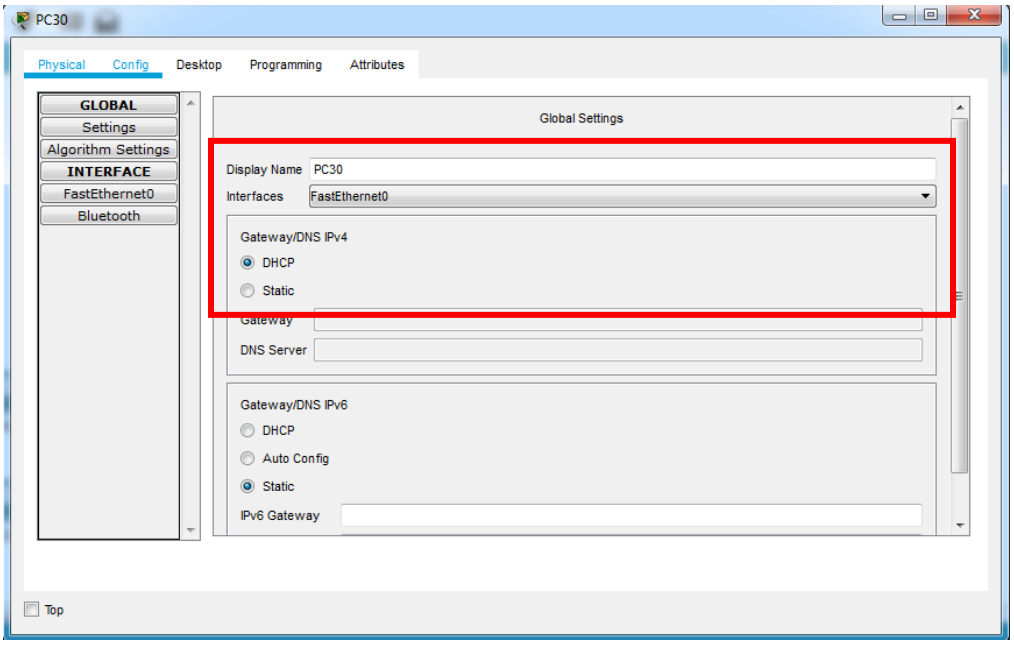

Figura 19 Configuración DHCP PC30

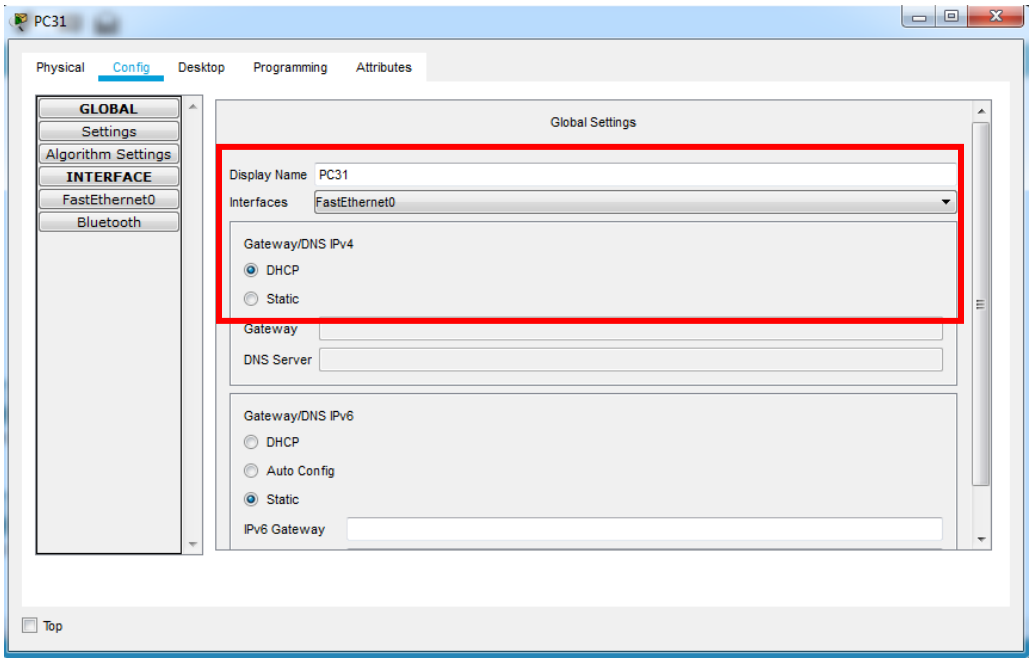

Figura 20 Configuración DHCP PC31

1.1.5 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.

Configuración de la NAT

```
R1(config)#interface s0/1/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface s0/1/1
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#ip nat pool INSIDE-DEVS 200.123.211.1 200.123.211.254 netmask 255.255.255.0
R1(config)#ip nat inside source list 1 pool INSIDE-DEVS overload
R1(config)#interface serial 0/0/0
R1(config-if)#ip nat inside
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
```

Verificación:

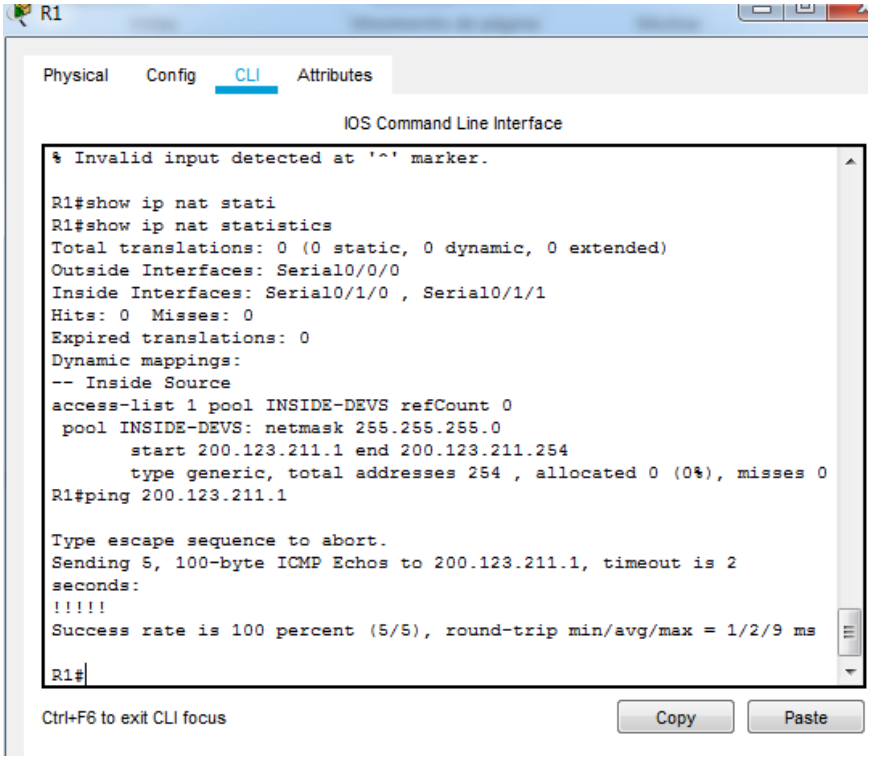

Figura 21 Verificación de NAT

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

R1(config-router)#ip route 0.0.0.0 0.0.0.0 s0/0/0

Verificación:

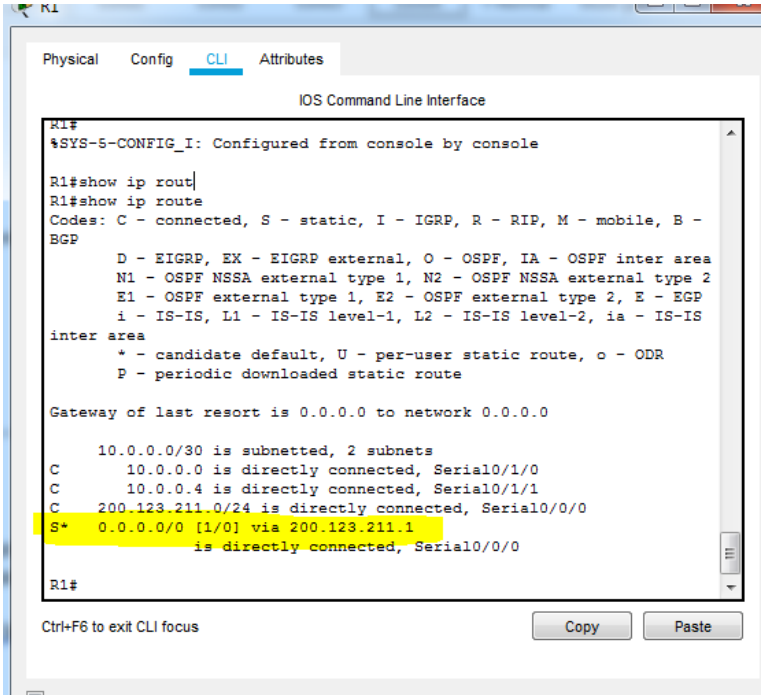

Figura 22 Vericación ruta estática

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

R2(config)#ip dhc excluded-address 10.0.0.2 10.0.0.9
R2(config)#ip dhcp pool INSIDE-DEVS
R2(dhcp-config)#network 192.168.21.100 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 0.0.0.0
R2(dhcp-config)#exit
R2(config)#ip dhcp pool LAPTOPS
R2(dhcp-config)#network 192.168.20.100 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 0.0.0.0
R2(dhcp-config)#exit

1.1.8 R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.

```
R2(config)#int vlan 100
R2(config-if)#ip address 192.168.20.1 255.255.255.0
% 192.168.20.0 overlaps with FastEthernet0/0.100
R2(config-if)#exit
R2(config)#int vlan 200
R2(config-if)#ip address 192.168.21.1 255.255.255.0
% 192.168.21.0 overlaps with FastEthernet0/0.200
R2(config-if)#end
```

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

```
R3(config)#ipv6 unicast-routing
R3(config)#int f0/0
R3(config-if)#ipv6 address 200:db8:130::9c0:80f:301/64
R3(config-if)#exit
```

Verificación de ping:

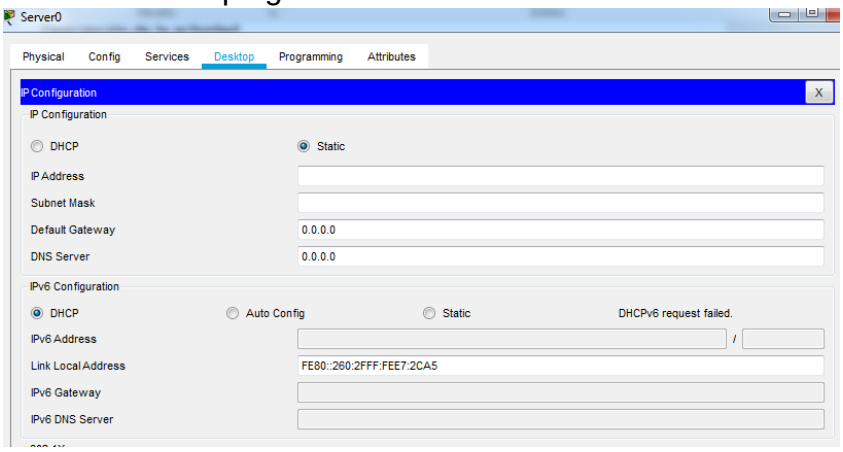

Figura 23 IPV6 del Server0

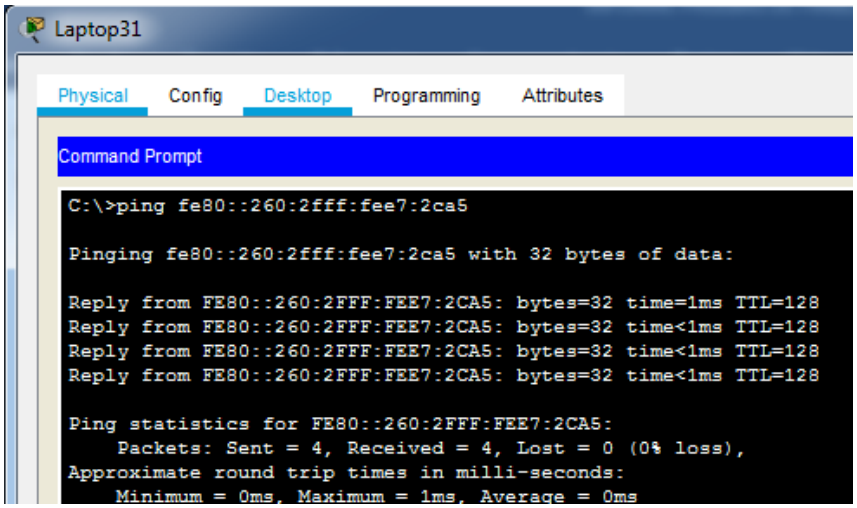

Figura 24 Verificación de ping a Server0 desde Laptop 31

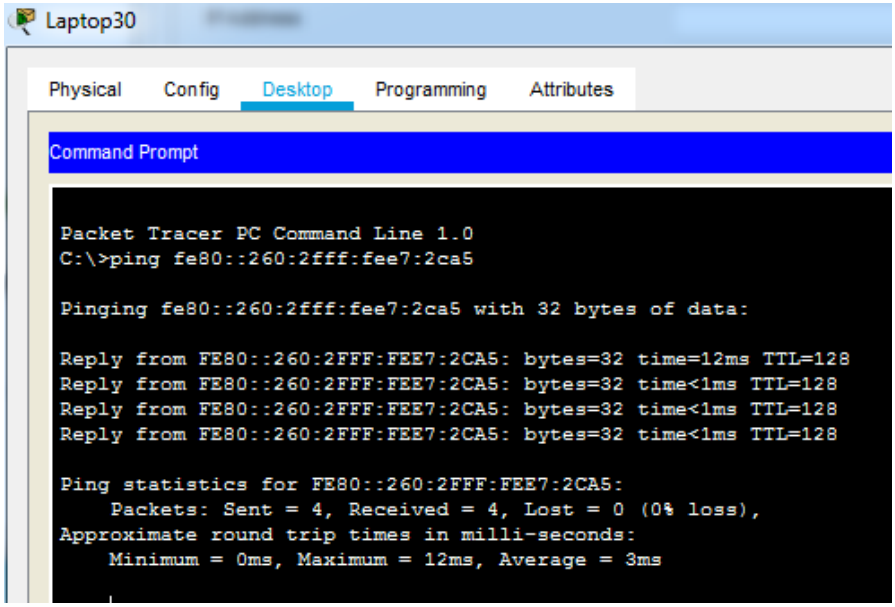

Figura 25Verificación de ping a Server0 desde Laptop 30

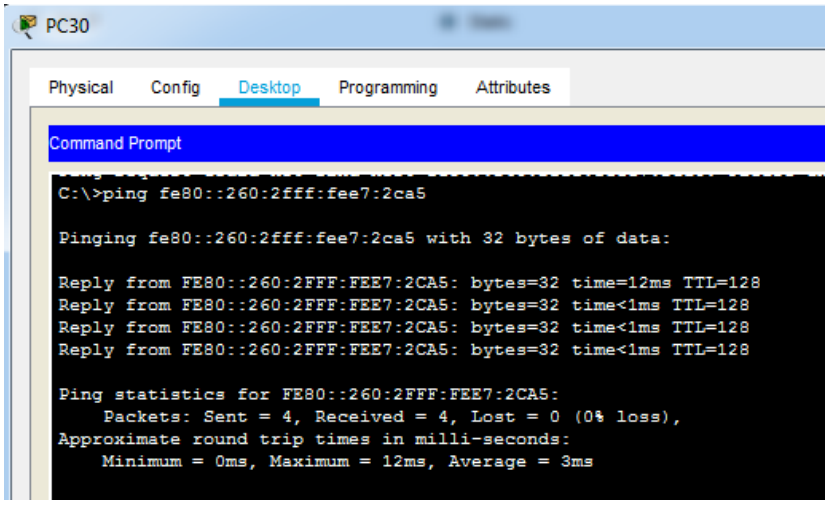

Figura 26 Verificación de ping a Server0 desde PC30

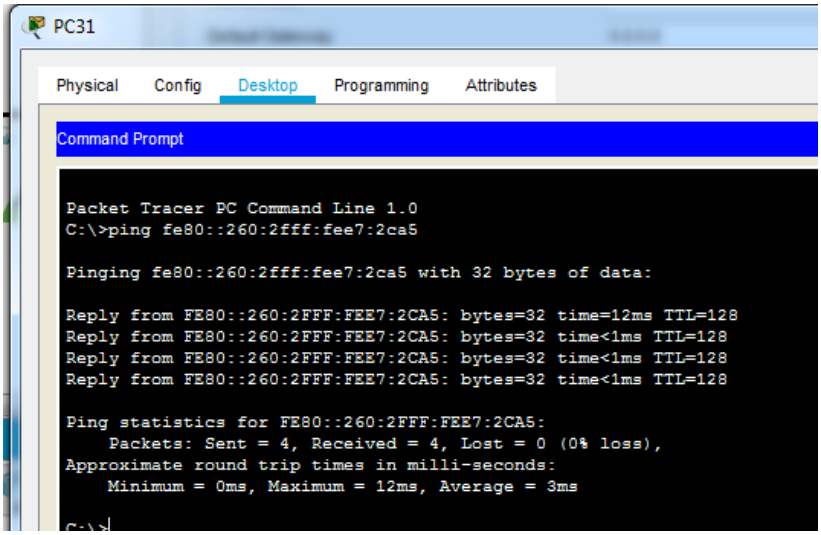

Figura 27 Verificación de ping a Server0 desde PC31

Adicionalmente se verifica que desde un pc que se encuentra fuera del router 3 no hay ping con el Server0

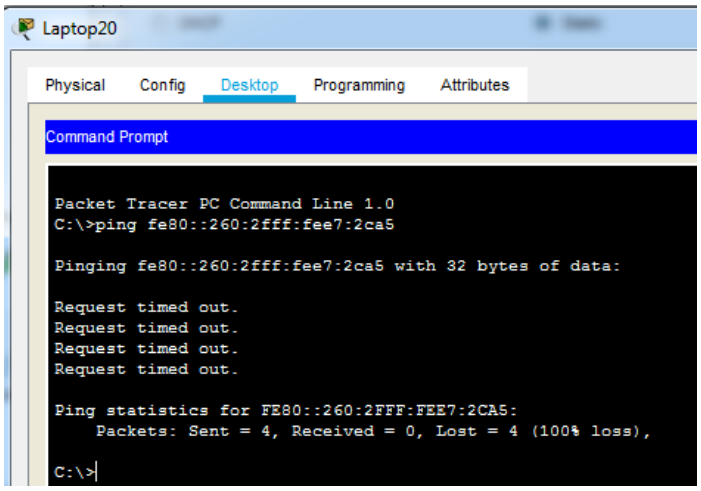

Figura 28 Verificación de No ping a Server0 desde Laptop 20

1.1.10 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.

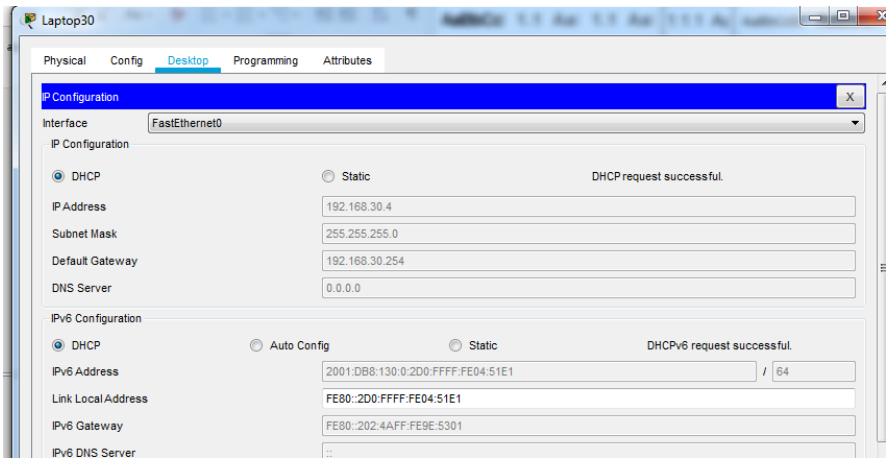

Figura 29 NIC dual Laptop30

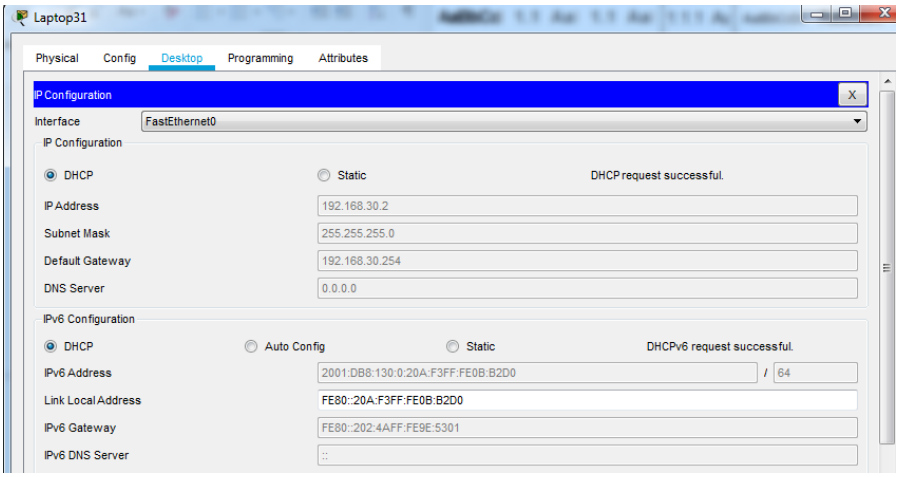

Figura 30 NIC dual Laptop31

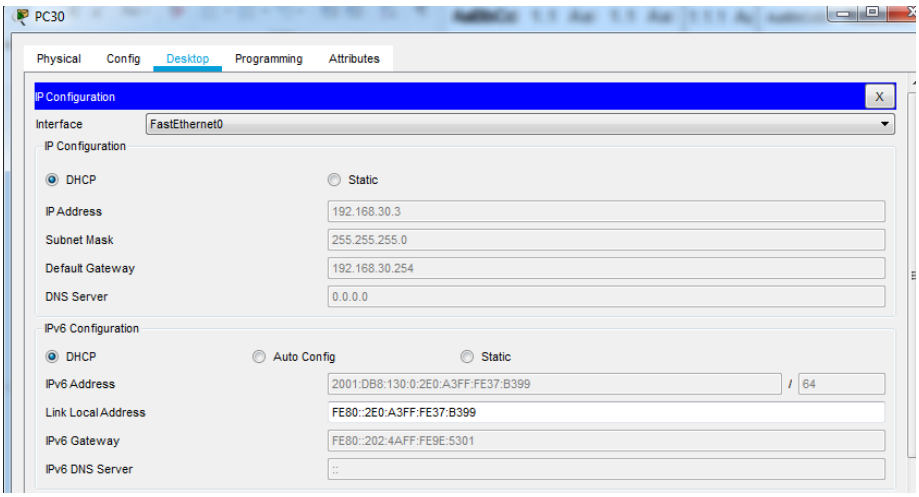

Figura 31 NIC dual PC30

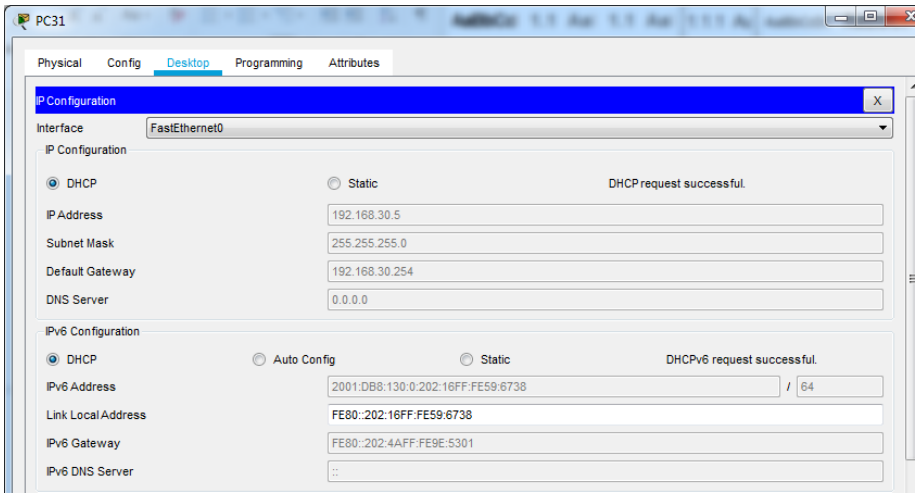

Figura 32 NIC dual PC31

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

R3(config)#ip dhcp pool DESKTOPS
R3(dhcp-config)#network 192.168.30.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.1.1
R3(dhcp-config)#end
R3(config)#ipv6 dhcp pool servidor
R3(config-dhcpv6)#prefix-delegation pool servidor
R3(config-dhcpv6)#exit
R3(config)#ipv6 general-prefix servidor 2001:db8:130::9c0:80f:300/64
R3(config)#ipv6 local pool servidor 2001:db8:130::9c0:90f:310/40 64
R3(config)#interface f0/0
R3(config-if)#ipv6 dhcp server servidor
R3(config-if)#end

Verificación:

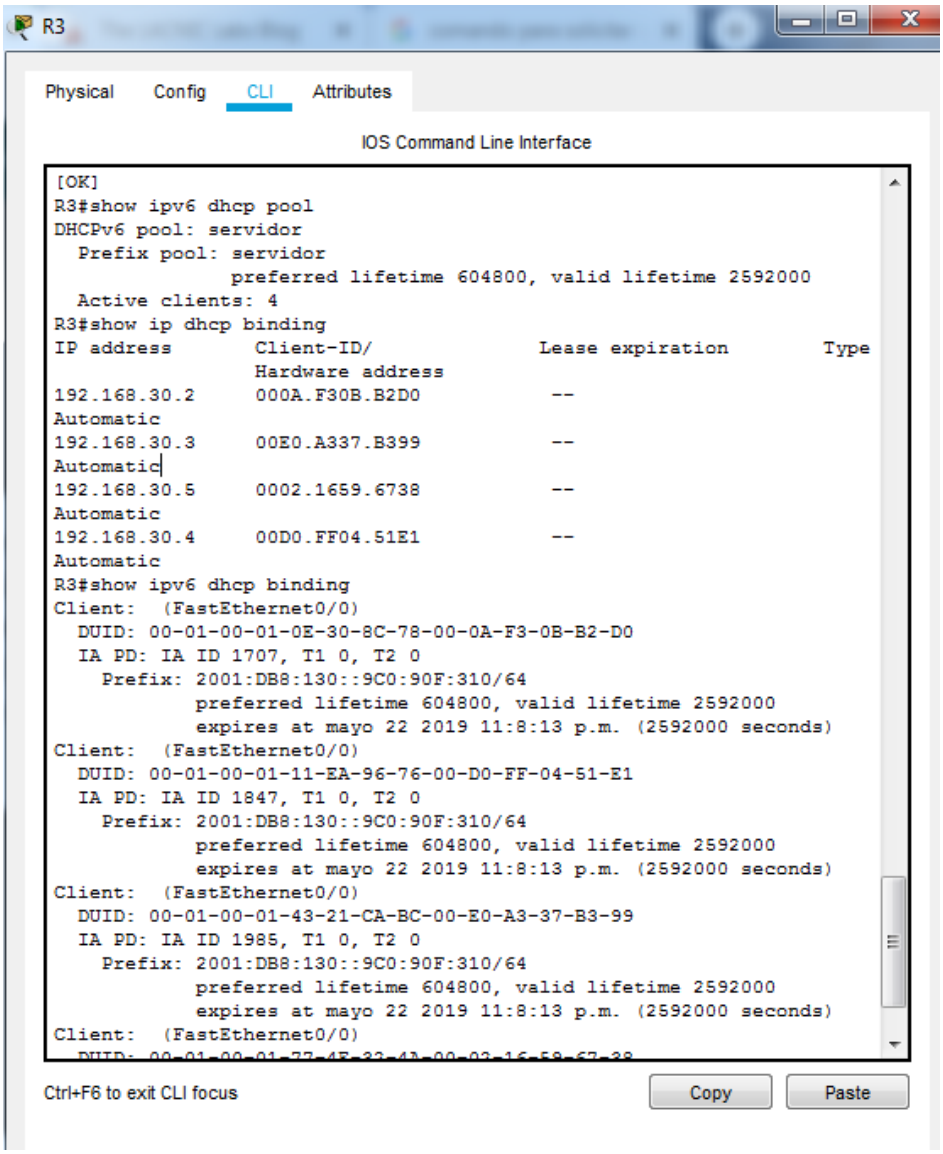

Figura 33 Verificación configuración DHCP

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

Para R1:
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 200.123.211.0
R1(config-router)#network 10.0.0.0
R1(config-router)#end

Para R2:
R2(config)#router rip

R2(config-router)#version 2
R2(config-router)#network 192.168.20.0
R2(config-router)#network 192.168.21.0
R2(config-router)#network 10.0.0.0
R2(config-router)#end

Para R3:
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 192.168.30.0
R3(config-router)#network 10.0.0.0
R3(config-router)#end

Verificación:

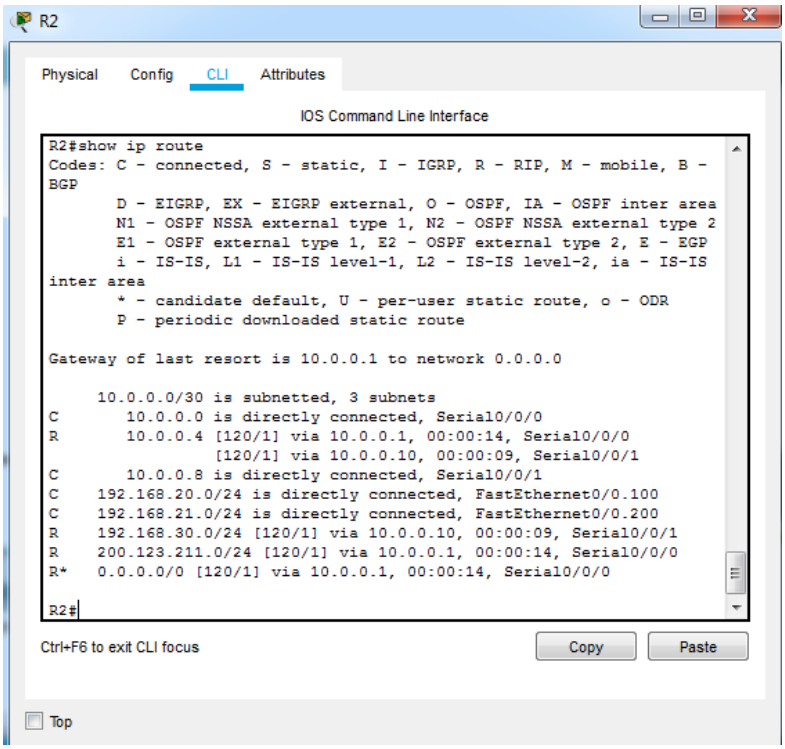

Figura 34 Verificación conexión RIP R2

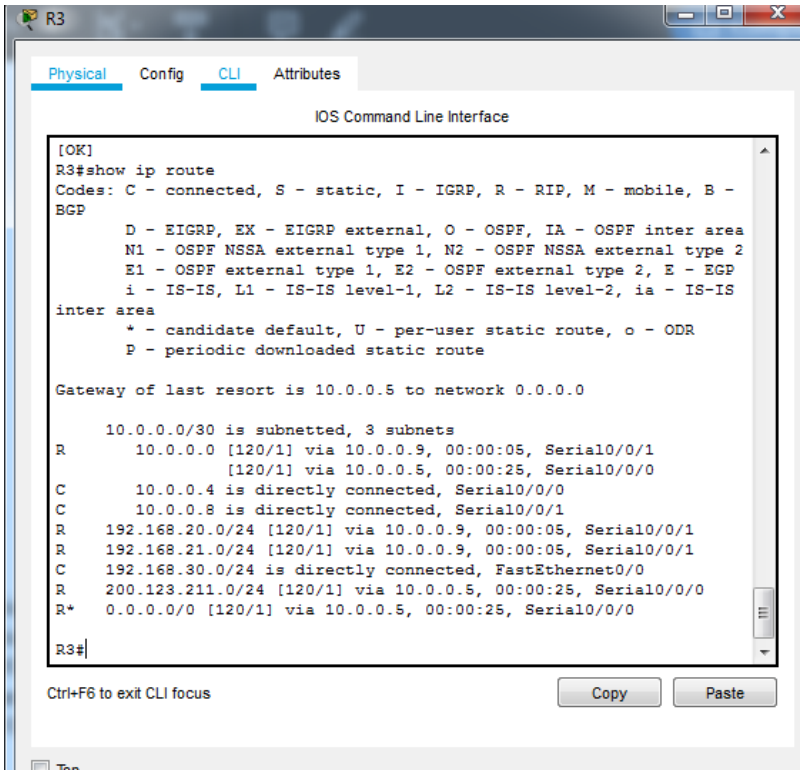

Figura 35 Verificación conexión RIP R3

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

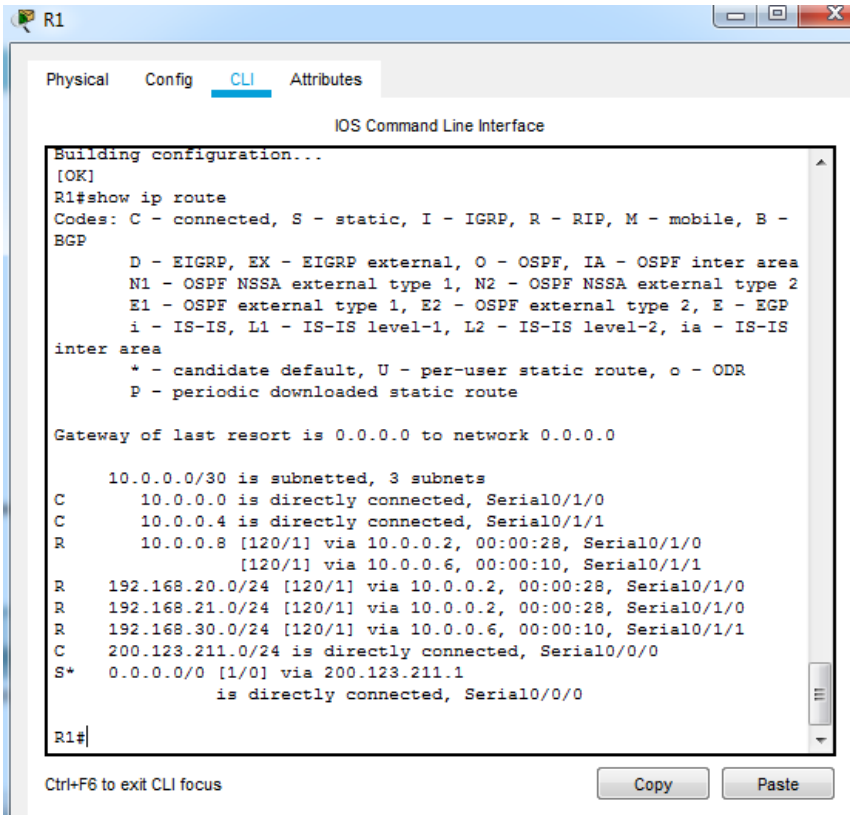

Figura 36 Rutas R1

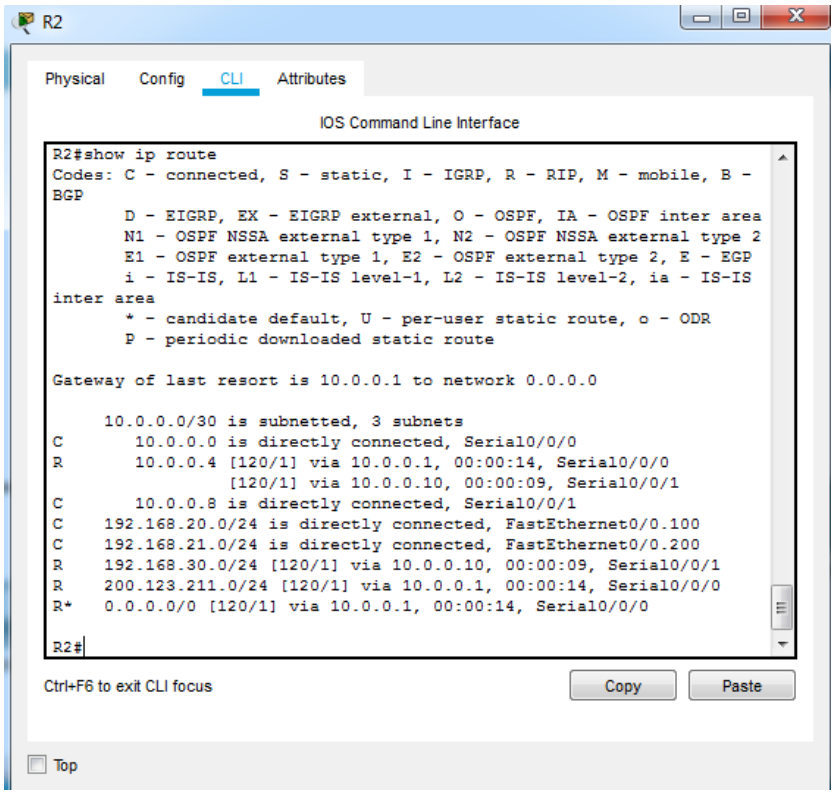

Figura 37 Rutas R2

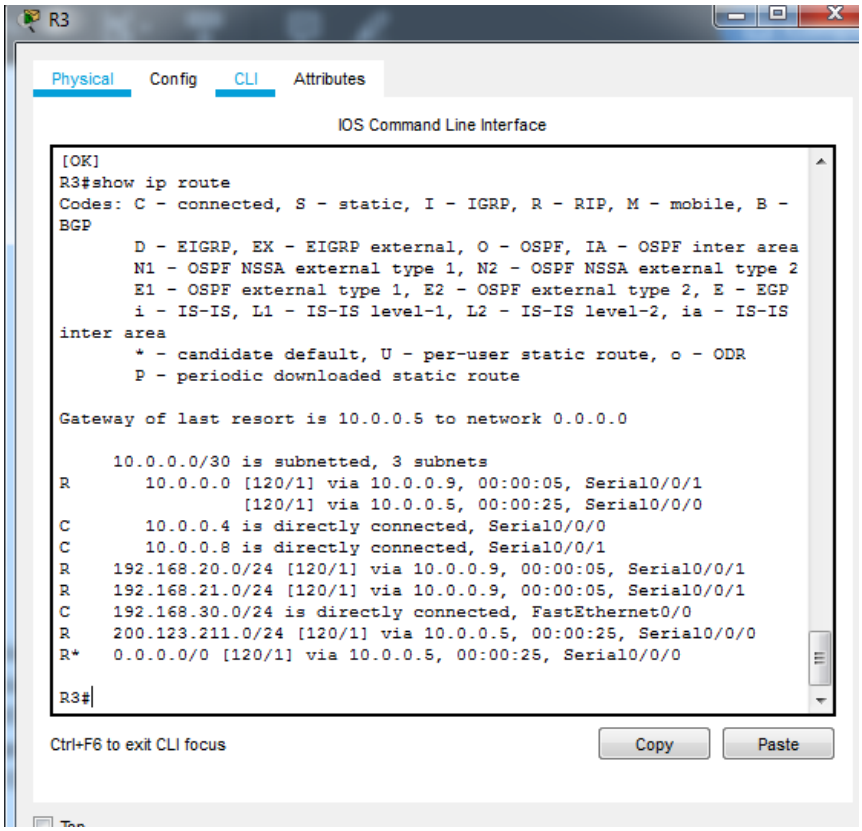

Figura 38 Rutas R3

1.1.14 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.

Verificación:

Ping desde PC20 a Laptop20 e ISP

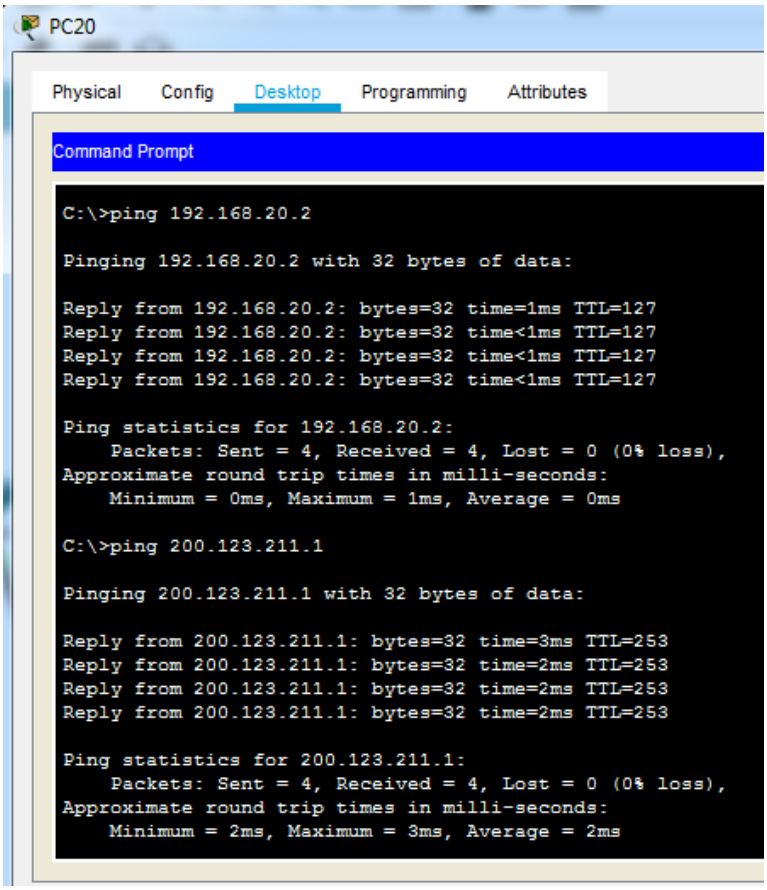

Figura 39 Verificación ping PC20, Laptop20 e ISP

Ping desde PC21 a Laptop21 e ISP.

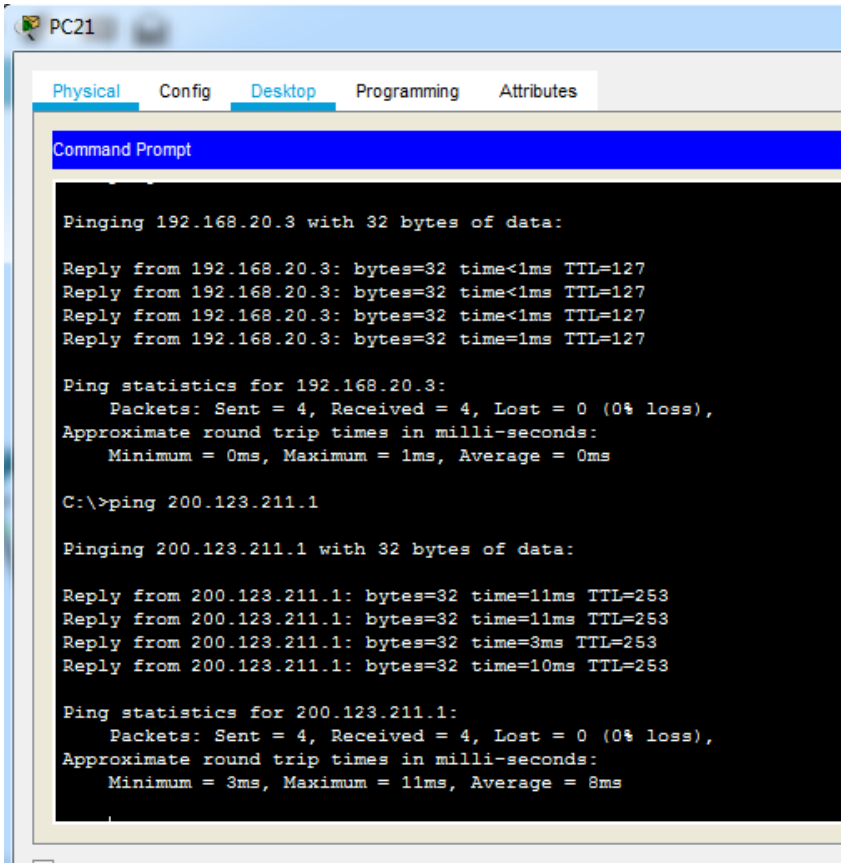

Figura 40 Verificación ping PC21, Laptop21 e ISP

Verificación ping Laptop20 a PC21 e ISP.

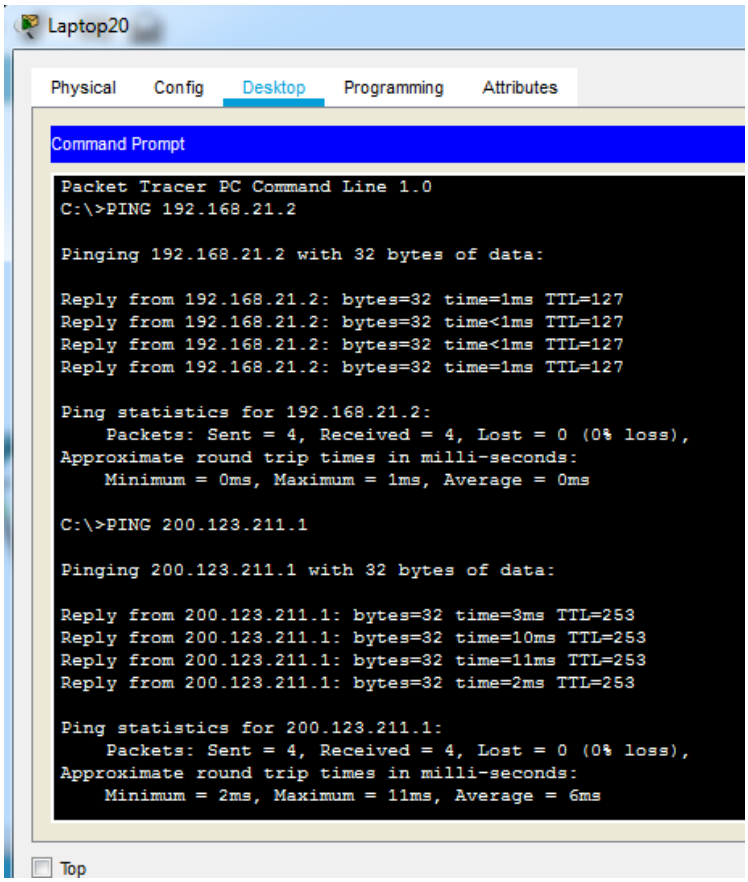

Figura 41 Verificación de ping Laptop20, PC21 e ISP

Verificación ping Laptop21 a PC20 e ISP.

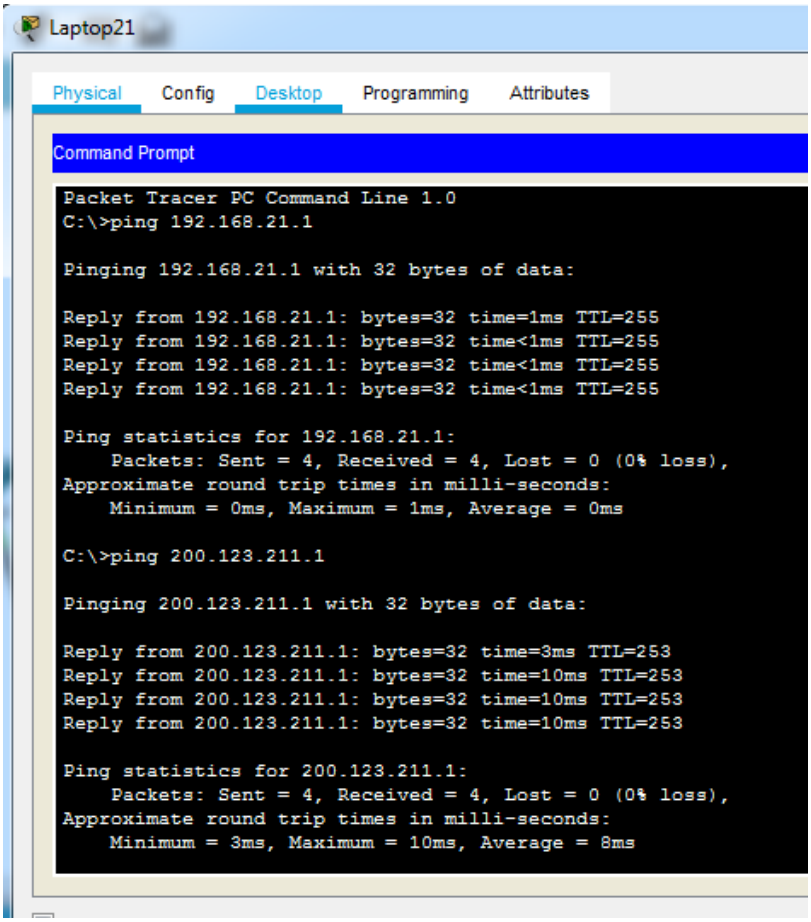

Figura 42 Verificación ping Laptop21, PC20 e ISP

Ping desde PC30 a Laptop31 e ISP

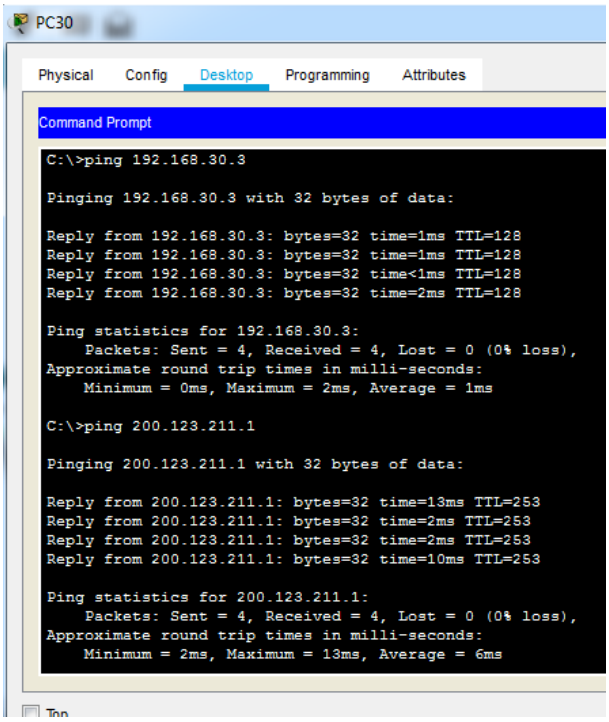

Figura 43 Verificación ping PC30, Laptop31 e ISP

Ping desde PC31 a Laptop30 e ISP

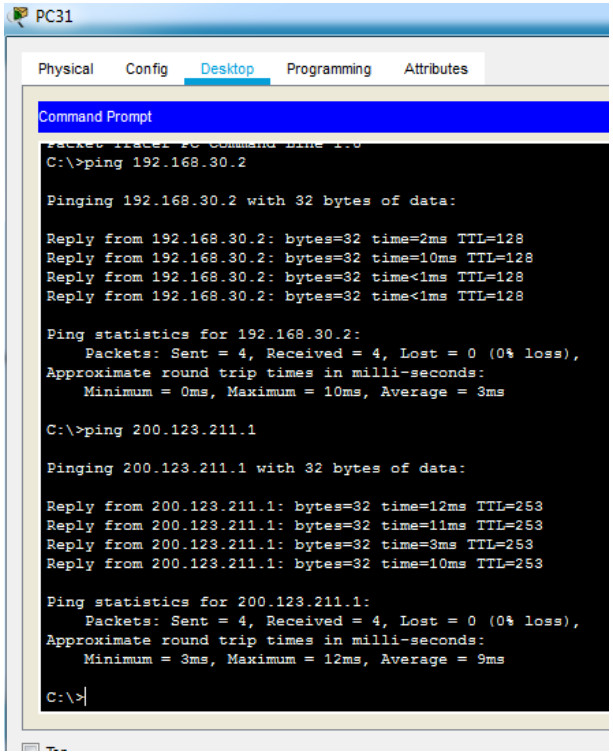

Figura 44 Verificación ping PC31, Laptop30 e ISP

Ping desde PC31 a PC30 y Laptop31

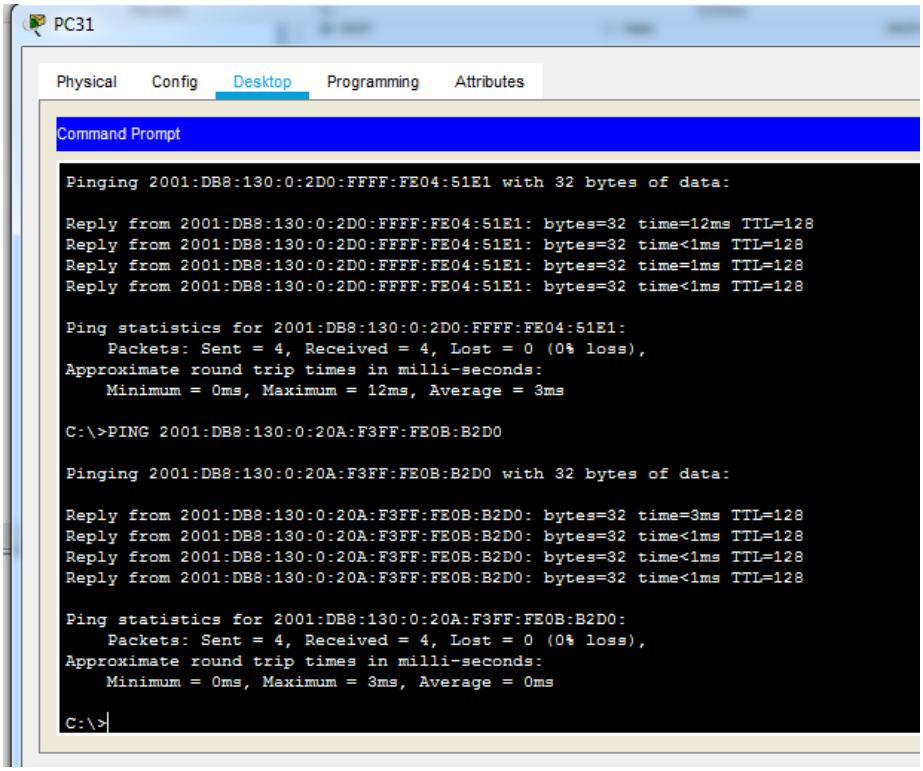

Figura 45 Verificación de ping IPv6 PC31 a PC30 y Laptop31

Ping desde Laptop30 a PC30 y Laptop31.

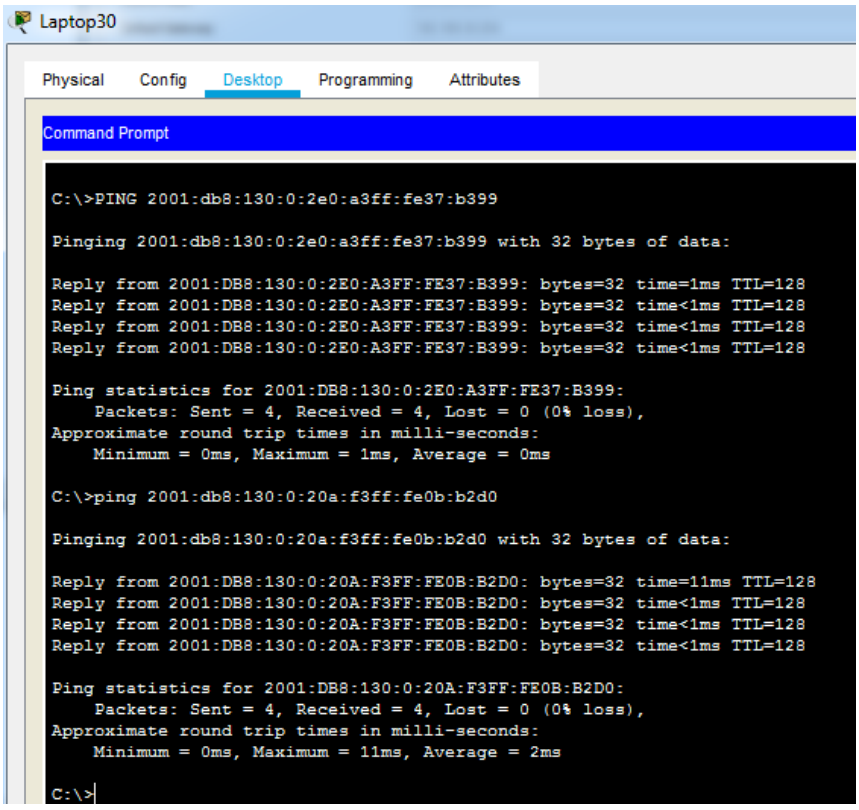

Figura 46 Verificación ping IPv6 Laptop30 a PC30 y Laptop31

1.2 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.

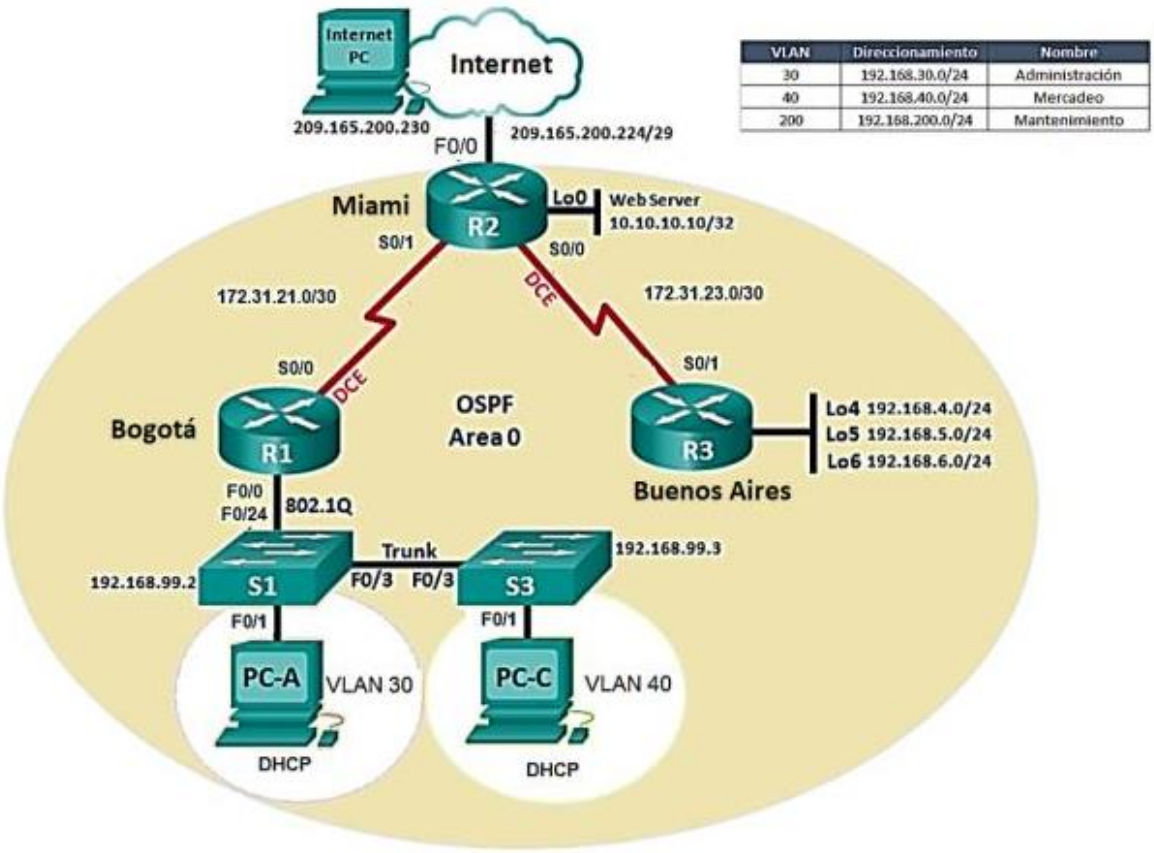

Figura 47 Topología escenario 2

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

A continuación, se muestra la tabla de direccionamiento utilizada:

Dispositivo	Interfaces	Dirección IP	Mascara de subred	Gateway predeterminado
R1	S0/0	172.31.21.1	255.255.255.252	N/A
	G0/0	192.168.99.1	255.255.255.0	N/A
	F0/0.30	192.168.30.1	255.255.255.0	N/A
	F0/0.40	192.168.40.1	255.255.255.0	N/A
R2	S0/1	172.31.21.2	255.255.255.252	N/A
	S0/0	172.31.23.1	255.255.255.252	N/A
	G0/0	209.165.200.225	255.255.255.248	
	Lo0	10.10.10.10	255.255.255.255	N/A
R3	S0/1	172.31.23.2	255.255.255.252	N/A

	Lo4	192.168.4.1	255.255.255.0	N/A
	Lo5	192.168.5.1	255.255.255.0	N/A
	Lo6	192.168.6.1	255.255.255.0	N/A
S1	VLAN 1	192.168.99.2	255.255.255.0	192.168.99.1
S3	VLAN 1	192.168.99.3	255.255.255.0	192.168.99.1
PC-A	NIC	DHCP	DHCP	DHCP
PC-B	NIC	DHCP	DHCP	DHCP
PC-INTERNET	NIC	209.165.200.230	255.255.255.248	

Configuración de puertos de suiches:

Puertos	Asignaciones	Red
S1 F0/3	Enlace troncal	NA
S1 F0/24	Enlace troncal 802.1Q	NA
S1 F0/1	VLAN 30: Administración	192.168.30.0/24
S3 F0/3	Enlace troncal	NA
S3 F0/3	VLAN 40: Mercadeo	192.168.40.0/24
	VLAN 200: Mantenimiento	192.168.200.0/24

1.2.2 Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

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

Figura 48 Características del OSPF

Inicialmente se reinician los routers, se habilita el modo EXEC privilegiado y se ejecuta el comando erase startup-config para eliminar el archivo de configuración de inicio de la NVRAM. Posterior a ello se ejecuta el comando reload para eliminar la configuración antigua de la memoria. A continuación, se listan los comandos utilizados para los tres routers:

```
Router>enable
Router#erase startup-config
Router#reload
```

Adicionalmente se configuran los nombres de los mismos y se deshabilita la búsqueda por DNS:

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
R1(config)#
R1(config)#no ip domain-lookup

Router>enable
Router#configure terminal
Router(config)#hostname R2
R2(config)#
R2(config)#no ip domain-lookup

Router>enable
Router#configure terminal
Router(config)#hostname R3
R3(config)#
R3(config)#no ip domain-lookup
```

Ahora se procede a asignar las direcciones IP según la tabla de direcciones.

Para R1:

```
R1(config)#interface s0/0/0
R1(config-if)#ip address 172.31.21.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
```

Para R2:

```
R2(config)#interface s0/0/0
R2(config-if)#ip address 172.31.23.1 255.255.255.252
R2(config-if)#clock rate 128000
R2(config-if)#no shutdown
R2(config)#interface s0/0/1
R2(config-if)#ip address 172.31.21.2 255.255.255.252
R2(config-if)#no shutdown
R2(config)#interface lo0

R2(config-if)#
R2(config-if)#ip address 10.10.10.10 255.255.255.255
R2(config-if)#no shutdown
R2(config)#interface g0/0
```

R2(config-if)#ip address 209.165.200.225 255.255.255.248
R2(config-if)#no shutdown
Para R3
R3(config)#interface s0/0/1
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#no shutdown
R3(config)#interface lo4
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#no shutdown
R3(config)#interface lo5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#no shutdown
R3(config)#interface lo5
R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#no shutdown

Ahora se procede a configurar el OSPF programando las interfaces que participan en el proceso del routing mediante el comando network.

Para el router 1:

R1(config)#router ospf 1
R1(config-router)#network 172.31.21.0 0.0.0.3 area 0
R1(config-router)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0
R1(config-router)#exit

Para el router 2:
R2(config)#router ospf 2
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.10 0.0.0.0 area 0
R2(config-router)#exit

Para el router 3:
R3(config)#router ospf 3
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
R3(config-router)#network 192.168.5.0 0.0.0.255 area 0
R3(config-router)#network 192.168.6.0 0.0.0.255 area 0
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#exit

A continuación se configura el router ID:
R1(config)#router ospf 1

R1(config-router)#router-id 1.1.1.1
R1(config-router)#Reload or use "clear ip ospf process" command, for this to take effect
R1(config-router)#end
R1#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

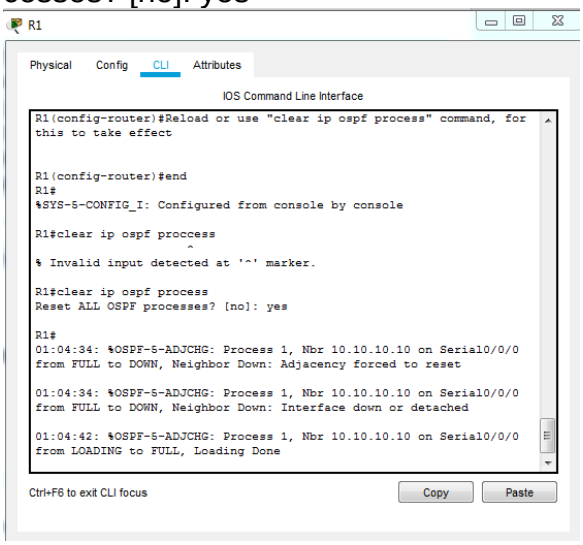

Figura 49 Reset para activar OSPF R1

Para R2:
R2(config)#router ospf 2
R2(config-router)#router-id 5.5.5.5
R2(config-router)#Reload or use "clear ip ospf process" command, for this to take effect
R2(config-router)#end
R2#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

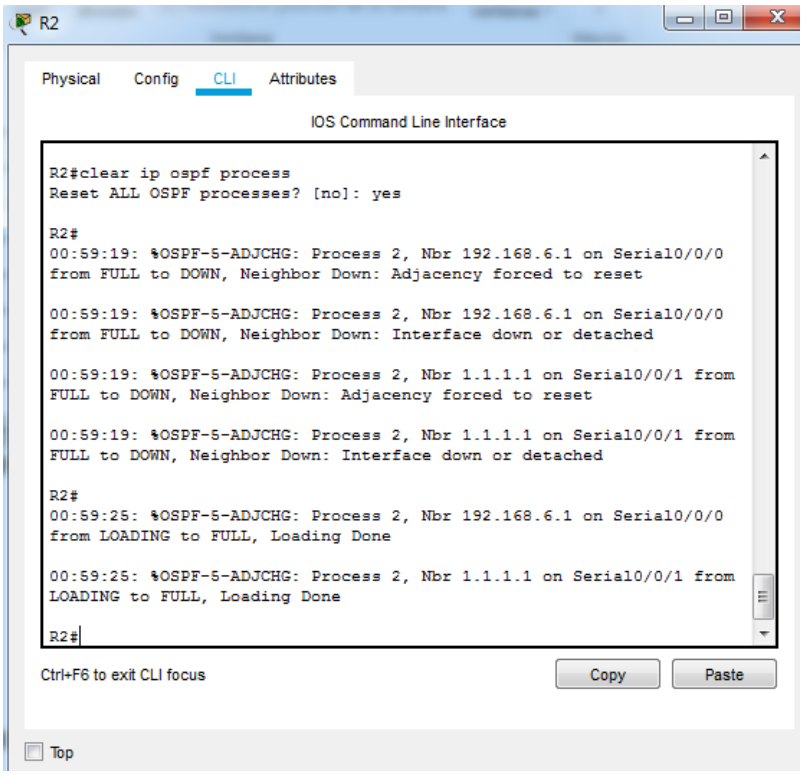

Figura 50 Reset para activar OSPF R2

Para R3:
R3(config)#router ospf 3
R3(config-router)#router-id 8.8.8.8
R3(config-router)#Reload or use "clear ip ospf process" command, for this to take effect
R3(config-router)#end
R3#clear ip ospf process
Reset ALL OSPF processes? [no]: yes

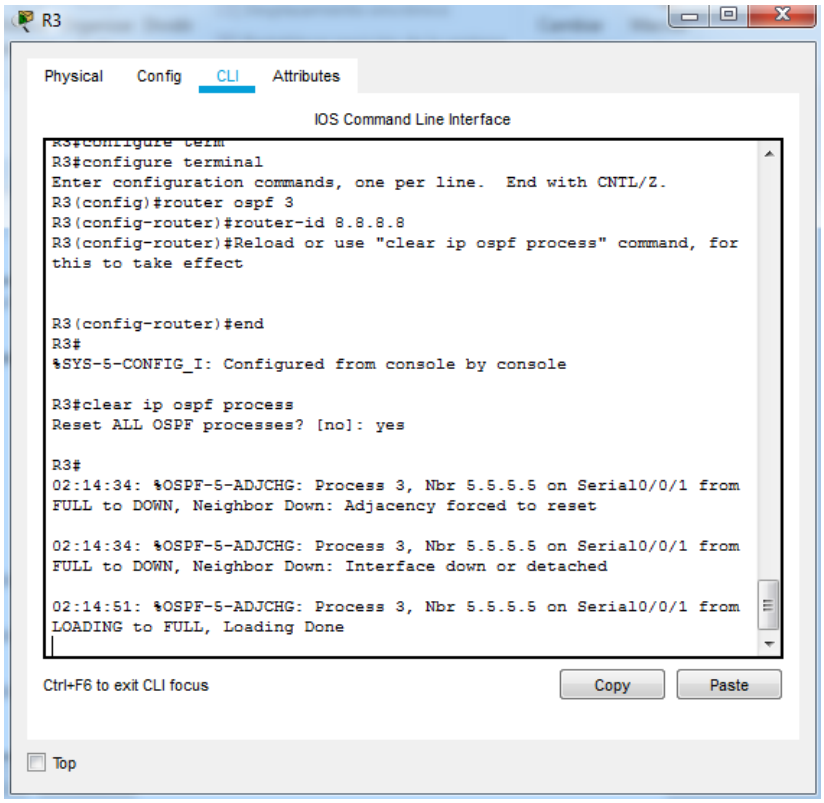

Figura 51 Reset para activar OSPF R3

Ahora se configuran las interfaces pasivas a las que no deben llegar los mensajes OSPF, es decir, la interfaz G0/0 del router 1, puesto que los demás no tienen interfaces LAN pasivas:

R1(config-router)#passive-interface gigabitEthernet 0/0
R1(config-router)#end

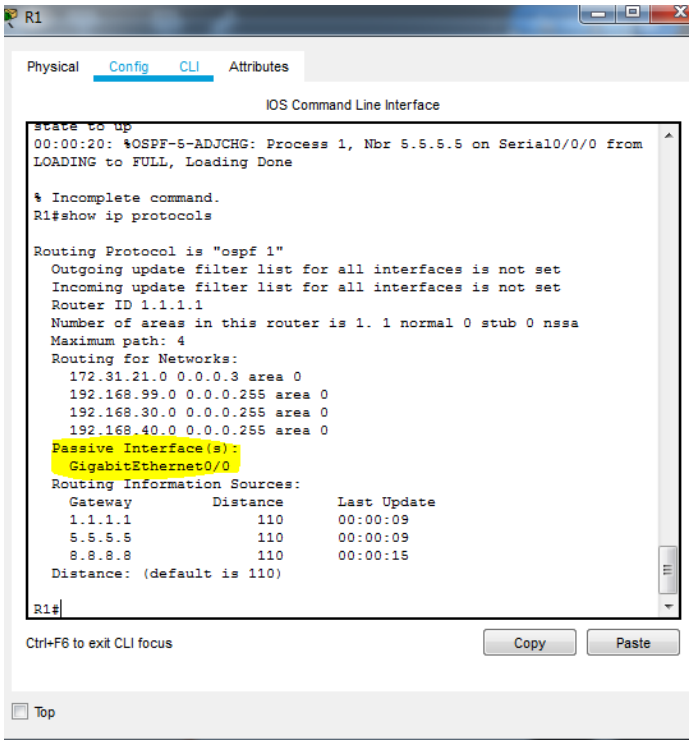

Figura 52 Interfaz pasiva

Configurando el ancho de banda de las interfaces a 256 kb/s

R1
R1(config)#interface s0/0/0
R1(config-if)#bandwidth 256
R1(config-if)#end

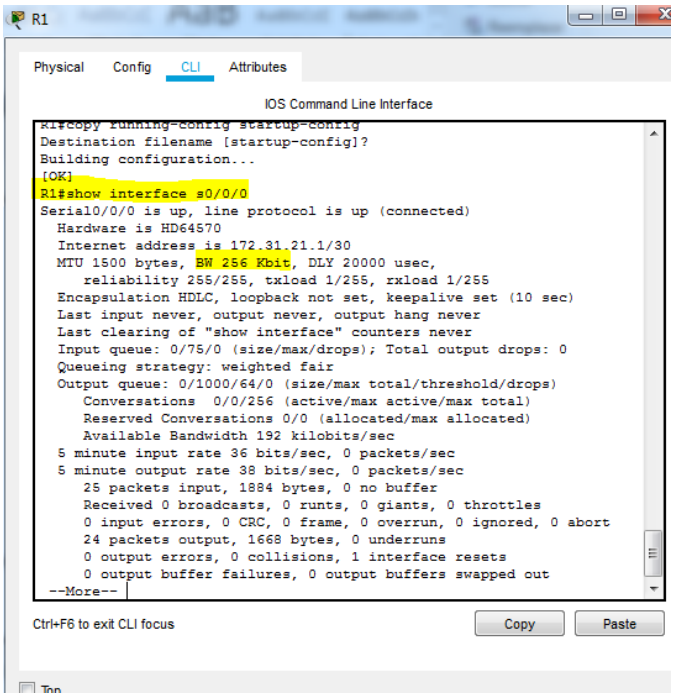

Figura 53 Verificación del ancho de banda R1

R2
R2(config)#interface s0/0/0
R2(config-if)#bandwidth 256
R2(config-if)#exit
R2(config)#interface s0/0/1
R2(config-if)#bandwidth 256
R2(config-if)#exit

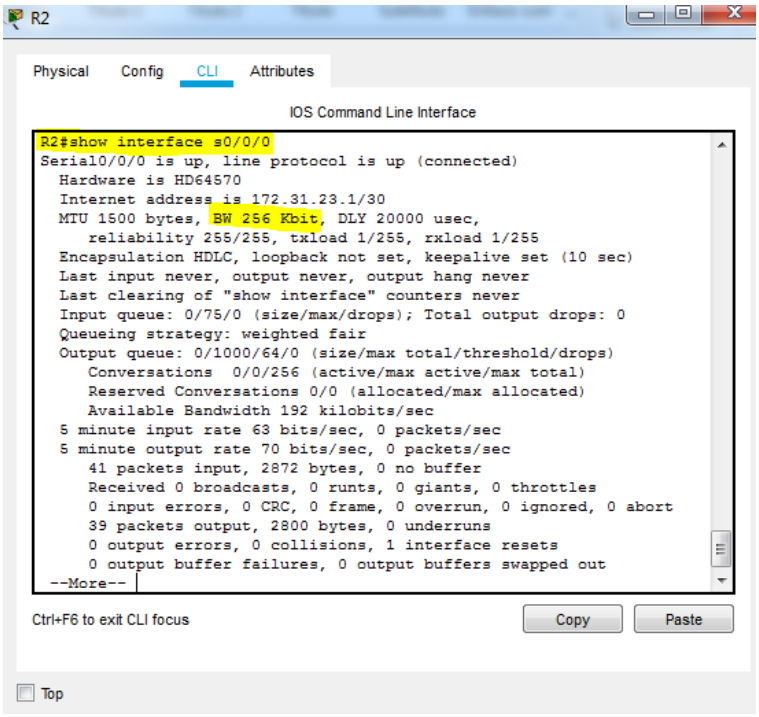

Figura 54 Verificación del ancho de banda R2 s0/0/0

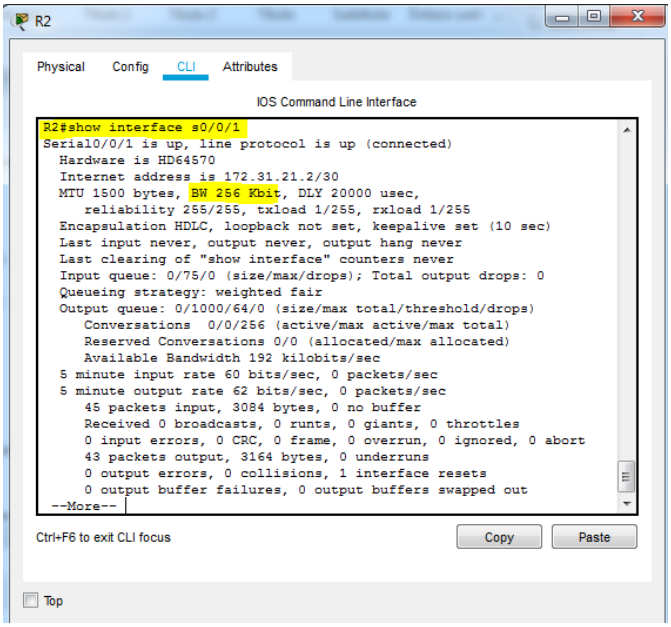

Figura 55 Verificación del ancho de banda R2 s0/0/1

R3
R3(config)#interface s0/0/1
R3(config-if)#bandwidth 256
R3(config-if)#exit

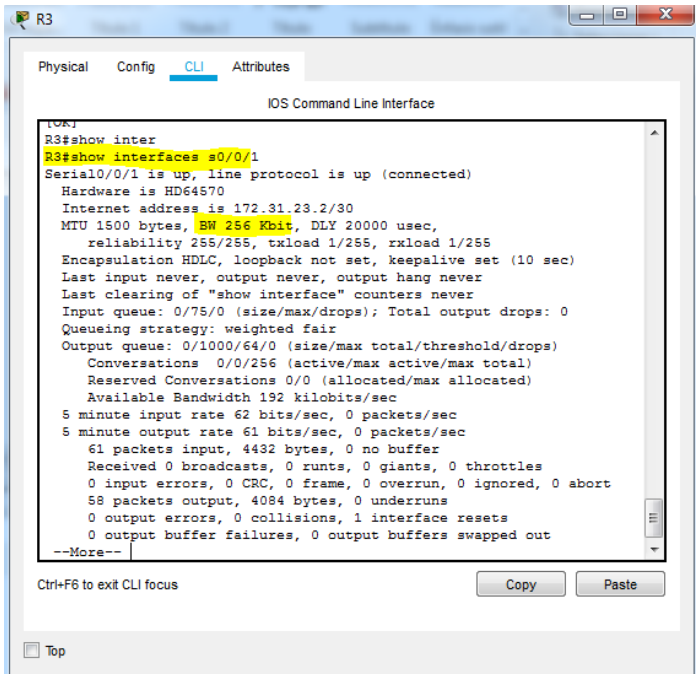

Figura 56 Verificación del ancho de banda R3

Dado que el costo de la métrica se debe configurar en 9500, se utiliza el comando ip ospf cost para los puertos seriales S0/0/0 de los routers 1 y 2.

Para R1:
R1(config)#interface s0/0/0
R1(config-if)#ip ospf cost 9500
R1(config-if)#end

Mediante el comando show ip ospf interface serial 0/0/0 se puede verificar el cambio de métrica realizado:

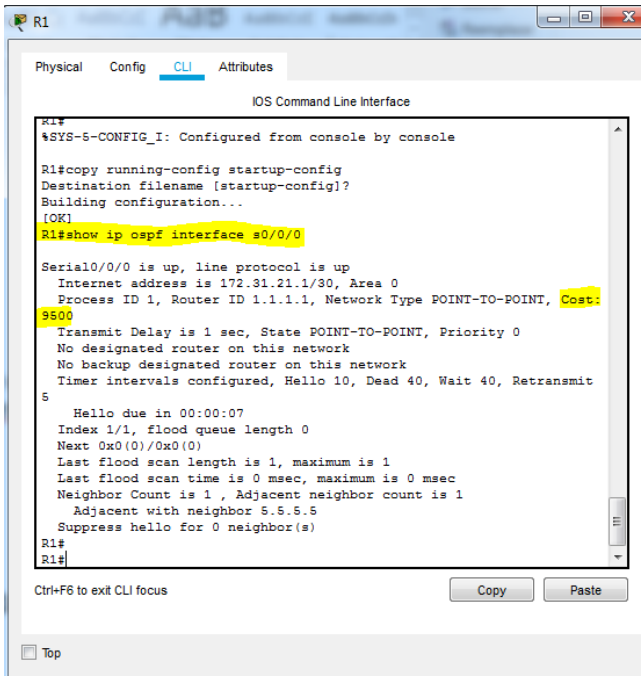

Figura 57 Verificación del costo R1

Para R2:
R2(config)#interface s0/0/0
R2(config-if)#ip ospf cost 9500
R2(config-if)#end

Verificación:

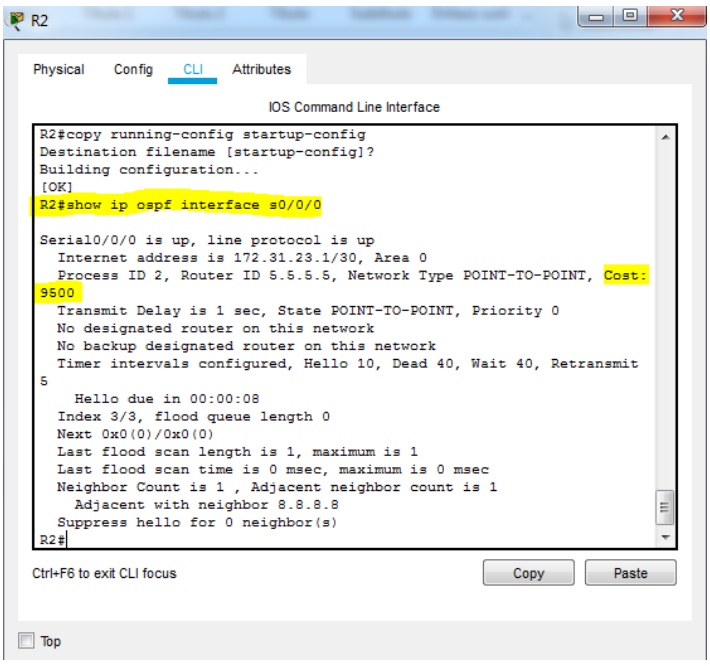

Figura 58 Verificación del costo R2

Verificar información de OSPF.

Para verificar la información básica de OSPF se utiliza el comando show ip protocols. La información incluye la ID del proceso OSPF, la ID del router, las redes que anuncia el router, los vecinos de los que el router recibe actualizaciones y la distancia administrativa predeterminada, que para OSPF es 110.

Para R1:

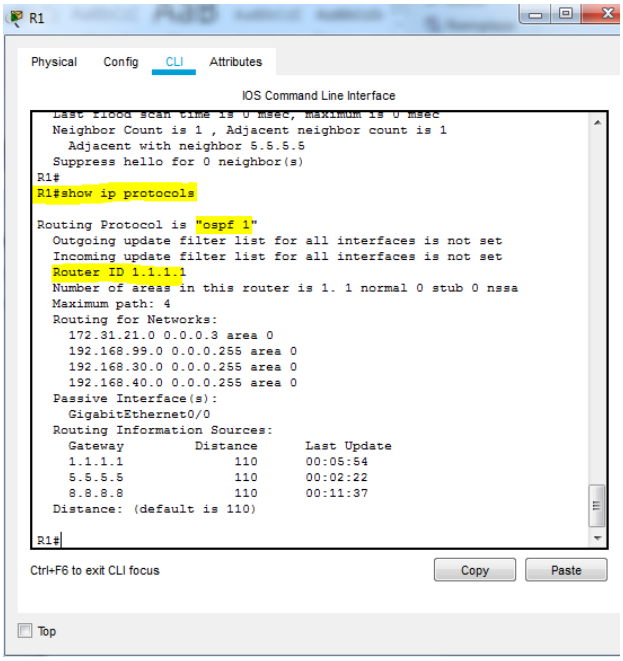

Figura 59 Verificación OSPF R1

Para R2:

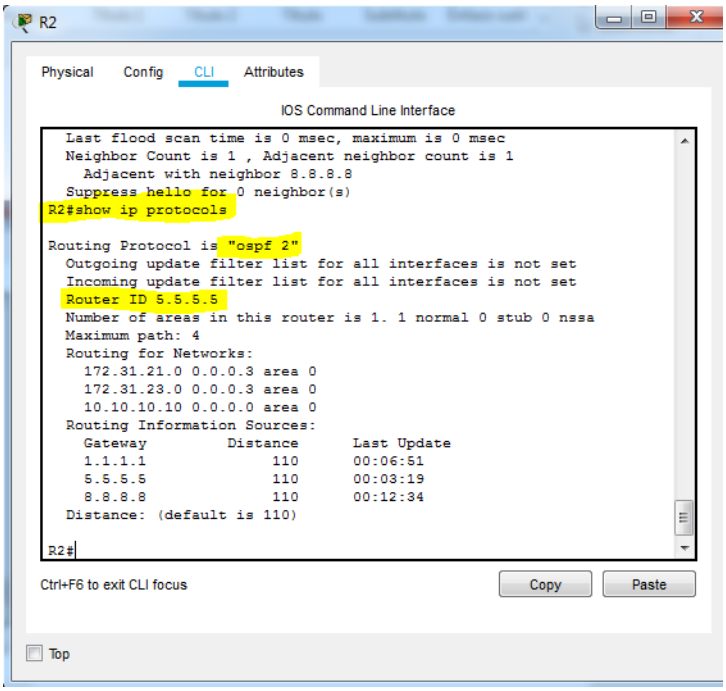

Figura 60 Verificación OSPF R2

Para R3:

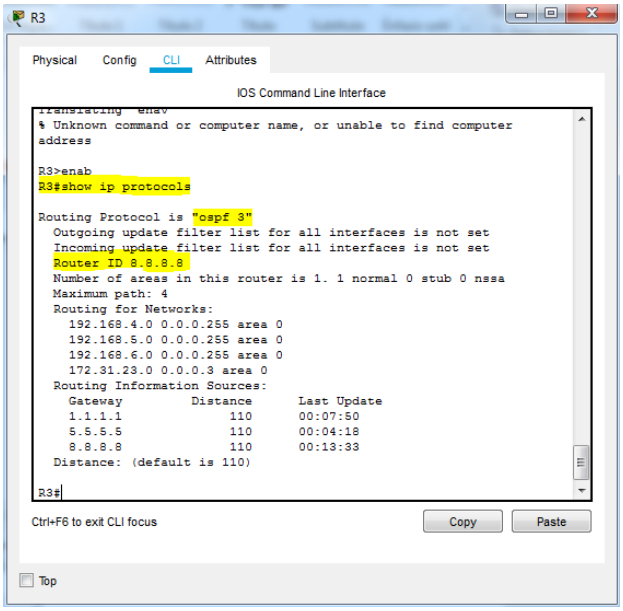

Figura 61 Verificación OSPF R3

Visualizar tablas de enrutamiento y routers conectados por OSPFv2

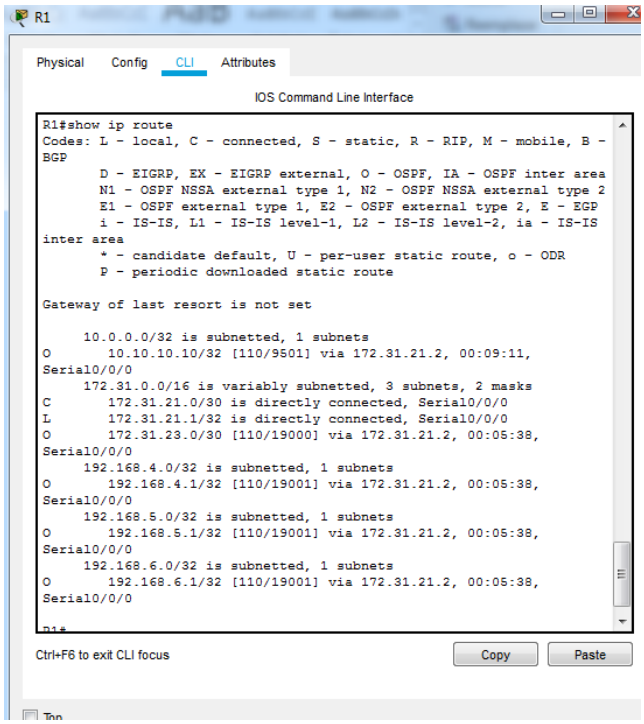

Figura 62 Enrutamiento R1

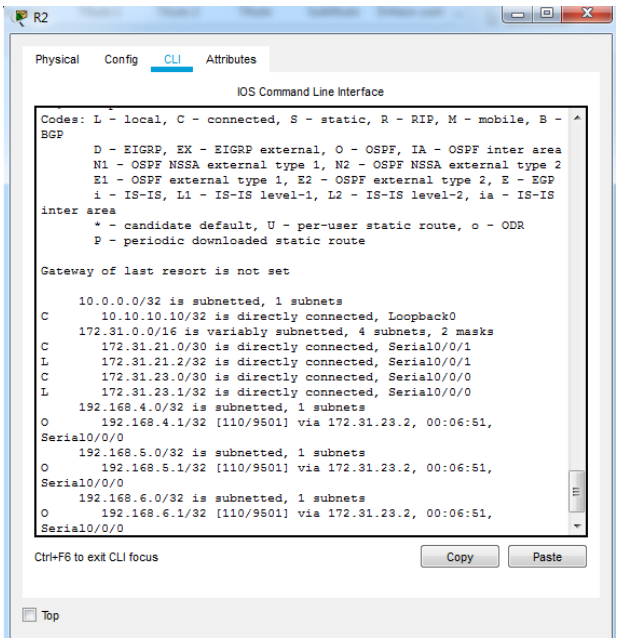

Figura 63 Enrutamiento R2

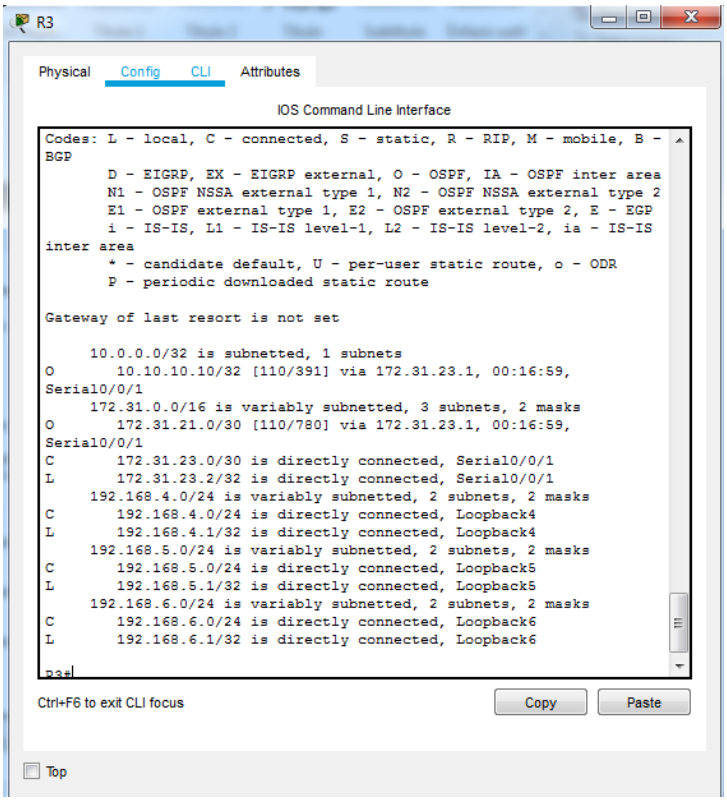

Figura 64 Enrutamiento R3

Se procede a verificar la adyacencia para los 3 routers con el comando show ip ospf neighbor

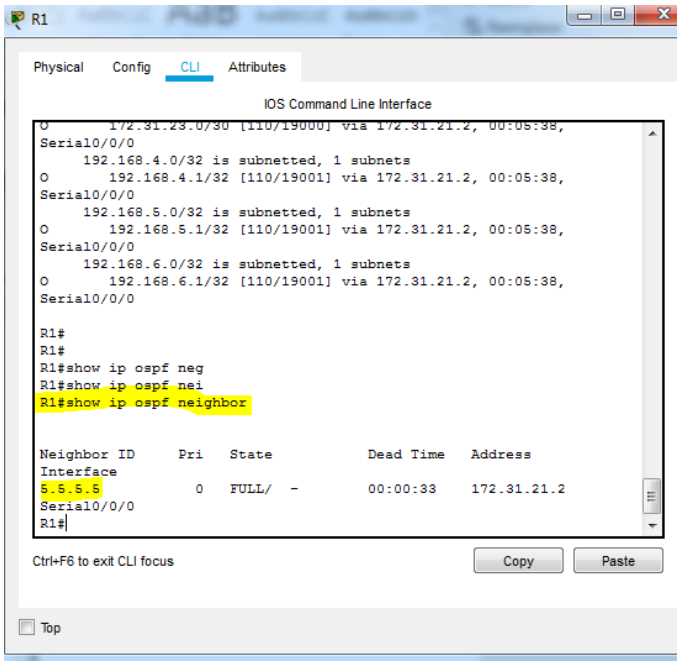

Figura 65 Verificación de adyacencias R1

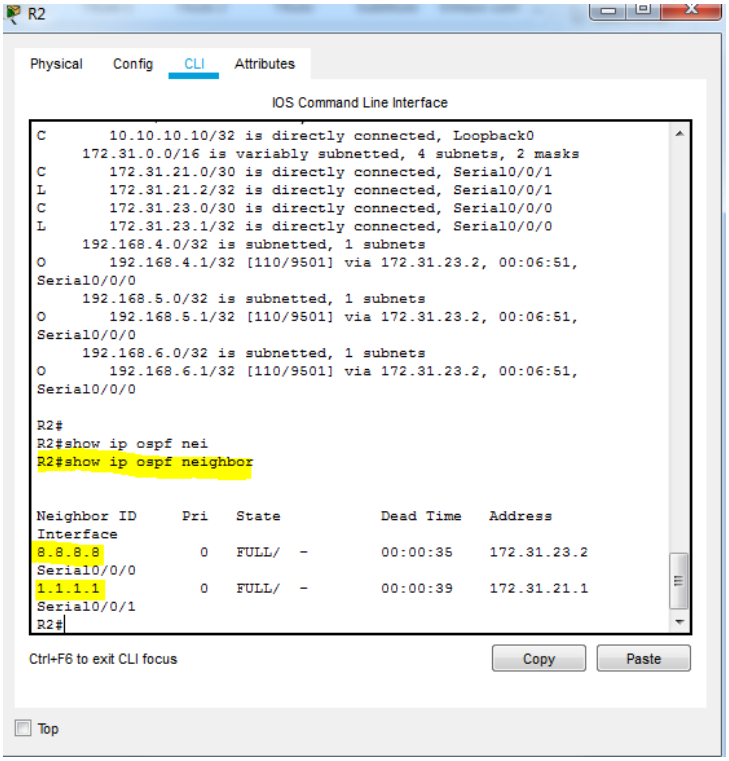

Figura 66 Verificación de adyacencias R2

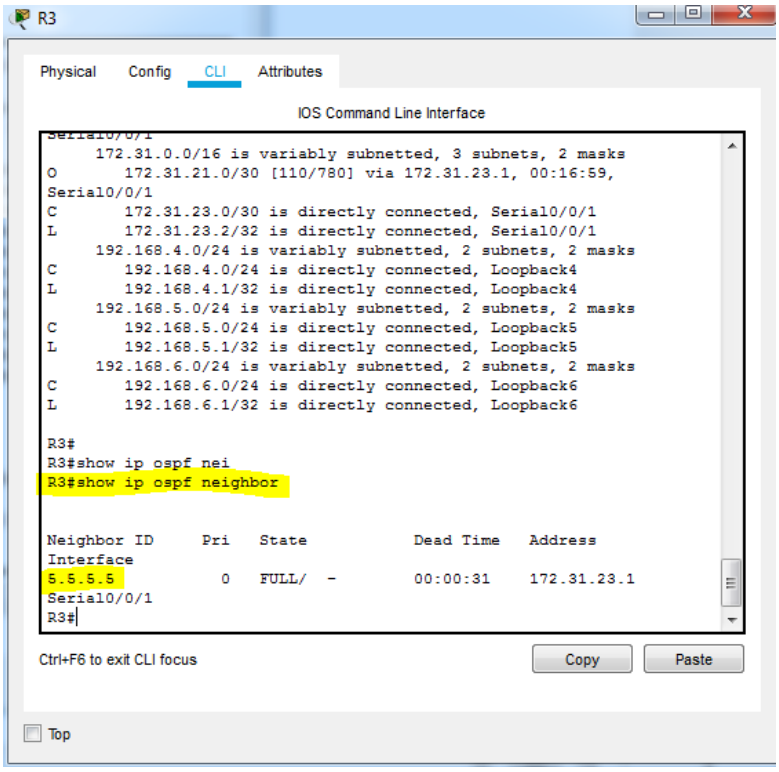

Figura 67 Verificación de adyacencias R3

Ahora se usa el comando show ip route ospf para mostrar solo las rutas OSPF descubiertas en la tabla de routing. A continuación, se muestra solo las rutas OSPF para los router 1,2 y 3 aplicando el comando show ip route ospf.

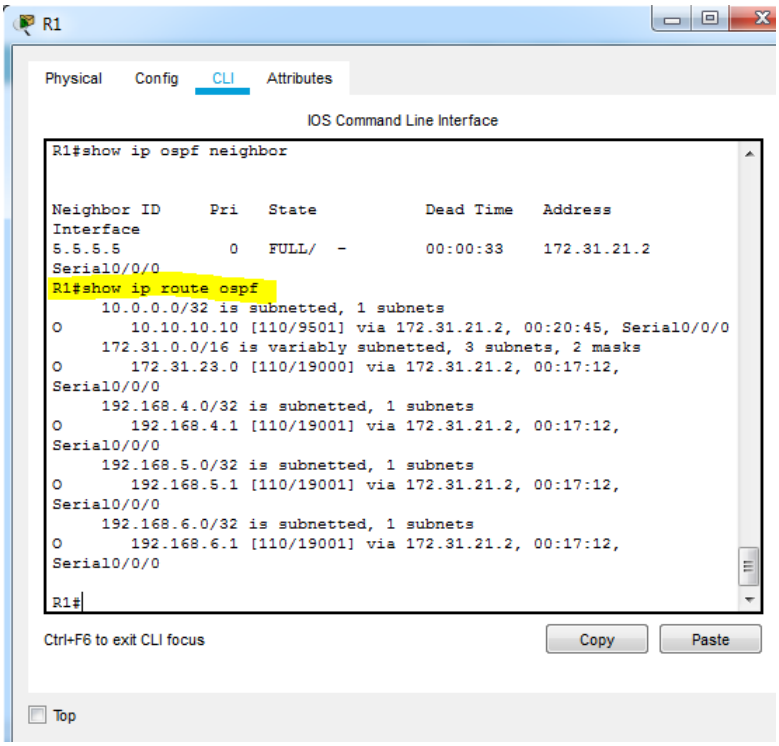

Figura 68 IP route desde OSPF R1

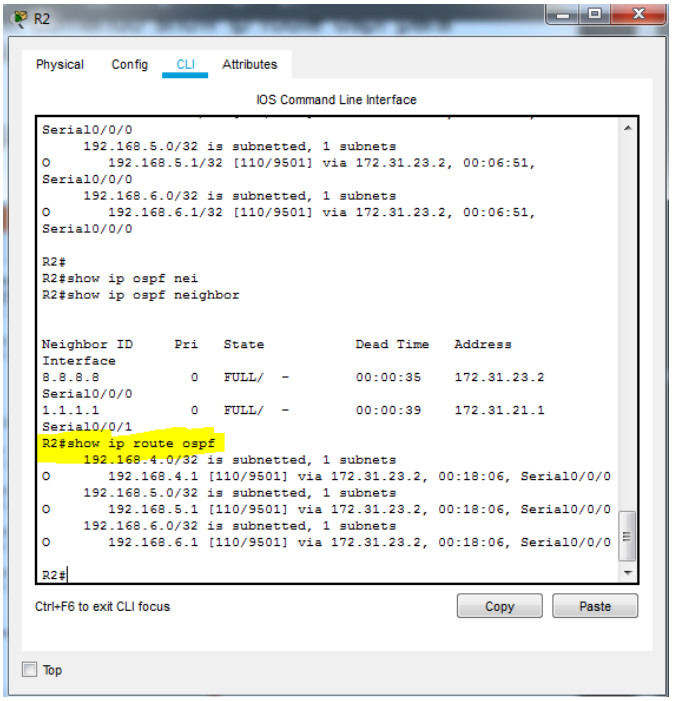

Figura 69 IP route desde OSPF R2

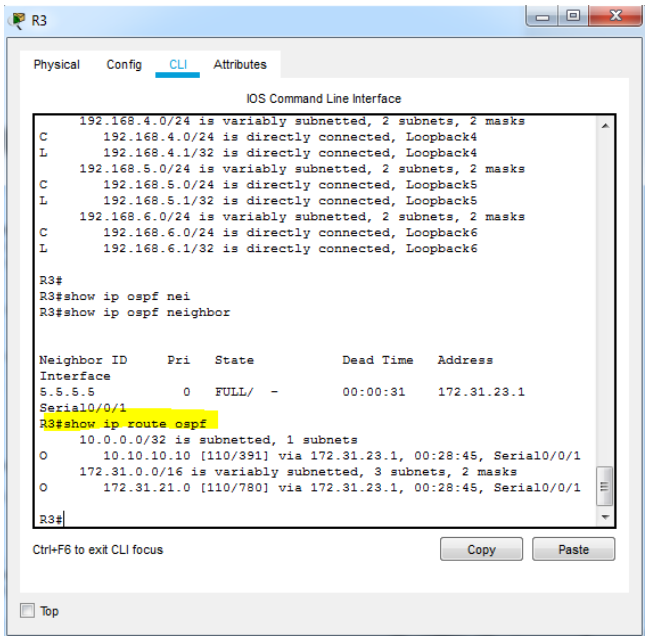

Figura 70 IP route desde OSPF R3

Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface.

Para esto se utiliza el comando show ip ospf interface s0/0/0

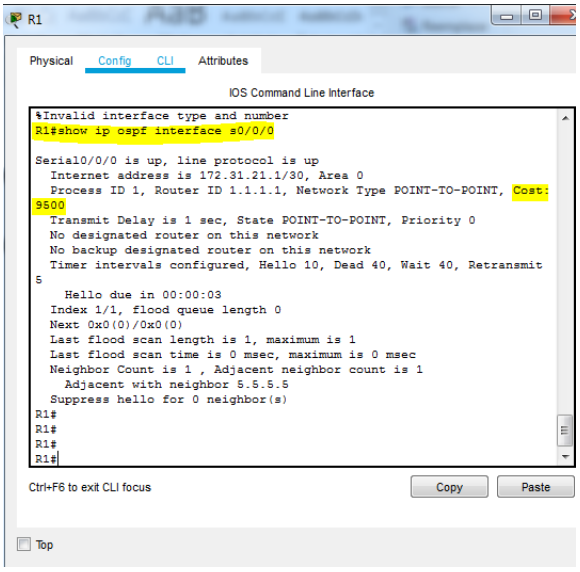

Figura 71 Verificación del costo de la interface R1

Router 2:

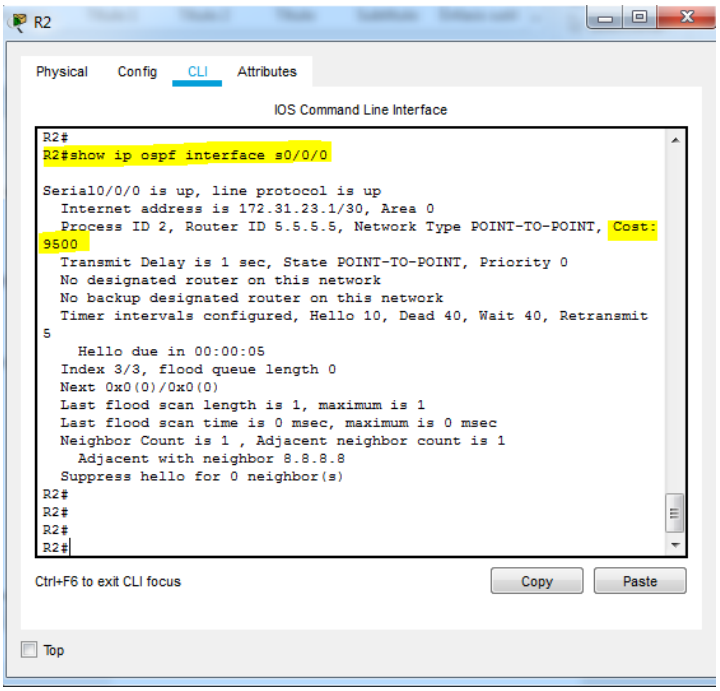

Figura 72 Verificación del costo de la interface R2

Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Para visualizar la ID del proceso OSPF y la ID del router se utiliza el comando show ip ospf para cada uno de los routers:

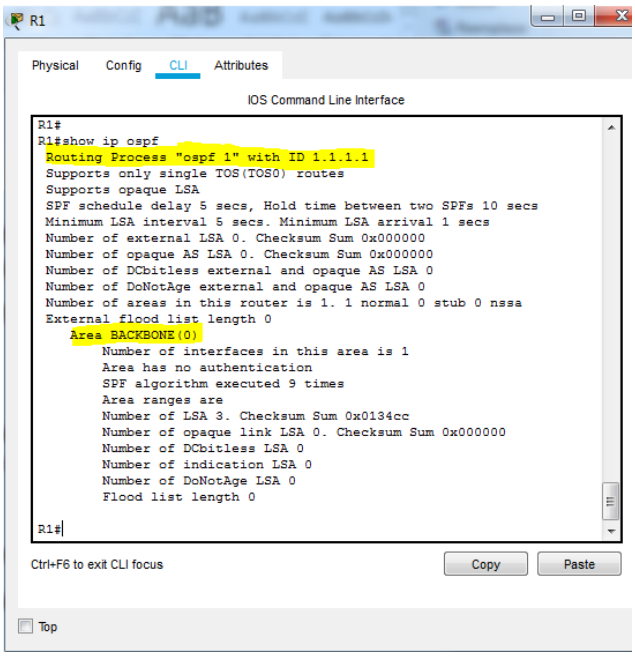

Figura 73 OSPF 1 R1

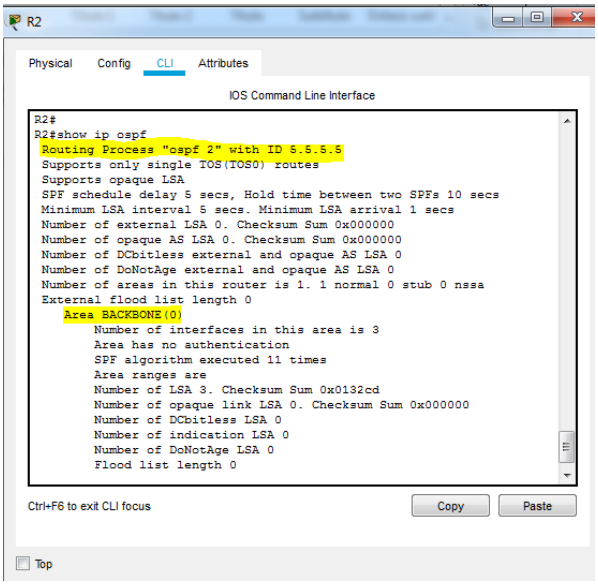

Figura 74 OSPF 2 R2

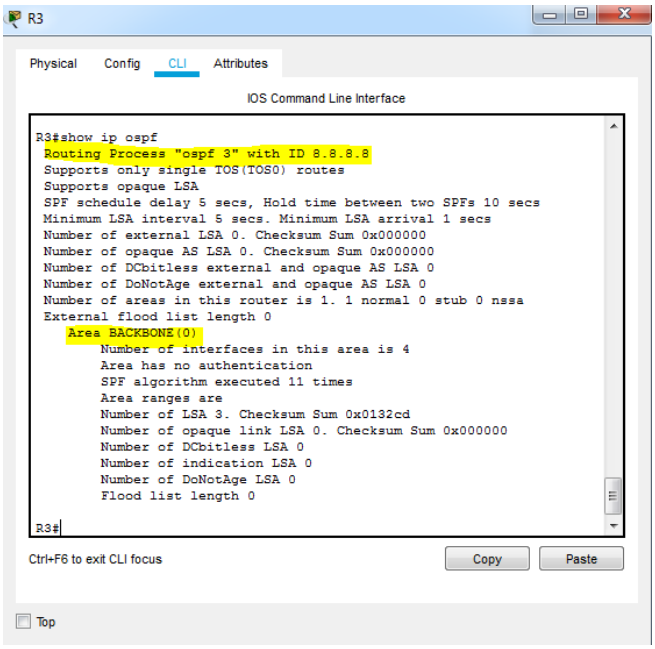

Figura 75 OSPF 3 R3

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

A continuación, se muestra la topología establecida para dar claridad sobre las VLAN que se implementarán en los suiches:

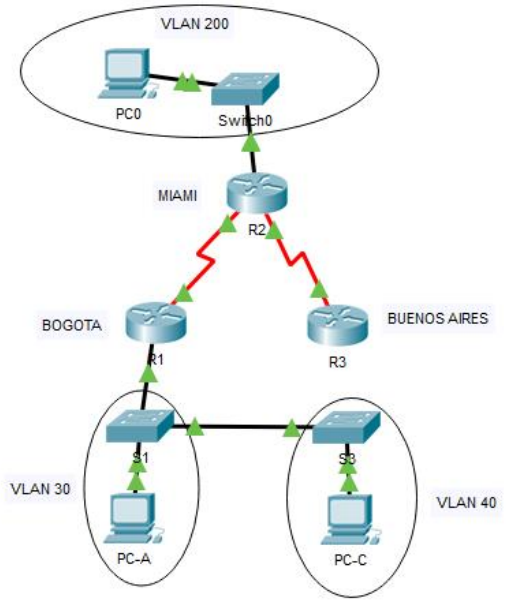

Figura 76 Topología implementada

Configuración para el suiche 1:
Switch(config)#hostname S1
S1(config)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#exit
S1(config)#interface f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#
S1(config-if)#exit
S1(config)#interface f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#exit
S1(config)#interface f0/24
S1(config-if)#switchport mode trunk

Verificación mediante el comando show vlan brief

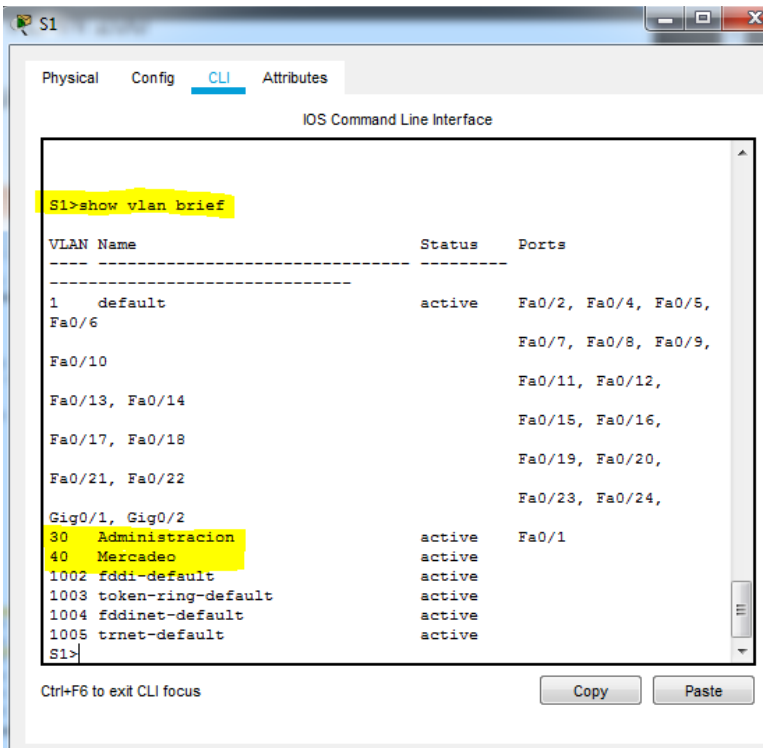

Figura 77 Verificación de VLAN S1

Con el fin de comprobar los enlaces troncales se utiliza el comando show interfaces ID-interfaz switchport.

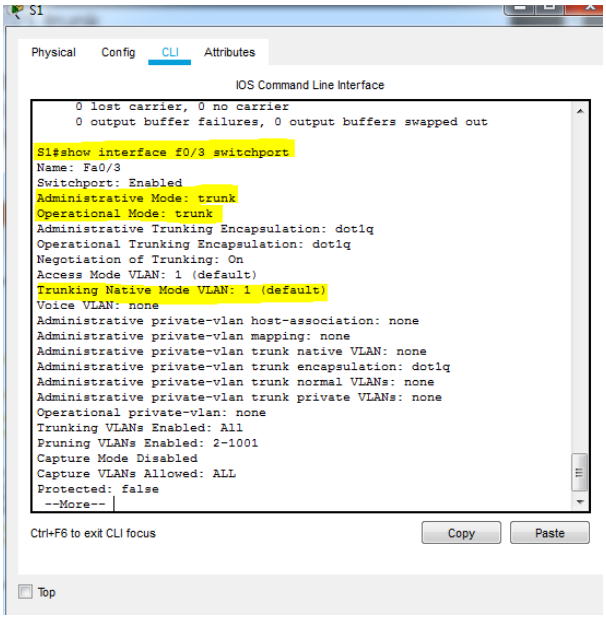

Figura 78 Verificación de enlaces troncales S1

Para el suiche 3:
Switch(config)#hostname S3
S3(config)#vlan 30
S3(config-vlan)#name Administracion
S3(config-vlan)#vlan 40
S3(config-vlan)#name Mercadeo
S3(config-vlan)#exit
S3(config)#interface f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#exit
S3(config)#interface f0/1
S3(config-if)#switchport access vlan 40
S3(config-if)#exit

Verificación:

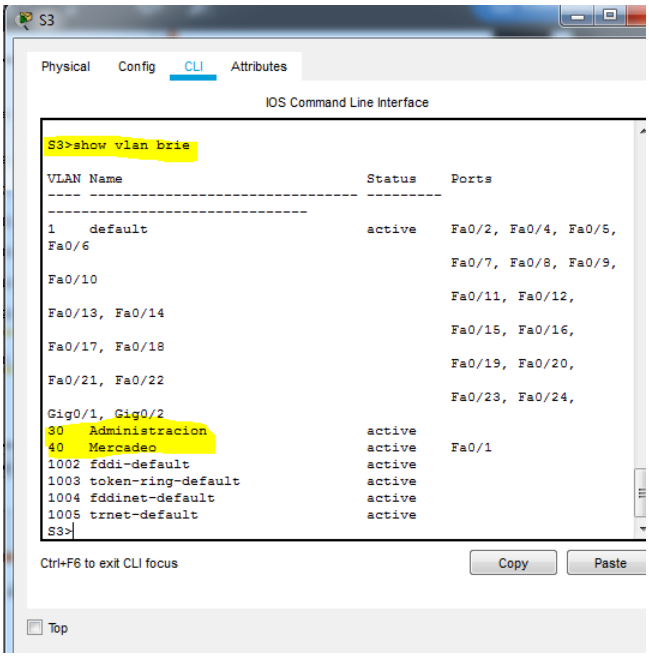

Figura 79 Verificación VLAN S3

Con el fin de comprobar los enlaces troncales se utiliza el comando show interfaces ID-interfaz switchport.

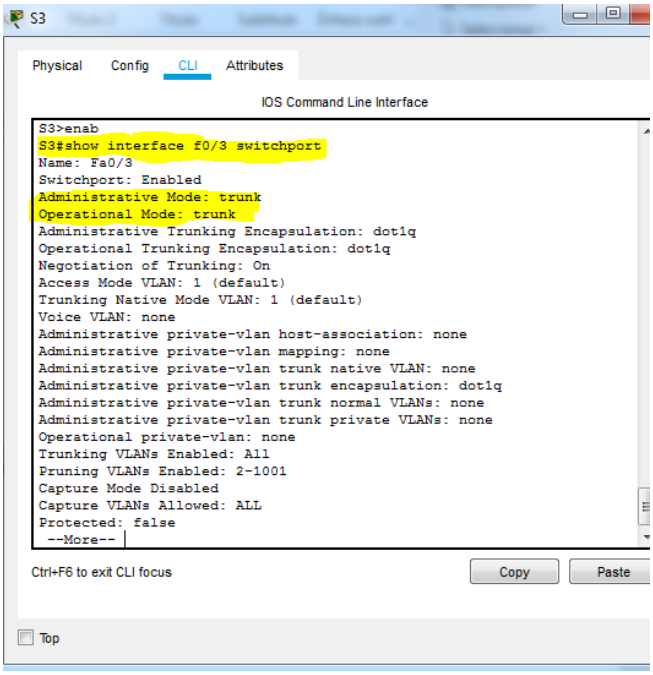

Figura 80 Verificación de enlaces troncales S3

Para el suiche 0

Switch(config)#hostname S0
S0(config)#vlan 200
S0(config-vlan)#name Mantenimiento
S0(config-vlan)#exit
S0(config)#interface f0/1
S0(config-if)#switchport mode trunk
S0(config-if)#exit
S0(config)#interface f0/2
S0(config-if)#switchport access vlan 200
S0(config-if)#exit

Verificación

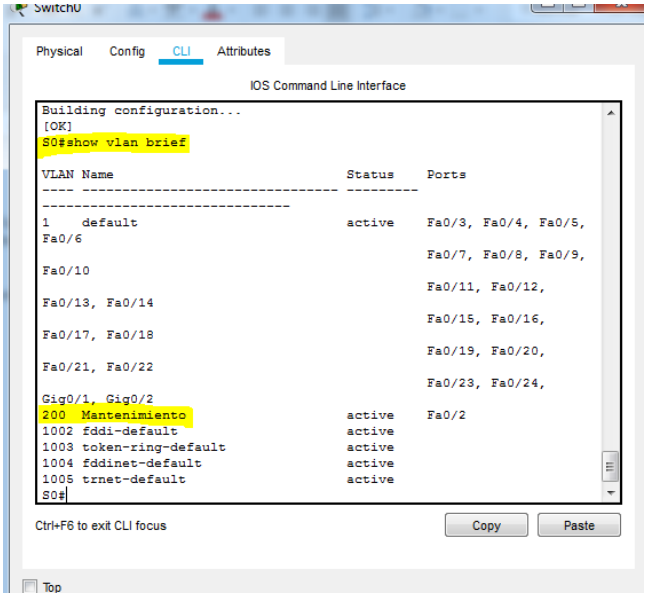

Figura 81 Verificación VLAN S0

Con el fin de comprobar los enlaces troncales se utiliza el comando show interfaces ID-interfaz switchport.

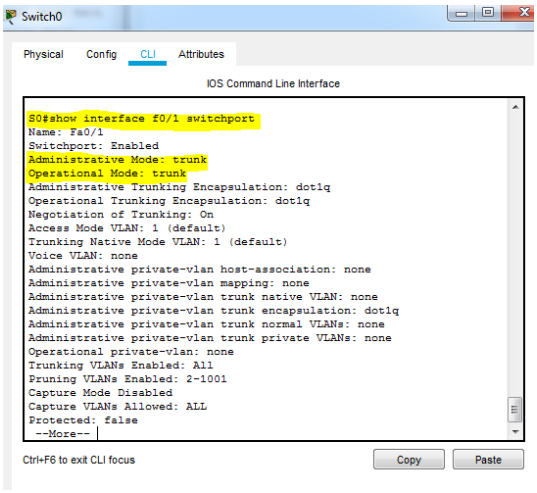

Figura 82 Verificación de enlaces troncales S0

Como se están usando switches Cisco Catalyst 2960 se utiliza de manera automática la encapsulación 802.1Q en los enlaces troncales. para otros switches generalmente se requiere la configuración manual de la encapsulación.

Paso seguido se configura el puerto G0/0 del router 1 para las subinterfaces de las VLAN 30 y 40.

```
R1(config)#interface g0/0.1
R1(config-subif)#encapsulation dot1Q 1
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#end
R1(config)#interface g0/0.30
R1(config-subif)#encapsulation dot1Q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#end
R1(config)#interface g0/0.40
R1(config-subif)#encapsulation dot1Q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#end
R1(config)#interface g0/0
R1(config-if)#no shutdown
```

Comprobación:

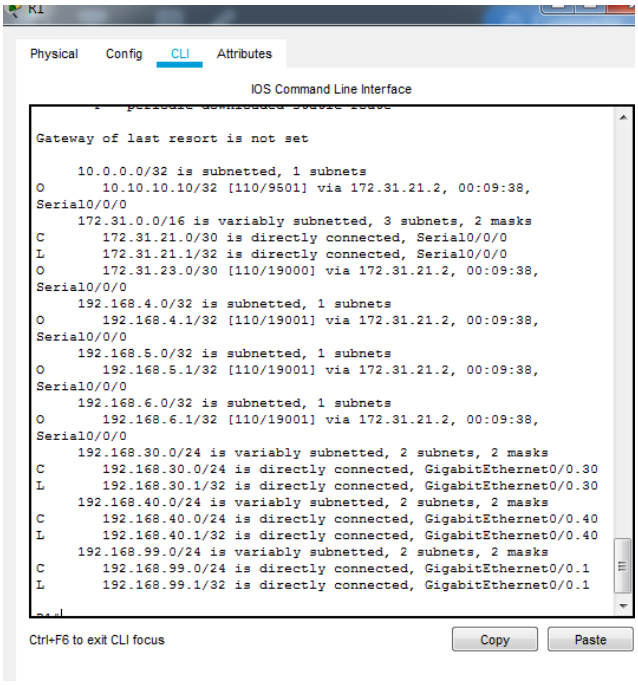

Figura 83 Verificación puerto G0/0 VLAN en R1

En R2 se habilita la subinterfaz 200

```
R2(config)#interface g0/0.200
R2(config-subif)#encapsulation dot1Q 200
R2(config-subif)#ip address 192.168.200.1 255.255.255.0
R2(config-subif)#end
R2(config)#interface g0/0
R2(config-if)#no shutdown
```

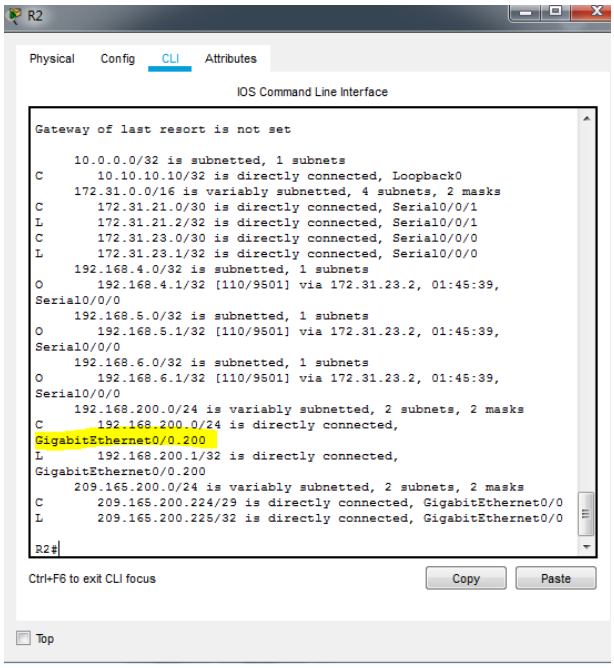

Figura 84 Verificación puerto G0/0 VLAN en R2

1.2.4 En el Switch 3 deshabilitar DNS lookup

Para deshabilitar el DNS, se utiliza el comando no ip domain-lookup:

S3(config)#no ip domain-lookup
S3(config)#exit

1.2.5 Asignar direcciones IP a los Switches acorde a los lineamientos.

Suiche 1:

S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#ip default-gateway 192.168.99.1
S1(config)#exit

S3(config)#interface vlan 1
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#ip default-gateway 192.168.99.1
S3(config)#exit
S0(config)#ip default-gateway 192.168.200.1

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

Para S1:
S1(config)#interface range fa0/4-23
S1(config-if-range)#shutdown
S1(config)#interface f0/2
S1(config-if)#shutdown
S1(config)#interface range gigabitEthernet 0/1-2
S1(config-if-range)#shutdown

Para S3:
S3(config)#interface range fa0/4-24
S3(config-if-range)#shutdown
S3(config)#interface fa0/2
S3(config-if)#shutdown
S3(config)#interface range gigabitEthernet 0/1-2
S3(config-if-range)#shutdown

Para S0:
S0(config)#interface range fa0/3-24
S0(config-if-range)#shutdown
S0(config)#interface range gigabitEthernet 0/1-2
S0(config-if-range)#shutdown

1.2.7 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.

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

Figura 85 Configuraciones DHCP

Primero se reservarán las primeras 30 direcciones IP de las VLAN 30 y 40:

```
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#exit
```

Ahora se configura el DCHP pool

```
R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.99.1
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#end
R1(config)#ip dhcp pool MERCADEO
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.99.1
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#exit
```

Dado que Packet Tracer no soporta algunos comandos, no se configuro el nombre de dominio con el comando domain-name ni la duración del arrendamiento mediante el comando léase. En este caso el valor de arrendamiento predeterminado para la dirección IP asignada es un día.
Ya que el servidor se encuentra en la misma LAN no es necesario un agente de retransmisión para el caso de estudio.

Verificación configuración del pool:

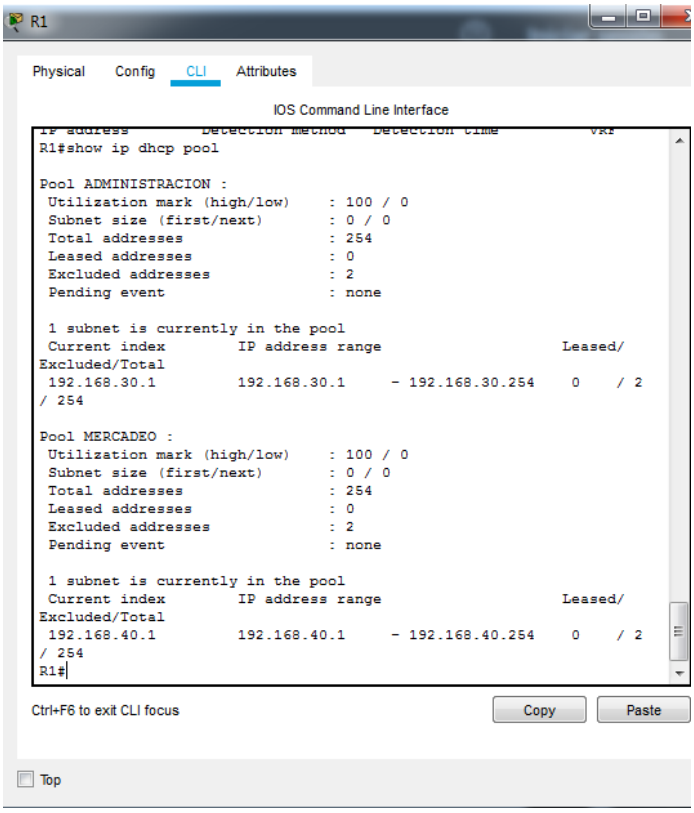

Figura 86 Verificación del pool R1

verificación del DHCP en los PC:

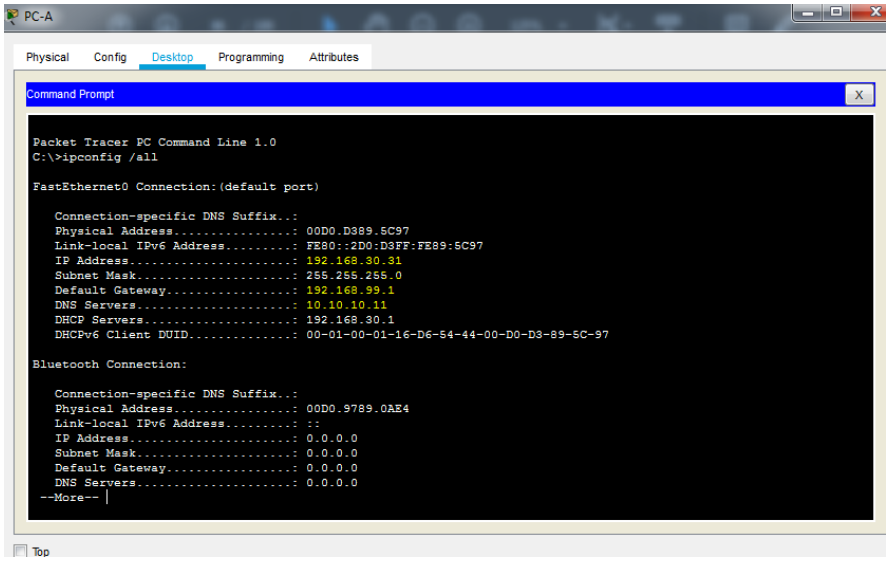

Figura 87 Validación del DHCP PC-A

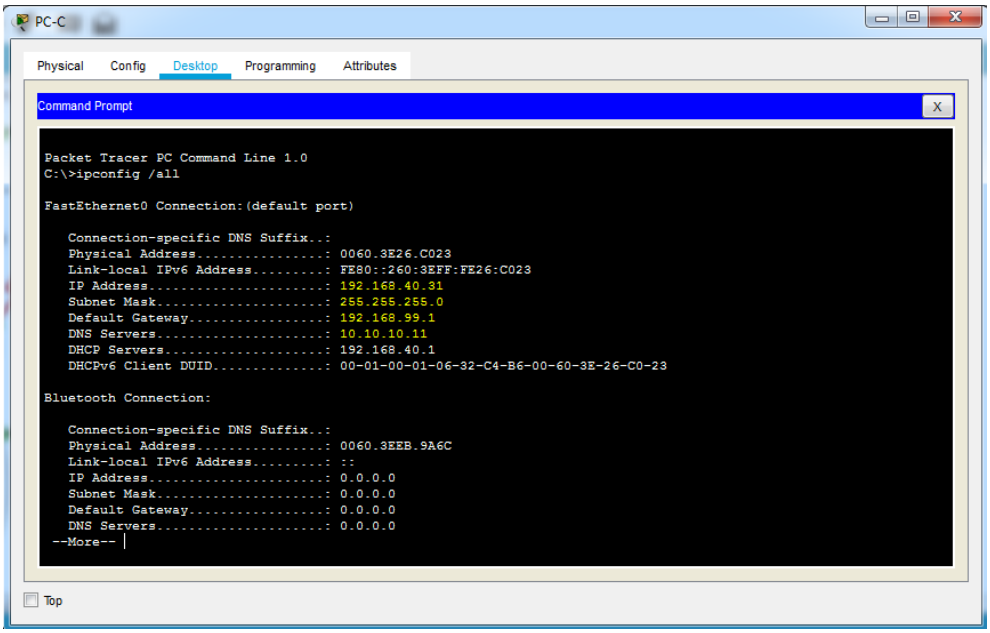

Figura 88 Validación del DHCP PC-C

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

Para configurar una NAT dinámica se utiliza se debe usar el comando ip nat pool.

```
R2(config)#ip nat pool NAT-POOL1 209.165.200.225 209.165.200.230
netmask 255.255.255.248
R2(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)#ip nat inside source list 1 pool NAT-POOL1
R2(config)#interface s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#interfa gigabitEthernet 0/0
R2(config-if)#ip nat outside
R2(config-if)#end
```

Verificación:

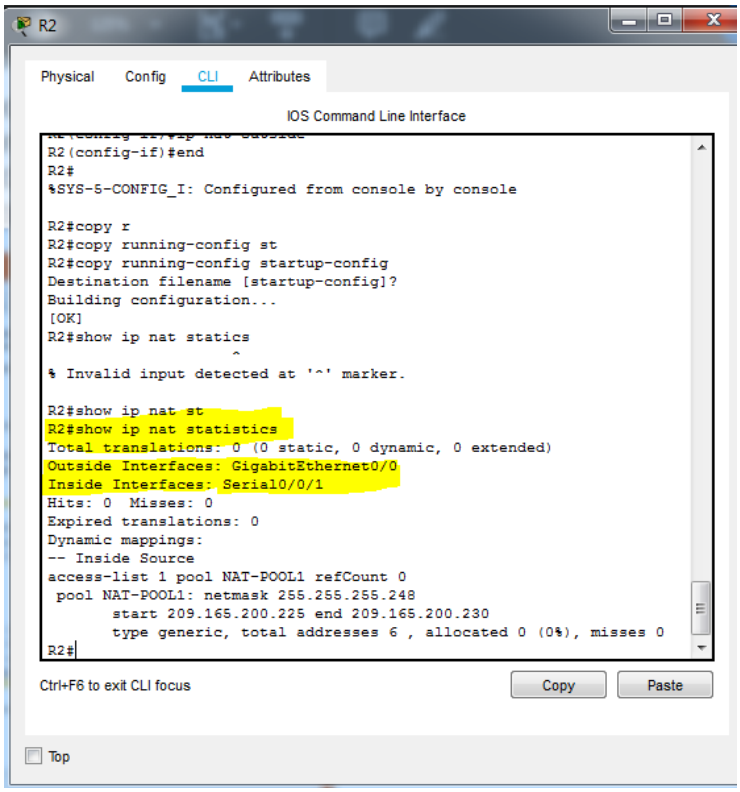

Figura 89 Verificación de NAT en R2

1.2.9 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.

Se decide configurar dos listas de acceso para permitir o denegar tráfico, para ello configuramos una ACL. Para el router R3 se bloquea el tráfico del pc con la IP 19.168.40.55, pero se permite el resto de tráfico:

R3(config)#access-list 1 deny host 192.168.40.55
R3(config)#access-list 1 permit any
R3(config)#interface g0/0.1
R3(config-subif)#ip access-group 1 in
R3(config-subif)#

Para verificar la programación utilizamos el comando show access list:

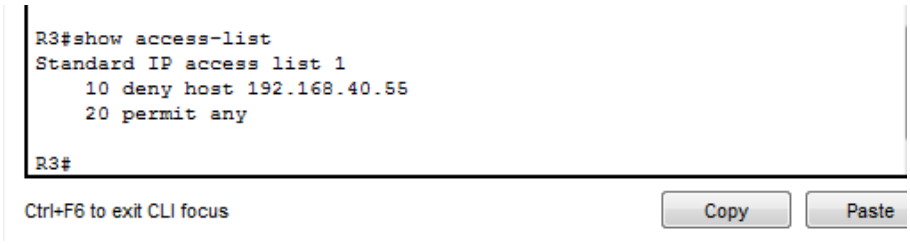

Figura 90 Verificación de listas de acceso R3

Ahora denegamos el acceso de la ip 192.168.30.99 para el router R1:

R1(config)#access-list 1 deny host 192.168.30.99
R1(config)#access-list 1 permit any
R1(config)#interface g0/0
R1(config-if)#ip access-group 1 in
R1(config-if)#exit

Verificación:

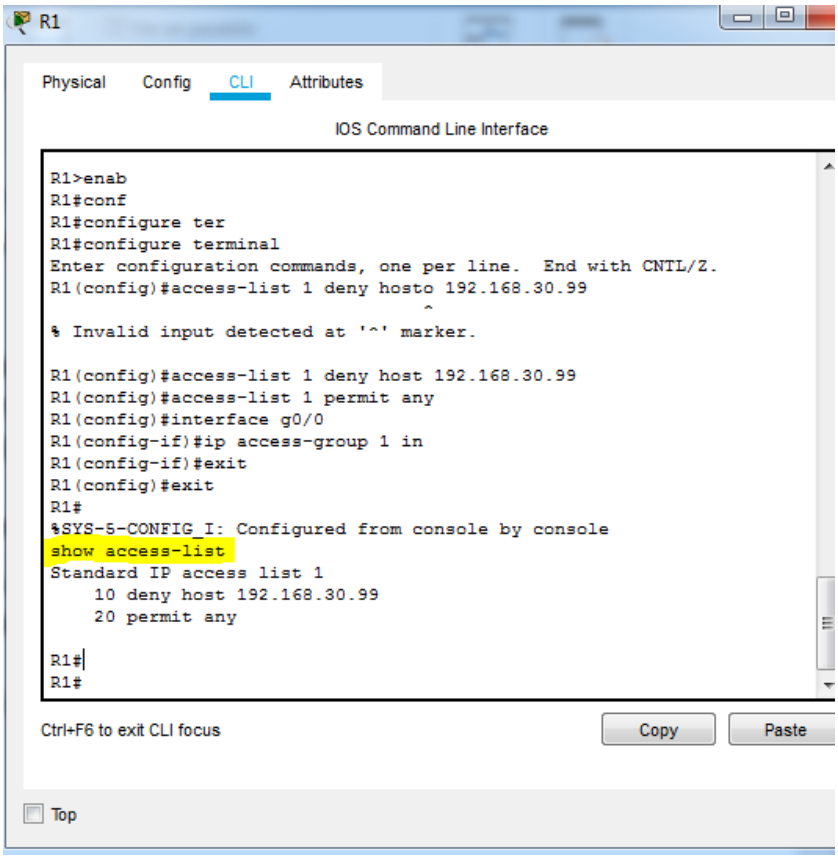

Figura 91 Verificación de listas de acceso R1

1.2.10 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.

Se debe utilizar el comando ip access-list extended nombre para definir un nombre para la ACL extendida. Para este caso se deniega el tráfico telnet de cualquier origen a la LAN 192.168.99.0/24 pero el permite el tráfico IP a través de la interfaz G0/0.1:

```
R1(config)#access-list 102 deny tcp any 192.168.99.0 0.0.0.255 eq 23
R1(config)#access-list 102 permit ip any any
R1(config)#interface g0/0.1
R1(config-subif)#ip access-group 102 out
R1(config-subif)#end
```

Verificación:

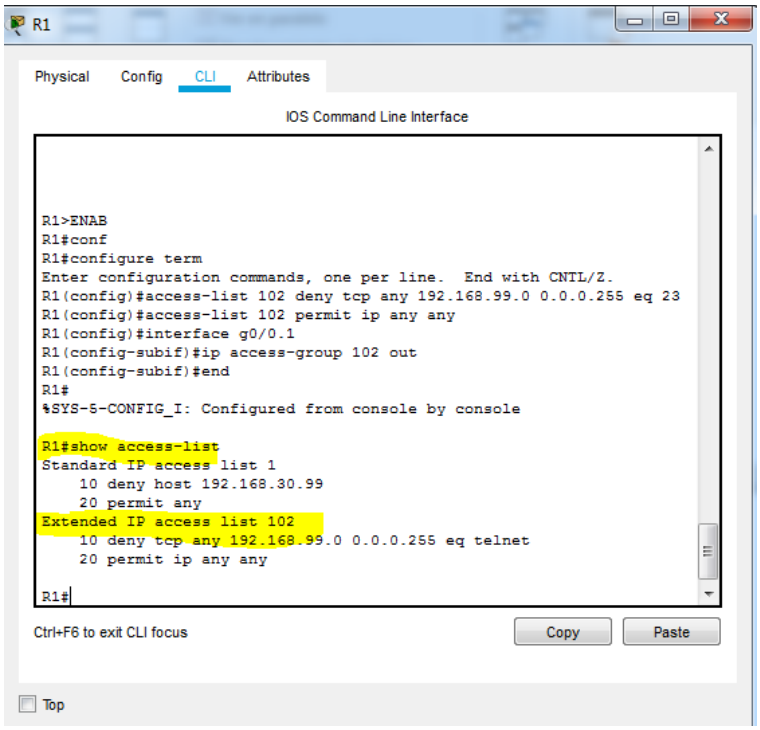

Figura 92 Verificación de listas extendidas R1

1.2.11 Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Trace route.

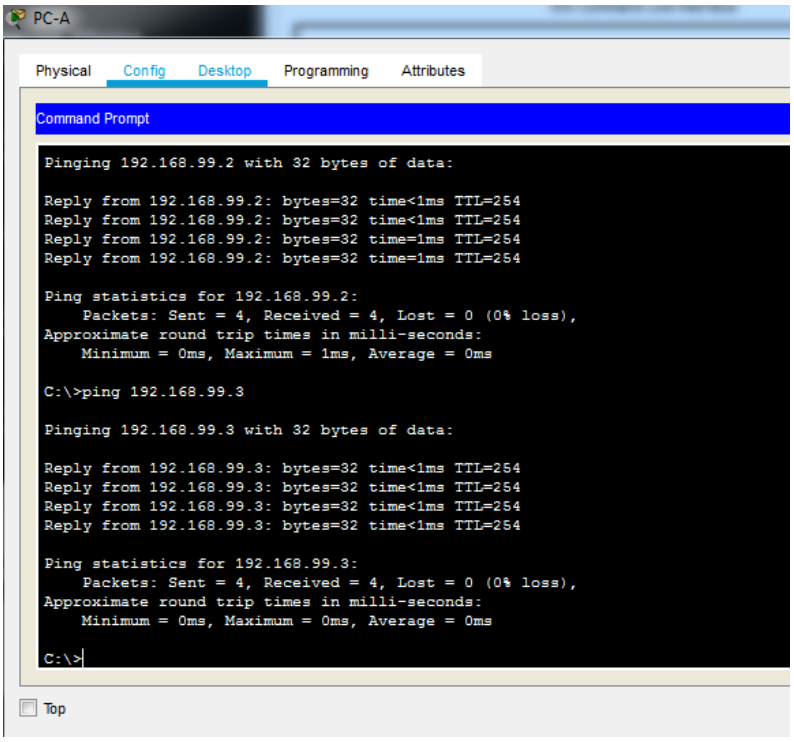

Figura 93 Verificación de pings PC-A

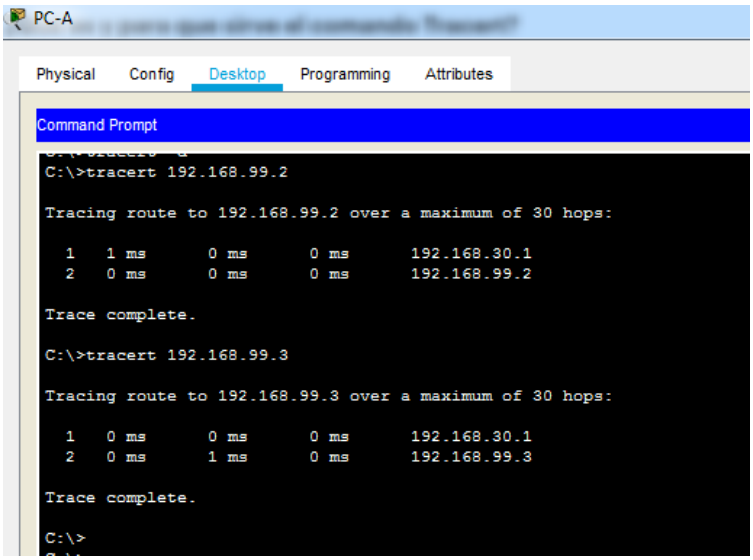

Figura 94 Tracert PC-A

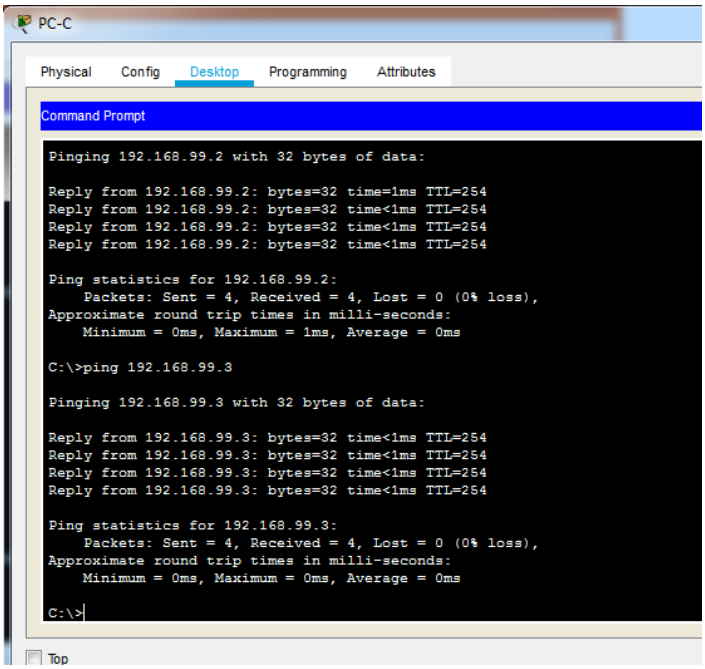

Figura 95 Verificación de pings PC-C

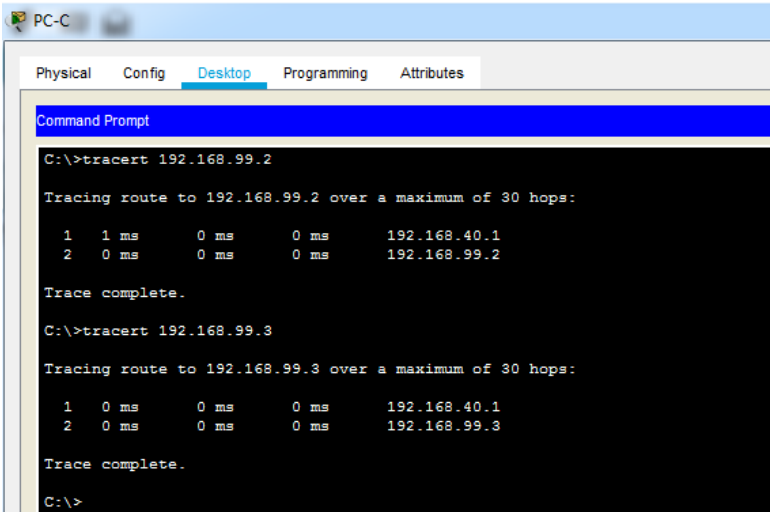

Figura 96 Tracert PC-C

CONCLUSIONES

- Con la elaboración del trabajo fue posible adquirir destrezas y conocimientos en el manejo del software Cisco Packet Tracer, además de solucionar problemas de la vida en un entorno de simulación.

- El uso de VLAN o redes locales virtuales permite la creación de redes lógicas diferentes dentro de una misma red física, facilitando la administración de la red y disminuyendo el dominio de difusión. El protocolo de etiquetado que más se utiliza es el IEEE 802.1Q.

- Se comprobó que el protocolo de configuración dinámica del servidor o DHCP permite que más de host obtengan la configuración de red de forma totalmente automática, sin que exista la necesidad de configurar manualmente las direcciones IP, mascara de subred y puerta de enlace predeterminada.

- Se puede usar la separación de privilegios mediante el uso de listas de control de acceso o ACL, permitiendo o denegando el tráfico de red de acuerdo a alguna condición en particular como bloquear protocolos en puertos específicos, lo que ayuda a prevenir tráfico indeseado en la red.

- Otra medida de seguridad que se debe tomar para prevenir el acceso no autorizado es deshabilitar los puertos que no se están usando tanto en los suiches como en los routers.

- El OSPF es un protocolo de direccionamiento llamado de estado de enlace que utiliza unos paquetes específicos para conocer dicho estado. Es muy práctico en redes heterogéneas y de gran tamaño puesto que puede recalcular las rutas en poco tiempo cuando se modifica la topología de la red.

REFERENCIAS BIBLIOGRÁFICAS

- LAN. (2018, 1 de octubre). Wikipedia, La enciclopedia libre. Fecha de consulta: 05:50, diciembre 13, 2018 desde https://es.wikipedia.org/w/index.php?title=VLAN&oldid=110982165.

- VLANs CISCO. (2018). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

- Open Shortest Path First. (2018, 14 de agosto). Wikipedia, La enciclopedia libre. Fecha de consulta: 00:47, diciembre 12, 2018 desde https://es.wikipedia.org/w/index.php?title=Open_Shortest_Path_First&oldid=109955865.

- Protocolo de configuración dinámica de host. (2018, 22 de septiembre). Wikipedia, La enciclopedia libre. Fecha de consulta: 00:48, diciembre 11, 2018 desde https://es.wikipedia.org/w/index.php?title=Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host&oldid=110778632.

- DHCP CISCO. (2018). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

- OSPF de una sola área CISCO. (2018). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

- Listas de control de acceso CISCO. (2018). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de: https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1