

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

LINA MARIA VARGAS VEJARANO

Código 1070586254

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS E INGENIERIA

FEBRERO 2019

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

LINA MARIA VARGAS VEJARANO

Informe habilidades prácticas CCNA

Director (a):

Juan Carlos Vesga

Diplomado de profundización Cisco (Diseño e implementación de soluciones integradas LAN / WAN) – Grupo 203092_1

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS E INGENIERIA

FEBRERO 2019

Nota de aceptación:

Jurado

Jurado

DEDICATORIA

Con el presente trabajo realizo la culminación de un proceso académico trascendental para el desarrollo de mi vida profesional, este trabajo es dedicado a mi familia, quienes me dieron su apoyo incondicional en todo momento y que creyeron en mí para llevar a cabo este proyecto de formación.

AGRADECIMIENTOS

Inicialmente, agradezco a Dios por darme la fortificación para empezar y ahora culminar este proceso académico de igual forma a los tutores que siempre fueron mi apoyo incondicional.

Tabla de contenido

	pág.
Resumen.....	11
Introducción.....	12
1. Escenario 1.....	13
2. Desarrollo de las actividades Escenario 1.....	16
2.1 Asignaciones de puertos y configuración de VLAN.....	16
2.2 Direccionamiento IP en ISP,R1,R2 y R3.....	17
2.3 Configuración de DHCP en host.....	19
2.4 Configuración de NAT.....	23
2.5 Configuración ruta estática.....	24
2.6 Configuración de DHCP en R2.....	24
2.7 Pruebas de ping al servidor0.....	25
2.8 Configuración dual-stack.....	28
2.9 Configuración dual-stack FastEthernet 0/0 de R3.....	31
2.10 Configuración RIPv2 en R1,R2 y R3.....	31
2.11 Consulta tabla de enrutamiento R1, R2 y R3.....	33

2.12 Pruebas de conectividad.....	36
3. Escenario 2.....	39
3.1 Direccionamiento IP.....	40
3.2 Configuración OSPFv2.....	42
3.3 Verificación información OSPF.....	44
3.4 Configuración switches.....	50
3.5 Deshabilitar DNS lookup.....	51
3.6 Asignación de direcciones IP a los switches.....	52
3.7 Desactivación Puertos.....	52
3.8 Implementación DHCP y NAT para IPv4.....	53
3.9 Configuración NAT.....	54
3.10 Listas de Acceso.....	54
3.11 Verificación comunicación.....	55
4. Conclusiones.....	58
5. Bibliografía.....	59

Tabla de ilustraciones

	pág.
Imagen 1 Escenario 1	13
Imagen 2 Laptop20.....	19
Imagen 3 Laptop21.....	19
Imagen 4 PC20.....	20
Imagen 5 PC21.....	20
Imagen 6 Laption30.....	21
Imagen 7 Laption31.....	21
Imagen 8 PC30.....	22
Imagen 9 PC31.....	22
Imagen 10 Ping a IPS.....	23
Imagen 11 Dirección IPv6 Servidor0 tomada por DHCPv6.....	25
Imagen 12 ping IPv6 de PC30 a Servidor0.....	26
Imagen 13 ping IPv6 de PC31 a Servidor0.....	27
Imagen 14 ping IPv6 de Laptop30 a Servidor0.....	27
Imagen 15 ping IPv6 de Laptop31 a Servidor0.....	28
Imagen 16 dual-stack Laptop30.....	29

Imagen 17 dual-stack Laptop31.....	29
Imagen 18 dual-stack PC30.....	30
Imagen 19 dual-stack PC31.....	30
Imagen 20 Tabla de enrutamiento R1.....	33
Imagen 21 Tabla de enrutamiento R2.....	34
Imagen 22 Tabla de enrutamiento R3.....	35
Imagen 23 <i>IPv 4 ping</i>	36
Imagen 24 ping IPv6 de Laptop31 a Servidor0.....	37
Imagen 25: ping IPv6 desde Servidor0 a PCs.....	38
Imagen 26 Escenario 2	39
Imagen 27 Direccionamiento Internet PC.....	40
Imagen 28 Verificación routing table R1.....	44
Imagen 29 Verificación routing table R2.....	45
Imagen 30 Verificación routing table R3.....	46
Imagen 31 Verificación R1.....	47
Imagen 32 Verificación en R2.....	48
Imagen 33 Verificación en R3.....	49
Imagen 34 PC-A pruebas de conectividad-	56

GLOSARIO

- **Cisco:** Empresa estadounidense proveedora de soluciones de red y fabricante de dispositivos de interconexión de redes de área local (LAN) y redes de área extensa (WAN). Fundada en 1984, Cisco tiene su sede en San José, California, y posee oficinas en todo el mundo, incluyendo Argentina, Brasil, Chile, Colombia, México y Perú.
- **Routing:** es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad. Dado que se trata de encontrar la mejor ruta posible, lo primero será definir qué se entien por "mejor ruta" y en consecuencia cuál es la "métrica" que se debe utilizar para medirla.
- **OSPF:** Protocolo de enrutamiento por estado de enlace jerárquico, que se ha propuesto como sucesor de RIP en la comunidad de Internet
- **Router:** Los routers se utilizan para conectar varias redes. Por ejemplo, puede utilizar un router para conectar sus computadoras en red a Internet y, de esta forma, compartir una conexión de Internet entre varios usuarios. El router actuará como distribuidor, seleccionado la mejor ruta de desplazamiento de la información para que la reciba rápidamente

RESUMEN

Las habilidades necesarias para aplicarlas en un campo de acción; en este caso se presenta una descripción de un escenario, en este trabajo muestra la arquitectura y la configuración básica de los routers y switches para su funcionamiento, la creación y configuración de vlans, enlaces troncales, la asignación de protocolo ospf de área única y dhcp en una red simulada de un escenario real en una empresa de tecnología con tres sucursales, en las ciudades de Miami, Bogotá y Buenos Aires, el administrador de esta red debe solucionar los problemas e interconectar los dispositivos correctamente siguiendo las especificaciones dadas por el ejercicio de la red, protocolos de enrutamiento y topología de la misma.

INTRODUCCIÓN

En este documento se desarrolló dos escenarios planteados para la culminación del diplomado de profundización CISCO, en el que como estudiante se presenta la solución a dichos planteamientos para su previo análisis, de esta manera se demostrara y aplicara los conocimientos adquiridos. Se evidencia la ejecución de los diferentes entornos a los que se exponen las soluciones integradas Wan y Lan.

Para que cada uno de los dispositivos anteriores tengan una buena comunicación dentro de su red es necesario hacer uso del comando correspondiente a cada uno de los dispositivos como lo son: Vlans, configuraciones OSPF, implementación de los protocolos DHCP – NAT y su respectiva verificación de los ACL

ESCENARIO 1

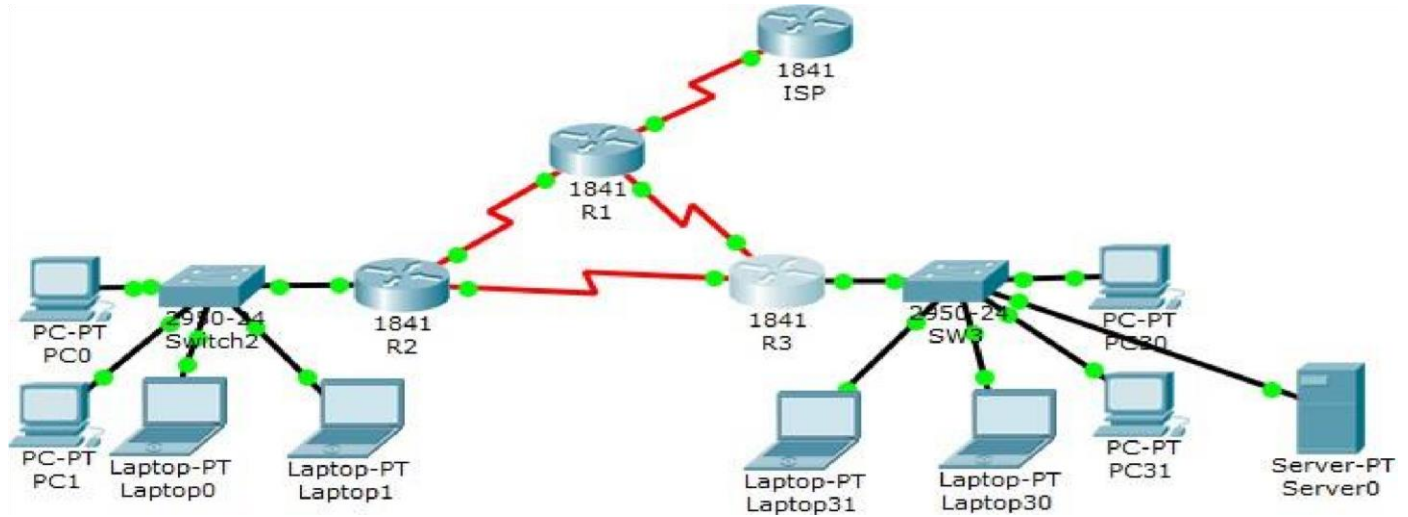


IMAGEN 1

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

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 de 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

Tabla de enlaces troncales

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

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.

Descripción de las actividades

- **SW1** VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.
- Los puertos de red que no se utilizan se deben deshabilitar.
- **La información** de dirección **IP R1, R2** y R3 debe cumplir con la tabla 1.
- **Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31** deben obtener información IPv4 del servidor DHCP.
- **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**.
- **R1** debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en **el dominio** RIPv2.
- **R2** es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.
- **R2** debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.
- El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).
- 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.
- La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).
- R1, R2 y R3 intercambian información de routing mediante RIP versión 2

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

2. DESARROLLO ESCENARIO 1

2.1. Asignaciones de puertos y configuración de VLAN

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

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

La solución de este punto, consiste, primero que nada, en darle un nombre al switch, seguidamente, darle el carácter que requiere la interfaz 0/1, el cual debe ser troncal, para permitir el paso de todas las vlan que creamos en el switch, luego, damos acceso a las vlan indicadas, los puertos asignados a terminales, por último, apagamos las interfaces que no sean utilizadas, esta acción agrega seguridad a la implementación, guardamos la configuración usando los comandos copy running-config startup-config o write El script requerido, lo escribimos a continuación: enable configure terminal hostname SW2

```
interface fast0/1
switchport mode trunk
vlan 100 vlan 200
interface fast0/2
switchport access vlan
100 switchport mode
access interface fast0/3
switchport access vlan
100 switchport mode
access interface fast0/4
switchport access vlan
```



```
200 switchport mode
access interface fast0/5
switchport access vlan
200 switchport mode
access interface range
f0/6-24 shutdown end
write
```

2.2. Direcccionamiento IP en ISP, R1, R2 y R3

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

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

El siguiente es el script que utilizaremos: **Para ISP**

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

```
R1: enable
configure
terminal host R1
inter s0/0/0

ip address 200.123.211.2
255.255.255.0 no shutdown inter
s0/1/0 ip address 10.0.0.1
255.255.255.252 no shutdown inter
s0/1/1 ip address 10.0.0.5
```

```
255.255.255.252 no shutdown end  
write
```

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

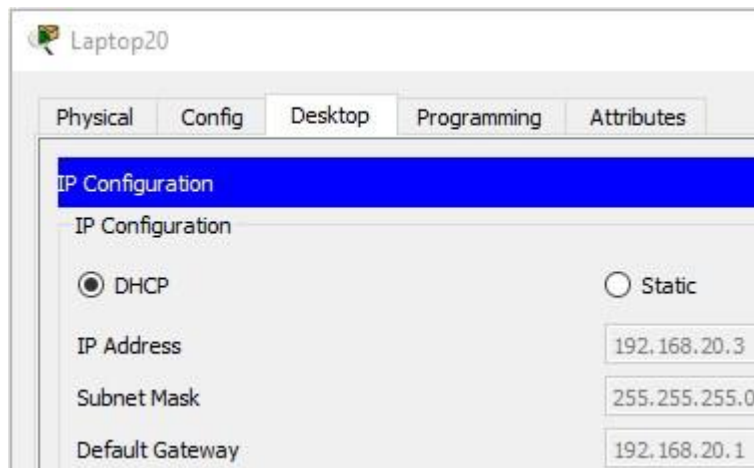
```
R3: enable configure terminal host R3  
interface fast0/0 ip address 192.168.30.1  
255.255.255.0 ipv6 address  
2001:DB8:130::9C0:80F:301/64 ipv6  
enable no shutdown interface serial0/0/0  
ip address 10.0.0.6  
255.255.255.252 inter s0/0/1 ip  
address 10.0.0.10  
255.255.255.252 no shutdown  
end write
```

2.3. Configuración de DHCP en host

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

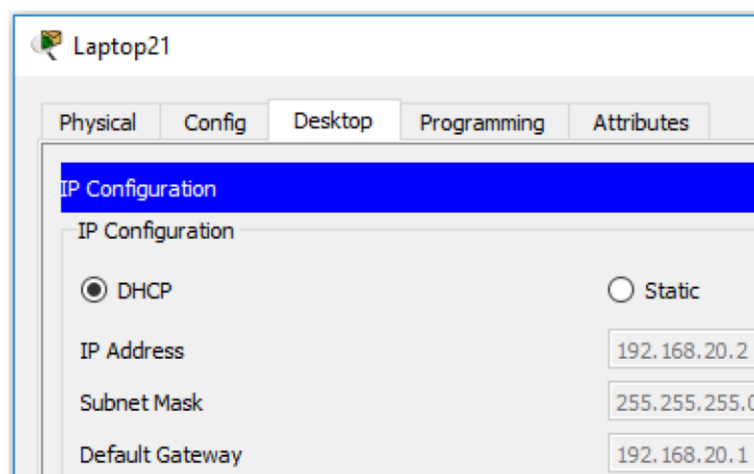
Luego de hacer las configuraciones de hacer las configuraciones en los routers sobre direccionamientos, pasamos a realizar lo mismo en los PC conectados, pero acá usamos la interfaz gráfica, para ello damos click sobre el terminal a modificar y luego en la pestaña Desktop, por último hacemos click en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

Imagen 2: Laptop20



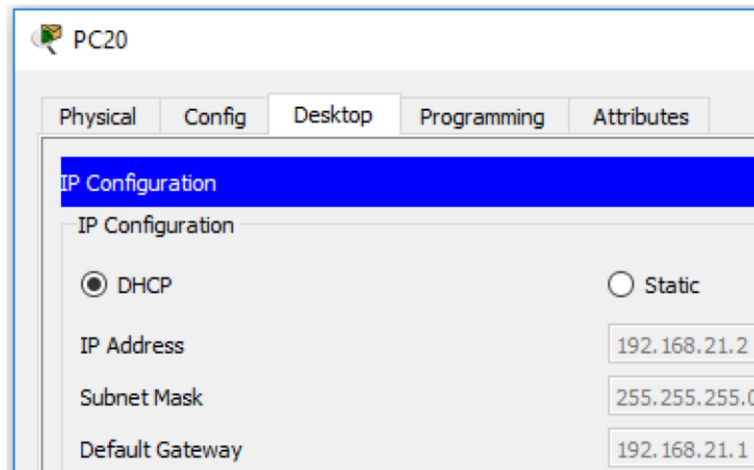
En esta parte vemos que a la Laptop20 se le seleccionó la opción DHCP y le dio una dirección 192.168.20.3/24 y gateway 192.168.20.1

Imagen 3: Laptop21



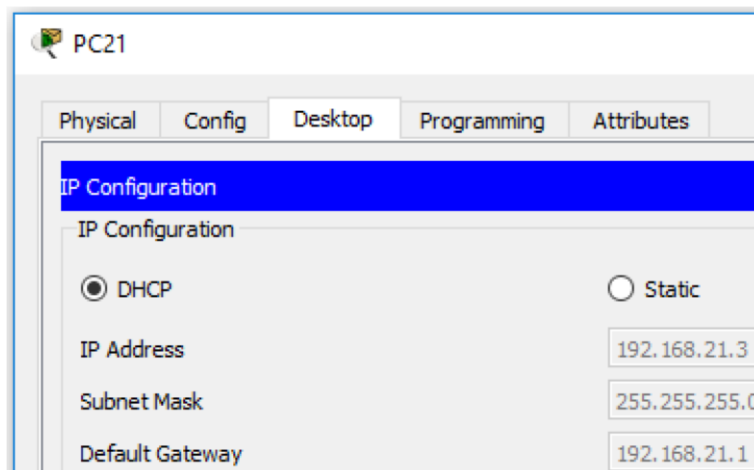
Se observa a la Laptop21 se le seleccionó DHCP y la dirección obtenida es 192.168.20.2/24 y gateway 192.168.20.1

Imagen 4: PC20



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

Imagen 5: PC21



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

Imagen 6: Laptop30

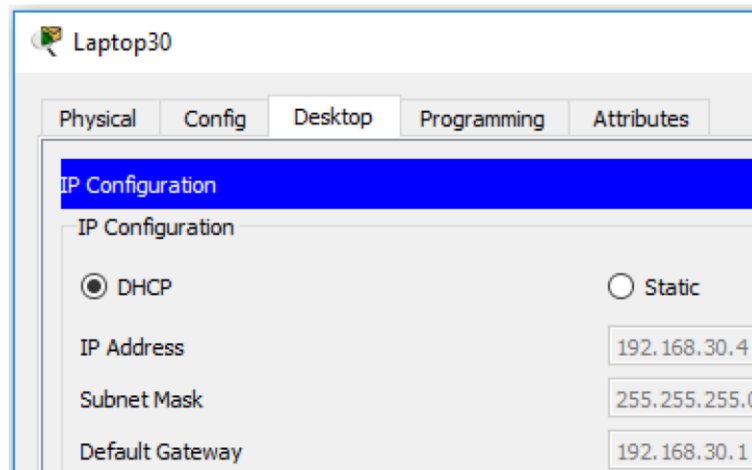


Imagen 7: Laptop31

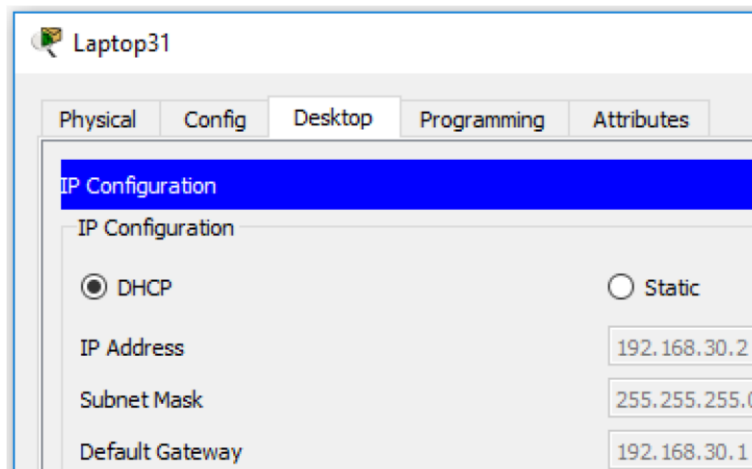
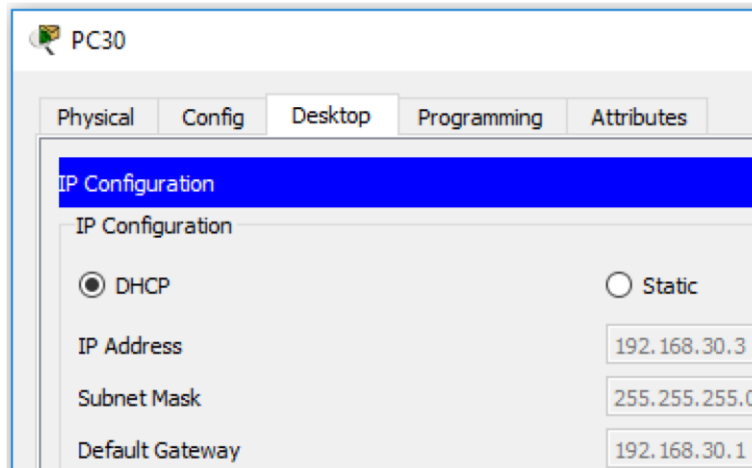
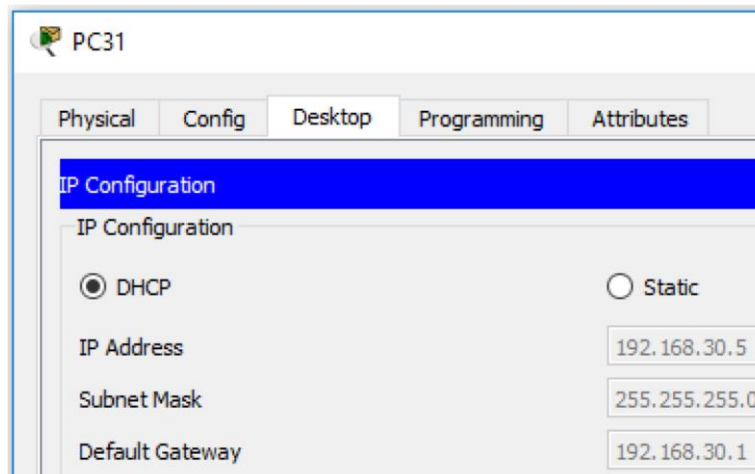


Imagen 8: PC30



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

Imagen 9: PC31



Respuesta de DHCP satisfactoria en PC31









2.4. Configuración de NAT

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

Es muy importante para los terminales alcancen a ISP y que, en la práctica en la vida real, se emplea esto a diario, ya que ayuda a alargar el tiempo de vida de las IPv4. Se muestra a continuación, el cli para que este proceso se ponga en función, debemos crear una lista de acceso, para indicar que terminales dentro de nuestra red pueden alcanzar ISP, posteriormente, escribimos la línea que indica como se hará NAT o mejor dicho PAT que es como se le conoce al NAT con sobrecarga, se indican las interfaces de entrada y salida y ya está: enable configure terminal ip access-list standard INSIDE-DEVS permit 192.168.0.0 0.0.255.255 ip nat inside source list INSIDE-DEVS inter s0/0/0 overload interface serial0/0/0 ip nat outside interface serial0/1/0 ip nat inside

```
inter s0/1/1
ip nat
inside end
write
```

Imagen 10 ping a IPS

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

Se evidencia que las pruebas de conectividad con ICMP bien trabajada.

2.5. Configuración ruta estática

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

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

```
enable
configure terminal
ip route 0.0.0.0 0.0.0.0
Serial0/0/0 end
write
```

2.6. Configuración de DHCP en R2

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

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

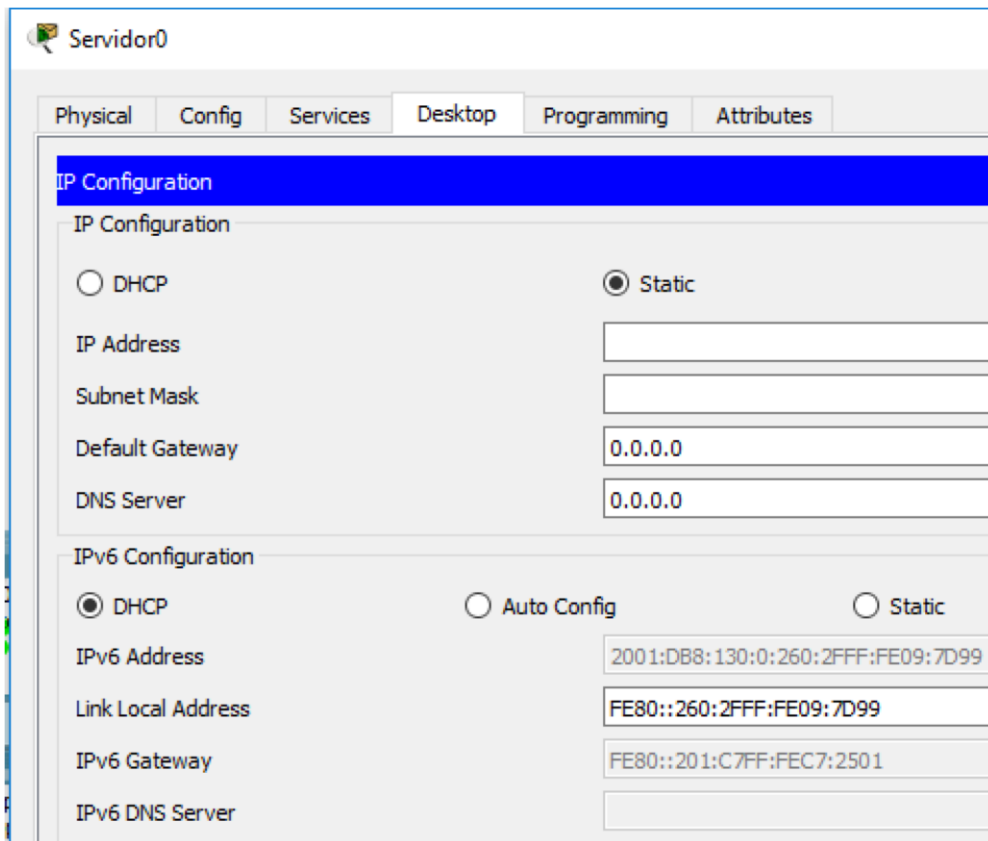
```
enable
configure terminal
ip dhcp
pool vlan_100 network
192.168.20.0 255.255.255.0
default-router 192.168.20.1
ip
dhcp pool vlan_200 network
192.168.21.0 255.255.255.0
default-router 192.168.21.1
end
write
```


2.7. Pruebas de ping al Servidor0

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

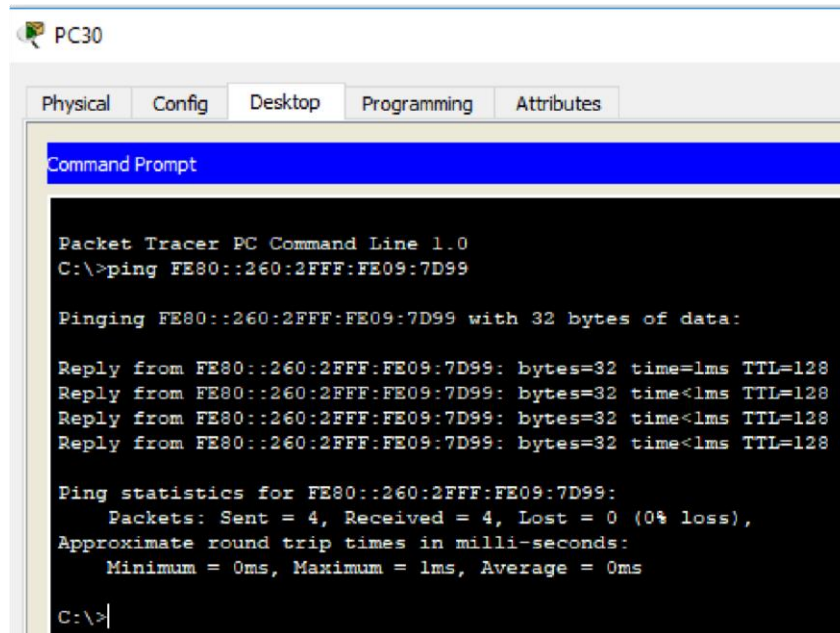
Ya hecho el paso anterior y con las direcciones obtenidas, se puede realizar las pruebas de conectividad, haciendo ping desde Servidor0, pero en protocolo IPv6, a continuación, las pruebas:

Imagen 11: Dirección IPv6 Servidor0 tomada por DHCPv6



Acá evidenciamos que hemos cambiado la configuración estática a la configuración por DHCP en versión IPv6, ya que el router se encuentra en doble stack, por lo que realizaremos las pruebas de conectividad:

Imagen 12: ping IPv6 de PC30 a Servidor0



```
PC30
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping FE80::260:2FFF:FE09:7D99

Pinging FE80::260:2FFF:FE09:7D99 with 32 bytes of data:

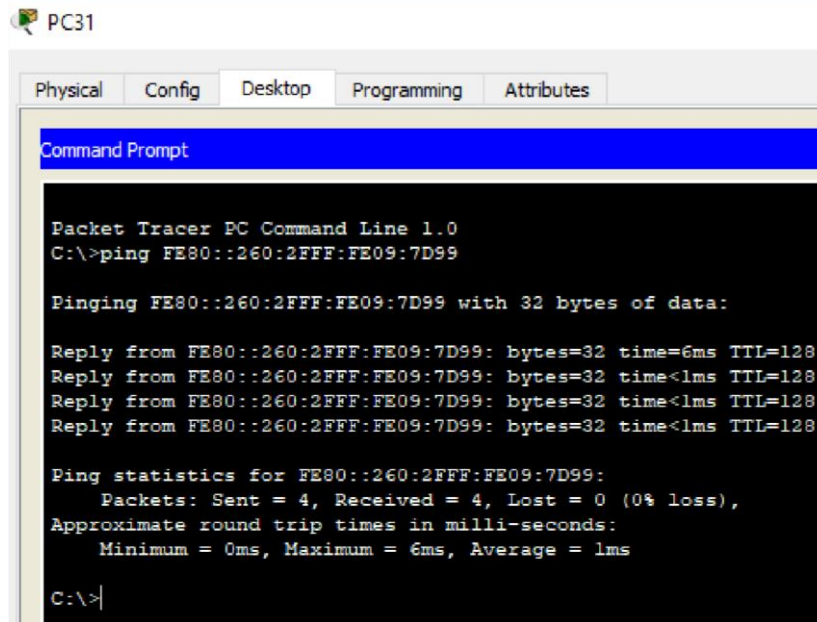
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time=1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128

Ping statistics for FE80::260:2FFF:FE09:7D99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

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

Imagen 13: ping IPv6 de PC31 a Servidor0



```
PC31
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping FE80::260:2FFF:FE09:7D99

Pinging FE80::260:2FFF:FE09:7D99 with 32 bytes of data:

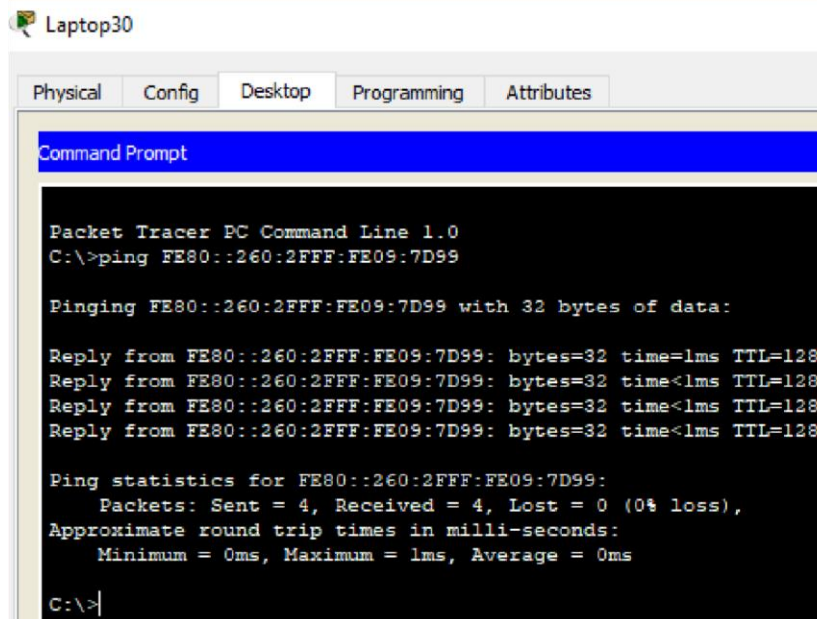
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time=6ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128

Ping statistics for FE80::260:2FFF:FE09:7D99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 1ms

C:\>
```

Desde PC31 se realiza el mismo paso y se obtiene el mismo resultado.

Imagen 14: ping IPv6 de Laptop30 a Servidor0



```
Laptop30
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping FE80::260:2FFF:FE09:7D99

Pinging FE80::260:2FFF:FE09:7D99 with 32 bytes of data:

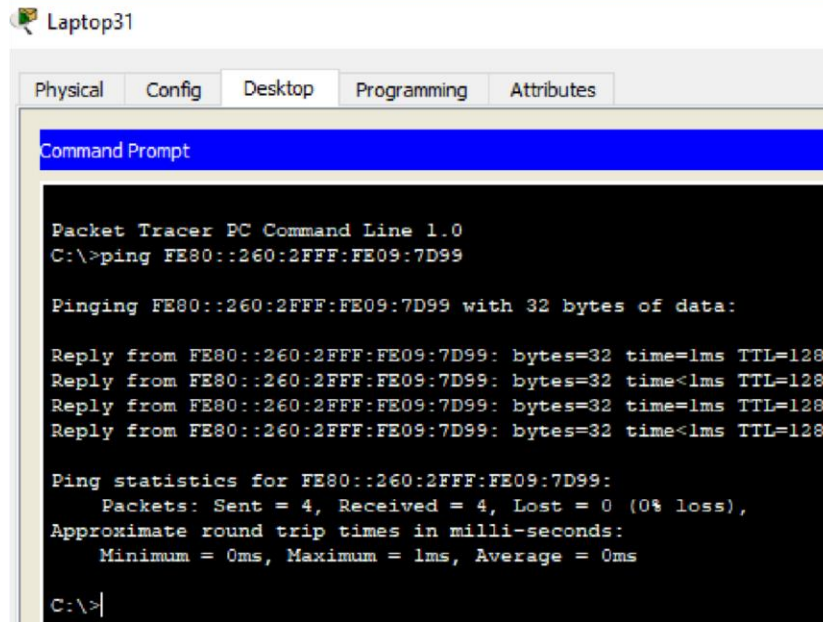
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time=1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128

Ping statistics for FE80::260:2FFF:FE09:7D99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

Desde las Laptop igualmente

Imagen 15: ping IPv6 de Laptop31 a Servidor0



```
Packet Tracer PC Command Line 1.0
C:\>ping FE80::260:2FFF:FE09:7D99

Pinging FE80::260:2FFF:FE09:7D99 with 32 bytes of data:

Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time=1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time=1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128

Ping statistics for FE80::260:2FFF:FE09:7D99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

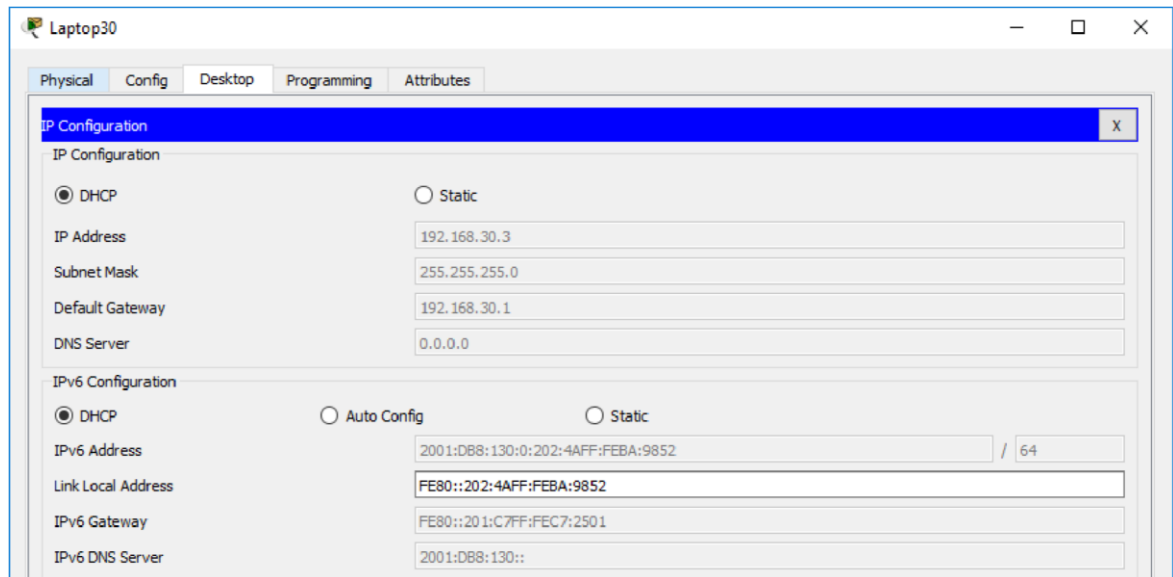
Todos han sido corroborados, lo que nos indica que la configuración para DHCPv6 es correcta.

2.8. Configuración dual-stack

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

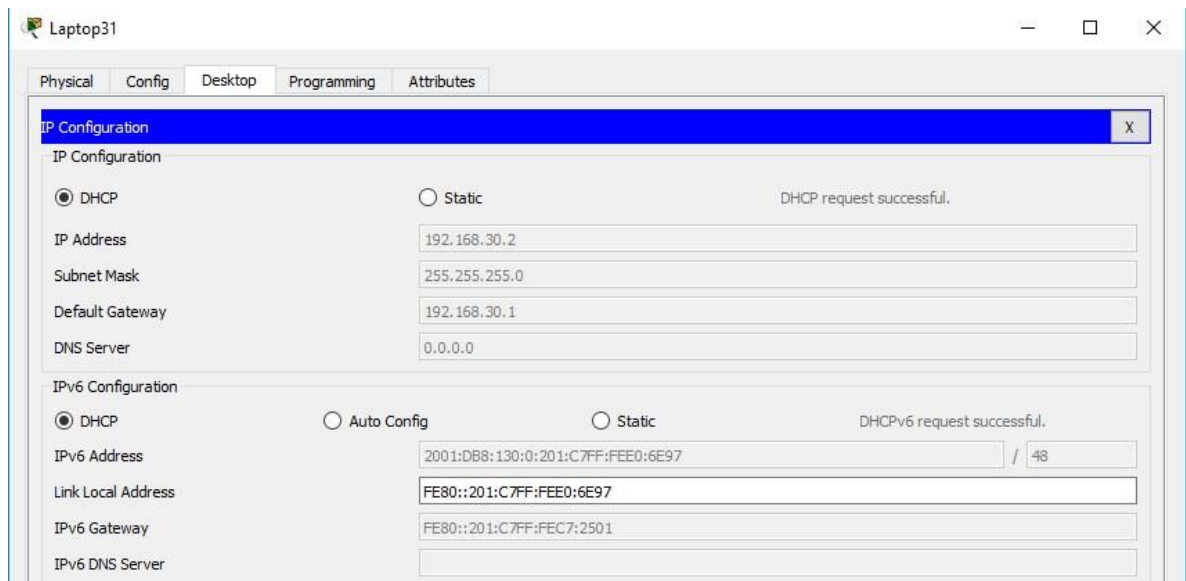
Para que los equipos obtengan direccionamiento de las dos pilas disponibles, solo debemos hacer click en el equipo a modificar, luego en la pestaña Desktop, IP Configuration, y selecciona en ambos apartados DHCP ya que por defecto viene estático:

Imagen 16: dual-stack Laptop30



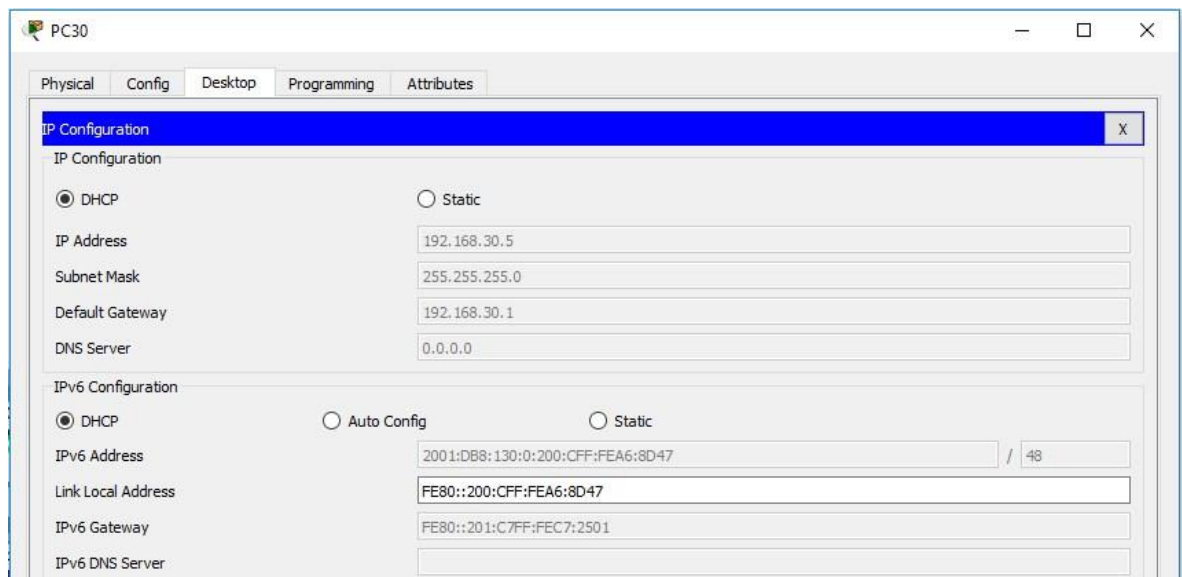
Se verifica que las 2 pilas tomaron direccionamiento con la numeración correspondiente, decimal para IPv4 y hexadecimal para IPv6.

Imagen 17: dual-stack Laptop31



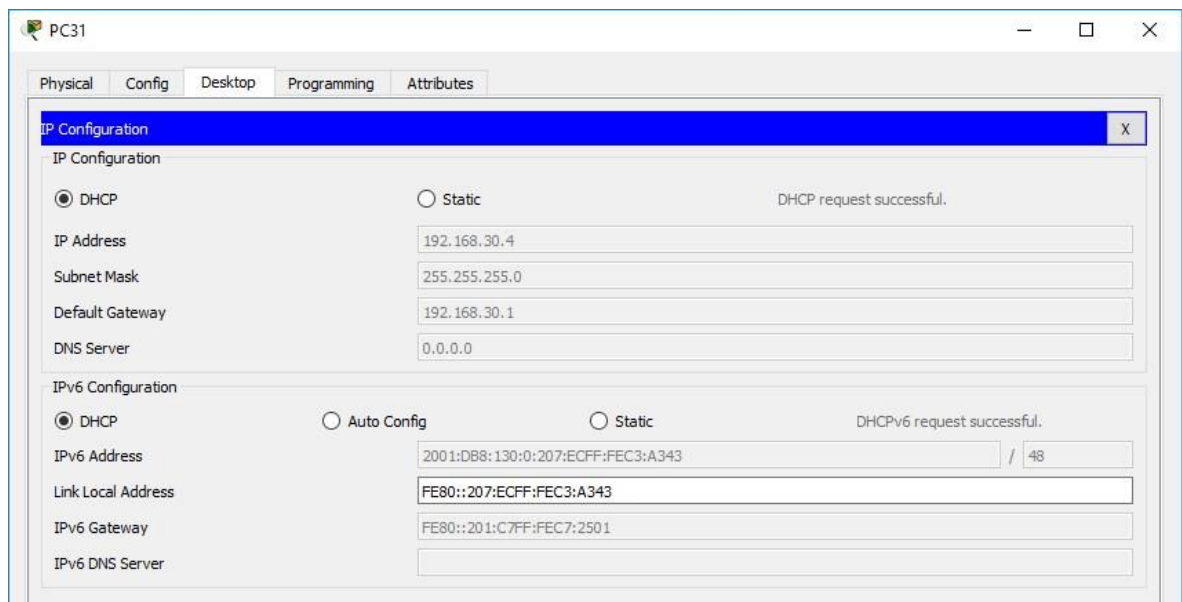
Creamos lo propio para cada uno de los terminales conectados a esa red, acá observamos que la respuesta del servidor DHCP fue satisfactoria.

Imagen 18: dual-stack PC30



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

Imagen 19: dual-stack PC31



Se evidencia, ya concluimos lo que sería la configuración a doble stack en la parte cliente.

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

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

La configuración necesaria a realizar en el router para que funcione el doble stack, para ello, lo principal es entrar a la interfaz involucrada y habilitar el unicast-routing en IPv6, crear el pool, darle la dirección IPv6 que queremos colocar, en este caso, la que tenemos en la tabla 1 para ello. Por último habilitamos en la interfaz el IPv6 y declaramos el pool DHCP creado, a continuación el script:

```
enable ipv6 unicast-  
routing ipv6 dhcp  
pool dhcpv6  
  
prefix-delegation pool dhcpv6-pool1 lifetime 1800 600  
exit
```

```
ipv6 local pool dhcpv6-pool1  
2001:DB8:130::9C0:80F:301/40 48 inter f0/0 ip addr  
192.168.30.1 255.255.255.0 ipv6 address  
2001:DB8:130::9C0:80F:301/64 ipv6 enable  
ipv6 dhcp server  
dhcpv6 end write
```

2.10. Configuración RIPv2 en R1, R2 Y R3

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

Aquí se estableciera los routers para que intercambien información de rutas y así los paquetes enviados desde los terminales, encuentren su destino, para ello, debemos habilitar el RIPv2 en el router y seguidamente, declarar las redes que puede ver directamente el router, no olvidamos guardar lo que configuramos con el

comando write o copy runningconfig startup-config, para que la configuración almacenada suba nuevamente en caso de reinicio.

```
R1: enable configure
terminal router rip
version 2 network
10.0.0.0 network
200.123.211.0 end
write
```

```
R2: enable configure
terminal router rip
version 2 network
10.0.0.0 network
192.168.20.0
network
192.168.21.0
network
200.123.211.0 end
write
```

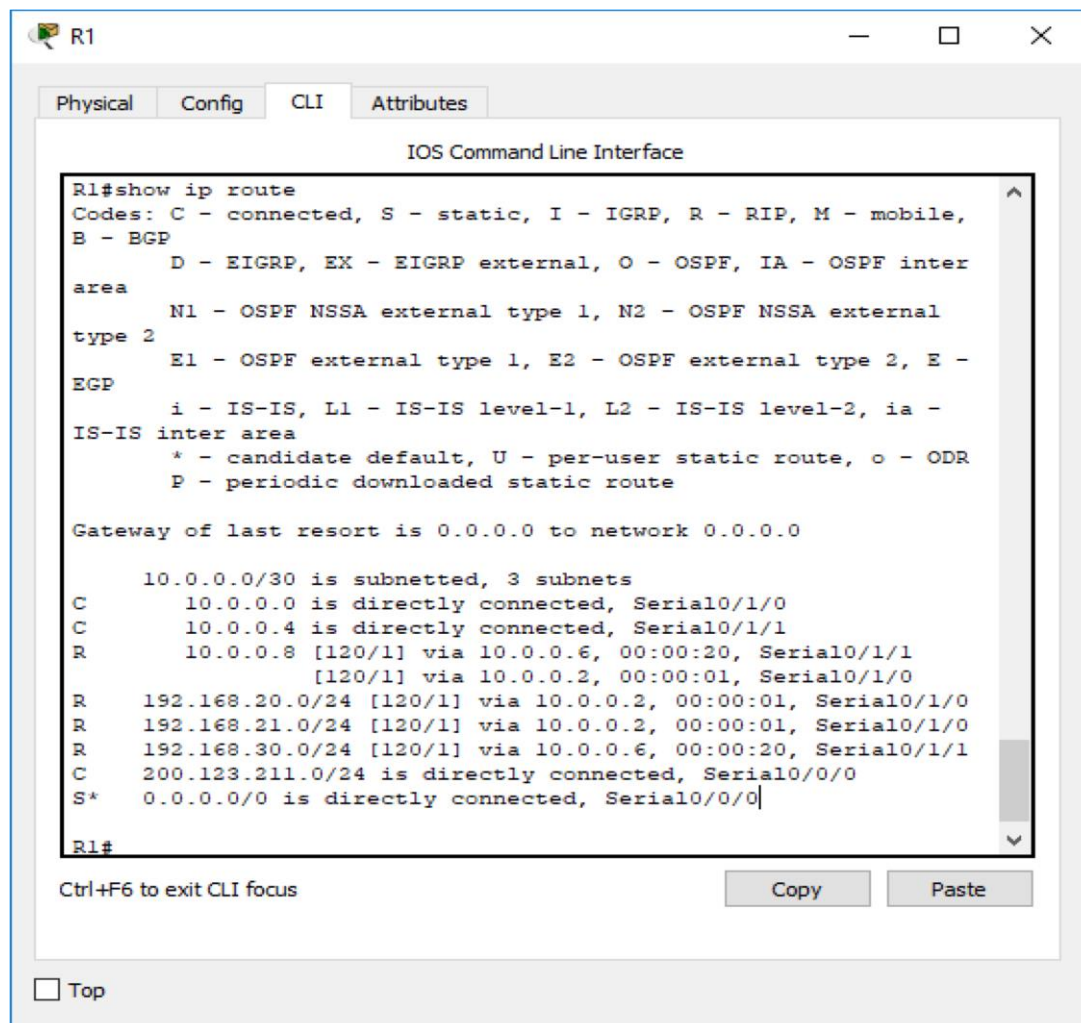
```
R3: enable configure
terminal router rip
version 2 network
10.0.0.0 network
192.168.30.0
network
200.123.211.0 end
write
```


2.11. Consulta tabla de enrutamiento R1, R2 y R3

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

Las tablas de enrutamiento estén todas las redes que se han configurado en cada uno de los routers, esto con el objetivo de tener la certeza que los paquetes van a llegar a destino sin necesidad de estar escribiendo las rutas una a una. Se resalta que en los RIPv1 y RIPv2 se usan saltos como métricas para determinar qué camino tomar para enrutar datos, ambos tienen un límite de 15 saltos, el salto 16 el paquete es descartado.

Imagen 20: Tabla de enrutamiento R1



```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

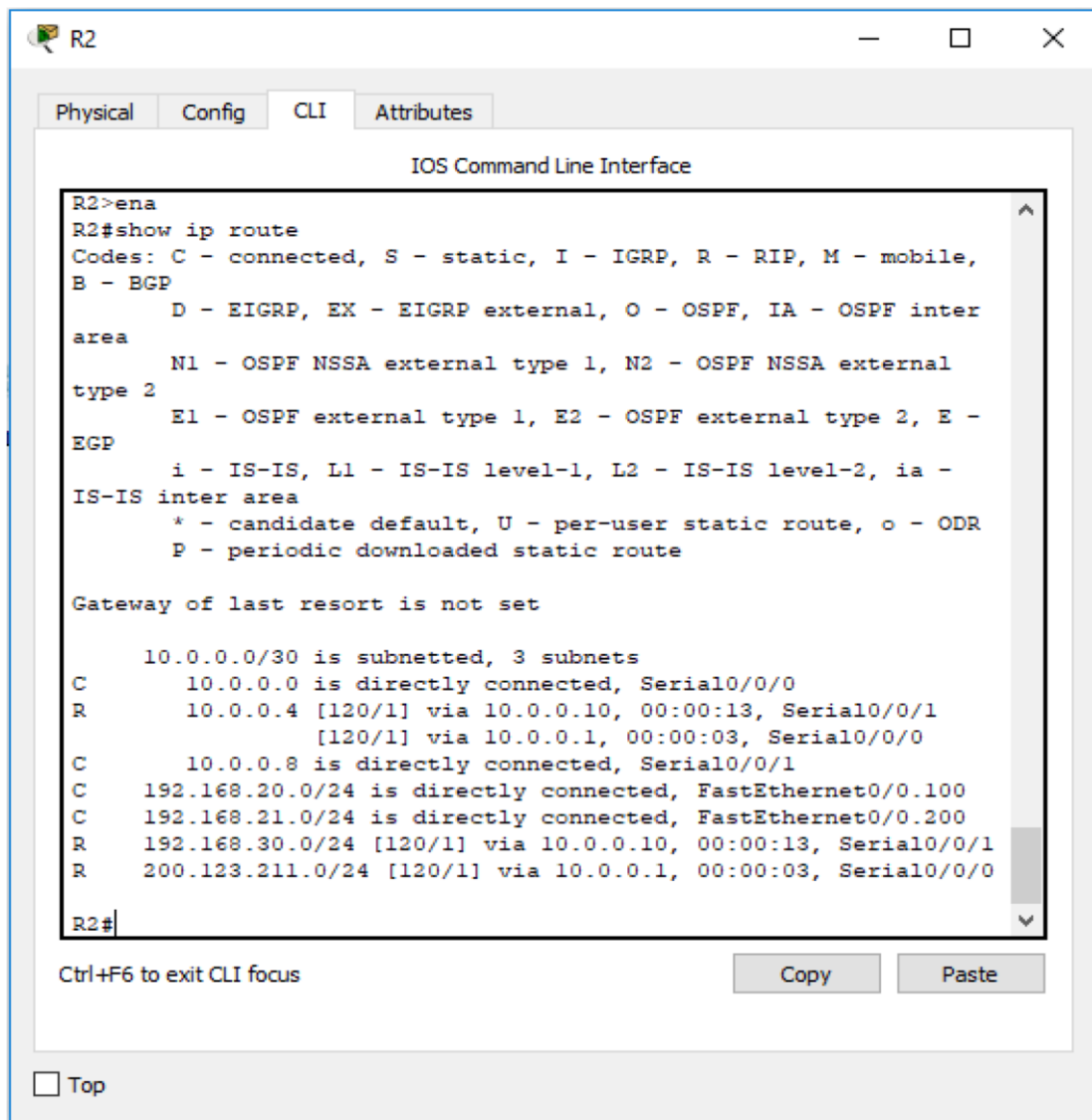
Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/30 is subnetted, 3 subnets
C       10.0.0.0 is directly connected, Serial0/1/0
C       10.0.0.4 is directly connected, Serial0/1/1
R       10.0.0.8 [120/1] via 10.0.0.6, 00:00:20, Serial0/1/1
         [120/1] via 10.0.0.2, 00:00:01, Serial0/1/0
R      192.168.20.0/24 [120/1] via 10.0.0.2, 00:00:01, Serial0/1/0
R      192.168.21.0/24 [120/1] via 10.0.0.2, 00:00:01, Serial0/1/0
R      192.168.30.0/24 [120/1] via 10.0.0.6, 00:00:20, Serial0/1/1
C      200.123.211.0/24 is directly connected, Serial0/0/0
S*     0.0.0.0/0 is directly connected, Serial0/0/0

R1#
```

Se evidencia que la tabla de enrutamiento de R1, y de como el router conoce las rutas directamente conectadas, pues son las que declaramos en el propio router, y las se adquirieron por RIP, para ello, al comienzo de cada línea hay una letra en mayúsculas, que indica cómo se adquirieron esas rutas, por ejemplo, si se obtuvo por RIP, la letra que le precede es R, si por el contrario es una ruta directamente conectada, le precede una C.

Imagen 21: Tabla de enrutamiento R2



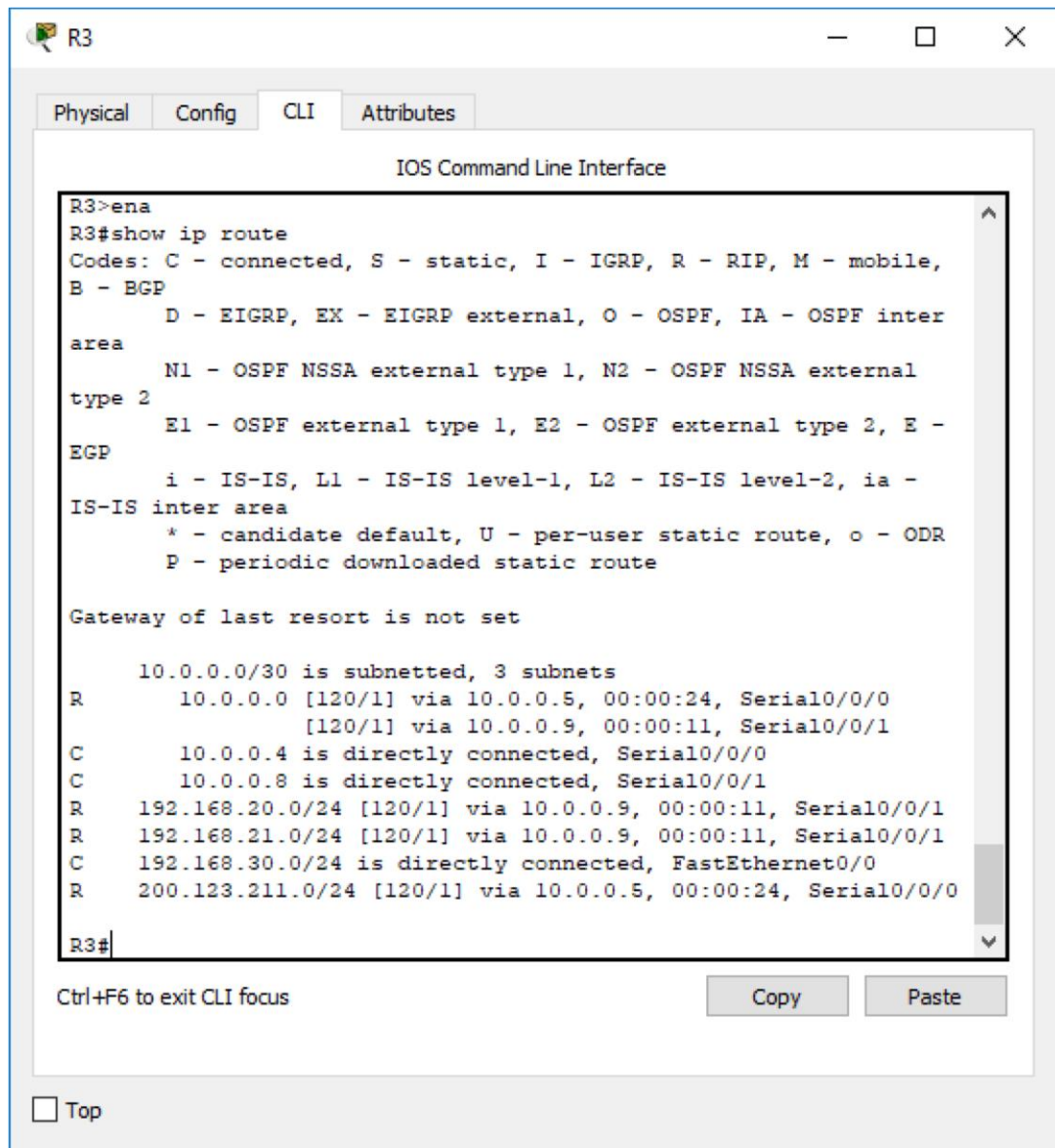
```
R2>ena
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external
type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia -
IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

      10.0.0.0/30 is subnetted, 3 subnets
C       10.0.0.0 is directly connected, Serial10/0/0
R       10.0.0.4 [120/1] via 10.0.0.10, 00:00:13, Serial10/0/1
        [120/1] via 10.0.0.1, 00:00:03, Serial10/0/0
C       10.0.0.8 is directly connected, Serial10/0/1
C       192.168.20.0/24 is directly connected, FastEthernet0/0.100
C       192.168.21.0/24 is directly connected, FastEthernet0/0.200
R       192.168.30.0/24 [120/1] via 10.0.0.10, 00:00:13, Serial10/0/1
R       200.123.211.0/24 [120/1] via 10.0.0.1, 00:00:03, Serial10/0/0
R2#
```

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

Imagen 22: Tabla de enrutamiento R3



Se evidencia los routers involucrados en la topología implementadas, conocen las rutas necesarias para poder intercomunicar los diferentes terminales con el ISP o inversamente.

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.

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

Imagen 23. IPv 4 ping

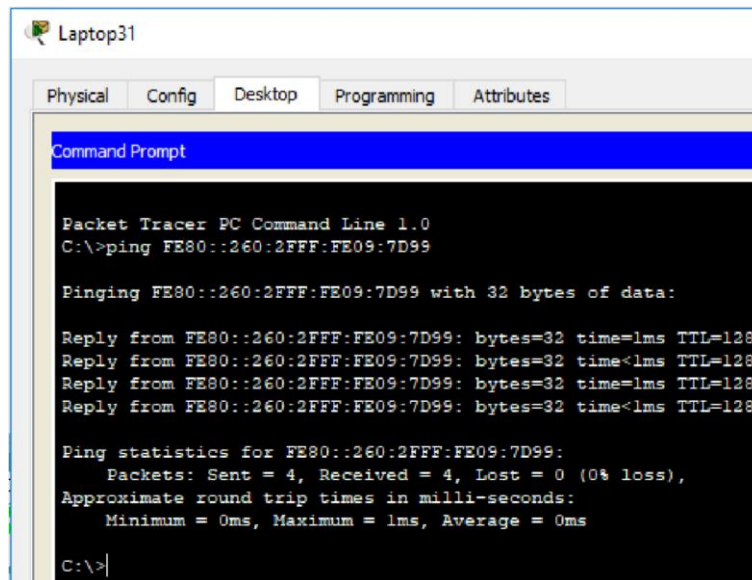
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC20	Laptop21	ICMP	Black	0.000	N	0	(edit)	(delete)
	Successful	PC20	ISP	ICMP	Purple	0.000	N	1	(edit)	(delete)
	Successful	PC20	PC31	ICMP	Yellow	0.000	N	2	(edit)	(delete)
	Successful	Lapto...	Laptop20	ICMP	Pink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

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC31	ISP	ICMP	Green	0.000	N	4	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP	Teal	0.000	N	5	(edit)	(delete)
	Successful	PC20	ISP	ICMP	Light Green	0.000	N	6	(edit)	(delete)
	Successful	PC21	ISP	ICMP	Blue	0.000	N	7	(edit)	(delete)

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Lapto...	ISP	ICMP	Purple	0.000	N	8	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP	Green	0.000	N	9	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP	Brown	0.000	N	10	(edit)	(delete)
	Successful	Lapto...	ISP	ICMP	Olive	0.000	N	11	(edit)	(delete)
	Successful	PC31	ISP	ICMP	Blue	0.000	N	12	(edit)	(delete)
	Successful	PC30	ISP	ICMP	Dark Blue	0.000	N	13	(edit)	(delete)

Se muestra que fue satisfactorio el ping para las diferentes terminales.

Imagen 24: ping IPv6 de Laptop31 a Servidor0



```
Packet Tracer PC Command Line 1.0
C:\>ping FE80::260:2FFF:FE09:7D99

Pinging FE80::260:2FFF:FE09:7D99 with 32 bytes of data:

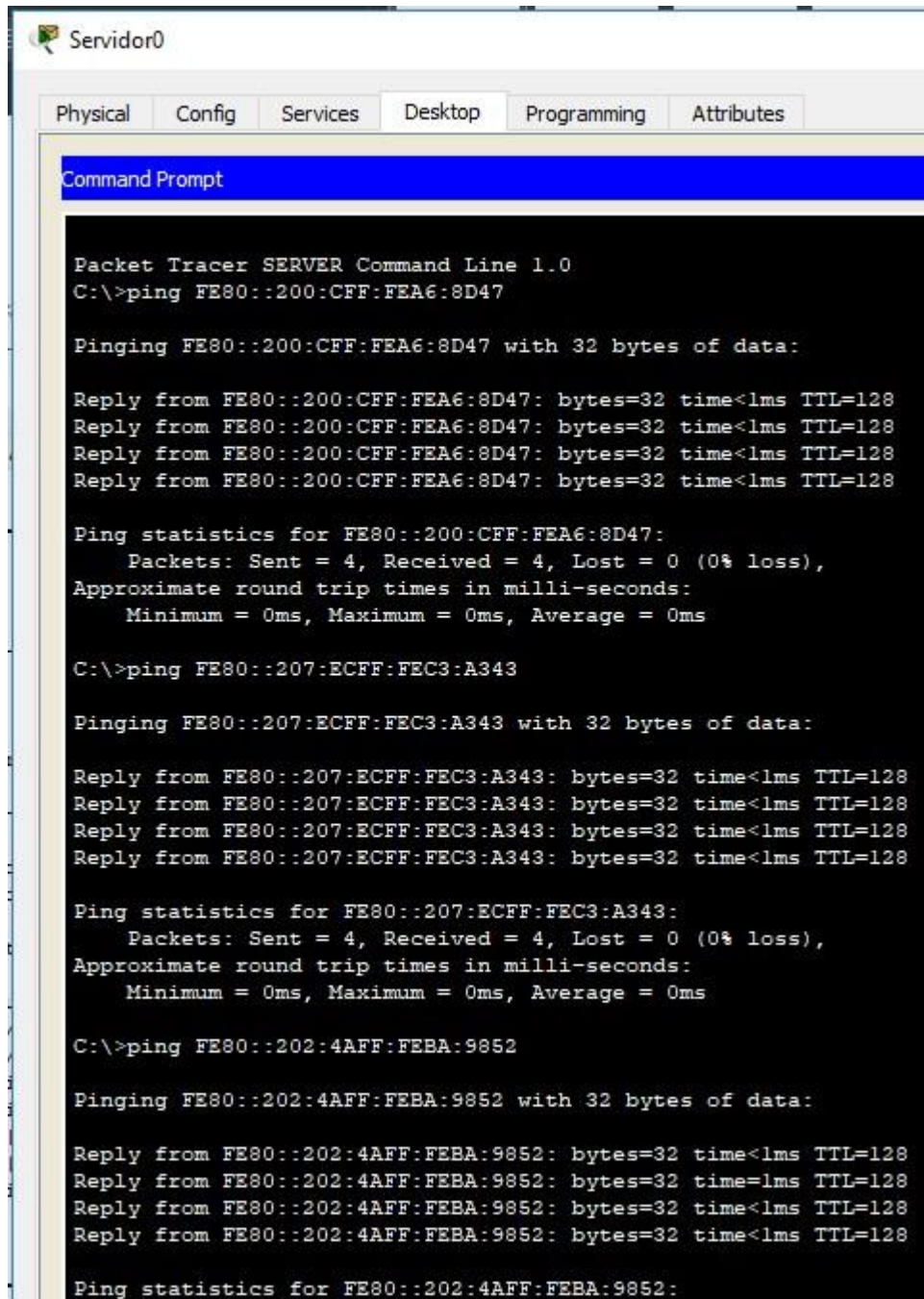
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128
Reply from FE80::260:2FFF:FE09:7D99: bytes=32 time<1ms TTL=128

Ping statistics for FE80::260:2FFF:FE09:7D99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

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

Imagen 25: ping IPv6 desde Servidor0 a PCs



```
Packet Tracer SERVER Command Line 1.0
C:\>ping FE80::200:CFF:FEA6:8D47

Pinging FE80::200:CFF:FEA6:8D47 with 32 bytes of data:

Reply from FE80::200:CFF:FEA6:8D47: bytes=32 time<lms TTL=128
Reply from FE80::200:CFF:FEA6:8D47: bytes=32 time<lms TTL=128
Reply from FE80::200:CFF:FEA6:8D47: bytes=32 time<lms TTL=128
Reply from FE80::200:CFF:FEA6:8D47: bytes=32 time<lms TTL=128

Ping statistics for FE80::200:CFF:FEA6:8D47:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping FE80::207:ECFF:FEC3:A343

Pinging FE80::207:ECFF:FEC3:A343 with 32 bytes of data:

Reply from FE80::207:ECFF:FEC3:A343: bytes=32 time<lms TTL=128
Reply from FE80::207:ECFF:FEC3:A343: bytes=32 time<lms TTL=128
Reply from FE80::207:ECFF:FEC3:A343: bytes=32 time<lms TTL=128
Reply from FE80::207:ECFF:FEC3:A343: bytes=32 time<lms TTL=128

Ping statistics for FE80::207:ECFF:FEC3:A343:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping FE80::202:4AFF:FEBA:9852

Pinging FE80::202:4AFF:FEBA:9852 with 32 bytes of data:

Reply from FE80::202:4AFF:FEBA:9852: bytes=32 time<lms TTL=128
Reply from FE80::202:4AFF:FEBA:9852: bytes=32 time=lms TTL=128
Reply from FE80::202:4AFF:FEBA:9852: bytes=32 time<lms TTL=128
Reply from FE80::202:4AFF:FEBA:9852: bytes=32 time<lms TTL=128

Ping statistics for FE80::202:4AFF:FEBA:9852:
```

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

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.

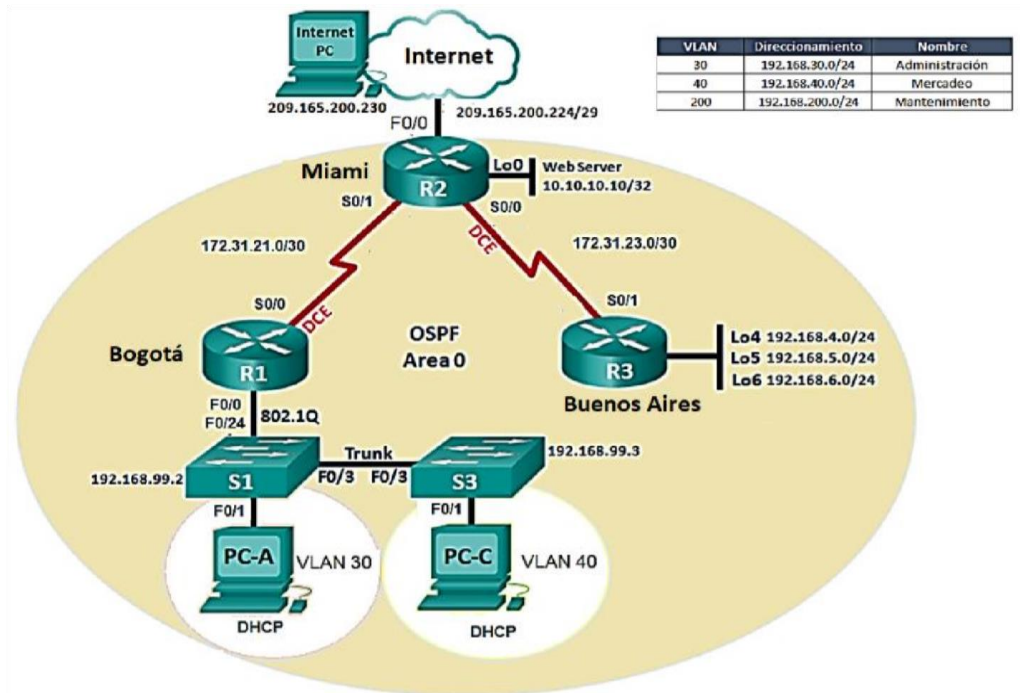


Imagen 26. Escenario 2

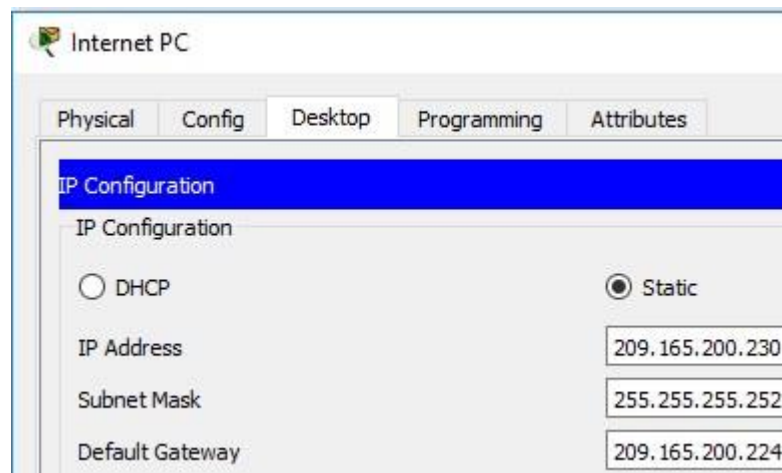
3. ELABORACIÓN DEL ESCENARIO 2

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.

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

Imagen 27: Direccionamiento Internet PC



Se debe de colocar de manera estática, por defecto esa es la opción que viene seleccionada.

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

```
El script: R1 enable configure
terminal host Bogota interface
fast0/0 no shutdown interface
fast/0.30 description
Administracion ip addr
```



```
192.168.30.1 255.255.255.0
interface fast0/0.40 description
Mercadeo
ip addr 192.168.40.1 255.255.255.0
interface fast0/0.99 description
Mantenimiento ip addr 192.168.99.1
255.255.255.0 inter s0/0/0 ip
address 172.31.21.2
255.255.255.252 no shutdown end
write
```

```
R2 enable configure terminal host
Miami inter lo0 description WebServer
ip addr 10.10.10.10 255.255.255.255
interface fast0/0 ip addr
209.165.200.229 255.255.255.248 no
shutdown inter s0/0/0 ip addr
172.31.23.1 255.255.255.252 no
shutdown inter s0/0/1 ip addr
172.31.21.1 255.255.255.252 no
shutdown end write
```

```
R3 enable
configure
terminal host
Buenos_Aires
inter lo4 ip addr
192.168.4.1
255.255.255.0
inter lo5 ip addr
192.168.5.1
255.255.255.0
```

```

inter lo6 ip addr
192.168.6.1
255.255.255.0
inter s0/0/1 ip
address
172.31.23.2
255.255.255.252
no shutdown end
write

```

Los switches se configura la dirección de gestión: **SW1 enable** configure terminal host S1
 vlan 99 inter vlan 99 ip addr 192.168.99.2
 255.255.255.0 end write

SW3 enable configure terminal
 host S3 vlan 99 inter vlan 99 ip
 addr 192.168.99.3
 255.255.255.0 end write

3.2. Configuración OSPFv2

Configurar el protocolo de enrutamiento OSPFv2 bajo los criterios de la tabla 3.

Tabla : 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

Comenzamos con el protocolo con un número de identificación, en este caso el 1, luego le damos el id de acuerdo con la tabla, nombramos las interfaces que no participan de OSPF como interfaces pasivas, a continuación se indica el CLI para implementar en cada router:

```
R1 enable configure terminal router ospf 1 router-id 1.1.1.1 passive-interface
FastEthernet0/0 network 172.31.21.0 0.0.0.3 area 0 network 192.168.30.0 0.0.0.255
area 0 network 192.168.40.0 0.0.0.255 area 0 network 192.168.200.0 0.0.0.255 area
0 interface Serial0/0/0 bandwidth 256 ip ospf cost 9500
end
write
```

```
R2 enable configure terminal router
ospf 1 router-id 5.5.5.5 passive-
interface FastEthernet0/0 passive-
interface Loopback0 network
209.165.200.224 0.0.0.7 area 0
network 172.31.21.0 0.0.0.3 area 0
network 172.31.23.0 0.0.0.3 area 0
network 10.10.10.10 0.0.0.0 area 0
interface Serial0/0/0 bandwidth 256
ip ospf cost 9500 interface
Serial0/0/1 bandwidth 256 end write
```

```
R3 enable configure terminal
router ospf 1 router-id 8.8.8.8
passive-interface Loopback4
passive-interface Loopback5
passive-interface Loopback6
network 172.31.23.0 0.0.0.3
area 0 network 192.168.4.0
```

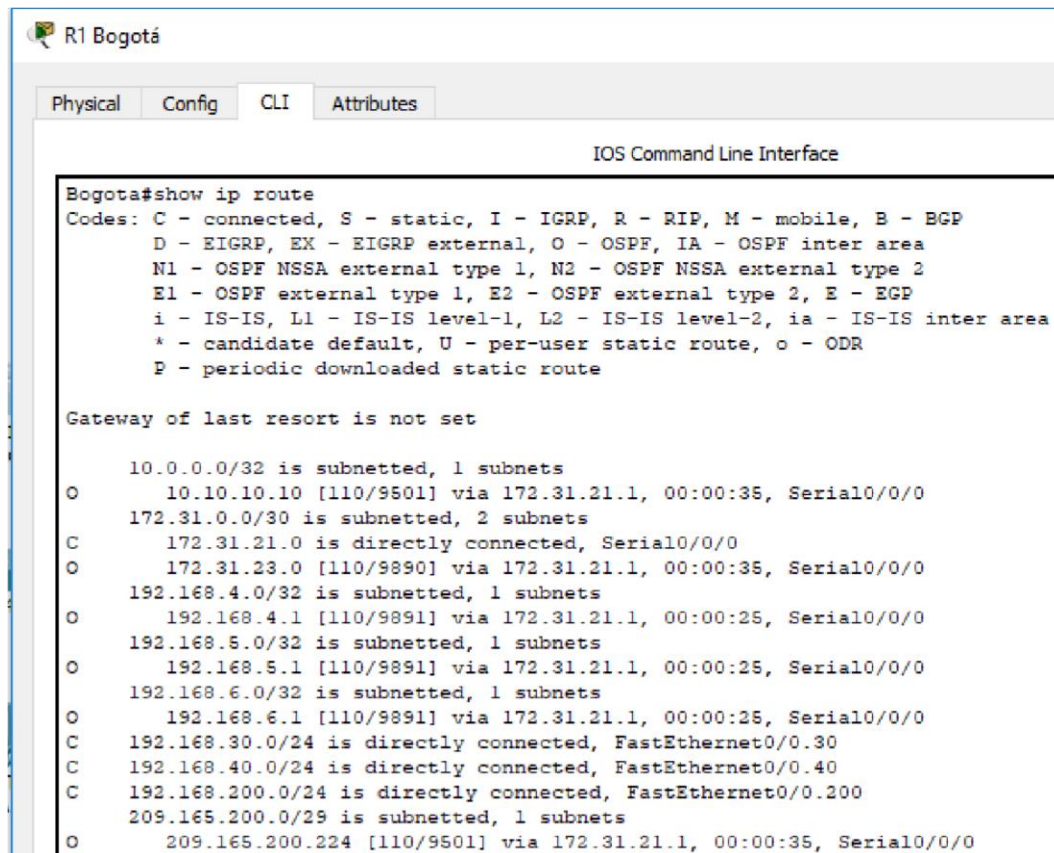
0.0.0.255 area 0 network
192.168.5.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255
area 0 interface Serial0/0/1
bandwidth 256 end write

3.3. Verificación información OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Se puede verificar las tablas de enrutamiento de cada router, para confirmar que los equipos involucrados estén compartiendo las tablas:

Imagen 28: Verificación routing table R1



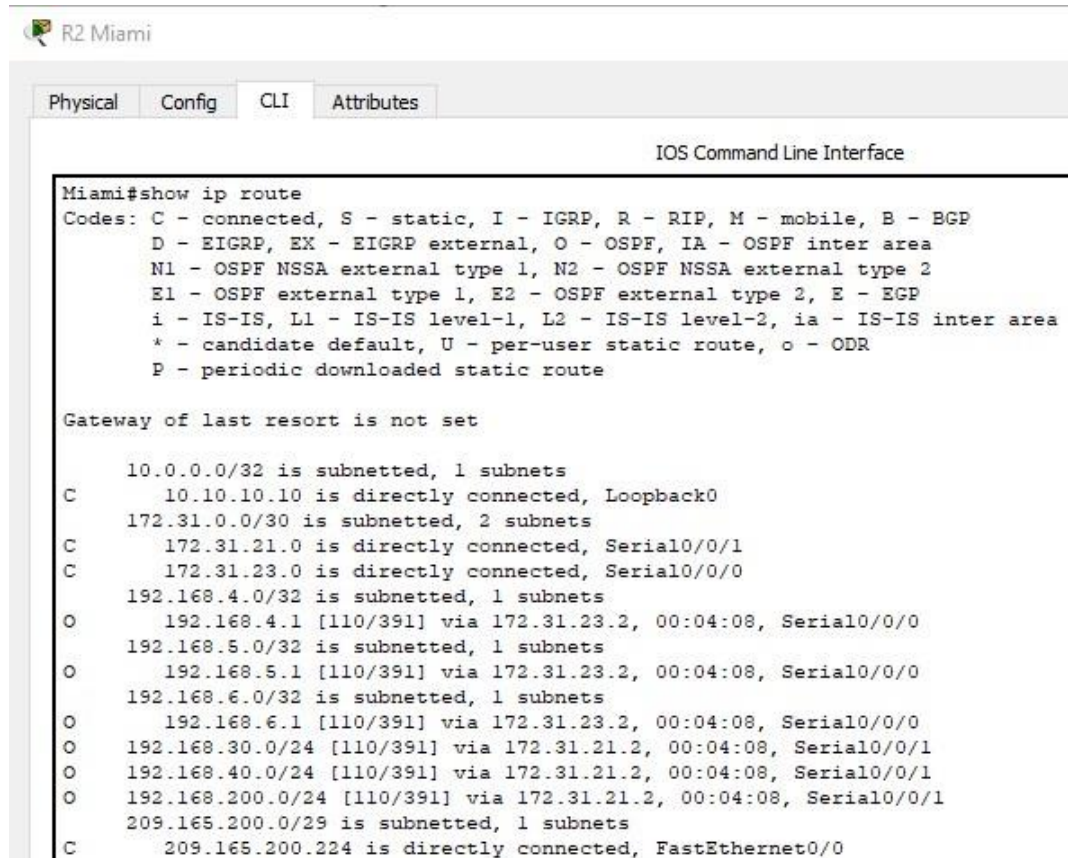
```
R1 Bogotá
Physical Config CLI Attributes
IOS Command Line Interface
Bogota#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

 10.0.0.0/32 is subnetted, 1 subnets
O   10.10.10.10 [110/9501] via 172.31.21.1, 00:00:35, Serial0/0/0
 172.31.0.0/30 is subnetted, 2 subnets
C   172.31.21.0 is directly connected, Serial0/0/0
O   172.31.23.0 [110/9890] via 172.31.21.1, 00:00:35, Serial0/0/0
 192.168.4.0/32 is subnetted, 1 subnets
O   192.168.4.1 [110/9891] via 172.31.21.1, 00:00:25, Serial0/0/0
 192.168.5.0/32 is subnetted, 1 subnets
O   192.168.5.1 [110/9891] via 172.31.21.1, 00:00:25, Serial0/0/0
 192.168.6.0/32 is subnetted, 1 subnets
O   192.168.6.1 [110/9891] via 172.31.21.1, 00:00:25, Serial0/0/0
C   192.168.30.0/24 is directly connected, FastEthernet0/0.30
C   192.168.40.0/24 is directly connected, FastEthernet0/0.40
C   192.168.200.0/24 is directly connected, FastEthernet0/0.200
 209.165.200.0/29 is subnetted, 1 subnets
O   209.165.200.224 [110/9501] via 172.31.21.1, 00:00:35, Serial0/0/0
```

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

Imagen 29: Verificación routing table R2



```
R2 Miami
Physical Config CLI Attributes
IOS Command Line Interface
Miami#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

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

Acá vemos que el router encontró 6 redes a través de OSPF y tiene 4 conectadas directamente.

Imagen 30: Verificación routing table R3

```
R3 Buenos Aires
Physical Config CLI Attributes
IOS Command Line Interface

% Invalid input detected at '^' marker.

Buenos_Aires#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

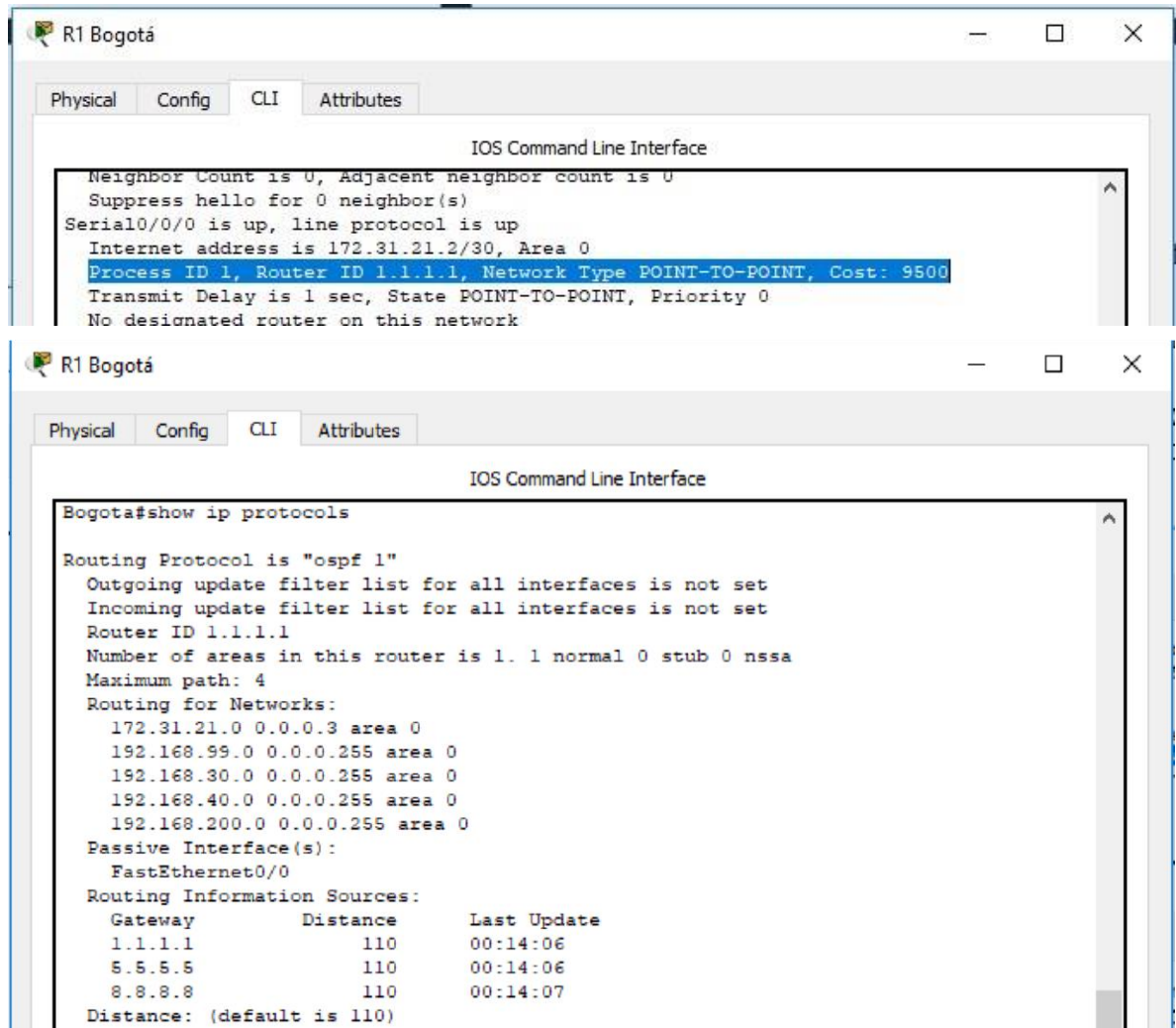
      10.0.0.0/32 is subnetted, 1 subnets
O       10.10.10.10 [110/391] via 172.31.23.1, 00:08:43, Serial0/0/1
      172.31.0.0/30 is subnetted, 2 subnets
O       172.31.21.0 [110/780] via 172.31.23.1, 00:08:43, Serial0/0/1
C       172.31.23.0 is directly connected, Serial0/0/1
C       192.168.4.0/24 is directly connected, Loopback4
C       192.168.5.0/24 is directly connected, Loopback5
C       192.168.6.0/24 is directly connected, Loopback6
O       192.168.30.0/24 [110/781] via 172.31.23.1, 00:08:43, Serial0/0/1
O       192.168.40.0/24 [110/781] via 172.31.23.1, 00:08:43, Serial0/0/1
O       192.168.200.0/24 [110/781] via 172.31.23.1, 00:08:43, Serial0/0/1
      209.165.200.0/29 is subnetted, 1 subnets
O       209.165.200.224 [110/391] via 172.31.23.1, 00:08:43, Serial0/0/1
```

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

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

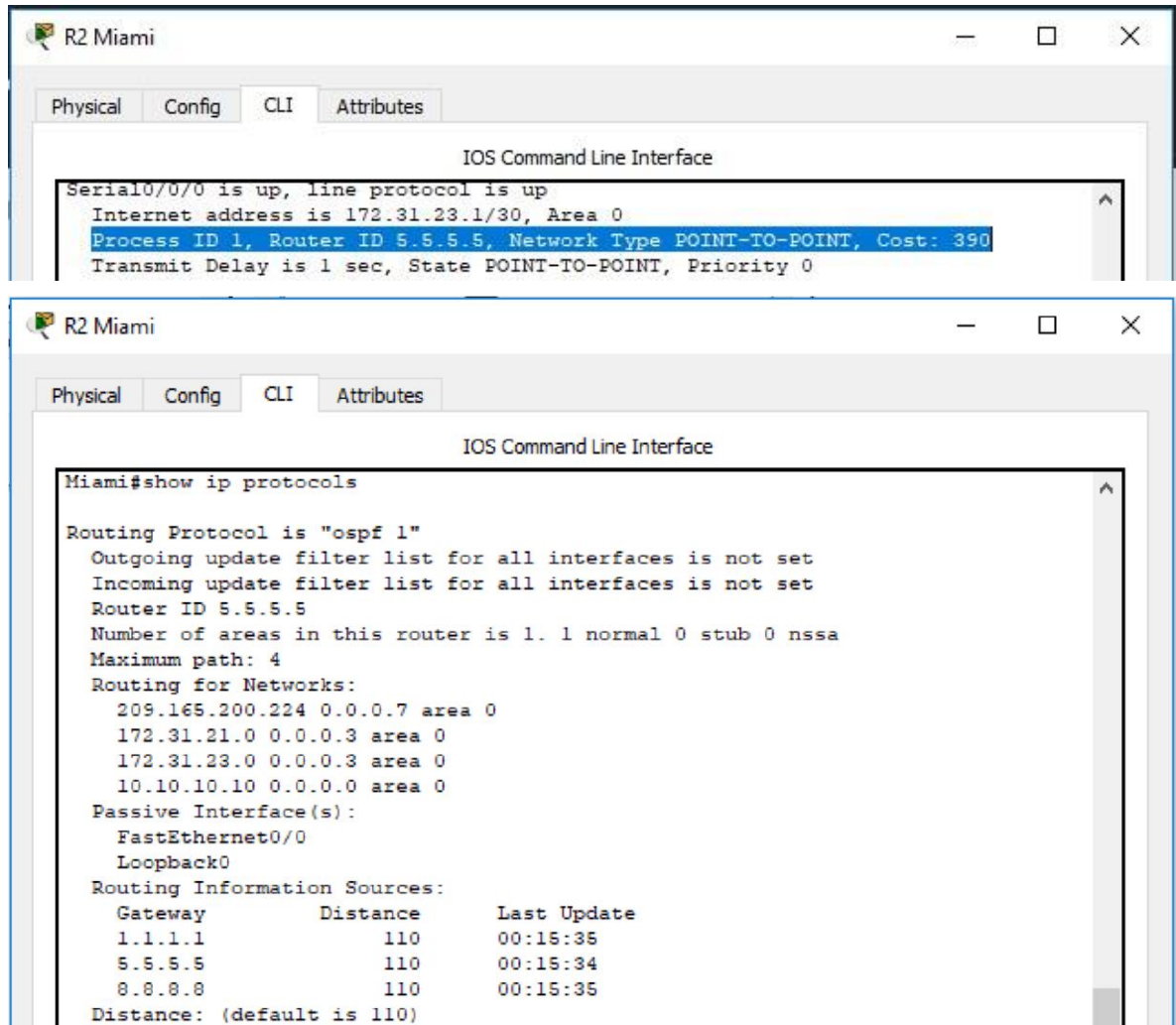
Para poder visualizar lo solicitado, aplicamos los comandos **show ip ospf interface** y **show ip protocols**, a continuación, los pantallazos de demostración de la información solicitada al router:

Imagen 31. Verificación R1



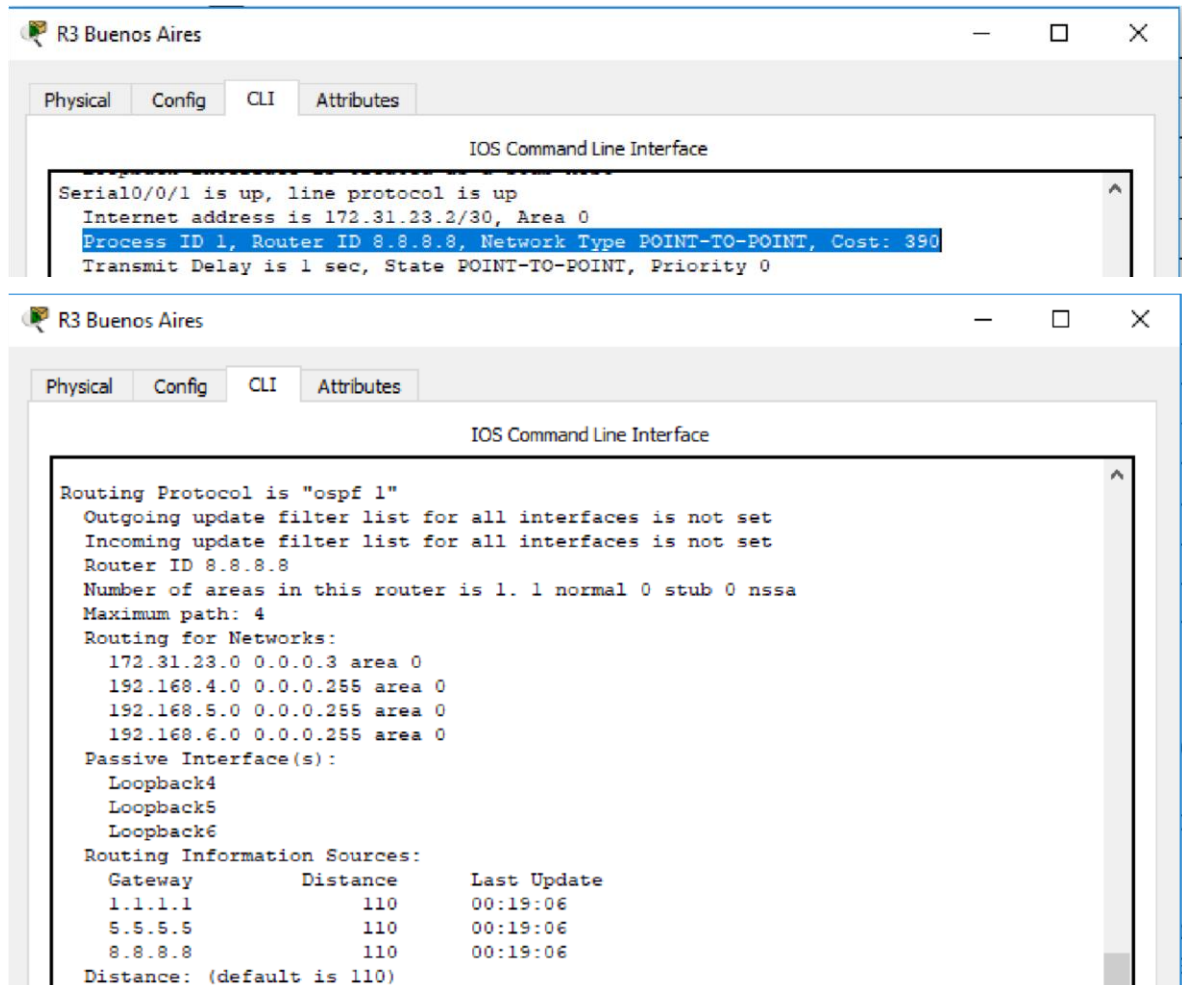
Esta imagen visualizamos el costo, el ID del router, el ID del proceso, las interfaces pasivas y las redes enrutadas.

Imagen 32. Verificación en R2



Se realiza lo mismo en el router y se comprueba que todo lo pedido en la guía.

Imagen 33. Verificación en R3



Terminado completamos la tarea con el R3

3.4. Configuración switches

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

Aca se debe nombrar las vlan, no es obligatorio el InterVLAN en el switch, ya que en el router se lleva a cabo ese proceso, después en las interfaces troncales, se asigna los puertos a las vlan indicadas y las que queden libres se apaga, y ya concluyendo, se configura la seguridad del switch.

SW1 enable configure

terminal vlan 30 vlan

40 interface fast0/3

switchport mode trunk

interface fast0/24

switchport mode trunk

interface

FastEthernet0/1

switchport access vlan

30 switchport mode

access exit enable

secret villamil enable

password villamil line

console 0 password

villamil login line vty 0 4

password villamil login

banner motd x Prohibido el Acceso no

Autorizado! x service password-encryption end

write

```
SW3 enable configure terminal vlan 40 interface
fast0/3 switchport mode trunk interface
FastEthernet0/1 switchport access vlan 40
switchport mode access exit enable secret
villamil enable password villamil line console 0
password villamil login line vty 0 4 password
villamil login banner motd x Prohibido el Acceso
no Autorizado! x service password-encryption
end write
```

3.5. Deshabilitar DNS lookup

En el Switch 3 deshabilitar DNS lookup

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.

El script:

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

3.6. Asignación de direcciones IP a los switches

Asignar direcciones IP a los Switches acorde a los lineamientos.

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

```
SW1: enable
configure terminal
vlan 99
inter vlan 99
ip addr 192.168.99.2 255.255.255.0
end
write
```

```
SW3: enable
configure terminal
vlan 200
inter vlan 200
ip addr 192.168.200.3 255.255.255.0
end
write
```

3.7. Desactivación Puertos

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

Por seguridad, este lineamiento debe ser configurado, así evitamos fallas provocadas por personas no entrenadas en la ingeniería de redes, a continuación, el script:

SW1: enable
configure terminal
inter range f0/2 , f0/4-
23 shutdown end write

SW3: enable
configure terminal
inter range f0/2 , f0/4-
24 shutdown end write

3.8. Implementación DHCP y NAT para IPv4

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

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

Configuración DHCP IPv4 enable configure
terminal ip dhcp excluded-address 192.168.30.2
192.168.30.32 ip dhcp excluded-address
192.168.40.2 192.168.40.32 ip dhcp pool
ADMINISTRACION network 192.168.30.0
255.255.255.0 default-router 192.168.30.1 dns-
server 10.10.10.11 ip dhcp pool MERCADEO
network 192.168.40.0 255.255.255.0 default-
router 192.168.40.1 dns-server 10.10.10.11 ip
domain-name ccna-unad.com end write

3.9. Configuración NAT

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

Se debe realizar PAT o, NAT con sobrecarga, ya que esta es la manera que tienen los terminales para alcanzar la red internet, para ello implementamos los parámetros de siempre, una lista de acceso que indique que redes o hosts pueden salir a internet, luego la aplicamos en el comando de NAT con sobrecarga. A continuación, el script:

```
enable
configure
terminal
```

```
ip access-list standard INTERNET
permit 192.168.0.0 0.0.255.255
permit 172.31.0.0 0.0.255.255

ip nat inside source list INTERNET interface FastEthernet0/0
overload interface fast0/0 ip nat outside inter s0/0/0 ip nat inside
inter s0/0/1
ip nat
inside end
write
```

3.10. Listas de Acceso

- Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.
- Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

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

```
enable configure terminal ip access-list standard lista_uno permit 192.168.30.0
0.0.0.255 deny 192.168.40.0 0.0.0.255 ip access-list standard lista_dos deny
192.168.30.0 0.0.0.255 permit 192.168.40.0 0.0.0.255 ip access-list extended
lista_tres permit ip 192.168.30.0 0.0.0.255 host 209.165.200.230 deny ip
192.168.40.0 0.0.0.255 host 209.165.200.230 ip access-list extended lista_cuatro
```

```
permit ip 192.168.40.0 0.0.0.255 host
209.165.200.230 deny ip 192.168.30.0 0.0.0.255
host 209.165.200.230 end write
```

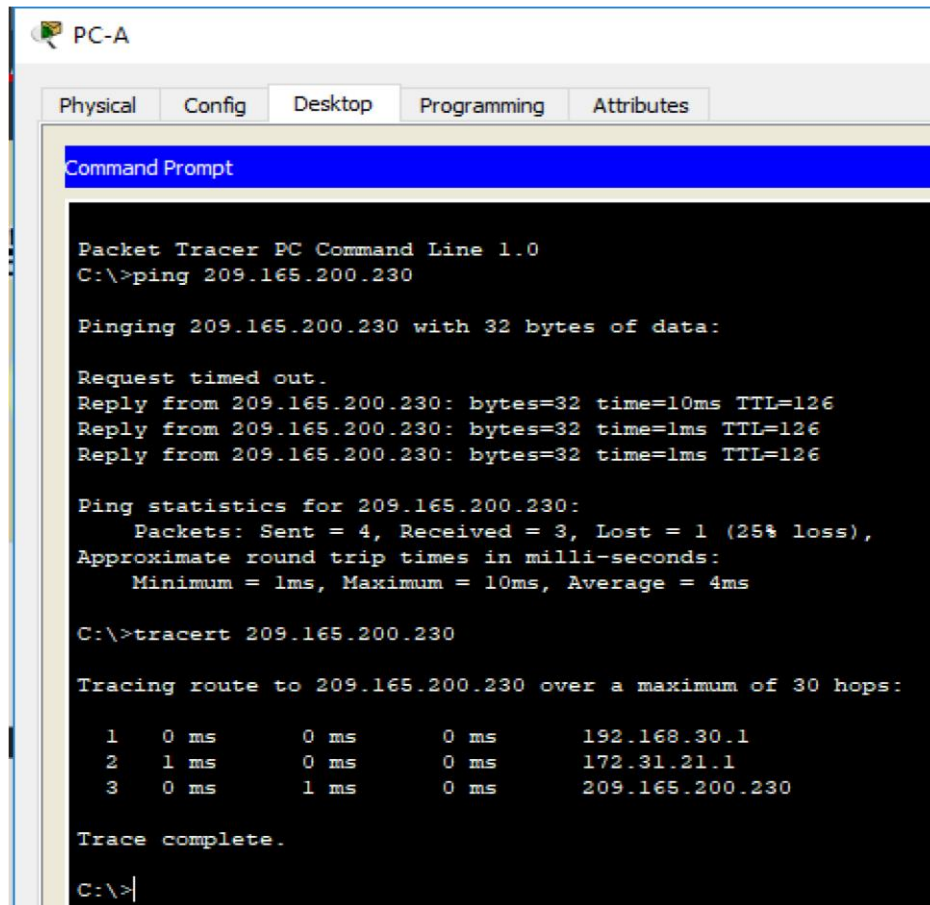
3.11. Verificación comunicación

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

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

PC-A:

Imagen 34: PC-A pruebas de conectividad



The image shows a Packet Tracer PC Command Line window for PC-A. The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active, showing a Command Prompt window. The Command Prompt displays the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Request timed out.
Reply from 209.165.200.230: bytes=32 time=10ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126
Reply from 209.165.200.230: bytes=32 time=1ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 10ms, Average = 4ms

C:\>tracert 209.165.200.230

Tracing route to 209.165.200.230 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    192.168.30.1
  1  1 ms    0 ms    0 ms    172.31.21.1
  2  0 ms    1 ms    0 ms    209.165.200.230

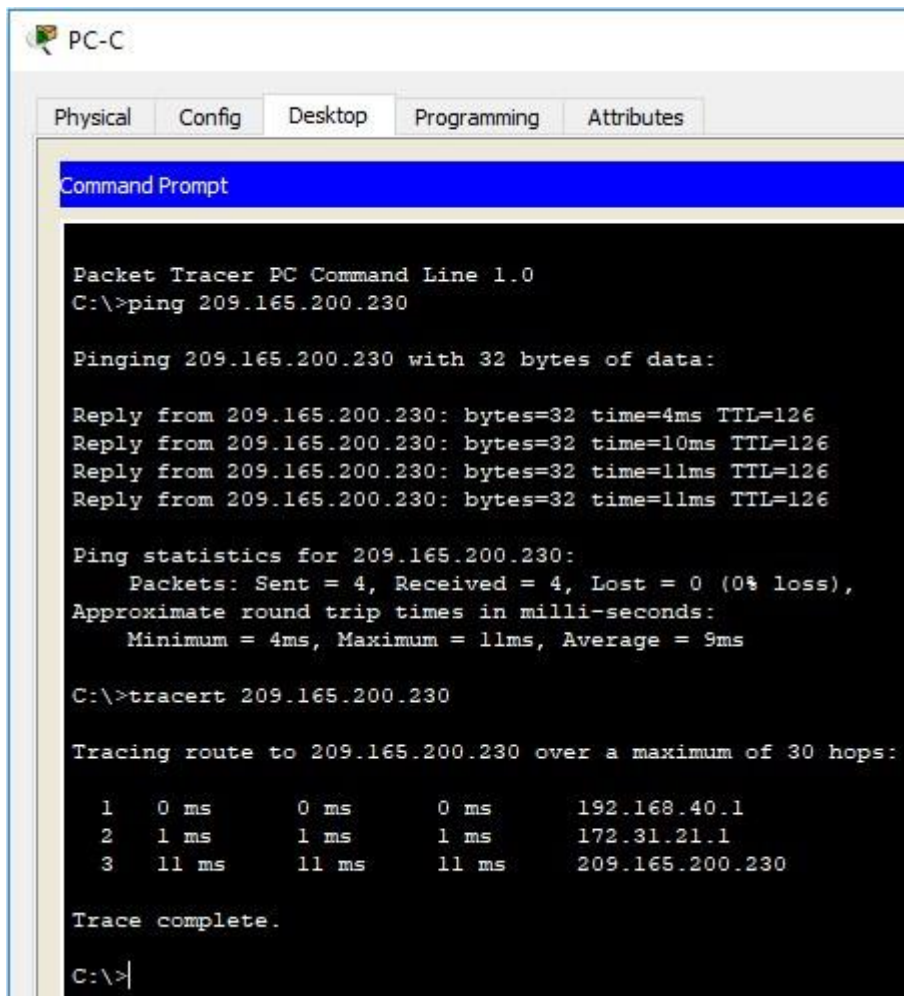
Trace complete.

C:\>
```

Se evidencia en esta imagen el ping fue exitoso, y mediante tracert, corroboramos cuantos saltos fueron necesarios para que el paquete alcanzara el destino.

PC-B:

Imagen 35: PC-C pruebas de conectividad



```
PC-C
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 209.165.200.230

Pinging 209.165.200.230 with 32 bytes of data:

Reply from 209.165.200.230: bytes=32 time=4ms TTL=126
Reply from 209.165.200.230: bytes=32 time=10ms TTL=126
Reply from 209.165.200.230: bytes=32 time=11ms TTL=126
Reply from 209.165.200.230: bytes=32 time=11ms TTL=126

Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 11ms, Average = 9ms

C:\>tracert 209.165.200.230

Tracing route to 209.165.200.230 over a maximum of 30 hops:

  0  0 ms    0 ms    0 ms    192.168.40.1
  1  1 ms    1 ms    1 ms    172.31.21.1
  2  11 ms   11 ms   11 ms   209.165.200.230

Trace complete.

C:\>
```

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

4. CONCLUSIONES

- Se realizó la configuración correspondiente para el escenario 1 y cada uno de sus dispositivos, donde se logra diseñar una topología estable ya que se hizo uso de la tabla de direccionamiento entregada en la respectiva guía.
- Internamente en el escenario 1 se realiza la configuración de la topología de manera exitosa basados en las VLAN y puertos asociados en la tabla.
- En el escenario 1 se logra implementar el enmascaramiento mejor conocido como NAT de los dispositivos correspondientes.
- Dentro del escenario 1 se realiza las diferentes configuraciones de routing y Vlan, las cuales incluyen direccionamiento IP entre troncales y subinterfaces.
- Entre los 2 escenarios se comprende de una manera más clara cual es la funcionalidad concreta del protocolo DHCP, donde se evidencia que su prioridad operativa es el ahorro de tiempo de la gestión correspondiente entre las IP de la topología diseñada.
- Dentro del escenario 2 se realiza la habilitación del protocolo DHCP sobre un servidor que cuenta con una administración centralizada de cada una de las diferentes direcciones IP que se encuentran dentro de la topología establecido.

5 BIBLIOGRAFÍA O REFERENCIAS

- DHCP. Principios de Enrutamiento y Conmutación. (2014) Recuperado de: <https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>
Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing IPv4 in the Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101
- CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>
- CISCO Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-courseassets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>
- CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-courseassets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1>
- Odom, W. (2013). CISCO Press (Ed). CCNA ICND1 Official Exam Certification Guide. Recuperado de <http://ptgmedia.pearsoncmg.com/images/9781587205804/samplepages/9781587205804.Pdf>