PRUEBA HABILIDADES PRACTICAS CCNA

DIPLOMADO DE PROFUNDIZACIÓN CISCO

ANDRES FELIPE MORENO ECHAVARRIA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

PROGRAMA INGENIERIA DE SISTEMAS

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

BOGOTA

2019

PRUEBA HABILIDADES PRACTICAS CCNA

DIPLOMADO DE PROFUNDIZACIÓN CISCO

ANDRES FELIPE MORENO ECHAVARRIA

Trabajo de Diplomado para optar obtener el título de ingeniero de sistemas

Ingeniero Efraín Alejandro Perez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

PROGRAMA INGENIERIA DE SISTEMAS

ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGENIERIA

BOGOTA

2019

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, 06 de febrero 2019

DEDICATORIA

En primera instancia doy gracias a Dios por darme la fortaleza, decisión, constancia y disciplina que me permitió tener para lograr llegar al final del proceso educativo y el permitirme desarrollar este diplomado para lograr obtener mi titulo como ingeniero de sistemas.

Quiero dedicar este gran logro a mi madre Gladys echavarria, mi padre Eduardo Moreno, mi hermana Francy Echavarria y hermano Alex Moreno, ya que con su apoyo y amor lograron apoyarme durante mi proceso educativo y darme la motivación para avanzar en cada fase.

De igual forma quiero agradecer a todos los tutores de la universidad por brindarme el conocimiento, experiencia y corregirme durante toda mi formación para un hacerme un mejor profesional.

AGRADECIMIENTOS

Quiero agradecer al director del diplomado Juan Carlos Vesga y también a mi tutor Efraín Alejandro Perez ya que gracias a sus orientaciones, conocimientos y asesoría constante fue posible aprobar el diplomado y obtener el conocimiento que tengo hoy día.

CONTENIDO

Pag

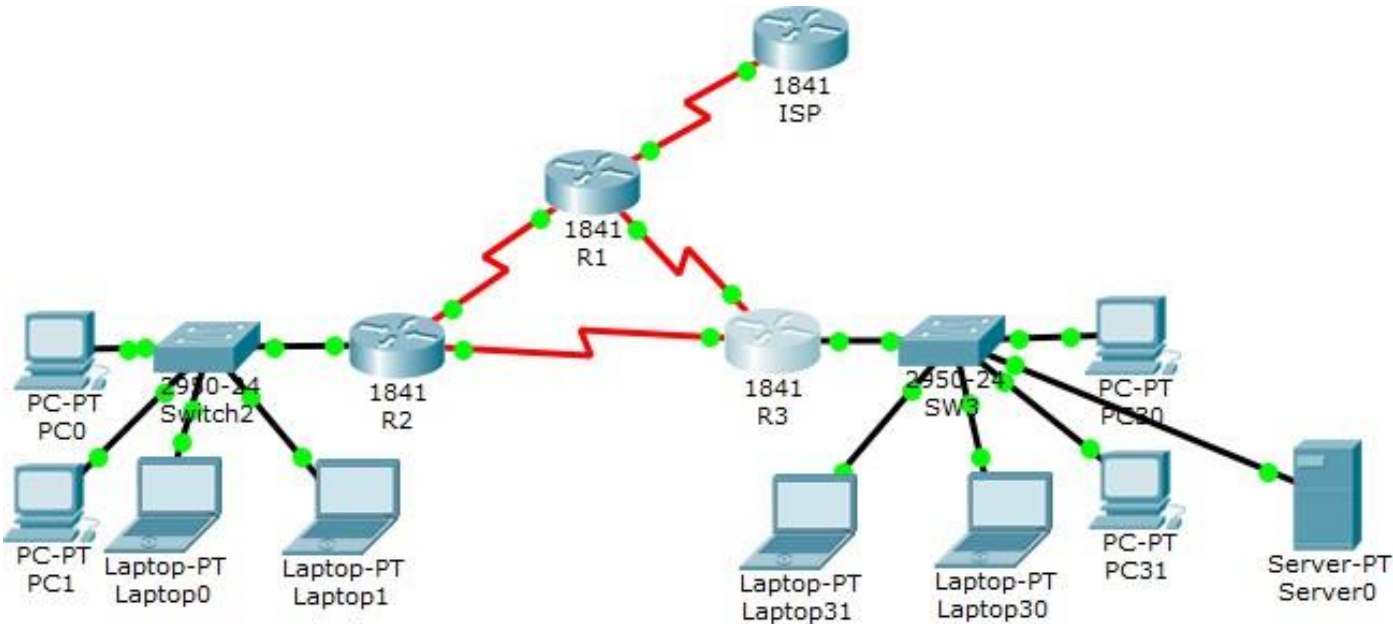
Lista de Figuras

Pág.

INTRODUCCIÓN

Durante el desarrollo del diplomado de cisco se adquirieron conocimientos en la estructura y los equipos que pueden conformar una red, para lo cual se establecieron una serie de prácticas para fortalecer los conceptos explicados en cada uno de los módulos, es por esto que se propone una serie de prácticas en las cuales se pretende verificar los conocimientos adquiridos y para lo cual se propone realizar una topología en base a routers, switches, servidores web y equipos cliente interconectados, llevando a cabo la administración de los equipos se propone realizar su configuración estableciendo NAT, DHCP, RIPv2 y VLAN. Esto con el objetivo de mejorar el nivel de seguridad que se tiene en la red tanto para el acceso de los dispositivos, así como también en la comunicación de estos, de esta manera de limita que dispositivos y redes se pueden ver entre sí lo que en un entorno real promueve un nivel de seguridad robusto, evitando posibles infiltraciones de usuarios no autorizados, robo de información o datos por tener un nivel de seguridad bajo.

1. ESCENARIO 1



1.1. 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

1.2 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

1.3 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.

1.4 Desarrollo Escenario 1

- **SW1 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.**

Rta: Se comenzará con la configuración del switch 2 en el cual se crearán las vlan según la tabla para lo cual utilizamos el siguiente comando.

```
S2>enable
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#vlan 100
S2(config-vlan)#name LAPTOPS
S2(config-vlan)#vlan 200
S2(config-vlan)#name DESKTOPS
S2(config-vlan)#exit
S2(config)#interface fa0/2
S2(config-if)#switchport access vlan 100
S2(config-if)#interface fa0/3
S2(config-if)#switchport access vlan 100
S2(config-if)#interface fa0/4
S2(config-if)#switchport access vlan 200
S2(config-if)#interface fa0/5
S2(config-if)#switchport access vlan 200
```

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

Rta: Se lleva a cabo la desactivación de los puertos que no se utilizaran en la topología, por medio del comando shutdown.

```
S2>enable
S2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S2(config)#interface range fa0/4-24
S2(config-if-range)#shutdown
```

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

Rta: Según la tabla los router se deben parametrizar con unas interfaces en cada uno de sus puertos seriales y fast ethernet a continuación se realiza la configuración de cada uno respectivamente.

ROUTER 1

```
R1>enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface s0/0/0
R1(config-if)#ip address 200.123.211.2 255.255.255.0
R1(config-if)#interface s0/1/0
R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#interface s0/1/1
R1(config-if)#ip address 10.0.0.5 255.255.255.252
```

ROUTER 2

```
R2>enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface fa0/0.100
R2(config-subif)#ip address 192.168.20.1 255.255.255.0
R2(config-subif)#interface fa0/0.200
R2(config-subif)#ip address 192.168.21.1 255.255.255.0
R2(config-subif)#exit
R2(config)#interface se0/0/0
R2(config-if)#ip address 10.0.0.2 255.255.255.252
R2(config-if)#interface se0/0/1
R2(config-if)#ip address 10.0.0.9 255.255.255.252
R2(config-if)#
```

ROUTER 3

```
R3>enable
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface fa0/0
R3(config-if)#ip address 192.168.30.1 255.255.255.0
R3(config-if)#ipv6 address 2001:db8:130::9C0:80F:301/64
R3(config-if)#interface se0/0/0
R3(config-if)#ip address 10.0.0.6 255.255.255.252
```

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

Rta: Se llevo a cabo la configuración de los PC y Laptops con configuración DHCP sobre las interfaces de cada uno de estos.

- **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.**

Rta: se establece una NAT con sobrecarga sobre el puerto serial conectado al ISP.

```
R1(config)#access-list 1 permit 10.0.0.1 0.0.0.252
R1(config)#ip nat pool public_access 200.123.211.1 200.123.211.2 netmask
255.255.255.0
R1(config)#ip nat inside source list 1 pool public_access overload
R1(config)#interface s0/1/0
R1(config-if)#ip nat inside
R1(config-if)#interface s0/0/0
R1(config-if)#ip nat outside
```

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

```
R1(config)#ip route 0.0.0.0 0.0.0.0 200.123.211.1
```

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

```
R2(config)#ip dhcp pool R1G1
```

R2(dhcp-config)#network 192.168.20.0 255.255.255.0
R2(dhcp-config)#default-router 192.168.20.1

- **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).**

Rta: Se realiza ping desde un pc conectado al R3 y permite realizar ping. Tambien se verifica un ping desde un equipo del R2 y no da respuesta.

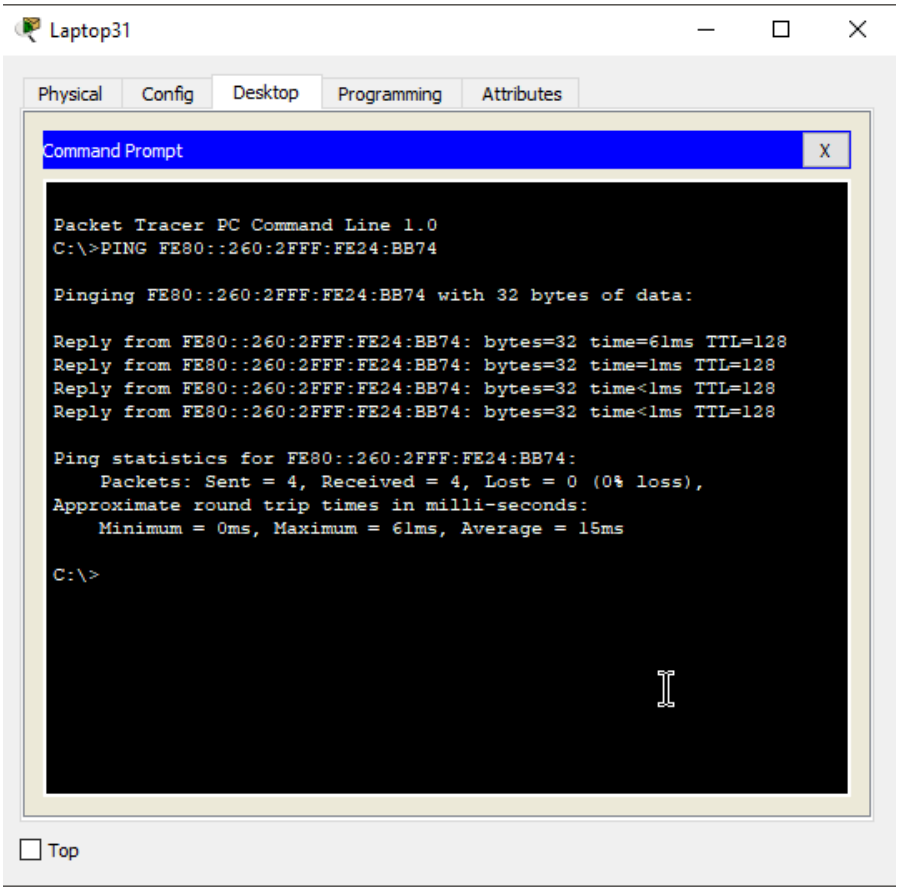


Figura 1 – Ping desde equipo conectado al R3

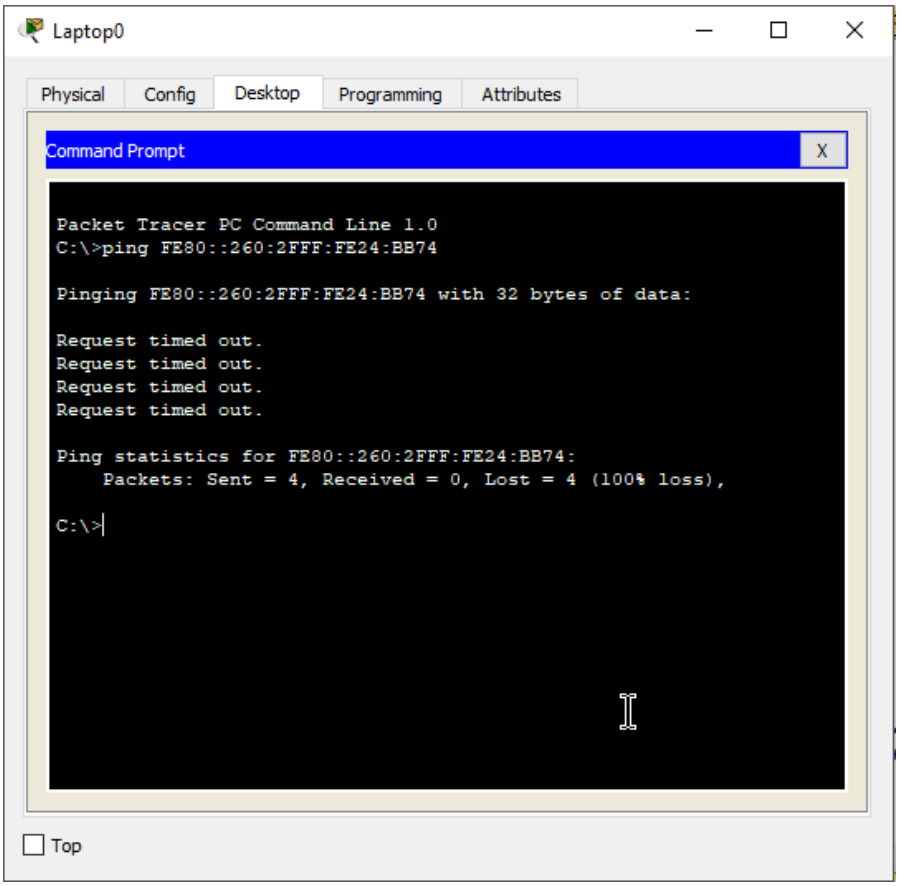


Figura 2- ping desde equipo conectado al router R2

- **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.**

Rta: Se establecieron las interfaces como DHCP para IPV4 e IPV6

- **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.**

Rta: Se lleva a cabo la configuración de RIP Versión 2 en cada uno de los routers

Router 1

R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network

R1(config-router)#network 200.123.211.2
R1(config-router)#network 10.0.0.1
R1(config-router)#network 10.0.0.5

Router 2

R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 192.168.20.1
R2(config-router)#network 192.168.21.1
R2(config-router)#network 10.0.0.2
R2(config-router)#network 10.0.0.9

Router 3

R3(config)#router rip
R3(config-router)#version
% Incomplete command.
R3(config-router)#version 2
R3(config-router)#network 192.168.30.1
R3(config-router)#network 10.0.0.6
R3(config-router)#network 10.0.0.10

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

Rta: Se configura como ruta predeterminada la dirección del R1 en los router 2 y 3

R2(config)#ip route 0.0.0.0 0.0.0.0 200.123.211.2

R3(config)#ip route 0.0.0.0 0.0.0.0 200.123.211.2

- **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.**

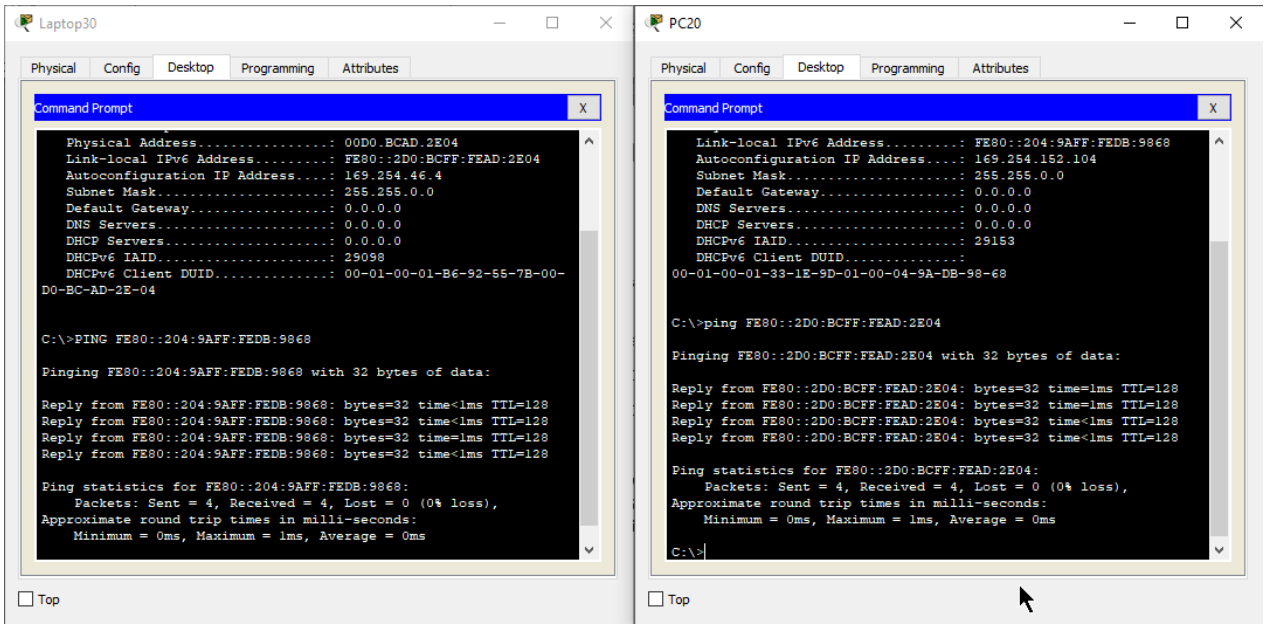


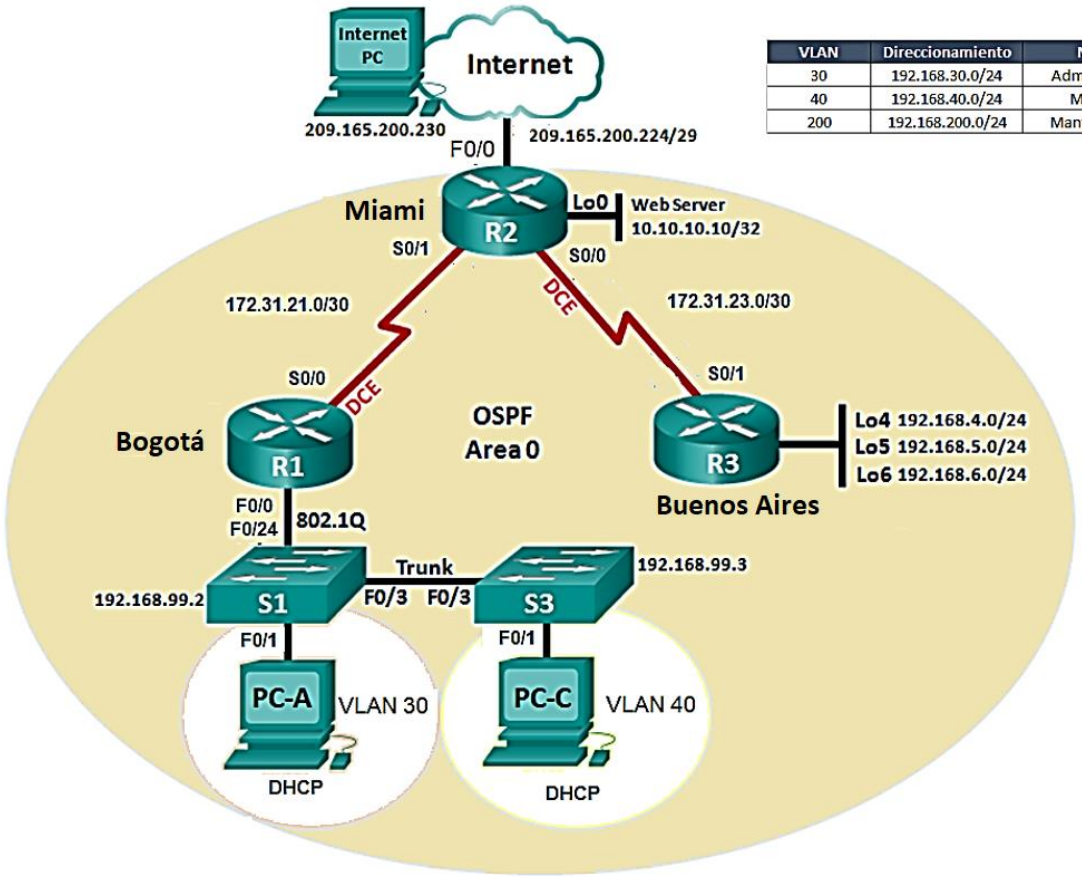
Figura 3 – Verificación de conectividad entre equipos conectados al router R3

Link de descarga escenario 1

https://drive.google.com/open?id=1mUbZ2rVH7JaPlVXMgTuITJoMWNV5Xr7Z

2. Escenario 2

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



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

2.1 Desarrollo Escenario 2

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

Rta: Se monta la topología según el esquema planteado para esto se utiliza

- ✓ 3 routers 1841
- ✓ 2 Switch 2950-24
- ✓ 3 PC genéricos
- ✓ Cables seriales, cobre directo, cobre cruzado para realizar la conexión entre dispositivos
- ✓ 1 servidor web

Se comienza parametrizando la IP Fija de la internet PC según lo mostrado en la gráfica se debe establecer los parámetros:

Dirección IP: 209.165.200.230
Mask: 255.255.255.248
Puerta Enlace: 209.165.200.225

Para los otros 2 PC se establece DHCP para que tomen direccionamiento automático.

Se comienza la configuración de los routers estableciendo los parámetros de seguridad básicos y su configuración de red.

Configuración seguridad inicial Router 1

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#pass cisco
R1(config-line)#login
```

```
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd "Prohibido el acceso no autorizado, sera sancionado según lo dispuesto por la ley"
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
```

Configuración seguridad inicial Router 2

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd "Prohibido el acceso no autorizado, sera sancionado según lo dispuesto por la ley"
R2(config)#int 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)#description connection to Buenos Aires
R2(config-if)#no shutdown
R2(config-if)#interface s0/0/1
R2(config-if)#ip address 172.31.21.2 255.255.255.252
R2(config-if)#description connection to Bogota
R2(config-if)#no shutdown
R2(config-if)#interface f0/0
R2(config-if)#ip address 209.165.200.225 255.255.255.248
R2(config-if)#no shutdown
R2(config-if)#interface f0/1
R2(config-if)#ip addresss 10.10.10.10 255.255.255.0
R2(config-if)#ip address 10.10.10.10 255.255.255.0
R2(config-if)#no shutdown
```

Configuración seguridad inicial Router 3

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd "Prohibido el acceso no autorizado, sera sancionado
según lo dispuesto por la ley"
R3(config)#interface s0/0/1
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#description connection to Buenos Aires
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#interface s0/0/1
R3(config-if)#int lo4
R3(config-if)#
R3(config-if)#ip add 192.168.4.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#int lo5
R3(config-if)#
R3(config-if)#ip add 192.168.5.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#int lo6
R3(config-if)#ip add 192.168.6.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#
```

Configuración inicial WEB SERVER

IP Address: 10.10.10.10
Subnet Mask: 255.255.255.0
Default Gateway: 10.10.10.1

Configuración inicial seguridad SWITCH 1

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#pass cisco
S1(config-line)#line vty 0 4
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd "Prohibido el acceso no autorizado, sera sancionado
según lo dispuesto por ley"
S1(config)#exit
S1#cop r s
Destination filename [startup-config]? y
S1#cop r s
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración inicial seguridad SWITCH 3

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#pass cisco
S3(config-line)#line vty 0 4
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd "Prohibido el ingreso a personal no autorizado, sera
sancionado según lo dispuesto por la ley"
S3(config)#exit
S3#cop r s
```

Destination filename [startup-config]?
Building configuration...
[OK]
S3#

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

Se establece la configuración del Router 1

Se ingresa a la configuración de la interfaz f0/0.30, se realiza el encapsulamiento y se establece la dirección IP. Esto también se realiza con la interfaz f0/0.40 y f0/0.200.

R1(config)#int f0/0.30
R1(config-subif)#description accouting LAN
R1(config-subif)#encapsulation dotlq 30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#int f0/0.40
R1(config-subif)#description accouting LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
R1(config-subif)#int f0/0.200
R1(config-subif)#description accouting LAN
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
R1(config-subif)#int f0/0
R1(config-if)#no shutdown

Se empieza a establecer la configuración del OSPF 1 con el id 1.1.1.1 para el router R1 y su respectiva dirección IP, se establece el ancho de banda a 128 y el costo de ospf a 7500.

```
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 172.31.21.0 0.0.0.3 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)#network 192.168.200.0 0.0.0.255 area 0
R1(config-router)#passive-interface f0/0.30
R1(config-router)#passive-interface f0/0.40
R1(config-router)#passive-interface f0/0.200
R1(config-router)#exit
R1(config)#int s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#ip ospf cost 7500
```

OSFP ROUTER 2

```
R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
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 10.10.10.0 0.0.0.255 area 0
R2(config-router)#passive-interface f0/1
R2(config-router)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#ip ospf cost 7500
```

OSFP ROUTER 3

```
R3>enable
Password:
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
```

```
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#exit
R3(config)#interface s0/0/1
R3(config-if)#bandwidth 128
R3(config-if)#ip ospf cost 7500
```

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

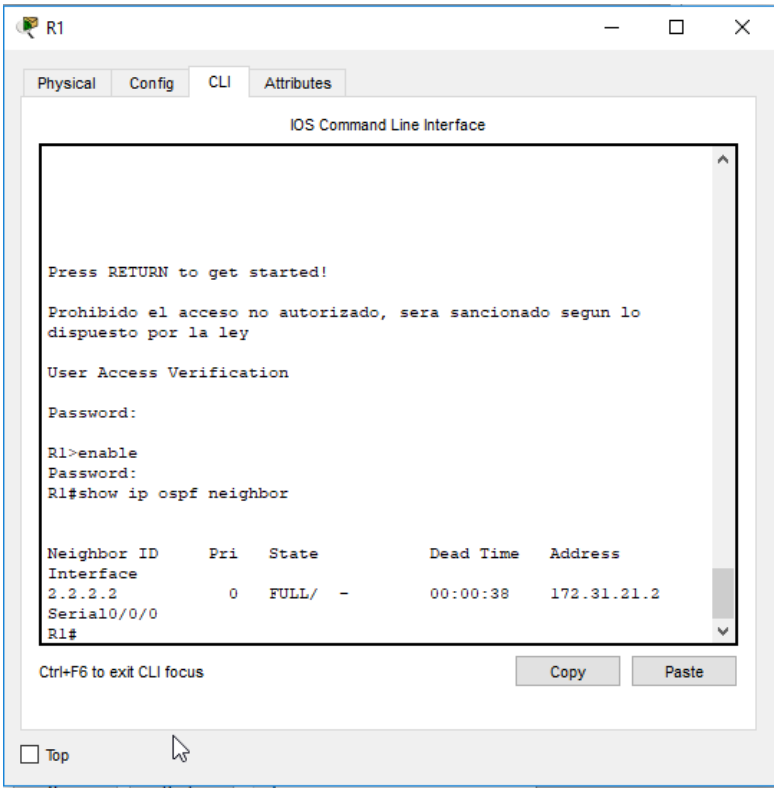


Figura 4 - Listado OSFP Router 1

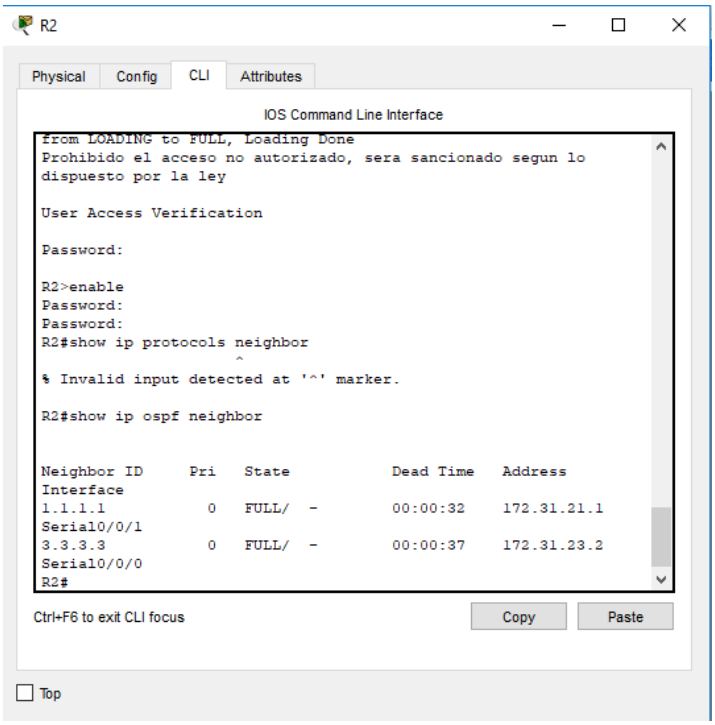


Figura 5 - Listado OSFP Router 2

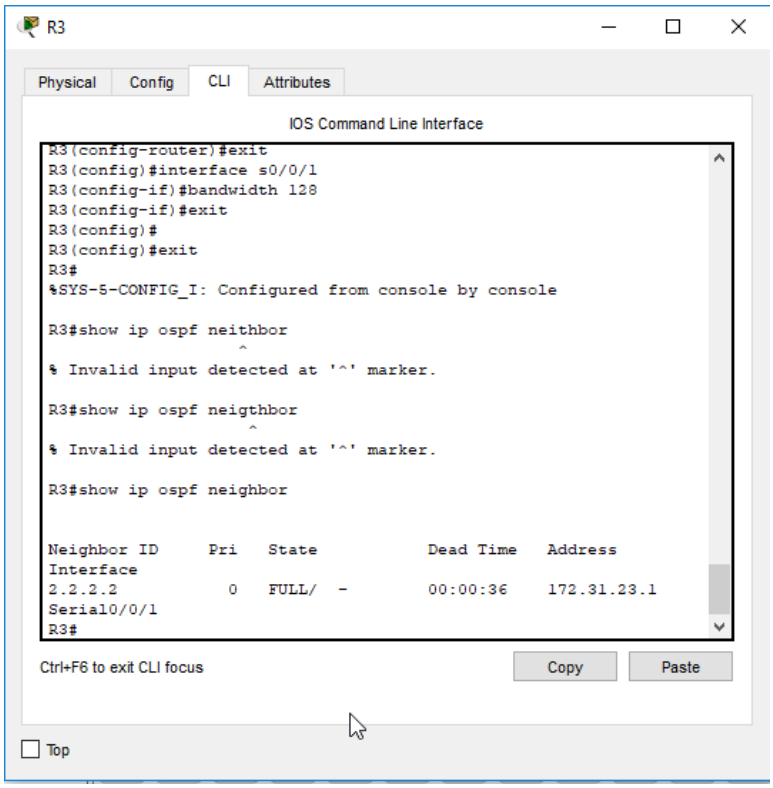


Figura 6- Listado OSFP Router 3

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

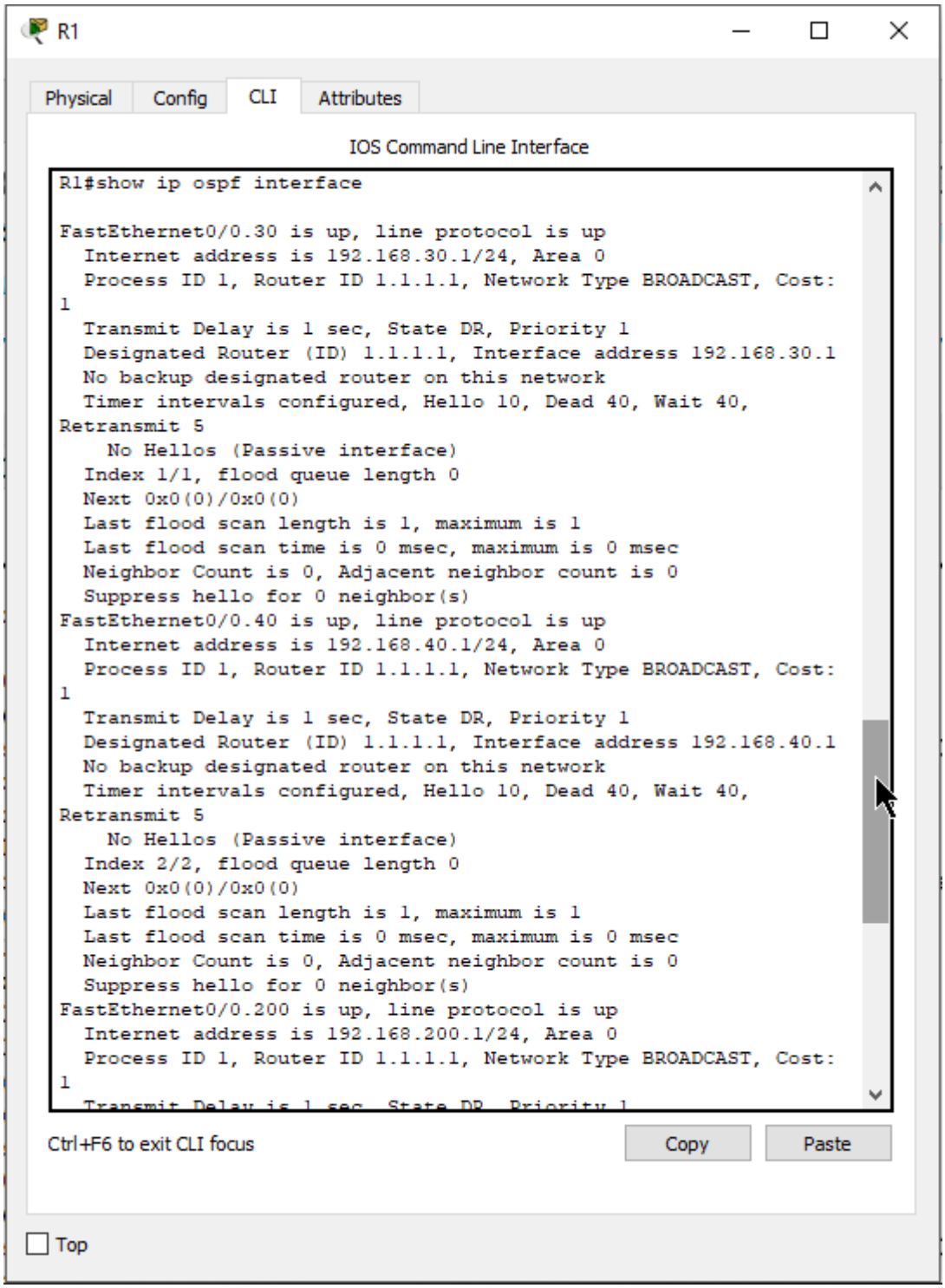


Figura 7 – Listado Costo OSPF Router 1 – Parte 1

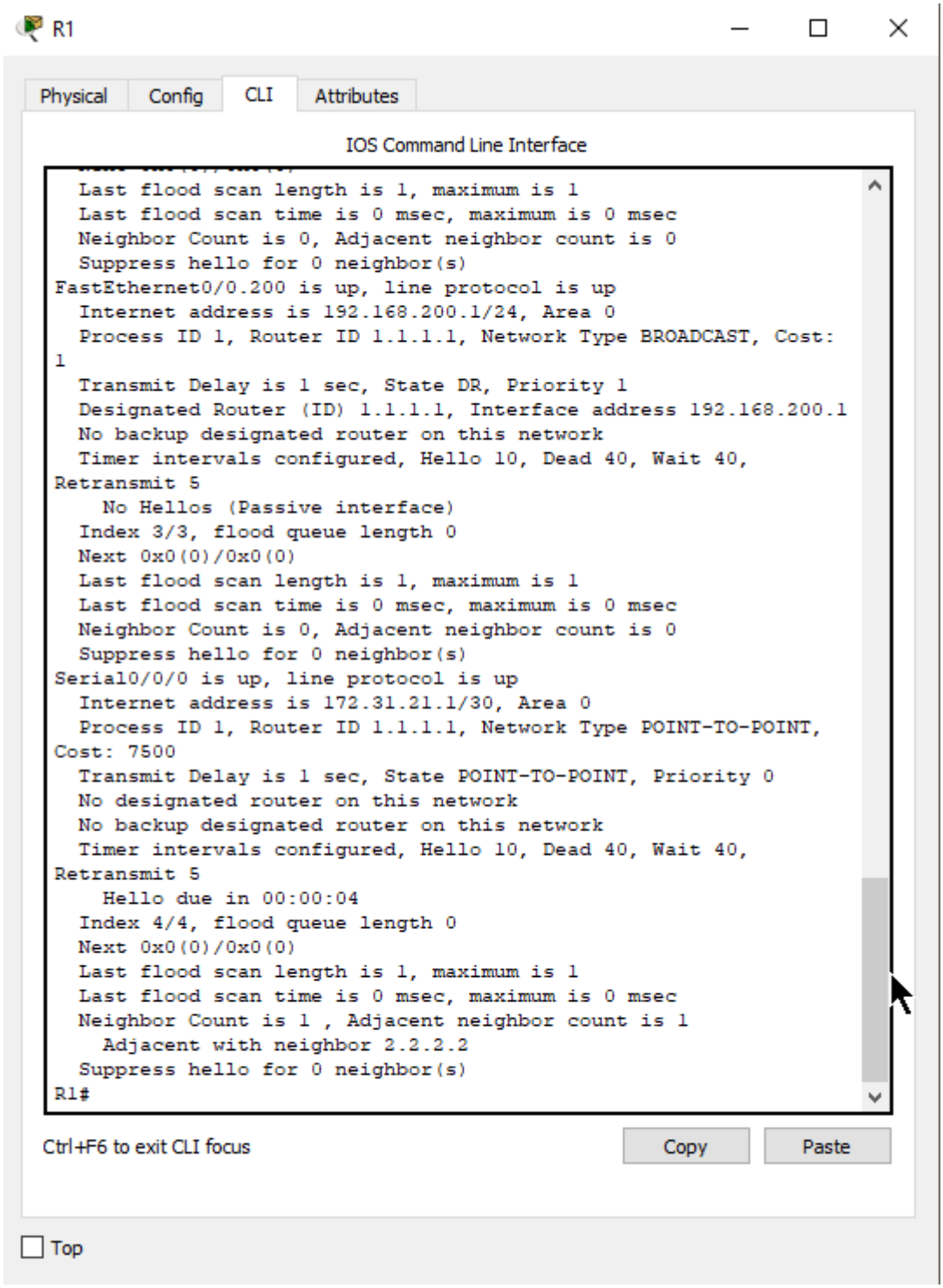


Figura 8 – Listado Costo OSPF Router 1 – Parte 2

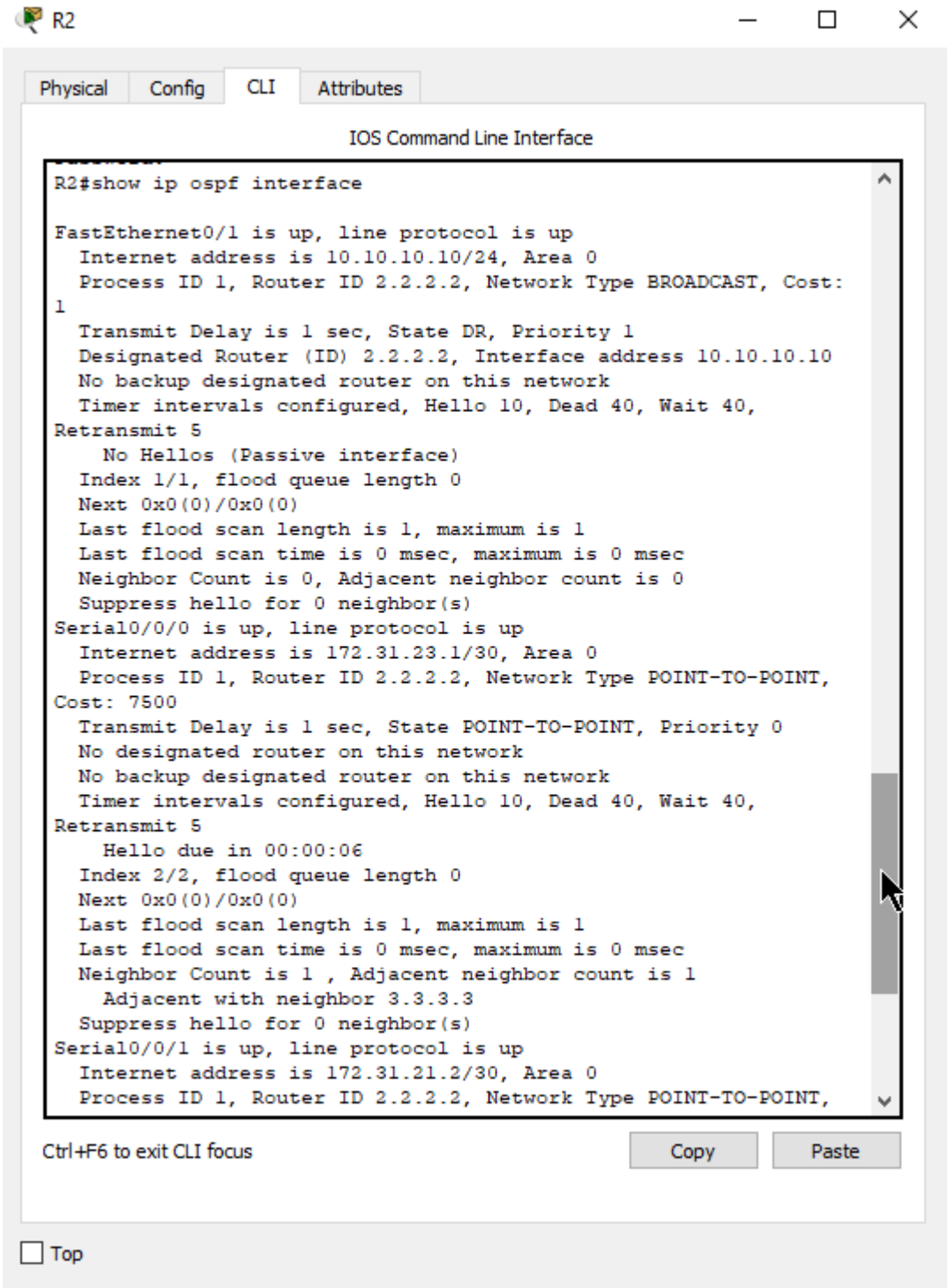


Figura 9 – Listado Costo OSPF Router 2 – Parte 1

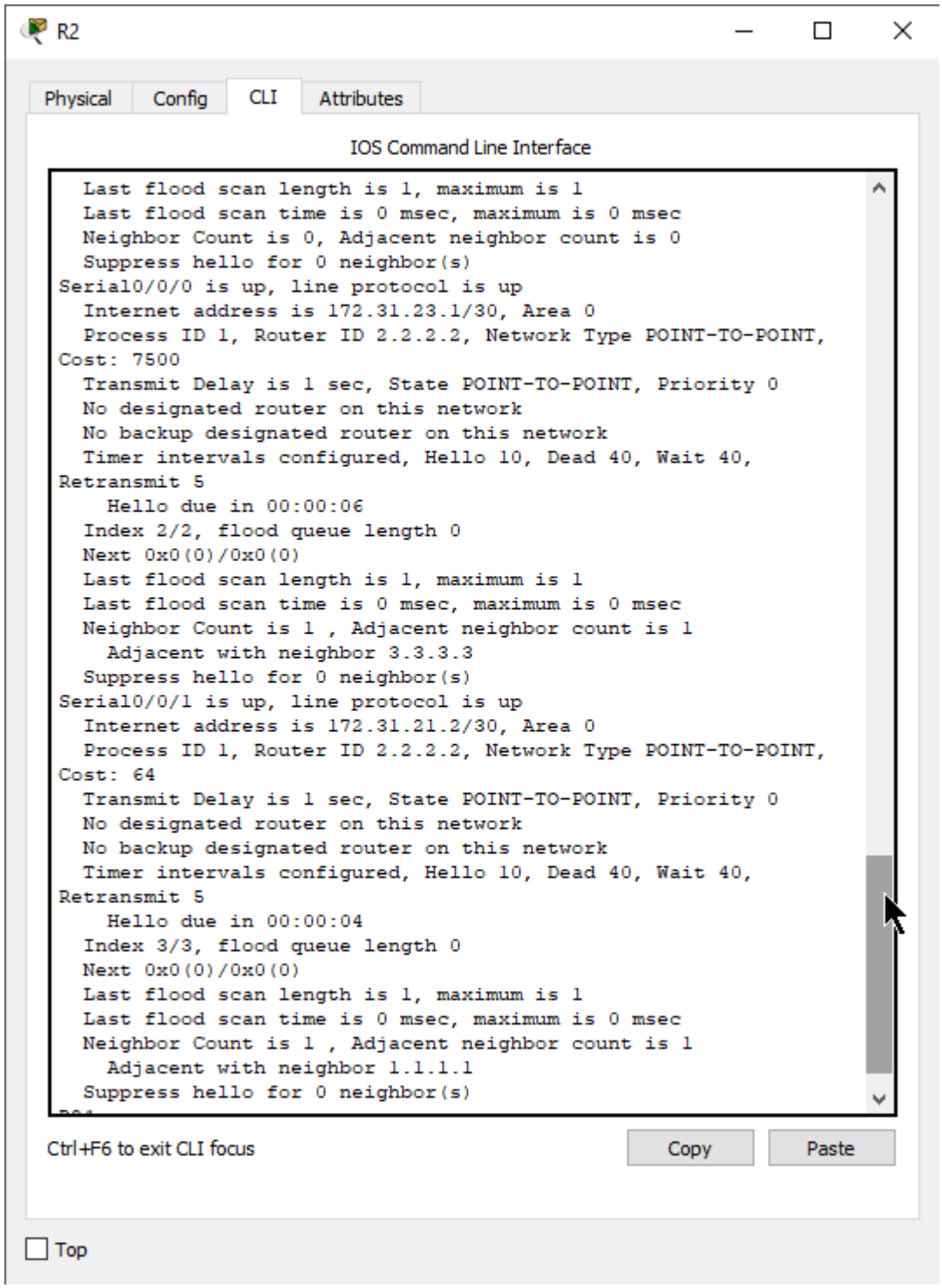


Figura 10 – Listado Costo OSPF Router 2 – Parte 1

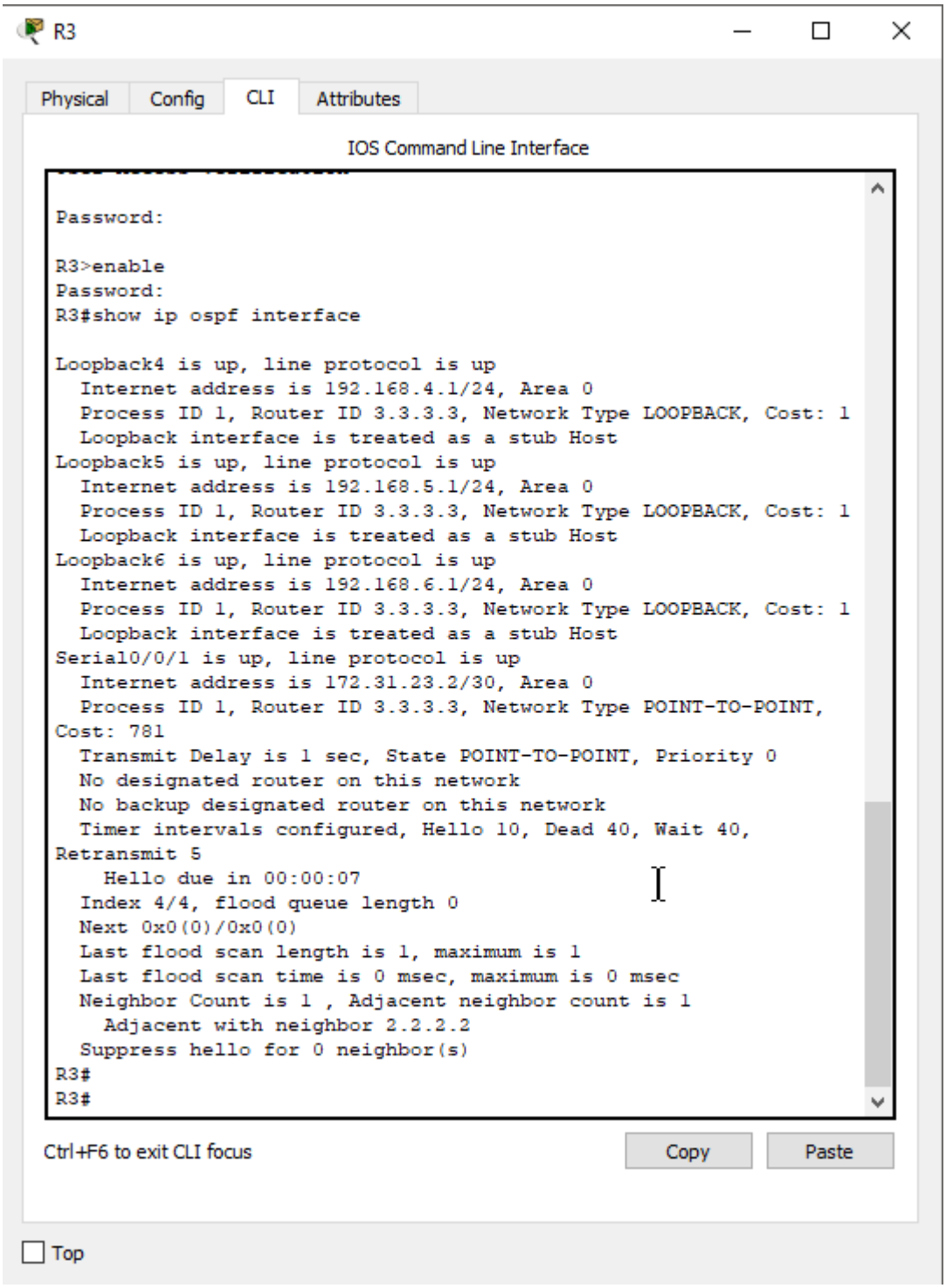


Figura 11 – Listado Costo OSPF Router 3

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

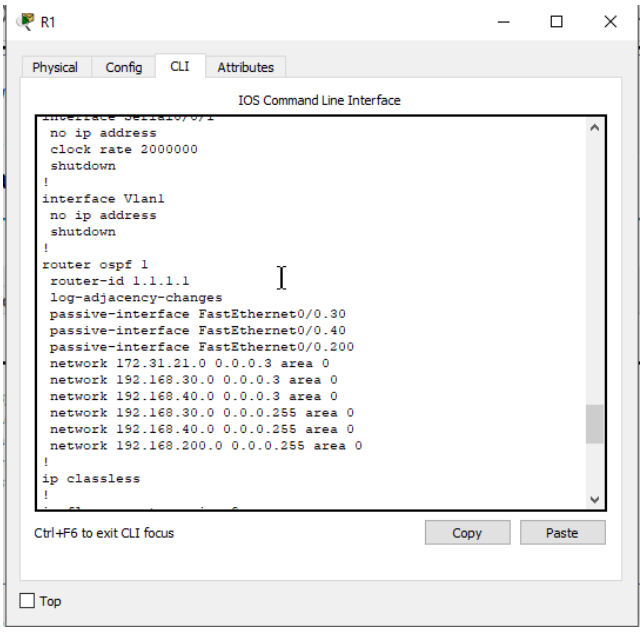


Figura 12 – Comando show running config para evidenciar configuración del router 1

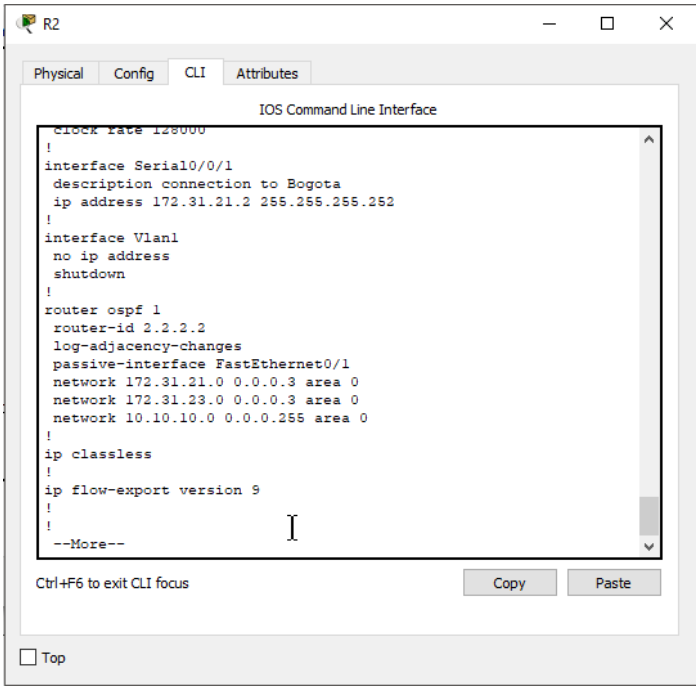


Figura 13 – Comando show running config para evidenciar configuración del router 2

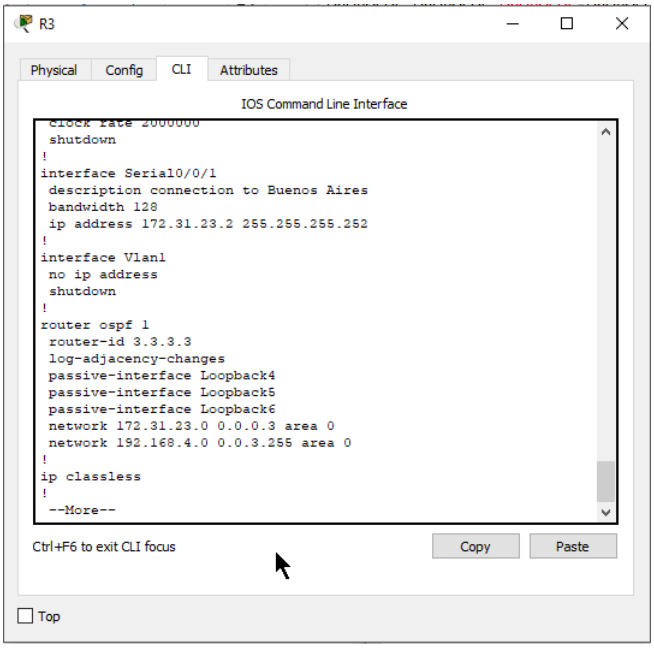


Figura 14 – Comando show running config para evidenciar configuración del router 3

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

Confirguración de las vlan 30,40 y 200 en el Switch 1

S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#exit
S1(config)#
S1(config)#interface vlan 200
S1(config-if)#ip add 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#interface f0/3
S1(config-if)#switchport mode trunk

```
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/24
S1(config-if)#switchport mode trunk

S1(config-if)#switchport trunk native vlan 1
```

Confirguración de las vlan 30,40 y 200 en el Switch 3

```
S3>enable
Password:
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 30
S3(config-vlan)#name Administracion
S3(config-vlan)#vlan 40
S3(config-vlan)#name Mercadeo
S3(config-vlan)#vlan 200
S3(config-vlan)#name Mantenimiento
S3(config-vlan)#exit
S3(config)#interface vlan 200
S3(config-if)#ip add 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#
```

4. En el Switch 3 deshabilitar DNS lookup

Desactivación del DNS Lookup en el switch 3

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#no ip domain-lookup
S3(config)#
S3#
```

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

Asignación de direcciones IP en el Switch 1

```
S1>enable
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
```

```
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
```

Asignación de direcciones IP en el Switch 3

```
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#exit
S3(config)#ip default-gateway 192.168.99.1
```

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

Desactivación de interfaces no utilizadas Switch 1

```
S1(config)#int range fa0/2,fa0/4-23
S1(config-if-range)#shutdown
```

Asignación de direcciones IP en el Switch 3

```
S3(config)#interface range fa0/2,fa0/4-24
S3(config-if-range)#shutdown
```

7. Implement DHCP and NAT for IPv4
8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.

Estableciendo DHCP para 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
```

9. 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.

```
R1(config)#ip dhcp pool admin
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#ip dhcp pool merca
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
```

10. Configurar NAT en R2 para permitir que los host puedan salir a internet

```
R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int f0/0
R2(config-if)#ip nat out
R2(config-if)#ip nat outside
R2(config-if)#int f0/1
R2(config-if)#ip nat inside
```

11. 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.

```
R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list l permit 192.168.30.0 0.0.0.255
^
% Invalid input detected at '^' marker.
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#ip access-list standard ADMIN_S
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN_S in
R2(config-line)#
```

12. 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.

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#access-list 101 permit tcp any host 209.165.200.229 eq www
R2(config)#int f0/0
R2(config-if)#ip access-group 101 in
R2(config-if)#int s0/0/0
R2(config-if)#ip access-group 101 out
R2(config-if)#int s0/0/1
R2(config-if)#ip access-group 101 out
R2(config-if)#int f0/1
R2(config-if)#ip access-group 101 out
```

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

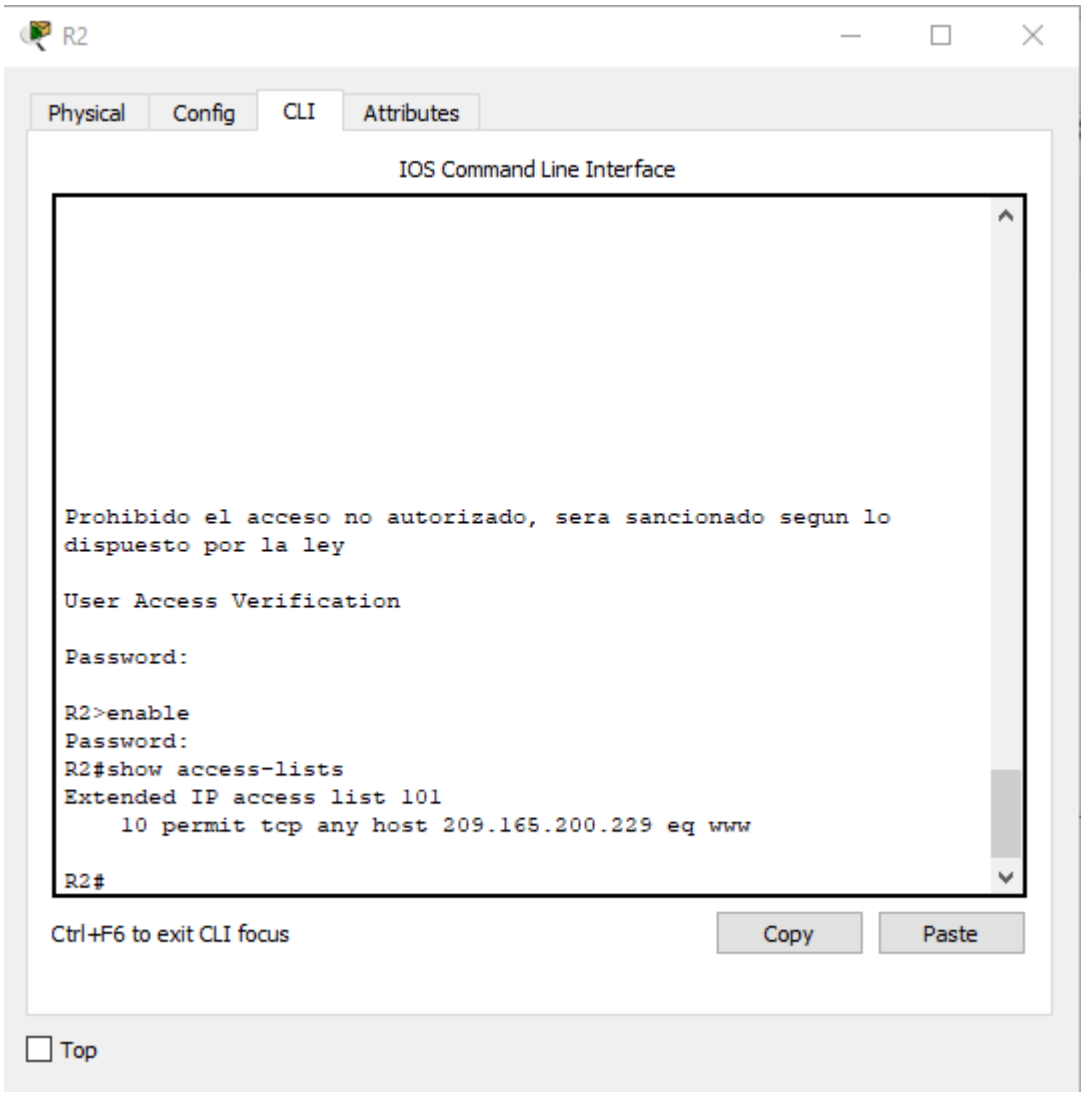


Figura 15 – Verificación de conectividad con el comando traceroute entre R1 y WebServer

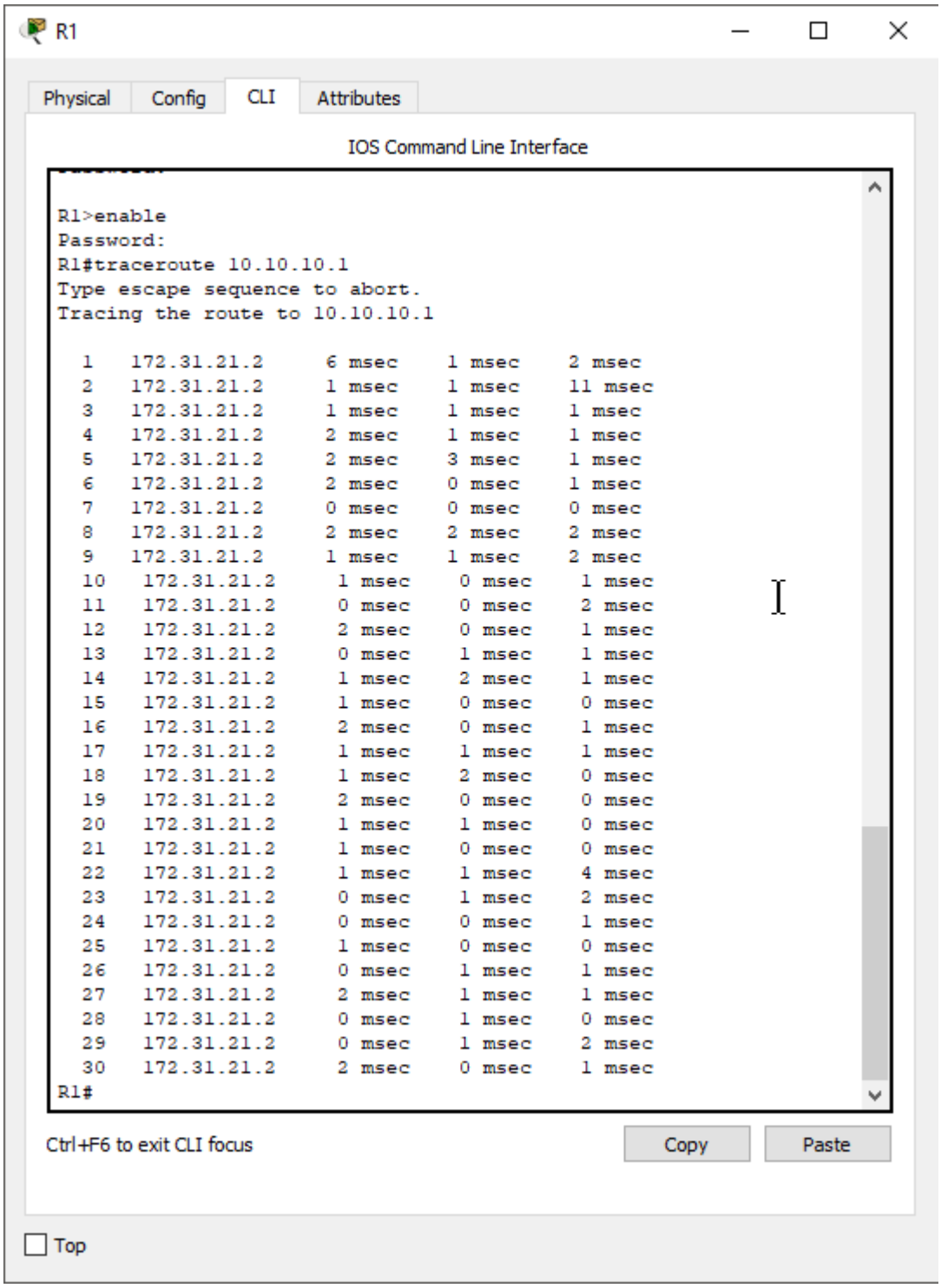


Figura 16 – Verificación de conectividad con el comando traceroute entre R1 y WebServer

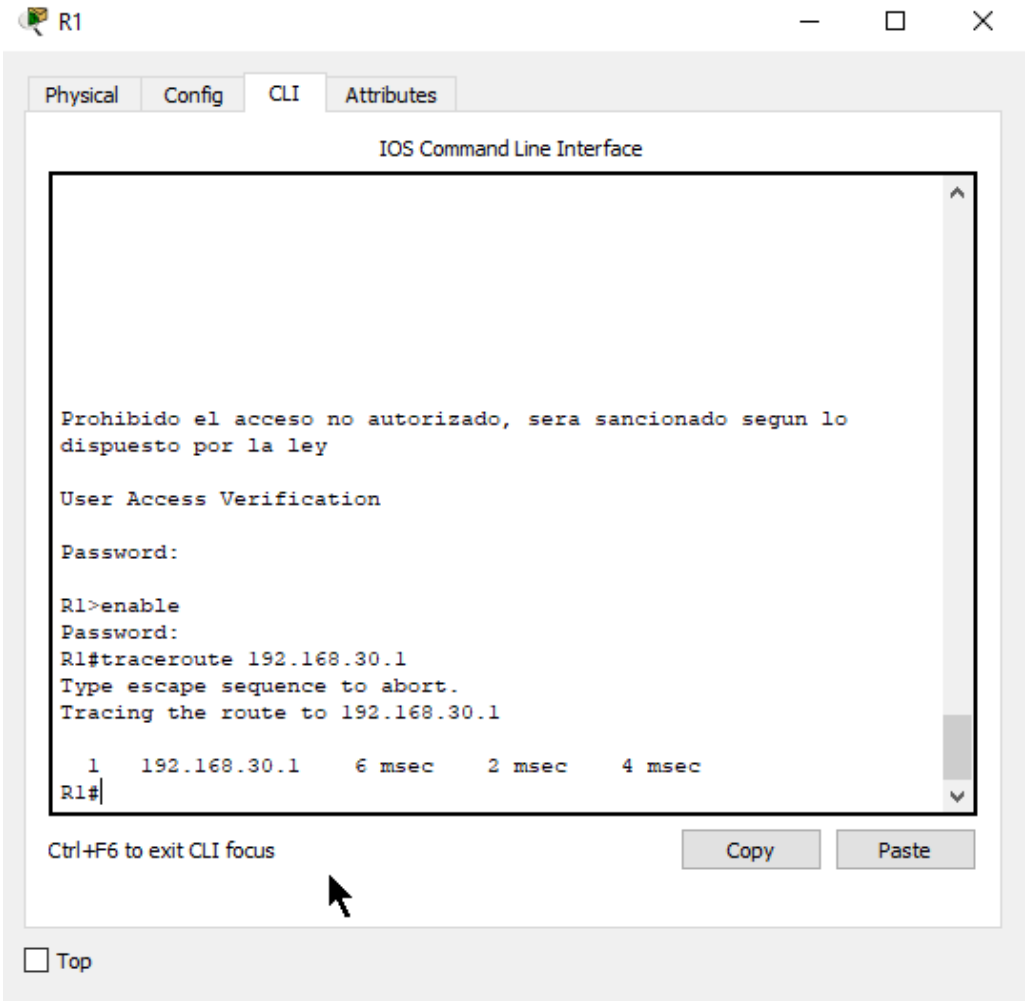


Figura 17 – Verificación de conectividad con el comando traceroute entre R1 y PC-A

Link de descarga escenario 2

https://drive.google.com/open?id=15YddkQkIG4c-pURY56fjfVucBgnTJi1w

3. Conclusiones

- Realizar la división de vlan permite mantener mayor control en nuestra red, permitiendo establecer que redes pueden estar intercomunicadas
- Dentro de la parametrización de los switch se puede nombrar las vlan para una fácil identificación, se puede también activar y desactivar interfaces a partir de rangos.
- Es recomendable desactivar interfaces que no se vayan a utilizar con el fin de no tener vacíos de seguridad por puertos que no estén configurados en una vlan especifica.
- La utilización del RIPv2 permite que los router puedan enviar su tabla de ruteo a los vecinos cada 30 segundos por si se presenta alguna caída o cambio en la red.
- Con el uso del OSPF se puede garantizar una recuperación de la red ante una caída, en vista de que converge nuevas rutas haciendo imperceptible en muchos casos la falla.
- Se debe establecer contraseña para los routers y switch que se usan en nuestra red como un mecanismo básico de seguridad.

4. Bibliografía

CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1

CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1

CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

UNAD (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

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

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1

CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1

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

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

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

UNAD (2014). Configuración de Switches y Routers [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgL9QChD1m9EuGqC

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2014). 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

CISCO. (2014). 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

CISCO. (2014). DHCP. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module10/index.html#10.0.1.1

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

UNAD (2014). Principios de Enrutamiento [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgOyjWeh6timi_Tm