DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN)

TRANSFERENCIA DEL CONOCIMIENTO FRENTE A LA ADMNISTRACIÓN DE UNA RED DESDE SU CREACIÓN, EJECUCIÓN Y MANTENIMIENTO

LIYIS RODRIGUEZ GARRIDO
CÓDIGO: 1067880654

GRUPO: 203092_34

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
PROGRAMA DE INGENIERIA DE SISTEMAS
CEAD JOSÉ ACEVEDO Y GÓMEZ
MAYO - 2018

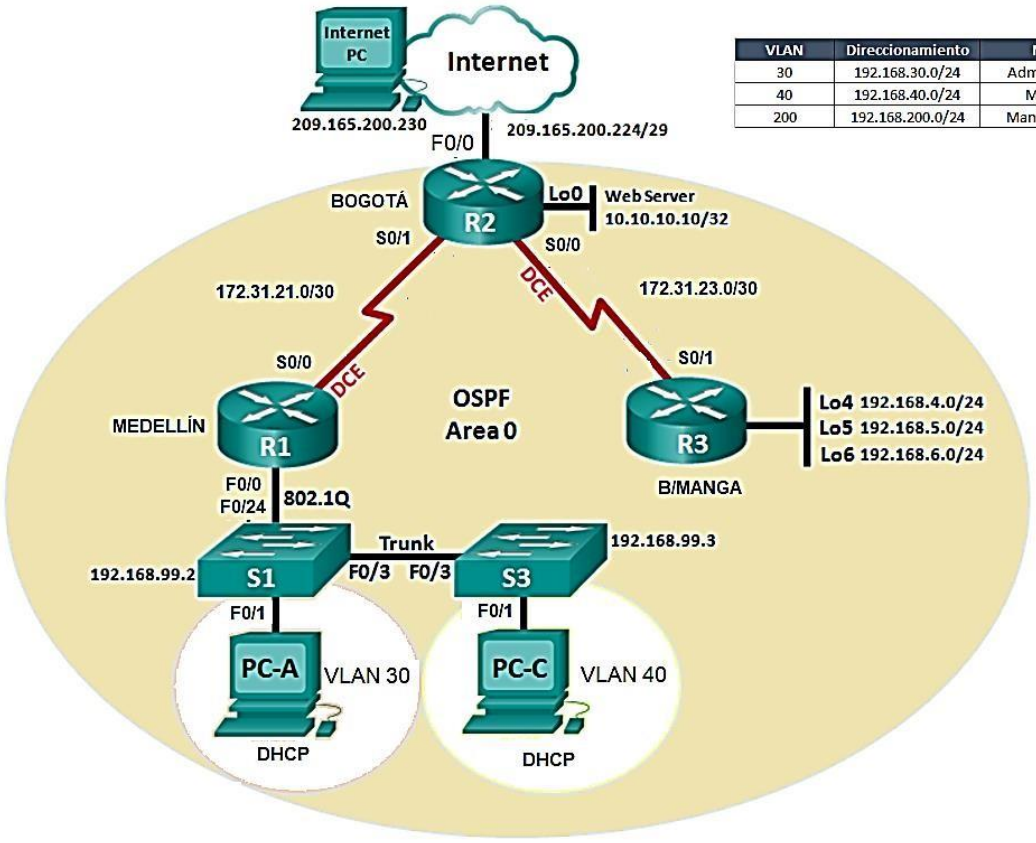
Introducción

La implementación de una red, así como su administración y mantenimiento, hace necesario que se pongan en marcha diferentes aspectos como son los lineamientos de direccionamiento IP, protocolos de enrutamiento, topologías de red, entre otros elementos necesarios para un buen funcionamiento de la misma. Es por ello que con este trabajo se pretende iniciar desde cero en la construcción y ejecución de una red de una empresa con sede en diferentes ciudades con el fin de satisfacer las necesidades inherentes al ámbito tecnológico y de comunicación.

Descripción del escenario propuesto

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Bogotá, Medellín y Bucaramanga, 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.

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

Solución

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

Se configura la red en el Sotfware Packet Tracer:

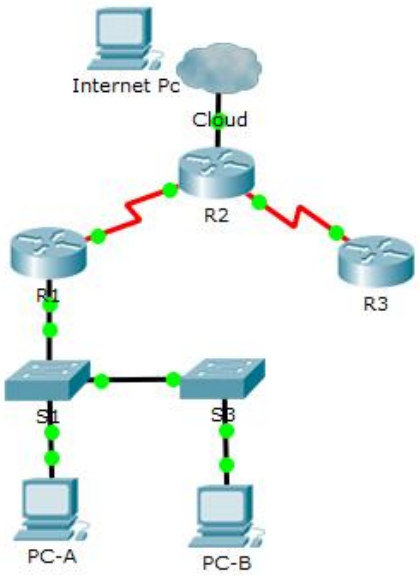


Figura 1. Implementacion de la red en Packet Tracer

Se crea tabla de direccionamiento IP para su aplicación.

Dispositivo	Interfaz	Dirección ip	Mascara de subred
R1	S0/0/0	172.31.21.1	255.255.255.252
R2	S0/0/0	172.31.21.2	255.255.255.252
	S0/0/1	172.31.23.2	255.255.255.252
	F 0/0	209.165.200.225	255.255.255.248
R3	S0/0/1	172.31.23.1	255.255.255.252
S1	Vlan 1	192.168.99.2	255.255.255.0
S2	Vlan 2	192.168.99.2	255.255.255.0
PC-A	NIC	DHCP	DHCP
PC-B	NIC	DHCP	DHCP
Internet Pc	NIC	200.165.200.230	255.255.255.0

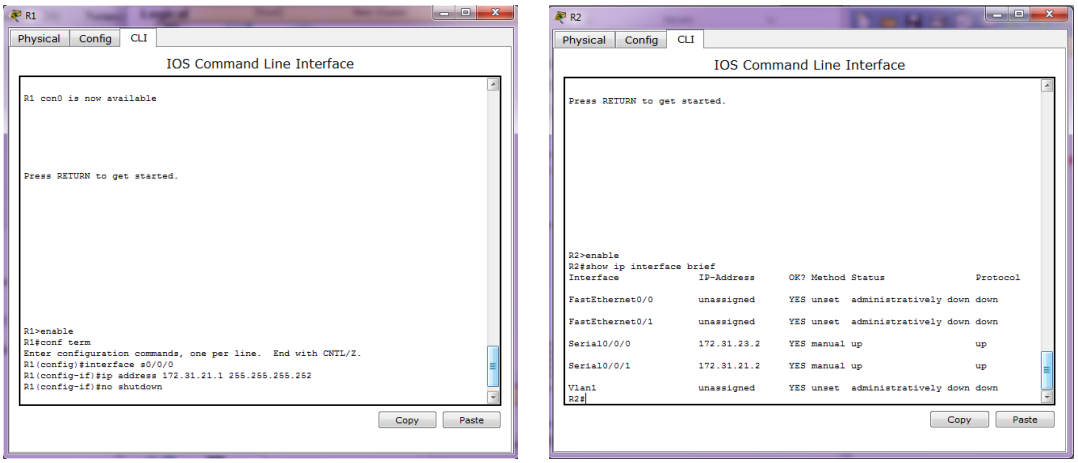


Figura 2. Configuración de Routers

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	2.2.2.2
Router ID R3	3.3.3.3
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	128 Kb/s
Ajustar el costo en la métrica de S0/0 a	7500

Se configura el protocolo OSPFv2 en todos los router con los criterios señalados especificando un número de protocolo y el área 0

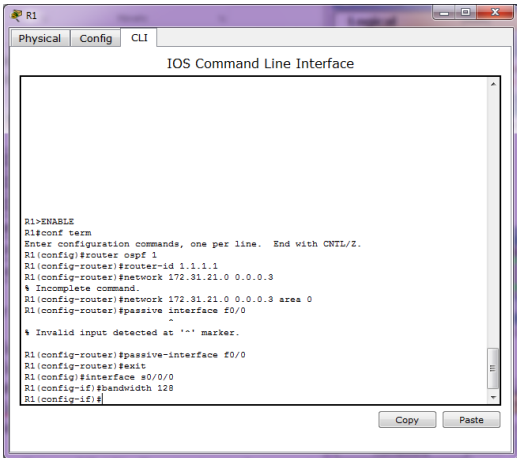


Figura 3. Protocolo OSPFv2

Verificar información de OSPF

Para verificar la información del protocolo de enrutamiento, se hace uso de los comandos:

Show ip protocols

Show ip ospf interface brief (o el *id de la interface*)

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

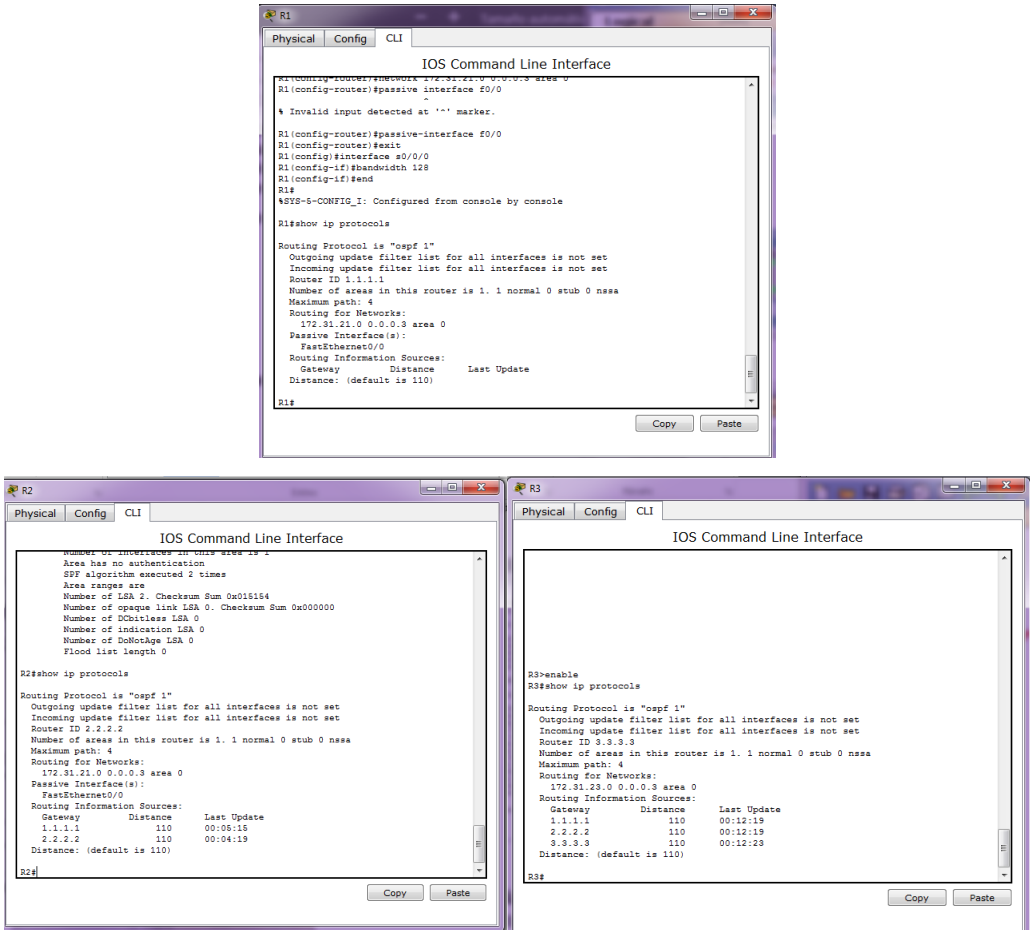


Figura 4. Comandos para visualizar tablas de enrutamiento y router conectados por OSPF

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

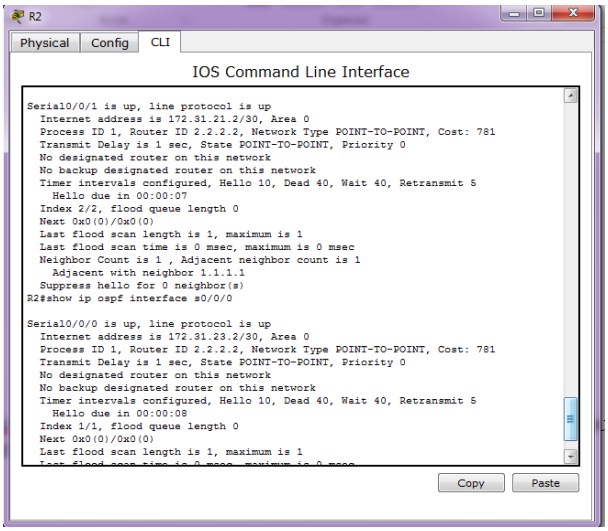


Figura 5. Comando Show ip ospf interface serial0/0/0

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

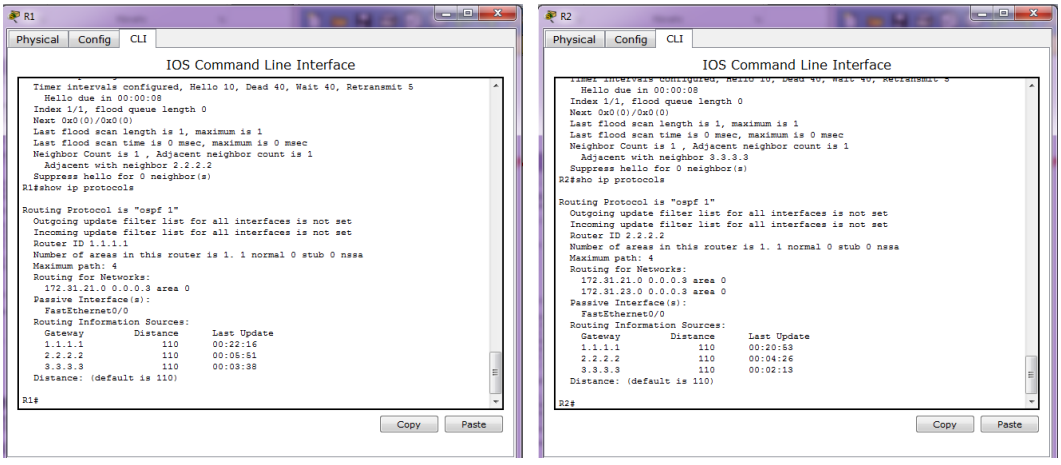


Figura 6. Comando Show ip protocols

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

Se configuran las Vlan 30, 40 y 200 en los switch S1 y S2, y se le asigna a cada interface del switch la vlan correspondiente a través del comando switchport mode acces, switchport acces vlan *#vlan:*

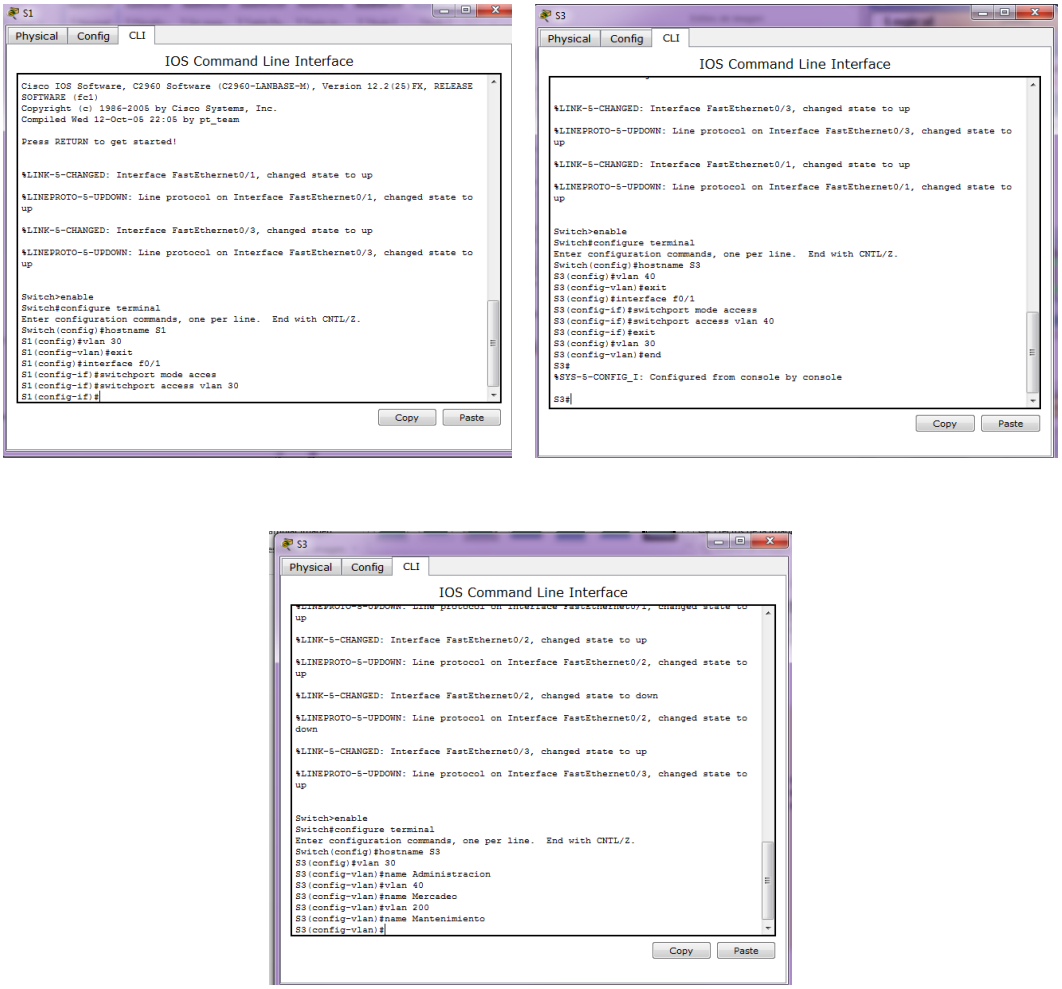


Figura 7. Configuracion Vlan 30, Vlan 40 y Vlan 200 en S1, S2 y S3

Para asignar puertos troncales que permitan la comunicación de las mismas Vlan en diferentes res se hace uso del comando switchport mode trunk en la interface que servirá de enlace troncal en ambos switches:

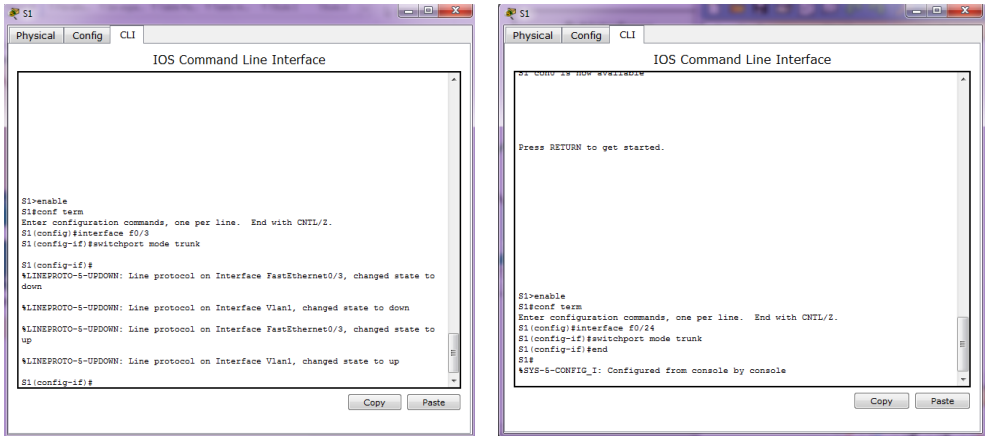


Figura 8. Comando Switchport mode trunk para la interface con enlace troncal

Para la creacion de las subinterfaces para cada Vlan y su encapsulacion se hace uso del comando encapsulation dot1q

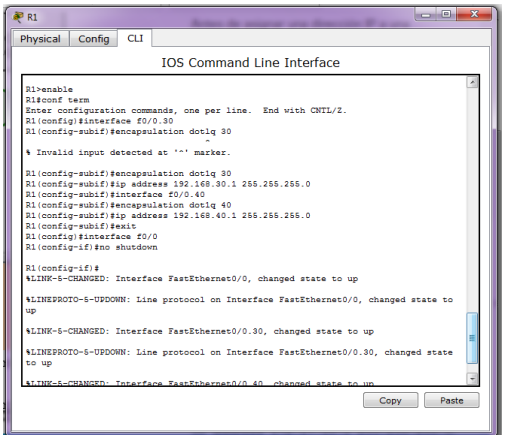


Figura 9. Encapsulacio n de interfaces con el comando dot1q

4. En el Switch 3 deshabilitar DNS lookup

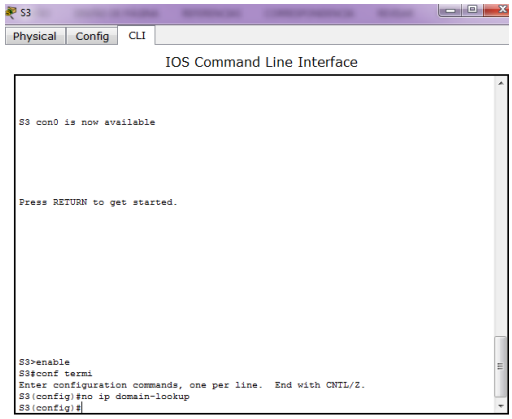


Figura 10. No ip domain-lookup

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

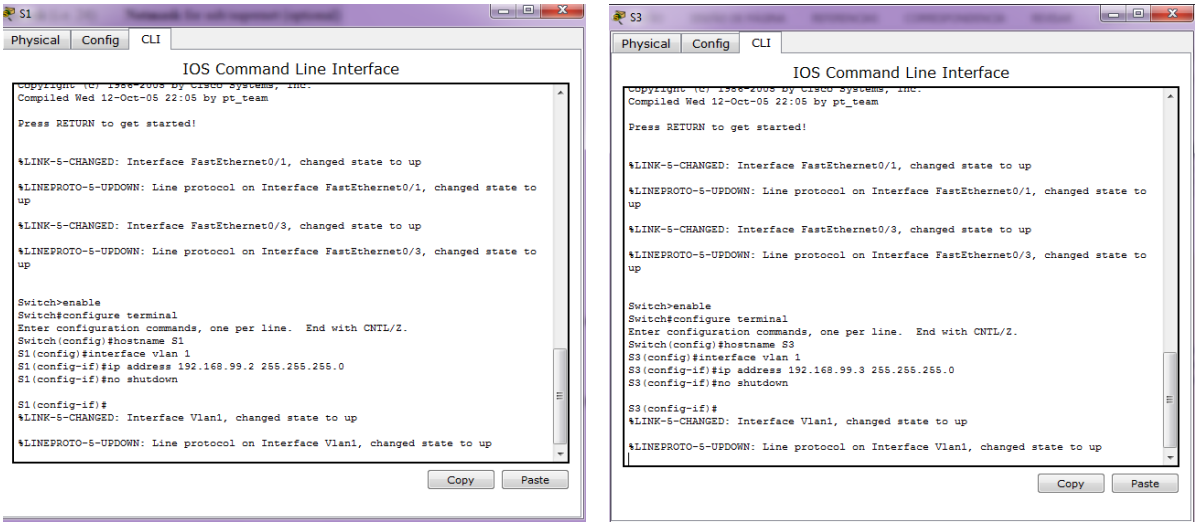


Figura 11. Direccionamiento ip en Switches

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

Para desactivar interface se especifica la interface y se escribe el comando shutdown:

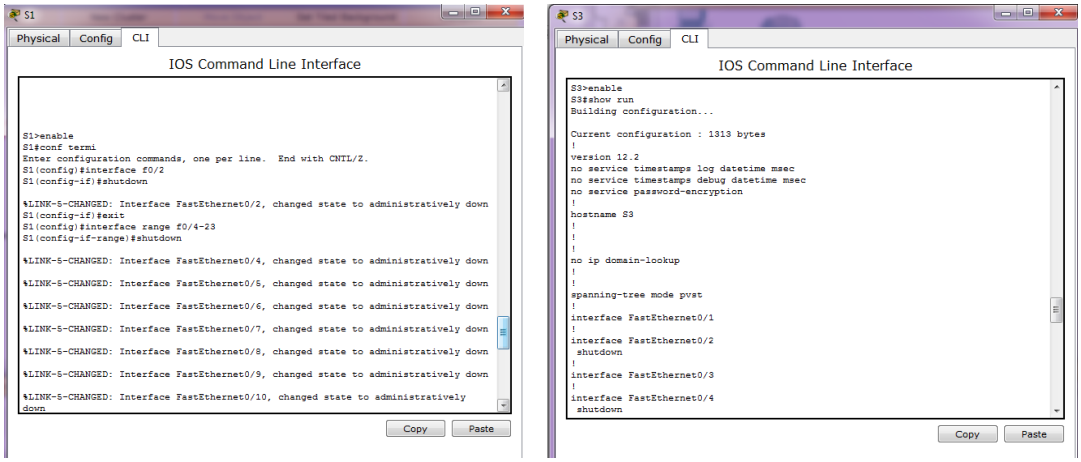


Figura 12. Comando No Shutdown para desactivar interfaces

7. Implementar DHCP and NAT for IPv4

Para implementar DHCP se debe especificar las direcciones IP que serán excluidas y a continuación crear un DHCP pool con el nombre y la red correspondiente, así como el Gateway predeterminado, el DNS-Server y el Domain Name.

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.

En cuanto a la aplicación de una NAT se debe especificar la interface interna y externa con las direcciones IP correspondientes.

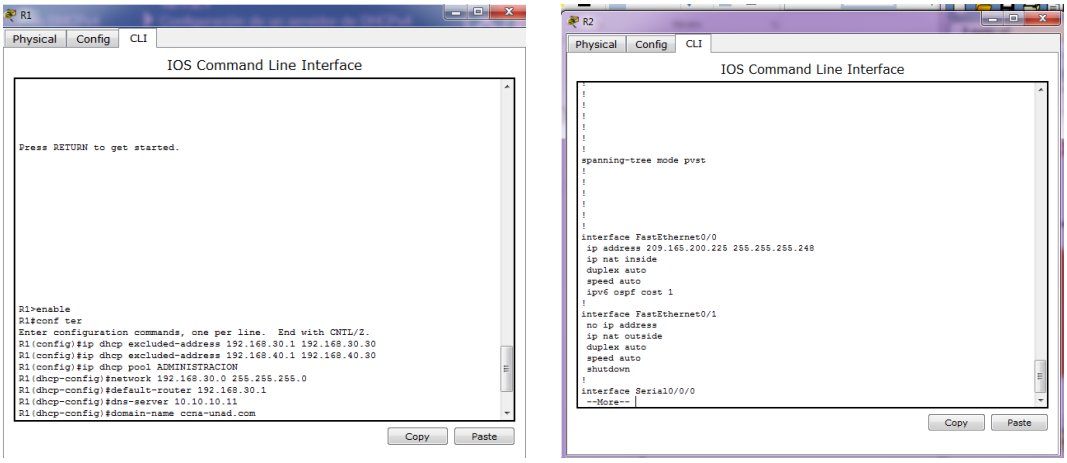


Figura 13. Creacion de un Dhcp pool e implementacion de Nat

8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.

Para configurar el R1 como servidor DHCP se especifica un pool de DHCP con las redes que le corresponden a cada una de las Vlan y se excluyen aquellas que se desean de forma estática.

9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

Para reservar las primeras 30 direcciones se usa el comando: ip dhcp excluded-address

```
R1>enable
R1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp pool ADMINISTRACION
```

Figura 14. Reserva o exlusión de direcciones IP

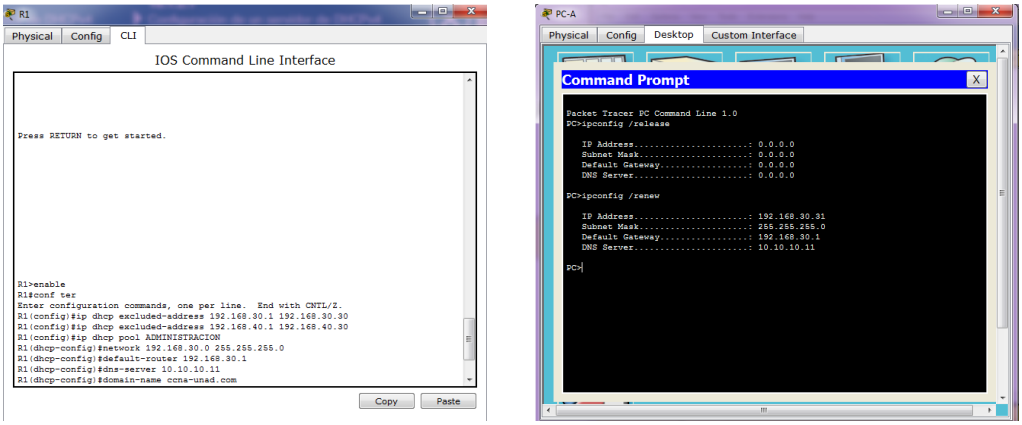


Figura 15. Funcionamiento DHCP en la asignacion de dirección IP de la PC-A

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

Se hace uso del comando ip nat source, y después se especifica la interface que será la de entrada (inside) y la de salida (outside)

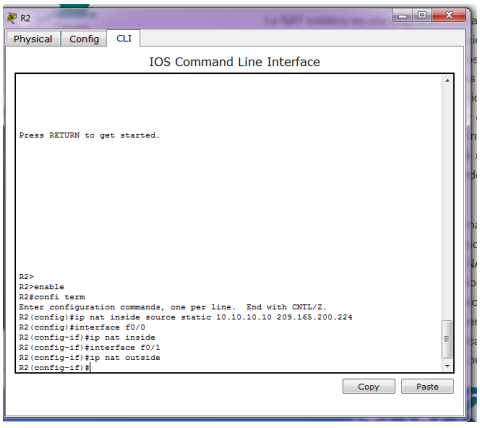


Figura 16. Ip Nat inside source

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.

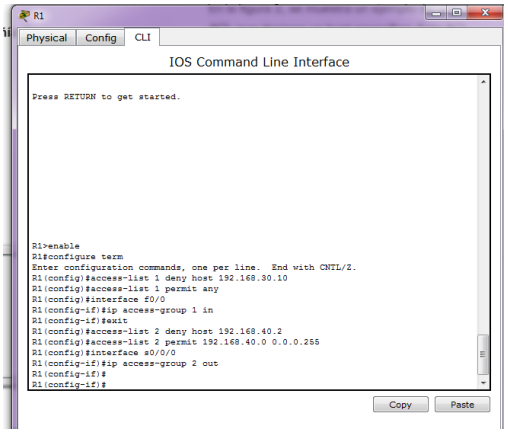


Figura 17. Creacion lista de acceso (ACL) tipo estándar

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.

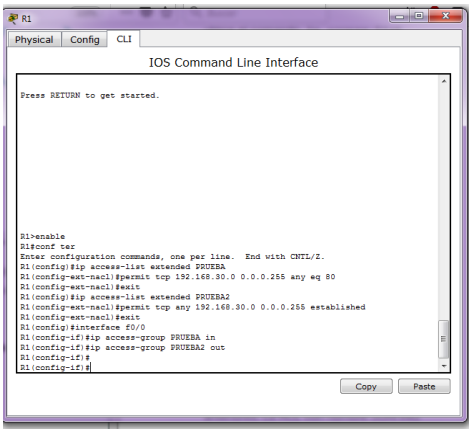


Figura 18. Creacion lista de acceso (ACL) tipo extendida

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

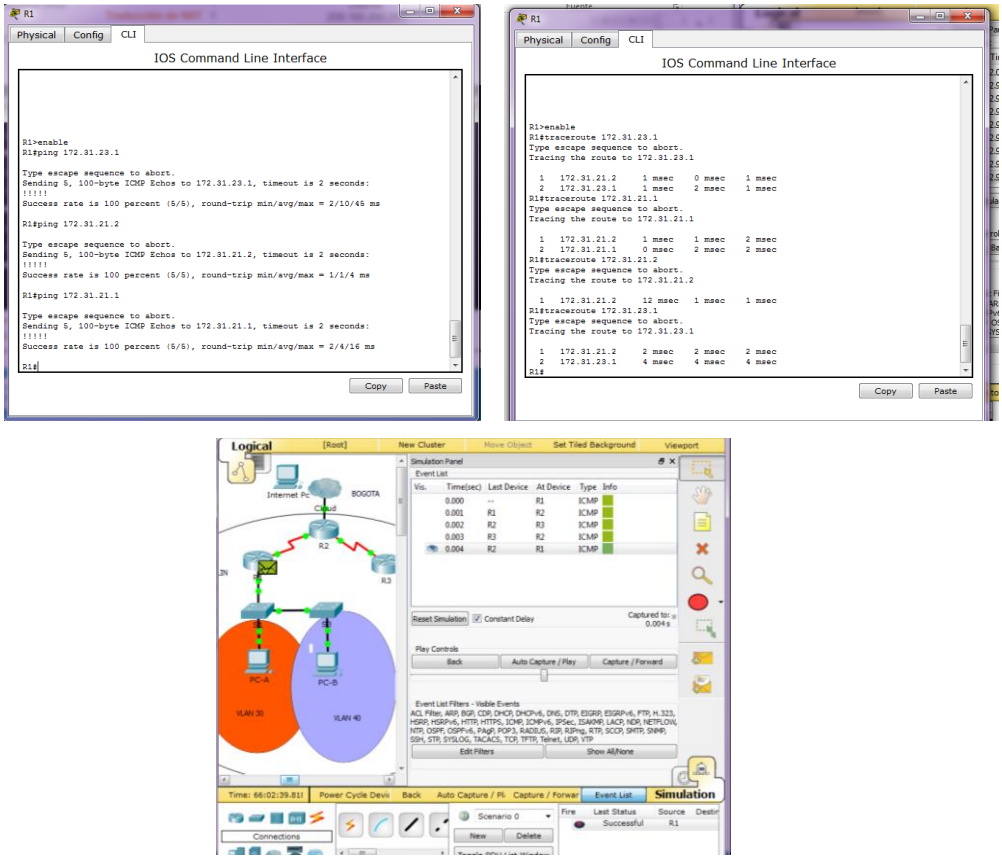


Figura 19. Comunicación y redireccionamiento de trafico en routers – Uso de los comando ping y traceroute.

Bibliografía

Cisco Networking Academy, CCNA R&S: Introduction to Networks; recuperado de https://1314297.netacad.com/courses/627676

Cisco Networking Academy, CCNA R&S: Routing and Swtiching; recuperado de https://1314297.netacad.com/courses/654717