

SOLUCION CASO DE ESTUDIO CCNA

GONZALO ANDRÉS NIÑO SAJONERO

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGIENERIA
PROGRAMA DE INGENIERIA ELECTRONICA
CALI
2018**

SOLUCION CASO DE ESTUDIO CCNA

GONZALO ANDRÉS NIÑO SAJONERO

Trabajo realizado como requisito para optar por el título de ingeniero electrónico

**PhD.
JUAN CARLOS VESGA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INGIENERIA
PROGRAMA DE INGENIERIA ELECTRONICA
CALI
2018**

Nota de Aceptación

Presidente del Jurado

Jurado

Jurado

Cali, Mayo 30 de 2018

Dedicatoria

Primero a Dios por darme fortaleza para enfrentar todo este camino hacia el desarrollo profesional y a mi familia que siempre creyeron en mí.

AGRADECIMIENTOS

Agradezco a familiares y amigos que estuvieron constantemente motivándome para culminar con éxito esta gran etapa de mi vida, además a los tutores de la unidad que me acompañaron en todo el proceso y que realizan un esfuerzo por la educación del país.

CONTENIDO

1	INTRODUCCIÓN	10
2	OBJETIVOS	11
2.1	OBJETIVO GENERAL.....	11
2.2	OBJETIVOS ESPECÍFICOS	11
3	PLANTEAMIENTO DEL PROBLEMA.....	12
3.1	DEFINICIÓN DEL PROBLEMA	12
3.2	JUSTIFICACIÓN	13
4	MARCO TEÓRICO.....	14
5	MATERIALES Y MÉTODOS	16
5.1	MATERIALES	16
5.2	METODOLOGÍA.....	16
6	DESARROLLO DEL PROYECTO	17
	CONCLUSIONES.....	45
	BIBLIOGRAFIA	46

LISTA DE FIGURAS

Figura 1. Topología de red. Fuente: Cisco.....	12
Figura 2. IP configurada en Internet PC.....	17
Figura 3. IP configurada en R1 para interface Serial 0/0/0.....	18
Figura 4. IP configurada en R2 para las interfaces serial 0/0/0, serial 0/0/1 y FastEthernet 0/0..	19
Figura 5. IP configurada en R2 para la interface FastEthernet 0/1.....	20
Figura 6. IP configurada en R3 para interface Serial 0/0/1.....	21
Figura 7. IP configurada en R3 para interfaces lo4, lo5, lo6.....	22
Figura 8. Router ID R1	23
Figura 9. Router ID R2	24
Figura 10. Router ID R3.....	25
Figura 11. Tabla de enrutamiento en R2	26
Figura 12. Lista de costo de cada interface de R2.....	27
Figura 13. Show ip portocols en R2.....	28
Figura 14. Show ip route ospf.....	29
Figura 15. Show running-config.....	30
Figura 16. Configuración Vlan en S1	31
Figura 17. Configuración Vlan en S3	32
Figura 18. Configuración de seguridad en S1	33
Figura 19. Configuración de seguridad en S3.....	34
Figura 20. No ip domain-lookup en S3.....	34
Figura 21. Ip configurada en S1.....	34
Figura 22. Ip configurada en S3.....	35
Figura 23. Shutdown para las interfaces sin uso en S1	35
Figura 24. Shutdown para las interfaces sin uso en S3	36
Figura 25. Reserva de las 30 primeras Ip	37
Figura 26. DHCP Vlan 30	37
Figura 27. DHCP Vlan 40	38
Figura 28. Configuración NAT en R2.....	38
Figura 29. Listas de acceso.....	39
Figura 30. Ip DHCP configurada en PC-A	39
Figura 31. Ip DHCP configurada en PC-C	40
Figura 32. Ping satisfactorio desde PC-A hacia PC-C	41
Figura 33. Ping satisfactorio desde PC-C hacia PC-A	42
Figura 34. Ping satisfactorio desde R1 hacia R2	42
Figura 35. Ping satisfactorio desde Internet PC hacia R2.....	43
Figura 36. Ping satisfactorio desde R2 hacia R3	44

GLOSARIO

- **Punto de acceso inalámbrico:** consta de un transmisor de radio que puede conectar dispositivos finales en forma inalámbrica.
- **Router:** reenvía paquetes de datos a Internet y recibe paquetes de datos de ella.
- **Switch:** conecta dispositivos finales mediante cables de red.
- **Dispositivo de firewall:** protege el tráfico saliente y restringe el tráfico entrante.

RESUMEN

Ser el administrador de una red; por ejemplo de una empresa de tecnología, se debe tener el conocimiento para configurar e interconectar entre sí cada uno de los dispositivos que forman parte de dicha red, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red que se estudiaron en el diplomado de cisco.

Los temas principales que sirvieron de apoyo y que se debieron utilizar como base para establecer un enlace en la red fue el enrutamiento inter VLAN que es el proceso de tráfico de enrutamiento entre diferentes VLAN, mediante un router dedicado o un switch multicapa. El enrutamiento inter VLAN facilita la comunicación entre los dispositivos aislados por los límites de la VLAN.

Además se realiza el uso de DHCPv4 para asignar de forma dinámica información de direccionamiento IPv4. Todos los nodos en una red requieren una dirección IP única que se comunique con otros dispositivos. La asignación estática de información de direccionamiento IP en una red grande similar a la utilizada en la empresa de tecnología que incluye 3 sucursales produce una carga administrativa que puede eliminarse mediante el uso de DHCPv4.

De los tres mecanismos de asignación de direcciones que utiliza DHCPv4 para proporcionar flexibilidad al asignar las direcciones IP, se utilizó la asignación automática para las PCs PC-A y PC-C la cual asigna automáticamente una dirección IPv4 estática de forma permanente a un dispositivo y la selecciona de un conjunto de direcciones disponibles. No hay arrendamiento, y la dirección se asigna de forma permanente al dispositivo.

Se usa la versión actual de OSPF para IPv4 la cual es OSPFv2, introducida en RFC 1247 y actualizada en RFC 2328 por John Moy. OSPF es un protocolo de routing de estado de enlace sin clase con una distancia administrativa predeterminada de 110 y se indica en la tabla de routing con el código de origen de ruta **O**.

Se utiliza NAT para contribuir a mitigar el agotamiento del espacio de direcciones IPv4. La NAT para IPv4 permite que los administradores de red utilicen el espacio de direcciones privadas, a la vez que proporciona conectividad a Internet, mediante una única dirección pública o una cantidad limitada de estas.

PALABRAS CLAVE: OSPF, VLAN, NAT, DHCP,

1 INTRODUCCIÓN

La globalización de internet ha producido un cambio significativo en el crecimiento y en cómo se comunican las empresas de tecnología, ya que ninguna quiere quedarse fuera de este constante desarrollo tecnológico. A medida que programadores y especialistas en TI evolucionen en crear cada vez lo imposible en el ámbito de las comunicaciones, las empresas seguirán su ritmo o si no desaparecerán.

En el presente escenario tenemos una empresa de tecnología con varias sucursales a nivel nacional, y se ha implementado una topología de red cuya administración de la misma requiere de un administrador calificado para que ésta funcione correctamente. El diplomado Cisco CCNA1 y CCNA2 disponen de las herramientas necesarias para generar en las personas que se certifiquen, la capacidad de realizar esta función.

En la topología de red que se centra el caso de estudio sobre una red empresarial, utiliza dispositivos y mucho más tráfico que una red doméstica sencilla, estos se suelen incorporar como dispositivos independientes y autónomos que proporcionan un servicio dedicado. Los dispositivos finales, como las computadoras portátiles y de escritorio, se conectan a los switches de red mediante conexiones por cable. Para enviar paquetes más allá de la red local, los switches de red se conectan a routers de red. Entre los demás dispositivos de infraestructura en una red, se incluyen los puntos de acceso inalámbrico y los dispositivos de seguridad dedicados, como los firewalls.

Para resolver este caso de estudio es necesario implementar configuración de enrutamiento dinámico, auto configuración de direcciones estáticas, configuración de protocolos de enrutamiento OSPFv2, DHCPv4 y diseñar e implementar NAT dinámicas y estáticas.

2 OBJETIVOS

2.1 OBJETIVO GENERAL

Desarrollar el caso de estudio ccna de la prueba de habilidades prácticas que forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, la cual busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado y a través de la cual se pondrá a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

2.2 OBJETIVOS ESPECÍFICOS

- Planificar e implementar redes pequeñas.
- Diseñar la topología de red utilizando Packet tracer.
- Configurar direccionamiento de dispositivos de red.
- Configurar Vlans en topología de redes.
- Establecer seguridad en los switches y routers utilizados en la red.
- Conocer los protocolos de enrutamiento.
- Verificar procesos de comunicación y redireccionamiento de tráfico.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

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

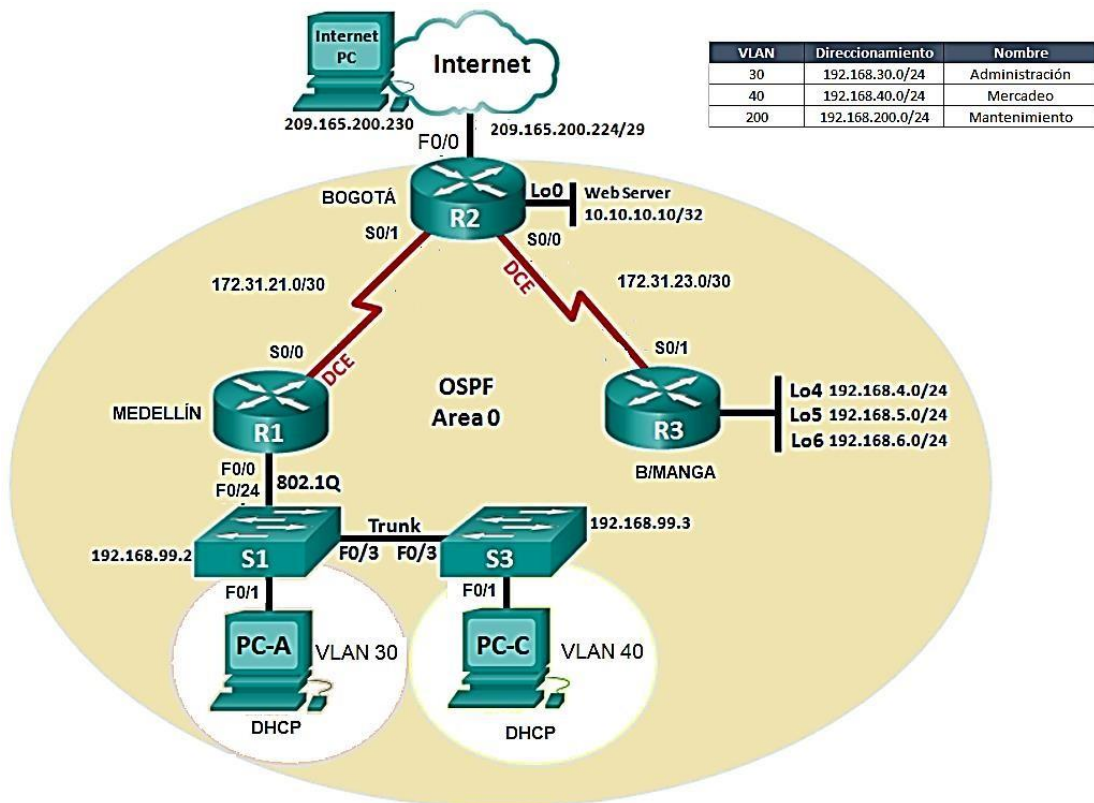


Figura 1. Topología de red. Fuente: Cisco

3.2 JUSTIFICACIÓN

El rendimiento de la red es un factor importante en la productividad de una organización, por tal razón es necesario que la implementación de la red del caso de estudio sea segura, confiable y totalmente productiva para la empresa de tecnología que tiene sus sucursales en Bogotá, Medellín y Bucaramanga. Una de las tecnologías que contribuyen a mejorar el rendimiento de la red es la división de los grandes dominios de difusión en dominios más pequeños. Las herramientas que se implementaran en la solución de conectividad están basadas en el protocolo de enrutamiento que usa OSPFv2 y la transmisión de información entre redes VLAN.

4 MARCO TEÓRICO

El uso de redes VLAN para segmentar una red conmutada proporciona mayor rendimiento, seguridad y capacidad de administración. Se utilizan enlaces troncales para transportar información de varias VLAN entre dispositivos. Sin embargo, debido a que estas VLAN segmentan la red, es necesario un proceso de capa 3 para permitir que el tráfico pase de un segmento de red a otro.

Este proceso de routing de capa 3 puede implementarse utilizando un router o una interfaz de switch de capa 3. El uso de un dispositivo de capa 3 proporciona un método para controlar el flujo de tráfico entre segmentos de red, incluidos los segmentos de red creados por las VLAN.

Los switches se usan para conectar varios dispositivos en la misma red. En una red diseñada correctamente, los switches LAN son responsables de controlar el flujo de datos en la capa de acceso y de dirigirlo a los recursos conectados en red. Los switches de Cisco son de configuración automática y no necesitan ninguna configuración adicional para comenzar a funcionar. Sin embargo, los switches Cisco ejecutan Cisco IOS y se pueden configurar manualmente para satisfacer mejor las necesidades de la red. Esto incluye el ajuste de los requisitos de velocidad, de ancho de banda y de seguridad de los puertos.

Además, los switches Cisco se pueden administrar de manera local y remota. Para administrar un switch de forma remota, este se debe configurar con una dirección IP y un Gateway predeterminado. Estos son solo dos de los parámetros de configuración que se analizan en este capítulo.

Los switches funcionan en lugares de la capa de acceso donde los dispositivos de red cliente se conectan directamente a la red y donde los departamentos de TI quieren que los usuarios accedan de forma simple a esta. Es una de las áreas más vulnerables de la red, ya que está muy expuesta al usuario. Los switches se deben configurar para que sean resistentes a los ataques de todo tipo y, al mismo tiempo, protejan los datos de los usuarios y permitan que haya conexiones de alta velocidad. La seguridad de puertos es una de las características de seguridad que proporcionan los switches administrados por Cisco.

Los routers conectan una red a otra red. El router es responsable de la entrega de paquetes a través de distintas redes. El destino de un paquete IP puede ser un servidor web en otro país o un servidor de correo electrónico en la red de área local.

El router usa su tabla de routing para encontrar la mejor ruta para reenviar un paquete. Es responsabilidad de los routers entregar esos paquetes a su debido tiempo. La efectividad de las comunicaciones de internetwork depende, en gran medida, de la capacidad de los routers de reenviar paquetes de la manera más eficiente posible.

Cuando un host envía un paquete a un dispositivo en una red IP diferente, el paquete se reenvía al Gateway predeterminado, ya que los dispositivos host no pueden comunicarse directamente con los dispositivos que están fuera de la red local. El Gateway predeterminado es el destino que enruta el tráfico desde la red local hacia los dispositivos en las redes remotas. Con frecuencia, se utiliza para conectar una red local a Internet.

El protocolo **OSPF** (Open Shortest Path First) es un protocolo de routing de estado de enlace desarrollado como reemplazo del protocolo de routing vector distancia RIP. Durante los comienzos de la tecnología de redes y de Internet, RIP era un protocolo de routing aceptable. Sin embargo, el hecho de que RIP dependiera del conteo de saltos como única métrica para determinar la mejor ruta rápidamente se volvió problemático. El uso del conteo de saltos no escala bien en redes más grandes con varias rutas de distintas velocidades. OSPF presenta ventajas importantes en comparación con RIP, ya que ofrece una convergencia más rápida y escala a implementaciones de red mucho más grandes.

OSPF es un protocolo de enrutamiento sin clase que utiliza el concepto de áreas para realizar la escalabilidad.

5 MATERIALES Y MÉTODOS

5.1 MATERIALES

- Software Cisco Packet Tracer Version 7.1.1.0137
- 3 PCs
- 2 Switch 2960
- 3 Router 2811

5.2 METODOLOGÍA

La función de proporcionar acceso a una LAN suele reservarse para los switches de capa de acceso. Se puede crear una red de área local virtual (VLAN) en un switch de capa 2 para reducir el tamaño de los dominios de difusión, similares a los dispositivos de capa 3. Por lo general, las VLAN se incorporan al diseño de red para facilitar que una red dé soporte a los objetivos de una organización. Si bien las VLAN se utilizan principalmente dentro de las redes de área local conmutadas, las implementaciones modernas de las VLAN les permiten abarcar redes MAN y WAN.

La metodología usada describe cómo configurar y administrar VLAN y enlaces troncales de VLAN, así como resolver problemas relacionados. También se analizan cuestiones y estrategias de seguridad relacionadas con las VLAN y los enlaces troncales, así como las prácticas recomendadas para el diseño de VLAN.

La introducción de un servidor de protocolo de configuración dinámica de host (DHCP) en la red local simplifica la asignación de direcciones IP tanto a los dispositivos de escritorio como a los móviles. El uso de un servidor de DHCP centralizado permite a las organizaciones administrar todas las asignaciones de direcciones IP desde un único servidor. Esta práctica hace que la administración de direcciones IP sea más eficaz y asegura la coherencia en toda la organización, incluso en las sucursales.

DHCP está disponible tanto para IPv4 (DHCPv4) como para IPv6 (DHCPv6).

6 DESARROLLO DEL PROYECTO

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

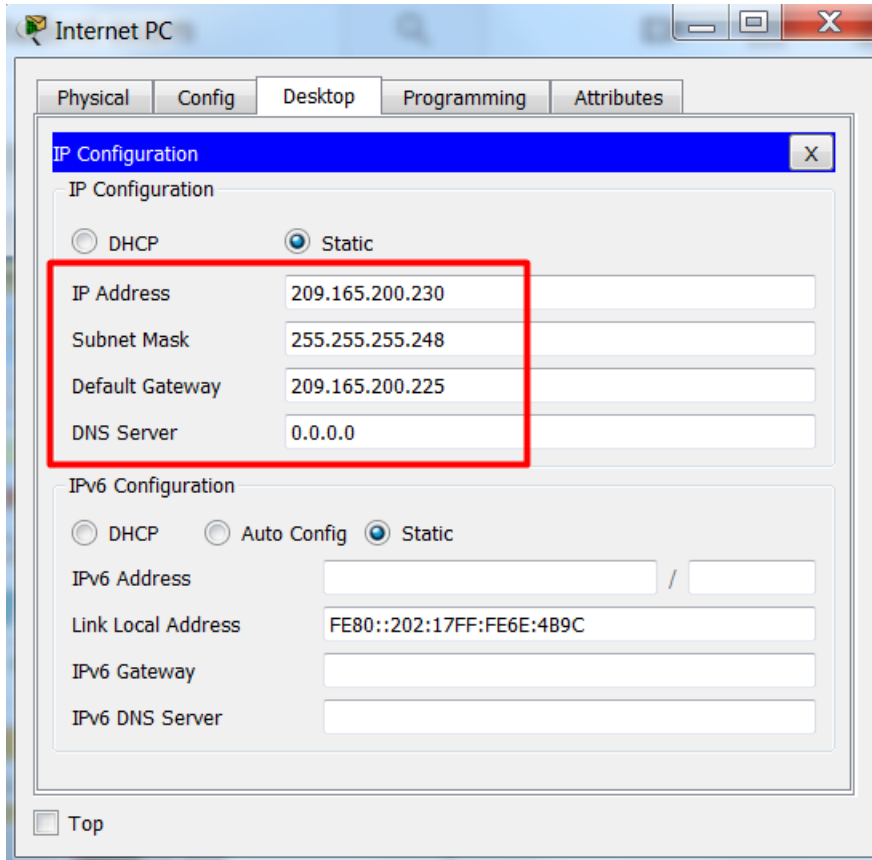


Figura 2. IP configurada en Internet PC

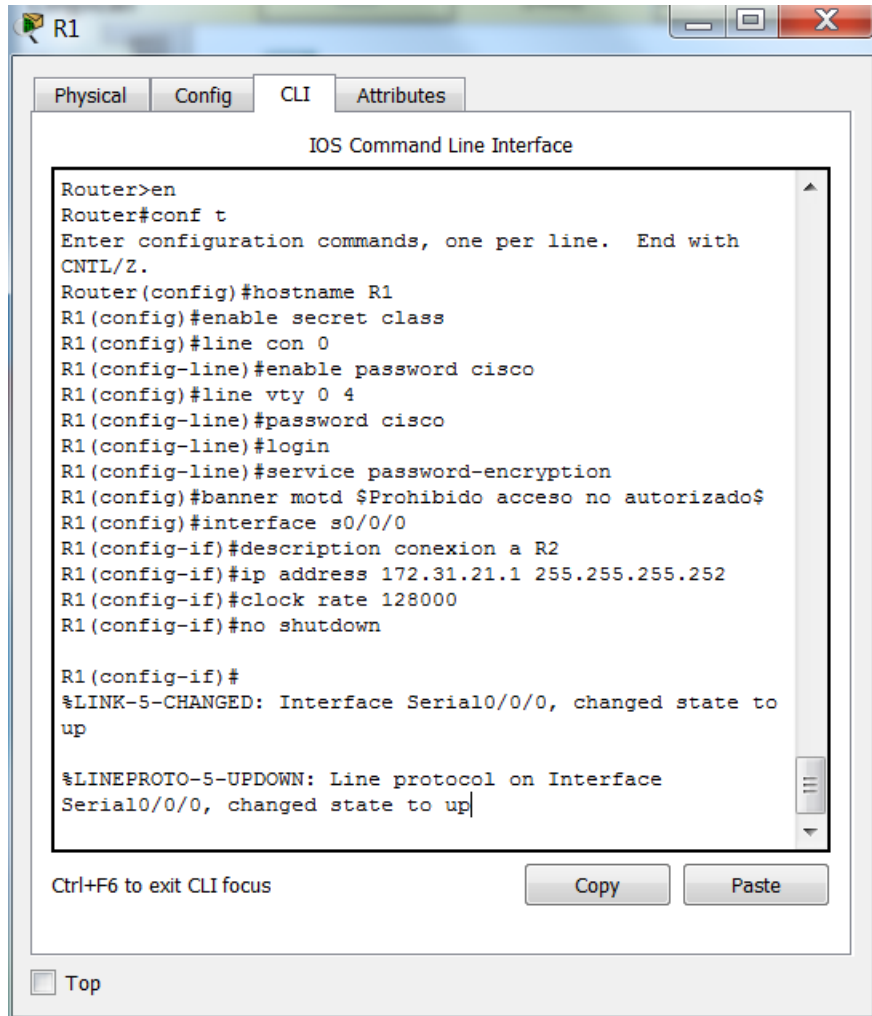


Figura 3. IP configurada en R1 para interface Serial 0/0/0

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#service password-encryption
R2(config)#banner motd $Prohibido acceso no autorizado$
R2(config)#interface s0/0/0
R2(config-if)#description Conexion a R3
R2(config-if)#Ip address 172.31.23.1 255.255.255.252
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to
down
R2(config-if)#
R2(config-if)#interface s0/0/1
R2(config-if)#description Conexion a R1
R2(config-if)#Ip address 172.31.21.2 255.255.255.252
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up

R2(config-if)#interface fa0/0
R2(config-if)#description Internet
R2(config-if)#Ip address 209.165.200.225 255.255.255.248
R2(config-if)#no shutdown

R2(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Figura 4. IP configurada en R2 para las interfaces serial 0/0/0, serial 0/0/1 y FastEthernet 0/0

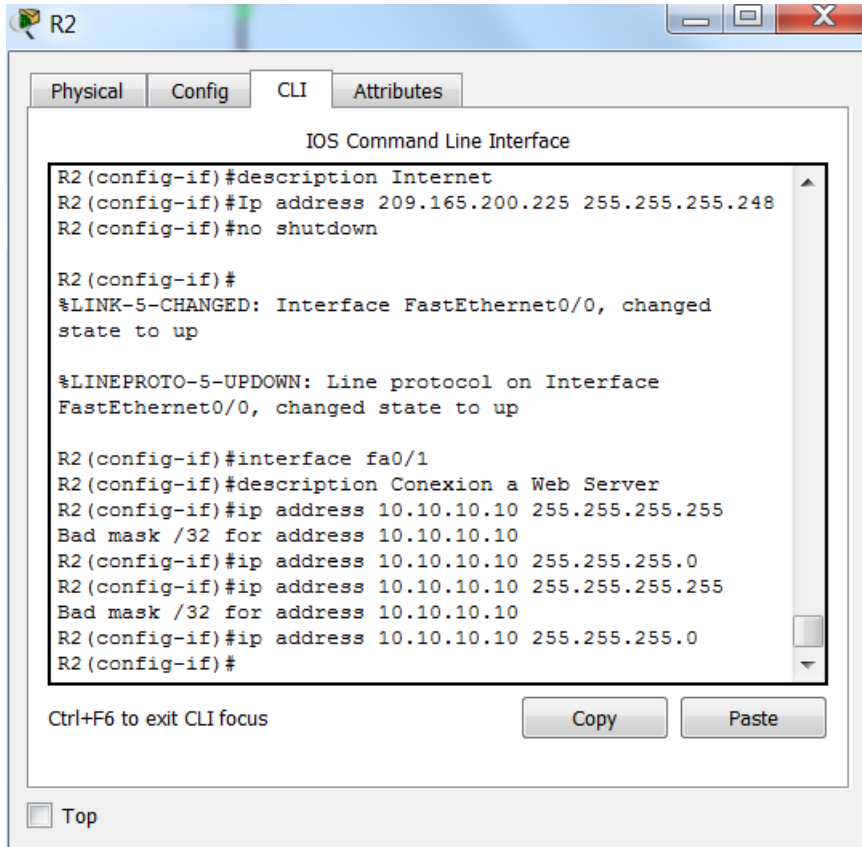


Figura 5. IP configurada en R2 para la interface FastEthernet 0/1

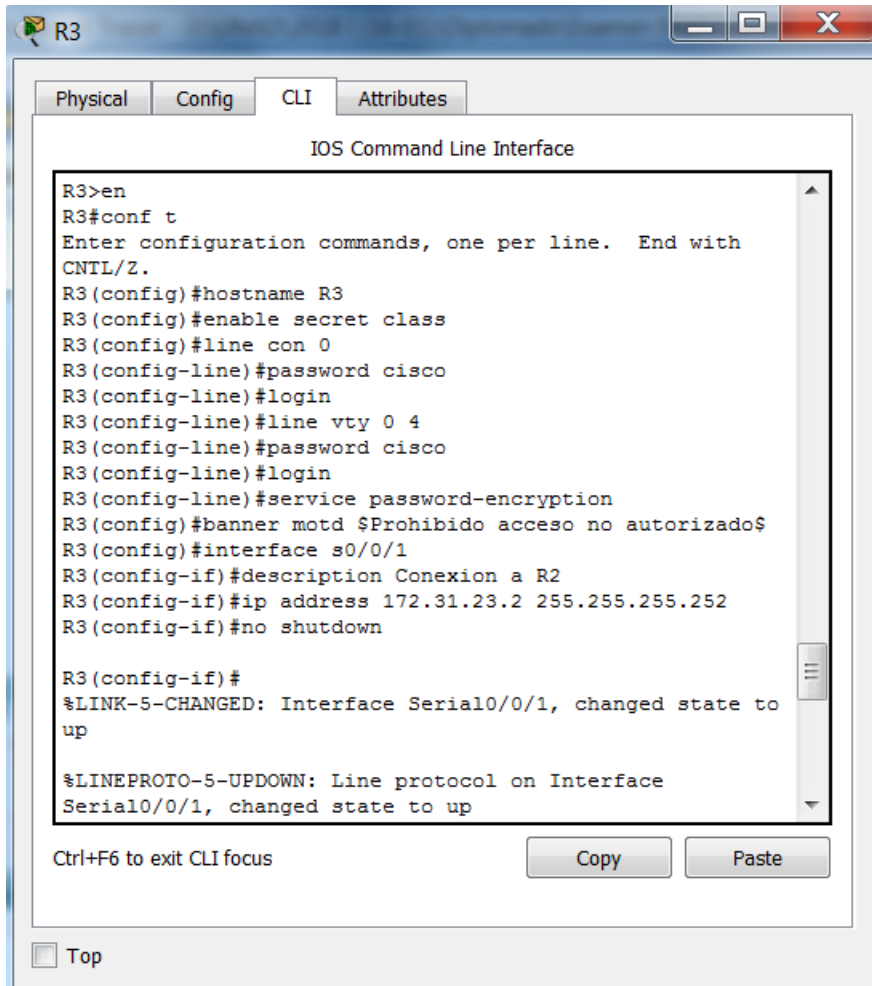


Figura 6. IP configurada en R3 para interface Serial 0/0/1

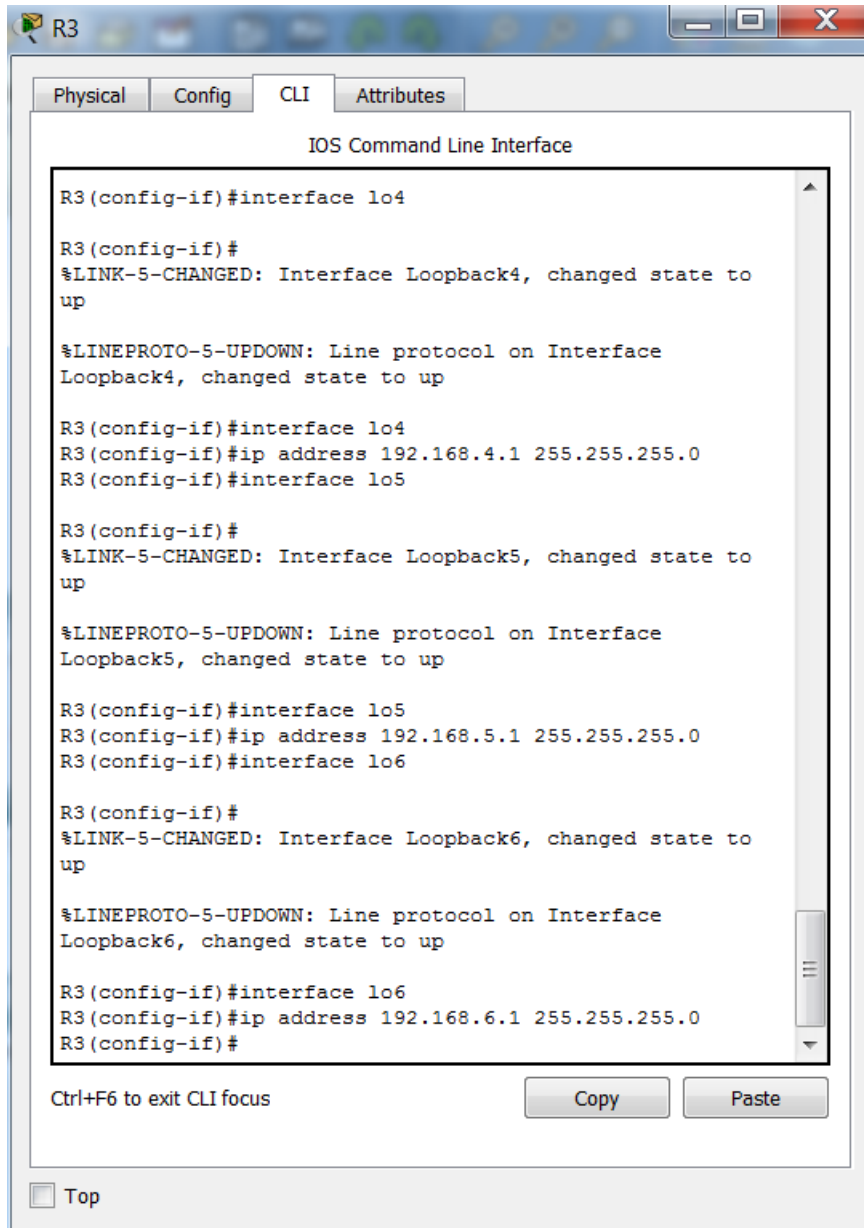


Figura 7. IP configurada en R3 para interfaces lo4, lo5, lo6

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

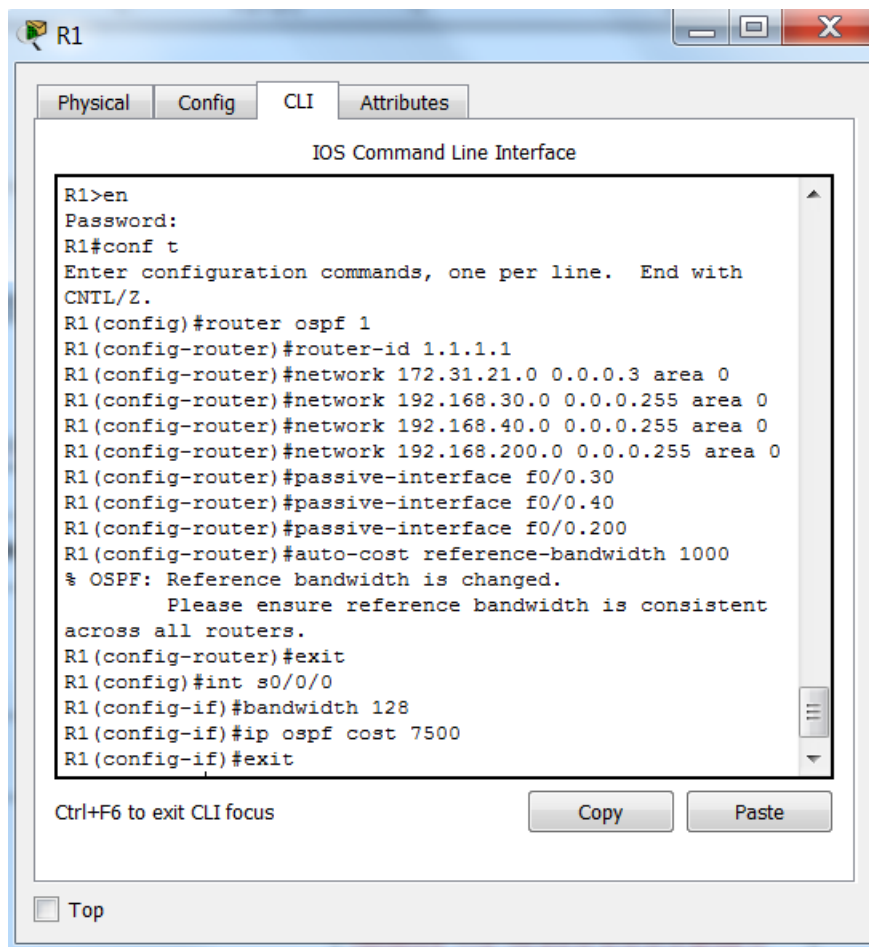


Figura 8. Router ID R1

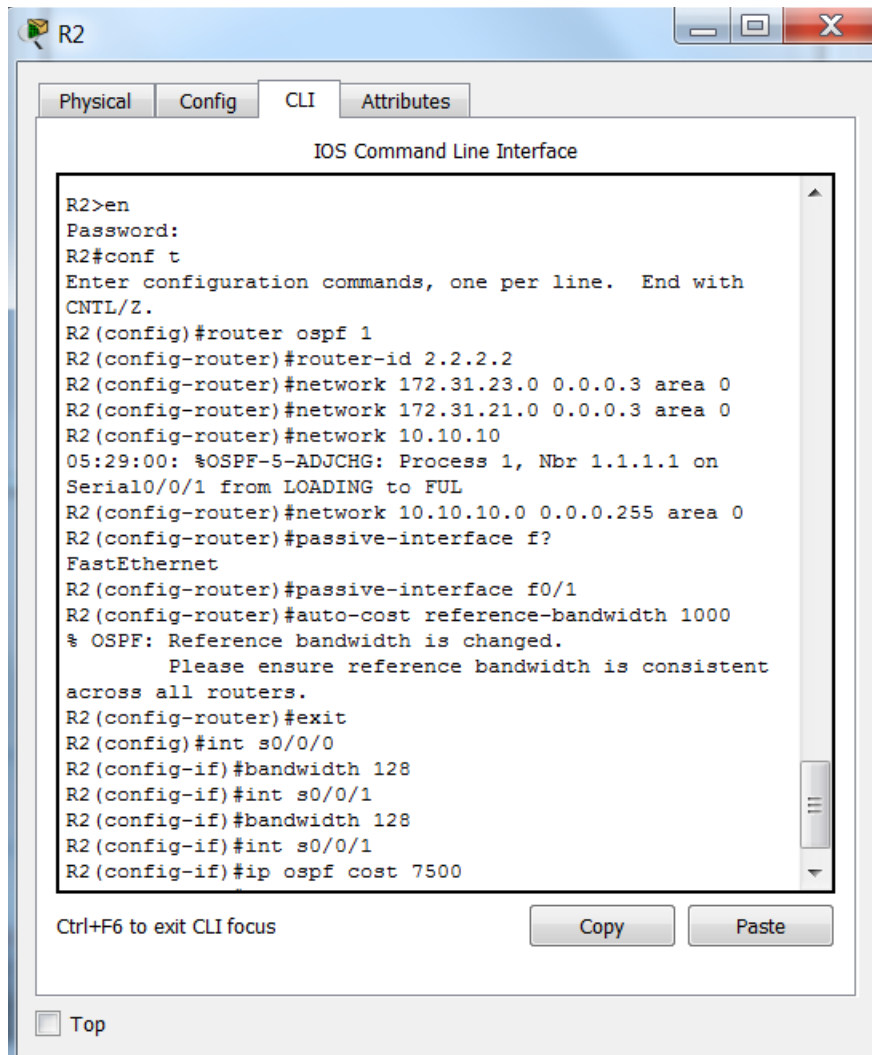


Figura 9. Router ID R2

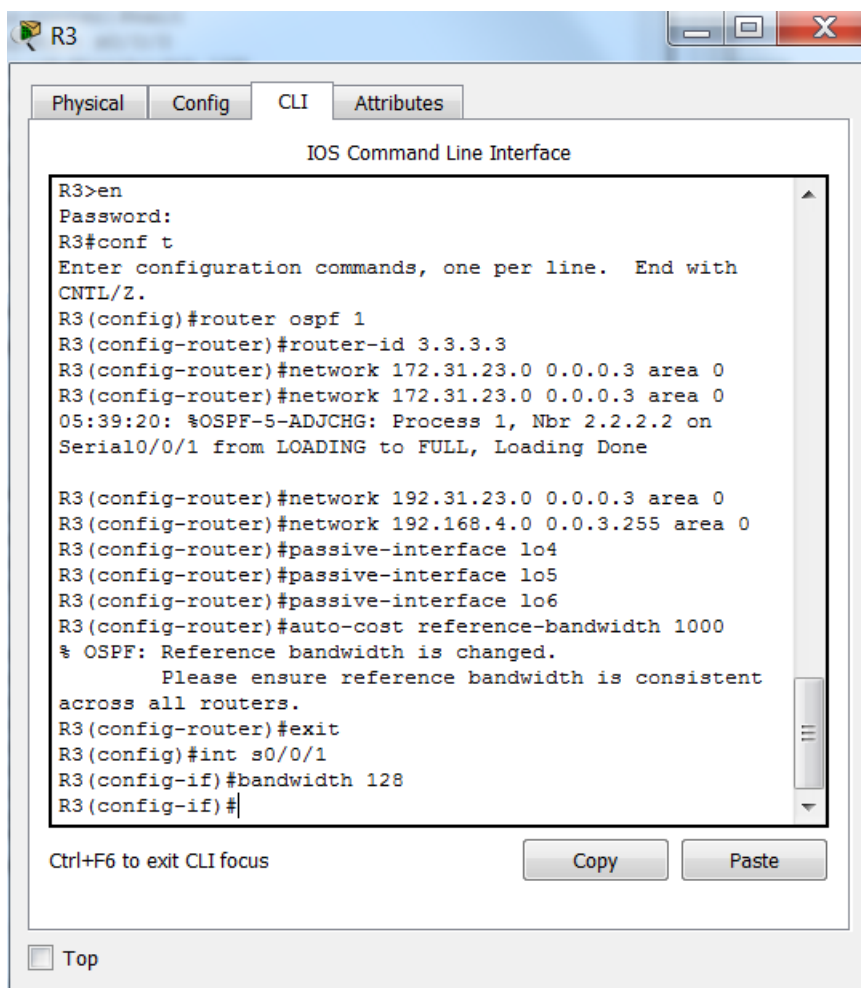


Figura 10. Router ID R3

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2.

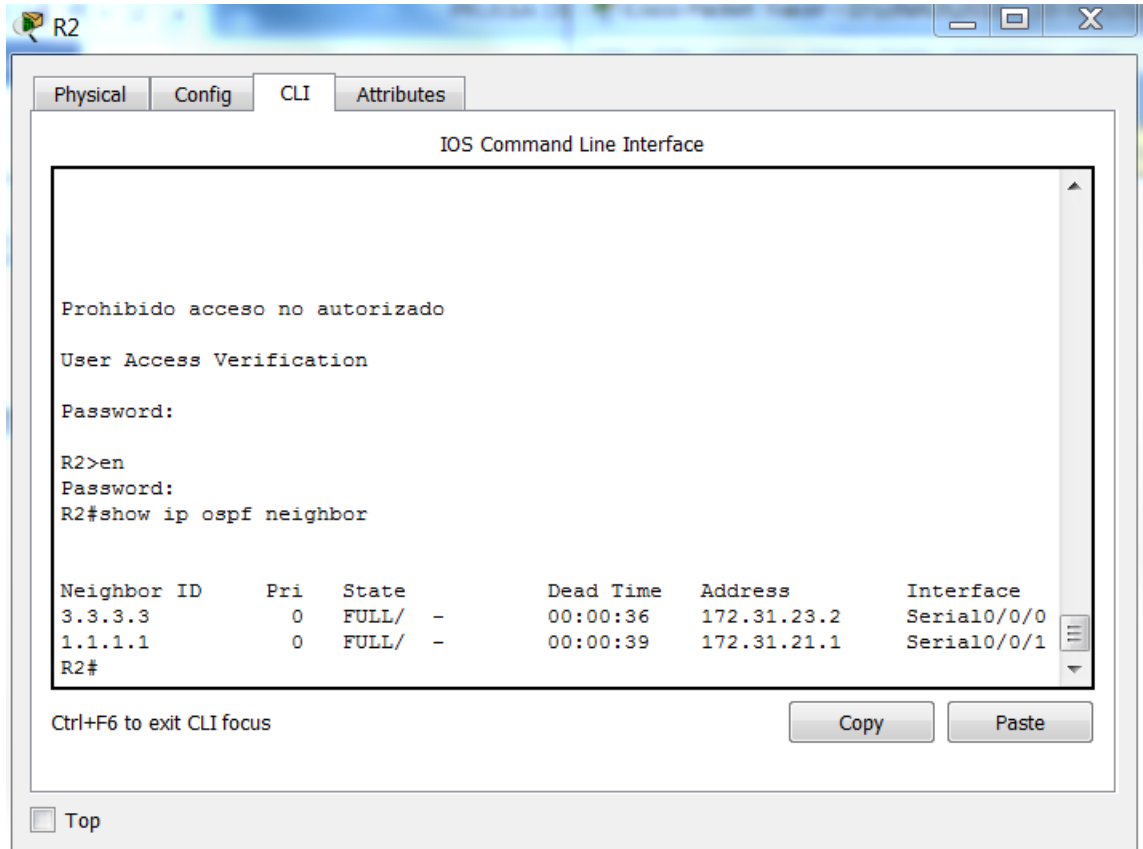


Figura 11. Tabla de enrutamiento en R2

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

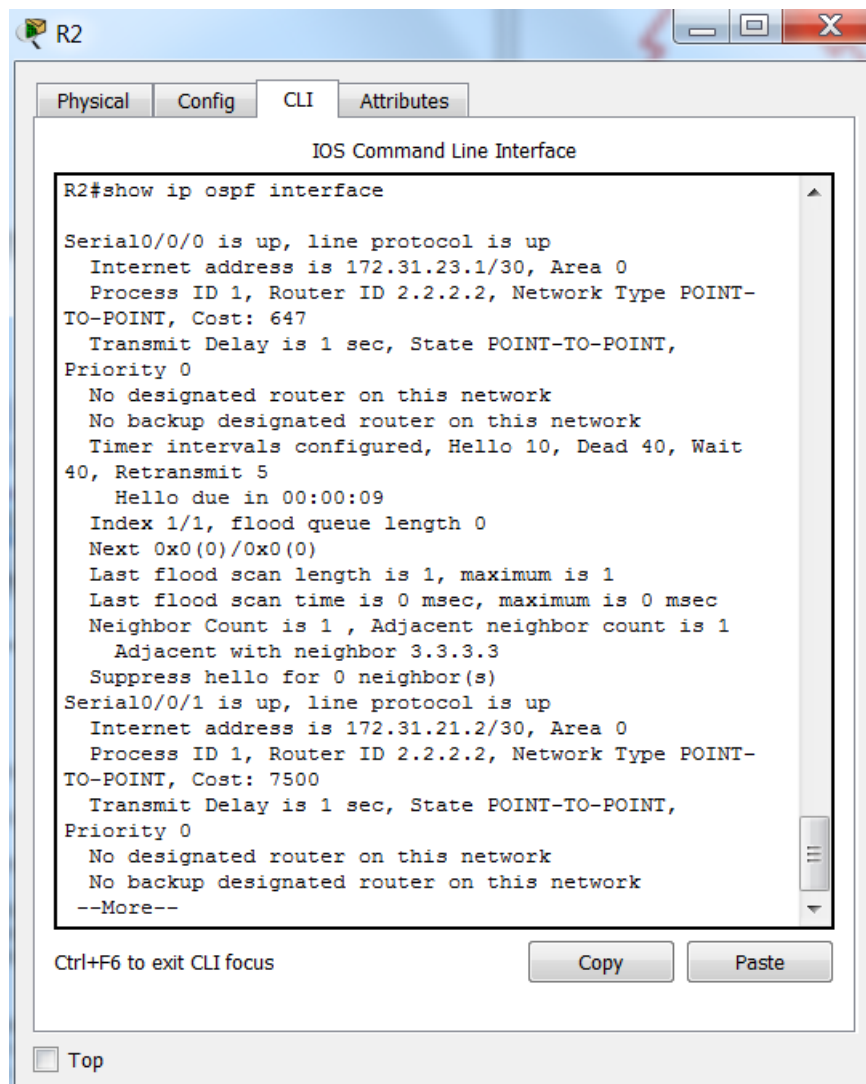


Figura 12. Lista de costo de cada interface de R2

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

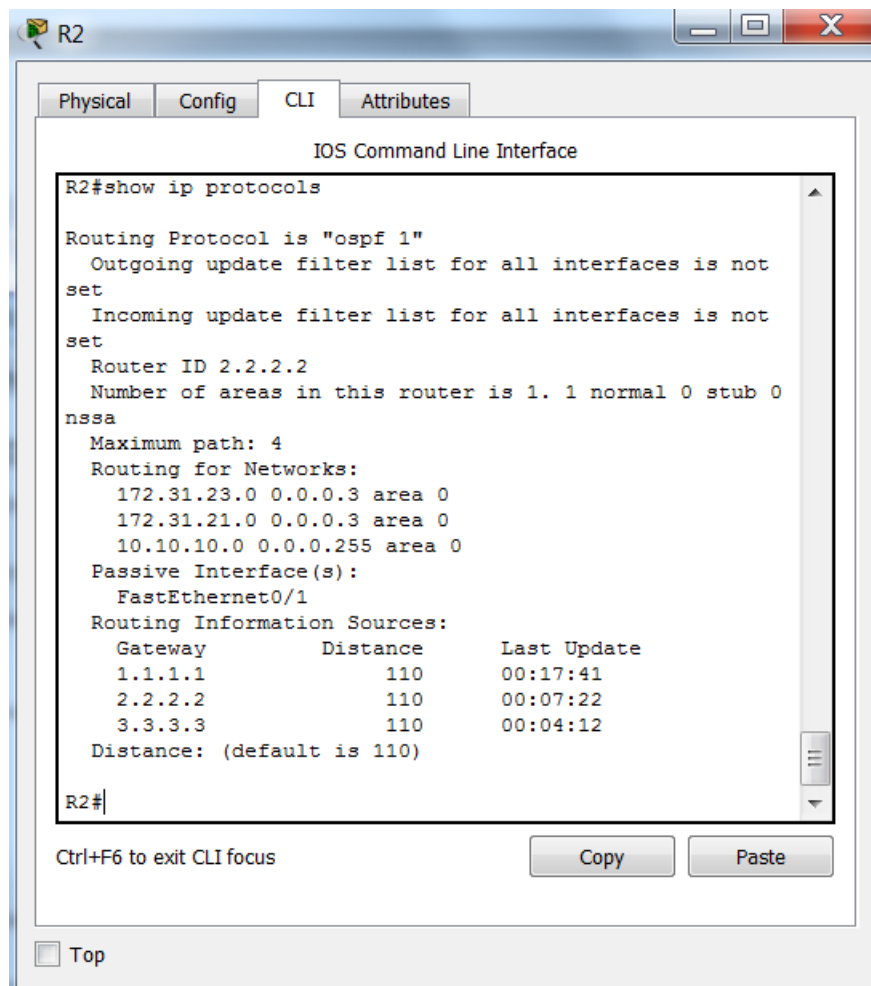


Figura 13. Show ip portocols en R2

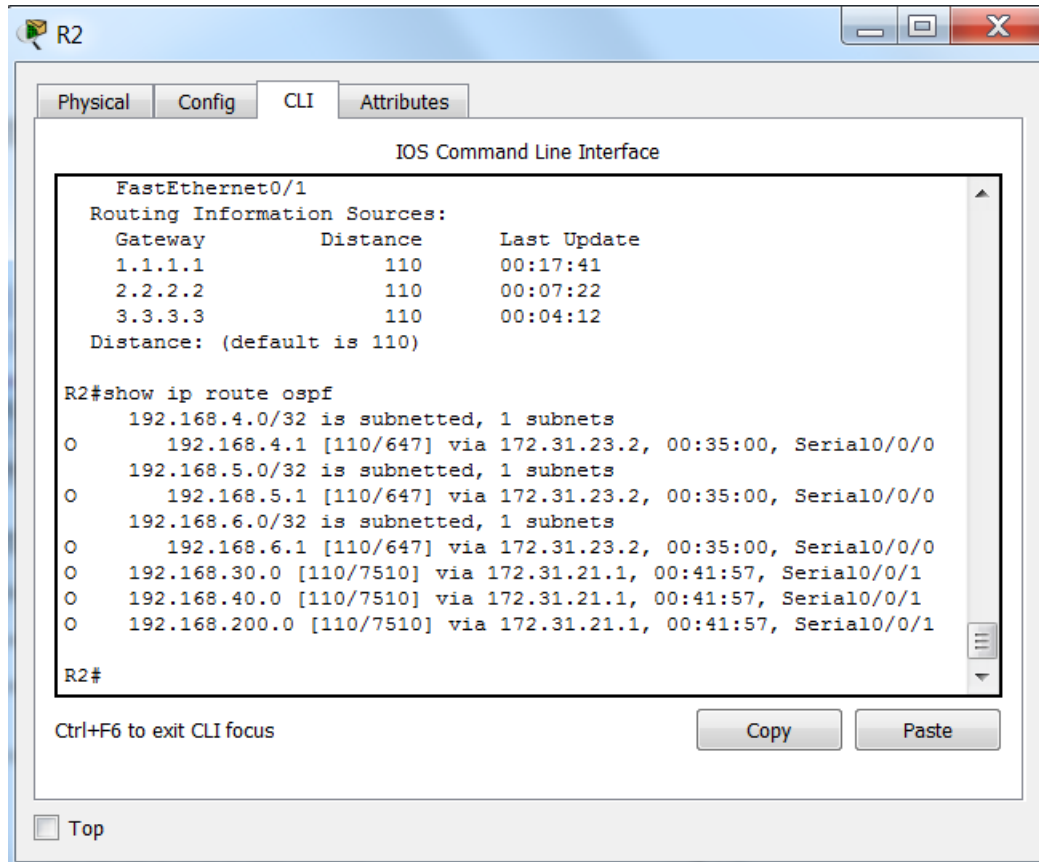


Figura 14. Show ip route ospf

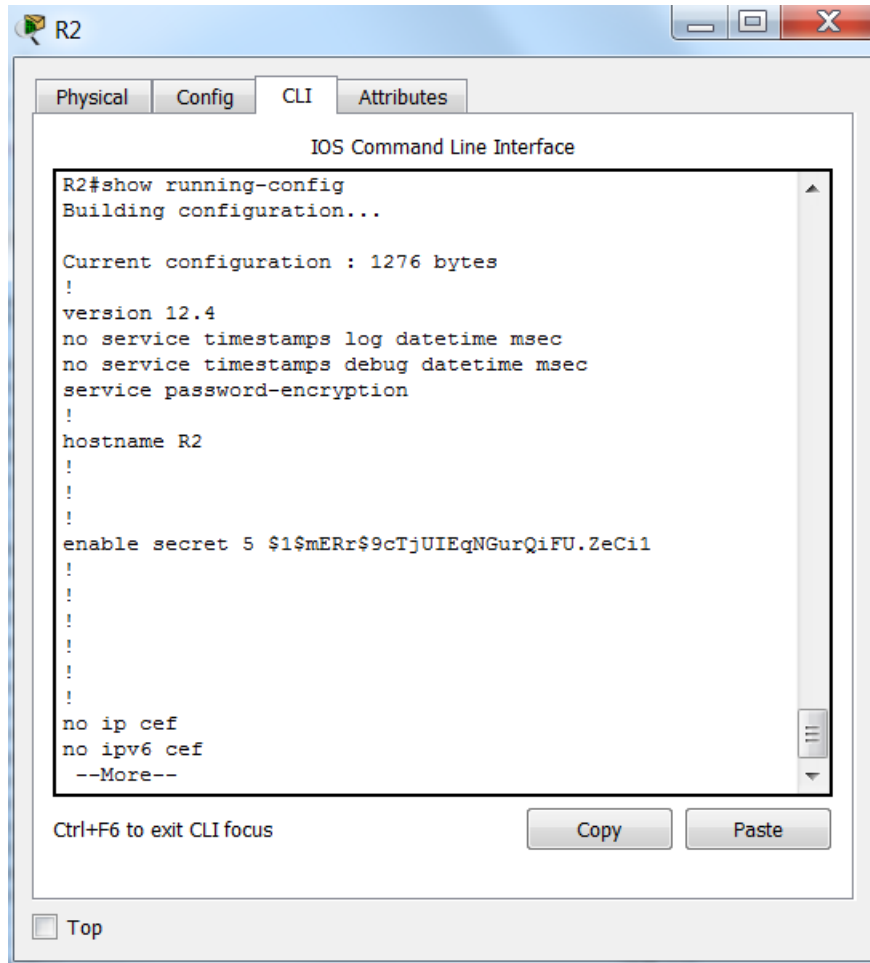


Figura 15. Show running-config

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

```
S1
Physical Config CLI Attributes
IOS Command Line Interface
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)#int vlan 200
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed
state to up

S1(config-if)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#ip default-gateway 192.168.200.1
S1(config)#interface fa0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface fa0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#interface range fa0/2, fa0/4-23, g0/1-2
S1(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
administratively down

Ctrl+F6 to exit CLI focus
Copy Paste
```

Figura 16. Configuración Vlan en S1

```
S3>en
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)#int vlan 200
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed
state to up

S3(config-if)#ip address 192.168.200.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.200.1
S3(config)#interface fa0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#interface fa0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#interface range fa0/2, fa0/4-24, g0/1-2
S3(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down

Ctrl+F6 to exit CLI focus
```

Figura 17. Configuración Vlan en S3

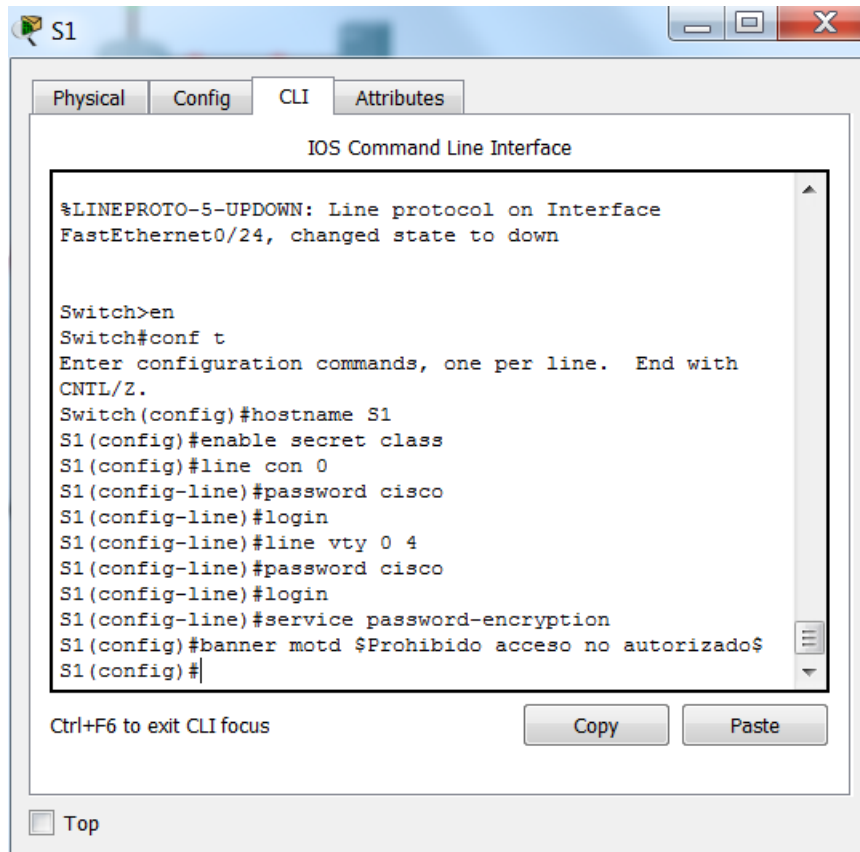


Figura 18. Configuración de seguridad en S1

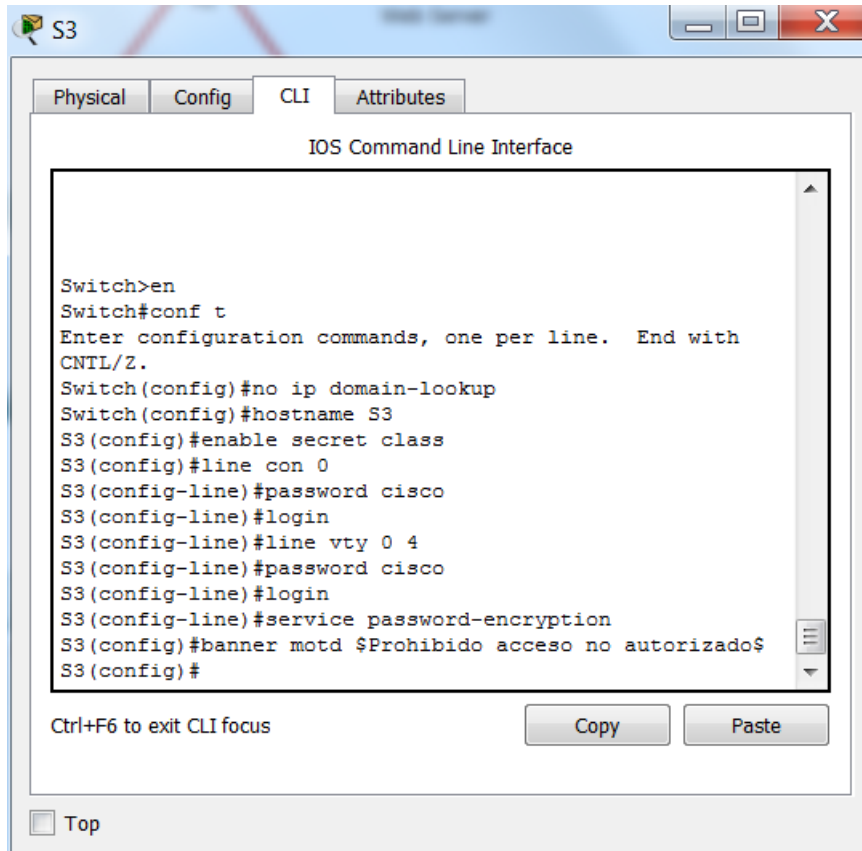


Figura 19. Configuración de seguridad en S3

4. En el Switch 3 deshabilitar DNS lookup

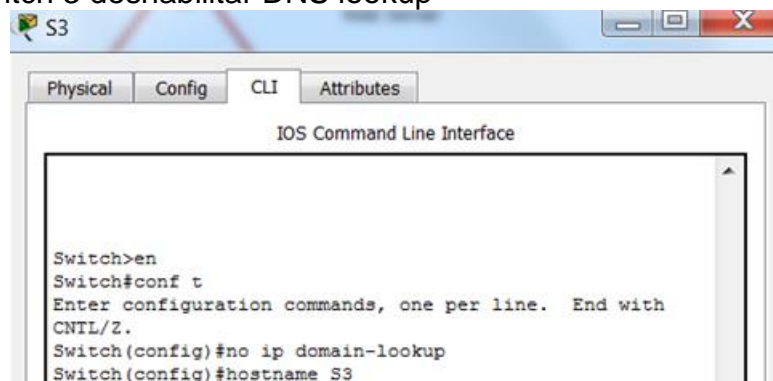


Figura 20. No ip domain-lookup en S3

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

```

S1(config-if)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shutdown

```

Figura 21. Ip configurada en S1

```
S3(config-if)#ip address 192.168.200.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
```

Figura 22. Ip configurada en S3

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

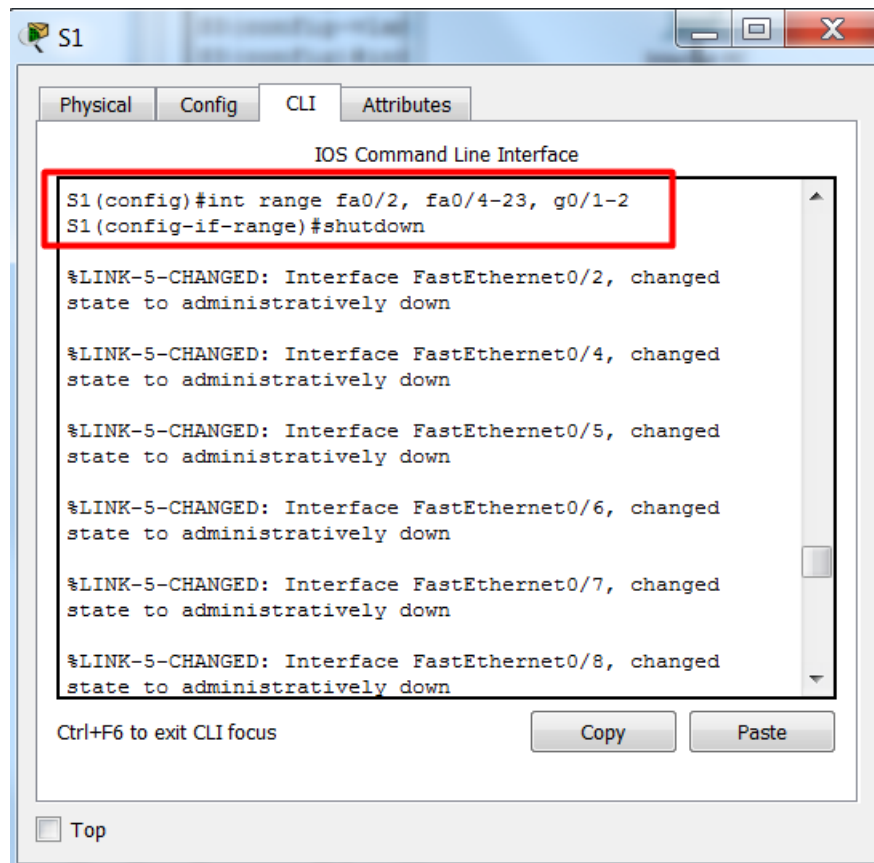


Figura 23. Shutdown para las interfaces sin uso en S1

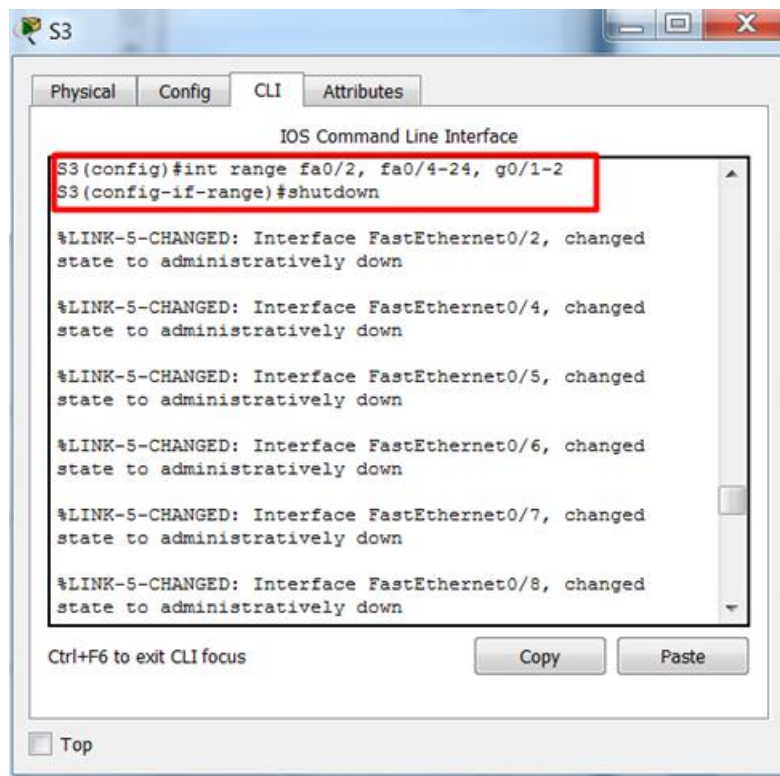


Figura 24. Shutdown para las interfaces sin uso en S3

- Implement DHCP and NAT for 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

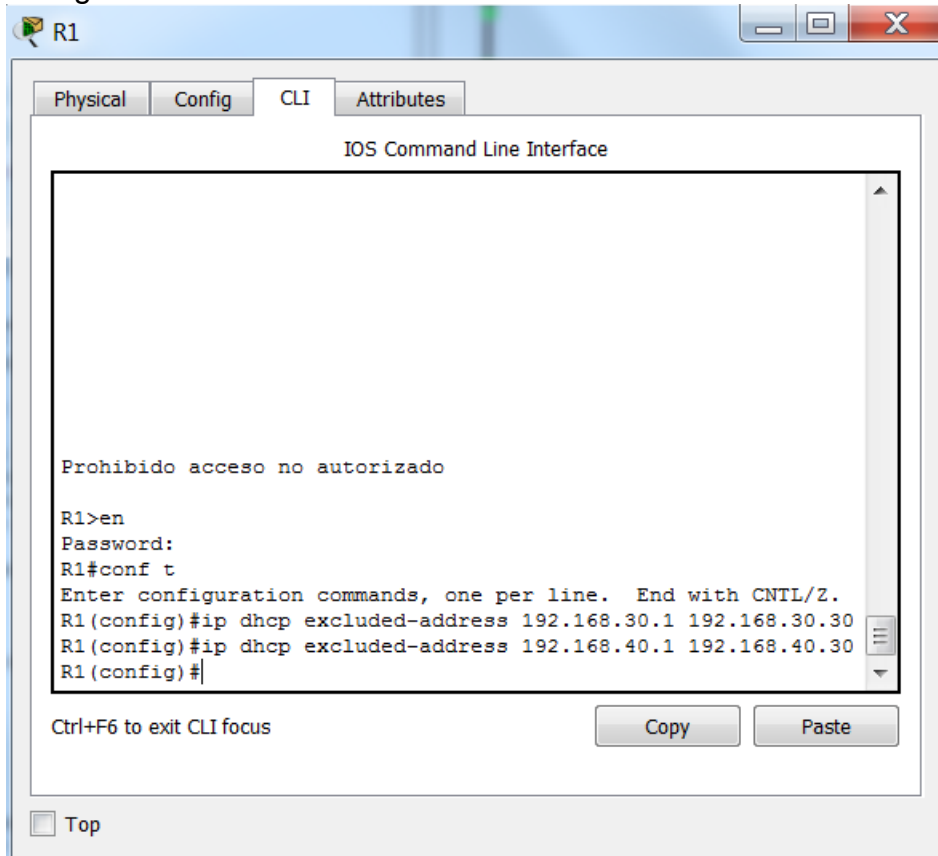


Figura 25. Reserva de las 30 primeras Ip

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

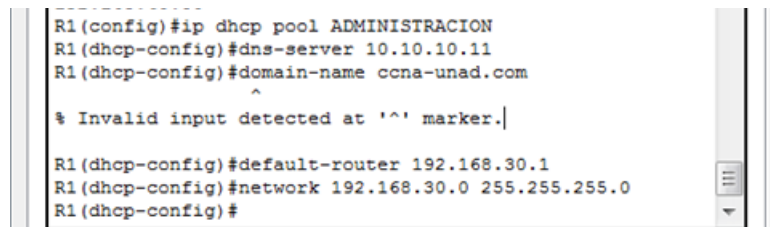


Figura 26. DHCP Vlan 30

Configurar DHCP pool para VLAN 40

Name: MERCADEO
DNS-Server: 10.10.10.11
Domain-Name: ccna-unad.com
Establecer default gateway.

```
R1(dhcp-config)#ip dhcp pool MERCADEO
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
^
% Invalid input detected at '^' marker.

R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#
```

Figura 27. DHCP Vlan 40

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

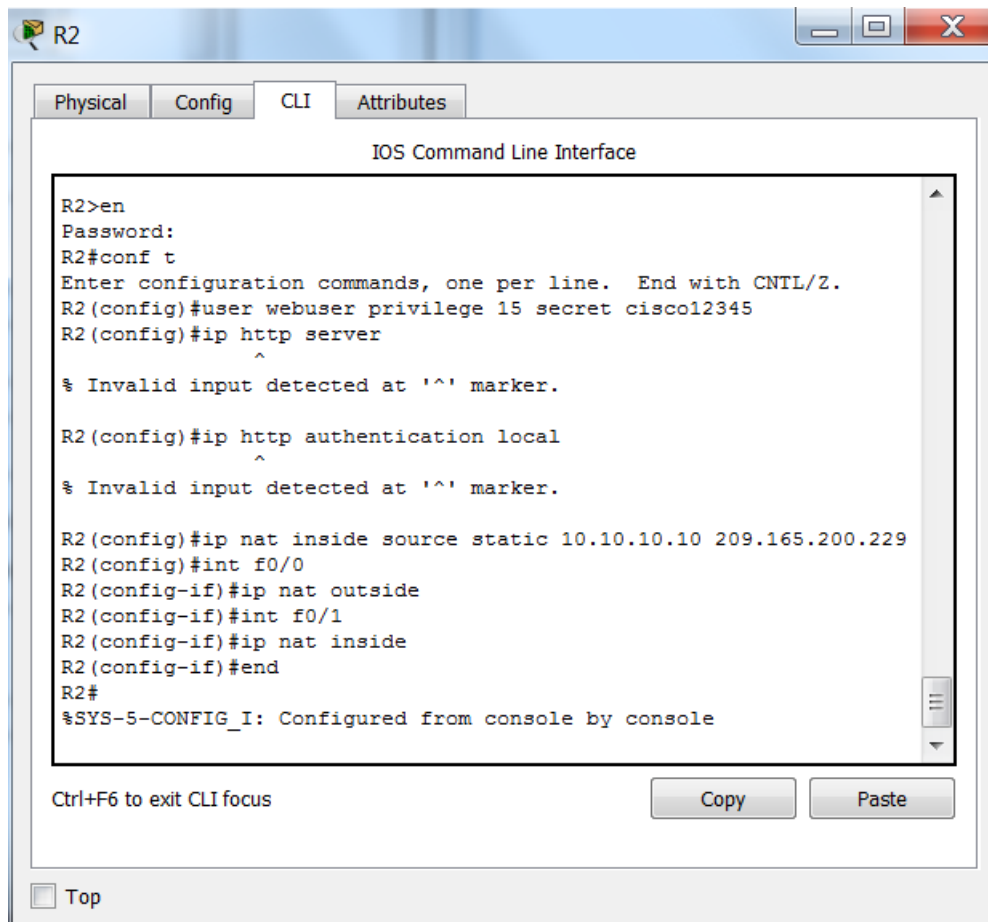


Figura 28. Configuración NAT en R2

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

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 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)#access-list 1 permit 192.168.4.0 0.0.3.255
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)#
```

Figura 29. Listas de acceso

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

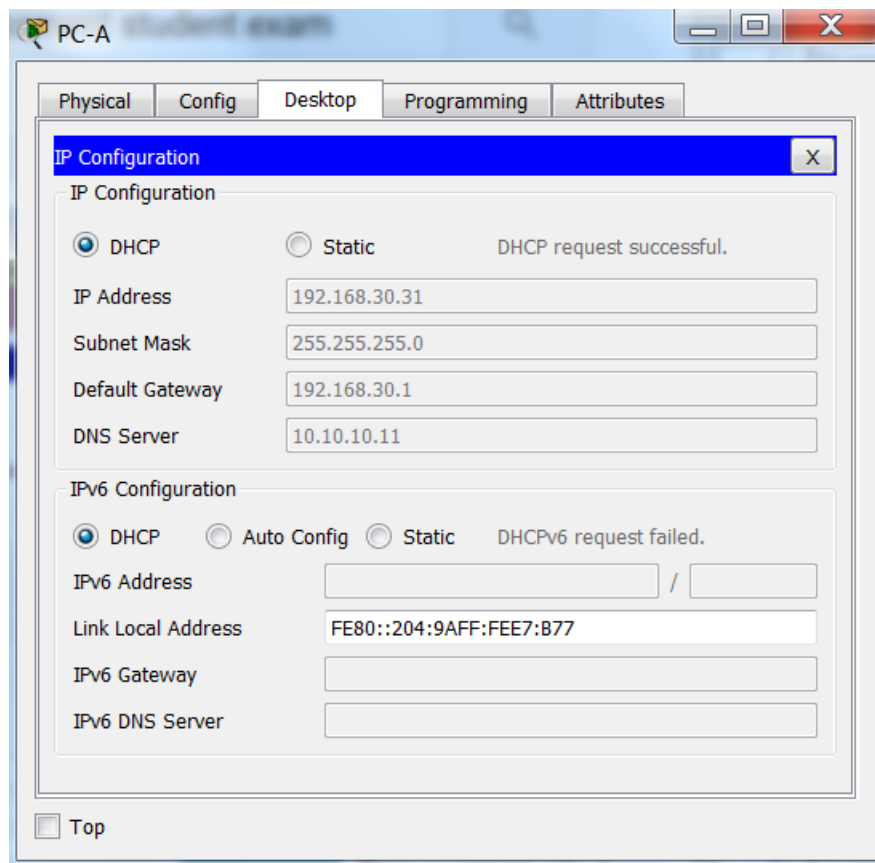


Figura 30. Ip DHCP configurada en PC-A

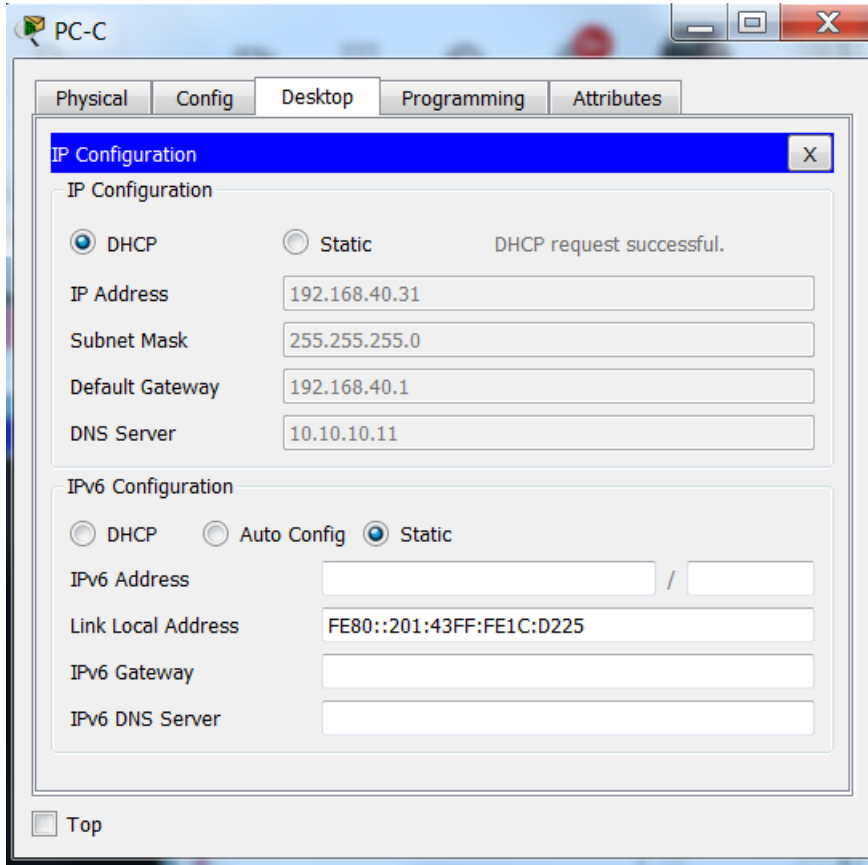


Figura 31. Ip DHCP configurada en PC-C

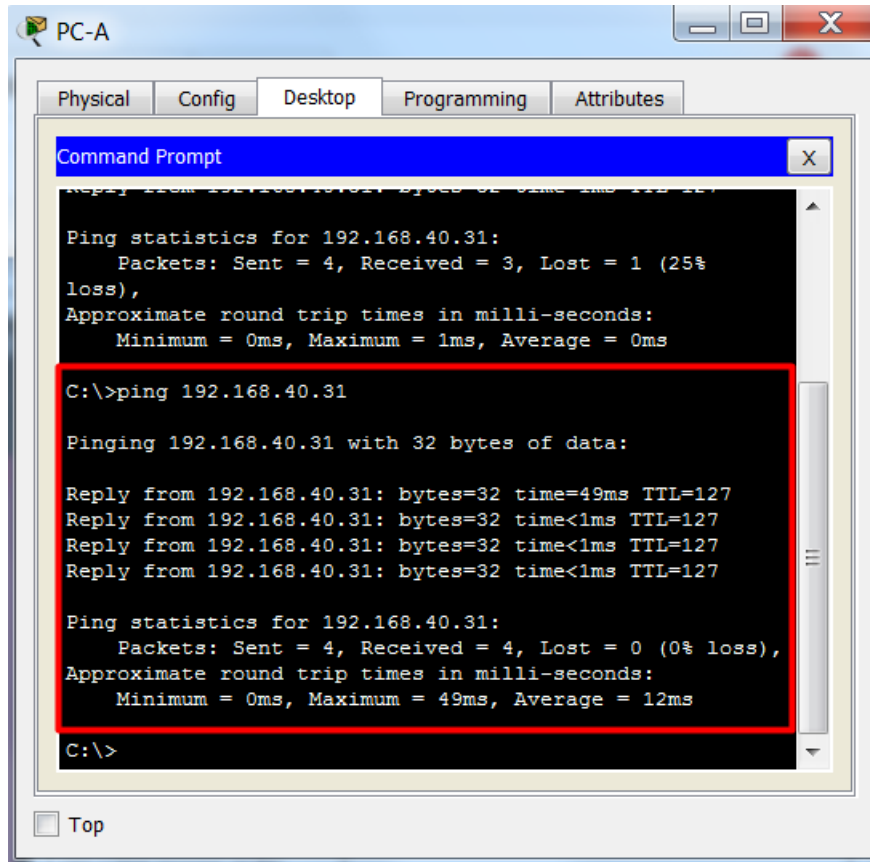


Figura 32. Ping satisfactorio desde PC-A hacia PC-C

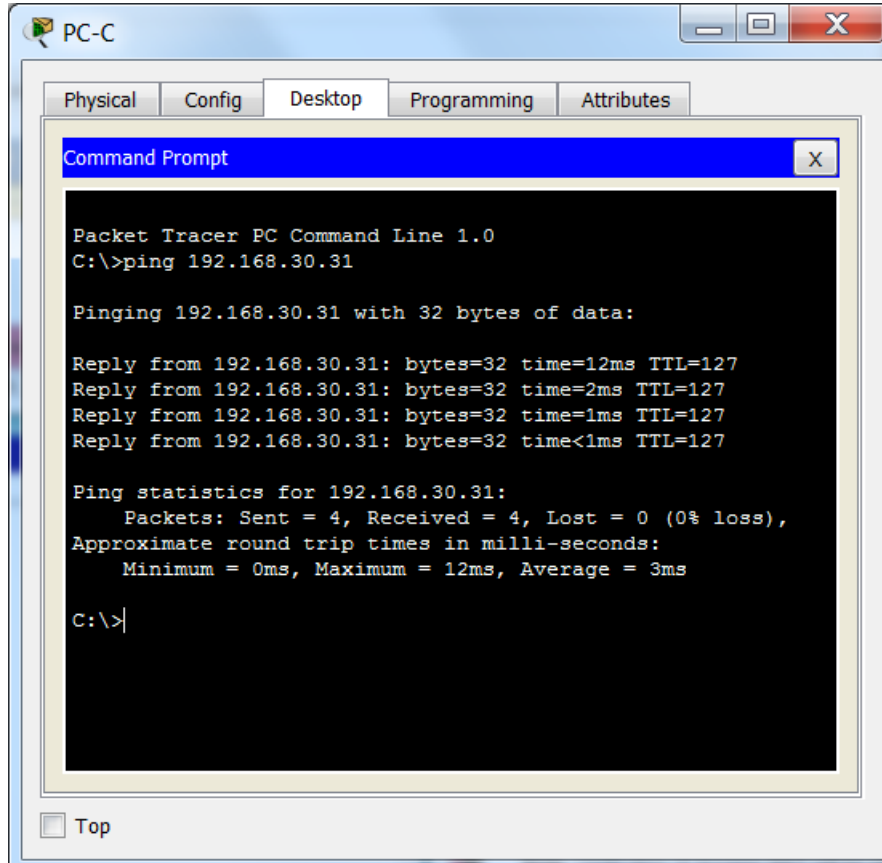


Figura 33. Ping satisfactorio desde PC-C hacia PC-A

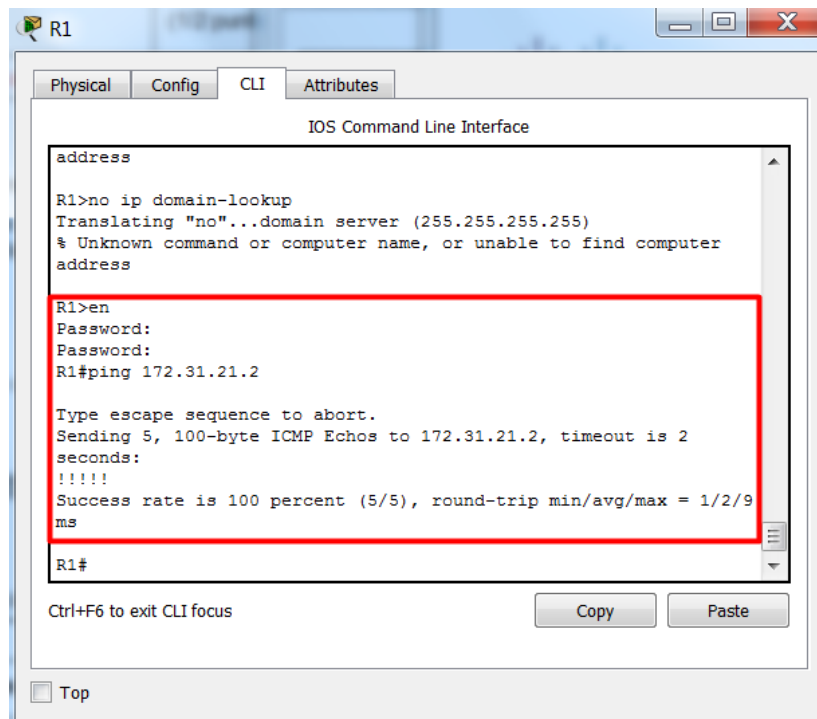


Figura 34. Ping satisfactorio desde R1 hacia R2

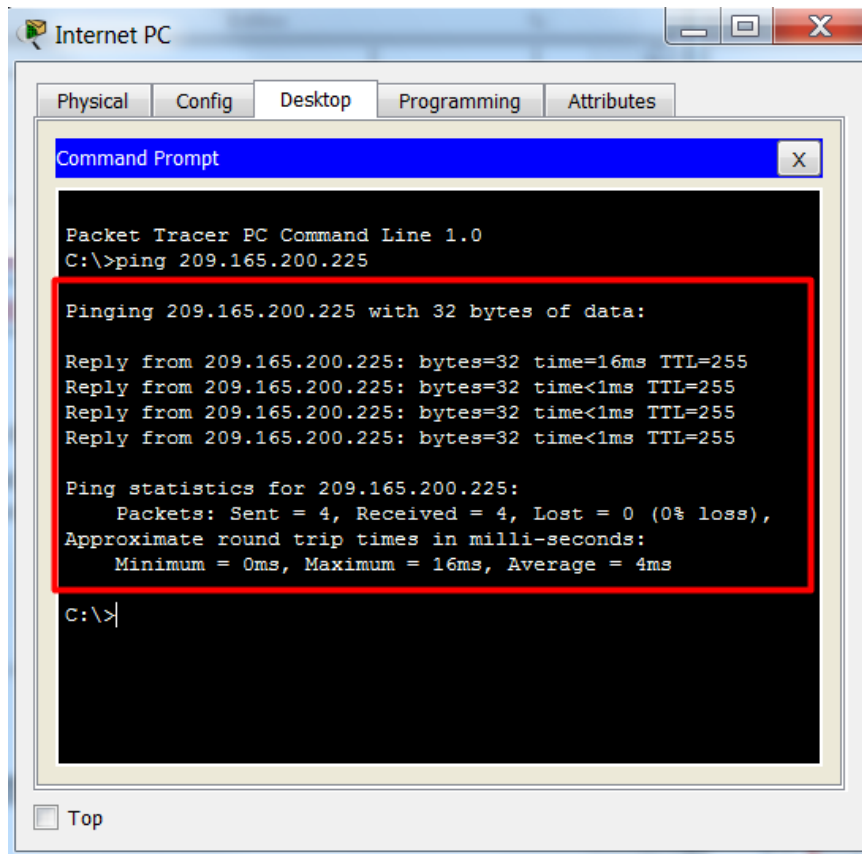


Figura 35. Ping satisfactorio desde Internet PC hacia R2

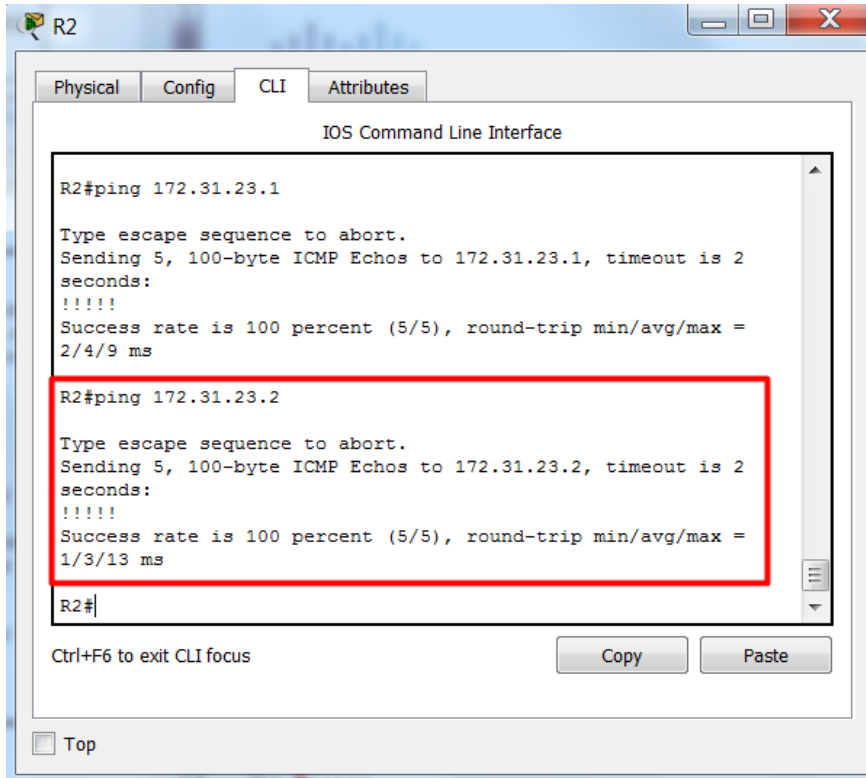


Figura 36. Ping satisfactorio desde R2 hacia R3

CONCLUSIONES

Se Desarrolló el caso de estudio ccna de la prueba de habilidades prácticas que forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, dando como resultado la comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Se planificó e implementó la topología de red establecida para la comunicación de la empresa de tecnología en sus 3 sucursales y se diseñó dicha topología en el software Packet tracer de la compañía Cisco.

Se aprendió a configurar redes Vlan, establecer seguridad en los switches y routers utilizados en la red que se implementó, se conoce los protocolos de enrutamiento OSPF y se verifican los procesos de comunicación y redireccionamiento del tráfico además de diagnosticar problemas tales como conflicto de direcciones ip y funcionamiento de las subredes con DHCP.

Se logra comprender y describir el propósito y los tipos de listas de control de acceso (ACL).

Se logra comprender y describir las operaciones y los beneficios de la traducción de direcciones de red (NAT).

BIBLIOGRAFIA

Cisco Systems, Inc. CCNA R&S Introduction to Networks [en línea]. CP CCNA1 I-2018. [EE UU]: Cisco, Feb. 2018 [citado 20 Mayo,. 2018] Disponible en Internet: <https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html>

Cisco Systems, Inc. CCNA R&S Routing and Switching Essentials [en línea]. CP CCNA2 I-2018. [EE UU]: Cisco, Feb. 2018 [citado 20 Mayo,. 2018] Disponible en Internet: <https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html>