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

EISON MONTOYA JIMENEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

CEAD MEDELLÍN

2018

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

Trabajo de grado

Efraín Alejandro Pérez

Tutor del curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

CEAD MEDELLÍN

MEDELLÍN

2018

TABLA DE CONTENIDO

TABLA DE FIGURAS

RESUMEN

Se ha dispuesto a realizar el desarrollo de un componente practico, dirigido a la implementación y el diseño de una red LAN/WAN. Utilizando las debidas técnicas de configuración de routing y swiching. Permitiendo desarrollar así un sistema de red funcional y eficiente. Con unas funciones y características definidas y programadas que facilitan la utilización y rendimiento de una red.

Se realizan di ententes tipos de configuraciones y maneras de implementar una red, tales como la configuración de red con IPv4 y con IPv6 implementando protocolos como los DHCP y NAT para la IPv4 y configuración como la OSPFv2.

Se realiza unas capturas de pantalla de los detalles de los para para la configuración de una red con el programa de simulación packet tracer.

INTRODUCCIÓN

Se ha dispuesto por parte de la UNAD el curso de profundización en redes LAN y WAN, surgiendo de esta manera un convenio entre la UNAD y la empresa CISCO, esto ha servido como complemento al conocimiento en el área de redes y telecomunicaciones, esto aplica como opción de grado y de esto surge el DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN).

En esta actividad final han propuesto tratar los temas: configuración de sistemas de red soportados en VLAN, configuración de control de ACL para IPv4, implementación de DHCP y NAT para IPv4, configuración OSPFv2

Para esta actividad hacemos uso de la herramienta de simulación cisco packet tracer, ya que esta herramienta nos ayuda a desarrollar la parte práctica a una escala muy similar a la realidad.

OBJETIVOS

Objetivo General

Desarrollar de manera satisfactoria todas las actividades propuestas por el DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN / WAN), obteniendo así todos los conocimientos que nos ofrece el diplomado y poniéndolos en práctica por medio del simulador packer tracer

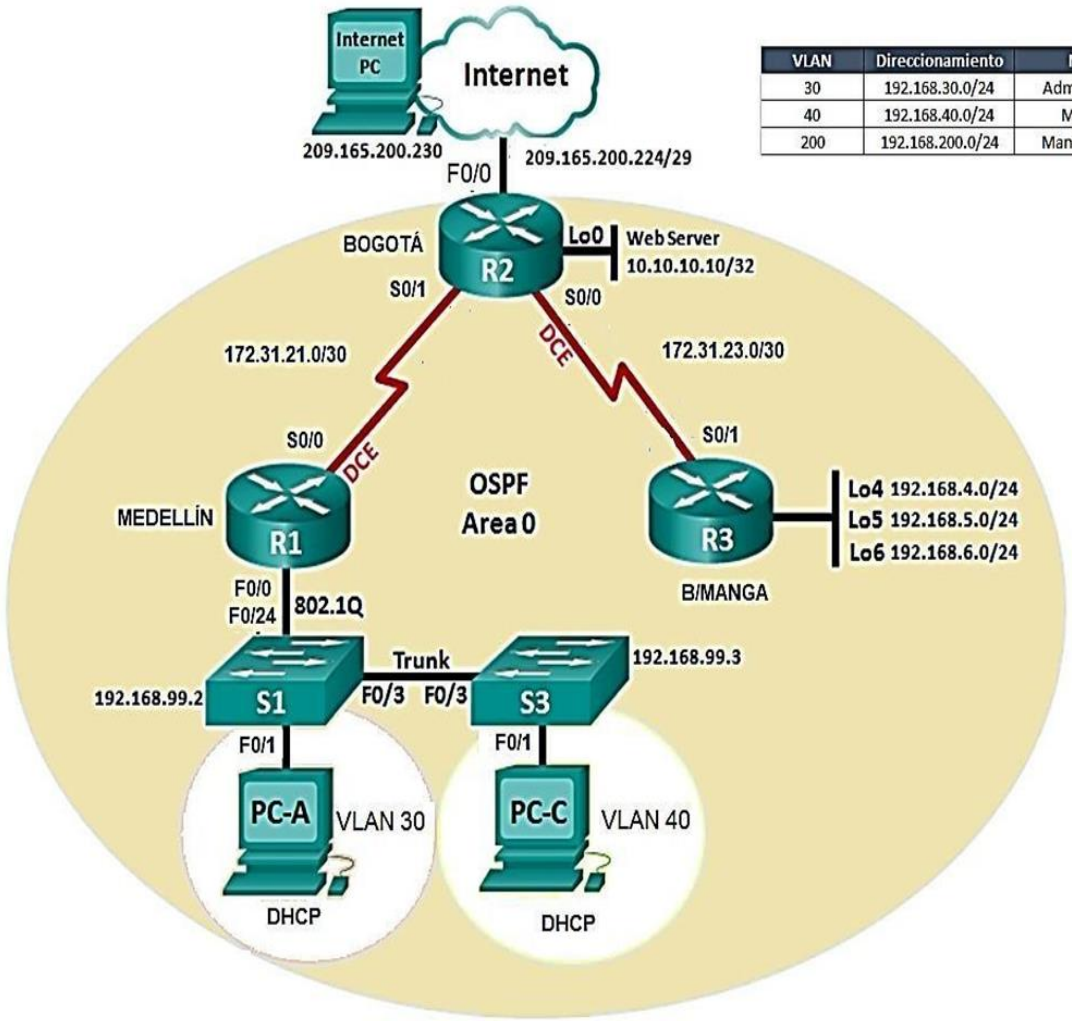
Objetivos Generales

- Realizar configuraciones de routers y swiches resolviendo problemas relacionados con la configuración de estos dispositivos.
- Configurar y controlar ACL para el protocolo de conexión IPv4 y descubrir los medios utilizados para transportar datos a través de la red.

1. Descripción Del Escenario Propuesto Para La Prueba De Habilidades

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 la 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

Figura 1

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

2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

OSPFv2 área 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

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2
- 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.

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

4. En el Switch 3 deshabilitar DNS lookup

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

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

7. Implementar DHCP and NAT for IPv4

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

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.

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

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.

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.

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

Desarrollo Del Proyecto

Solución Prueba de Habilidades Prácticas CCNA

Armado de la Red

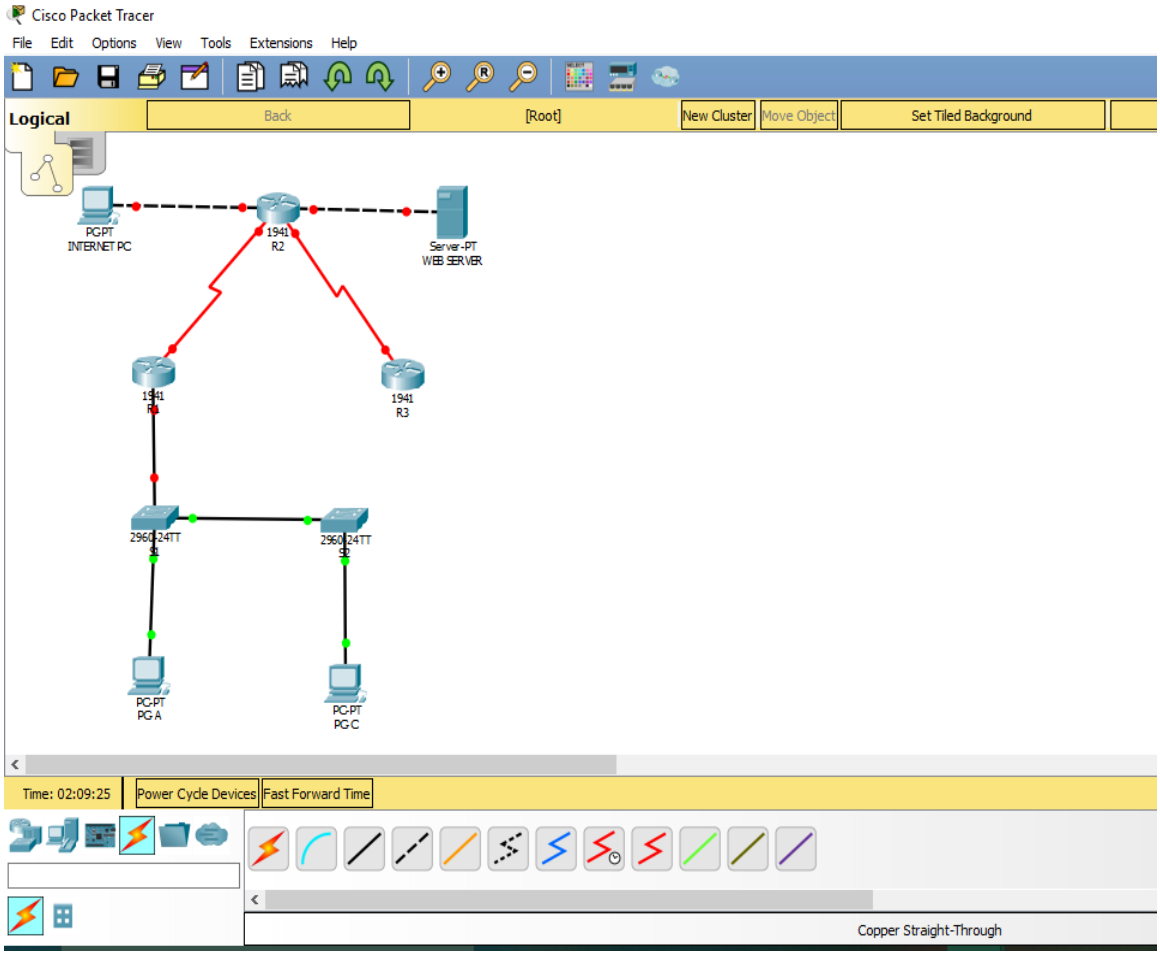


Figura 2

Inicializando y Cargando los Routers y Switches

Se procede a borrar las configuraciones de inicio y a recargar los dispositivos.

Para los Routers las tareas que realizo a continuación son: borrar el archivo de configuración de inicio en todos los enrutadores. Del mismo modo se procede a recargarlos.

Router R1

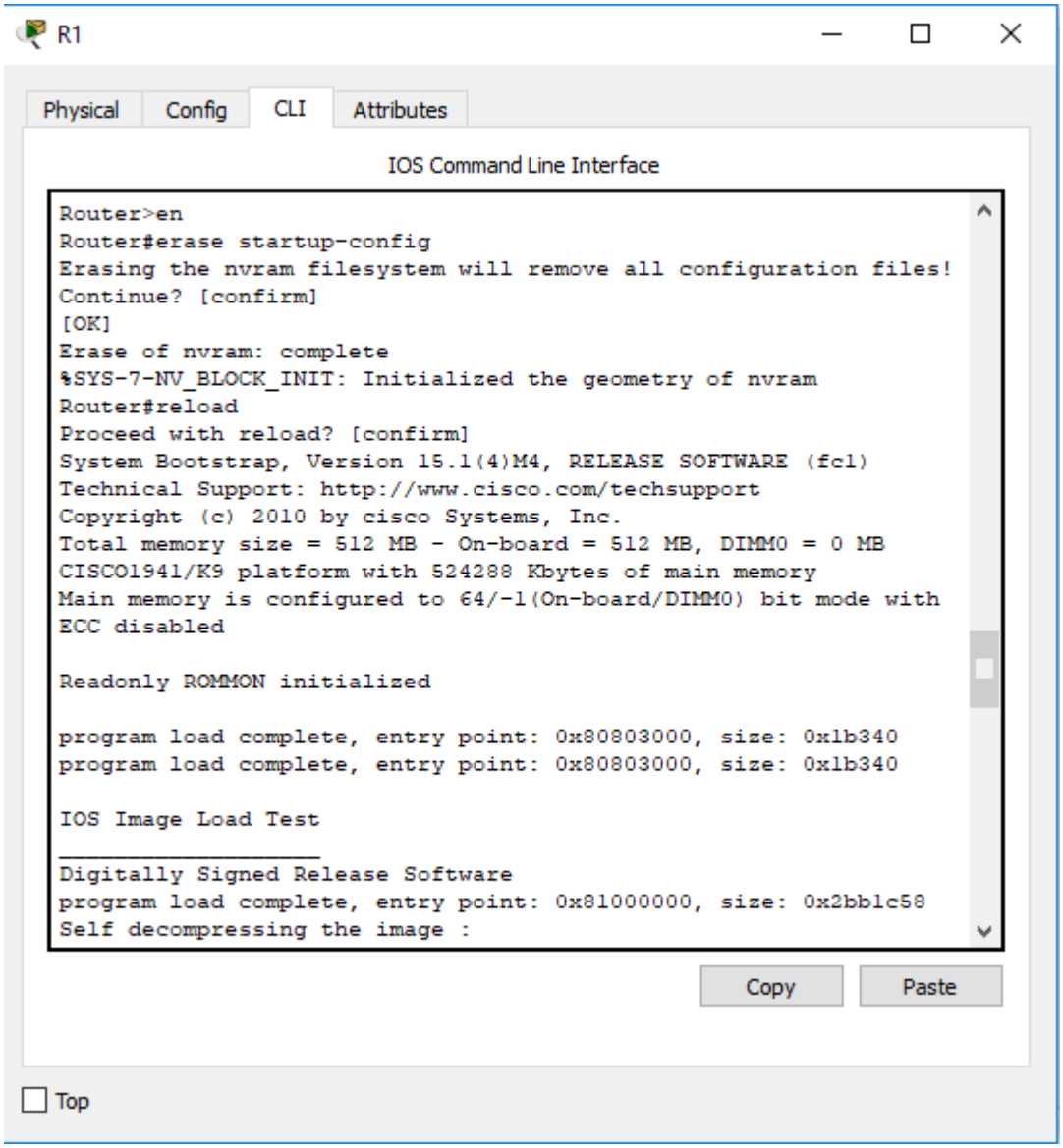


Figura 3

Router R2

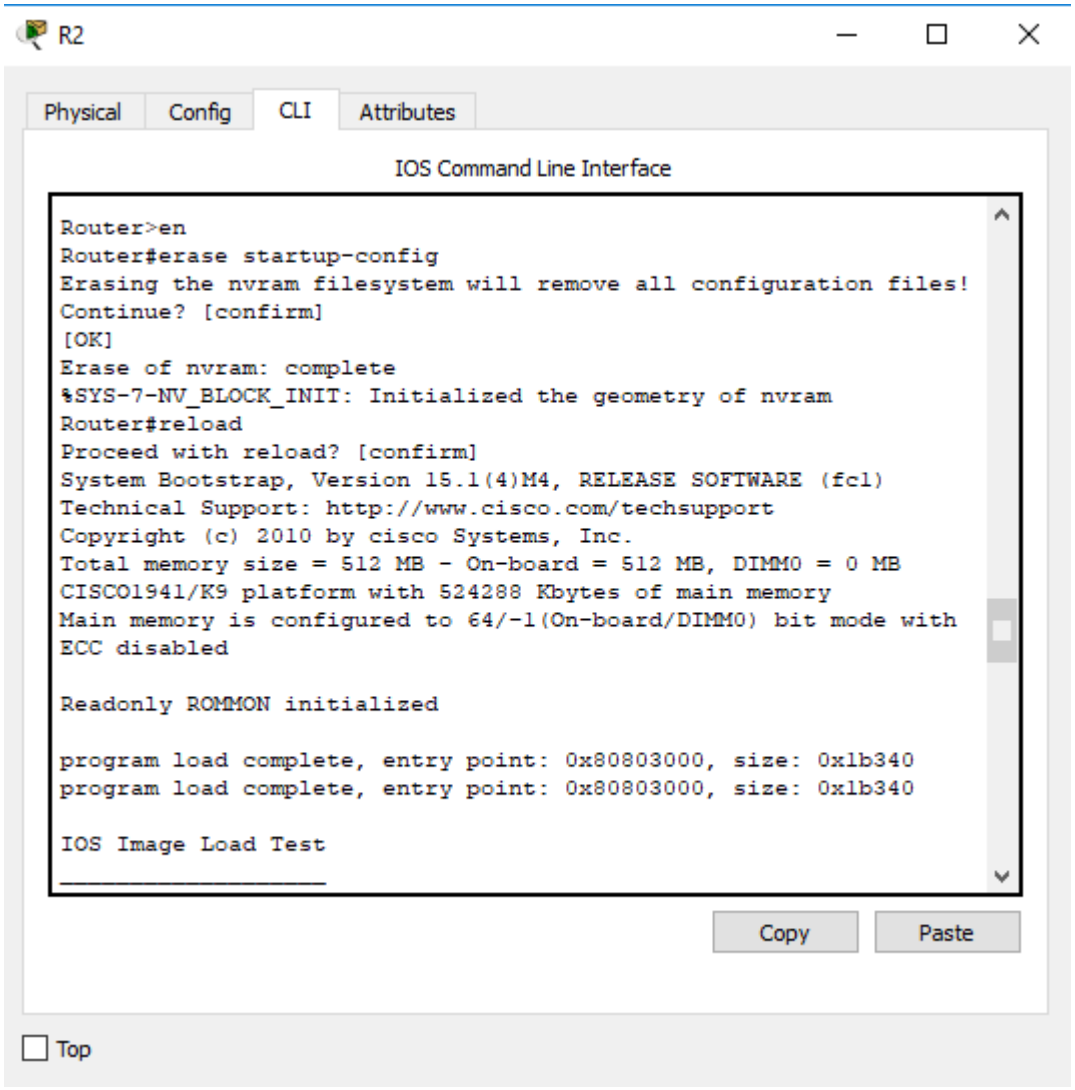


Figura 4

Router R3

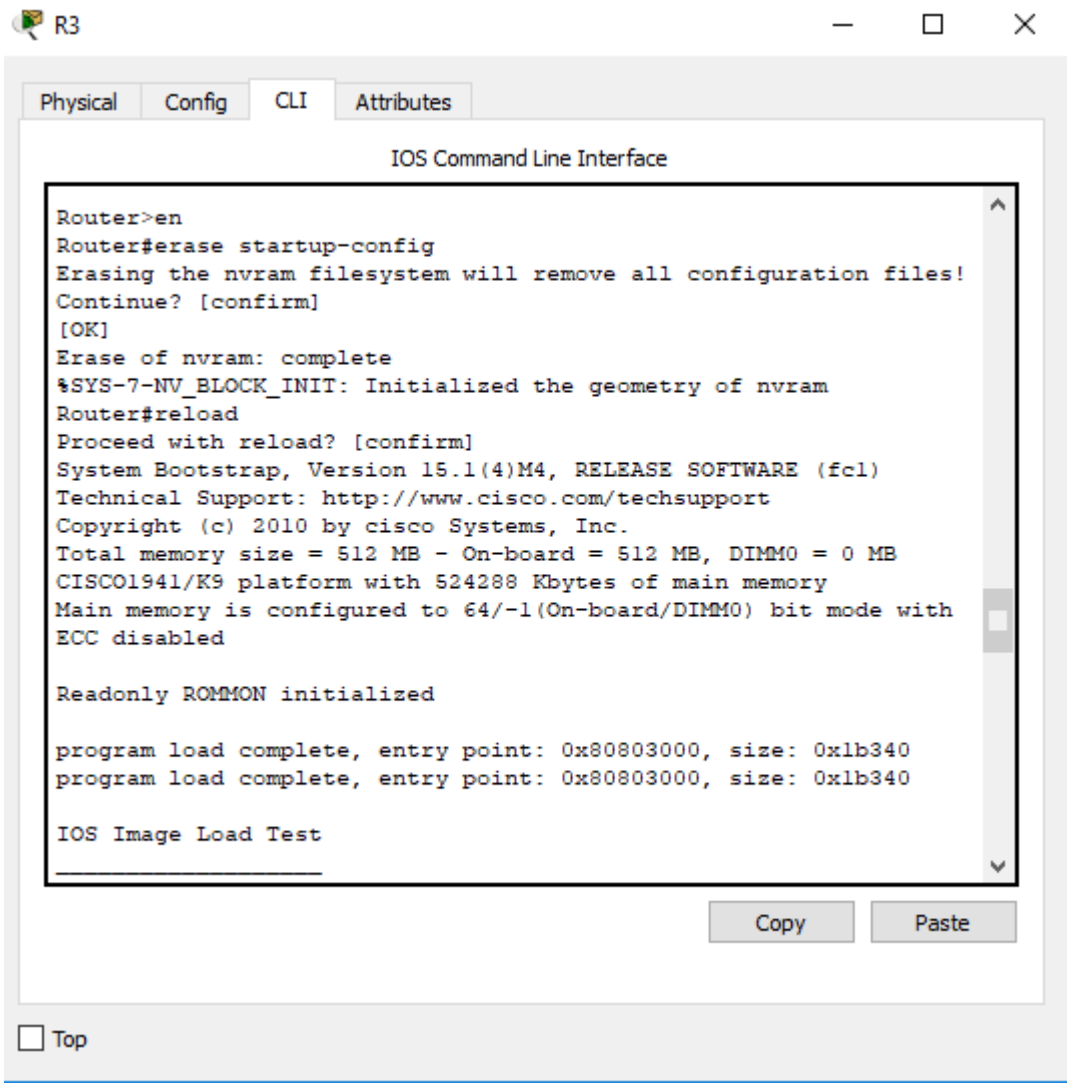


Figura 5

Se procede a borrar el archivo startup-config en todos los switches y se elimina la antigua base de datos VLAN.

Switch S1

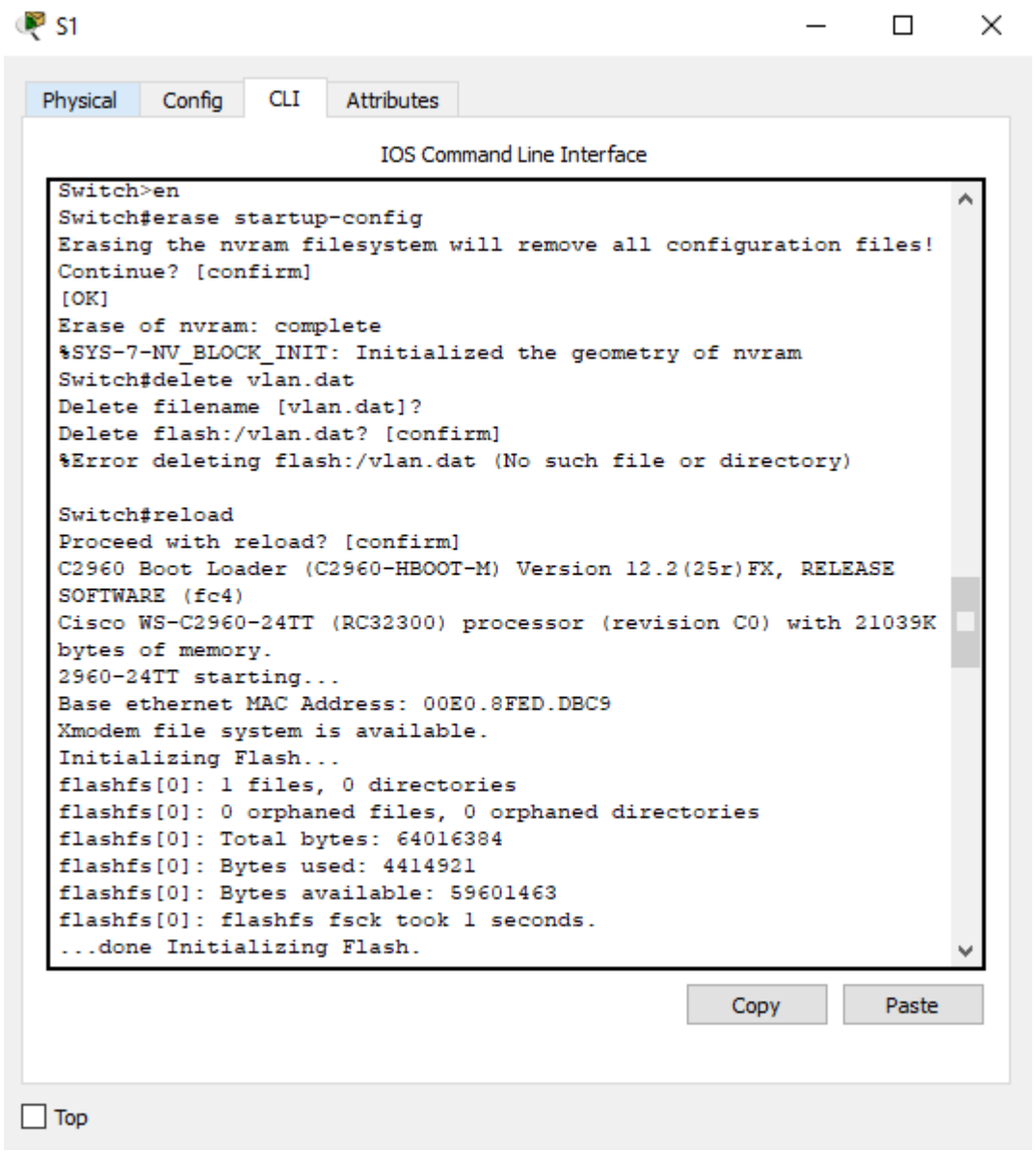


Figura 6

Switch S2

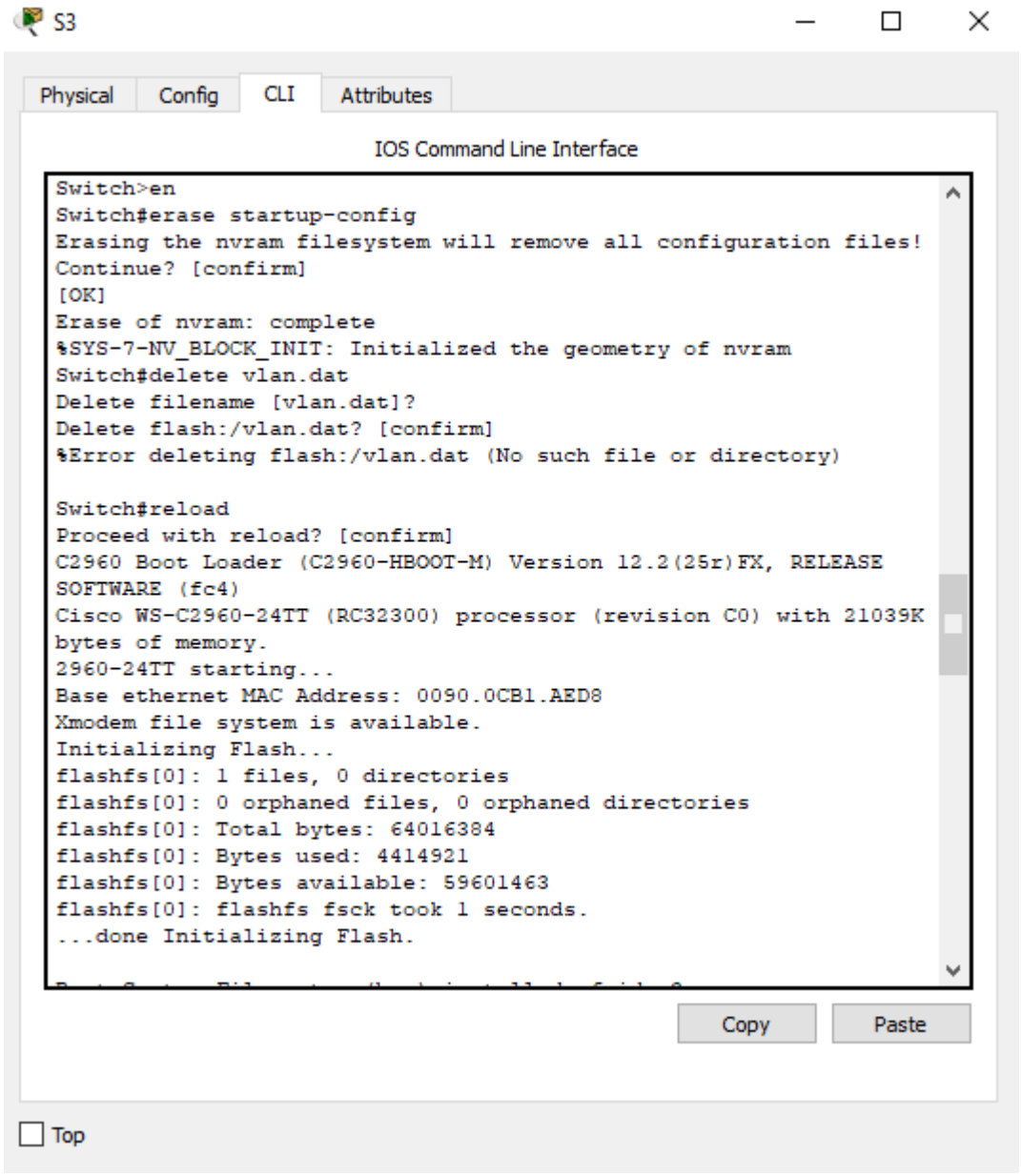


Figura 7

Configuración Básica de los Dispositivos “Direccionamiento IPV4”

Tareas de configuración para la Internet PC incluyendo: IP Address, Subnet Mask, Default Gateway.

Configurando la Internet PC.

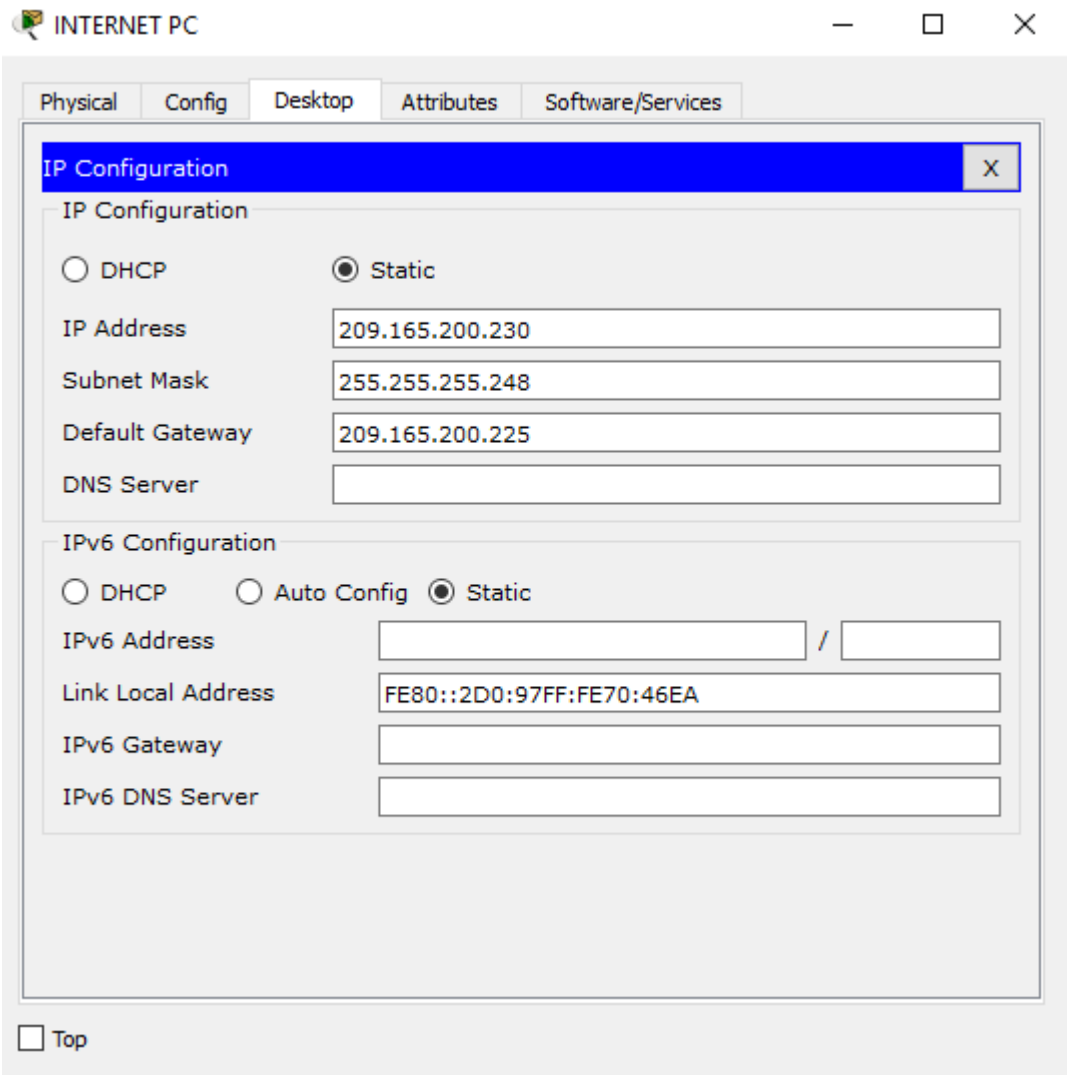


Figura 8

Tareas de configuración para R1 incluyendo: Disable DNS lookup, Nombre, Interface S0/0/0, Default route.

Configurando R1.

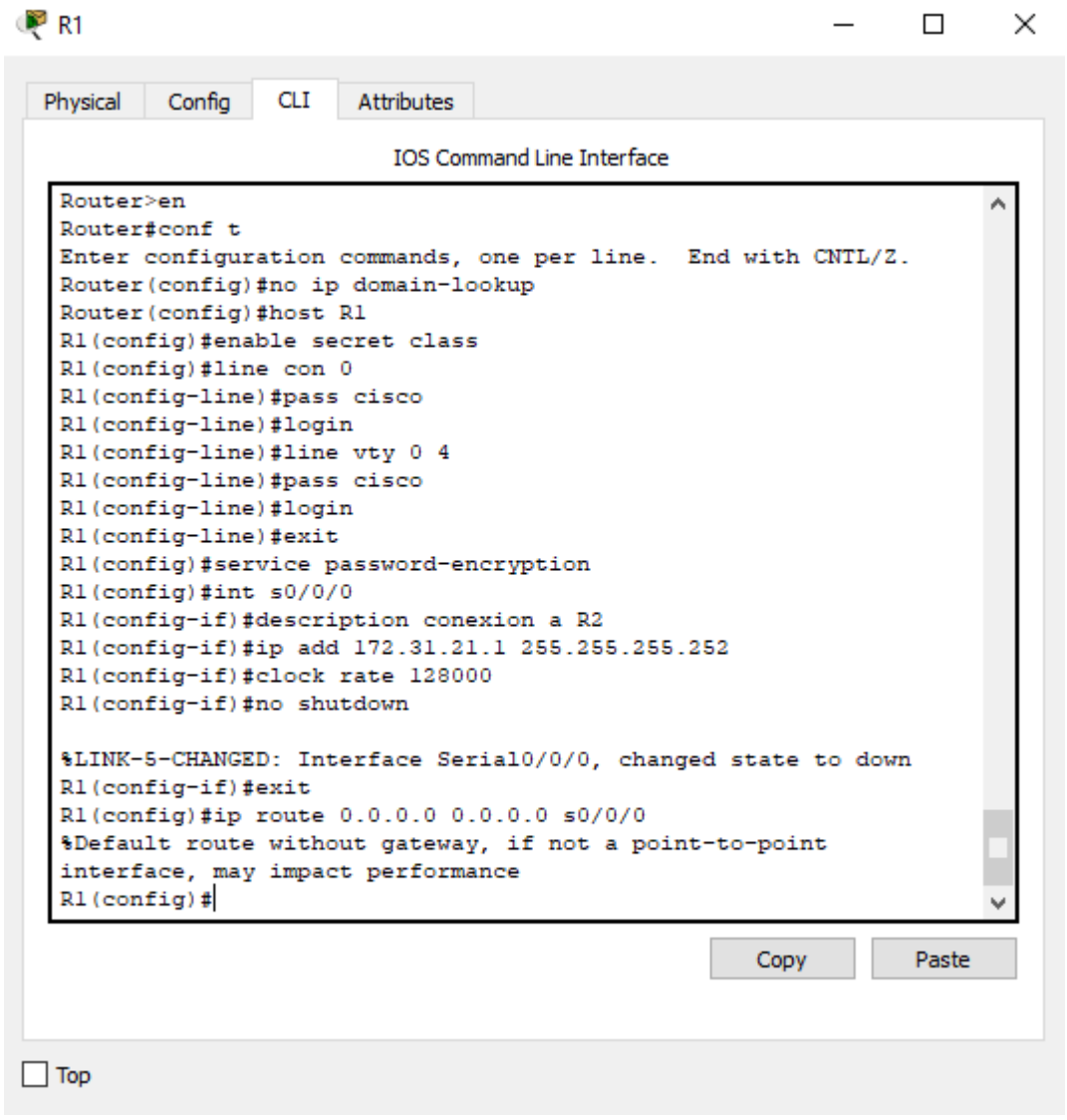


Figura 9

Tareas de configuración para R2 incluyendo: Disable DNS lookup, Nombre, Interface S0/0/0, Interface S0/0/1, Interface G0/0 (Internet Simulado), Default route.

Configurando R2.

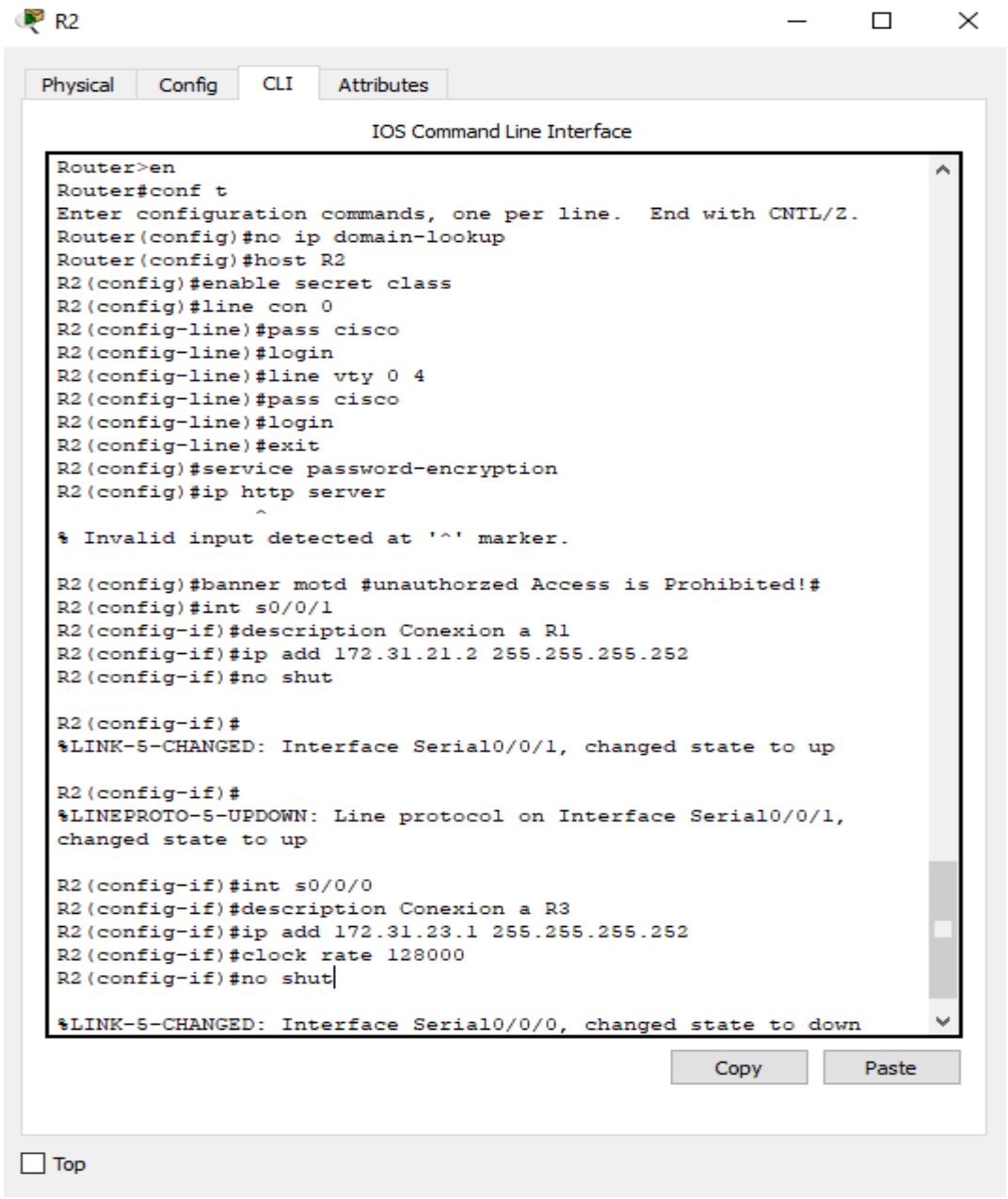


Figura 10

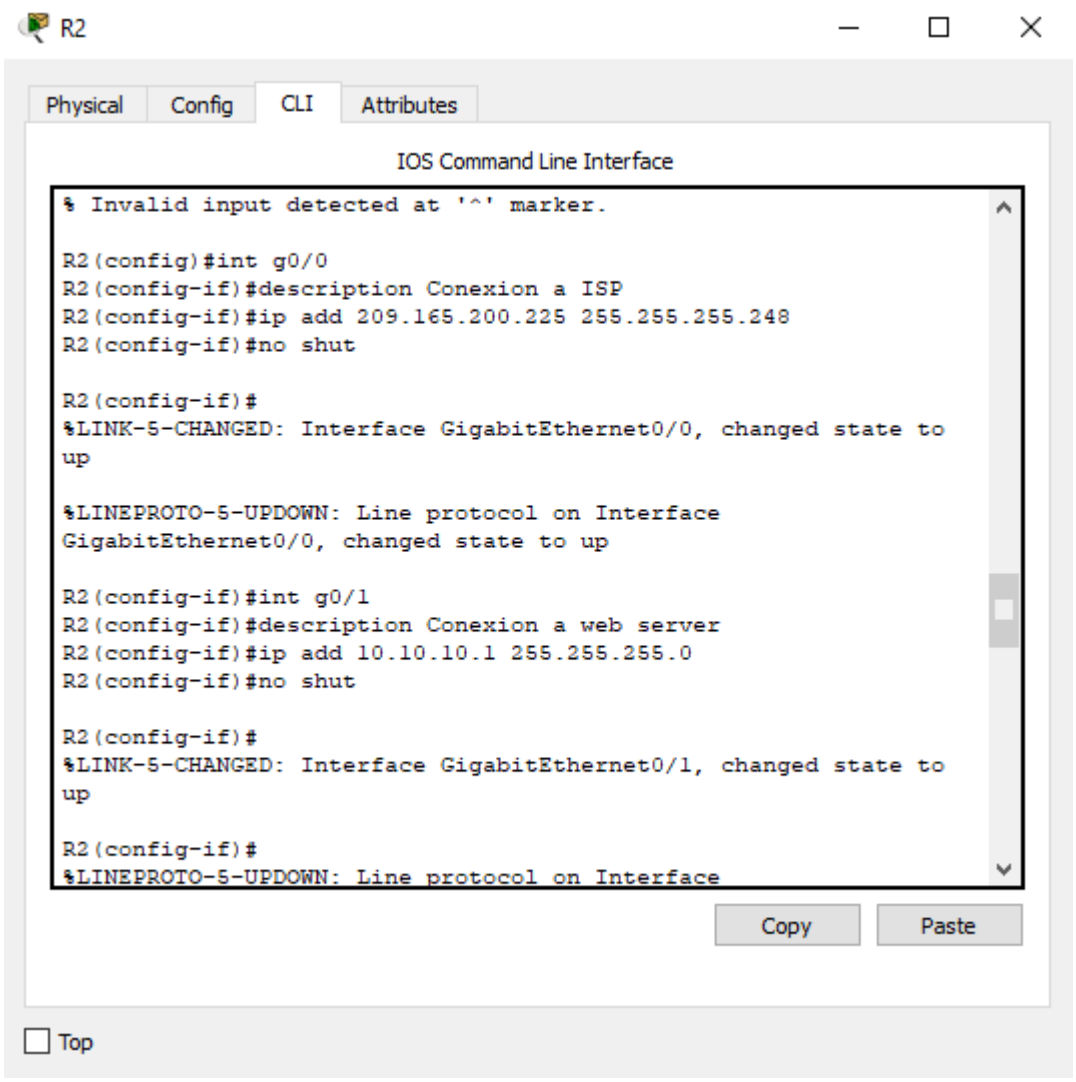

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
% Invalid input detected at '^' marker.
R2(config)#int g0/0
R2(config-if)#description Conexion a ISP
R2(config-if)#ip add 209.165.200.225 255.255.255.248
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
R2(config-if)#int g0/1
R2(config-if)#description Conexion a web server
R2(config-if)#ip add 10.10.10.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
R2(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface
Copy
Paste
Top

Figura 11

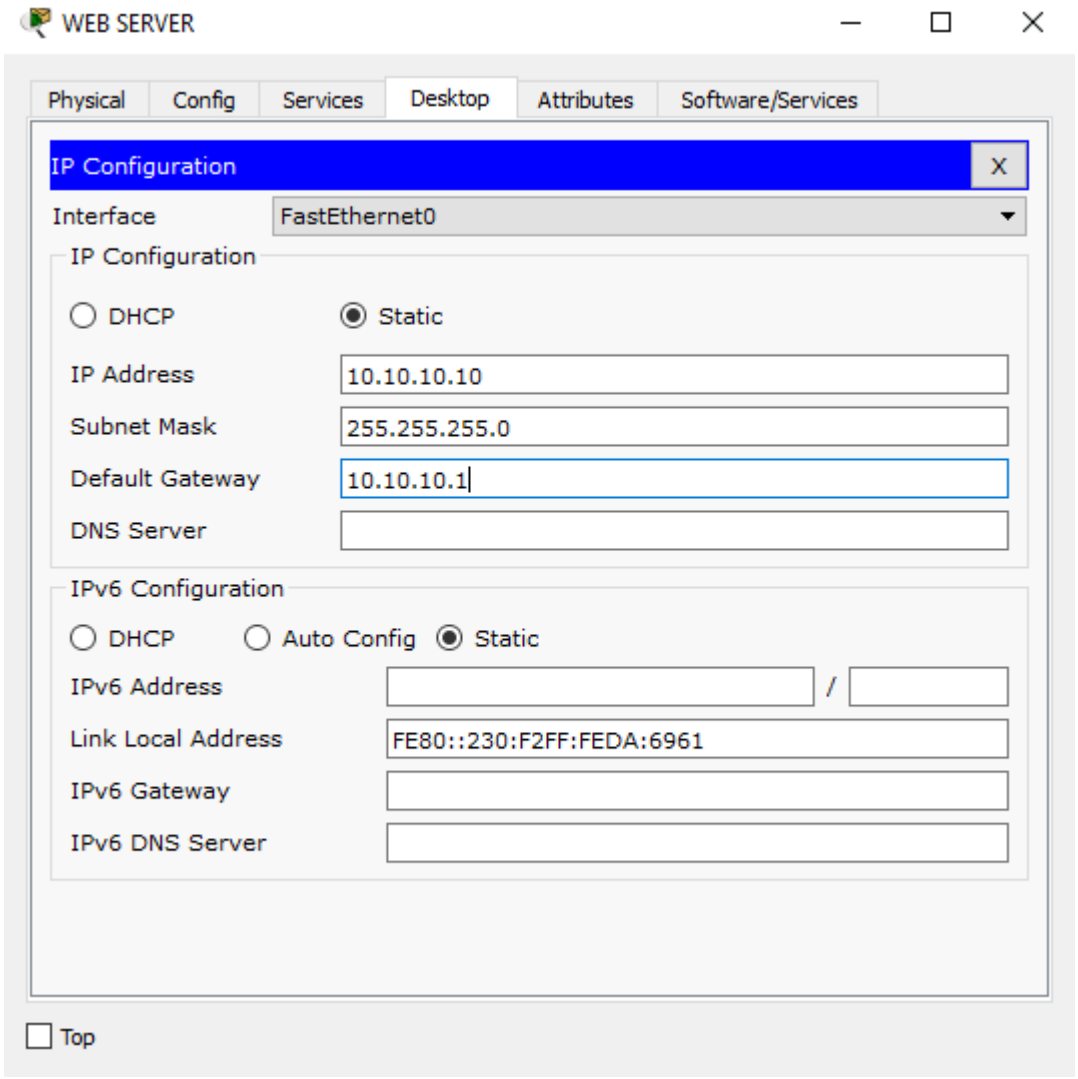


Figura 12

Tareas de configuración para R3 incluyendo: Disable DNS lookup, Nombre, Interface Loopback 4, Interface Loopback 5, Interface Loopback 6, Default route.

Configurando R3.

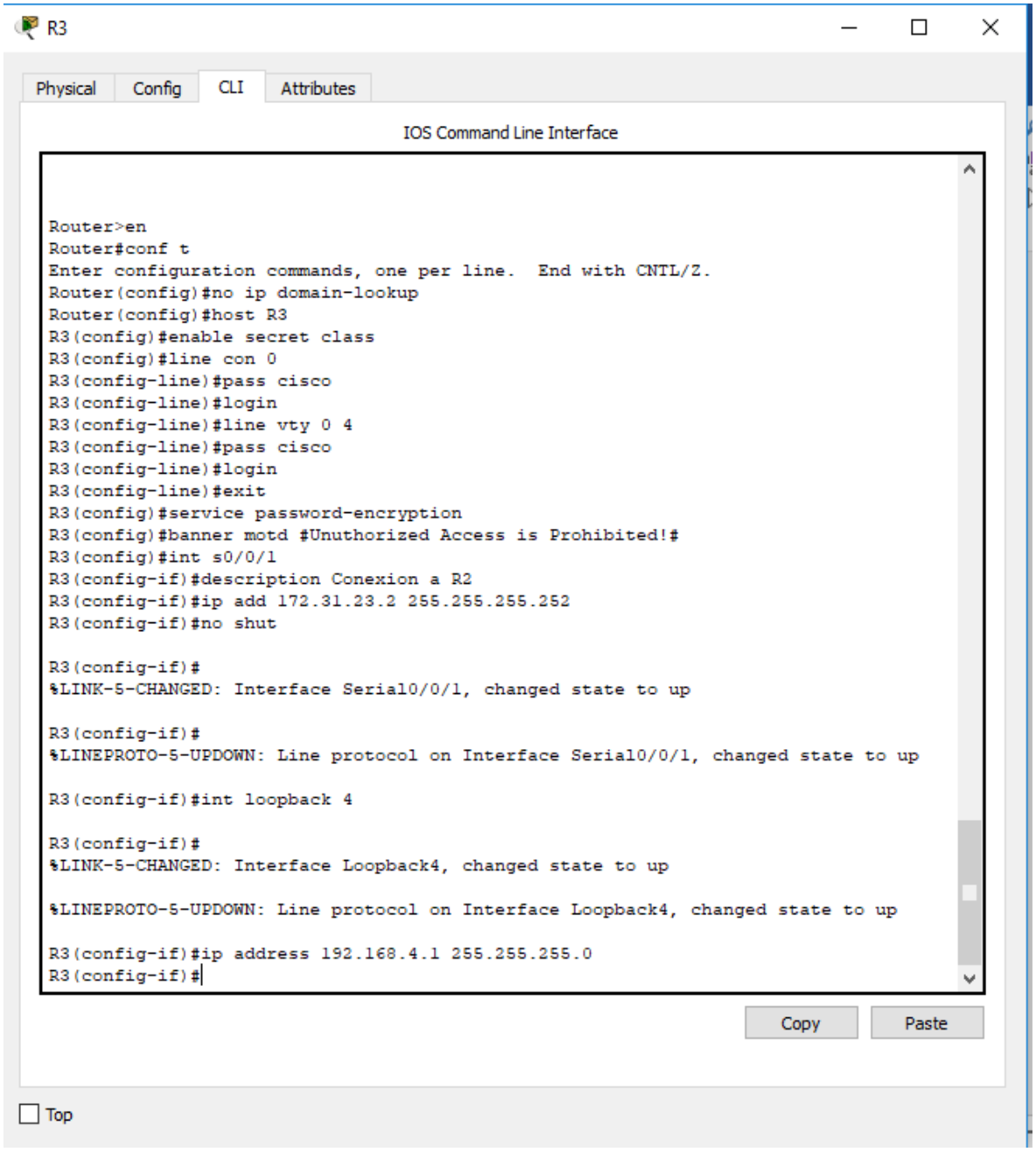


Figura 13

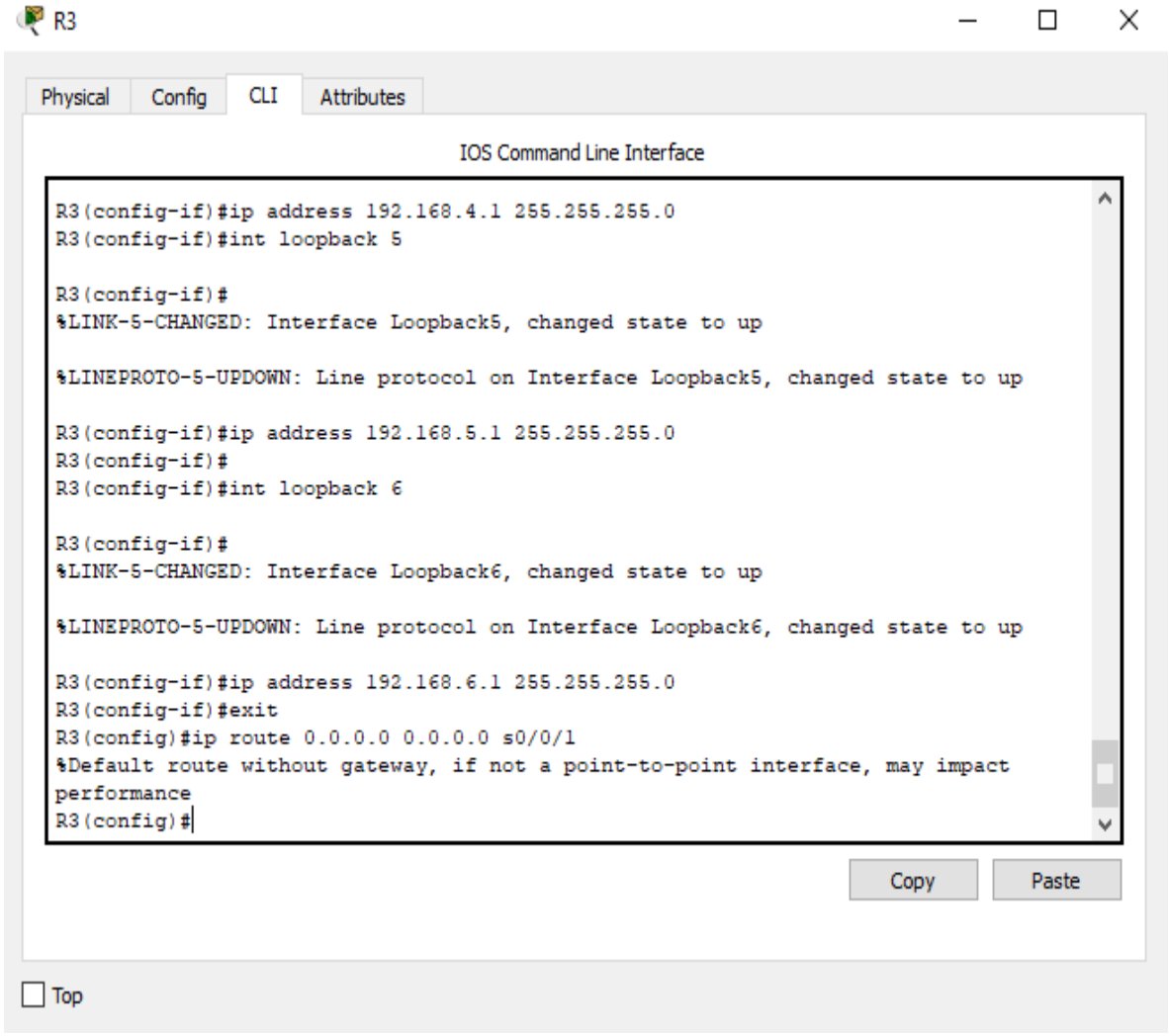


Figura 14

Tareas de configuración para S1 incluyendo: Disable DNS lookup, Nombre.

Configurando S1.

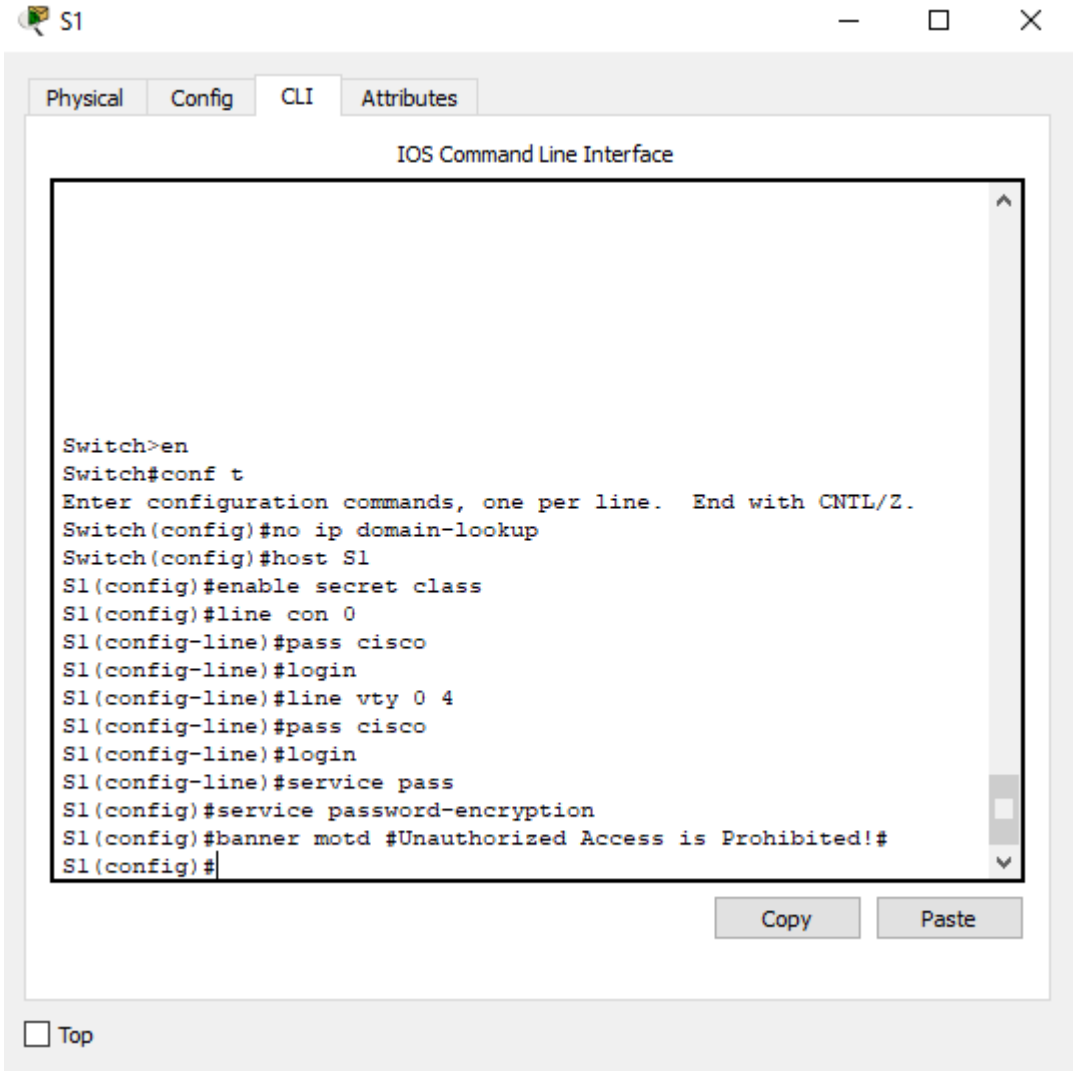


Figura 15

Tareas de configuración para S3 incluyendo: Disable DNS lookup, Nombre.

Configurando S3.

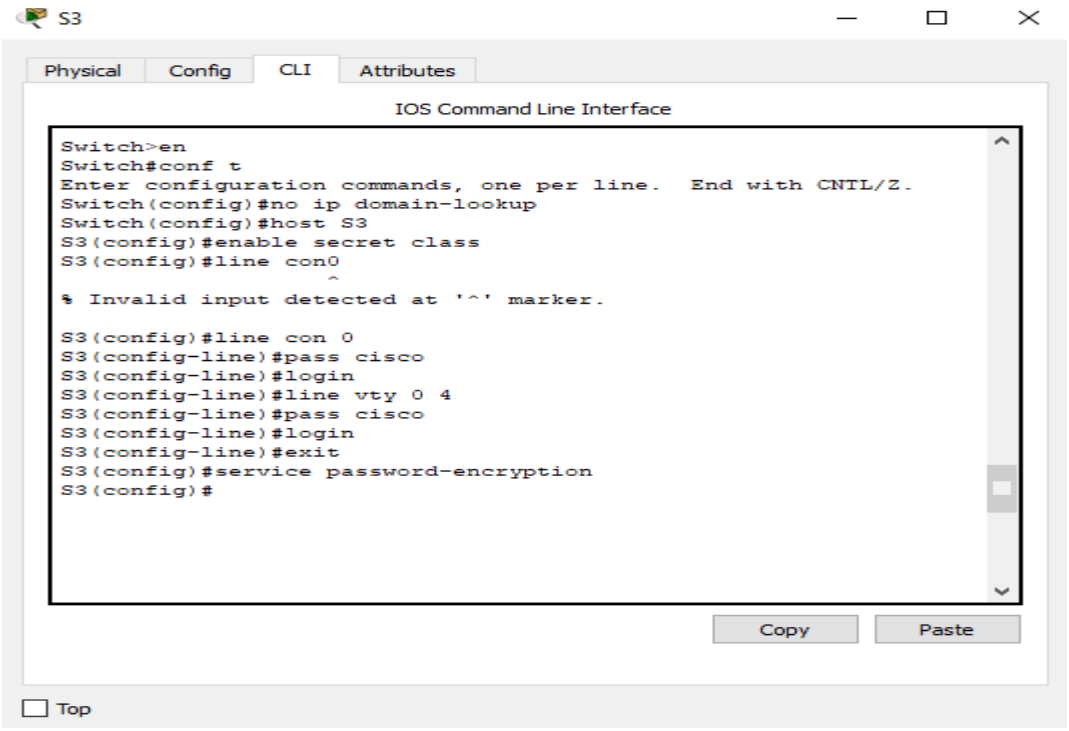


Figura 17

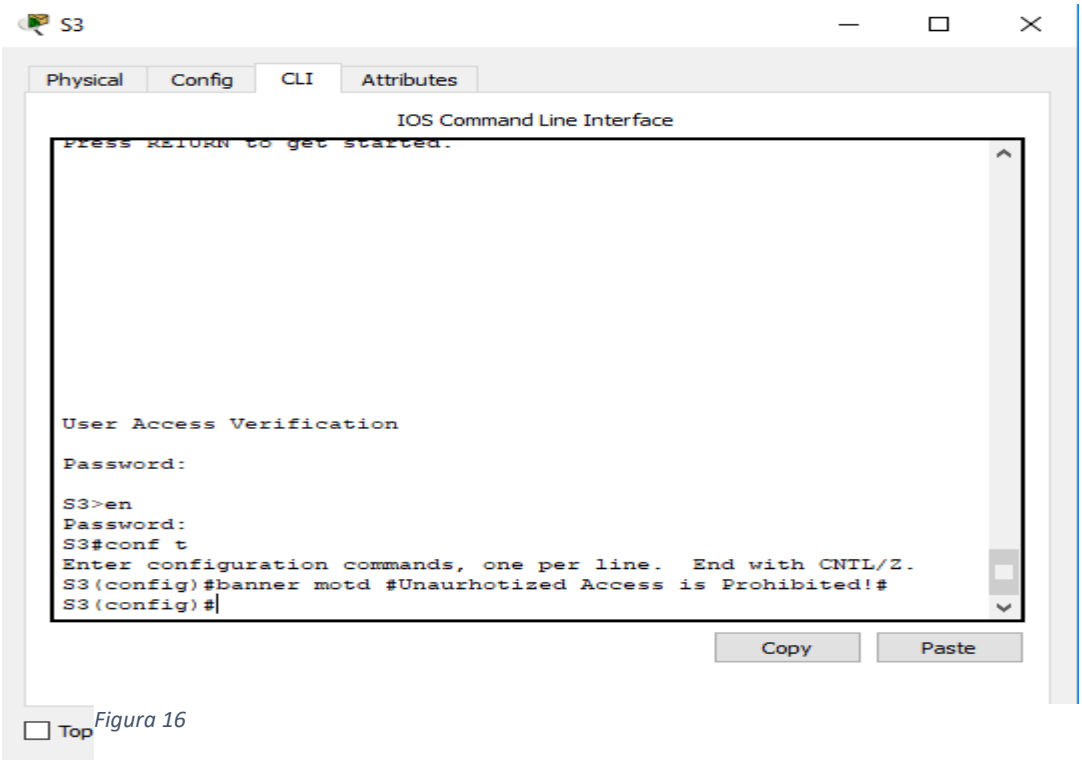


Figura 16

Verificación de la Conectividad de la Red

Se usa el comando ping para probar la conectividad entre dispositivos de red.

Ping desde R1 a R2, S0/0/0

```
R1#ping 172.31.21.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4
ms

R1#
```

Figura 18

Ping desde R3 a R2, S0/0/1

```
R3#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
2/6/19 ms

R3#
```

Figura 19

Ping desde Internet PC a Puerta de Enlace Predeterminada

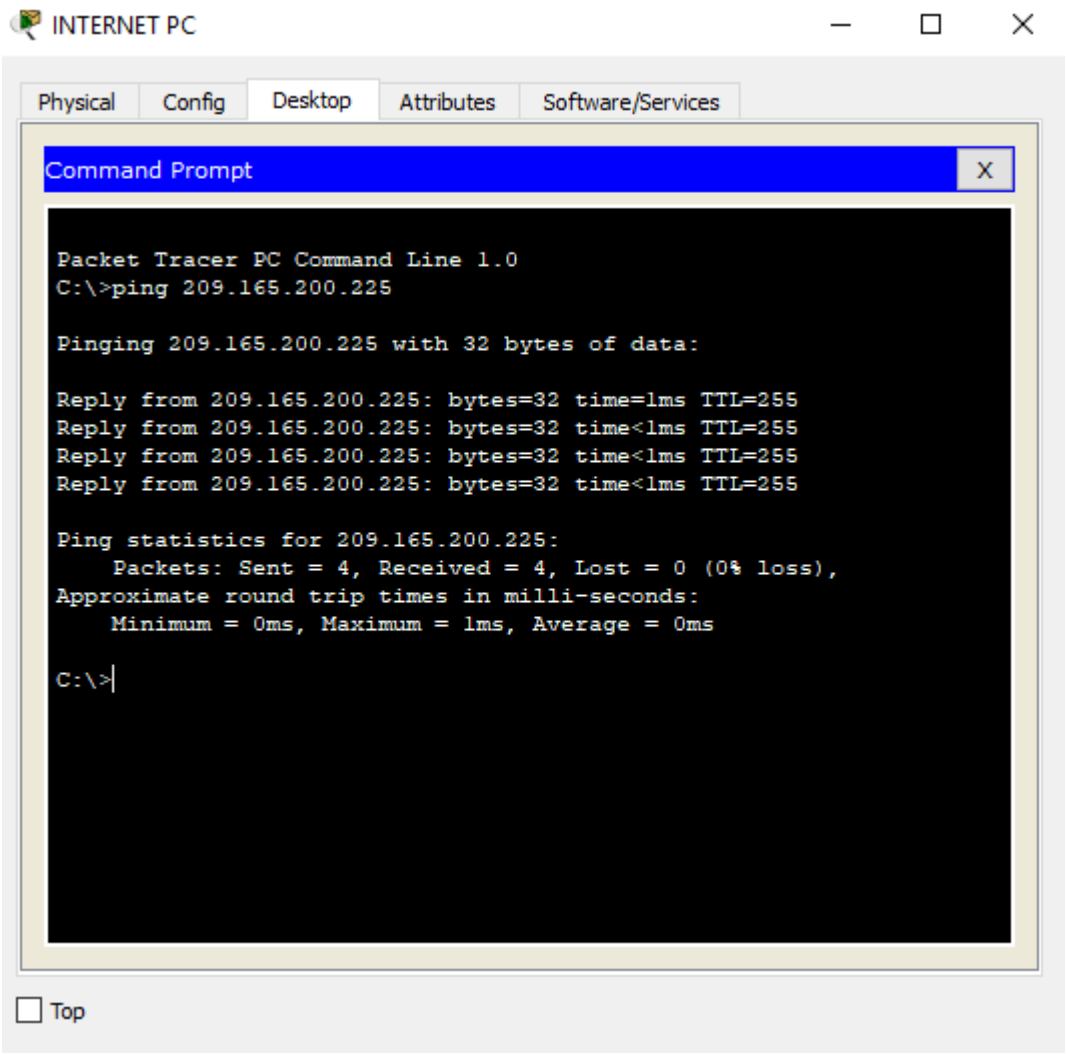


Figura 20

Configuración de Switch Security, VLANS e Inter VLAN Routing

Tareas de configuración para S1 incluyendo: Crear la base de datos VLAN, asignar la dirección IP de administración, asignar la puerta de enlace predeterminada, forzar la conexión troncal en la interfaz F0/3, forzar la conexión troncal en la interfaz F0/24, configurar todos los demás puertos como puertos de acceso, asignar F0/1 a la VLAN 30, apagar todos los puertos no utilizados.

Configurando S1.

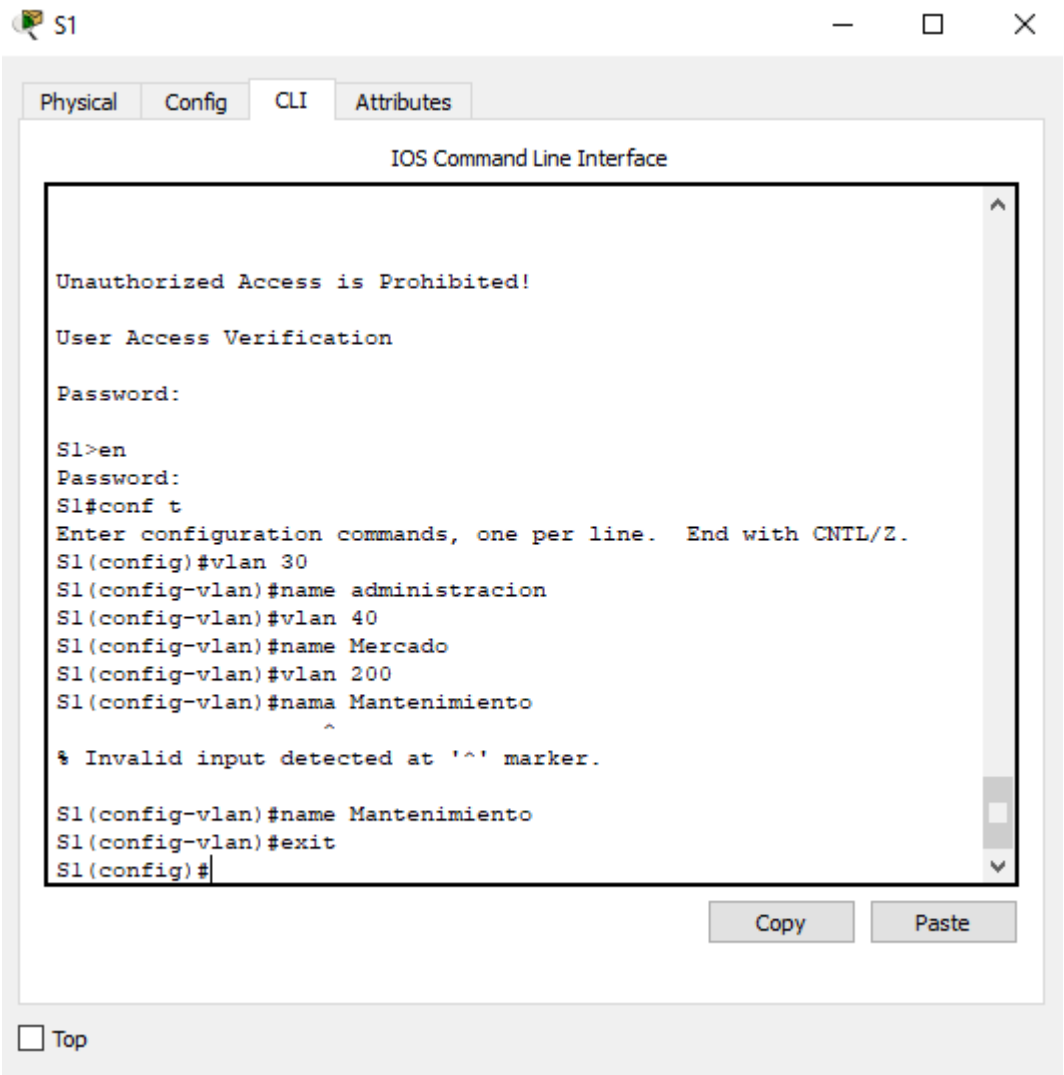


Figura 21

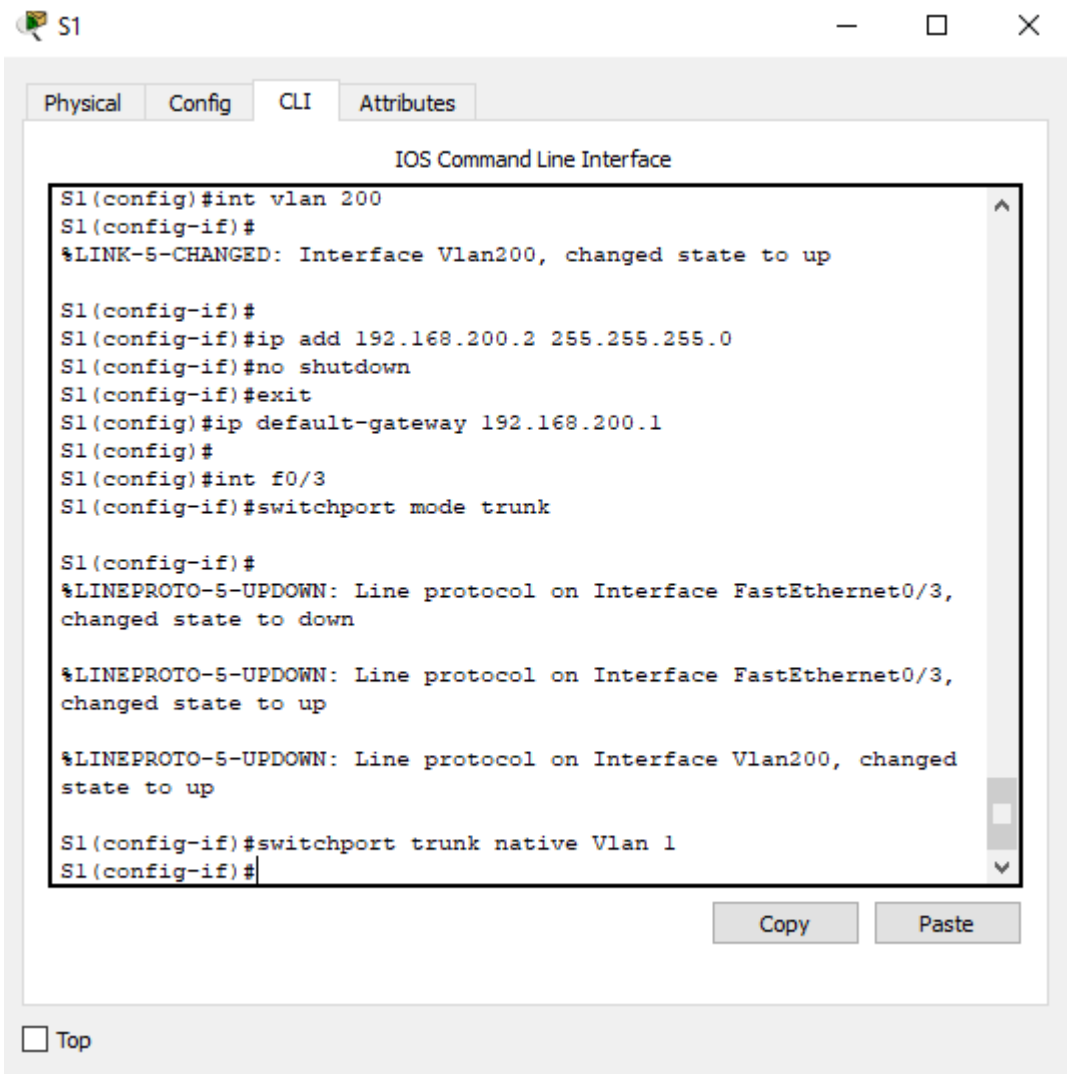

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
S1(config)#int vlan 200
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
S1(config-if)#
S1(config-if)#ip add 192.168.200.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.200.1
S1(config)#
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up
S1(config-if)#switchport trunk native Vlan 1
S1(config-if)#
Copy
Paste
Top

Figura 22

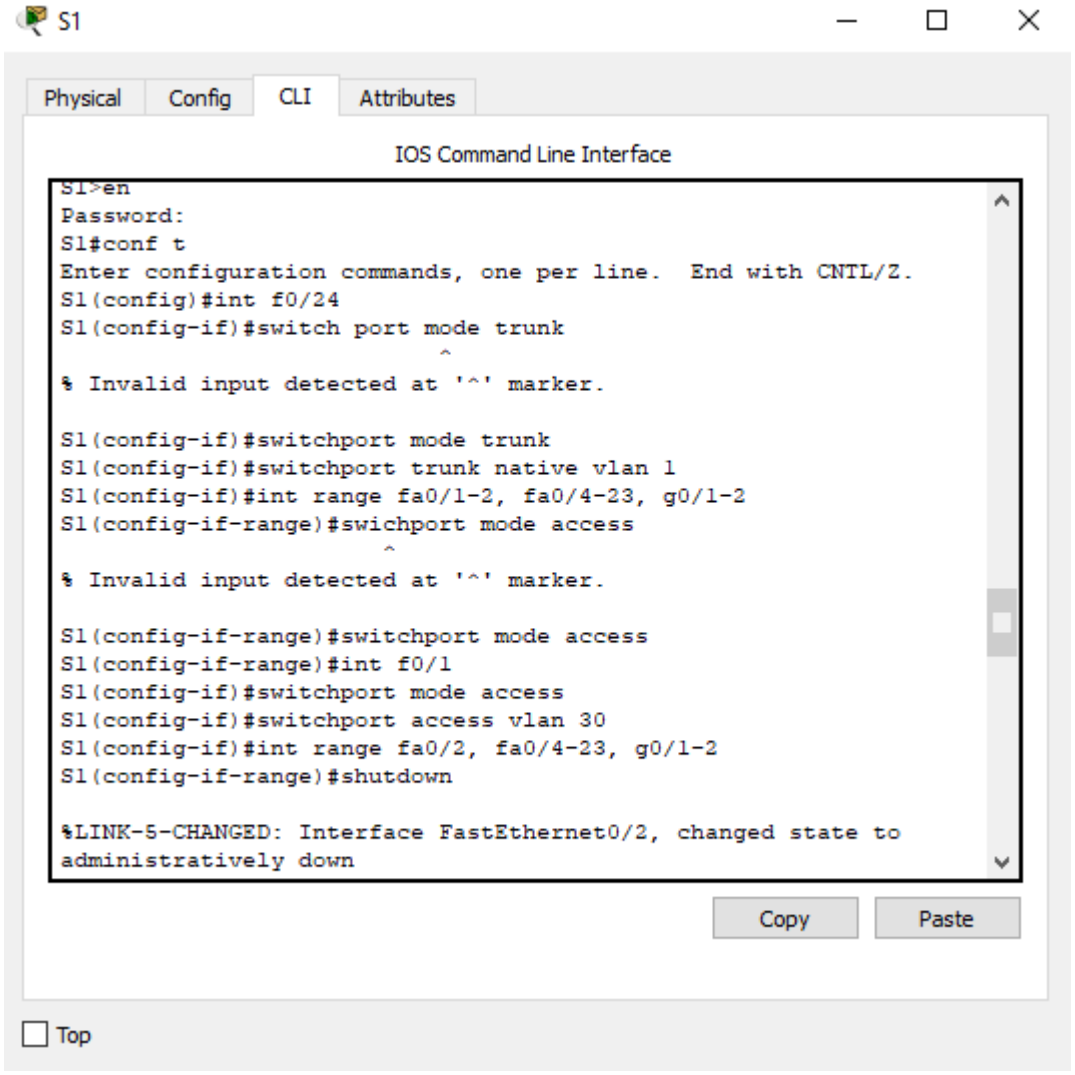

S1
Physical
Config
CLI
Attributes
IOS Command Line Interface
S1>en
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int f0/24
S1(config-if)#switch port mode trunk
                          ^
% Invalid input detected at '^' marker.
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range fa0/1-2, fa0/4-23, g0/1-2
S1(config-if-range)#swichport mode access
                   ^
% Invalid input detected at '^' marker.
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#int 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
Copy
Paste
Top

Figura 23

Tareas de configuración para S3 incluyendo: Crear la base de datos VLAN, asignar la dirección IP, asignar la puerta de enlace predeterminada, forzar la conexión troncal en la interfaz F0/3, configurar todos los demás puertos como puertos de acceso, asignar F0/1 a la VLAN 40, apagar todos los puertos no utilizados.

Configurando S3.

Figura 24

Tareas de configuración para R1 incluyendo: Configurar la subinterfaz 802.1Q .31 en G0/0, configurar la subinterfaz 802.1Q .33 en G0/0, configurar la subinterfaz 802.1Q .99 en G0/0, activar la interfaz G0/0.

Configurando R1.

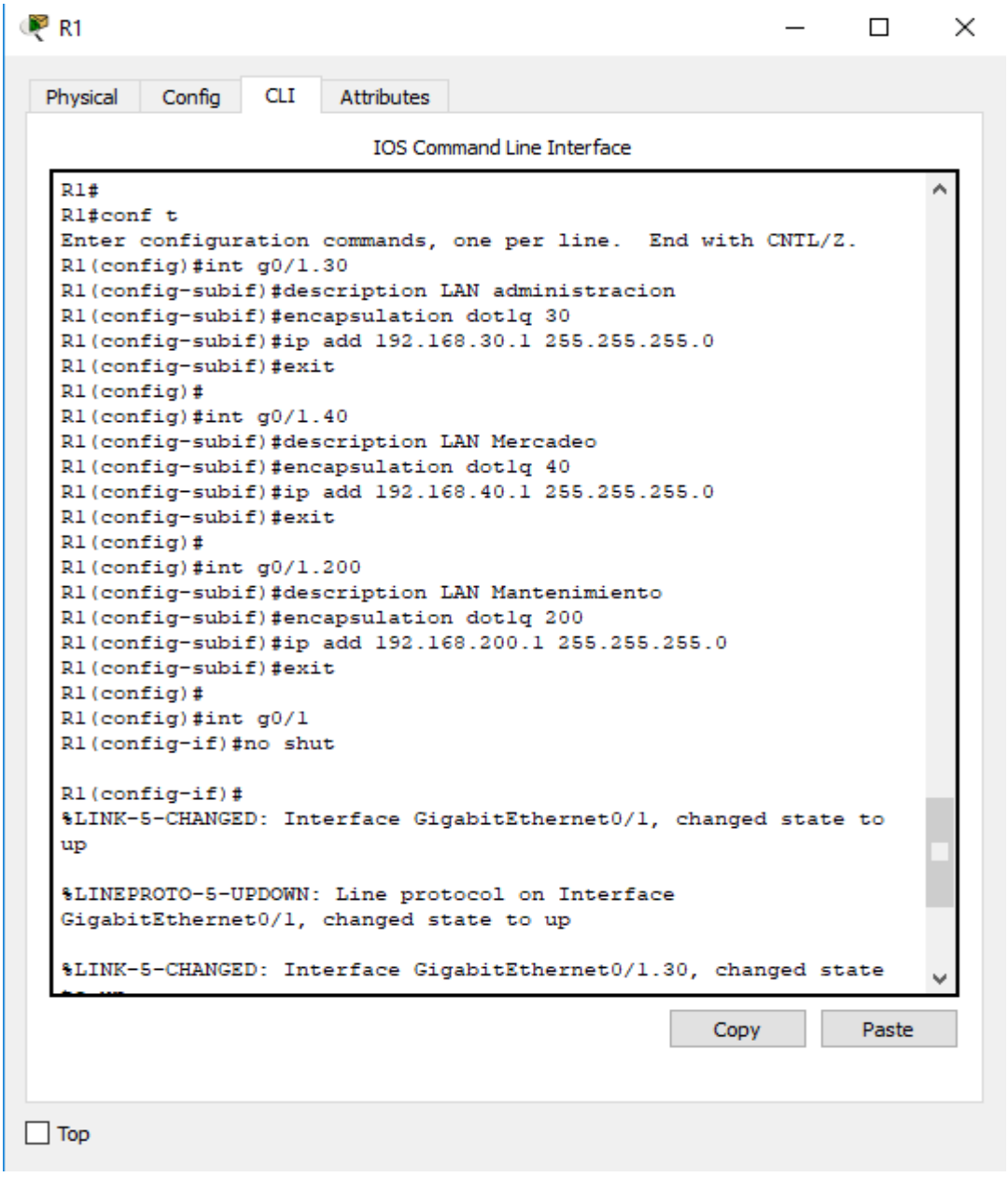


Figura 25

Verificar la conectividad de la red

Se usa el comando ping para probar la conectividad entre los swiches y R1.

Ping desde S1 a R1 dirección VLAN 200

```
S1#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0
ms

S1#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1
ms

S1#
```

Figura 26

Ping desde S3 a R1, direccion VALN 200

```
S3#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/3
ms

S3#ping 192.168.200.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4
ms
```

Figura 27

Pin desde S1 a R1, Dirección VLAN 30

```
S1#ping 192.168.30.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4
ms

S1#
```

Figura 28

Ping desde S3 a R1, direccion VLAN 40

```
S3#ping 192.168.40.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
0/2/11 ms

S3#
```

Figura 29

Configurar el Protocolo de Enrutamiento Dinámico OSPFv2

Tareas de configuración para R1 incluyendo: ID de proceso OSPF, ID de enrutador, anunciar redes conectadas directamente, establecer todas las interfaces LAN como pasivas, cambiar el ancho de banda de referencia de costo predeterminado para admitir cálculos de interfaz Gigabit, establecer el ancho de banda de la interfaz en serie, ajustar el costo métrico de S0/0/0.

Configurando OSPFv2 en R1.

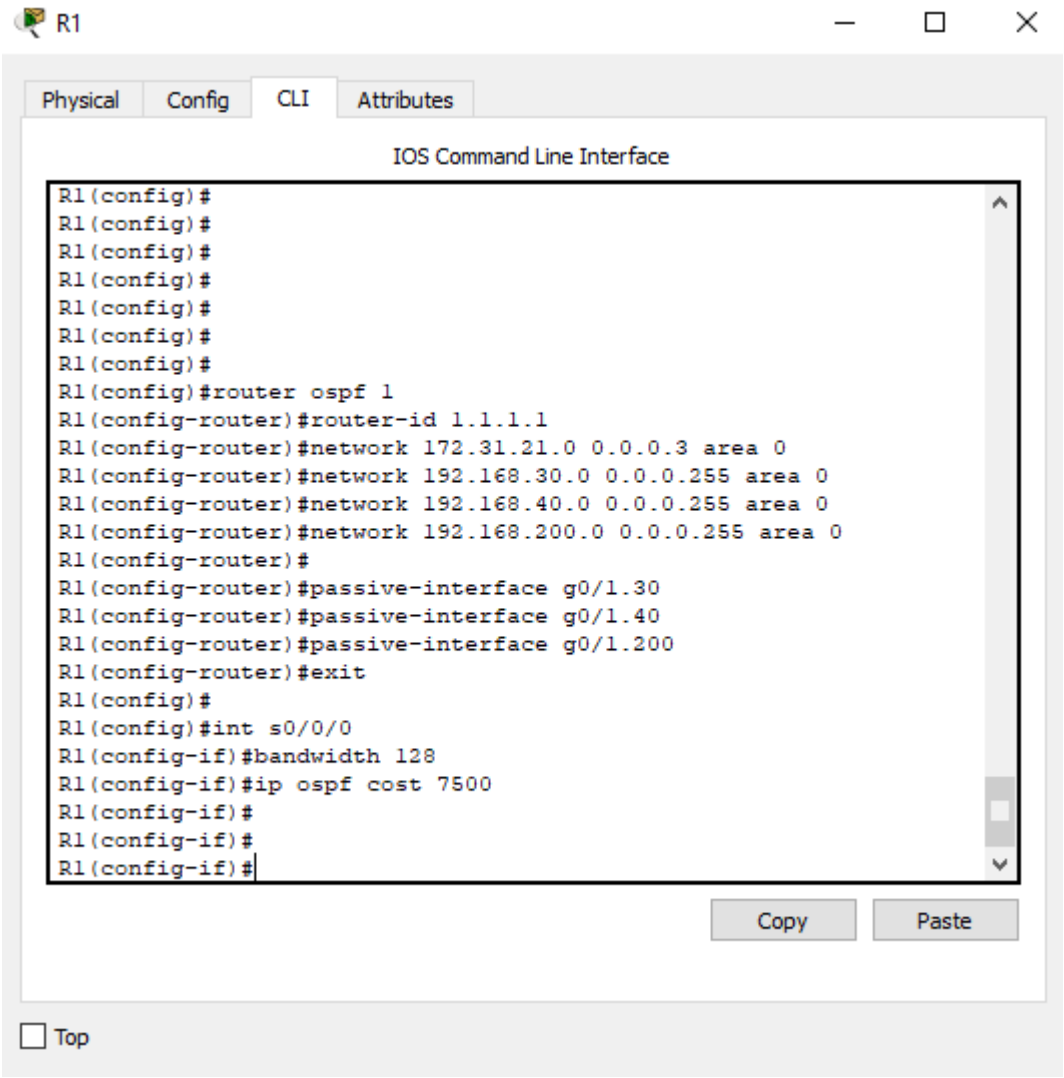


Figura 30

Tareas de configuración para R2 incluyendo: ID de proceso OSPF, ID de enrutador, anunciar redes conectadas directamente, configurar la interfaz LAN (Loopback) como pasiva, establecer todas las interfaces LAN como pasivas, cambiar el ancho de banda de referencia de costo predeterminado para admitir cálculos de interfaz Gigabit, establecer el ancho de banda en todas las interfaces seriales, ajustar el costo métrico de S0/0/0.

Configurando OSPFv2 en R2.

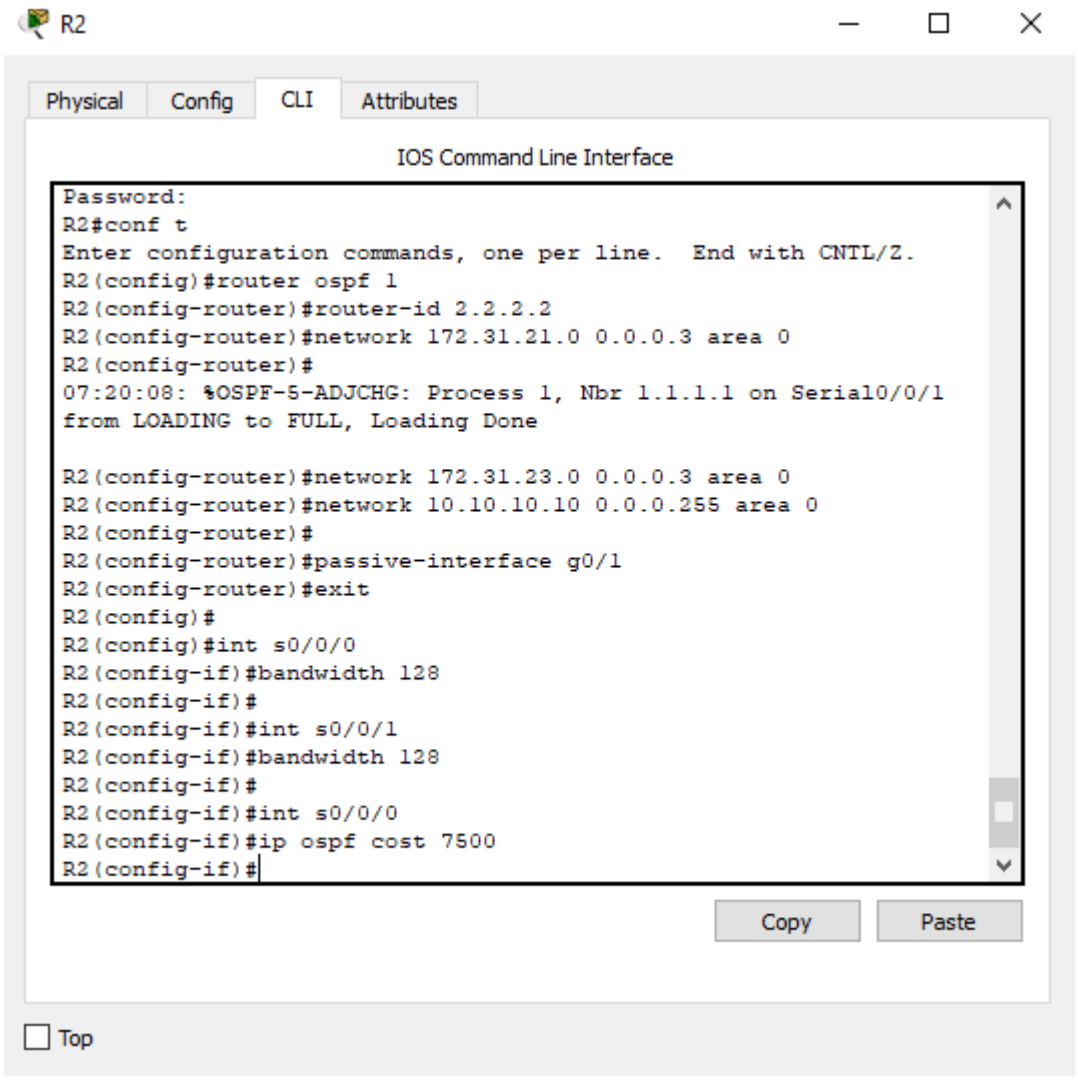


Figura 31

Tareas de configuración para R3 incluyendo: ID de proceso OSPF, ID de enrutador, anunciar redes conectadas directamente, configurar la interfaz LAN (Loopback) como pasiva, establecer todas las interfaces LAN (loopback) como pasivas, cambiar el ancho de banda de referencia de costo predeterminado para

admitir cálculos de interfaz Gigabit, establecer el ancho de banda en la interface serial.

Configurando OSPFv2 en R3.

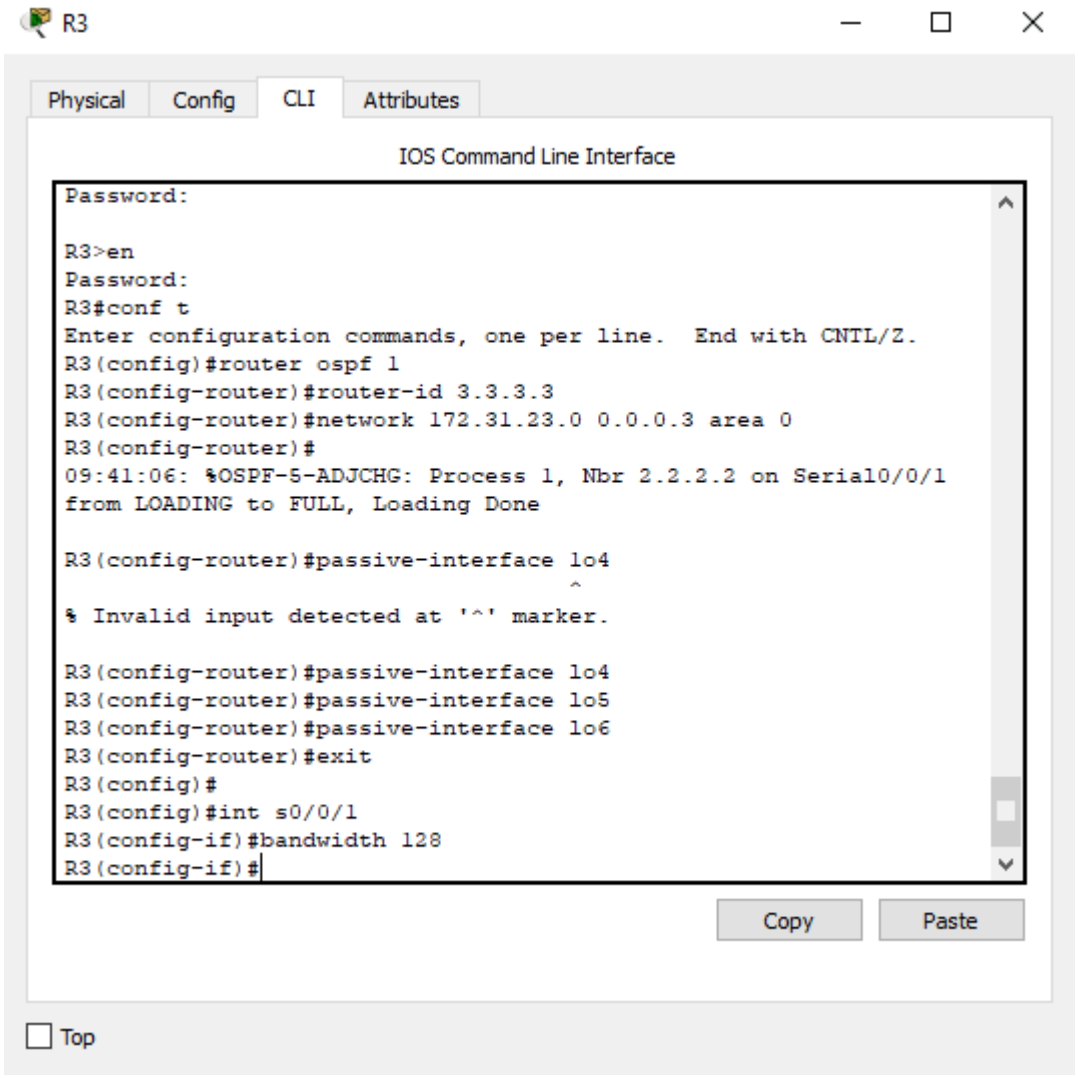


Figura 32

Verificación de la información de OSPF

En siguiente es un ejemplo de la verificación en el router R2

Routers conectados por OSPFv2

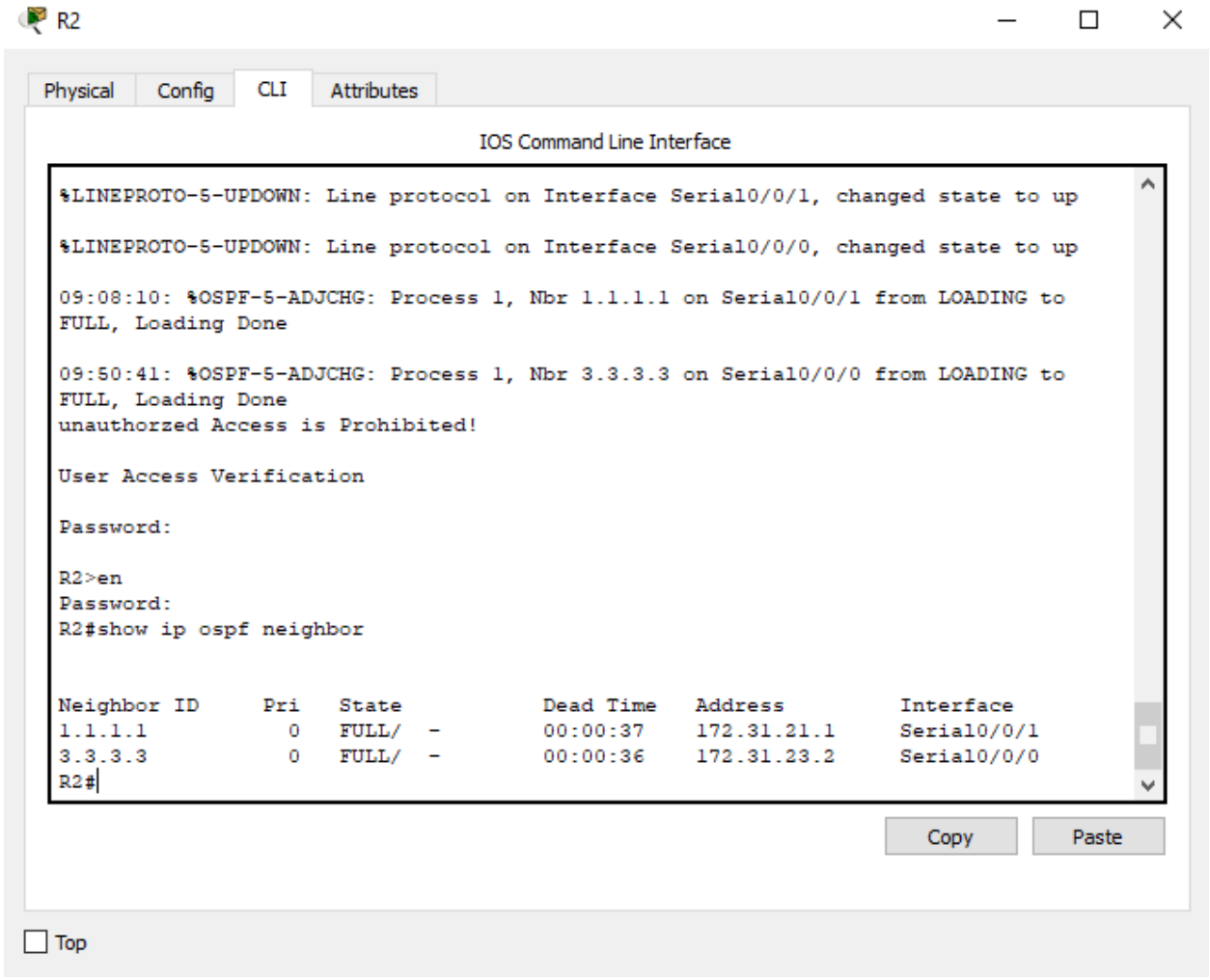


Figura 33

Resumen de las interfaces OSPF que incluye una columna para el Costo de cada Interfaz

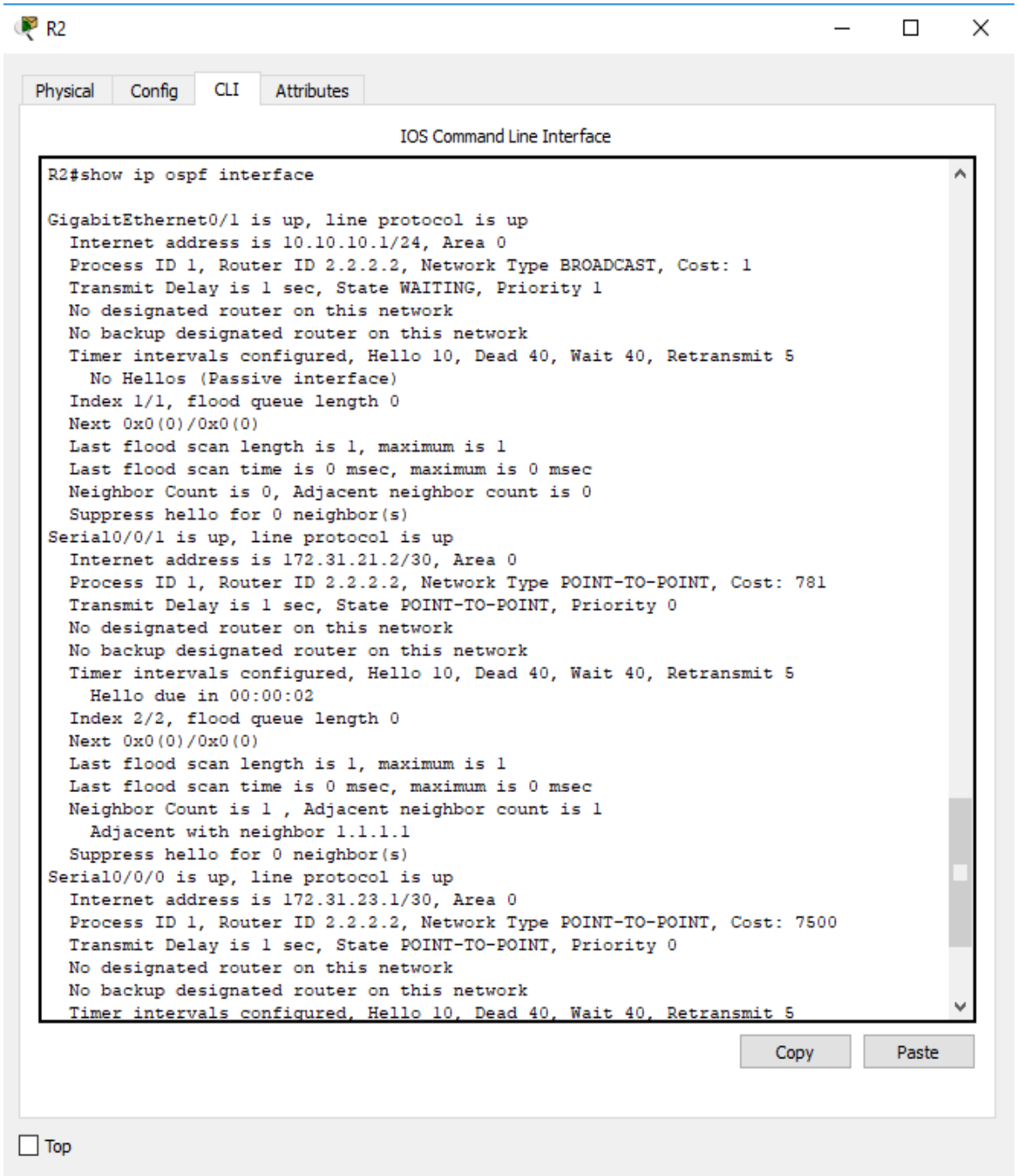


Figura 34

OSPF Process ID, Router ID, Address summarizations, Routing Networks, y passive interfaces configuradas en un Router

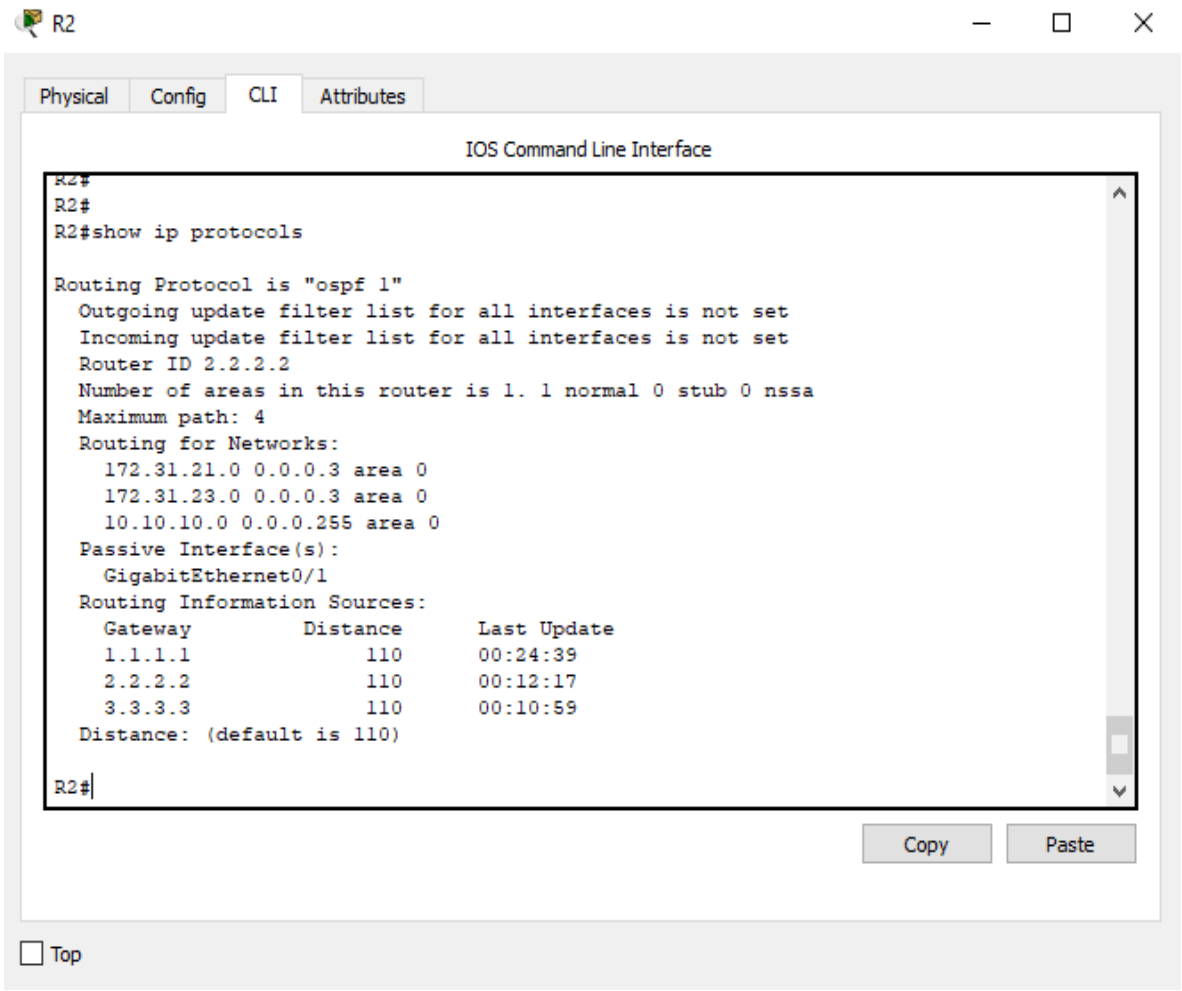


Figura 35

Mostrar solo las rutas OSPF

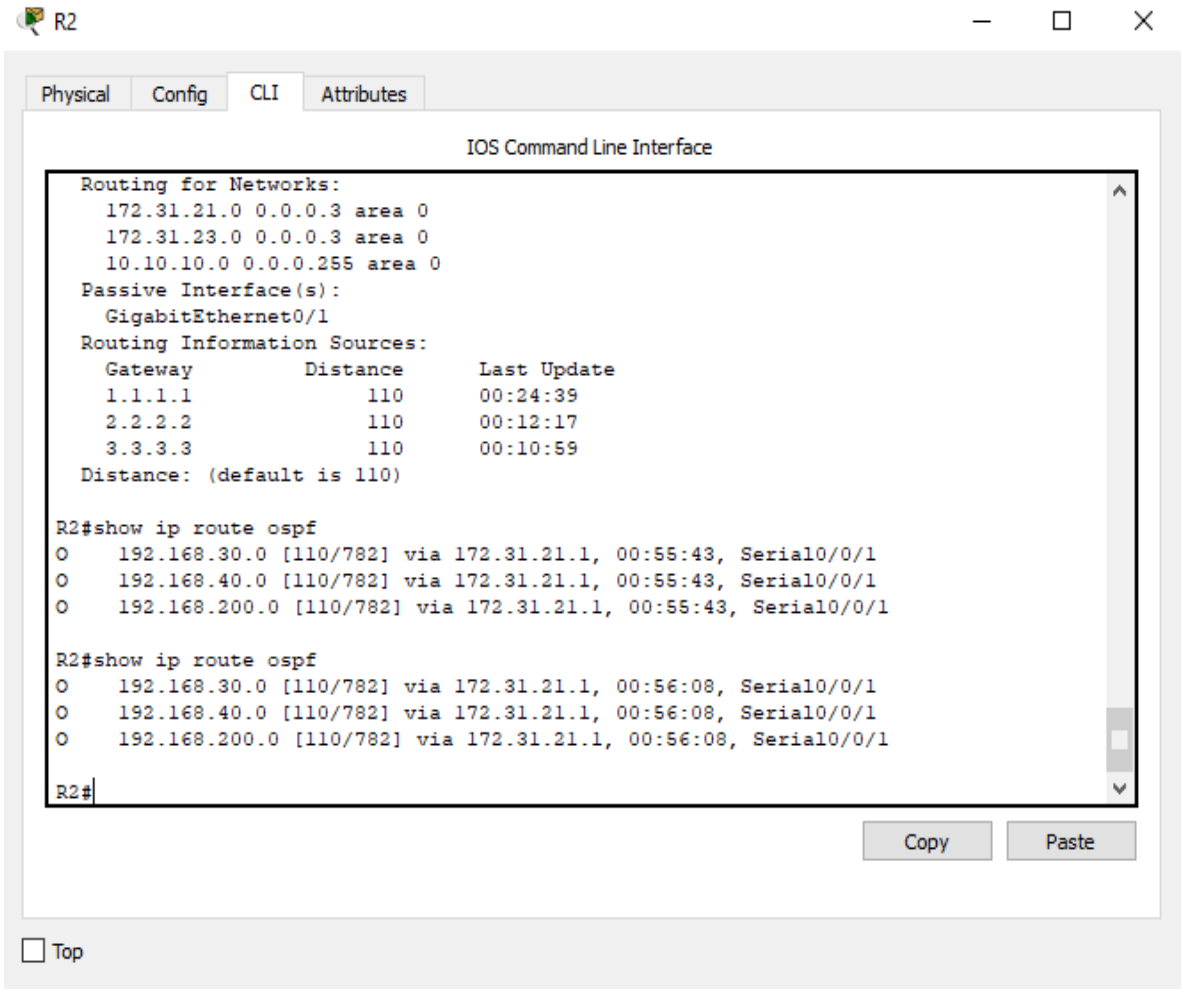


Figura 36

Sección OSPF de la configuración en ejecución

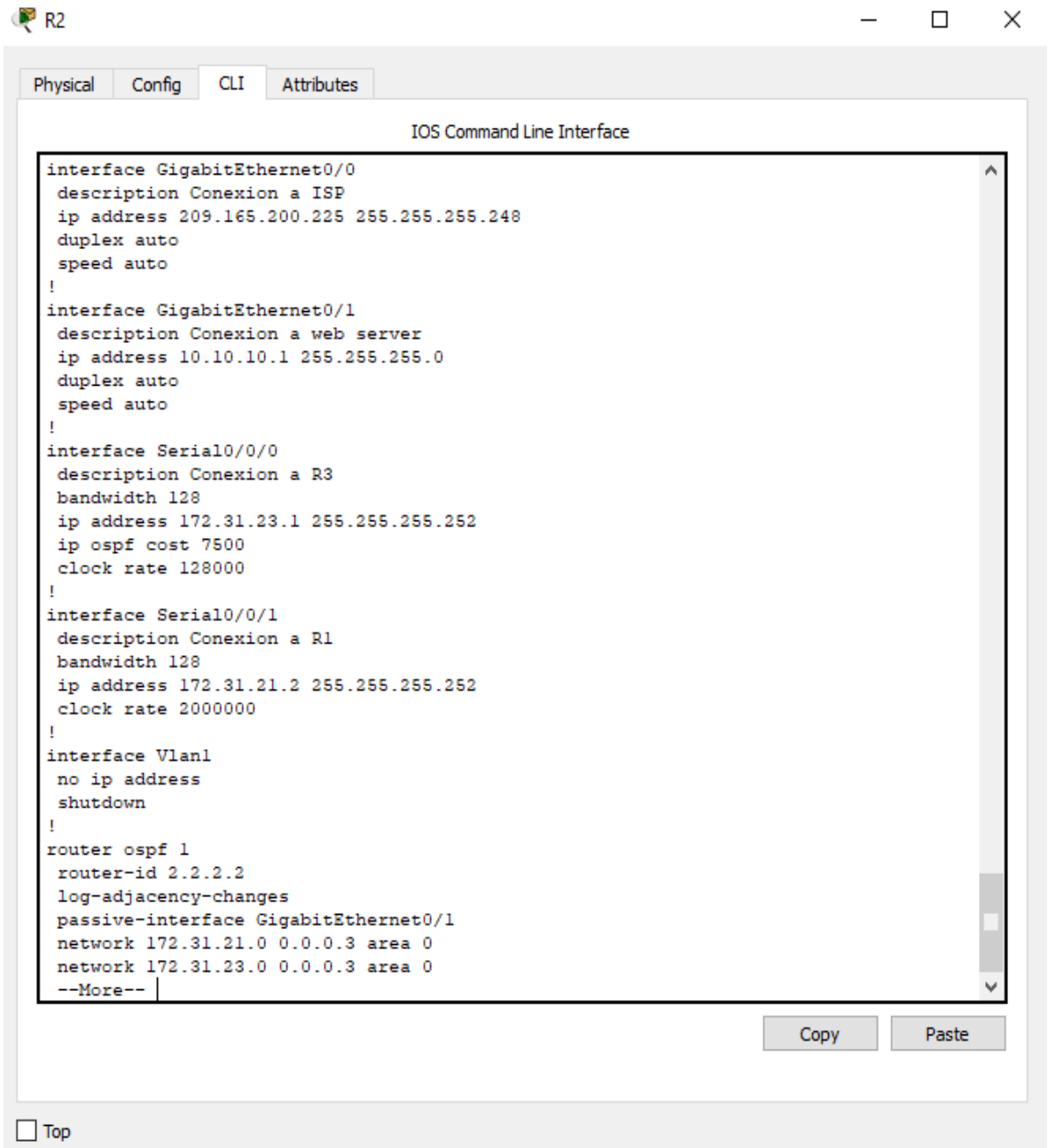


Figura 37

Implementación DHCP y NAT para IPv4

Tareas de configuración para R1 incluyendo: Reservar las primeras 30 direcciones IP en la VLAN 30 para configuraciones estáticas, reservar las primeras 30 direcciones IP en la VLAN 40 para configuraciones estáticas, crear una agrupación DHCP para la VLAN 30, crear una agrupación DHCP para la VLAN 40.

Configurando R1 como el servidor DHCP para las VLAN 30 y 40.

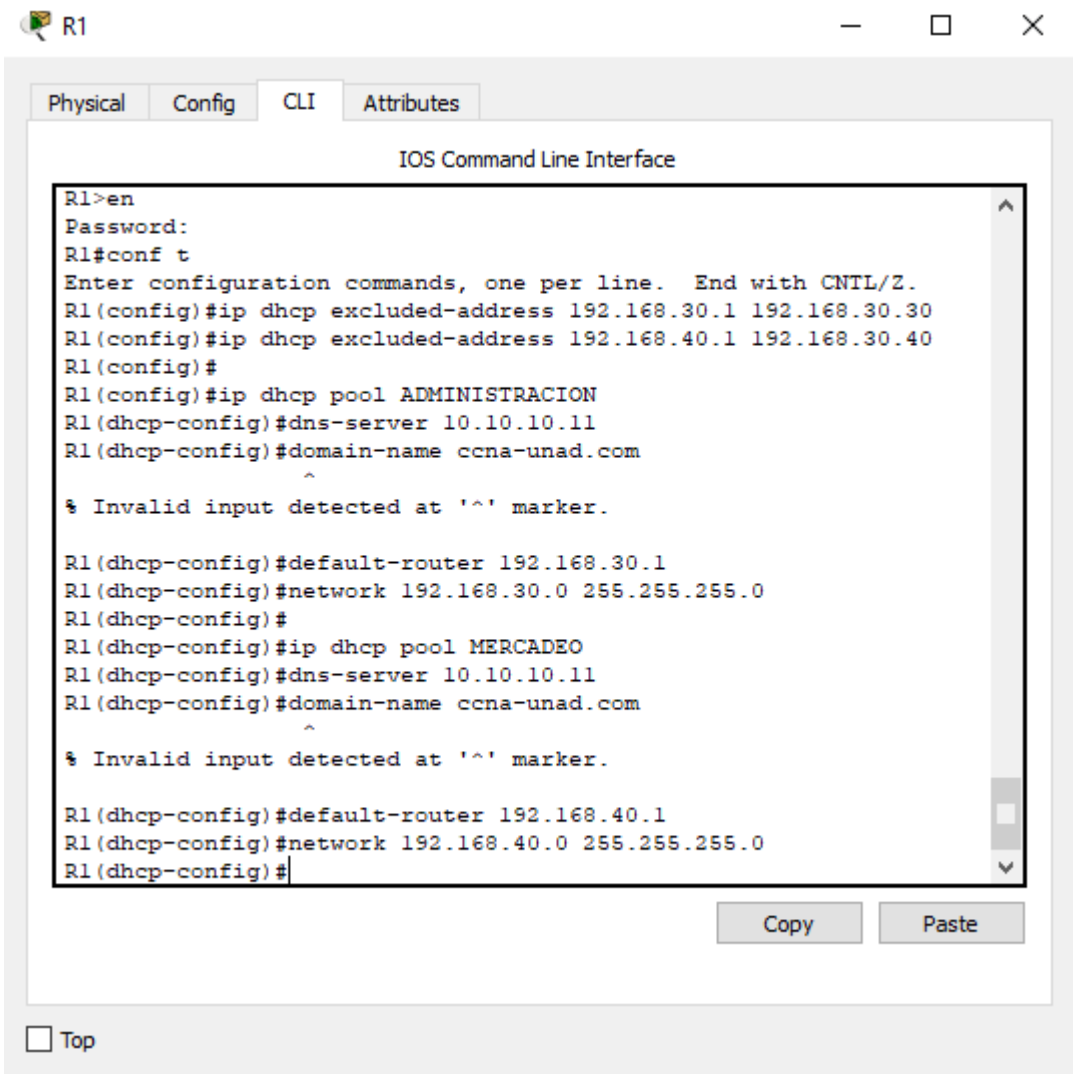


Figura 38

Tareas de configuración para R2 incluyendo: Crear una base de datos local con 1 cuenta de usuario, habilitar el servicio de servidor HTTP, configurar el servidor HTTP para usar la base de datos local para la autenticación, crear una NAT estática para el servidor web, asignar la interfaz interna y externa para la NAT estática, configurar la NAT dinámica dentro de la ACL privada, definir el grupo de direcciones IP públicas utilizables, definir la traducción dinámica de NAT.

Configurando NAT Estático y Dinámico en R2.

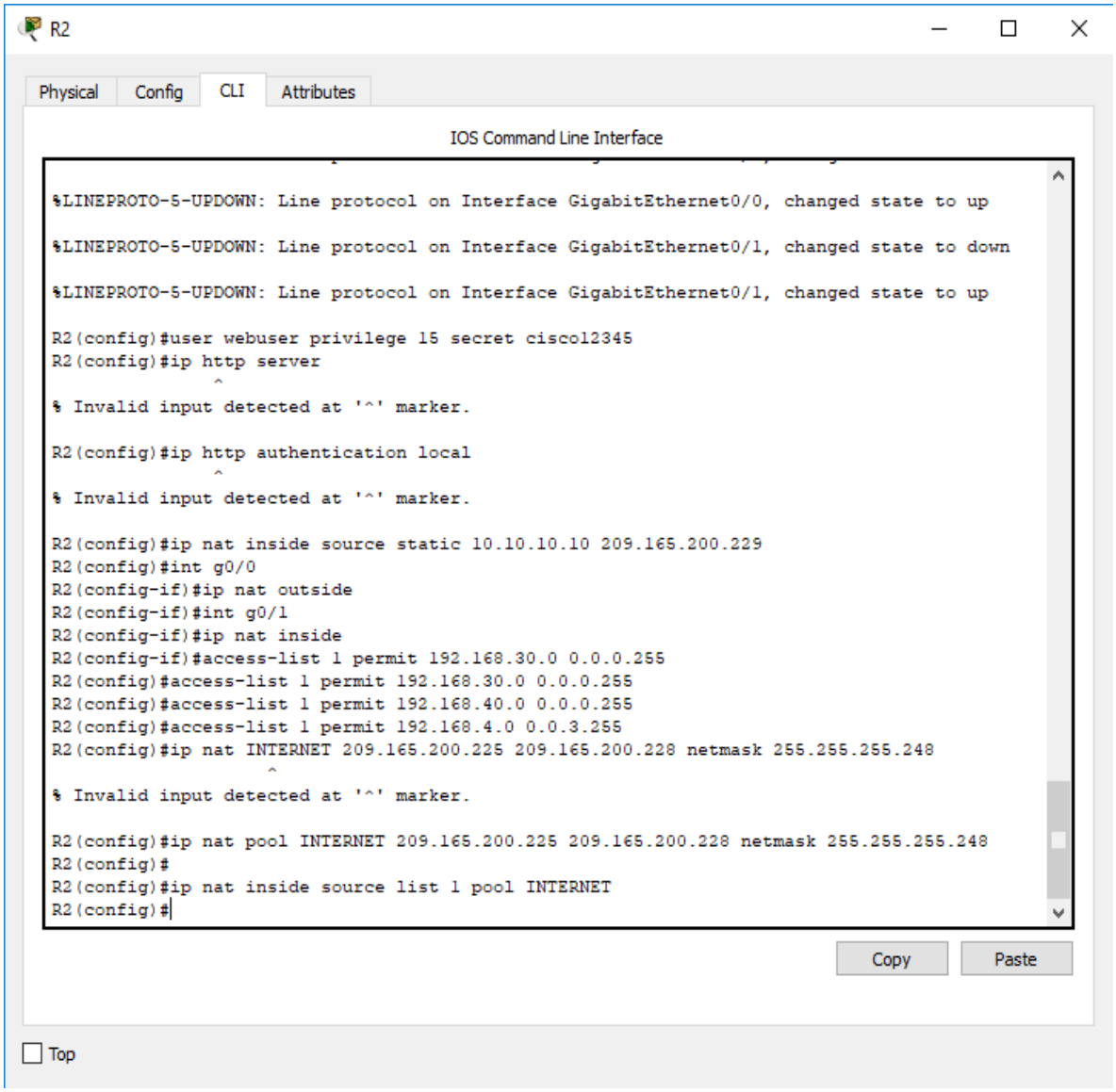


Figura 39

Verificando DHCP y NAT estática.

Verificando que la PC-A haya adquirido la información IP del servidor DHCP

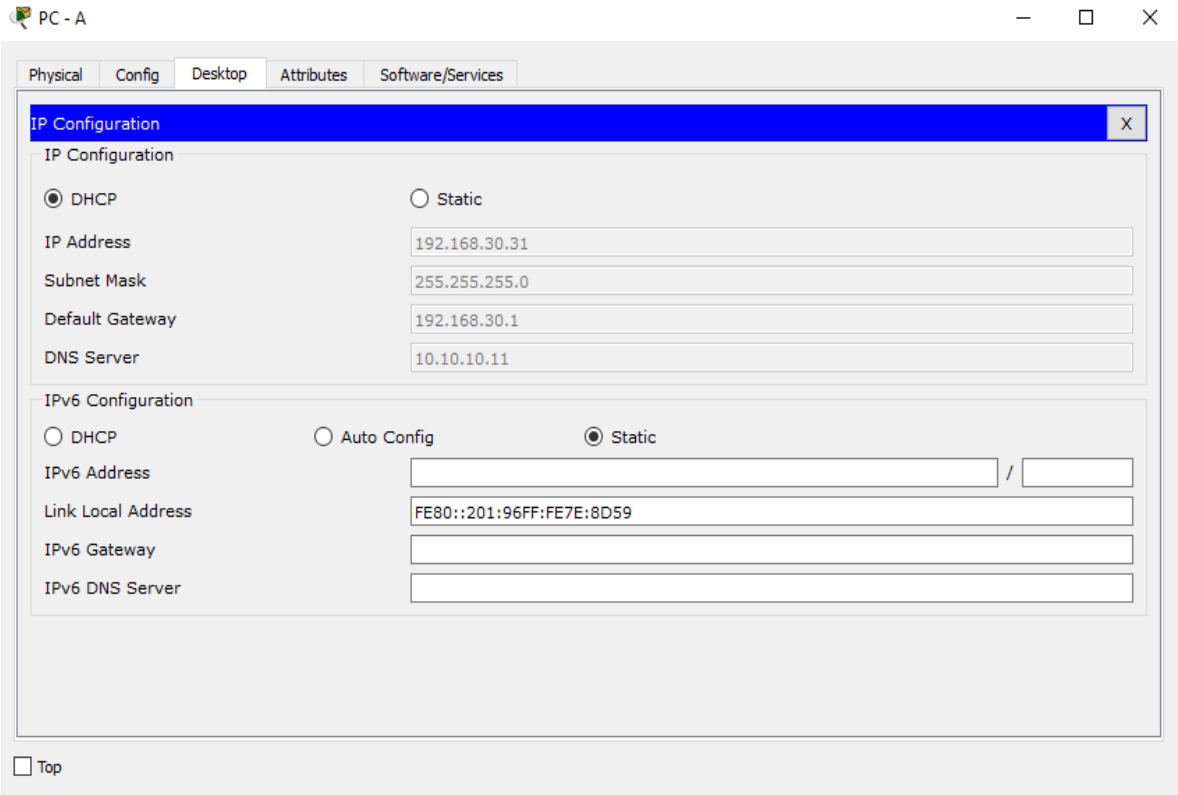


Figura 40

Verificando que la PC-C haya adquirido la información IP del servidor DHCP

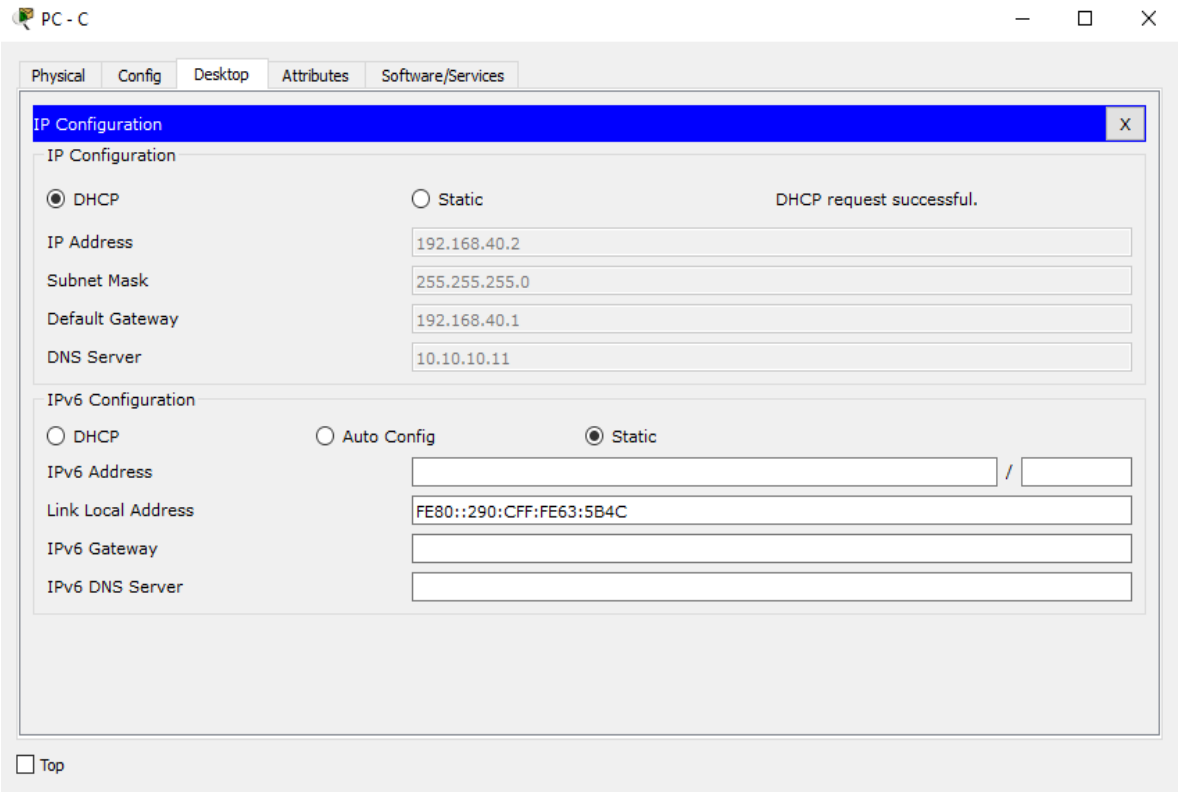


Figura 41

Verificando que la PC-A pueda hacer ping a la PC-C.

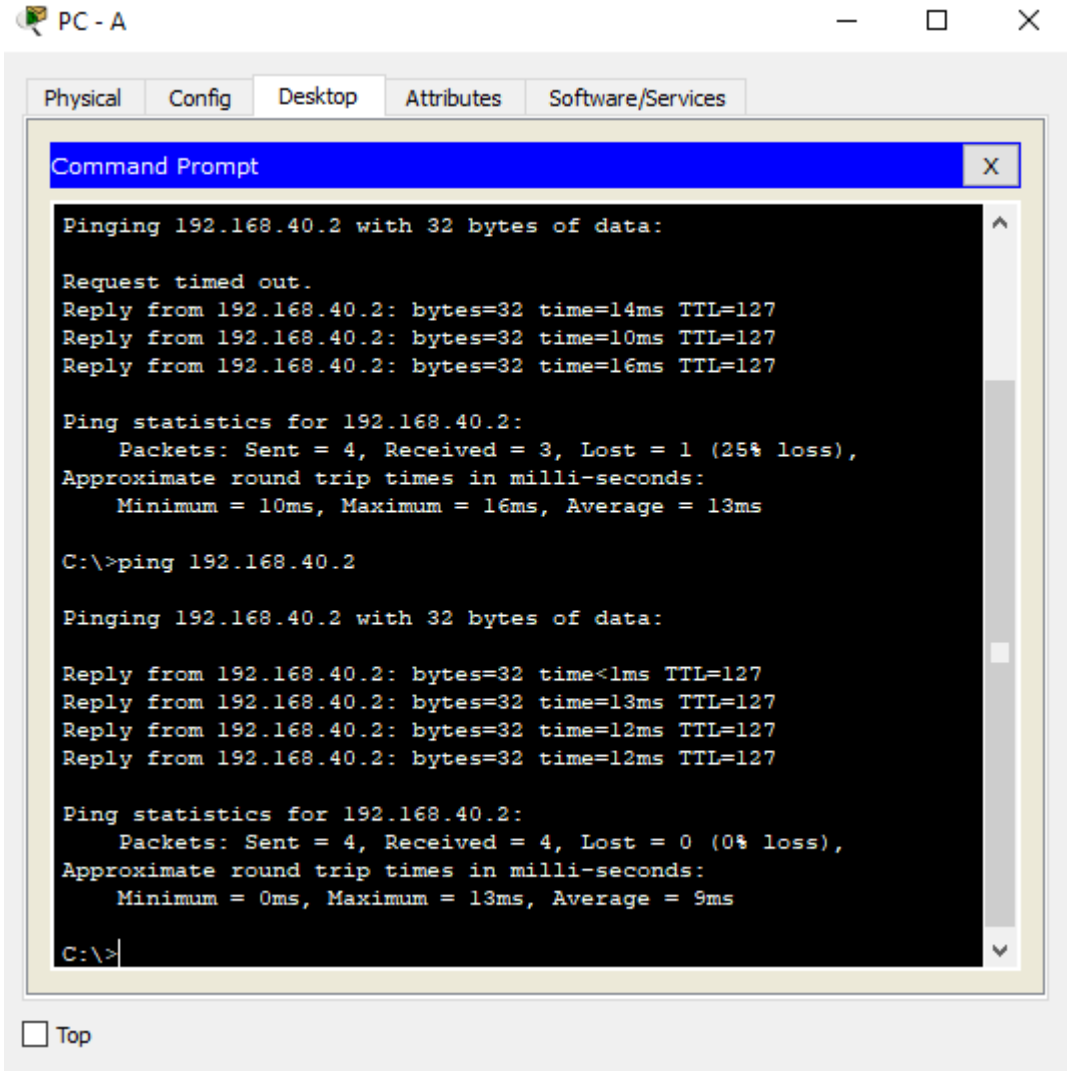


Figura 42

Configuración y verficando listas de control de acceso (ACL) restringiendo el acceso a las líneas VTY en R2

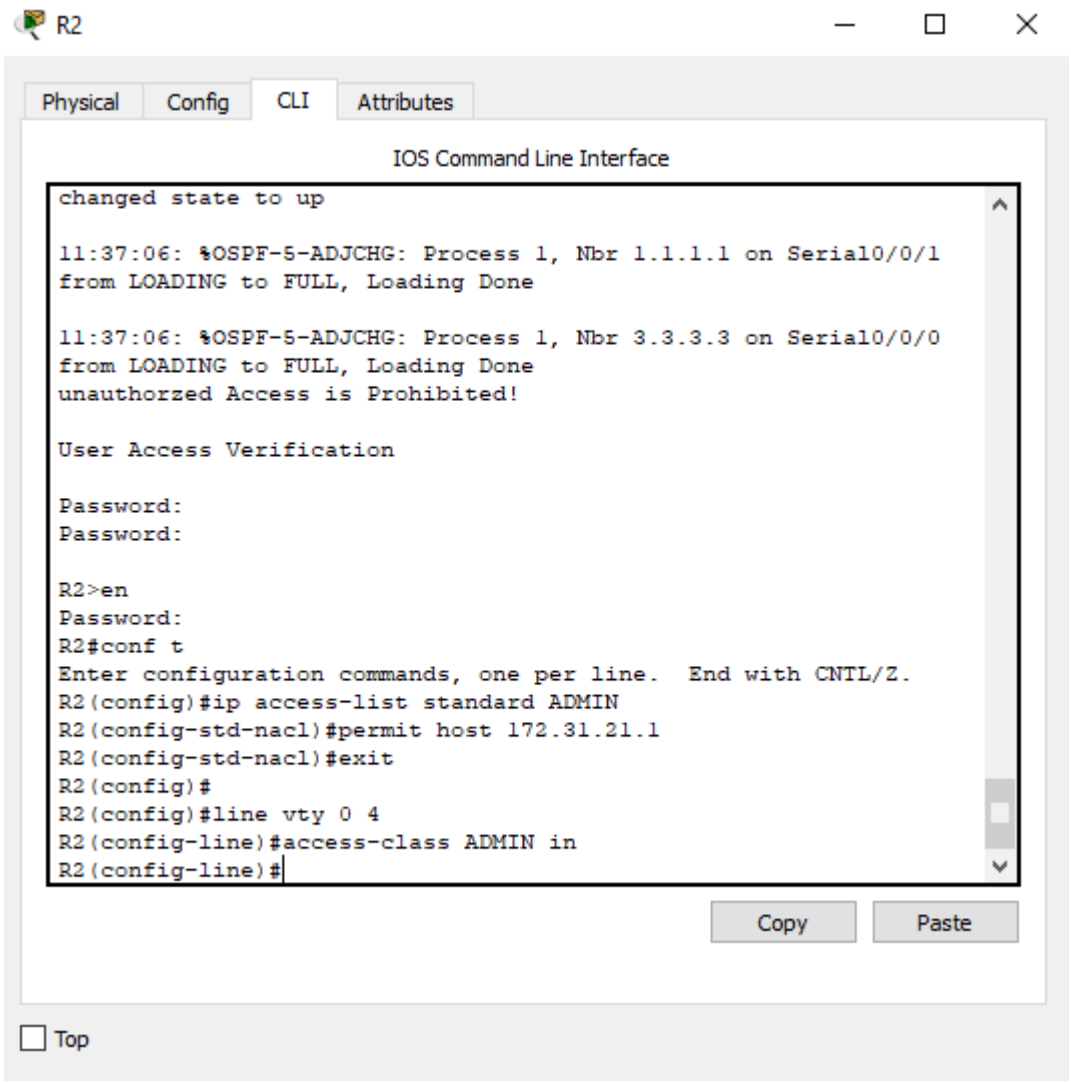


Figura 43

Asegurando la Red del Tráfico de Internet

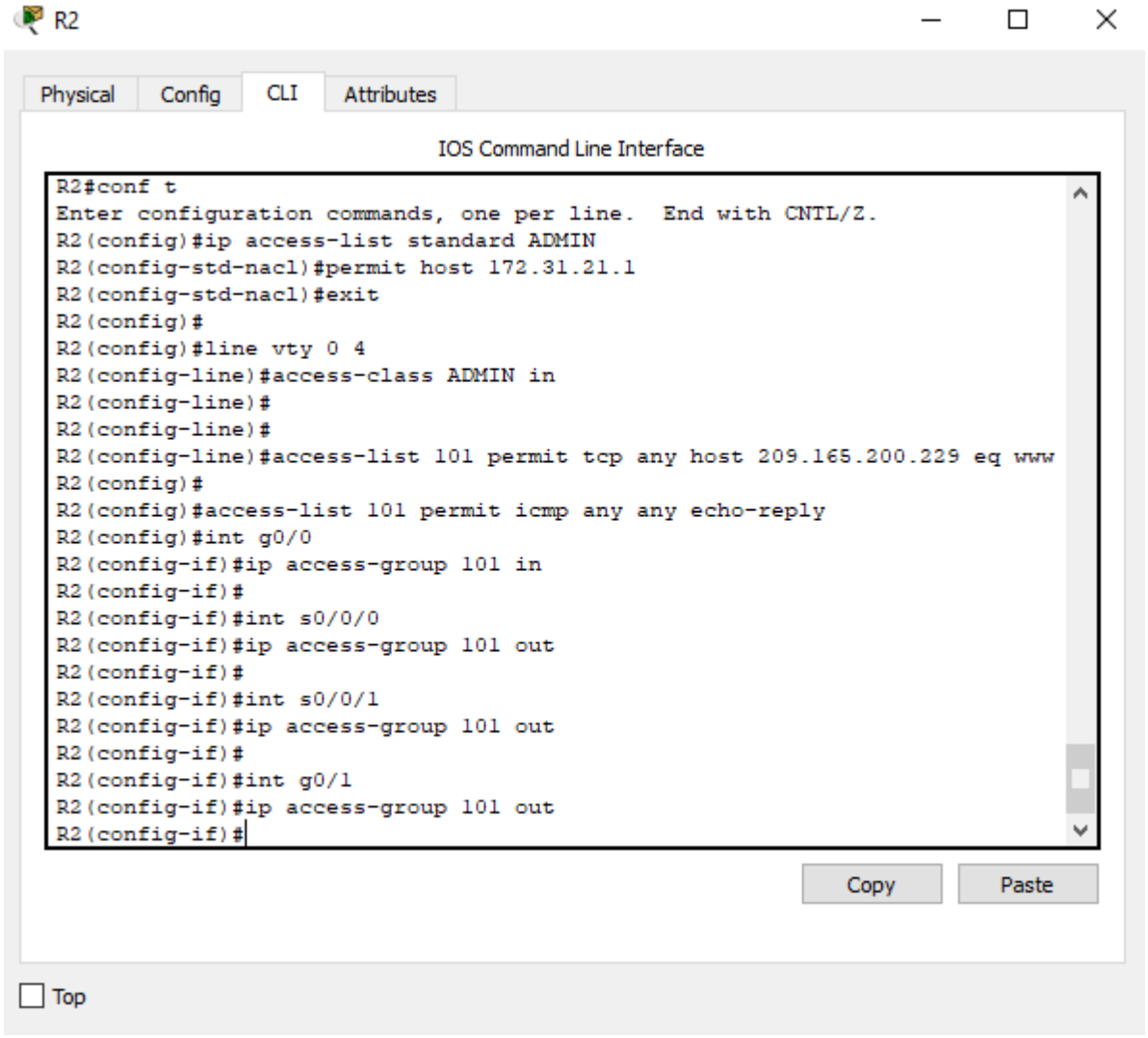


Figura 44

Verificando que la ACL esté funcionando

Ping PC-A

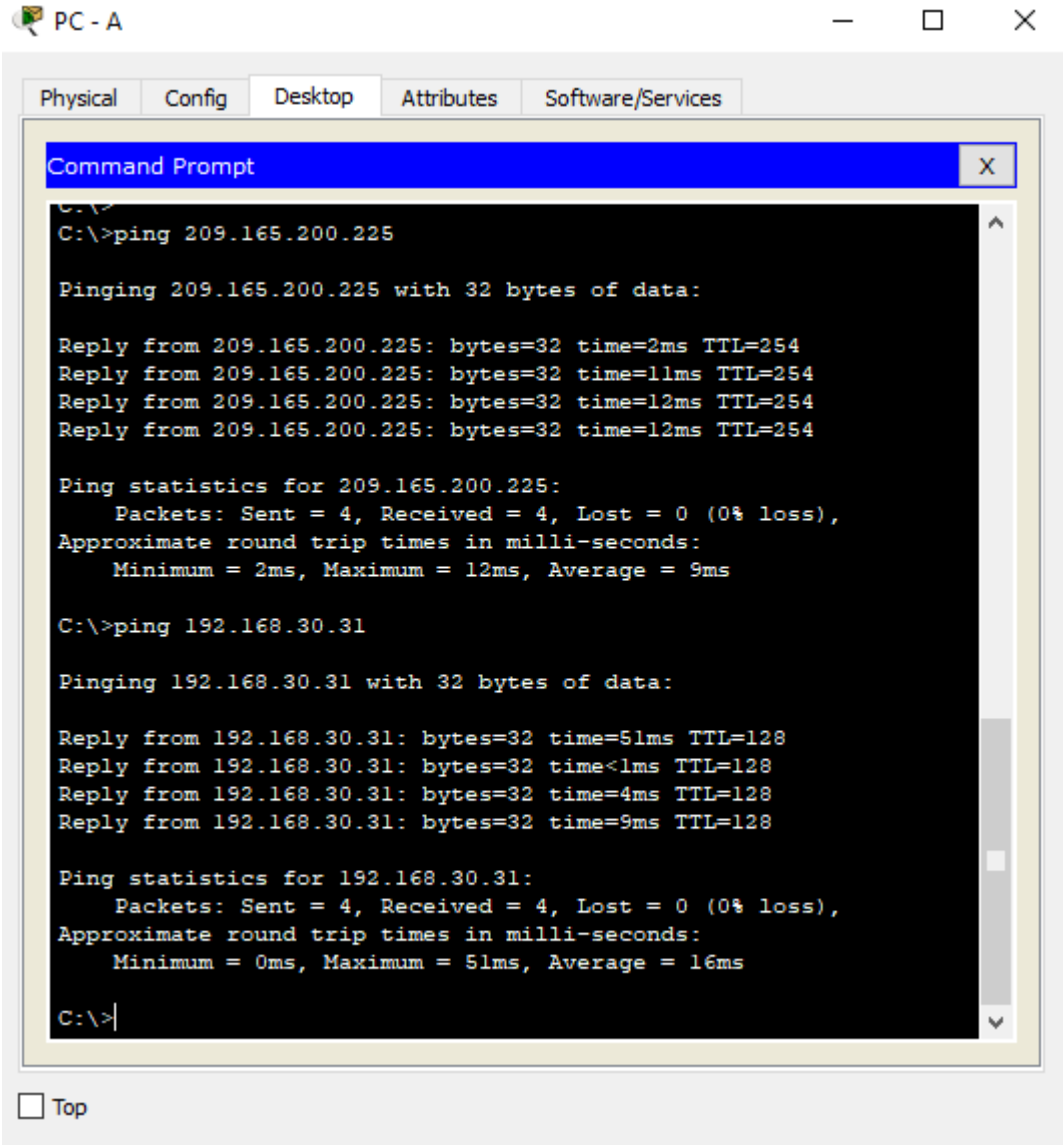


Figura 45

Ping PC-C

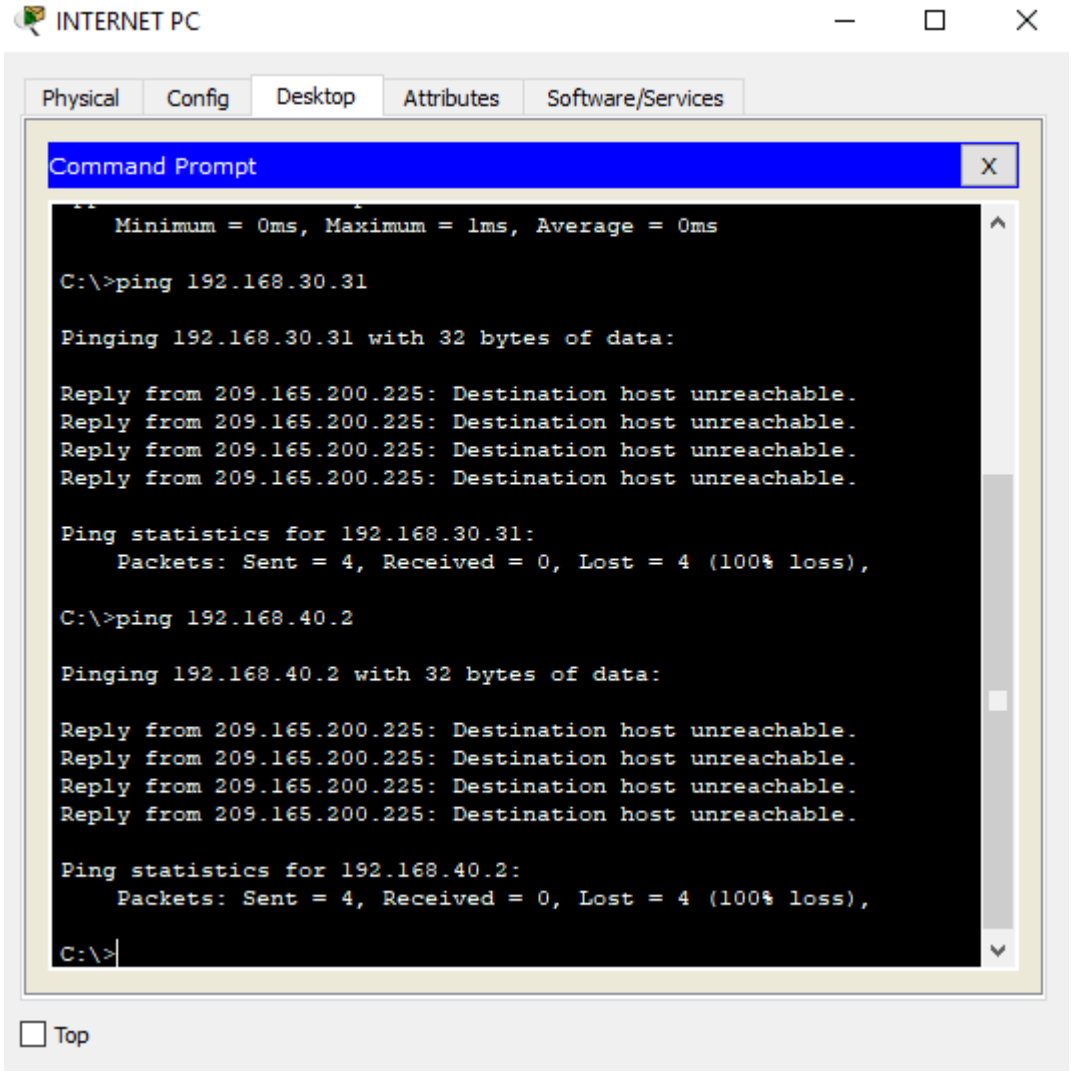


Figura 46

Desde R1, Ping a la Internet PC (Ping debería tener éxito).

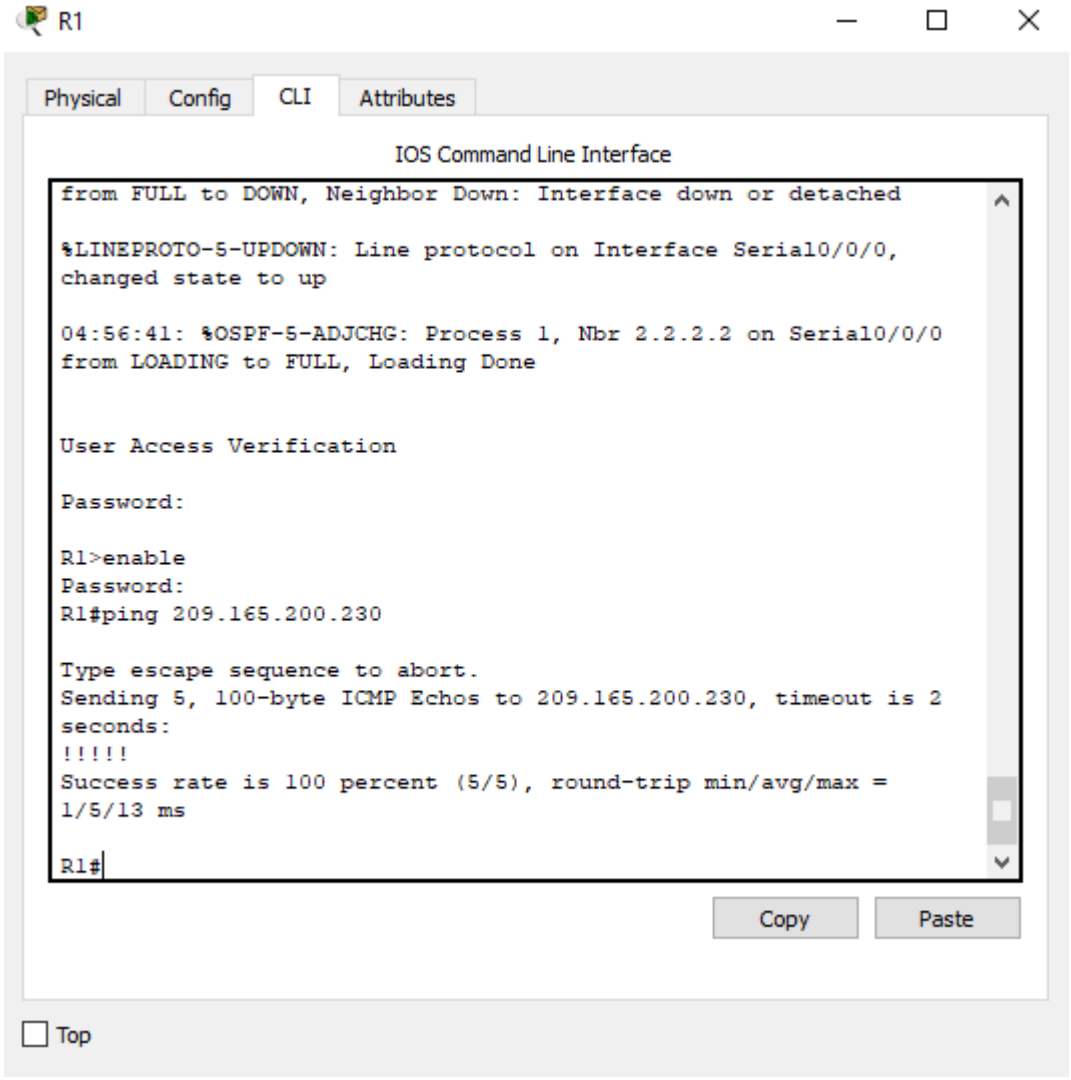


Figura 47

Verificación de la Información de las ACLs

Coincidencias que han recibido las listas de acceso.

```
R2#show access-lists
Standard IP access list 1
    10 permit 192.168.30.0 0.0.0.255
    20 permit 192.168.40.0 0.0.0.255
    30 permit 192.168.4.0 0.0.3.255
Standard IP access list ADMIN
    10 permit host 172.31.21.1
Extended IP access list 101
    10 permit tcp any host 209.165.200.229 eq www
    20 permit icmp any any echo-reply (10 match(es))

R2#
```

Figura 48

Diagrama de la Topología de Red totalmente Funcional

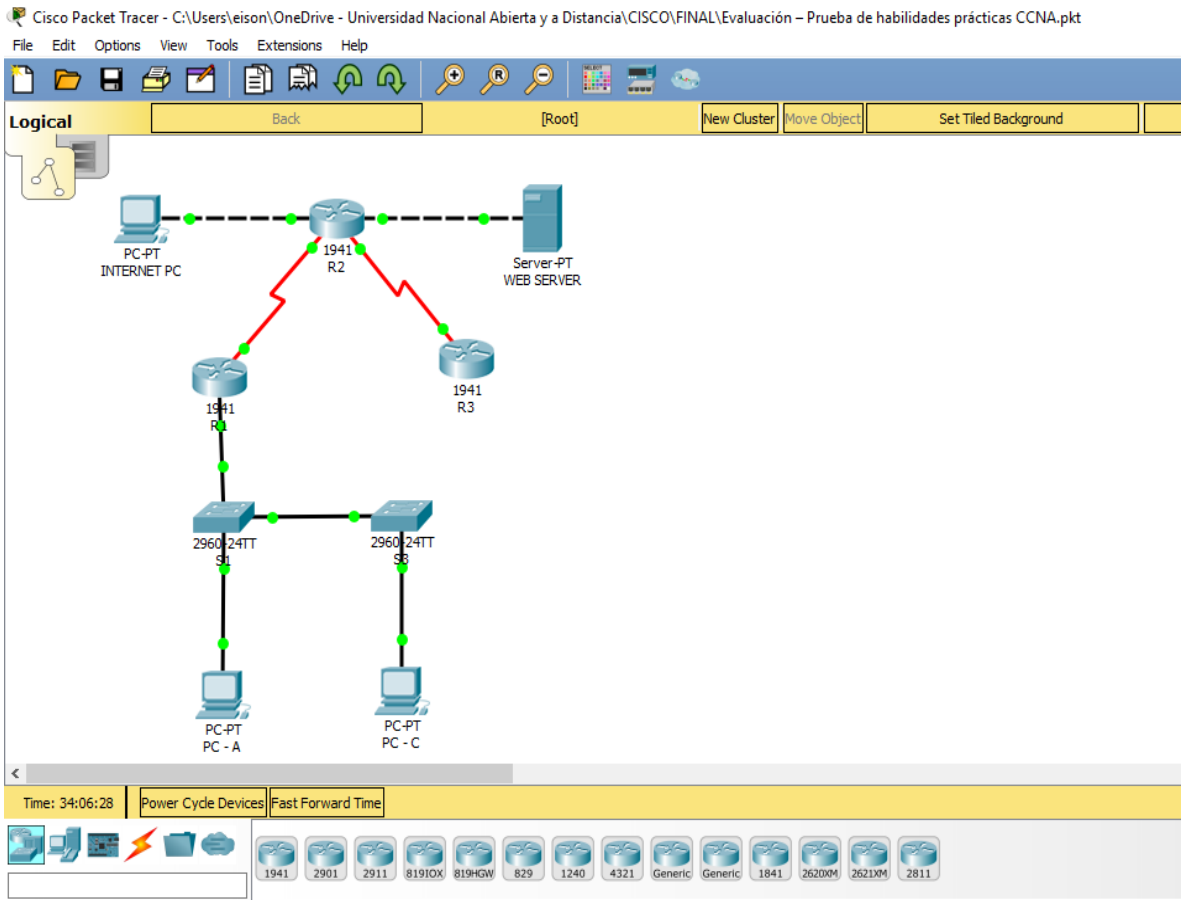


Figura 49

CONCLUSIONES

Realizando el desarrollo y practica de los principios básicos del routing y swiching de CCNA, la meta fue poder culminar en su totalidad las actividades propuestas por el diplomado y de esta manera entender los conceptos y tecnologías base de la una red.

Podemos indicar que fue de gran ayuda el material de apoyo proporcionado por el diplomado ya que nos ayudó a desarrollar las actitudes necesarias para planificar e implementar redes pequeñas con una variedad de aplicaciones.

Así como se indica en el desarrollo de la prueba de habilidades practicas CCNA, esta actividad practica se centró en el aprendizaje del funcionamiento de los routers y swiches y sus funciones en una red, en esta actividad aprendimos y pusimos en práctica todos los conceptos y conocimientos que obtuvimos a lo largo del curso.

BIBLIOGRAFIA

CISCO . (2014). Conceptos de routing. Obtenido de NETACAD: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#4.0.1.1

CISCO. (2014). Configuración y conceptos básicos de switching. Obtenido de NETACAD: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#2.0.1.1

CISCO. (2014). DHCP. Obtenido de NETACAD: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#10.0.1.1

CISCO. (2014). Enrutamiento entre VLAN. Obtenido de NETACAD: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#5.0.1.1

CISCO. (2014). Enrutamiento estatico. Obtenido de NETACAD: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#6.0.1.1

CISCO. (2014). Introduccióna a redes comutadas. Obtenido de NETACAD: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#1.0.1.1

CISCO. (2014). Listas de control . Obtenido de NETACAD: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#9.0.1.1

CISCO. (2014). OSPF de área única. Obtenido de NETACAD: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#8.0.1.1

CISCO. (2014). Routing dimámico. Obtenido de NETACAD: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#7.0.1.1

CISCO. (2014). VLAN. Obtenido de NETACAD: https://static-course-assets.s3.amazonaws.com/RSE503/es/index.html#3.0.1.1