

**Desarrollo e Implementación De Red Estructurada En Simulador Cisco  
Packet Tracer**

Elaborado por:  
Diego Andrés Sterling  
Cód. 1117494462

Grupo: 203092\_30

Presentado a:  
Efraín Alejandro Pérez

Universidad Nacional Abierta y a Distancia Unad  
Escuela de Ciencias Básicas, Tecnología e Ingeniería  
Programa de Ingeniería de Sistemas  
Diplomado de Profundización Cisco  
Florencia – Caquetá  
Mayo – 2018

## Tabla de Contenido

Introducción.....	3
Desarrollo e Implementación De Red Estructurada En Simulador Cisco Packet Tracer .....	4
1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario .....	5
2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios: .....	13
3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida. ....	18
4. En el Switch 3 deshabilitar DNS lookup .....	24
5. Asignar direcciones IP a los Switches acorde a los lineamientos.....	24
6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.....	24
7. Implement DHCP and NAT for IPv4.....	25
8. Configurar NAT en R2 para permitir que los host puedan salir a internet .....	26
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.....	28
10. 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.....	28
11. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.....	29
Conclusiones.....	33
Bibliografía .....	34

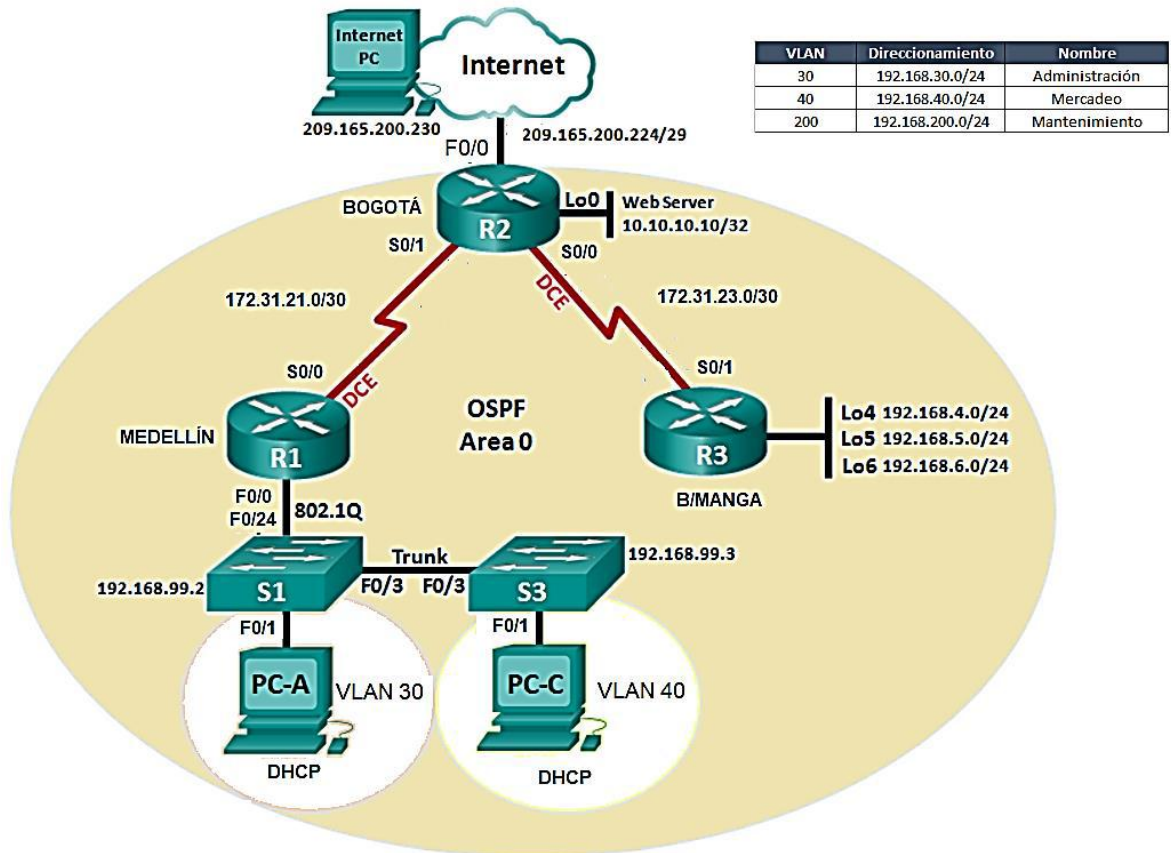
## **Introducción**

En la presente actividad se desarrolla y analiza las temáticas de cisco CCNA1 y CCNA2 enfocadas en la identificación y solución de un problema planteado y relacionado con el enrutamiento mediante comandos del ios. Conoceremos los diferentes protocolos de routing, la implementación y configuración básica de OSPF, se analizaran y desarrollaran las instrucciones necesarias para utilizar las ACL estándar y extendidas en un router Cisco, implementaremos cada una de las funciones de DHCPv4 y se analizara la implementación de NAT con el fin de usar de forma más eficaz las direcciones IPv4, lo anterior se ejecuta utilizando la información contenida en la prueba de habilidades prácticas de la plataforma de Cisco Networking Academy, desarrollando un componente practico con la ayuda del software Packet Tracer.

## Desarrollo e Implementación De Red Estructurada En Simulador Cisco Packet Tracer

**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.

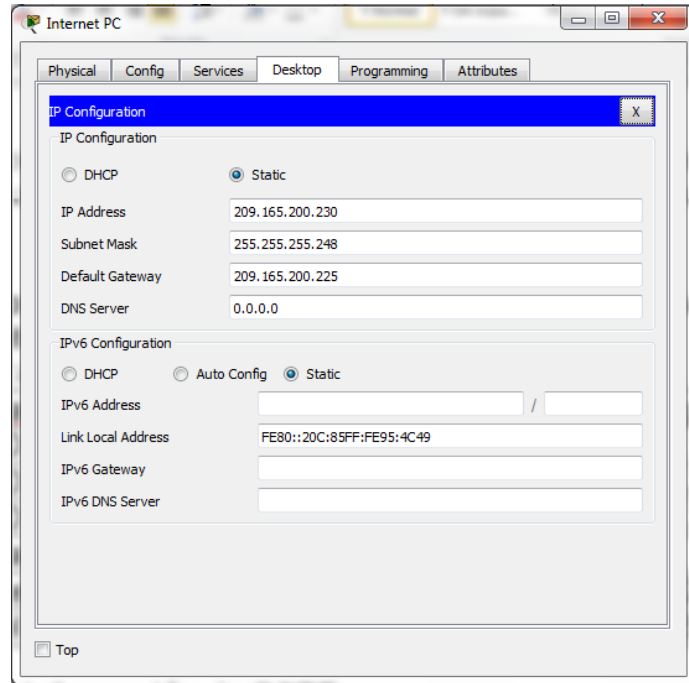
### Topología de red



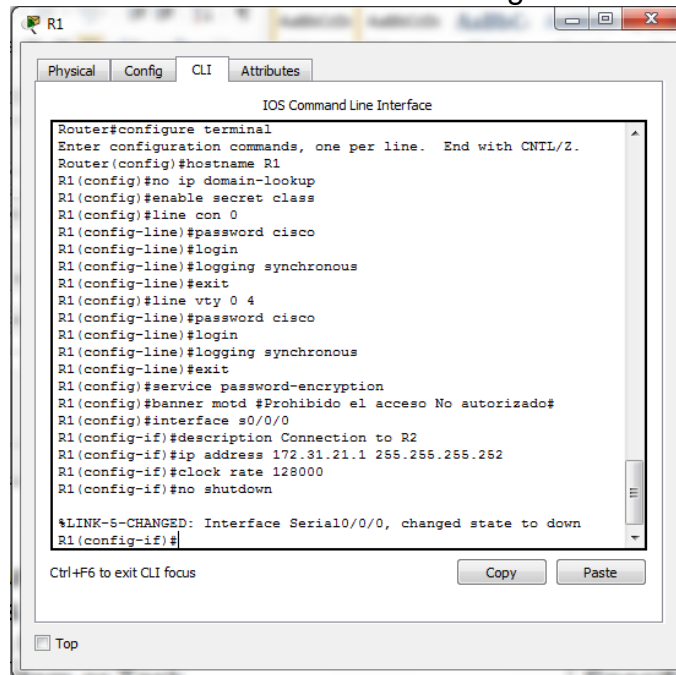
**Nota:** En los router R1 y R2 no se utiliza las interfaces F0/0, en cambio se utiliza G0/0 y el web server se configura con un equipo conectado a G0/1

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

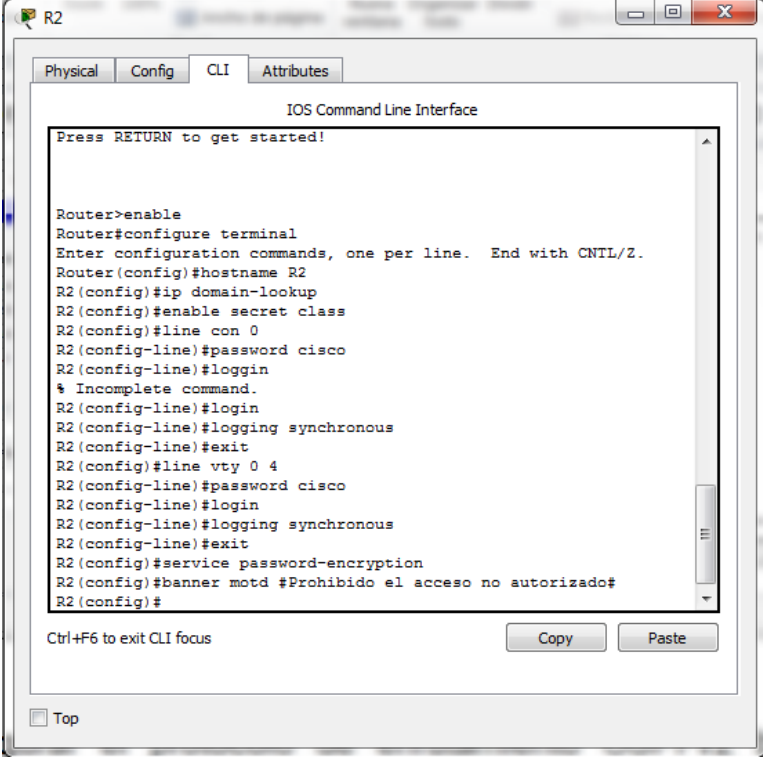
### Configuración de Internet Pc



### Configuración de Router 1 – La G0/0 se configura mas adelante



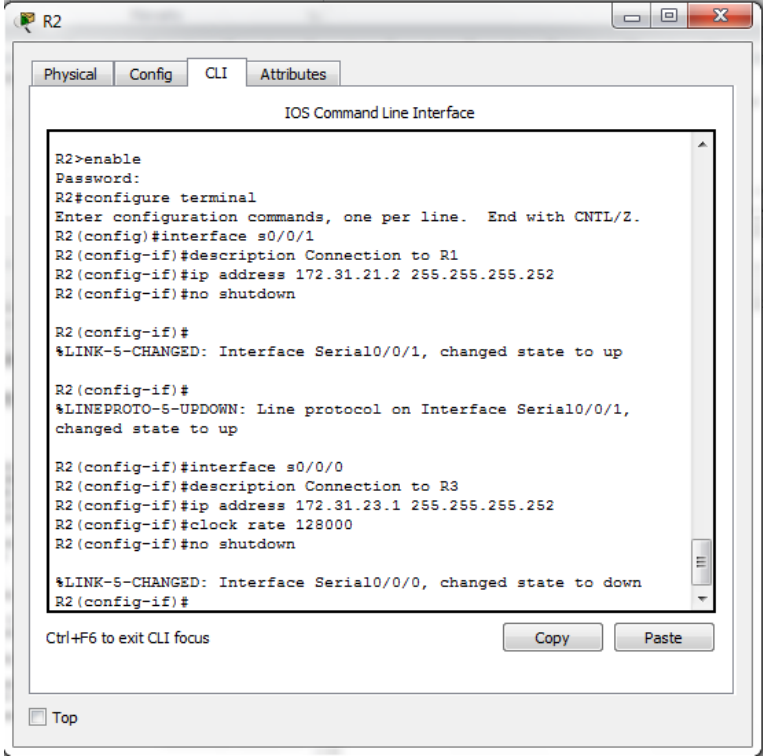
## Configuración de Router 2



The screenshot shows the CLI window for Router 2. The window title is 'R2' and it has tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The text in the window is as follows:

```
Press RETURN to get started!  
  
Router>enable  
Router#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)#hostname R2  
R2(config)#ip domain-lookup  
R2(config)#enable secret class  
R2(config)#line con 0  
R2(config-line)#password cisco  
R2(config-line)#login  
% Incomplete command.  
R2(config-line)#login  
R2(config-line)#logging synchronous  
R2(config-line)#exit  
R2(config)#line vty 0 4  
R2(config-line)#password cisco  
R2(config-line)#login  
R2(config-line)#logging synchronous  
R2(config-line)#exit  
R2(config)#service password-encryption  
R2(config)#banner motd #Prohibido el acceso no autorizado#  
R2(config)#
```

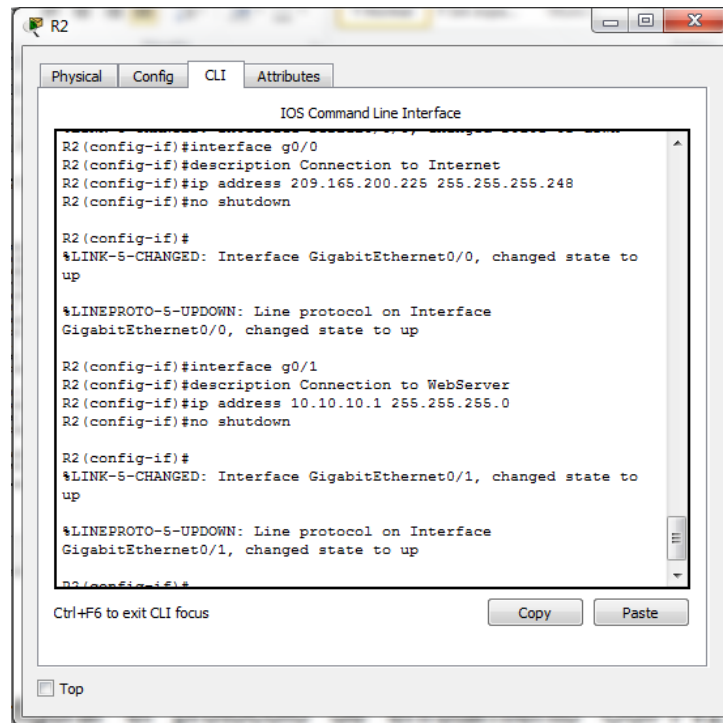
At the bottom of the window, there are buttons for 'Copy' and 'Paste', and a 'Top' button.



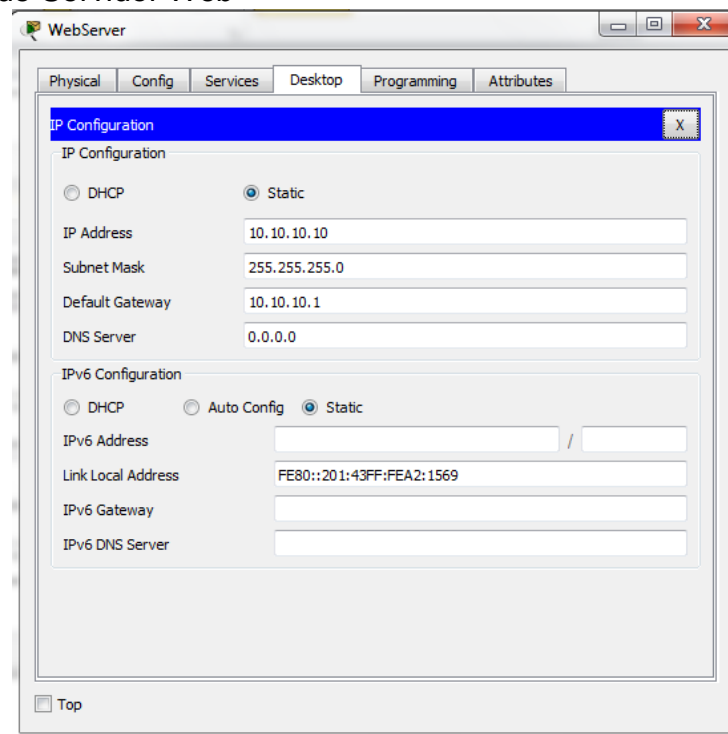
The screenshot shows the CLI window for Router 2, continuing the configuration. The text in the window is as follows:

```
R2>enable  
Password:  
R2#configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
R2(config)#interface s0/0/1  
R2(config-if)#description Connection to R1  
R2(config-if)#ip address 172.31.21.2 255.255.255.252  
R2(config-if)#no shutdown  
  
R2(config-if)#  
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up  
  
R2(config-if)#  
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,  
changed state to up  
  
R2(config-if)#interface s0/0/0  
R2(config-if)#description Connection to R3  
R2(config-if)#ip address 172.31.23.1 255.255.255.252  
R2(config-if)#clock rate 128000  
R2(config-if)#no shutdown  
  
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down  
R2(config-if)#
```

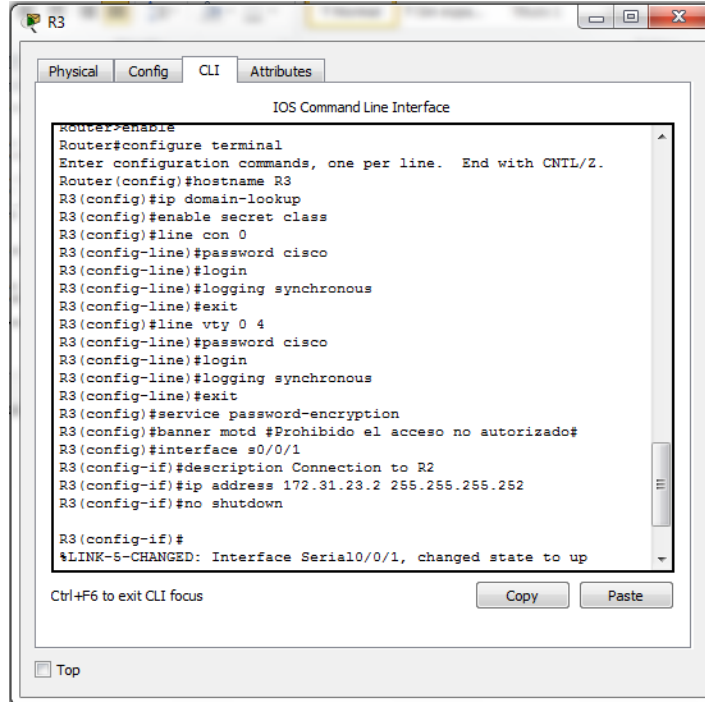
At the bottom of the window, there are buttons for 'Copy' and 'Paste', and a 'Top' button.



## Configuracion de Servidor Web



## Configuracion de Router 3

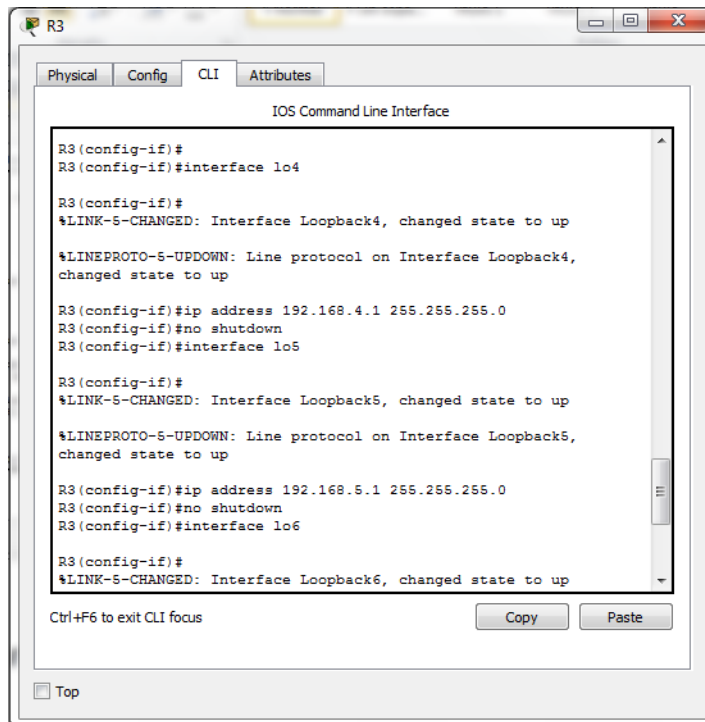


The screenshot shows the CLI window for Router 3. The window title is 'R3' and it has tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The terminal output shows the following commands and their outputs:

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R3
R3(config)#ip domain-lookup
R3(config)#enable secret class
R3(config)#line con 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#logging synchronous
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd #Prohibido el acceso no autorizado#
R3(config)#interface s0/0/1
R3(config-if)#description Connection to R2
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#no shutdown

R3(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
```

At the bottom of the window, there is a 'Top' button and a 'Ctrl+F6 to exit CLI focus' message. There are also 'Copy' and 'Paste' buttons.



The screenshot shows the CLI window for Router 3, continuing the configuration. The terminal output shows the following commands and their outputs:

```
R3(config-if)#
R3(config-if)#interface lo4

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4,
changed state to up

R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface lo5

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up

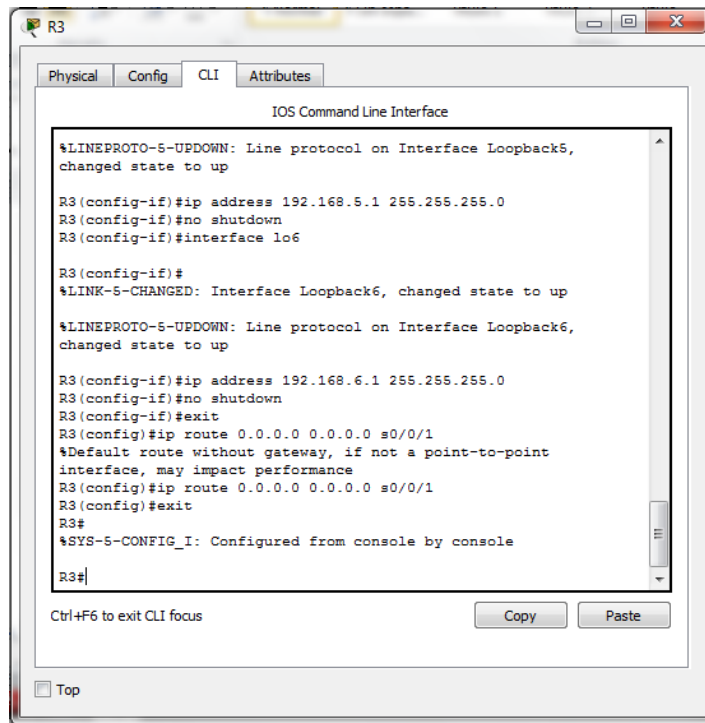
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5,
changed state to up

R3(config-if)#ip address 192.168.5.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface lo6

R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
```

At the bottom of the window, there is a 'Top' button and a 'Ctrl+F6 to exit CLI focus' message. There are also 'Copy' and 'Paste' buttons.





The screenshot shows a Cisco IOS Command Line Interface window for router R3. The window has tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following configuration commands and system messages:

```
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5,
changed state to up

R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#interface lo6

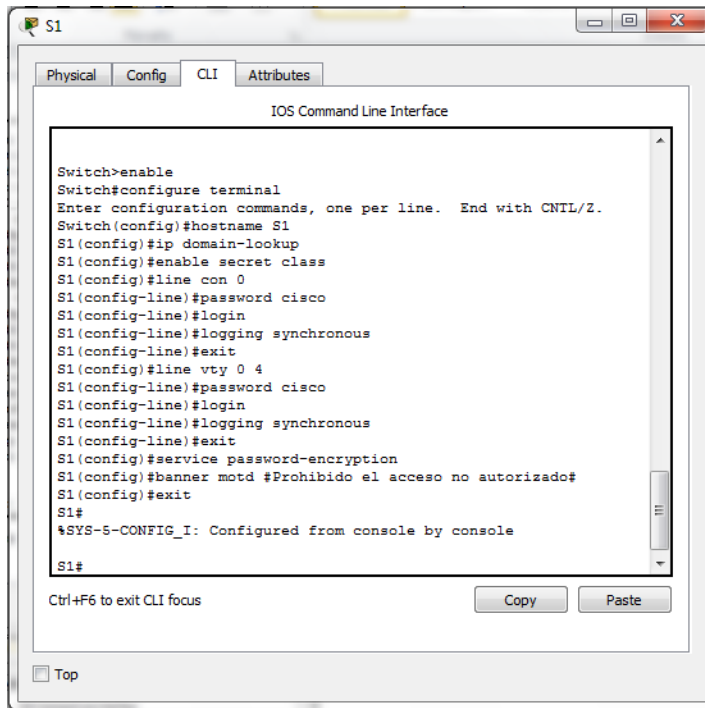
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6,
changed state to up

R3(config-if)#ip address 192.168.6.1 255.255.255.0
R3(config-if)#no shutdown
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point
interface, may impact performance
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#
```

At the bottom of the window, there are buttons for "Copy" and "Paste", and a "Top" button. A note indicates "Ctrl+F6 to exit CLI focus".

## Configuracion de Switch 1



The screenshot shows a Cisco IOS Command Line Interface window for switch S1. The window has tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the following configuration commands and system messages:

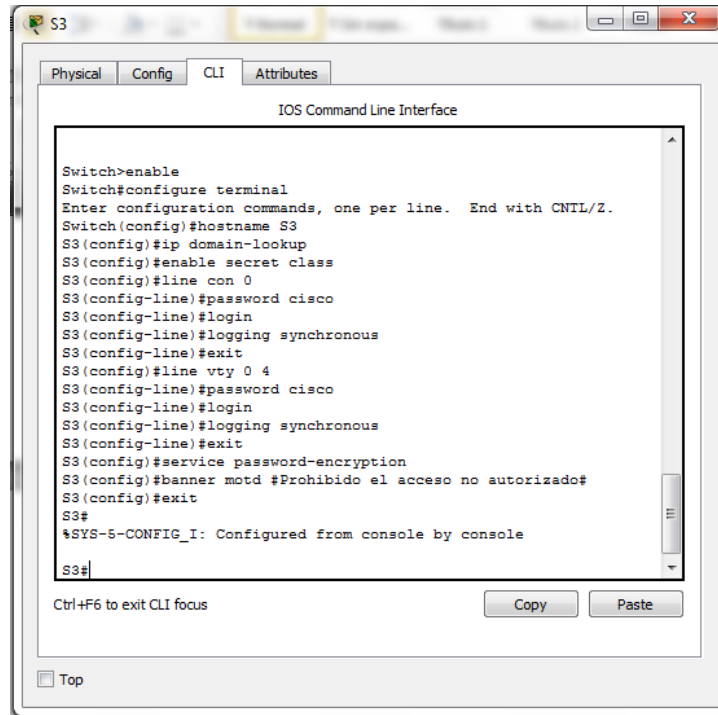
```
IOS Command Line Interface

Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#ip domain-lookup
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#logging synchronous
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd #Prohibido el acceso no autorizado#
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#
```

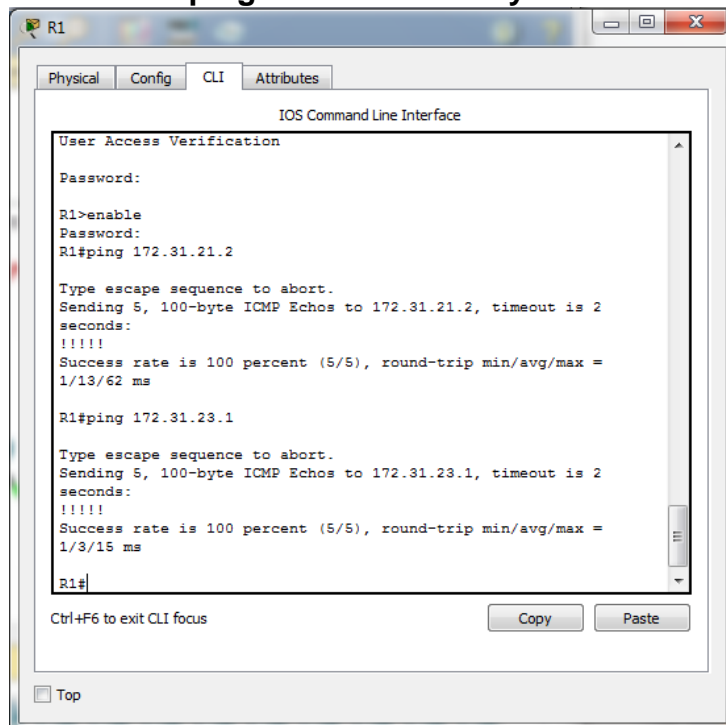
At the bottom of the window, there are buttons for "Copy" and "Paste", and a "Top" button. A note indicates "Ctrl+F6 to exit CLI focus".

## Configuración de Switch 3



```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#ip domain-lookup
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #Prohibido el acceso no autorizado#
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#
```

## Verificar la conectividad – ping entre los router y servidores



```
User Access Verification

Password:

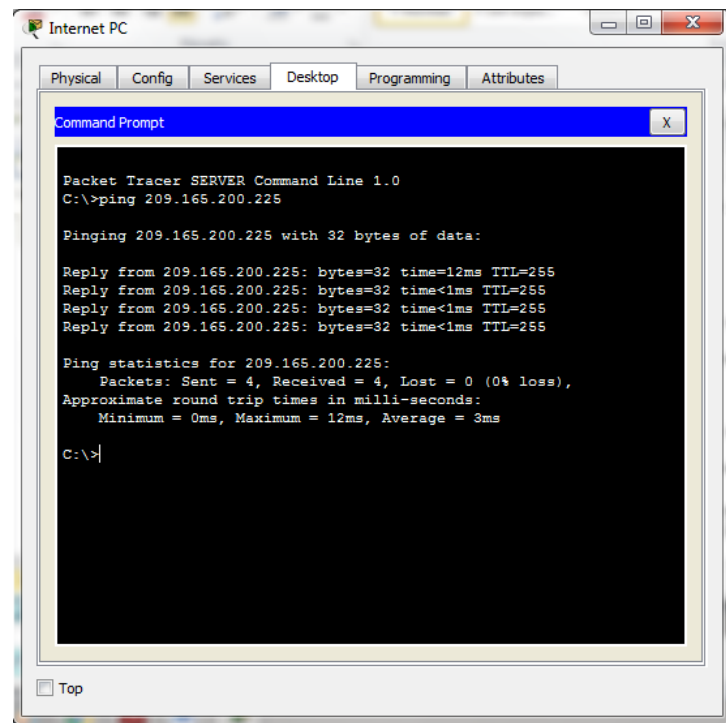
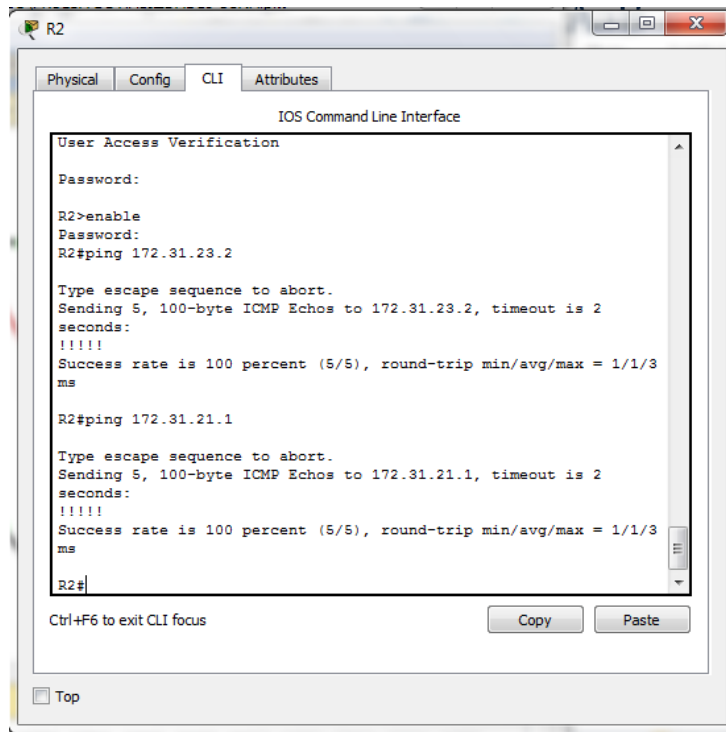
R1>enable
Password:
R1#ping 172.31.21.2

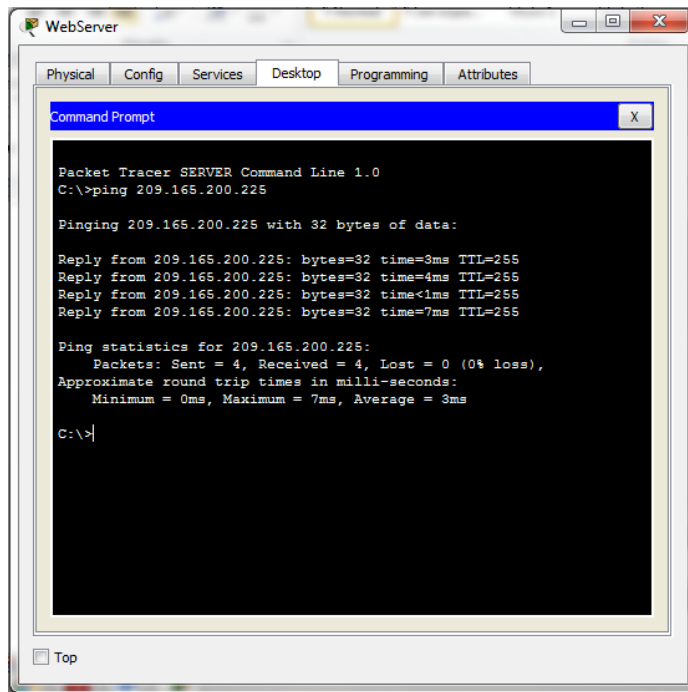
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/13/62 ms

R1#ping 172.31.23.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.1, timeout is 2
seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
1/3/15 ms

R1#
```





- 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

```

R1>enable
Password:
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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 192.168.99.0 0.0.0.255 area 0
R1(config-router)#
R1(config-router)#passive-interface g0/0.30
R1(config-router)#passive-interface g0/0.40
R1(config-router)#passive-interface g0/0.200
R1(config-router)#exit
R1(config)#interface s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#ip ospf cost 7500
R1(config-if)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
R1#
  
```

```

R2>enable
Password:
R2#configure terminal
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 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 172.31.21.0 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 g0/1
R2(config-router)#
R2(config-router)#interface s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#ip ospf cost 7500
R2(config-if)#interface s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#exit
R2(config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
  
```

```

R3>enable
Password:
R3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#
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)#
01:47:45: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/1
from LOADING to FULL, Loading Done

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)#exit
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#

```

### 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.

```

01:47:45: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/0/0 from LOADING to
FULL, Loading Done

Prohibido el acceso no autorizado

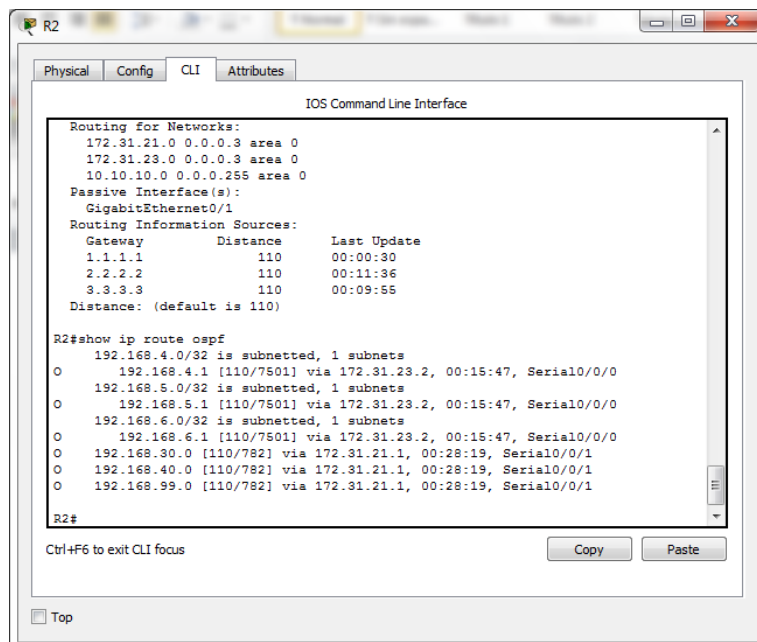
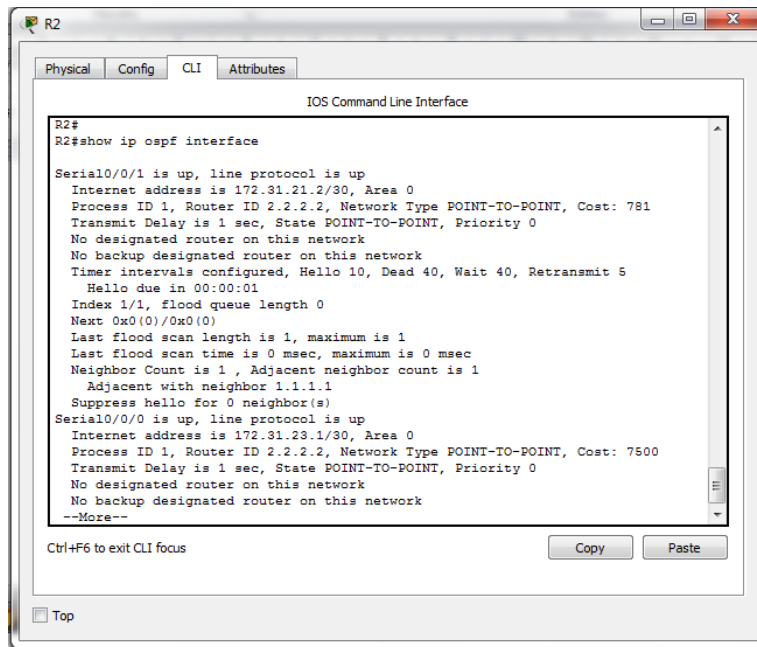
User Access Verification

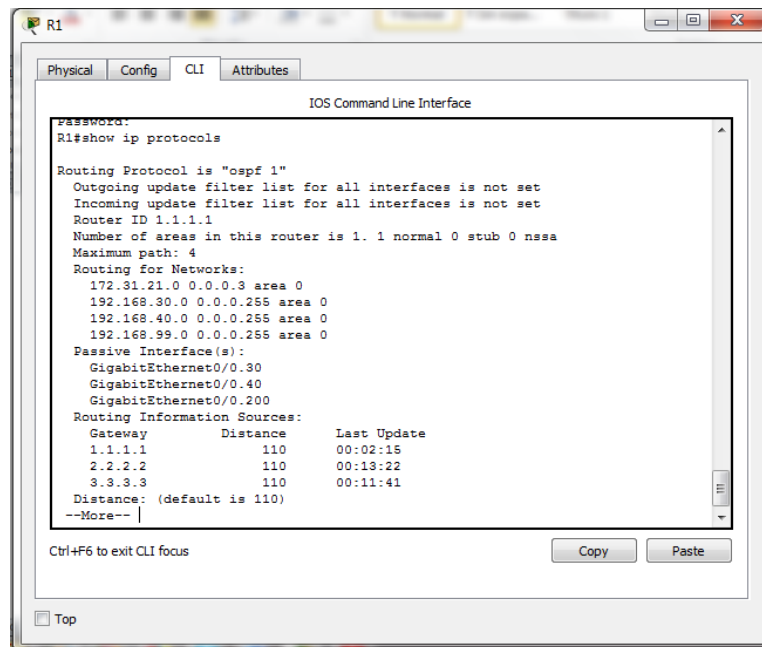
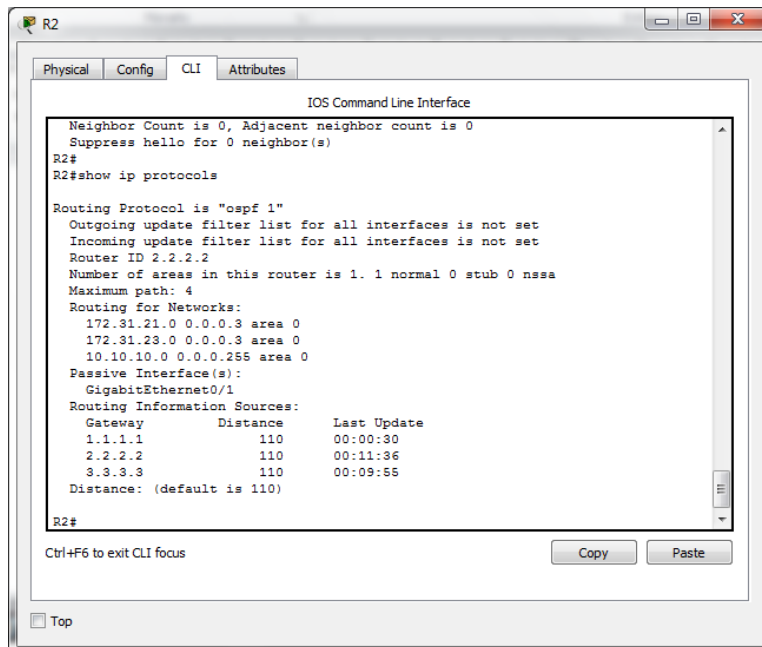
Password:

R2>enable
Password:
R2#show ip ospf neighbor

Neighbor ID    Pri  State           Dead Time   Address        Interface
3.3.3.3        0    FULL/ -         00:00:36   172.31.23.2   Serial0/0/0
1.1.1.1        0    FULL/ -         00:00:39   172.31.21.1   Serial0/0/1
R2#
R2#

```







R3

Physical Config CLI Attributes

IOS Command Line Interface

```
R3>enable
Password:
R3#show ip protocols

Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 3.3.3.3
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.23.0 0.0.0.3 area 0
    192.168.4.0 0.0.3.255 area 0
  Passive Interface(s):
    Loopback4
    Loopback5
    Loopback6
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1           110          00:03:48
    2.2.2.2           110          00:14:54
    3.3.3.3           110          00:13:13
  Distance: (default is 110)

R3#
```

Ctrl+F6 to exit CLI focus

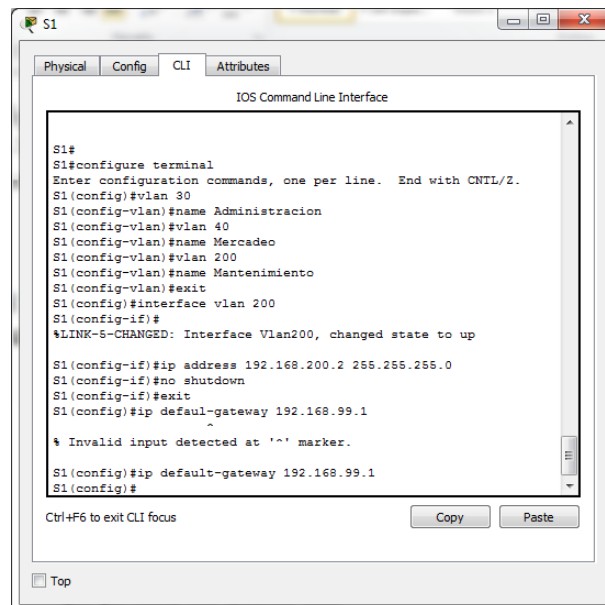
Copy Paste

Top

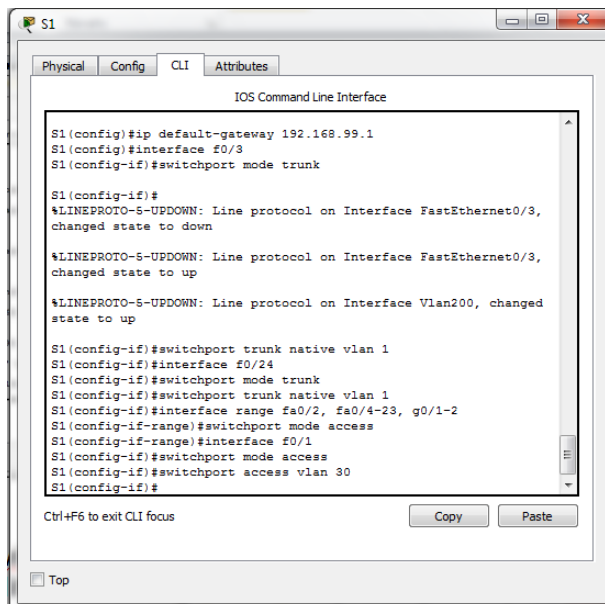
3. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

Después de terminar la configuración de las VLANs, no pasaba las pruebas con el comando ping, se verifica y se identifica que se debe cambiar el direccionamiento de la VLAN 200, ya que la dirección que da la topología no corresponde con el direccionamiento de los switch. Al realizar el cambio y corregir esto se realizan las pruebas de comunicación con el comando ping sin contratiempos, en los pantallazos al final se puede ver claramente. Las gráficas resaltadas en rojo indican las correcciones y cambios que se realizan para que funcionen las VLAN.

VLAN 200 – 192.168.200.0/24 es remplazada por 192.168.99.0/24



```
S1#
S1#configure terminal
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)#interface vlan 200
S1(config-if)#
%LINK-5-CHANGED: 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)#exit
S1(config)#ip default-gateway 192.168.99.1
~
% Invalid input detected at '^' marker.
S1(config)#ip default-gateway 192.168.99.1
S1(config)#
```



```
S1(config)#ip default-gateway 192.168.99.1
S1(config)#interface 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)#interface f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface range fa0/2, fa0/4-23, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#interface f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#
```

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1(config-if-range)#exit
S1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

### Corrección realizada a la vlan 200

S1

Physical Config CLI Attributes

IOS Command Line Interface

```
password 7 082245D0A16
logging synchronous
login
line vty 5 15
  login
  !
  !
  !
end

S1#
S1#
S1#
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan 200
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console
S1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

S3

Physical Config CLI Attributes

IOS Command Line Interface

```
% Invalid input detected at '^' marker.

S3(config)#vlan 30
S3(config-vlan)#name Administrador
S3(config-vlan)#vlan 40
S3(config-vlan)#name Mercadeo
S3(config-vlan)#vlan 200
S3(config-vlan)#Mantenimiento
^
% Invalid input detected at '^' marker.

S3(config-vlan)#name Mantenimiento
S3(config-vlan)#exit
S3(config)#interface 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 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

S3

Physical Config CLI Attributes

IOS Command Line Interface

```
% Invalid input detected at '^' marker.

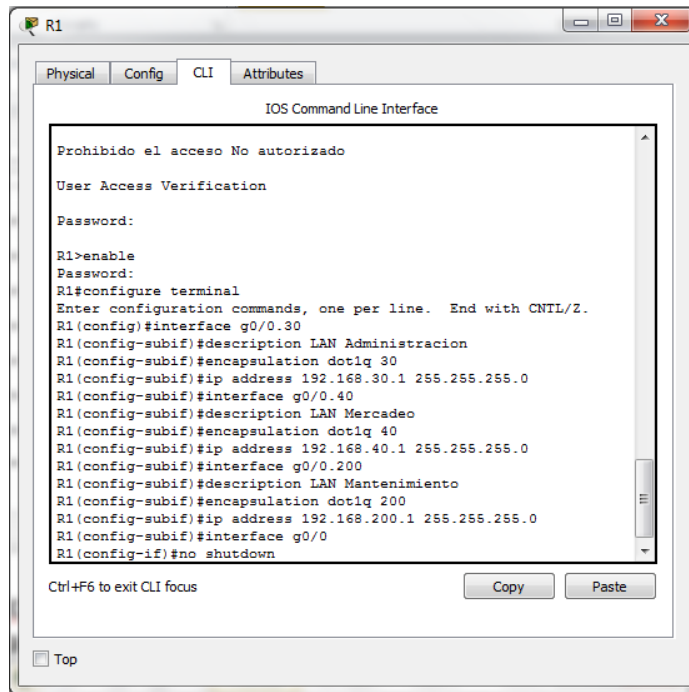
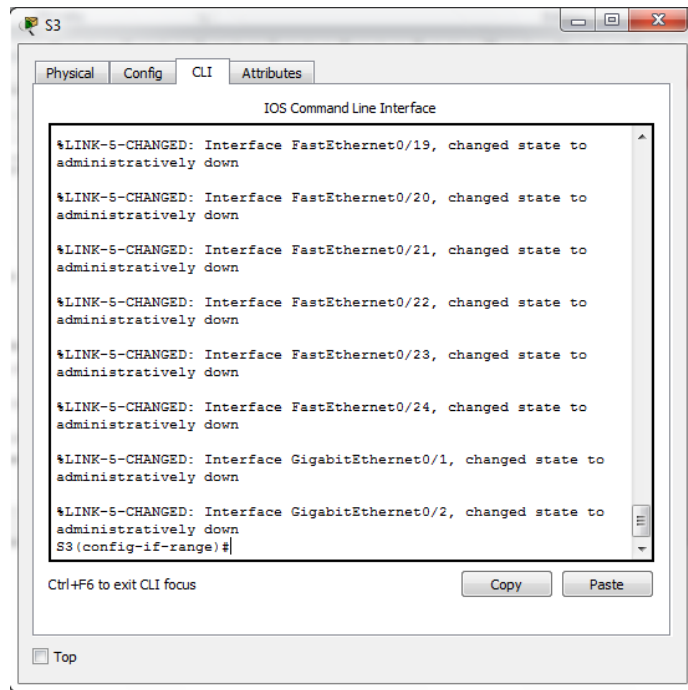
S3(config-vlan)#name Mantenimiento
S3(config-vlan)#exit
S3(config)#interface vlan 200
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed
state to up

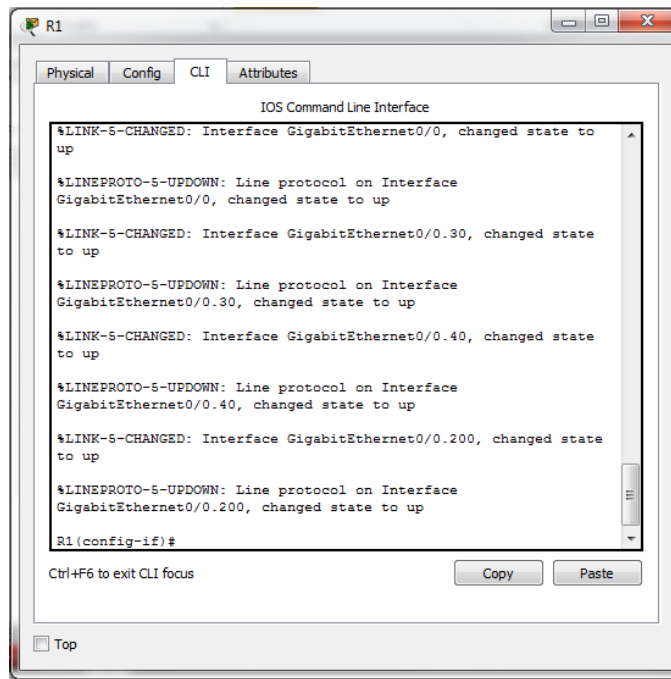
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
S3(config)#
S3(config)#interface fa0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#interface range fa0/1-2, fa0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#interface fa0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#
```

Ctrl+F6 to exit CLI focus

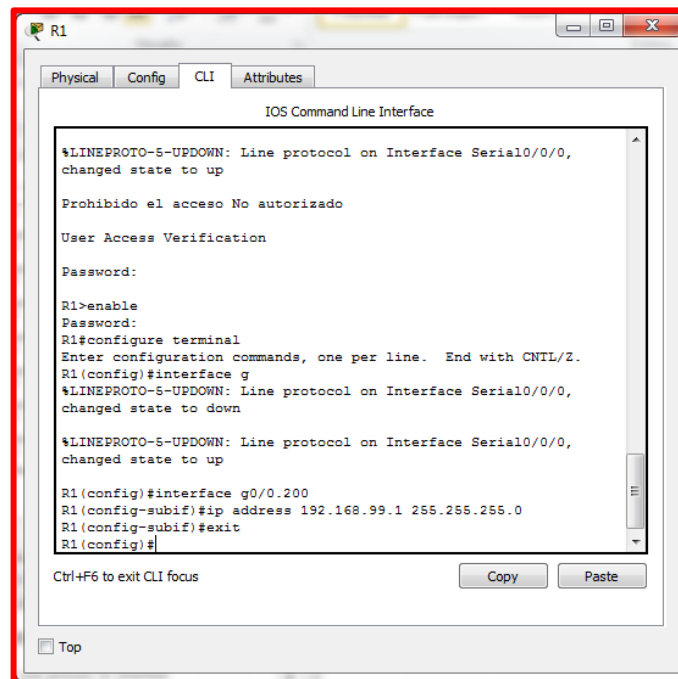
Copy Paste

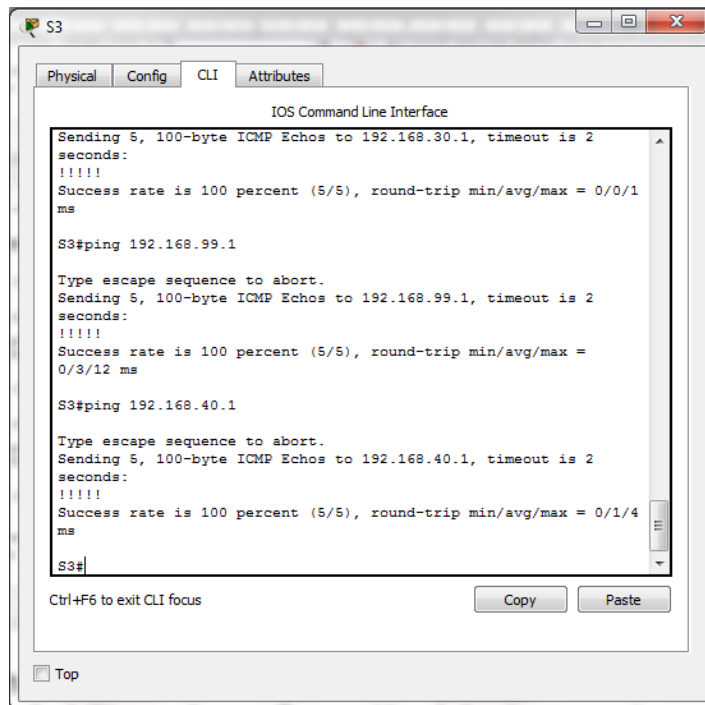
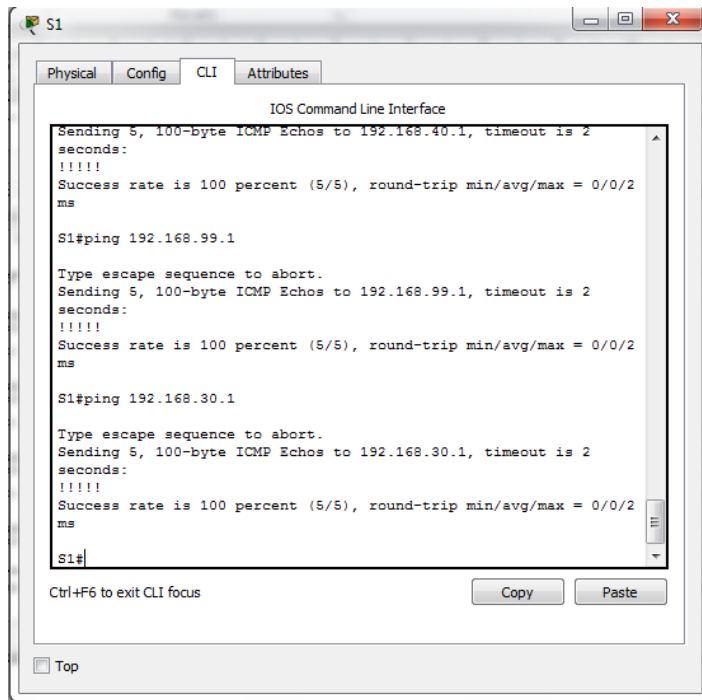
Top





### Corrección realizada a la vlan 200





4. En el Switch 3 deshabilitar DNS lookup  
Ya se encuentra deshabilitado. Se deshabilita en la configuración del primer punto

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S3
S3(config)#ip domain-lookup
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#logging synchronous
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd #Prohibido el acceso no autorizado#
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
S3#
```

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

### Parámetros ya configurados en los puntos 1 y 3

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

### Parámetros ya configurados en el punto 3

```
%LINK-5-CHANGED: Interface FastEthernet0/18, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S1(config-if-range)#exit
S1(config)#
```

```
%LINK-5-CHANGED: Interface FastEthernet0/19, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/20, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/21, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/22, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/23, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-5-CHANGED: Interface GigabitEthernet0/2, changed state to administratively down
S3(config-if-range)#
```



## 7. 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.

```

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

00:00:10: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0 from LOADING to FULL, Loading Done

Prohibido el acceso No autorizado

User Access Verification

Password:

R1>enable
Password:
R1#configure terminal
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)#
R1(config)#
  
```

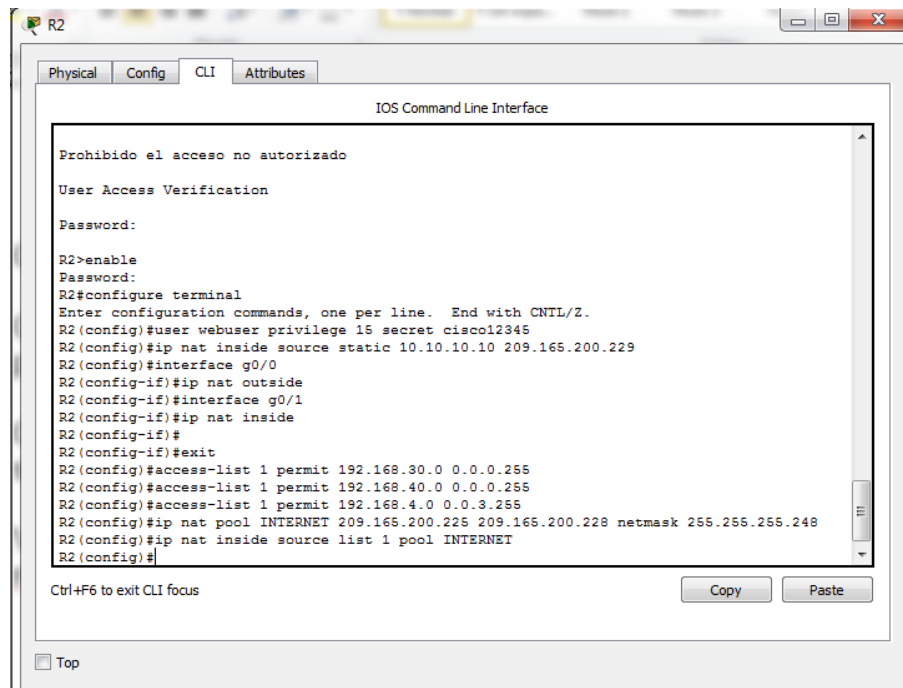
Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway

```

R1>enable
Password:
R1#configure terminal
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)#
R1(config)#ip dhcp pool ADMINISTRACION
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 MERCADEO
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
R1(dhcp-config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#
  
```

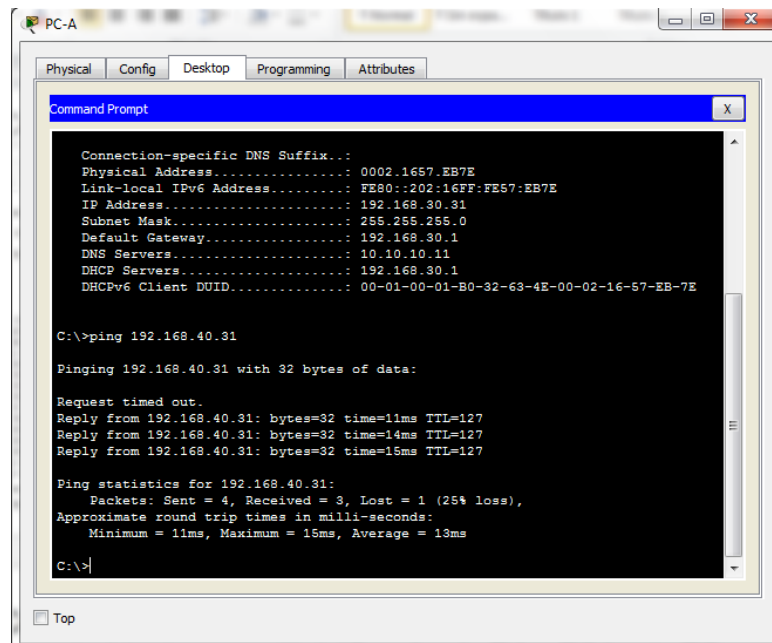
## 8. Configurar NAT en R2 para permitir que los host puedan salir a internet



The screenshot shows the CLI window for router R2. The window title is 'R2' and it has tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The main area is titled 'IOS Command Line Interface'. The text in the window shows the following commands and their outputs:

```
Prohibido el acceso no autorizado
User Access Verification
Password:
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#interface g0/0
R2(config-if)#ip nat outside
R2(config-if)#interface g0/1
R2(config-if)#ip nat inside
R2(config-if)#
R2(config-if)#exit
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)#
```

At the bottom of the window, there is a 'Ctrl+F6 to exit CLI focus' message and 'Copy' and 'Paste' buttons. A 'Top' button is also visible at the bottom left.



The screenshot shows the Command Prompt window for PC-A. The window title is 'PC-A' and it has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes'. The main area is titled 'Command Prompt'. The text in the window shows the following commands and their outputs:

```
Connection-specific DNS Suffix...:
Physical Address.....: 0002.1657.EB7E
Link-local IPv6 Address.....: FE80::202:16FF:FE57:EB7E
IP Address.....: 192.168.30.31
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.30.1
DNS Servers.....: 10.10.10.11
DHCP Servers.....: 192.168.30.1
DHCPv6 Client DUID.....: 00-01-00-01-B0-32-63-4E-00-02-16-57-EB-7E

C:\>ping 192.168.40.31

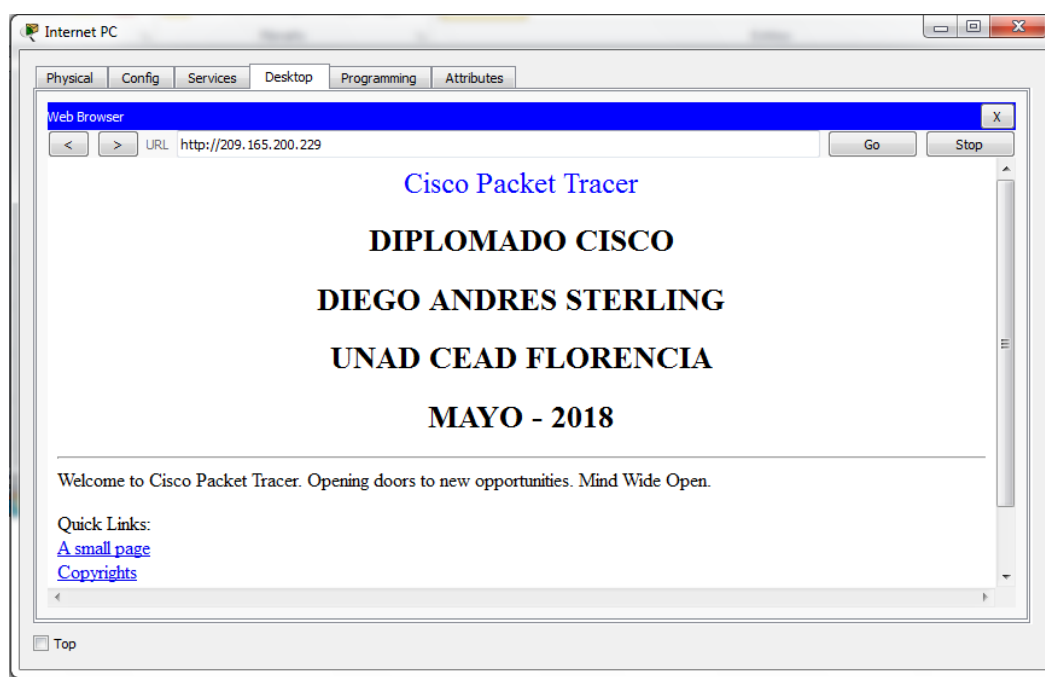
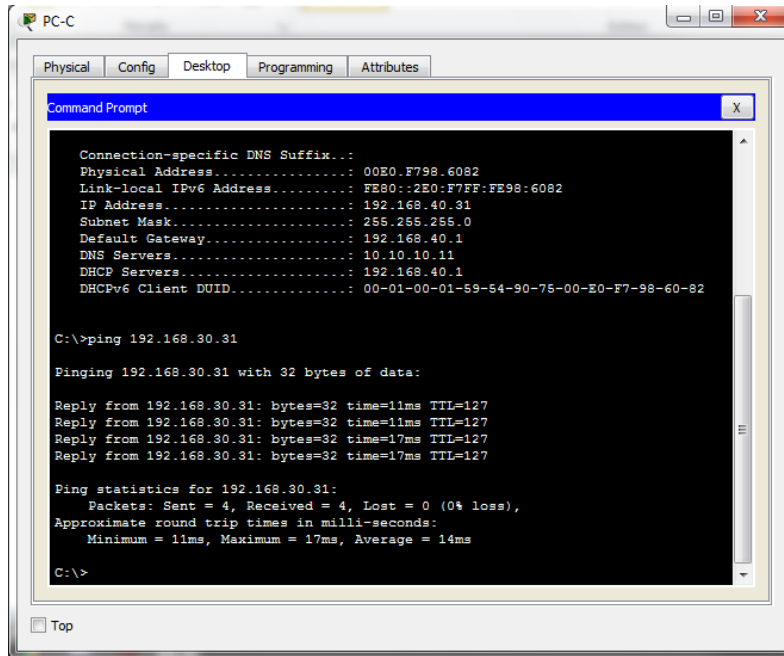
Pinging 192.168.40.31 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.31: bytes=32 time=11ms TTL=127
Reply from 192.168.40.31: bytes=32 time=14ms TTL=127
Reply from 192.168.40.31: bytes=32 time=15ms TTL=127

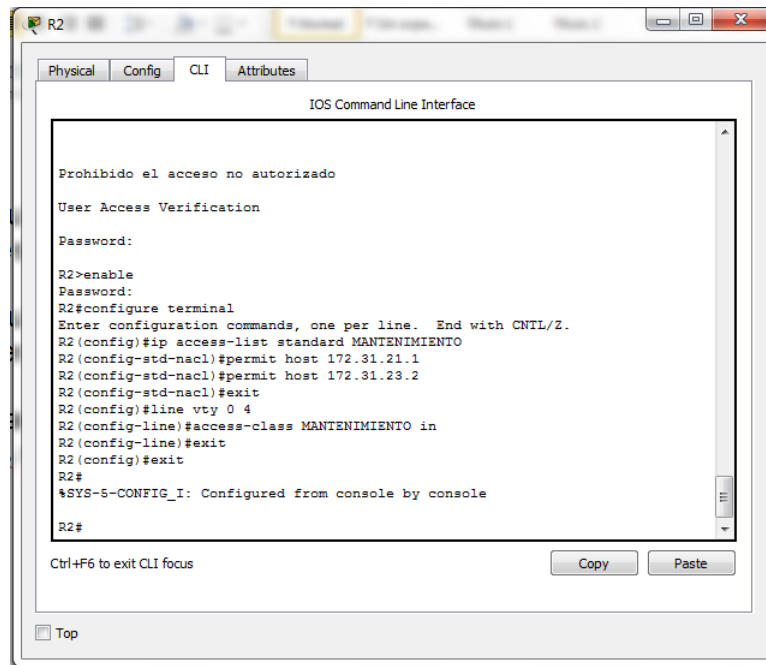
Ping statistics for 192.168.40.31:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 15ms, Average = 13ms

C:\>|
```

At the bottom of the window, there is a 'Top' button.



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.



```
R2
Physical Config CLI Attributes
IOS Command Line Interface

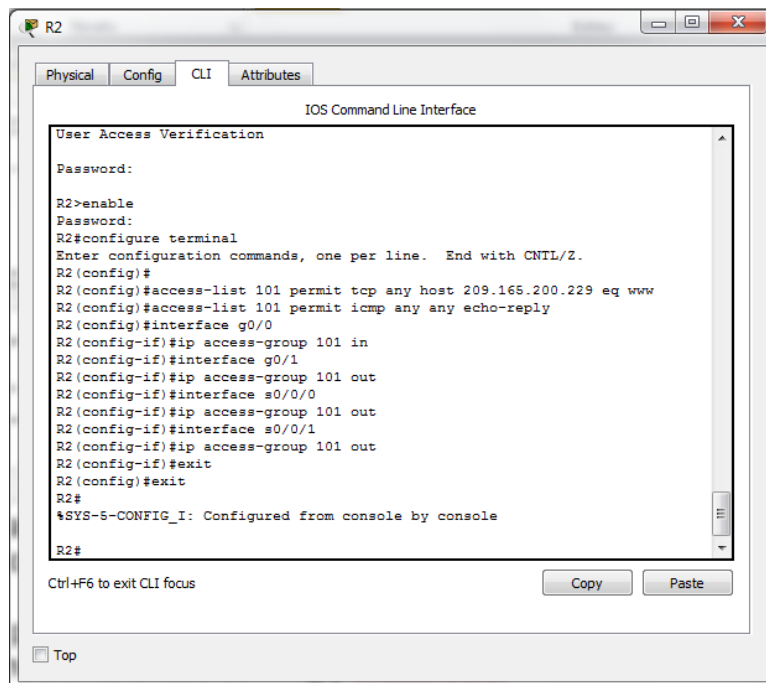
Prohibido el acceso no autorizado

User Access Verification

Password:

R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#ip access-list standard MANTENIMIENTO
R2 (config-std-nacl)#permit host 172.31.21.1
R2 (config-std-nacl)#permit host 172.31.23.2
R2 (config-std-nacl)#exit
R2 (config)#line vty 0 4
R2 (config-line)#access-class MANTENIMIENTO in
R2 (config-line)#exit
R2 (config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

10. 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.



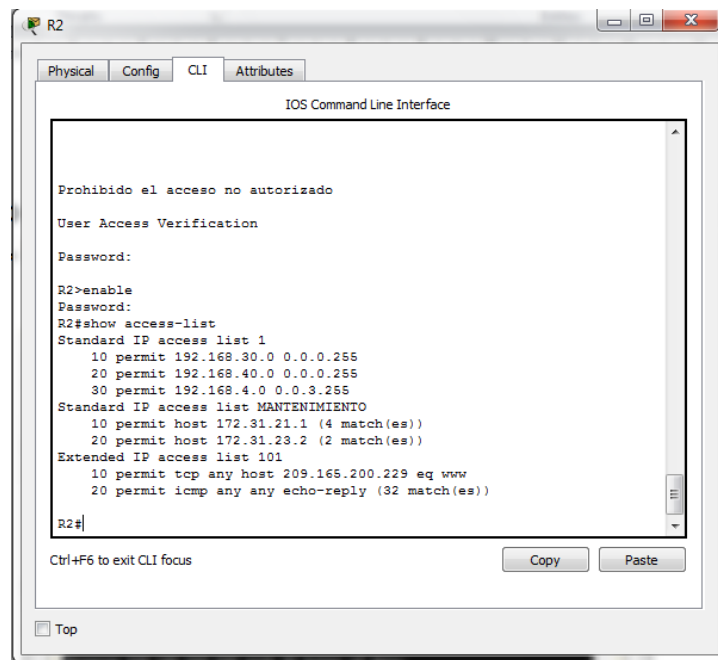
```
R2
Physical Config CLI Attributes
IOS Command Line Interface

User Access Verification

Password:

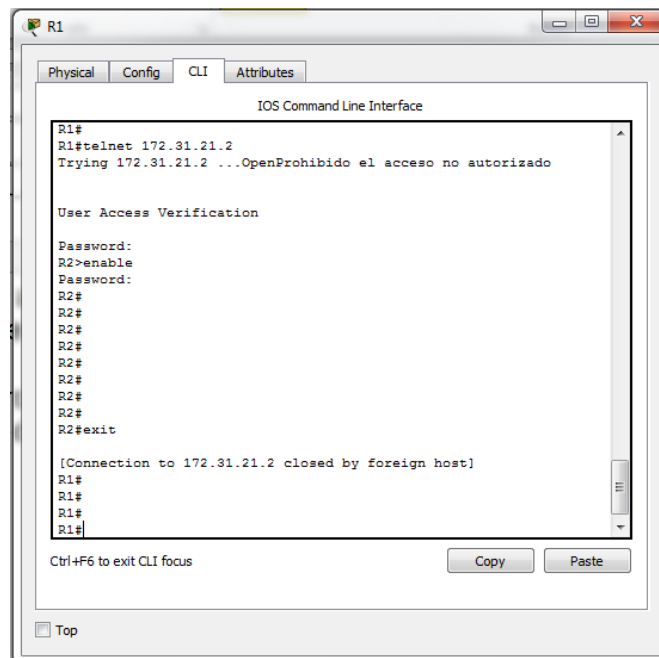
R2>enable
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2 (config)#
R2 (config)#access-list 101 permit tcp any host 209.165.200.229 eq www
R2 (config)#access-list 101 permit icmp any any echo-reply
R2 (config)#interface g0/0
R2 (config-if)#ip access-group 101 in
R2 (config-if)#interface g0/1
R2 (config-if)#ip access-group 101 out
R2 (config-if)#interface s0/0/0
R2 (config-if)#ip access-group 101 out
R2 (config-if)#interface s0/0/1
R2 (config-if)#ip access-group 101 out
R2 (config-if)#exit
R2 (config)#exit
R2#
%SYS-5-CONFIG_I: Configured from console by console
R2#
```

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



```
R2#
R2>enable
R2#show access-list
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 MANTENIMIENTO
 10 permit host 172.31.21.1 (4 match(es))
 20 permit host 172.31.23.2 (2 match(es))
Extended IP access list 101
 10 permit tcp any host 209.165.200.229 eq www
 20 permit icmp any any echo-reply (32 match(es))
R2#
```

Listas de acceso estándar donde se puede conectar por medio de telnet a R2 desde R1 y R3, pero desde los host no es permitido

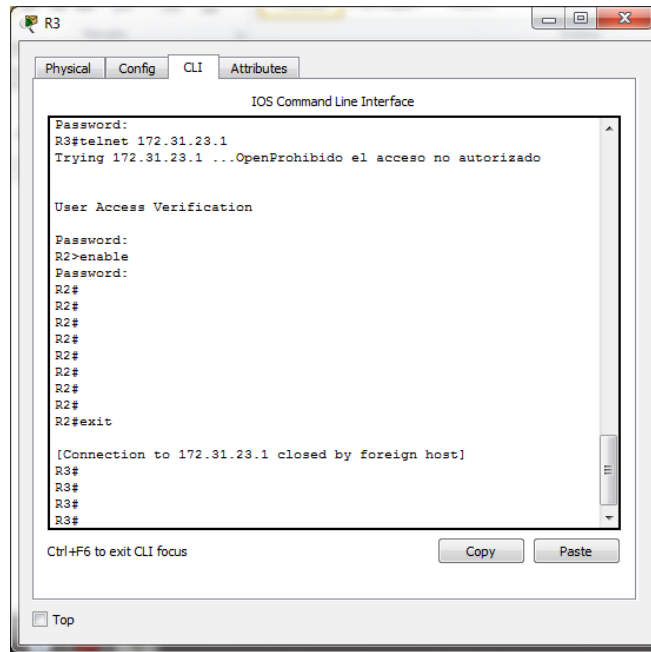


```
R1#
R1#telnet 172.31.21.2
Trying 172.31.21.2 ...OpenProhibido el acceso no autorizado

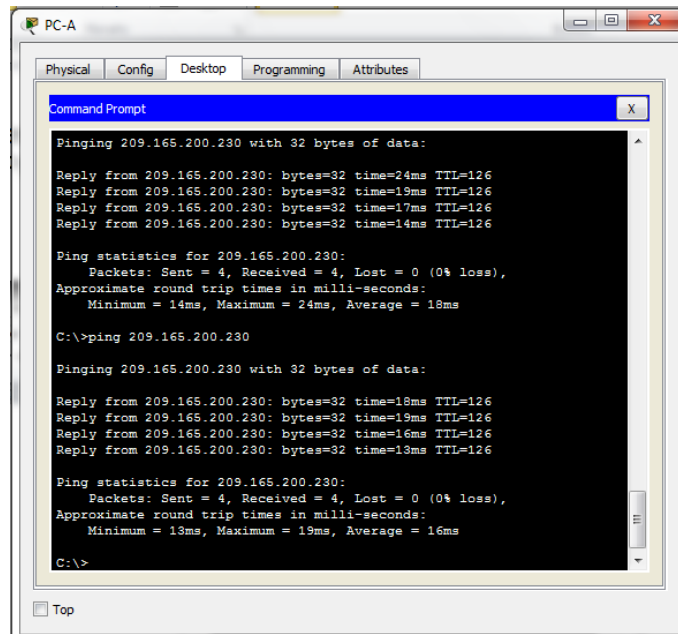
User Access Verification

Password:
R2>enable
Password:
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#
R2#exit

[Connection to 172.31.21.2 closed by foreign host]
R1#
R1#
R1#
R1#
```



Listas de acceso extendidas, permiten hacer ping desde los host PC-A y PC-C al host Internet PC, pero no permite hacer ping del host Internet PC a los host PC-A y PC-C



```
PC-C
Physical Config Desktop Programming Attributes
Command Prompt
Pinging 209.165.200.230 with 32 bytes of data:
Reply from 209.165.200.230: bytes=32 time=31ms TTL=126
Reply from 209.165.200.230: bytes=32 time=18ms TTL=126
Reply from 209.165.200.230: bytes=32 time=22ms TTL=126
Reply from 209.165.200.230: bytes=32 time=18ms TTL=126
Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 18ms, Maximum = 31ms, Average = 22ms
C:\>ping 209.165.200.230
Pinging 209.165.200.230 with 32 bytes of data:
Reply from 209.165.200.230: bytes=32 time=14ms TTL=126
Reply from 209.165.200.230: bytes=32 time=14ms TTL=126
Reply from 209.165.200.230: bytes=32 time=13ms TTL=126
Reply from 209.165.200.230: bytes=32 time=13ms TTL=126
Ping statistics for 209.165.200.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 14ms, Average = 13ms
C:\>
```

```
Internet PC
Physical Config Services Desktop Programming Attributes
Command Prompt
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.30.31
Pinging 192.168.30.31 with 32 bytes of data:
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Ping statistics for 192.168.30.31:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>ping 192.168.40.31
Pinging 192.168.40.31 with 32 bytes of data:
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Reply from 209.165.200.225: Destination host unreachable.
Ping statistics for 192.168.40.31:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

```
PC-A
Physical Config Desktop Programming Attributes
Command Prompt
Connection-specific DNS Suffix...:
Physical Address.....: 0002.1657.EB7E
Link-local IPv6 Address.....: FE80::202:16FF:FE57:EB7E
IP Address.....: 192.168.30.31
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.30.1
DNS Servers.....: 10.10.10.11
DHCP Servers.....: 192.168.30.1
DHCPv6 Client DUID.....: 00-01-00-01-B0-32-63-4E-00-02-16-57-EB-7E

C:\>ping 192.168.40.31

Pinging 192.168.40.31 with 32 bytes of data:

Request timed out.
Reply from 192.168.40.31: bytes=32 time=11ms TTL=127
Reply from 192.168.40.31: bytes=32 time=14ms TTL=127
Reply from 192.168.40.31: bytes=32 time=15ms TTL=127

Ping statistics for 192.168.40.31:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 15ms, Average = 13ms

C:\>
```

```
PC-C
Physical Config Desktop Programming Attributes
Command Prompt
Connection-specific DNS Suffix...:
Physical Address.....: 00E0.F798.6082
Link-local IPv6 Address.....: FE80::2E0:F7FF:FE98:6082
IP Address.....: 192.168.40.31
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.40.1
DNS Servers.....: 10.10.10.11
DHCP Servers.....: 192.168.40.1
DHCPv6 Client DUID.....: 00-01-00-01-59-54-90-75-00-E0-F7-98-60-82

C:\>ping 192.168.30.31

Pinging 192.168.30.31 with 32 bytes of data:

Reply from 192.168.30.31: bytes=32 time=11ms TTL=127
Reply from 192.168.30.31: bytes=32 time=11ms TTL=127
Reply from 192.168.30.31: bytes=32 time=17ms TTL=127
Reply from 192.168.30.31: bytes=32 time=17ms TTL=127

Ping statistics for 192.168.30.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 17ms, Average = 14ms

C:\>
```

NOTA: No se adjuntan más pantallazos para no extender más el documento y evitar que quede más pesado y a medida que se fue desarrollando la actividad se hacían pruebas, se puede ver en los pantallazos del proceso. De igual manera se anexa el archivo de packet tracer para evidencia y su validación.

La prueba de habilidades cuenta con 13 puntos, durante el proceso se integraron algunos con el fin de darle más orden al documento quedando en total 11 puntos



## Conclusiones

- Se logró comprender y utilizar los diferentes protocolos de routing disponibles dependiendo de las necesidades de la red.
- Se conoció y desarrollo la implementación y configuración básica de OSPF de área única.
- Se analizaron y ejecutaron las instrucciones necesarias para utilizar las ACL estándar y extendida en un router Cisco.
- Se identificó cada una de las funciones, la configuración y la aplicación de DHCPv4.
- Se estudió la implementación de NAT combinada sobre la red configurada con direcciones IPv4.

## Bibliografía

- 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>