

EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

POR:

JUAN MANUEL MUSKUS MUSKUS – COD. 79690305

GRUPO:

203092_6

TUTOR

Ing. GIOVANNI ALBERTO BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

PROGRAMA DE INGENIERÍA DE SISTEMAS

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

2018

Contenido

INTRODUCCIÓN.....	4
OBJETIVOS	5
OBJETIVO GENERAL.....	5
OBJETIVOS ESPECÍFICOS	5
DESCRIPCIÓN DEL ESCENARIO PROPUESTO PARA LA PRUEBA DE HABILIDADES.....	6
DESARROLLO DE LA ACTIVIDAD.....	7
CONCLUSIONES.....	28
REFERENCIAS BIBLIOGRÁFICAS	29

Tabla de Imágenes

Imagen 1. Topología desarrollada	7
Imagen 2 – Habilitar DHCP en PC-A	8
Imagen 3 – Habilitar DHCP en PC-C	8
Imagen 4 – Habilitar IP estática en Internet_PC	9
Imagen 5 - Configuración R1	9
Imagen 6 - Configuración R2: Parte 1.....	10
Imagen 7 - Configuración R2: Parte 2.....	11
Imagen 8 - Configuración IP Web Server	11
Imagen 9 - Configuración R3: Parte 1.....	12
Imagen 10 - Configuración R3: Parte 2.....	13
Imagen 11 - Configuración S1	14
Imagen 12 - Configuración OSPF en R1	15
Imagen 13 - Configuración OSPF en R2	16
Imagen 14 - Configuración OSPF en R3	17
Imagen 15 - Listado OSPF	17
Imagen 16 - Listado OSPF costo	18
Imagen 17 - Comando show running-config	18
Imagen 18 – S1: Creación de Vlan Parte 1.....	19
Imagen 19 – S1: Creación y configuración de Vlan Parte 2.....	20
Imagen 20 – S1: Creación y configuración de Vlan Parte 3.....	20
Imagen 21 – S3: Creación y configuración de Vlan Parte 1.....	21
Imagen 22 - R1: Creación y configuración de Vlan.....	22
Imagen 23 - Comando no ip domain-lookup	22
Imagen 24 - IP para S1	22
Imagen 25 - IP para S3.....	23
Imagen 26 - Desactivando interfaces en S1	23
Imagen 27 - Desactivando interfaces en S3	23
Imagen 28 - Configuración de los puntos 7, 8 y 9.....	24
Imagen 29 - Configuración en R2 para internet	24
Imagen 30 - Configuración de entrada y salida en R2.....	25
Imagen 31 - Control de IP desde R2.....	25
Imagen 32 – Configuración de acceso de tipo estándar	26
Imagen 33 - – Configuración de acceso de tipo extendido	26
Imagen 34 - Lista de accesos	27
Imagen 35 - Ping de R1 a PC internet	27

INTRODUCCIÓN

Hoy día la línea ADSL obtiene a casi todos los hogares y empresas. Este progreso significa un ancho de banda suficiente para mantener una conversación telefónica PC a PC a través de Internet con suficiente calidad, considerando que ésta está claramente relacionada con el ancho de banda asimismo con el equipo utilizado para enlazar a Internet, los accesorios a utilizar al instante de realizar la conversación y del programa mediador a utilizar, es por esto que su uso se divulgó no solo a empresas y profesionales con hosts personales sino que fue potencial su uso para miles de usuarios residenciales en diferentes partes.

Teniendo en cuenta las necesidades de la empresa de tecnología para establecer una comunicación efectiva de servicios convergentes y aprovechando los beneficios que han surgido tras las nuevas tecnologías en el campo de las telecomunicaciones se propone una solución de acuerdo con los requerimientos descritos en la prueba de habilidades, cuyo único objeto será ampliar su cobertura y mejorar la disponibilidad de su infraestructura de telecomunicaciones para su sede principal y sus sucursales.

OBJETIVOS

OBJETIVO GENERAL

Conceptualizar y aplicar la temática de: conectividad IPv4, seguridad de switch enrutamiento inter VLAN, OSPFv2, DHCP, NAT dinámica / estática y listas de control de acceso (ACL) mediante un caso práctico propuesto por el tutor del diplomado.

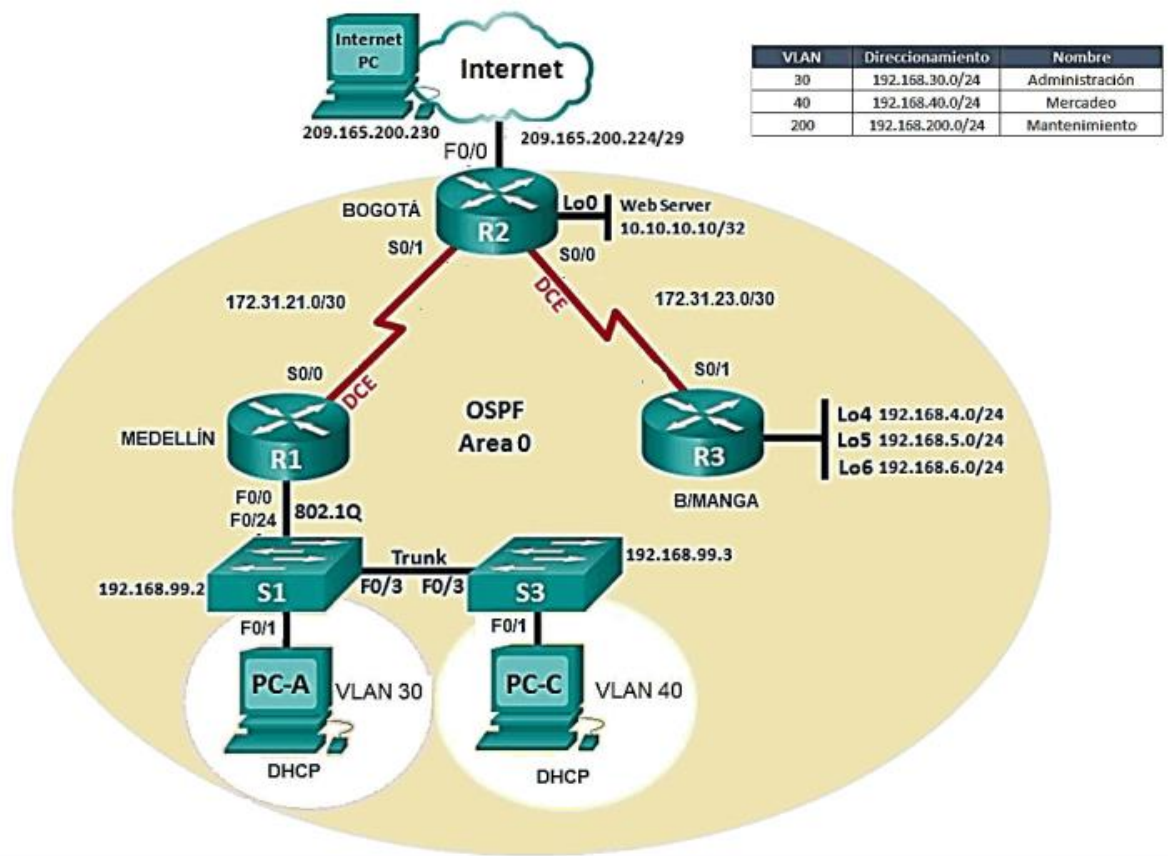
OBJETIVOS ESPECÍFICOS

- Analizar los conceptos de conectividad IPv4, seguridad de switch, enrutamiento inter VLAN, OSPFv2, DHCP, NAT dinámica / estática y listas de control de acceso (ACL) previo a la configuración de dispositivos.
- Desarrollar un informe con evidencias donde se aplique y configure una solución práctica descrita en el escenario propuesto en la prueba de habilidades.
- Generar un escenario virtual en Packet Tracer (archivo de extensión pka) con la configuración sugerida en la prueba de habilidades.
- Verificar la conectividad de los dispositivos virtuales mediante el uso de comandos: ping, traceroute, show ip route, entre otros. Y así cumplir con los requisitos del escenario virtual.

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 RED



DESARROLLO DE LA ACTIVIDAD

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

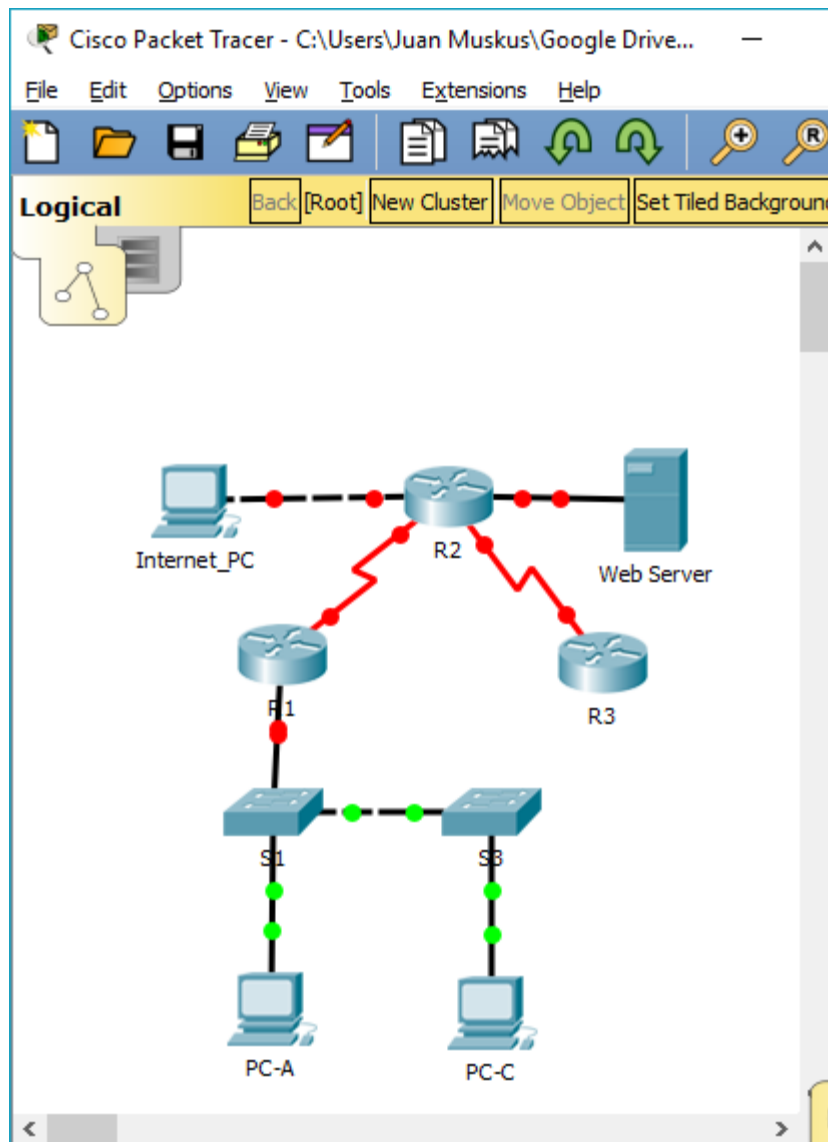


Imagen 1. Topología desarrollada

NOTA: Si inserta a la topología un servidor ya que el Router (R2) no soporta el servicio http.

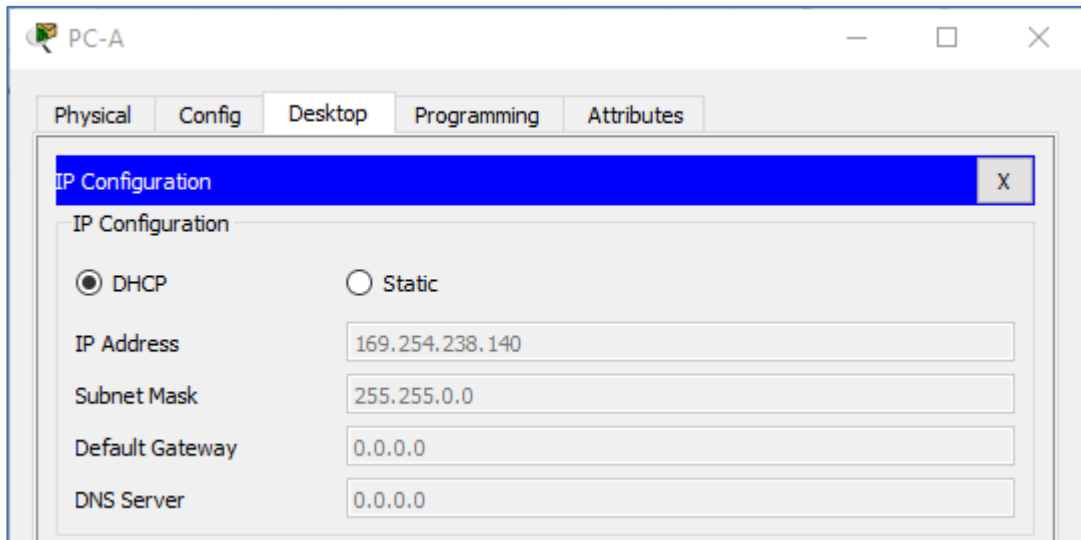


Imagen 2 – Habilitar DHCP en PC-A

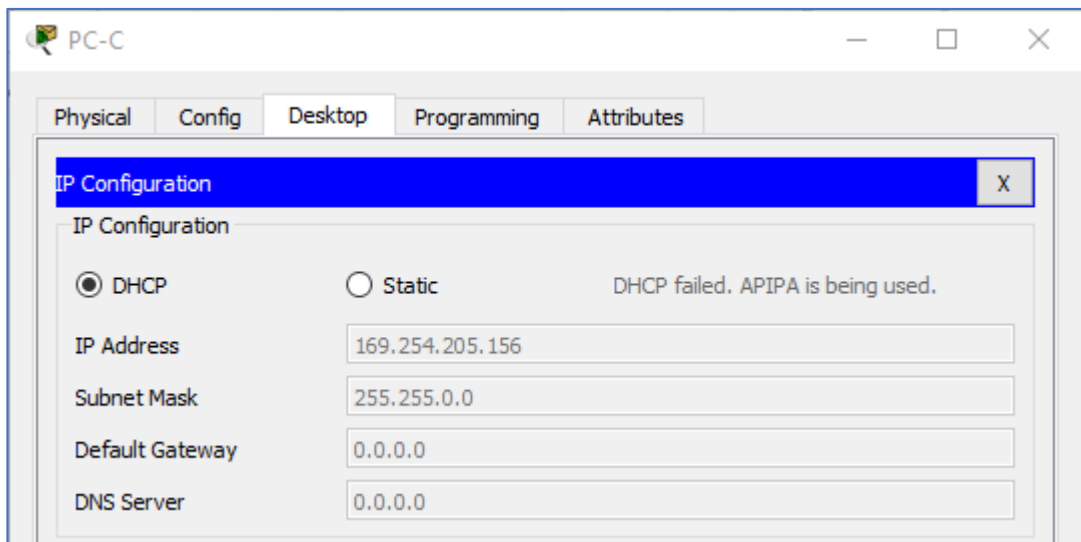


Imagen 3 – Habilitar DHCP en PC-C

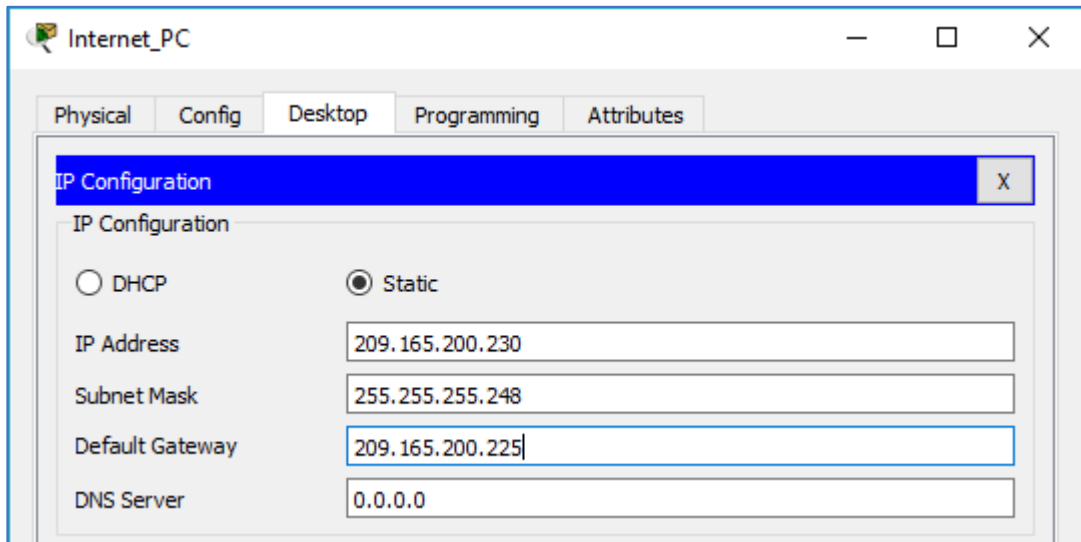


Imagen 4 – Habilitar IP estática en Internet_PC

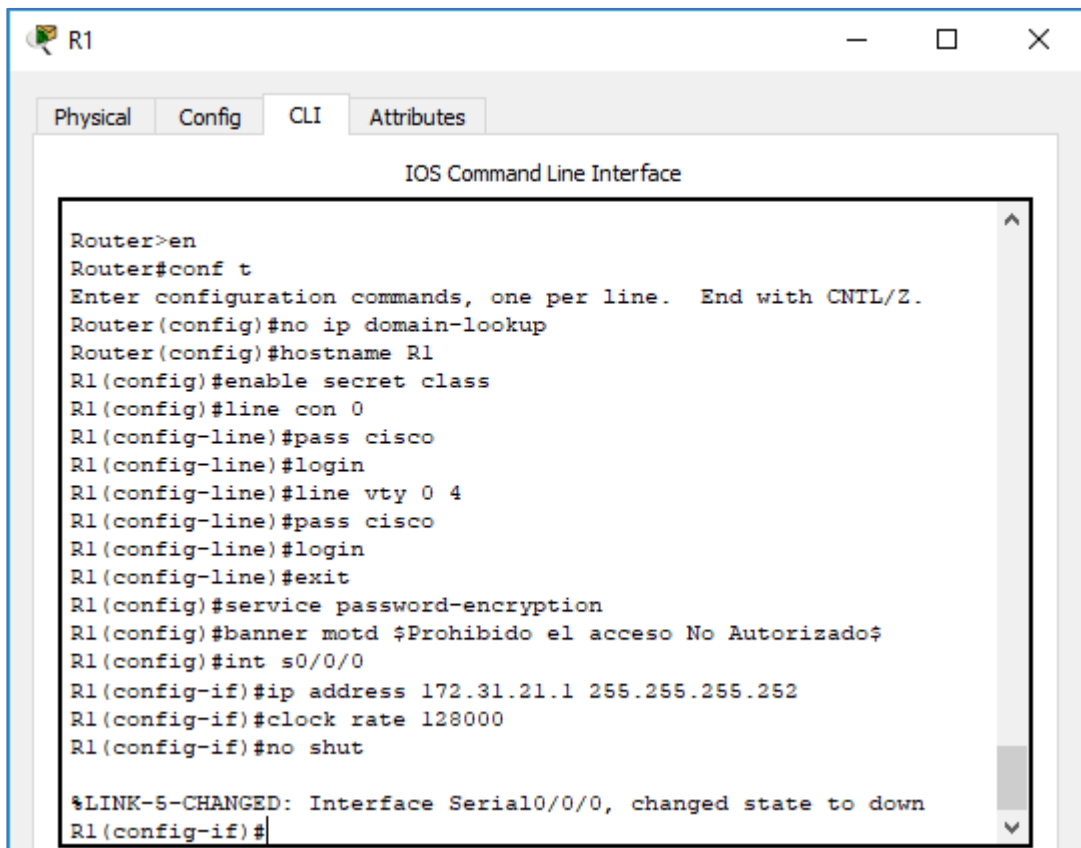
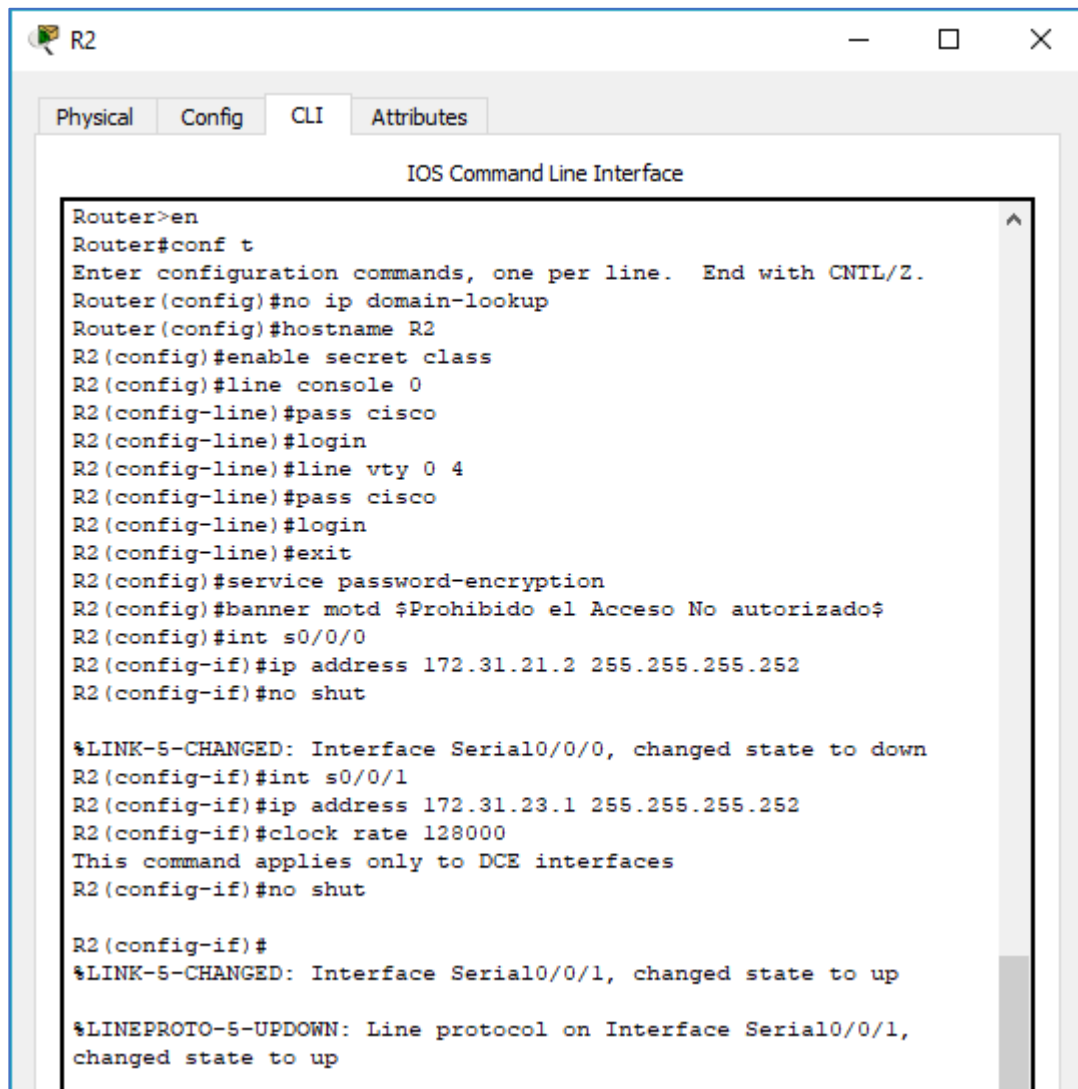


Imagen 5 - Configuración R1



```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd $Prohibido el Acceso No autorizado$
R2(config)#int s0/0/0
R2(config-if)#ip address 172.31.21.2 255.255.255.252
R2(config-if)#no shut

%LINK-S-CHANGED: Interface Serial0/0/0, changed state to down
R2(config-if)#int s0/0/1
R2(config-if)#ip address 172.31.23.1 255.255.255.252
R2(config-if)#clock rate 128000
This command applies only to DCE interfaces
R2(config-if)#no shut

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

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

Imagen 6 - Configuración R2: Parte 1

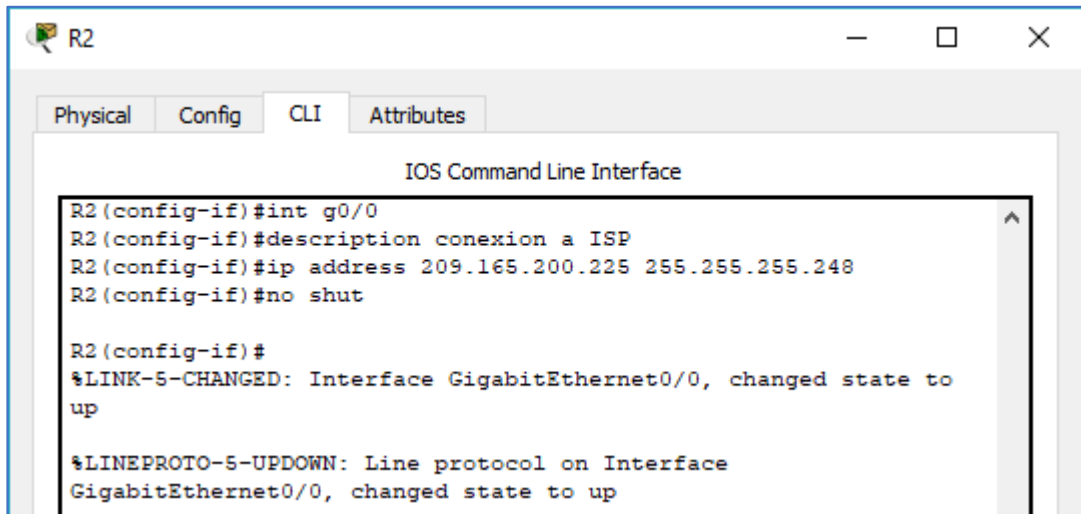


Imagen 7 - Configuración R2: Parte 2

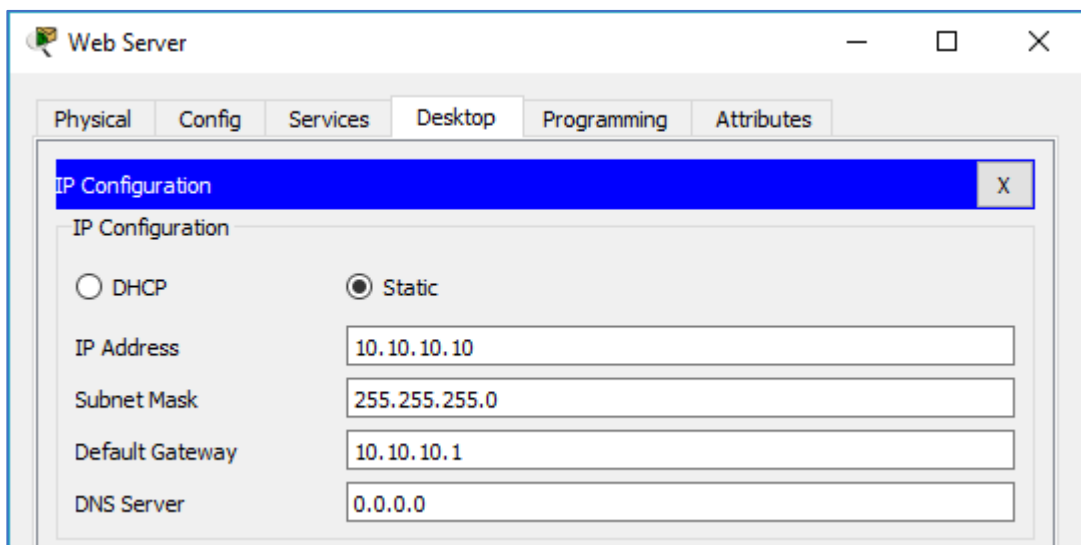
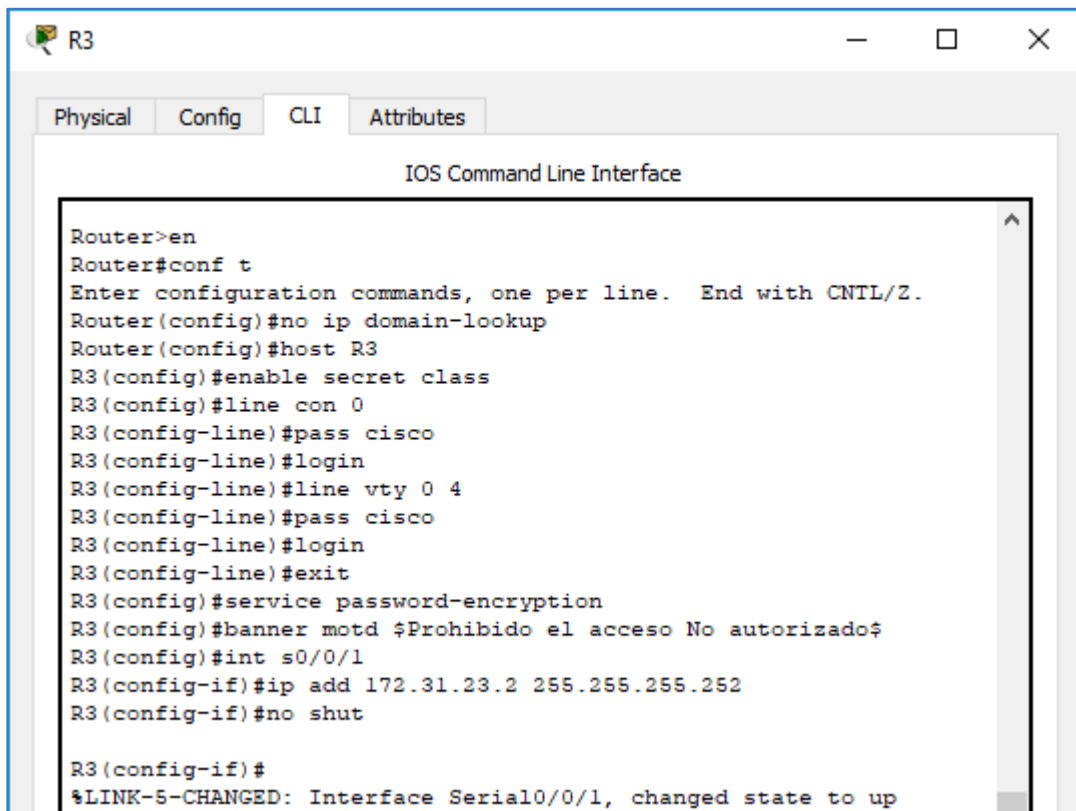


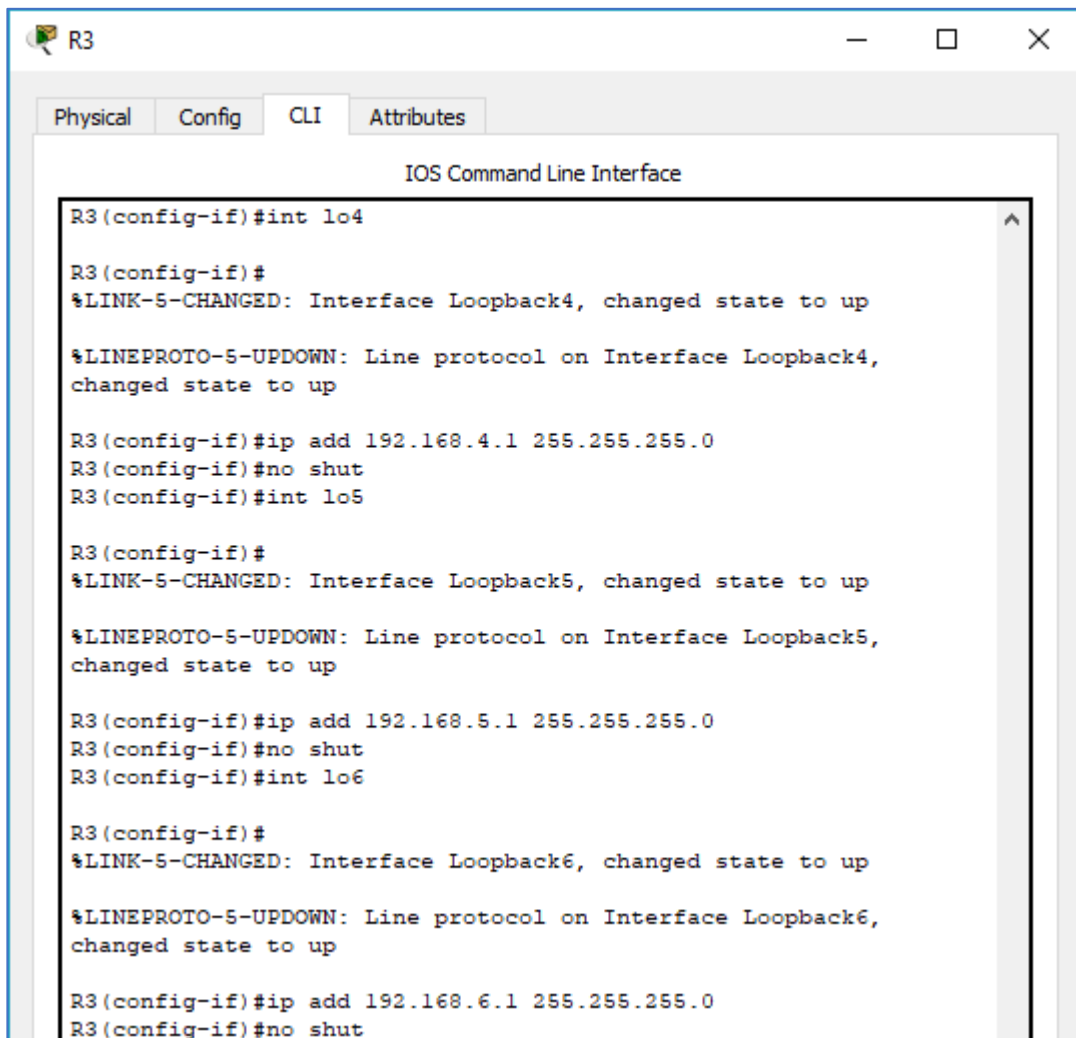
Imagen 8 - Configuración IP Web Server



```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#host R3
R3(config)#enable secret class
R3(config)#line con 0
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#line vty 0 4
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd $Prohibido el acceso No autorizado$
R3(config)#int s0/0/1
R3(config-if)#ip add 172.31.23.2 255.255.255.252
R3(config-if)#no shut

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

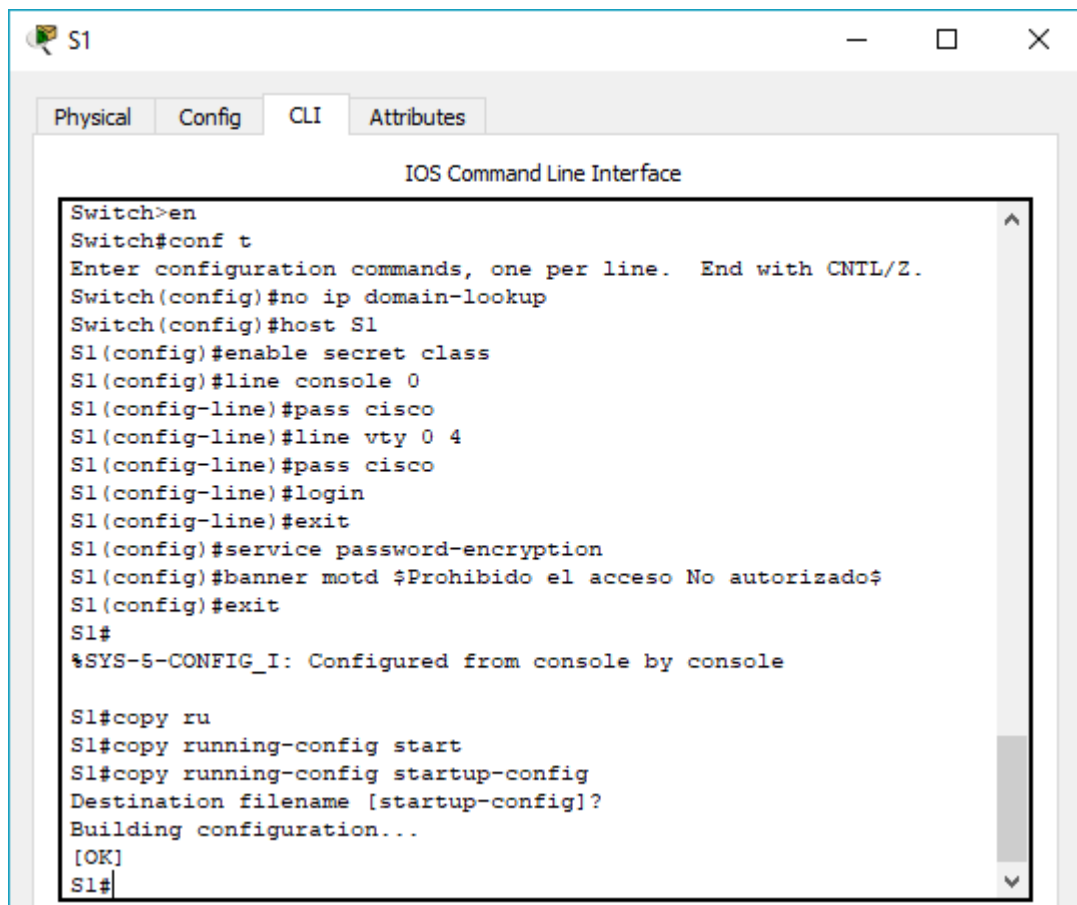
Imagen 9 - Configuración R3: Parte 1



The screenshot shows a window titled "R3" with tabs for "Physical", "Config", "CLI", and "Attributes". The "CLI" tab is active, displaying the "IOS Command Line Interface". The terminal output shows the following sequence of commands and responses:

```
R3(config-if)#int 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 add 192.168.4.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int 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 add 192.168.5.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int 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 add 192.168.6.1 255.255.255.0
R3(config-if)#no shut
```

Imagen 10 - Configuración R3: Parte 2



```

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

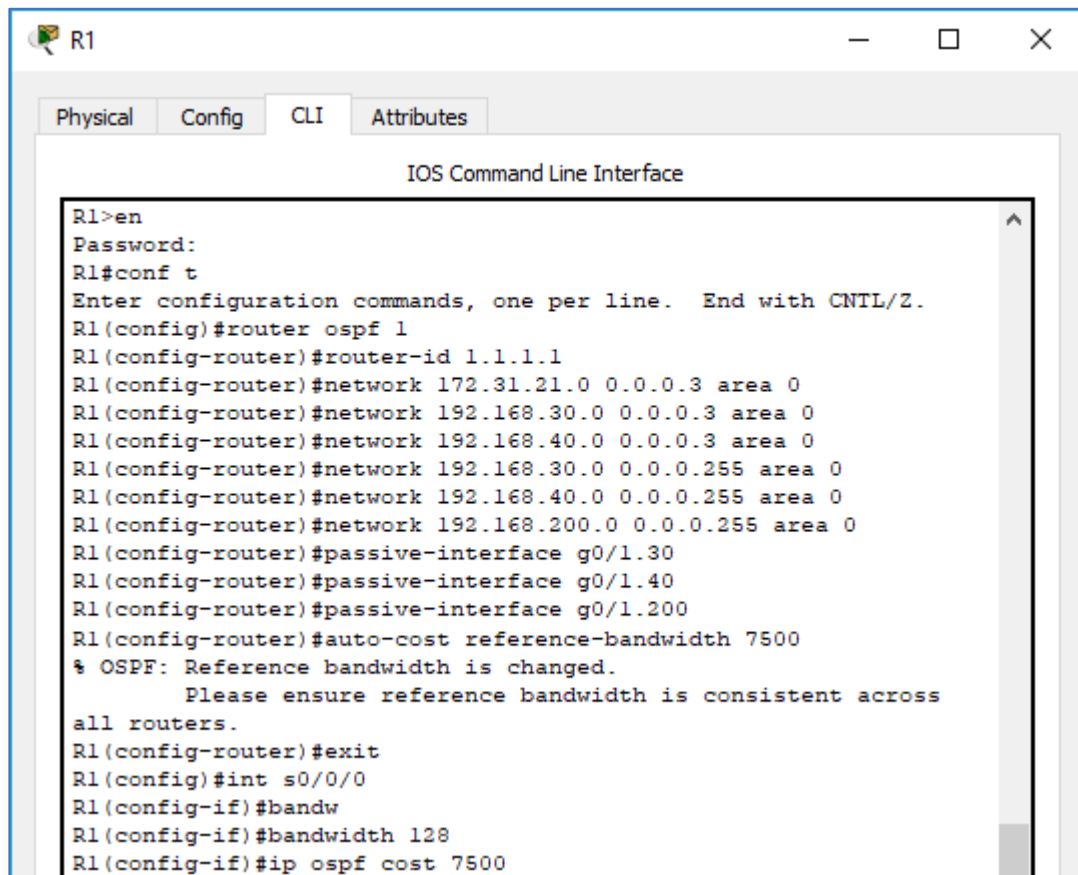
S1#copy ru
S1#copy running-config start
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
  
```

Imagen 11 - Configuración S1

NOTA: La anterior configuración aplica también a S3.

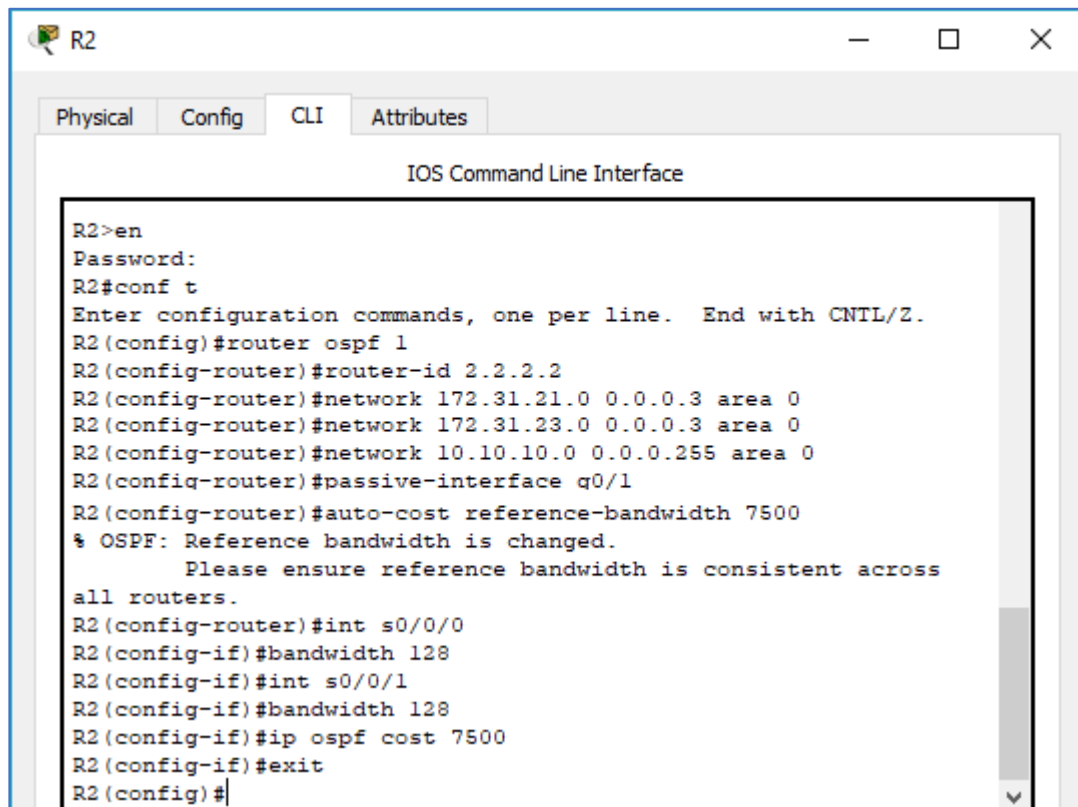
2. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

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



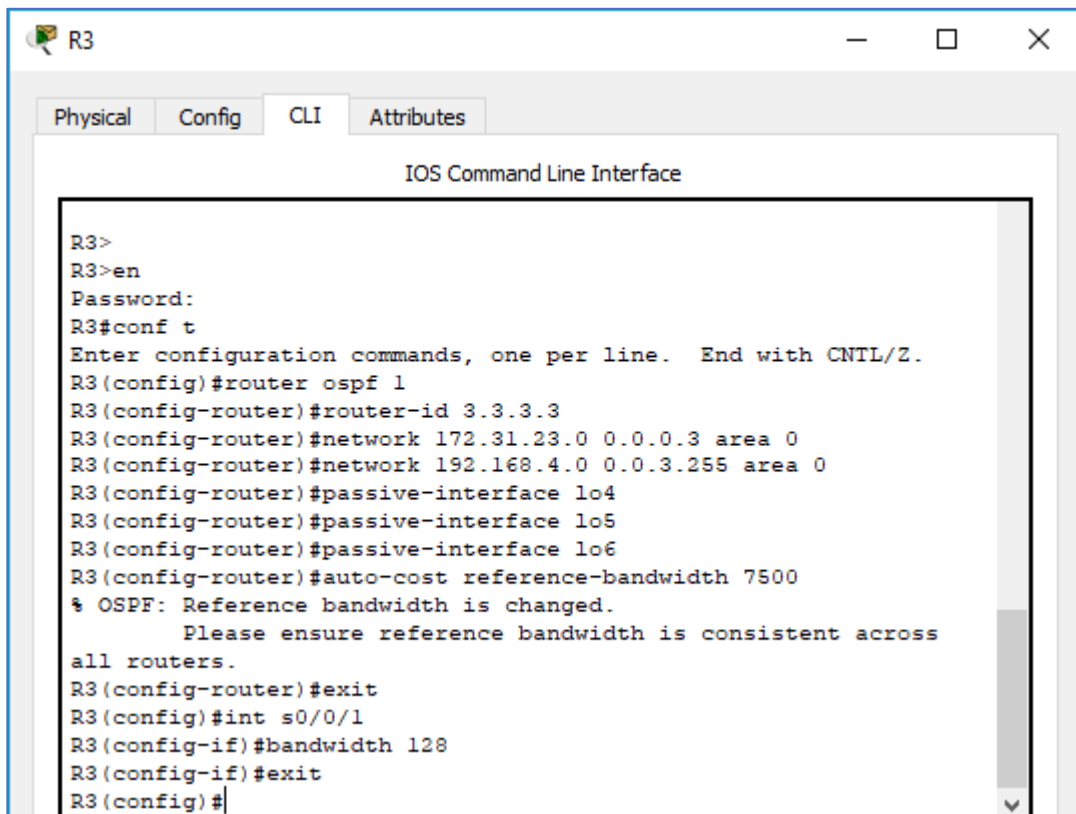
```
R1
Physical Config CLI Attributes
IOS Command Line Interface
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 172.31.21.0 0.0.0.3 area 0
R1(config-router)#network 192.168.30.0 0.0.0.3 area 0
R1(config-router)#network 192.168.40.0 0.0.0.3 area 0
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 0
R1(config-router)#passive-interface g0/1.30
R1(config-router)#passive-interface g0/1.40
R1(config-router)#passive-interface g0/1.200
R1(config-router)#auto-cost reference-bandwidth 7500
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across
all routers.
R1(config-router)#exit
R1(config)#int s0/0/0
R1(config-if)#bandw
R1(config-if)#bandwidth 128
R1(config-if)#ip ospf cost 7500
```

Imagen 12 - Configuración OSPF en R1



```
R2
Physical Config CLI Attributes
IOS Command Line Interface
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 2.2.2.2
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#passive-interface q0/1
R2(config-router)#auto-cost reference-bandwidth 7500
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across
all routers.
R2(config-router)#int s0/0/0
R2(config-if)#bandwidth 128
R2(config-if)#int s0/0/1
R2(config-if)#bandwidth 128
R2(config-if)#ip ospf cost 7500
R2(config-if)#exit
R2(config)#
```

Imagen 13 - Configuración OSPF en R2

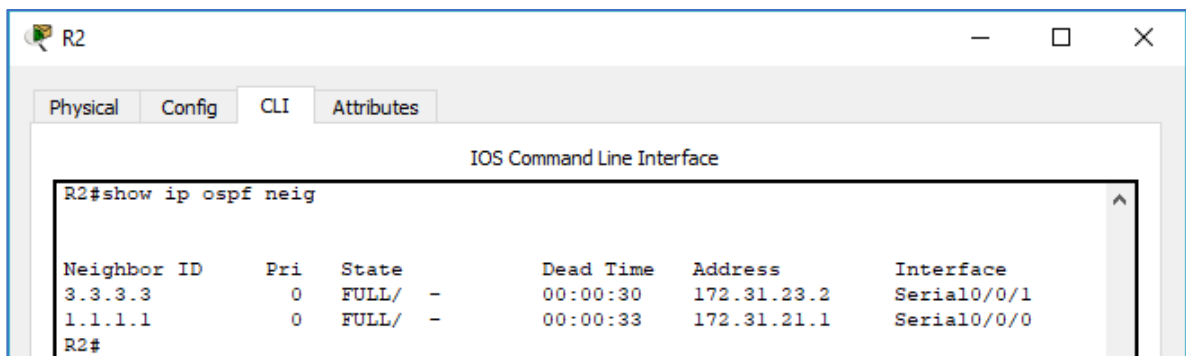


```

R3>
R3>en
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 3.3.3.3
R3(config-router)#network 172.31.23.0 0.0.0.3 area 0
R3(config-router)#network 192.168.4.0 0.0.3.255 area 0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#auto-cost reference-bandwidth 7500
% OSPF: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across
all routers.
R3(config-router)#exit
R3(config)#int s0/0/1
R3(config-if)#bandwidth 128
R3(config-if)#exit
R3(config)#
  
```

Imagen 14 - Configuración OSPF en R3

Visualizar tablas de enrutamiento y routers conectados por OSPFv2



```

R2#show ip ospf neig

```

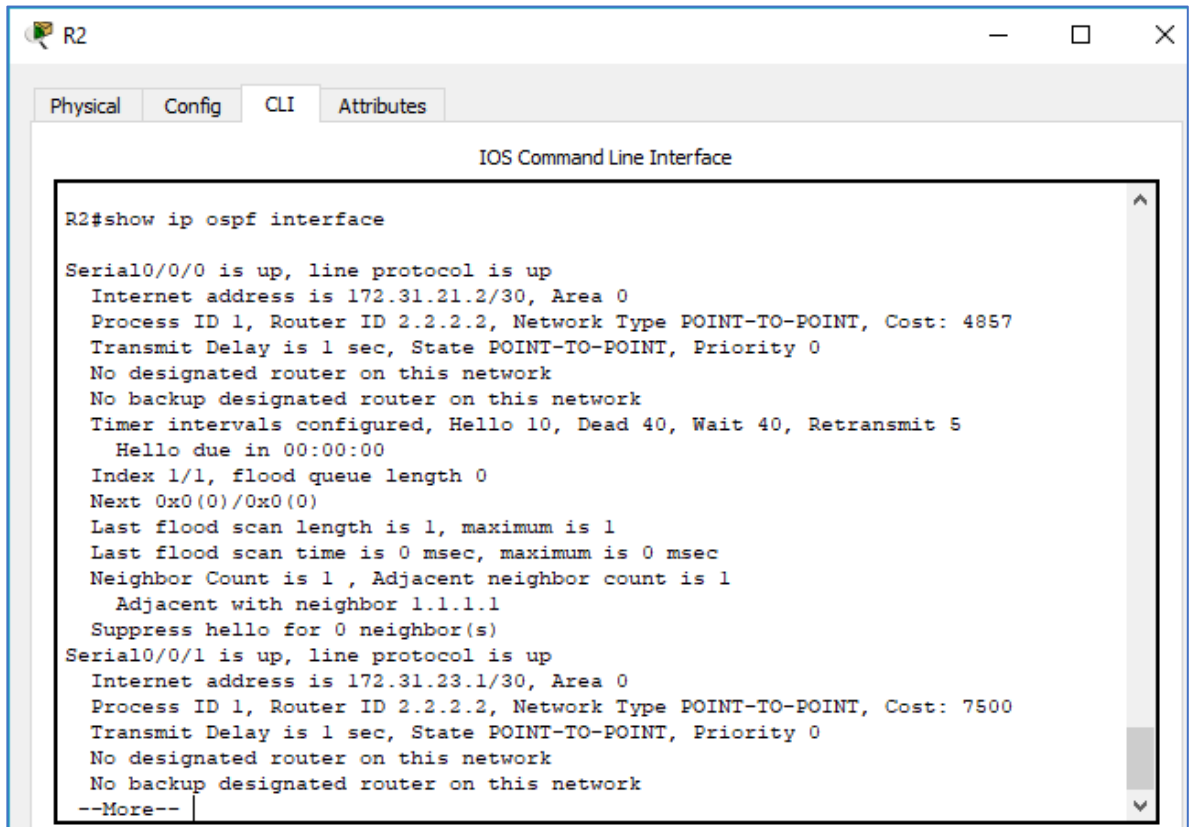
Neighbor ID	Pri	State	Dead Time	Address	Interface
3.3.3.3	0	FULL/ -	00:00:30	172.31.23.2	Serial0/0/1
1.1.1.1	0	FULL/ -	00:00:33	172.31.21.1	Serial0/0/0

```

R2#
  
```

Imagen 15 - Listado OSPF

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

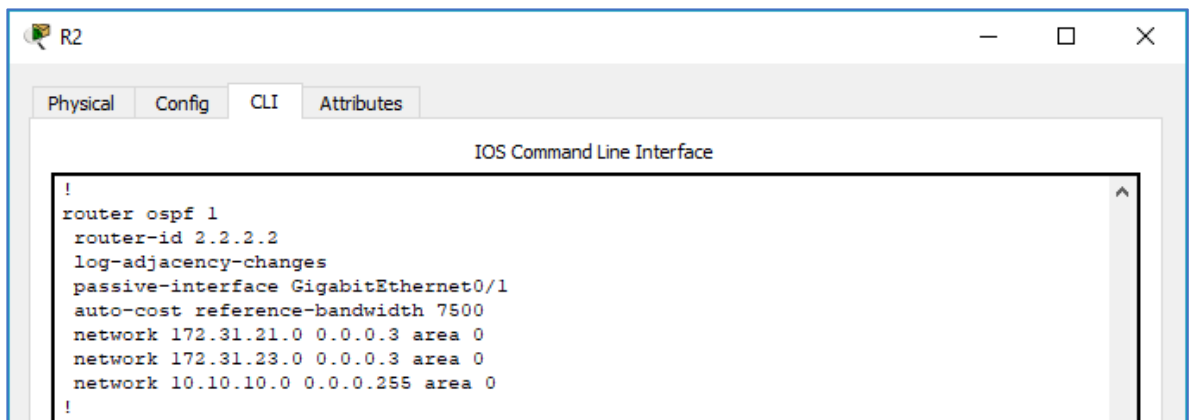


```
R2#show ip ospf interface

Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.21.2/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 4857
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
Serial0/0/1 is up, line protocol is up
  Internet address is 172.31.23.1/30, Area 0
  Process ID 1, Router ID 2.2.2.2, Network Type POINT-TO-POINT, Cost: 7500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
--More--
```

Imagen 16 - Listado OSPF costo

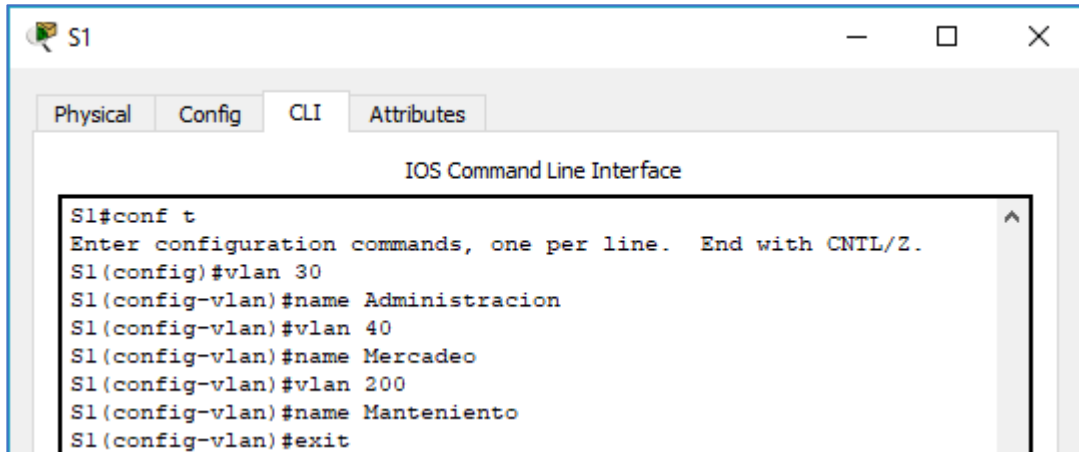
Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.



```
!
router ospf 1
  router-id 2.2.2.2
  log-adjacency-changes
  passive-interface GigabitEthernet0/1
  auto-cost reference-bandwidth 7500
  network 172.31.21.0 0.0.0.3 area 0
  network 172.31.23.0 0.0.0.3 area 0
  network 10.10.10.0 0.0.0.255 area 0
!
```

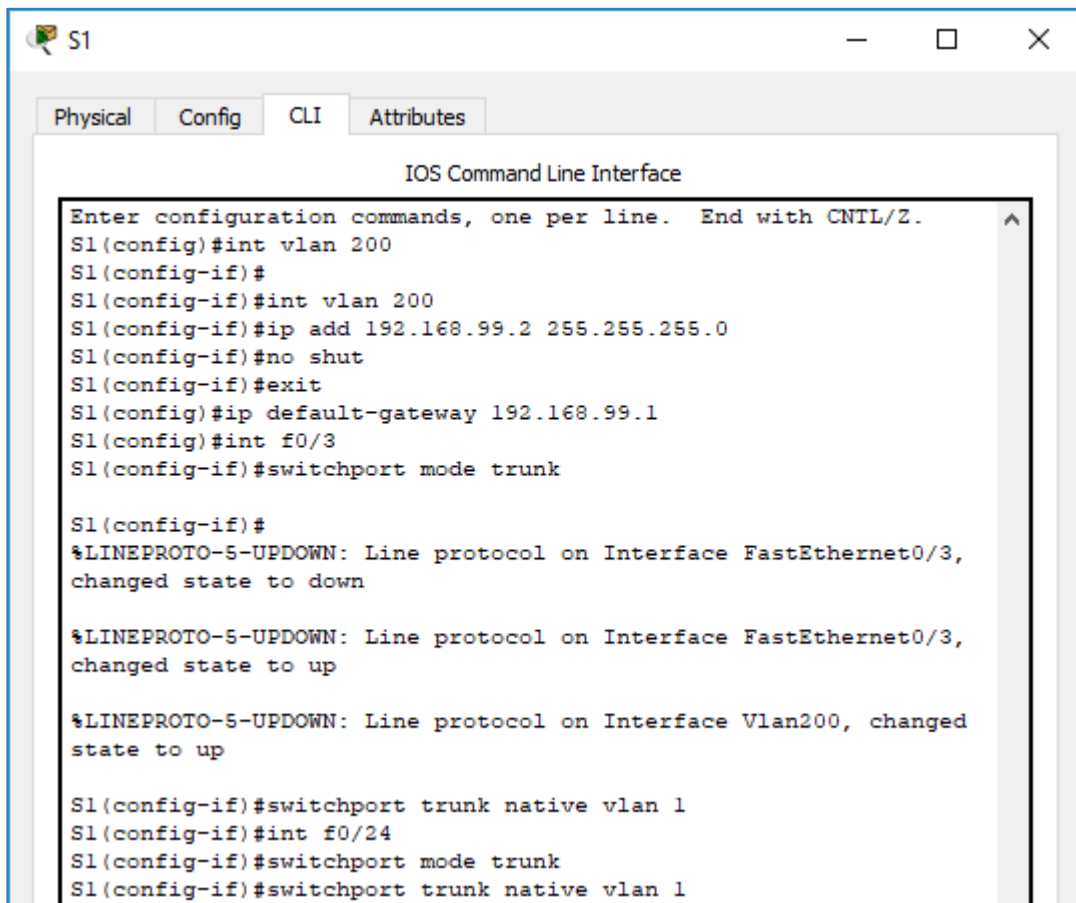
Imagen 17 - Comando show running-config

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#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#exit
```

Imagen 18 – S1: Creación de Vlan Parte 1



The screenshot shows the CLI interface of a switch named S1. The user is in configuration mode and has just finished configuring Vlan 200. The output shows the configuration commands and the resulting state of the interfaces.

```
S1
Physical Config CLI Attributes
IOS Command Line Interface
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int vlan 200
S1(config-if)#
S1(config-if)#int vlan 200
S1(config-if)#ip add 192.168.99.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

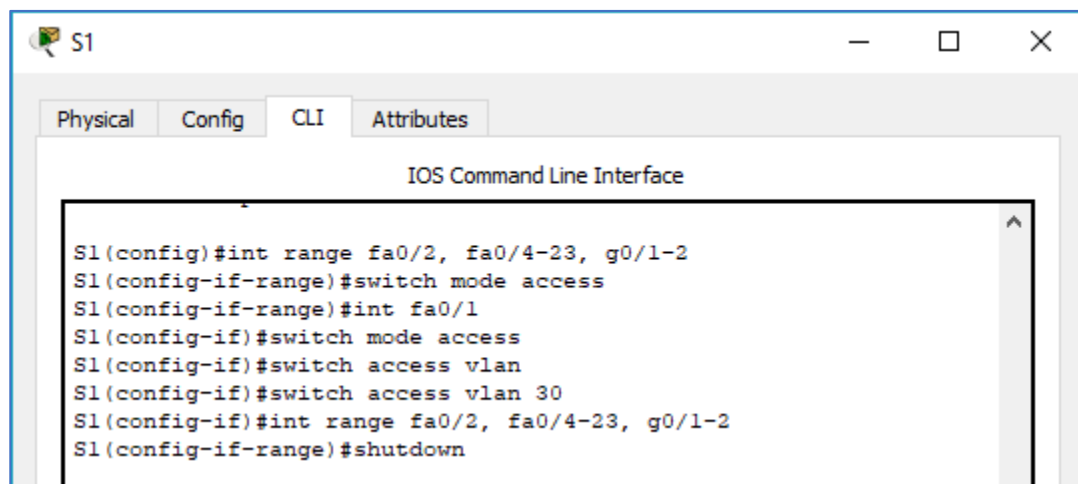
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to down

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

Imagen 19 – S1: Creación y configuración de Vlan Parte 2

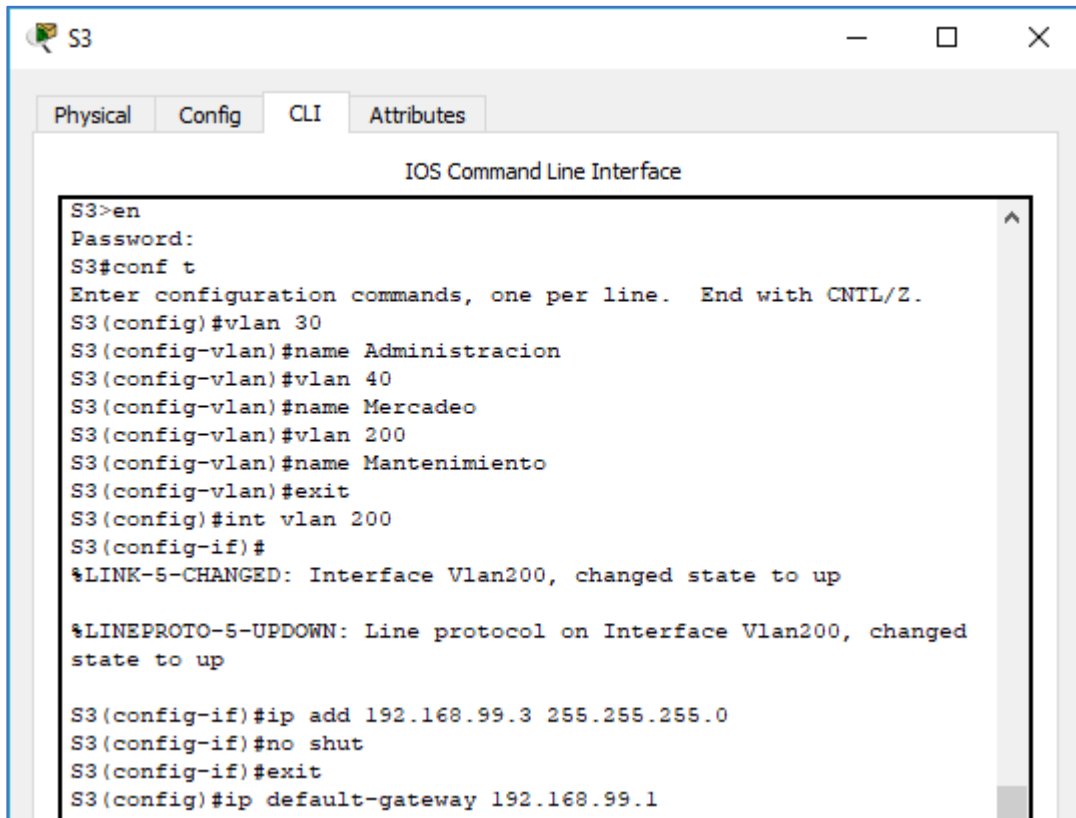


The screenshot shows the CLI interface of a switch named S1. The user is in configuration mode and has just finished configuring Vlan 30. The output shows the configuration commands and the resulting state of the interfaces.

```
S1
Physical Config CLI Attributes
IOS Command Line Interface

S1(config)#int range fa0/2, fa0/4-23, g0/1-2
S1(config-if-range)#switch mode access
S1(config-if-range)#int fa0/1
S1(config-if)#switch mode access
S1(config-if)#switch access vlan
S1(config-if)#switch access vlan 30
S1(config-if)#int range fa0/2, fa0/4-23, g0/1-2
S1(config-if-range)#shutdown
```

Imagen 20 – S1: Creación y configuración de Vlan Parte 3

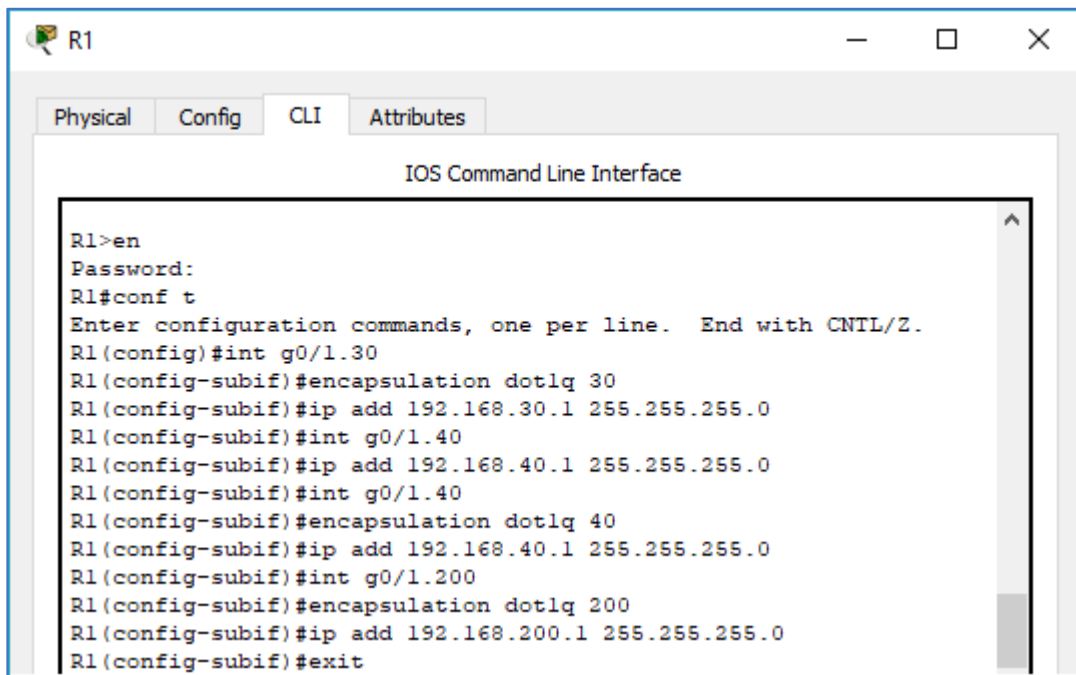


```
S3>en
Password:
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 30
S3(config-vlan)#name Administracion
S3(config-vlan)#vlan 40
S3(config-vlan)#name Mercadeo
S3(config-vlan)#vlan 200
S3(config-vlan)#name Mantenimiento
S3(config-vlan)#exit
S3(config)#int vlan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

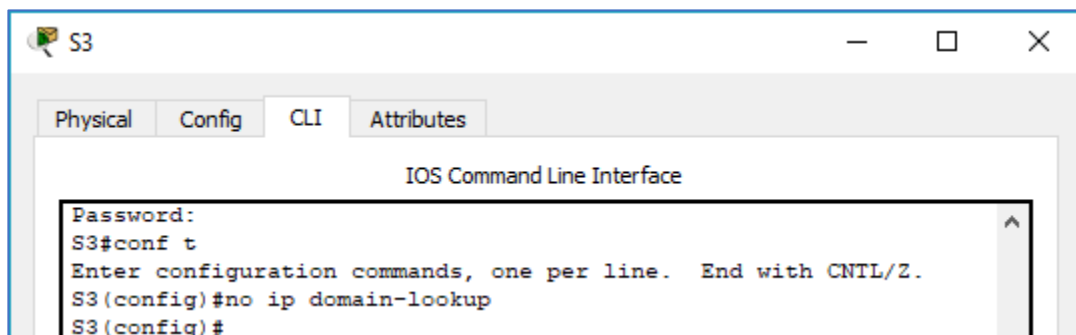
Imagen 21 – S3: Creación y configuración de Vlan Parte 1

A screenshot of a network device terminal window titled 'R1'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The terminal displays the 'IOS Command Line Interface' with the following commands and output:

```
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip add 192.168.30.1 255.255.255.0
R1(config-subif)#int g0/1.40
R1(config-subif)#ip add 192.168.40.1 255.255.255.0
R1(config-subif)#int g0/1.40
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip add 192.168.40.1 255.255.255.0
R1(config-subif)#int g0/1.200
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip add 192.168.200.1 255.255.255.0
R1(config-subif)#exit
```

Imagen 22 - R1: Creación y configuración de Vlan

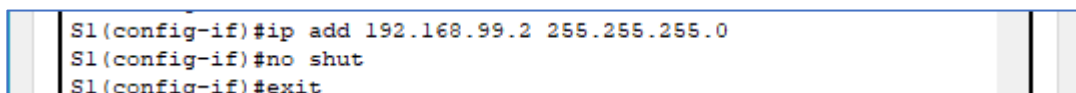
4. En el Switch 3 deshabilitar DNS lookup

A screenshot of a network device terminal window titled 'S3'. The window has tabs for 'Physical', 'Config', 'CLI', and 'Attributes', with 'CLI' selected. The terminal displays the 'IOS Command Line Interface' with the following commands and output:

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

Imagen 23 - Comando no ip domain-lookup

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

A screenshot of a network device terminal window showing the configuration for S1. The terminal displays the following commands and output:

```
S1(config-if)#ip add 192.168.99.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
```

Imagen 24 - IP para S1

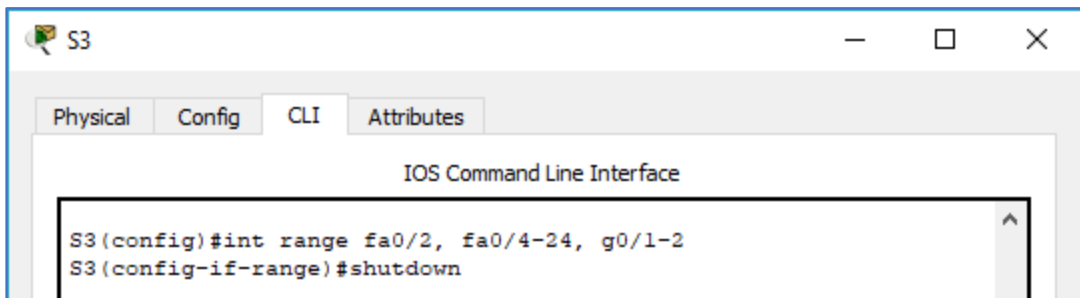
```
S3(config-if)#ip add 192.168.99.3 255.255.255.0
S3(config-if)#no shut
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1
```

Imagen 25 - IP para S3

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

```
S1(config-if)#int range fa0/2, fa0/4-23, g0/1-2
S1(config-if-range)#shutdown
```

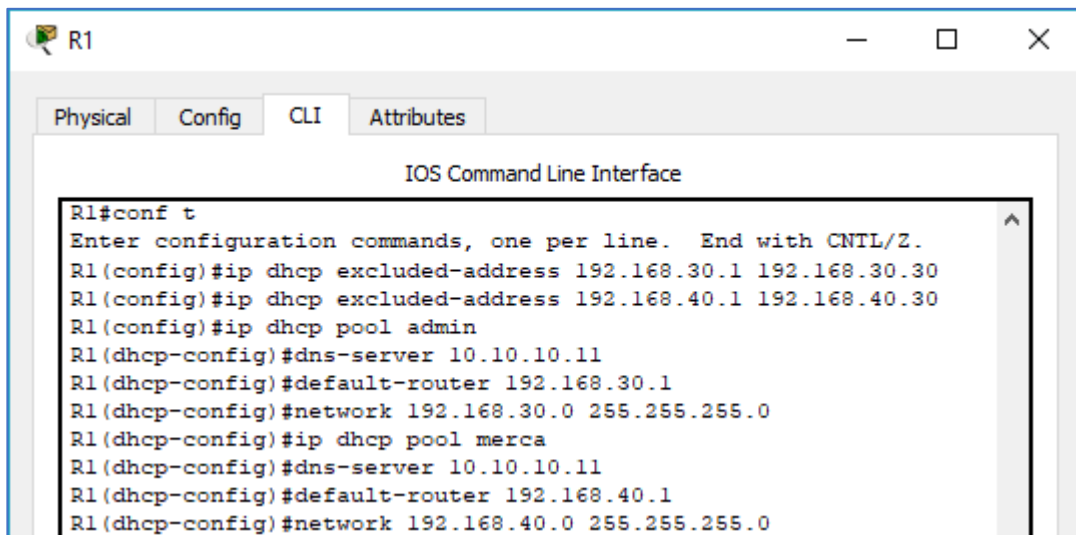
Imagen 26 - Desactivando interfaces en S1



```
S3
Physical Config CLI Attributes
IOS Command Line Interface
S3(config)#int range fa0/2, fa0/4-24, g0/1-2
S3(config-if-range)#shutdown
```

Imagen 27 - Desactivando interfaces en S3

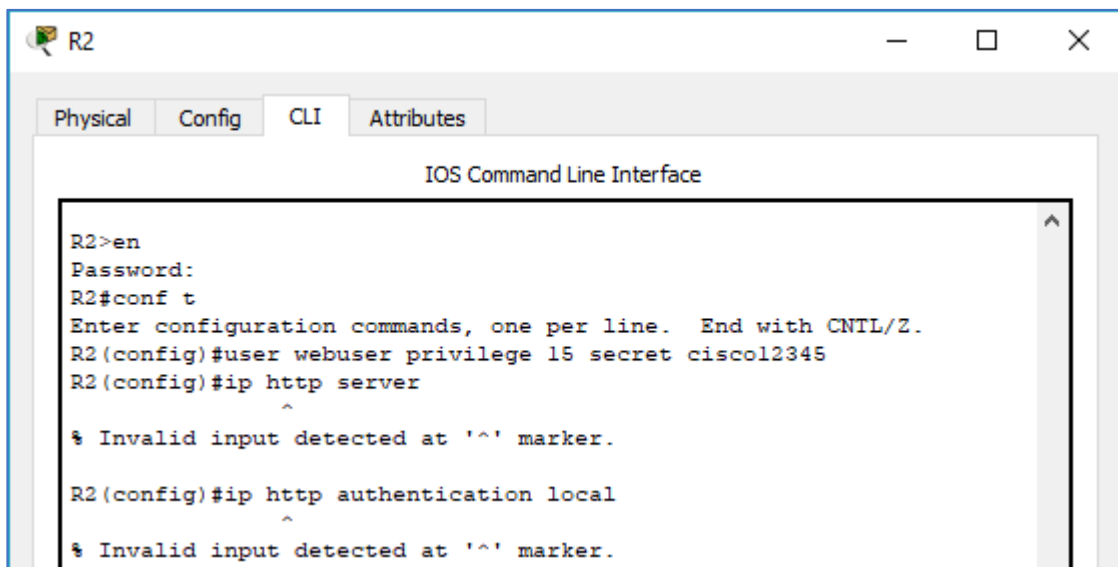
7. Implement DHCP and NAT for IPv4
8. Configurar R1 como servidor DHCP para las VLANs 30 y 40.
9. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.



```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp pool admin
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#ip dhcp pool merca
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
```

Imagen 28 - Configuración de los puntos 7, 8 y 9.

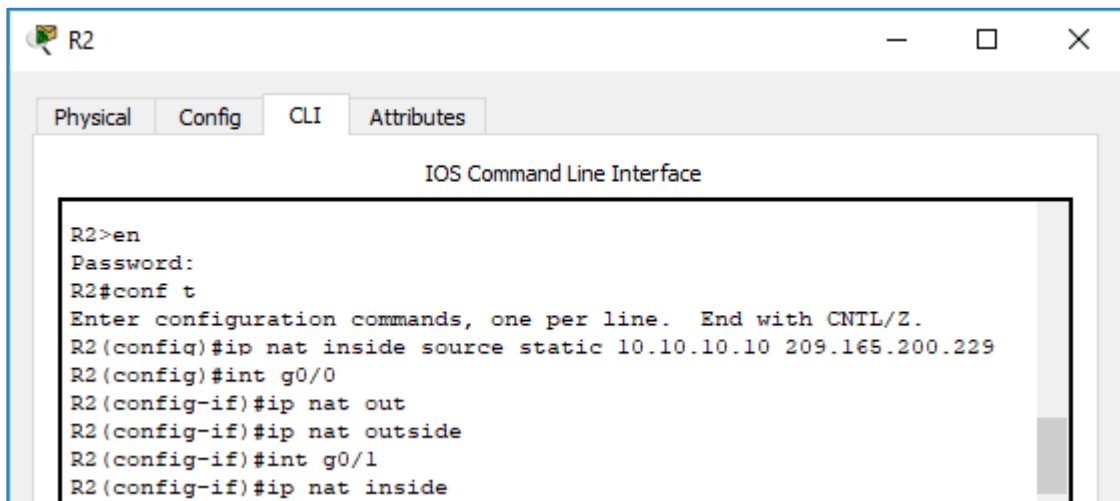
10. Configurar NAT en R2 para permitir que los host puedan salir a internet.



```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip http server
^
% Invalid input detected at '^' marker.
R2(config)#ip http authentication local
^
% Invalid input detected at '^' marker.
```

Imagen 29 - Configuración en R2 para internet

Nota: dado que no se pueden utilizar los comandos: ip http server y ip http authentication local, se emplea un servidor dentro de la topología.

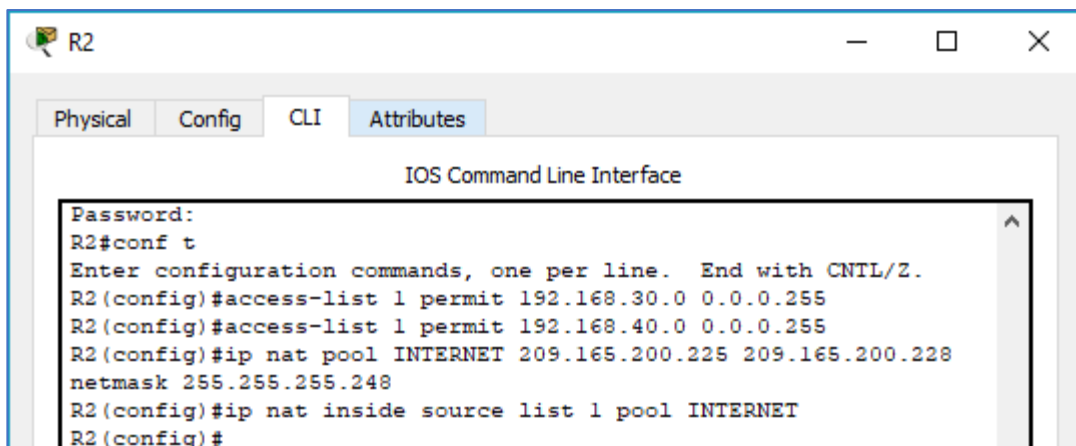


The screenshot shows a terminal window titled 'R2' with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the 'IOS Command Line Interface'. The user enters 'en' to enter enable mode, followed by a password prompt. Then, they enter 'conf t' to enter configuration mode. The following commands are entered: 'ip nat inside source static 10.10.10.10 209.165.200.229', 'int g0/0', 'ip nat out', 'ip nat outside', 'int g0/1', and 'ip nat inside'.

```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int g0/0
R2(config-if)#ip nat out
R2(config-if)#ip nat outside
R2(config-if)#int g0/1
R2(config-if)#ip nat inside
```

Imagen 30 - Configuración de entrada y salida en R2.

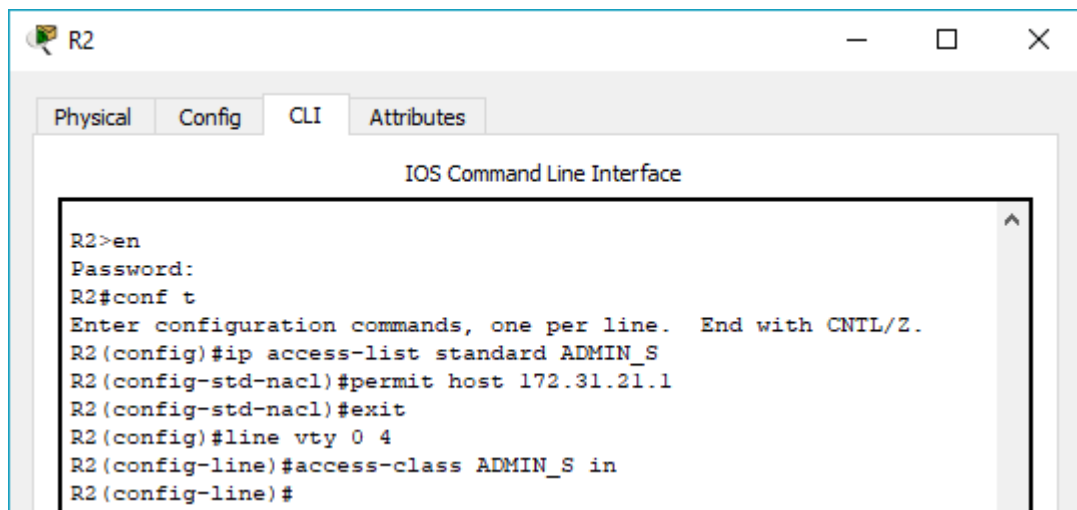
11. Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.



The screenshot shows a terminal window titled 'R2' with tabs for Physical, Config, CLI, and Attributes. The CLI tab is active, displaying the 'IOS Command Line Interface'. The user enters 'en' to enter enable mode, followed by a password prompt. Then, they enter 'conf t' to enter configuration mode. The following commands are entered: 'access-list 1 permit 192.168.30.0 0.0.0.255', 'access-list 1 permit 192.168.40.0 0.0.0.255', 'ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask 255.255.255.248', and 'ip nat inside source list 1 pool INTERNET'.

```
Password:
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)#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)#
```

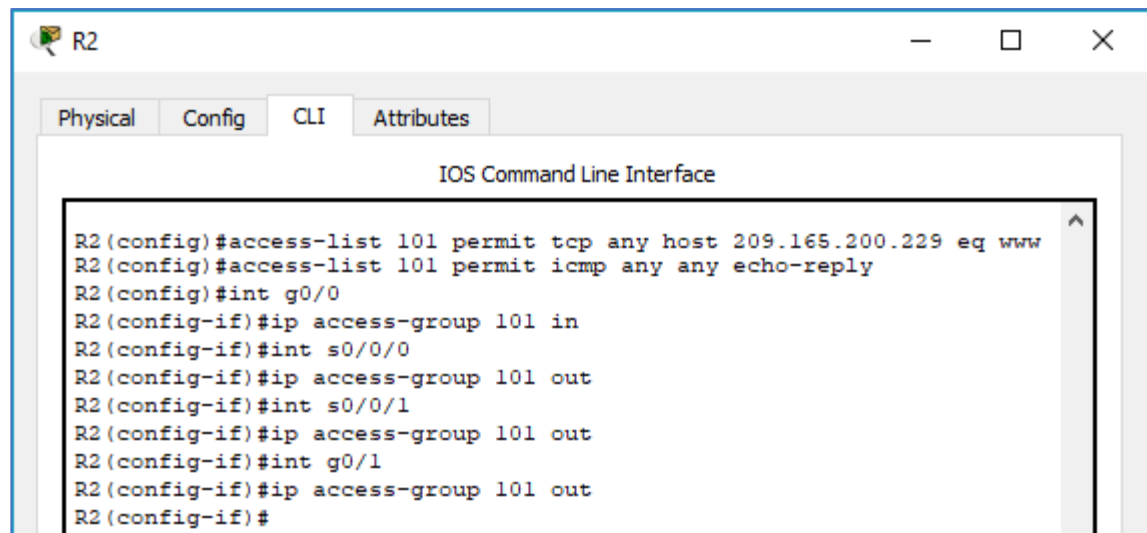
Imagen 31 - Control de IP desde R2



```
R2>en
Password:
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip access-list standard ADMIN_S
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#access-class ADMIN_S in
R2(config-line)#
```

Imagen 32 – Configuración de acceso de tipo estándar

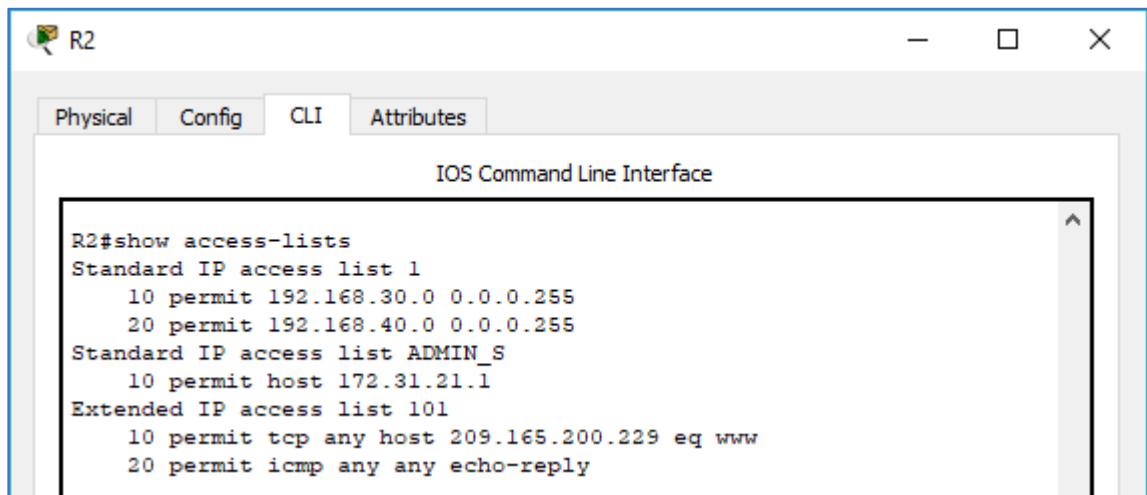
12. Configurar al menos dos listas de acceso de tipo extendido o nombradas a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.



```
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)#int g0/0
R2(config-if)#ip access-group 101 in
R2(config-if)#int s0/0/0
R2(config-if)#ip access-group 101 out
R2(config-if)#int s0/0/1
R2(config-if)#ip access-group 101 out
R2(config-if)#int g0/1
R2(config-if)#ip access-group 101 out
R2(config-if)#
```

Imagen 33 - - Configuración de acceso de tipo extendido

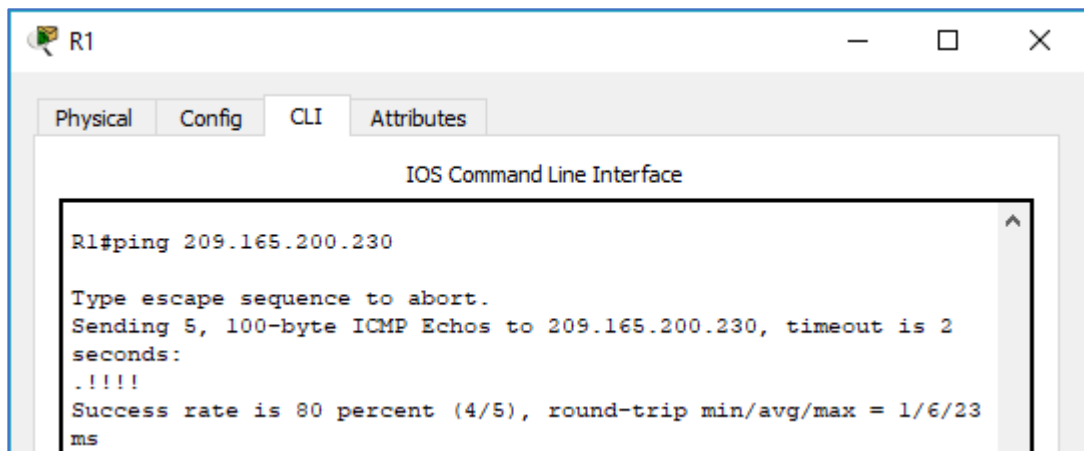
13. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.



The screenshot shows a terminal window for router R2. The window title is 'R2' and it has standard window controls. Below the title bar are tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, and the terminal displays the output of the 'show access-lists' command. The output shows three access lists: a standard IP access list '1' with two permit rules, a standard IP access list 'ADMIN_S' with one permit rule, and an extended IP access list '101' with two permit rules.

```
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
Standard IP access list ADMIN_S
 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
```

Imagen 34 - Lista de accesos



The screenshot shows a terminal window for router R1. The window title is 'R1' and it has standard window controls. Below the title bar are tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, and the terminal displays the output of the 'ping 209.165.200.230' command. The output shows that 5 ICMP Echoes were sent, 4 were received, and the success rate is 80 percent.

```
R1#ping 209.165.200.230

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.230, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/6/23
ms
```

Imagen 35 - Ping de R1 a PC internet

CONCLUSIONES

- De acuerdo con los contenidos analizados en el diplomado, podemos conceptualizar con claridad el termino de red, que no es más que un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.) y servicios (acceso a internet, e-mail, chat), etc.
- El protocolo DHCP está diseñado fundamentalmente para ahorrar tiempo gestionando direcciones IP en una red grande. El servicio DHCP se encuentra activo en un servidor donde se centraliza la administración de las direcciones IP de la red.
- OSPF es un protocolo que gestiona un sistema autónomo (AS) en áreas. Dichas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de encaminamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área.
- Las listas de control de acceso desempeñan un gran papel como medida de seguridad lógica, ya que su cometido siempre es controlar el acceso a los recursos o activos del sistema.

REFERENCIAS BIBLIOGRÁFICAS

Shaughnessy, T., Velte, T., & Sánchez García, J. I. (2000). Manual de CISCO.

Ariganello, E., & Sevilla, B. (2011). Redes CISCO - guía de estudio para la certificación CCNP (No. 004.6 A73).

Benchimol, D. (2010). Redes Cisco-Instalacion y administracion de hardware y software.

CISCO. (s.f.). Principios básicos de routing y switching: Listas de Control de Acceso. (2017), Tomado de: <https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#9.0.1>

Principios básicos de routing y switching: Traducción de direcciones de red para IPv4. (2017), Tomado de: <https://static-courseassets.s3.amazonaws.com/RSE503/es/index.html#11.0>

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

Teare, D., Vachon B., Graziani, R. (2015). CISCO Press (Ed). Implementing IPv4 in the Enterprise Network. Implementing Cisco IP Routing (ROUTE) Foundation Learning Guide CCNP ROUTE 300-101. Recuperado de <https://1drv.ms/b/s!AmIJYei-NT1lInMfy2rhPZHwEoWx>

Segui, F. B. (2015). Configuración DHCP en routers CISCO.

Chamorro Serna, L., Montaña Torres, O., Guzmán Pérez, E. H., Daza Navia, M. Y., & Castillo Ortiz, O. F. (2018). Diplomado de Profundización Cisco-Enrutamiento en soluciones de red.

Es.wikipedia.org. (2018). Open Shortest Path First. [online] disponible en: https://es.wikipedia.org/wiki/Open_Shortest_Path_First [28 May 2018].