

Evaluación – Prueba de habilidades prácticas CCNA

Elkin Alan Gutiérrez de Piñeres Parra

Presentado A:

Efraín Alejandro Pérez

Grupo 203092_4

Universidad Nacional y a Distancia
Facultad, Ingeniería de Sistemas
Ciudad, Colombia
Año 2018

Contenido

Contenido	III
Tabla de Imagenes	IV
Descripción de escenarios propuestos para la prueba de habilidades	8
Capítulo 1.....	8
1. Escenario 1	8
Descripción de las actividades	11
Desarrollo del Escenario 1.....	12
Part 1: Asignación VLAN y de puertos	12
Part 2: Desactivamos los puertos que no se van a utilizar	15
Part 3: Configuración IP para R1, R2 y R3.....	16
Part 4: Configuración IPv4.....	19
Part 5: Configurar NAT.....	19
Part 6: Configurar R1 ruta estática.....	20
Part 7: R2 como servidor DHCP	21
Part 8: R2, ruta entre las VLAN 100 y 200.	22
Part 9: El Servidor0 es sólo un servidor IPv6.....	22
Part 10: Configurar como DHCP y DHCPv6.....	24
Part 11: Tener direcciones IPv4 e IPv6 configuradas (dual- stack).	26
Part 12: R1, R2 y R3 intercambian información de routing mediante RIP.....	27
Part 13: Enlazar R1, R2 y R3	28
Part 14: Verificando la conectividad.	29
Capítulo 2.....	31
2. Escenario 2	31
Desarrollo Escenario 2.....	32
Part 1: Configuraciones e inicialización de los dispositivos.	32

Part 2: Configurar el direccionamiento IP	37
Verificamos la conectividad	43
Part 3: Configurar el protocolo de enrutamiento OSPFv2	45
Verificar información de OSPF.....	50
Part 4: Visualizar procesos OSPF.....	53
Part 5: Configuración Puertos troncales.....	56
Part 6: Implement DHCP and NAT for IPv4.....	64
Part 7: Configurar R1 como servidor DHCP para las VLANs 30 y 40.	64
Part 8: Reservar direcciones.....	65
Part 9: Configurar NAT	66
Part 10: Verificar DHCP y NAT estática.	68
Part 11: Configurar listas de acceso	69
Part 12: Configurar al menos dos listas de acceso de tipo extendido.....	69
Part 13: Verificar procesos de comunicación	69
Conclusiones	76
Bibliografía	77

Tabla de Imagenes

Imagen 1-1 Escenario 1	8
Imagen 2-1 Resultados vlan R2	13
Imagen 3-1 Resultados vlan R3	14
Imagen 4-1 IPv4 para Laptop 31	19
Imagen 5-1 Conectividad con el Servidor0	23
Imagen 6-1 Laptop31 configuración DHCP	24
Imagen 7-1 Laptop30 configuración DHCP	24
Imagen 8-1 PC-31 configuración DHCP	25
Imagen 9-1 PC-30 configuración DHCP	25
Imagen 10-1 Enlace entre R1,R2,R3.....	28
Imagen 11-1 Verificando conectividad Modo gráfico 1.....	30
Imagen 12-1 Verificando conectividad Modo gráfico 2.....	30
Imagen 13-2 Escenario 2	31

Imagen 14-2 Escenario 2 Packet Tracer	32
Imagen 15-2 Iniciando R2	35
Imagen 16-2 Iniciando S1	36
Imagen 17-2 Iniciando S3	36
Imagen 18-2 Configuración IP PC-B	37
Imagen 19-2 Configuración R3	40
Imagen 20-2 Configurar Web Server	41
Imagen 21-2 Configuración servidor 1	42
Imagen 22-2 Configurando S3	43
Imagen 23-2 Verificando Conectividad 1	44
Imagen 24-2 Verificando Conectividad 2	44
Imagen 25-2 Configuración OSPFv2 en R1	46
Imagen 26-2 OSPFv2 en R2	48
Imagen 27-2 Direcciones	48
Imagen 28-2 OSPFv2 en R3	50
Imagen 29-2 Show ip ospf neig en R1	51
Imagen 30-2 Show ip ospf neig en R2	51
Imagen 31-2 Show ip ospf neig en R3	52
Imagen 32-2 Ip protocols en R1	53
Imagen 33-2 Show Ip protocols en R2	54
Imagen 34-2 Show ip protocols en R3	55
Imagen 35-2 Configuración en R1	62
Imagen 36-2 Conectividad S1	63
Imagen 37-2 Conectividad S3	64
Imagen 38-2 Reservando direcciones en R1	66
Imagen 39-2 Configuración NAT	67
Imagen 40-2 DHCP en PC-A	68
Imagen 41-2 DHCP en PC-C	69
Imagen 43-2 Comprobación desde R1	71
Imagen 44-2 Comprobación desde R3	72
Imagen 45-2 Protección de la red	72
Imagen 46-2 Ping de comprobación	73
Imagen 47-2 Ping desde R1	74
Imagen 48-2 Traceroute R1	74
Imagen 49-2 Traceroute R1-2	75

Introducción

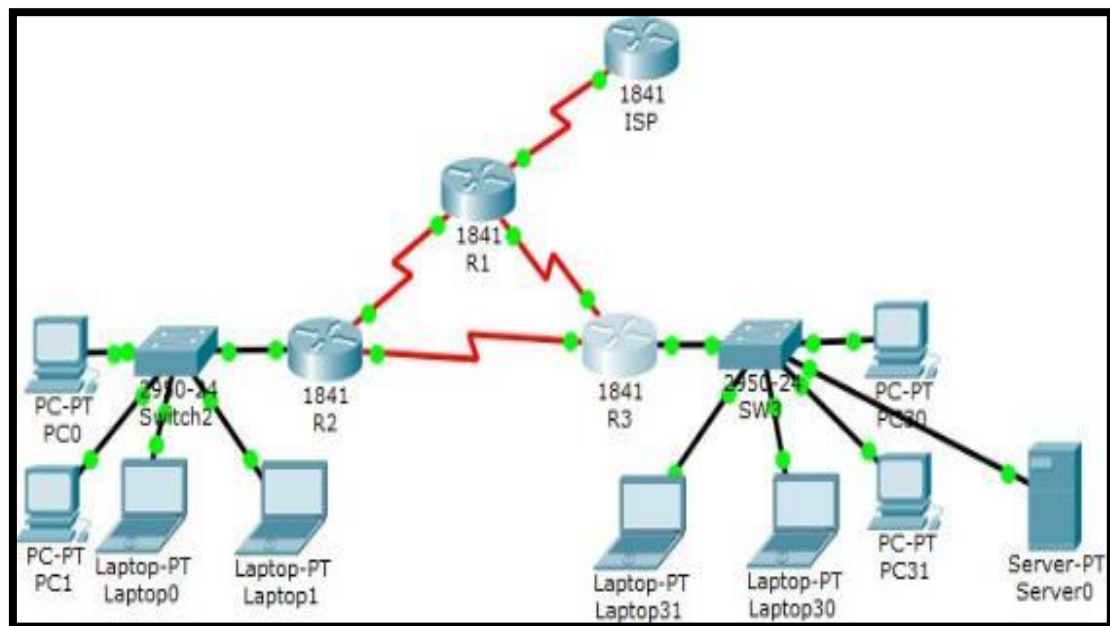
Las tecnologías de la información son la base del desarrollo del mundo y la globalización lo ha demostrado, es tan importante su conocimiento como implementación y uso, por eso diplomados en redes donde se pueda adquirir el afianzamiento académico necesario para entender y conceptualizar las necesidades que pueda tener determinada empresa, es prudente ya que de un verdadero análisis del problema podemos ajustar cualquier requerimiento a una necesidad real, la configuración y alistamiento de las redes, router, la seguridad, enrutamiento OSPF, son parte de los ejercicios planteados, donde recordaremos lo realizado en el trayecto del diplomado, y muy seguramente podremos reforzar y aplicar en estos dos escenarios lo aprendido, en mi caso creo que fue un excelente abrebocas sobre este mundo de las redes, vale la pena reforzar y aplicar e intentar de nuevo otro curso que motive como lo fue este.

Descripción de escenarios propuestos para la prueba de habilidades

Capítulo 1

1. Escenario 1

Imagen 1-1 Escenario 1



Fuente: Proporcionada por la UNAD- Año 2018

Tabla de direccionamiento

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
ISP	S0/0/0	200.123.211.1	255.255.255.0	N/D
R1	Se0/0/0	200.123.211.2	255.255.255.0	N/D
	Se0/1/0	10.0.0.1	255.255.255.252	N/D
	Se0/1/1	10.0.0.5	255.255.255.252	N/D
R2	Fa0/0,100	192.168.20.1	255.255.255.0	N/D
	Fa0/0,200	192.168.21.1	255.255.255.0	N/D
	Se0/0/0	10.0.0.2	255.255.255.252	N/D
	Se0/0/1	10.0.0.9	255.255.255.252	N/D
R3	Fa0/0	192.168.30.1	255.255.255.0	N/D
		2001:db8:130::9C0:80F:301	/64	N/D
	Se0/0/0	10.0.0.6	255.255.255.252	N/D
	Se0/0/1	10.0.0.10	255.255.255.252	N/D
SW2	VLAN 100	N/D	N/D	N/D
	VLAN 200	N/D	N/D	N/D
SW3	VLAN1	N/D	N/D	N/D
PC20	NIC	DHCP	DHCP	DHCP
PC21	NIC	DHCP	DHCP	DHCP
PC30	NIC	DHCP	DHCP	DHCP
PC31	NIC	DHCP	DHCP	DHCP
Laptop20	NIC	DHCP	DHCP	DHCP
Laptop21	NIC	DHCP	DHCP	DHCP
Laptop30	NIC	DHCP	DHCP	DHCP
Laptop31	NIC	DHCP	DHCP	DHCP

Fuente: Proporcionada por la UNAD- Año 2018

Tabla de asignación de VLAN y de puertos

Dispositivo	VLAN	Nombre	Interfaz
SW2	100	LAPTOPS	Fa0/2-3
SW2	200	DESTOPS	Fa0/4-5
SW3	1	-	Todas las interfaces

Fuente: Proporcionada por la UNAD- Año 2018

Tabla de enlaces troncales

Dispositivo local	Interfaz local	Dispositivo remoto
SW2	Fa0/2-3	100

Fuente: Proporcionada por la UNAD- Año 2018

SITUACIÓN

Para desarrollar el escenario N.1, se desarrollará el siguiente planteamiento:

En esta actividad, demostrará y reforzará su capacidad para implementar NAT, servidor de DHCP, RIPV2 y el routing entre VLAN, incluida la configuración de direcciones IP, las VLAN, los enlaces troncales y las subinterfaces. Todas las pruebas de alcance deben realizarse a través de ping únicamente

Descripción de las actividades

- SW1 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.
- Los puertos de red que no se utilizan se deben deshabilitar.
- La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.
- Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP.
- R1 debe realizar una NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se llama INSIDE-DEVS.
- R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.
- R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.
- R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.
- El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).
- La NIC instalado en direcciones IPv4 e IPv6 de Laptop30, de Laptop31, de PC30 y obligación de configurados PC31 simultáneas (dual-stack). Las direcciones se deben configurar mediante DHCP y DHCPv6.
- La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).
- R1, R2 y R3 intercambian información de routing mediante RIP versión 2.
- R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.
- Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre ellos y el servidor.

Para el desarrollo de los escenarios planteados se usó como simulador Packet Tracer 7.1.1

Desarrollo del Escenario 1

Part 1: Asignación VLAN y de puertos

- SW1 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1

Para R2:

A continuación, se describe los pasos y configuración para R2

- Ingresamos a CLI de R2

```
SW2>en
SW2# config t
SW2# hostname R2
R2(config)# vlan 100
R2(config-vlan) # name LAPTOPS
R2(config-vlan)# end
R2(config)# vlan 200
R2(config-vlan)# name DESTOPS
R2(config-vlan)#exit
R2(config)#end
R2#
```

- Ahora asignamos los puertos

```
R2#conf t
R2(config)#int range f0/2-3
R2(config-if-range)#switchport mode access
R2(config-if-range)#switchport access vlan 100
R2(config-if-range)#int range f0/4-5
```

```
R2(config-if-range)#switchport mode access
R2(config-if-range)#switchport access vlan 200
R2(config-if-range)#exit
R2(config-if-range)#exit
```

- Verificamos usando el comando Show vlan

```
R2#show vlan
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int f0/1
R2(config-if)#switchport mode trunk
R2(config-if)#
```

Se muestra la configuración vlan con el comando show

Imagen 2-1 Resultados vlan R2

```
R2#show vlan

VLAN Name                Status    Ports
-----
 1    default                active    Fa0/6, Fa0/9, Fa0/10, Fa0/11
                                           Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                           Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                           Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                           Fa0/24
100  LAPTOPS                active    Fa0/2, Fa0/3
200  DESTOPS                active    Fa0/4, Fa0/5, Fa0/7, Fa0/8
1002 fddi-default          active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active

VLAN Type  SAID      MTU   Parent  RingNo BridgeNo Stp  BrdgMode Transl  Trans2
-----
 1    enet    100001    1500  -       -       -   -       -       0       0
100  enet    100100    1500  -       -       -   -       -       0       0
200  enet    100200    1500  -       -       -   -       -       0       0
1002 fddi    101002    1500  -       -       -   -       -       0       0
1003 tr     101003    1500  -       -       -   -       -       0       0
--More-- |
```

Ahora bien, los pasos a seguir y configuración para R3

Para R3:

```
SW3>en
```

```

SW3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#hostname R3
R3(config)#vlan 1
R3(config-vlan)#exit
R3(config)#int range f0/1-24
R3(config-if-range)#switchport mode access
R3(config-if-range)#switchport access vlan 1
R3(config-if-range)#exit
R3(config)#end
R3#show vlan

```

Imagen 3-1 Resultados vlan R3

```

R3#show vlan

VLAN Name                Status    Ports
-----
 1    default                active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24

1002 fddi-default         active
1003 token-ring-default   active
1004 fddinet-default      active
1005 trnet-default        active

VLAN Type  SAID      MTU   Parent  RingNo BridgeNo  Stp   BrdgMode Trans1 Trans2
-----
 1    enet    100001   1500   -       -       -     -       0       0
1002 fddi    101002   1500   -       -       -     -       0       0
1003 tr     101003   1500   -       -       -     -       0       0
1004 fdnet  101004   1500   -       -       -     ieee    0       0
1005 trnet  101005   1500   -       -       -     ibm     0       0

--More-- |

```

```

R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int f0/1
R3(config-if)#switchport mode trunk

R3(config-if)#

```

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

R3(config-if)#end

R3#

Part 2: Desactivamos los puertos que no se van a utilizar

Como los puertos de red que no se utilizan se deben deshabilitar realizamos las siguientes instrucciones tanto en R3 como en R2.

Para R3:

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#int range f0/6-23

R3(config-if-range)#shutdown

R3(config-if-range)#

R3(config-if-range)#exit

R3(config)#end

R3#

%SYS-5-CONFIG_I: Configured from console by console

wr

Building configuration...

[OK]

R3#

En R2

R2>en

R2#

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#int range f0/6-24

R2(config-if-range)#shut

```
R2(config-if-range)#exit
R2(config)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]
```

Part 3: Configuración IP para R1, R2 y R3

- La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.

En R1:

```
R1#
R1#en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0/0
R1(config-if)#ip address 200.123.211.2
% Incomplete command.
R1(config-if)#ip address 200.123.211.2 255.255.255.0
R1(config-if)#exit
R1(config)#int s0/1/0
R1(config-if)#ip address 10.0.0.1 255.255.255.252
R1(config-if)#exit
R1(config)#int s0/1/1
R1(config-if)#ip address 10.0.0.5 255.255.255.252
R1(config-if)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#wr
Building configuration...
```


[OK]

R1#

En R2:

R2>en

R2#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)#int f0/0.100

R2(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.100, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.100, changed state to up

R2(config-subif)#encapsulation dot1Q 100

R2(config-subif)#ip address 192.168.20.1 255.255.255.0

R2(config-subif)#exit

R2(config)#int f0/0.200

R2(config-subif)#

%LINK-5-CHANGED: Interface FastEthernet0/0.200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.200, changed state to up

R2(config-subif)#encapsulation dot1Q 200

R2(config-subif)#ip address 192.168.21.1 255.255.255.0

R2(config-subif)#exit

R2(config)#int s0/0/0%DHCPD-4-PING_CONFLICT: DHCP address conflict: server pinged 192.168.21.1.

R2(config-if)#int s0/0/0

R2(config-if)#ip address 10.0.0.2 255.255.255.252

R2(config-if)#exit

R2(config)#int s0/0/1

R2(config-if)#ip address 10.0.0.9 255.255.255.252

R2(config-if)#exit

R2(config)#end

R2#

%SYS-5-CONFIG_I: Configured from console by console

wr

Building configuration...

[OK]

R2#

En R3:

R3>en

R3#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#int f0/0

R3(config-if)#ip address 192.168.30.1 255.255.255.0

R3(config-if)#exit

R3(config)#ipv6 unicast-routing

R3(config)#int s0/0/0

R3(config-if)#ip address 10.0.0.6 255.255.255.0

% 10.0.0.0 overlaps with Serial0/0/1

R3(config-if)#exit

R3(config)#int s0/0/1

R3(config-if)#int s0/0/0

R3(config-if)#ip address 10.0.0.6 255.255.255.252

R3(config-if)#exit

R3(config)#int s0/0/1

R3(config-if)#ip address 10.0.0.10 255.255.255.252

R3(config-if)#exit

R3(config)#end

R3#

%SYS-5-CONFIG_I: Configured from console by console

R3#wr

Building configuration...

[OK]

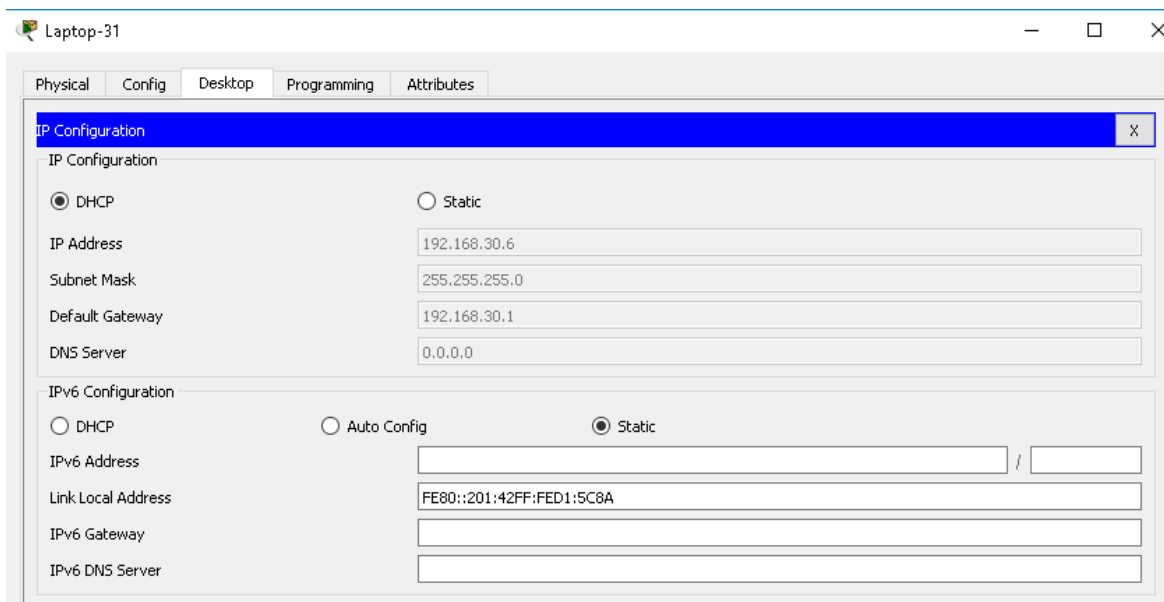
R3#

Part 4: Configuración IPv4

- Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP.

Se realiza el mismo procedimiento para cada PC, incluyendo el servidor.

Imagen 4-1 IPv4 para Laptop 31



Part 5: Configurar NAT

R1 debe realizar una NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se llama INSIDE-DEVS.

```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/1/1
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#int s0/1/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#int s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat pool INSIDE-DEVS 200.123.211.20 200.123.211.128 netmask 255.255.255.0
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255
R1(config)#ip nat inside source list 1 interface s0/0/0 overload
R1(config)#ip nat inside source static tcp 192.168.30.6 80 200.123.211.1 80
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#exit
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

Verificamos

```
R1#show ip nat translations
Pro Inside Global Inside Local Outside Local Outside global
top 200.123.211.1:80 192.168.30.6:80 --- ---
```

```
R1#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 1 extended)
Outside Interfaces: Serial0/0/0
Inside Interfaces: Serial0/1/0, Serial0/1/1
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
R1#
R1#
```

Part 6: Configurar R1 ruta estática

- R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.

```
R1(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R1(config)#access-list 1 permit 10.0.0.0 0.255.255.255
R1(config)#ip nat inside source list 1 interface s0/0/0 overload
R1(config)#ip nat inside source static tcp 192.168.30.6 80 200.123.211.1 80
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#exit
R1(config)#end
R1#
```

Part 7: R2 como servidor DHCP

- R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip dhcp excluded-address 10.0.0.2 10.0.0.9
R2(config)#ip dhcp pool INSIDE-DEVS
R2(dhcp-config)#network 192.168.20.1 255.255.255.0
R2(dhcp-config)#network 192.168.21.1 255.255.255.0
R2(dhcp-config)#
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 0.0.0.0
R2(dhcp-config)#exit
R2(config)#
```

Part 8: R2, ruta entre las VLAN 100 y 200.

- R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.

Ingresamos las siguientes sentencias en R2:

```
R2(config)#int vlan 100
R2(config-if)#ip address 192.168.20.1 255.255.255.0
% 192.168.20.0 overlaps with FastEthernet0/0.100
R2(config-if)#exit
R2(config)#int vlan 200
R2(config-if)#ip address 192.168.21.1 255.255.255.0
% 192.168.21.0 overlaps with FastEthernet0/0.200
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#wr
Building configuration...
[OK]

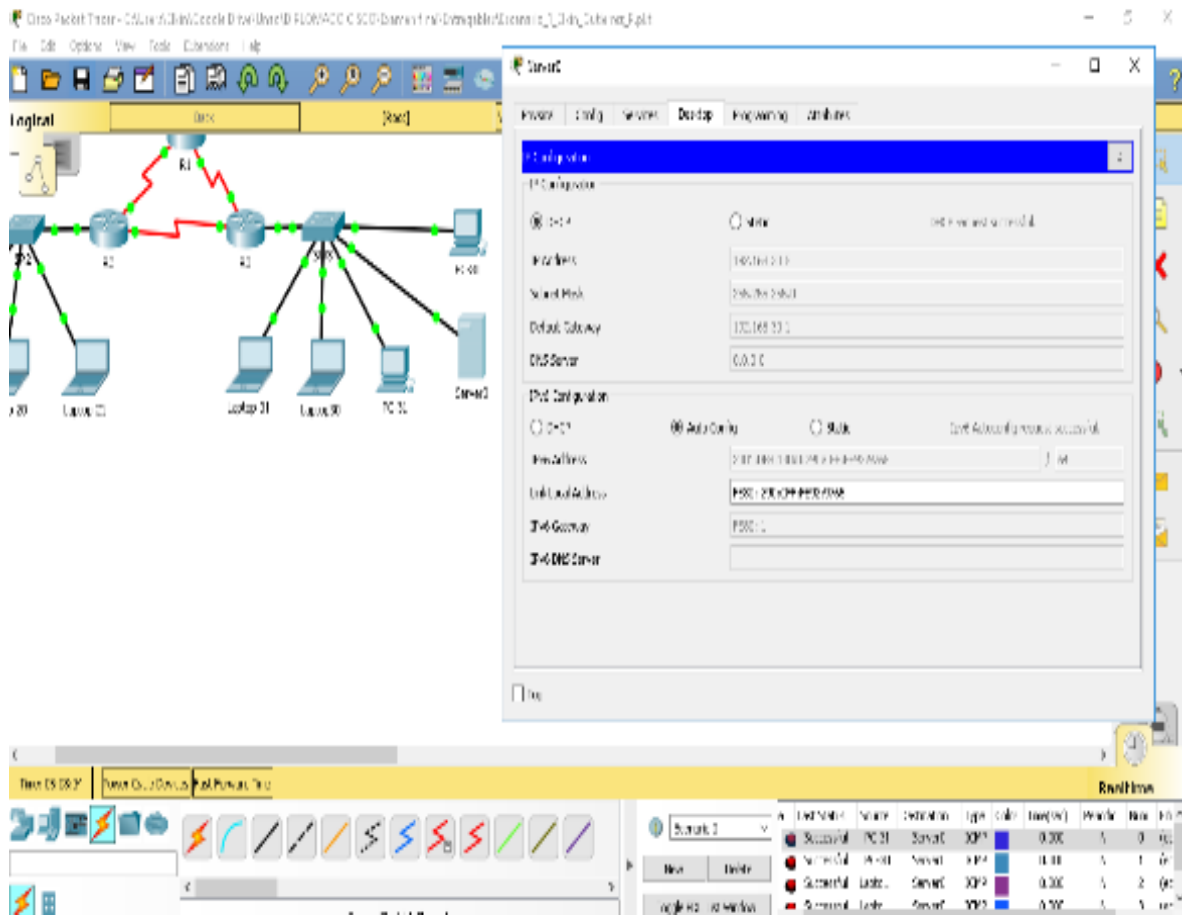
R2#
```

Part 9: El Servidor0 es sólo un servidor IPv6

- El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).

Se configura el servidor y se hace ping, modo gráfico, con resultados satisfactorios.

Imagen 5-1 Conectividad con el Servidor0



Part 10: Configurar como DHCP y DHCPv6.

- La NIC instalado en direcciones IPv4 e IPv6 de Laptop30, de Laptop31, de PC30 y obligación de configurados PC31 simultáneas (dual-stack). Las direcciones se deben configurar mediante DHCP y DHCPv6.

Imagen 6-1 Laptop31 configuración DHCP

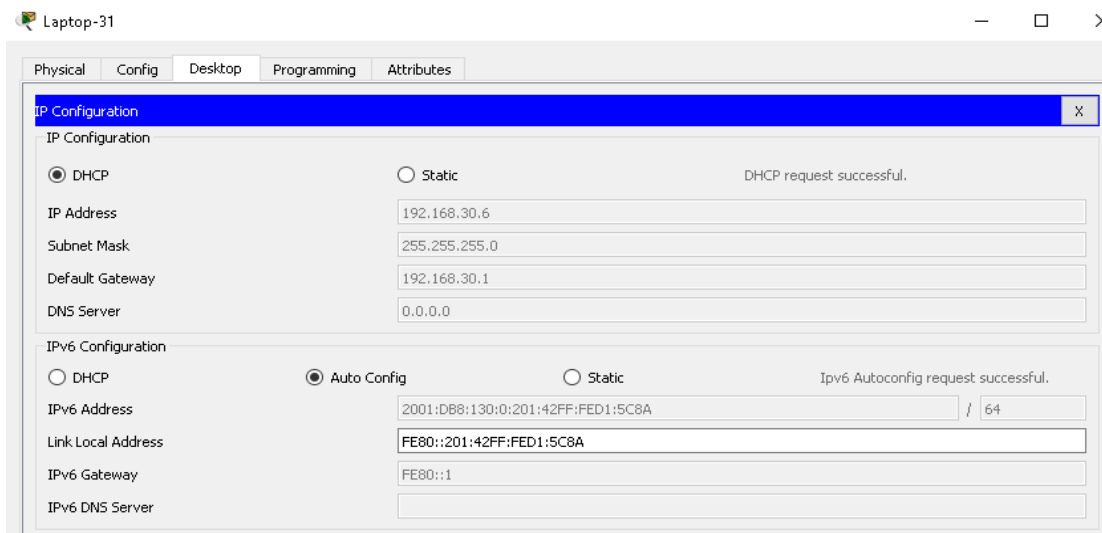
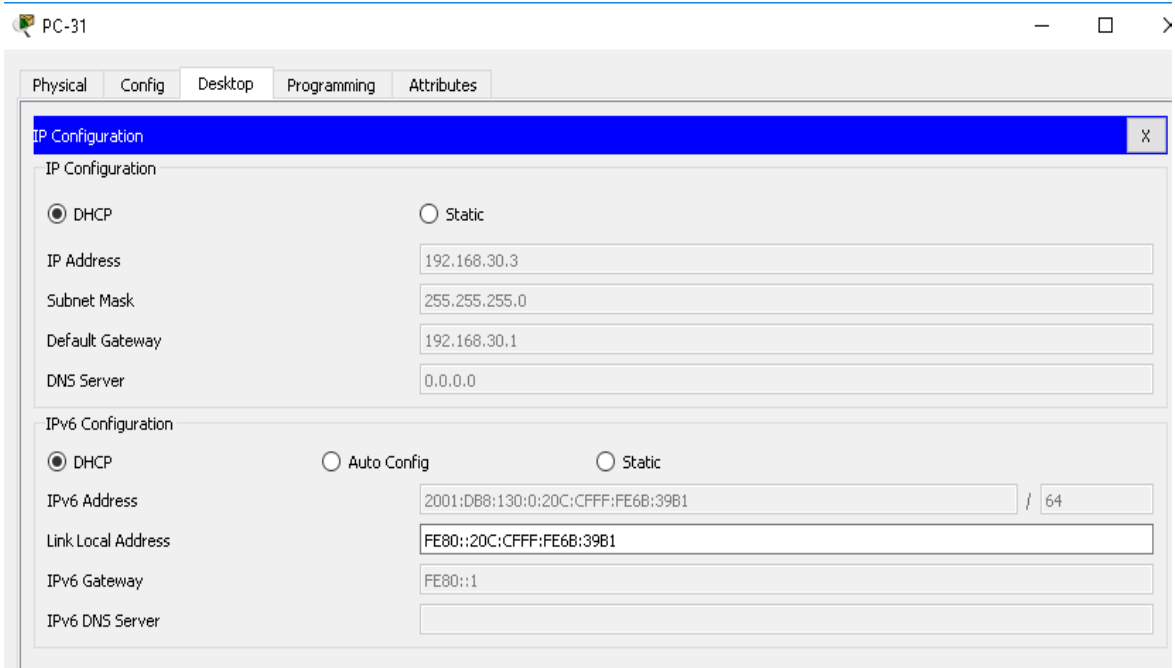
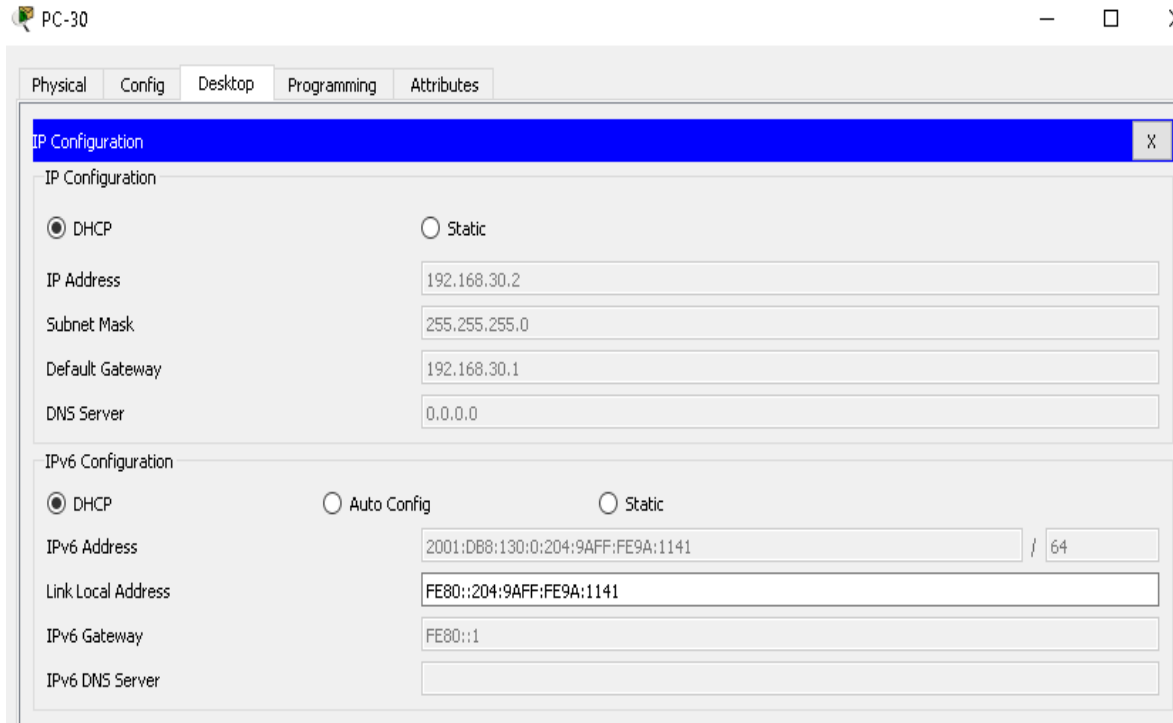


Imagen 7-1 Laptop30 configuración DHCP

**Imagen 8-1** PC-31 configuración DHCP**Imagen 9-1** PC-30 configuración DHCP



Part 11: Tener direcciones IPv4 e IPv6 configuradas (dual-stack).

Por terminal debemos configurar las direcciones dual stack de la siguiente manera:

```
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#int f0/0
R3(config-if)#ipv6 enable
R3(config-if)#ip address 192.168.30.1 255.255.255.0
R3(config-if)#ipv6 address 2001:db8:130::9C0:80F:301/64
R3(config-if)#no shutdown
R3(config-if)#
```

Part 12: R1, R2 y R3 intercambian información de routing mediante RIP

R1, R2 y R3 intercambian información de routing mediante RIP versión 2.

En R1:

```
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#ipv6 unicast-routing
R3(config)#int f0/0
R3(config-if)#ipv6 enable
R3(config-if)#ip address 192.168.30.1 255.255.255.0
R3(config-if)#ipv6 address 2001:db8:130::9C0:80F:301/64
R3(config-if)#no shutdown
R3(config-if)#
```

En R2:

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#network 10.0.0.0
R2(config-router)#network 10.0.0.8
R2(config-router)#do show ip route connected
C 10.0.0.0/30 is directly connected, Serial0/0/0
C 10.0.0.8/30 is directly connected, Serial0/0/1
C 192.168.20.0/24 is directly connected, FastEthernet0/0.100
C 192.168.21.0/24 is directly connected, FastEthernet0/0.200

R2(config-router)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#wr
Building configuration...
[OK]
R2#

R2#
```

En R3:

```
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#network 10.0.0.0
R3(config-router)#network 10.0.0.8
R3(config-router)#end
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#show ip route connected
C 10.0.0.4/30 is directly connected, Serial0/0/0
C 10.0.0.8/30 is directly connected, Serial0/0/1
C 192.168.30.0/24 is directly connected, FastEthernet0/0

R3#wr
Building configuration...
[OK]
R3#

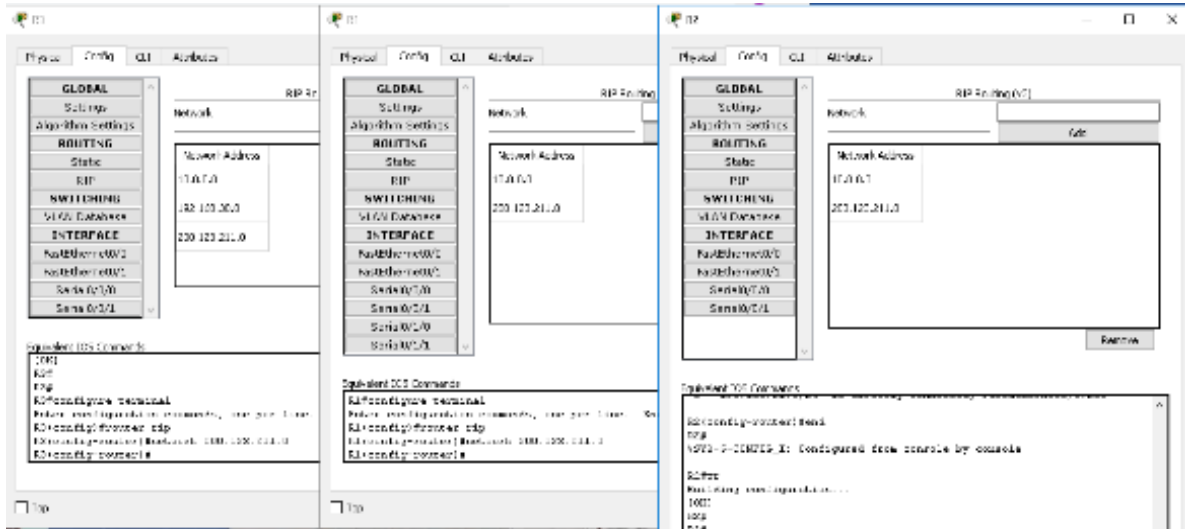
R3#
```

Part 13: Enlazar R1, R2 y R3

R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.

- El protocolo ya está activo y configurado.

Imagen 10-1 Enlace entre R1,R2,R3



Part 14: Verificando la conectividad.

Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre ellos y el servidor.

En el punto (Parte 9) ya existía una restricción para que el servidor solo se conectara dentro de este grupo, por lo que vamos a verificar, no se podría entonces hacer ping al grupo de R2.

Imagen 11-1 Verificando conectividad Modo gráfico 1

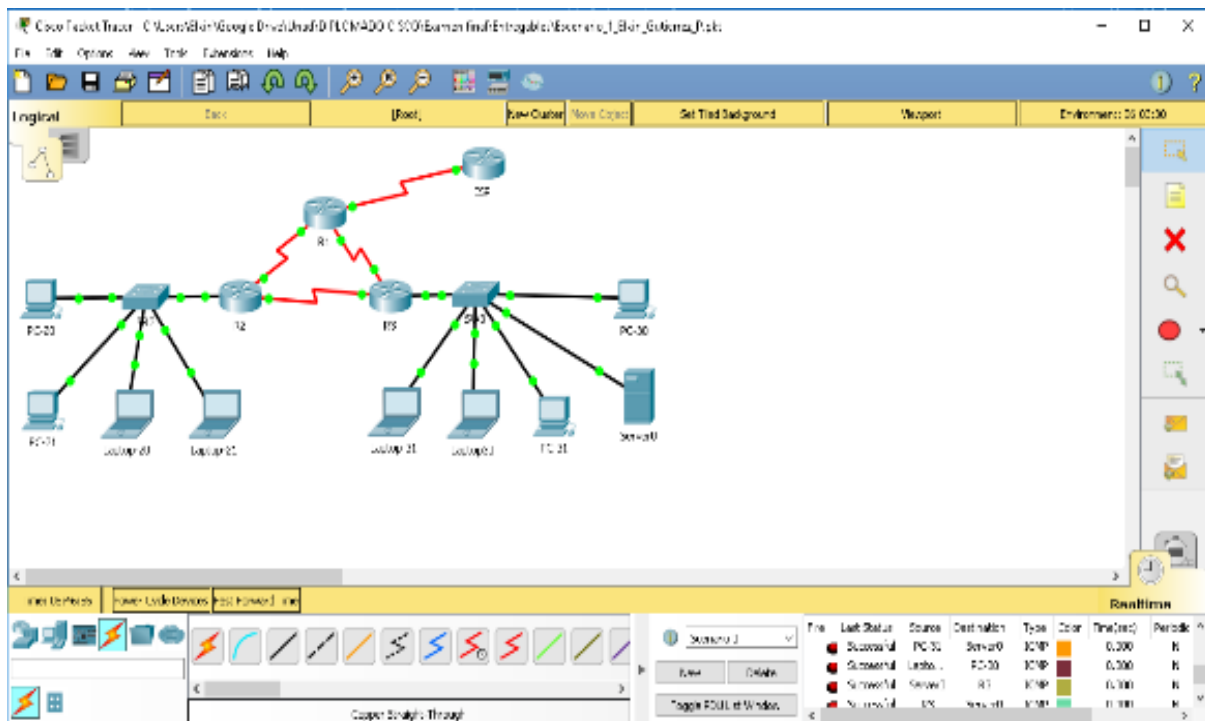


Imagen 12-1 Verificando conectividad Modo gráfico 2

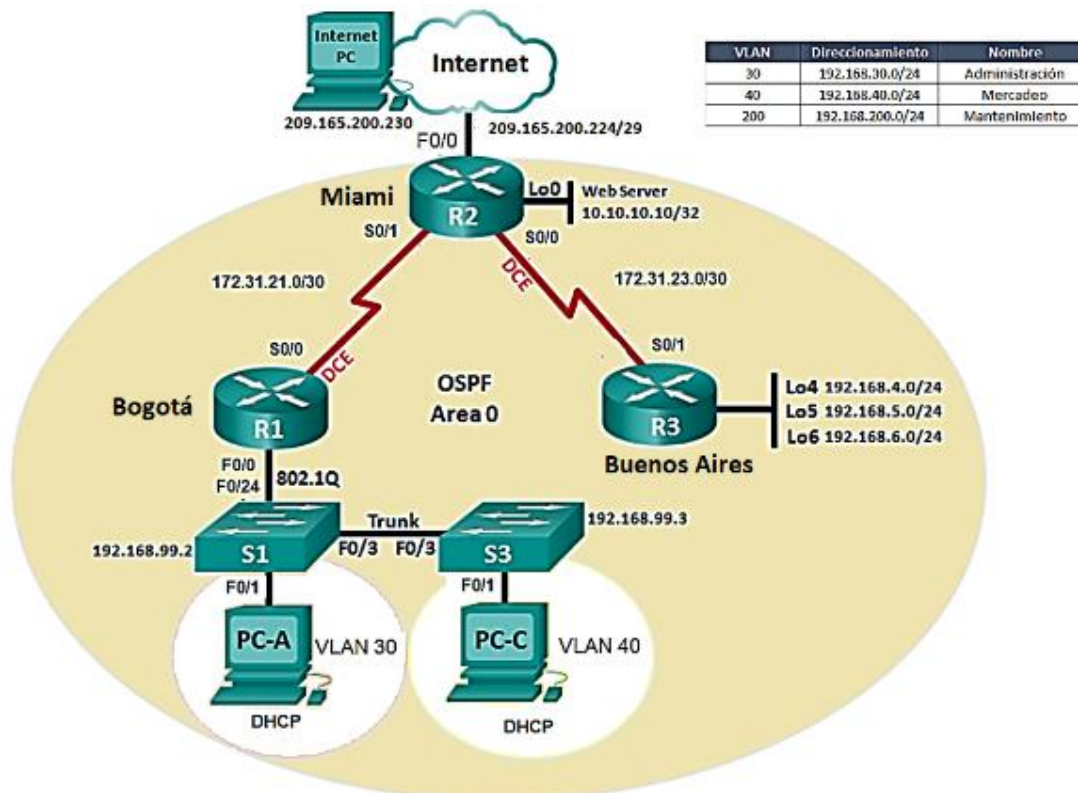
Realtime							
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Successful	PC-31	Server0	ICMP		0.000	N
	Successful	Lapto...	PC-30	ICMP		0.000	N
	Successful	Server0	R3	ICMP		0.000	N
	Successful	R3	Server0	ICMP		0.000	N

Capítulo 2

2. Escenario 2

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, 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.

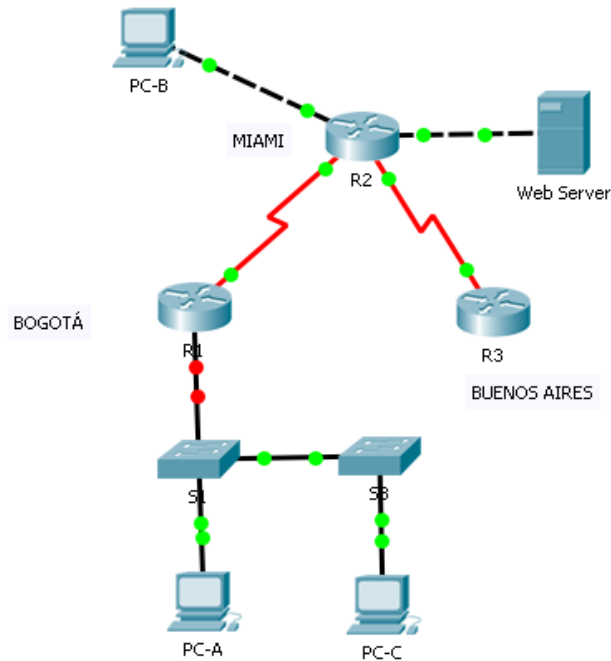
Imagen 13-2 Escenario 2



Fuente: Proporcionada por la UNAD- Año 2018

Desarrollo Escenario 2

Imagen 14-2 Escenario 2 Packet Tracer



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

Part 1: Configuraciones e inicialización de los dispositivos.

Para comenzar el ejercicio comenzamos con la iniciación de los dispositivos, asegurando que no tenga una configuración previa o determinada por defecto.

Hacemos uso de los comandos:

- ❖ Erase startup-config
- ❖ reload

Para R1:

```
Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
```


[OK]

Erase of nvram: complete

%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram

Router#reload

Proceed with reload? [confirm]

System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 2010 by cisco Systems, Inc.

Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB

CISCO1941/K9 platform with 524288 Kbytes of main memory

Main memory is configured to 64/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340

program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software

program load complete, entry point: 0x81000000, size: 0x2bb1c58

Self decompressing the image:

#####

[OK]

Smart Init is enabled

smart init is sizing iomem

TYPE MEMORY_REQ

HWIC Slot 0 0x00200000 Onboard devices &

buffer pools 0x01E8F000

TOTAL: 0x0268F000

Rounded IOMEM up to: 40Mb.

Using 6 percent iomem. [40Mb/512Mb]

Restricted Rights Legend

Use, duplication, or disclosure by the Government is

subject to restrictions as set forth in subparagraph

(c) of the Commercial Computer Software - Restricted

Rights clause at FAR sec. 52.227-19 and subparagraph

(c) (1) (ii) of the Rights in Technical Data and Computer

Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.

170 West Tasman Drive

San Jose, California 95134-1706

Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4,
RELEASE SOFTWARE (fc2)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2012 by Cisco Systems, Inc.

Compiled Thurs 5-Jan-12 15:41 by pt_team
Image text-base: 0x2100F918, data-base: 0x24729040

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!

Para R2:

```
Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
Router#reload
    Proceed with reload? [confirm]
```

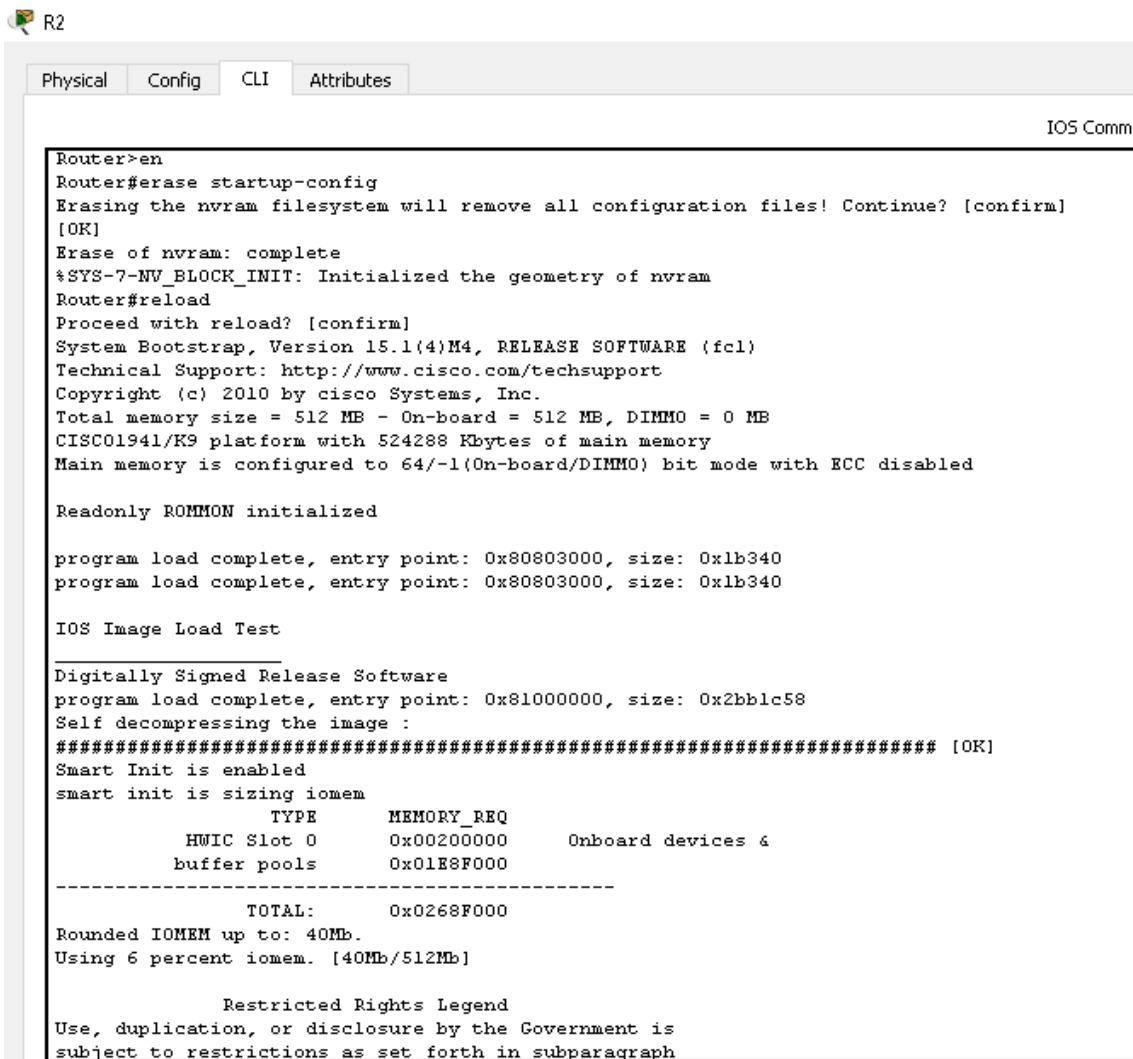
Para R3:

```

Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
Router#reload

Proceed with reload? [confirm]

```

Comprobaciones**Imagen 15-2 Iniciando R2**


```

R2
Physical Config CLI Attributes
IOS Comm
Router>en
Router#erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by Cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMMO = 0 MB
CISCO1941/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 64/-1(On-board/DIMMO) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x2bb1c58
Self decompressing the image :
##### [OK]
Smart Init is enabled
smart init is sizing iomem

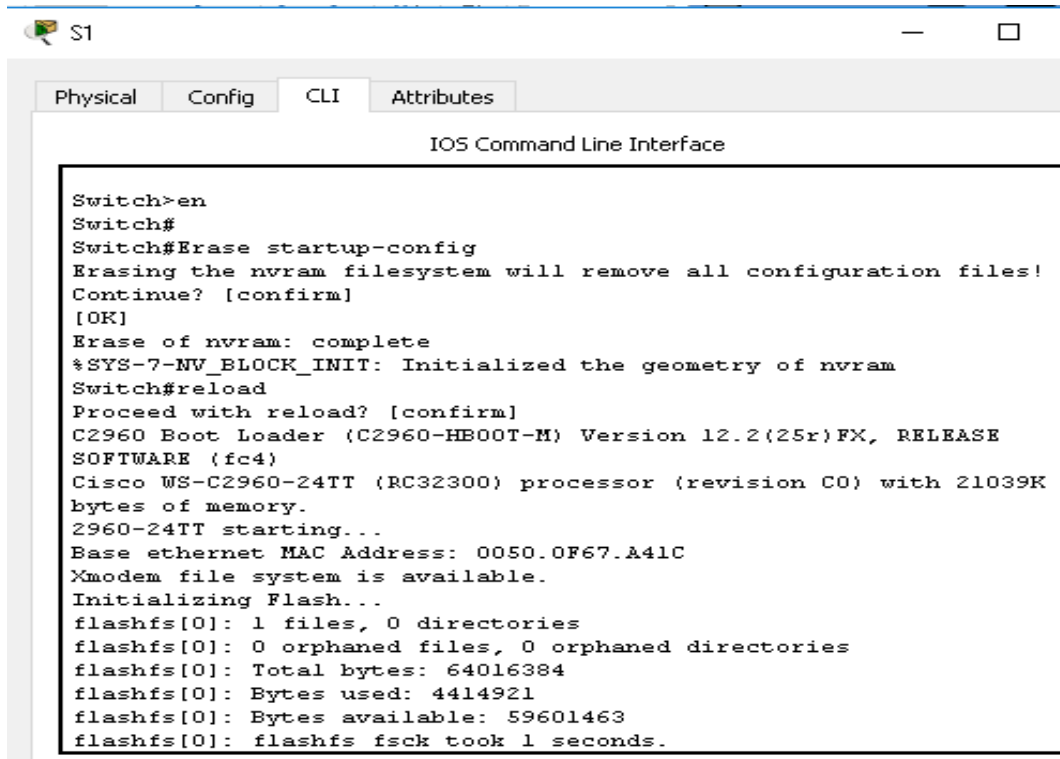
          TYPE          MEMORY_REQ          Onboard devices &
          HWIC Slot 0    0x00200000
          buffer pools   0x01E8F000
-----
TOTAL:          0x0268F000
Rounded IOMEM up to: 40Mb.
Using 6 percent iomem. [40Mb/512Mb]

Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph

```

Para S1:

Imagen 16-2 Iniciando S1



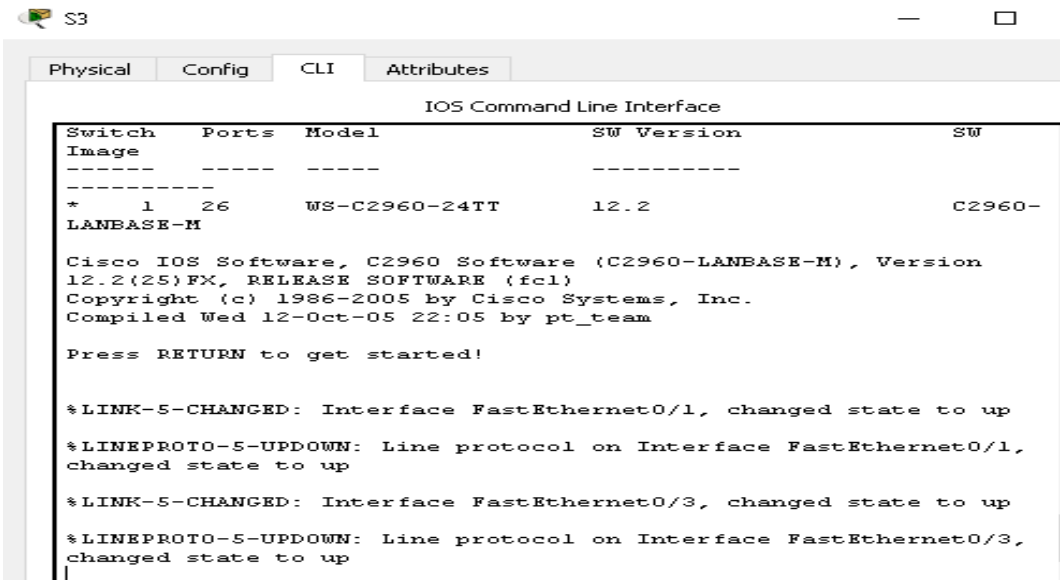
```

Switch>en
Switch#
Switch#Erase startup-config
Erasing the nvram filesystem will remove all configuration files!
Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#reload
Proceed with reload? [confirm]
C2960 Boot Loader (C2960-HB00T-M) Version 12.2(25r)FX, RELEASE
SOFTWARE (fc4)
Cisco WS-C2960-24TT (RC32300) processor (revision C0) with 21039K
bytes of memory.
2960-24TT starting...
Base ethernet MAC Address: 0050.0F67.A41C
Xmodem file system is available.
Initializing Flash...
flashfs[0]: 1 files, 0 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 64016384
flashfs[0]: Bytes used: 4414921
flashfs[0]: Bytes available: 59601463
flashfs[0]: flashfs fsck took 1 seconds.

```

Para S3:

Imagen 17-2 Iniciando S3



```

Switch  Ports  Model          SW Version      SW
Image   -----  -----  -----
*       1    26    WS-C2960-24TT  12.2            C2960-
LANBASE-M

Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3,
changed state to up

```

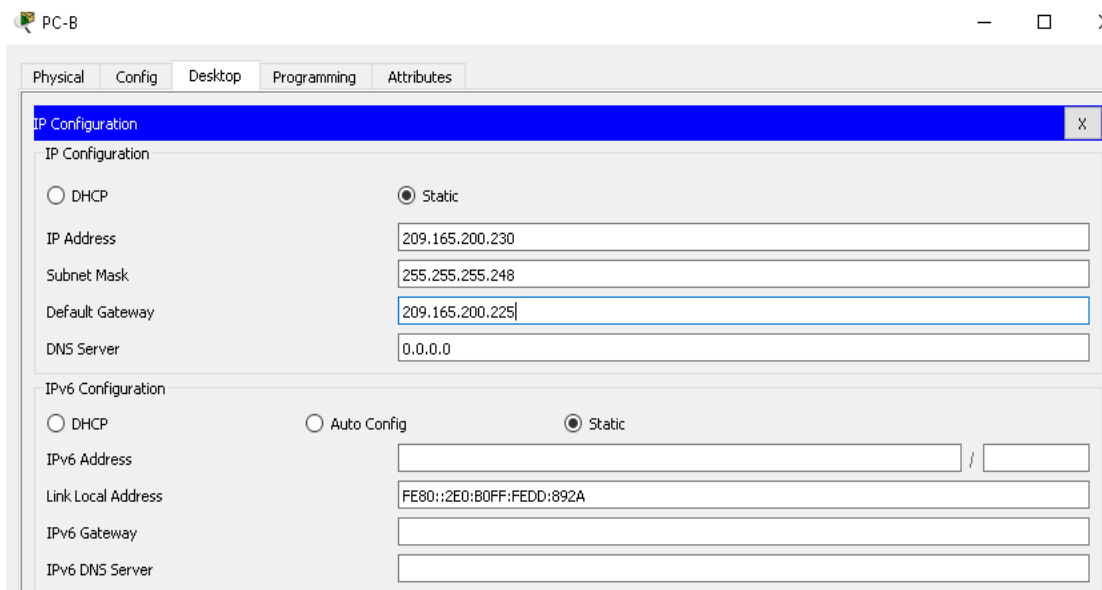
Part 2: Configurar el direccionamiento IP

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

Step 1: Configuración direcciones Ip

Usamos la dirección ip dada para cada equipo y la configuramos así:

Imagen 18-2 Configuración IP PC-B



PC-B

Physical Config Desktop Programming Attributes

IP Configuration

IP Configuration

DHCP Static

IP Address: 209.165.200.230

Subnet Mask: 255.255.255.248

Default Gateway: 209.165.200.225

DNS Server: 0.0.0.0

IPv6 Configuration

DHCP Auto Config Static

IPv6 Address: /

Link Local Address: FE80::2E0:B0FF:FEDD:892A

IPv6 Gateway:

IPv6 DNS Server:

Step 2: Configuración Iniciales

Primero vamos a configurar para los equipos el nombre, contraseñas y banner en caso de que sea un acceso no autorizado.

Configuración para R1

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
```

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service password-encryption
R1(config)#banner motd #El acceso está prohibido!#
R1(config)#
```

```
R1#
```

```
R1(config)#int s0/0/0
R1(config-if)#description R1-R2
R1(config-if)#ip address 172.31.21.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
```

Configuración para R2

```
Router>en
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname R2
R2(config)#enable secret class
R2(config)#line console 0
26
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd #El acceso está prohibido!#
R2(config)#ip http sever
```

```
R2(config)#int s0/0/1
R2(config-if)#description R2-R1
R2(config-if)#ip address 172.31.21.2 255.255.255.252
R2(config-if)#no shutdown
R2(config)#int s0/0/0
R2(config-if)#description R2-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
R2(config)#int G0/0
R2(config-if)#description R2-Internet
R2(config-if)#ip address 209.165.200.225 255.255.255.248
R2(config-if)#no shutdown
R2(config)#int G0/1
R2(config-if)#description R2-Web Server
R2(config-if)#ip address 10.10.10.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 f0/0
R2(config)#
```

Configuramos R3

```
Router>en
Router#config t
Router(config)#no ip domain-lookup
Router(config)#hostname R3
R3(config)#enable secret class
R3(config)#line console 0
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
```

```

R3(config)#banner motd #El acceso no autorizado está prohibido!#
R3(config)#int s0/0/1
R3(config-if)#description R3-R2
R3(config-if)#ip address 172.31.23.2 255.255.255.252
R3(config-if)#no shut
R3(config-if)#int lo4
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)#ip add 192.168.5.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo6
R3(config-if)#ip add 192.168.6.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
R3(config)#exit

```

Imagen 19-2 Configuración R3

The screenshot shows a Cisco IOS CLI session for router R3. The user is in the configuration mode and has entered the following commands: `banner motd #El acceso no autorizado está prohibido!#`, `int s0/0/1`, `description R3-R2`, `ip address 172.31.23.2 255.255.255.252`, `no shut`, `int lo4`, `ip add 192.168.4.1 255.255.255.0`, `no shut`, `int lo5`, `ip add 192.168.5.1 255.255.255.0`, `no shut`, `int lo6`, `ip add 192.168.6.1 255.255.255.0`, `no shut`, `exit`, `ip route 0.0.0.0 0.0.0.0 s0/0/1`, and `exit`. The output shows that the interfaces are now up and the default route is applied. The prompt returns to `R3#`.

```

R3
Physical Config CLI Attributes
IOS Comm.

% Invalid input detected at '^' marker.
R3(config)#R3(config-if)#no shut
^
% Invalid input detected at '^' marker.

R3(config)#int lo4

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)#ip add 192.168.5.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo6

R3(config-if)#ip add 192.168.6.1 255.255.255.0
R3(config-if)#no shut
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)#exit
%LINK-5-CHANGED: Interface Loopback4, changed state to up

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

%LINK-5-CHANGED: Interface Loopback5, changed state to up

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

%LINK-5-CHANGED: Interface Loopback6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up

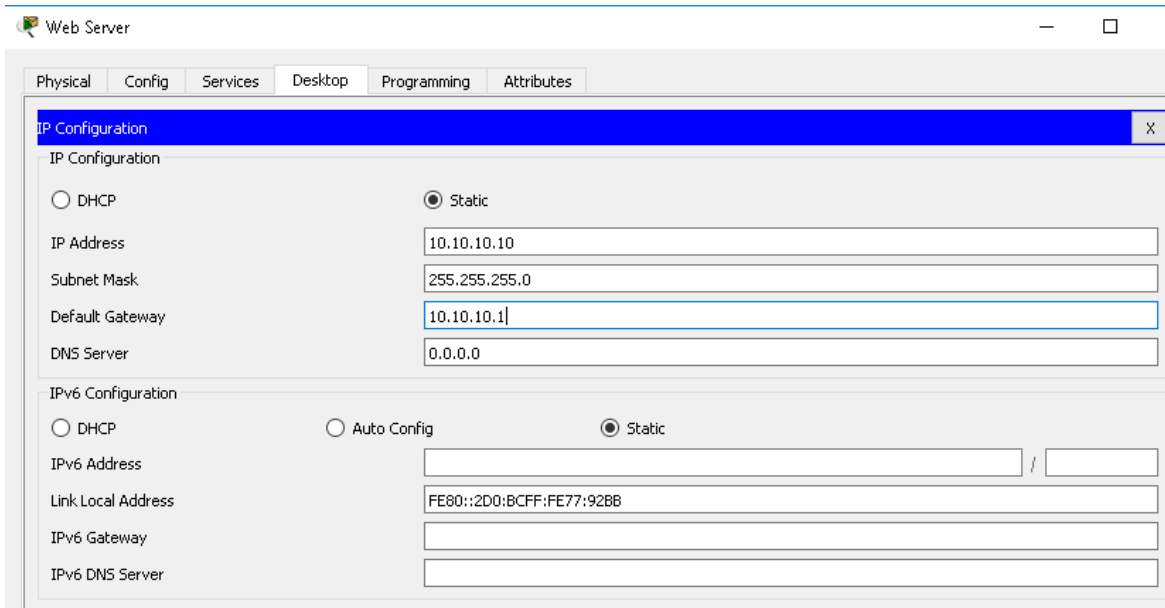
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#

```


Configurar Web Server.

Imagen 20-2 Configurar Web Server

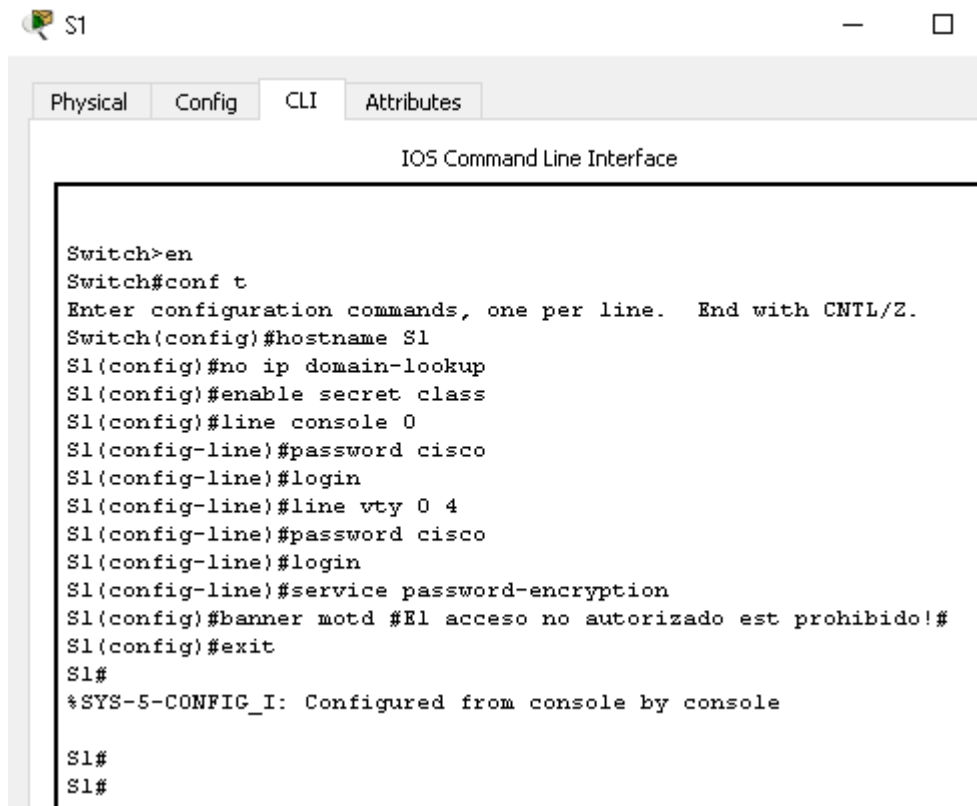


Configurar Servidor 1 (S1)

De igual manera configuramos el servidor S1 con parámetros iniciales nombre, contraseña y banner de acceso prohibido.

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#no ip domain-lookup
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd #El acceso no autorizado está prohibido!#
S1(config)#exit
```

Imagen 21-2 Configuración servidor 1

The image shows a screenshot of a Cisco IOS CLI window titled "S1". The window has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main content area is titled "IOS Command Line Interface" and displays the following text:

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

S1#
S1#
...
```

Configurar S3.

Switch>

Switch>en

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#no ip domain-lookup

Switch(config)#hostname S3

S3(config)#enable secret class

S3(config)#line console 0

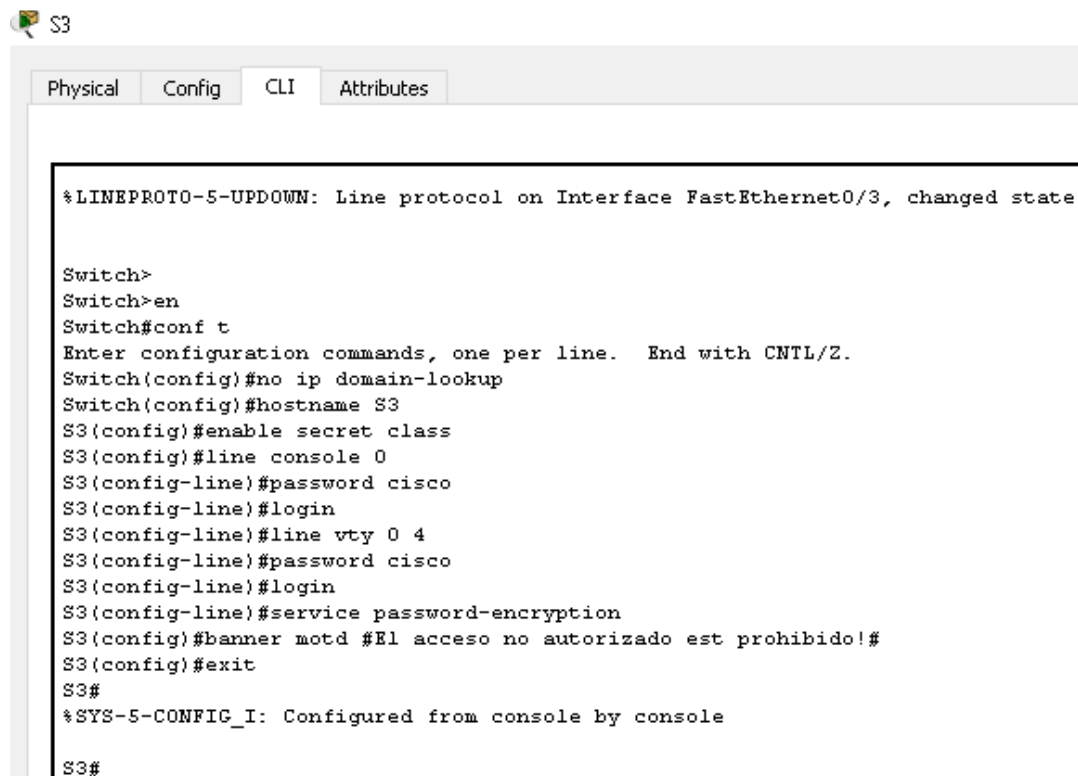
S3(config-line)#password cisco

S3(config-line)#login

S3(config-line)#line vty 0 4

S3(config-line)#password cisco

```
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd #El acceso no autorizado está prohibido!#
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

Imagen 22-2 Configurando S3The image shows a screenshot of a network device's configuration interface. At the top, there are four tabs: 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is selected. The main area displays a terminal window with the following text:

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state

Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd #El acceso no autorizado est prohibido!#
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console

S3#
```

Verificamos la conectividad

En este momento realizamos una verificamos por modo gráfico de la conectividad, si no se logra tener conectividad, se debe repetir los pasos para estar seguros de que todo está bien, antes de seguir.

Imagen 23-2 Verificando Conectividad 1

The diagram shows a network topology with three routers: R1 (BOGOTÁ), R2 (MIAMI), and R3 (BUENOS AIRES). R1 is connected to switches S1 and S2, which are connected to PCs A and C. R2 is connected to PC B and a Web Server. R1 and R2 are connected to each other, and R2 and R3 are connected to each other. A 'Realtime' log window is open at the bottom, displaying the following data:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Successful	R2	Web Server	ICMP	Light Blue	0.000	N	5
●	Successful	R2	R3	ICMP	Brown	0.000	N	6
●	Successful	R3	R2	ICMP	Brown	0.000	N	7
●	Successful	R1	R2	ICMP	Purple	0.000	N	8

Imagen 24-2 Verificando Conectividad 2

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
●	Successful	R2	Web Server	ICMP	Light Blue	0.000	N	5
●	Successful	R2	R3	ICMP	Brown	0.000	N	6
●	Successful	R3	R2	ICMP	Brown	0.000	N	7
●	Successful	R1	R2	ICMP	Purple	0.000	N	8

Part 3: Configurar el protocolo de enrutamiento OSPFv2

Configurar el protocolo OSPFv2 bajo los siguientes criterios para cada uno de los dispositivos enunciados en la siguiente tabla:

OSPFv2 area 0

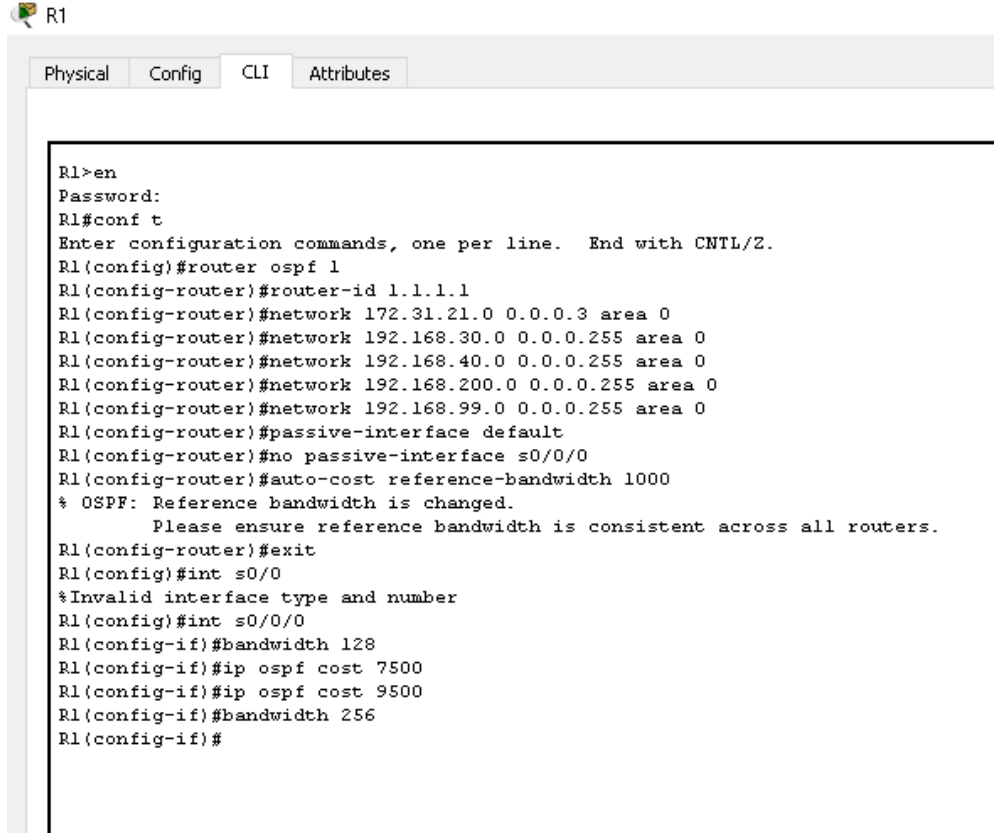
Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

Empezamos:

Configurar OSPFv2 en R1.

```
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 0.0.0.255 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)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
R1(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#exit
R1(config)#int s0/0
%Invalid interface type and number
R1(config)#int s0/0/0
R1(config-if)#bandwidth 256
R1(config-if)#ip ospf cost 9500
```

Imagen 25-2 Configuración OSPFv2 en R1



```

R1
Physical Config CLI Attributes
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 0.0.0.255 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)#network 192.168.99.0 0.0.0.255 area 0
R1(config-router)#passive-interface default
R1(config-router)#no passive-interface s0/0/0
R1(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
    Please ensure reference bandwidth is consistent across all routers.
R1(config-router)#exit
R1(config)#int s0/0
%Invalid interface type and number
R1(config)#int s0/0/0
R1(config-if)#bandwidth 128
R1(config-if)#ip ospf cost 7500
R1(config-if)#ip ospf cost 9500
R1(config-if)#bandwidth 256
R1(config-if)#

```

Configurar OSPFv2 en R2.

```
R2#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R2(config)#router ospf 1
```

```
R2(config-router)#router-id 5.5.5.5
```

```
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
```

```
R2(config-router)#
```

```
02:53:40: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done
```

```
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 f0/1
%Invalid interface type and number
R2(config-router)#passive-interface f0/0/1
%Invalid interface type and number
R2(config-router)#passive-interface g0/0/1
%Invalid interface type and number
R2(config-router)#passive-interface g0/1
R2(config-router)#auto-cost reference-bandwidth 1000
R2(config-router)#exit
R2(config)#int s0/0/1
R2(config-if)#bandwidth 265
R2(config-if)#int s0/0/0
R2(config-if)#bandwidth 256
R2(config-if)#ip ospf cost 9500
R2(config-if)#exit
R2(config)#
```

Imagen 26-2 OSPFv2 en R2

```

R2
Physical Config CLI Attributes
IOS Command Line Interfac

User Access Verification
Password:

R2>en
Password:
R2#router ospf 1
^
% Invalid input detected at '^' marker.

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 5.5.5.5
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#
02:53:40: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from LOADING to FULL, Loading Done

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 f0/1
%Invalid interface type and number
R2(config-router)#passive-interface f0/0/1
%Invalid interface type and number
R2(config-router)#passive-interface g0/0/1
%Invalid interface type and number
R2(config-router)#passive-interface g0/1
R2(config-router)#auto-cost reference-bandwidth 1000
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
R2(config-router)#exit
R2(config)#int s0/0/1
R2(config-if)#bandwidth 265
R2(config-if)#int s0/0/0
R2(config-if)#bandwidth 256
R2(config-if)#ip ospf cost 9500
R2(config-if)#exit
R2(config)#

```

Configurar OSPFv2 en R3.

Imagen 27-2 Direcciones

192	168	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	192.168.4.0
192	168	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	192.168.5.0
192	168	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	192.168.6.0
192	168	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	192.168.4.0/22

R3#config t

Enter configuration commands, one per line. End with CNTL/Z.

R3(config)#router ospf 1

R3(config-router)#router-id 8.8.8.8

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)#

01:03:09: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING to FULL, Loading Done

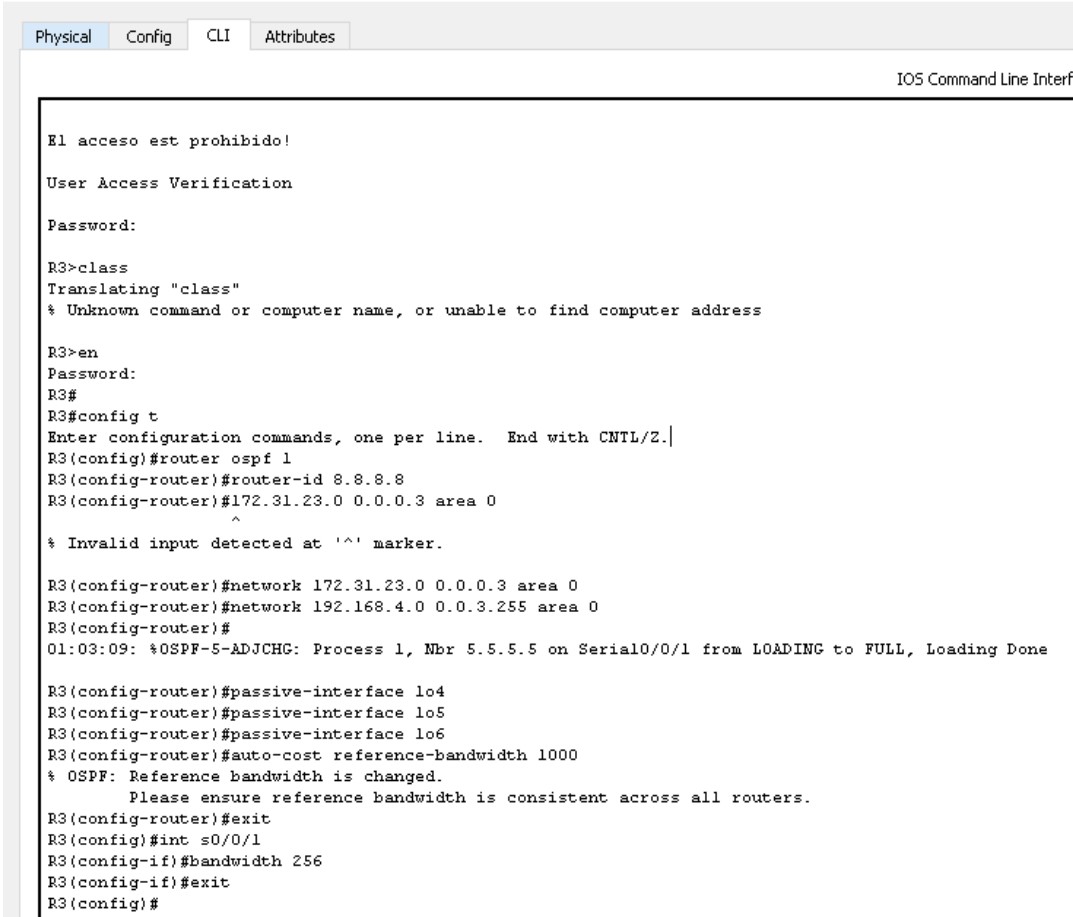

```
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#auto-cost reference-bandwidth 1000
```

% 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 256
R3(config-if)#exit
R3(config)#
```

Imagen 28-2 OSPFv2 en R3



```
R3
Physical Config CLI Attributes
IOS Command Line Interf.

El acceso est prohibido!
User Access Verification
Password:

R3>class
Translating "class"
% Unknown command or computer name, or unable to find computer address

R3>en
Password:
R3#
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router ospf 1
R3(config-router)#router-id 8.8.8.8
R3(config-router)#172.31.23.0 0.0.0.3 area 0
^
% Invalid input detected at '^' marker.

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)#
01:03:09: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from LOADING to FULL, Loading Done

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 1000
% 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 256
R3(config-if)#exit
R3(config)#
```

Verificar información de OSPF

Verificamos la información OSPF de los dispositivos usando el comando show ip ospf neig

Para R1:

```
show ip ospf neig
```

Imagen 29-2 Show ip ospf neig en R1

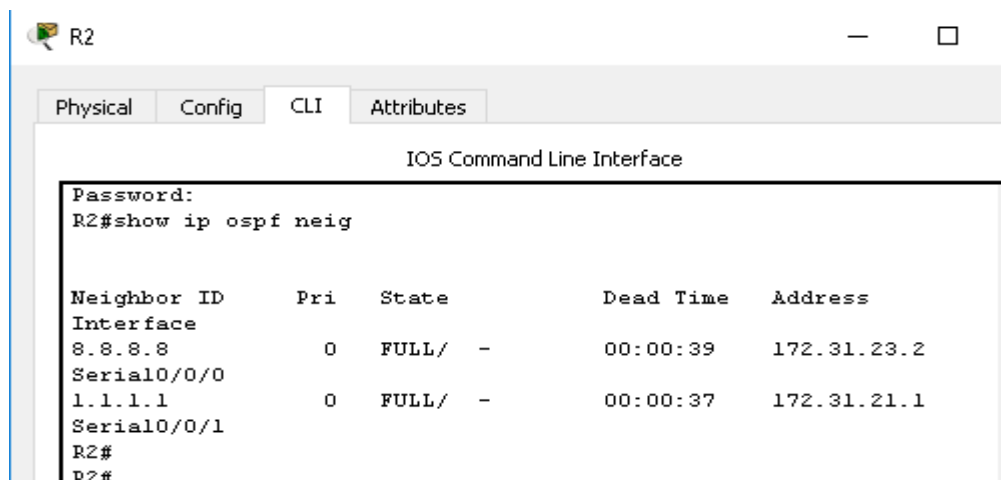
```
R1#show ip ospf neig
```

Neighbor ID	Pri	State	Dead Time	Address
Interface				
5.5.5.5	0	FULL/ -	00:00:30	172.31.21.2
Serial0/0/0				

Para R2

```
show ip ospf neig
```

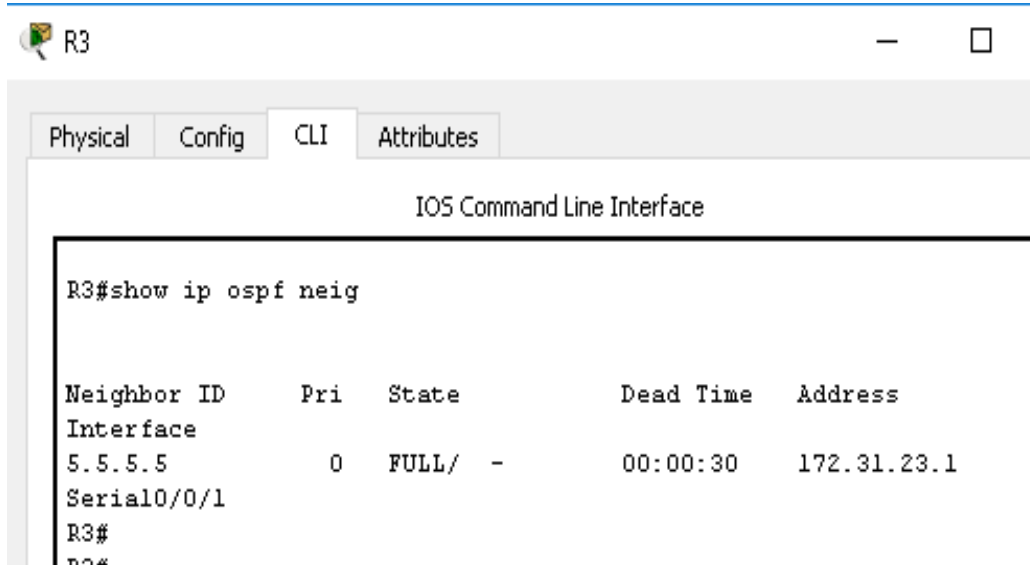
Imagen 30-2 Show ip ospf neig en R2



Para R3

Usando el comando R3#show ip ospf neig

Imagen 31-2 Show ip ospf neig en R3



```
R3#show ip ospf neig

Neighbor ID      Pri   State           Dead Time   Address
Interface
5.5.5.5          0    FULL/ -         00:00:30   172.31.23.1
Serial10/0/1
R3#
```

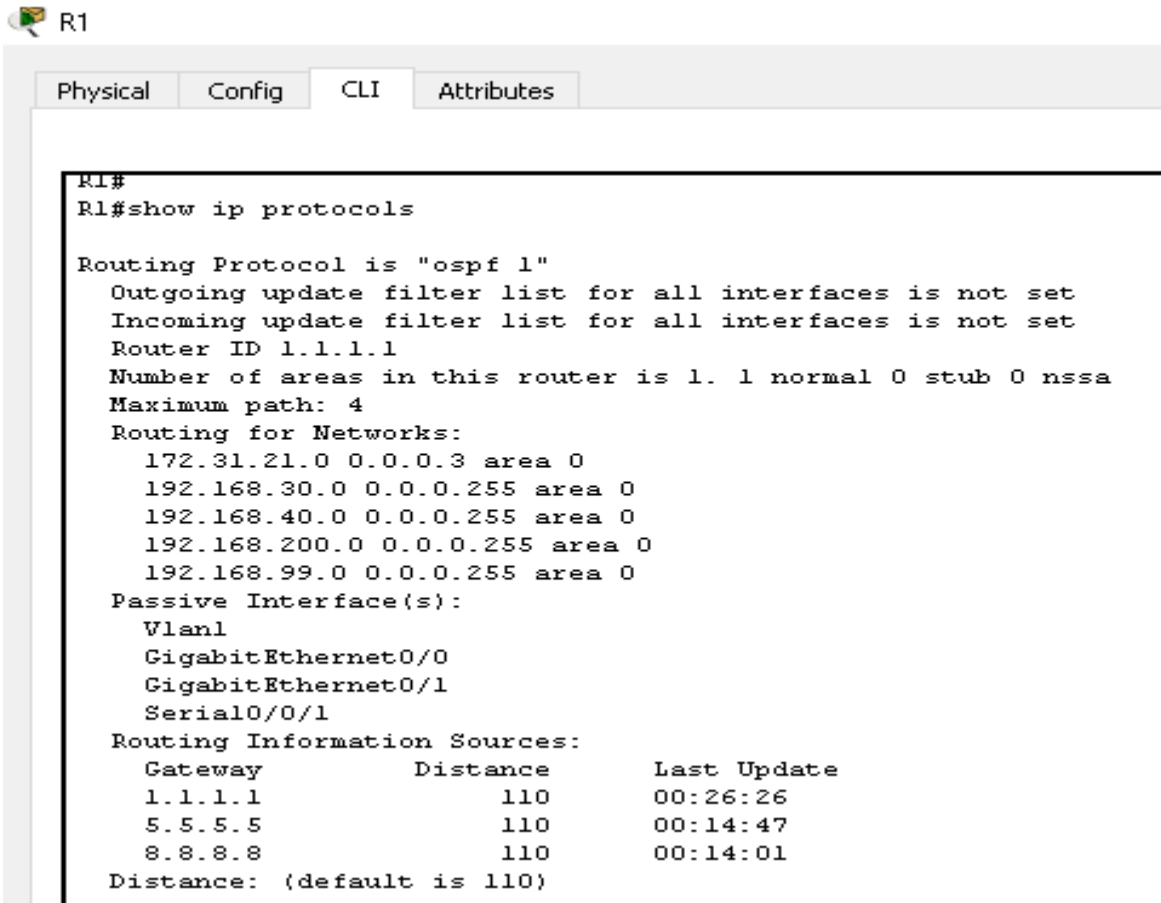
Part 4: Visualizar procesos OSPF

A continuación, vamos a Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, y passive interfaces configuradas en cada router.

Para R1 usando el comando

```
R1#show ip protocols
```

Imagen 32-2 Ip protocols en R1

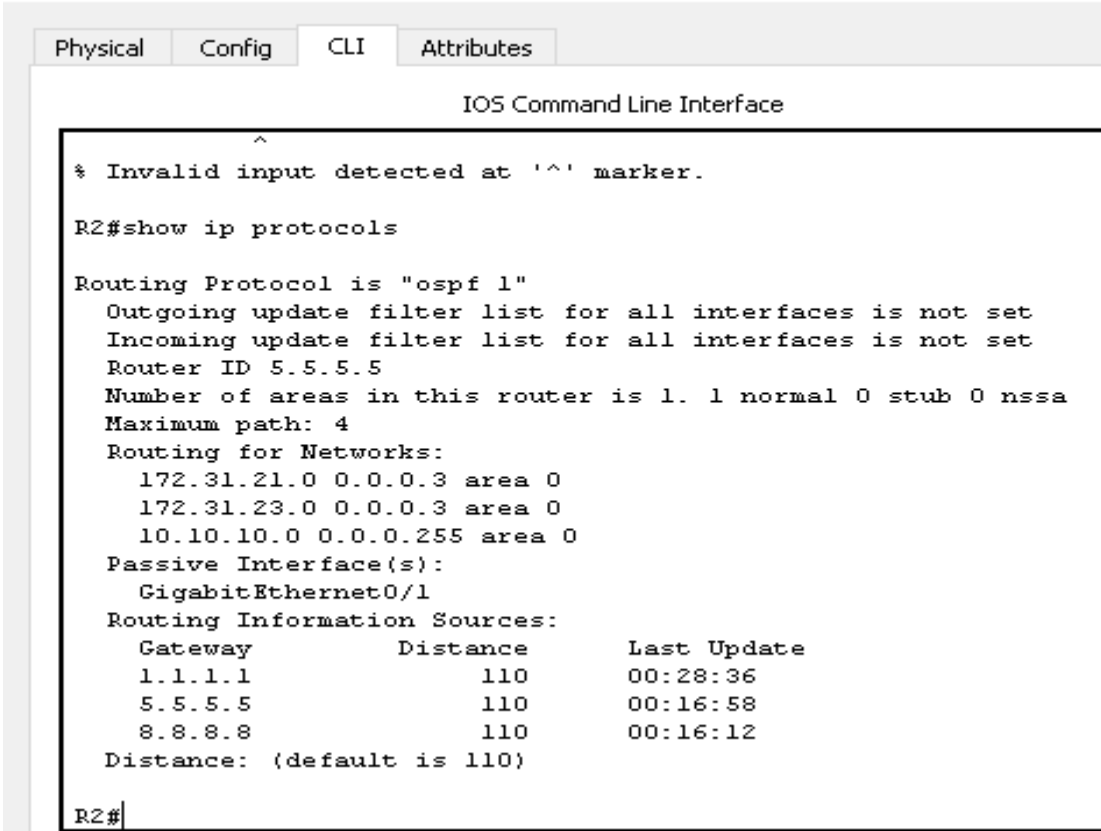


```
R1#
R1#show ip protocols

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 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    192.168.30.0 0.0.0.255 area 0
    192.168.40.0 0.0.0.255 area 0
    192.168.200.0 0.0.0.255 area 0
    192.168.99.0 0.0.0.255 area 0
  Passive Interface(s):
    Vlan1
    GigabitEthernet0/0
    GigabitEthernet0/1
    Serial0/0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:26:26
    5.5.5.5          110          00:14:47
    8.8.8.8          110          00:14:01
  Distance: (default is 110)
```

Para R2 usando el comando

R2#show ip protocols

Imagen 33-2 Show Ip protocols en R2

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

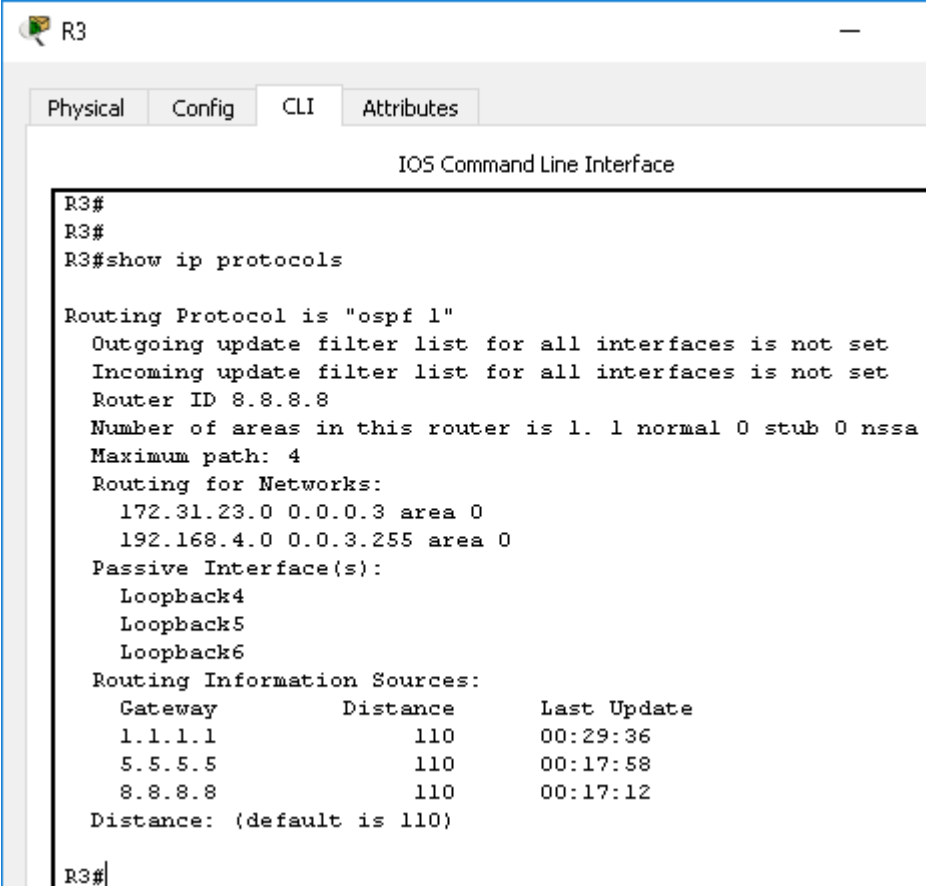
R2#show ip protocols

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 5.5.5.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    172.31.21.0 0.0.0.3 area 0
    172.31.23.0 0.0.0.3 area 0
    10.10.10.0 0.0.0.255 area 0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    1.1.1.1          110          00:28:36
    5.5.5.5          110          00:16:58
    8.8.8.8          110          00:16:12
  Distance: (default is 110)

R2#
```

Para R3 usando el comando

R3#show ip protocols

Imagen 34-2 Show ip protocols en R3

The screenshot shows a terminal window titled 'R3' with tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'CLI' tab is active, displaying the 'IOS Command Line Interface'. The user has entered the command 'show ip protocols', and the output is as follows:

```
R3#
R3#
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 8.8.8.8
  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          00:29:36
    5.5.5.5          110          00:17:58
    8.8.8.8          110          00:17:12
  Distance: (default is 110)

R3#
```

Part 5: Configuración Puertos troncales

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

Configuramos los siguientes ítems en el proceso para los dispositivos:

1. En el Switch 3 deshabilitar DNS lookup
2. Asignar direcciones IP a los Switches acorde a los lineamientos.
3. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

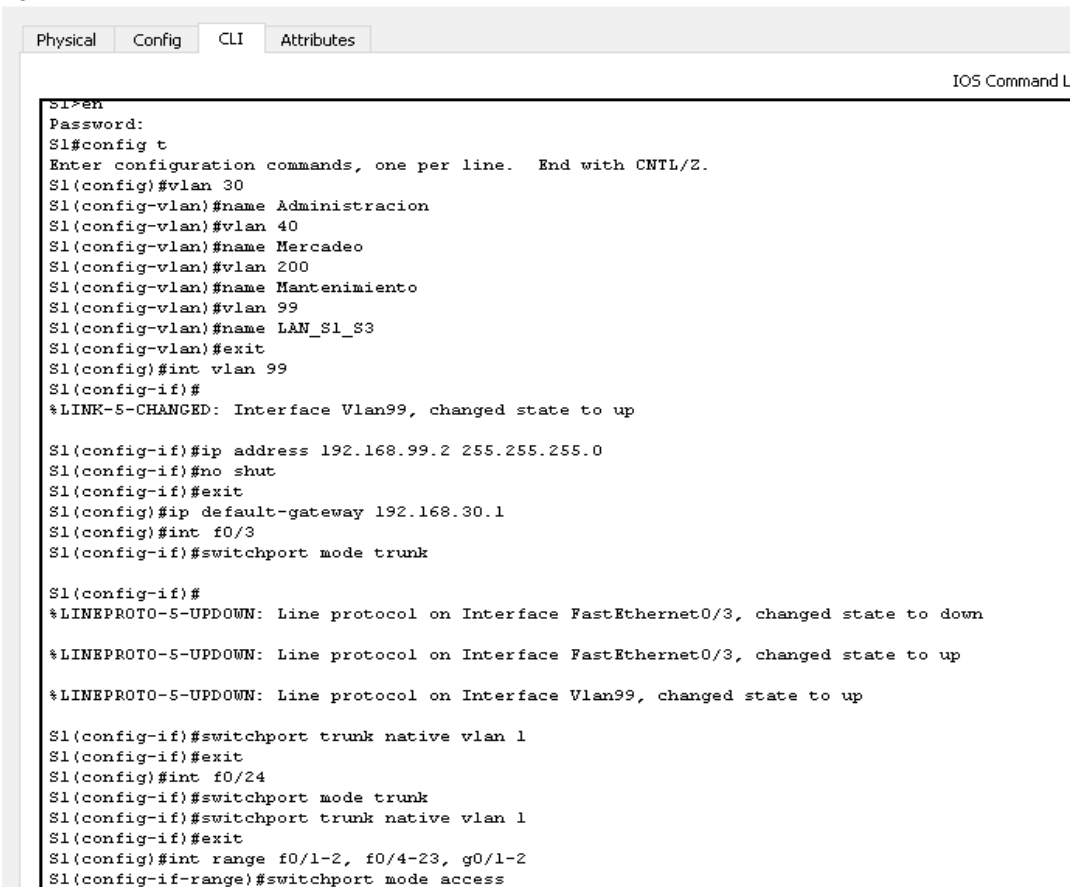
- Pasos a seguir:

Configuración para S1

```
S1#config t
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)#vlan 99
S1(config-vlan)#name LAN_S1_S3
S1(config-vlan)#exit
S1(config)#int vlan 99
S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.30.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
```



```
S1(config)#int f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int range f0/1-2, f0/4-23, g0/1-2
S1(config-if-range)#switchport mode access
S1(config)#int f0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#int range f0/2, f0/4-23, g0/1-2
S1(config-if)#shutdown
S1(config-if)#exit
```

Imagen 35-2 Para R1

```
S1
Physical Config CLI Attributes
IOS Command L
S1>en
Password:
S1#config 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)#vlan 99
S1(config-vlan)#name LAN_S1_S3
S1(config-vlan)#exit
S1(config)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.30.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

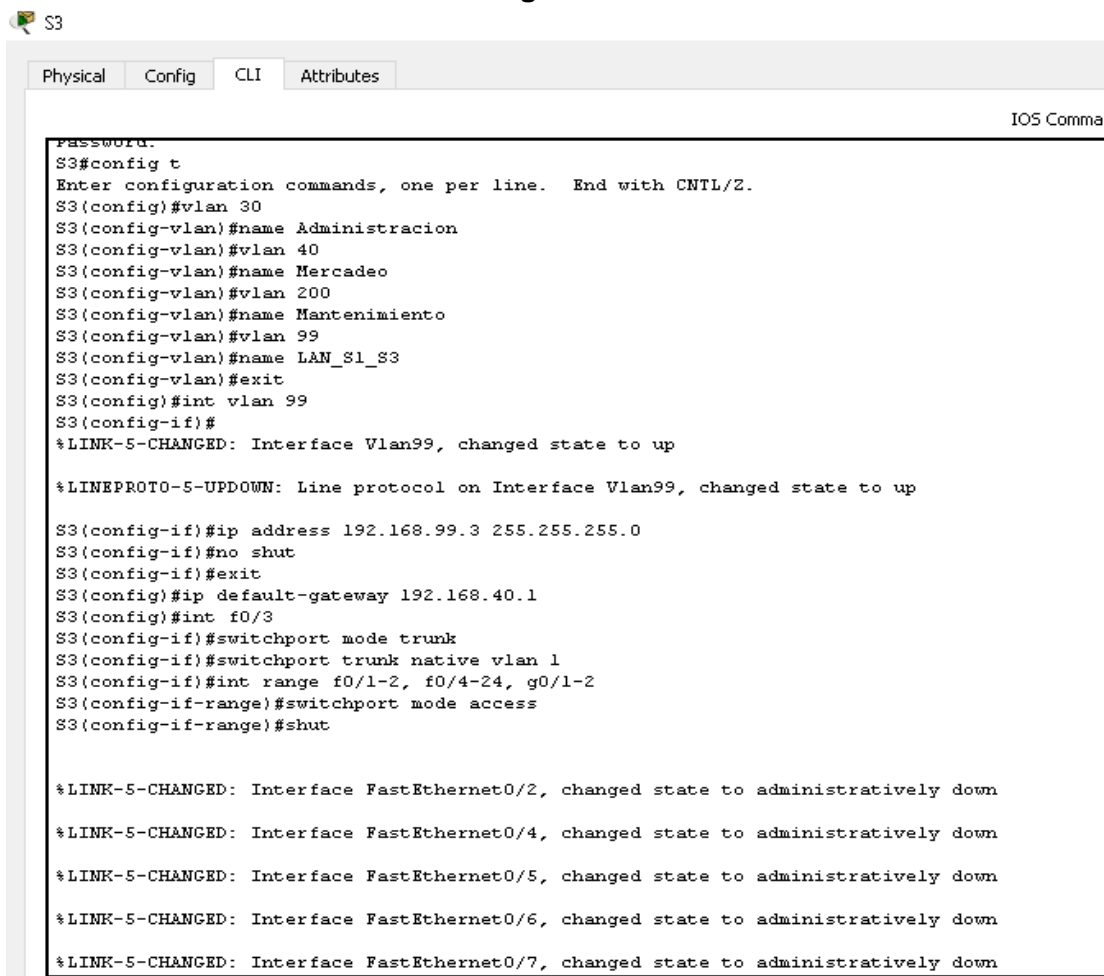
S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#exit
S1(config)#int range f0/1-2, f0/4-23, g0/1-2
S1(config-if-range)#switchport mode access
```

Configuración para S3.

```
S3#config t
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)#vlan 99
S3(config-vlan)#name LAN_S1_S3
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shut
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.40.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#shut
S3(config-if-range)#exit
S3(config)#int f0/1
S3(config-if)#no shut
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#exit
```

Imagen 36-2 En S3



```

S3
Physical Config CLI Attributes
IOS Comma
Password.
S3#config 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)#vlan 99
S3(config-vlan)#name LAN_S1_S3
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shut
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.40.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#shut

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

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

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

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

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

```

Imagen 37-2 En S3 continuación

```

%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%LINK-5-CHANGED: Interface FastEthernet0/17, changed state to administratively down
%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 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)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

S3(config-if-range)#exit
S3(config)#int f0/1
S3(config-if)#no shut

S3(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#exit
S3(config)#

```

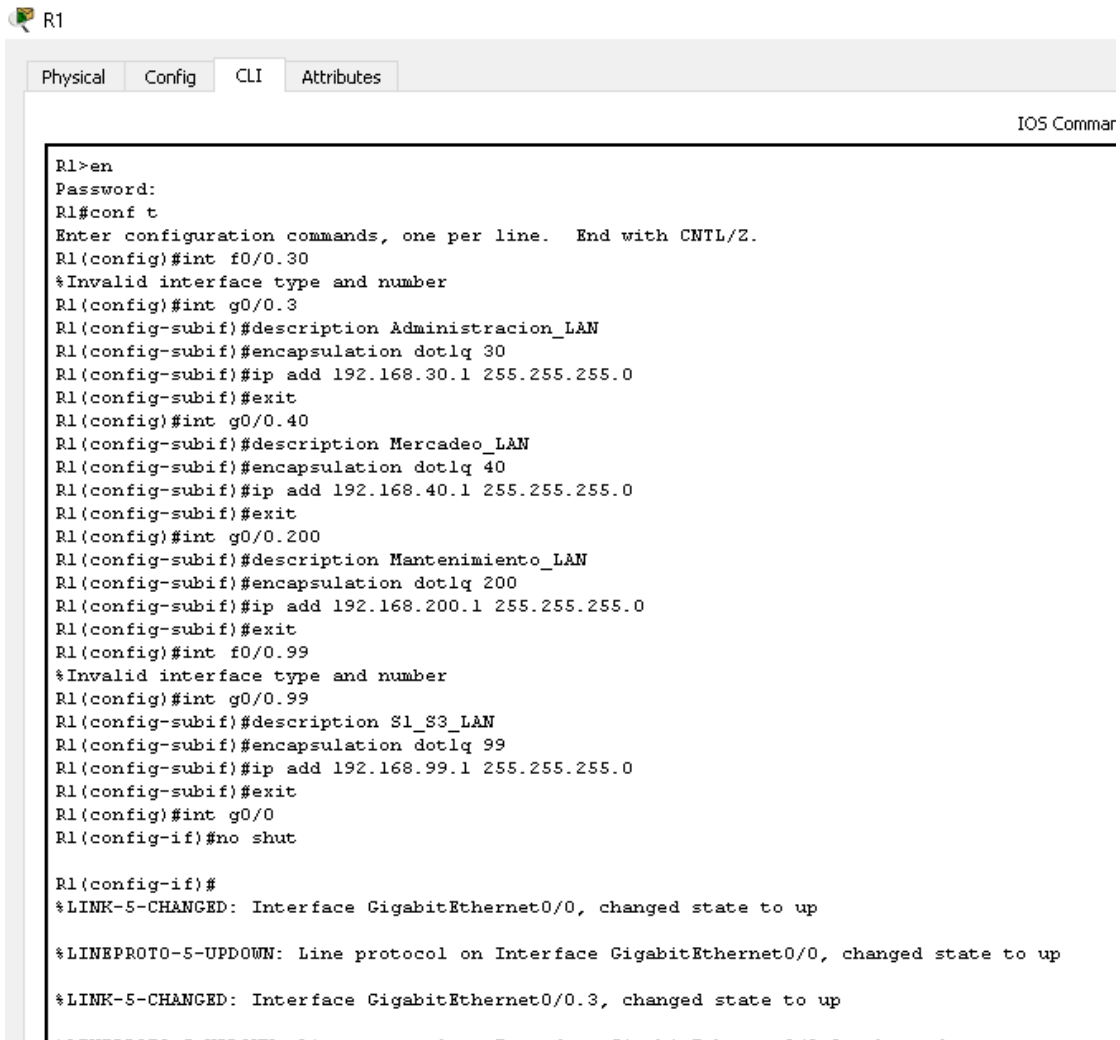
Configuración para R1.

```

R1#config t
R1(config)#int f0/0.30
R1(config-subif)#description Administracion_LAN
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip add 192.168.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.40

```

```
R1(config-subif)#description Mercadeo_LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip add 192.168.40.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.200
R1(config-subif)#description Mantenimiento_LAN
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip add 192.168.200.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.99
R1(config-subif)#description S1_S3_LAN
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0
R1(config-if)#no shut
R1(config-subif)#exit
```

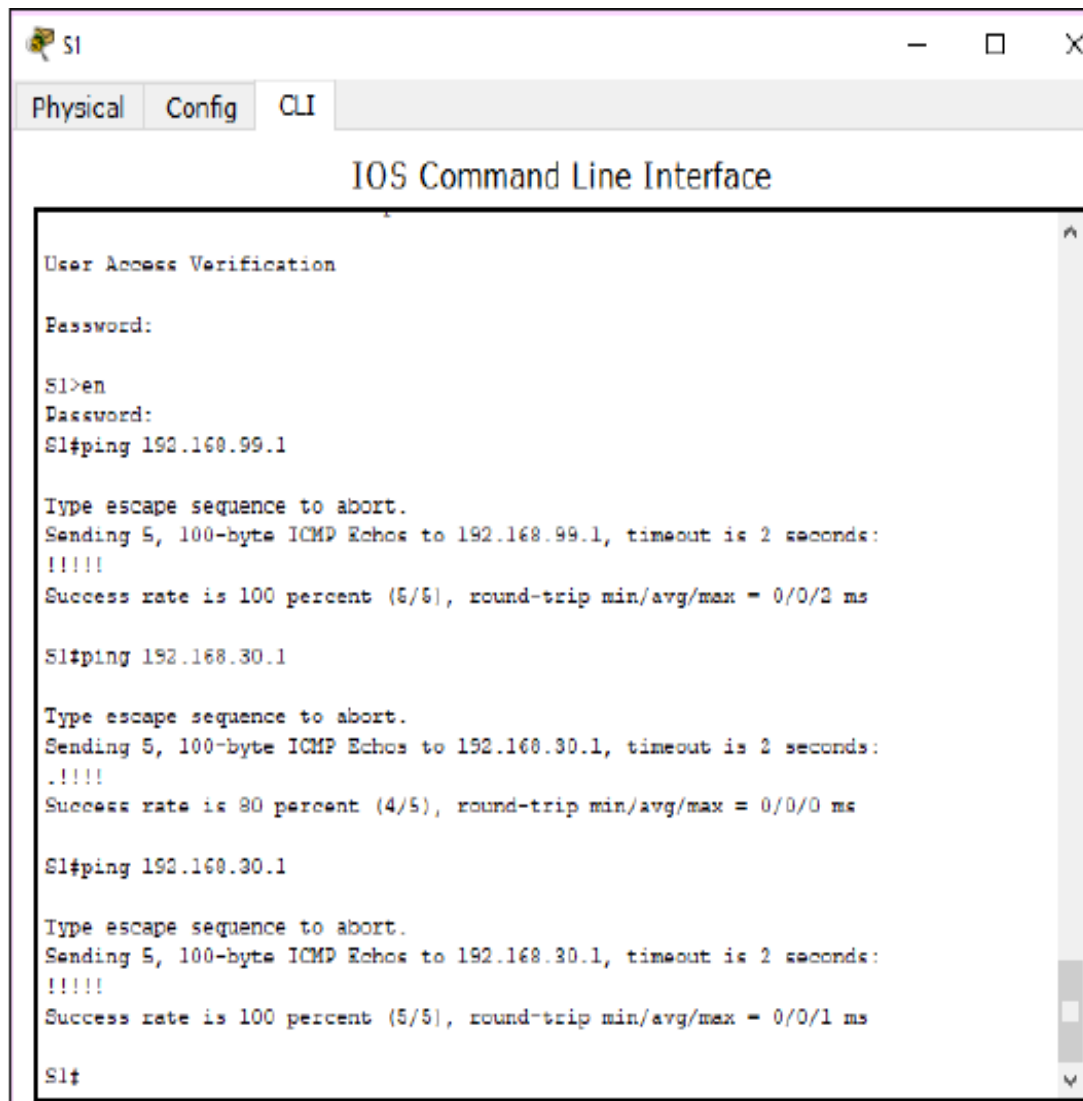
Imagen 35-2 Configuración en R1

```
R1
Physical Config CLI Attributes
IOS Commar
R1>en
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int f0/0.30
%Invalid interface type and number
R1(config)#int g0/0.3
R1(config-subif)#description Administracion_LAN
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip add 192.168.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0.40
R1(config-subif)#description Mercadeo_LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip add 192.168.40.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0.200
R1(config-subif)#description Mantenimiento_LAN
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip add 192.168.200.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.99
%Invalid interface type and number
R1(config)#int g0/0.99
R1(config-subif)#description S1_S3_LAN
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip add 192.168.99.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int g0/0
R1(config-if)#no shut
R1(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
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to up
```

Verificar la conectividad de la red.

Después de la configuración de los dispositivos S1, S2 y R1 se observa en la simulación que todos los puntos de conexión se encuentran en color verde lo que indica su correcta comunicación, pero se debe comprobar usando el comando ping.

Imagen 36-2 Conectividad S1



```
S1
Physical Config CLI
IOS Command Line Interface

User Access Verification

Password:

S1>en
Password:
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/2 ms

S1#ping 192.168.30.1

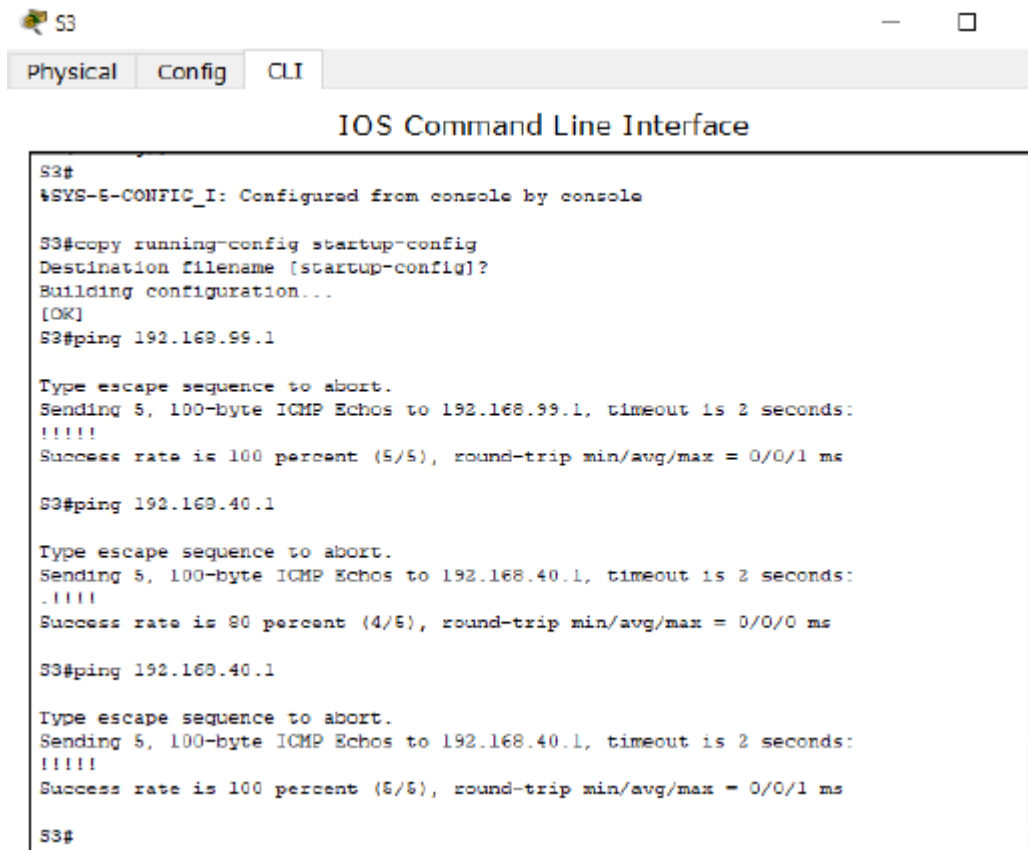
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.160.30.1

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 = 0/0/1 ms

S1#
```

La conectividad para S1 es satisfactoria como se ve en la imagen.

Imagen 37-2 Conectividad S3

```
S3#
%SYS-E-CONFIG_I: Configured from console by console

S3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

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 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

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 = 0/0/1 ms

S3#
```

S3 también está conectando por lo que se puede continuar

Part 6: Implement DHCP and NAT for IPv4

Part 7: Configurar R1 como servidor DHCP para las VLANs 30 y 40.

Part 8: Reservar direcciones

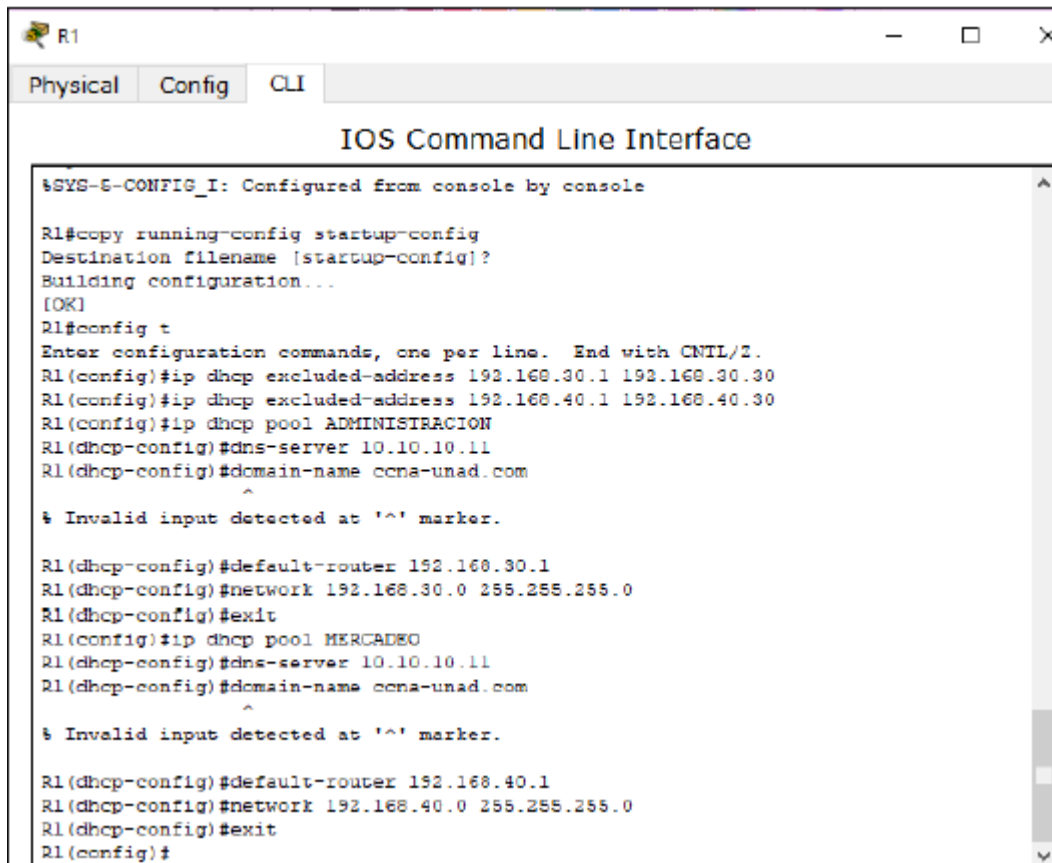
Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas

- Resolviendo para los puntos parte 4, parte 5 y parte 6.

Configurando para el router 1

```
R1#config t
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool MERCADEO
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
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
```

Imagen 38-2 Reservando direcciones en R1



```

R1
Physical Config CLI
IOS Command Line Interface
%SYS-5-CONFIG_I: Configured from console by console

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#config 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 ADMINISTRACION
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
^
% Invalid input detected at '^' marker.

R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#exit
R1(config)#ip dhcp pool MERCADERO
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#domain-name ccna-unad.com
^
% Invalid input detected at '^' marker.

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

```

Part 9: Configurar NAT

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

Configurar NAT estática y dinámica en R2

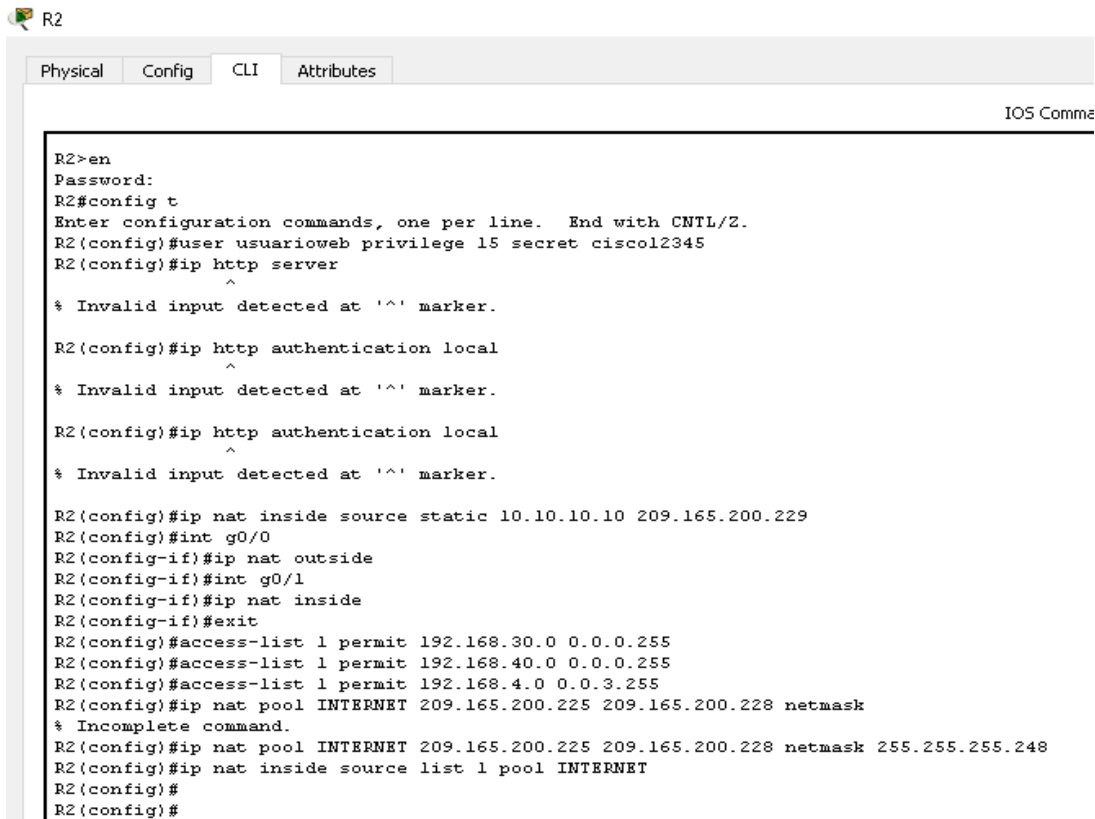
```

R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user usuarioweb 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.
R2(config)#ip http authentication local
^
% Invalid input detected at '^' marker.

```

```
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 outside
R2(config-if)#int g0/1
R2(config-if)#ip nat inside
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
% Incomplete command.
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
```

Imagen 39-2 Configuración NAT



```
R2
Physical Config CLI Attributes
IOS Comm

R2>en
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user usuarioweb 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.
R2(config)#ip http authentication local
^
% Invalid input detected at '^' marker.
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 outside
R2(config-if)#int g0/1
R2(config-if)#ip nat inside
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
% Incomplete command.
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)#
R2(config)#
```

Part 10: Verificar DHCP y NAT estática.

Para esto pasamos las computadoras PC-A y PC-C a modo DHCP

Imagen 40-2 DHCP en PC-A

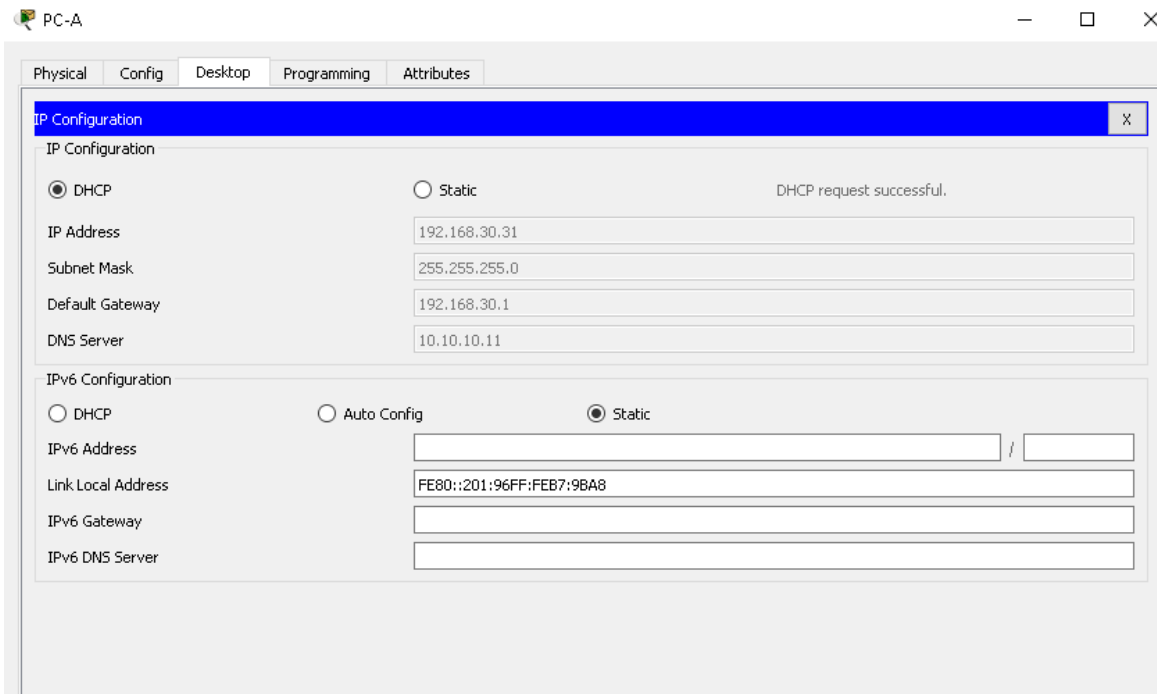
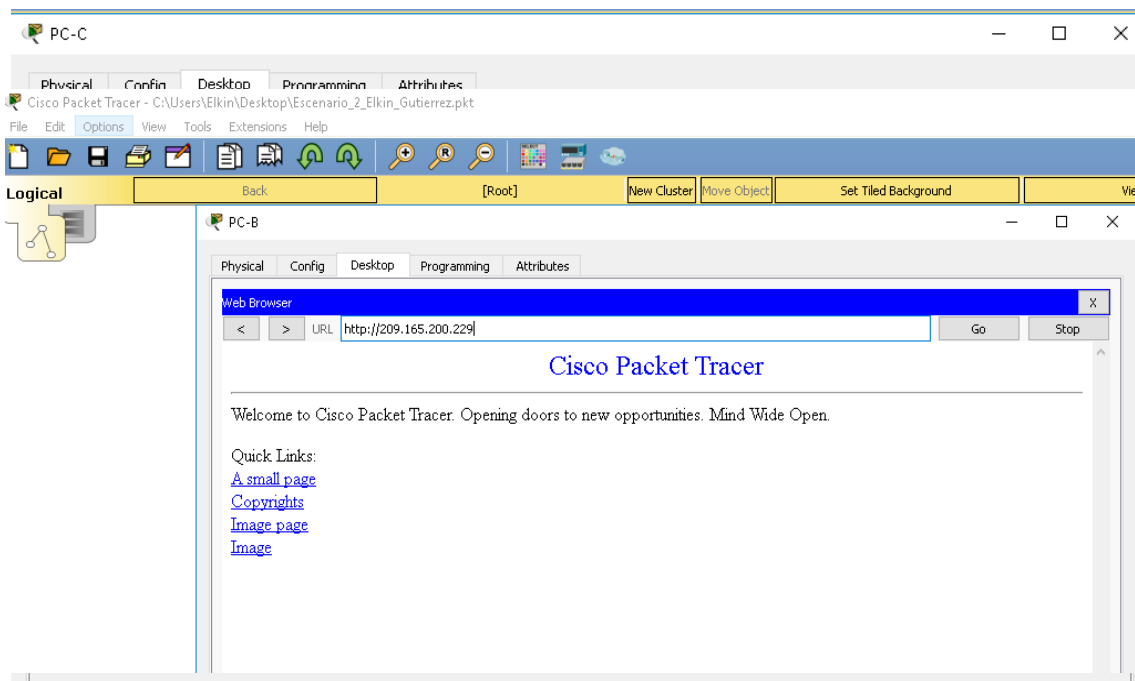


Imagen 41-2 DHCP en PC-C

Part 11: Configurar listas de acceso

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.

Part 12: Configurar al menos dos listas de acceso de tipo extendido

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.

Part 13: Verificar procesos de comunicación

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

Resolviendo para los puntos anteriores

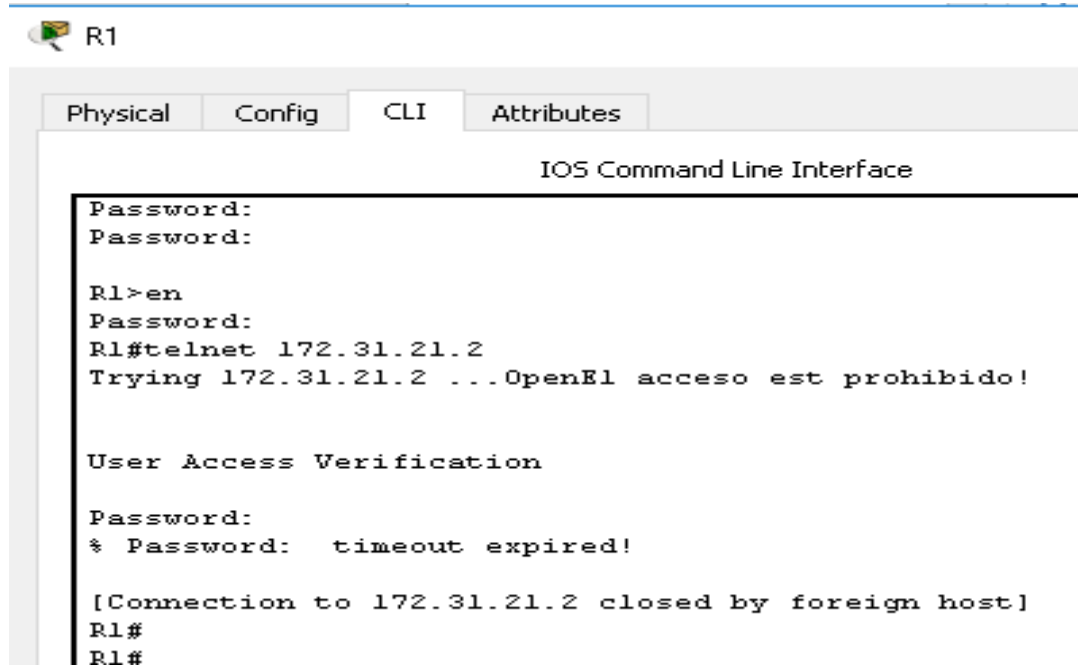
Restringir el acceso a las líneas VTY en R2:

Configuramos en R2

```
R2>en
Password:
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip access-list standard ADMIN-UNAD
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-UNAD in
R2(config-line)#exit
R2(config)#
```

Hacemos la verificación o comprobación desde R1:

```
R1#telnet 172.31.21.2
Trying 172.31.21.2 ...OpenEl acceso está prohibido!
User Access Verification
Password:
R2>en
Passw
Password:
R2#
```

Imagen 42-2 Comprobación desde R1

The screenshot shows the CLI interface of a Cisco router named R1. The interface has 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 and provides a password. Then, they enter 'telnet 172.31.21.2'. The output shows the router attempting to connect to 172.31.21.2, receiving a message 'OpenEl acceso est prohibido!', and then a 'User Access Verification' prompt. The user provides another password, but it times out with the message '* Password: timeout expired!'. Finally, the connection is closed with the message '[Connection to 172.31.21.2 closed by foreign host]'. The prompt returns to 'R1#'.

```
R1
Physical Config CLI Attributes
IOS Command Line Interface
Password:
Password:
R1>en
Password:
R1#telnet 172.31.21.2
Trying 172.31.21.2 ...OpenEl acceso est prohibido!

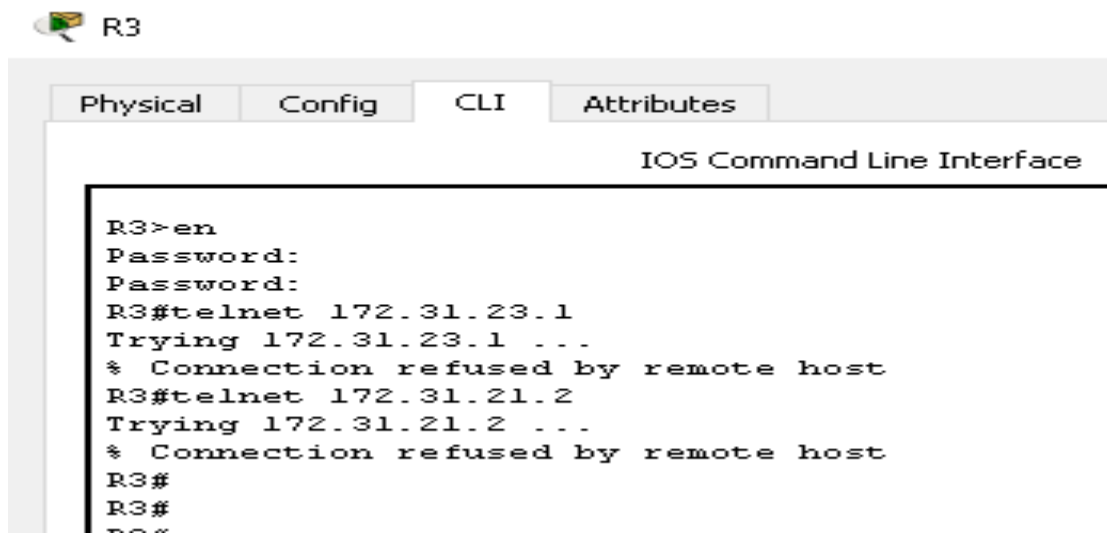
User Access Verification

Password:
* Password: timeout expired!

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

Comprobación desde R3

```
R3#telnet 172.31.23.1
Trying 172.31.23.1 ...
% Connection refused by remote host
R3#telnet 172.31.21.2
Trying 172.31.21.2 ...
% Connection refused by remote host
R3#
```

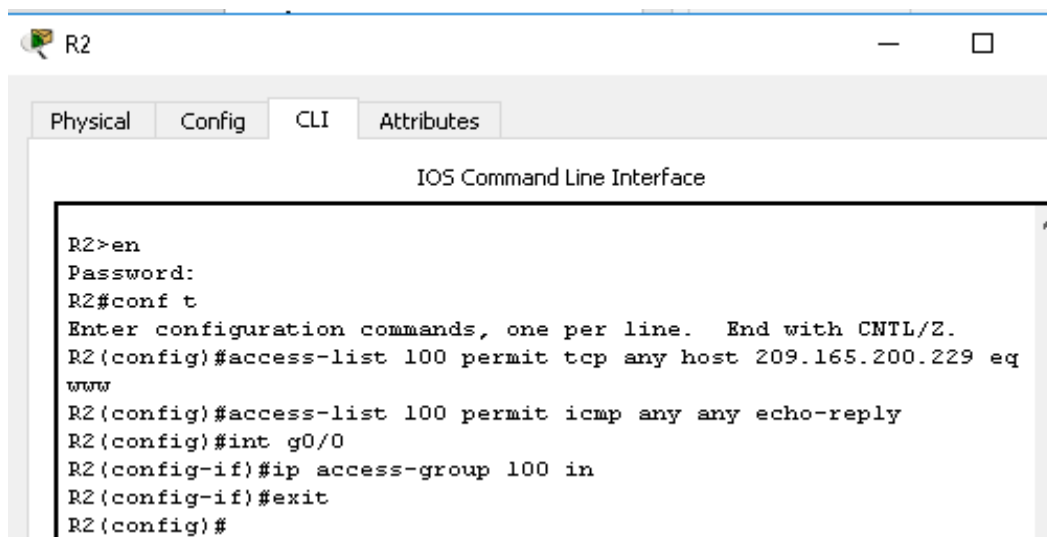
Imagen 43-2 Comprobación desde R3

```
R3
Physical Config CLI Attributes
IOS Command Line Interface
R3>en
Password:
Password:
R3#telnet 172.31.23.1
Trying 172.31.23.1 ...
% Connection refused by remote host
R3#telnet 172.31.21.2
Trying 172.31.21.2 ...
% Connection refused by remote host
R3#
R3#
R3#
```

Las restricciones están funcionando como se puede observar en las imágenes.

Proteger la red del tráfico de Internet.

Protegemos un segmento de la red para que no puedan acceder a internet.

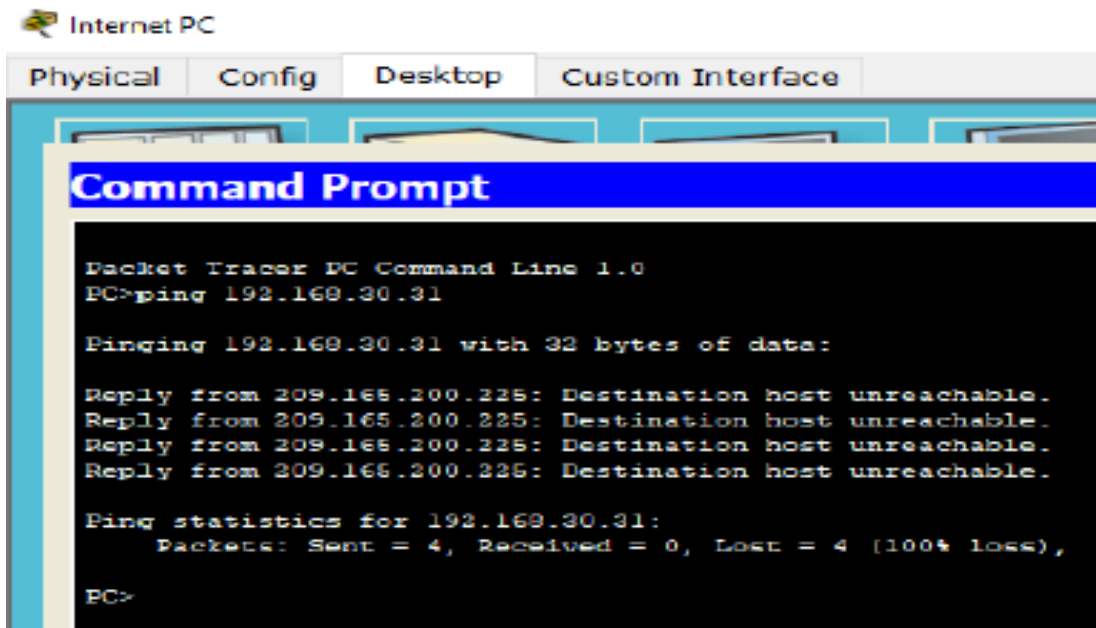
Imagen 44-2 Protección de la red

```
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)#access-list 100 permit tcp any host 209.165.200.229 eq
www
R2(config)#access-list 100 permit icmp any any echo-reply
R2(config)#int g0/0
R2(config-if)#ip access-group 100 in
R2(config-if)#exit
R2(config)#
```


Hacemos ping dentro los equipos para verificar si hay conexión entre los tramos.

- Ping de Internet PC a PC-A. PC>ping 192.168.30.31
- Ping de Internet PC a PC-C. PC>ping 192.168.40.31

Imagen 45-2 Ping de comprobación



En este caso no hay comunicación como se esperaba.

Imagen 46-2 Ping desde R1

```

R1
Physical Config CLI
IOS Command Line Interface

Press RETURN to get started.

El acceso no autorizado est prohibido!
User Access Verification
Password:
R1>en
Password:
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 100 percent (5/5), round-trip min/avg/max = 1/5/13 ms
...

```

Verificamos en R1 usando el comando Traceoute

R1#traceroute 192.168.30.31

Imagen 47-2 Traceroute R1

```

R1
Physical Config CLI
IOS Command Line Interface

R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#telnet 172.31.21.2
Trying 172.31.21.2 ...OpenUnauthorized Access is Prohibited!

User Access Verification
Password:
R2>en
Password:
R2#exit

[Connection to 172.31.21.2 closed by foreign host]
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 100 percent (5/5), round-trip min/avg/max = 1/4/17 ms

R1#traceroute 192.168.30.31
Type escape sequence to abort.
Tracing the route to 192.168.30.31

 0  192.168.30.31  1 msec  0 msec  0 msec
R1#

```

Traceroute entre R2 y PC-A. R2#traceroute 192.168.30.31

Imagen 48-2 Traceroute R1-2

```
R1
Physical Config CLI
IOS Command Line Interface
R1#telnet 172.31.21.2
Trying 172.31.21.2 ...OpenUnauthorized Access is Prohibited!

User Access Verification
Password:
R2>en
Password:
R2#exit

[Connection to 172.31.21.2 closed by foreign host]
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 100 percent (5/5), round-trip min/avg/max = 1/4/17 ms

R1#traceroute 192.168.30.31
Type escape sequence to abort.
Tracing the route to 192.168.30.31

 0  192.168.30.31  1 msec  0 msec  0 msec
R1#traceroute 192.168.40.31
Type escape sequence to abort.
Tracing the route to 192.168.40.31

 0  192.168.40.31  1 msec  3 msec  3 msec
R1#
```

Conclusiones

Las simulaciones realizadas bajo Packet Tracer, en el desarrollo de este ejercicio dan cuenta de los fundamentos vistos durante el curso se pudo evidenciar la configuración y enrutamiento de cada uno de los dispositivos y su puesta en marcha y verificación, con algunos problemas que fueron superados, los dos escenarios garantizaron la apropiación de los temas propuestos en este diplomado de profundización.

Que agradecer y decir que repasaré con mucho placer cada uno de los ejercicios para poder tener certeza de los conocimientos adquiridos, me pareció un excelente diplomado.

Bibliografía

- Temática: Introducción a redes conmutadas
CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>
- Temática: Configuración y conceptos básicos de Switching
CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>
- Temática: VLANs
CISCO. (2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>
- Temática: Conceptos de Routing
CISCO. (2014). Conceptos de Routing. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module4/index.html#4.0.1.1>
- Temática: Enrutamiento entre VLANs
CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>
- Temática: Enrutamiento Estático
CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>
- Temática: Enrutamiento Dinámico
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>
- Temática: OSPF de una sola área
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>
- Temática: Listas de control de acceso
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>
- Temática: DHCP
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>