EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

JOHN JAIRO PEQUI AGUDELO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA-UNAD
PROGRAMA DE INGENIERÍA DE SISTEMAS
DIPLOMADO DE PROFUNDIZACIÓN CISCO (DISEÑO E IMPLEMENTACIÓN DE SOLUCIONES INTEGRADAS LAN/WAN)
POPAYÁN-CAUCA
2024

TABLA DE COTENIDO

LISTA DE TABLAS....3
LISTA DE FIGURAS....4
INTRODUCCIÓN....5
1. ESCENARIO 1....6
1.1 DESCRIPCIÓN....6
1.1.1 Requerimiento....6
1.1.2 Desarrollo....9
1.2 DESARROLLO....9
1.2.1 Configuración inicial (nombre, direcciones ip, seguridad, valn)....9
1.2.2 Configuración servidor DCHP en el router 2....16
1.2.3 Enrutamiento RIP....17
1.2.4 Ruta estática predeterminada desde R2 al ISP....18
1.2.5 NAT Con sobrecarga (PAT) en router 1....18
2 ESCENARIO 2....23
2.1 DESCRIPCIÓN....23
2.1.1 Requerimiento....23
2.2 DESARROLLO....25
2.2.1 Configuración inicial (nombre, direcciones IP, seguridad)....25
2.2.2 Switch (Vlan, modo trunk)....28
2.2.3 Configuración DHCP en R1 (Bogotá)....32
2.2.4 Configuración loopback....33
2.2.5 OSPF, interfaces pasivas y NAT....33
2.2.6 NAT....36
2.2.7 Lista de control de acceso estándar y extendida....37
2.2.8 Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute....40

CONCLUSIONES....42
REFERENCIAS....43

LISTA DE TABLAS

Tabla 1 Direccionamiento IP 7
Tabla 2 Direccionamiento IP computadoras.....7
Tabla 3 Direccionamiento IP computadoras.....8
Tabla 4 Hardware requerido.....9
Tabla 5 Configuración dispositivos.....24
Tabla 6 Configuración VLAN y DHCP 25

LISTA DE FIGURAS

Figura 1 Topología a desarrollar 6
Figura 2 Asignaciones de puertos de VLAN.....10
Figura 3 Puertos deshabilitados.....11
Figura 4 Asignaciones direcciones IP 13
Figura 5 Configuración VLAN.....14
Figura 6 Funcionamiento dual-stack 15
Figura 7 Configuración dual-stack en fa0/0.....15
Figura 8 Configuración DHCP en R2 16
Figura 9 Funcionamiento DHCP en las VLANS 16
Figura 10 Tablas de enrutamiento RIP.....18
Figura 11 Configuración ruta estática al ISP 18
Figura 12 Configuración NAT.....19
Figura 13. Salida con direcciones IP asignadas por la NAT.....19
Figura 14 Configuración IPV6 del server0.....20
Figura 15 Prueba de ping desde dentro y fuera de R3.....20
Figura 16 Ping de dispositivos en R3 pero diferente VLAN.....21
Figura 17 Ping de dispositivo de R2 al dispositivo de R3.....21
Figura 18 Ping de un dispositivo de R3 al ISP 22
Figura 19. Ping entre dispositivo de R2 al ISP 22
Figura 20 Topología a desarrollar 23
Figura 21 Deshabilitar lookup.....28
Figura 22 Configuración seguridad Switch y seguridad 29
Figura 23 Asignaciones de puertos de VLAN.....29
Figura 24 Asignación de direcciones IP a los Switchs 30
Figura 25 Configuración interfaces que no se estén utilizando SW3 31
Figura 26 Configuración interfaces que no se estén utilizando SW1 31
Figura 27 Asignación direcciones DCHP 32
Figura 28 Tablas de enrutamiento OSPF.....34
Figura 29 Visualización resumida OSPF.....35
Figura 30 Visualización OSPF R1 y R2.....35
Figura 31 Visualización OSPF R3.....35
Figura 32 Funcionamiento NAT desde la red 192.168.40.0 36
Figura 33 Funcionamiento NAT desde la red 192.168.30.0 37
Figura 34 Prueba de ping a la IP 10.10.10.10.....38
Figura 35 Prueba ping a la IP 192.168.4.1.....38
Figura 36 Bloqueo del puerto 80 mediante lista de acceso.....39
Figura 37 Bloqueo puerto 443 mediante lista de acceso.....40
Figura 38 Verificando conectividad mediante ping y tracert 40
Figura 39 Ping y tracert, en la segunda figura no hace ping ya que una lista de acceso configurada lo bloquea 41

INTRODUCCIÓN

El presente trabajo se realiza con el fin de demostrar y aplicar los conocimientos adquiridos en los módulos CP CCNA1 II-2018 y CP CCNA2 II-2018 de la plataforma NETACAD, en el cual se abordaron diferentes temas relacionados con el funcionamiento y configuración de las redes CISCO.

Para la realización de los ejercicios se empleó la aplicación Packet Tracer, con la cual se les dio solución a los diferentes escenarios propuestos para la presente actividad.

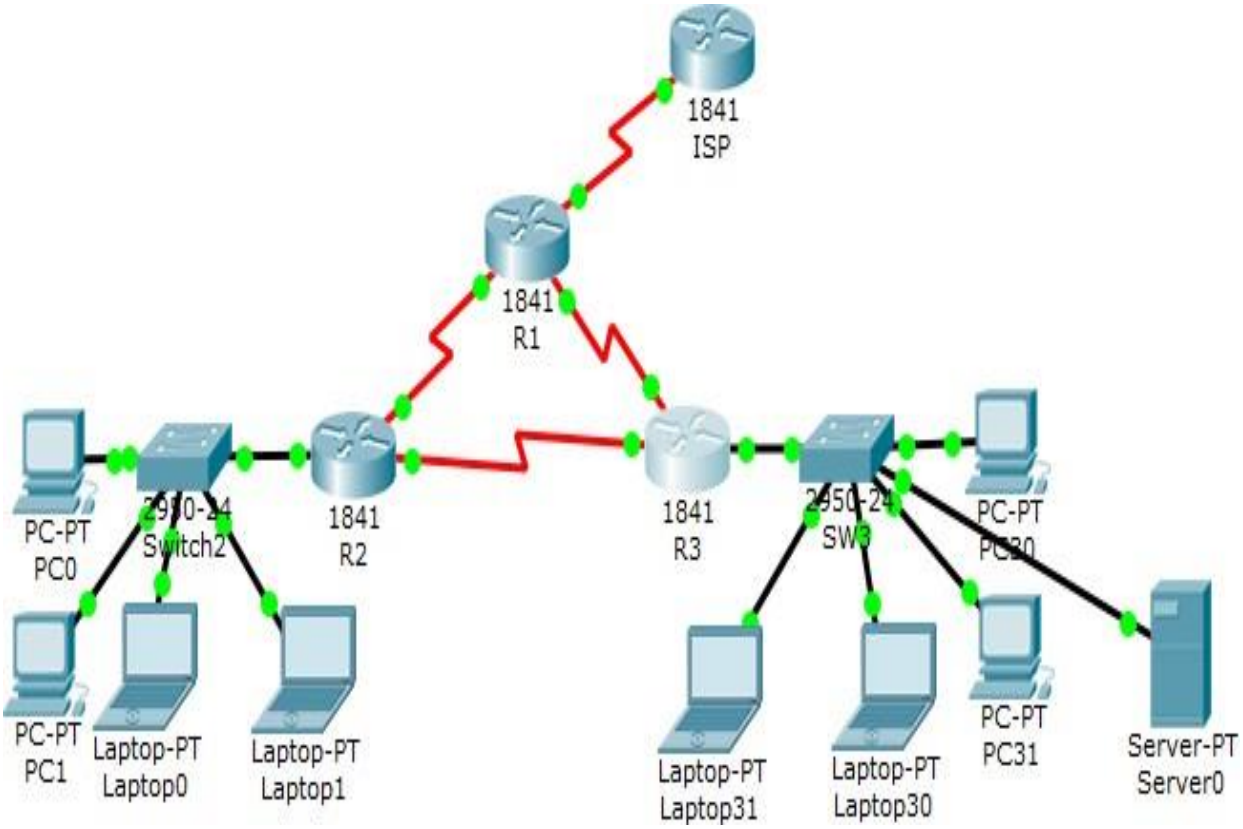
Es de anotar que para resolver los dos ejercicios se aplicaran los conocimientos adquiridos en un problema práctico de la vida diría, el cual se le puede presentar a un ingeniero al momento de implementar soluciones de conectividad en la que se necesita realizar diferentes configuraciones, diferentes VLAN, pruebas de conectividad, implementación de troncales, etc.

1. ESCENARIO 1

1.1 DESCRIPCIÓN

1.1.1 Requerimiento

Figura 1. Topología a desarrollar



Fuente. CISCO

Tabla 1. Direccionamiento IP

Administrador	Interfaces	Dirección IP	Máscara 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		192.168.30.1	255.255.255.0	N/D
	Fa0/0	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

Fuente. CISCO

Tabla 2. Direccionamiento IP computadoras

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. CISCO

Tabla 3. Direccionamiento IP computadoras

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

Fuente. CISCO

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.

- Requerimiento 1: SW1 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.
- Requerimiento 2: Los puertos de red que no se utilizan se deben deshabilitar.
- Requerimiento 3: La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.
- Requerimiento 4: Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP.
- Requerimiento 5: 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.
- Requerimiento 6: R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.
- Requerimiento 7: R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.
- Requerimiento 8: R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.
- Requerimiento 9: El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).

- Requerimiento 10: 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.
- Requerimiento 11: La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).
- Requerimiento 12: R1, R2 y R3 intercambian información de routing mediante RIP versión 2.
- Requerimiento 13: R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.
- Requerimiento 14: 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.

1.1.2 Desarrollo

Tabla 4. Hardware requerido

Cantidad	Hardware
4	Router
2	Switch
4	PC
4	Laptop
1	Servidor

Fuente. Autoría propia

Se procedió a crear la topología de acuerdo al diseño sugerido, a los router se les anexo tarjetas seriales, se colocó nombre a desktop y laptop y se realiza la conexión de las interfaces de acuerdo a la conectividad requerida

1.2 DESARROLLO

1.2.1 Configuración inicial (nombre, direcciones ip, seguridad, valn)

Swich 2:

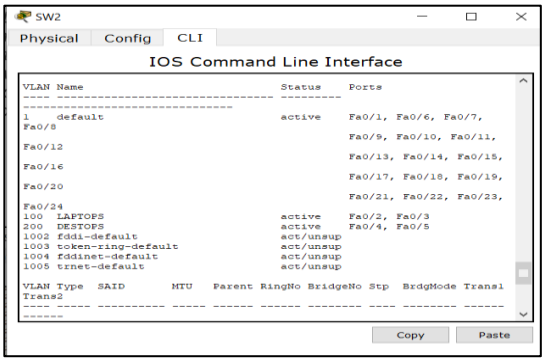
```
enable
config terminal
hostname SW2
```

service password-encryption
line console 0
password cisco
login
exit
enable secre cisco
no ip domain lookup
line vty 0 15
exit
banner motd %solo personal autorizado%

vlan 100
name LAPTOPS
exit
interface range f0/2-3
switchport mode access
switchport access vlan 100
exit
vlan 200
name DESTOPS
exit
interface range f0/4-5
switchport mode access
switchport access vlan 200
exit
interface range f0/6-24
shutdown
Interface fa0/1
switchport mode trunk
exit
do wr

Lo cual da cumplimiento al requerimiento 1: SW1 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.

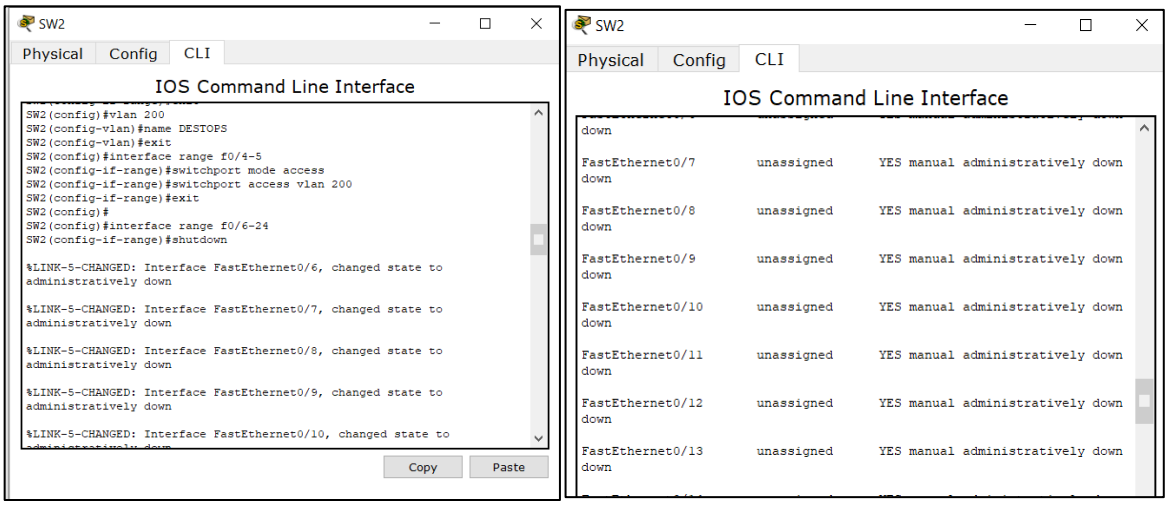
Figura 2. Asignaciones de puertos de VLAN



Fuente. Autoría propia

Lo cual da cumplimiento al requerimiento 2: Los puertos de red que no se utilizan se deben deshabilitar.

Figura 3. Puertos deshabilitados



Fuente. Autoría propia

Swich 3:

enable
config terminal
hostname SW3
interface range f0/7-24
shutdown

service password-encryption
line console 0
password cisco
login
exit
enable secre cisco
no ip domain lookup
line vty 0 15
exit
banner motd %solo personal autorizado%

Router ISP:

enable
config terminal
hostname ISP

service password-encryption
line console 0

password cisco
login
exit
enable secre cisco
no ip domain lookup
line vty 0 15
exit
banner motd %solo personal autorizado%

interface S0/0/0
ip address 200.123.211.1 255.255.255.0
no shutdown
do wr

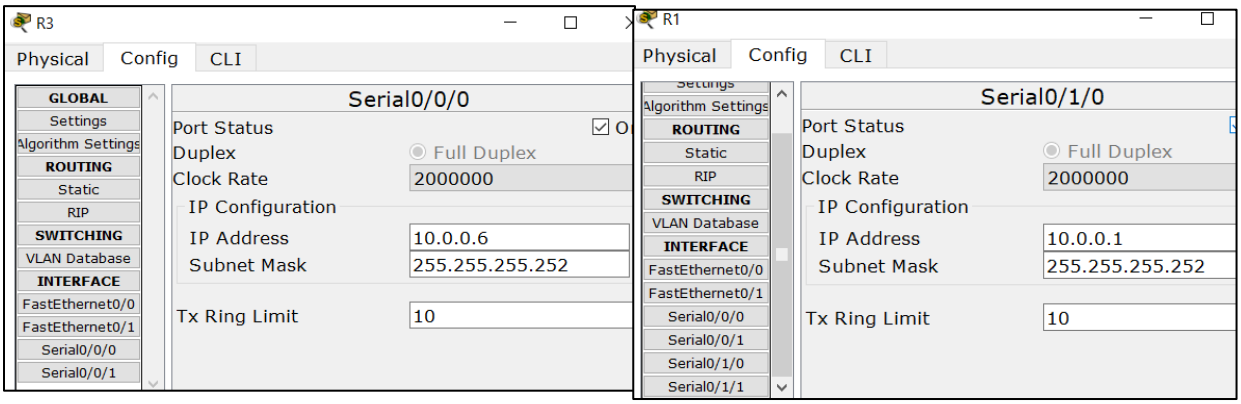
Router R1:
enable
config terminal
hostname R1

service password-encryption
line console 0
password cisco
login
exit
enable secre cisco
no ip domain lookup
line vty 0 15
exit
banner motd %solo personal autorizado%

interface S0/0/0
ip address 200.123.211.2 255.255.255.0
no shutdown
exit
interface S0/1/0
ip address 10.0.0.1 255.255.255.252
no shutdown
exit
interface S0/1/1
ip address 10.0.0.5 255.255.255.252
no shutdown
exit
do wr

Lo cual da cumplimiento al requerimiento 3: La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.

Figura 4. Asignaciones direcciones IP



Fuente. Autoría propia

Router R2:

enable
config terminal
hostname R2

service password-encryption
line console 0
password cisco
login
exit
enable secre cisco
no ip domain lookup
line vty 0 15
exit
banner motd %solo personal autorizado%

interface Serial0/0/0
ip address 10.0.0.2 255.255.255.252
no shutdown
exit

interface Serial0/0/1
ip address 10.0.0.9 255.255.255.252
no shutdown
exit

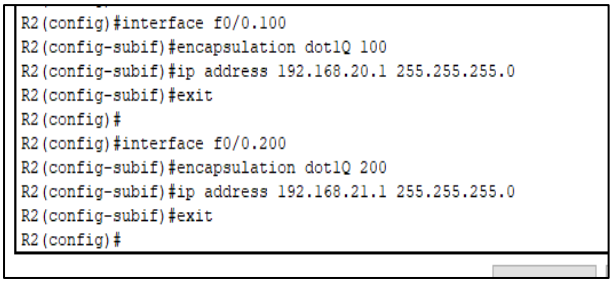
interface f0/0
no shutdown
exit

interface f0/0.100
encapsulation dot1Q 100
ip address 192.168.20.1 255.255.255.0
exit

interface f0/0.200
encapsulation dot1Q 200
ip address 192.168.21.1 255.255.255.0
exit
do wr

Lo cual da cumplimiento al requerimiento 8: R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.

Figura 5. Configuración VLAN



Fuente. Autoría propia

Router 3:
enable
config terminal
hostname R3

service password-encryption
line console 0
password cisco
login
exit
enable secre cisco
no ip domain lookup
line vty 0 15
exit
banner motd %solo personal autorizado%

ipv6 unicast-routing

interface Serial0/0/0
ip address 10.0.0.6 255.255.255.252

no shutdown

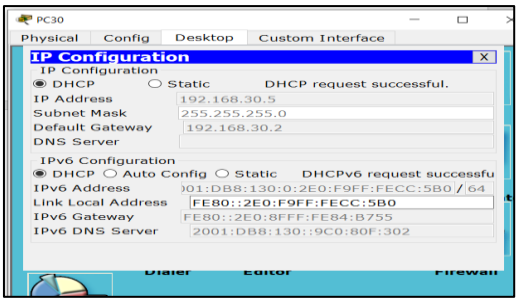
interface Serial0/0/1
ip address 10.0.0.10 255.255.255.252
no shutdown

interface f0/0
ip address 192.168.30.1 255.255.255.0
ipv6 address 2001:db8:130::9C0:80F:301/64
no shutdown
Ipv6 nd other-config-flag

ip dhcp pool SERVER0
default-router 192.168.30.1
network 192.168.30.0 255.255.255.0

Lo cual da cumplimiento al requerimiento 10: 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.

Figura 6. Funcionamiento dual-stack



Fuente. Autoría propia

Lo cual da cumplimiento al requerimiento 11: La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).

Figura 7. Configuración dual-stack en fa0/0

```
R3(config-if)#
R3(config-if)#interface f0/0
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)#Ipv6 nd other-config-flag
R3(config-if)#
R3(config-if)#ip dhcp pool SERVER0
R3(dhcp-config)#default-router 192.168.30.2
R3(dhcp-config)#network 192.168.30.0 255.255.255.0
R3(dhcp-config)#
```

Fuente. Autoría propia

1.2.2 Configuración servidor DCHP en el router 2

ip dhcp pool SERVER1
default-router 192.168.20.1
network 192.168.20.0 255.255.255.0
ip dhcp pool SERVER2
default-router 192.168.21.1
network 192.168.21.0 255.255.255.0
exit
do wr

Lo cual da cumplimiento al requerimiento 7: R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0

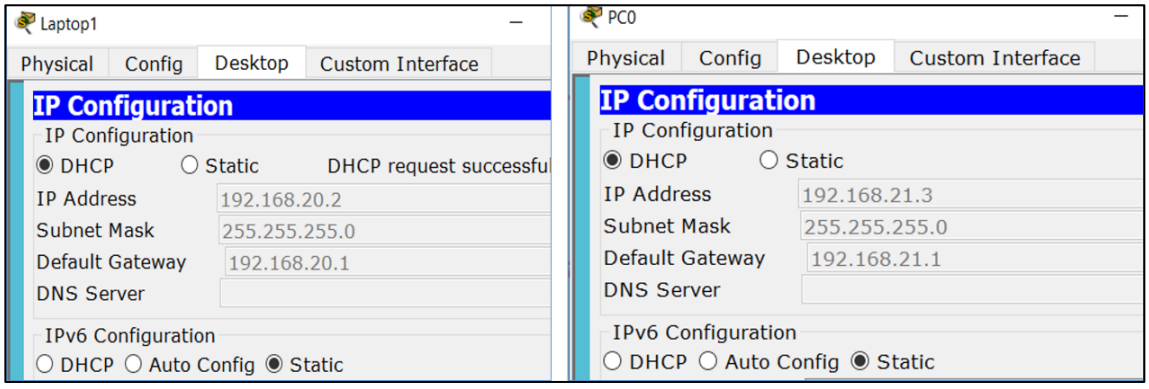
Figura 8. Configuración DHCP en R2

```
R2#config t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#ip dhcp pool SERVER1
R2(dhcp-config)#default-router 192.168.20.1
R2(dhcp-config)#network 192.168.20.0 255.255.255.0
R2(dhcp-config)#ip dhcp pool SERVER2
R2(dhcp-config)#default-router 192.168.21.1
R2(dhcp-config)#network 192.168.21.0 255.255.255.0
R2(dhcp-config)#exit
R2(config)#do wr
Building configuration...
[OK]
```

Fuente. Autoría propia

Lo cual da cumplimiento al requerimiento 4: Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP

Figura 9. Funcionamiento DHCP en las VLANS



Fuente. Autoría propia

1.2.3 Enrutamiento RIP

Router 1:

Router rip
version 2
ip route 0.0.0.0 0.0.0.0 s0/0/0
router rip
network 10.0.0.4
network 10.0.0.0
default-information originate

Router 2:

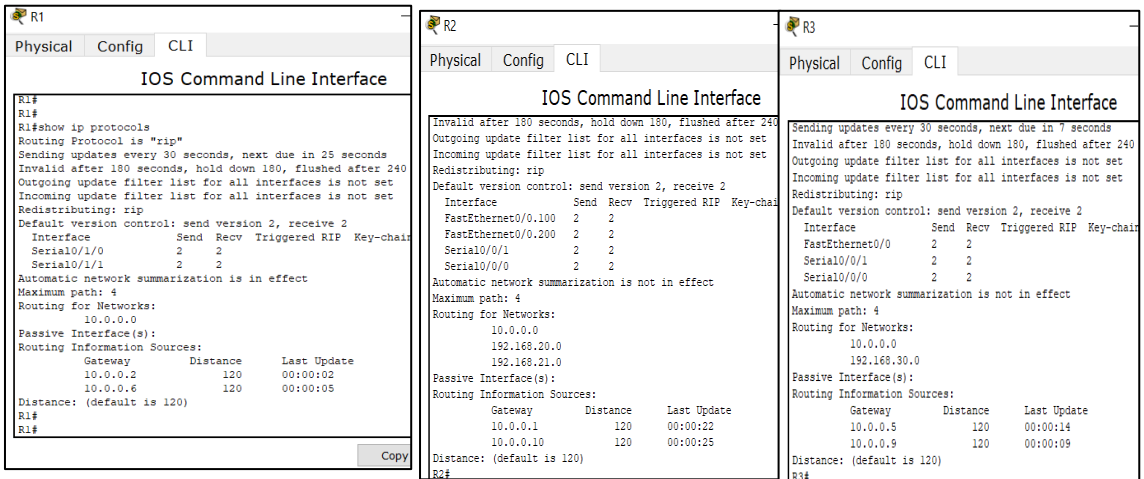
Enable
Config terminal
Router rip
version 2
network 192.168.20.0
network 192.168.21.0
network 10.0.0.9
network 10.0.0.2
no auto-summary
exit

Router 3:

enable
config terminal
router rip
version 2
network 192.168.30.0
network 10.0.0.6
network 10.0.0.10
no auto-summary
exit
ipv6 unicast-routing
ipv6 router rip RIPR3
exit
interface f0/0
ipv6 rip RIPR3 enable
exit
interface serial 0/0/1
ipv6 rip RIPR3 enable

Lo cual da cumplimiento al requerimiento 12: R1, R2 y R3 intercambian información de routing mediante RIP versión 2.

Figura 10. Tablas de enrutamiento RIP



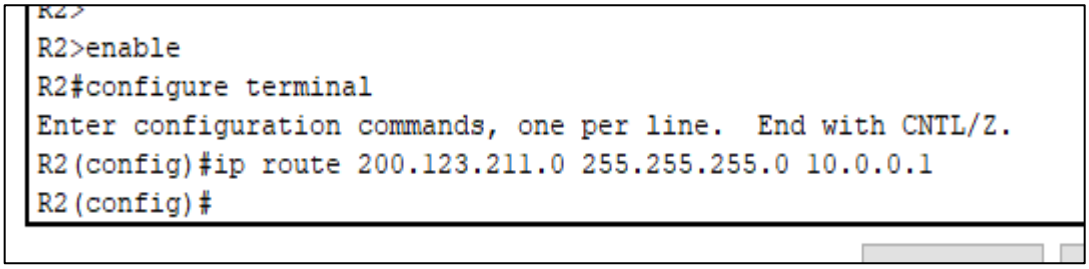
Fuente. Autoría propia

1.2.4 Ruta estática predeterminada desde R2 al ISP

enable
configure terminal
ip route 200.123.211.0 255.255.255.0 10.0.0.1

Lo cual da cumplimiento al requerimiento 6: R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.

Figura 11. Configuración ruta estática al ISP



Fuente. Autoría propia

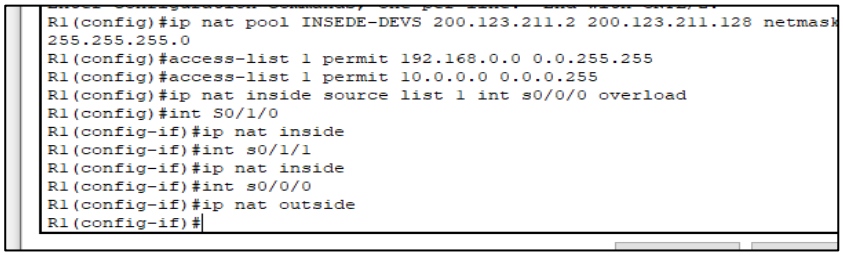
1.2.5 NAT Con sobrecarga (PAT) en router 1

ip nat pool INSEDE-DEVS 200.123.211.2 200.123.211.128 netmask 255.255.255.0
access-list 1 permit 192.168.0.0 0.0.255.255

access-list 1 permit 10.0.0.0 0.0.0.255
ip nat inside source list 1 int s0/0/0 overload
int S0/1/0
ip nat inside
int s0/1/1
ip nat inside
int s0/0/0
ip nat outside

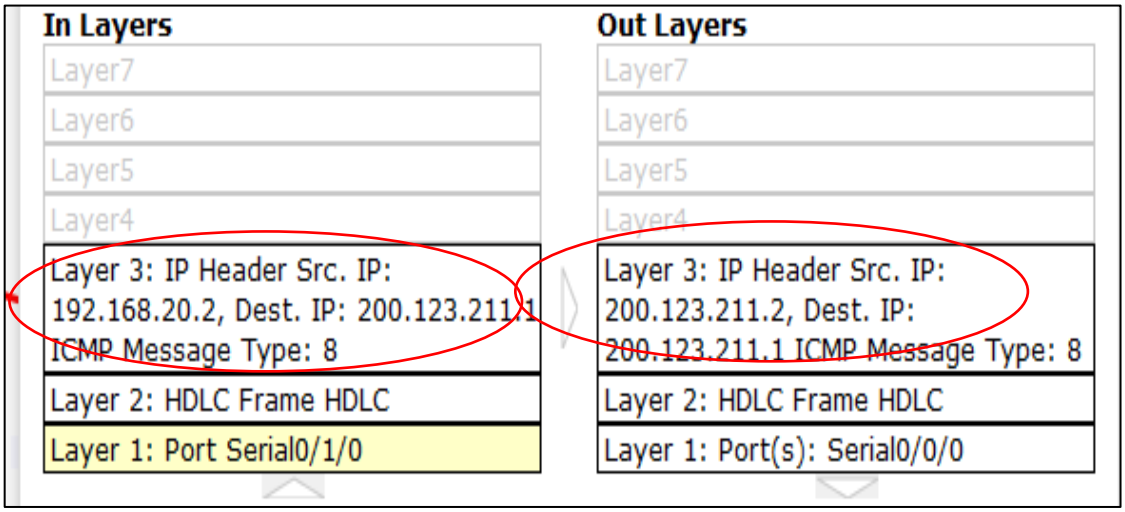
Lo cual da cumplimiento al requerimiento 5: R1 debe realizar una NAT con sobrecarga sobre una dirección IPv4 pública. Asegúrese de que todos los terminales pueden comunicarse con Internet pública (haga ping a la dirección ISP) y la lista de acceso estándar se llama INSIDE-DEVS.

Figura 12. Configuración NAT



Fuente. Autoría propia

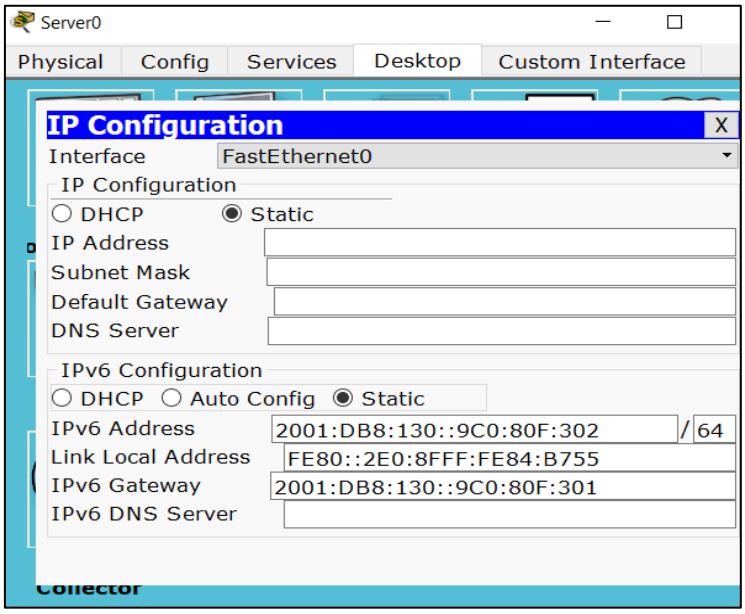
Figura 13. Salida con direcciones IP asignadas por la NAT



Fuente. Autoría propia

El servidor “Server0” es servidor solo con direcionamiento IPV6, con cual da cumplimiento al requerimiento 9: El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping):

Figura 14. Configuración IPV6 del server0

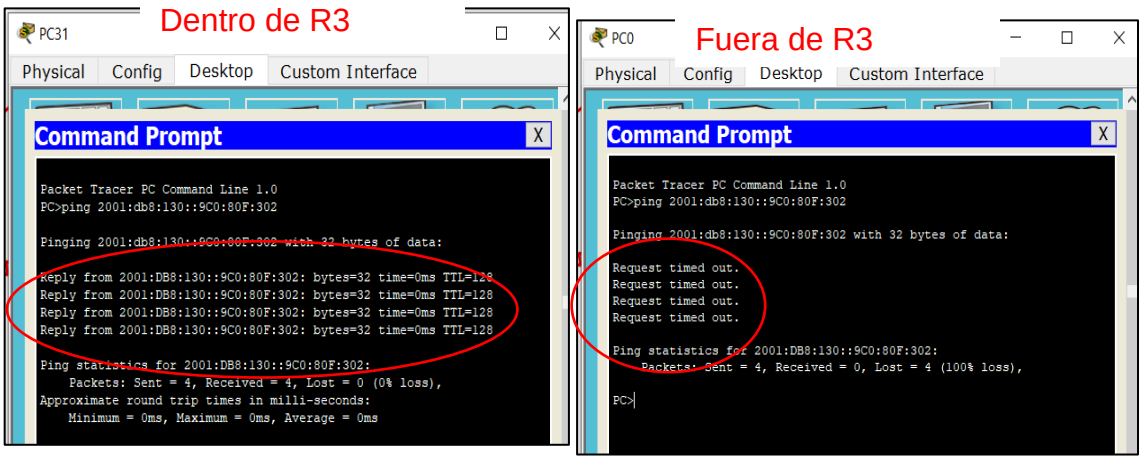


Fuente. Autoría propia

Prueba ping de dispositivo dentro de R3 y fuera de R3

Lo cual da cumplimiento al requerimiento 12: R1, R2 y R3 intercambian información de routing mediante RIP versión 2.

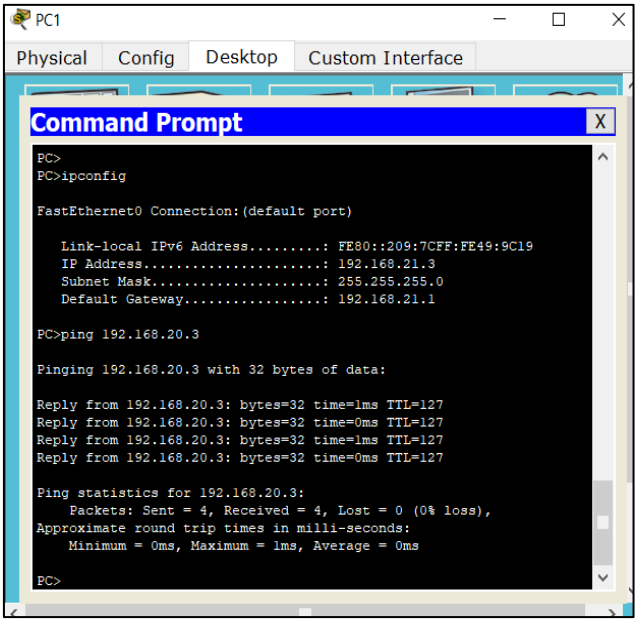
Figura 15. Prueba de ping desde dentro y fuera de R3



Fuente. Autoría propia

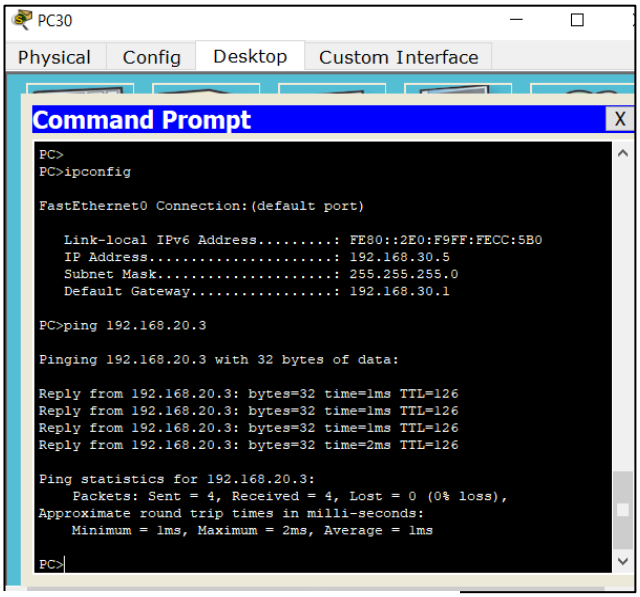
Lo cual da cumplimiento al requerimiento 14: Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre ellos y el servidor.

Figura 16. Ping de dispositivos en R3 pero diferente VLAN



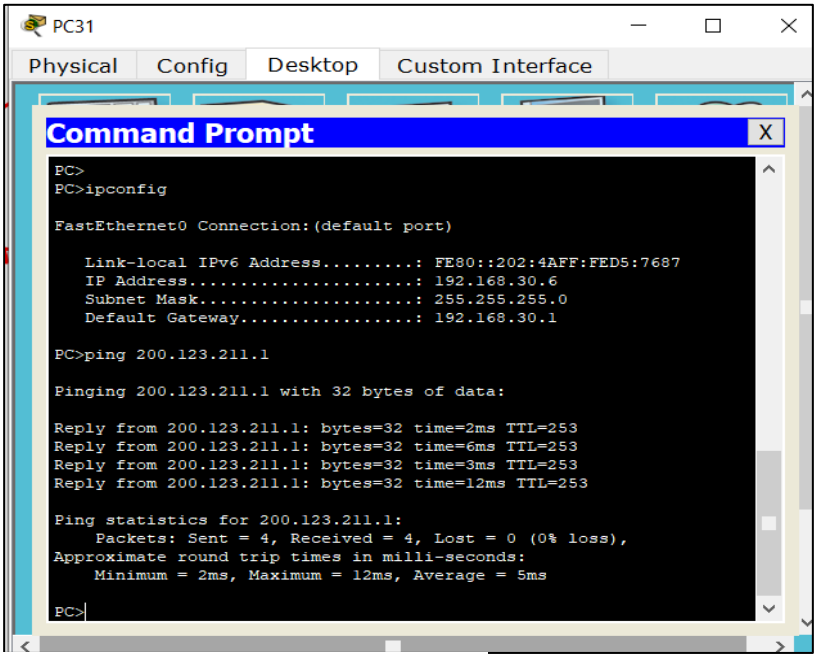
Fuente. Autoría propia

Figura 17. Ping de dispositivo de R2 al dispositivo de R3



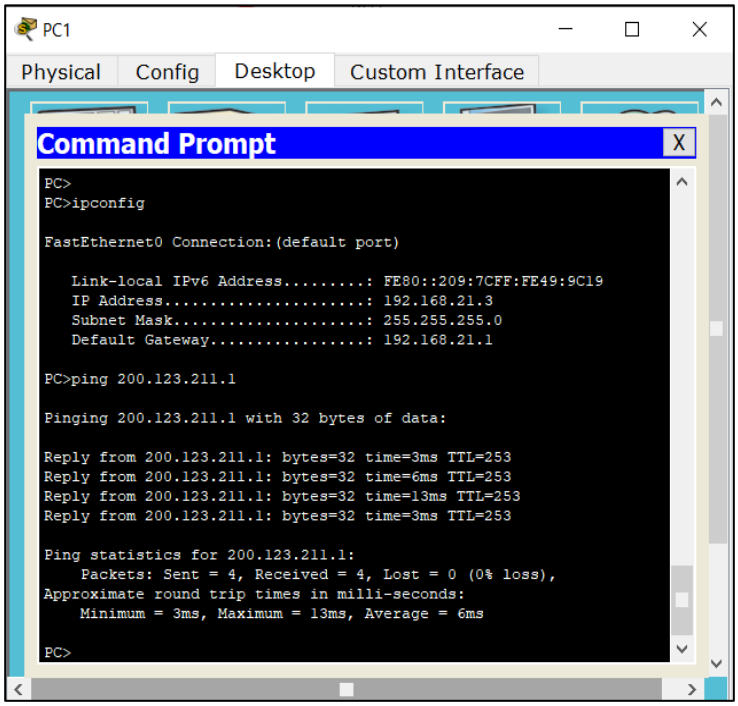
Fuente. Autoría propia

Figura 18. Ping de un dispositivo de R3 al ISP



Fuente. Autoría propia

Figura 19. Ping entre dispositivo de R2 al ISP



Fuente. Autoría propia

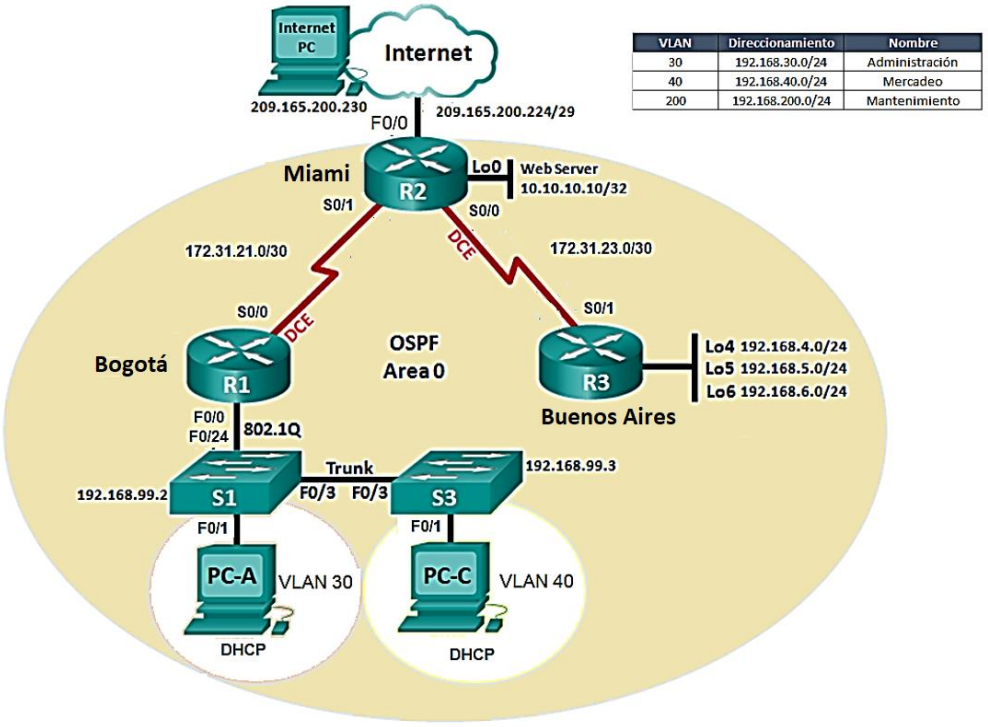
2 ESCENARIO 2

2.1 DESCRIPCIÓN

2.1.1 Requerimiento

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.

Figura 20. Topología a desarrollar



VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

Fuente. CISCO

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

Requerimiento1: Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:
OSPFv2 area 0

Tabla 5. Configuración dispositivos

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

Fuente. CISCO

Verificar información de OSPF

Requerimiento 2: Visualizar tablas de enrutamiento y routers conectados por OSPFv2
Requerimiento 3: Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface.
Requerimiento 4: Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Requerimiento 5: Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

Requerimiento 6: En el Switch 3 deshabilitar DNS lookup

Requerimiento 7: Asignar direcciones IP a los Switches acorde a los lineamientos.

Requerimiento 8: Desactivar todas las interfaces que no sean utilizadas en el esquema de red.
Requerimiento 9: Implement DHCP and NAT for IPv4.

Requerimiento 10: Configurar R1 como servidor DHCP para las VLANs 30 y 40.

Tabla 6. Configuración VLAN y DHCP

Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

Fuente. CISCO

Requerimiento 11: Configurar NAT en R2 para permitir que los host puedan salir a internet

Requerimiento 12: 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.

Requerimiento 13: 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.

Requerimiento 14: Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

2.2 DESARROLLO

2.2.1 Configuración inicial (nombre, direcciones IP, seguridad)

R1 Bogotá:

```
enable
config terminal
hostname R1

service password-encryption
line console 0
password cisco
login
```

exit
enable secre cisco
no ip domain lookup
line vty 0 15
exit
banner motd %solo personal autorizado%

interface Serial0/0/0
ip address 172.31.21.1 255.255.255.252
clock rate 128000
no shutdown
exit
do wr

R2 Miami:
enable
config terminal
hostname R2

service password-encryption
line console 0
password cisco
login
exit
enable secre cisco
no ip domain lookup
line vty 0 15
exit
banner motd %solo personal autorizado%
interface Serial0/0/1
ip address 172.31.21.2 255.255.255.252
no shutdown

interface Serial0/0/0
ip address 172.31.23.1 255.255.255.252
clock rate 128000
no shutdown

interface fa0/0
ip address 209.165.200.224 255.255.255.0
no shutdown

interface fa0/1
ip address 10.10.10.1 255.255.255.0
no shutdown

R3 Buenos Aires:
enable

config terminal
hostname R3

service password-encryption
line console 0
password cisco
login
exit
enable secre cisco
no ip domain lookup
line vty 0 15
exit
banner motd %solo personal autorizado%

interface Serial0/0/1
ip address 172.31.23.2 255.255.255.252
no shutdown
do wr

SW1:
enable
config terminal
hostname SW1

service password-encryption
line console 0
password cisco
login
exit
enable secre cisco
no ip domain lookup
line vty 0 15
exit
banner motd %solo personal autorizado%

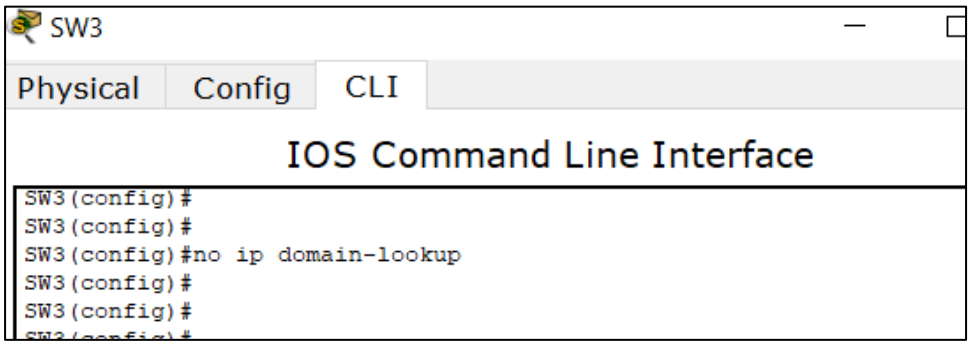
SW3:
enable
config terminal
hostname SW3

service password-encryption
line console 0
password cisco
login
exit
enable secre cisco
no ip domain lookup

line vty 0 15
exit
banner motd %solo personal autorizado%
no ip domain-lookup

Lo cual da cumplimiento al requerimiento 6: En el Switch 3 deshabilitar DNS lookup

Figura 21. Deshabilitar lookup



Fuente. Autoría propia

2.2.2 Switch (Vlan, modo trunk)

SW1:

vlan 30
name ADMINISTRACION
interface f0/1
switchport mode access
switchport access vlan 30
exit

vlan 200
name MANTENIMIENTO
interface f0/2
switchport mode access
switchport access vlan 200
exit

vlan 40
name MERCADEO
exit

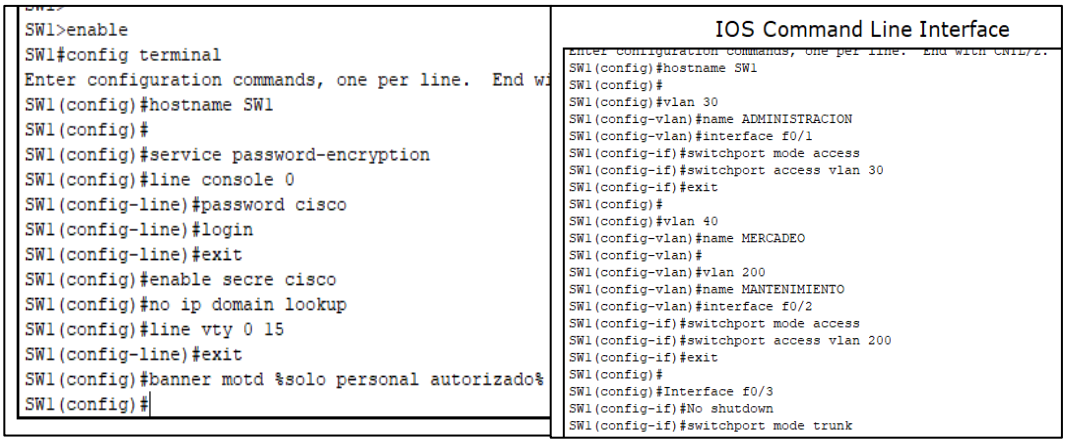
Interface f0/3
No shutdown
switchport mode trunk

Interface f0/24
No shutdown
switchport mode trunk

interface vlan 200
ip address 192.168.99.2 255.255.255.0
no shutdown
ip default-gateway 192.168.200.1

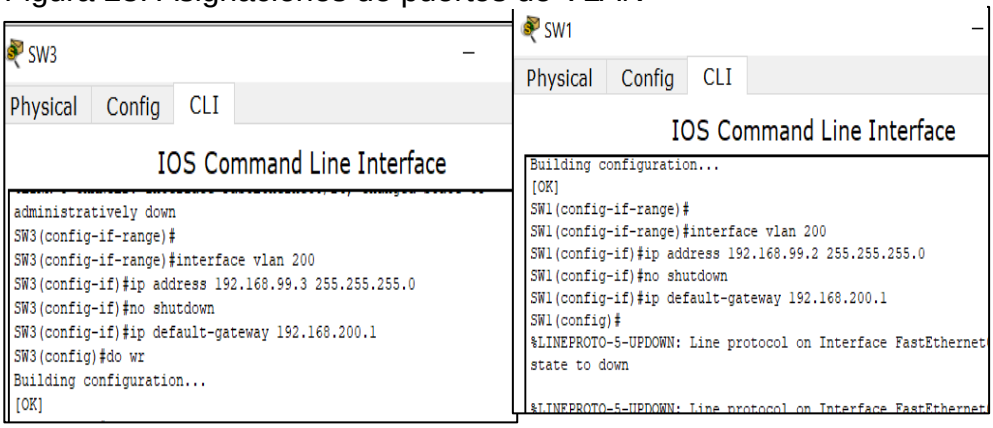
Lo cual da cumplimiento al requerimiento **5:** Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.

Figura 22. Configuración seguridad Switch y seguridad



Fuente. Autoría propia

Figura 23. Asignaciones de puertos de VLAN



Fuente. Autoría propia

vlan 40
name MERCADEO
interface f0/1
switchport mode access
switchport access vlan 40
exit

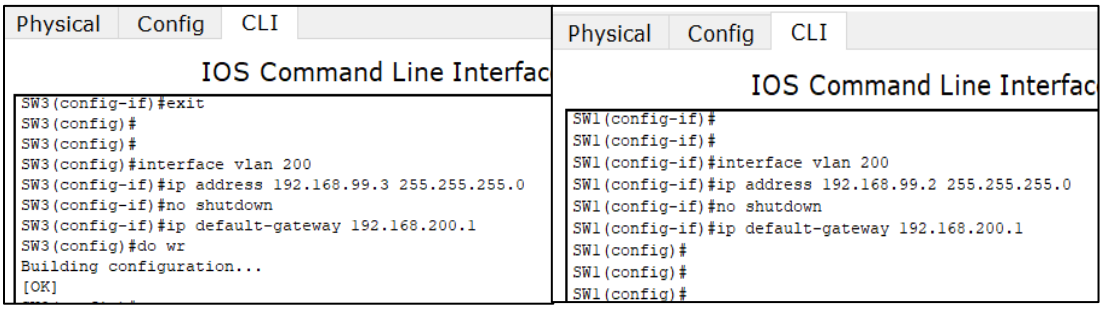
vlan 200
name MANTENIMIENTO
interface f0/2
switchport mode access
switchport access vlan 200
exit

Interface fa0/3
switchport mode trunk
exit

interface vlan 200
ip address 192.168.99.3 255.255.255.0
no shutdown
ip default-gateway 192.168.200.1
do wr

Lo cual da cumplimiento al requerimiento 7: Asignar direcciones IP a los Switches acorde a los lineamientos.

Figura 24. Asignación de direcciones IP a los Switchs



Fuente. Autoría propia

Desactivar todas las interfaces que no sean utilizadas

SW1:

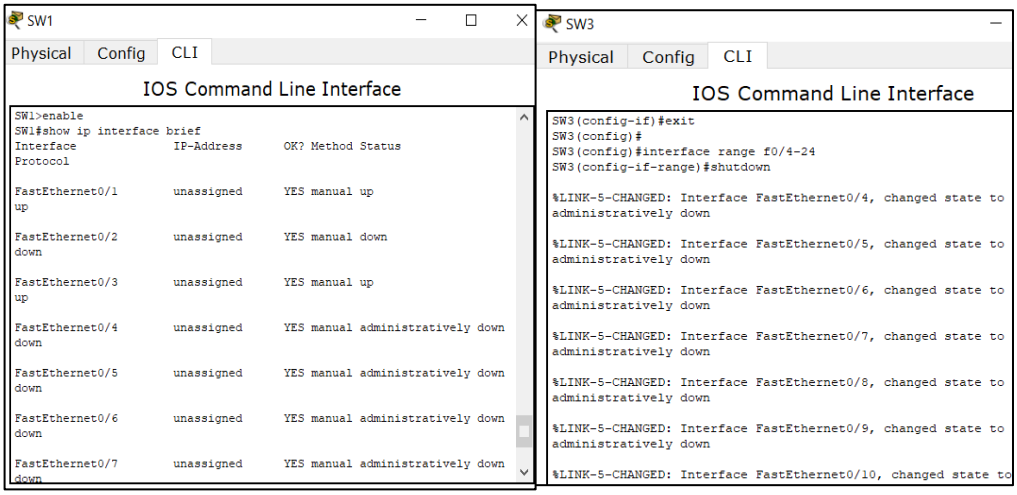
interface range f0/4-23
shutdown

do wr

SW3:
interface range f0/4-24
shutdown

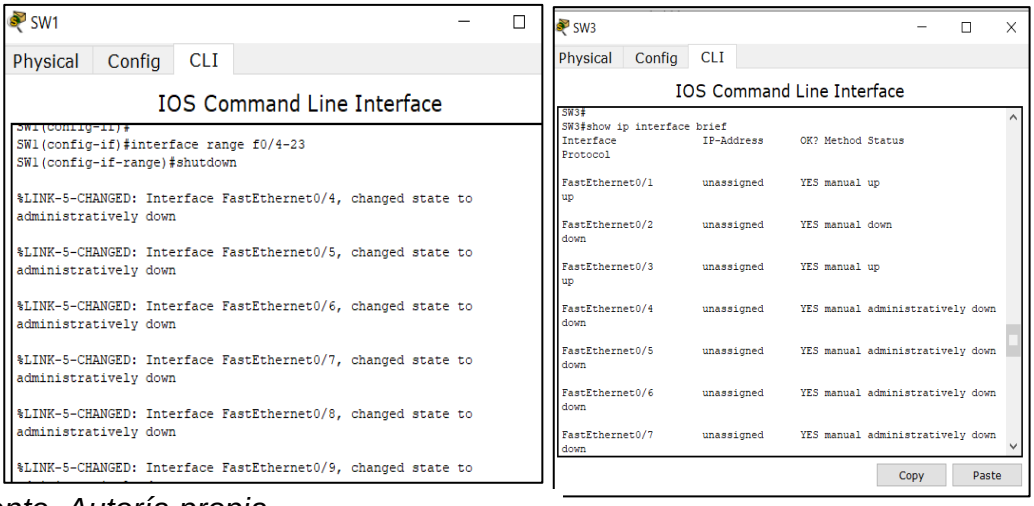
Lo cual da cumplimiento al requerimiento 8: Desactivar todas las interfaces que no sean utilizadas en el esquema de red.

Figura 25. Configuración interfaces que no se estén utilizando SW3



Fuente. Autoría propia

Figura 26. Configuración interfaces que no se estén utilizando SW1



Fuente. Autoría propia

R1 Bogotá:
enable
config terminal

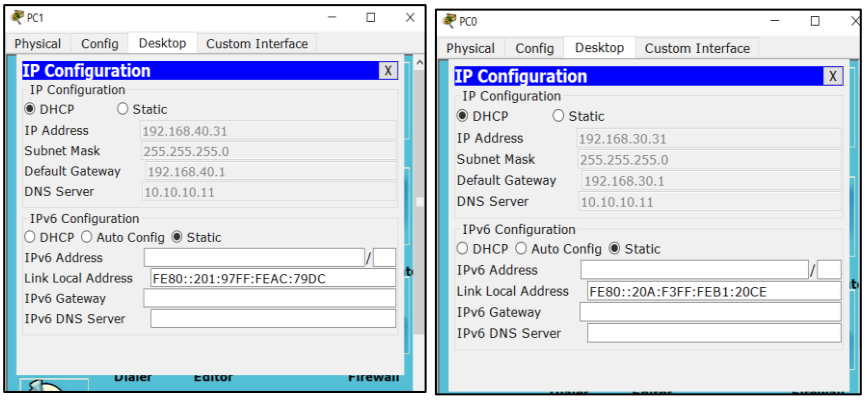
```
interface f0/0
no shutdown

interface f0/0.30
encapsulation dot1Q 30
ip address 192.168.30.1 255.255.255.0

interface f0/0.40
encapsulation dot1Q 40
ip address 192.168.40.1 255.255.255.0

interface f0/0.200
encapsulation dot1Q 200
ip address 192.168.200.1 255.255.255.0
exit
do wr
```

2.2.3 Configuración DHCP en R1 (Bogotá)

```
ip dhcp pool ADMINISTRACION
network 192.168.30.0 255.255.255.0
default-router 192.168.30.1
dns-server 10.10.10.11
exit
ip dhcp excluded-address 192.168.30.1 192.168.30.30
ip dhcp pool MERCADEO
network 192.168.40.0 255.255.255.0
default-router 192.168.40.1
dns-server 10.10.10.11
ip dhcp excluded-address 192.168.40.1 192.168.40.30
```

Lo cual da cumplimiento al requerimiento 10: Configurar R1 como servidor DHCP para las VLANs 30 y 40.

Figura 27. Asignación direcciones DCHP



Fuente. Autoría propia

2.2.4 Configuración loopback

R3 Buenos Aires:

interface loopback 4
ip address 192.168.4.1 255.255.255.0
no shutdown

interface loopback 5
ip address 192.168.5.1 255.255.255.0
no shutdown

interface loopback 6
ip address 192.168.6.1 255.255.255.0
no shutdown

2.2.5 OSPF, interfaces pasivas y NAT

R1 Bogotá:

router ospf 1
router-id 1.1.1.1
network 172.31.21.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
network 192.168.99.0 0.0.0.255 area 0

passive-interface f0/0.30
passive-interface f0/0.40
passive-interface f0/0.200

interface s0/0/0
bandwidth 255
ip ospf cost 9500

R2 Miami:

router ospf 1
router-id 5.5.5.5
network 209.165.200.230 0.0.0.255 area 1
network 172.31.23.0 0.0.0.3 area 0
network 172.31.21.0 0.0.0.3 area 0
network 10.10.10.0 0.0.0.255 area 0
passive-interface f0/0
passive-interface f0/1

interface s0/0/0
bandwidth 255

ip ospf cost 9500

interface s0/0/1
bandwidth 255
ip ospf cost 9500

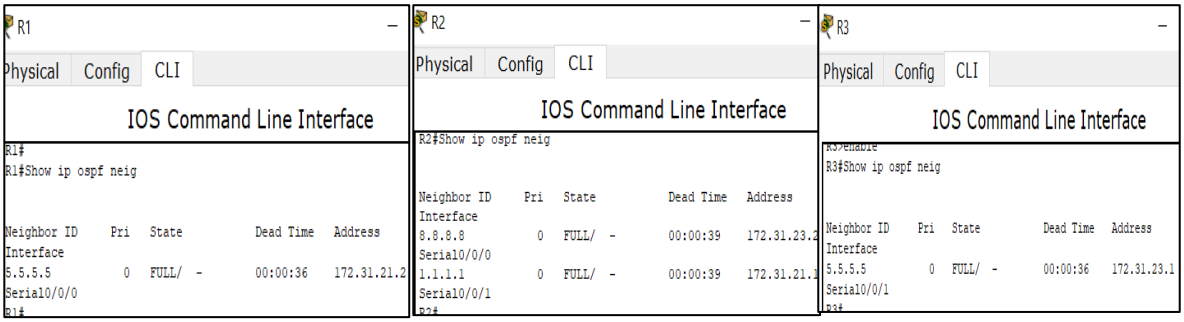
R3 Buenos aires:
router ospf 1
router-id 8.8.8.8
network 192.168.4.0 0.0.0.255 area 0
network 192.168.5.0 0.0.0.255 area 0
network 192.168.6.0 0.0.0.255 area 0
network 172.31.23.0 0.0.0.3 area 0

passive-interface lo4
passive-interface lo5
passive-interface lo6

interface s0/0/1
bandwidth 255
ip ospf cost 9500
do wr

Requerimiento 2: Visualizar tablas de enrutamiento y routers conectados por OSPFv2

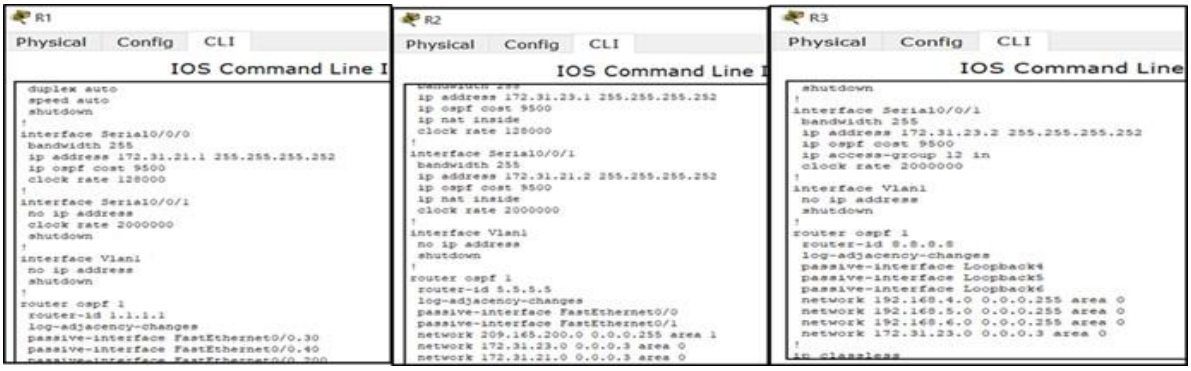
Figura 28. Tablas de enrutamiento OSPF



Fuente. Autoría propia

Requerimiento 3: Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface.

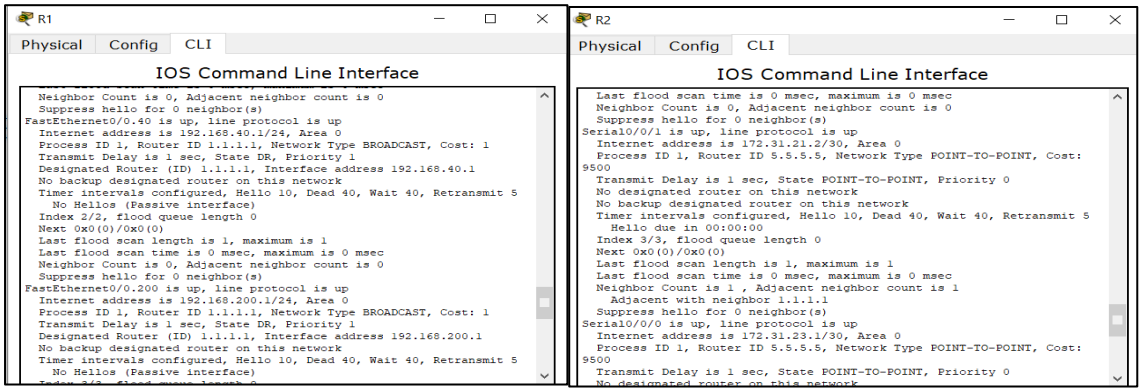
Figura 29. Visualización resumida OSPF



Fuente. Autoría propia

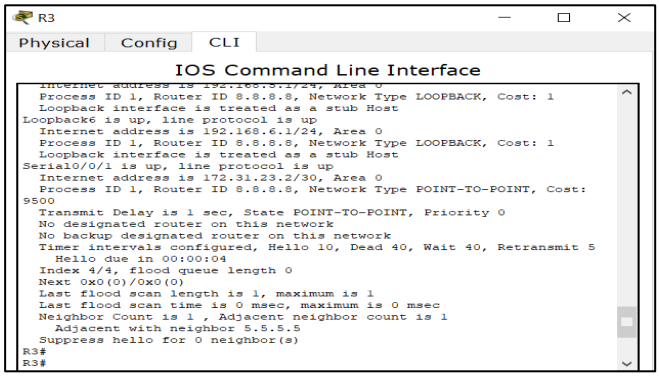
Requerimiento 4: Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

Figura 30. Visualización OSPF R1 y R2



Fuente. Autoría propia

Figura 31. Visualización OSPF R3



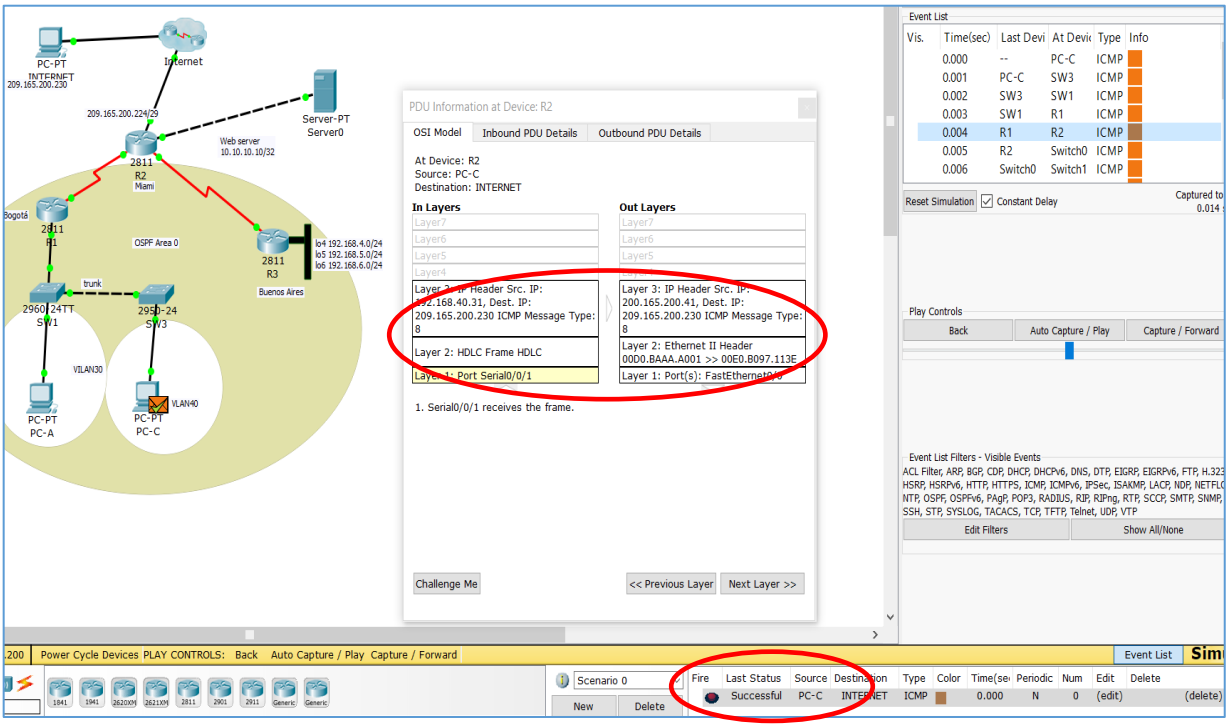
Fuente. Autoría propia

2.2.6 NAT

```
ip nat pool MIAMI 200.165.200.40 200.165.200.50 netmask 255.255.255.0
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
access-list 1 permit 172.31.23.2 0.0.0.3
ip nat inside source list 1 pool MIAMI

interface  s0/0/1
ip nat inside
exit

interface  s0/0/0
ip nat inside
exit

interface f0/0
ip nat outside
```

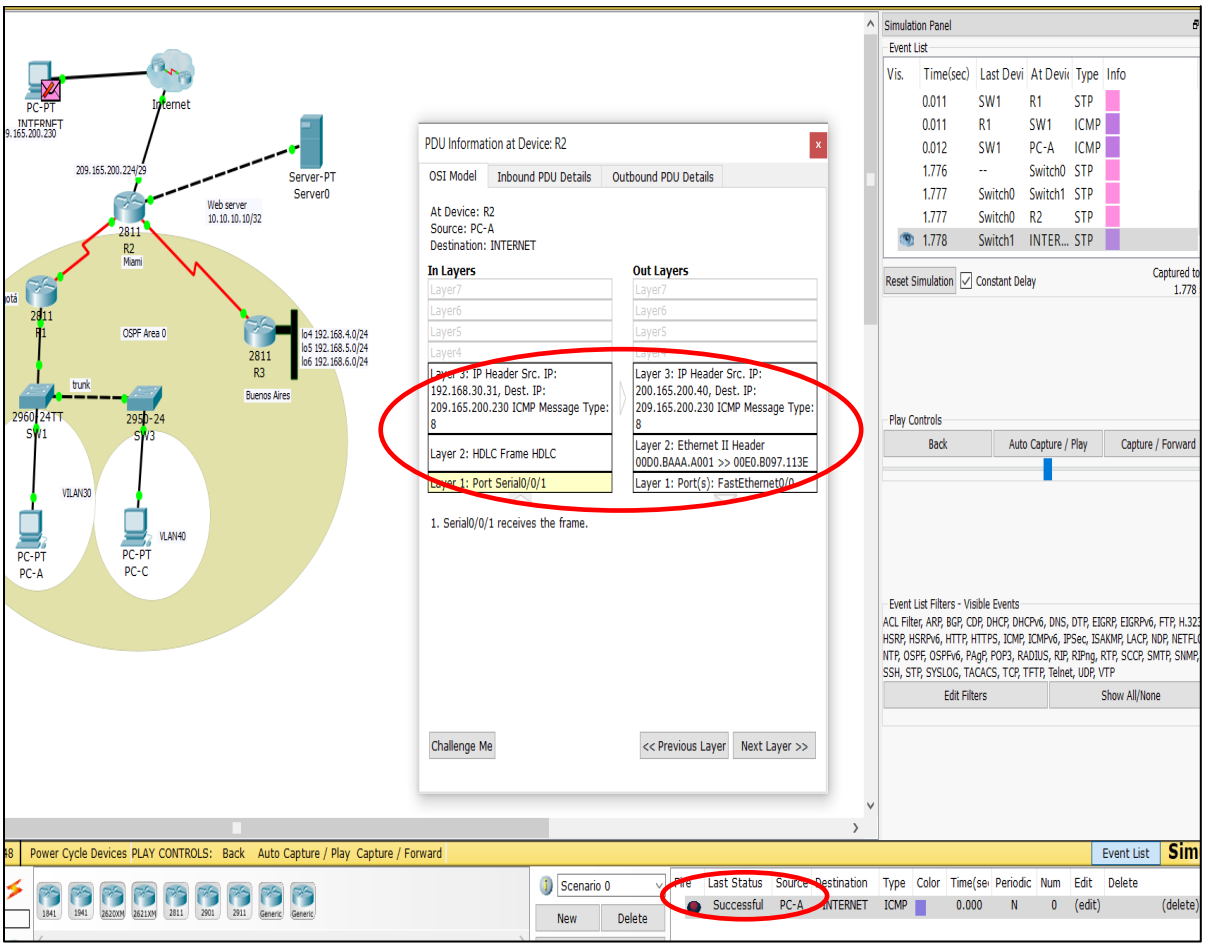
Lo cual da cumplimiento al requerimiento 11: Configurar NAT en R2 para permitir que los host puedan salir a internet

Figura 32. Funcionamiento NAT desde la red 192.168.40.0



Fuente. Autoría propia

Figura 33. Funcionamiento NAT desde la red 192.168.30.0



Fuente. Autoría propia

2.2.7 Lista de control de acceso estándar y extendida

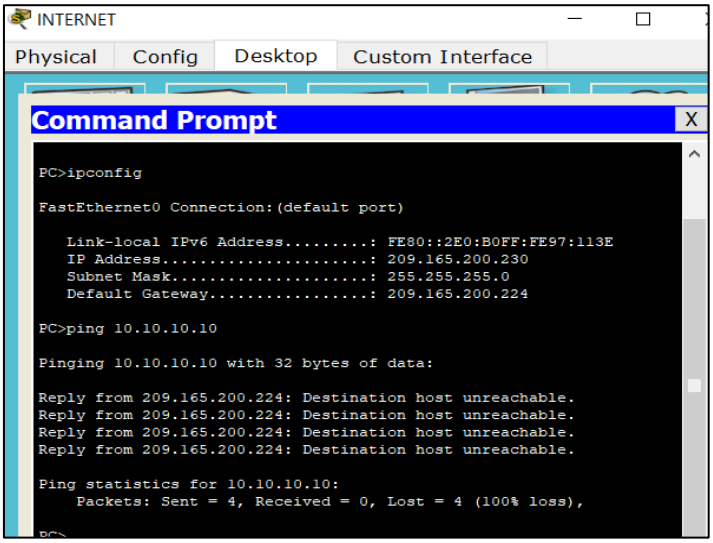
Listas de acceso estandar:

Crearemos dos listas de acceso estandar, de la siguiente manera:

Lista de acceso estandar que no permita la comunicación desde el PC de Internet de dirección IP 209.165.200.230 al servidor de dirección IP 10.10.10.10, la cual se configurará en el router R2:

```
access-list 11 deny 209.165.200.230 0.0.0.255
access-list 11 permit any
interface fa0/1
ip access-group 11 out
```

Figura 34. Prueba de ping a la IP 10.10.10.10

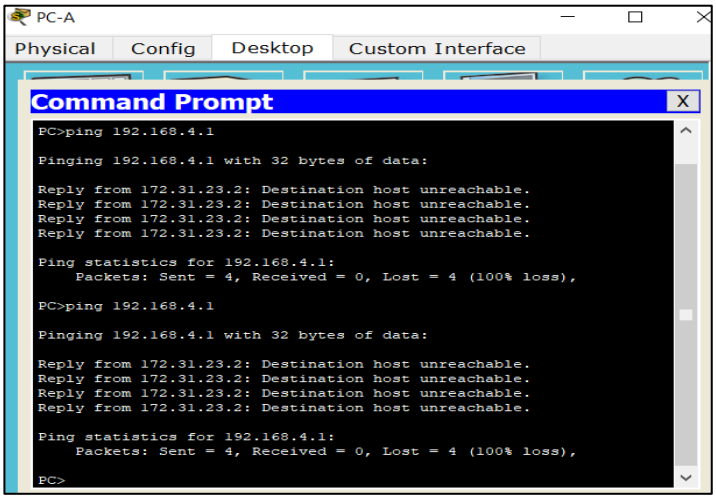


Fuente. Autoría propia

Lista de acceso estándar que bloquea la conectividad desde la red 192.168.30.0 con el router R3, la cual se configurará en el router R3:

```
access-list 12 deny 192.168.30.0 0.0.0.255
access-list 12 permit any
interface s0/0/1
ip access-group 12 in
exit
do wr
```

Figura 35. Prueba ping a la IP 192.168.4.1



Fuente. Autoría propia

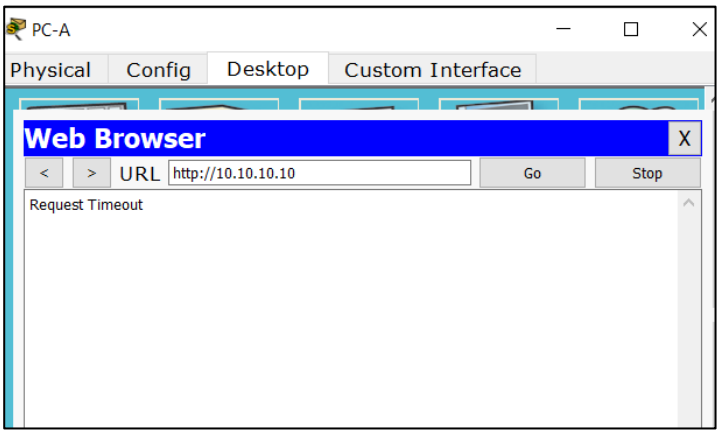
Lo cual da cumplimiento al requerimiento 12: Configurar al menos dos listas de acceso de tipo estándar a su criterio en para restringir o permitir tráfico desde R1 o R3 hacia R2.

Lista de acceso extendida:

Crearemos una listas de acceso extendida, que bloquearan la conectividad desde la red 192.168.30.0 al puerto 80 (navegación de Internet) del servidor de dirección IP 10.10.10.10, el cual se configurará en el router R1

```
access-list 102 deny tcp 192.168.30.0 0.0.0.255 host 10.10.10.10 eq 80
access-list 102 permit ip any any
interface f0/0.30
ip access-group 102 in

exit
```

Figura 36. Bloqueo del puerto 80 mediante lista de acceso

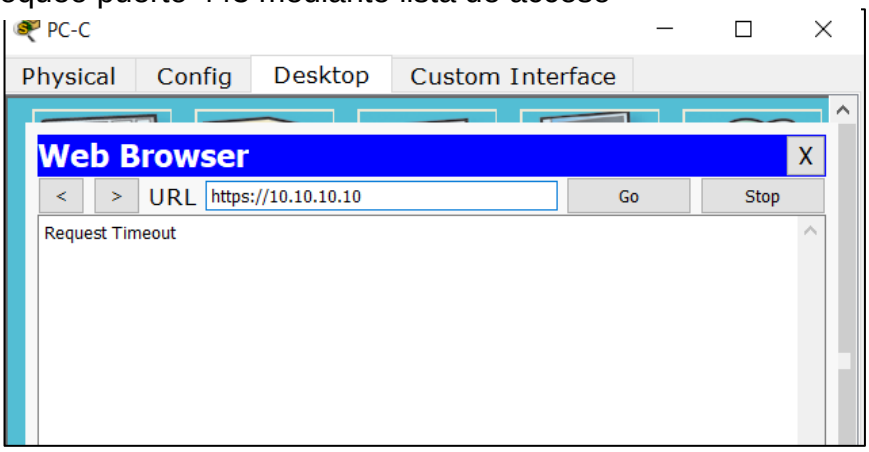


Fuente. Autoría propia

Crearemos una listas de acceso extendida, que bloquearan la conectividad desde la red 192.168.40.0 al puerto 443 (navegación segura de Internet) del servidor de dirección IP 10.10.10.10, el cual se configurará en el router R1

```
access-list 103 deny tcp 192.168.40.0 0.0.0.255 host 10.10.10.10 eq 443
access-list 103 permit ip any any
interface f0/0.40
ip access-group 103 in
exit
do wr
```

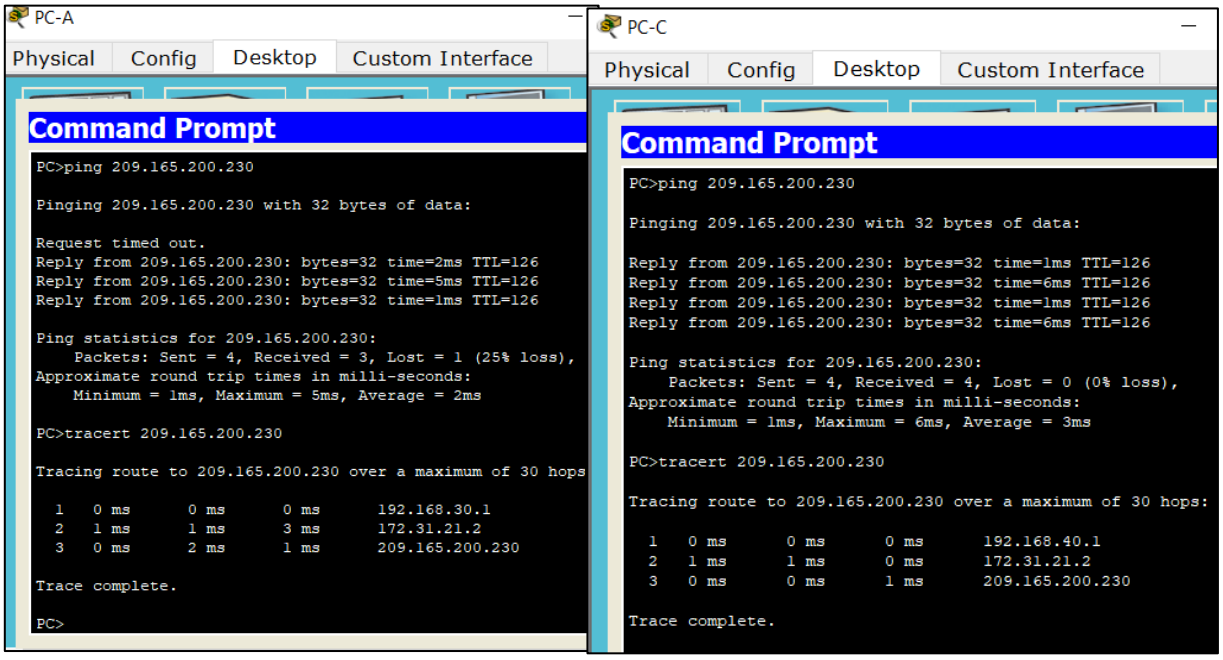
Figura 37. Bloqueo puerto 443 mediante lista de acceso



Fuente. Autoría propia

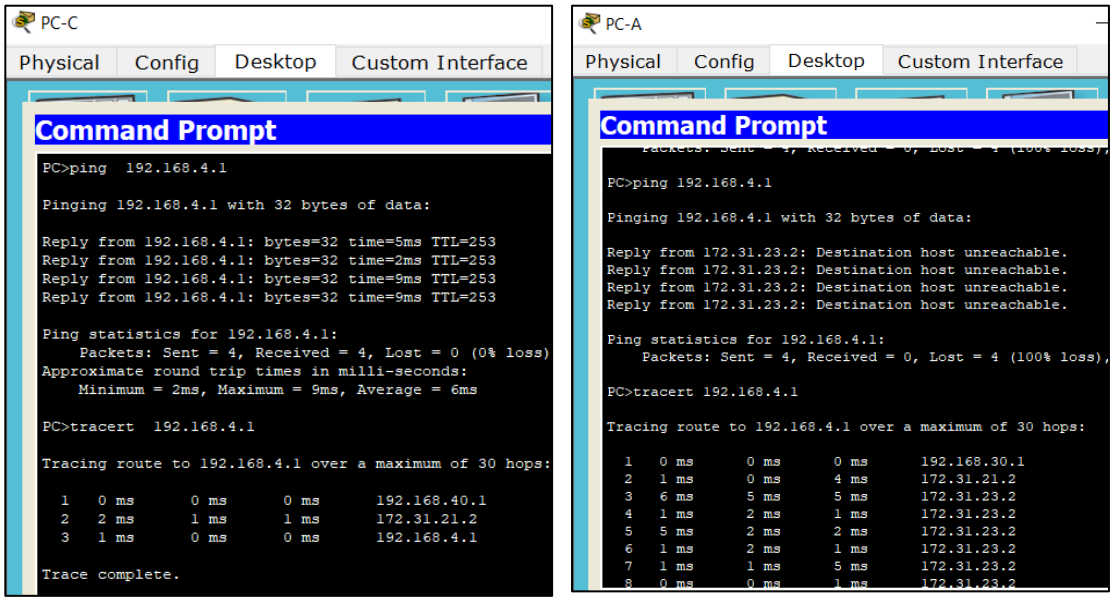
2.2.8 Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.

Figura 38. Verificando conectividad mediante ping y tracert



Fuente. Autoría propia

Figura 39. Ping y tracert, en la segunda figura no hace ping ya que una lista de acceso configurada lo bloquea



Fuente. Autoría propia

Link de acceso a los archivos configurados

https://drive.google.com/drive/folders/1ebTV1HMHTWZggDbaRhAJe-BsVZC3p7Kj

CONCLUSIONES

- Con base a los conocimientos adquiridos en los módulos CP CCNA1 II-2018 y CP CCNA2 II-2018 de la plataforma NETACAD se dio solución a los dos escenarios hipotéticos propuestos para ser desarrollados en el presente trabajo, para lo cual se realizó su diseño y respectivas pruebas de conectividad entre los diferentes dispositivos implicados en cada una de las redes, para lo cual se empleó la herramienta Packet Tracer.

- Para el desarrollo de cada escenario se anexó capturas de pantallas de su implementación, funcionamiento y pruebas de conectividad, de igual forma se anexó el código de configuración usado para los escenarios propuestos.

REFERENCIAS

CISCO. (s.f.). *Exploración de la red. Fundamentos Networking.* Obtenido de https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1

Lammle, T. (2010). *Cisco Certified Network Associate Study Guide.* CISCO Press. Obtenido de https://1drv.ms/b/s!AmIJYei-NT1Im3GQVfFFrjnEGFFU