SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

MILTON ANDRÉS ZÚÑIGA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA –ECBTI
INGENIERÍA ELECTRONICA
NEIVA
2019

SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

PRESENTADO POR:
MILTON ANDRÉS ZÚÑIGA

DIRECTOR
JUAN VESGA

DIPLOMADO DE PROFUNDIZACION CISCO (DISEÑO E IMPLEMENTACION DE SOLUCIONES INTEGRADAS LAN/WAN)

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA –ECBTI
INGENIERÍA ELECTRONICA
NEIVA
2019

CONTENIDO

1. INTRODUCCION

En el presente trabajo se mostrará la solución de dos escenario practicos los cuales fueron propuestos como parte de la culminación del diplomado, en el que se mostrará todas las habilidades adquiridas durante el curso.

Con el gran avanace tecnológico que dia a día crece exponencialmente se desarrollan nuevas tecnologías capaces de realizar comunicaciones de una manera rápida con un gran ancho de banda y muy prácticas para quien lo utilice.

Existen algunos problemas cuando se desea innovar un estableciemiento o también el surgimiento de una nueva empresa dónde se deben realizar planos esquemáticos de estos lugares y además la adaptación según el medio donde se va a instalar esta tecnología y es aquí donde el estudiante debe ser capaz de dar solución a cualquier problemática que se presente o tener una gran idea de como dar solución a esta.

Para el desarrollo de este trabajo se hizo uso del simulador packet tracer debido a que es muy fácil de utilizar, tiene una interfaz muy bien desarrollada y además con éste simulador se trabajo durante todo el curso. En la solución del trabajo se muestran los algoritmos utilizados, como tambien de algunas imaganés correspondiente al funcionamiento de éste.

2. DESARROLLO DE LOS ESCENARIOS

2.1 ESCENARIO 1:

Figura 1. Topologia de la Red del Escenario 1 en Packet Tracer.

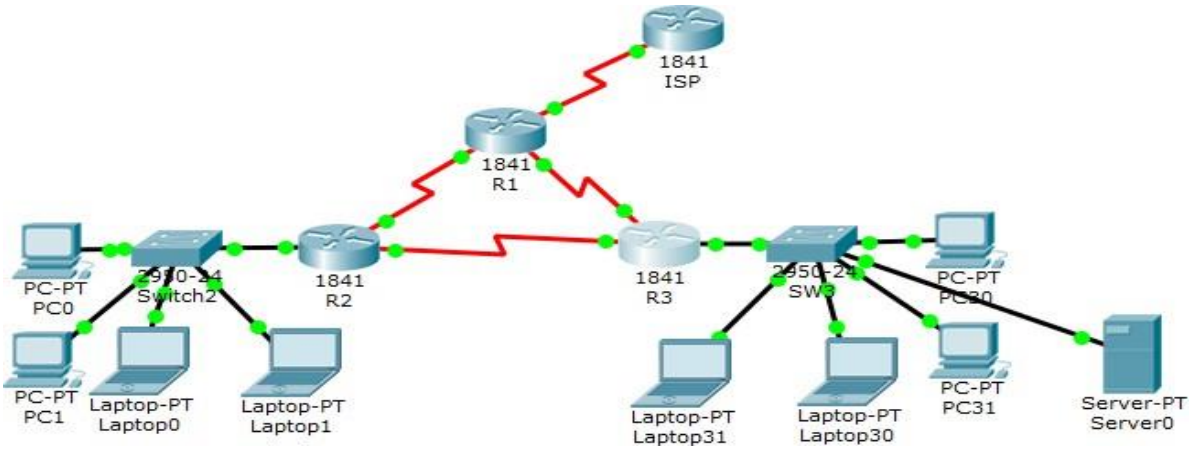


Tabla de direccionamiento

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

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

Tabla de enlaces troncales

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

Situación

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

- **SW2** VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.

S2:

```
Switch2>en
Switch2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#enable password class
Switch2(config)#
Switch2(config)#vlan 100
Switch2(config-vlan)#name LAPTOPS
Switch2(config)#int range fa0/2-3
Switch2(config-if-range)#switch mode acces
Switch2(config-if-range)#switch access vlan 100
Switch2(config-if-range)#end
Switch2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#vlan 200
Switch2(config-vlan)#name DESKTOPS
Switch2(config-vlan)#exit
Switch2(config)#int range fa0/4-5
Switch2(config-if-range)#switch mode acces
Switch2(config-if-range)#switch access vlan 200
```

S3:

```
SW3>en
SW3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#enable password class
SW3(config)#vlan 1
SW3(config)#int range fa0/1-24
SW3(config-if-range)#switch mode acces
SW3(config-if-range)#switch access vlan 1
SW3(config-if-range)#end
```

- Los puertos de red que no se utilizan se deben deshabilitar.

S2:

```
Switch2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch2(config)#int range fa0/1, fa0/6-24
Switch2(config-if-range)#sh
```

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

R1:

```
R1>en
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable password class
R1(config)#int s0/0/0
R1(config-if)#ip add 200.123.211.2 255.255.255.0
R1(config-if)#no sh
R1(config)#int s0/1/0
R1(config-if)#ip add 10.0.0.1 255.255.255.252
R1(config-if)#no sh
R1(config)#int s0/1/1
R1(config-if)#ip add 10.0.0.5 255.255.255.252
R1(config-if)#no sh
R1(config)#line con 0
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#end
```

R2:

```
R2> en
R2# conf t
R2(config)#enable password class
R2(config)#line con 0
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#int s0/0/0
R2(config-if)#ip add 10.0.0.2 255.255.255.252
R2(config-if)#no sh
R2(config-if)#int s0/0/1
R2(config-if)#ip add 10.0.0.9 255.255.255.252
R2(config-if)#no sh
```

R3:

```
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#enable password class
R3(config)#line con 0
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#int s0/0/0
R3(config-if)#ip add 10.0.0.6 255.255.255.252
R3(config-if)#no sh
R3(config-if)#int s0/0/1
R3(config-if)#ip add 10.0.0.10 255.255.255.252
R3(config-if)#no sh
R3(config-if)#exit
R3(config)#int fa0/0
R3(config-if)#ip add 192.168.30.1 255.255.255.0
R3(config-if)#no sh
R3(config-if)#exit
R3(config)#int fa0/0
R3(config-if)#ipv6 add
R3(config-if)#ipv6 address 2001:db8:130::9C0:80F:301/64
R3(config-if)#no sh
```

- **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#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int f0/0
R2(config-if)#ip add dhcp
R2(config-if)#no sh
```

- **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).

Figura 2. Interfaz FastEhternet 0/0.

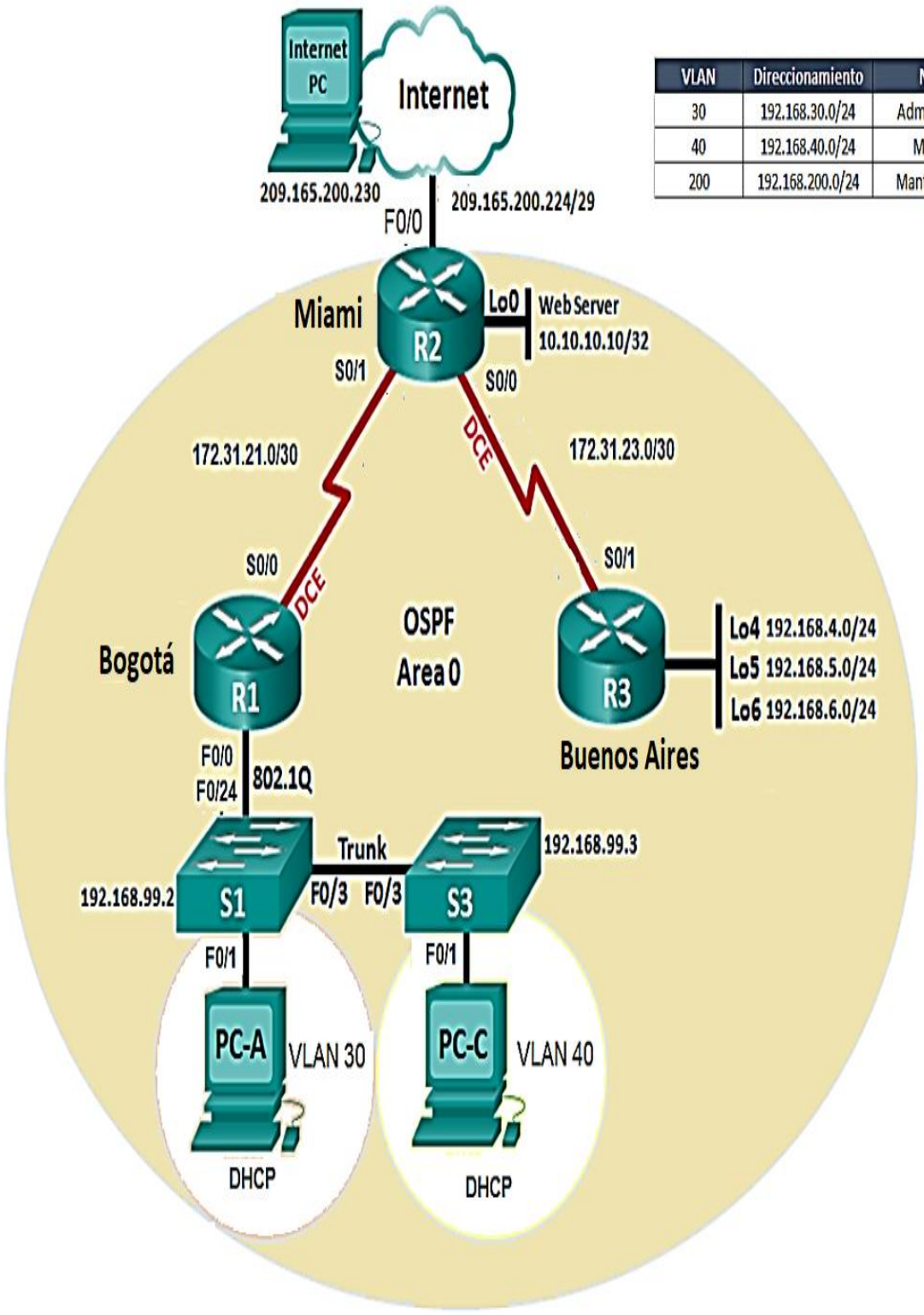
```
interface FastEthernet0/0
 ip address 192.168.30.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2001:DB8:130::9C0:80F:301/64
```

- 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.

2.2 ESCENARIO 2

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 3. Topología de Red del Escenario 2.



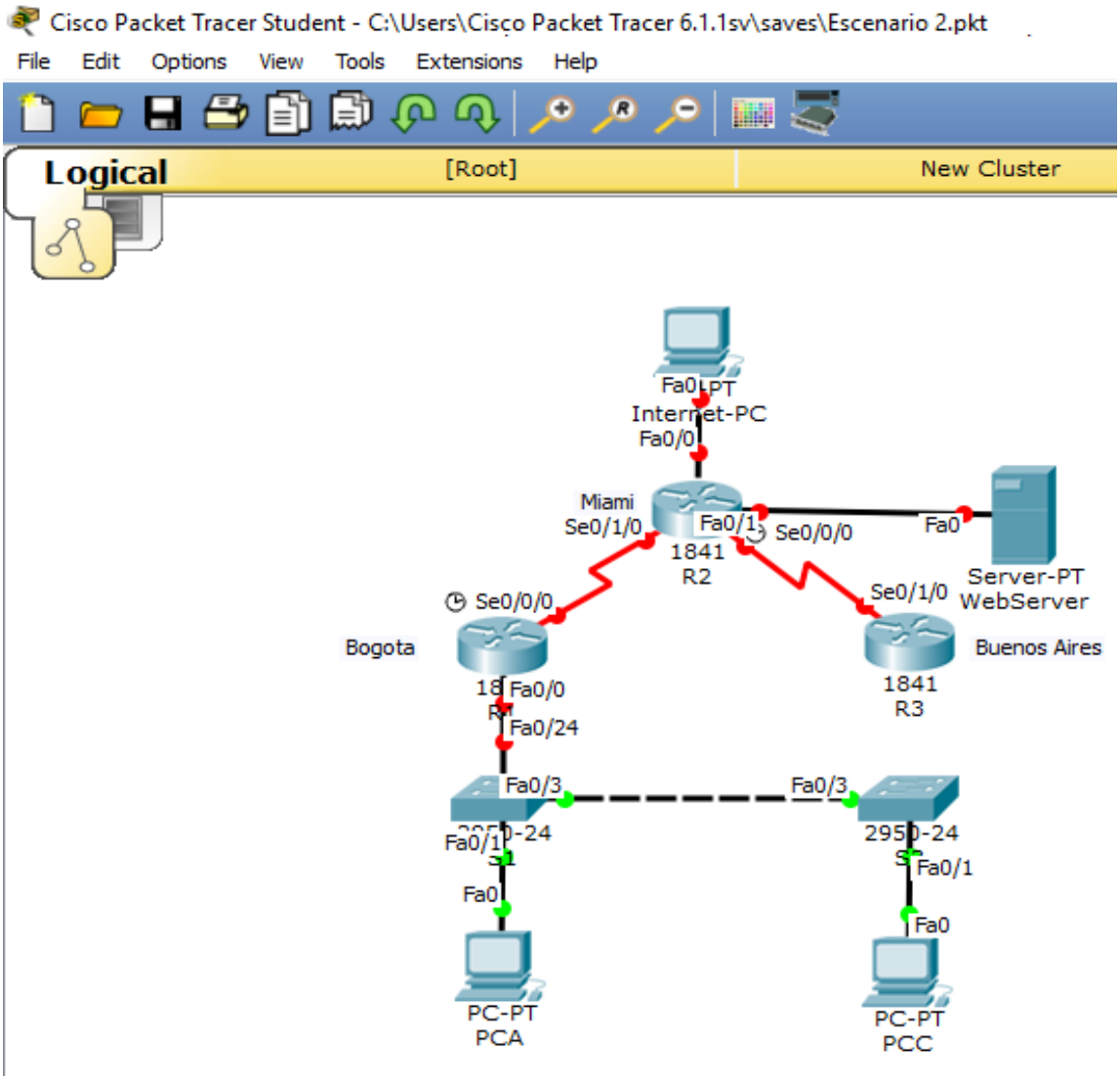
VLAN	Direccionamiento	Nombre
30	192.168.30.0/24	Administración
40	192.168.40.0/24	Mercadeo
200	192.168.200.0/24	Mantenimiento

SOLUCION

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

   - Password: cisco R1-R3
   - Password: CISCO R2
   - Enable password: class R1-R2-R3-S1-S2

Figura 4. Topología de Red del Escenario 2 en Packet Tracer.



Sede y Dir. Red	mask	Octeto	Octeto	Dir. Subred	Gateway	Final (PC)
WebServer	32	3er 1010	4to 1010	10.10.10.0	10.10.10.1	10.10.10.10
Administracion Vlan 30 192.168.30.0	24	3er 11110	4to 000-----	192.168.30.0	192.168.30.1	192.168.30.31
Mercadeo Vlan 40 192.168.40.0	24	3er 101000	4to 00------	192.168.40.0	192.168.40.1	192.168.40.41
R1 Bogota S0/0/0 172.31.21.0	30	3er 10101	4to 000000--	172.31.21.0	172.31.21.1	
R2 Miami S0/1/0 172.31.21.0	30	3er 10101	4to 000000--	172.31.21.0	172.31.21.2	
Miami S0/0/0 172.31.23.0	30	3er 10111	4to 000000--	172.31.23.0	172.31.23.1	
Buenos Aires S0/1/0 172.31.23.0	30	3er 10111	4to 000000--	172.31.23.0	172.31.23.2	

Figura 5. Configuración del servidor web.

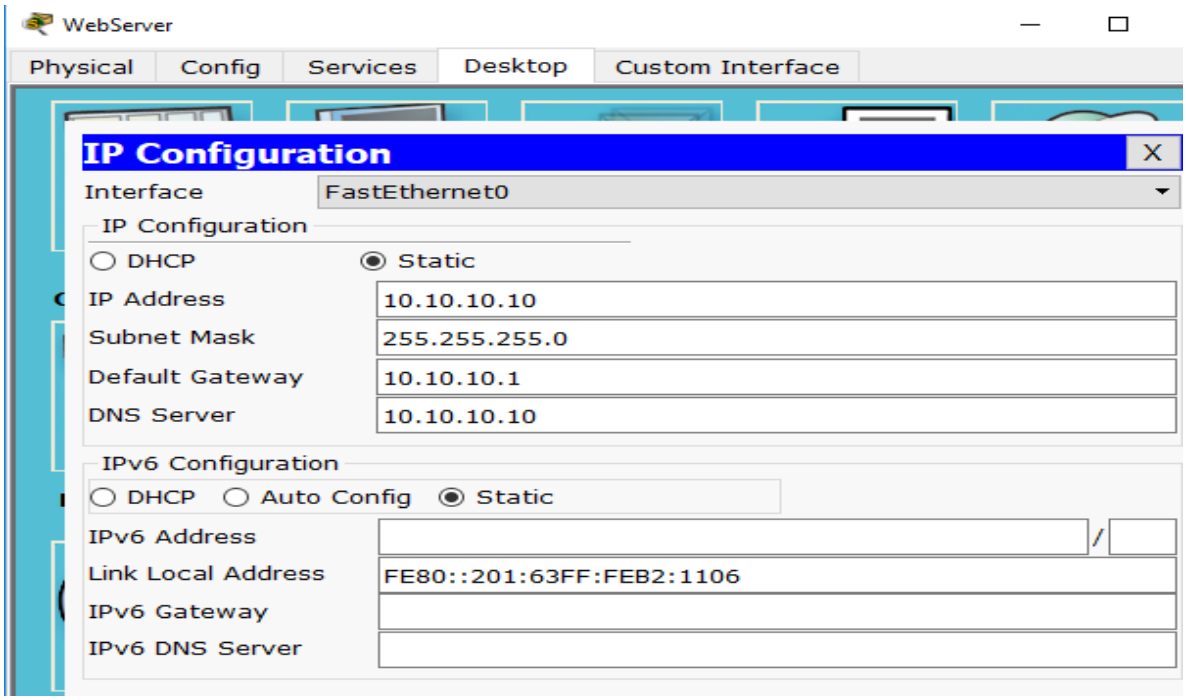


Figura 6. Configuración de la PCA.

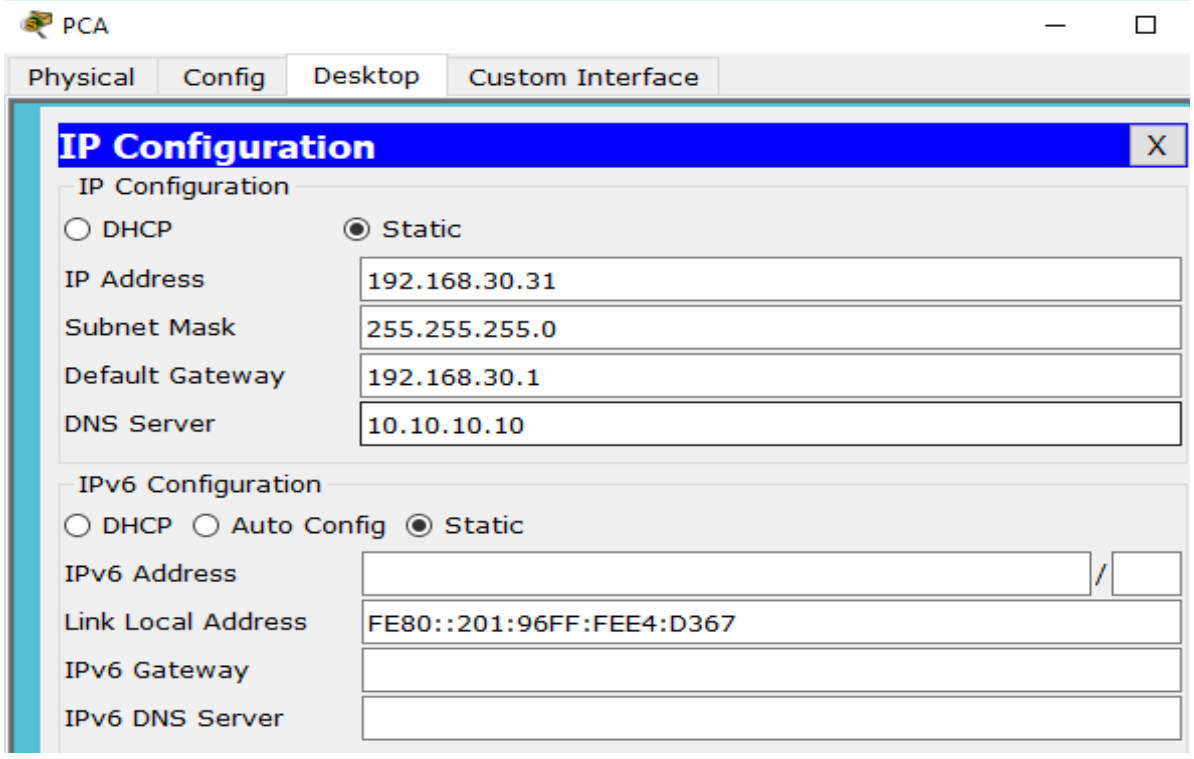
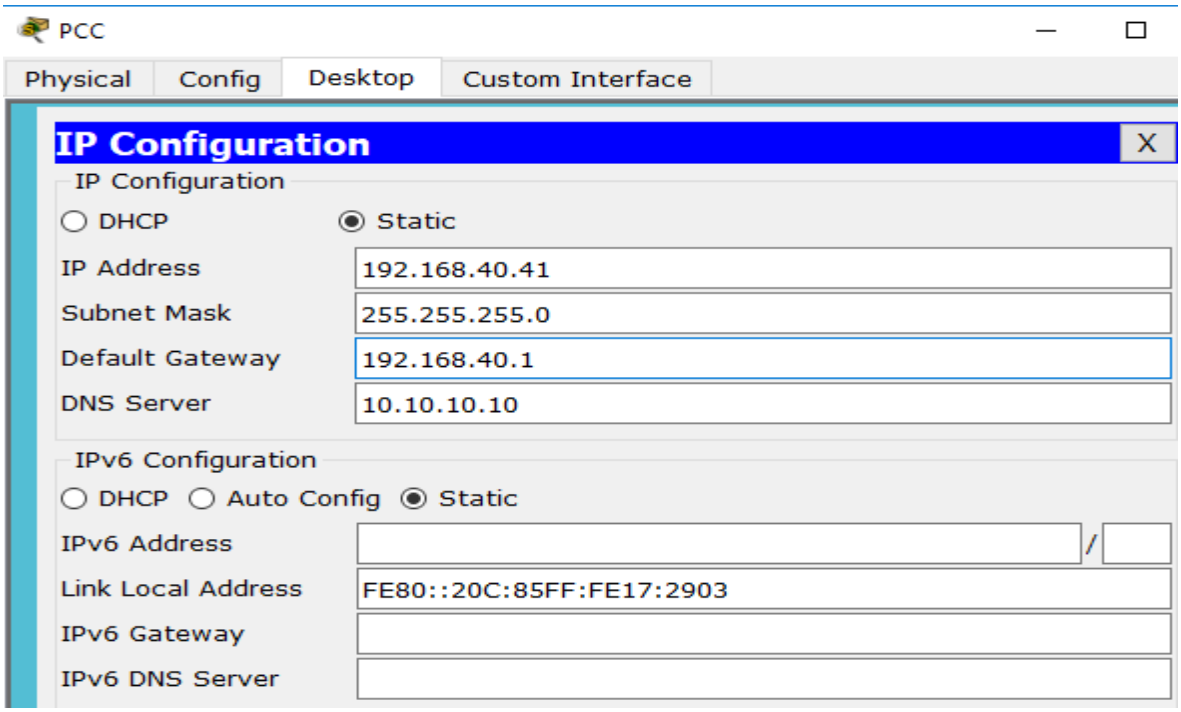


Figura 7. Configuración de la PCC.



R1 configuracion CLI:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BOGOTA
BOGOTA(config)#no ip domain-lookup
BOGOTA(config)#enable secret class
BOGOTA(config)#line con 0
BOGOTA(config-line)#pass cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#line vty 0 4
BOGOTA(config-line)#pass cisco
BOGOTA(config-line)#login
BOGOTA(config-line)#exit
BOGOTA(config)#service password-encryption
BOGOTA(config)#banner motd $Unathorized Access is Prohibited$
BOGOTA(config)#int s0/0
BOGOTA(config-if)#ip address 172.31.21.1 255.255.255.252
BOGOTA(config-if)#no sh
```

R2 configuracion CLI:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname MIAMI
MIAMI(config)#no ip domain-lookup
MIAMI(config)#enable secret class
MIAMI(config)#line con 0
MIAMI(config-line)#pass cisco
MIAMI(config-line)#login
MIAMI(config-line)#line vty 0 4
MIAMI(config-line)#pass cisco
MIAMI(config-line)#login
MIAMI(config-line)#exit
MIAMI(config)#service password-encryption
MIAMI(config)#banner motd $Unathorized Access is Prohibited$
MIAMI(config)#int s0/1/0
MIAMI(config-if)#ip address 172.31.21.2 255.255.255.252
MIAMI(config-if)#no sh
MIAMI(config-if)#int s0/0/0
MIAMI(config-if)#ip address 172.31.23.1 255.255.255.252
MIAMI(config-if)#clock rate 128000
MIAMI(config-if)#no sh
```

R3 configuracion CLI:

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname BUENOS-AIRES
BUENOS-AIRES(config)#no ip domain-lookup
BUENOS-AIRES(config)#enable secret class
BUENOS-AIRES(config)#line con 0
BUENOS-AIRES(config-line)#pass cisco
BUENOS-AIRES(config-line)#login
BUENOS-AIRES(config-line)#line vty 0 4
BUENOS-AIRES(config-line)#pass cisco
BUENOS-AIRES(config-line)#login
BUENOS-AIRES(config-line)#exit
BUENOS-AIRES(config)#service password-encryption
BUENOS-AIRES(config)#banner motd $Unathorized Access is Prohibited$
BUENOS-AIRES(config)#int s0/1/0
BUENOS-AIRES(config-if)#ip address 172.31.23.2 255.255.255.252
BUENOS-AIRES(config-if)#no sh
```

```
BUENOS-AIRES(config)#int lo4
BUENOS-AIRES(config-if)#ip add 192.168.4.1 255.255.255.0
BUENOS-AIRES(config-if)#no sh
BUENOS-AIRES(config-if)#int lo5
BUENOS-AIRES(config-if)#ip add 192.168.5.1 255.255.255.0
BUENOS-AIRES(config-if)#no sh
BUENOS-AIRES(config-if)#int lo6
BUENOS-AIRES(config-if)#ip add 192.168.6.1 255.255.255.0
BUENOS-AIRES(config-if)#no sh
```

S1 configuracion CLI:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#host S1
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#pass cisco
S1(config-line)#line vty 0 4
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#exit
S1(config)#service password-encryption
S1(config)#banner motd $Unathorized Access is Prohibited$
S1(config)#exit
```

S3 configuracion CLI:

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#host S3
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#pass cisco
S3(config-line)#line vty 0 4
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#exit
S3(config)#service password-encryption
S3(config)#banner motd $Unathorized Access is Prohibited$
S3(config)#exit
```

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

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

ROUTER ID R1:

```
BOGOTA>en
Password:
BOGOTA#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOGOTA(config)#router ospf 1
BOGOTA(config-router)#router-id 1.1.1.1
BOGOTA(config-router)#network 172.31.21.0 0.0.0.3 area 0
BOGOTA(config-router)#network 192.168.30.0 0.0.0.3 area 0
BOGOTA(config-router)#network 192.168.40.0 0.0.0.3 area 0
BOGOTA(config-router)#network 192.168.30.0 0.0.0.255 area 0
BOGOTA(config-router)#network 192.168.40.0 0.0.0.255 area 0
BOGOTA(config-router)#network 192.168.200.0 0.0.0.255 area 0
BOGOTA(config-router)#auto-cost reference-bandwidth 9500
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
BOGOTA(config-router)#exit
BOGOTA(config)#int s0/0/0
BOGOTA(config-if)#bandw 256
BOGOTA(config-if)#ip ospf cost 9500
```

ROUTER ID R2:

```
MIAMI>en
Password:
MIAMI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MIAMI(config)#router ospf 1
MIAMI(config-router)#router-id 5.5.5.5
MIAMI(config-router)#network 172.31.21.0 0.0.0.3 area 0
```

MIAMI(config-router)#network 172.31.23.0 0.0.0.3 area 0
MIAMI(config-router)#network 10.10.10.0 0.0.0.255 area 0
MIAMI(config-router)#auto-cost reference-bandwidth 9500
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
MIAMI(config-router)#int s0/0/0
MIAMI(config-if)#bandw 256
MIAMI(config-if)#int s0/1/0
MIAMI(config-if)#bandw 256
MIAMI(config-if)#ip ospf cost 9500

MIAMI(config-if)#exit

ROUTER ID R3:

BUENOS-AIRES#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BUENOS-AIRES(config)#router ospf 1
BUENOS-AIRES(config-router)#router-id 8.8.8.8
BUENOS-AIRES(config-router)#network 172.31.23.0 0.0.0.3 area 0
BUENOS-AIRES(config-router)#network 192.168.4.0 0.0.3.255 area 0
BUENOS-AIRES(config-router)#passive-interface lo4
BUENOS-AIRES(config-router)#passive-interface lo5
BUENOS-AIRES(config-router)#passive-interface lo6
BUENOS-AIRES(config-router)#auto-cost reference-bandwidth 9500
% OSPF: Reference bandwidth is changed.
Please ensure reference bandwidth is consistent across all routers.
BUENOS-AIRES(config-router)#exit
BUENOS-AIRES(config)#int s0/1/0
BUENOS-AIRES(config-if)#bandwidth 256

BUENOS-AIRES(config-if)#exit

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

Figura 8. Tablas de enrutamiento y routers conectados por OSPFv2 en Buenos Aires.

```
BUENOS-AIRES#sh ip ospf neig

Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           0   FULL/  -        00:00:30    172.31.23.1     Serial0/1/0
BUENOS-AIRES#
```

Figura 9. Tablas de enrutamiento y routers conectados por OSPFv2 en Bogotá.

```
BOGOTA#sh ip ospf neig

Neighbor ID     Pri   State           Dead Time   Address         Interface
5.5.5.5           0   FULL/  -        00:00:34    172.31.21.2     Serial0/0/0
BOGOTA#
```

Figura 10. Tablas de enrutamiento y routers conectados por OSPFv2 en Miami.

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.6.1       0   FULL/  -        00:00:35    172.31.23.2     Serial0/0/0
1.1.1.1           0   FULL/  -        00:00:36    172.31.21.1     Serial0/1/0
MIAMI#
```

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

Figura 11. Lista resumida de interfaces por OSPF.

```
MIAMI#sh ip ospf int

Serial0/1/0 is up, line protocol is up
  Internet address is 172.31.21.2/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT, Cost: 9500
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1 , Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1
  Suppress hello for 0 neighbor(s)
Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.23.1/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT, Cost: 6152
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
 --More--
```

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

Figura 12. OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.

```
!
router ospf 1
 router-id 5.5.5.5
 log-adjacency-changes
 auto-cost reference-bandwidth 9500
 network 172.31.21.0 0.0.0.3 area 0
 network 172.31.23.0 0.0.0.3 area 0
 network 10.10.10.0 0.0.0.255 area 0
!
```

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

SWITCH 1:

S1>en
Password:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#exit
S1(config-if)#int vlan 200
S1(config-if)#ip add 192.168.99.2 255.255.255.0
S1(config-if)#no sh
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1

S1(config)#int range fa0/2, fa0/4-23

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

SWITCH 3:
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 30
S3(config-vlan)#name Administracion
S3(config-vlan)#vlan 40
S3(config-vlan)#name Mercadeo
S3(config-vlan)#vlan 200
S3(config-vlan)#name Mantenimiento
S3(config-vlan)#exit
S3(config)#vlan 200
S3(config-vlan)#exit
S3(config)#int vlan 200
S3(config-if)#
S3(config-if)#ip add 192.168.99.3 255.255.255.0
S3(config-if)#no sh
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1

3. En el Switch 3 deshabilitar DNS lookup

SWITCH 3:
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#no ip domain-lookup

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

SWITCH 1:
S1(config-if)#int vlan 200
S1(config-if)#ip add 192.168.99.2 255.255.255.0
S1(config-if)#no sh
S1(config-if)#exit

SWITCH 3:

S3(config)#int vlan 200
S3(config-if)#
S3(config-if)#ip add 192.168.99.3 255.255.255.0
S3(config-if)#no sh
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.99.1

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

SWITCH 1:
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int range fa0/2, fa0/4-23

S1(config-if-range)#sh

SWITCH 3:
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#int range fa0/2, fa0/4-24
S3(config-if-range)#sh

6. Implement DHCP and NAT for IPv4

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

8. 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.

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

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

10. 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.

```
MIAMI#conf t
Enter configuration commands, one per line. End with CNTL/Z.
MIAMI(config)#access-list 1 permit 192.168.30.0 0.0.0.255
MIAMI(config)#access-list 1 permit 192.168.40.0 0.0.0.255
MIAMI(config)#ip nat inside source static 10.10.10.10 209.165.200.229
MIAMI(config)#int g0/0
%Invalid interface type and number
MIAMI(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228
% Incomplete command.
MIAMI(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask
255.255.255.248
MIAMI(config)#ip nat inside source list 1 pool INTERNET
MIAMI(config)#
```

11. 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.

```
MIAMI(config)#access-list 101 permit tcp any host 209.165.200.229 eq www
MIAMI(config)#access-list 101 permit icmp any any echo-reply
MIAMI(config)#int s0/0/0
MIAMI(config-if)#ip access-group 101 out
MIAMI(config-if)#int s0/1/0
MIAMI(config-if)#ip access-group 101 out
```

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

Figura 13. Verificación.

```
MIAMI#sh access-lists
Standard IP access list 1
    10 permit 192.168.30.0 0.0.0.255
    20 permit 192.168.40.0 0.0.0.255
Extended IP access list 101
    10 permit tcp any host 209.165.200.229 eq www
    20 permit icmp any any echo-reply
```

3. CONCLUSIONES

Con el desarrollo de este trabajo se pusieron en practicas muchas habilidades las cuales fueron adquiridas durante este diplomado, desarrollando un muy buena idea en base a la codificación necesaria al momento de programar dispositivos en Red, también, de conocer cuales son los protocolos adecuados al momento de realizar una Red y brindarle mucha seguridad a ésta debido a que en el amplio mundo del Internet los sistemas pueden ser vulnerables ante cualquier ataque, se adquirió gran conocimiento y en base a ésto dar solución ante cualquier problemática de red o también, poder crear unad red, con ayuda de herramientas como packet tracer y otros softwares muy útiles en el mercado.

El protocolo DHCP ahorra tiempo gestionando direcciones IP en una red grande. El servicio DHCP se encuentra activo en un servidor donde se centraliza la administración de las direcciones IP de la red.

OSPF (Open Shortest Path First) es un protocolo de red que gestiona un sistema autónomo en áreas, utilizando el algorithmo de Dijkstra para calcular cuál es la ruta mas corta entre dos nodos, éstos nodos están compuesto por routers los cuales se dividen en áreas con la información pertinente al momento de entablecer una comunicación con el servidor.

4. REFERENCIAS BIBLIOGRAFICAS

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: 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

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

CISCO. (2014). Traducción de direcciones IP para IPv4. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module11/index.html#11.0.1.1

CISCO. (2014). OSPF de una sola área. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module8/index.html#8.0.1.1

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1

CISCO. (2014). Enrutamiento Dinámico. Principios de Enrutamiento y Conmutación. Recuperado de https://static-course-assets.s3.amazonaws.com/RSE50ES/module7/index.html#7.0.1.1