

SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

LUIS ANGEL ALZATE QUICENO

PROGRAMA DE INGENIERIA DE SISTEMAS
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
PALMIRA, diciembre 10 de 2018

SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA CISCO

LUIS ANGEL ALZATE QUICENO

Trabajo de grado presentado como requisito para optar al título de
INGENIERO DE SISTEMAS

Ingeniera Nancy Amparo Guaca Giron

PROGRAMA DE INGENIERIA DE SISTEMAS
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
PALMIRA, diciembre 10 de 2018

DEDICATORIA

Primero, dar gracias al todo poderoso, que me ha permitido terminar satisfactoriamente este diplomado.

Dedico con todo mi amor y cariño este trabajo a mis padres: Gilberto Alzate y Mariela Quiceno. A mis hermanos: Gloria Amparo Alzate, Juan Carlos Alzate y Sandra Milena Alzate; y a mi esposa e hijo: Angela Johana Escobar y Joan Sebastian Alzate, en quienes siempre encontré palabras de aliento y mucho apoyo.

AGRADECIMIENTOS

Mis más sinceros agradecimientos a mi querida universidad que me dio la oportunidad de cursar mi carrera en ella, a todos los directores y tutores en quienes siempre encontré una guía y apoyo incondicional durante mi carrera.

CONTENIDO

1. Introducción	8
2. Descripción general de la prueba de habilidades	9
3. Descripción de escenarios propuestos para la prueba de habilidades	10
3.1 Escenario 1	10
3.2 Situación.....	11
3.3 Actividades	11
3.3.1 SW1 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.	11
3.3.2 SW3 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.	13
3.3.3 Puertos que no se utilizan, deshabilitados.....	14
3.3.4 La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1. 15	
3.3.5 Laptop20, Laptop21, PC20, PC21, Laptop30, Laptop31, PC30 y PC31 deben obtener información IPv4 del servidor DHCP.	17
3.3.6 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.....	18
3.3.7 R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2.	19
3.3.8 R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.....	20
3.3.9 R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.....	20
3.3.10 El Servidor0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).....	21
3.3.11 La interfaz FastEthernet 0/0 del R3 también debe tener direcciones IPv4 e IPv6 configuradas (dual- stack).	21
3.3.12 R1, R2 y R3 intercambian información de routing mediante RIP versión 2. 22	
3.3.13 Verificación de 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	23

3.4	Escenario 2.....	27
3.4.1	Configuración de direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.....	28
3.4.2	Configuración de Routers.....	30
3.4.3	Configuración de Switches.....	32
3.4.4	Configuración de el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:	32
3.4.5	Lista resumida de interfaces por OSPF en donde se ilustra el costo de cada interface.....	36
3.4.6	Visualización de el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.....	37
3.4.7	Configurar VLANs, Puertos troncales, puertos de acceso, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida. 38	
3.4.8	Deshabilitación de DNS lookup en el Switch 3.	43
3.4.9	Asignación de direcciones IP a los Switches acorde a los lineamientos.....	43
3.4.10	Desactivación de todas las interfaces que no son utilizadas en el esquema de red.	44
3.4.11	Implementación DHCP and NAT for IPv4 y Configuración R1 como servidor DHCP para las VLANs 30 y 40.	44
3.4.12	Reservación las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.	45
3.4.13	Configuración NAT en R2 para permitir que los hosts puedan salir a internet. 46	
3.4.14	Configuración acces list tipo estándar y extendido R2.	46
3.4.15	Verificación de procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.	47
4.	Conclusiones.....	52
5.	Bibliografía	53

LISTA DE TABLAS

Tabla 1. Direccionamiento escenario 1	10
Tabla 2. Asignación de VLAN y de puertos escenario 1	11
Tabla 3. Enlaces troncales escenario 1.....	11
Tabla 4. OSPFv2 area 0	32

LISTA DE IMAGENES

Imagen 1. Topología escenario 1	10
Imagen 2. VLAN y puertos en SW2	13
Imagen 3. VLAN y puertos en SW3	14
Imagen 4. DHCP en Laptop 20, 21, PC 20 y 21	17
Imagen 5. DHCP en Laptop 30, 31, PC 30 y 31	18
Imagen 6. show ip nat translation	19
Imagen 7. show ip nat statistics.....	20
Imagen 8. Accesibilidad al Servidor0	21
Imagen 9. Ping de R2 a PC20, PC21, Laptop20 y Laptop21	23
Imagen 10. Ping de R3 a PC30, PC31, Laptop30 y Laptop31	24
Imagen 11. Ping de todos los terminales al ISP	25
Imagen 12. IPv6-Ping del Server0 a PC20, PC21, Laptop30 y Laptop31	26
Imagen 13. Escenario 2	27
Imagen 14. Topología en Packet Tracer	28
Imagen 15. Configuración PC-Internet.....	29
Imagen 16. Configuración Web Server.....	29
Imagen 17. OSPF en R1	35
Imagen 18. OSPF en R2.....	35
Imagen 19. OSPF en R3.....	35
Imagen 20. Interfaces por OSPF	36
Imagen 21. OSPF Process ID.....	37
Imagen 22. OSPF router.....	38
Imagen 23. Ping de R1 a R2.....	47
Imagen 24. Ping de R2 a R3.....	47
Imagen 25. Acceso desde PC-Internet a Web Server	48
Imagen 26. Ping de S1 a las VLAN	48
Imagen 27. Ping de S3 a las VLAN	49
Imagen 28. DHCP en PC-A	49
Imagen 29. DHCP en PC-C	50

Imagen 30. Ping de PC-A a PC-C.....	50
Imagen 31. Tracert del PC-A al PC Internet.....	51
Imagen 32. Tracert del PC-A al Web Server	51
Imagen 33. Tracert del PC-A al PC-Internet.....	51
Imagen 34. Tracert del PC-C a la Lo6	51

1. INTRODUCCIÓN

Actualmente con los grandes avances que ha generado la tecnología, es necesario que los futuros Ingenieros se instruyan para enfrentar los retos que implica dicho progreso y, es ahí donde radica la importancia de contar con los conocimientos teóricos y prácticos relacionados con las redes de datos. Es así como el diplomado de profundización de Cisco brinda las herramientas necesarias para lograr la preparación que se requiere para asumir un rol activo como ingenieros en el ambiente tecnológico.

En el presente informe de prácticas de laboratorio desarrolladas, se pretende comprender el análisis de modelos actuales de diseño de red, con el estudio de los módulos del diplomado de profundización de Cisco (CCNA) se trabajan los conceptos y tecnologías fundamentales en redes, tales como protocolos de enrutamiento RIP, listas de control de acceso (ACL), dhcp, servicios NAT y PAT etc. Para lograr un óptimo desarrollo del curso, se emplea la herramienta de simulación de Cisco (Packet Tracer) con la cual se desarrollan las actividades prácticas del curso.

De esta manera, se presenta a continuación el desarrollo del laboratorio final planteado como evaluación final de habilidades practicas del diplomado de profundización Cisco (CCNA), el cual fue trabajado en Packet Tracer aplicando los conceptos teóricos estudiados en dicho curso.

2. DESCRIPCIÓN GENERAL DE LA PRUEBA DE HABILIDADES

La evaluación denominada “Prueba de habilidades prácticas”, forma parte de las actividades evaluativas del Diplomado de Profundización CCNA, y busca identificar el grado de desarrollo de competencias y habilidades que fueron adquiridas a lo largo del diplomado. Lo esencial es poner a prueba los niveles de comprensión y solución de problemas relacionados con diversos aspectos de Networking.

Para esta actividad, el estudiante dispone de cerca de dos semanas para realizar las tareas asignadas en cada uno de los dos (2) escenarios propuestos, acompañado de los respectivos procesos de documentación de la solución, correspondientes al registro de la configuración de cada uno de los dispositivos, la descripción detallada del paso a paso de cada una de las etapas realizadas durante su desarrollo, el registro de los procesos de verificación de conectividad mediante el uso de comandos ping, traceroute, show ip route, entre otros.

Teniendo en cuenta que la Prueba de habilidades está conformada por dos (2) escenarios, el estudiante deberá realizar el proceso de configuración de usando cualquiera de las siguientes herramientas: Packet Tracer o GNS3.

3. DESCRIPCIÓN DE ESCENARIOS PROPUESTOS PARA LA PRUEBA DE HABILIDADES

3.1 ESCENARIO 1

Imagen 1. Topología escenario 1

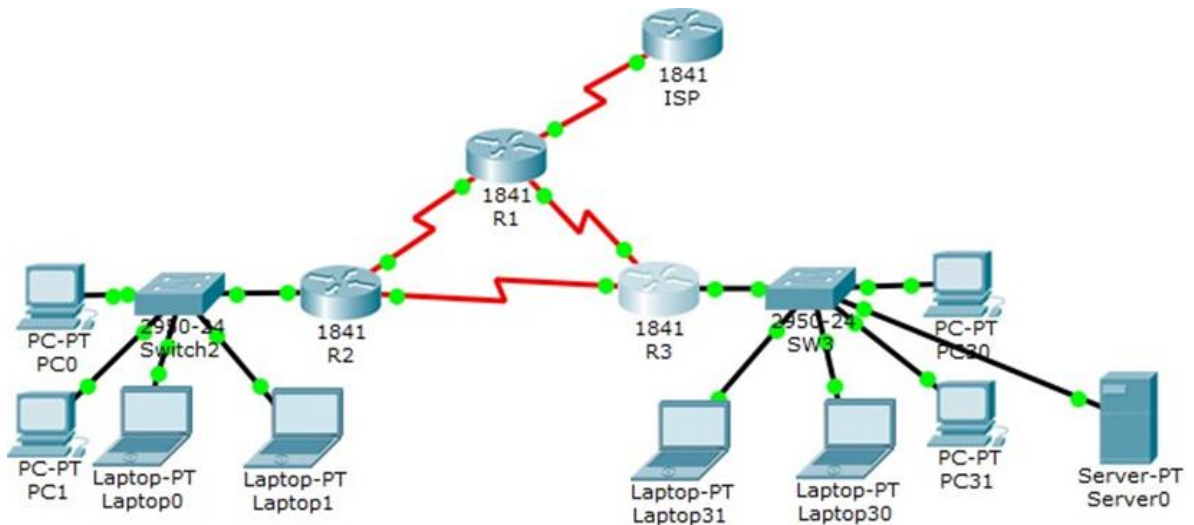


Tabla 1. Direccionamiento escenario 1

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
R2	Se0/1/1	10.0.0.5	255.255.255.252	N/D
	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
R3	Se0/0/1	10.0.0.9	255.255.255.252	N/D
	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 2. Asignación de VLAN y de puertos escenario 1

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

Tabla 3. Enlaces troncales escenario 1

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

3.2 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.

3.3 ACTIVIDADES

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

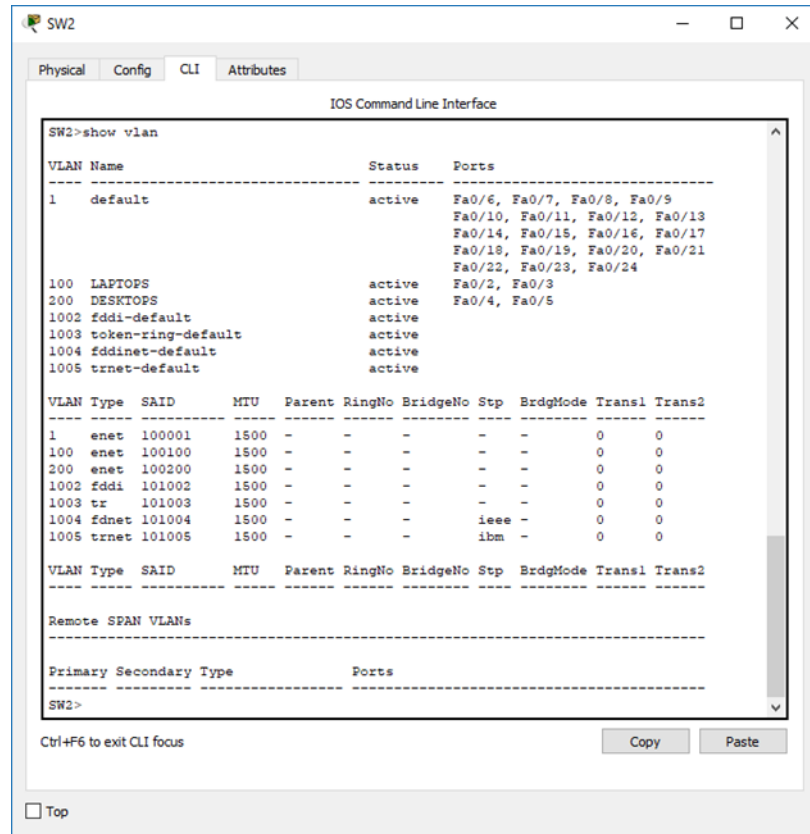
3.3.1.1 Creación de VLAN.

```
SW2>enable
SW2#conf t
SW2(config)#vlan 100
SW2(config-vlan)#name LAPTOPS
SW2(config-vlan)#exit
SW2(config)#vlan 200
SW2(config-vlan)#name DESTOPS
SW2(config-vlan)#end
SW2#wr
Building configuration...
[OK]
```

3.3.1.2 Asignación de puertos a las VLAN.

```
SW2(config)#interface range f0/2-3
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 100
SW2(config-if-range)#interface range f0/4-5
SW2(config-if-range)#switchport mode access
SW2(config-if-range)#switchport access vlan 200
SW2#wr
```

Imagen 2. VLAN y puertos en SW2



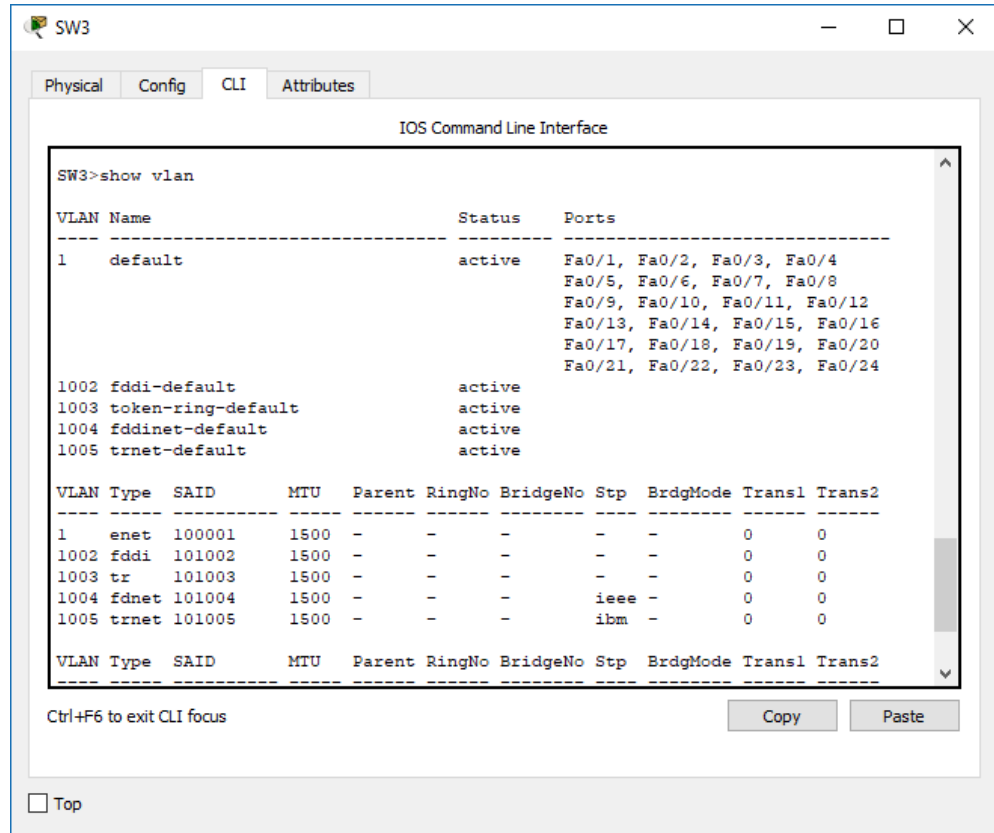
3.3.2 SW3 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 1.

3.3.2.1 Creación de VLAN.

```
SW3>enable
SW3#conf t
SW3(config)#vlan 1
SW3(config-vlan)#exit
SW3(config)#interface range f0/1-24
SW3(config-if-range)#switchport mode access
SW3(config-if-range)#switchport access vlan 1
SW3(config-if-range)#end
SW3#wr
```

[OK]
SW3#

Imagen 3. VLAN y puertos en SW3



3.3.3 Puertos que no se utilizan, deshabilitados.

SW2

SW2>enable

SW2#configure terminal

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

SW2(config)#interface range f0/6-24

SW2(config-if-range)#shutdown

SW2#wr

[OK]

SW2#


```
SW3
SW3>enable
SW3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW3(config)#interface range f0/6-23
SW3(config-if-range)#shutdown
SW3#wr
[OK]
```

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

3.3.4.1 Configuración R1.

```
R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0/0
R1(config-if)#ip address 200.123.211.2 255.255.255.0
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#wr
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
R1#
```

3.3.4.2 Configuración R2

```
R2>enable
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int f0/0.100
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)#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
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)#end
R2#wr
```

3.3.4.3 Configuración R3

```
R3>enable
R3#configure terminal
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 10.0.0.6 255.255.255.252
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)#end
```

```
R3#wr
```

```
[OK]
```

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

Imagen 4. DHCP en Laptop 20, 21, PC 20 y 21

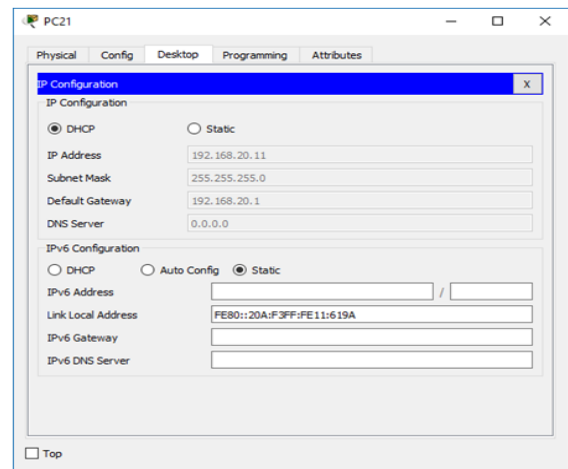
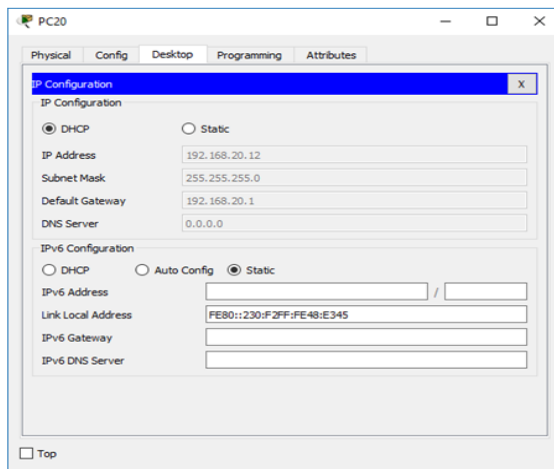
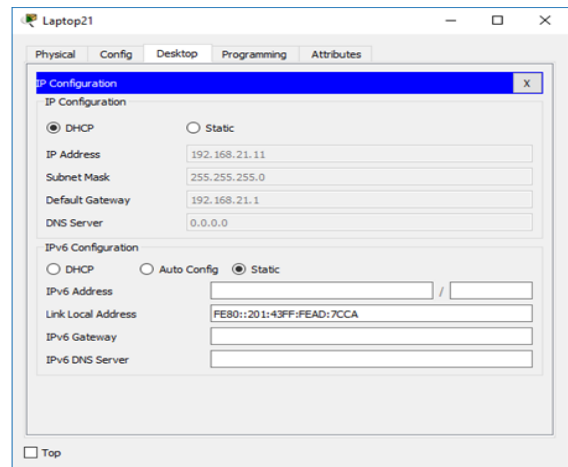
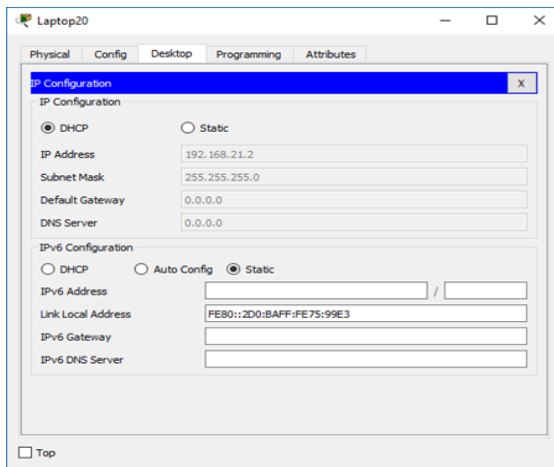
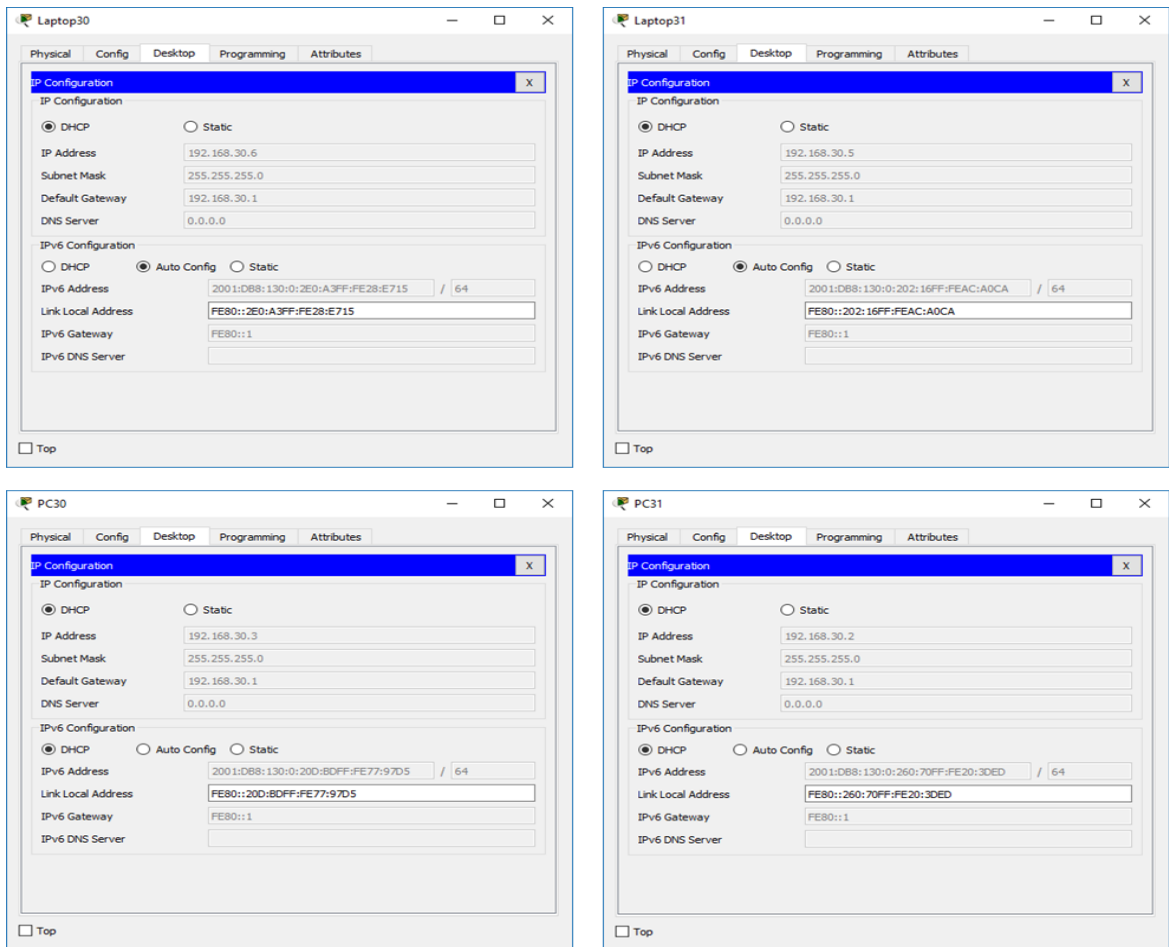


Imagen 5. DHCP en Laptop 30, 31, PC 30 y 31



3.3.6 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>enable
```

```
R1#configure terminal
```

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 inside
R1(config-if)#exit
R1(config)#ip nat pool INSIDE-DEVS 200.123.211.2 200.123.211.128 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

```

Imagen 6. show ip nat translation

```

R1>show ip nat translation
Pro  Inside global    Inside local    Outside local    Outside global
tcp  200.123.211.1:80  192.168.30.6:80  ---             ---
R1>

```

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

```

R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 10.0.0.0
R1(config-router)#network 10.0.0.4
R1(config-router)#end
R1#wr
[OK]

```

Imagen 7. show ip nat statistics

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

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

```
R2>enable
```

```
R2#configure terminal
```

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)#default-router 192.168.1.1
```

```
R2(dhcp-config)#dns-server 0.0.0.0
```

```
R2(dhcp-config)#exit
```

```
R2(config)#
```

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

```
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
```

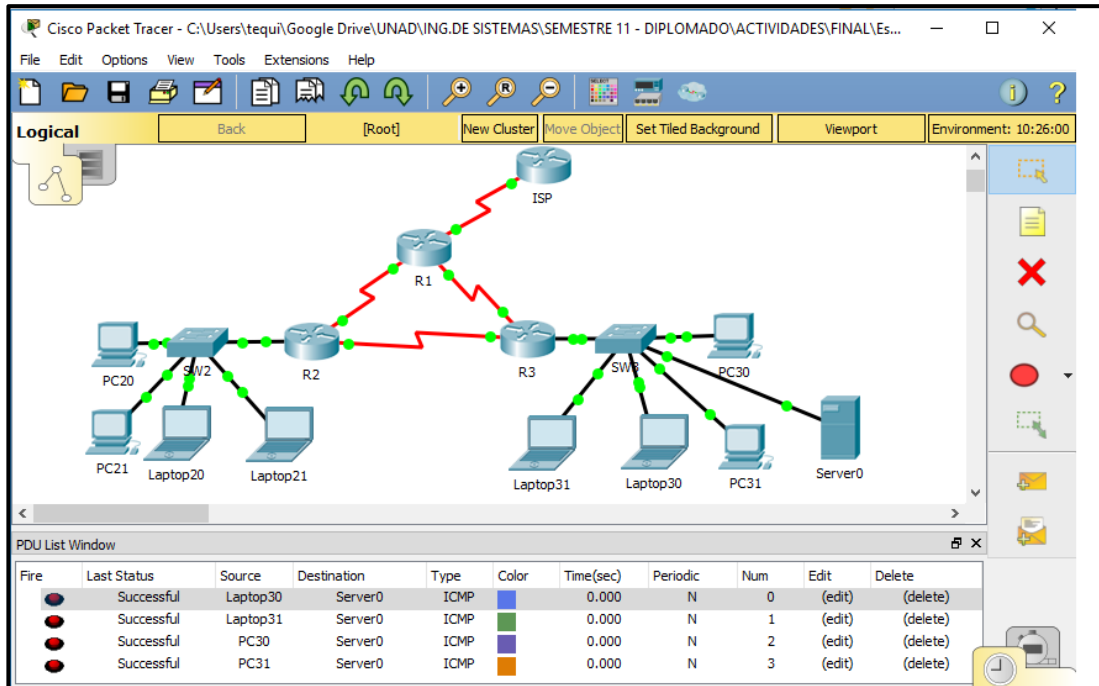
```
R2(config-if)#end
```

```
R2#wr
```

```
[OK]
```

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

Imagen 8. Accesibilidad al Servidor0



3.3.11 La interfaz FastEthernet 0/0 del R3 también debe tener direcciones IPv4 e IPv6 configuradas (dual- stack).

```
R3>enable
```

```
R3#configure terminal
```

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
```

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

R1

```
R1>enable
```

```
R1#configure terminal
```

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

```
R1(config)#router rip
```

```
R1(config-router)#version 2
```

```
R1(config-router)#network 10.0.0.0
```

```
R1(config-router)#network 10.0.0.4
```

```
R1(config-router)#end
```

```
R1#wr
```

```
[OK]
```

R2

```
R2>enable
```

```
R2#configure terminal
```

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)#end
```

```
R2#wr
```

```
[OK]
```

R3

```
R3>enable
```

```
R3#configure terminal
```

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#wr
[OK]

```

3.3.13 Verificación de 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.

Imagen 9. Ping de R2 a PC20, PC21, Laptop20 y Laptop21

The screenshot displays the Cisco Packet Tracer interface. The main workspace shows a network topology with routers R1, R2, R3, and an ISP. R2 is connected to R1, which is connected to the ISP. R2 is also connected to R3. R2 is connected to a switch SW2, which is connected to PC20, PC21, Laptop20, and Laptop21. R3 is connected to a switch SW3, which is connected to Laptop30, Laptop31, PC30, and PC31. Server0 is also connected to SW3. A red path highlights the connection from R2 to R1 and then to the ISP.

The PDU List Window at the bottom shows the following data:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	R2	PC20	ICMP		0.000	N	0	(edit)	(delete)
	Successful	R2	PC21	ICMP		0.000	N	1	(edit)	(delete)
	Successful	R2	Laptop20	ICMP		0.000	N	2	(edit)	(delete)
	Successful	R2	Laptop21	ICMP		0.000	N	3	(edit)	(delete)

The interface also shows a Realtime section with a Scenario 0 dropdown and buttons for New and Delete. The PDU List Window is currently visible and shows the results of the ping tests.

Imagen 10. Ping de R3 a PC30, PC31, Laptop30 y Laptop31

The screenshot displays the Cisco Packet Tracer interface. The main workspace shows a network topology with routers R1, R2, and R3, switches SW1 and SW2, and various end devices including PC20, PC21, Laptop20, Laptop21, Laptop31, Laptop30, PC30, PC31, and Server0. A red path indicates the route of the ping from R3 through R2 and R1 to the destination devices.

The PDU List Window at the bottom shows the following data:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	R3	PC30	ICMP	Red	0.000	N	0	(edit)	(delete)
	Successful	R3	PC31	ICMP	Green	0.000	N	1	(edit)	(delete)
	Successful	R3	Laptop30	ICMP	Purple	0.000	N	2	(edit)	(delete)
	Successful	R3	Laptop31	ICMP	Blue	0.000	N	3	(edit)	(delete)

The interface also shows the time as 24:46:29 and the Realtime mode selected. The PDU List Window is currently toggled on.

Imagen 11. Ping de todos los terminales al ISP

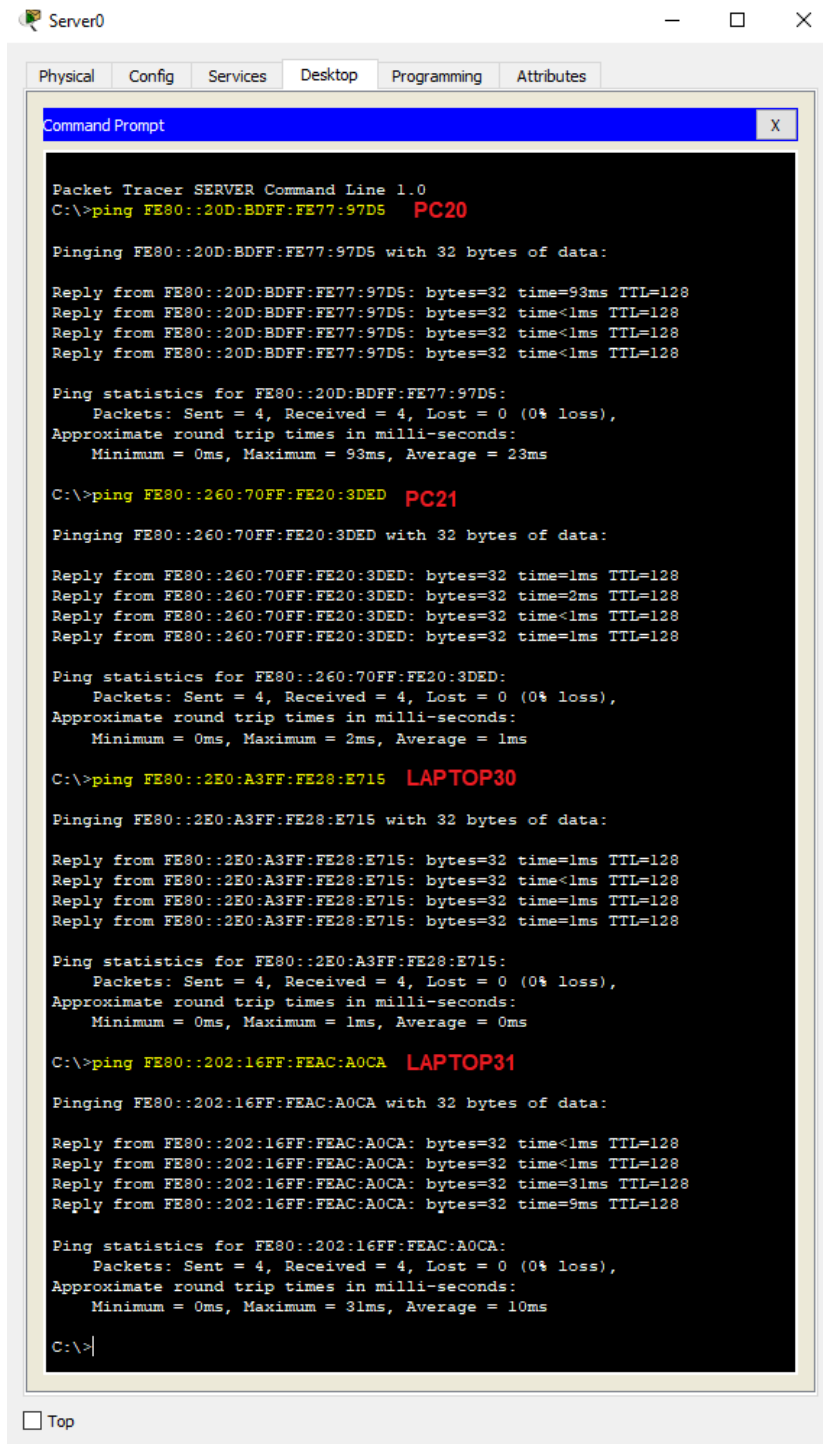
The screenshot displays the Cisco Packet Tracer interface. The main workspace shows a network topology with three routers (R1, R2, R3) and two switches (SW1, SW2). R1 is connected to an ISP. R2 is connected to SW2, which is connected to PC20, Laptop20, and Laptop21. R3 is connected to SW1, which is connected to Laptop31, Laptop30, PC31, and Server0. Red lines indicate the path of the ping requests from the various devices to the ISP.

The PDU List Window is open, showing a table of 10 successful ping events:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	R1	ISP	ICMP	Blue	0.000	N	0	(edit)	(delete)
	Successful	R2	ISP	ICMP	Purple	0.000	N	1	(edit)	(delete)
	Successful	R3	ISP	ICMP	Dark Blue	0.000	N	2	(edit)	(delete)
	Successful	PC20	ISP	ICMP	Teal	0.000	N	3	(edit)	(delete)
	Successful	PC21	ISP	ICMP	Light Green	0.000	N	4	(edit)	(delete)
	Successful	Laptop20	ISP	ICMP	Green	0.000	N	5	(edit)	(delete)
	Successful	Laptop21	ISP	ICMP	Light Green	0.000	N	6	(edit)	(delete)
	Successful	PC30	ISP	ICMP	Dark Green	0.000	N	7	(edit)	(delete)
	Successful	PC31	ISP	ICMP	Light Green	0.000	N	8	(edit)	(delete)
	Successful	Laptop30	ISP	ICMP	Light Green	0.000	N	9	(edit)	(delete)
	Successful	Laptop31	ISP	ICMP	Purple	0.000	N	10	(edit)	(delete)

The interface also shows the Realtime mode, a scenario named 'Scenario 0', and a PDU List Window toggle.

Imagen 12. IPv6-Ping del Server0 a PC20, PC21, Laptop30 y Laptop31



The screenshot shows a Packet Tracer window titled 'Server0' with a 'Command Prompt' tab. The command prompt displays the results of four IPv6 ping commands. Each command is followed by four replies and a summary of ping statistics. The destinations are PC20, PC21, LAPTOP30, and LAPTOP31.

```
Packet Tracer SERVER Command Line 1.0
C:\>ping FE80::20D:BDFF:FE77:97D5 PC20

Pinging FE80::20D:BDFF:FE77:97D5 with 32 bytes of data:

Reply from FE80::20D:BDFF:FE77:97D5: bytes=32 time=93ms TTL=128
Reply from FE80::20D:BDFF:FE77:97D5: bytes=32 time<1ms TTL=128
Reply from FE80::20D:BDFF:FE77:97D5: bytes=32 time<1ms TTL=128
Reply from FE80::20D:BDFF:FE77:97D5: bytes=32 time<1ms TTL=128

Ping statistics for FE80::20D:BDFF:FE77:97D5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 93ms, Average = 23ms

C:\>ping FE80::260:70FF:FE20:3DED PC21

Pinging FE80::260:70FF:FE20:3DED with 32 bytes of data:

Reply from FE80::260:70FF:FE20:3DED: bytes=32 time=1ms TTL=128
Reply from FE80::260:70FF:FE20:3DED: bytes=32 time=2ms TTL=128
Reply from FE80::260:70FF:FE20:3DED: bytes=32 time<1ms TTL=128
Reply from FE80::260:70FF:FE20:3DED: bytes=32 time=1ms TTL=128

Ping statistics for FE80::260:70FF:FE20:3DED:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\>ping FE80::2E0:A3FF:FE28:E715 LAPTOP30

Pinging FE80::2E0:A3FF:FE28:E715 with 32 bytes of data:

Reply from FE80::2E0:A3FF:FE28:E715: bytes=32 time=1ms TTL=128
Reply from FE80::2E0:A3FF:FE28:E715: bytes=32 time<1ms TTL=128
Reply from FE80::2E0:A3FF:FE28:E715: bytes=32 time=1ms TTL=128
Reply from FE80::2E0:A3FF:FE28:E715: bytes=32 time=1ms TTL=128

Ping statistics for FE80::2E0:A3FF:FE28:E715:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping FE80::202:16FF:FEAC:A0CA LAPTOP31

Pinging FE80::202:16FF:FEAC:A0CA with 32 bytes of data:

Reply from FE80::202:16FF:FEAC:A0CA: bytes=32 time<1ms TTL=128
Reply from FE80::202:16FF:FEAC:A0CA: bytes=32 time<1ms TTL=128
Reply from FE80::202:16FF:FEAC:A0CA: bytes=32 time=31ms TTL=128
Reply from FE80::202:16FF:FEAC:A0CA: bytes=32 time=9ms TTL=128

Ping statistics for FE80::202:16FF:FEAC:A0CA:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 31ms, Average = 10ms

C:\>
```

3.4 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.

Imagen 13. Escenario 2

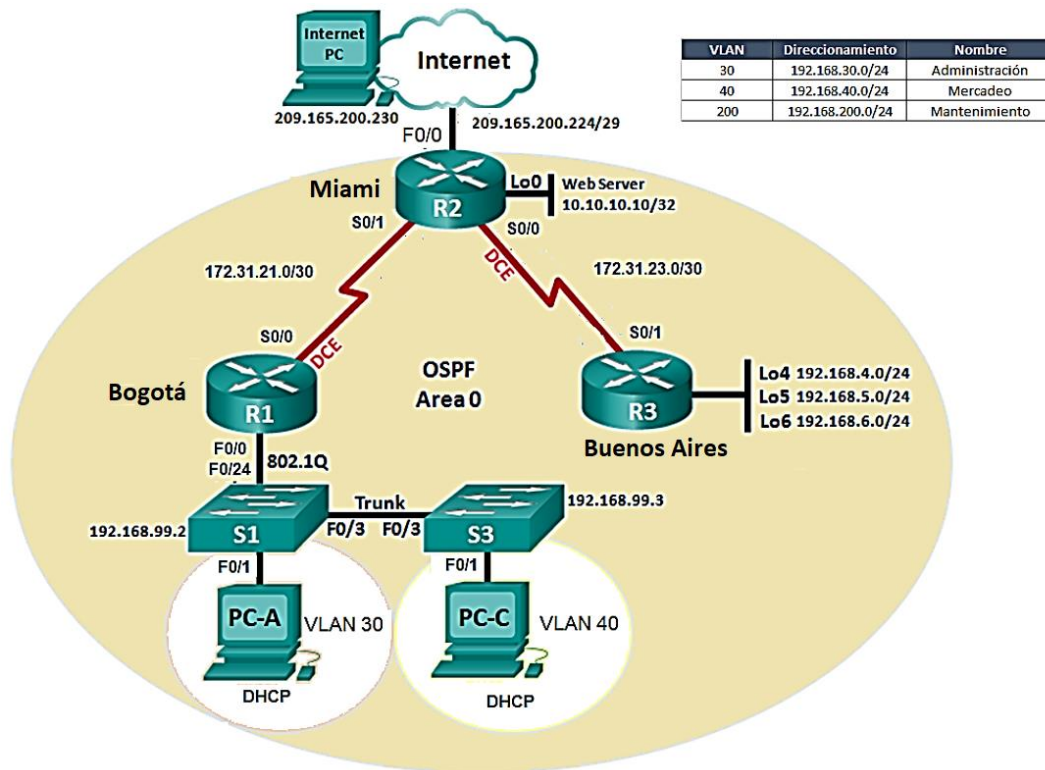
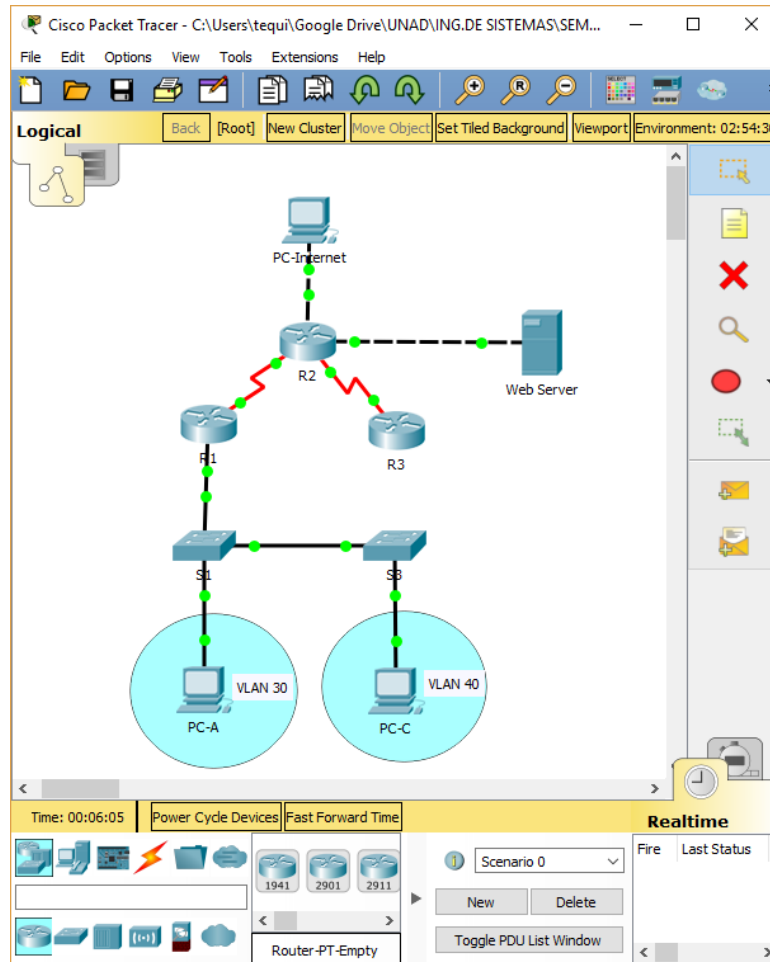


Imagen 14. Topología en Packet Tracer



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

Imagen 15. Configuración PC-Internet

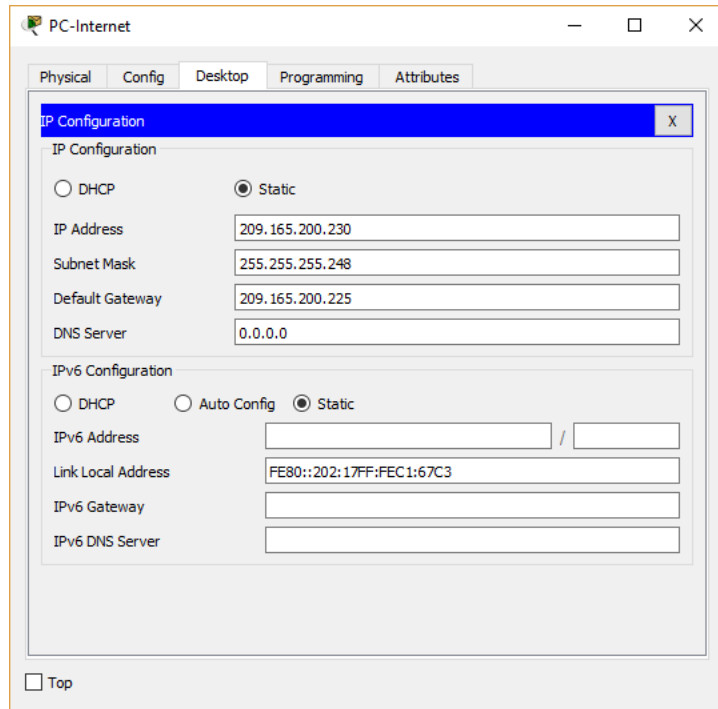
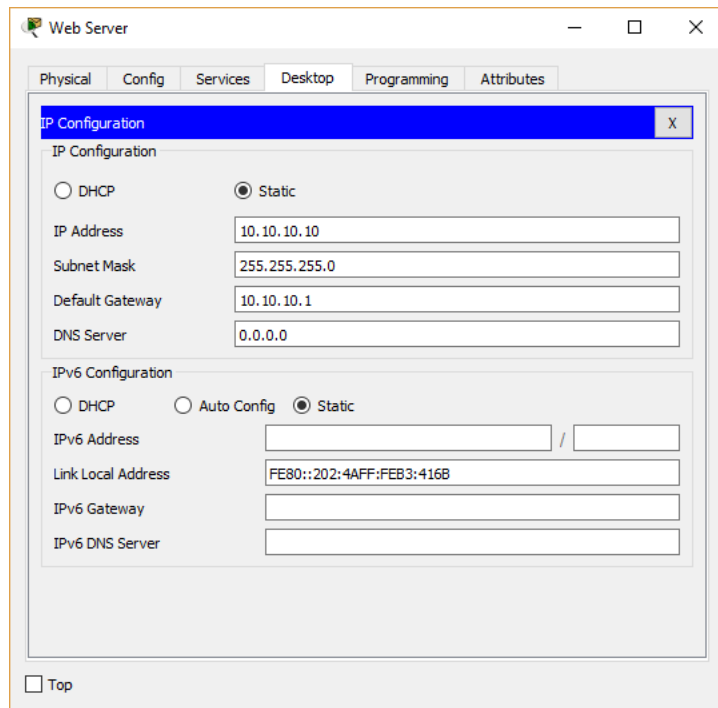


Imagen 16. Configuración Web Server



3.4.2 Configuración de Routers

R1

```
Router>en
```

```
Router#conf t
```

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

```
Router(config)#host R1
```

```
R1(config)#int s0/0/0
```

```
R1(config-if)#description connection to R2
```

```
R1(config-if)#ip add 172.31.21.1 255.255.255.252
```

```
R1(config-if)#clock rate 128000
```

This command applies only to DCE interfaces

```
R1(config-if)#no shut
```

R2

```
Router>en
```

```
Router#conf t
```

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

```
Router(config)#host R2
```

```
R2(config)#int s0/0/1
```

```
R2(config-if)#descrip connection to R1
```

```
R2(config-if)#ip add 172.31.21.2 255.255.255.252
```

```
R2(config-if)#no shut
```

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

```
R2(config-if)#descrip connection to R3
```

```
R2(config-if)#ip add 172.31.23.1 255.255.255.252
```

```
R2(config-if)#clock rate 128000
```

```
R2(config-if)#no shut
```

```
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
```

```
R2(config-if)#int f0/0
```

```
R2(config-if)#descrip internet
```

```
R2(config-if)#ip add 209.165.200.225 255.255.255.248
```



```
R2(config-if)#no shut
R2(config-if)#int f0/1
R2(config-if)#ip add 10.10.10.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#description connection to web server
R2(config-if)#exit
R2(config)#ip route 0.0.0.0 0.0.0.0 f0/0
```

R3

```
Router>en
```

```
Router#conf t
```

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

```
Router(config)#host R3
```

```
R3(config)#int s0/0/1
```

```
R3(config-if)#description connection to R2
```

```
R3(config-if)#ip add 172.31.23.2 255.255.252.252 Bad mask 0xFFFFCFC for
address 172.31.23.2
```

^

% Invalid input detected at '^' marker.

```
R3(config-if)#ip add 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)#exit
```

```
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
```

3.4.3 Configuración de Switches

S1

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)#

S3

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)#

3.4.4 Configuración de el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:

Tabla 4. 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

R1- OSPFv2 y encapsulamiento

R1>enable

R1#conf t

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

```
R1(config)#int f0/0.30
R1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.30, changed state to up
R1(config-subif)#description accounting LAN
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-subif)#exit
R1(config)#int f0/0.40
R1(config-subif)#description accounting LAN
R1(config-subif)#encapsulation dot1q 40
R1(config-subif)#ip address 192.168.40.1 255.255.255.0
%LINK-5-CHANGED: Interface FastEthernet0/0.40, changed state to up
R1(config-subif)#exit
R1(config)#int f0/0.200
R1(config-subif)#description accounting LAN
R1(config-subif)#encapsulation dot1q 200
R1(config-subif)#ip address 192.168.200.1 255.255.255.0
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)#passive-interface f0/0.30
%Invalid interface type and number
R1(config-router)#passive-interface f0/0.40
%Invalid interface type and number
R1(config-router)#passive-interface f0/0.200
%Invalid interface type and number
R1(config-router)#exit
R1(config)#int s0/0/0
```

```
R1(config-if)#bandwidth 256
R1(config-if)#ip ospf cost 9500
R1(config-if)#
```

R2

```
R2>en
```

```
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)#network 172.31.23.0 0.0.0.3 area 0
```

```
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
```

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

```
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
```

```
R2(config-router)#passive-interface f0/0
```

```
R2(config-router)#int s0/0/0
```

```
R2(config-if)#bandwidth 256
```

```
R2(config-if)#int s0/0/1
```

```
R2(config-if)#bandwidth 256
```

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

```
R2(config-if)#ip ospf cost 9500
```

```
R2(config-if)#
```

R3

```
R3>en
```

```
R3#conf 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 0.0.0.255 area 0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#exit
R3(config)#interface s0/0/1
R3(config-if)#bandwidth 256
R3(config-if)#

```

Imagen 17. OSPF en R1

```

R1#show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
Interface
5.5.5.5          0    FULL/ -         00:00:35   172.31.21.2
Serial0/0/0
R1#

```

Imagen 18. OSPF en R2

```

R2>show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
Interface
8.8.8.8          0    FULL/ -         00:00:39   172.31.23.2
Serial0/0/0
1.1.1.1          0    FULL/ -         00:00:31   172.31.21.1
Serial0/0/1
R2>

```

Imagen 19. OSPF en R3

```

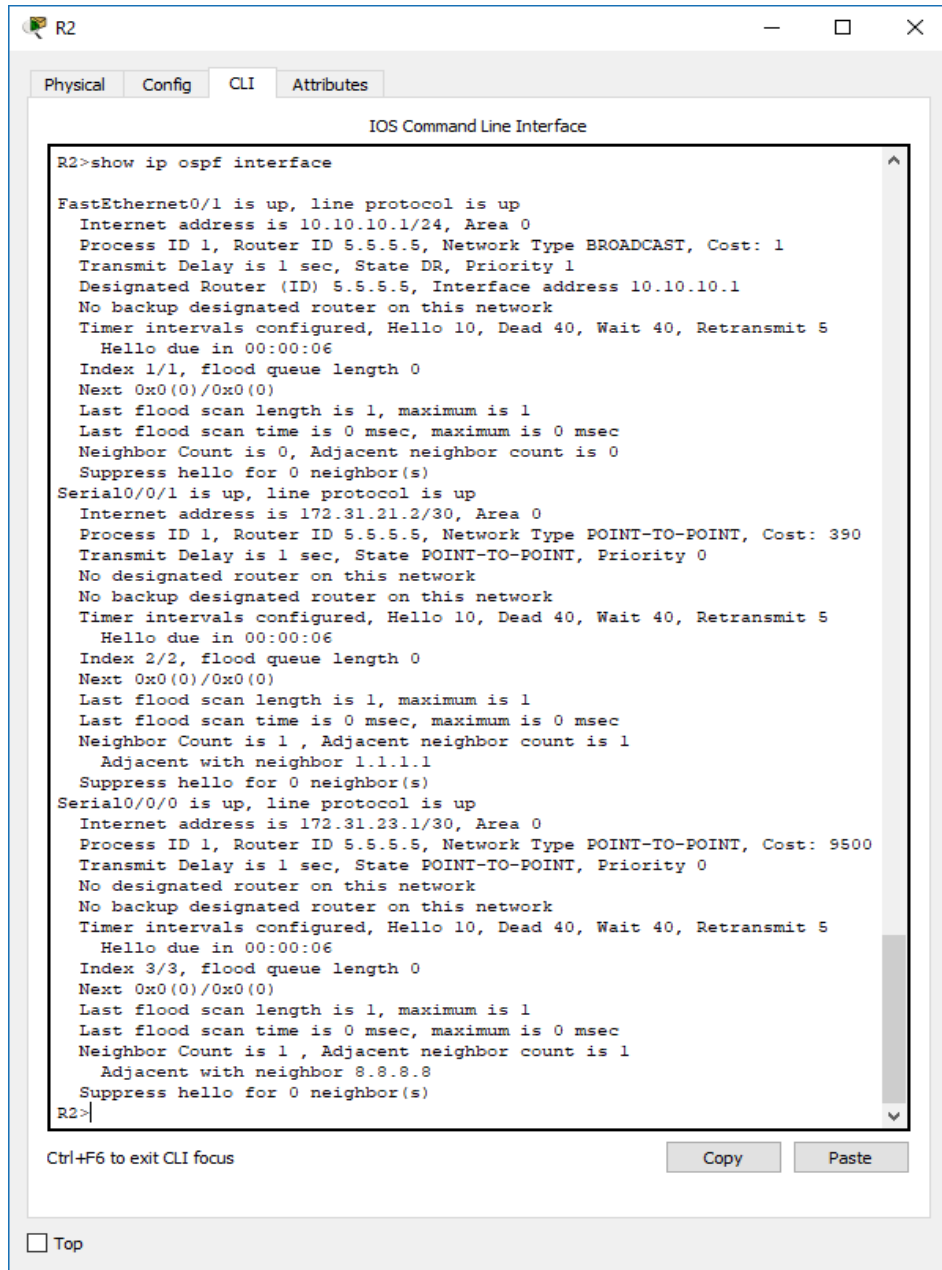
R3>show ip ospf neighbor

Neighbor ID      Pri   State           Dead Time   Address
Interface
5.5.5.5          0    FULL/ -         00:00:38   172.31.23.1
Serial0/0/1
R3>

```

3.4.5 Lista resumida de interfaces por OSPF en donde se ilustra el costo de cada interface.

Imagen 20. Interfaces por OSPF



```
R2>show ip ospf interface

FastEthernet0/1 is up, line protocol is up
 Internet address is 10.10.10.1/24, Area 0
 Process ID 1, Router ID 5.5.5.5, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State DR, Priority 1
 Designated Router (ID) 5.5.5.5, Interface address 10.10.10.1
 No backup designated router on this network
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
 Hello due in 00:00:06
 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 0, Adjacent neighbor count is 0
 Suppress hello for 0 neighbor(s)
Serial0/0/1 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: 390
 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 00:00:06
 Index 2/2, 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: 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, Retransmit 5
 Hello due in 00:00:06
 Index 3/3, 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 8.8.8.8
 Suppress hello for 0 neighbor(s)
R2>
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

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

Imagen 21. OSPF Process ID

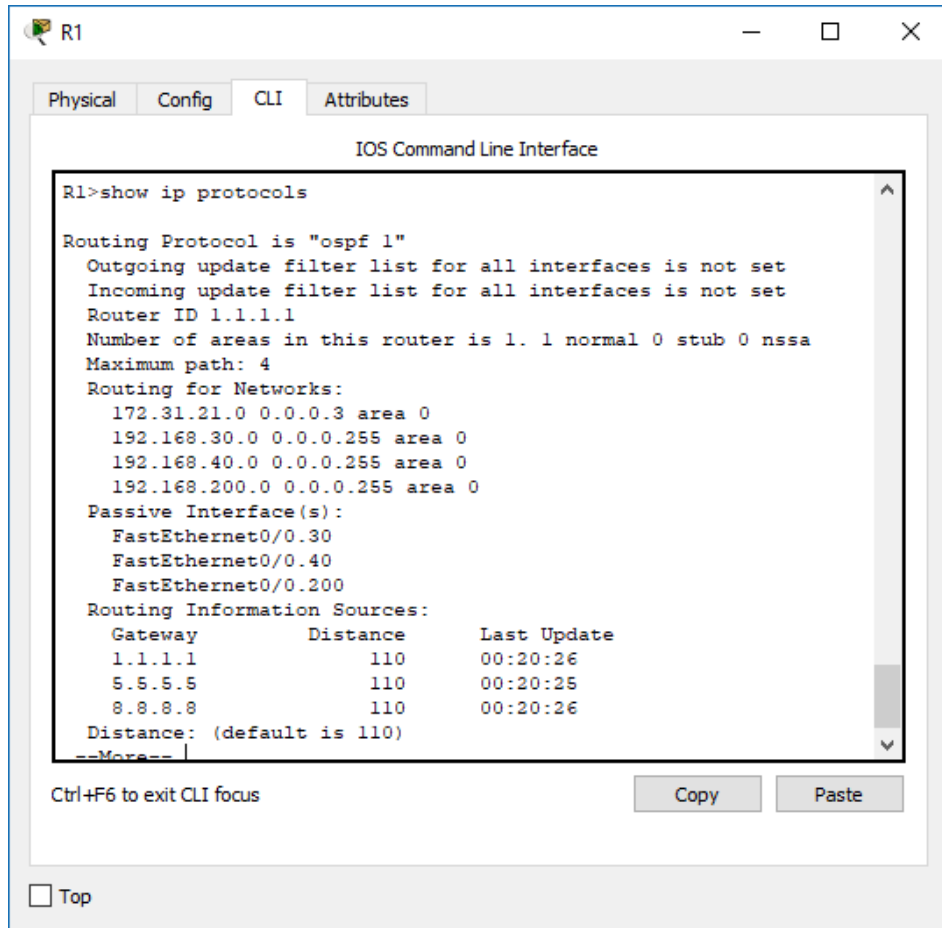
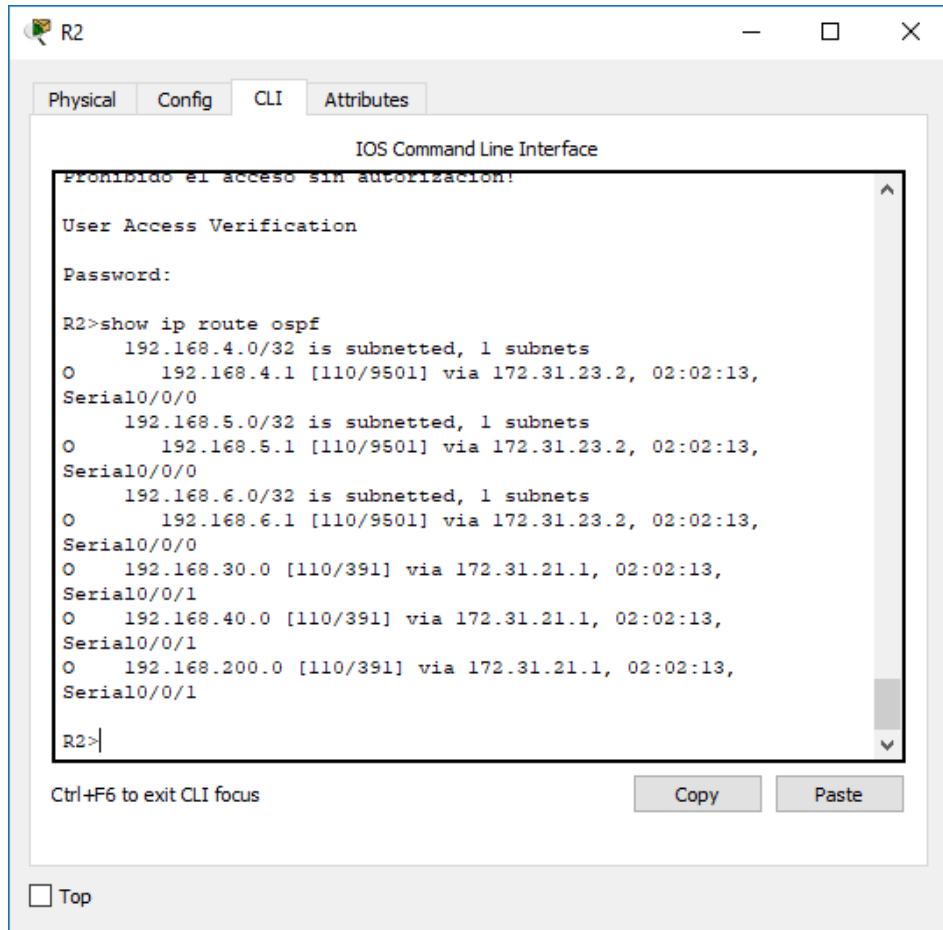


Imagen 22. OSPF router



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

3.4.7.1 Configuración de seguridad.

R1>en

R1#conf t

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

R1(config)#enable secret class

R1(config)#line con 0

R1(config-line)#pass cisco

R1(config-line)#login


```
R1(config-line)#line vty 0 4
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service pass
R1(config)#service password-encryption
R1(config)#banner motd $Prohibido el acceso sin autorizacion!$
R1(config)#
```

```
R2>en
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#enable secret class
R2(config)#line con 0
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#line vty 0 4
R2(config-line)#pass cisco
R2(config-line)#login
R2(config-line)#exit
R2(config)#service password-encryption
R2(config)#banner motd $Prohibido el acceso sin autorizacion!$
R2(config)#
```

```
R3>en
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#enable secret class
R3(config)#line con 0
R3(config-line)#pass cisco
R3(config-line)#login
```

```
R3(config-line)#line vty 0 4
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd $Prohibido el acceso sin autorizacion!$
R3(config)#
```

```
S1>en
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd "Prohibido el acceso sin autorizacion!"
S1(config)#no ip domain-lookup
S1(config)#
```

```
S3>en
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#enable secret class
S3(config)#line con 0
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#line vty 0 4
```

```
S3(config-line)#pass cisco
S3(config-line)#login
S3(config-line)#service password-encryption
S3(config)#banner motd "Prohibido el acceso sin autorizacion!"
S3(config)#no ip domain-lookup
S3(config)#
```

3.4.7.2 Cofiguración de VLANs.

```
S1>en
S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain-lookup
S1(config)#vlan 30
S1(config-vlan)#name Administratcion
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)#int vlan 200
S1(config-if)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.200.1
S1(config)#interface f0/3
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface f0/24
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#interface range fa0/1-2, fa0/4-24, GigabitEthernet0/1-2
```

```
S1(config-if-range)#switchport mode access
S1(config-if-range)#interface fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#interface range fa0/2, fa0/4-23, GigabitEthernet0/1-2
S1(config-if-range)#shutdown
```

```
S3>en
```

```
S3#conf term
```

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

```
S3(config)#hostname S3
```

```
S3(config)#no ip domain-lookup
```

```
S3(config)#vlan 30
```

```
S3(config-vlan)#name Administratcion
```

```
S3(config-vlan)#vlan 40
```

```
S3(config-vlan)#name Mercadeo
```

```
S3(config-vlan)#vlan 200
```

```
S3(config-vlan)#name Mantenimiento
```

```
S3(config-vlan)#exit
```

```
S3(config)#int vlan 200
```

```
S3(config-if)#ip address 192.168.200.3 255.255.255.0
```

```
S3(config-if)#no shut
```

```
S3(config-if)#exit
```

```
S3(config)#ip default-gateway 192.168.200.1
```

```
S3(config)#interface f0/3
```

```
S3(config-if)#switchport mode trunk
```

```
S3(config-if)#switchport trunk native vlan 1
```

```
S3(config-if)#interface range fa0/1-2, fa0/4-24, GigabitEthernet0/1-2
```

```
S3(config-if-range)#switchport mode access
```

```
S3(config-if-range)#interface fa0/1
```

```
S3(config-if)#switchport mode access
```

```
S3(config-if)#switchport access vlan 40
S3(config-if)#interface range fa0/2, fa0/4-24, GigabitEthernet0/1-2
S3(config-if-range)#shutdown
```

3.4.8 Deshabilitación de DNS lookup en el Switch 3.

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

3.4.9 Asignación de direcciones IP a los Switches acorde a los lineamientos.

```
S1>en
S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int vlan 200
S1(config-if)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.200.1
```

```
S3>en
S3#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#int vlan 200
S3(config-if)#ip address 192.168.200.3 255.255.255.0
S3(config-if)#no shut
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.200.1
```

3.4.10 Desactivación de todas las interfaces que no son utilizadas en el esquema de red.

```
S1>en
```

```
S1#conf term
```

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

```
S1(config)#interface range fa0/1-2, fa0/4-23, GigabitEthernet0/1-2
```

```
S1(config-if-range)#switchport mode access
```

```
S1(config-if-range)#interface fa0/1
```

```
S1(config-if)#switchport mode access
```

```
S1(config-if)#switchport access vlan 30
```

```
S1(config-if)#interface range fa0/2, fa0/4-23, GigabitEthernet0/1-2
```

```
S1(config-if-range)#shutdown
```

```
S3>en
```

```
S3#conf term
```

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

```
S3(config)#interface range fa0/1-2, fa0/4-24, GigabitEthernet0/1-2
```

```
S3(config-if-range)#switchport mode access
```

```
S3(config-if-range)#interface fa0/1
```

```
S3(config-if)#switchport mode access
```

```
S3(config-if)#switchport access vlan 40
```

```
S3(config-if)#interface range fa0/2, fa0/4-24, GigabitEthernet0/1-2
```

```
S3(config-if-range)#shutdown
```

3.4.11 Implementación DHCP and NAT for IPv4 y Configuración R1 como servidor DHCP para las VLANs 30 y 40.

```
R1>en
```

```
R1#conf t
```

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

```
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)#ip dhcp pool MERCADEO
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
```

3.4.12 Reservación las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.

```
R1>en
```

```
R1#conf t
```

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

```
R1(config)#ip dhcp excluded-address 192.168.31.1 192.168.31.30
R1(config)#ip dhcp excluded-address 192.168.31.1 192.168.31.30
R1(config)#no ip dhcp excluded-address 192.168.31.1 192.168.31.30
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)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#ip dhcp pool MERCADEO
R1(dhcp-config)#dns-server 10.10.10.11
```

```
R1(dhcp-config)#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
```

3.4.13 Configuración NAT en R2 para permitir que los hosts puedan salir a internet.

```
R2>en
```

```
R2#conf t
```

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

```
R2(config)#access-list 1 permit 192.168.30.1 0.0.0.255
```

```
R2(config)#access-list 1 permit 192.168.40.1 0.0.0.255
```

```
R2(config)#no access-list 1 permit 192.168.30.1 0.0.0.255
```

```
R2(config)#no access-list 1 permit 192.168.40.1 0.0.0.255
```

```
R2(config)#access-list 1 permit 192.168.30.0 0.0.0.255
```

```
R2(config)#access-list 1 permit 192.168.40.0 0.0.0.255
```

```
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
```

```
R2(config)#ip nat pool INTERNET 209.165.200.225 209.165.200.228 netmask  
255.255.255.248
```

```
R2(config)#ip nat inside source list 1 pool INTERNET
```

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
```

3.4.14 Configuración acces list tipo estándar y extendido R2.

```
R2>en
```

```
R2#conf t
```

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

```
R2(config)#access-list 101 permit tcp any host 209.165.200.229 eq www
```

```
R2(config)#access-list 101 permit icmp any any echo-reply
```

```
R2(config)#int f0/0
```

```
R2(config-if)#ip access-group 101 in
```



```
R2(config-if)#int s0/0/1
R2(config-if)#ip access-group 101 out
R2(config-if)#int s0/0/0
R2(config-if)#ip access-group 101 out
R2(config-if)#int f0/1
R2(config-if)#ip access-group 101 out
```

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

Imagen 23. Ping de R1 a R2

```
R1#ping 172.31.21.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/13 ms
```

Imagen 24. Ping de R2 a R3

```
R2#ping 172.31.23.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Imagen 25. Acceso desde PC-Internet a Web Server

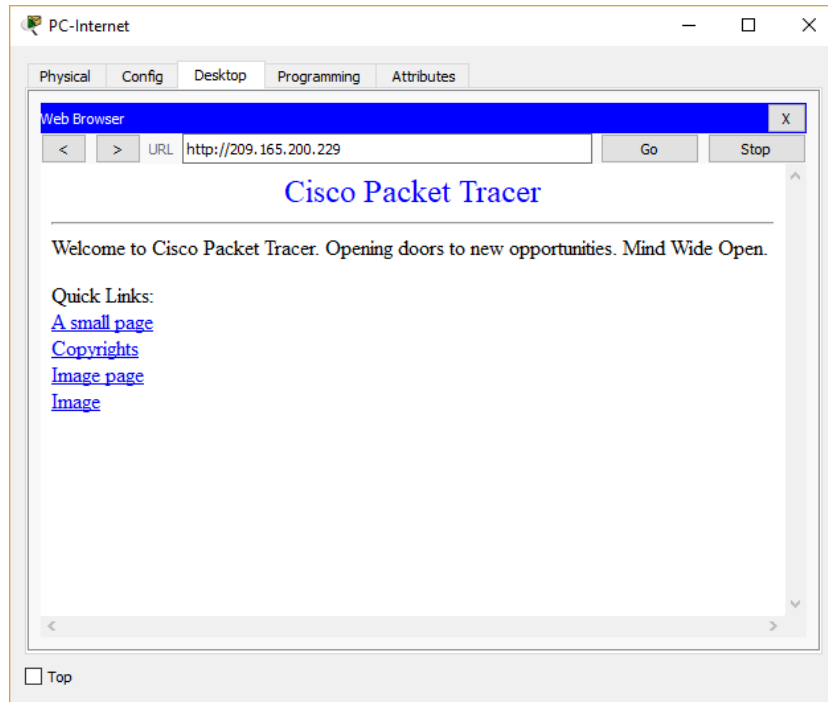


Imagen 26. Ping de S1 a las VLAN

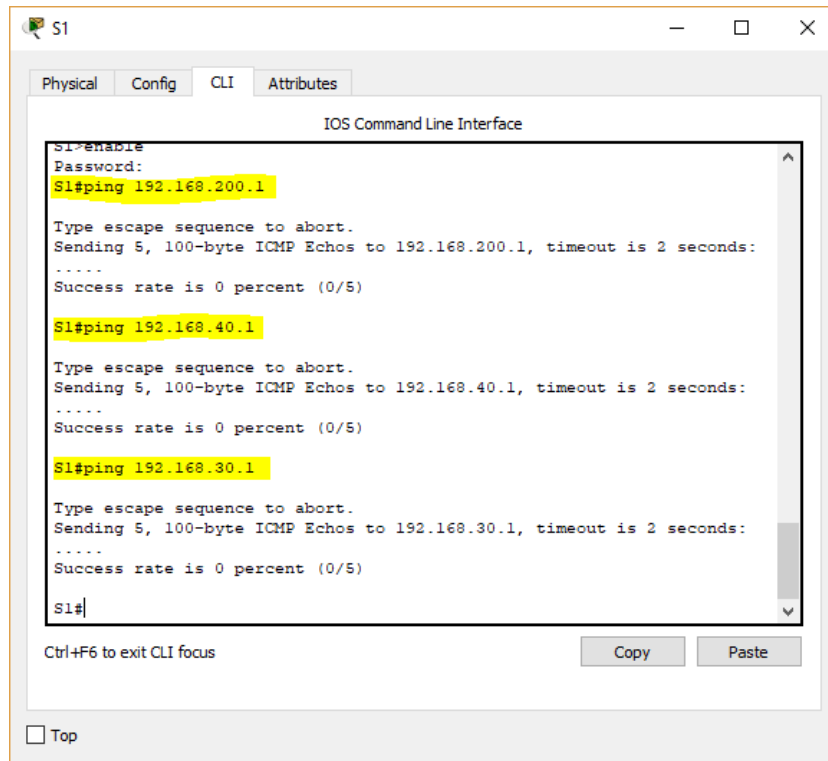


Imagen 27. Ping de S3 a las VLAN

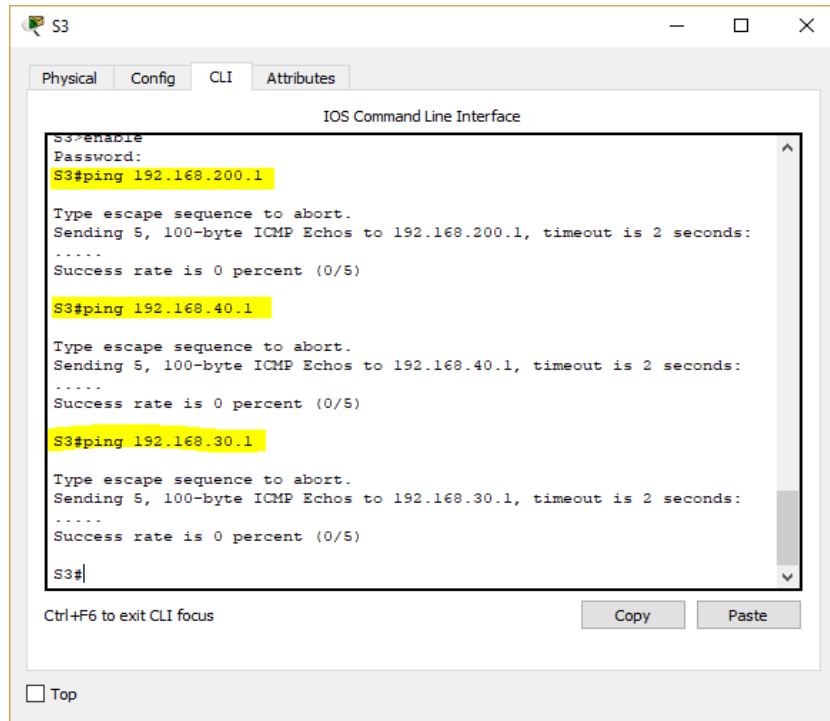


Imagen 28. DHCP en PC-A

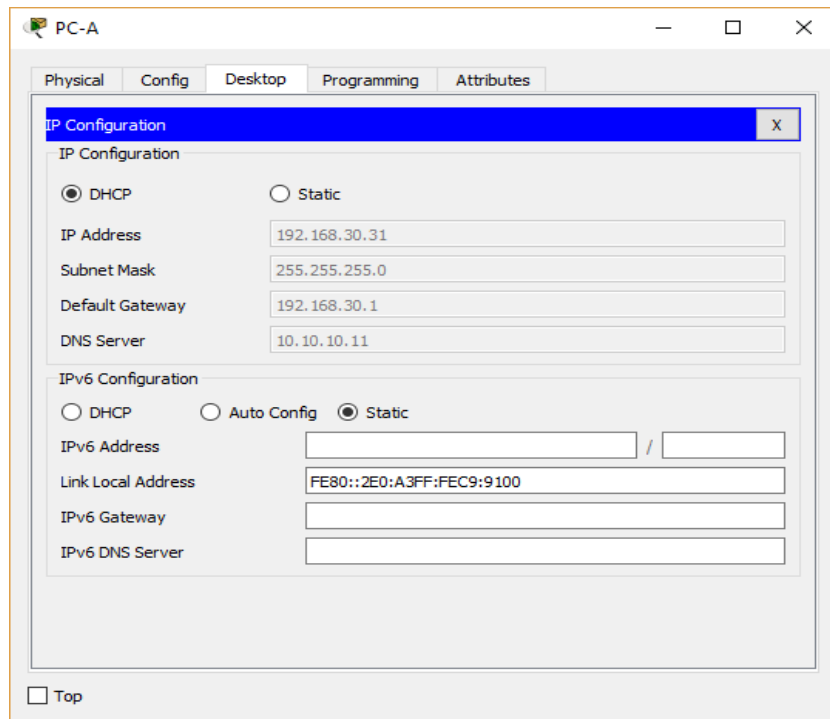


Imagen 29. DHCP en PC-C

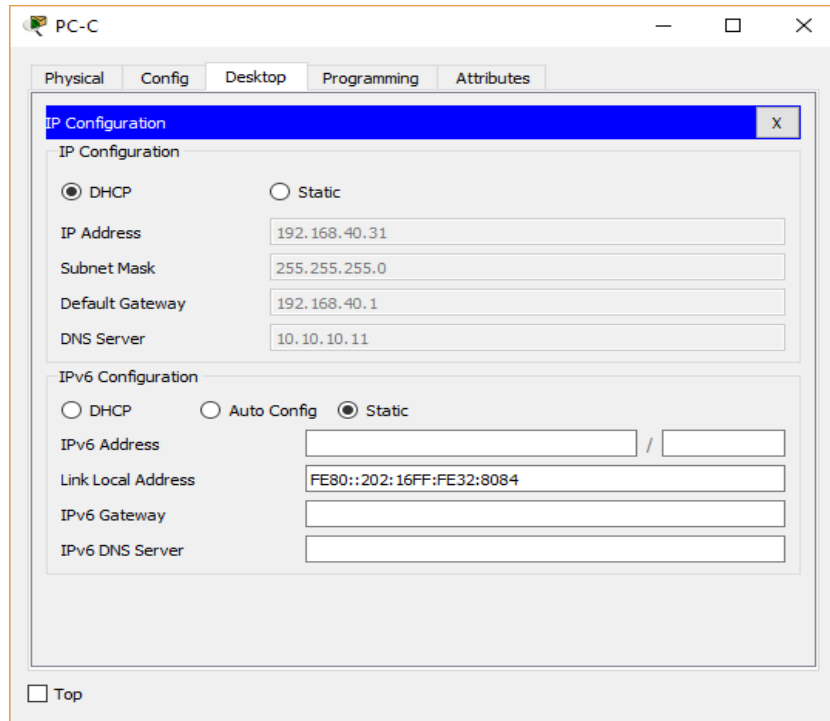


Imagen 30. Ping de PC-A a PC-C

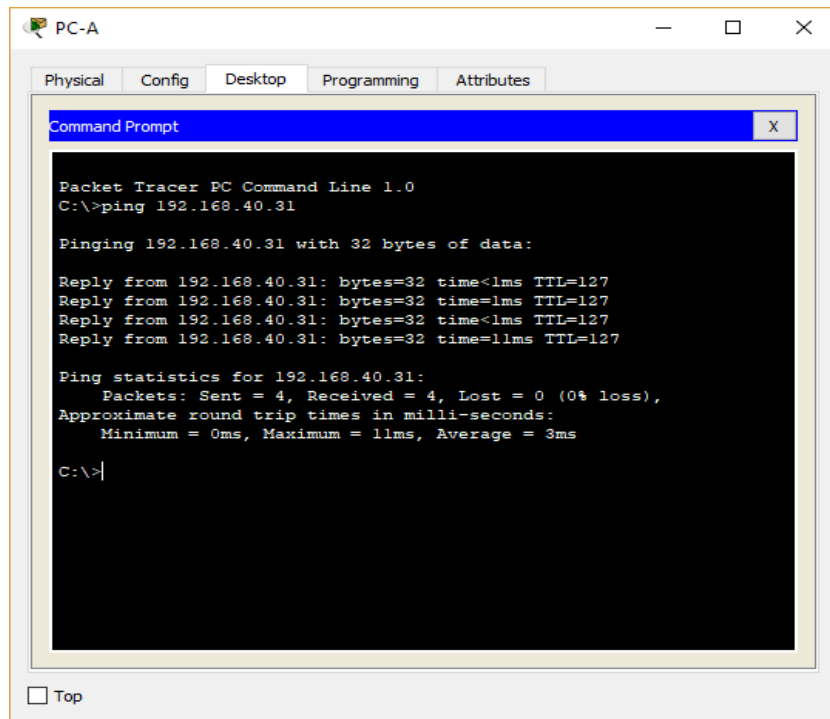


Imagen 31. Tracert del PC-A al PC Internet

```
C:\>tracert 192.168.40.31

Tracing route to 192.168.40.31 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.30.1
  2  0 ms    0 ms    0 ms    192.168.40.31

Trace complete.
```

Imagen 32. Tracert del PC-A al Web Server

```
C:\>tracert 10.10.10.10

Tracing route to 10.10.10.10 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.30.1
  2  0 ms    1 ms    11 ms   172.31.21.2
  3  10 ms   1 ms    0 ms    10.10.10.10

Trace complete.
```

Imagen 33. Tracert del PC-A al PC-Internet

```
C:\>tracert 209.165.200.230

Tracing route to 209.165.200.230 over a maximum of 30 hops:

  1  2 ms    0 ms    0 ms    192.168.30.1
  2  0 ms    0 ms    0 ms    172.31.21.2
  3  1 ms    1 ms    1 ms    209.165.200.230

Trace complete.
```

Imagen 34. Tracert del PC-C a la Lo6

```
C:\>tracert 192.168.6.1

Tracing route to 192.168.6.1 over a maximum of 30 hops:

  1  0 ms    0 ms    0 ms    192.168.40.1
  2  0 ms    0 ms    0 ms    172.31.21.2
  3  1 ms    0 ms    0 ms    192.168.6.1

Trace complete.
```

4. CONCLUSIONES

El DHCP actúa en un servidor el cual es el eje de la administración de las direcciones IP de la red. Está diseñado fundamentalmente para ahorrar tiempo gestionando direcciones IP en una red grande.

Los cambios en un área de la red no tienen por qué afectar en un todo, y buena parte del tráfico puede ser "parcelado" en su área. Esto debido a que las áreas son unidades de encaminamiento, o sea, todos los routers de la misma área contienen la misma información topológica en su base de datos de estado-enlace (Link State Database).

Las listas de control de acceso ((ACL) son las que permiten el acceso de direcciones IP específicas, de esta manera se asegura que solo la computadora del administrador tenga permiso para acceder al Router mediante telnet o SSH.

5. BIBLIOGRAFÍA

CISCO. (2014). Exploración de la red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module1/index.html#1.0.1.1>

CISCO. (2014). Configuración de un sistema operativo de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#2.0.1.1>

CISCO. (2014). Protocolos y comunicaciones de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#3.0.1.1>

CISCO. (2014). Acceso a la red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#4.0.1.1>

CISCO. (2014). Ethernet. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#5.0.1.1>

CISCO. (2014). Capa de red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module2/index.html#6.0.1.1>

CISCO. (2014). Capa de Transporte. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module7/index.html#7.0.1.1>

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1>

CISCO. (2014). SubNetting. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module9/index.html#9.0.1.1>

CISCO. (2014). Capa de Aplicación. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module10/index.html#10.0.1.1>

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de <https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1>

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>

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>

(2014). VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module3/index.html#3.0.1.1>

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>

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). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>

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

CISCO. (2014). Listas de control de acceso. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module9/index.html#9.0.1.1>

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

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