

**SOLUCIÓN DE ESTUDIOS DE CASO BAJO EL USO DE TECNOLOGÍA
CISCO**

PRESENTADO POR:

LUISA PATRICIA SANMIGUEL ROJAS

Código: 1069176088

Director: Juan Carlos Vesga

**Universidad Nacional Abierta y a Distancia
Escuela de Ciencias Básicas, Tecnología e Ingeniería
Ingeniería de Sistemas
2018**

CONTENIDO

INTRODUCCIÓN	5
Escenario 1	6
Tabla de direccionamiento	6
Tabla descripción de computadores	7
Tabla de asignación de VLAN y de puertos	7
Tabla de enlaces troncales	7
DESARROLLO ESCENARIO 1	8
ESCENARIO 2.....	24
CONCLUSIONES	41
REFERENCIAS	42
ANEXOS	44
IMAGENES.....	44
TABLAS	45

INTRODUCCIÓN

Las redes de comunicaciones son un tema fundamental en el día a día, puesto que hoy todo el mundo tiene la necesidad de estar conectado, para ser más eficiente en sus actividades laborales, o por costumbre. Es por ello que el diplomado de profundización cisco abarcó, desde las temáticas más básicas de las redes de comunicaciones, hasta temas un poco más avanzados y esenciales como enrutamiento y la implementación de protocolos. En el transcurso de los cursos de CCNA, se identificaron diferentes comandos para la configuración de equipos, asignación de direcciones IP, VLANS, protocolos, y visualización de todas las configuraciones ya nombradas, lo anterior acompañado de diferentes conceptos que permitieron desarrollar las habilidades necesarias para crear y configurar redes de acuerdo a diferentes casos de estudio, con requerimientos diversos, teniendo en cuenta las necesidades y las ventajas y desventajas que ofrece un protocolo u otro. De la misma manera el curso resalto la importancia de la seguridad en la configuración y en los activos de una red, implementándola a través de diferentes comandos. En el siguiente documento se desarrollan dos escenarios, cumpliendo con los requerimientos e implementando los protocolos DHCP, OSPF, NAT entre otros.

Escenario 1

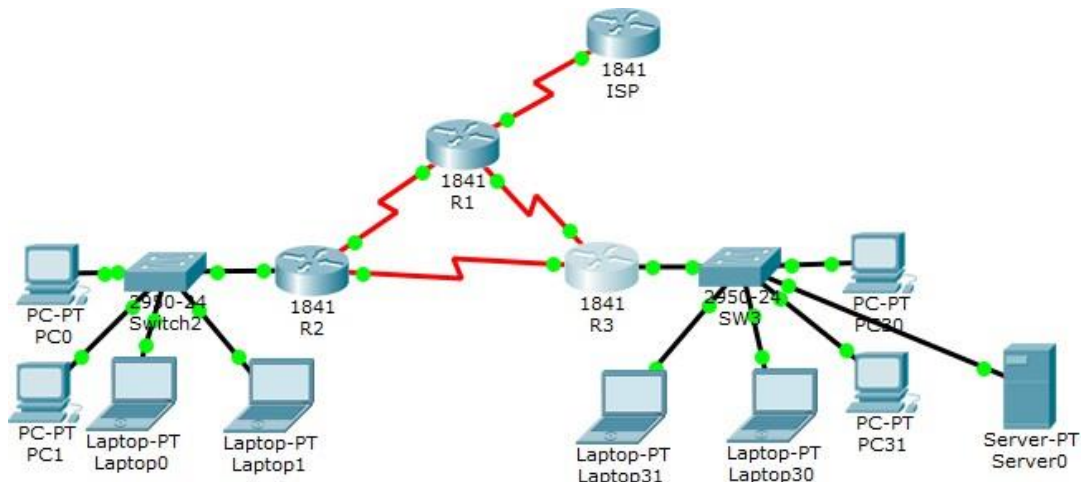


Imagen 1 – Escenario1

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:30/64 1		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

Tabla 1 – Enrutamiento escenario 1

Tabla descripción de computadores

EQUIPO	PROTOCOLO
PC20	DHCP
PC21	DHCP
PC30	DHCP
PC31	DHCP
Laptop20	DHCP
Laptop21	DHCP
Laptop30	DHCP
Laptop31	DHCP

Tabla 2 – Escenario 1 Lista Computadores

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 3 – Escenario 1 Asignación VLAN y puertos

Tabla de enlaces troncales

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

Tabla 4 – Escenario 1 enlace de troncales

DESARROLLO ESCENARIO 1

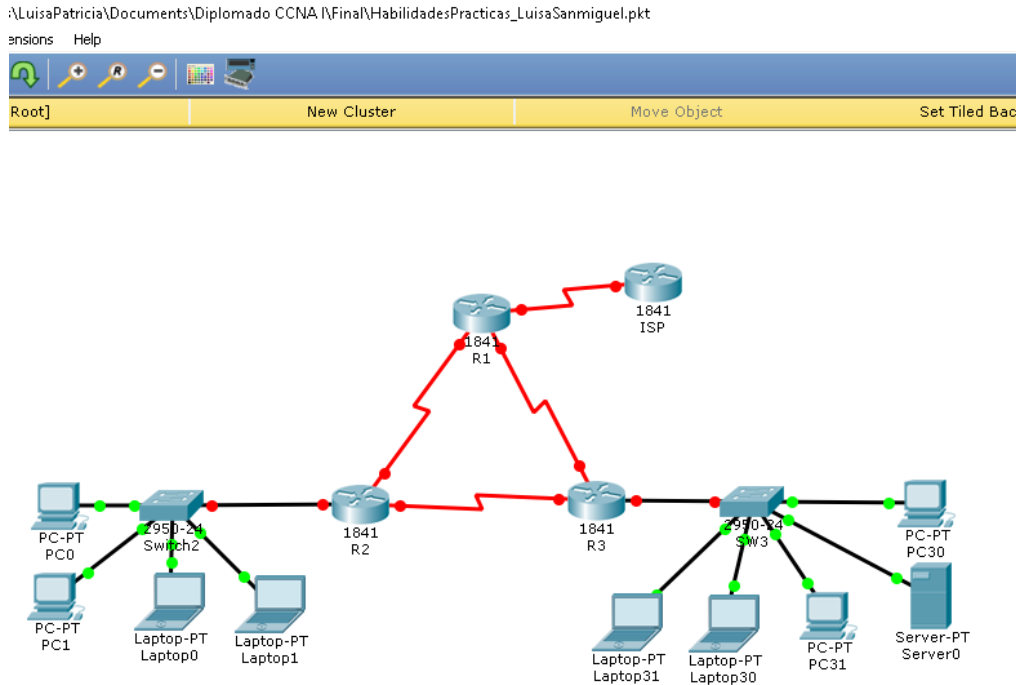


Imagen 2 –Escena 1 sin configuración

- ✓ **Configuración del switch número 2 SW2 VLAN y las asignaciones de puertos de VLAN deben cumplir con la tabla 3.**

Seleccionamos el equipo switch 2 e ingresamos al modo de comando, luego se ingresa al modo de configuración global y posterior le asigna el nombre sw2.

- Switch>enable
- Switch#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- Switch(config)#hostname SW2

Luego en el mismo equipo switch 2, también en el modo de configuración global, se crean las VLANS, asignando al número de Vlan el nombre indicado en la tabla 3

- 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

Luego en el switch 2, en el modo de configuración se asignan los puertos a las VLANS 100 y 200 de acuerdo a la descripción de la tabla 3

- SW2(config)#interface FastEthernet 0/2
- SW2(config-if)#switchport mode access
- SW2(config-if)#exit
- SW2(config)#interface FastEthernet 0/3
- SW2(config-if)#switchport mode access
- SW2(config-if)#switchport access vlan 100
- SW2(config-if)#exit
- SW2(config)#interface range FastEthernet 0/4 -5
- SW2(config-if)#switchport mode access
- SW2(config-if)#switchport access vlan 200
- SW2(config-if)#exit

Se configura la troncal en el switch 2 de acuerdo a la tabla 4

- SW2#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- SW2(config)#interface range fa0/2 -3
- SW2(config-if)#switchport mode trunk
- SW2(config-if)#no shutdown
- SW2(config-if)#exit

✓ **Los puertos de red que no se utilizan se deben deshabilitar.**

Se verifican que puertos de red están sin uso, en este caso los puertos fastethernet desde el 0/6 hasta el 0/24 y se deshabilitan por medio de los siguientes comandos:

- SW2>enable
- SW2#configure terminal
- SW2(config)#interface range fa0/6-24
- SW2(config-if-range)#shutdown

✓ **La información de dirección IP R1, R2 y R3 debe cumplir con la tabla 1**
Configuración ISP

Para configurar el nombre del router ISP, primero se selecciona el equipo, posteriormente se ingresa a la consola, por medio de comandos se ingresa al modo configuración y se asigna el nombre ISP con los comandos que están a continuación:

- Router> enable
- Router#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- Router(config)#hostname ISP
-

En el router ISP, en modo configuración, se selecciona la interface serial 0/0/0 que se encuentra conectada a Router 1, y se le asigna la dirección IP y la máscara de red de acuerdo a la tabla 1, luego se habilita el puerto.

- ISP(config)#interface serial 0/0/0
- ISP(config-if)#ip address 200.123.211.1 255.255.255.0
- ISP(config-if)#no shutdown

✓ Configuración del router R1

Seleccionamos el router 1, se ingresa a la consola, luego se ingresa a configuración global por medio de los comandos y se asigna el nombre de acuerdo a la tabla 1.

- Router>enable
- Router#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- Router(config)#Hostname R1

Luego ingresando a cada una de las tres interfaces de tipo serial del Router, se asignan las direcciones de acuerdo a la tabla 1, al terminar se habilita la interfaz.

- R1(config)#Interface serial 0/0/0
- R1(config-if)#Ip address 200.123.211.2 255.255.255.0
- R1(config-if)#No shutdown
- R1(config-if)#exit

- R1(config)#Interface serial 0/1/0
- R1(config-if)#Ip address 10.0.0.1 255.255.255.252
- R1(config-if)#No shutdown
- R1(config-if)#exit

- R1(config)#Interface serial 0/1/1
- R1(config-if)#Ip address 10.0.0.5 255.255.255.252
- R1(config-if)#No shutdown
- R1(config-if)#exit

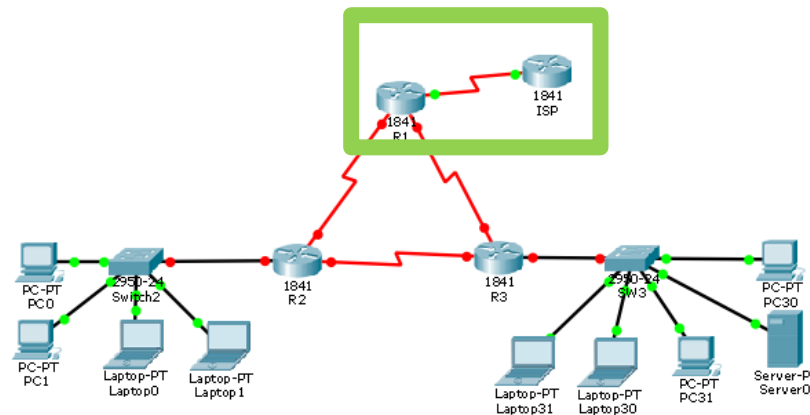
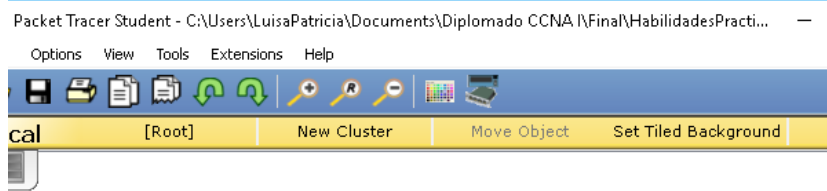


Imagen 3- Conexión desde ISP a R1 configurado

✓ Configuración del router 2 (R2)

Se selecciona el equipo R2, se ingresa a la consola, luego a modo configuración y por medio del comando “hostname” se asigna el nombre del router R2, como se muestra a continuación:

- R2>enable
- R2#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- Router(config)#Hostname R2

Se configuran las dos interfaces de tipo serial del Router 2, asignándoles las direcciones de acuerdo a la tabla 1 de enrutamiento y luego se habilitan los puertos, de la siguiente manera:

- R2(config)#Interface serial 0/0/0
- R2(config-if)#Ip address 10.0.0.2 255.255.255.252
- R2(config-if)#No shutdown
- R2(config-if)#exit

- R2(config)#Interface serial 0/0/1
- R2(config-if)#Ip address 10.0.0.9 255.255.255.252
- R2(config-if)#No shutdown
- R2(config-if)#exit

Se configura la interfaz de tipo fastEthernet del Router 2, asignándoles las direcciones de acuerdo a la tabla 1 de enrutamiento y luego se habilitan los puertos.

- R2>enable
- R2#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- R2(config-if)#interface FastEthernet0/0.100
- R2(config-subif)#encapsulation dot1Q 100
- R2(config-subif)#ip address 192.168.20.1 255.255.255.0
- R2(config-subif)#shutdown
- R2(config-subif)#exit

- R2(config)#interface fastEthernet 0/0.200
- R2(config-subif)#
- %LINK-5-CHANGED: Interface FastEthernet0/0.200, changed state to up

- %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.200, changed state to up
- R2(config-subif)#encapsulation dot1Q 200
- R2(config-subif)#ip address 192.168.21.1 255.255.255.0
- R2(config-subif)#interface f0/0
- R2(config-if)#no shutdown

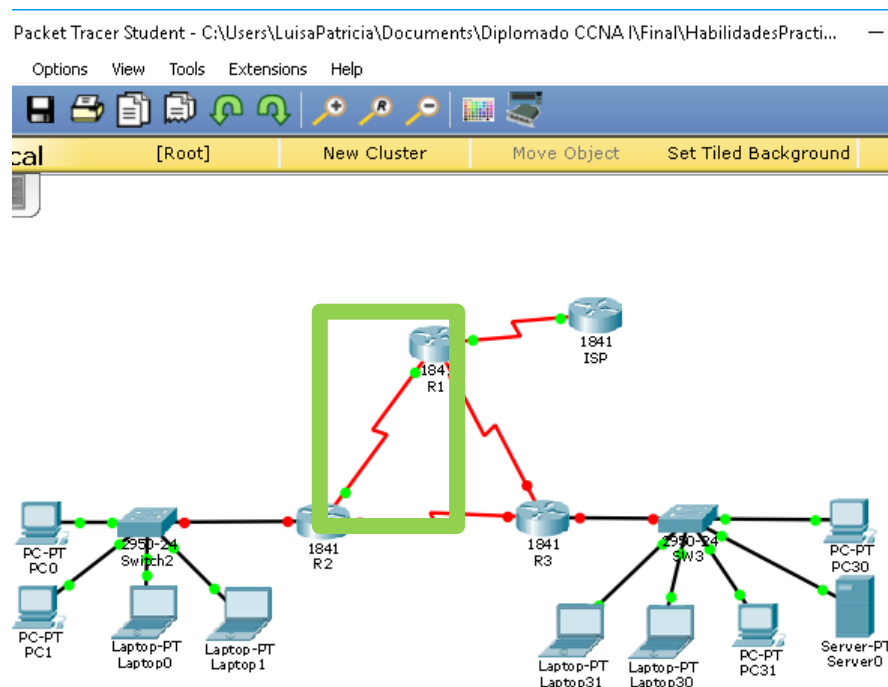


Imagen 4 – Conexiones R2 a R1 configurada

✓ Configuración del router 3 R3

Se selecciona el equipo R3, se ingresa a la consola, y por medio del modo configuración se configura el nombre R3, como se muestra a continuación:

- Router>enable
- Router#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- Router(config)#hostname R3

En R3 por medio del modo configuración global, se activa el reenvío de tráfico Ipv6 a través de los siguientes comandos:

- Router>enable
- Router#configure terminal
- R3(config)#ipv6 unicast-routing

Se configuran las dos interfaces de tipo serial del Router 3, asignándoles las direcciones de acuerdo a la tabla 1 de enrutamiento y luego se habilitan los puertos.

- Router>enable
- Router#configure terminal
- R3(config)# interface serial 0/0/0
- R3(config-if)#ip address 10.0.0.6 255.255.255.252
- R3(config-if)#exit

- R3(config)# interface serial 0/0/1
- R3(config-if)#ip address 10.0.0.10 255.255.255.252
- R3(config-if)#exit

- R3(config)#interface fastEthernet 0/0
- R3(config-if)#ipv6 address 2001:db8:130::9c0:80f:301/64
- R3(config-if)#ipv6 dhcp server vlan_1
- R3(config-if)#ipv6 nd other-config-flag
- R3(config-if)#ip address 192.168.30.1 255.255.255.0
- R3(config-if)#no shutdown
- R3(config-if)#exit

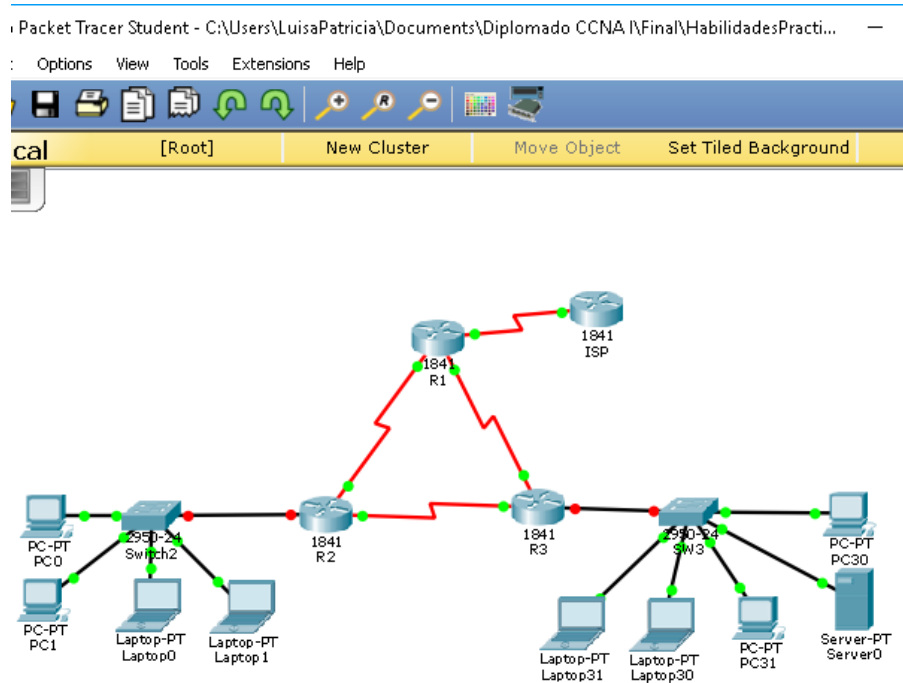


Imagen 5 – Conexiones de ISP, R1, R2 Y R3 configuradas

- ✓ **En R1 se realizar una NAT con sobrecarga sobre una dirección IPv4 pública.**
Se ingresa a R1 modo configuración global, luego se configura la lista de acceso estándar de nombre **INSIDE-DEVS**, asignando el rango de direcciones y la máscara de red, luego se indican las restricciones y permisos, con los siguientes comandos:

- R1>enable
- R1#configure terminal
- R1(config)#interface s0/1/0
- R1(config-if)#ip nat inside
- R1(config-if)#interface s0/1/1
- R1(config-if)#ip nat inside
- R1(config-if)#interface s0/0/0
- R1(config-if)#ip nat outside
- 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

- ✓ **R1 configura una ruta estática predeterminada al ISP e incluye esa ruta en el dominio RIPv2 por medio de los siguientes comandos:**

- 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)#ip route 0.0.0.0 0.0.0.0 s0/0/0
- R1(config)#router rip

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

Se ingresa al R2, modo configuración global, se crea un grupo para el enrutamiento por medio del protocolo DHCP para la VLAN 100, se indica la red y la máscara a la que se le dará el enrutamiento, se realiza lo mismo para la VLAN 200, por último se indica la red del router estándar, por medio de los siguientes comandos:

- R2>enable
- R2#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- R2(config)#ip dhcp pool vlan_100
- R2(dhcp-config)#network 192.168.20.1 255.255.255.0
- R2(dhcp-config)#default-router 192.168.20.1
- R2(dhcp-config)#exit
- R2(config)#ip dhcp pool vlan_200
- R2(dhcp-config)#network 192.168.21.1 255.255.255.0
- R2(dhcp-config)#default-router 192.168.21.1

R2 enrutamiento

R2 debe, además de enrutamiento a otras partes de la red, se debe configurar la las direcciones IP de VLAN 100 y 200, por medio de los siguientes comandos:

- R2#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- 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)#exit

- ✓ El servidor Server0 es sólo un servidor IPv6 y solo debe ser accesibles para los dispositivos en R3 (ping).

Se realiza la verificación por medio de ping que se realiza mediante el protocolo ICMP, comprobando que únicamente los equipos del router 3 tengan acceso.

Cisco Packet Tracer Student - C:\Users\LuisaPatricia\Documents\Diplomado CCNA I\Final\1.HabilidadesPracticas_LuisaSanmiguel.pkt

File Edit Options View Tools Extensions Help

Logical [Root] New Cluster Move Object

1841 R1 1841 ISP

1841 R2 1841 R3

2950-24 SW2 2950-24 SW3

PC-PT PC0 Laptop-PT Laptop0 Laptop-PT Laptop1 Laptop-PT Laptop31 Laptop-PT Laptop30 PC-PT PC31 Server-PT Server0

PDU List Window

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC30	Server0	ICMP		0.000	N	0	(edit)	
	Successful	PC31	Server0	ICMP		0.000	N	1	(edit)	
	Successful	Laptop...	Server0	ICMP		0.000	N	2	(edit)	
	Successful	Laptop...	Server0	ICMP		0.000	N	3	(edit)	
	Successful	Server0	Laptop31	ICMP		0.000	N	4	(edit)	
	Failed	Laptop1	Server0	ICMP		0.000	N	5	(edit)	
	Failed	Laptop0	Server0	ICMP		0.000	N	6	(edit)	
	Failed	PC1	Server0	ICMP		0.000	N	7	(edit)	
	Failed	PC0	Server0	ICMP		0.000	N	8	(edit)	

Imagen 6 – Verificación del acceso a Server0

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

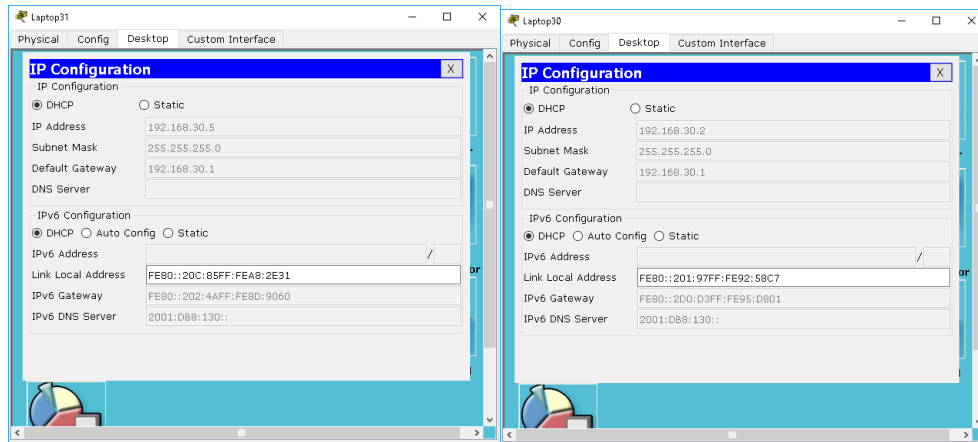


Imagen 7 – Configuración protocolo DHCPv4 y DHCPv6 Laptop31 y Laptop30– DualStack

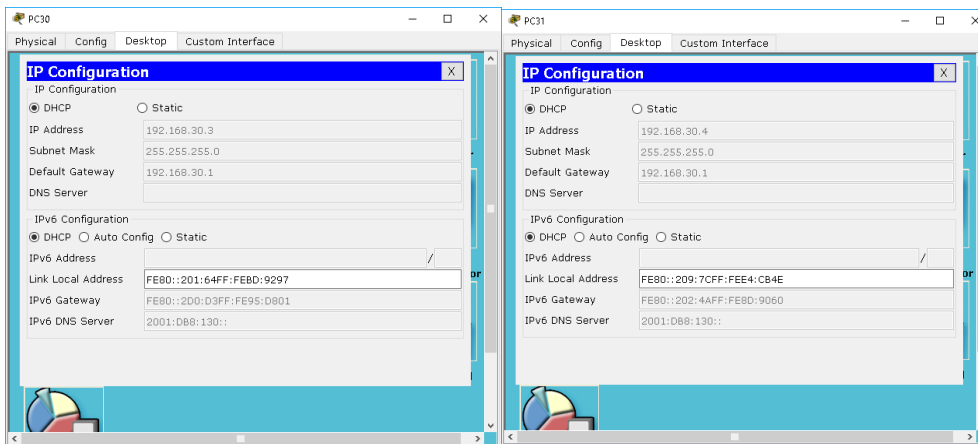


Imagen 8- Configuración protocolo DHCPv4 Y DHCPv6 PC30 y PC 31 – DualStack

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

Se configuran la interfaz de tipo FastEthernet 0/0 del Router 2, asignándole direccionamiento ipv6 e ipv4 de acuerdo a la tabla1 de enrutamiento y luego se habilitan los puertos. Se relaciona el direccionamiento ipv6 mediante el protocolo DHCP con la interfaz 0/0, con los comandos que se muestran a continuación:

- R3(config)#interface fastEthernet 0/0
- R3(config-if)#ipv6 address 2001:db8:130::9c0:80f:301/64

- R3(config-if)#ipv6 dhcp server vlan_1
- R3(config-if)#ipv6 nd other-config-flag
- R3(config-if)#ip address 192.168.30.1 255.255.255.0
- R3(config-if)#no shutdown
- R3(config-if)#exit

- R3(config)#ip dhcp pool vlan_1
- R3(dhcp-config)#network 192.168.30.1 255.255.255.0
- R3(dhcp-config)#default-router 192.168.30.1
- R3(dhcp-config)#ipv6 dhcp pool vlan_1
- R3(config-dhcp)#dns-server 2001:db8:130::
- R3(config-dhcp)#exit

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

- 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)#ip route 0.0.0.0 0.0.0.0 s0/0/0
- R1(config)#router rip
- R1(config-router)#network 10.0.0.4
- R1(config-router)#network 10.0.0.0
- R1(config-router)#default-information originate
- R1(config-router)#

- R2(config)#router rip
- R2(config-router)#version 2
- R2(config-router)#network 192.168.30.0
- R2(config-router)#network 192.168.20.0
- R2(config-router)#network 192.168.21.0
- R2(config-router)#network 10.0.0.0
- R2(config-router)#network 10.0.0.8
- R2(config-router)#

- R3>enable
- R3#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.

- R3(config)#route rip
- R3(config-router)#version 2
- R3(config-router)#network 192.168.0.0
- R3(config-router)#network 10.0.0.8
- R3(config-router)#network 10.0.0.4
- R3(config-router)#exit

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

Mediante el comando show ip route, se verifica en los routers R1, R2 y R3, con el fin de evidenciar las rutas por medio del protocolo rip v2 teniendo en cuenta que las que se encuentren marcadas al inicio con la letra R pertenecen al protocolo RIP y si tienen un asterisco* están configuradas por defecto con el protocolo que indique como se muestra a continuación:

R1>show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 * - candidate default, U - per-user static route, o - ODR
 P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

```

10.0.0.0/30 is subnetted, 3 subnets
C    10.0.0.0 is directly connected, Serial0/1/0
C    10.0.0.4 is directly connected, Serial0/1/1
R    10.0.0.8 [120/1] via 10.0.0.2, 00:00:18, Serial0/1/0
      [120/1] via 10.0.0.6, 00:00:22, Serial0/1/1
R    192.168.20.0/24 [120/1] via 10.0.0.2, 00:00:18, Serial0/1/0
R    192.168.21.0/24 [120/1] via 10.0.0.2, 00:00:18, Serial0/1/0
R    192.168.30.0/24 [120/1] via 10.0.0.6, 00:00:22, Serial0/1/1
C    200.123.211.0/24 is directly connected, Serial0/0/0
S*   0.0.0.0/0 is directly connected, Serial0/0/0

```

R2>show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.0.0.1 to network 0.0.0.0

10.0.0.0/30 is subnetted, 3 subnets

```
C 10.0.0.0 is directly connected, Serial0/0/0
R 10.0.0.4 [120/1] via 10.0.0.1, 00:00:19, Serial0/0/0
  [120/1] via 10.0.0.10, 00:00:07, Serial0/0/1
C 10.0.0.8 is directly connected, Serial0/0/1
C 192.168.20.0/24 is directly connected, FastEthernet0/0.100
C 192.168.21.0/24 is directly connected, FastEthernet0/0.200
R 192.168.30.0/24 [120/1] via 10.0.0.10, 00:00:07, Serial0/0/1
R 200.123.211.0/24 [120/1] via 10.0.0.1, 00:00:19, Serial0/0/0
R* 0.0.0.0/0 [120/1] via 10.0.0.1, 00:00:19, Serial0/0/0
```

R3>show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 10.0.0.5 to network 0.0.0.0

10.0.0.0/30 is subnetted, 3 subnets

```
R 10.0.0.0 [120/1] via 10.0.0.5, 00:00:09, Serial0/0/0
  [120/1] via 10.0.0.9, 00:00:09, Serial0/0/1
C 10.0.0.4 is directly connected, Serial0/0/0
C 10.0.0.8 is directly connected, Serial0/0/1
R 192.168.20.0/24 [120/1] via 10.0.0.9, 00:00:09, Serial0/0/1
R 192.168.21.0/24 [120/1] via 10.0.0.9, 00:00:09, Serial0/0/1
C 192.168.30.0/24 is directly connected, FastEthernet0/0
R 200.123.211.0/24 [120/1] via 10.0.0.5, 00:00:09, Serial0/0/0
R* 0.0.0.0/0 [120/1] via 10.0.0.5, 00:00:09, Serial0/0/0
```

- ✓ 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.

re	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Server0	R3	ICMP		0.000	N	0
	Successful	PC30	R3	ICMP		0.000	N	1
	Successful	Server0	R1	ICMP		0.000	N	2
-	-	-	-	-	-	-	-	-

Imagen 9 – Verificación estado configuración Ping server0 a R3, PC30 a R3 y Server0 a R1

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	Server0	ISP	ICMP		0.000	N	3
	Successful	PC30	ISP	ICMP		0.000	N	4
	Successful	R3	R2	ICMP		0.000	N	5
-	-	-	-	-	-	-	-	-

Imagen 10 – Verificación estado configuración Ping Server0 a ISP, PC30 a ISP y R3 a R2

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	R1	R3	ICMP		0.000	N	6
	Successful	R1	R2	ICMP		0.000	N	7
	Successful	Laptop1	R2	ICMP		0.000	N	8
-	-	-	-	-	-	-	-	-

Imagen 11 – Verificación estado configuración Ping R1 a R3, R1 a R2 Laptop1 a R2

re	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	R2	ICMP		0.000	N	0
	Successful	PC1	R2	ICMP		0.000	N	1
	Successful	Laptop0	R2	ICMP		0.000	N	2
-	-	-	-	-	-	-	-	-

Imagen 12- Verificación estado configuración Ping PC0 a R2, PC1 a R2 y Laptop0 a R2

ESCENARIO 2

Escenario: Una empresa de Tecnología posee tres sucursales distribuidas en las ciudades de Miami, Bogotá y Buenos Aires, en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red.

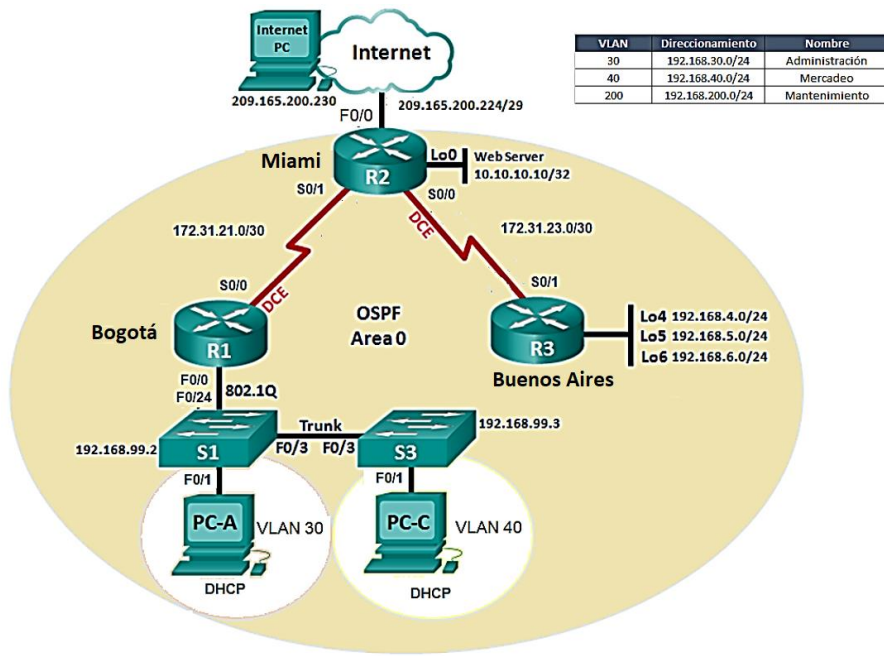


Imagen 13 – Escenario 2

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
ISP	Gi0/0	209.165.200.230	255.255.255.248	N/D
R1	Se0/0/0	172.31.21.1	255.255.255.252	N/D
	Fa 0/0,30	192.168.30.1	255.255.255.0	N/D
	Fa0/0,40	192.168.40.1	255.255.255.0	N/D
	Fa0/0,200	192.168.200.1	255.255.255.0	N/D
	Fa0/0,99	192.168.99.1	255.255.255.0	N/D
R2	Se0/0/0	172.31.23.1	255.255.255.252	N/D

	Se0/0/1	172.31.21.2	255.255.255.252	N/D
	Fa0/0	209.165.200.255	255.255.255.248	N/D
	Lo0	10.10.10.10	255.255.255.255	
R3	Se0/0/1	172.31.23.2	255.255.255.252	N/D
	Lo4	192.168.4.1	255.255.255.0	N/D
	Lo5	192.168.5.1	255.255.255.0	N/D
	Lo6	192.168.6.1	255.255.255.0	N/D
SW1	VLAN 99	192.168.99.2	255.255.255.0	N/D
SW3	VLAN 99	192.168.99.3	255.255.255.0	N/D
PC A	VLAN 30	DINAMICO		
PC C	VLAN 40	DINAMICO		

Tabla 5 –Enrutamiento escenario 2

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

Se realiza la configuración de los routers R1, R2 Y R3 Configuración de R1, primero se configura para cada uno de los router el nombre, las contraseñas de seguridad luego se configuran las interfaces con las direcciones que se encuentran en la tabla 5 de enrutamiento, por último se habilita el puerto.

Configuración R1

- Router>Enable
- Router#configure terminal
- R1(config)#line console 0
- R1(config-line)#password cisco
- R1(config-line)#login
- R1(config-line)#line vty 0 4
- R1(config-line)#password cisco
- R1(config-line)#login
- R1(config-line)#exit

- Enter configuration commands, one per line. End with CNTL/Z.
- Router(config)#no ip domain-lookup

- Router(config)#hostname R1
- R1(config)#interface serial 0/0/0
- R1(config-if)#ip address 172.31.21.1 255.255.255.252
- R1(config-if)#clock rate 120000
- R1(config-if)#no shutdown

- R1(config)#interface gigabitEthernet 0/0.30
- R1(config-subif)#description Administracion
- 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)#interface gigabitEthernet 0/0.40
- R1(config-subif)#description Mercadeo
- R1(config-subif)#encapsulation dot1q 40
- R1(config-subif)#ip address 192.168.40.1 255.255.255.0
- R1(config-subif)#exit

- R1(config-subif)#interface gigabitEthernet 0/0.200
- R1(config-subif)#description Mantenimiento
- R1(config-subif)#encapsulation dot1q 200
- R1(config-subif)#ip address 192.168.200.1 255.255.255.0
- R1(config-subif)#exit

- R1(config)#interface gigabitEthernet 0/0
- R1(config-if)#no shutdown
- R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
- %Default route without gateway, if not a point-to-point interface, may impact performance

Configuración Router R2

- Router >enable
- Router #configure terminal
- Router(config)#hostname R2

- R2(config)#enable secret class
- R2(config)#line console 0
- R2(config-line)#password cisco
- R2(config-line)#login
- R2(config-line)#line vty 0 4
- R2(config-line)#password cisco
- R2(config-line)#login
- R2(config-line)#exit

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

- R2(config)#interface serial 0/0/1
- R2(config-if)#ip address 171.31.21.2 255.255.255.252
- R2(config-if)#no shutdown
- %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up

- R2(config-if)#interface serial 0/0/0
- R2(config-if)#ip address 171.31.23.1 255.255.255.252
- R2(config-if)#clock rate 128000
- R2(config-if)#no shutdown
- %LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

- %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
- R2#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- R2(config)#interface gigabitEthernet 0/1
- R2(config-if)#ip address 10.10.10.1 255.255.255.0
- R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up

- R2(config-if)#interface gigabitEthernet 0/0
- R2(config-if)#ip address 209.165.200.225 255.255.255.248
- R2(config-if)#no shutdown
- R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0

Configuración Router R3

- Router >enable
- Router #configure terminal
- Router(config)#hostname R3
- R3(config)#line console 0
- R3(config-line)#password cisco
- R3(config-line)#login
- R3(config-line)#line vty 0 4
- R3(config-line)#password cisco
- R3(config-line)#login
- Enter configuration commands, one per line. End with CNTL/Z.
- R3(config)#interface serial 0/0/1
- R3(config-if)#ip address 172.31.23.2 255.255.255.252
- R3(config-if)#no shutdown
- %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
- %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
- %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
- R3>enable
- R3#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- R3(config)#interface serial 0/0/1
- R3(config-if)#ip address 172.31.23.2 255.255.255.252
- R3(config-if)#no shutdown
- %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
- %LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
- %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
- %SYS-5-CONFIG_I: Configured from console by console

- R3(config)#interface loopback 4
- %LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
- R3(config-if)#ip address 192.168.4.1 255.255.255.0
 - R3(config-if)#no shutdown
 - R3(config-if)#interface loopback 5
- %LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
- R3(config-if)#ip address 192.168.5.1 255.255.255.0
 - R3(config-if)#no shutdown
 - R3(config-if)#exit
 - R3(config)#interface loopback 6
- %LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
- R3(config-if)#ip address 192.168.6.1 255.255.255.0
 - R3(config-if)#no shutdown
- Router(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
 - %Default route without gateway, if not a point-to-point interface, may impact performance

✓ 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

Tabla 6 – Enrutamiento protocolo OSPFv2

- ✓ **Verificar información de OSPF.**
- ✓ **Visualizar tablas de enrutamiento y routers conectados por OSPFv2.**
- ✓ **Visualizar lista resumida de interfaces por OSPF en donde se ilustre el costo de cada interface.**
- ✓ **Visualizar el OSPF Process ID, Router ID, Address summarizations, Routing Networks, and passive interfaces configuradas en cada router.**

Configuración del protocolo OSPF en el router 1

- 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 gigabitEthernet 0/0.30
- R1(config-router)#passive-interface gigabitEthernet 0/0.40
- R1(config-router)#passive-interface gigabitEthernet 0/0.200
- R1(config)#int s0/0/0
- R1(config-if)#bandwidth 256
- R1(config-if)#ip ospf cost 9500
- R1(config-if)#exit

Configuración del protocolo OSPF en el router 2

- 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 10.10.10.0 0.0.0.255 area 0
- R2(config-router)#passive-interface g0/0
- R2(config-router)#exit
- R2(config)#interface serial 0/0/0

- R2(config-if)#bandwidth 256
- R2(config-if)#ip ospf cost 9500
- R2(config-if)#exit
- R2(config)#interface serial 0/0/1
- R2(config-if)#bandwidth 256

Configuración del protocolo OSPF en el router 3

- 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)#

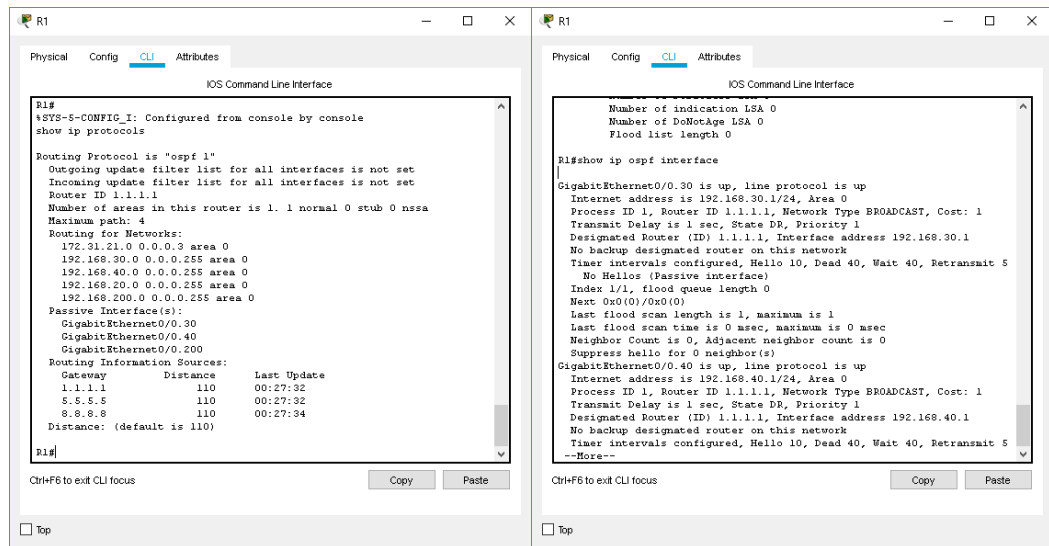


Imagen 14 – Router 1 protocolos configurados y verificación protocolo OSPF

- ✓ Configuración de VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la tabla 5.

Primero se configuran los parámetros básicos del switch 1, se asigna el nombre y luego las contraseñas de la seguridad

- Switch>enable
- Switch#configure terminal
- Switch(config)#hostname S1
-
- S1(config)#enable secret class
- S1(config)#line console 0
- S1(config-line)#password cisco
- S1(config-line)#login
- S1(config-line)#exit
-
- S1(config)#line vty 0 4
- S1(config-line)#password cisco
- S1(config-line)#login
- S1(config-line)#exit
-
- S1(config)#service password-encryption

Primero se configuran los parámetros básicos del switch 3, se asigna el nombre y

luego las contraseñas de la seguridad, con los comandos que se muestran a continuación:

- Switch>enable
- Switch#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- Switch(config)#hostname S3

- S3(config)#enable secret class
- S3(config)#line console 0
- S3(config-line)#password cisco
- S3(config-line)#login
- S3(config-line)#exit

- S3(config)#line vty 0 4
- S3(config-line)#password cisco
- S3(config-line)#login
- S3(config-line)#exit
- S3(config)#service password-encryption

Se crean las VLANS 30, 40 y 200 en el switch 1, colocando los nombres de acuerdo a la imagen 13 escenario 2.

- S1(config)#vlan 30
- S1(config-vlan)#name Administración
- S1(config-vlan)#exit

- S1(config)#vlan 40
- S1(config-vlan)#name Mercadeo
- S1(config-vlan)#exit

- S1(config)#Vlan 200
- S1(config-vlan)#name Mantenimiento
- ip address 192.168.200.2 255.255.255.0
- S1(config-if)#no shutdown
- S1(config-if)#ip default-gateway 192.168.200.1
- S1(config)#
- %SYS-5-CONFIG_I: Configured from console by console

✓ **Se deshabilita el DNS lookup en el switch 3, con el siguiente comando:**
S3(config)#no ip domain-lookup

✓ **Asignar direcciones IP a los Switches acorde a la tabla 5 de enrutamiento escenario 2.**

Se asignan las interfaces y el modo del puerto a las VLANS, en el switch 1 por medio de los siguientes comandos:

- S1#configure terminal
- Enter configuration commands, one per line. End with CNTL/Z.
- S1(config)#interface fastEthernet 0/1
- S1(config-if)#switchport mode access
- S1(config-if)#switchport access vlan 30
- S1(config-if)#

- S1(config)#interface fastethernet 0/3
- S1(config-if)#switchport mode trunk
- S1(config-if)#switchport trunk native vlan 1
- S1(config-if)#no shutdown

- S1(config)#interface FastEthernet0/24
- S1(config-if)#switchport mode trunk
- S1(config-if)#switchport trunk native vlan 1
- S1(config-if)#no shutdown

Se asignan las interfaces y el modo del puerto a las VLANS, en el switch 3 por medio de los siguientes comandos:

- S3(config)#vlan 40
- S3(config-vlan)#name Mercadeo
- S3(config-vlan)#exit
- S3(config)#vlan 200
- S3(config-vlan)#name Mantenimiento
- S3(config-vlan)#interface vlan 200
- S3(config-if)#ip address 192.168.200.3 255.255.255.0
- S3(config-if)#no shutdown
- S3(config-if)#ip default-gateway 192.168.200.1
- S3(config)#

- S3(config)#interface fastethernet 0/1
- S3(config-if)#switchport mode access
- S3(config-if)#switchport access vlan 40
- S3(config-if)#exit

- S3(config)#interface fastEthernet 0/3
- S3(config-if)#switchport mode trunk
- S3(config-if)#switchport trunk native vlan 1

- ✓ **Desactivar todas las interfaces que no sean utilizadas en el esquema de red.**

Deshabilitar los puertos del ROUTER1

- R1(config)#interface FastEthernet0/1/3
- R1(config-if)#shutdown
- %LINK-5-CHANGED: Interface FastEthernet0/1/3, changed state to administratively down
- R1(config-if)#exit
-
- R1(config)#interface FastEthernet0/1/2
- R1(config-if)#shutdown
- %LINK-5-CHANGED: Interface FastEthernet0/1/2, changed state to administratively down
- R1(config-if)#exit
-
- R1(config)#interface FastEthernet0/1/1
- R1(config-if)#shutdown
- %LINK-5-CHANGED: Interface FastEthernet0/1/1, changed state to administratively down
- R1(config-if)#exit
-
- R1(config)#interface FastEthernet0/1/0
- R1(config-if)#shutdown
- R1(config-if)#
- %LINK-5-CHANGED: Interface FastEthernet0/1/0, changed state to administratively down
- R1(config-if)#exit

Deshabilitar los puertos del switch 1

- S1(config)#interface range fa0/2, fa0/4-23
- S1(config-if-range)#shutdown
-

Deshabilitar los puertos del switch 3

- S3(config)#interface range fa0/2, fa0/4-24
- S3(config-if-range)#shutdown

- ✓ **Configurar DHCP and NAT for IPv4**

Router 2

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

- R2(config)#int g0/0
- R2(config-if)#ip nat outside
- R2(config-if)#int g0/1
- R2(config-if)#ip nat inside

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

- 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)#exit
- R1(config)#ip dhcp pool Mercadeo
- R1(dhcp-config)#dns-server 10.10.10.11
- R1(dhcp-config)#default-router 192.168.40.1
- R1(dhcp-config)#network 192.168.40.0 255.255.255.0

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

- R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.31
- R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.31

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.

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

- R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
- R2(config)#interface g0/1
- R2(config-if)#ip nat outside
- R2(config-if)#interface g0/0
- R2(config-if)#ip nat inside
- R2(config-if)#exit

✓ **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.

- R2(config)#access-list 1 permit 192.168.30.0 0.0.0.225
- R2(config)#access-list 1 permit 192.168.40.0 0.0.0.225
- R2(config)#access-list 1 permit 192.168.4.0 0.0.4.225
- 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

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

- R2(config)#ip nat inside source list 1 pool internet
- R2(config)#ip access-list standard admin-mant
- R2(config-std-nacl)#permit host 172.31.21.1
- R2(config-std-nacl)#line vty 0 4
- R2(config-line)#access-class admin-mant in

- R2(config)#access-list 101 permit tcp any host 209.165.229.230 eq www
- R2(config)#access-list 101 permit icmp any any echo-reply

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

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

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

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

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

```

PC30
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.21.3

Pinging 192.168.21.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.21.3: bytes=32 time=23ms TTL=126
Reply from 192.168.21.3: bytes=32 time=22ms TTL=126
Reply from 192.168.21.3: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.21.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 23ms, Average = 19ms
C:\>

Pinging 192.168.21.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.21.3: bytes=32 time=23ms TTL=126
Reply from 192.168.21.3: bytes=32 time=22ms TTL=126
Reply from 192.168.21.3: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.21.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 23ms, Average = 19ms
C:\>

Pinging 192.168.21.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.21.2: bytes=32 time=34ms TTL=126
Reply from 192.168.21.2: bytes=32 time=30ms TTL=126
Reply from 192.168.21.2: bytes=32 time=30ms TTL=126

Ping statistics for 192.168.21.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 30ms, Maximum = 34ms, Average = 31ms
C:\>

```

Imagen 15 PING para la verificación de comunicación pc 30 con otros equipos

```

C:\>tracert 192.168.20.3

Tracing route to 192.168.20.3 over a maximum of 30 hops:

  0  1 ms    14 ms   12 ms   192.168.30.1
  1  29 ms   22 ms   17 ms   10.0.0.9
  2  32 ms   33 ms   32 ms   192.168.20.3

Trace complete.

C:\>tracert 192.168.21.3

Tracing route to 192.168.21.3 over a maximum of 30 hops:

  0  12 ms    0 ms    11 ms   192.168.30.1
  1  20 ms   14 ms   15 ms   10.0.0.9
  2  15 ms   12 ms   26 ms   192.168.21.3

Trace complete.

C:\>tracert 192.168.21.2

Tracing route to 192.168.21.2 over a maximum of 30 hops:

  0  14 ms    1 ms    0 ms    192.168.30.1
  1  2 ms     18 ms   16 ms   10.0.0.9
  2  32 ms   26 ms   32 ms   192.168.21.2

Trace complete.

```

Imagen 16 Tracert para verificar las rutas desde el pc30 a otros equipos

```

Pinging 192.168.21.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.21.2: bytes=32 time=34ms TTL=126
Reply from 192.168.21.2: bytes=32 time=30ms TTL=126
Reply from 192.168.21.2: bytes=32 time=30ms TTL=126

Ping statistics for 192.168.21.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 30ms, Maximum = 34ms, Average = 31ms
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
C:\>tracert 192.168.20.2

Tracing route to 192.168.20.2 over a maximum of 30 hops:

  0  34 ms   16 ms   15 ms   192.168.30.1
  1  19 ms   24 ms   15 ms   10.0.0.9
  2  33 ms   25 ms   41 ms   192.168.20.2

Trace complete.

```

Imagen 17 ping y tracert para verificar las comunicaciones con otros equipos

```

Pinging 192.168.20.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126
Reply from 192.168.20.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\>ping 192.168.20.3

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.3: bytes=32 time=30ms TTL=126
Reply from 192.168.20.3: bytes=32 time=35ms TTL=126
Reply from 192.168.20.3: bytes=32 time=24ms TTL=126

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 35ms, Average = 29ms

Pinging 192.168.20.3 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.3: bytes=32 time=30ms TTL=126
Reply from 192.168.20.3: bytes=32 time=35ms TTL=126
Reply from 192.168.20.3: bytes=32 time=24ms TTL=126

Ping statistics for 192.168.20.3:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 24ms, Maximum = 35ms, Average = 29ms

```

Imagen 18 verificación de conexión y comunicación

```

C:\>tracert 192.168.20.2

Tracing route to 192.168.20.2 over a maximum of 30 hops:

  0  34 ms   16 ms   15 ms   192.168.30.1
  1  19 ms   24 ms   15 ms   10.0.0.9
  2  33 ms   25 ms   41 ms   192.168.20.2

Trace complete.

C:\>tracert 192.168.20.3

Tracing route to 192.168.20.3 over a maximum of 30 hops:

  0  1 ms    14 ms   12 ms   192.168.30.1
  1  29 ms   22 ms   17 ms   10.0.0.9
  2  32 ms   33 ms   32 ms   192.168.20.3

Trace complete.

Tracing route to 192.168.21.2 over a maximum of 30 hops:

  0  14 ms   1 ms    0 ms    192.168.30.1
  1  2 ms    18 ms   16 ms   10.0.0.9
  2  32 ms   26 ms   32 ms   192.168.21.2

Trace complete.

C:\>tracert 192.168.30.3
C:\>tracert 192.168.30.3

Tracing route to 192.168.30.3 over a maximum of 30 hops:

  0  34 ms   5 ms    0 ms    192.168.30.3

Trace complete.

C:\>tracert 200.123.11.1

Tracing route to 200.123.11.1 over a maximum of 30 hops:

  0  2 ms    15 ms   14 ms   192.168.30.1
  1  13 ms   14 ms   12 ms   10.0.0.5
  2  42 ms   22 ms   19 ms   200.123.211.1
  3  14 ms   5 ms    21 ms   200.123.211.1

```

Imagen 19 verificación de rutas

```

C:\>tracert 192.168.30.3

Tracing route to 192.168.30.3 over a maximum of 30 hops:

  0  34 ms   5 ms    0 ms    192.168.30.3

Trace complete.

```

PDU List Window ✕

Fire	Last Status	Source	Destination
●	Successful	PC0	PC1
●	Successful	R1	R2
●	Successful	R3	R2
●	Successful	PC0	Server0

Imagen 20 verificación de conexión por medio del comando tracert y ping

Se verifican las conexiones, protocolos y rutas por medio del comando show ip route, el protocolo OSPF se encuentra caracterizado con la letra O

R1#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

```
10.0.0.0/24 is subnetted, 1 subnets
O 10.10.10.0/24 [110/9501] via 172.31.21.2, 01:47:44, Serial0/0/0
172.31.0.0/16 is variably subnetted, 3 subnets, 2 masks
C 172.31.21.0/30 is directly connected, Serial0/0/0
L 172.31.21.1/32 is directly connected, Serial0/0/0
O 172.31.23.0/30 [110/19000] via 172.31.21.2, 01:47:44, Serial0/0/0
192.168.4.0/32 is subnetted, 1 subnets
O 192.168.4.1/32 [110/19001] via 172.31.21.2, 01:47:34, Serial0/0/0
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0.30
L 192.168.30.1/32 is directly connected, GigabitEthernet0/0.30
192.168.40.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.40.0/24 is directly connected, GigabitEthernet0/0.40
L 192.168.40.1/32 is directly connected, GigabitEthernet0/0.40
192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.200.0/24 is directly connected, GigabitEthernet0/0.200
L 192.168.200.1/32 is directly connected, GigabitEthernet0/0.200
S* 0.0.0.0/0 is directly connected, Serial0/0/0
```

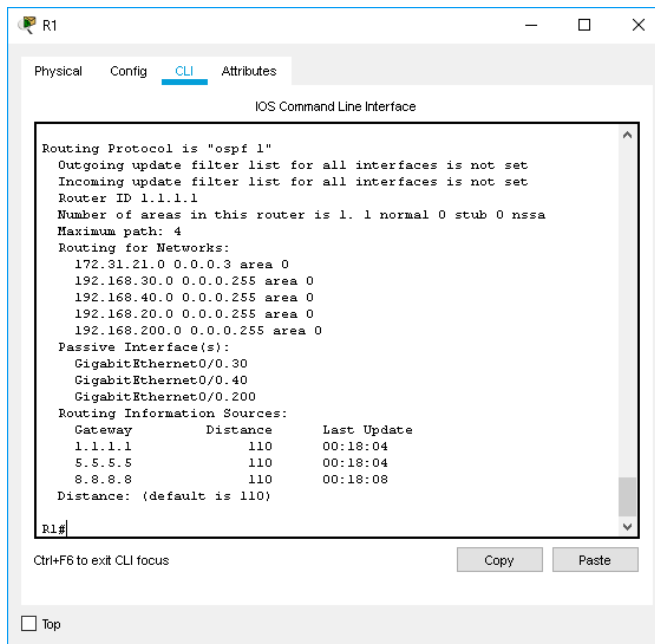


Imagen 21 Verificación de configuración del protocolo OSPF en R1

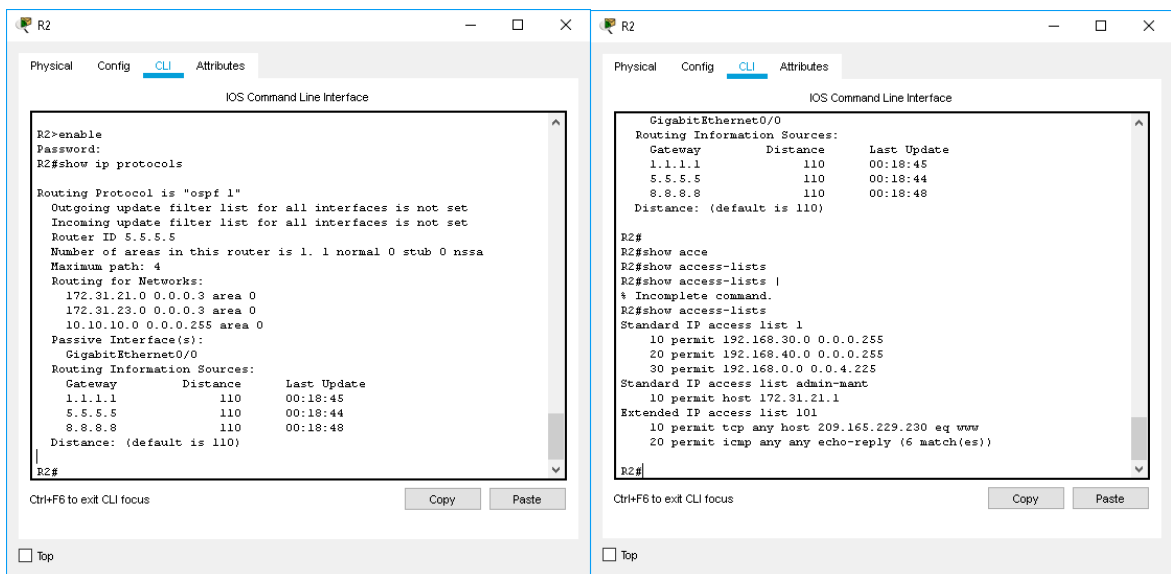


Imagen 22 del protocolo en R2 Y listas de acceso

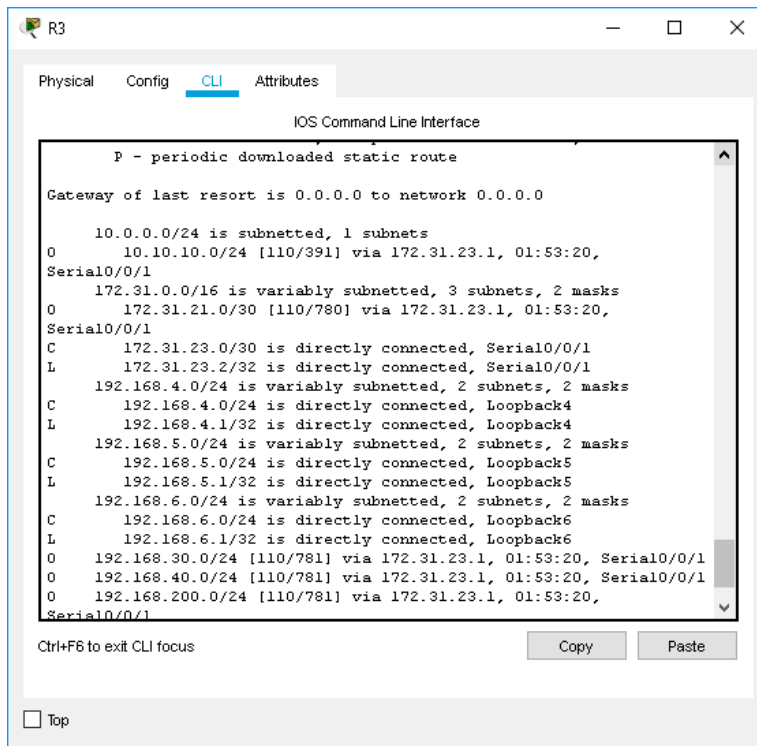


Imagen 23 Verificación de la configuración del protocolo OSPF en R3

CONCLUSIONES

- ✓ El direccionamiento mediante el protocolo DHCP facilita la asignación de direcciones y minimiza los errores.
- ✓ Las listas de control de acceso ofrecen mayor seguridad a una red, puesto que deciden que direcciones pueden o no acceder a una parte de la red.
- ✓ El protocolo RIP permite que el enrutamiento se realice de una manera más sencilla, teniendo en cuenta que cada router dará a conocer a los otros dispositivos que redes tiene conectadas.
- ✓ El comando show ip protocols sirve para visualizar los protocolos habilitados en el router, con las configuraciones correspondientes.
- ✓ Los protocolos de enrutamiento dinámico facilitan la asignación de direcciones y permite una rápida y precisa configuración entre todos los dispositivos de la red.
- ✓ Los comandos como show ip route – show running-config permite verificar las configuraciones y conexiones para identificar problemas en la red o simplemente para hacerse una idea de las conexiones físicas y lógicas de la misma.

REFERENCIAS

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). 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>

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>

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>

ANEXOS

IMAGENES

IMAGEN 1 – ESCENARIO1	6
IMAGEN 2 –ESCENA 1 SIN CONFIGURACIÓN	8
IMAGEN 3- CONEXIÓN DESDE ISP A R1 CONFIGURADO	12
IMAGEN 4 – CONEXIONES R2 A R1 CONFIGURADA	14
IMAGEN 5 – CONEXIONES DE ISP, R1, R2 Y R3 CONFIGURADAS	15
IMAGEN 6 – VERIFICACIÓN DEL ACCESO A SERVER0	18
IMAGEN 7 – CONFIGURACIÓN PROTOCOLO DHCPV4 Y DHCPV6 LAPTOP31 Y LAPTOP30– DUALSTACK	19
IMAGEN 8- CONFIGURACIÓN PROTOCOLO DHCPV4 Y DHCPV6 PC30 Y PC 31 – DUALSTACK	19
IMAGEN 9 – VERIFICACIÓN ESTADO CONFIGURACIÓN PING SERVER0 A R3, PC30 A R3 Y SERVER0 A R1	23
IMAGEN 10 – VERIFICACIÓN ESTADO CONFIGURACIÓN PING SERVER0 A ISP, PC30 A ISP Y R3 A R2	23
IMAGEN 11 – VERIFICACIÓN ESTADO CONFIGURACIÓN PING R1 A R3, R1 A R2 LAPTOP1 A R2	23
IMAGEN 12- VERIFICACIÓN ESTADO CONFIGURACIÓN PING PC0 A R2, PC1 A R2 Y LAPTOP0 A R2.....	23
IMAGEN 13 – ESCENARIO 2	24
IMAGEN 14 – ROUTER 1 PROTOCOLOS CONFIGURADOS Y VERIFICACIÓN PROTOCOLO OSPF .	30
IMAGEN 15 PING PARA LA VERIFICACIÓN DE COMUNICACIÓN PC 30 CON OTROS EQUIPOS	36
IMAGEN 16 TRACERT PARA VERIFICAR LAS RUTAS DESDE EL PC30 A OTROS EQUIPOS	36
IMAGEN 17 PING Y TRACERT PARA VERIFICAR LAS COMUNICACIONES CON OTROS EQUIPOS	36
IMAGEN 18 VERIFICACIÓN DE CONEXIÓN Y COMUNICACIÓN	37
IMAGEN 19 VERIFICACIÓN DE RUTAS	37
IMAGEN 20 VERIFICACIÓN DE CONEXIÓN POR MEDIO DEL COMANDO TRACERT Y PING	37
IMAGEN 21 VERIFICACIÓN DE CONFIGURACIÓN DEL PROTOCOLO OSPF EN R1	39
IMAGEN 22 DEL PROTOCOLO EN R2 Y LISTAS DE ACCESO	39
IMAGEN 23 VERIFICACIÓN DE LA CONFIGURACIÓN DEL PROTOCOLO OSPF EN R3.....	40

TABLAS

TABLA 1 – ENRUTAMIENTO ESCENARIO 1	6
TABLA 2 – ESCENARIO 1 LISTA COMPUTADORES	7
TABLA 3 – ESCENARIO 1 ASIGNACIÓN VLAN Y PUERTOS	7
TABLA 4 – ESCENARIO 1 ENLACE DE TRONCALES.....	7
TABLA 5 –ENRUTAMIENTO ESCENARIO 2	25
TABLA 6 – ENRUTAMIENTO PROTOCOLO OSPFV2	28