

PRUEBA DE HABILIDADES PRÁCTICAS

PRESENTADO POR:

JHON EDIER URIBE GORDILLO – 10051672

CEL – 3218038623

CURSO:

DIPLOMADO DE PROFUNDIZACIÓN CISCO

PRESENTADO A:

ING. NILSON ALBEIRO FERREIRA

TUTOR

ING. JUAN CARLOS VESGA

DIRECTOR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

INGENIERIA DE SISTEMAS

CEAD DOSQUEBRADAS

2018

TABLA DE CONTENIDO

Contenido

RESUMEN	3
INTRODUCCION	5
OBJETIVOS	6
1. DESARROLLO DE ESCENARIOS	7
3.1 ESCENARIO 1	7
3.2 ESCENARIO 2	16
2. CODIGO	26
3. CONCLUSIONES	45
4. BIBLOGRAFIA	46

RESUMEN

En la actualidad los sistemas informáticos se encuentran en casi todos los hogares y empresas, y con ellos el acceso a líneas ADSL y otras. Con la elaboración de estas pruebas finales la Universidad Nacional Abierta Y a Distancia 'UNAD' en conjunto con CISCO a través del Diplomado de profundización en redes basadas en el uso de tecnología cisco es un diplomado en el cual se aprende todo lo relacionado de las redes en implementación; esto nos permitió estudiar escenarios que pueden ser aplicados en la vida real.

Hoy en día ante las necesidades de las empresas en las telecomunicaciones es importante tener un conocimiento de base para realizar la administración de una red ya que es de vital importancia para sus negocios servicios a prestar, cuyo único objeto será ampliar su cobertura y mejorar la disponibilidad de su infraestructura de telecomunicaciones para su sede principal y sus sucursales.

ABSTRAC

At present, computer systems are found in almost all homes and businesses, and with them access to ADSL and other lines. With the elaboration of these final tests, the National Open and Distance University 'UNAD' in conjunction with CISCO through the Diploma of deepening in the networks in the use of technology is a diploma in which everything related to the story is learned. of the networks in implementation; This allows us to study so that they can be applied in real life.

Nowadays, in view of the needs of companies in telecommunications, it is important to have a knowledge of the base to carry out the administration of a network and which is of vital importance for your business or services at your service, whose sole purpose is to expand your coverage and improve the availability of its telecommunications infrastructure for its headquarters and its branches

INTRODUCCION

El examen de habilidades comprende protocolos de routing dinámico (RIPv2, OSPF), configuración de servers DHCP, Network Address Translation (NAT), Listas de Control de Acceso (ACL), dichas configuraciones pueden ser implementadas en routers para aumentar la seguridad de una red o implementar políticas de entrada y salida de paquetes para ciertos equipos específicos.

Se configuraron servidores DHCP, este es un protocolo de difusión que trabaja de forma predeterminada en donde sus paquetes no pasan a través de enrutadores; un agente de DHCP recibe cualquier difusión DHCP de la subred y la reenvía a la dirección IP especificada en una subred distinta.

En la actualidad ante las necesidades de las empresas en las telecomunicaciones es importante saber y administrar una red ya que es de vital importancia para sus negocios o servicios a prestar. El caso de estudio planteado en este módulo es para aplicar la configuración del protocolo de enrutamiento OSPF, entender al manejo y aplicarlo en el Packet Tracer.

OBJETIVOS

2.1 OBJETIVO GENERAL

Conceptualizar y aplicar las habilidades prácticas, teóricas y experiencia por parte de nosotros como futuros ingenieros de Sistemas de la Universidad Nacional Abierta y a Distancia, mediante un caso práctico propuesto por la Universidad en compañía de sus tutores y Cisco.

2.2 OBJETIVOS ESPECÍFICOS

- Identificar que dispositivos y periféricos a utilizar para la construcción de una topología de red.
- Determinar la configuración necesaria para la implementación de OPSFv2, protocolo dinámico de Routing.
- Configurar y verificar listas de control de acceso ACL
- Verificar conectividad entre los dispositivos de una topología
- Desarrollar un informe con evidencias donde se aplique y configure una solución práctica descrita en el escenario propuesto en la prueba de habilidades.
- Generar un escenario virtual en Packet Tracer (archivo de extensión pka)

1. DESARROLLO DE ESCENARIOS

3.1 ESCENARIO 1

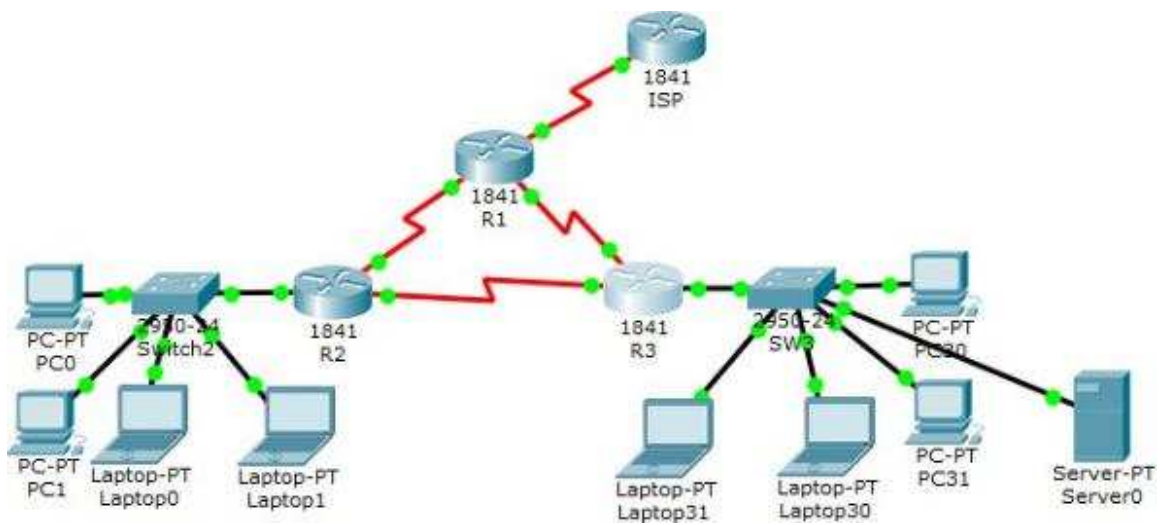


Tabla de direccionamiento

El administrador	Interfaces	Dirección IP	Máscara de subred	Gateway predeterminado
ISP	S0/0/0	200.123.211.1	255.255.255.0	N/D
	Se0/0/0	200.123.211.2	255.255.255.0	N/D
R1	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
		192.168.30.1	255.255.255.0	N/D

R3	Fa0/0	2001:db8:130::9C0:80F:301	/64	N/D
	Se0/0/0	10.0.0.6	255.255.255.252	N/D
	Se0/0/1	10.0.0.10	255.255.255.252	N/D
SW2	VLAN 100	N/D	N/D	N/D
	VLAN 200	N/D	N/D	N/D
SW3	VLAN1	N/D	N/D	N/D

PC20	NIC	DHCP	DHCP	DHCP
PC21	NIC	DHCP	DHCP	DHCP
PC30	NIC	DHCP	DHCP	DHCP
PC31	NIC	DHCP	DHCP	DHCP
Laptop20	NIC	DHCP	DHCP	DHCP
Laptop21	NIC	DHCP	DHCP	DHCP
Laptop30	NIC	DHCP	DHCP	DHCP
Laptop31	NIC	DHCP	DHCP	DHCP

Tabla de asignación de VLAN y de puertos

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

Tabla de enlaces troncales

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

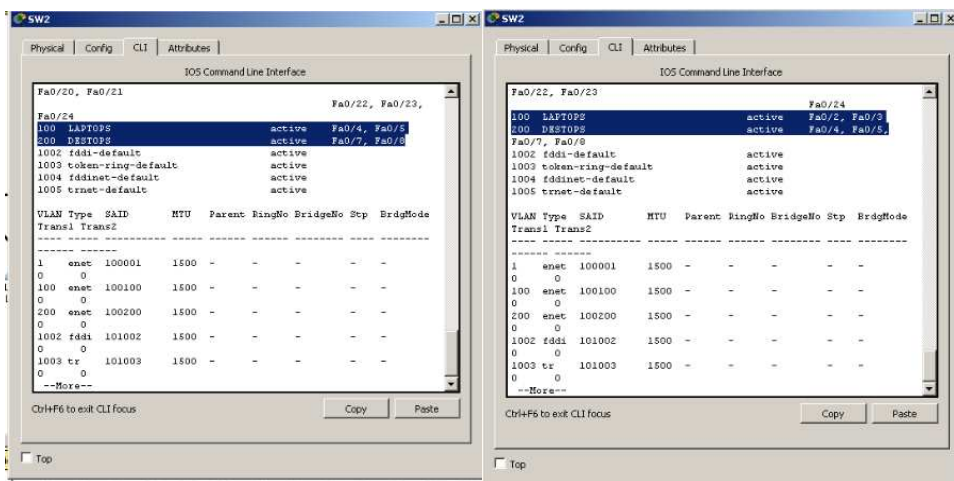
Situación

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

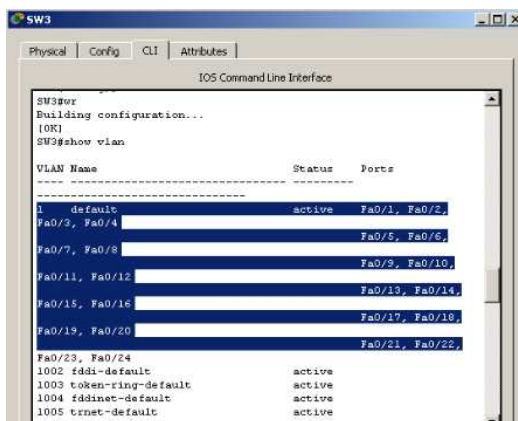
3.1.1 Descripción De Las Actividades

- Se realiza la configuración del SW2 VLAN y se dan las asignaciones de puertos de VLAN deben cumplir con la tabla 1. Para esto se utilizaron los comandos Enable y Configure terminal

Se cambia el nombre del dispositivo con el comando hostname y el nombre del asignado al dispositivo switch con el nombre SW2



- Aquí se describen los rangos de puertos activos a través del comando Show Vlan, de igual manera se configura el puerto del switch con el comando switchport mode trunk



- Los puertos de red que no se utilizan se deben deshabilitar, se hace uso del comando Shutdown.

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	--	--	0090.2BB1.BA96
FastEthernet0/2	Up	1	--	00E0.B068.8868
FastEthernet0/3	Up	1	--	0009.7C31.0889
FastEthernet0/4	Up	1	--	00D0.FEB9.48BD
FastEthernet0/5	Up	1	--	0007.EC16.4D7E
FastEthernet0/6	Down	1	--	0001.C941.226C
FastEthernet0/7	Down	1	--	000A.4198.5509
FastEthernet0/8	Down	1	--	0000.0C54.8C4C
FastEthernet0/9	Down	1	--	0090.0C95.1C34
FastEthernet0/10	Down	1	--	000A.4182.43C6
FastEthernet0/11	Down	1	--	0001.9777.8A4D
FastEthernet0/12	Down	1	--	000A.F3BE.28D6
FastEthernet0/13	Down	1	--	0000.0CB0.2E83
FastEthernet0/14	Down	1	--	0060.3E7E.C5E4
FastEthernet0/15	Down	1	--	0004.9A03.A822
FastEthernet0/16	Down	1	--	0060.5C3B.176A
FastEthernet0/17	Down	1	--	0000.0CE0.5B15
FastEthernet0/18	Down	1	--	0060.2F9B.7E87
FastEthernet0/19	Down	1	--	0003.E42D.28C2
FastEthernet0/20	Down	1	--	0030.F285.CC81
FastEthernet0/21	Down	1	--	0001.4388.6802
FastEthernet0/22	Down	1	--	0002.48EB.D73A
FastEthernet0/23	Down	1	--	0060.704B.7888
FastEthernet0/24	Up	1	--	0030.A314.EE90
Vlan1	Down	1	<not set>	00D0.58E0.16EB

Hostname: SW3
Physical Location: Interurbano, Ciudad de residencia, Oficina corporativa, Armario de cableado principal

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Up	--	--	0000.0CB5.7301
FastEthernet0/2	Up	100	--	0000.0CB5.7302
FastEthernet0/3	Up	100	--	0000.0CB5.7303
FastEthernet0/4	Up	200	--	0000.0CB5.7304
FastEthernet0/5	Up	200	--	0000.0CB5.7305
FastEthernet0/6	Down	1	--	0000.0CB5.7306
FastEthernet0/7	Down	200	--	0000.0CB5.7307
FastEthernet0/8	Down	200	--	0000.0CB5.7308
FastEthernet0/9	Down	1	--	0000.0CB5.7309
FastEthernet0/10	Down	1	--	0000.0CB5.730A
FastEthernet0/11	Down	1	--	0000.0CB5.730B
FastEthernet0/12	Down	1	--	0000.0CB5.730C
FastEthernet0/13	Down	1	--	0000.0CB5.730D
FastEthernet0/14	Down	1	--	0000.0CB5.730E
FastEthernet0/15	Down	1	--	0000.0CB5.730F
FastEthernet0/16	Down	1	--	0000.0CB5.7310
FastEthernet0/17	Down	1	--	0000.0CB5.7311
FastEthernet0/18	Down	1	--	0000.0CB5.7312
FastEthernet0/19	Down	1	--	0000.0CB5.7313
FastEthernet0/20	Down	1	--	0000.0CB5.7314
FastEthernet0/21	Down	1	--	0000.0CB5.7315
FastEthernet0/22	Down	1	--	0000.0CB5.7316
FastEthernet0/23	Down	1	--	0000.0CB5.7317
FastEthernet0/24	Down	1	--	0000.0CB5.7318
Vlan1	Down	1	<not set>	0002.4A25.026D

Hostname: SW2
Physical Location: Interurbano, Ciudad de residencia, Oficina corporativa, Armario de cableado principal

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

```

R1>enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/0/0
R1(config-if)#ip add 200.123.211.2 255.255.255.0
R1(config-if)#exit
R1(config)#int S0/1/0
R1(config-if)#ip add 10.0.0.1 255.255.255.252
R1(config-if)#exit
R1(config)#int S0/1/1
R1(config-if)#ip add 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]

```

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	<not set>	<not set>	<not set>	0060.3E21.BA01
FastEthernet0/0.100	Up	--	192.168.20.1/24	<not set>	0060.3E21.BA01
FastEthernet0/0.200	Up	--	192.168.21.1/24	<not set>	0060.3E21.BA01
FastEthernet0/1	Up	--	<not set>	<not set>	0060.3E21.BA02
Serial0/0/0	Up	--	10.0.0.2/30	<not set>	<not set>
Serial0/0/1	Up	--	10.0.0.9/30	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	0003.E434.7022

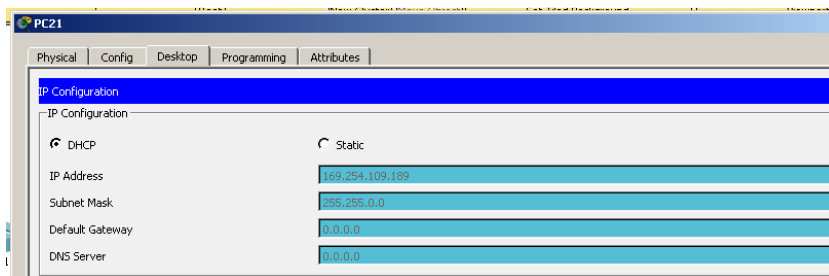
Hostname: R2
Physical Location: Interurbano, Ciudad de residencia, Oficina corporativa, Armario de cableado principal

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
FastEthernet0/0	Up	--	192.168.30.1/24	2001:DB8:130::9C0:80F:301/64	00E0.F762.CC62
FastEthernet0/1	Up	--	<not set>	<not set>	0090.0CB8.E568
Serial0/0/0	Up	--	10.0.0.6/30	<not set>	<not set>
Serial0/0/1	Up	--	10.0.0.10/30	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	000C.859C.4C35

Hostname: R3

Physical Location: Interurbano, Ciudad de residencia, Oficina corporativa, Armario de cableado principal

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



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

```

R1#
R1#enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int s0/1/1
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#int s0/1/0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#int s0/0/0
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#ip nat pool INSIDE-DEVS 200.123.211.2 200.123.211.128
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(config)#exit
R1#end
*SYS-5-CONFIG_I: Configured from console by console

Translating "end"...domain server (255.255.255.255)

```

- R1 debe tener una ruta estática predeterminada al ISP que se configuró y que incluye esa ruta en el dominio RIPv2. Se procede con la ejecución del comando SHOW IP NAT STATIC , es sus respectivas interfaces.

```

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

```

- R2 es un servidor de DHCP para los dispositivos conectados al puerto FastEthernet0/0.
- R2 debe, además de enrutamiento a otras partes de la red, ruta entre las VLAN 100 y 200.

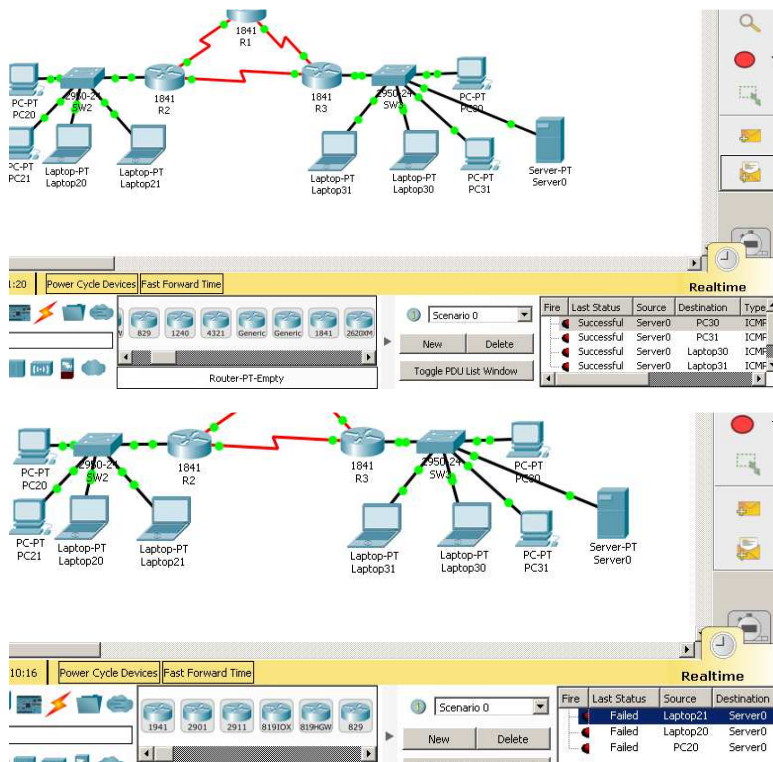
```

R2>enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#ip dhcp excluded-address 10.0.0.2 10.0.0.9
R2(config)#ip dhcp pool INSIDE-DEVS
R2(dhcp-config)#network 192.168.20.1 255.255.255.0
R2(dhcp-config)#network 192.168.21.1 255.255.255.0
R2(dhcp-config)#default-router 192.168.1.1
R2(dhcp-config)#dns-server 0.0.0.0
R2(dhcp-config)#exit
R2(config)#int vlan 100
R2(config-if)#ip add 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 add 192.168.21.1 255.255.255.0
% 192.168.21.0 overlaps with FastEthernet0/0.200
R2(config-if)#exit
R2(config)#end
R2#wr
%SYS-5-CONFIG_I: Configured from console by console

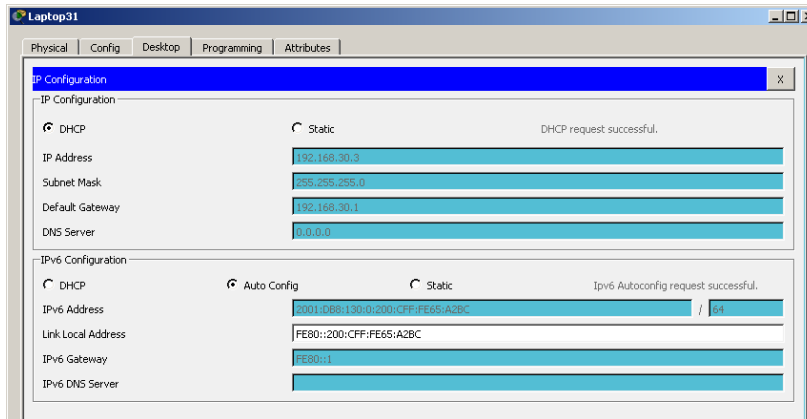
Building configuration...
[OK]

```

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



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

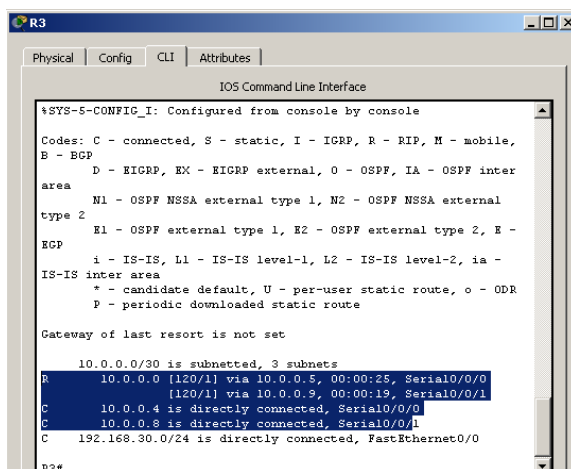


- La interfaz FastEthernet 0/0 del R3 también deben tener direcciones IPv4 e IPv6 configuradas (dual- stack).

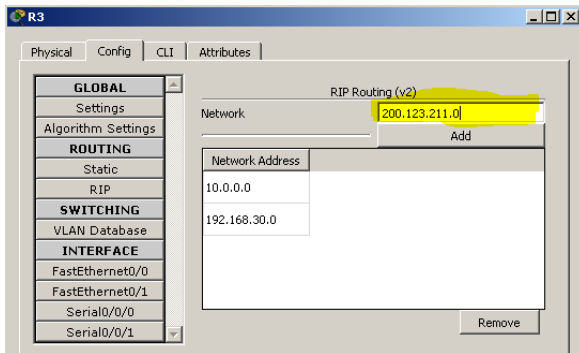
```
R3>enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#route rip
R3(config-router)#version 2
R3(config-router)#do show ip route connected
C 10.0.0.4/30 is directly connected, Serial0/0/0
C 10.0.0.8/30 is directly connected, Serial0/0/1
C 192.168.30.0/24 is directly connected, FastEthernet0/0

R3(config-router)#net
R3(config-router)#network 10.0.0.4
R3(config-router)#net
R3(config-router)#network 10.0.0.8
R3(config-router)#do show ip route connected
C 10.0.0.4/30 is directly connected, Serial0/0/0
C 10.0.0.8/30 is directly connected, Serial0/0/1
C 192.168.30.0/24 is directly connected, FastEthernet0/0
```

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

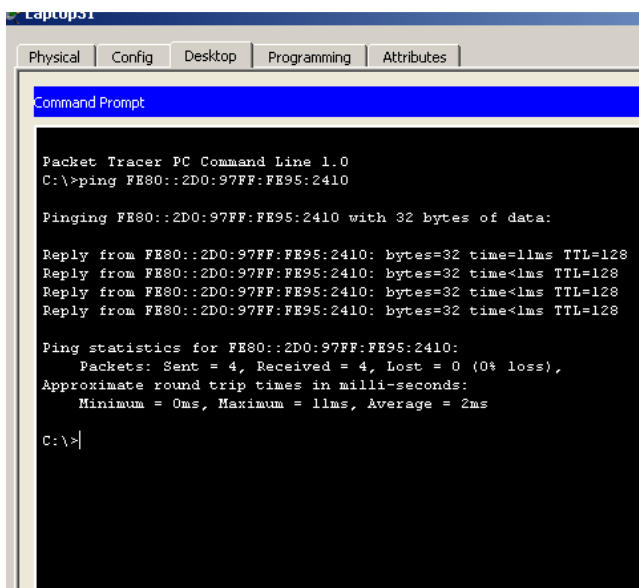


- R1, R2 y R3 deben saber sobre las rutas de cada uno y la ruta predeterminada desde R1.

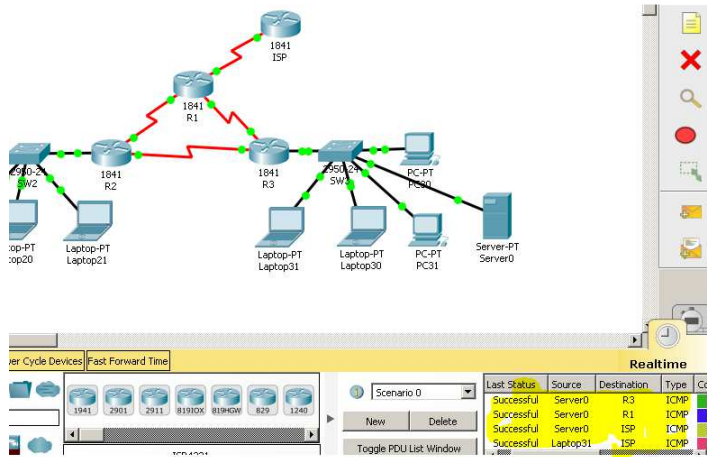


Verifique la conectividad. Todos los terminales deben poder hacer ping entre sí y a la dirección IP del ISP. Los terminales bajo el R3 deberían poder hacer IPv6-ping entre ellos y el servidor.

Se evidencia el ping de los terminales , desde el Laptop 31

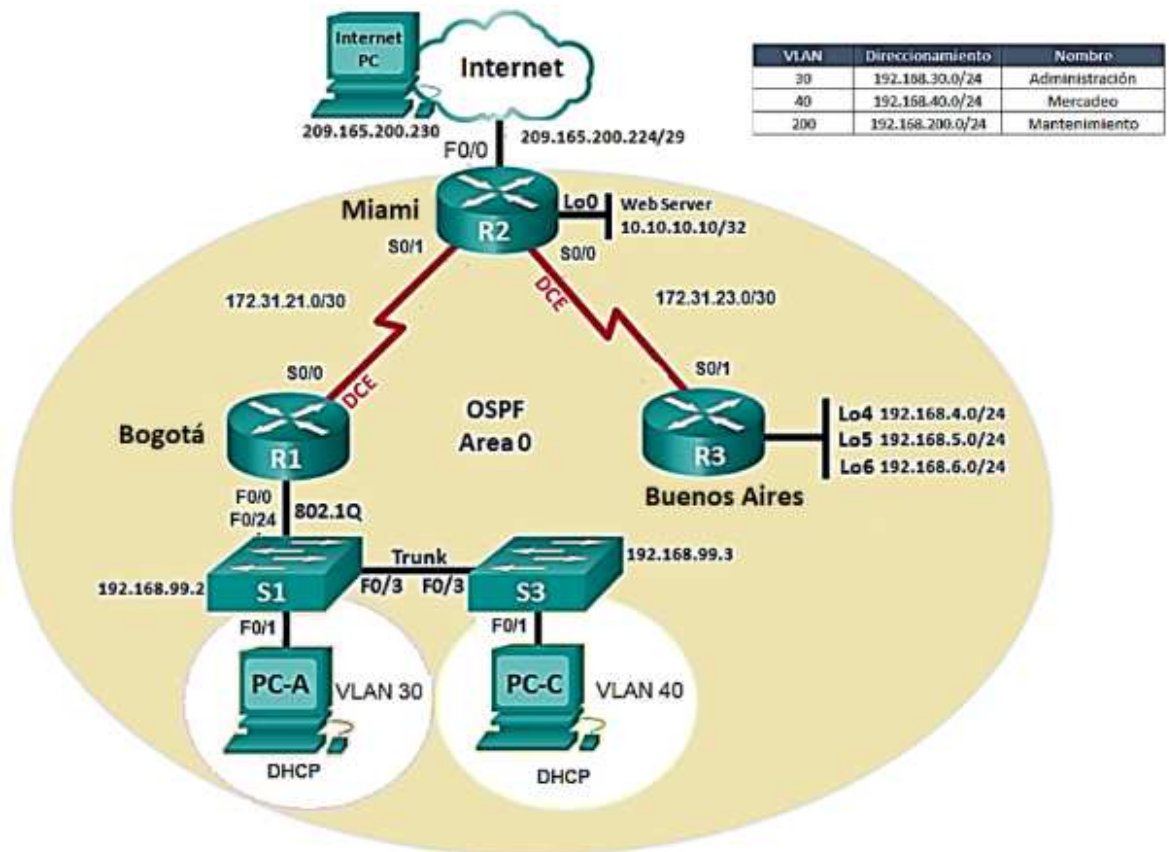


Por medio de este gráfico se evidencia cada uno los dispositivos conectados entre sí.



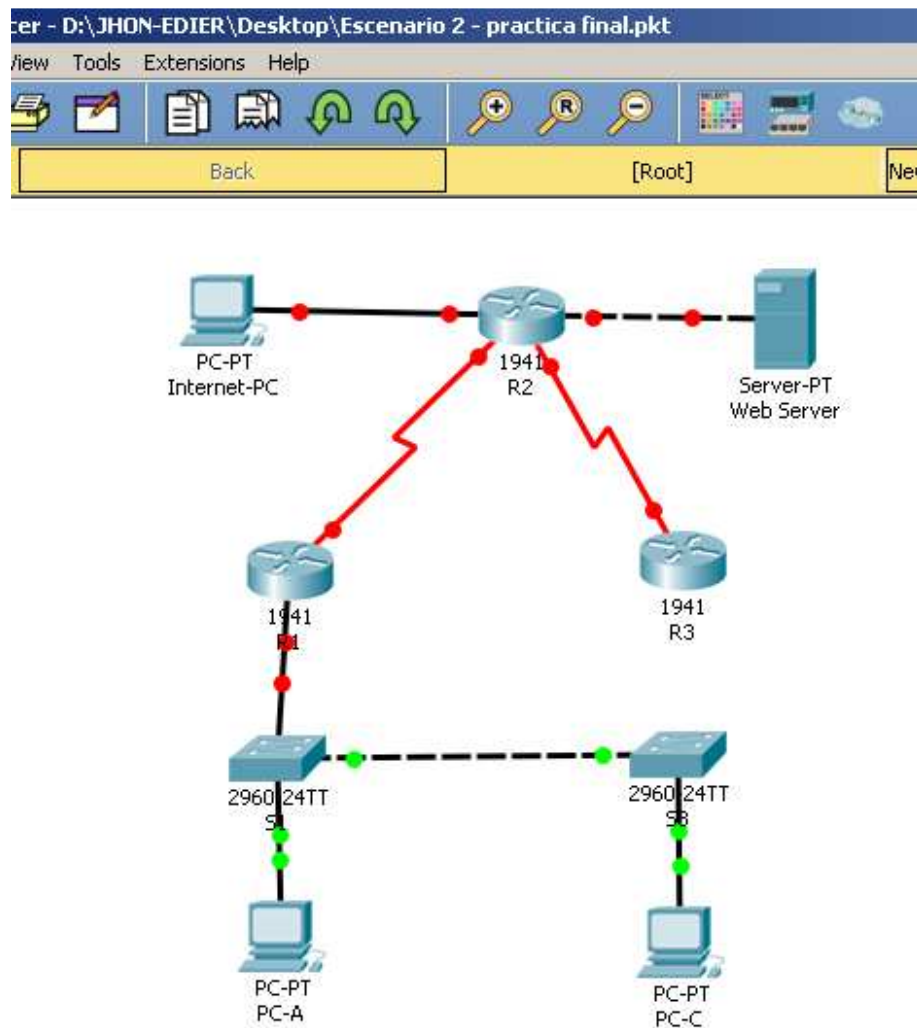
3.2 ESCENARIO 2

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



3.2.1 Desarrollo Del Ejercicio

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



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


```

R3>enable
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#int lo4
R3(config-if)#ip add 192.168.4.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo5
R3(config-if)#ip add 192.168.5.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo6
R3(config-if)#ip add 192.168.6.1 255.255.255.0
R3(config-if)#

```

- Se realiza configuración de los dispositivos S1-S3

<pre> S1>en Password: S1#enable S1#conf t Enter configuration commands, one per line. S1(config)#no ip domain-lookup S1(config)#hostname S1 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)#exit S1(config)#service password-encryption S1(config)#banner motd \$Prohibido el Acceso S1(config)#exit S1#copy running-config startup-config !SYS-5-CONFIG_I: Configured from console by Destination filename [startup-config]? Building configuration... [OK] S1# </pre>	<pre> S3>enable Password: S3#enable S3#conf t Enter configuration commands, one per line. End with CNTL/Z. S3(config)#no ip domain-lookup S3(config)#hostname S3 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)#exit S3(config)#service password-encryption S3(config)#banner motd \$Prohibido el Acceso No Autorizado\$ S3(config)#exit S3#copy running-config startup-config !SYS-5-CONFIG_I: Configured from console by console Destination filename [startup-config]? Building configuration... [OK] S3# </pre>
--	---

2. 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

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.

```

Enter configuration commands, one per line.
R1(config)#router ospf 1
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 172.31.21.0 0.0.0.0
R1(config-router)#network 192.168.30.0 0.0.0.0
R1(config-router)#network 192.168.40.0 0.0.0.0
R1(config-router)#network 192.168.200.0 0.0.0.0
R1(config-router)#passive-interface g0/1.30
%Invalid interface type and number
R1(config-router)#passive-interface g0/1.40
%Invalid interface type and number
R1(config-router)#passive-interface g0/1.200
%Invalid interface type and number
R1(config-router)#auto-cost reference-bandwidth 1
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)#exitReload or use "clear ip ospf cost"
for this to take effect
R1(config)#

Password:
R2>enable
Password:
R2#enable
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 0.0.0.0
R2(config-router)#network 10.10.10.0 0.0.0.0
R2(config-router)#passive-interface s0/0/1
% OSPF: Reference bandwidth is changed. Please ensure reference bandwidth is the same on all routers.
R2(config-router)#exit
R2(config)#int s0/0/0
R2(config-if)#bandwidth 256
R2(config-if)#int s0/0/1
R2(config-if)#bandwidth 256
R2(config-if)#ip ospf cost 9500
R2(config-if)#exit
R2(config)#

R3(config)#ip ospf cost 9500
^
% Invalid input detected at '^' marker.
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console
R3#enable
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 0.0.3.255 area 0
R3(config-router)#passive-interface lo4
R3(config-router)#passive-interface lo5
R3(config-router)#passive-interface lo6
R3(config-router)#auto-cost reference-bandwidth 9500
R3(config-router)#exit
R3(config)#int s0/0/1
R3(config-if)#bandwidth 256
R3(config-if)#ip ospf cost 9500
R3(config-if)#exit
R3(config)#

```

```

R2#show ip ospf interface

Serial0/0/0 is up, line protocol is up
  Internet address is 172.31.21.2/30, Area 0
  Process ID 1, Router ID 5.5.5.5, Network Type POINT-TO-POINT,
  Cost: 6152
  Transmit Delay is 1 sec, State POINT-TO-POINT, Priority 0
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:04
  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
  Suppress hello for 0 neighbor(s)
Serial0/0/1 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, Wait 40,

```

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

Configuración VLAN 30 y 40 en el S1, S2 Y S3

```

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line 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 password-encryption
R1(config)#banner motd $Prohibido el
R1(config)#int s0/0/0
R1(config-if)#ip add 172.31.21.1 255.255.255.255
R1(config-if)#clock rate 128000
R1(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%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(config-if)#
%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

R2(config-if)#int c0/0
R2(config-if)#description conexion a ISP
R2(config-if)#ip add 209.165.200.255 255.255.255.255
Bad mask /29 for address 209.165.200.255
R2(config-if)#no shut

R2(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up

R2(config-if)#
%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

Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R3
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 No Autorizado
R3(config)#int s0/0/1
R3(config-if)#ip add 172.31.23.2 255.255.255.252
R3(config-if)#no shut

R3(config-if)#
%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

```

4. En el Switch 3 deshabilitar DNS lookup, se procede a realizar la configuración del dispositivo

```

Switch>
Switch#enable
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

```

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

6. Desactivar todas las interfaces que no sean utilizadas en el esquema de red. Por lo tanto se desactivan las interfaces en el R1, R2 Y R3

```

R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface f0/0
R1(config-if)#interface f0/1
R1(config-if)#shutdown
R1(config-if)#interface s0/0/1
R1(config-if)#shutdown
R1(config-if)#

```

```

R2>enable
R2#config t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface f0/1
R2(config-if)#shutdown
R2(config-if)#

```

```

R3>enable
R3#config t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#interface f0/0
R3(config-if)#shutdown
R3(config-if)#interface f0/1
R3(config-if)#shutdown
R3(config-if)#interface s0/0/0
R3(config-if)#shutdown
R3(config-if)#

```

7. Implement DHCP and NAT for IPv4, se procede a realizar la configuración DHCP y NAT Router 1

```
R1>enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp pool ADMINISTRACION
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.30.1
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#enable
R1#config t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp pool MERCADEO
R1(dhcp-config)#network 192.168.40.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.40.1
R1(dhcp-config)#dns-server 10.10.10.11
R1(dhcp-config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console
```

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

El dispositivo R1, se configura como Servidor DHCP de las VLANs 30 y 40

```
R1#show ip dhcp binding
IP address      Client-ID/      Lease expiration   Type
Hardware address
192.168.30.31   0004.SAE7.0B77  --                 Automatic
192.168.40.31   0001.431C.D225  --                 Automatic
```

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

Configurar DHCP pool para VLAN 30	Name: ADMINISTRACION DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.
Configurar DHCP pool para VLAN 40	Name: MERCADEO DNS-Server: 10.10.10.11 Domain-Name: ccna-unad.com Establecer default gateway.

```

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

```

10. Configurar NAT en R2 para permitir que los host puedan salir a internet, se procede a realizar la configuración.

```

R2>en
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#user webuser privilege 15 secret cisco12345
R2(config)#ip http server
      ^
% Invalid input detected at '^' marker.

R2(config)#ip http authentication local
      ^
% Invalid input detected at '^' marker.

R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int f0/0
R2(config-if)#ip nat outside
R2(config-if)#int f0/1
R2(config-if)#ip nat inside
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

```

11. 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)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int f0/0
R2(config-if)#ip nat outside
R2(config-if)#int f0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#acc
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)#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 acc
R2(config)#ip access-list sta
R2(config)#ip access-list standard ADMIN_S
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#acc
R2(config-line)#acce
R2(config-line)#access-class ADMIN_S in

```

12. 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. Se configuran las listas de acceso en el R2

```
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.229
R2(config)#int f0/0
R2(config-if)#ip nat outside
R2(config-if)#int f0/1
R2(config-if)#ip nat inside
R2(config-if)#end
R2#
%SYS-5-CONFIG_I: Configured from console by console

R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
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)#
```

```
R2(config)#ip access-list sta
R2(config)#ip access-list standard ADMIN_S
R2(config-std-nacl)#permit host 172.31.21.1
R2(config-std-nacl)#exit
R2(config)#line vty 0 4
R2(config-line)#acc
R2(config-line)#acce
R2(config-line)#access-class ADMIN_S in
R2(config-line)#exit
R2(config)#access
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
R2(config-if)#ip access-group 101 in
R2(config-if)#int s0/0/0
R2(config-if)#ip access
R2(config-if)#ip access-group 101 out
R2(config-if)#ip access
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 f0/1
R2(config-if)#ip access-group 101 out
```

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

Evidencia del comando ping en la comunicación con los routers, desde el PC-A

```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 169.254.188.230

Pinging 169.254.188.230 with 32 bytes of data:

Reply from 169.254.188.230: bytes=32 time=13ms TTL=128
Reply from 169.254.188.230: bytes=32 time=4ms TTL=128
Reply from 169.254.188.230: bytes=32 time<1ms TTL=128
Reply from 169.254.188.230: bytes=32 time<1ms TTL=128

Ping statistics for 169.254.188.230:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 4ms
```

Evidencia del comando ping en la comunicación con los routers desde el PC-C

```
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 169.254.196.144

Pinging 169.254.196.144 with 32 bytes of data:

Reply from 169.254.196.144: bytes=32 time=12ms TTL=128
Reply from 169.254.196.144: bytes=32 time<1ms TTL=128
Reply from 169.254.196.144: bytes=32 time<1ms TTL=128
Reply from 169.254.196.144: bytes=32 time<1ms TTL=128

Ping statistics for 169.254.196.144:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

Evidencia de comunicación Web Server



2. CODIGO

3.1 Escenario 1

```
--SW2
enable
conf t
vlan 100
name LAPTOPS
exit
vlan 200
name DESTOPS
exit
end
wr
show vlan

enable
conf t
int range fa0/2-3
switchport mode access
switchport access vlan 100
int range fa0/4-5
switchport mode access
switchport access vlan 200
exit
end
```

```
--SW3
enable
conf t
vlan 1
exit
int range fa0/1-24
switchport mode access
switchport access vlan 1
exit
end
wr
show vlan
```

```
conf t
int range fa0/6-23
shutdown
end
wr
```

```
--SW3
enable
conf t
int range fa0/6-23
shutdown
exit
```

```
int f0/1
switchport mode trunk
end
wr
```

```
--SW2
conf t
int range fa0/6-24
shutdown
exit
end
wr
```

```
conf t
int f0/1
switchport mode trunk
end
wr
```

```
--R1
enable
conf t
int s0/0/0
ip add 200.123.211.2 255.255.255.0
exit
int S0/1/0
ip add 10.0.0.1 255.255.255.252
exit
int S0/1/1
ip add 10.0.0.5 255.255.255.252
end
wr
```

```
--R2
enable
```

```
conf t
int f0/0.100
encapsulation dot1Q 100
ip add 192.168.20.1 255.255.255.0
exit
int f0/0.200
encapsulation dot1Q 200
ip add 192.168.21.1 255.255.255.0
exit
int s0/0/0
ip add 10.0.0.2 255.255.255.252
exit
int s0/0/1
ip add 10.0.0.9 255.255.255.252
exit
end
wr
```

```
--R3
enable
conf t
int f0/0
ip add 192.168.30.1 255.255.255.0
exit
ipv6 unicast-routing
int s0/0/0
ip add 10.0.0.6 255.255.255.0
int s0/0/1
ip add 10.0.0.10 255.255.255.0
exit
end wr
```

```
--R1
enable
conf t
int s0/1/1
ip nat inside
exit
int s0/1/0
ip nat inside
exit
int s0/0/0
ip nat outside
exit
ip nat pool INSIDE-DEVS 200.123.211.2 200.123.211.128 netmask
255.255.255.0
access-list 1 permit 192.168.0.0 0.0.255.255
access-list 1 permit 10.0.0.0 0.255.255.255
ip nat inside source list 1 interface s0/0/0 overload
ip nat inside source static tcp 192.168.30.6 80 200.123.211.1 80
exit
end
```

```
--R1
enable
conf t
router rip
version 2
network 10.0.0.0
exit
end
wr
show ip nat translations
```

```
show ip nat statistics
```

```
--R2
```

```
enable
```

```
conf t
```

```
ip dhcp excluded-address 10.0.0.2 10.0.0.9
```

```
ip dhcp pool INSIDE-DEVS
```

```
network 192.168.20.1 255.255.255.0
```

```
network 192.168.21.1 255.255.255.0
```

```
default-router 192.168.1.1
```

```
dns-server 0.0.0.0
```

```
exit
```

```
end
```

```
--R2
```

```
enable
```

```
conf t
```

```
int vlan 100
```

```
ip add 192.168.20.1 255.255.255.0
```

```
exit
```

```
int vlan 200
```

```
ip add 192.168.21.1 255.255.255.0
```

```
exit
```

```
end
```

```
wr
```

```
--R3
```

```
enable
```

```
conf t
```

```
ipv6 unicast-routing
```

```
int f0/0
```

```
ipv6 enable
ip address 192.168.30.1 255.255.255.0
ipv6 address 2001:db8:130::9C0:80F:301/64
no shut
```

```
--R1
enable
conf t
router rip
version 2
network 10.0.0.0
network 10.0.0.4
do show ip route connected
end
wr
```

```
--R2
enable
conf t
router rip
version 2
network 10.0.0.0
network 10.0.0.8
do show ip route connected
end
wr
```

```
--R3
enable
conf t
router rip
```



```
version 2
network 10.0.0.0
network 10.0.0.8
do show ip route connected
end
wr
show ip route
```

3.2 Escenario 2

```
--R1
enable
conf t
no ip domain-lookup
hostname R1
enable secret class
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
exit
service password-encryption
banner motd $Prohibido el Acceso No Autorizado$
int s0/0/0
ip add 172.31.21.1 255.255.255.252
clock rate 128000
no shut
```

```
--R2
enable
conf t
no ip domain-lookup
hostname R2
enable secret class
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
exit
service password-encryption
banner motd $Prohibido el Acceso No Autorizado$
int s0/0/0
ip add 172.31.21.2 255.255.255.252
no shut
int s0/0/1
ip add 172.31.23.1 255.255.255.252
no shut
int G0/0
description conexion a ISP
ip add 209.165.200.255 255.255.255.248
no shut
```

```
--R3
enable
conf t
no ip domain-lookup
hostname R3
enable secret class
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
exit
service password-encryption
banner motd $Prohibido el Acceso No Autorizado$
int s0/0/1
ip add 172.31.23.2 255.255.255.252
no shut
int lo4
ip add 192.168.4.1 255.255.255.0
no shut
int lo5
ip add 192.168.5.1 255.255.255.0
no shut
int lo6
ip add 192.168.6.1 255.255.255.0
```

```
--S1
enable
conf t
no ip domain-lookup
hostname S1
enable secret class
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
exit
service password-encryption
banner motd $Prohibido el Acceso No Autorizado$
exit
copy running-config startup-config
```

```
--S3
enable
conf t
no ip domain-lookup
hostname S3
enable secret class
line con 0
pass cisco
login
```

```
line vty 0 4
pass cisco
login
exit
service password-encryption
banner motd $Prohibido el Acceso No Autorizado$
exit
copy running-config startup-config

--R1
enable
conf t
router ospf 1
router-id 1.1.1.1
network 172.31.21.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.3 area 0
network 192.168.40.0 0.0.0.3 area 0
network 192.168.30.0 0.0.0.255 area 0
network 192.168.40.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
passive-interface g0/1.30
passive-interface g0/1.40
passive-interface g0/1.200
auto-cost reference-bandwidth 9500
exit
int s0/0/0
bandwidth 256
```

```
ip ospf cost 9500
```

```
exit
```

```
--R2
```

```
enable
```

```
conf t
```

```
router ospf 1
```

```
router-id 5.5.5.5
```

```
network 172.31.21.0 0.0.0.3 area 0
```

```
network 172.31.23.0 0.0.0.3 area 0
```

```
network 10.10.10.10 0.0.0.255 area 0
```

```
passive-interface g0/1
```

```
auto-cost reference-bandwidth 9500
```

```
exit
```

```
int s0/0/0
```

```
bandwidth 256
```

```
int s0/0/1
```

```
bandwidth 256
```

```
ip ospf cost 9500
```

```
exit
```

```
--R3
```

```
enable
```

```
conf t
```

```
router ospf 1
```

```
router-id 8.8.8.8
```

```
network 172.31.23.0 0.0.0.3 area 0
```

```
network 192.168.4.0 0.0.3.255 area 0
passive-interface lo4
passive-interface lo5
passive-interface lo6
auto-cost reference-bandwidth 9500
exit
int s0/0/1
bandwidth 256
ip ospf cost 9500
exit
```

--S1

```
conf t
vlan 30
name Administracion
vlan 40
name Mercadeo
vlan 200
name Mantenimiento
exit
```

```
int vlan 200
ip add 192.168.99.2 255.255.255.0
no shut
exit
ip default-gateway 192.168.99.1
int f0/3
```

```
switchport mode trunk
switchport trunk native vlan 1
int f0/24
switchport mode trunk
switchport trunk native vlan 1

int range fa0/2, fa0/4-23, g0/1-2
switch mode access
int fa0/1
switch mode access
switch access vlan 30
int range fa0/2, fa0/4-23, g0/1-2
shutdown

--S3
conf t
vlan 30
name Administracion
vlan 40
name Mercadeo
vlan 200
name Mantenimiento
exit
int vlan 200
ip add 192.168.99.3 255.255.255.0
no shut
exit
```



```
ip default-gateway 192.168.99.1
```

```
--R1
```

```
conf t
```

```
int g0/1.30
```

```
encapsulatio dot1q 30
```

```
ip add 192.168.30.1 255.255.255.0
```

```
int g0/1.40
```

```
encapsulatio dot1q 40
```

```
ip add 192.168.40.1 255.255.255.0
```

```
int g0/1.200
```

```
encapsulatio dot1q 200
```

```
ip add 192.168.200.1 255.255.255.0
```

```
exit
```

En el Switch 3 deshabilitar DNS lookup

```
--S3
```

```
enable
```

```
conf t
```

```
no ip domain-lookup
```

Asignar direcciones IP a los Switches acorde a los lineamientos.

```
--S1
```

```
enable
```

```
conf t
```

```
ip add 192.168.99.2 255.255.255.0
```

```
no shut
```

```
exit
```

```
--S3
```

```
enable
```

```
conf t
```

```
ip add 192.168.99.3 255.255.255.0
```

```
no shut
```

```
exit
```

```
ip default-gateway 192.168.99.1
```

```
--S1
```

```
int range fa0/2, fa0/4-23, g0/1-2
```

```
shutdown
```

```
--S3
```

```
int range fa0/2, fa0/4-24, g0/1-2
```

```
shutdown
```

Implement DHCP and NAT for IPv4

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

```
--R1
```

```
conf t
```

```
ip dhcp excluded-address 192.168.30.1 192.168.30.30
```

```
ip dhcp excluded-address 192.168.40.1 192.168.40.30
```

```
ip dhcp pool administracion
dns-server 10.10.10.11
default-router 192.168.30.1
network 192.168.30.0 255.255.255.0
ip dhcp pool mercadeo
dns-server 10.10.10.11
default-router 192.168.40.1
network 192.168.40.0 255.255.255.0
```

```
--R2
conf t
ip http server
ip http authentication local
ip nat inside source static 10.10.10.10 209.165.200.229
int S0/0/0
ip nat outside
int S0/0/1
ip nat inside
```

```
--R2
conf t
access-list 1 permit 192.168.30.0 0.0.0.255
access-list 1 permit 192.168.40.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.3.255
ip nat pool Internet 209.165.200.225 209.165.200.229 netmask 255.255.255.248
ip nat inside source list 1 pool Internet
```

```
--R2
conf t
ip access-list standard ADMIN_S
permit host 172.31.21.1
exit
line vty 0 4
access-class ADMIN_S in
```

```
--R2
access-list 101 permit tcp any host 209.165.200.229 eq www
access-list 101 permit icmp any any echo-reply
int g0/0
ip access-group 101 in
int s0/0/0
ip access-group 101 out
int s0/0/1
ip access-group 101 out
int g0/1
ip access-group 101 out
```

3. CONCLUSIONES

Durante el curso destacamos la importancia de ampliar nuestros conocimientos y habilidades los cuales nos permiten una mejor configuración de los dispositivos que requerimos usar, con la elaboración de este proyecto notamos como podemos interconectar varias redes como lo haríamos en un caso de la vida real; para esto se tuvieron en cuenta los conceptos, situaciones estudiadas, las configuraciones que aplicamos de manera correcta y óptimas en los diferentes dispositivos, logrando integrar las sedes que se plantearon, logrando así centralizar la información brindando seguridad y organización.

Para finalizar es importante resaltar como con el desarrollo del presente trabajo y demás prácticas ejecutadas fue posible demostrar destrezas en cuanto a la configuración de equipos de red Cisco, como Routers y Switches.

4. BIBLOGRAFIA

Temática: Enrutamiento entre VLANs

CISCO. (2014). Enrutamiento entre VLANs. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module5/index.html#5.0.1.1>

Temática: Enrutamiento Estático

CISCO. (2014). Enrutamiento Estático. Principios de Enrutamiento y Conmutación. Recuperado de <https://static-course-assets.s3.amazonaws.com/RSE50ES/module6/index.html#6.0.1.1>

Temática: Enrutamiento Dinámico

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

Temática: Listas de control de acceso

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

Temática: DHCP

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

Temática: Traducción de direcciones IP para IPv4

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>