

Evaluación – Prueba de habilidades prácticas CCNA

Ruben Dario Pencue Puentes

CC. 1079606725

Grupo 203092_36

Tutor

Giovanni Alberto Bracho

Director del curso

Juan Carlos Vesga

Universidad Nacional Abierta y a Distancia –
UNAD
Diplomado de Profundización CISCO

2019

Resumen

El certificado me permitió profundizar y aprender todo lo relacionado con la introducción a las redes, gracias a su material multimedia y actividades prácticas, logre aprender a configurar e interconectar dispositivo y que lograran comunicarse entre sí, el trabajo colaborativo me permitió aprender de mis compañeros y coordinar las actividades para obtener un buen resultado y aprender algo nuevo durante el proceso. Por otro lado, los exámenes pusieron a prueba lo investigado en los módulos del curso y encontrar las falencias que tenía en el momento para así mismo solucionarlas.

Abstrac

The certified allowed me to deepen and learn everything related to the introduction to networks, thanks to its multimedia material and practical activities, I managed to learn how to configure and interconnect device and that they managed to communicate with each other, the collaborative works allowed me to learn from my colleagues and coordinate activities to obtain a good result and learn something new during the process. On the other hand, the exams put to the test what was investigated in the modules of the course and find the flaws that it had in the moment to solve them.

Introducción

El presente trabajo pone en evidencia lo aprendido durante el desarrollo del curso de CCNA2 2018, en donde se abordaron los temas de Introducción a las redes el cual fue de mucho interés para mí y me permitió conocer los aspectos básicos de las redes. Por último, se desarrolló el curso de CCNA2 II 2018 el cual trata de Routing and Switching y se aprendió sobre configuraciones de enrutadores, los protocolos que se deben manejar y los diferentes tipos de direccionamiento, vlans y comandos para programar los Switches.

Objetivos

- Demostrar el dominio en el tema
- Evidenciar las habilidades adquiridas
- Realizar las configuraciones de equipos de manera satisfactoria

Tabla de contenido

Contenido

Evaluación – Prueba de habilidades prácticas CCNA	1
Introducción	3
Objetivos	4
Tabla de contenido	5
1.1 Escenario 1.....	7
1.1.1 Descripción de las actividades	8
Escenario 2.....	16
1. Configurar el direccionamiento IP acorde con la topología de red para cada uno de los dispositivos que forman parte del escenario.....	17
Configuración del direccionamiento ip de “Internet PC”	17
Configuración de “Web Server”.....	18
Configuración de “R1”	19
Configuración del “R2”	19
Configuración del “R3”	21
Configuración de “S1”	23
Configuración de “S3”	24
Configuración del direccionamiento ip de “PC-A”	24
Configuración del direccionamiento ip de “PC-C”	24
1. Configurar el protocolo de enrutamiento OSPFv2 bajo los siguientes criterios:	25
Configuración en R2	27
Configuración en R3	28
Verificar información de OSPF.....	29
1. Configurar VLANs, Puertos troncales, puertos de acceso, encapsulamiento, Inter-VLAN Routing y Seguridad en los Switches acorde a la topología de red establecida.....	31
Seguridad en el router R2.....	32
Configuración de seguridad en R3.....	33
Configuración de seguridad en S1	34
Seguridad en S3	34
Configuración de vlan en S1	35
Configuración vlan en S3.....	37
1. En el Switch 3 deshabilitar DNS lookup.....	38
2. Asignar direcciones IP a los Switches acorde a los lineamientos.....	39
Configuración de direcciones IP en S3	39
3. Desactivar todas las interfaces que no sean utilizadas en el esquema de red.	40
Desactivar interfaces en S3	40
4. Implement DHCP and NAT for IPv4 Configuración para R1.....	41
5. Configurar R1 como servidor DHCP para las VLANs 30 y 40.	42
6. Reservar las primeras 30 direcciones IP de las VLAN 30 y 40 para configuraciones estáticas.	43



7. Configurar NAT en R2 para permitir que los host puedan salir a internet.....	44
8. 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.	45
9. 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.....	45
10. Verificar procesos de comunicación y redireccionamiento de tráfico en los routers mediante el uso de Ping y Traceroute.	46
Conclusiones	49
Bibliografía.....	50

1.1 Escenario 1

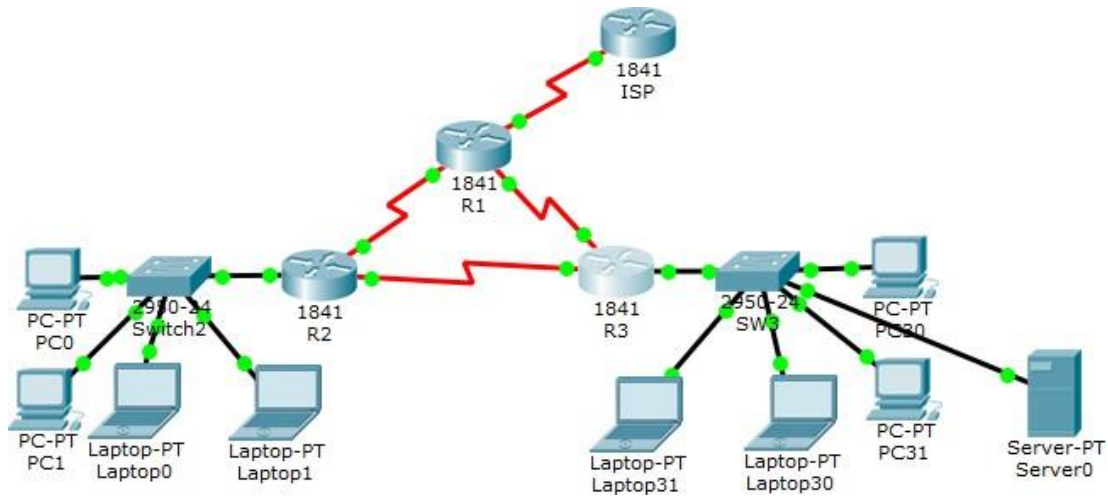


Figura 1

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
R1	Se0/0/0	200.123.211.2	255.255.255.0	N/D
	Se0/1/0	10.0.0.1	255.255.255.252	N/D
	Se0/1/1	10.0.0.5	255.255.255.252	N/D
R2	Fa0/0,100	192.168.20.1	255.255.255.0	N/D
	Fa0/0,200	192.168.21.1	255.255.255.0	N/D
	Se0/0/0	10.0.0.2	255.255.255.252	N/D
	Se0/0/1	10.0.0.9	255.255.255.252	N/D
R3	Fa0/0	192.168.30.1	255.255.255.0	N/D
		2001:db8:130::9C0:80F:301	/64	N/D
	Se0/0/0	10.0.0.6	255.255.255.252	N/D
	Se0/0/1	10.0.0.10	255.255.255.252	N/D
SW2	VLAN 100	N/D	N/D	N/D
	VLAN 200	N/D	N/D	N/D
SW3	VLAN1	N/D	N/D	N/D

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

2 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

3. 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.

1.1.1 Descripción de las actividades

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

SW2>show vlan

VLAN Name Status Ports

```
-----
1 default active Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/10, Fa0/11, Fa0/12, Fa0/13
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/22, Fa0/23, Fa0/24, Gig0/1
Gig0/2
100 VLAN0100 active Fa0/2, Fa0/3
```



```
200 VLAN0200 active Fa0/4, Fa0/5
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active
```

```
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
```

```
-----
1 enet 100001 1500 - - - - 0 0
100 enet 100100 1500 - - - - 0 0
200 enet 100200 1500 - - - - 0 0
1002 fddi 101002 1500 - - - - 0 0
```

--More--

- Los puertos de red que no se utilizan se deben deshabilitar.
- **La información** de dirección IP R1, R2 y R3 debe cumplir con la tabla 1.

Figura 2

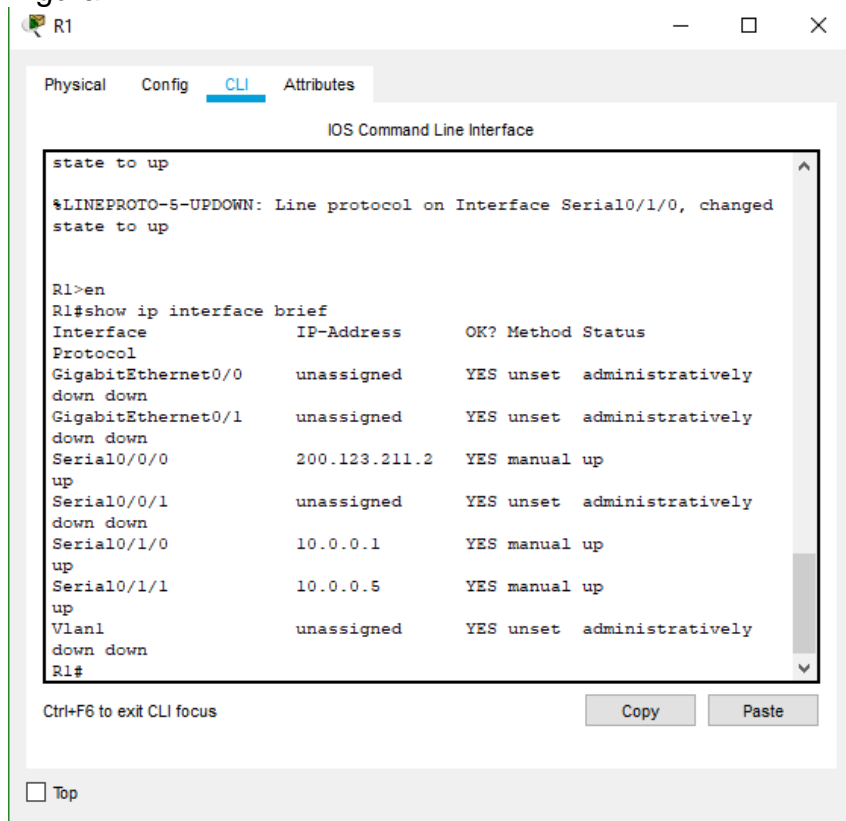


Figura 3

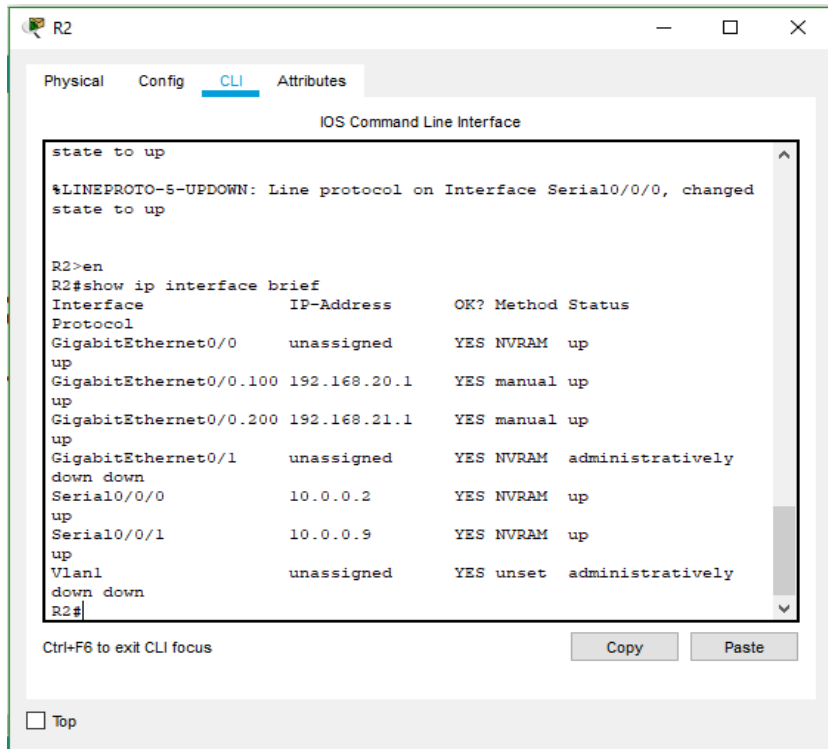
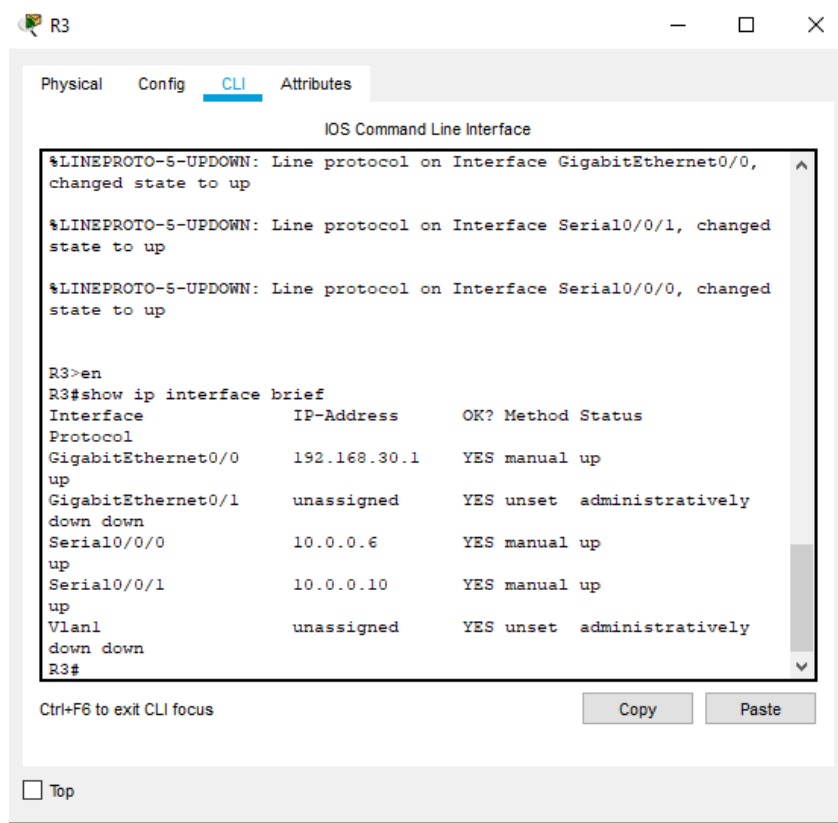


Figura 4



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

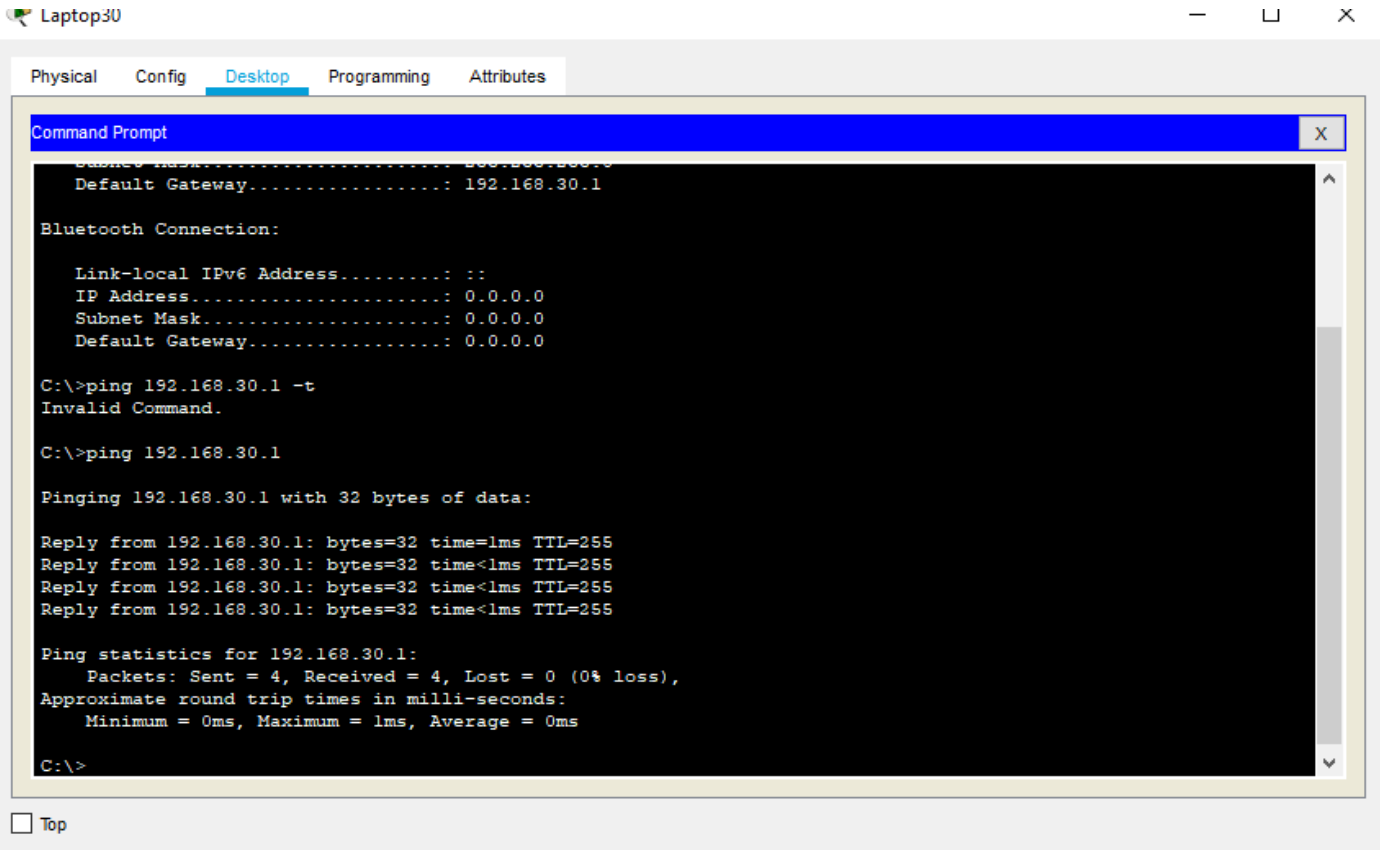


Figura 5
Figura 6

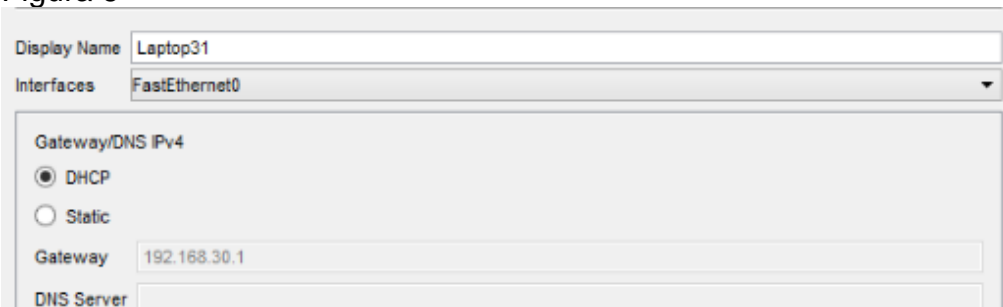


Figura 7

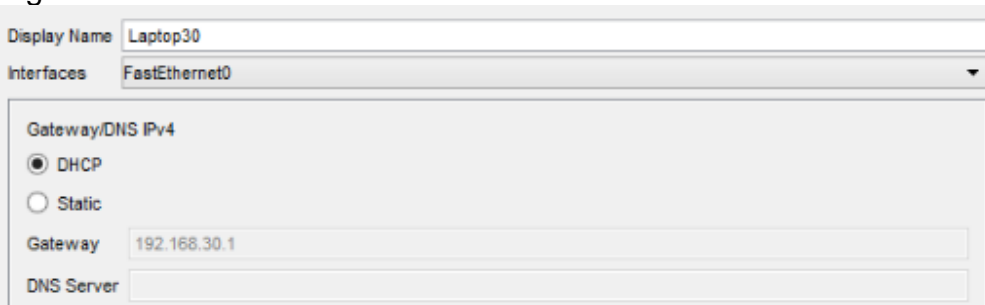


Figura 8

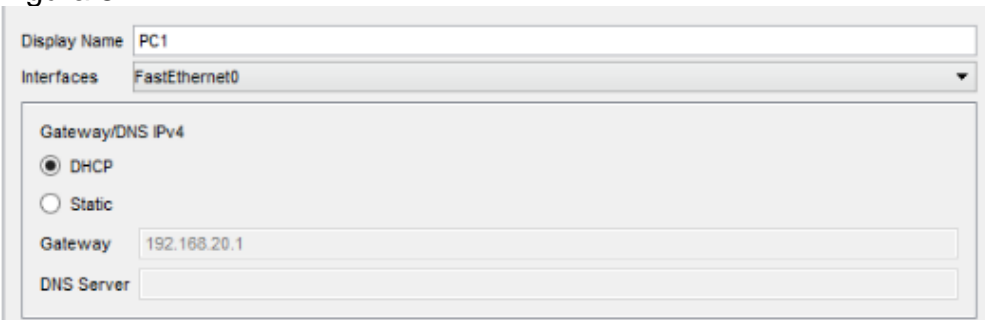
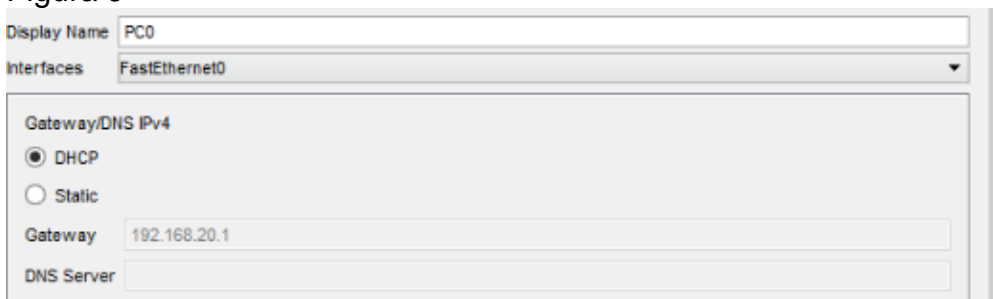


Figura 9



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

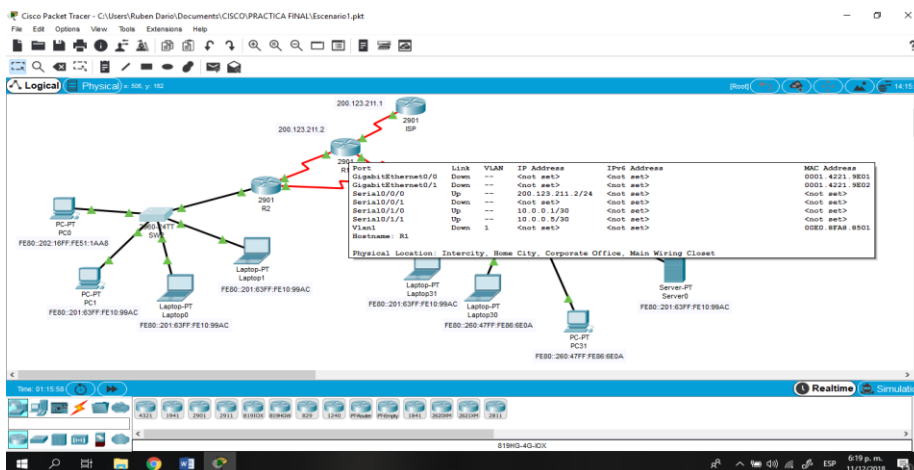


Figura 10

- e incluye esa ruta en el dominio RIPv2.
- 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.

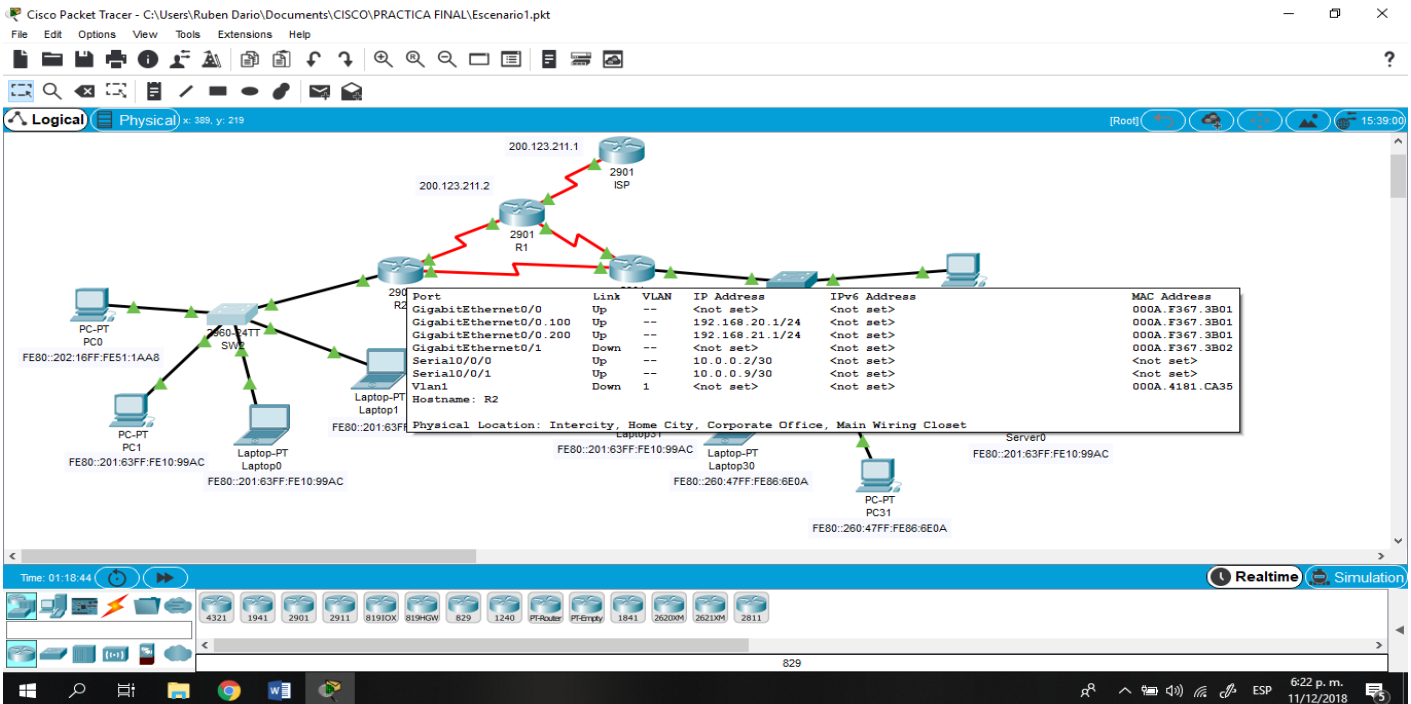


Figura 11

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

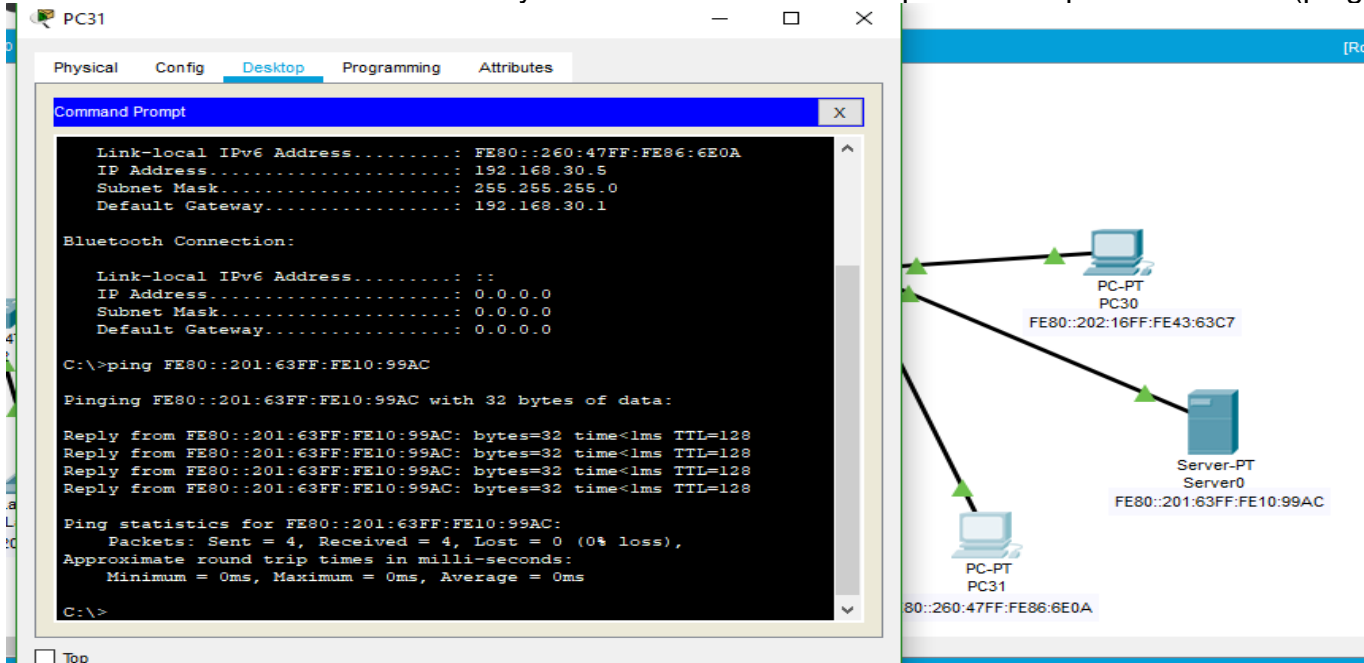


Figura 12

The screenshot displays the Cisco Packet Tracer interface. The main window shows a network topology with three routers (R1, R2, R3) and three switches (SW1, SW2, SW3). R1 is connected to an ISP. R2 and R3 are interconnected. SW1 is connected to R1 and R2, and has several PCs and laptops attached. SW2 is connected to R2 and R3, and has several laptops attached. SW3 is connected to R3 and has several PCs and laptops attached. A terminal window for Laptop30 is open, showing the following output:

```

Command Prompt

Pinging 192.168.30.1 with 32 bytes of data:

Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255
Reply from 192.168.30.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.30.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 200.123.211.1

Pinging 200.123.211.1 with 32 bytes of data:

Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253
Reply from 200.123.211.1: bytes=32 time=2ms TTL=253

Ping statistics for 200.123.211.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\>
    
```

Figura 13

- 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).
- 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.

Command Prompt (Laptop31):

```

Link-local IPv6 Address.....: FE80::201:63FF:FE10:99AC
IP Address.....: 192.168.30.3
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.30.1

Bluetooth Connection:

Link-local IPv6 Address.....: ::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

C:\>ping FE80::201:63FF:FE10:99AC

Pinging FE80::201:63FF:FE10:99AC with 32 bytes of data:

Reply from FE80::201:63FF:FE10:99AC: bytes=32 time=3ms TTL=128
Reply from FE80::201:63FF:FE10:99AC: bytes=32 time=2ms TTL=128
Reply from FE80::201:63FF:FE10:99AC: bytes=32 time=3ms TTL=128
Reply from FE80::201:63FF:FE10:99AC: bytes=32 time<1ms TTL=128

Ping statistics for FE80::201:63FF:FE10:99AC:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 3ms, Average = 2ms

C:\>
    
```

Network Diagram: Shows a central switch (SW3) connected to a router (R3) and several devices: Laptop-PT Laptop31 (FE80::201:63FF:FE10:99AC), Laptop-PT Laptop30 (FE80::260:47FF:FE86:6E0A), PC-PT PC30 (FE80::202:16FF:FE43:63C7), and Server-PT Server0 (FE80::201:63FF:FE10:99AC). A red lightning bolt icon labeled '2901 ISP' is connected to R3.

Figura 14: Se evidencia ping desde laptop 31

Command Prompt (PC30):

```

Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.30.1

Bluetooth Connection:

Link-local IPv6 Address.....: ::
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0

C:\>
C:\>ping FE80::260:47FF:FE86:6E0A

Pinging FE80::260:47FF:FE86:6E0A with 32 bytes of data:

Reply from FE80::260:47FF:FE86:6E0A: bytes=32 time=33ms TTL=128
Reply from FE80::260:47FF:FE86:6E0A: bytes=32 time<1ms TTL=128
Reply from FE80::260:47FF:FE86:6E0A: bytes=32 time<1ms TTL=128
Reply from FE80::260:47FF:FE86:6E0A: bytes=32 time<1ms TTL=128

Ping statistics for FE80::260:47FF:FE86:6E0A:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 33ms, Average = 8ms

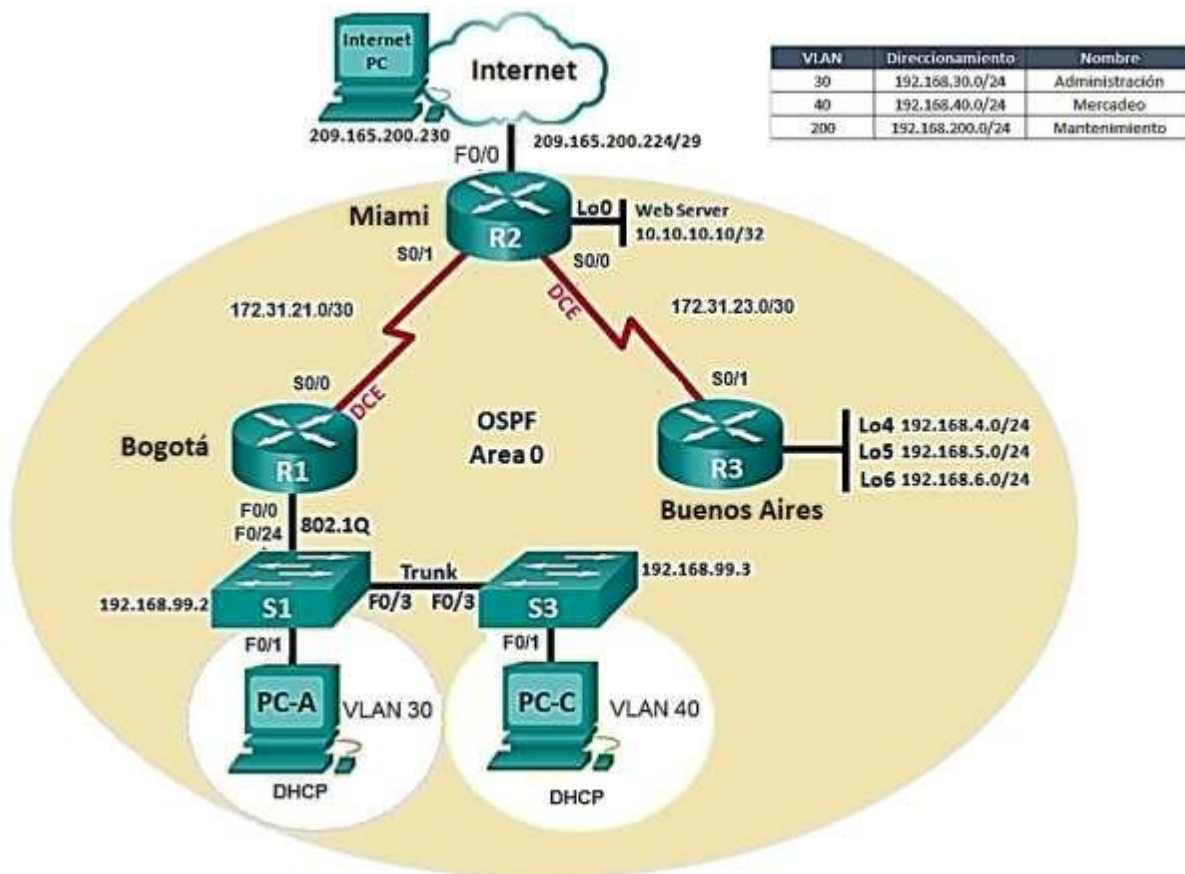
C:\>
    
```

Network Diagram: Shows a central switch (SW3) connected to several devices: PC-PT PC0 (FE80::202:16FF:FE51:1AA8), PC-PT PC1 (FE80::201:63FF:FE10:99AC), PC-PT PC30 (FE80::202:16FF:FE43:63C7), and PC-PT PC31 (FE80::260:47FF:FE86:6E0A). A red lightning bolt icon labeled '2901 ISP' is connected to SW3.

Figura 15: Conexión establecida en pc 31

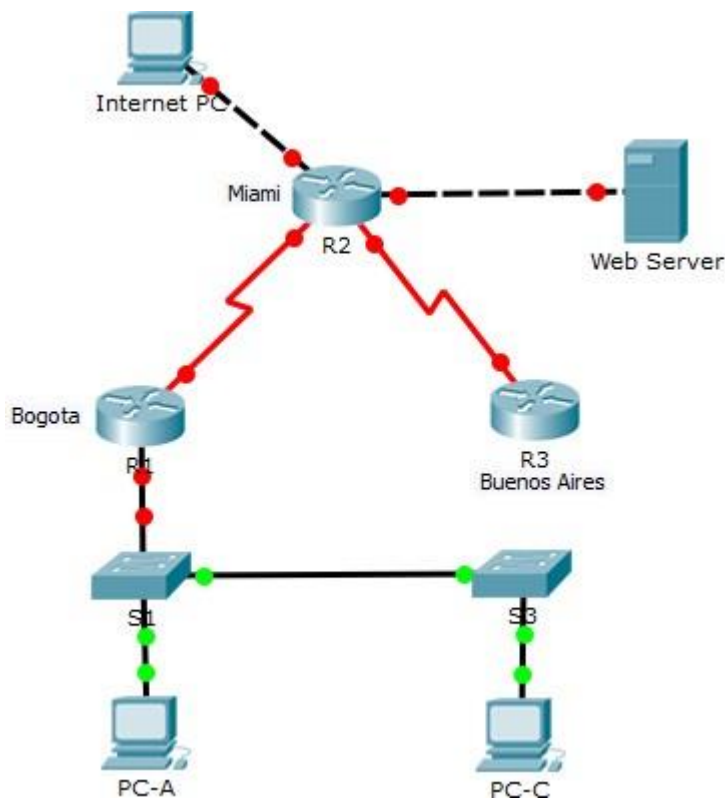
Escenario 2

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.



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

Realizamos la topología como se muestra en la figura



Configuración del direccionamiento ip de “Internet PC”

Seleccionamos la configuración IP estática y configuramos lo siguiente: IP

address: 209.165.200.230

Mascara de subred: 255.255.255.248 Gateway

predeterminado: 209.165.200.225

Configuración de “Web Server”

Seleccionamos la configuración IP estática y configuramos lo siguiente: IP

address: 10.10.10.10

Mascara de subred: 255.255.255.0 Gateway

predeterminado: 10.10.10.1

Configuración de “R1”

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int s0/0/0
R1(config-if)#description connection to R2 R1(config-
if)#ip add 172.31.21.1 255.255.255.252
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0 R1(config)#
```

Configuración del “R2”

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R2
R2(config)#int s0/0/1
R2(config-if)#descrip connection to R1
R2(config-if)#ip add 172.31.21.2 255.255.255.252
R2(config-if)#no shutdown
```

```
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 s0/0/0
```

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

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

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

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

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

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

```
R2(config-if)#descrip Internet PC
```

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

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

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

```
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
```

```
R2(config-if)#int f0/1
```

```
R2(config-if)#ip address 10.10.10.1 255.255.255.0
```

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

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

```
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up
```

```
R2(config-if)#description connection to web server
```

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

```
R2(config)#ip route 0.0.0.0 0.0.0.0 f0/0 R2(config)#
```

```
%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
```

Configuración del “R3”

```
Router>enable
```

```
Router#configure terminal
```

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

```
Router(config)#hostname R3
```

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

```
R3(config-if)#description connection to R2 R3(config-
if)#ip add 172.31.23.2 255.255.252.252
```

```
Bad mask 0xFFFFFCFC for address 172.31.23.2
```

```
R3(config-if)#ip add 172.31.23.2 255.255.255.252
```

```
R3(config-if)#no shutdown
```

```
R3(config-if)#
```

```
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up int l
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to  
up
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
R3(config-if)#int lo4
```

```
R3(config-if)#
```

```
%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)#int lo5
```

```
R3(config-if)#
```

```
%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 add 192.168.5.1 255.255.255.0
```

```
R3(config-if)#no shutdown
```

```
R3(config-if)#int lo6
```

```
R3(config-if)#
```

```
%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 add 192.168.6.1 255.255.255.0
```

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

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

Configuración de “S1”

```
Switch>enable
```

```
Switch#configure terminal
```

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

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

```
Switch(config)#hostname S1 S1(config)#exit
```

```
S1#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración de “S3”

```
Switch>enable
```

```
Switch#configure terminal
```

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

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

```
Switch(config)#hostname S3 S3(config)#exit
```

```
S3#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

Configuración del direccionamiento ip de “PC-A”

Seleccionamos la configuración IP por DHCP y nos queda de la siguiente manera: IP

```
address: 169.254.139.60
```

```
Mascara de subred: 255.255.0.0 Gateway
```

```
predeterminado: 0.0.0.0
```

Configuración del direccionamiento ip de “PC-C”

Seleccionamos la configuración IP por DHCP y nos queda de la siguiente manera: IP

```
address: 169.254.236.160
```

```
Mascara de subred: 255.255.0.0 Gateway
```

```
predeterminado: 0.0.0.0
```


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

OSPFv2 area 0

Configuration Item or Task	Specification
Router ID R1	1.1.1.1
Router ID R2	5.5.5.5
Router ID R3	8.8.8.8
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en	256 Kb/s
Ajustar el costo en la métrica de S0/0 a	9500

Configuración en R1

```
R1>enable R1#configure
```

```
terminal
```

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

```
R1(config)#router ospf 1
```

```
R1(config-router)#router-id 1.1.1.1
```

R1(config-router)#Reload or use "clear ip ospf process" command, for this to take effect

```
R1(config-router)#no router-id 1.1.1.1
```

```
R1(config-router)#router-id 1.1.1.1
```

R1(config-router)#Reload or use "clear ip ospf process" command, for this to take



effect

```
R1(config-router)#network 172.31.21.0 0.0.0.3 area 0
```

```
R1(config-router)#network 192.168.30.0 0.0.0.255 area 0
```

```
R1(config-router)#network 192.168.40.0 0.0.0.255 area 0
R1(config-router)#network 192.168.200.0 0.0.0.255 area 0
R1(config-router)#passive-interface f0/0
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)#
```

Configuración en R2

```
R2>enable R2#configure
terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
R2(config-router)#router-id 5.5.5.5
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#
02:12:01: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Serial0/0/1 from
LOADING to FULL, Loading Done

R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 172.31.23.0 0.0.0.3 area 0
R2(config-router)#network 172.31.21.0 0.0.0.3 area 0
R2(config-router)#network 10.10.10.0 0.0.0.255 area 0
R2(config-router)#passive-interface f0/0
R2(config-router)#interface s0/0/0
R2(config-if)#bandwidth 256
R2(config-if)#interface s0/0/1
R2(config-if)#bandwidth 256
R2(config-if)#interface s0/0/0
```

```
R2(config-if)#ip ospf cost 7500
```

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

Configuración en R3

```
R3>enable R3#configure
```

```
terminal
```

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)#
```

```
02:25:30: %OSPF-5-ADJCHG: Process 1, Nbr 5.5.5.5 on Serial0/0/1 from  
LOADING to FULL, Loading Done
```

```
R3(config-router)#network 192.168.4.0 0.0.0.255 area 0
```

```
R3(config-router)#passive-interface lo4
```

```
R3(config-router)#passive-interface lo5
```

```
R3(config-router)#passive-interface lo6
```

```
R3(config-router)#exit
```

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

```
if)#bandwidth 256 R3(config-if)#ip
```

```
ospf cost 9500
```

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

Verificar información de OSPF

- Visualizar tablas de enrutamiento y routers conectados por OSPFv2

```
R2>enable
```

```
R2#show ip ospf neighbor
```

```
Neighbor ID Pri State Dead Time Address Interface 1.1.1.1
```

```
0 FULL/ - 00:00:30 172.31.21.1 Serial0/0/1
```

```
8.8.8.8 0 FULL/ - 00:00:39 172.31.23.2 Serial0/0/0
```

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

Para este paso se utiliza el comando **show ip ospf interface brief** pero este comando no es soportado por Packet tracer

```
R2#show ip ospf interface brief
```

```
^
```

```
% Invalid input detected at '^' marker.
```

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

```
R2#show ip protocols
```

```
Routing Protocol is "ospf 1"
```

```
Outgoing update filter list for all interfaces is not set
```

```
Incoming update filter list for all interfaces is not set
```

```
Router ID 5.5.5.5
```

```
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
```

```
Maximum path: 4
```

```
Routing for Networks:
```

```
172.31.21.0 0.0.0.3 area 0
```

```
172.31.23.0 0.0.0.3 area 0
```

```
10.10.10.0 0.0.0.255 area 0 Passive
```

```
Interface(s): FastEthernet0/0
```

```
Routing Information Sources:
```

```
Gateway Distance Last Update
```

```
1.1.1.1 110 00:28:05
```

```
5.5.5.5 110 00:17:56
```

```
8.8.8.8 110 00:13:05
```

```
Distance: (default is 110)
```

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

Primero configuramos la seguridad en R1

```
R1>enable R1#configure
terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#enable secret class
R1(config)#line con 0
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#line vty 0 4
R1(config-line)#pass cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#service pass
R1(config)#service password-encryption
R1(config)#banner motd #Prohibido El Acceso No Autorizado#
R1(config)# exit
R1#copy running-config startup-config
Destination filename [startup-config]?
```

Building configuration...

[OK]

Seguridad en el router R2

```
R2>enable R2#configure
```

```
terminal
```

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

```
R2(config)#enable secret class
```

```
R2(config)#line con 0
```

```
R2(config-line)#pass cisco
```

```
R2(config-line)#login
```

```
R2(config-line)#line vty 0 4
```

```
R2(config-line)#pass cisco
```

```
R2(config-line)#login
```

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

```
R2(config)#service password-encryption
```

```
R2(config)#banner motd #Prohibido El Acceso No Autorizado#
```

```
R2(config)#exit
```

```
R2#
```

```
%SYS-5-CONFIG_I: Configured from console by console
```

```
R2#copy running-config startup-config
```

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```


Configuración de seguridad en R3

```
R3>enable R3#configure
terminal
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#enable secret class
R3(config)#line con 0
R3(config-line)#pass cisco
R3(config-line)#login
R3(config-line)#exit
R3(config)#service password-encryption
R3(config)#banner motd #Prohibido El Acceso No Autorizado#
R3(config)#exit
R3#
%SYS-5-CONFIG_I: Configured from console by console

R3#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Configuración de seguridad en S1

```
S1>enable Password:
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#enable secret class
S1(config)#line con 0
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#line vty 0 4
S1(config-line)#pass cisco
S1(config-line)#login
S1(config-line)#service password-encryption S1(config)#banner
motd #Prohibido El Acceso No Autorizado# S1(config)#exit
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Seguridad en S3

```
S3>enable S3#configure
terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#hostname S3
S3(config)#no ip domain-lookup
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#
%SYS-5-CONFIG_I: Configured from console by console
```

Configuracion de vlan en S1

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#no ip domain-lookup
S1(config)#vlan 30
S1(config-vlan)#name Administracion
S1(config-vlan)#vlan 40
S1(config-vlan)#name Mercadeo
S1(config-vlan)#vlan 200
S1(config-vlan)#name Mantenimiento
S1(config-vlan)#exit
S1(config)#int vlan 200
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan200, changed state to up
S1(config-if)#ip address 192.168.200.2 255.255.255.0
S1(config-if)#no shut
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.200.1
```

```
S1(config)#interface f0/3
```

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

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

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed  
state to down
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed  
state to up
```

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up
```

```
S1(config-if)#switchport trunk native vlan 1
```

```
S1(config-if)#interface f0/24
```

```
S1(config-if)#switchport mode trunk S1(config-  
if)#switchport trunk native vlan 1
```

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

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

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

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

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

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

```
S1(config-if-range)#no shutdown
```

Configuración vlan en S3

Prohibido El Acceso No Autorizado

User Access Verification Password:

S3>enable Password:

S3#configure terminal

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

S3(config)#hostname S3

S3(config)#no ip domain-lookup

S3(config)#vlan 30

S3(config-vlan)#name Administracion

S3(config-vlan)#vlan 40

S3(config-vlan)#name Mercadeo

S3(config-vlan)#vlan 200

S3(config-vlan)#name Mantenimiento

S3(config-vlan)#exit

S3(config)#int vlan 200

S3(config-if)#

%LINK-5-CHANGED: Interface Vlan200, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan200, changed state to up

S3(config-if)#ip address 192.168.200.3 255.255.255.0

S3(config-if)#no shutdown

S3(config-if)#exit

S3(config)#ip default-gateway 192.168.200.1

```
S3(config)#interface f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#interface range fa0/1-2, fa0/4-24, GigabitEthernet0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#interface fa0/1
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 40
S3(config-if)#
S3(config-if)#interface range fa0/2, fa0/4-24, GigabitEthernet0/1-2
S3(config-if-range)#shutdown
```

1. En el Switch 3 deshabilitar DNS lookup

```
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#no ip domain-lookup
S3(config)#exit
S3#
%SYS-5-CONFIG_I: Configured from console by console
```

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

Configuración de direcciones IP en S1

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

Configuración de direcciones IP en S3

```
Prohibido El Acceso No Autorizado

User Access Verification Password:

S3>enable Password:

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

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

Desactivar interfaces en S1

```
S1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#
S1(config)#interface range fa0/1-2, fa0/4-23, GigabitEthernet0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#interface fa0/1
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
S1(config-if)#interface range fa0/2, fa0/4-23, GigabitEthernet0/1-2
S1(config-if-range)#shutdown
S1(config-if-range)#
```

Desactivar interfaces en S3

```
S3>enable Password:
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#int vlan 200
S3(config-if)#ip address 192.168.200.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#exit
S3(config)#ip default-gateway 192.168.200.1
S3(config)#
S3(config)#interface range fa0/1-2, fa0/4-24, GigabitEthernet0/1-2
S3(config-if-range)#switchport mode access
```



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

4. Implement DHCP and NAT for

IPv4 Configuración para R1

```
R1#configure terminal
```

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#configure
```

```
terminal
```

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
```

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

```
R1#configure terminal
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 excluded-address 192.168.40.1 192.168.40.30
^
% Invalid input detected at '^' marker.
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp pool Administracion
^
% Invalid input detected at '^' marker. R1(config)#ip
dhcp pool ADMINISTRACION R1(dhcp-
config)#dns-server 10.10.10.11 R1(dhcp-
config)#domain-name ccna-unad.com
```

```
% Invalid input detected at '^' marker. R1(dhcp-
config)#default-router 192.168.30.1

R1(dhcp-config)#network 192.168.30.0 255.255.255.0

R1(dhcp-config)#exit

R1(config)#exit
```

6. 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#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.31.1 192.168.31.30
R1(config)#ip dhcp excluded-address 192.168.31.1 192.168.31.30
R1(config)#no ip dhcp excluded-address 192.168.31.1 192.168.31.30
R1(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.30
R1(config)#ip dhcp excluded-address 192.168.40.1 192.168.40.30
R1(config)#ip dhcp pool Administracion
R1(dhcp-config)#dns-server 10.10.10.11 R1(dhcp-
config)#domain-name ccna-unad.com
```

```
% Invalid input detected at '^' marker. R1(dhcp-
config)#default-router 192.168.30.1
R1(dhcp-config)#network 192.168.30.0 255.255.255.0
R1(dhcp-config)#ip dhcp pool Mercadeo
R1(dhcp-config)#dns-server 10.10.10.11 R1(dhcp-
config)#domain-name ccna-unad.com
^
% Invalid input detected at '^' marker. R1(dhcp-
config)#default-router 192.168.40.1
    R1(dhcp-config)#network 192.168.40.0 255.255.255.0
        R1(dhcp-config)#
```

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

```
R2#configure terminal

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

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

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

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

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

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

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

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

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

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

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

```
R2(config)#
```

8. 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#configure terminal
```

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

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

```
R2(config)#access-list 101 permit icmp any any echo-reply R2(config)#int  
f0/0
```

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

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

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

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

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

```
R2(config-if)#int f0/1
```

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

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

9. 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#configure terminal
```

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

```
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)#
```

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

Verificación con el comando ping

Ping de R1 a R2

```
R1#ping 172.31.21.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.31.21.2, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/22 ms
```

Ping de R2 A R3

```
R2#ping 172.31.23.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.23.2, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/11 ms
```

Web Server

```
SERVER>ping 209.165.200.225

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=1ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255
Reply from 209.165.200.225: bytes=32 time=0ms TTL=255

Ping statistics for 209.165.200.225:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

SERVER>
```


Conclusiones

- Con la utilización del ping para el rastreo y así probar las rutas que se le asignan a las topologías
- Se configura y verifica el direccionamiento IPv4 e IPv6
- Con el desarrollo del presente trabajo fue posible demostrar destrezas en cuanto a la configuración de equipos de red Cisco, como Routers y Switches.
- Se logró llevar a cabo de manera exitosa protocolos de enrutamiento dinámico como OSPF y otros servicios como DHCP, listas de acceso, Nat y aseguramiento de dispositivos Cisco

Bibliografía

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

UNAD (2014). PING y TRACER como estrategia en procesos de Networking [OVA]. Recuperado de: <https://1drv.ms/u/s!AmlJYei-NT1lhgTCtKY-7F5KIRC3>

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>

Lucas, M. (2009). Cisco Routers for the Desperate : Router and Switch Management, the Easy Way. San Francisco: No Starch Press. Recuperado de: <http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=440032&lang=es&site=ehost-live>

Odom, W. (2013). CISCO Press (Ed). CCNA ICND2 Official Exam Certification Guide. Recuperado de: <http://een.iust.ac.ir/profs/Beheshti/Computer%20networking/Auxiliary%20materials/Cisco-ICND2.pdf>

Lammle, T. (2010). CISCO Press (Ed). Cisco Certified Network Associate Study Guide. Recuperado de: <http://gonda.nic.in/swangonda/pdf/ccna1.pdf>

CISCO. (2014). Introducción a redes conmutadas. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module1/index.html#1.0.1.1>

CISCO. (2014). Configuración y conceptos básicos de Switching. Principios de Enrutamiento y Conmutación. Recuperado de: <https://static-course-assets.s3.amazonaws.com/RSE50ES/module2/index.html#2.0.1.1>

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>

UNAD (2014). Configuración de Switches y Routers [OVA]. Recuperado de: <https://1drv.ms/u/s!AmlJYei-NT1lhgL9QChD1m9EuGqC>