

### Laboratorio 4 – Capa de transporte

#### Integrantes (Grupo 3 – Sección 1):

David Cuevas Alba – 202122284

Lina Gómez – 201923531

Eduardo Herrera – 201912865

Nicolás Pérez – 202116903

Gastón Alessandro Metzger – 201921517

1 Objetivos .....	1
2. Configuración protocolo enrutamiento RIPv1 .....	2
2.1. Configuración básica de enrutadores .....	2
2.2. Configuración del protocolo de enrutamiento .....	2
2.3. Análisis de la topología RIPv1 .....	3

## 1 Objetivos

Este laboratorio pretende comprender el rol de los protocolos de enrutamiento dinámico RIP y OSPF en redes IP usando la versión 4, y la versión 6.

Los principales objetivos son:

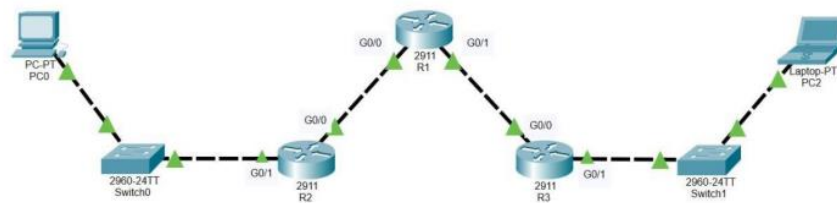
- Comprender las principales características y diferencias de los protocolos de enrutamiento de vector distancia y los protocolos de enrutamiento de estado de enlace.
- Configurar el protocolo de enrutamiento dinámico RIP en routers en una topología de red con múltiples enrutadores.
- Explorar y comprender las diferencias entre las versiones del protocolo RIP. • Configurar el protocolo de enrutamiento dinámico OSPF en routers en una topología de red con múltiples enrutadores.
- Configurar las distintas formas de enrutamiento en redes IPv6.

## 2. Configuración protocolo enrutamiento RIPv1

### 2.1. Configuración básica de enrutadores

Primero se replicó la topología propuesta en el laboratorio en Cisco Packet Tracer en la vida real.

*Figura 1. Topología de red para actividad 4.1.*



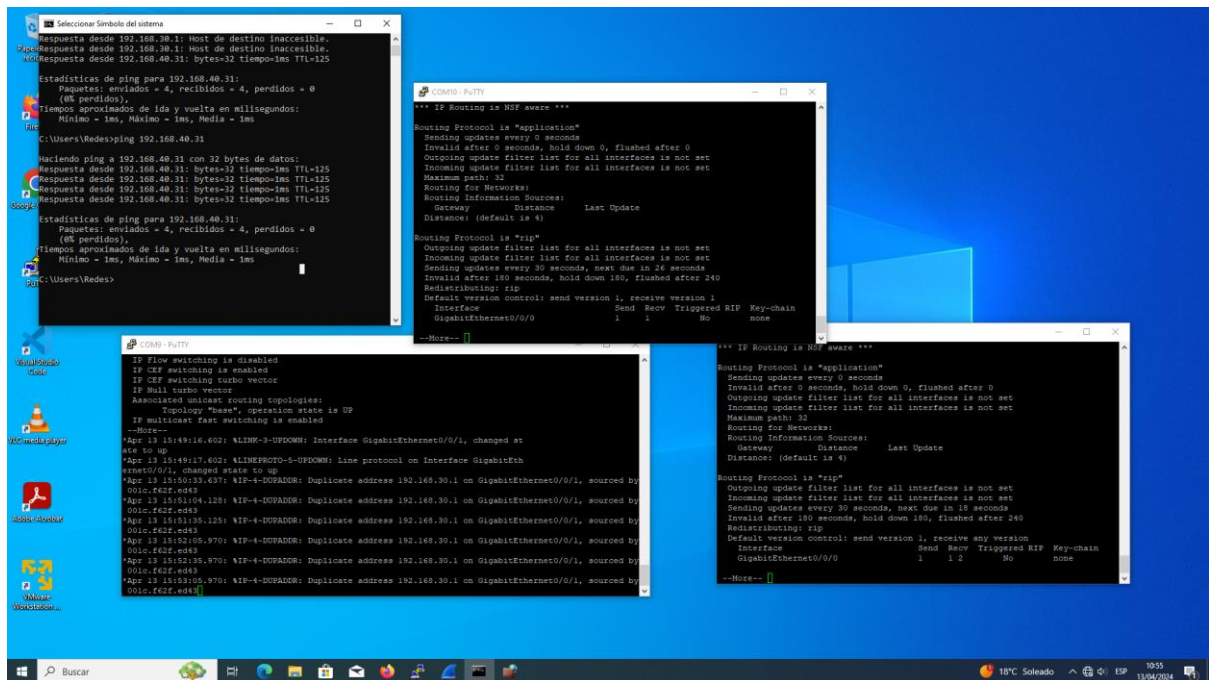
Luego se habilitaron las interfaces de red en los routers por medio de la consola utilizando los siguientes comandos:

```
LABORATORIO> enable  
LABORATORIO# configure  
terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
LABORATORIO(config)# interface Ethernet0/0  
LABORATORIO(config-if)# ip address 192.168.10.5 255.255.255.0  
LABORATORIO(config-if)# no shutdown
```

### 2.2. Configuración del protocolo de enrutamiento

Se configuro el protocolo de enrutamiento RIPv1 en los routers utilizando los siguientes comandos en la consola:

```
Router(config)# router rip Router(config-router)# network  
<dirección_de_red_a_publicar_1> Router(config-router)# network  
<dirección_de_red_a_publicar_2> Router(config-router)# network  
<dirección_de_red_a_publicar_n> Router(config-router)# version <1 | 2>
```



## 2.3. Análisis de la topología RIPv1

No.	Time	Source	Destination	Protocol	Length	Info
29	7.900787	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
30	8.000193	Cisco_2F:ed:43	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
31	8.111719	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
32	9.000644	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
33	9.150563	Cisco_2F:ed:43	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
34	9.150567	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
35	9.248860	192.168.40.1	255.255.255.255	RIPv1	100	Response
36	9.294227	192.168.40.1	192.168.40.31	ICMP	74	Echo (ping) request 14-000001, seq=85/22768, ttl=128 (reply in 37)
37	9.352138	192.168.40.31	192.168.40.31	ICMP	74	Echo (ping) reply 14-000001, seq=85/22768, ttl=128 (request in 36)
38	10.111561	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
39	10.150564	Cisco_2F:ed:43	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
40	10.150567	192.168.40.1	192.168.40.31	ICMP	74	Echo (ping) request 14-000001, seq=86/22816, ttl=128 (no response found)
41	10.300193	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
42	11.000786	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
43	11.000786	Cisco_2F:ed:43	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
44	11.100787	192.168.30.31	192.168.40.31	ICMP	74	Echo (ping) request 14-000001, seq=87/22770, ttl=128 (no response found)
45	11.300786	192.168.40.1	255.255.255.255	RIPv1	100	Response
46	12.000786	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
47	12.000786	Cisco_2F:ed:43	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
48	12.000786	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
49	12.100786	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
50	12.100786	Cisco_2F:ed:43	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
51	12.100786	04:00:00:00:00:00	Broadcast	ARP	60	Gratuitous ARP for 192.168.30.1 (Reply) (duplicate use of 192.168.30.1 detected)
52	12.300899	192.168.30.31	192.168.40.31	ICMP	74	Echo (ping) request 14-000001, seq=88/22818, ttl=128 (reply in 53)
53	12.300899	192.168.40.31	192.168.30.31	ICMP	74	Echo (ping) reply 14-000001, seq=88/22818, ttl=128 (request in 52)
54	13.100786	192.168.40.1	255.255.255.255	RIPv1	100	Response

En esta parte, podemos observar dos tráficos que corresponden al protocolo RIPv1. Estos tráficos se manifiestan en mensajes con dirección de destino Broadcast, enviados por los routers con el propósito de intercambiar información de enrutamiento. Específicamente, estos mensajes contienen datos sobre las redes alcanzables y las métricas asociadas a esas redes (Siendo estas métricas el número de saltos que tienen que hacer para llegar al destino). El objetivo principal de este intercambio es mantener una tabla de enrutamiento actualizada en cada router, lo que permite a los dispositivos calcular las rutas más eficientes para alcanzar destinos específicos en la red. Este proceso dinámico de actualización de enrutamiento es esencial para garantizar la conectividad y la eficiencia en la red, ya que permite a los routers adaptarse continuamente a cambios en la topología de la red y a condiciones de enrutamiento variables.