

**UNIVERSIDAD DE LOS ANDES  
DEPARTAMENTO DE INGENIERÍA  
DE SISTEMAS Y COMPUTACIÓN**



**LABORATORIO 4: PROTOCOLOS DE  
ENRUTAMIENTO DINÁMICOS CON REDES IPv4 e  
IPv6**

**ISIS 3204 – INFRAESTRUCTURA DE  
COMUNICACIONES**

**Carlos Lozano  
Nathalia Quiroga**

**Grupo 6  
Alejandra Fruto Osorio 202311287  
Daniel Stiven Roa Uribe 202215803  
Lex Betancourt 202110854**

**2025-20**

## **Contenido**

1. Topología 1	3
2. Topología 2	6
3. Topología 3	8
4. Evidencias de trabajo	12

## 1. Topología 1

### 1.1 Mapa de la topología 1

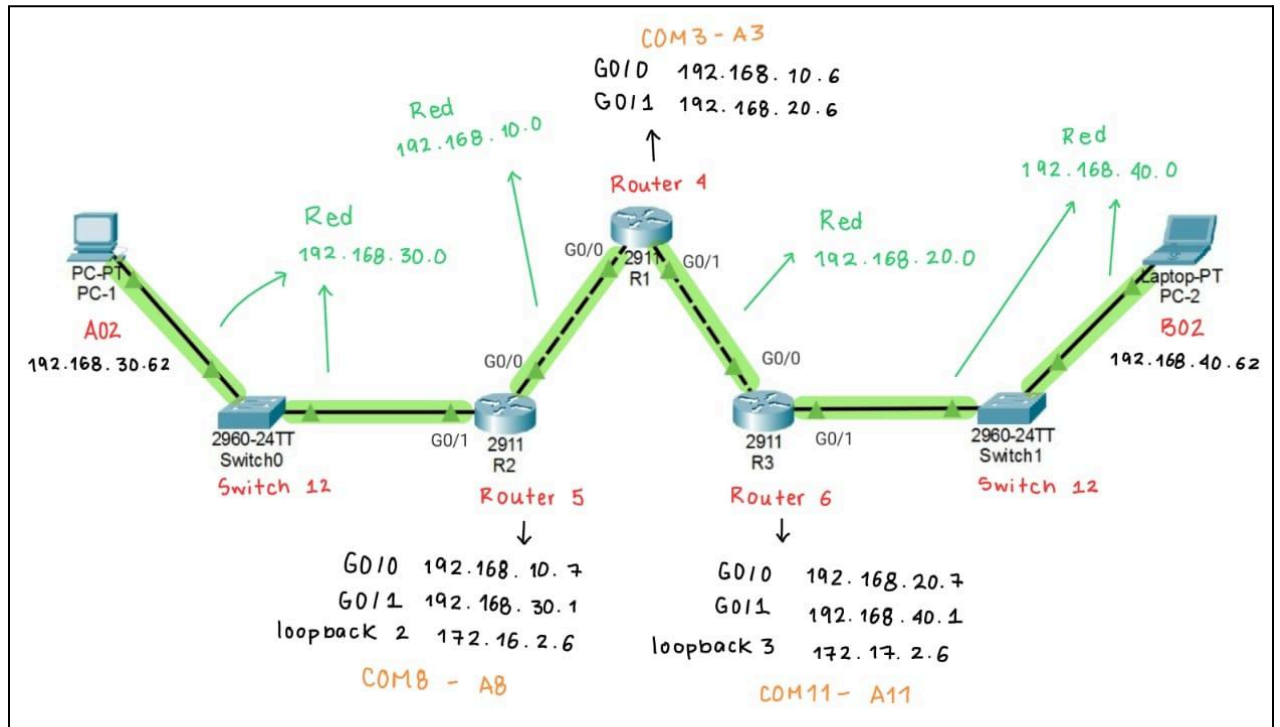


Imagen 1. Mapa de la topología 1

### 1.2 Análisis de capturas con protocolo RIPv1

#### Paquetes ICMP

No.	Time	Source	Destination	Protoc	Leng	Info
66	25.361251	192.168.30.62	192.168.40.62	ICMP	74	Echo (ping) request id=0x0001, seq=711/50946, ttl=128 (reply in 67)
67	25.362682	192.168.40.62	192.168.30.62	ICMP	74	Echo (ping) reply id=0x0001, seq=711/50946, ttl=125 (request in 66)

Imagen 2. Ping del PC1 al PC2 con RIPv1

No.	Time	Source	Destination	Protoc	Leng	Info
18	8.996916	192.168.40.62	192.168.30.62	ICMP	74	Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (reply in 19)
19	8.998599	192.168.30.62	192.168.40.62	ICMP	74	Echo (ping) reply id=0x0001, seq=47/12032, ttl=125 (request in 18)

Imagen 3. Ping del PC2 al PC1 con RIPv1

La captura de paquetes ICMP (pings) se llevó a cabo entre las estaciones finales PC-1 y PC-2 después de que RIPv1 se hubiera configurado correctamente.

En las anteriores imágenes, se puede observar una serie exitosa de mensajes ICMP Echo Request (solicitud de ping, Tipo 8, Código 0) y ICMP Echo Reply (respuesta de ping, Tipo 0, Código 0). Esto

confirma que hay conectividad de extremo a extremo entre las dos LAN de la Topología 1.

Al recibir ambos equipos los paquetes, se confirma que los paquetes han pasado por los routers R2, R1 y R3 y que la ruta está funcionando.

### Paquetes de enrutamiento

No.	Time	Source	Destination	Protocol	Length	Info
57	19.705797	192.168.40.1	255.255.255.255	RIPv1	146	Response
59	21.446683	192.168.30.1	255.255.255.255	RIPv1	146	Response
133	48.414672	192.168.30.1	255.255.255.255	RIPv1	146	Response
134	48.525505	192.168.40.1	255.255.255.255	RIPv1	146	Response

*Imagen 4. Paquetes RIPv1 (protocolo RIPv1)*

En esta captura podemos ver los paquetes RIPv1, los cuales son Responses (Tipo 2) que incluyen entradas de ruta (RTE) con la dirección de red y la métrica (conteo de saltos). El protocolo RIPv1 es un protocolo de vector de distancia que utiliza UDP en el puerto 520. Su análisis confirma que los routers han intercambiado información de ruta, lo que ha permitido el ping exitoso.

> Frame 134: Packet, 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface \Device\NPF_{B4D471F2-32CE-4F46-B20B-8A}
> Ethernet II, Src: Cisco_2b:91:11 (70:7d:b9:2b:91:11), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.40.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 520, Dst Port: 520
▼ Routing Information Protocol
Command: Response (2)
Version: RIPv1 (1)
> IP Address: 172.16.0.0, Metric: 3
> IP Address: 172.17.0.0, Metric: 1
> IP Address: 192.168.10.0, Metric: 2
> IP Address: 192.168.20.0, Metric: 1
> IP Address: 192.168.30.0, Metric: 3

*Imagen 5. Información de enrutamiento (protocolo RIPv1)*

Esta captura muestra un paquete de actualización RIPv1 Response que el Router R3 (192.168.40.1) envió a través de broadcast. Esto indica que R3 está comunicando a sus vecinos, especialmente a R1, las rutas que tiene registradas, incluyendo las redes LAN (192.168.30.0/24) y las interfaces Loopback (172.16.0.0/16) de otros routers, junto con sus métricas correspondientes (el conteo de saltos).

La aparición de estos mensajes confirma que la infraestructura básica está funcionando correctamente y que los routers han intercambiado dinámicamente sus tablas de enrutamiento, lo que ha permitido el reenvío de los paquetes ICMP a través de toda la red.

### 1.3 Análisis de capturas con protocolo OSPF

#### Paquetes ICMP

No.	Time	Source	Destination	Protoc	Leng	Info
13	4.271709	192.168.30.62	192.168.40.62	ICMP	74	Echo (ping) request id=0x0001, seq=724/54274, ttl=128 (reply in 14)
14	4.273002	192.168.40.62	192.168.30.62	ICMP	74	Echo (ping) reply id=0x0001, seq=724/54274, ttl=125 (request in 13)

*Imagen 6. Ping del PC1 al PC2 con OSPF*

No.	Time	Source	Destination	Protoc	Leng	Info
27	8.169028	192.168.40.62	192.168.30.62	ICMP	74	Echo (ping) request id=0x0001, seq=58/14848, ttl=125 (reply in 28)
28	8.169213	192.168.30.62	192.168.40.62	ICMP	74	Echo (ping) reply id=0x0001, seq=58/14848, ttl=128 (request in 27)

*Imagen 7. Ping del PC2 al PC1 con OSPF*

Al igual que con RIPv1, la captura ICMP valida la conectividad extremo a extremo. En estas imágenes también se observa la misma secuencia exitosa de ICMP Echo Request y ICMP Echo Reply entre PC-1 y PC-2.

#### Paquetes de enrutamiento

No.	Time	Source	Destination	Protocol	Lengtl	Info
4	0.667976	192.168.40.1	224.0.0.5	OSPF	90	Hello Packet
12	4.092253	192.168.30.1	224.0.0.5	OSPF	90	Hello Packet
34	9.699873	192.168.40.1	224.0.0.5	OSPF	90	Hello Packet
48	13.640224	192.168.30.1	224.0.0.5	OSPF	90	Hello Packet
77	19.499795	192.168.40.1	224.0.0.5	OSPF	90	Hello Packet
86	23.148241	192.168.30.1	224.0.0.5	OSPF	90	Hello Packet

*Imagen 8. Paquetes OSPF (protocolo OSPF)*

Para este caso la captura muestra los mensajes OSPF Hello, lo que confirma que estamos en la fase inicial del protocolo OSPFv2 en la Topología 1. Estos mensajes se envían desde las direcciones de gateway de las LAN: 192.168.40.1 (R3) y 192.168.30.1 (R2). El destino es la dirección multicast 224.0.0.5 (Todos los routers OSPF), lo que indica que se están anunciando a todos los routers OSPF en el segmento de red.

Por otro lado, se puede observar que los mensajes se envían de manera periódica, aproximadamente cada 10 segundos. La presencia y el intercambio constante de estos paquetes Hello demuestran que los routers R2 y R3 están activos y operativos, y están trabajando para mantener su adyacencia OSPF con el router central (R1).

## 2. Topología 2

### 2.1 Mapa de la topología 2

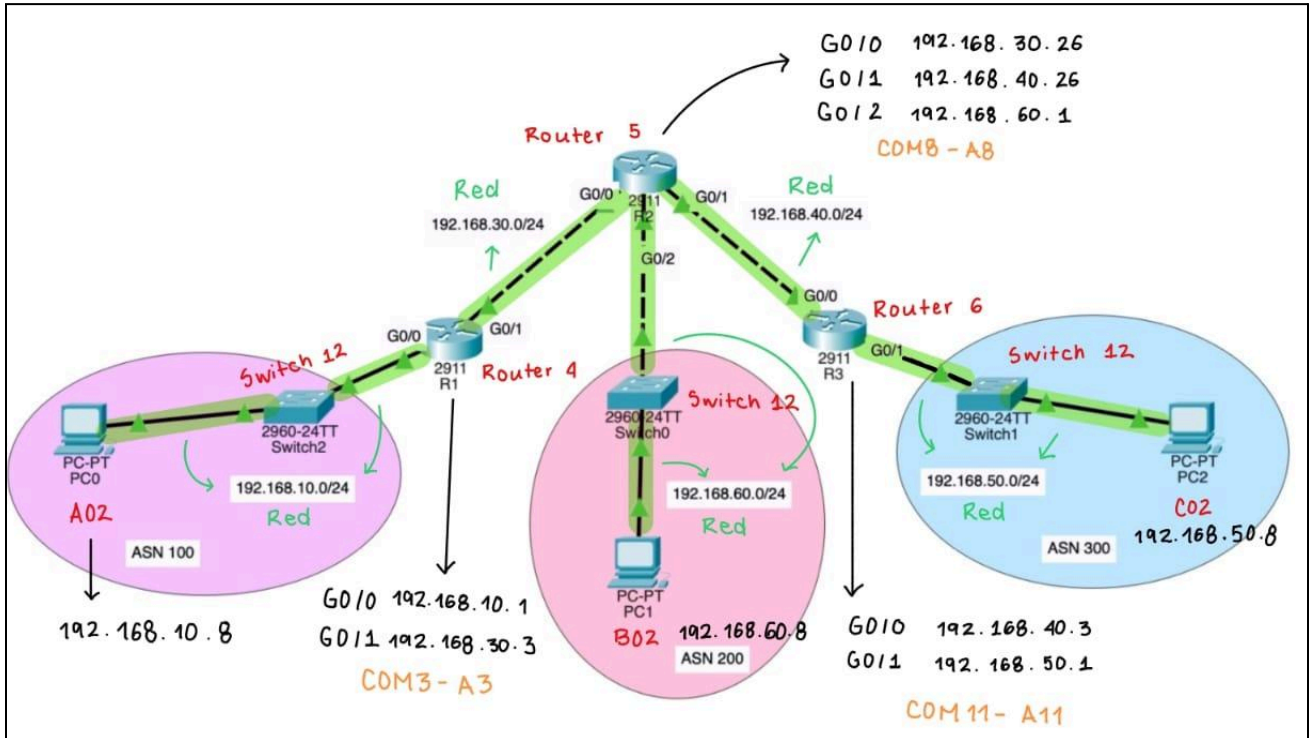


Imagen 9. Mapa de la topología 2

### 2.2 Análisis de capturas con protocolo BGP

#### Paquetes ICMP

No.	Time	Source	Destination	Protoc	Leng	Info
245	128.578136	192.168.10.8	192.168.50.8	ICMP	74	Echo (ping) request id=0x0001, seq=693/46338, ttl=128 (reply in 246)
246	128.579448	192.168.50.8	192.168.10.8	ICMP	74	Echo (ping) reply id=0x0001, seq=693/46338, ttl=125 (request in 245)

Imagen 10. Ping del PC0 al PC2 con BGP

No.	Time	Source	Destination	Protoc	Leng	Info
29	13.157798	192.168.10.8	192.168.60.8	ICMP	74	Echo (ping) request id=0x0001, seq=698/47618, ttl=126 (reply in 30)
30	13.157921	192.168.60.8	192.168.10.8	ICMP	74	Echo (ping) reply id=0x0001, seq=698/47618, ttl=128 (request in 29)

Imagen 11. Ping del PC0 al PC1 con BGP

No.	Time	Source	Destination	Protoc	Leng	Info
119	67.735816	192.168.60.8	192.168.10.8	ICMP	74	Echo (ping) request id=0x0001, seq=34/8704, ttl=126 (reply in 120)
120	67.736001	192.168.10.8	192.168.60.8	ICMP	74	Echo (ping) reply id=0x0001, seq=34/8704, ttl=128 (request in 119)

Imagen 12. Ping del PC1 al PC0 con BGP

No.	Time	Source	Destination	Protocol	Leng	Info
230	125.815853	192.168.50.8	192.168.10.8	ICMP	74	Echo (ping) request id=0x0001, seq=589/19714, ttl=125 (reply in 231)
231	125.816041	192.168.10.8	192.168.50.8	ICMP	74	Echo (ping) reply id=0x0001, seq=589/19714, ttl=128 (request in 230)

*Imagen 13. Ping del PC2 al PC0 con BGP*

No.	Time	Source	Destination	Protocol	Leng	Info
22	11.170495	192.168.50.8	192.168.60.8	ICMP	74	Echo (ping) request id=0x0001, seq=593/20738, ttl=126 (reply in 23)
23	11.170572	192.168.60.8	192.168.50.8	ICMP	74	Echo (ping) reply id=0x0001, seq=593/20738, ttl=128 (request in 22)

*Imagen 14. Ping del PC2 al PC1 con BGP*

A partir de las imágenes anteriores (de la 10 a la 14), se observan los paquetes ICMP enviados entre las estaciones de trabajo para demostrar que la conexión está activa y funcional. Estos paquetes corresponden a *Echo (ping) Request* (Tipo 8, Código 0), enviado por el computador que realiza el ping, y *Echo (ping) Reply* (Tipo 0, Código 0), la respuesta del computador al que se le hace el ping.

Al obtener ambos paquetes, se confirma que la topología de red funciona correctamente, ya que, para que estos mensajes lleguen a su destino, deben atravesar los routers, switches y gateways de cada PC.

Además, en cada uno de los paquetes se puede observar las direcciones IP de origen y destino, correspondientes a las IPs de cada uno de los PCs.

Por otro lado, en la imagen 14 se observa que los paquetes atraviesan los routers necesarios, ya que el TTL del *Echo Request* proveniente del PC2 es 126, lo que indica que el paquete atravesó dos routers. Dado que normalmente el TTL inicia en 128 y se reduce en 1 cada vez que pasa por un router. Asimismo, el *Echo Reply* inicia en 128 porque se origina del PC que realiza las capturas.

## Paquetes de enrutamiento

No.	Time	Source	Destination	Protocol	Leng	Info
163	86.488518	Cisco_5f:41:97	CDP/VTP/DTP/PAGP/UDLD	CDP	416	Device ID: Switch Port ID: GigabitEthernet1/0/23
57	31.473696	Cisco_5f:41:97	CDP/VTP/DTP/PAGP/UDLD	CDP	416	Device ID: Switch Port ID: GigabitEthernet1/0/23

*Imagen 15. Paquetes CDP (protocolo BGP)*

Los paquetes CDP mostrados en la imagen anterior anuncian a los dispositivos Cisco entre sí para poder intercambiar información de la vecindad. Estos paquetes sirven para verificar que la conectividad física y de enlace entre routers existe antes de que BGP pueda establecer su sesión. Por lo tanto, la aparición de los paquetes confirma que la infraestructura base sobre la cual operará el protocolo de enrutamiento está funcionando y que la topología está correctamente conectada.

### 3. Topología 3

#### 3.1 Mapa de la topología 3

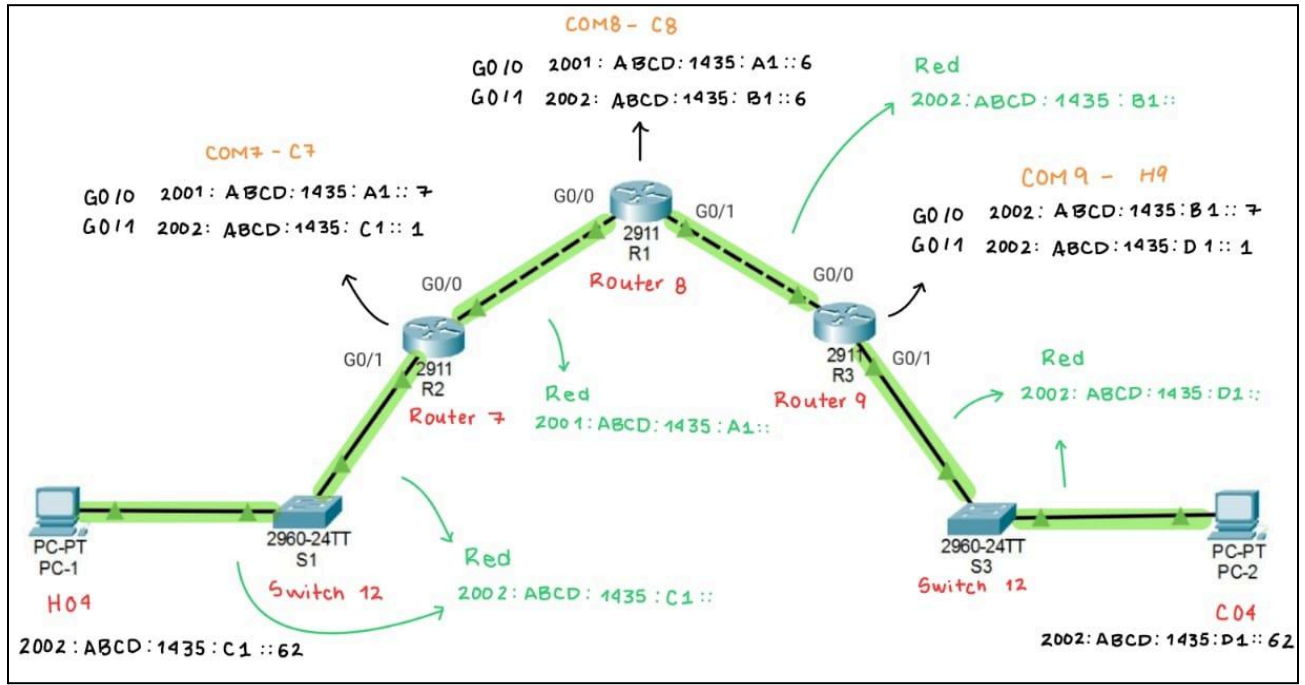


Imagen 16. Mapa de la topología 3

#### 3.2 Análisis de capturas con protocolo RIPng

##### Paquetes ICMPv6

No.	Time	Source	Destination	Protocol	Length	Info
21	1.031546	2002:abcd:1435:c1:4...	2002:abcd:1435:c1::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=243, hop limit=128 (reply in 22)
22	1.031627	2002:abcd:1435:c1::...	2002:abcd:1435:c1:4...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=243, hop limit=64 (request in 21)

Imagen 17. Ping del PC1 al PC2 con RIPng

No.	Time	Source	Destination	Protocol	Length	Info
20	2.327796	2002:abcd:1435:c1:4...	2002:abcd:1435:c1::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=236, hop limit=128 (reply in 21)
21	2.328217	2002:abcd:1435:c1::...	2002:abcd:1435:c1:4...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=236, hop limit=64 (request in 20)

Imagen 18. Ping del PC2 al PC1 con RIPng

En las capturas se evidencian los paquetes ICMPv6 Echo Request y Echo Reply generados durante la prueba de conectividad entre los equipos finales de la topología 3 configurada con RIPng.

En la primera imagen se observa el Echo Request desde 2002:ABCD:1435:C1:49df:5422:afd6:a64a hacia 2002:ABCD:1435:C1::62 con id=0x0001, seq=243 y hop limit=128, seguido de su Echo Reply con hop limit=64, confirmando que la solicitud llegó al destino y que la respuesta retornó correctamente.

La segunda captura muestra el mismo proceso en sentido inverso (PC2 a PC1) con la secuencia 236, evidenciando la comunicación bidireccional entre ambas redes.

Además, es importante notar que en las capturas realizadas desde los PCs el source y destination pertenecen al mismo prefijo IPv6. Esto sucede porque Wireshark solo observa el tráfico dentro de la red local (LAN) y, en IPv6, los hosts envían el primer salto del ping directamente a su gateway dentro del mismo segmento —no al destino final. Es decir, aunque el ping sea de PC1 a PC2, la PC1 solo ve el envío hacia su router local (en el prefijo C1), quien luego reenvía el paquete hacia las otras redes mediante RIPng. Por eso, en las capturas del extremo, las direcciones parecen locales aunque el ping atraviese toda la topología.

La presencia de ambos pares request/reply demuestra que existe conectividad IPv6 end-to-end y que RIPng está funcionando correctamente, distribuyendo las rutas entre los routers R1, R2 y R3 sin necesidad de configuración estática.

### Paquetes de enrutamiento

No.	Time	Source	Destination	Protocol	Length	Info
4305	15.425201	fe80::21c:f6ff:fe2f:ed43	ff02::9	RIPng	106	Command Response, Version 1
4369	23.024426	fe80::21c:f6ff:fe2f:ed43	ff02::9	RIPng	106	Command Response, Version 1
4461	31.782011	fe80::727d:b9ff:fe2b:d1e1	ff02::9	RIPng	106	Command Response, Version 1
4594	42.130575	fe80::21c:f6ff:fe2f:ed43	ff02::9	RIPng	106	Command Response, Version 1
4657	50.549758	fe80::21c:f6ff:fe2f:ed43	ff02::9	RIPng	106	Command Response, Version 1

*Imagen 19. Paquetes RIPng ( protocolo RIPng)*

En la captura se observan los mensajes RIPng Response, versión 1, enviados desde las direcciones de enlace local de los routers hacia el grupo de multidifusión ff02::9, que identifica a todos los routers RIPng del enlace.

Estos paquetes, transmitidos por UDP puerto 521, contienen los prefijos IPv6 y métricas que cada router anuncia a sus vecinos para actualizar sus tablas de enrutamiento.

La presencia de estos mensajes confirma que RIPng está activo y propagando rutas IPv6 entre los routers R1, R2 y R3, permitiendo la conectividad completa entre las redes sin usar rutas estáticas.

```

> Frame 44: Packet, 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{B4D471F2-32CE-4F46-B20B-8A170...
> Ethernet II, Src: Cisco_2b:d1:e1 (70:7d:b9:2b:d1:e1), Dst: IPv6mcast_09 (33:33:00:00:00:09)
> Internet Protocol Version 6, Src: fe80::727d:b9ff:fe2b:d1e1, Dst: ff02::9
> User Datagram Protocol, Src Port: 521, Dst Port: 521
  > RIPng
    Command: Response (2)
    Version: 1
    Reserved: 0000
    > Route Table Entry: IPv6 Prefix: 2001:abcd:1435:a1::/64 Metric: 1
    > Route Table Entry: IPv6 Prefix: 2002:abcd:1435:c1::/64 Metric: 1

```

*Imagen 20. Información de enrutamiento ( protocolo RIPng)*

```

> Frame 4594: Packet, 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface \Device\NPF_{B4D471F2-32CE-4F46-B20B-8A170ABB00CF}, id 0
> Ethernet II, Src: Cisco_2f:ed:43 (00:1c:f6:2f:ed:43), Dst: IPv6mcast_09 (33:33:00:00:00:09)
> Internet Protocol Version 6, Src: fe80::21c:f6ff:fe2f:ed43, Dst: ff02::9
> User Datagram Protocol, Src Port: 521, Dst Port: 521
▼ RIPng
  Command: Response (2)
  Version: 1
  Reserved: 0000
  ▶ Route Table Entry: IPv6 Prefix: 2002:abcd:1435:d1::/64 Metric: 1
  ▶ Route Table Entry: IPv6 Prefix: 2002:abcd:1435:b1::/64 Metric: 1

```

*Imagen 21. Información 2 de enrutamiento (protocolo RIPng)*

Las capturas muestran dos mensajes RIPng Response (versión 1) enviados por los routers de la topología para anunciar las rutas IPv6 que conocen. En ambos casos, los paquetes se transmiten mediante el grupo de multidifusión ff02::9, utilizado por todos los routers que participan en RIPng.

En la primera imagen, el router R3 anuncia los prefijos 2001:ABCD:1435:A1::/64 y 2002:ABCD:1435:C1::/64, cada uno con métrica 1, informando a sus vecinos (R1 y R2) sobre las redes a las que tiene acceso directo.

En la segunda imagen, el router R1 envía un paquete similar anunciando los prefijos 2002:ABCD:1435:D1::/64 y 2002:ABCD:1435:B1::/64, también con métrica 1, permitiendo que R2 y R3 actualicen sus tablas de enrutamiento.

La presencia de estos mensajes confirma que RIPng está intercambiando dinámicamente la información de rutas IPv6 entre todos los routers de la topología, asegurando que cada uno conozca las redes vecinas presentes en la infraestructura. Gracias a estas actualizaciones periódicas, el reenvío de los paquetes ICMPv6 entre PC1 y PC2 se logra correctamente sin necesidad de configurar rutas estáticas.

### 3.3 Análisis de capturas con protocolo OSPFv3

#### Paquetes ICMPv6

No.	Time	Source	Destination	Protocol	Length Info
38	5.832004	2002:abcd:1435:c1:4...	2002:abcd:1435:c1::...	ICMPv6	94 Echo (ping) request id=0x0001, seq=288, hop limit=128 (reply in 39)
39	5.832048	2002:abcd:1435:c1::...	2002:abcd:1435:c1:4...	ICMPv6	94 Echo (ping) reply id=0x0001, seq=288, hop limit=64 (request in 38)

*Imagen 22. Ping del PC1 al PC2 con OSPFv3*

No.	Time	Source	Destination	Protocol	Length Info
9	2.646846	2002:abcd:1435:c1:4...	2002:abcd:1435:c1::...	ICMPv6	94 Echo (ping) request id=0x0001, seq=288, hop limit=128 (reply in 10)
10	2.647138	2002:abcd:1435:c1::...	2002:abcd:1435:c1:4...	ICMPv6	94 Echo (ping) reply id=0x0001, seq=288, hop limit=64 (request in 9)

*Imagen 23. Ping del PC2 al PC1 con OSPFv3*

En las capturas se observan los paquetes ICMPv6 Echo Request y Echo Reply utilizados para comprobar la conectividad extremo a extremo entre los equipos finales de la topología 3 configurada con OSPFv3. Cada intercambio corresponde al envío de un Echo Request (Tipo 128, Código 0) desde el host de origen y su respectivo Echo Reply (Tipo 129, Código 0) desde el host destino.

En ambos sentidos se aprecia el mismo id=0x0001 y seq=288, con un Hop Limit de 128 en el Request y 64 en el Reply. La reducción del Hop Limit confirma que los mensajes atraviesan los routers intermedios antes de regresar al remitente, evidenciando que las rutas IPv6 están siendo correctamente calculadas por OSPFv3.

Es importante notar que, en las capturas realizadas desde los PCs, las direcciones source y destination pertenecen al mismo prefijo IPv6. Esto se debe a que Wireshark solo observa el tráfico dentro de la LAN local, por lo que el host no envía el ping directamente al equipo final remoto, sino al gateway de su red. El router se encarga luego de reenviar el paquete hacia las demás redes a través del proceso de enrutamiento OSPFv3. Por esta razón, las direcciones visibles en la captura son locales, aunque el ping sí esté cruzando toda la topología.

La recepción correcta de los Echo Reply confirma que la topología OSPFv3 está plenamente operativa, ya que las rutas IPv6 se distribuyen automáticamente entre los routers R1, R2 y R3, garantizando la conectividad entre todas las redes.

#### Paquetes de enrutamiento

No.	Time	Source	Destination	Protocol	Length	Info
3	0.332747	fe80::21c:f6ff:fe2f...	ff02::5	OSPF	94	Hello Packet
65	7.940540	fe80::727d:b9ff:fe2...	ff02::5	OSPF	94	Hello Packet
88	10.331793	fe80::21c:f6ff:fe2f...	ff02::5	OSPF	94	Hello Packet
3261	17.232455	fe80::727d:b9ff:fe2...	ff02::5	OSPF	94	Hello Packet
4266	20.330489	fe80::21c:f6ff:fe2f...	ff02::5	OSPF	94	Hello Packet
4307	26.860403	fe80::727d:b9ff:fe2...	ff02::5	OSPF	94	Hello Packet
4347	30.329684	fe80::21c:f6ff:fe2f...	ff02::5	OSPF	94	Hello Packet
4389	35.892076	fe80::727d:b9ff:fe2...	ff02::5	OSPF	94	Hello Packet
4416	40.328628	fe80::21c:f6ff:fe2f...	ff02::5	OSPF	94	Hello Packet

*Imagen 24. Paquetes OSPF( protocolo OSPFv3)*

En esta captura se muestran los paquetes OSPFv3 Hello, intercambiados entre las direcciones de enlace local de los routers hacia el grupo de multidifusión ff02::5, que identifica a todos los routers OSPF.

Estos mensajes permiten que los routers detecten vecinos, establezcan relaciones de adyacencia y mantengan activa la sesión OSPFv3.

Cada paquete “Hello” contiene el Router ID, intervalos de hello/dead y lista de vecinos, asegurando que la topología se mantenga sincronizada. La presencia periódica de estos mensajes confirma que OSPFv3 está operativo y propagando rutas IPv6 entre los routers, lo que garantiza la conectividad de todas las redes de la topología.

#### 4. Evidencias de trabajo



*Imagen 25. Foto en el laboratorio*

#### **Bibliografía**

Kurose, J. F., & Ross, K. W. (2012). *Computer Networking: A Top-Down Approach* (6th ed.). Addison-Wesley. Secciones 4.3–4.6



