Universidad de los Andes

Departamento de Ingeniería de Sistemas

Laboratorio #4: Protocolo de enrutamiento dinámicos con redes IPv4 e IPv6

ISIS3204 - Infraestructura de Comunicaciones

Grupo 3:

Juan Esteban Quiroga - 202013216
Juan Manuel Rodriguez - 202013372
Andres Felipe Ortiz - 201727662

2025-10

Contents

Introducción

El presente laboratorio tiene como objetivo principal **comprender y aplicar los protocolos de enrutamiento dinámico RIP y OSPF en entornos IPv4 e IPv6**, destacando sus diferencias estructurales y operativas. A través de la configuración práctica de routers Cisco en el simulador *Cisco Packet Tracer*, se busca afianzar los conceptos teóricos sobre el funcionamiento de los protocolos de vector distancia y de estado de enlace, así como el proceso de intercambio de información de enrutamiento y la construcción de tablas de rutas en topologías multi-router.

Durante el desarrollo de la práctica se implementan diferentes escenarios de red que integran el direccionamiento IP, la configuración de interfaces, y la activación de protocolos de enrutamiento dinámico. Esto permite observar cómo los routers actualizan sus tablas de enrutamiento de manera automática y cómo se comporta la red ante variaciones en la topología o fallos en los enlaces.

El laboratorio permite:

- Diferenciar los principios de funcionamiento de **RIP (Routing Information Protocol)** y **OSPF (Open Shortest Path First)**, tanto en su versión IPv4 como IPv6.
- Configurar y verificar el intercambio de rutas dinámicas entre múltiples routers, observando métricas como el conteo de saltos y el costo por ancho de banda.
- Comprender el proceso de **asignación jerárquica de direcciones IP**, el uso de máscaras de subred y prefijos en IPv6, así como la importancia del direccionamiento correcto en la conectividad de red.
- Analizar el impacto de los protocolos de enrutamiento en la convergencia de la red y en la eficiencia del encaminamiento de paquetes.

De esta forma, la práctica integra los conceptos fundamentales del **nivel de red del modelo OSI**, brindando una experiencia completa que abarca el diseño, configuración y validación de una infraestructura de comunicación moderna y funcional.

1 Protocolo RIP (Routing Information Protocol)

El protocolo **RIPv1** es un protocolo de enrutamiento dinamico con clase que utiliza el algoritmo belmanfort para encontrar el camino con menor cantidad de saltos; a esto le llamamos vector distancia. Vale la pena mencionar que este protocolo (RIP en general) no se utiliza para más de 15 saltos, esto por el algoritmo utilizado, al pasar de 15 saltos se considerara inalcanzable, por lo que **RIP** solo se utiliza para redes pequeñas.

1.1 Analisis del protocolo de enrutamiento

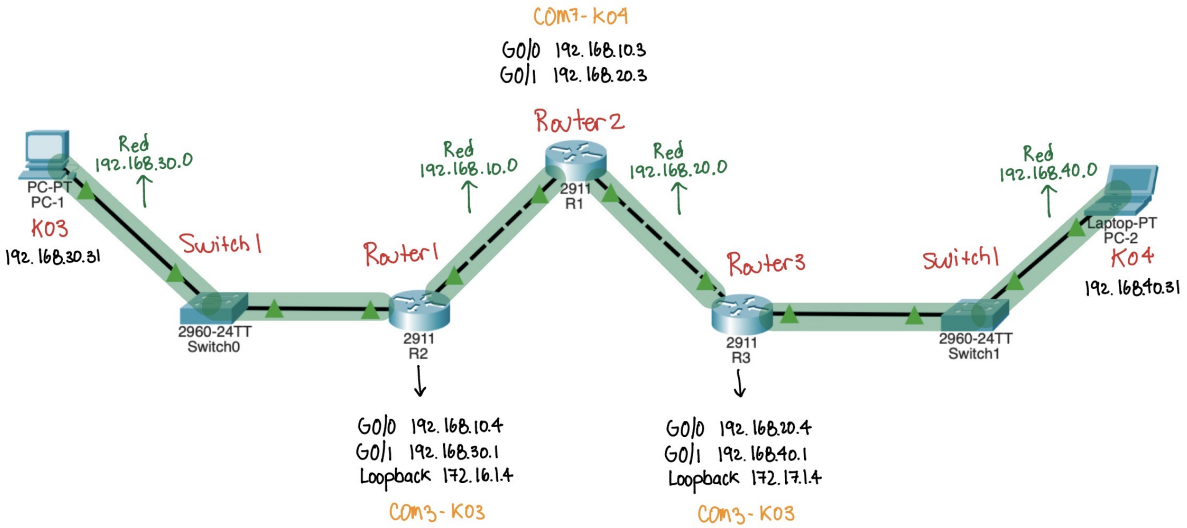

Figure 1: *Mapa topologia numero 1.*

Para empezar, usaremos la topologia 1, donde, como se ve en la imagen, tendremos 3 routers (numero de saltos menor a 15), y las capturas de los paquetes que veremos a continuacion corresponderan a las capturas del computador marcado como *PC-2*. A continuacion vemos los paquetes que capturados con el protocolo **RIP**

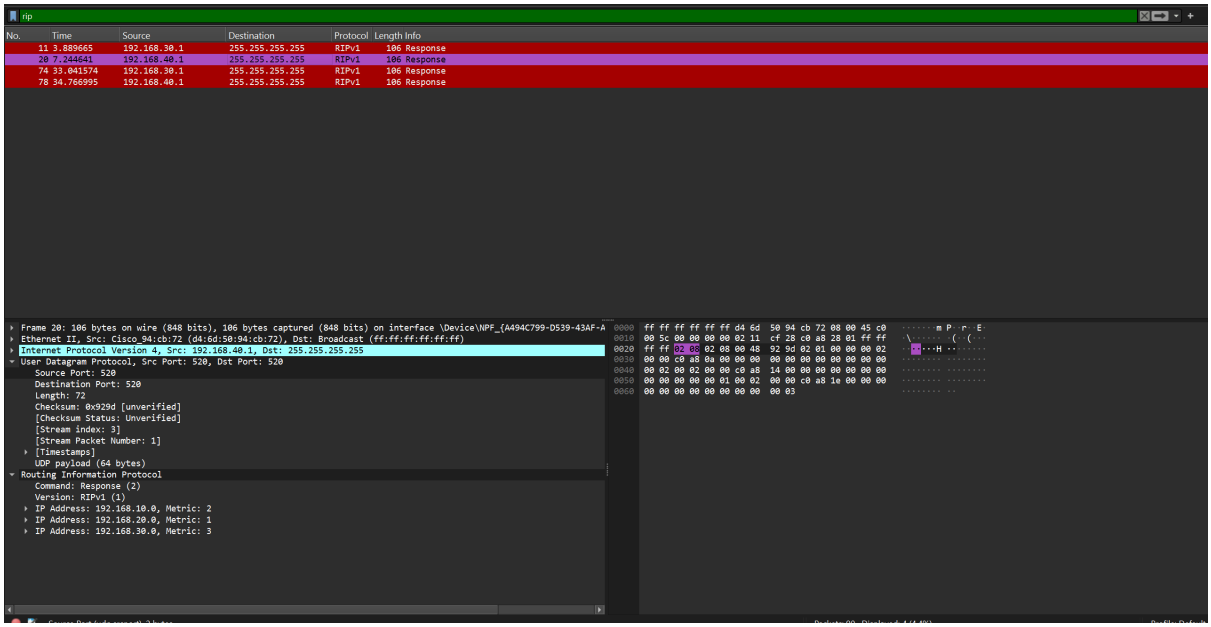

Figure 2: *Capturas del protocolo RIPv1.*

En esta captura podemos ver varias caracteristicas importantes del protocolo **RIP**, una de ellas es el uso del protocolo de la capa de transporte *UDP* con el puerto 520. Tambien, podemos ver el uso de la direccion de destino *255.255.255.255* mostrando que en efecto estamos usando **RIPv1** pues en esta version del protocolo se utiliza una direccion broadcast, a diferencia de la version 2 del protocolo que utiliza una direccion de multicast. Ahora bien, y más relevante aun, podemos ver las rutas que esta tomando el protocolo, junto con su numero de saltos, como lo podemos ver a continuacion en la siguiente tabla e imagen:

Figure 3: *Rutas del protocolo RIPv1.*

Tabla 1: *Rutas anunciadas en el mensaje RIPv1*

Dirección IP	Métrica	Interpretación
192.168.10.0	2	Red alcanzable a 2 saltos
192.168.20.0	2	Red alcanzable a 2 saltos
192.168.30.0	3	Red alcanzable a 3 saltos

Como lo mencionabamos anteriormente, vemos la cantidad de saltos que necesita desde cierto router para alcanzar las diferentes redes que hay habilitadas, ademas, muestra como cada uno de los routers "anuncia" a los demas componentes de la red su tabla de enrutamiento para la llegada a los diferentes segmentos de la red.

1.2 Prueba de conectividad

Ahora vamos a ver la evidencia del correcto funcionamiento del enrutamiento a traves de los paquetes icmp, usando el comando *ping* entre los computadores *PC-0, ip: 192.168.40.31* y *PC-2, ip: 192.168.30.31*

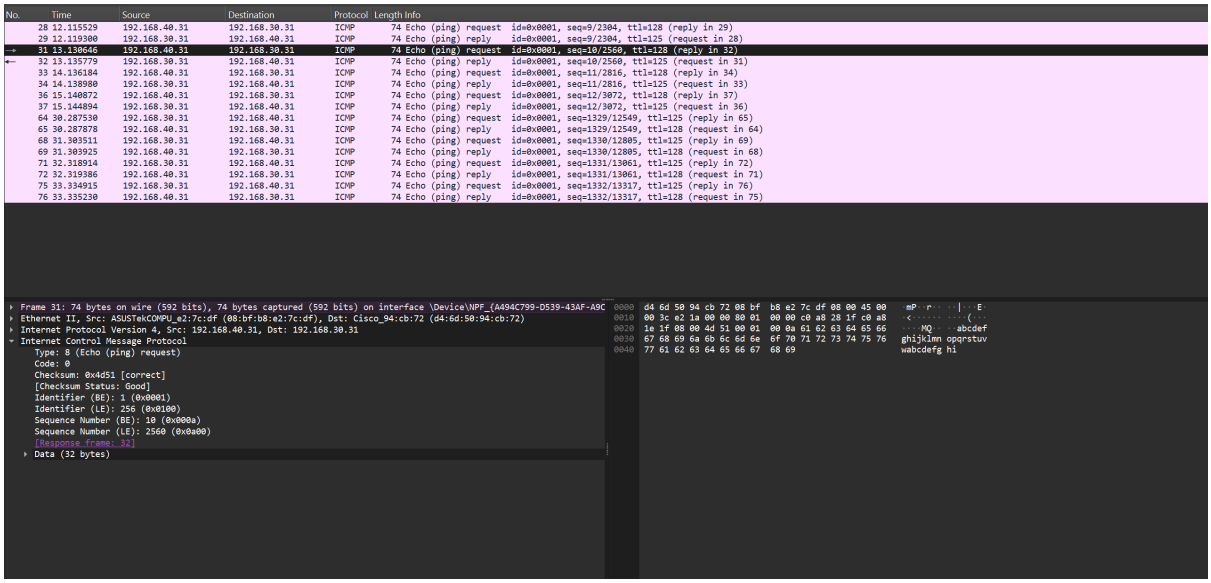

Figure 4: *Prueba de conectividad protocolo RIPv1.*

En la captura podemos observar los mensajes del protocolo **ICMP** que se generan al ejecutar el comando *ping* desde el *PC-2* (`192.168.40.31`) hacia el *PC-0* (`192.168.30.31`). En este caso, se aprecia el intercambio correcto de solicitudes y respuestas de eco (*Echo Request* y *Echo Reply*), lo que evidencia que el proceso de enrutamiento entre las redes funciona de manera adecuada.

Cada paquete ICMP de tipo 8 (solicitud de eco) enviado desde el equipo origen recibe su correspondiente paquete de tipo 0 (respuesta de eco) desde el destino, confirmando que los datos están llegando correctamente y regresando sin pérdida alguna. Los valores de *Checksum* aparecen como correctos, lo que indica que no existen errores de transmisión en los mensajes capturados.

El tiempo de respuesta entre cada solicitud y su respectiva respuesta es aproximadamente de **0.021 milisegundos**, lo cual es un valor bajo y característico de una red local (LAN) bien configurada. Este tiempo refleja que la comunicación entre ambos extremos es eficiente y que no hay retardos significativos durante el tránsito de los paquetes a través de los routers.

Adicionalmente, el valor del campo *TTL (Time To Live)* en los mensajes capturados permite inferir que existe al menos un salto intermedio entre los dos equipos, lo que concuerda con la topología establecida y confirma que los routers están realizando el reenvío de paquetes correctamente. De igual forma, se identifican las direcciones físicas de origen y destino (`08:bf:b8:e2:7c:df` y `d4:6d:50:94:cb:72`), correspondientes a los dispositivos involucrados en la comunicación.

2 Protocolo BGP (Border Gateway Protocol)

El **Border Gateway Protocol (BGP)** es un protocolo de enrutamiento exterior (EGP) utilizado para el intercambio de información de enrutamiento entre sistemas autónomos (AS). A diferencia de los protocolos de gateway interior (IGP) como RIP u OSPF, que se utilizan dentro de un dominio administrativo, BGP opera entre dominios, tomando decisiones de enrutamiento basadas en políticas y reglas definidas por el administrador de red más que en métricas técnicas.

En este laboratorio, se implementó una topología de tres routers interconectados, donde se configuró BGP entre los sistemas autónomos definidos para permitir la conectividad entre redes IPv4 de diferentes dominios. Posteriormente, se realizaron pruebas de conectividad mediante mensajes ICMP (*ping*) para validar el intercambio de rutas entre routers.

2.1 Pruebas de Conectividad

Para la verificación del correcto funcionamiento de BGP, se capturaron paquetes ICMP entre las redes 192.168.10.0/24, 192.168.50.0/24 y 192.168.60.0/24. En los siguientes análisis de Wireshark se observan

las solicitudes y respuestas de *Echo (ping)* entre las distintas interfaces de los routers.

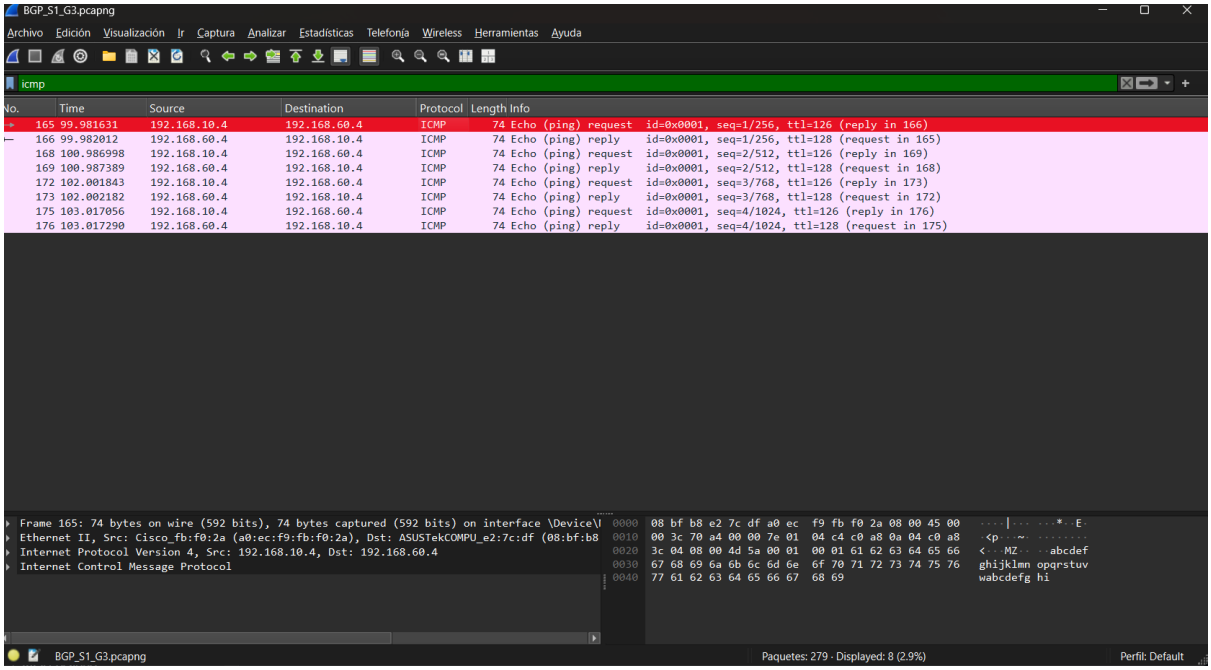

Figure 5: *Tráfico ICMP entre las redes 192.168.10.4 y 192.168.60.4 (primer intercambio de pings).*

En la captura anterior se aprecia el envío y la respuesta de paquetes ICMP entre los nodos de las subredes 192.168.10.0 y 192.168.60.0, evidenciando la correcta propagación de rutas mediante BGP. Cada solicitud (request) tiene su respectiva respuesta (reply), con un *Time To Live (TTL)* inicial de 126 para el envío y de 128 para la respuesta, lo que confirma el reenvío exitoso a través de múltiples saltos.

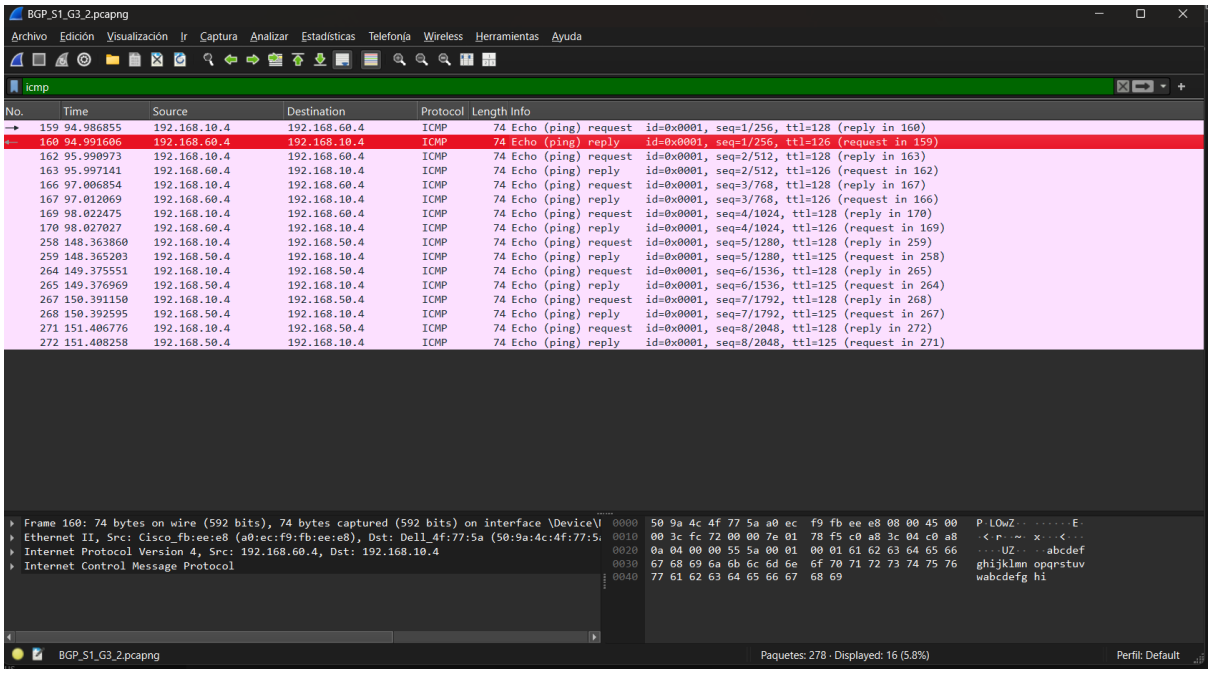

Figure 6: *Intercambio de paquetes ICMP entre 192.168.10.4 y 192.168.60.4 durante pruebas extendidas.*

En esta segunda captura se verifica que el intercambio de mensajes ICMP continúa estable en ambas direcciones. El identificador (`id=0x0001`) y el número de secuencia (`seq`) incrementan de forma correcta, mostrando la continuidad del flujo de datos entre las redes asociadas a los diferentes routers configurados bajo BGP.

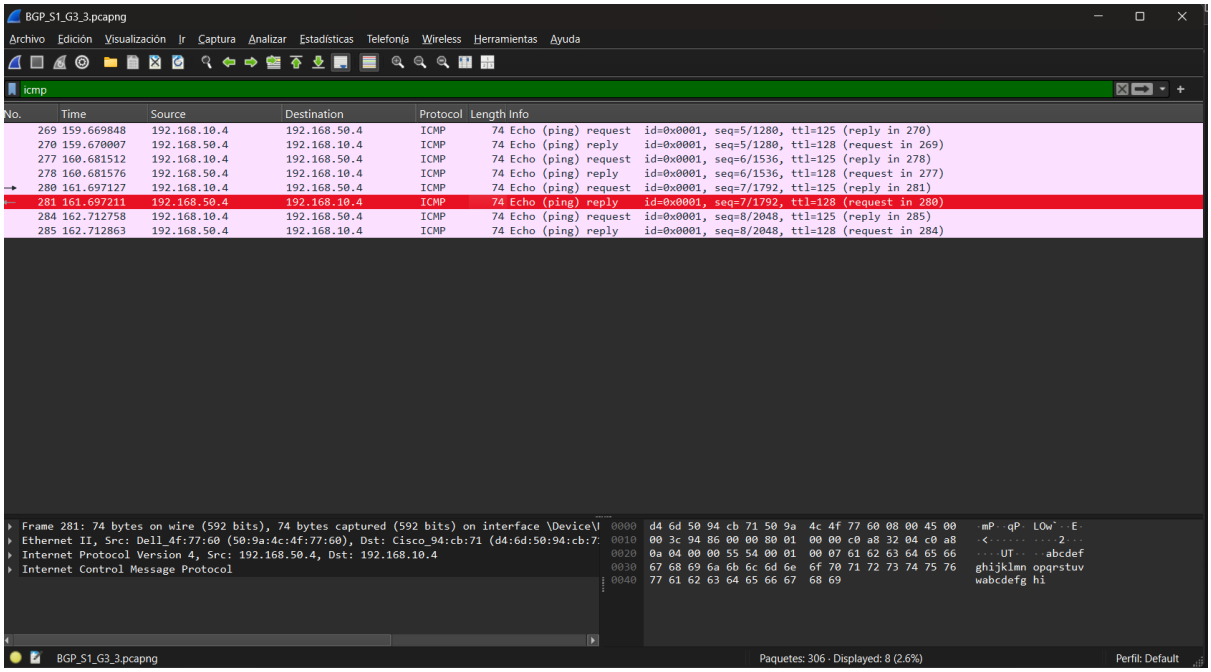

Figure 7: *Comunicación ICMP entre las redes 192.168.10.4 y 192.168.50.4 (enlace verificado).*

Finalmente, en la tercera captura se observa el intercambio exitoso de paquetes entre las redes 192.168.10.0 y 192.168.50.0. El correcto establecimiento de las sesiones BGP permitió el anuncio y la propagación de rutas entre los sistemas autónomos, garantizando la conectividad total entre los extremos.

2.2 Conclusión del BGP

Los resultados de las pruebas confirman que el protocolo BGP se configuró correctamente, permitiendo la propagación de rutas entre diferentes sistemas autónomos y asegurando la conectividad completa entre las subredes. Las capturas en Wireshark demuestran que los routers establecieron correctamente las sesiones BGP y que los paquetes ICMP alcanzan los destinos remotos, evidenciando la convergencia exitosa del protocolo y la efectividad del enrutamiento exterior.

References

[1] Computer Networking, a top-down approach. James Kurose, Keith Ross. Addison-Wesley, 6th ed.