García Ferrer Daniel Guadalupe
Práctica: Administración y Supervisión de Redes
Área: Intercomunicación de Redes

Consideraciones de diseño: En la interconexión de redes, el diseño es una etapa crítica. Implica planificar cómo se conectarán y comunicarán las redes para garantizar un rendimiento eficiente y confiable. Algunos aspectos clave a considerar en el diseño de la interconexión de redes incluyen la topología de la red (estrella, anillo, malla, etc.), la selección de protocolos, la seguridad, la redundancia, la escalabilidad y la capacidad de adaptarse a futuros cambios.

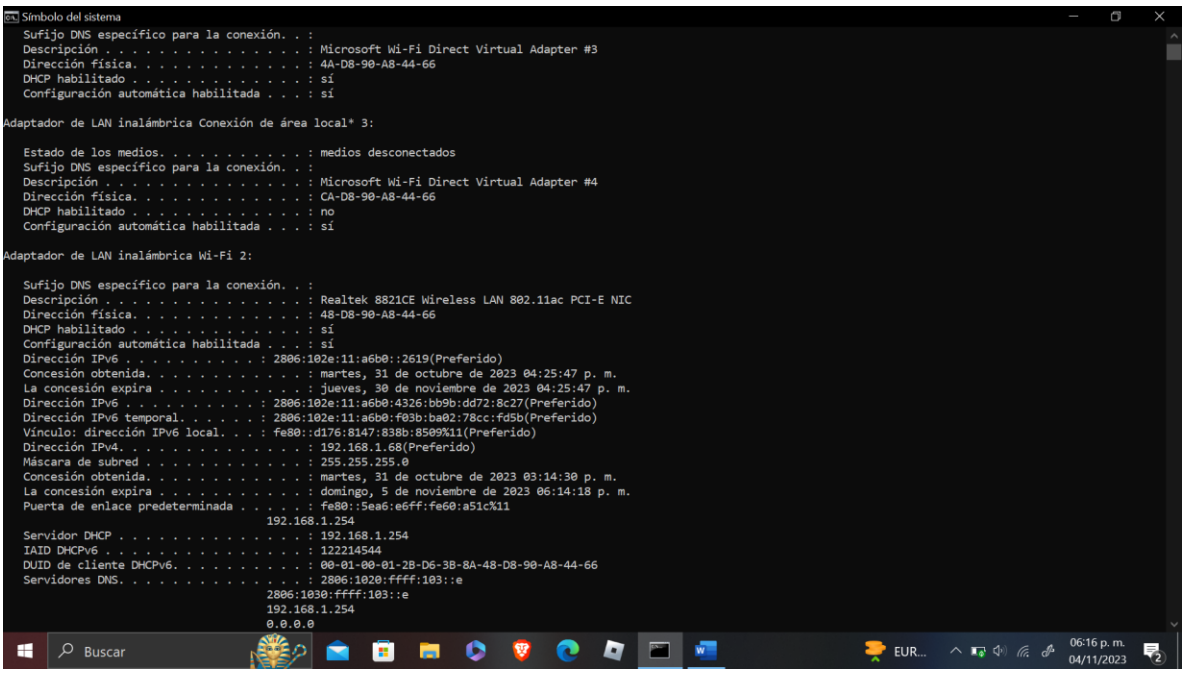
Análisis de la generación de tráfico producida por los diferentes protocolos: Este tema se refiere al estudio de cómo los diferentes protocolos de comunicación afectan la generación de tráfico en una red. Algunos protocolos generan más tráfico que otros debido a la cantidad de datos de control, encabezados y cargas útiles que transmiten. Comprender cómo los protocolos influyen en la generación de tráfico es esencial para dimensionar adecuadamente la red y garantizar un rendimiento óptimo.

Sistemas heterogéneos: Los sistemas heterogéneos se refieren a la interconexión de redes o dispositivos que utilizan diferentes tecnologías, protocolos o estándares. Esto es común en entornos de redes, donde puede haber dispositivos con diversas interfaces y sistemas operativos. La interconexión de sistemas heterogéneos a menudo requiere el uso de pasarelas o protocolos de traducción para que puedan comunicarse eficazmente.

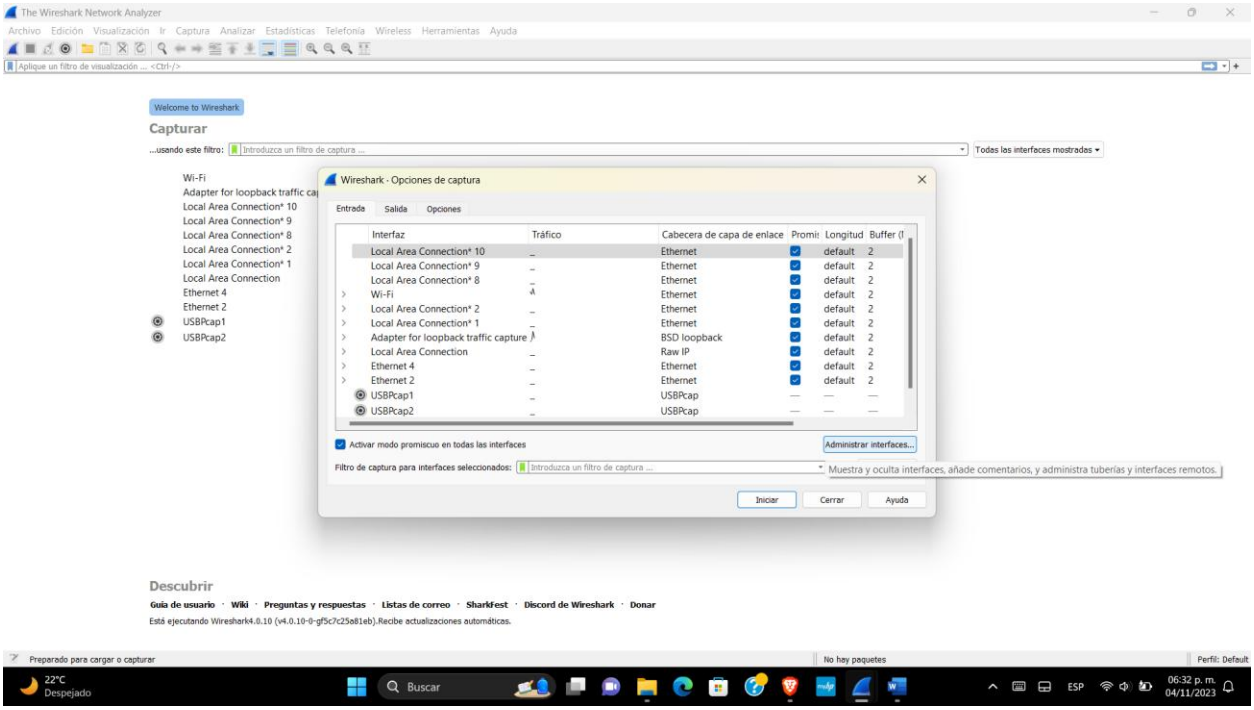
Administración y supervisión: La administración y supervisión de redes es esencial para garantizar un funcionamiento eficiente y confiable. Involucra la configuración, supervisión y mantenimiento de dispositivos de red, la gestión de la seguridad, el seguimiento del tráfico, la resolución de problemas y la recopilación de datos para optimizar el rendimiento. La administración de red también incluye la implementación de políticas de seguridad, actualizaciones de software y la gestión de recursos

Desarrollo de la práctica.

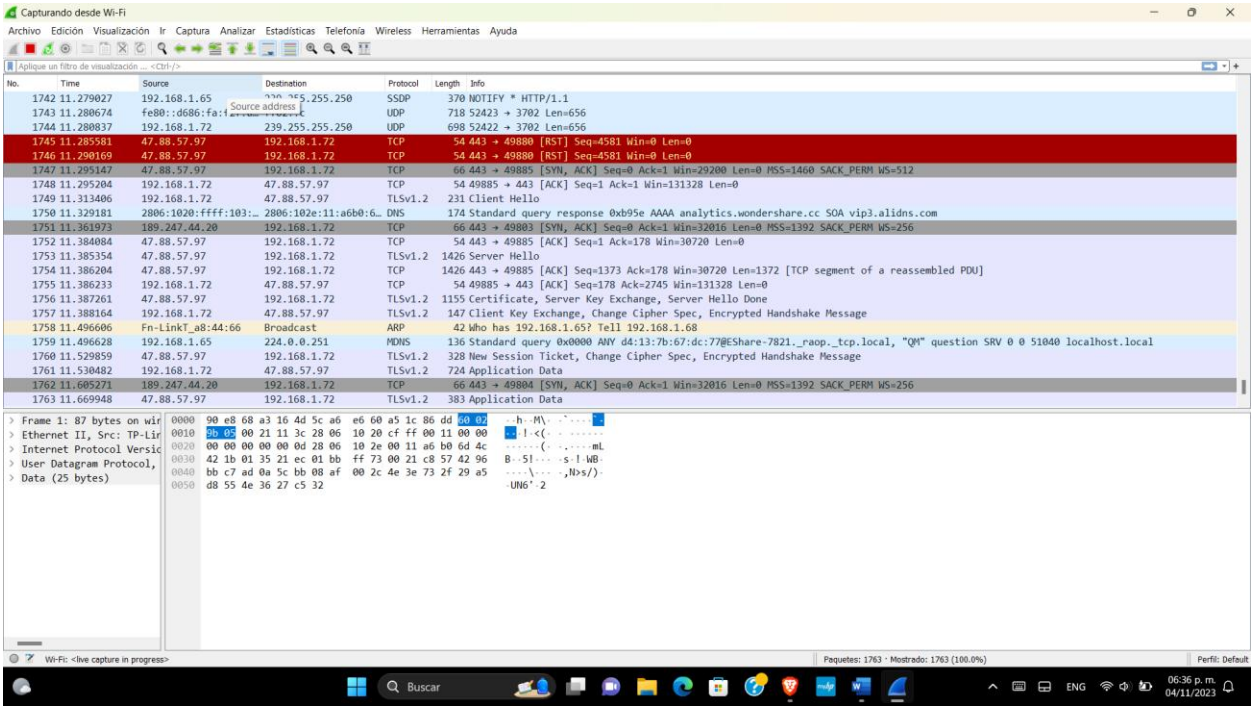
En una PC de la Red, abrimos el CMD y ejecutamos el comando “ipconfig/all” y en la información que aparece ubicamos la Direccion Física y la Direccion Local de la PC2.



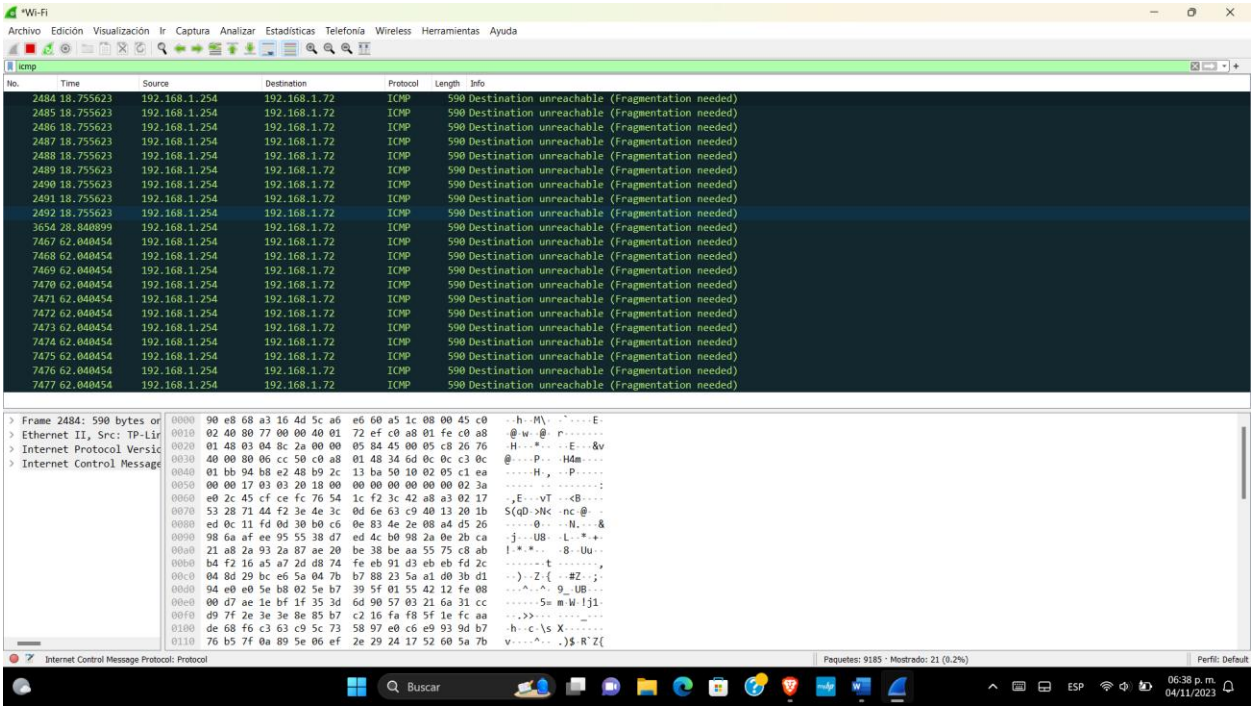
Abrimos WIRESHARK en el menú “Capturar Interfaces”



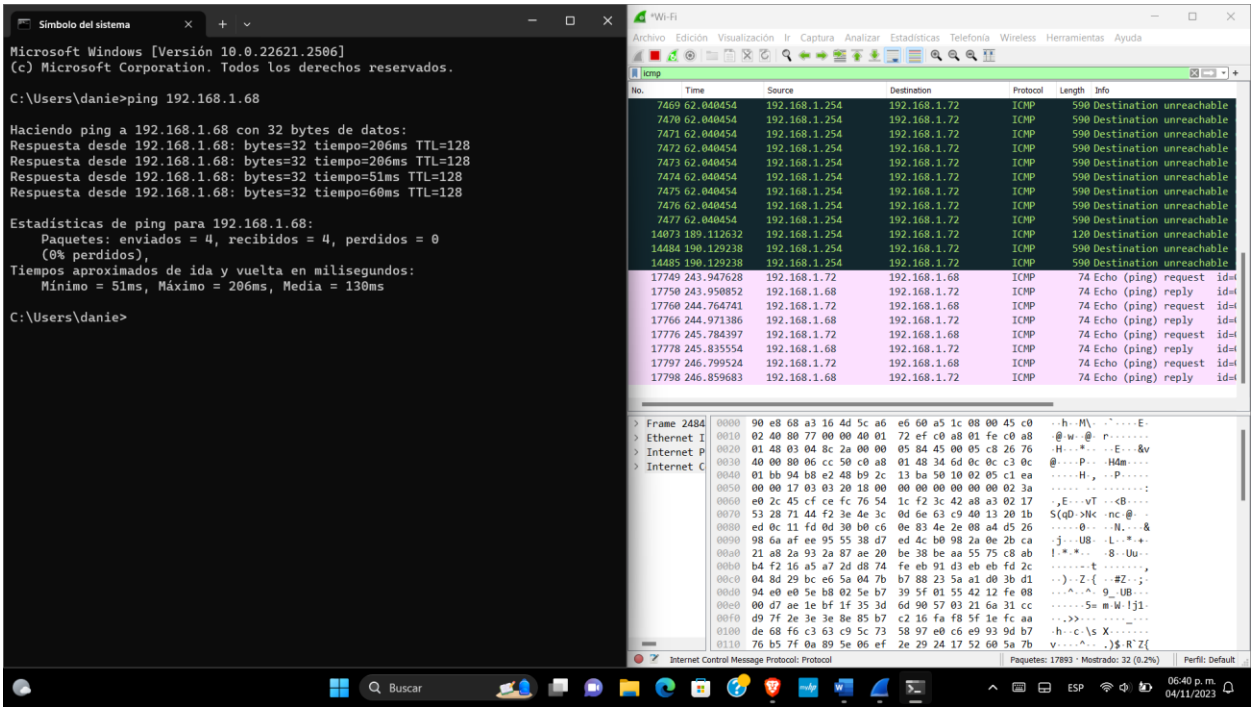
Iniciamos la captura de datos.



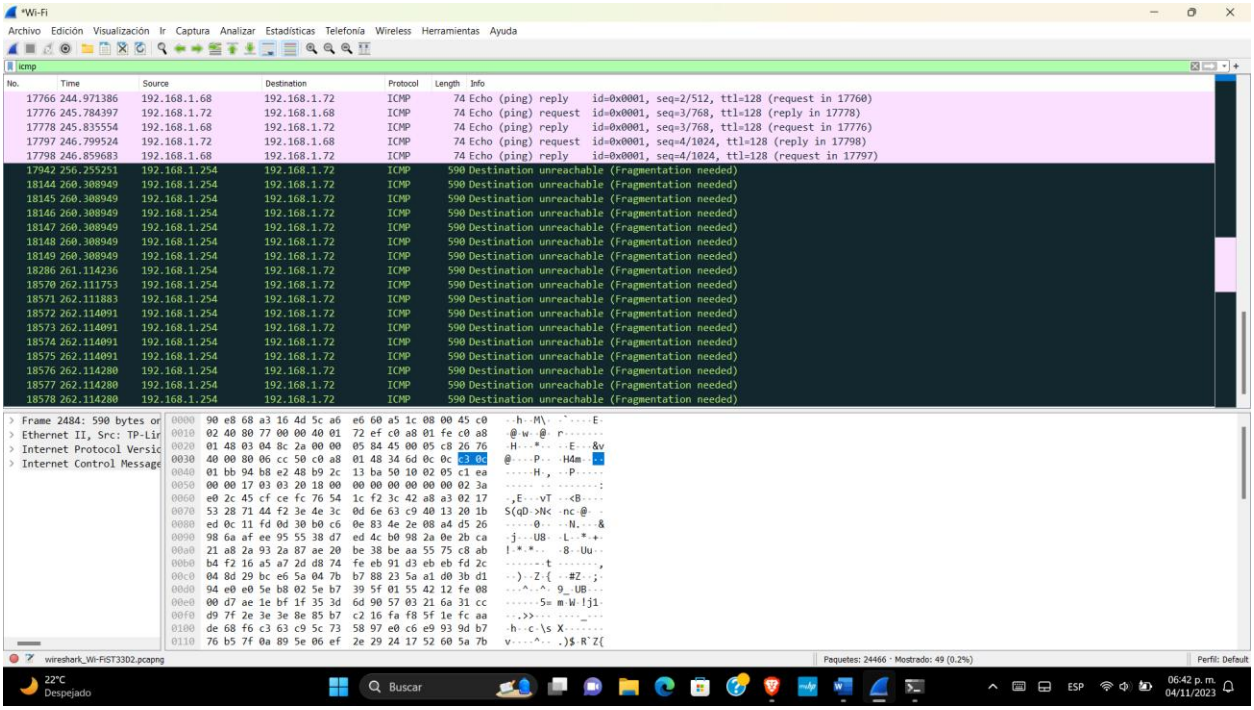
Aplicamos el filtro “icmp”



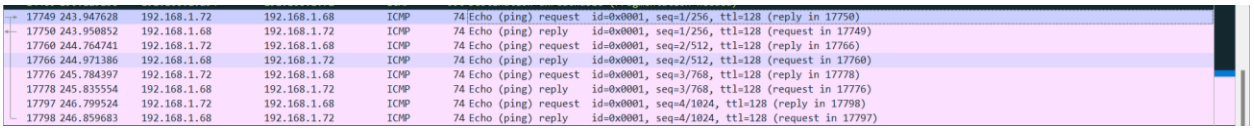
Al hacer ping de mi PC a la PC2 de mi área de red, el programa WIRESHARK empieza a mostrar más datos.



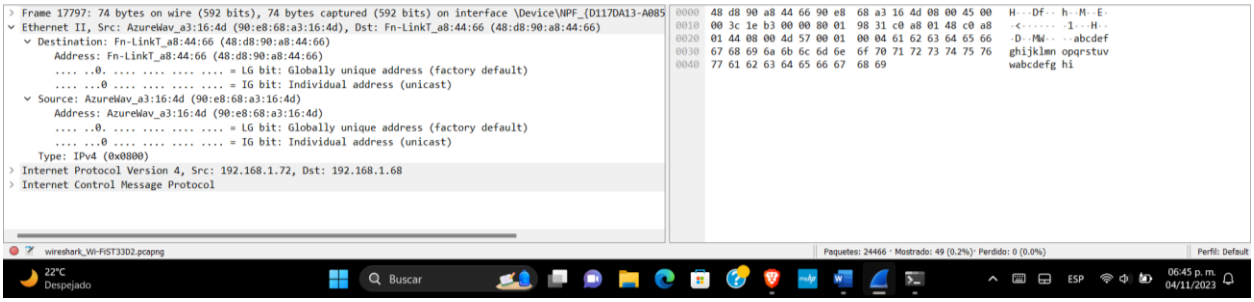
Detenemos la captura de datos y los analizamos.



Visualizamos la ejecución del PING de mi PC al PC2



Ahora vemos las direcciones MAC de origen y del destino



¿La dirección MAC de origen coincide con la interfaz de su PC? Efectivamente, las direcciones MAC coinciden perfectamente.

¿La dirección MAC de destino en Wireshark coincide con la dirección MAC del compañero de equipo? Efectivamente, las direcciones MAC coinciden perfectamente.

¿De qué manera su PC obtiene la dirección MAC de la PC a la que hizo ping?

Cuando realizamos un comando "ping" desde nuestra PC a otra PC en una red local o a través de Internet, mi computadora necesita la dirección MAC (Media Access Control) de la PC de destino para enviar paquetes de datos a esa dirección física específica en la red local. La dirección MAC se utiliza en la capa de enlace de datos del modelo OSI para identificar de manera única dispositivos dentro de una red local.

El proceso de obtención de la dirección MAC de la PC de destino cuando haces un "ping" generalmente implica varias etapas:

1. Resolución ARP (Address Resolution Protocol): Cuando envías un paquete "ping" a una dirección IP de destino, tu PC primero debe determinar la dirección MAC asociada con esa dirección IP en la red local. Para hacerlo, realiza una solicitud ARP. Tu computadora crea un paquete ARP que contiene la dirección IP de destino y lo difunde a todos los dispositivos en la red local.

2. Respuesta ARP: La PC de destino, si está en la misma red local, responderá a la solicitud ARP con su propia dirección MAC. Esta respuesta ARP es recibida por tu computadora y se almacena en una tabla ARP local, que asocia la dirección IP de destino con su dirección MAC correspondiente.

3. Envío del paquete: Con la dirección MAC de destino conocida, tu PC puede construir un paquete Ethernet que contiene la dirección MAC del destinatario y el paquete "ping" (ICMP). Luego, envía el paquete a través de la red local.

En resumen, nuestra PC obtiene la dirección MAC de la PC a la que hizo ping a través de una solicitud ARP y una respuesta ARP. Una vez que la dirección MAC se ha resuelto, nuestra PC puede dirigir eficazmente los paquetes a la dirección física correcta en la red local para establecer la comunicación.

Referencias.

Sites, G. (2016, 16 mayo). Práctica de laboratorio: Uso de Wireshark para ver el tráfico de la red. Recuperado 5 de agosto de 2020, de: site