

**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 Dirección Física y la Dirección Local de la PC2.

```
Símbolo del sistema
Suíjo DNS específico para la conexión. . . :
Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
Dirección física. . . . . : 4A-D8-90-A8-44-66
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Conexión de área local* 3:

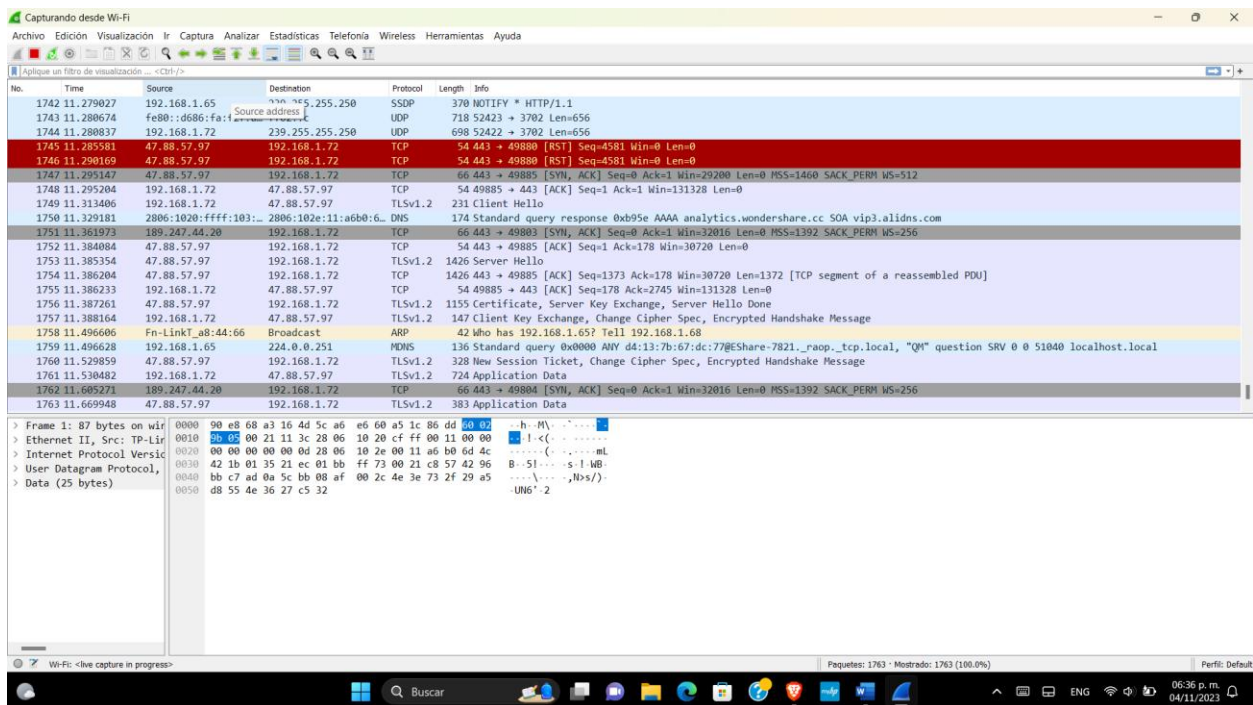
Estado de los medios. . . . . : medios desconectados
Suíjo DNS específico para la conexión. . . :
Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
Dirección física. . . . . : CA-D8-90-A8-44-66
DHCP habilitado . . . . . : no
Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Wi-Fi 2:

Suíjo DNS específico para la conexión. . . :
Descripción . . . . . : Realtek 8821CE Wireless LAN 802.11ac PCI-E NIC
Dirección física. . . . . : 48-D8-90-A8-44-66
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Dirección IPv6 . . . . . : 2806:102e:11:a6b0::2619(Preferido)
Concesión obtenida. . . . . : martes, 31 de octubre de 2023 04:25:47 p. m.
La concesión expira . . . . . : jueves, 30 de noviembre de 2023 04:25:47 p. m.
Dirección IPv6 . . . . . : 2806:102e:11:a6b0:4326:bb9b:dd72:8c27(Preferido)
Dirección IPv6 temporal. . . . . : 2806:102e:11:a6b0:f03b:ba02:78cc:fd5b(Preferido)
Vínculo: dirección IPv6 local. . . : fe80::d176:8147:838b:8509%11(Preferido)
Dirección IPv4. . . . . : 192.168.1.68(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : martes, 31 de octubre de 2023 03:14:30 p. m.
La concesión expira . . . . . : domingo, 5 de noviembre de 2023 06:14:18 p. m.
Puerta de enlace predeterminada . . . : fe80::5ea6:e6ff:fe60:a51c%11
192.168.1.254
Servidor DHCP . . . . . : 192.168.1.254
IAID DHCPv6 . . . . . : 122214544
DUID de cliente DHCPv6. . . . . : 00-01-00-01-28-D6-3B-8A-48-D8-90-A8-44-66
Servidores DNS. . . . . : 2806:1020:ffff:103::e
192.168.1.254
0.0.0.0
```



Iniciamos la captura de datos.



## Aplicamos el filtro "icmp"

Wireshark capture showing ICMP Echo (ping) requests and replies. The filter 'icmp' is applied. The packet list shows multiple 'Destination unreachable' messages. The packet details pane shows the structure of an ICMP Echo request.

No.	Time	Source	Destination	Protocol	Length	Info
2484	18.755623	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
2485	18.755623	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
2486	18.755623	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
2487	18.755623	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
2488	18.755623	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
2489	18.755623	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
2490	18.755623	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
2491	18.755623	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
2492	18.755623	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
3654	28.840899	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7467	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7468	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7469	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7470	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7471	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7472	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7473	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7474	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7475	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7476	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)
7477	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable (Fragmentation needed)

Frame 2484: 590 bytes on wire (4720 bits) captured (0.000000000 seconds) on interface 0:00:00:00:00:00 from 192.168.1.254 to 192.168.1.72

Ethernet II, Src: TP-LINK (08:00:00:00:00:00), Dst: 192.168.1.72 (08:00:00:00:00:00)

Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.72

Internet Control Message Protocol, Type: Echo (ping) request (8)

0000 90 e8 68 a3 16 4d 5c a6 e6 60 a5 1c 08 00 45 c0 --h-M\-----E-  
0010 02 40 80 77 00 00 40 01 72 ef c0 a8 01 fe c0 a8 --@w@-n-----  
0020 01 a8 03 04 8c 2a 00 00 05 84 45 00 05 c8 26 76 --H-\*---E---&v  
0030 40 00 00 06 cc 50 c0 a8 01 48 34 6d 0c 0c c3 0c --@---P---Hd---  
0040 01 bb 94 b8 e2 48 b9 2c 13 ba 50 10 02 05 c1 ea -----H---P-----  
0050 00 00 17 03 03 20 18 00 00 00 00 00 00 02 3a -----  
0060 e0 2c 45 cf ce fc 76 54 1c f2 3c 42 a8 a3 02 17 --,E---vT---<B---  
0070 53 28 71 44 f2 3e 4e 3c 0d 6e 63 c9 40 13 20 1b S(qd>Nc-nc@-  
0080 ed 0c 11 fd 0d 30 b0 c6 0e 83 4e 2e 08 a4 d5 26 --0---0---N---&  
0090 98 6a af ee 95 55 38 d7 ed 4c b0 98 2a 0e 2b ca --j---UB---L---\*---  
00a0 21 a8 2a 93 2a 87 ae 20 be 38 be aa 55 75 c8 ab l-\*---8-Uu---  
00b0 b4 f2 16 a5 a7 2d d8 74 fe eb 91 d3 eb eb fd 2c -----t-----  
00c0 04 8d 29 bc e6 5a 04 7b b7 88 23 5a a1 d0 3b d1 --)-Z(-#Z-;  
00d0 94 e0 e0 5e b8 02 5e b7 39 5f 01 55 42 12 fe 08 --^---^---9\_UB---  
00e0 00 d7 ae 1e bf 1f 35 3d 6d 90 57 03 21 6a 31 cc -----5-m-W-lj1-  
00f0 d9 7f 2e 3e 3e 8e 85 b7 c2 16 fa f8 5f 1e fc aa -->--->--->--->---  
0100 de 68 f6 c3 63 c9 5c 73 58 97 e0 c6 e9 93 9d b7 --h-c\>S X-----  
0110 76 b5 7f 0a 89 5e 06 ef 2e 29 24 17 52 60 5a 7b v-----)\$.R'Z{

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

Wireshark capture showing ICMP Echo (ping) requests and replies. The filter 'icmp' is applied. The packet list shows multiple 'Echo (ping) request' and 'Echo (ping) reply' messages. The packet details pane shows the structure of an ICMP Echo request.

No.	Time	Source	Destination	Protocol	Length	Info
7468	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
7470	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
7471	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
7472	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
7473	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
7474	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
7475	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
7476	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
7477	62.040454	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
14073	189.112632	192.168.1.254	192.168.1.72	ICMP	120	Destination unreachable
14084	190.129238	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
14485	190.129238	192.168.1.254	192.168.1.72	ICMP	590	Destination unreachable
17749	243.947628	192.168.1.72	192.168.1.68	ICMP	74	Echo (ping) request
17750	243.950852	192.168.1.68	192.168.1.72	ICMP	74	Echo (ping) reply
17760	244.764741	192.168.1.72	192.168.1.68	ICMP	74	Echo (ping) request
17766	244.971386	192.168.1.68	192.168.1.72	ICMP	74	Echo (ping) reply
17776	245.784397	192.168.1.72	192.168.1.68	ICMP	74	Echo (ping) request
17778	245.835554	192.168.1.68	192.168.1.72	ICMP	74	Echo (ping) reply
17797	246.799524	192.168.1.72	192.168.1.68	ICMP	74	Echo (ping) request
17798	246.859683	192.168.1.68	192.168.1.72	ICMP	74	Echo (ping) reply

Frame 2484: 590 bytes on wire (4720 bits) captured (0.000000000 seconds) on interface 0:00:00:00:00:00 from 192.168.1.254 to 192.168.1.72

Ethernet II, Src: TP-LINK (08:00:00:00:00:00), Dst: 192.168.1.72 (08:00:00:00:00:00)

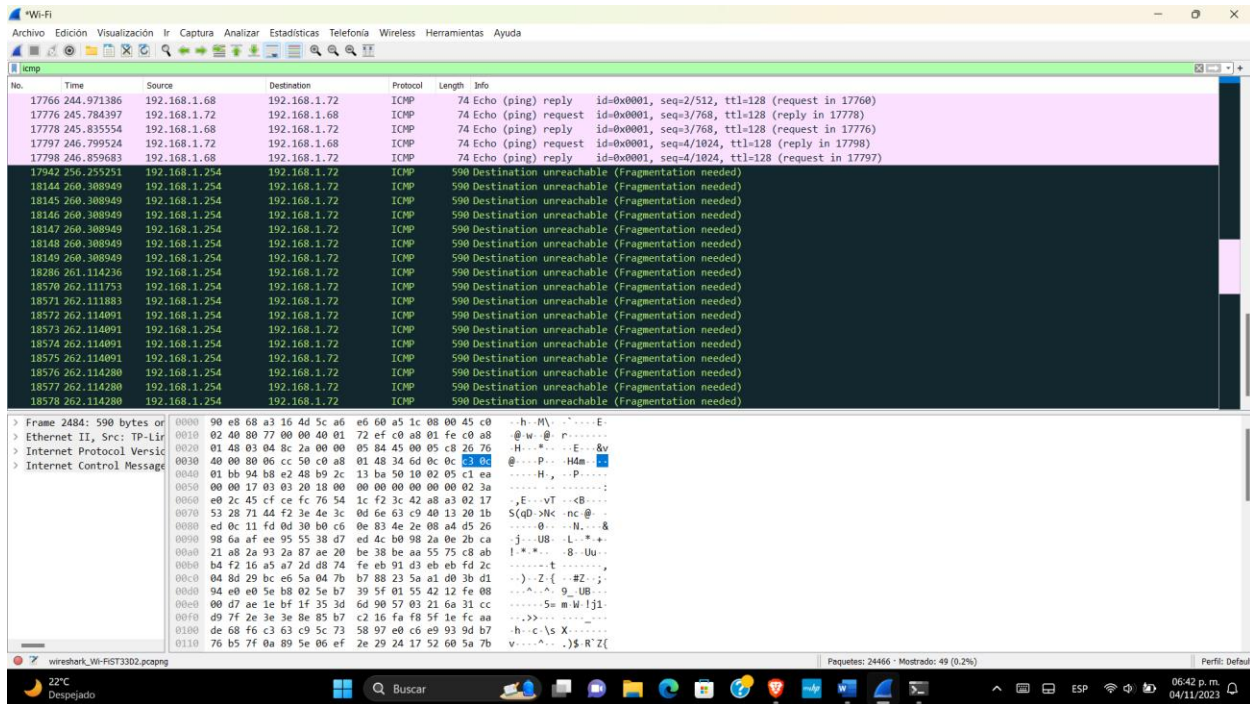
Internet Protocol Version 4, Src: 192.168.1.254, Dst: 192.168.1.72

Internet Control Message Protocol, Type: Echo (ping) request (8)

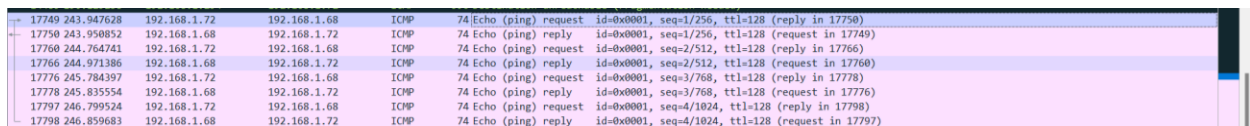
0000 90 e8 68 a3 16 4d 5c a6 e6 60 a5 1c 08 00 45 c0 --h-M\-----E-  
0010 02 40 80 77 00 00 40 01 72 ef c0 a8 01 fe c0 a8 --@w@-n-----  
0020 01 a8 03 04 8c 2a 00 00 05 84 45 00 05 c8 26 76 --H-\*---E---&v  
0030 40 00 00 06 cc 50 c0 a8 01 48 34 6d 0c 0c c3 0c --@---P---Hd---  
0040 01 bb 94 b8 e2 48 b9 2c 13 ba 50 10 02 05 c1 ea -----H---P-----  
0050 00 00 17 03 03 20 18 00 00 00 00 00 00 02 3a -----  
0060 e0 2c 45 cf ce fc 76 54 1c f2 3c 42 a8 a3 02 17 --,E---vT---<B---  
0070 53 28 71 44 f2 3e 4e 3c 0d 6e 63 c9 40 13 20 1b S(qd>Nc-nc@-  
0080 ed 0c 11 fd 0d 30 b0 c6 0e 83 4e 2e 08 a4 d5 26 --0---0---N---&  
0090 98 6a af ee 95 55 38 d7 ed 4c b0 98 2a 0e 2b ca --j---UB---L---\*---  
00a0 21 a8 2a 93 2a 87 ae 20 be 38 be aa 55 75 c8 ab l-\*---8-Uu---  
00b0 b4 f2 16 a5 a7 2d d8 74 fe eb 91 d3 eb eb fd 2c -----t-----  
00c0 04 8d 29 bc e6 5a 04 7b b7 88 23 5a a1 d0 3b d1 --)-Z(-#Z-;  
00d0 94 e0 e0 5e b8 02 5e b7 39 5f 01 55 42 12 fe 08 --^---^---9\_UB---  
00e0 00 d7 ae 1e bf 1f 35 3d 6d 90 57 03 21 6a 31 cc -----5-m-W-lj1-  
00f0 d9 7f 2e 3e 3e 8e 85 b7 c2 16 fa f8 5f 1e fc aa -->--->--->--->---  
0100 de 68 f6 c3 63 c9 5c 73 58 97 e0 c6 e9 93 9d b7 --h-c\>S X-----  
0110 76 b5 7f 0a 89 5e 06 ef 2e 29 24 17 52 60 5a 7b v-----)\$.R'Z{



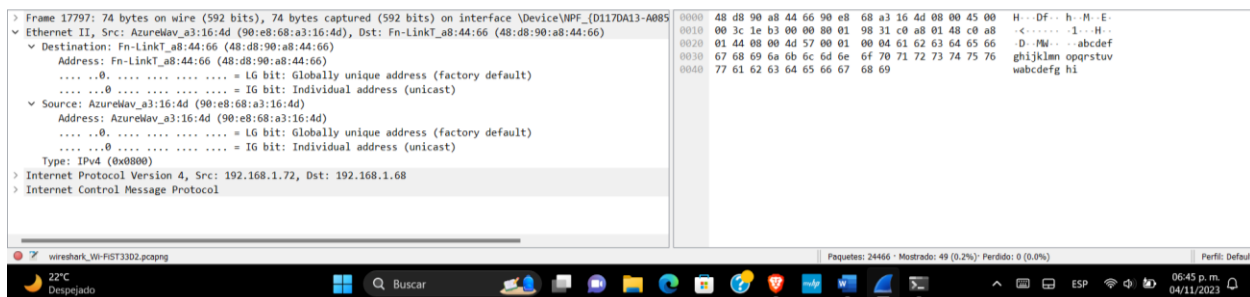
Detenemos la captura de datos y los analizamos.



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](#)