

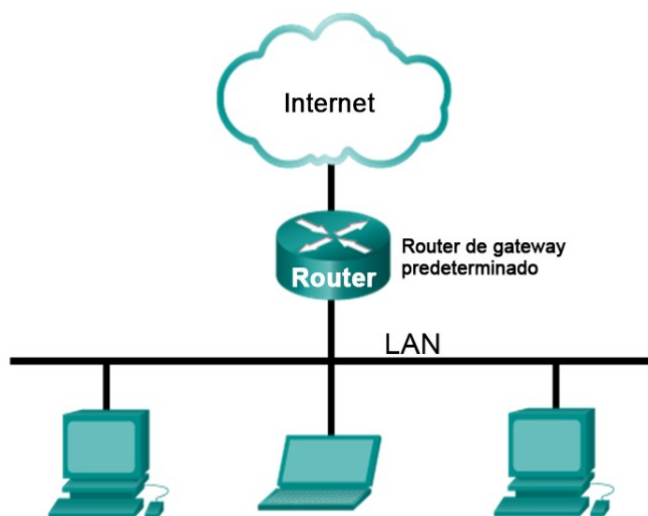
Práctica 2

Ejercicio 1 (2,5 puntos)

Se va a utilizar Wireshark para capturar tramas de Ethernet locales examinando la información incluida en los campos de encabezado de la trama

Se irán indicando los pasos a realizar y la entrega necesaria en alguno de ellos (algunos pasos no necesitan justificante, sino que es la explicación de lo que se tiene que hacer)

La topología de la red es



Nota aclaratoria – Esta primera práctica está suponiendo que puedes hacer ping desde tu equipo al de otro compañero. Si el firewall está activado es probable que no te deje. Tendrás que avisar al profesor para que momentáneamente te desactive el firewall o bien montar un par de equipos conectados en modo NAT (que es lo que se hace en la práctica 4)

Paso 1: Recuperar las direcciones de interfaz de la PC

Deberá recuperar la dirección IP de la PC y la dirección física de la tarjeta de interfaz de red (NIC), que también se conoce como “dirección MAC”.

- Abra una ventana de comandos, escriba `ipconfig /all` y luego presione Entrar.

```

C:\> Seleccionar Símbolo del sistema
Microsoft Windows [Versión 10.0.19043.1706]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\smralumno>ipconfig /all

Configuración IP de Windows

    Nombre de host. . . . . : SMR1-02
    Sufijo DNS principal . . . . . :
    Tipo de nodo. . . . . : híbrido
    Enrutamiento IP habilitado. . . : no
    Proxy WINS habilitado . . . . . : no
    Lista de búsqueda de sufijos DNS: magarinos.local

Adaptador de Ethernet Ethernet 3:

    Sufijo DNS específico para la conexión. . :
    Descripción . . . . . : VirtualBox Host-Only Ethernet Adapter
    Dirección física. . . . . : 0A-00-27-00-00-06
    DHCP habilitado . . . . . : no
    Configuración automática habilitada . . . : sí
    Vínculo: dirección IPv6 local. . . : fe80::708c:9620:52e7:d64%6(Preferido)
    Dirección IPv4. . . . . : 192.168.56.1(Preferido)
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :
    IAID DHCPv6 . . . . . : 436863015
    DUID de cliente DHCPv6. . . . . : 00-01-00-01-28-D0-E6-34-3C-52-82-64-5C-3B
    Servidores DNS. . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . : magarinos.local
    Descripción . . . . . : Intel(R) Ethernet Connection (5) I219-LM
    Dirección física. . . . . : 3C-52-82-64-5C-3B
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí
    Vínculo: dirección IPv6 local. . . : fe80::353b:d1ba:cc3:8e0c%8(Preferido)
    Dirección IPv4. . . . . : 192.168.3.2(Preferido)
    Máscara de subred . . . . . : 255.255.255.0
    Concesión obtenida. . . . . : lunes, 23 de mayo de 2022 8:46:31
    La concesión expira . . . . . : lunes, 23 de mayo de 2022 9:06:31
    Puerta de enlace predeterminada . . . . . : 192.168.3.250
    Servidor DHCP . . . . . : 192.168.3.250
    IAID DHCPv6 . . . . . : 591155842
    DUID de cliente DHCPv6. . . . . : 00-01-00-01-28-D0-E6-34-3C-52-82-64-5C-3B
    Servidores DNS. . . . . : 192.168.6.201
    NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de LAN inalámbrica Conexión de área local* 9:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
    Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
    Dirección física. . . . . : F8-59-71-EA-07-AF
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Conexión de área local* 10:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
    Descripción . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
    Dirección física. . . . . : FA-59-71-EA-07-AE
    DHCP habilitado . . . . . : no
    Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Wi-Fi 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
    Descripción . . . . . : Intel(R) Dual Band Wireless-AC 8265
    Dirección física. . . . . : F8-59-71-EA-07-AE
    DHCP habilitado . . . . . : sí
    Configuración automática habilitada . . . : sí

C:\Users\smralumno>

```

- b) Observe la dirección IP y la dirección MAC (física) de la interfaz de la PC. ¿Cuáles son?

```

Adaptador de Ethernet Ethernet 2:

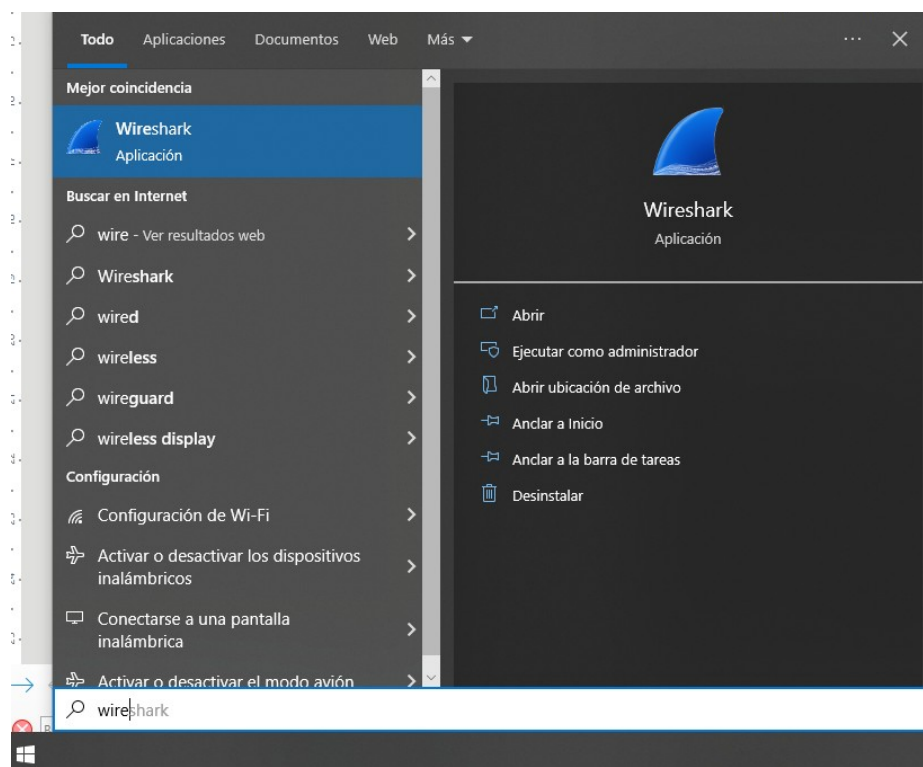
Sufijo DNS específico para la conexión. . . : magarinos.local
Descripción . . . . . : Intel(R) Ethernet Connection (5) I219-LM
Dirección física. . . . . : 3C-52-82-64-5C-3B
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::353b:d1ba:cc3:8e0c%8(Preferido)
Dirección IPv4. . . . . : 192.168.3.2(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : lunes, 23 de mayo de 2022 8:46:31
La concesión expira . . . . . : lunes, 23 de mayo de 2022 9:06:31
Puerta de enlace predeterminada . . . . . : 192.168.3.250
Servidor DHCP . . . . . : 192.168.3.250
IAID DHCPv6 . . . . . : 591155842
DUID de cliente DHCPv6. . . . . : 00-01-00-01-28-D0-E6-34-3C-52-82-64-5C-3B
Servidores DNS. . . . . : 192.168.6.201
NetBIOS sobre TCP/IP. . . . . : habilitado
  
```

Ipv4:192.168.3.2 Mac:3C-52-82-64-5C-3B

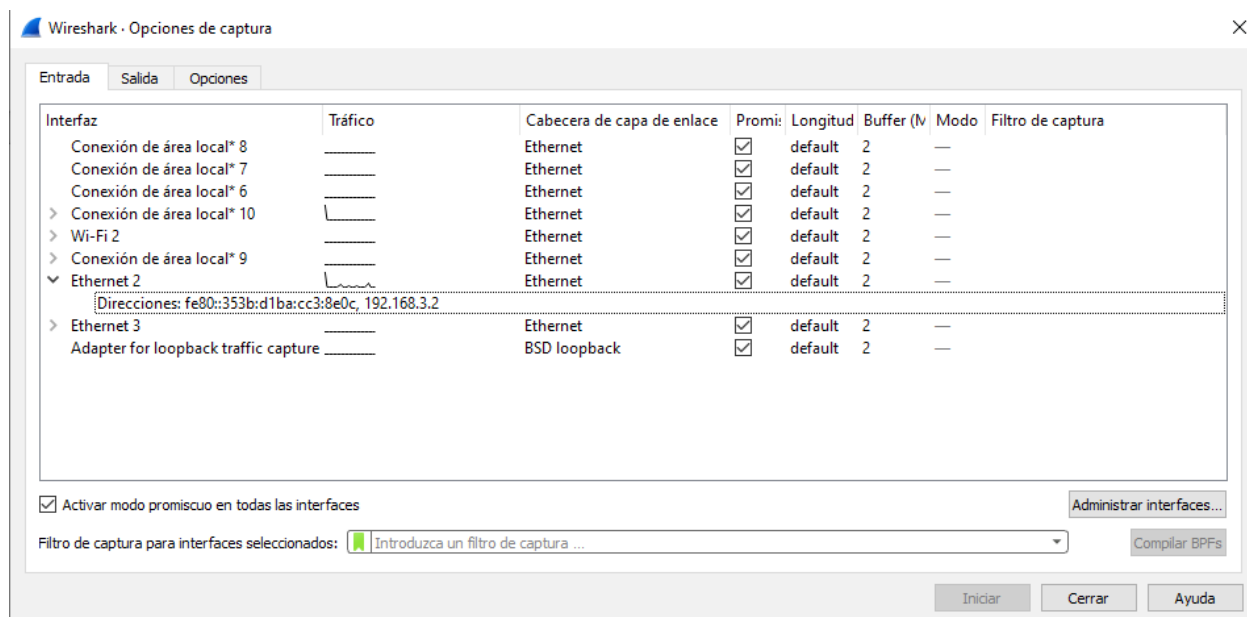
- c) Solicite a un miembro del equipo la dirección IP de su PC y proporciónese la suya. En esta instancia, no proporcione su dirección MAC.
192.168.3.4

Paso 2: Iniciar Wireshark y comenzar a capturar datos

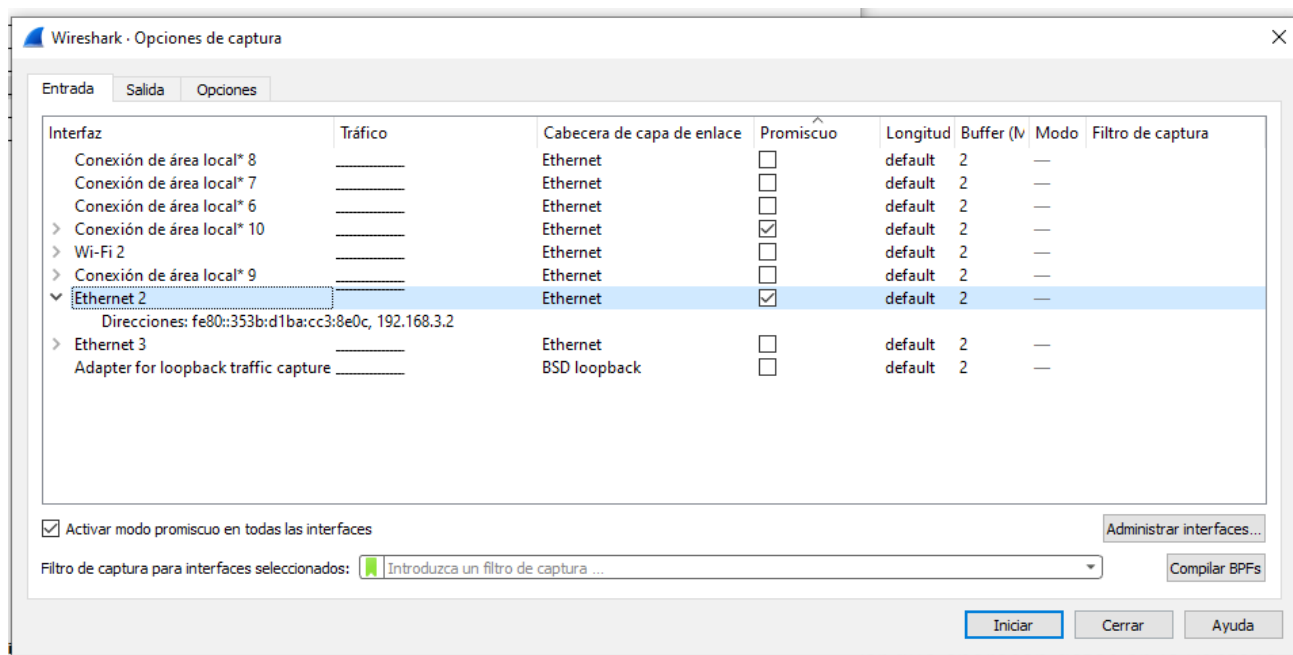
- a) En la PC, haga clic en el botón Inicio de Windows para ver Wireshark como uno de los programas en el menú emergente. Haga doble clic en Wireshark.

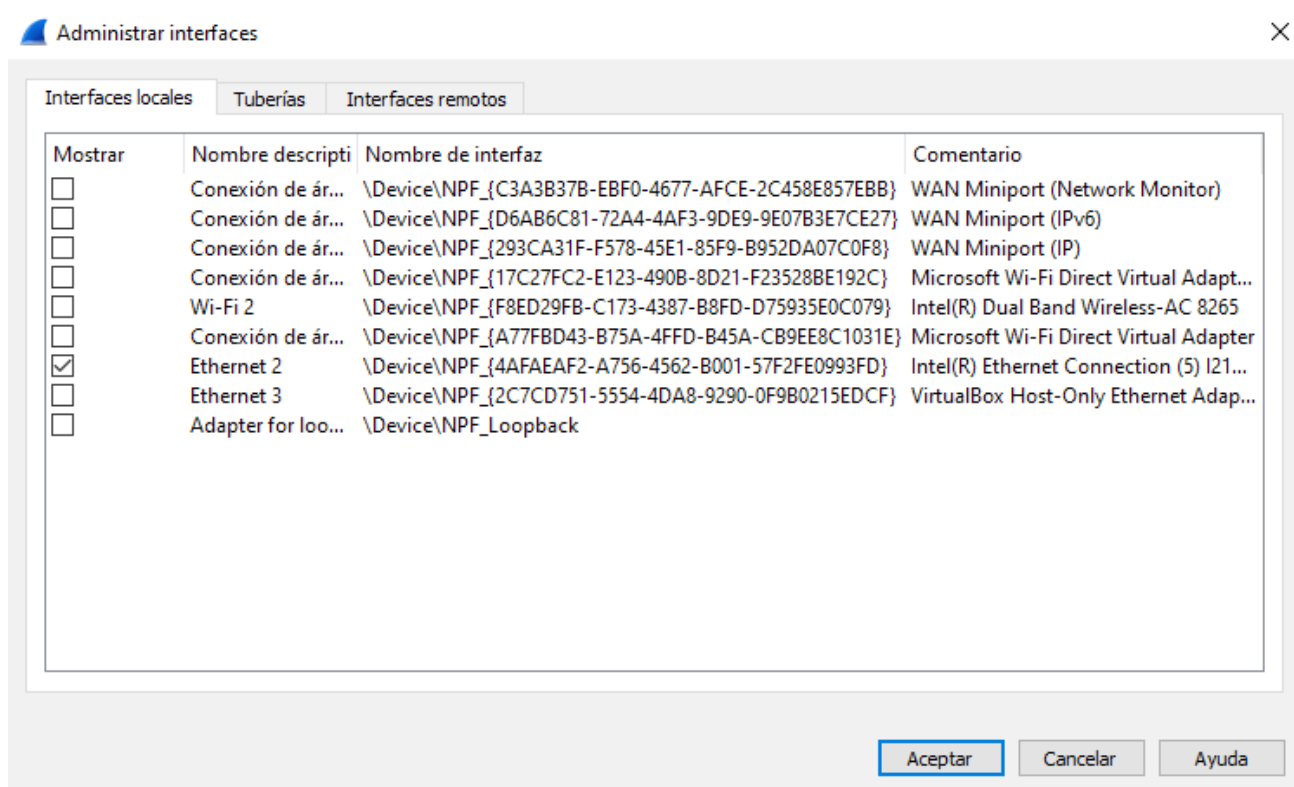


b) Una vez que se inicia Wireshark, haga clic en Interface List (Lista de interfaces).



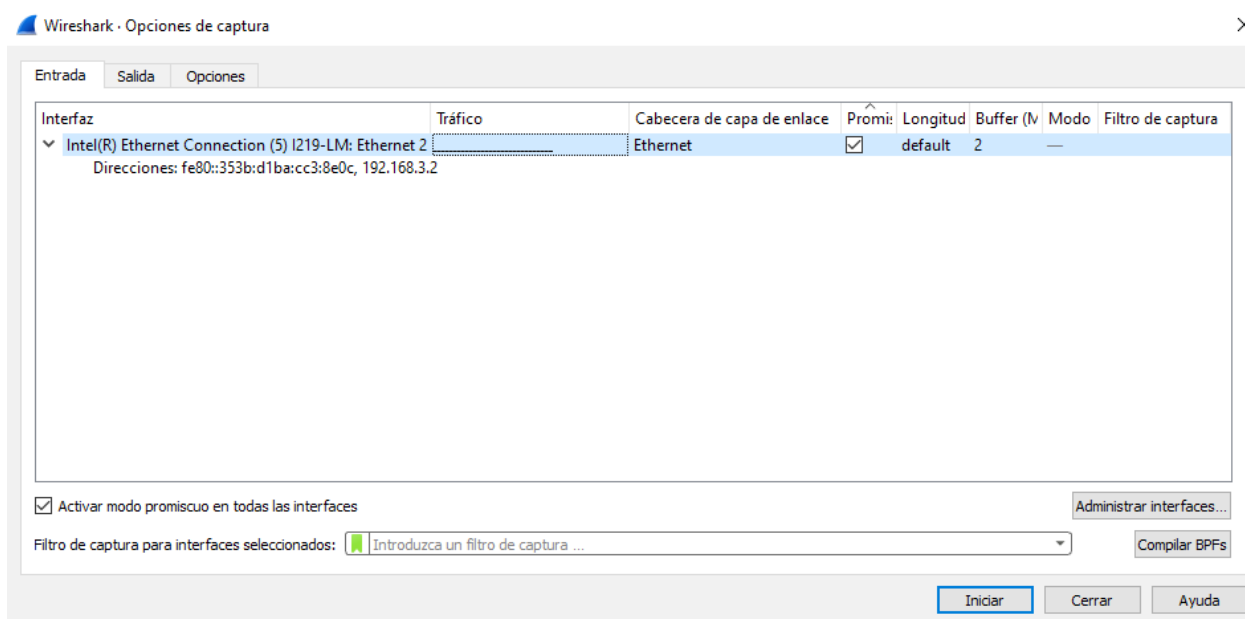
c) En la ventana Wireshark: Capture Interfaces (Wireshark: capturar interfaces), haga clic en la casilla de verificación junto a la interfaz conectada a la LAN.





Nota: si se indican varias interfaces, y no está seguro de cuál activar, haga clic en el botón Details (Detalles) y, a continuación, haga clic en la ficha 802.3 (Ethernet). Verifique que la dirección MAC coincida con lo que observó en el paso 1b. Después de verificar la interfaz correcta, cierre la ventana Interface Details (Detalles de la interfaz).

- d) Después de activar la interfaz correcta, haga clic en Start (Comenzar) para comenzar la captura de datos



La información comienza a desplazar hacia abajo la sección superior de Wireshark. Las líneas de datos aparecen en diferentes colores según el protocolo.

Mostrar captura de pantalla

Capturing from Intel(R) Ethernet Connection (5) I219-LM: Ethernet 2

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	HewlettP_5f:85:6f	Broadcast	ARP	60	Who has 192.168.60.1? Tell 192.168.60.9
2	0.092918	192.168.3.14	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
3	0.996130	HewlettP_5f:85:74	Spanning-tree-(for-...	STP	60	RST. Root = 32768/0/d8:94:03:5f:85:6f Cost = 0 Port = 0x8004
4	1.108325	192.168.3.14	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5	1.882801	192.168.3.12	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
6	2.660726	192.168.3.8	192.168.3.255	NBNS	92	Name query NB SMR1-08<1c>
7	2.732122	192.168.3.4	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1

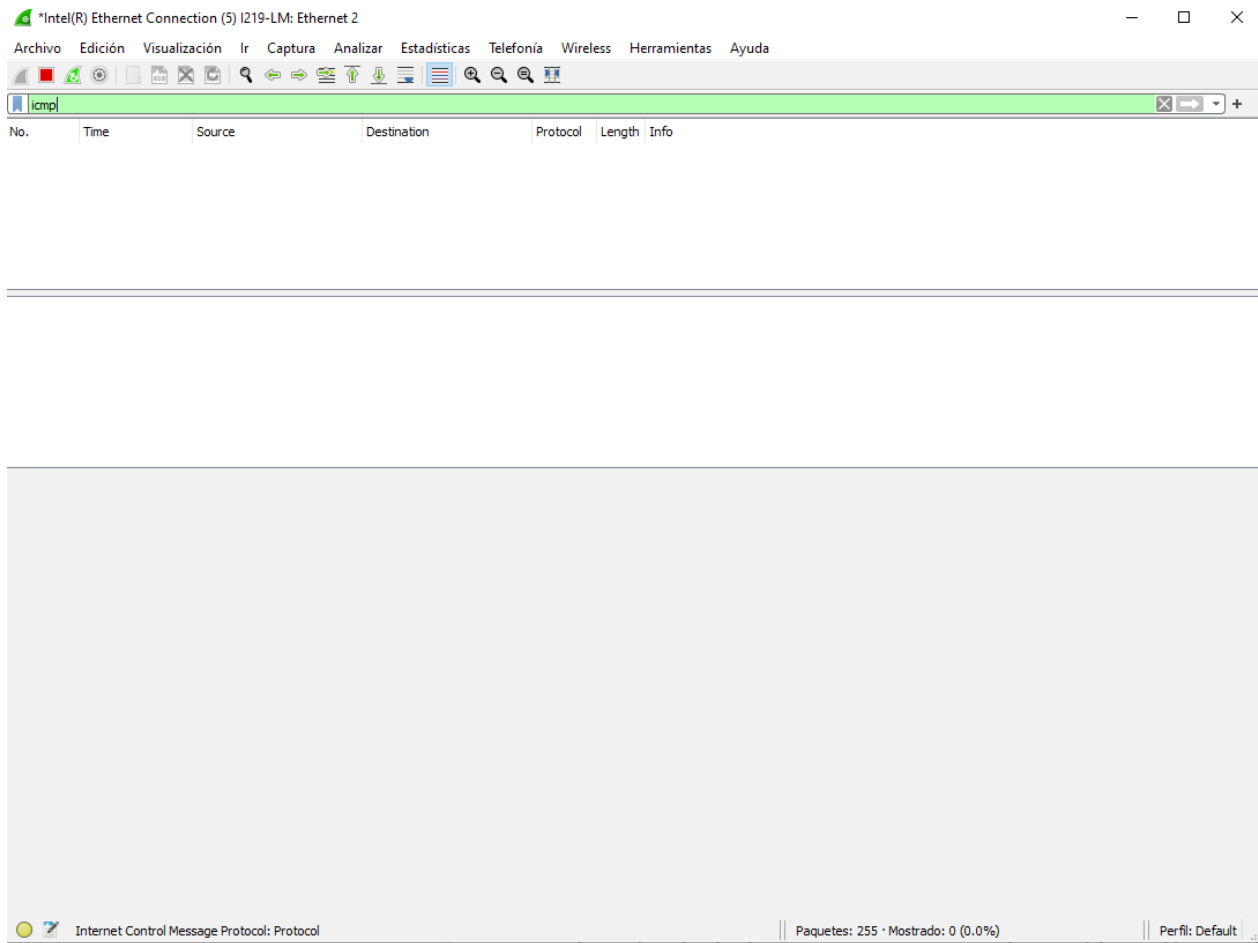
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{4AFAEAF2-A756-4562-B001-57F2FE0993FD}, id 0
 > Ethernet II, Src: HewlettP_5f:85:6f (d8:94:03:5f:85:6f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 > Address Resolution Protocol (request)

```

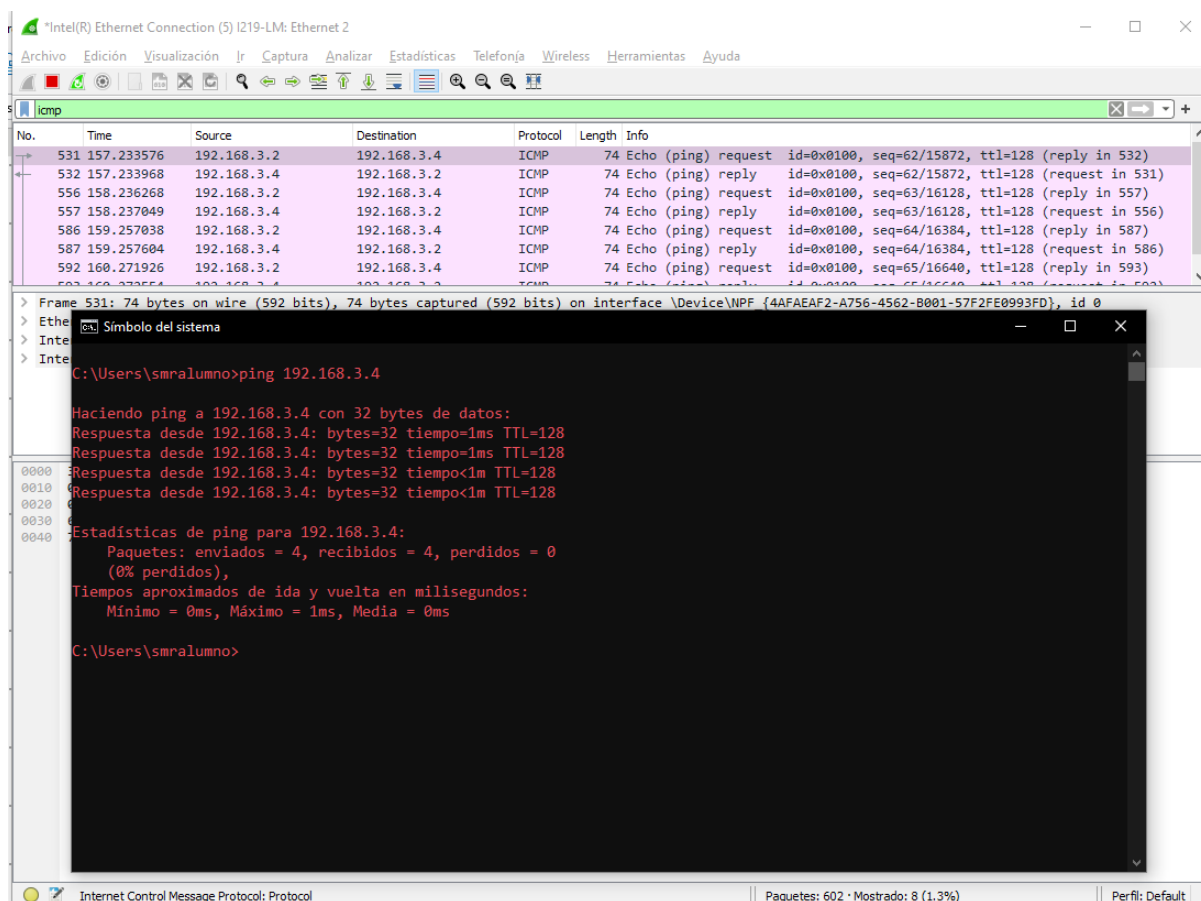
0000  ff ff ff ff ff ff d8 94 03 5f 85 6f 08 06 00 01  .....  .o....
0010  08 00 06 04 00 01 d8 94 03 5f 85 6f c0 a8 3c 09  .....  .o...<
0020  00 00 00 00 00 00 c0 a8 3c 01 00 00 00 00 00 00  .....  <.....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....  ....
  
```

Intel(R) Ethernet Connection (5) I219-LM: Ethernet 2: <live capture in progress> | Paquetes: 69 · Mostrado: 69 (100.0%) | Perfil: Default

- e) Es posible desplazarse muy rápidamente por esta información según la comunicación que tiene lugar entre la PC y la LAN. Se puede aplicar un filtro para facilitar la vista y el trabajo con los datos que captura Wireshark. Para esta práctica de laboratorio, solo nos interesa mostrar las PDU de ICMP (ping). Escriba icmp en el cuadro Filter (Filtro) que se encuentra en la parte superior de Wireshark y presione Entrar o haga clic en el botón Apply (Aplicar) para ver solamente PDU de ICMP (ping).



- f) Este filtro hace que desaparezcan todos los datos de la ventana superior, pero se sigue capturando el tráfico en la interfaz. Abra la ventana del símbolo del sistema que abrió antes y haga ping a la dirección IP que recibió del miembro del equipo. Comenzará a ver que aparecen datos en la ventana superior de Wireshark nuevamente



Nota: si la PC del miembro del equipo no responde a sus pings, es posible que se deba a que el firewall de la PC está bloqueando estas solicitudes. Consulte Apéndice: Permitir el tráfico ICMP a través de un firewall para obtener información sobre cómo permitir el tráfico ICMP a través del firewall

Mostrar captura de pantalla

- g) Detenga la captura de datos haciendo clic en el ícono Stop Capture (Detener captura)

Intel(R) Ethernet Connection (5) I219-LM: Ethernet 2

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Detiene captura de paquetes

No.	Time	Source	Destination	Protocol	Length	Info
531	157.233576	192.168.3.2	192.168.3.4	ICMP	74	Echo (ping) request id=0x0100, seq=62/15872, ttl=128 (reply in 532)
532	157.233968	192.168.3.4	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=62/15872, ttl=128 (request in 531)
556	158.236268	192.168.3.2	192.168.3.4	ICMP	74	Echo (ping) request id=0x0100, seq=63/16128, ttl=128 (reply in 557)
557	158.237049	192.168.3.4	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=63/16128, ttl=128 (request in 556)
586	159.257038	192.168.3.2	192.168.3.4	ICMP	74	Echo (ping) request id=0x0100, seq=64/16384, ttl=128 (reply in 587)
587	159.257604	192.168.3.4	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=64/16384, ttl=128 (request in 586)
592	160.271926	192.168.3.2	192.168.3.4	ICMP	74	Echo (ping) request id=0x0100, seq=65/16640, ttl=128 (reply in 593)

> Frame 531: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4AFAEAF2-A756-4562-B001-57F2FE0993FD}, id 0

> Ethernet II, Src: HewlettP_64:5c:3b (3c:52:82:64:5c:3b), Dst: HewlettP_58:ba:59 (3c:52:82:58:ba:59)

> Internet Protocol Version 4, Src: 192.168.3.2, Dst: 192.168.3.4

> Internet Control Message Protocol

```

0000  3c 52 82 58 ba 59 3c 52 82 64 5c 3b 08 00 45 00  <R·X·Y<R·d\;··E·
0010  00 3c b0 fd 00 00 01 00 00 c0 a8 03 02 c0 a8  ·<·.....
0020  03 04 08 00 4c 1e 01 00 00 3e 61 62 63 64 65 66  ····L···->abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69  wabcdefg hi
  
```

Internet Control Message Protocol: Protocol

Paquetes: 712 · Mostrado: 8 (1.1%)

Perfil: Default

Paso 3: Examinar los datos capturados

Examine los datos que se generaron mediante las solicitudes de ping de la PC del miembro del equipo. Los datos de Wireshark se muestran en tres secciones: 1) la sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IP enumerada, 2) la sección media indica información de la PDU para la trama seleccionada en la parte superior de la pantalla y separa una trama de PDU capturada por las capas de protocolo, y 3) la sección inferior muestra los datos sin procesar de cada capa. Los datos sin procesar se muestran en formatos hexadecimal y decimal.

- Haga clic en las primeras tramas de PDU de la solicitud de ICMP en la sección superior de Wireshark. Observe que la columna Source (Origen) contiene la dirección IP de su PC y la columna Destination (Destino) contiene la dirección IP de la PC del compañero de equipo a la que hizo ping. Mostrar dicha captura marcando la IP de su compañero

Intel(R) Ethernet Connection (5) I219-LM: Ethernet 2

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
531	157.233576	192.168.3.2	192.168.3.4	ICMP	74	Echo (ping) request id=0x0100, seq=62/15872, ttl=128 (reply in 532)
532	157.233968	192.168.3.4	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=62/15872, ttl=128 (request in 531)
556	158.236268	192.168.3.2	192.168.3.4	ICMP	74	Echo (ping) request id=0x0100, seq=63/16128, ttl=128 (reply in 557)
557	158.237049	192.168.3.4	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=63/16128, ttl=128 (request in 556)
586	159.257038	192.168.3.2	192.168.3.4	ICMP	74	Echo (ping) request id=0x0100, seq=64/16384, ttl=128 (reply in 587)
587	159.257604	192.168.3.4	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=64/16384, ttl=128 (request in 586)
592	160.271926	192.168.3.2	192.168.3.4	ICMP	74	Echo (ping) request id=0x0100, seq=65/16640, ttl=128 (reply in 593)
593	160.272554	192.168.3.4	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=65/16640, ttl=128 (request in 592)

... 0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: ICMP (1)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.3.2
Destination Address: 192.168.3.4

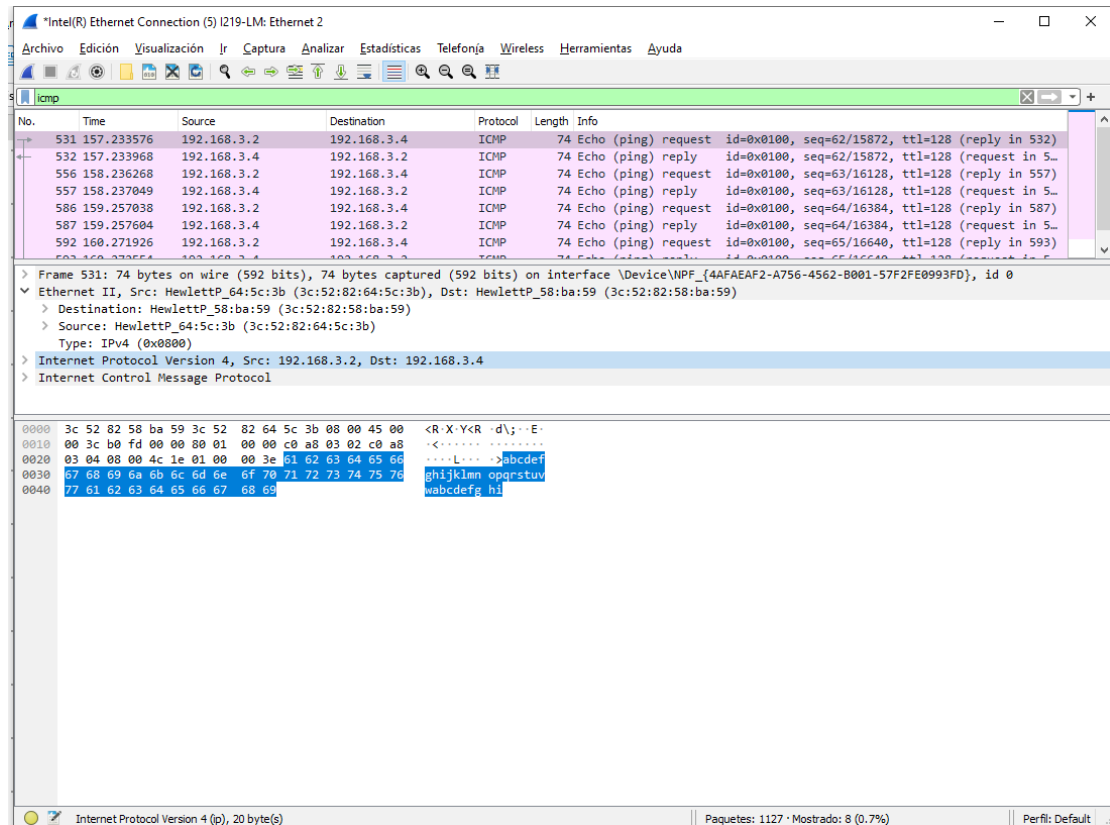
Internet Control Message Protocol

```

0000  3c 52 82 58 ba 59 3c 52 82 64 5c 3b 08 00 45 00  <R-X-Y<R-d\;-E-
0010  00 3c b0 fd 00 00 80 01 00 00 c0 a8 03 02 c0 a8  <-----
0020  03 04 08 00 4c 1e 01 00 00 3e 61 62 63 64 65 66  ...L...>abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```

Destination Address (ip.dst), 4 byte(s) | Paquetes: 1127 · Mostrado: 8 (0.7%) | Perfil: Default

- b) Con esta trama de PDU aún seleccionada en la sección superior, navegue hasta la sección media. Haga clic en el signo más que está a la izquierda de la fila de Ethernet II para ver las direcciones MAC de origen y destino.
- ¿Cuáles son? Origen: 3c:52:82:64:5c:3b Dest: 3c:52:82:58:ba:59
 - ¿La dirección MAC de origen coincide con la interfaz de su PC? Si c:52:82:64:5c:3b
 - ¿La dirección MAC de destino en Wireshark coincide con la dirección MAC del miembro del equipo? Si 3c:52:82:58:ba:59



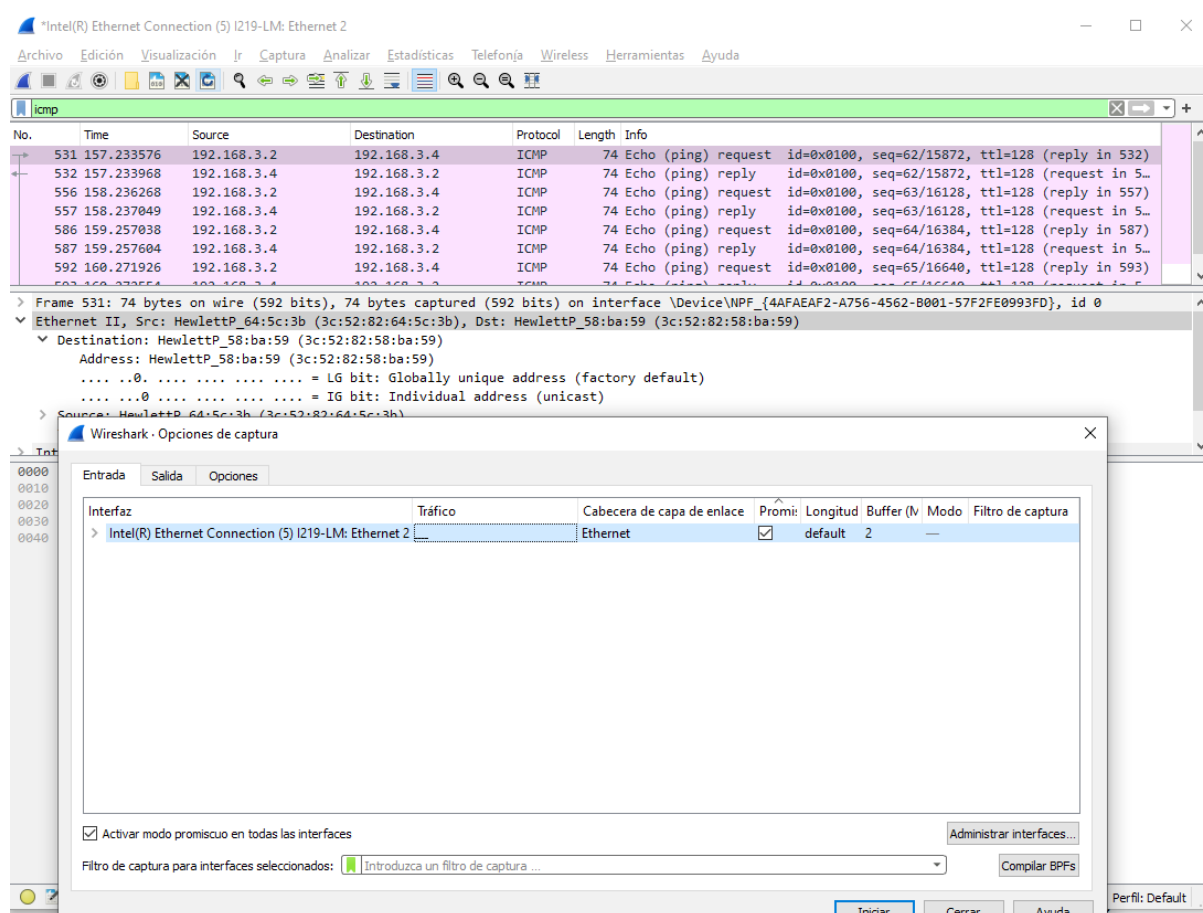
Ejercicio 2 (2,5 puntos)

Se va a utilizar Wireshark para capturar tramas de Ethernet remotas examinando la información incluida en los campos de encabezado de la trama

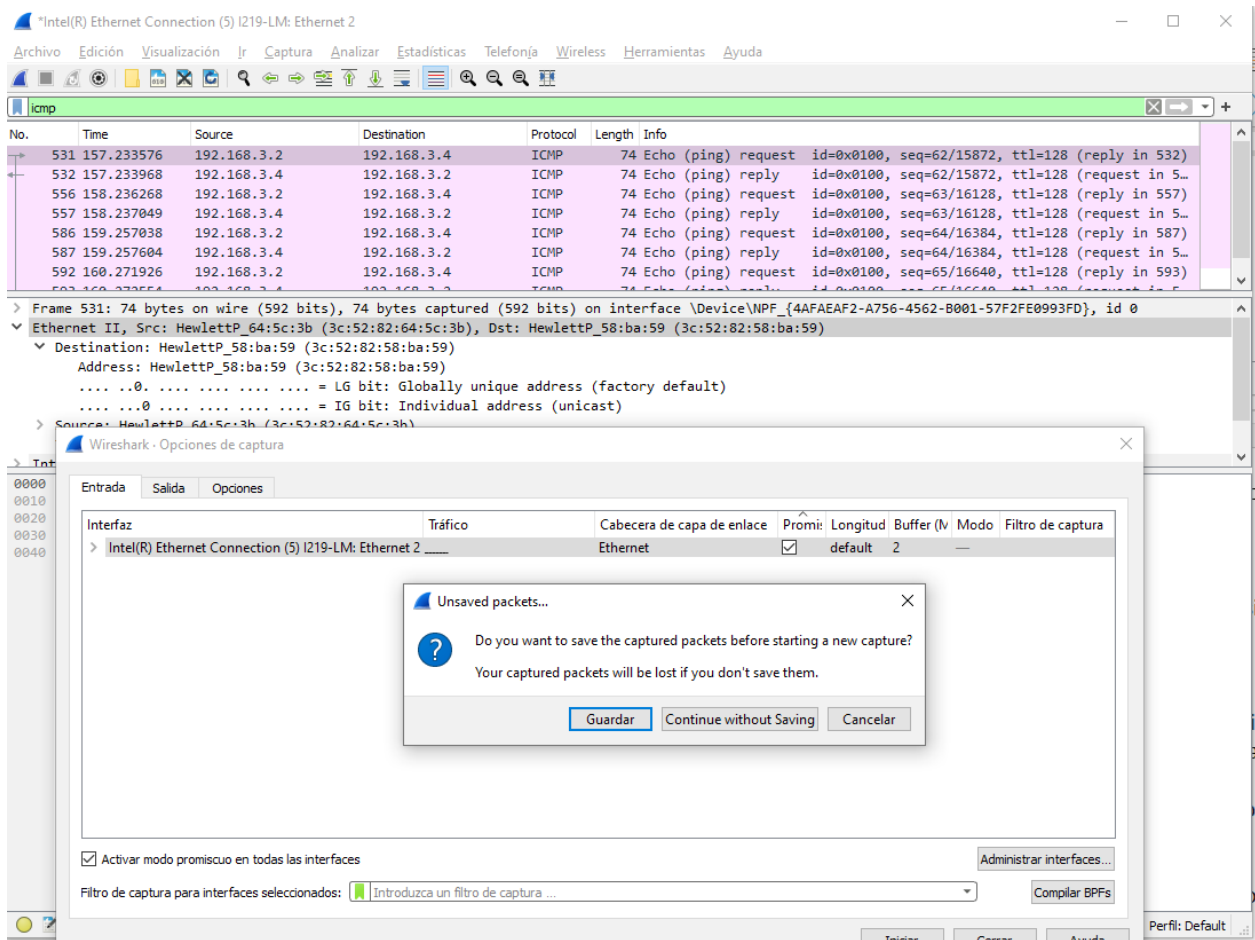
Se irán indicando los pasos a realizar y la entrega necesaria en alguno de ellos (algunos pasos no necesitan justificante, sino que es la explicación de lo que se tiene que hacer)

Paso 1: Comenzar a capturar datos en la interfaz

- Haga clic en el ícono Interface List (Lista de interfaces) para volver a abrir la lista de interfaces de la PC
- Asegúrese de que la casilla de verificación junto a la interfaz LAN esté activada y, a continuación, haga clic en Start (Comenzar).



- c) Se abre una ventana que le solicita guardar los datos capturados anteriormente antes de comenzar otra captura. No es necesario guardar esos datos. Haga clic en Continue without Saving (Continuar sin guardar).



- d) Con la captura activa, haga ping a los URL de los dos sitios Web siguientes:
- www.yahoo.com
 - www.google.com

Nota: al hacer ping a los URL que se indican, observe que el servidor de nombres de dominio (DNS) traduce el URL a una dirección IP. Observe la dirección IP recibida para cada URL.

Capturing from Intel(R) Ethernet Connection (5) I219-LM: Ethernet 2

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
598	33.290078	192.168.3.2	87.248.100.215	ICMP	74	Echo (ping) request id=0x0100, seq=66/16896, ttl=128 (reply in 602)
602	33.363753	87.248.100.215	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=66/16896, ttl=41 (request in 598)
608	34.296326	192.168.3.2	87.248.100.215	ICMP	74	Echo (ping) request id=0x0100, seq=67/17152, ttl=128 (reply in 610)
610	34.368975	87.248.100.215	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=67/17152, ttl=41 (request in 608)
614	35.309012	192.168.3.2	87.248.100.215	ICMP	74	Echo (ping) request id=0x0100, seq=68/17408, ttl=128 (reply in 616)
616	35.381646	87.248.100.215	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=68/17408, ttl=41 (request in 614)
617	36.325184	192.168.3.2	87.248.100.215	ICMP	74	Echo (ping) request id=0x0100, seq=69/17664, ttl=128 (reply in 619)

> Frame 598: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4AFAEAF2-A756-4562-B001-57F2FE0993FD}, id 0

Ethernet II, Src: HewlettP 64:5c:3b (3c:52:82:64:5c:3b), Dst: Routerbo c4:7c:b4 (2c:c8:1b:c4:7c:b4)

Símbolo del sistema

```
Microsoft Windows [Versión 10.0.19043.1706]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\smralumno>ping www.yahoo.com

Haciendo ping a new-fp-shed.wg1.b.yahoo.com [87.248.100.215] con 32 bytes de datos:
Resposta desde 87.248.100.215: bytes=32 tiempo=73ms TTL=41
Resposta desde 87.248.100.215: bytes=32 tiempo=72ms TTL=41
Resposta desde 87.248.100.215: bytes=32 tiempo=72ms TTL=41
Resposta desde 87.248.100.215: bytes=32 tiempo=72ms TTL=41

Estadísticas de ping para 87.248.100.215:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 72ms, Máximo = 73ms, Media = 72ms

C:\Users\smralumno>
```

Ethernet (eth), 14 byte(s) Paquetes: 650 · Mostrado: 8 (1.2%) Perfil: Default

e) Puede detener la captura de datos haciendo clic en el ícono Stop Capture (Detener captura).

Capturing from Intel(R) Ethernet Connection (5) I219-LM: Ethernet 2

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
617	36.325184	192.168.3.2	87.248.100.215	ICMP	74	Echo (ping) request id=0x0100, seq=69/17664, ttl=128 (reply in 619)
619	36.397704	87.248.100.215	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=69/17664, ttl=41 (request in 617)
1694	106.539909	192.168.3.2	172.217.168.164	ICMP	74	Echo (ping) request id=0x0100, seq=70/17920, ttl=128 (reply in 1695)
1695	106.566472	172.217.168.164	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=70/17920, ttl=108 (request in 1694)
1707	107.555733	192.168.3.2	172.217.168.164	ICMP	74	Echo (ping) request id=0x0100, seq=71/18176, ttl=128 (reply in 1709)
1709	107.582022	172.217.168.164	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=71/18176, ttl=108 (request in 1707)
1735	108.572367	192.168.3.2	172.217.168.164	ICMP	74	Echo (ping) request id=0x0100, seq=72/18432, ttl=128 (reply in 1736)

> Frame 1694: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4AFAEAF2-A756-4562-B001-57F2FE0993FD}, id 0

Ethernet II, Src: HewlettP 64:5c:3b (3c:52:82:64:5c:3b), Dst: Routerbo c4:7c:b4 (2c:c8:1b:c4:7c:b4)

Símbolo del sistema

```
Microsoft Windows [Versión 10.0.19043.1706]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\smralumno>ping www.yahoo.com

Haciendo ping a new-fp-shed.wg1.b.yahoo.com [87.248.100.215] con 32 bytes de datos:
Resposta desde 87.248.100.215: bytes=32 tiempo=73ms TTL=41
Resposta desde 87.248.100.215: bytes=32 tiempo=72ms TTL=41
Resposta desde 87.248.100.215: bytes=32 tiempo=72ms TTL=41
Resposta desde 87.248.100.215: bytes=32 tiempo=72ms TTL=41

Estadísticas de ping para 87.248.100.215:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 72ms, Máximo = 73ms, Media = 72ms

C:\Users\smralumno>ping www.google.com

Haciendo ping a www.google.com [172.217.168.164] con 32 bytes de datos:
Resposta desde 172.217.168.164: bytes=32 tiempo=26ms TTL=108
Resposta desde 172.217.168.164: bytes=32 tiempo=26ms TTL=108
Resposta desde 172.217.168.164: bytes=32 tiempo=26ms TTL=108
Resposta desde 172.217.168.164: bytes=32 tiempo=26ms TTL=108

Estadísticas de ping para 172.217.168.164:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 26ms, Máximo = 26ms, Media = 26ms

C:\Users\smralumno>
```

Ethernet (eth), 14 byte(s) Paquetes: 2015 · Mostrado: 16 (0.8%) Perfil: Default

Paso 2: Inspeccionar y analizar los datos de los hosts remotos

- a) Revise los datos capturados en Wireshark y examine las direcciones IP y MAC de las dos ubicaciones a las que hizo ping.

Indique las direcciones IP y MAC de destino para las dos ubicaciones

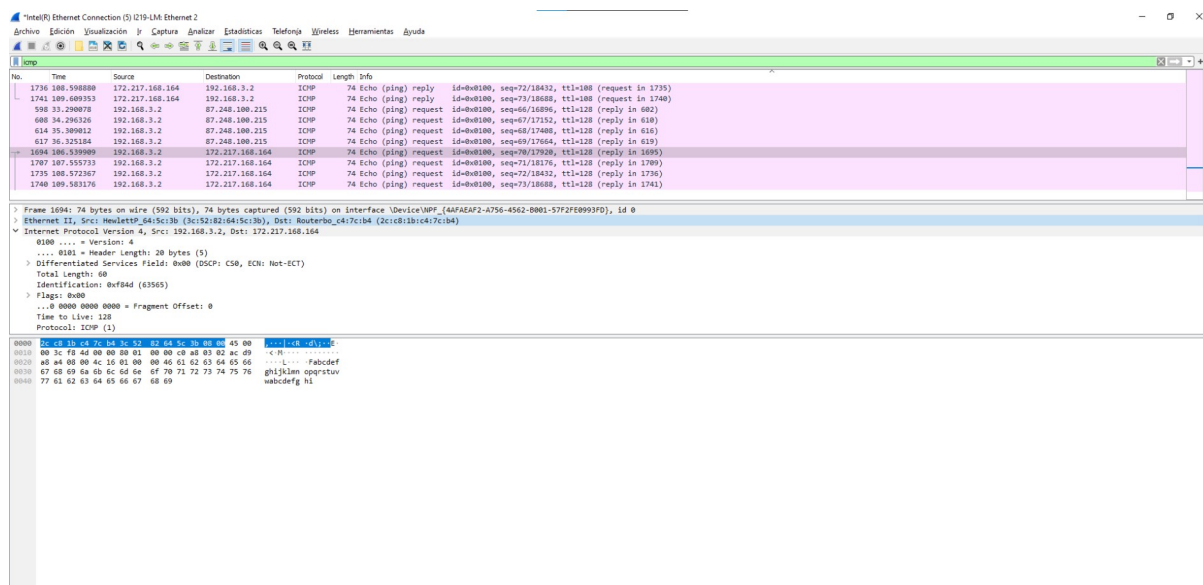
The screenshot shows a Wireshark capture on the 'icmp' filter. The packet list displays several ICMP Echo (ping) requests and replies. The first request is from 192.168.3.2 to 87.248.100.215. The packet details pane shows the Ethernet II frame with source MAC 3c:52:82:64:5c:3b and destination MAC 2c:c8:1b:c4:7c:b4. The Internet Protocol Version 4 section shows the source IP 192.168.3.2 and destination IP 87.248.100.215. The packet bytes pane shows the raw data of the ICMP echo request.

Mac:

Orig: 3c:52:82:64:5c:3b Dst: 2c:c8:1b:c4:7c:b4

The screenshot shows the details pane of a Wireshark capture. The selected packet is an ICMP Echo (ping) request. The packet details pane shows the Ethernet II frame with source MAC 3c:52:82:64:5c:3b and destination MAC 2c:c8:1b:c4:7c:b4. The Internet Protocol Version 4 section shows the source IP 192.168.3.2 and destination IP 87.248.100.215. The packet bytes pane shows the raw data of the ICMP echo request.

Org: 192.168.3.2 Dst: 87.248.100.215



Mac:

Org: 3c:52:82:64:5c:3b Dst: 2c:c8:1b:c4:7c:b4

Ip:

Org: 192.168.3.2 Dst: 172.217.168.164

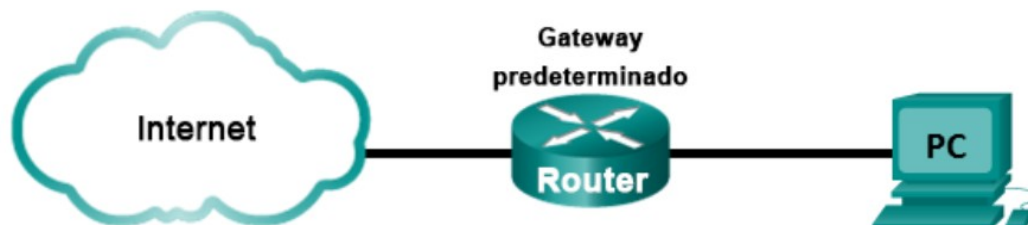
¿Por qué Wireshark muestra la dirección MAC vigente de los hosts locales, pero no la dirección MAC vigente de los hosts remotos? **Solo aparecen las mac de los routers, por que el firewall esconde las mac por motivos de seguridad**

Ejercicio 3 (2,5 puntos)

Se va a utilizar Wireshark para capturar tramas de Ethernet locales y remotas examinando la información incluida en los campos de encabezado de la trama

Se irán indicando los pasos a realizar y la entrega necesaria en alguno de ellos (algunos pasos no necesitan justificante, sino que es la explicación de lo que se tiene que hacer)

La topología de la red es



Paso 1: Determinar la dirección IP del gateway predeterminado en la PC

Abra una ventana del símbolo del sistema y emita el comando ipconfig. ¿Cuál es la dirección IP del gateway predeterminado de la PC?

```

Símbolo del sistema

Configuración IP de Windows

Adaptador de Ethernet Ethernet 3:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::708c:9620:52e7:d64%6
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . :

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . . : magarinos.local
    Vínculo: dirección IPv6 local. . . : fe80::353b:d4ba:cc2:8a0-%8
    Dirección IPv4. . . . . : 192.168.3.2
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 192.168.3.250
  
```

Paso 2: Iniciar la captura de tráfico en la NIC de la PC

- Abra Wireshark.
- En la barra de herramientas de Wireshark Network Analyzer, haga clic en el ícono Interface List (Lista de interfaces)
- En la ventana Wireshark: Capture Interfaces (Wireshark: capturar interfaces), seleccione la interfaz para iniciar la captura de tráfico haciendo clic en la casilla de verificación apropiada, y luego haga clic en Start (Comenzar). Si no está seguro de qué interfaz activar, haga clic en Details (Detalles) para obtener más información sobre cada interfaz enumerada
- Observe el tráfico que aparece en la ventana Packet List (Lista de paquetes). Mostrar una captura de pantalla

Wireshark Network Analyzer interface showing a packet capture on the Intel(R) Ethernet Connection (3) I219-LM Ethernet 2 interface. The packet list shows several QUIC packets, and the packet details pane shows the structure of a QUIC packet.

No.	Time	Source	Destination	Protocol	Length	Info
28	5.057795	216.58.215.138	192.168.3.2	QUIC	67	Protected Payload (KPB), DCID=16cc355faf5a467e
29	5.057813	192.168.3.2	216.58.215.138	QUIC	76	Protected Payload (KPB), DCID=16cc355faf5a467e
30	5.057969	216.58.215.138	192.168.3.2	QUIC	67	Protected Payload (KPB), DCID=16cc355faf5a467e
31	5.063516	192.168.3.2	216.58.215.138	QUIC	76	Protected Payload (KPB), DCID=16cc355faf5a467e
32	5.108558	216.58.215.138	192.168.3.2	QUIC	1288	Protected Payload (KPB), DCID=16cc355faf5a467e
33	5.108558	216.58.215.138	192.168.3.2	QUIC	302	Protected Payload (KPB), DCID=16cc355faf5a467e
34	5.108558	216.58.215.138	192.168.3.2	QUIC	272	Protected Payload (KPB), DCID=16cc355faf5a467e
35	5.112274	192.168.3.2	216.58.215.138	QUIC	80	Protected Payload (KPB), DCID=16cc355faf5a467e
36	5.112971	192.168.3.2	216.58.215.138	QUIC	75	Protected Payload (KPB), DCID=16cc355faf5a467e
37	5.139408	216.58.215.138	192.168.3.2	QUIC	67	Protected Payload (KPB), DCID=16cc355faf5a467e

Frame 1: 68 bytes on wire (480 bits), 68 bytes captured (480 bits) on interface \Device\NPF_{44FAEAF2-A756-4562-B801-57F2FE8993FD}, id 0

Ethernet II, Src: Intel(R) Ethernet Connection (3) I219-LM Ethernet 2, Dst: 08:00:27:00:00:00

Logical-Link Control

Spanning Tree Protocol

0000 01 00 c2 00 00 00 00 04 03 5f 85 74 00 27 42 42t'08

0010 03 00 00 02 02 2c 00 00 08 94 03 5f 85 6f 00 00t'00

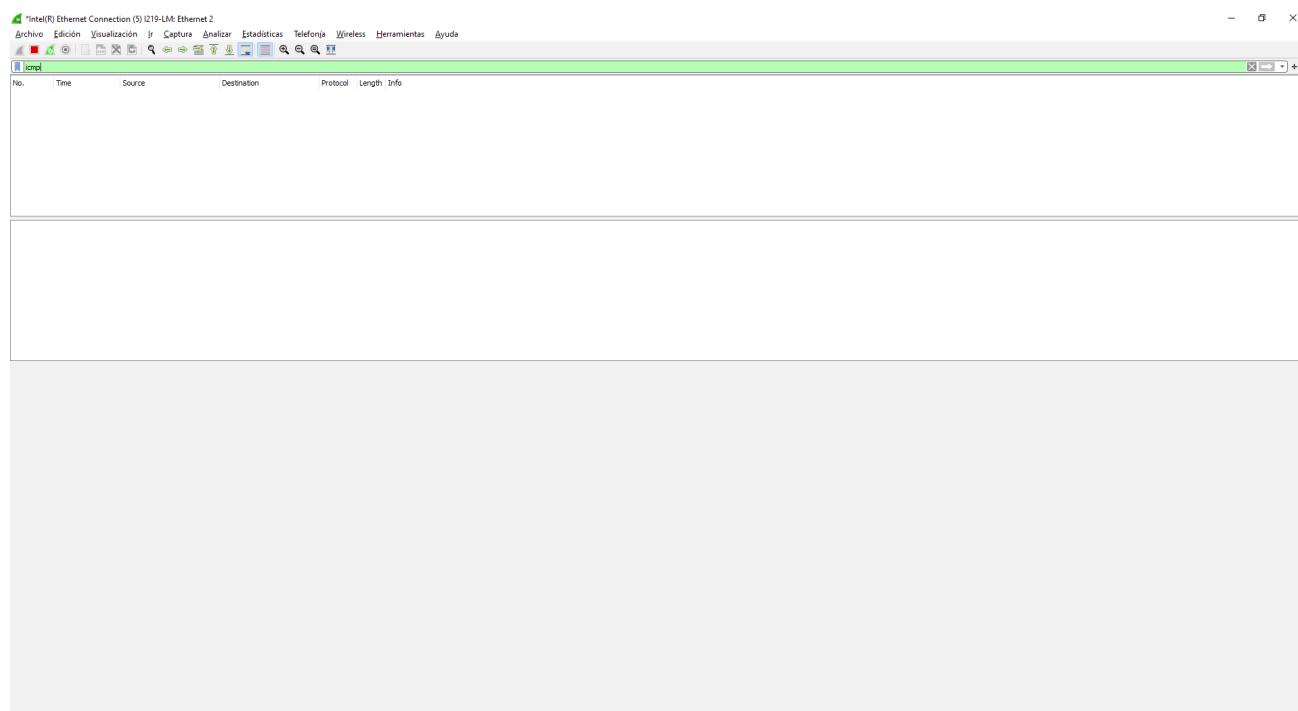
0020 00 00 00 08 08 04 03 5f 85 6f 80 04 00 00 14 00t'00

0030 02 00 0f 00 00 00 00 00 00 00 00 00 00 00 00t'00

Paso 3: Filtrar Wireshark para mostrar solamente el tráfico de ICMP

En el cuadro Filter (Filtrar) de Wireshark, escriba icmp. Si escribió el filtro correctamente, el cuadro se volverá verde. Si el cuadro está de color verde, haga clic en Apply (Aplicar) para aplicar el filtro.

Mostrar captura de pantalla con el resultado



Paso 4: En la ventana del símbolo del sistema, haga ping al gateway predeterminado de la PC

En la ventana del símbolo del sistema, haga ping al gateway predeterminado de la PC

```
Símbolo del sistema

C:\Users\smralumno>ping 192.168.3.250

Haciendo ping a 192.168.3.250 con 32 bytes de datos:
Respuesta desde 192.168.3.250: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.250: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.250: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.3.250: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.3.250:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\smralumno>
```

Paso 5: Detener la captura de tráfico en la NIC

Haga clic en el ícono Stop Capture (Detener captura) para detener la captura de tráfico

Intel(R) Ethernet Connection (5) I219-LM: Ethernet 2

Archivo Edición Visualización Jr Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Detiene captura de paquetes

No.	Time	Source	Destination	Protocol	Length	Info
559	85.774918	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=91/23296, ttl=128 (reply in 560)
560	85.775233	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=91/23296, ttl=64 (request in 559)
563	86.780906	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=92/23552, ttl=128 (reply in 564)
564	86.781210	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=92/23552, ttl=64 (request in 563)
567	87.795976	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=93/23808, ttl=128 (reply in 568)
568	87.796282	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=93/23808, ttl=64 (request in 567)
571	88.815291	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=94/24064, ttl=128 (reply in 572)
572	88.815668	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=94/24064, ttl=64 (request in 571)

> Frame 559: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4AFAEAF2-A756-4562-B001-57F2FE0993FD}, id 0

> Ethernet II, Src: HewlettP_64:5c:3b (3c:52:82:64:5c:3b), Dst: Routerbo_c4:7c:b4 (2c:c8:1b:c4:7c:b4)

> Internet Protocol Version 4, Src: 192.168.3.2, Dst: 192.168.3.250

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 60

Identification: 0xb7fe (47102)

> Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: ICMP (1)

0000 2c c8 1b c4 7c b4 3c 52 82 64 5c 3b 08 00 45 00 ,...|<R d\;..E.

0010 00 3c b7 fe 00 00 80 01 00 00 c0 a8 03 02 c0 a8 <.....

0020 03 fa 08 00 4c 01 01 00 00 5b 61 62 63 64 65 66L... [abcdef

0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Paso 6: Examinar la primera solicitud de eco (ping) en Wireshark

La ventana principal de Wireshark está dividida en tres secciones: el panel de la lista de paquetes (Arriba), el panel de detalles del paquete (Medio) y el panel de bytes del paquete (Abajo). Si seleccionó la interfaz correcta para la captura de paquetes en el paso 3, Wireshark mostrará la información ICMP en el panel de la lista de paquetes de Wireshark

Mostrar dicha captura

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
559	85.774918	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=91/23296, ttl=128 (reply in 560)
560	85.775233	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=91/23296, ttl=64 (request in 559)
563	86.780906	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=92/23552, ttl=128 (reply in 564)
564	86.781210	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=92/23552, ttl=64 (request in 563)
567	87.795976	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=93/23808, ttl=128 (reply in 568)
568	87.796282	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=93/23808, ttl=64 (request in 567)
571	88.815291	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=94/24064, ttl=128 (reply in 572)
572	88.815668	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=94/24064, ttl=64 (request in 571)

> Frame 559: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4AFAEAF2-A756-4562-B001-57F2FE0993FD}, id 0
 > Ethernet II, Src: HewlettP_64:5c:3b (3c:52:82:64:5c:3b), Dst: Routerbo_c4:7c:b4 (2c:c8:1b:c4:7c:b4)
 > Internet Protocol Version 4, Src: 192.168.3.2, Dst: 192.168.3.250
 > Internet Control Message Protocol

```

0000  2c c8 1b c4 7c b4 3c 52 82 64 5c 3b 08 00 45 00  .<..|<R .d\;..E.
0010  00 3c b7 fe 00 00 80 01 00 00 c0 a8 03 02 c0 a8  .<.....
0020  03 fa 08 00 4c 01 01 00 00 5b 61 62 63 64 65 66  .<L... .[abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```

- a) En el panel de la lista de paquetes (sección superior), haga clic en la primera trama que se indica. Debería ver Echo (ping) request (Solicitud de eco [ping]) debajo del encabezado Info (Información). Esta acción debería resaltar la línea en color azul.

*Intel(R) Ethernet Connection (5) I219-LM: Ethernet 2

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
559	85.774918	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=91/23296, ttl=128 (reply in 560)
560	85.775233	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=91/23296, ttl=64 (request in 559)
563	86.780906	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=92/23552, ttl=128 (reply in 564)
564	86.781210	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=92/23552, ttl=64 (request in 563)
567	87.795976	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=93/23808, ttl=128 (reply in 568)
568	87.796282	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=93/23808, ttl=64 (request in 567)
571	88.815291	192.168.3.2	192.168.3.250	ICMP	74	Echo (ping) request id=0x0100, seq=94/24064, ttl=128 (reply in 572)
572	88.815668	192.168.3.250	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=94/24064, ttl=64 (request in 571)

> Frame 559: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4AFAEAF2-A756-4562-B001-57F2FE0993FD}, id 0
 > Ethernet II, Src: HewlettP_64:5c:3b (3c:52:82:64:5c:3b), Dst: Routerbo_c4:7c:b4 (2c:c8:1b:c4:7c:b4)
 > Internet Protocol Version 4, Src: 192.168.3.2, Dst: 192.168.3.250
 > Internet Control Message Protocol

Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x4c01 [correct]
 [Checksum Status: Good]
 Identifier (8E): 256 (0x0100)
 Identifier (LE): 1 (0x0001)
 Sequence Number (8E): 91 (0x005b)
 Sequence Number (LE): 23296 (0x5b00)

```

0000  2c c8 1b c4 7c b4 3c 52 82 64 5c 3b 08 00 45 00  .<..|<R .d\;..E.
0010  00 3c b7 fe 00 00 80 01 00 00 c0 a8 03 02 c0 a8  .<.....
0020  03 fa 08 00 4c 01 01 00 00 5b 61 62 63 64 65 66  .<L... .[abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
  
```

- b) Examine la primera línea del panel de detalles del paquete (sección media). En esta línea, se muestra la longitud de la trama. ¿Qué tamaño tiene? 74bytes

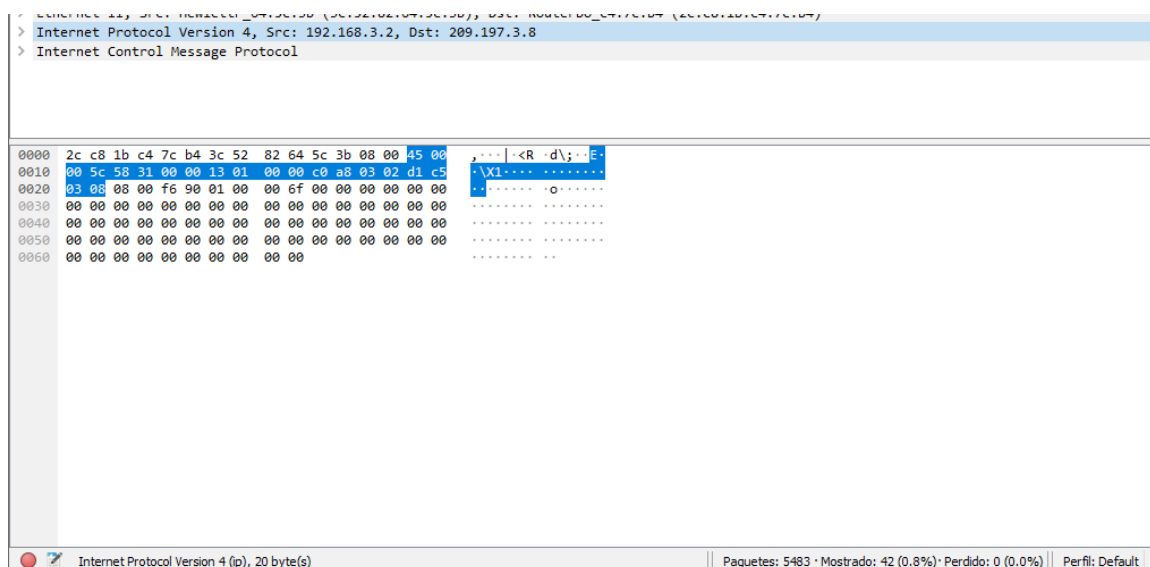
Wireshark packet details for ICMP Echo (ping) request. The packet list shows a request from 192.168.3.2 to 192.168.3.250. The packet details pane shows Ethernet II, Internet Protocol Version 4, and ICMP Echo (ping) request. The packet length is 74 bytes.

- c) En la segunda línea del panel de detalles del paquete, se muestra que es una trama de Ethernet II. También se muestran las direcciones MAC de origen y destino
- ¿Cuál es la dirección MAC de la NIC de la PC? 3c:52:82:64:5c:3b
 - ¿Cuál es la dirección MAC del gateway predeterminado? 2c:c8:1b:c4:7c:b4

Wireshark packet details for Ethernet II. The packet details pane shows Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet length is 74 bytes. The MAC address of the source is 3c:52:82:64:5c:3b and the destination is 2c:c8:1b:c4:7c:b4.

Org: 3c:52:82:64:5c:3b Dst: 2c:c8:1b:c4:7c:b4

- d) Puede hacer clic en el signo más (+) que se encuentra al comienzo de la segunda línea para obtener más información sobre la trama de Ethernet I
- ¿Qué tipo de trama se muestra? **IPv4**
- e) Las dos últimas líneas que se muestran en la sección media proporcionan información sobre el campo de datos de la trama. Observe que los datos contienen la información de la dirección IPv4 de origen y destino.
- ¿Cuál es la dirección IP de origen? **192.168.3.2**
 - ¿Cuál es la dirección IP de destino? **209.197.3.8**
- f) Puede hacer clic en cualquier línea de la sección media para resaltar esa parte de la trama (hexadecimal y ASCII) en el panel de bytes del paquete (sección inferior). Haga clic en la línea Internet Control Message Protocol (Protocolo de mensajes de control de Internet) en la sección media y examine qué está resaltado en el panel de bytes del paquete
- Mostrar la captura de pantalla



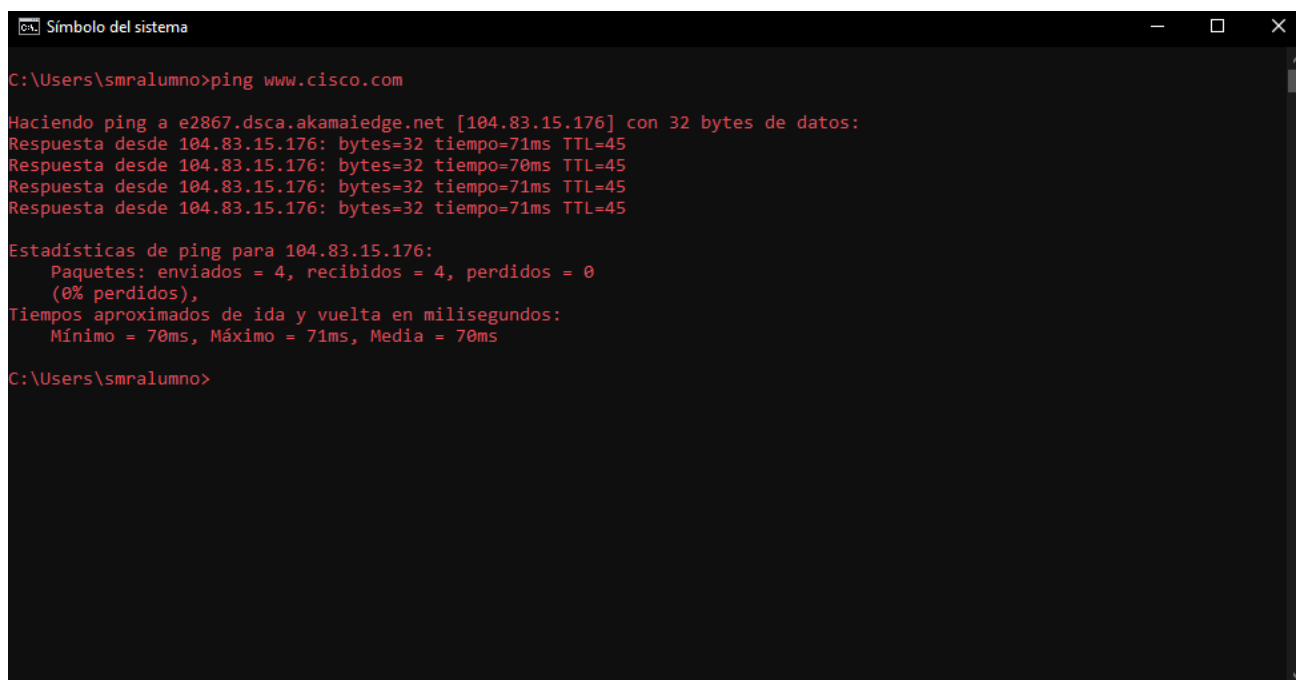
- ¿Qué indican los dos últimos octetos resaltados?
- Las ips de Origen y destino**
- g) Haga clic en la trama siguiente de la sección superior y examine una trama de respuesta de eco. Observe que las direcciones MAC de origen y destino se invirtieron, porque esta trama se envió desde el router del gateway predeterminado como una respuesta al primer ping.
- ¿Qué dirección de dispositivo y dirección MAC se muestran como la dirección de destino?

La direccion Mac de mi PC

Paso 7: Reiniciar la captura de paquetes en Wireshark

Haga clic en el ícono Start Capture (Iniciar captura) para iniciar una nueva captura de Wireshark. Aparece una ventana emergente en la que se le pregunta si desea guardar los paquetes capturados anteriormente en un archivo antes de iniciar una nueva captura. Haga clic en Continue without Saving (Continuar sin guardar).

Paso 8: En la ventana del símbolo del sistema, hacer ping a www.cisco.com



```
CA Símbolo del sistema
C:\Users\smralumno>ping www.cisco.com

Haciendo ping a e2867.dsca.akamaiedge.net [104.83.15.176] con 32 bytes de datos:
Respuesta desde 104.83.15.176: bytes=32 tiempo=71ms TTL=45
Respuesta desde 104.83.15.176: bytes=32 tiempo=70ms TTL=45
Respuesta desde 104.83.15.176: bytes=32 tiempo=71ms TTL=45
Respuesta desde 104.83.15.176: bytes=32 tiempo=71ms TTL=45

Estadísticas de ping para 104.83.15.176:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 70ms, Máximo = 71ms, Media = 70ms

C:\Users\smralumno>
```

Paso 9: Detener la captura de paquetes

Paso 10: Examinar los datos nuevos en el panel de la lista de paquetes de Wireshark

En la primera trama de solicitud de eco (ping), ¿cuáles son las direcciones MAC de origen y destino?

Wireshark interface showing network traffic analysis. The packet list displays ICMP Echo (ping) requests and replies. The packet details pane shows the structure of frame 150: Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
155	28.628869	192.168.3.2	104.83.15.176	ICMP	74	Echo (ping) request id=0x0100, seq=113/28928, ttl=128 (rep)
156	28.699456	104.83.15.176	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=113/28928, ttl=45 (requ)
162	29.638927	192.168.3.2	104.83.15.176	ICMP	74	Echo (ping) request id=0x0100, seq=114/29184, ttl=128 (rep)
163	29.710125	104.83.15.176	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=114/29184, ttl=45 (requ)
168	30.657009	192.168.3.2	104.83.15.176	ICMP	74	Echo (ping) request id=0x0100, seq=115/29440, ttl=128 (rep)
169	30.728392	104.83.15.176	192.168.3.2	ICMP	74	Echo (ping) reply id=0x0100, seq=115/29440, ttl=45 (requ)

Frame 150: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4AFAEAF2-A756-4562-B001-57F2FE0993FD}, id 0

Ethernet II, Src: HewlettP_64:5c:3b (3c:52:82:64:5c:3b), Dst: Routerbo_c4:7c:b4 (2c:c8:1b:c4:7c:b4)

Internet Protocol Version 4, Src: 192.168.3.2, Dst: 104.83.15.176

Internet Control Message Protocol

0000 2c c8 1b c4 7c b4 3c 52 82 64 5c 3b 08 00 45 00<R .d\; .E-

0010 00 3c d3 2e 00 00 80 01 00 00 c0 a8 03 02 68 53 .< hS

0020 0f b0 08 00 4b ec 01 00 00 70 61 62 63 64 65 66Kpabcdef

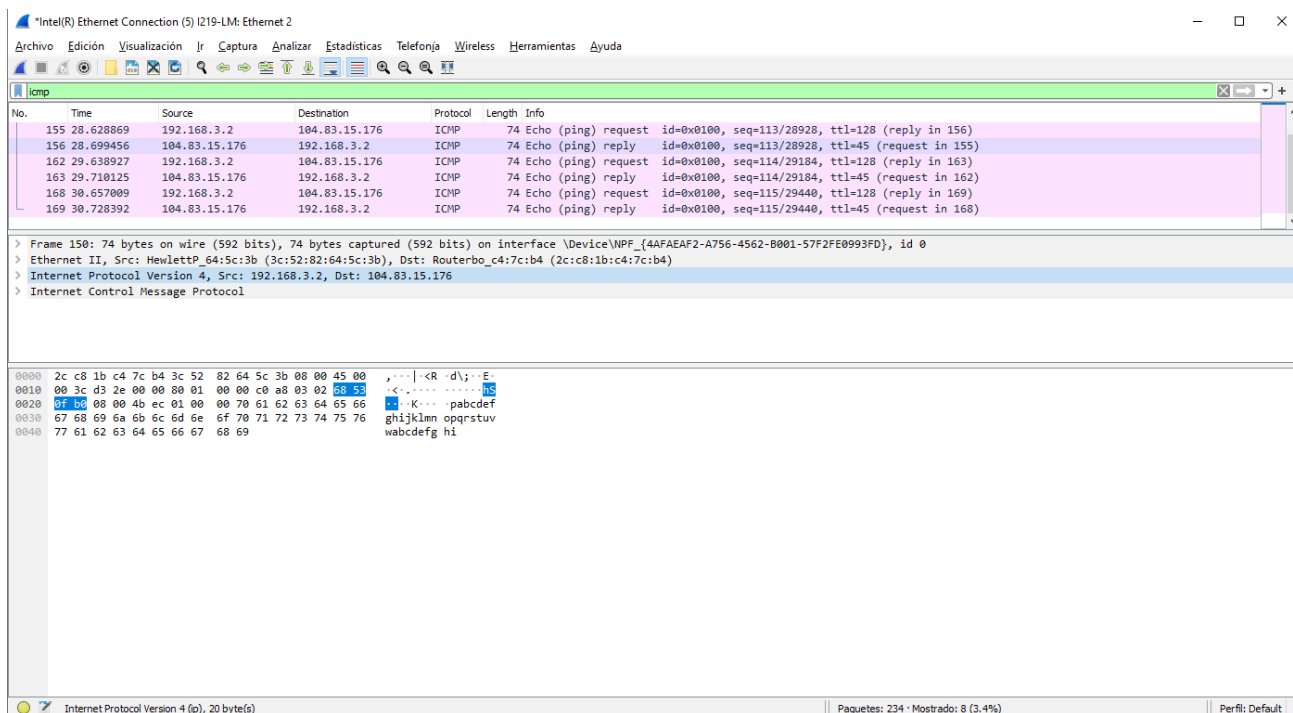
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv

0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi

Ethernet (eth), 14 byte(s) | Paquetes: 234 · Mostrado: 8 (3.4%) | Perfil: Default

Org: 3c:52:82:64:5c:3b Dst: 2c:c8:1b:c4:7c:b4

¿Cuáles son las direcciones IP de origen y destino incluidas en el campo de datos de la trama?



Org: 192.168.3.2 Dst: 104.83.15.176

Compare estas direcciones con las direcciones que recibió en el paso 7. La única dirección que cambió es la dirección IP de destino. ¿Por qué la dirección IP de destino cambió y la dirección MAC de destino siguió siendo la misma?

Por que la ip de destino es la www.cisco.com pero la Mac es la del router por el que sale a internet

Ejercicio 4 (2,5 puntos)

Montar un par de equipos conectados en modo Red NAT ambos en linux. Asegurarse que están en la misma red

Instalar la herramienta Wireshark en Ubuntu para capturar paquetes de una conexión telnet.

Para ello, instalar en primer lugar Wireshark en Ubuntu. Luego elegir en filter el protocolo telnet e iniciar la captura.

Desde la otra máquina, hacer una conexión telnet a la máquina de la red.

Mostrar una captura de pantalla del programa con la captura de los paquetes telnet de forma que veas la contraseña asociada al mismo (puesto que telnet es no seguro y no va cifrado)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
70	68.842423355	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
71	68.842663545	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
73	68.945546718	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
74	68.945790571	192.168.10.4	192.168.10.5	TELNET	67	Telnet Data ...
76	69.279729027	192.168.10.5	192.168.10.4	TELNET	68	Telnet Data ...
77	69.280932380	192.168.10.4	192.168.10.5	TELNET	78	Telnet Data ...
79	70.362051254	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
81	70.544196415	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
83	70.801426461	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
85	71.321627812	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
87	71.487789805	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
89	71.672014040	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
91	71.945392026	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
94	72.313526932	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...

Frame 79: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_85:c7:d8 (08:00:27:85:c7:d8), Dst: PcsCompu_bb:d8:5c (08:00:27:bb:d8:5c)
 Internet Protocol Version 4, Src: 192.168.10.5, Dst: 192.168.10.4
 Transmission Control Protocol, Src Port: 60508, Dst Port: 23, Seq: 155, Ack: 131, Len: 1
 Telnet
 Data: a

0000 08 00 27 bb d8 5c 08 00 27 85 c7 d8 08 00 45 10 ...E
 0010 00 35 a6 f0 40 00 40 06 fe 68 c0 a8 0a 05 c0 a8 ...5-@-@-h
 0020 0a 04 ec 5c 00 17 ec 98 e7 45 d6 3b ba f0 80 18 ...-X-@-E-
 0030 01 f6 fd 1a 00 00 01 01 08 0a cf 49 be 39 bf 5b ...-I-9-
 0040 e2 ea 01 ...

Data (telnet.data), 1 byte(s) Packets: 140 · Displayed: 51 (36.4%) Profile: Default

Ubuntu 20.04.2 [Corriendo] - Oracle VM VirtualBox

Archivos Máquina Ver Entrada Dispositivos Ayuda

23 de may 14:38

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

telnet

No.	Time	Source	Destination	Protocol	Length	Info
70	68.842423355	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
71	68.842663545	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
73	68.945546718	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
74	68.945790571	192.168.10.4	192.168.10.5	TELNET	67	Telnet Data ...
76	69.279729027	192.168.10.5	192.168.10.4	TELNET	68	Telnet Data ...
77	69.280932380	192.168.10.4	192.168.10.5	TELNET	78	Telnet Data ...
79	70.362051254	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
81	70.544196415	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
83	70.801426461	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
85	71.321627812	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
87	71.487789805	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
89	71.672014040	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...
91	71.945392026	192.168.10.5	192.168.10.4	TELNET	67	Telnet Data ...

Frame 79: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface enp0s3, id 0
 Ethernet II, Src: PcsCompu_85:c7:d8 (08:00:27:85:c7:d8), Dst: PcsCompu_bb:d8:5c (08:00:27:bb:d8:5c)
 Internet Protocol Version 4, Src: 192.168.10.5, Dst: 192.168.10.4
 Transmission Control Protocol, Src Port: 60508, Dst Port: 23, Seq: 155, Ack: 131, Len: 1
 Telnet
 Data: a

0000 08 00 27 bb d8 5c 08 00 27 85 c7 d8 08 00 45 10 ...E
 0010 00 35 a6 f0 40 00 40 06 fe 68 c0 a8 0a 05 c0 a8 ...5-@-@-h
 0020 0a 04 ec 5c 00 17 ec 98 e7 45 d6 3b ba f0 80 18 ...-X-@-E-
 0030 01 f6 fd 1a 00 00 01 01 08 0a cf 49 be 39 bf 5b ...-I-9-
 0040 e2 ea 01 ...

Data (telnet.data), 1 byte(s) Packets: 282 · Displayed: 113 (40.1%) Profile: Default

leticia@leticia-VirtualBox:~\$ telnet 192.168.10.4
 Trying 192.168.10.4...
 Connected to 192.168.10.4.
 Escape character is '^'.
 Ubuntu 20.04.2 LTS
 leticia-VirtualBox login: leticia
 Password:
 Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.8.0-43-generic x86_64)

* Documentation: <https://help.ubuntu.com>
 * Management: <https://landscape.canonical.com>
 * Support: <https://ubuntu.com/advantage>

465 actualizaciones se pueden instalar inmediatamente.
 296 de estas actualizaciones adicionales ejecute: apt list --upgradable
 Para ver estas actualizaciones adicionales ejecute: apt list --upgradable

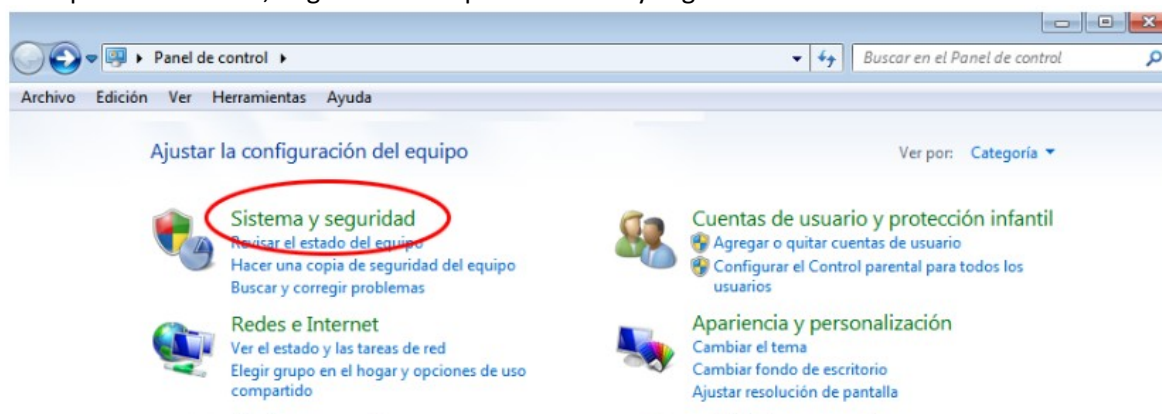
Your Hardware Enablement Stack (HWE) is supported until April 2025.
 Last login: Mon May 23 14:33:01 CEST 2022 from 192.168.10.5 on pts/2
 leticia@leticia-VirtualBox:~\$

Apéndice: Permitir el tráfico ICMP a través de un firewall

Si los miembros del equipo no pueden hacer ping a su PC, es posible que el firewall esté bloqueando esas solicitudes. En este apéndice, se describe cómo crear una regla en el firewall para permitir las solicitudes de ping. También se describe cómo deshabilitar la nueva regla ICMP después de haber completado la práctica de laboratorio

Paso 1: Crear una nueva regla de entrada que permita el tráfico ICMP a través del firewall

- a) En el panel de control, haga clic en la opción Sistema y seguridad



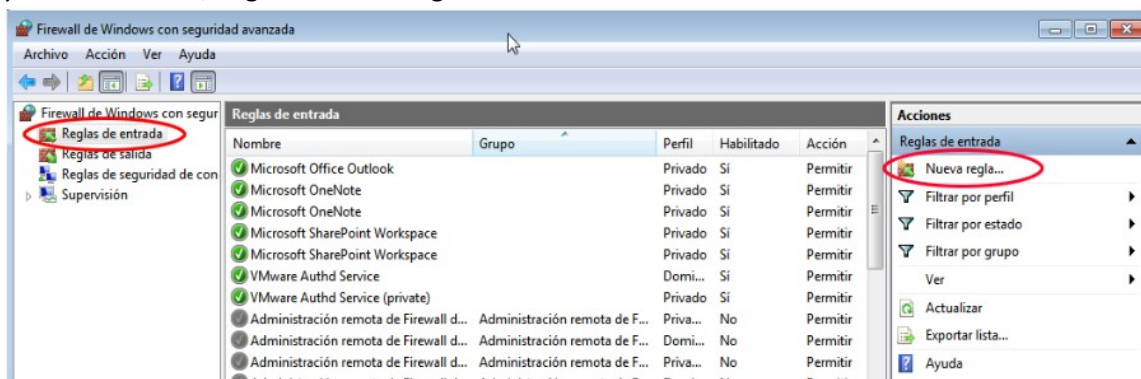
- b) En la ventana Sistema y seguridad, haga clic en Firewall de Windows



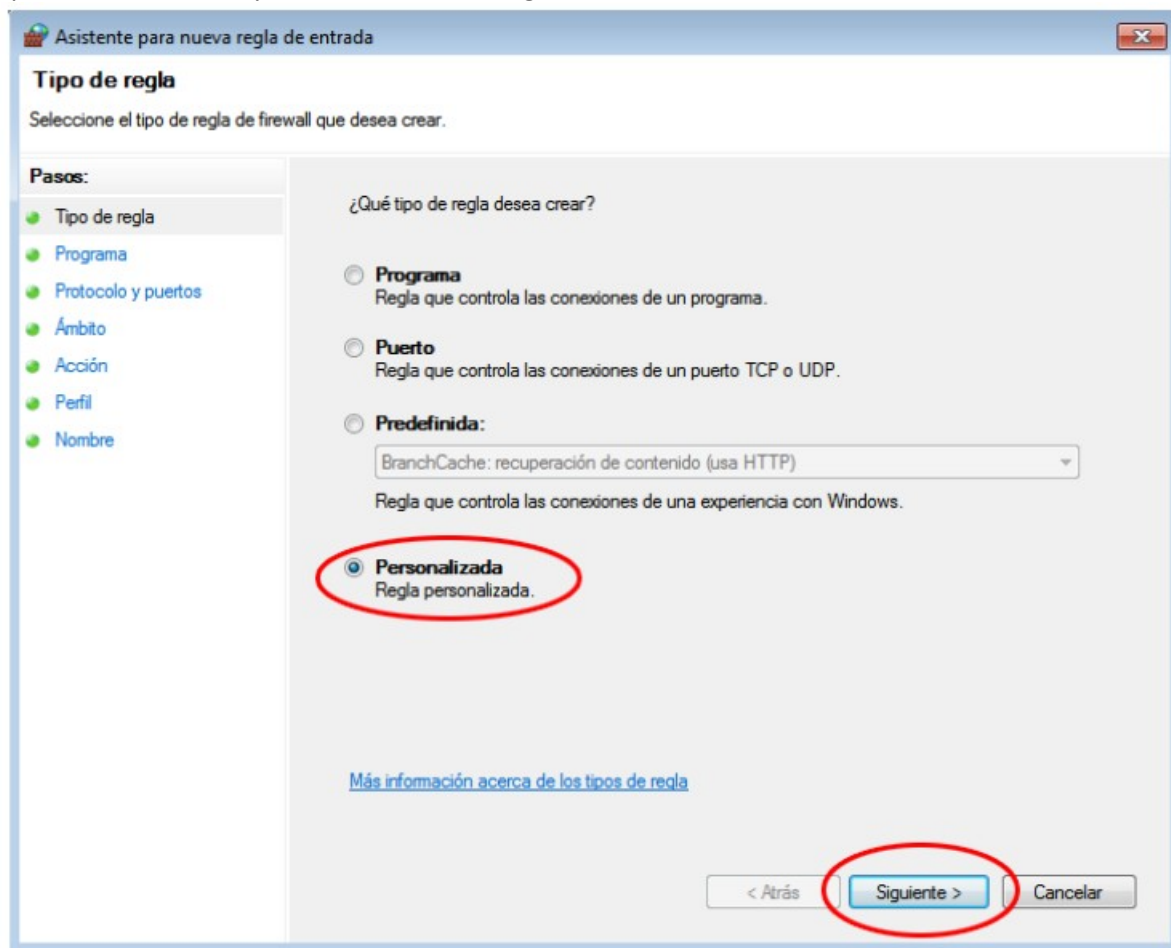
- c) En el panel izquierdo de la ventana Firewall de Windows, haga clic en Configuración avanzada



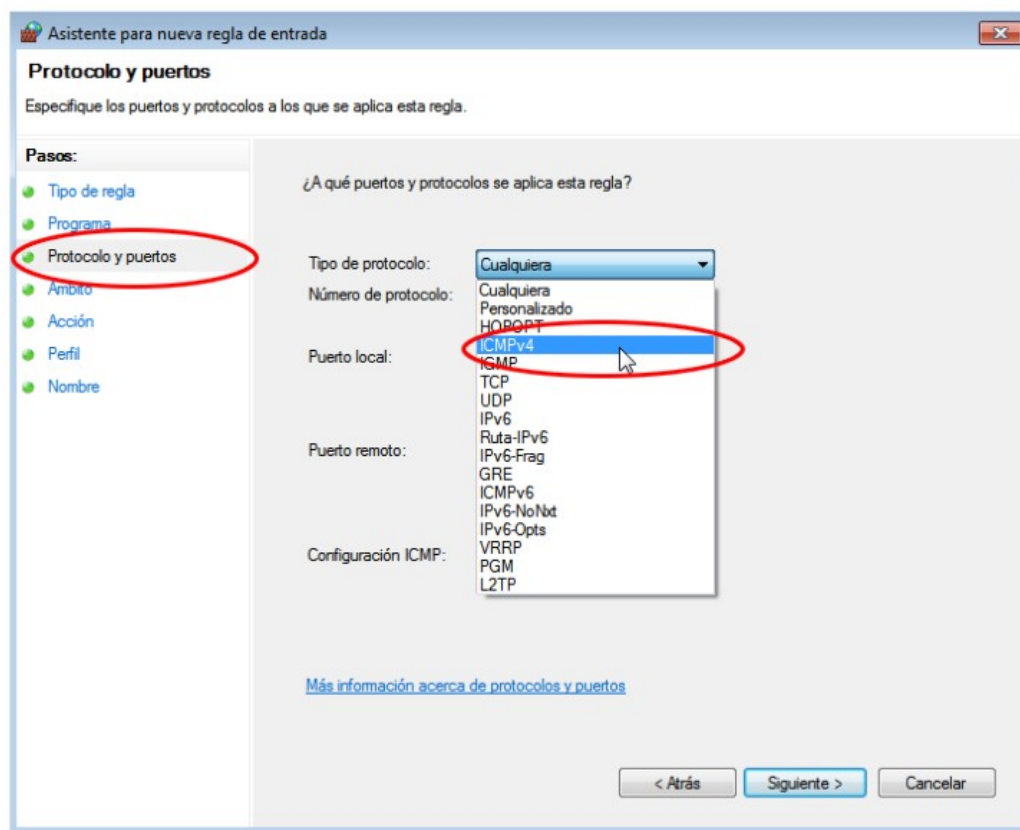
- d) En la ventana Seguridad avanzada, seleccione la opción Reglas de entrada en la barra lateral izquierda y, a continuación, haga clic Nueva regla en la barra lateral derecha



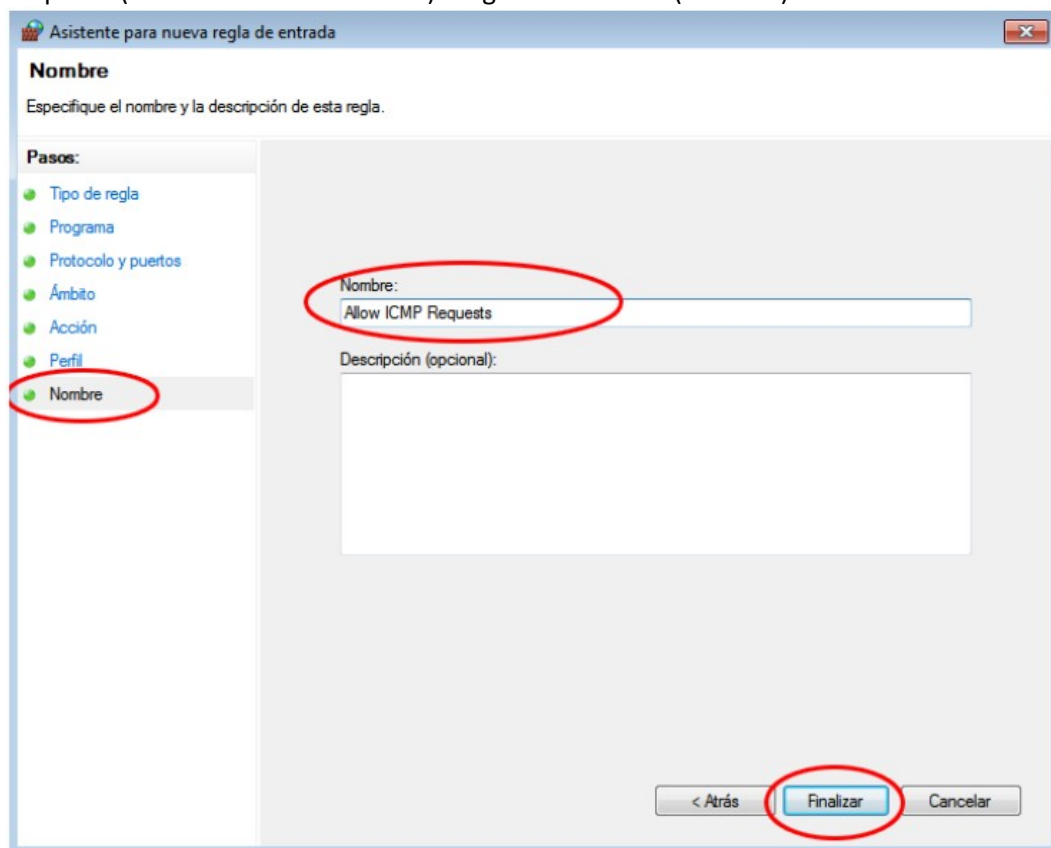
- e) Se inicia el Asistente para nueva regla de entrada. En la pantalla Tipo de regla, haga clic en el botón de opción Personalizada y, a continuación, en Siguiente.



- f) En el panel izquierdo, haga clic en la opción Protocolo y puertos, y en el menú desplegable Tipo de protocolo, seleccione ICMPv4; a continuación, haga clic en Siguiente.



- g) En el panel izquierdo, haga clic en la opción Nombre, y en el campo Nombre, escriba Allow ICMP Requests (Permitir solicitudes ICMP). Haga clic en Finish (Finalizar)

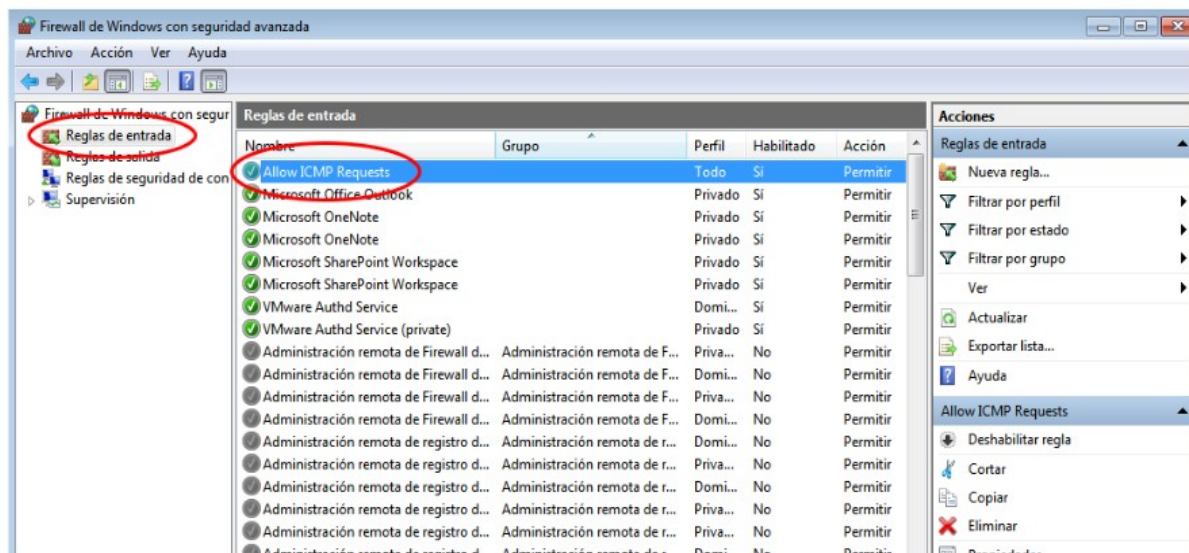


Esta nueva regla debe permitir que los miembros del equipo reciban respuestas de ping de su PC.

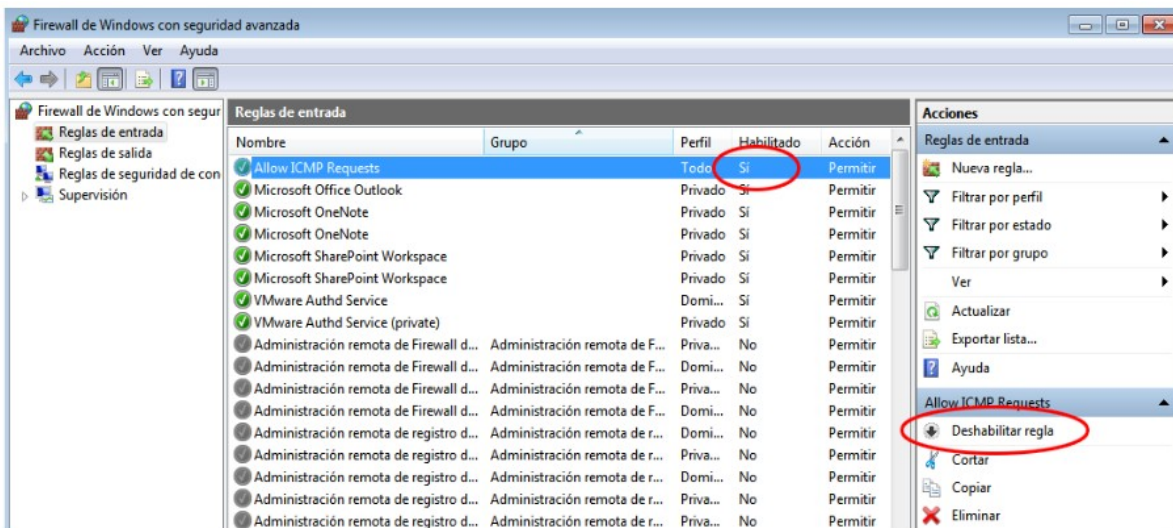
Paso 2: Deshabilitar o eliminar la nueva regla ICMP

Una vez completada la práctica de laboratorio, es posible que desee deshabilitar o incluso eliminar la nueva regla que creó en el paso 1. La opción Deshabilitar regla permite volver a habilitar la regla en una fecha posterior. Al eliminar la regla, esta se elimina permanentemente de la lista de Reglas de entrada.

- a) En el panel izquierdo de la ventana Seguridad avanzada, haga clic en Reglas de entrada y, a continuación, ubique la regla que creó en el paso 1.



- b) Para deshabilitar la regla, haga clic en la opción Deshabilitar regla. Al seleccionar esta opción, verá que esta cambia a Habilitar regla. Puede alternar entre deshabilitar y habilitar la regla; el estado de la regla también se muestra en la columna Habilitada de la lista Reglas de entrada.



- c) Para eliminar permanentemente la regla ICMP, haga clic en Eliminar. Si elige esta opción, deberá volver a crear la regla para permitir las respuestas de ICMP.

