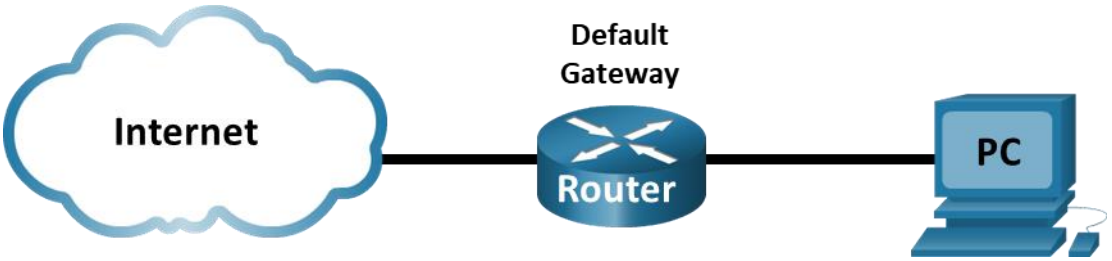
Laboratorio: utilice Wireshark para examinar tramas de Ethernet

Topología



Nombre: Daniel Sierra

Objetivos

Parte 1: Examinar los campos de encabezado de una trama de Ethernet II

Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

Aspectos básicos/situación

Cuando los protocolos de capa superior se comunican entre sí, los datos fluyen por las capas de interconexión de sistemas abiertos (OSI) y se encapsulan en una trama de capa 2. La composición de la trama depende del tipo de acceso al medio. Por ejemplo, si los protocolos de capa superior son TCP e IP, y el acceso a los medios es Ethernet, el encapsulamiento de tramas de capa 2 es Ethernet II. Esto es típico para un entorno LAN.

Al aprender sobre los conceptos de la capa 2, es útil analizar la información del encabezado de la trama. En la primera parte de esta práctica de laboratorio, revisará los campos que contiene una trama de Ethernet II. En la parte 2, utilizará Wireshark para capturar y analizar campos de encabezado de tramas de Ethernet II de tráfico local y remoto.

Recursos necesarios

- 1 PC (Windows con acceso a internet y con Wireshark instalado)

Instrucciones

Parte 1: Examinar los campos de encabezado de una trama de Ethernet II

En la parte 1, examinará los campos de encabezado y el contenido de una trama de Ethernet II. Se utilizará una captura de Wireshark para examinar el contenido de esos campos.

Paso 1: Revisar las descripciones y longitudes de los campos de encabezado de Ethernet II

Preámbulo	Dirección de destino	Dirección de origen	Tipo de trama	Datos	FCS
8 bytes	6 bytes	6 bytes	2 bytes	46 a 1500 bytes	4 bytes

Paso 2: Examinar la configuración de red de la PC

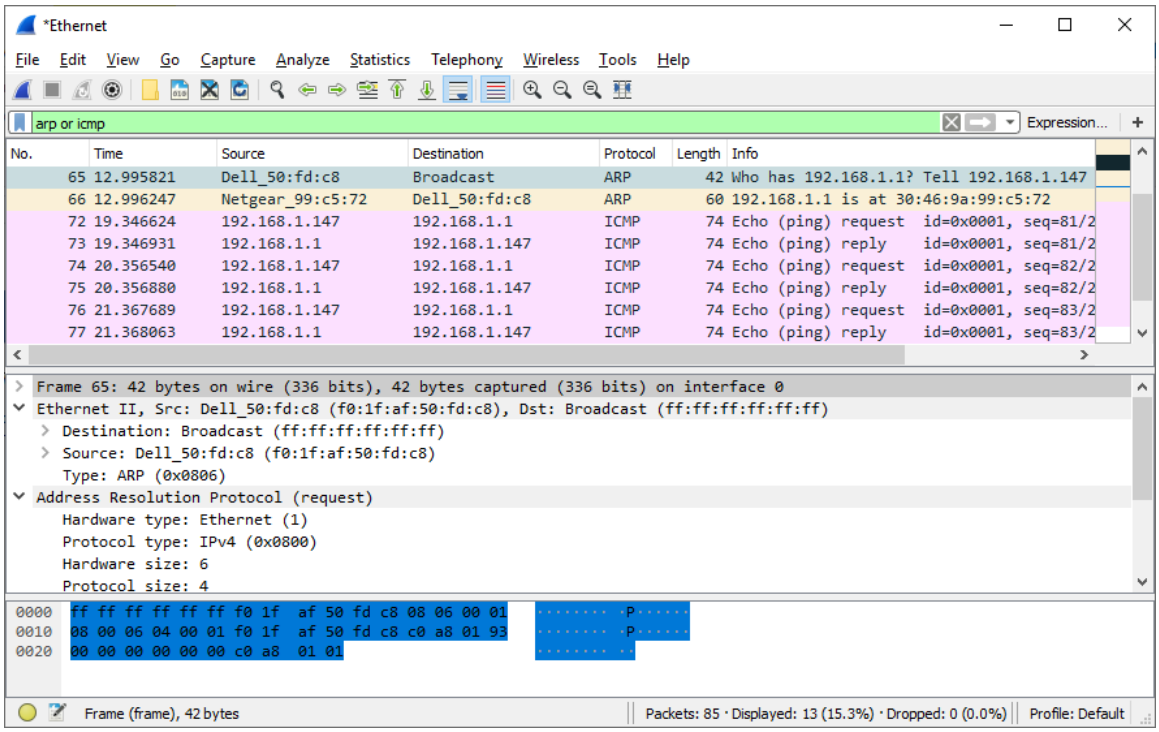
En este ejemplo, la dirección IP del host de esta PC es 192.168.1.147 y la puerta de enlace predeterminada tiene una dirección IP de 192.168.1.1.

```
C:\> ipconfig /all

Ethernet adaptador Ethernet:

   Sufijo de conexión específica DNS. :
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connection
   Physical Address. . . . . . . . . : F0-1F-AF-50-FD-C8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . .: fe80: :58c 5:45 f 2:7 e5e:29c 2% 11 (Preferido)
   IPv4 Address. . . . . . . . . . . : 192.168.1.147(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : viernes 6 de septiembre de 2019 11:08:36
   Lease Expires . . . . . . . . . . : sábado 7 de septiembre de 2019 11:08:36
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
<output omitted>
```

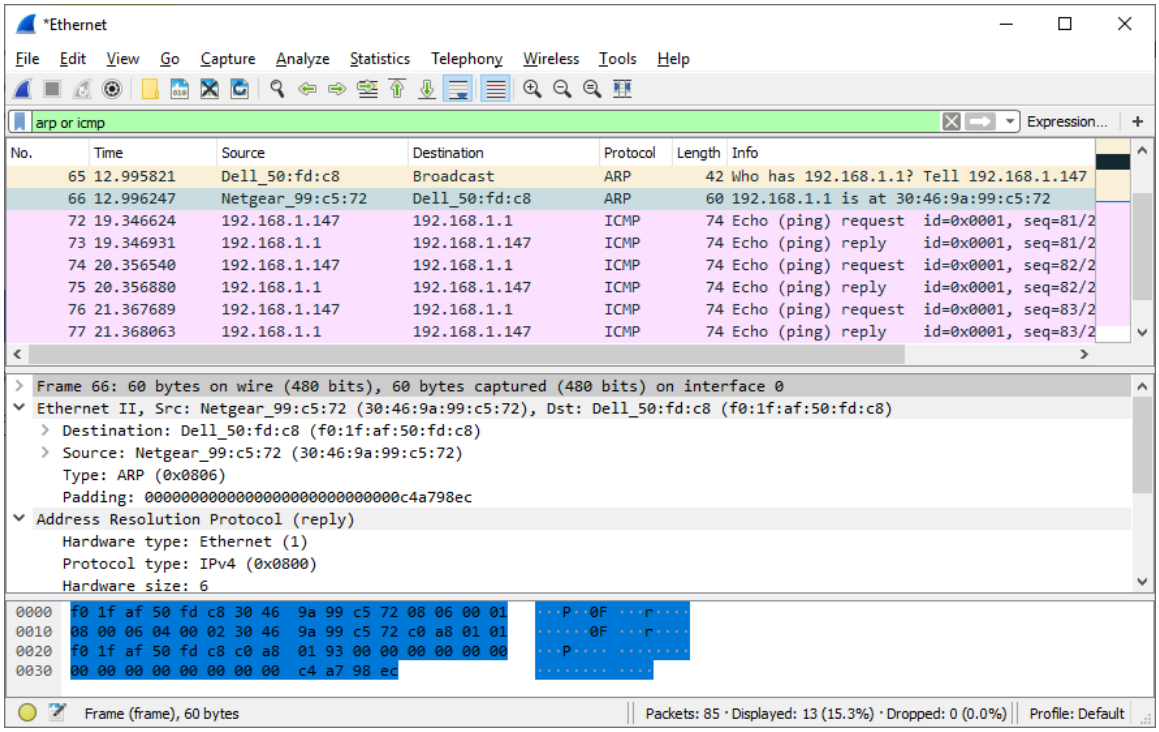
Paso 3: Examinar las tramas de Ethernet en una captura de Wireshark

Las imágenes de la captura de Wireshark a continuación muestran los paquetes generados por un ping emitido desde un host de PC a su puerta de enlace predeterminada. Se le aplicó un filtro a Wireshark para ver solamente el protocolo de resolución de direcciones (ARP) y el protocolo de mensajes de control de Internet (ICMP). ARP significa protocolo de resolución de direcciones. ARP es un protocolo de comunicación que se utiliza para determinar la dirección MAC asociada a la dirección IP. La sesión comienza con una consulta ARP para obtener la dirección MAC del router de la puerta de enlace seguida de cuatro solicitudes y respuestas de ping.

Esta captura de pantalla resalta los detalles del fotograma de una solicitud ARP.



Esta captura de pantalla resalta los detalles de la trama para una respuesta ARP.



Paso 4: Examinar el contenido del encabezado de Ethernet II de una solicitud de ARP

En la siguiente tabla, se toma la primera trama de la captura de Wireshark y se muestran los datos de los campos de encabezado de Ethernet II.

Campo	Valor	Descripción
Preámbulo	No se muestra en la captura.	Este campo contiene bits de sincronización, procesados por el hardware de la NIC.
Dirección de destino Dirección de origen	Broadcast (ff:ff:ff:ff:ff:ff) (Difusión [ff:ff:ff:ff:ff:ff]) NetGear_99:C 5:72 (30:46:9 a:99:c 5:72)	Direcciones de capa 2 para la trama. Cada dirección tiene una longitud de 48 bits, o 6 octetos, expresada como 12 dígitos hexadecimales (`0-9, A-F`). Un formato común es `12:34:56:78:9A:BC.` Los primeros seis números hexadecimales indican el fabricante de la tarjeta de interfaz de red (NIC), y los últimos seis números son el número de serie de la NIC. La dirección de destino puede ser de difusión, que contiene todos números uno, o de unidifusión. La dirección de origen siempre es de unidifusión.
Tipo de trama	0x0806	Para las tramas de Ethernet II, este campo contiene un valor hexadecimal que se utiliza para indicar el tipo de protocolo de capa superior del campo de datos. Ethernet II admite varios protocolos de capa superior. Dos tipos comunes de trama son los siguientes: Valor Descripción `0x0800` Protocolo IPv4 `0x0806` Protocolo de resolución de direcciones (ARP)
Datos	ARP	Contiene el protocolo de nivel superior encapsulado. El campo de datos tiene entre 46 y 1500 bytes.
FCS	No se muestra en la captura.	Secuencia de verificación de trama, utilizada por la NIC para identificar errores durante la transmisión. El equipo emisor calcula el valor abarcando las direcciones de trama, campo de datos y tipo. El receptor lo verifica.

¿Qué característica significativa tiene el contenido del campo de dirección de destino?

La característica significativa del campo de dirección de destino es que determina a quién está dirigida la trama: puede ser una dirección unicast (a un solo dispositivo), broadcast (a todos los dispositivos de la red), o multicast (a un grupo específico de dispositivos).

¿Por qué envía la PC un ARP de difusión antes de enviar la primera solicitud de ping?

Es para obtener la dirección MAC correspondiente a la dirección IP de destino. Permite que la PC reconozca la dirección física MAC del dispositivo que desea enviar el ping.

¿Cuál es la dirección MAC del origen en la primera trama?

30:46:9a:99:c5:72

¿Cuál es el ID de proveedor (OUI) de la NIC de origen en la respuesta ARP?

El OUI es 30:46:9a

¿Qué porción de la dirección MAC corresponde al OUI?

Este es el identificador de los **primeros 3 bytes** de la dirección MAC y corresponde al fabricante de la tarjeta de red.

¿Cuál es el número de serie de la NIC del origen?

El **número de serie de la NIC del origen** es la **porción final de la dirección MAC**, es decir, los **últimos 3 bytes** (24 bits).

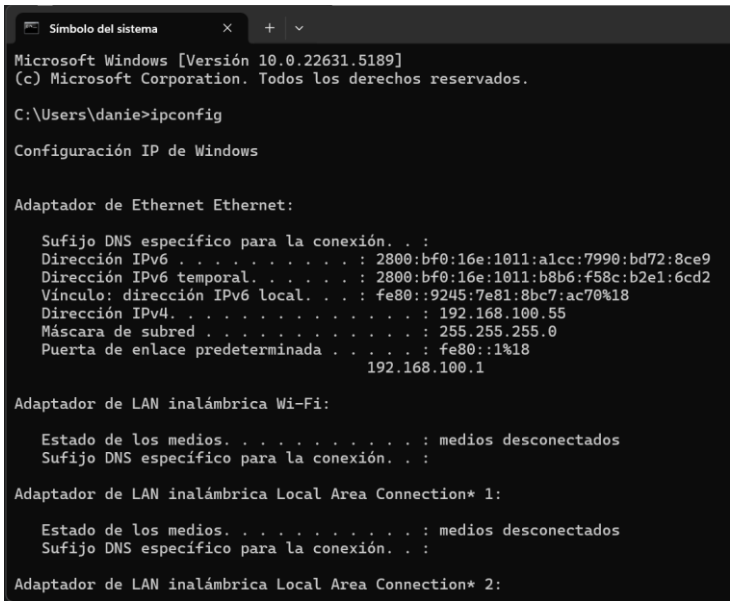
Parte 2: Utilizar Wireshark para capturar y analizar tramas de Ethernet

En la parte 2, utilizará Wireshark para capturar tramas de Ethernet locales y remotas. Luego, examinará la información que contienen los campos de encabezado de las tramas.

Paso 1: Determinar la dirección IP del gateway predeterminado de 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?



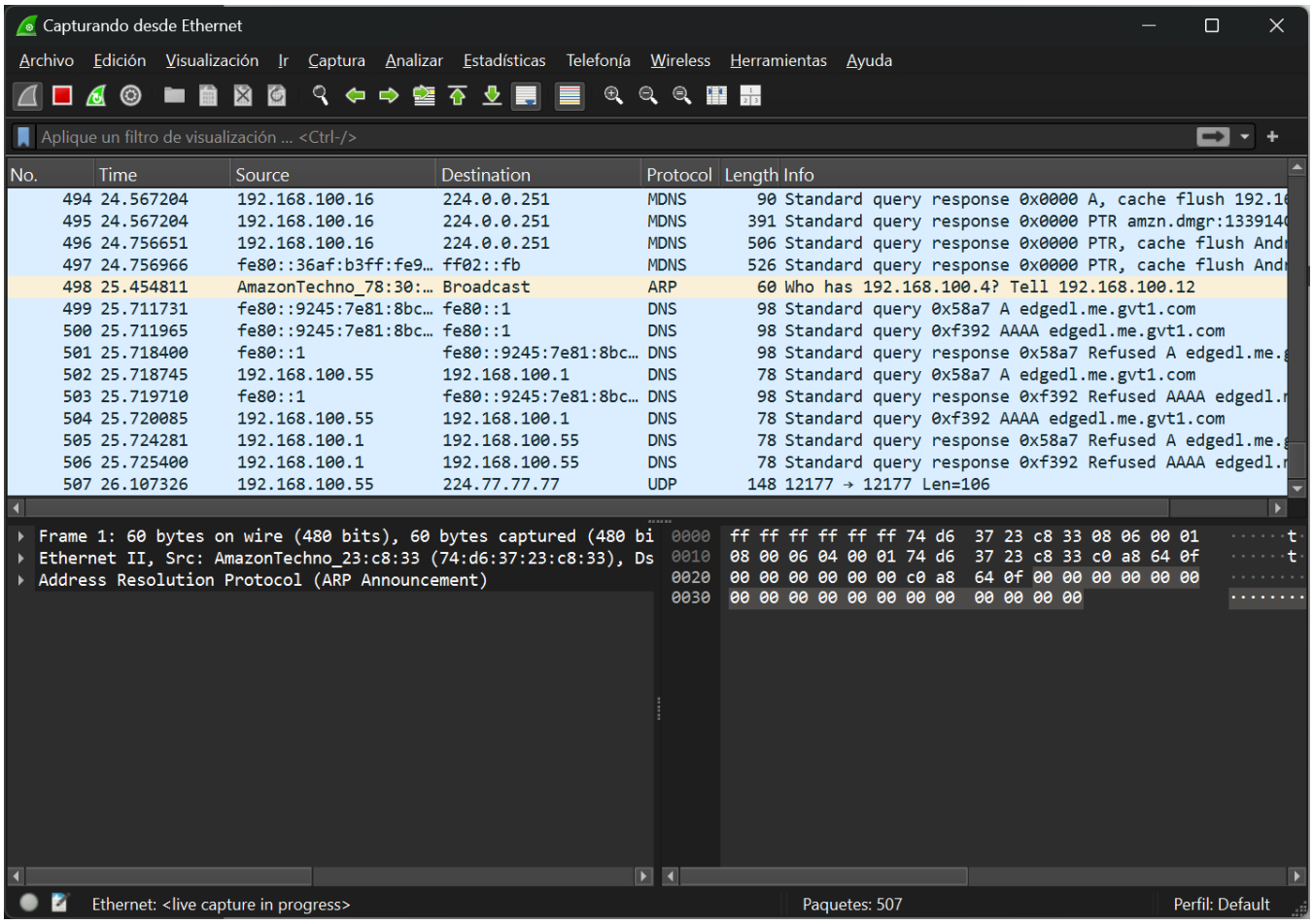
La **dirección IP del gateway predeterminado** de la PC es:

192.168.100.1

Paso 2: Comenzar a capturar el tráfico de la NIC de la PC

a. Abrir Wireshark para iniciar la captura de datos.

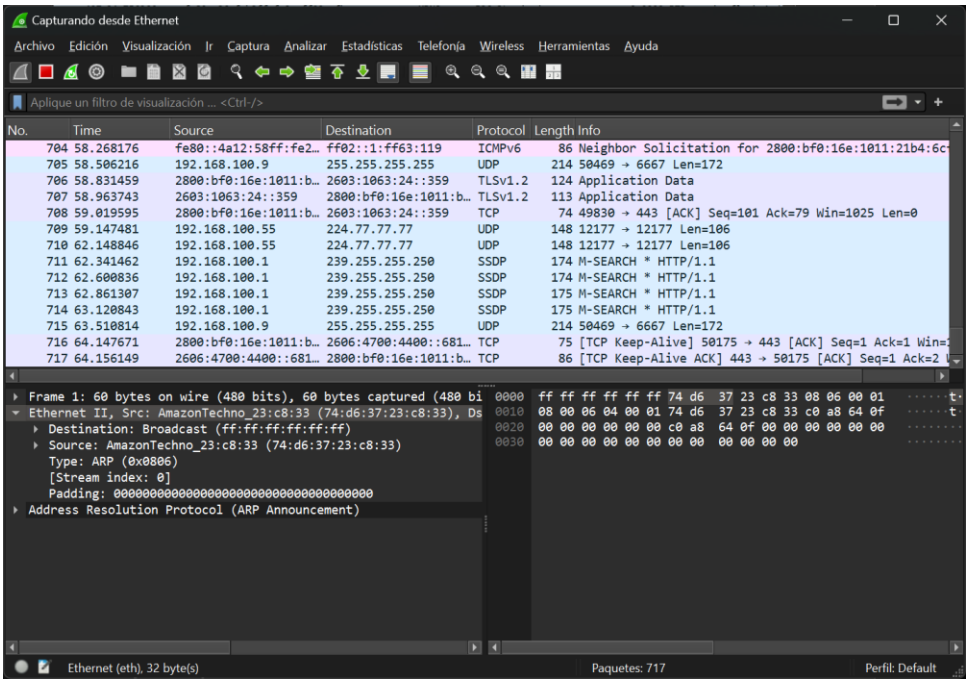
b. Observe el tráfico que aparece en la ventana Packet List (Lista de paquetes).



Paso 3: Filtrar Wireshark para que solamente se muestre el tráfico ICMP

Puede usar el filtro de Wireshark para bloquear la visibilidad del tráfico no deseado. El filtro no bloquea la captura de datos no deseados; solo filtra lo que desea mostrar en la pantalla. Por el momento, solo se debe visualizar el tráfico ICMP.

En el cuadro **Filter (Filtro)** de Wireshark, escriba **icmp**. Si escribió el filtro correctamente, el cuadro debe volverse de color verde. Si el cuadro está de color verde, haga clic en **Apply** (Aplicar) (la flecha hacia la derecha) para que se aplique el filtro.

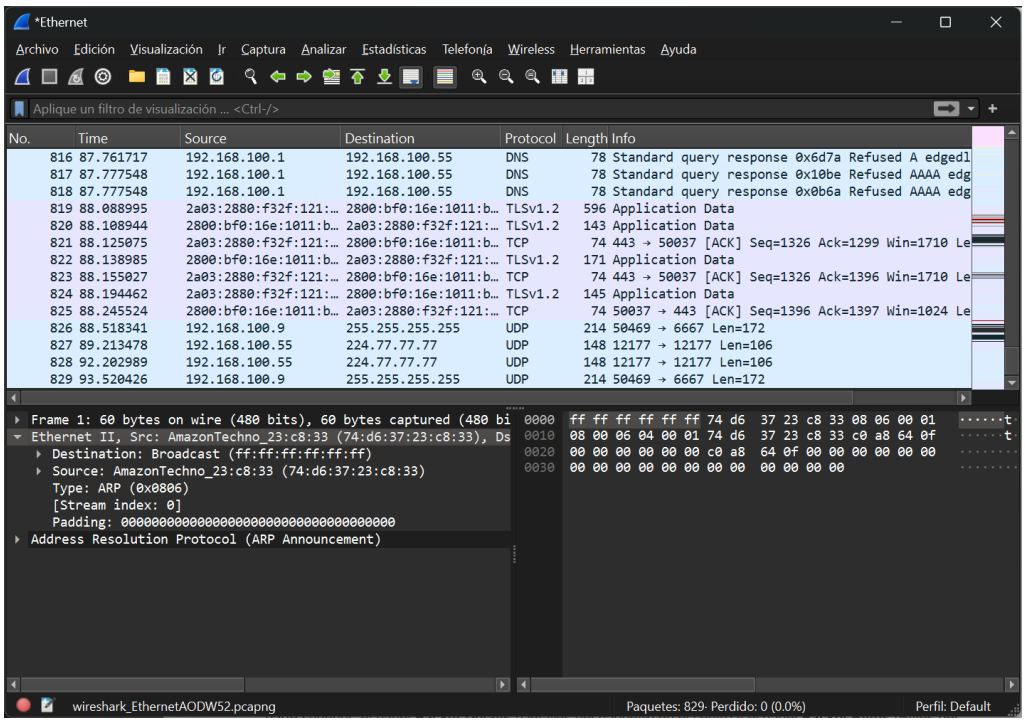


Paso 4: En la ventana del símbolo del sistema, hacer un ping al gateway predeterminado de la PC

En la ventana del símbolo del sistema, haga un ping al gateway predeterminado con la dirección IP registrada en el paso 1.

Paso 5: Dejar de capturar el tráfico de la NIC

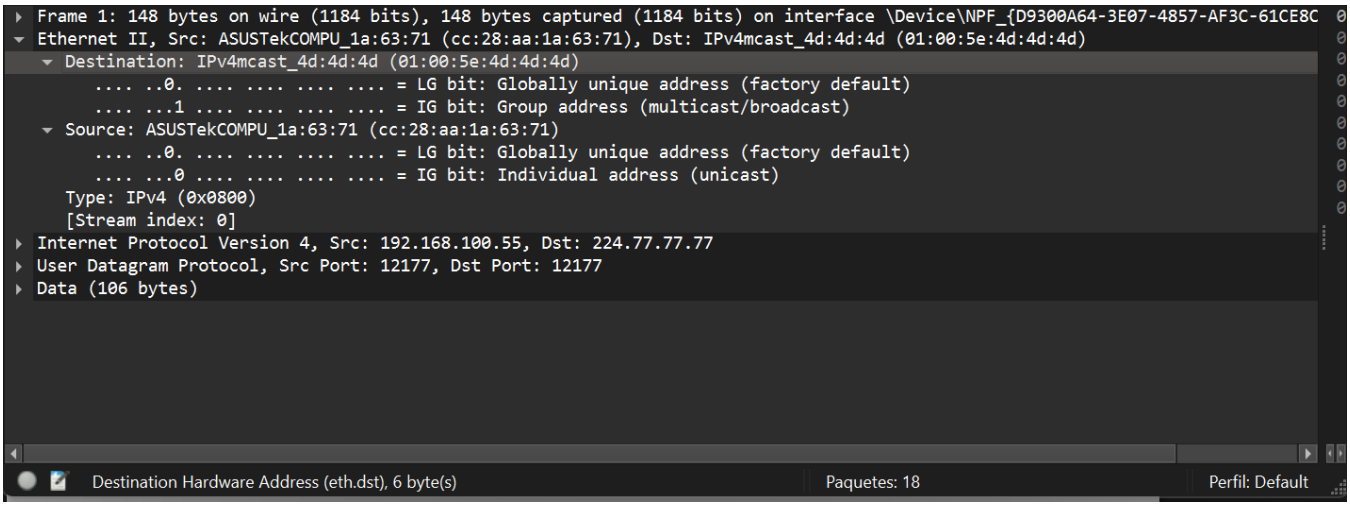
Haga click en el ícono de **Detener captura de paquetes** para detener la captura de tráfico



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

La ventana principal de Wireshark se divide en tres secciones: el panel Packet List (Lista de paquetes) en la parte superior, el panel **Packet Details** (Detalles del paquete) en el centro y el panel **Packet Bytes** (Bytes del paquete) en la parte inferior. Si seleccionó la interfaz correcta para la captura de paquetes anteriormente, Wireshark debería mostrar la información ICMP en el panel de la lista de paquetes de Wireshark.

a. En el panel Packet List (Lista de paquetes) de la parte superior, haga clic en la primera trama de la lista. Debería ver el texto **Echo (ping) request (Solicitud de eco [ping])** debajo del encabezado **Info (Información)**. La línea debe resaltarse ahora.



b. Examine la primera línea del panel Packet Details (Detalles del paquete) de la parte central. Esta línea muestra la longitud de la trama.

60 bytes (480 bits)

c. En la segunda línea del panel Packet Details (Detalles del paquete), se muestra que es una trama de Ethernet II. También se muestran las direcciones MAC de origen y de destino.

¿Cuál es la dirección MAC de la NIC de la PC?

74:d6:37:23:c8:33

¿Cuál es la dirección MAC del gateway predeterminado?

01:00:5e:4d:4d:4d

d. Puede hacer clic en el signo mayor que (>) al comienzo de la segunda línea para obtener más información sobre la trama de Ethernet II.

¿Qué tipo de trama se muestra?

IPv4 (0x0800)

e. En las últimas dos líneas de la parte central, se proporciona información sobre el campo de datos de la trama. Observe que los datos contienen información sobre las direcciones IPv4 de origen y de destino.

¿Cuál es la dirección IP de origen?

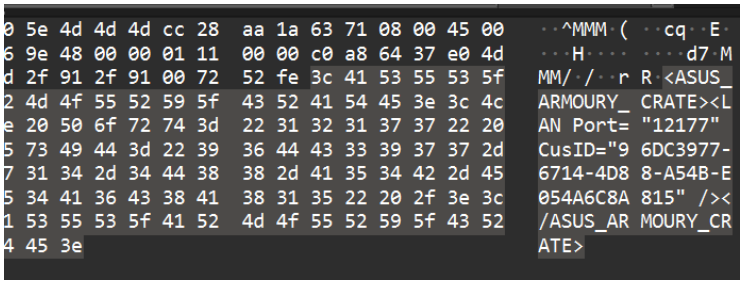
192.168.100.55

¿Cuál es la dirección IP de destino?

244.77.77.77

f. Puede hacer clic en cualquier línea de la parte central para resaltar esa parte de la trama (hexadecimal y ASCII) en el panel **Packet Bytes** (Bytes del paquete) de la parte inferior. Haga clic en la línea **Internet**

Control Message Protocol (Protocolo de mensajes de control de Internet) de la parte central y examine lo que se resalta en el panel **Packet Bytes** (Bytes de paquete).



```
0 5e 4d 4d 4d cc 28  aa 1a 63 71 08 00 45 00    ··^MMM·(  ··cq··E·
6 9e 48 00 00 01 11  00 00 c0 a8 64 37 e0 4d    ··H·····  ····d7·M
d 2f 91 2f 91 00 72  52 fe 3c 41 53 55 53 5f    MM/·/··r R·<ASUS_
2 4d 4f 55 52 59 5f  43 52 41 54 45 3e 3c 4c    ARMOURY_ CRATE><L
e 20 50 6f 72 74 3d  22 31 32 31 37 37 22 20    AN Port= "12177"
5 73 49 44 3d 22 39  36 44 43 33 39 37 37 2d    CusID="9 6DC3977-
7 31 34 2d 34 44 38  38 2d 41 35 34 42 2d 45    6714-4D8 8-A54B-E
5 34 41 36 43 38 41  38 31 35 22 20 2f 3e 3c    054A6C8A 815" /><
1 53 55 53 5f 41 52  4d 4f 55 52 59 5f 43 52    /ASUS_AR MOURY_CR
4 45 3e                                         ATE>
```

¿Qué texto muestran los últimos dos octetos resaltados?

Muestra ATE>

g. Haga clic en la siguiente trama de la parte superior y examine una trama de respuesta de eco. Observe que las direcciones MAC de origen y de destino se invirtieron porque esta trama se envió desde el router del gateway predeterminado como respuesta al primer ping.

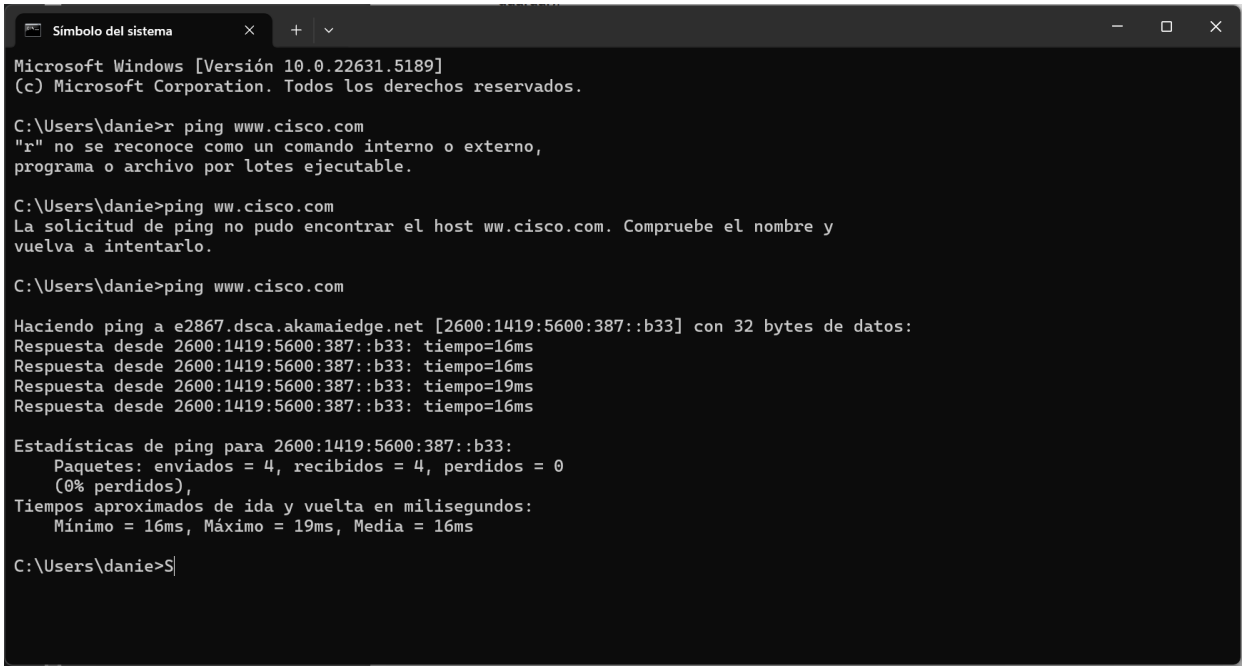
¿Qué dispositivo y qué dirección MAC se muestran como dirección de destino?

- **Dispositivo de destino**: Es una dirección de multidifusión (multicast).
- Dirección MAC de destino: 01:00:5e:4d:4d:4d

Paso 7: Capturar paquetes para un host remoto.

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

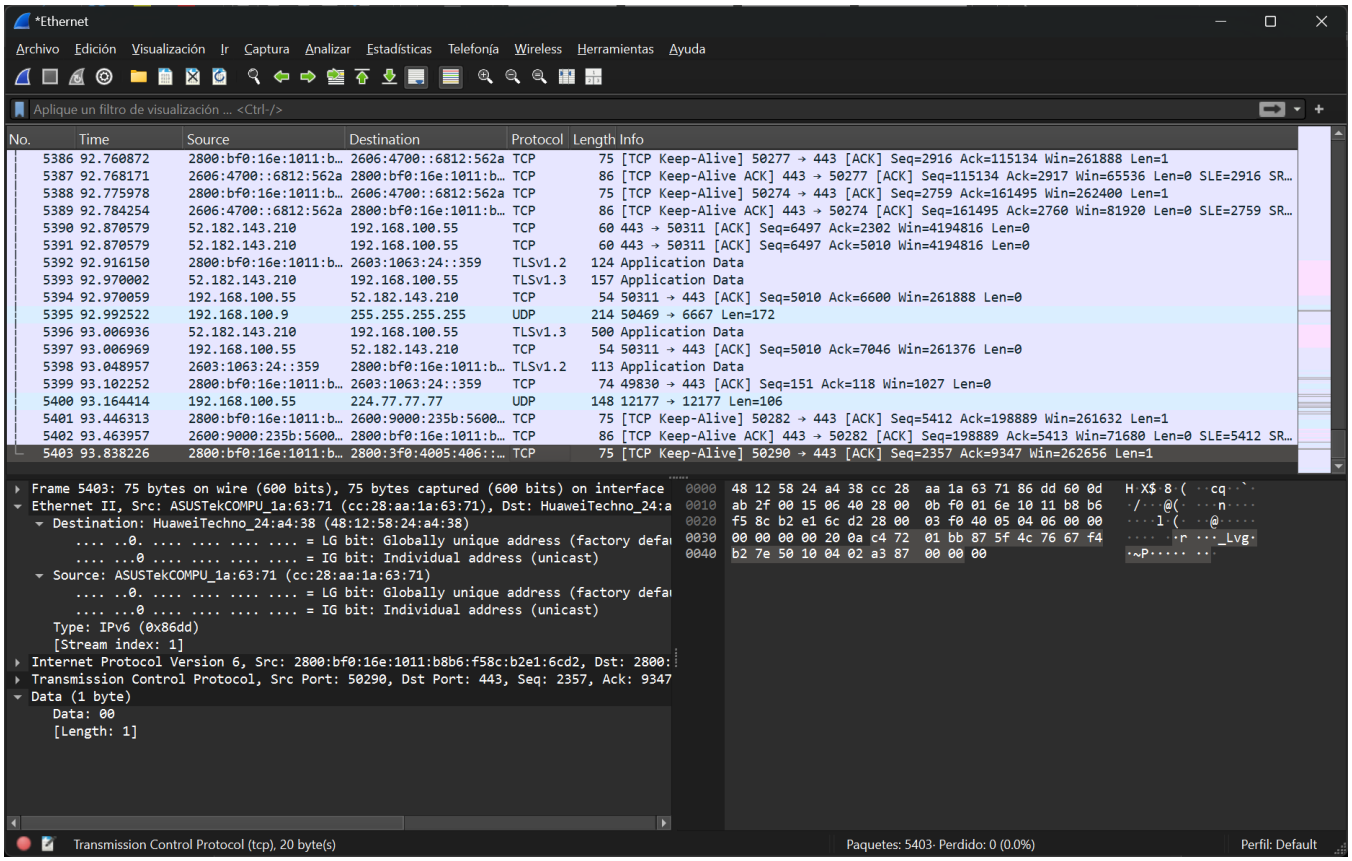
b. En la ventana del símbolo del sistema, hacer ping a www.cisco.com



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.22631.5189]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\danie>r ping www.cisco.com
"r" no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.

C:\Users\danie>ping ww.cisco.com
La solicitud de ping no pudo encontrar el host ww.cisco.com. Compruebe el nombre y
vuelva a intentarlo.

C:\Users\danie>ping www.cisco.com

Haciendo ping a e2867.dsca.akamaiedge.net [2600:1419:5600:387::b33] con 32 bytes de datos:
Respuesta desde 2600:1419:5600:387::b33: tiempo=16ms
Respuesta desde 2600:1419:5600:387::b33: tiempo=16ms
Respuesta desde 2600:1419:5600:387::b33: tiempo=19ms
Respuesta desde 2600:1419:5600:387::b33: tiempo=16ms

Estadísticas de ping para 2600:1419:5600:387::b33:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 16ms, Máximo = 19ms, Media = 16ms

C:\Users\danie>S
```

c. Dejar de capturar paquetes.

d. Examinar los nuevos datos del 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 de destino?

Fuente:

28:aa:1a:63:71

Destino:

48:12:58:24:a4:38

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

Fuente:

192.168.100.9

Destino:

255.255.255.255

Compare estas direcciones con las direcciones que recibió en el paso 6. La única dirección que cambió es la dirección IP de destino. ¿Por qué cambió la dirección IP de destino mientras que la dirección MAC permaneció igual?

La IP de destino es diferente ya que estamos apuntando a diferentes destinos. Sin embargo, cuando hacemos ping fuera de la red local, el paquete primero se envía al default Gateway, que es el primer salto para llegar a Internet y este se encargará de reenviar mi paquete al siguiente salto en el camino hacia www.cisco.com

Pregunta de reflexión

En Wireshark, no se muestra el campo de preámbulo de un encabezado de trama. ¿Qué contiene el preámbulo?

El **preámbulo** de una trama Ethernet **no se muestra en Wireshark** porque es eliminado por la tarjeta de red antes de entregar los datos al sistema operativo.

El preámbulo **contiene 8 bytes**:

- **7 bytes** de la secuencia: 10101010 (en binario), usados para **sincronizar** el receptor.
- **1 byte** llamado **Start Frame Delimiter (SFD)** con el valor 10101011, que indica el inicio real de la trama.

Estos bits permiten que el receptor se sincronice con la señal antes de recibir los datos útiles de la trama.