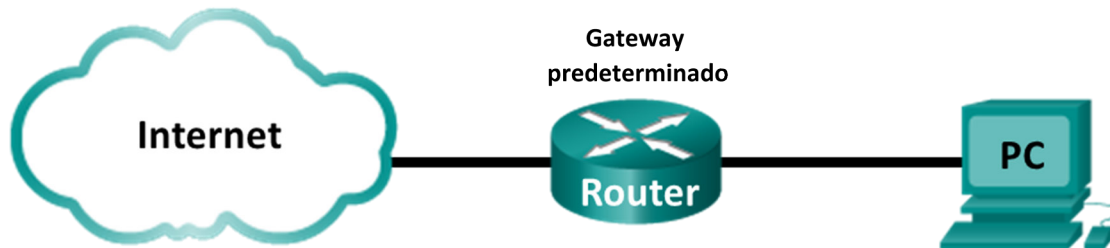


Práctica de laboratorio: Uso de Wireshark para examinar las tramas de Ethernet

Topología



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 7, 8 o 10 con acceso a Internet y Wireshark instalado)

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

La dirección IP de este equipo host es 192.168.1.147, y el gateway predeterminado tiene la dirección IP 192.168.1.1.

```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-C73CB0M
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
Physical Address. . . . . : 00-26-B9-DD-00-91
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d809:d939:110f:1b7f%20(Preferred)
IPv4 Address. . . . . : 192.168.1.147(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
```

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

En la siguiente captura de Wireshark, se muestran los paquetes generados por un ping que se hace de un equipo host a su gateway predeterminado. 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). La sesión comienza con una consulta ARP para obtener la dirección MAC del router del gateway seguida de cuatro solicitudes y respuestas de ping.

The screenshot shows the Wireshark interface with the packet capture filter `arp or icmp` applied. The packet list shows several packets, with packet 25 selected. The packet details pane shows the following structure:

- Frame 25: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
- Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: Dell_dd:00:91 (00:26:b9:dd:00:91)
- Address Resolution Protocol (request)

The hex dump and ASCII representation of the frame data are as follows:

```

0000  00 26 b9 dd 00 91 14 91 82 9f 6b 8c 08 06 00 01  .&.....k....
0010  08 00 06 04 00 01 14 91 82 9f 6b 8c c0 a8 01 01  .....k....
0020  00 00 00 00 00 00 c0 a8 01 93 00 00 00 00 00 00  .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
  
```

The status bar at the bottom indicates: Frame (frame), 60 bytes | Packets: 48 · Displayed: 12 (25.0%) | Profile: Default

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	Broadcast (ff:ff:ff:ff:ff:ff) (Difusión [ff:ff:ff:ff:ff:ff])	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.						
Dirección de origen	BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)	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: <table><tr><th>Valor</th><th>Descripción</th></tr><tr><td>0x0800</td><td>Protocolo IPv4</td></tr><tr><td>0x0806</td><td>Protocolo de resolución de direcciones (ARP)</td></tr></table>	Valor	Descripción	0x0800	Protocolo IPv4	0x0806	Protocolo de resolución de direcciones (ARP)
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?

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

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

¿Cuál es el identificador de proveedor (OUI) de la NIC del origen? _____

¿Qué porción de la dirección MAC corresponde al OUI?

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

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.

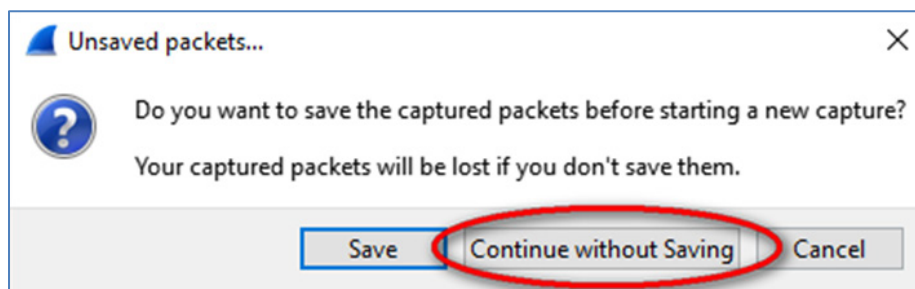
Paso 1: Determinar la dirección IP del gateway predeterminado de la PC

Abra una ventana del símbolo del sistema y emita el comando `ipconfig`.

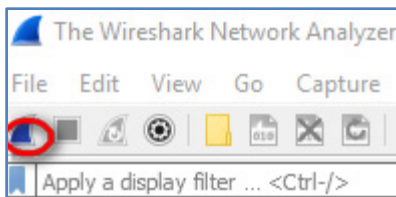
¿Cuál es la dirección IP del gateway predeterminado de la PC? _____

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

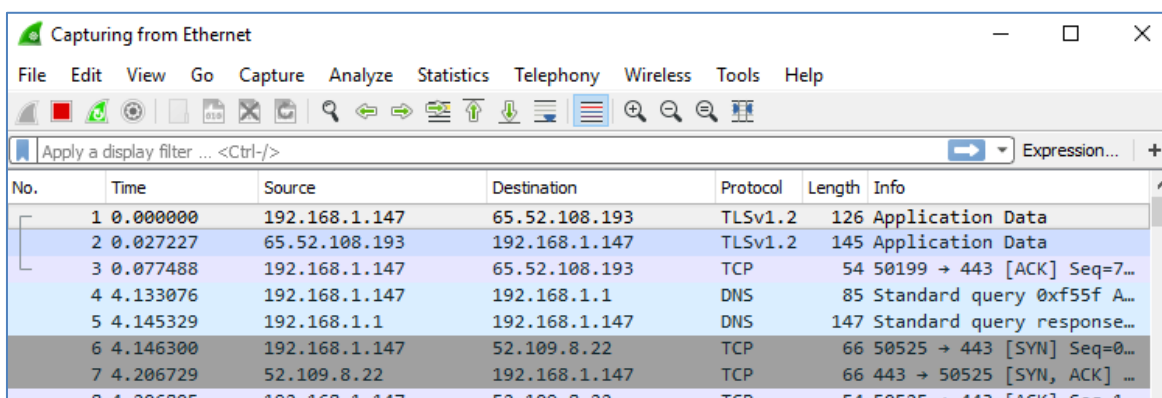
- a. Cierre Wireshark. No es necesario guardar los datos capturados.



- b. Abra Wireshark e inicie la captura de datos.



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

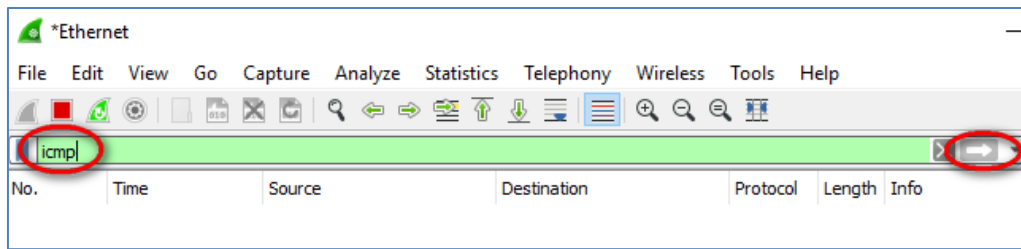


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.147	65.52.108.193	TLSv1.2	126	Application Data
2	0.027227	65.52.108.193	192.168.1.147	TLSv1.2	145	Application Data
3	0.077488	192.168.1.147	65.52.108.193	TCP	54	50199 → 443 [ACK] Seq=7...
4	4.133076	192.168.1.147	192.168.1.1	DNS	85	Standard query 0xf55f A...
5	4.145329	192.168.1.1	192.168.1.147	DNS	147	Standard query response...
6	4.146300	192.168.1.147	52.109.8.22	TCP	66	50525 → 443 [SYN] Seq=0...
7	4.206729	52.109.8.22	192.168.1.147	TCP	66	443 → 50525 [SYN, ACK] ...
8	4.206805	192.168.1.147	52.109.8.22	TCP	64	50525 → 443 [ACK] Seq=1...

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, sino lo que se muestra en 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.

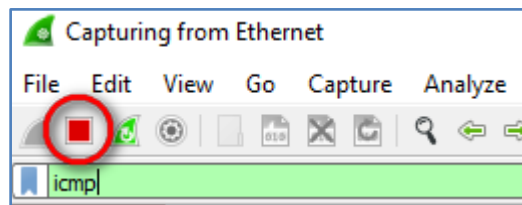


Paso 4: En la ventana del símbolo del sistema, hacer un ping al gateway predeterminado de la PC

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

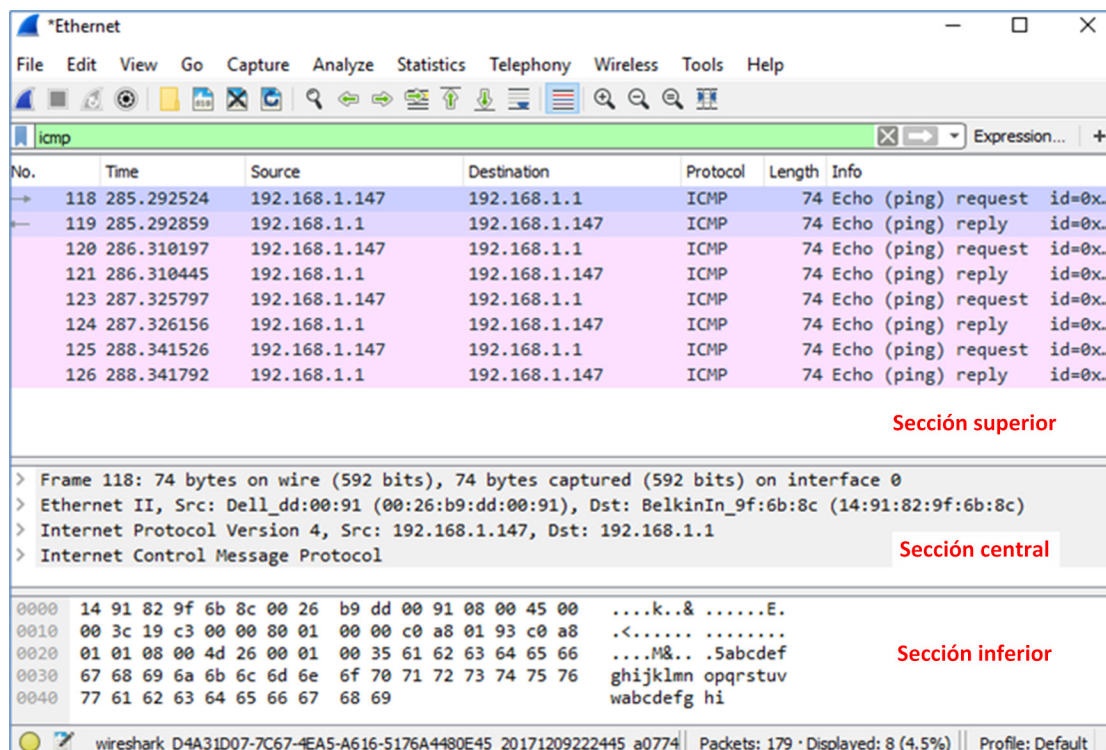
Paso 5: Dejar de capturar el tráfico de la NIC

Haga clic en el ícono **Stop Capture** (Detener captura) para dejar de capturar el tráfico.



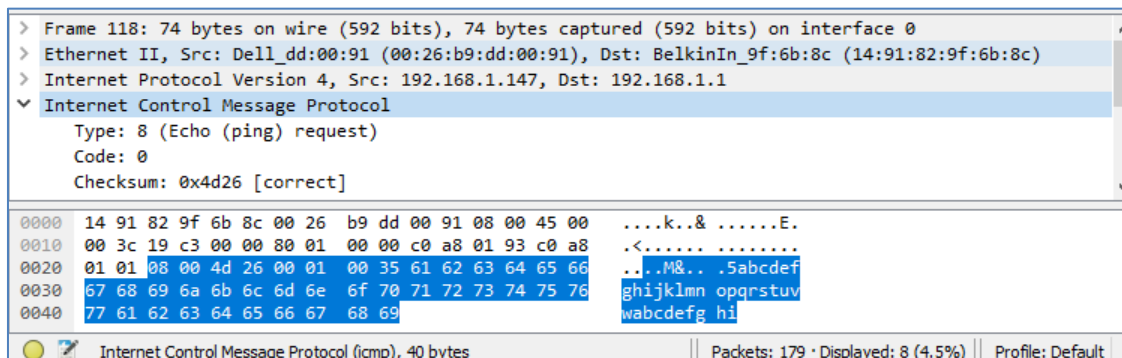
Paso 6: Examinar la primera solicitud de eco (ping) en Wireshark

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 en el paso 3, Wireshark debería mostrar la información de ICMP en el panel Packet List (Lista de paquetes), de manera similar a la del siguiente ejemplo.



- 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). Con esta acción, se debe resaltar la línea con color azul.
- Examine la primera línea del panel Packet Details (Detalles del paquete) de la parte central. En esta línea, se muestra la longitud de la trama (en el ejemplo, 74 bytes).
- 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? _____
 - ¿Cuál es la dirección MAC del gateway predeterminado? _____
- Puede hacer clic en el signo más (+) al principio de la segunda línea para obtener más información sobre la trama de Ethernet II. Observe que el signo más se transforma en un signo menos (-).
 - ¿Qué tipo de trama se muestra? _____
- 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? _____
 - ¿Cuál es la dirección IP de destino? _____

- 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).



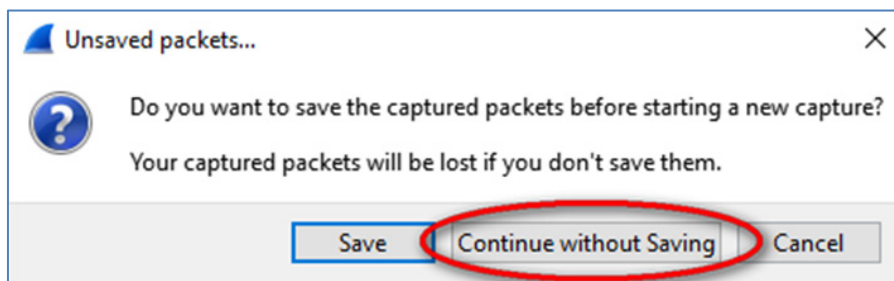
¿Qué texto muestran los últimos dos octetos resaltados? _____

- 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?

Paso 7: Reiniciar la captura de paquetes en Wireshark

Haga clic en el ícono **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).



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

Paso 9: Dejar de capturar paquetes

Paso 10: Examinar los nuevos datos del panel de Packet List (Lista de paquetes) de Wireshark

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

Origen: _____

Destino: _____

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

Origen: _____

Destino: _____

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?

Reflexión

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