Laboratorio: utilice Wireshark para examinar tramas de Ethernet

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 Parte 1, 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 (opción de sistema operativo con Wireshark instalado)
- Acceso a Internet

Instrucciones

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

En esta parte, examinará los campos de encabezado y el contenido de una trama 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

Linea en blanco, sin información adicional

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. (Para Linux y MAC OS, utilice el comando **ifconfig** en la terminal).

C:\> **ipconfig /all**

Ethernet adapter Ethernet:

Connection-specific DNS Suffix. :

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

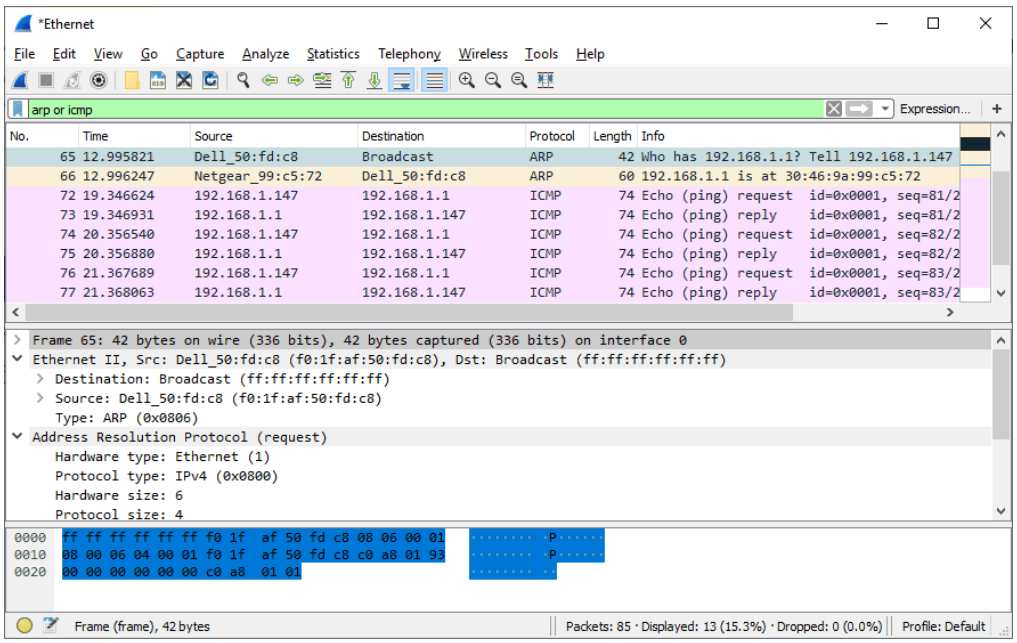
DHCP Server . . . . . : 192.168.1.1

<output omitted>

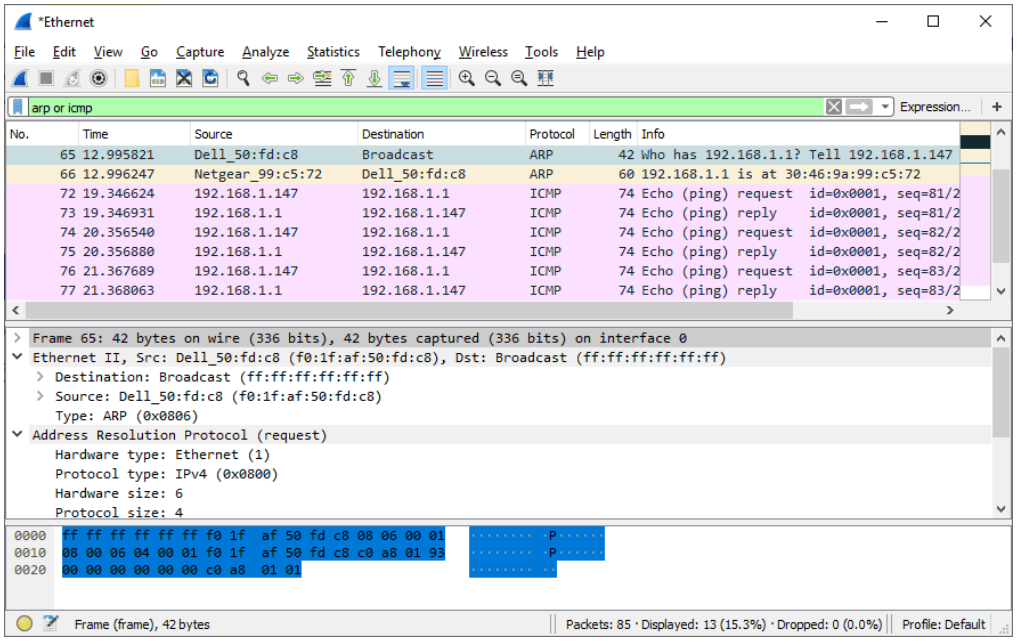
Paso 3: Examinar las tramas de Ethernet en una captura de Wireshark

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 aplicó un filtro (arp o icmp) a Wireshark para ver solo los protocolos ARP e 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	Broadcast	Direcciones de capa 2 para la trama. Cada dirección

Campo	Valor	Descripción
Dirección de origen	(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)	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.

Linea en blanco, sin información adicional

Preguntas:

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

Todos los hosts de la LAN reciben esta trama de difusión. El host que tiene la dirección IP 192.168.1.1 (gateway predeterminado) envía una respuesta de unidifusión al origen (equipo host). Esta respuesta contiene la dirección MAC de la NIC del gateway predeterminado.

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

el PC no puede enviar una solicitud de ping al host mientras no conozca su MAC, i pueda rellenar el frame header para esa solicitud ping. La difusión de ARP se utiliza para solicitar la dirección MAC del host con la dirección IP incluida en el ARP.

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

f 0:1 f:af:50:fd:c8.

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

Dell.

¿Qué porción de la dirección MAC corresponde al OUI?

Los primeros 3 octetos de la dirección MAC indican el OUI.

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

Puede variar, ene este caso es 99:c5:72

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

En esta parte, 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 de intérprete de comandos de Windows

Abra una ventana del símbolo del sistema y emita el comando **ipconfig**. (Para Linux y MAC OS, introduzca el comando **netstat -rn** en una terminal).

Pregunta:
Registrre la dirección IP de la puerta de enlace predeterminada de la PC

Cierre la ventana de intérprete de comandos de Windows

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

a. Abrir Wireshark para iniciar la captura de datos. Haga doble clic en la interfaz del dispositivo de red deseado con tráfico de red para iniciar la captura.

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

Abra una ventana de intérprete de comandos de Windows

En la ventana del símbolo del sistema, haga un ping a la puert de enlace predeterminada con la dirección IP registrada en el Paso 1.

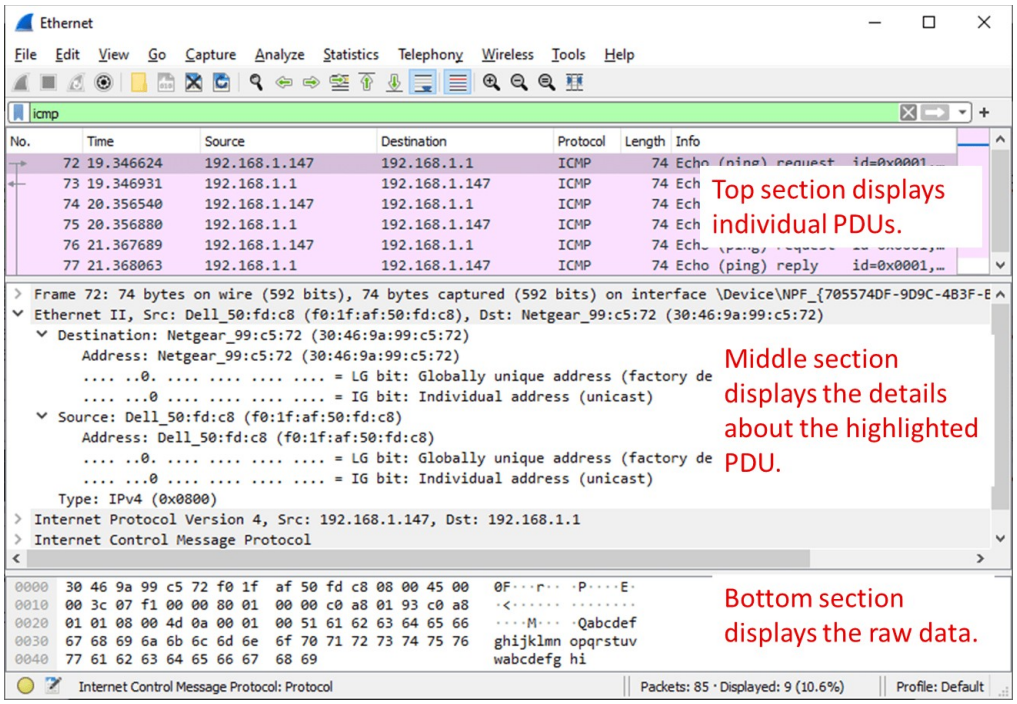
Cierre el símbolo del sistema de Windows.

Paso 5: Dejar de capturar el tráfico de la NIC

Haga click en el ícono de **Detener Captura de Paquetes** (el cuadro rojo) 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 la parte central 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.

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.

Preguntas:

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

la dirección MAC de la PC es f0:1f:af:50:fd:c8.

¿Cuál es la dirección MAC de la puerta de enlace predeterminada?

la dirección MAC de la puerta de enlace predeterminada es 30:46.9a:99:c5:72.

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.

Pregunta:
¿Qué tipo de trama se muestra?

0x0800 o un tipo de trama IPv4

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.

Preguntas:
¿Cuál es la dirección IP de origen?

la dirección IP de origen es 192.168.1.147.

¿Cuál es la dirección IP de destino?

la dirección IP de origen es 192.168.1.1.

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).

Pregunta:
¿Qué texto muestran los últimos dos octetos resaltados?

hola

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.

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

La dirección MAC de destino será para su PC.

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

c. Dejar de capturar paquetes.

d. Examinar los nuevos datos del panel de la lista de paquetes de Wireshark.

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

Fuente:

Esta será la dirección MAC de la PC.

Destino:

Esta debería ser la dirección MAC de la Puerta de Enlace Predeterminada.

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

Fuente:

sigue siendo la dirección IP de la PC.

Destino:

la dirección del servidor en www.cisco.com.

Comparen estas direcciones con las direcciones que recibió en el paso anterior. 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?

Las tramas de capa 2 nunca abandonan la LAN. Cuando se hace ping a un host remoto, el origen utiliza la dirección MAC del gateway predeterminado para el destino de la trama. El gateway predeterminado recibe el paquete, le quita la información de trama de capa 2 y crea un nuevo encabezado de trama con la dirección MAC del siguiente salto. Este proceso continúa de router a router hasta que el paquete llega a la dirección IP de destino.

Pregunta de reflexión

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

El campo de preámbulo contiene siete octetos de secuencias alternantes de “1010” y un octeto que indica el comienzo de una trama: 10101011.