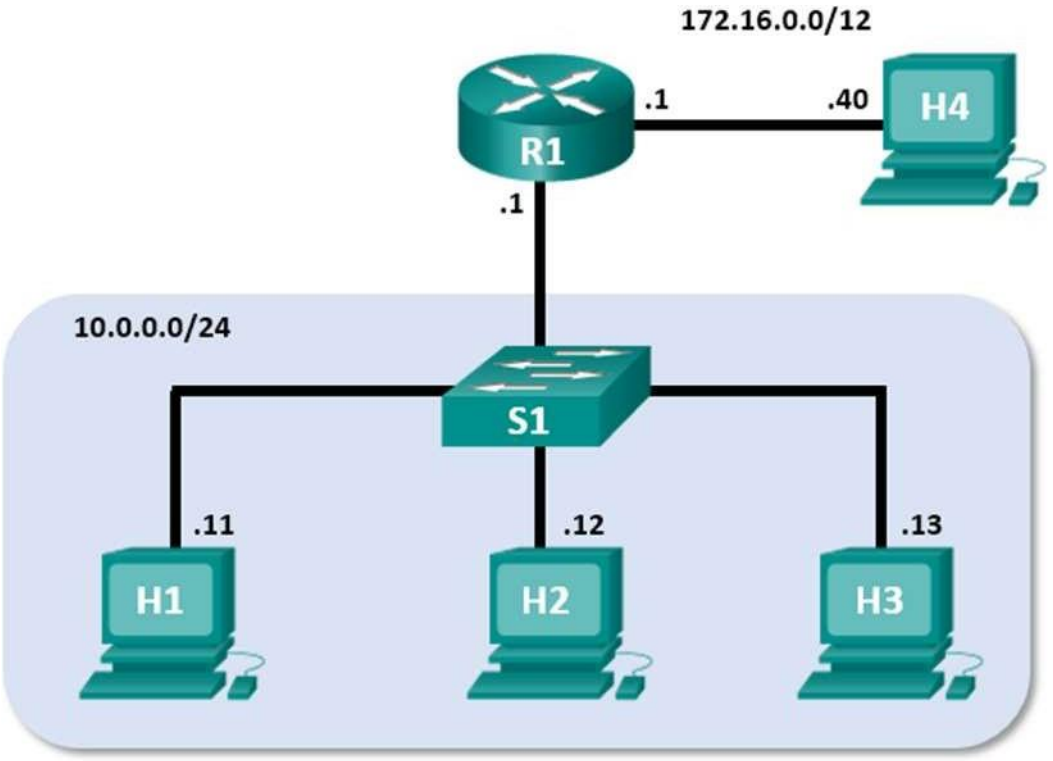
Práctica de laboratorio: Uso de Wireshark para examinar las tramas de Ethernet
Topología Mininet



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

- Máquina virtual (Virtual Machine) CyberOps Workstation

Instrucciones

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

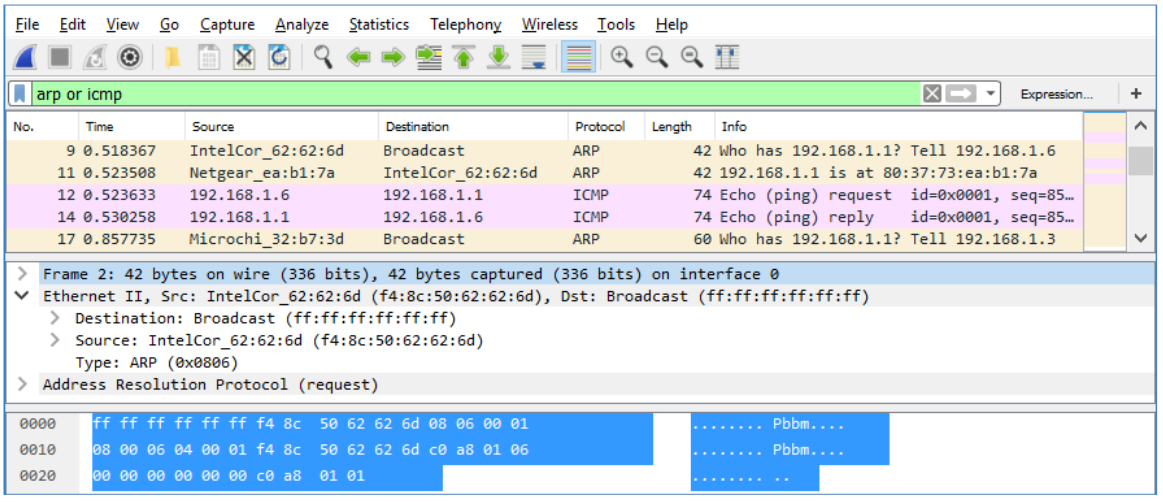
En la Parte 1, examinarán los campos de encabezado y el contenido de una trama de Ethernet II dada. Se utilizará una captura de Wireshark para examinar el contenido de esos campos.

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 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.



Paso 3: 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]) IntelCor_62:62:6d (f4:8c:50:62:62:6d)	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?

¿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: Examinar la configuración de red de H3

a. Abra sus estación de trabajo VM CyberOps e inicie sesión con las siguientes credenciales:

Nombre de usuario: **analyst** Contraseña: **cyberops**

b. Abra un emulador de terminales para iniciar Mininet e introduzca el siguiente comando. Cuando el sistema se lo solicite, introduzca **cyberops** como la contraseña.

```
[analyst@secOps ~]$ sudo ./lab.support.files/scripts/cyberops_topo.py
[sudo] contraseña para analyst:
```

c. En el cursor de Mininet, inicien ventanas del terminal en H3.

```
*** Starting CLI:
mininet> xterm H3
```

d. En el prompt en Node: H3, introducir **ip address** para verificar la dirección IPv4 y registrar la dirección MAC.

Host-interfaz	Dirección IP	Dirección MAC
H3-eth0		

e. En el cursor de Node: H3, introduzca **netstat -r** para mostrar la información del gateway predeterminado.

```
[root@secOps ~]# netstat -r
Kernel IP routing table
Destination Gateway Genmask Flags MSS Window irtt Iface
default 10.0.0.1 0.0.0.0 UG 0 0 0 H3-eth0
10.0.0.0 0.0.0.0 255.255.255.0 U 0 0 0 H3-eth0
```

¿Cuál es la dirección IP del gateway predeterminado correspondiente al host H3?

Paso 2: Borre la memoria caché de ARP en H3 y empiece a capturar el tráfico en H3-eth0.

a. En la ventana del terminal correspondiente a Node: H3, introduzca **arp -n** para mostrar el contenido del caché de ARP.

```
[root@secOps analyst]# arp -n
```

b. Si ya hay información de ARP en el caché, bórrela con el siguiente comando: **arp -d *dirección IP***. Repitan la operación hasta haber borrado toda la información en caché.

```
[root@secOps analyst]# arp -n
Address HWtype HWaddress Flags Mask Iface
10.0.0.11 ether 5a:d0:1d:01:9f:be C H3-eth0

[root@secOps analyst]# arp -d 10.0.0.11
Address HWtype HWaddress Flags Mask Iface
```

```
10.0.0.11 (incomplete) C H3-eth0
```

c. En la ventana del terminal correspondiente a Node: H3, abra Wireshark y comience la captura de paquetes para la interfaz H3-eth0.

```
[root@secOps analyst]# wireshark-gtk &
```

Paso 3: Hagan ping a H1 desde H3.

a. Desde el terminal de H3, haga ping al gateway predeterminado y deténgalo después de enviar 5 paquetes de solicitudes eco.

```
[root@secOps analyst]# ping -c 5 10.0.0.1
```

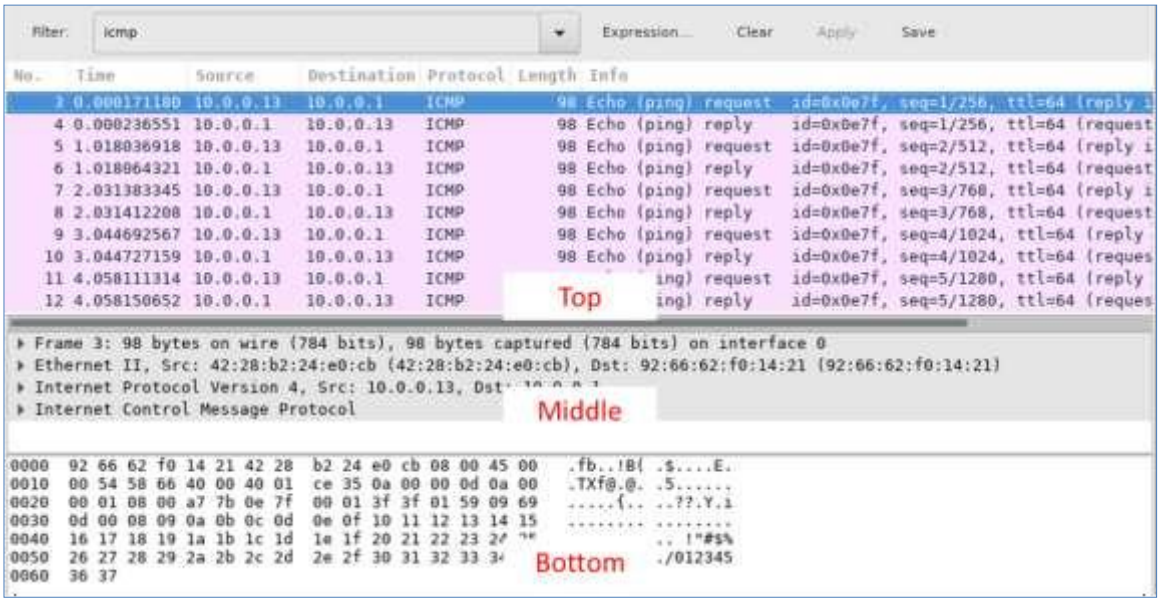
b. Cuando haya finalizado el ping, detenga la captura de Wireshark.

Paso 4: Filtrar Wireshark para que solamente se muestre el tráfico ICMP

Aplique el filtro **icmp** al tráfico capturado para que solo aparezca el tráfico ICMP en los resultados.

Paso 5: Examinar la primera solicitud de eco (ping) en Wireshark.

La ventana principal de Wireshark se divide en tres secciones: el panel Packet List 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 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.



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)**. Con esta acción, se debe resaltar la línea con color azul.

b. 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, 98 bytes).

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?

¿Cuál es la dirección MAC del gateway predeterminado?

d. Pueden hacer clic en la flecha que se encuentra al principio de la segunda línea para obtener más información sobre la trama de Ethernet II.

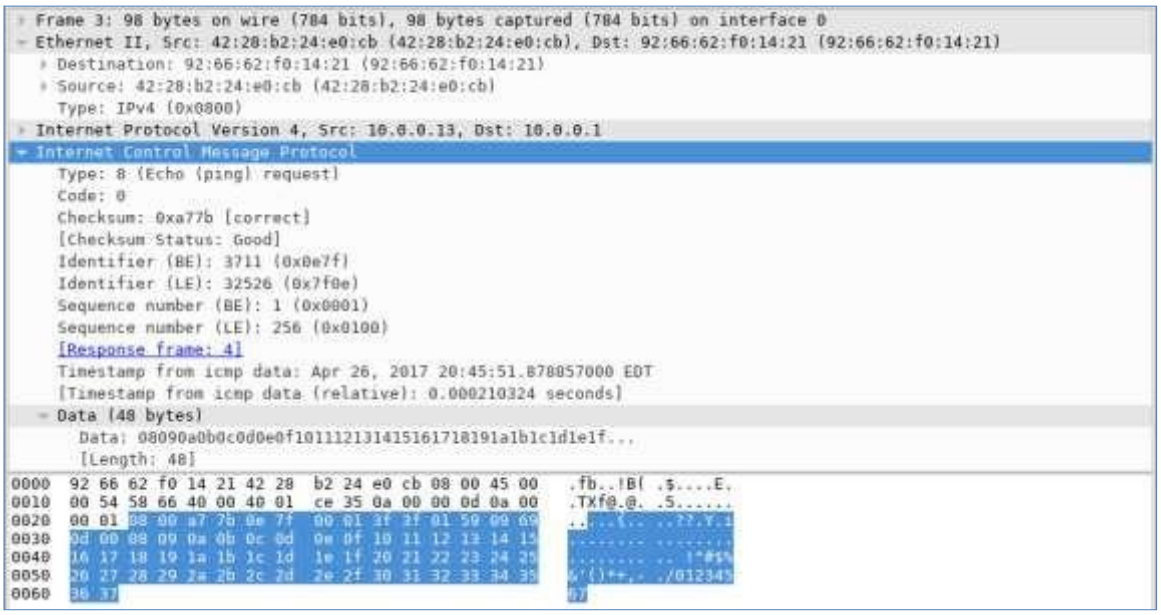
¿Qué tipo de trama se muestra?

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?

¿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 de la parte inferior. Haga clic en la línea **Internet Control Message Protocol (Protocolo de mensajes de control de Internet) (ICMP)** de la parte central y examine lo que se resalta en el panel Packet Bytes.



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 6: Iniciar una nueva captura en Wireshark

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 terminal de Nodo: H3, envíe 5 solicitudes echo a 172.16.0.40.

c. Deje de capturar paquetes cuando hayan terminado los pings.

Paso 7: 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:

Destino:

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

Fuente:

Destino:

Comparen estas direcciones con las direcciones que recibió en el paso 5. 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?