Práctica de Laboratorio - Ver Tráfico ARP en Wireshark

Objetivos

Parte 1 : Capturar y analizar datos de ARP en Wireshark

= Inicie y detenga la captura de datos del tráfico de ping a los hosts remotos.

= Localice la información de las direcciones IPv4 y MAC en las PDU capturadas.

= Analice el contenido de los mensajes ARP intercambiados entre los dispositivos en la LAN.

Parte 2: Ver las entradas de caché ARP en la PC

= Acceder a la línea de comandos de Windows.

= Use el comando arp de Windows para ver la caché de la tabla ARP local en la PC.

Aspectos básicos / situación

TCP/IP usa el protocolo de resolución de direcciones (ARP) para asignar una dirección IPv4 de capa 3 a una dirección MAC de capa 2. Cuando se transmite una trama Ethernet en la red, debe tener una dirección MAC de destino. Para detectar dinámicamente la dirección MAC de un destino conocido, el dispositivo de origen difunde una solicitud ARP en la red local. El dispositivo que está configurado con la dirección IPv4 de destino responde la solicitud con una respuesta ARP y la dirección MAC se registra en la caché ARP.

Cada dispositivo de la LAN mantiene su propia caché ARP. La caché ARP es un área pequeña en la RAM que conserva las respuestas ARP. Al abrir la caché ARP de una PC se puede ver la dirección IPv4 y la dirección MAC de cada dispositivo en la LAN con el que la PC ha intercambiado mensajes ARP.

Wireshark es un analizador de protocolos de software o una aplicación “husmeador de paquetes” que se utiliza para la solución de problemas de red, análisis, desarrollo de protocolo y software y educación. Cuando los flujos de datos van y vienen por la red, el detector "captura" cada unidad de datos del protocolo (PDU) y puede decodificar y analizar su contenido de acuerdo con las especificaciones de protocolo correspondientes.

Wireshark es una herramienta útil para cualquier persona que trabaja con redes y se puede usar con la mayoría de los laboratorios en los cursos de Cisco para realizar análisis de datos y solución de problemas. Esta práctica de laboratorio proporciona instrucciones para descargar e instalar Wireshark, aunque es posible que ya esté instalado. En este laboratorio, usará Wireshark para capturar intercambios ARP en la red local.

Recursos necesarios

= 1 PC (Elección de sistema operativo con Wireshark instalado)

= Se pueden usar PC o dispositivos móviles adicionales en una red de área local (LAN) para responder a las solicitudes de ping. Si no hay dispositivos adicionales en la LAN, la dirección de la puerta de enlace predeterminada se puede usar para responder a las solicitudes de ping.

Instrucciones

Parte 1: Capturar y analizar los datos ARP locales en Wireshark

En esta parte, hará ping a otra PC en la LAN y capturará solicitudes y respuestas ARP en Wireshark. También verá dentro de las tramas capturadas para obtener información específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados de paquetes para transmitir datos al destino.

Nota: Las instrucciones están escritas para PC que ejecutan el sistema operativo Windows para su referencia.

Paso 1: Recupere las direcciones de interfaz de la PC.

Para este laboratorio, deberá conocer la dirección IPv4 y la dirección MAC de la PC. (El comando **ifconfig** para Linux y MAC OS puede proporcionar resultados similares).

a. Navegue a una ventana del Símbolo del Sistema, escriba **ipconfig /all** en el indicador.

b. Observe qué adaptador de red está usando la PC para acceder a la red. Registre la dirección IPv4 y la dirección MAC (dirección física) de la interfaz de la PC.

C:\Users\Student> **ipconfig /all**

<output omitted>

Conexión de red inalámbrica del adaptador de LAN inalámbrico:

Connection-specific DNS Suffix. :

Description . . . . . : Intel(R) Centrino(R) Advanced-N 6205

Physical Address. . . . . : A4-AE-31-AD-78-4C

DHCP Enabled. . . . . : Yes

Autoconfiguration Enabled . . . . : Yes

Link-local IPv6 Address . . . . . : fe80::f9e7:e41d:a772:f993%11(Preferred)

IPv4 Address. . . . . : 192.168.1.8(Preferred)

Subnet Mask . . . . : 255.255.255.0

Lease Obtained. . . . . : Thursday, August 04, 2016 05:35:35 PM

Lease Expires . . . . : Friday, August 05, 2016 05:35:35 PM

Default Gateway . . . . : 192.168.1.1

DHCP Server . . . . : 192.168.1.1

DHCPv6 IAID . . . . : 245648945

DHCPv6 IAID . . . . : 00-01-00-01-1B-87-BF-52-A4-4E-31-AD-78-4C

DNS Servers . . . . : 192.168.1.1

NetBIOS over Tcpip. . . . . : Disabled

c. En la línea de comandos introduzca el comando **ipconfig**.

Pregunta:
Registre las direcciones IPv4 de la puerta de enlace predeterminada y las otras PC de la LAN.

la puerta de enlace predeterminada es 192.168.1.1 y la dirección IPv4 es 192.168.1.8.

Nota: Si utiliza un dispositivo móvil para hacer ping a la solicitud de respuesta, busque las direcciones para encontrar la dirección IP y la dirección MAC de Wi-Fi de su dispositivo móvil.

Nota: Si solo tiene un dispositivo, la dirección IP de la otra PC puede ser el gateway predeterminado.

Paso 2: Inicie Wireshark y comiene a capturar datos

a. En su PC, inicie **Wireshark**.

Nota: De manera alternativa, es posible que su instalación de Wireshark también le dé la opción Wireshark Legacy. Esto muestra Wireshark en la GUI anterior, más antigua pero bien conocida. El resto de esta práctica de laboratorio se completó con la GUI más nueva.

b. Después de que se inicie Wireshark , seleccione la interfaz de red que identificó con el comando **ipconfig**. Escriba **arp** en el cuadro del filtro. Esta selección configura Wireshark para que solo muestre los paquetes que son parte de los intercambios ARP entre los dispositivos de la red local. Haga clic con el botón derecho en la interfaz y haga clic en **Iniciar Captura** para comenzar la captura de datos.

La información comienza a desplazar hacia abajo la sección superior de Wireshark. Cada línea representa un mensaje que se está enviando entre un dispositivo de origen y uno de destino en la red.

c. En una ventana del Símbolo del Sistema, haga ping a la puerta de enlace predeterminada para probar la conectividad con la dirección de la puerta de enlace predeterminada que se identificó en el paso anterior. (Para Linux y MAC OS, utilice el comando **ping -c 4 192.168.1.1** en este ejemplo).

C:\Users\Student> **ping 192.168.1.1**

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=7ms TTL=64

Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Reply from 192.168.1.1: bytes=32 time=6ms TTL=64

Ping statistics for 192.168.1.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 7ms, Average = 4ms

d. Haga ping a las direcciones IPv4 de otras PC o dispositivos móviles en la LAN que registró en el paso anterior.

Nota: Si su otro dispositivo no responde a sus pings, es posible que el firewall esté bloqueando estas solicitudes. Busque **desbloquear el firewall** para su sistema operativo en Internet.

e. Deje de capturar datos haciendo clic en **Detener captura** (Stop Capture) (icono de cuadrado rojo) en la barra de herramientas.

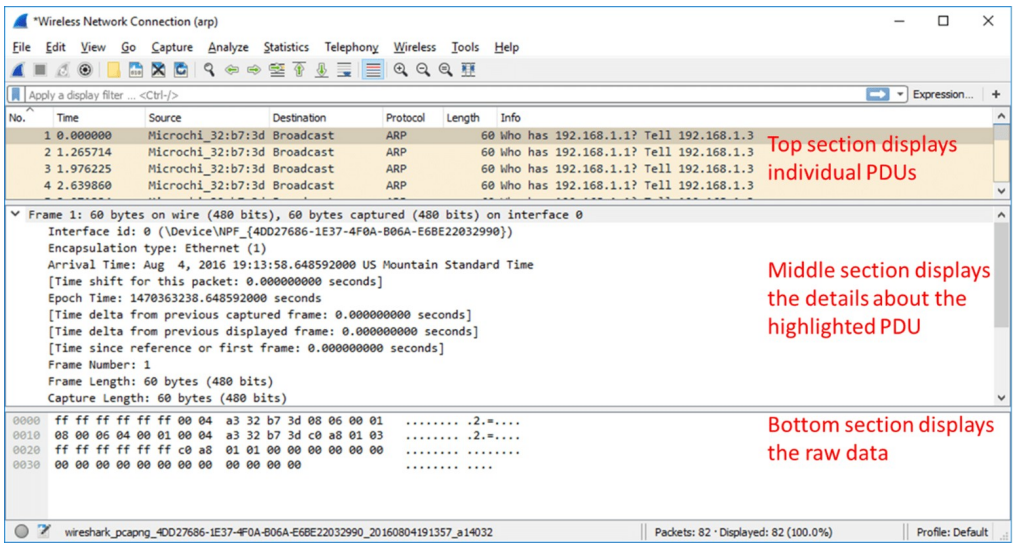
Paso 3: Examine los datos capturados

En este paso examinarán los datos que se generaron mediante las solicitudes de **ping** de la PC miembro de su equipo. Los datos de Wireshark se muestra en tres secciones:

1) La sección superior muestra la lista de tramas de PDU capturadas con un resumen de la información de paquetes IPv4.

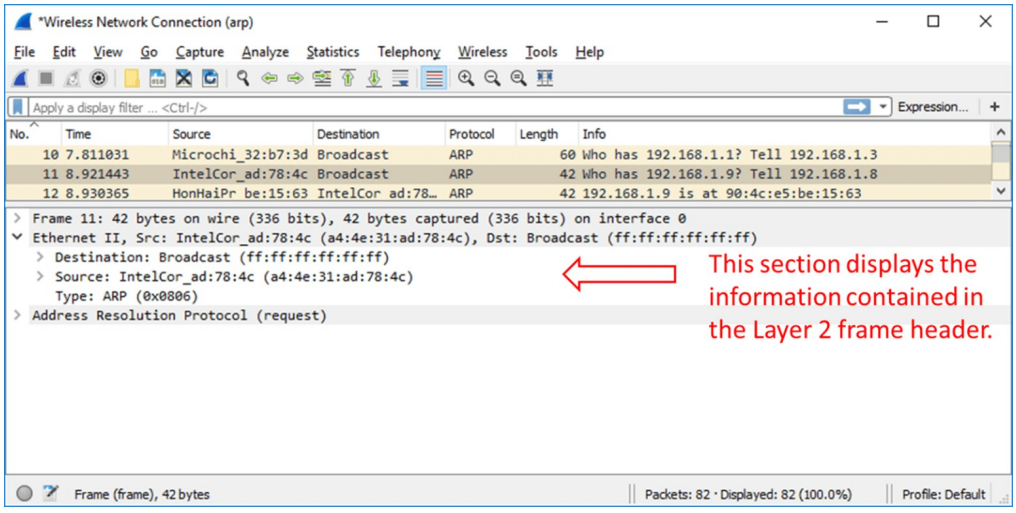
2) La sección del medio muestra la información de PDU de la trama seleccionada en la parte superior de la pantalla y separa una trama de PDU capturada por las capas del protocolo.

3) La sección inferior muestra los datos de cada capa sin formato. Los datos sin procesar se muestran en formatos hexadecimal y decimal.



b. Haga clic en una de las tramas ARP de la parte superior que tenga la dirección MAC de la PC como dirección de origen en la trama y “difusión” como el destino de la trama.

c. Con esta trama de PDU aún seleccionada en la sección superior, navegue hasta la sección media. Haga clic en la flecha que se encuentra a la izquierda de la fila Ethernet II para ver las direcciones MAC de origen y de destino.

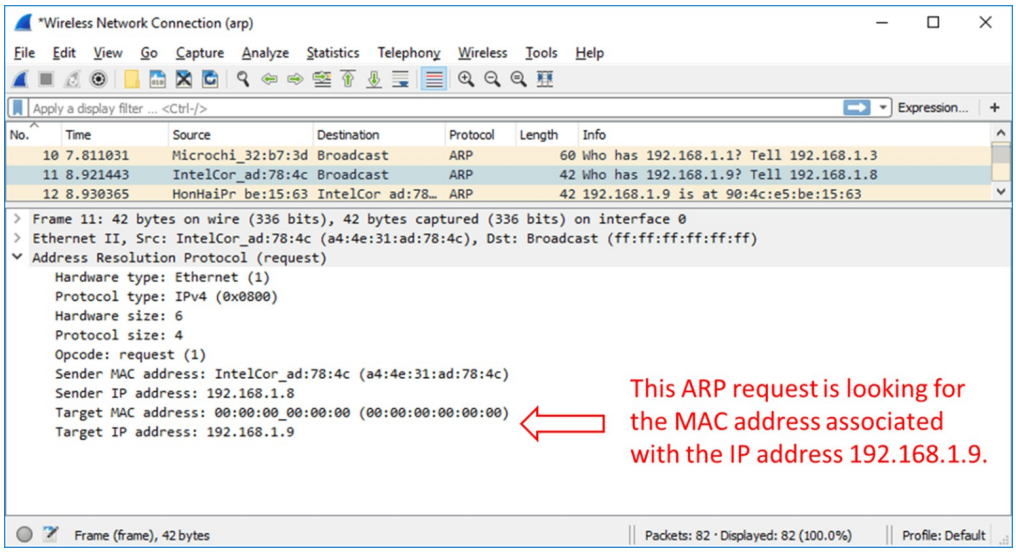


Pregunta:

¿La dirección MAC de origen coincide con la interfaz de su PC?

Sí.

d. Haga clic en la flecha que se encuentra a la izquierda de la fila Protocolo de resolución de direcciones (solicitud) para ver el contenido de la solicitud ARP.



Paso 4: Localice la trama de respuesta ARP que corresponde a la solicitud ARP que seleccionó.

a. Con la dirección IPv4 de destino en la solicitud ARP, localice la trama de respuesta ARP en la sección superior de la pantalla de la captura de Wireshark.

Pregunta:
¿Cuál es la dirección IPv4 del dispositivo de destino de su solicitud ARP?

192.168.1.9.

b. Seleccione la trama de respuesta en la sección superior del resultado de Wireshark. Es posible que deba desplazarse por la ventana para encontrar la trama de respuesta que coincida con la dirección IPv4 de destino identificada en el paso anterior. Amplíe las filas Ethernet II y Protocolo de resolución de direcciones (respuesta) en la sección del medio de la pantalla.

Preguntas:
¿La trama de respuesta ARP es una trama de difusión?

No.

¿Cuál es la dirección MAC de destino de la trama?

la dirección MAC de destino sería a4:4e:31:ad:78:4c

¿Es la dirección MAC de su PC?

Sí.

¿Qué dirección MAC es el origen de la trama?

El dispositivo que responde a la solicitud de ping.

c. Verifique que la dirección MAC coincida con la dirección MAC del dispositivo que ha seleccionado para responder a las solicitudes de ping.

Parte 2: Examine las entradas de la caché ARP en la PC.

Después de recibir la respuesta ARP en la PC, la asociación de la dirección MAC con la dirección IPv4 se almacena en la memoria caché en la PC. Estas entradas permanecerán en la memoria por un breve período (de 15 a 45 segundos); luego, si no se usan durante ese período, se borran de la caché. (**Nota**: busque en Internet para encontrar los comandos relacionados con ARP para una PC con sistema operativo Linux o MAC).

a. Abra una ventana de línea de comandos en la PC. En la línea de comandos ingrese **arp –a** y presione enter.

C:\Users\Student> **arp -a**

Interface: 192.168.1.8 --- 0xb

Internet Address Physical Address Type

192.168.1.1 00-37-73-ea-b1-7a dynamic

192.168.1.9 90-4c-e5-be-15-63 dynamic

192.168.1.13 a4-4e-31-ad-78-4c dynamic

224.0.0.5 01-00-5e-00-00-05 static

224.0.0.6 01-00-5e-00-00-06 static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.252 01-00-5e-00-00-fc static

224.0.0.253 01-00-5e-00-00-fd static

239.255.255.250 01-00-5e-7f-ff-fa static

255.255.255.255 ff-ff-ff-ff-ff-ff static

La salida del comando **arp –a** muestra las entradas que están en el caché de la PC. En el ejemplo, la PC tiene entradas para el gateway predeterminado (192.168.1.1) y para dos PC que se encuentran en la misma LAN (192.168.1.9 y 192.168.1.13).

Pregunta:
¿Cuál es el resultado de ejecutar el comando **arp – a** en tu PC?

El comando enumera los enlaces de direcciones MAC a IPv4 conocidos.

b. El comando **arp** en la PC con Windows tiene otra función. Introduzca **arp /?** en el símbolo del sistema y presione enter. Las opciones del comando **arp** le permiten ver, agregar y eliminar entradas de la tabla ARP si es necesario.

Pregunta:
¿Qué opción elimina una entrada de la caché ARP?

arp -d

c. ¿Cuál sería el resultado de emitir el comando **arp –d ***?

Eliminaría las asignaciones de direcciones actuales en la caché ARP.

Reflexión

1. ¿Cuál es el beneficio de mantener las entradas de la caché ARP en memoria en la computadora de origen?

El PC revisa siempre su caché local antes de solicitar información de otros dispositivos en la red. La caché ARP retiene las asociaciones de direcciones obtenidas dinámicamente correspondientes a un período breve. Cuando se intercambia tráfico a menudo entre el origen y el destino, la caché ARP evita que el host difunda solicitudes ARP innecesariamente.

2. Si la dirección IPv4 de destino no se encuentra en la misma red que el host de origen, ¿qué dirección MAC se usará como dirección MAC de destino en la trama?

El PC usará la dirección MAC de la puerta de enlace predeterminada.