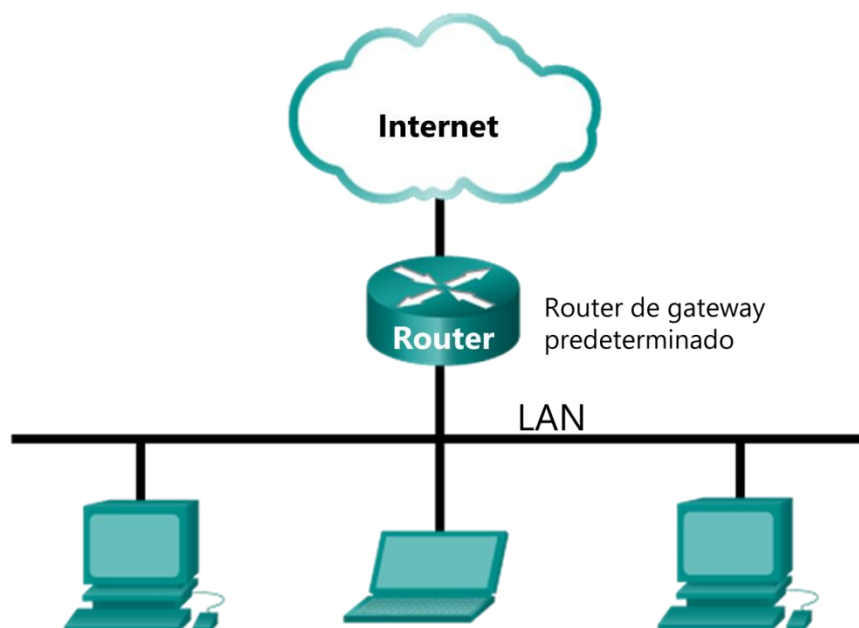


Laboratorio: Protocolo de resolución de direcciones (ARP)

Topología



Objetivos

Parte 1: Descargar e instalar Wireshark

Parte 2: Capturar y analizar datos de ARP en Wireshark

- Iniciar y detener la captura de datos del tráfico de ping a los hosts remotos.
- Localizar la información de las direcciones IPv4 y MAC en las PDU capturadas.
- Analizar el contenido de los mensajes ARP intercambiados entre los dispositivos en la LAN.

Parte 3: Ver las entradas de caché ARP en la PC

- Ingresar a la línea de comandos de Windows.
- Usar 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 con Windows 10 y acceso a Internet
- Se usarán PC adicionales en una red de área local (LAN) para responder las solicitudes **ping**. Si no hay PC adicionales en la LAN, la dirección del gateway predeterminado se usará para responder las solicitudes **ping**.

Parte 1: Descargar e instalar Wireshark

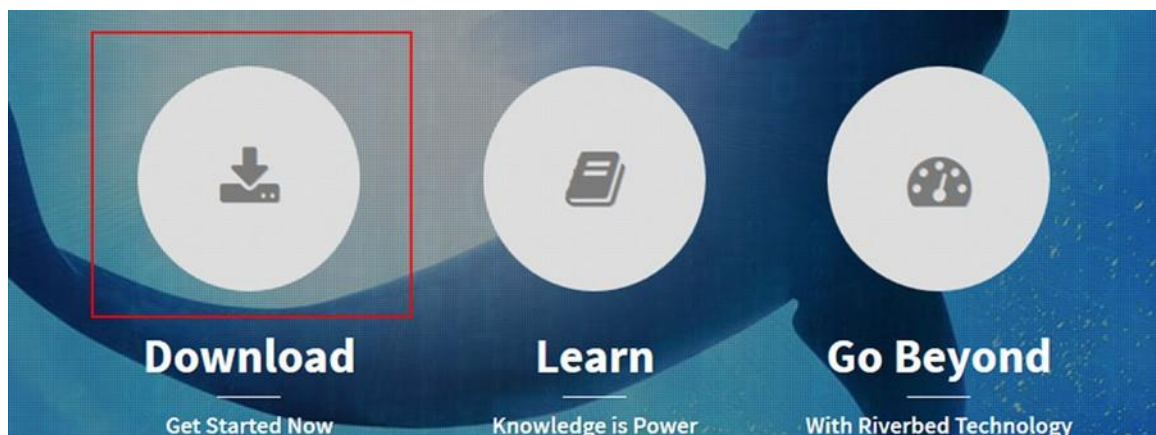
Wireshark se convirtió en el programa detector de paquetes estándar del sector que utilizan los ingenieros de redes. Este software de código abierto está disponible para muchos sistemas operativos diferentes, incluidos Windows, MAC y Linux.

Si Wireshark ya está instalado en la PC, puede omitir la parte 1 e ir directamente a la parte 2. Si Wireshark no está instalado en la PC, consulte con el instructor acerca de la política de descarga de software de la academia.

Paso 1: Descargue Wireshark.

Wireshark se puede descargar en www.wireshark.org.

Haga clic en **Download (Descargar)**.



Elija la versión de software que necesita según la arquitectura y el sistema operativo de la PC. Por ejemplo, si tiene una PC de 64 bits con Windows, seleccione **Instalador de Windows (64 bits)**.

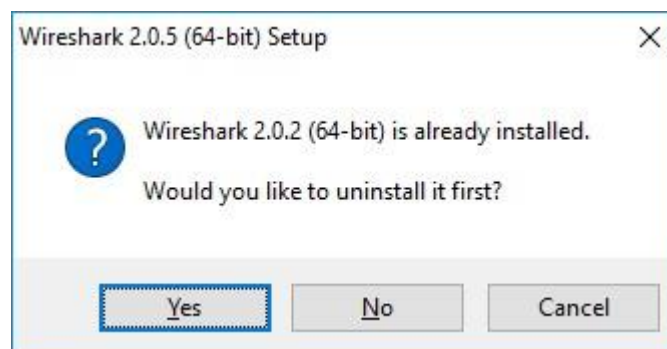


Después de realizar la selección, comienza la descarga. Haga clic en **Guardar archivo**, si aparece un mensaje de confirmación. La ubicación del archivo descargado depende del navegador y del sistema operativo que utiliza.

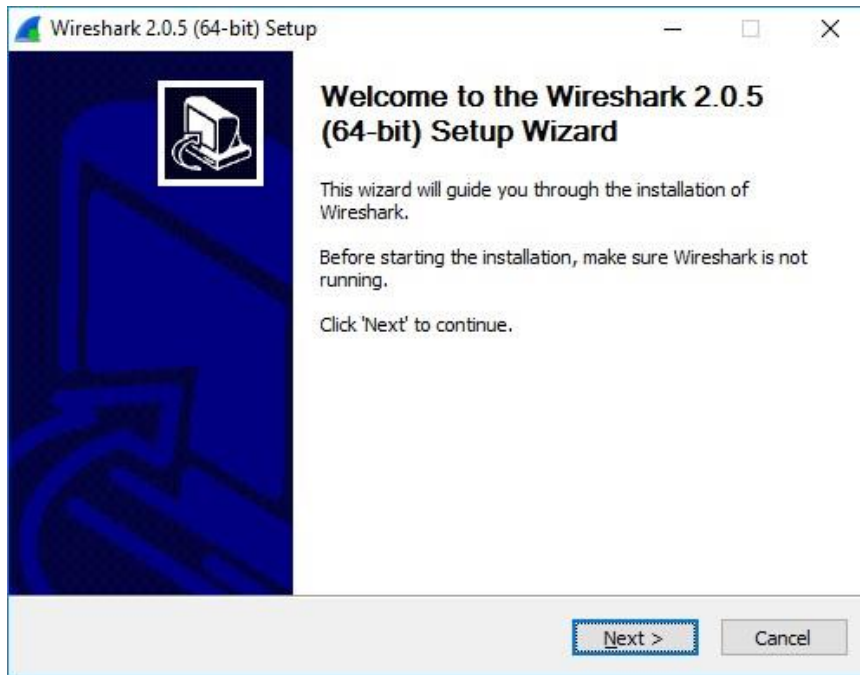
Para los usuarios de Windows, la ubicación predeterminada es la carpeta **Descargas**.

Paso 2: Instale Wireshark.

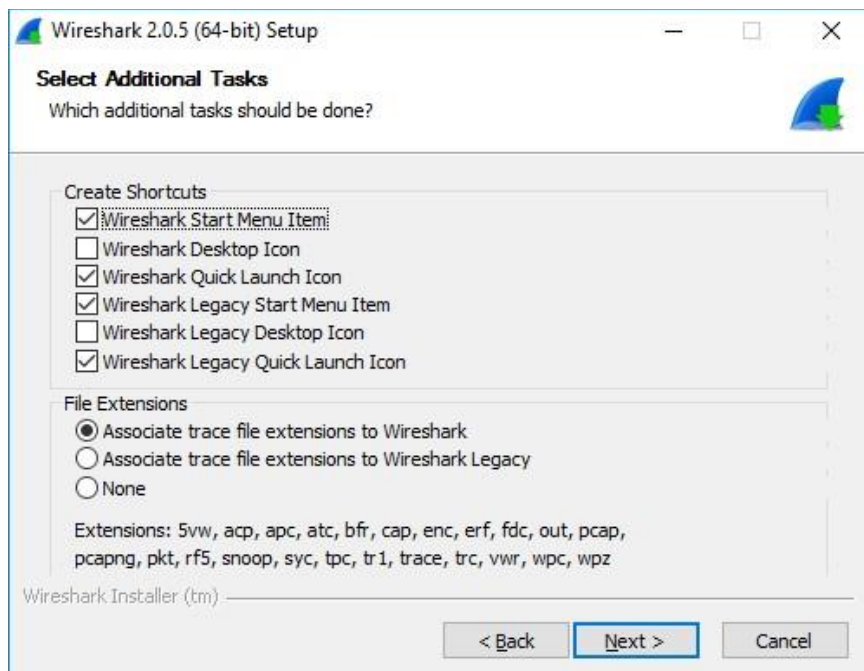
- El archivo descargado se llama **Wireshark-win64-x.x.x.exe**, donde **x** es el número de versión. Haga doble clic en el archivo para iniciar el proceso de instalación. En este ejemplo es la versión 2.0.5.
- Responda los mensajes de seguridad que aparezcan en la pantalla. Si ya tiene una copia de Wireshark en la PC, se le solicitará desinstalar la versión anterior antes de instalar la versión nueva. Se recomienda eliminar la versión anterior de Wireshark antes de instalar otra versión. Haga clic en **Yes** (Sí) para desinstalar la versión anterior de Wireshark.



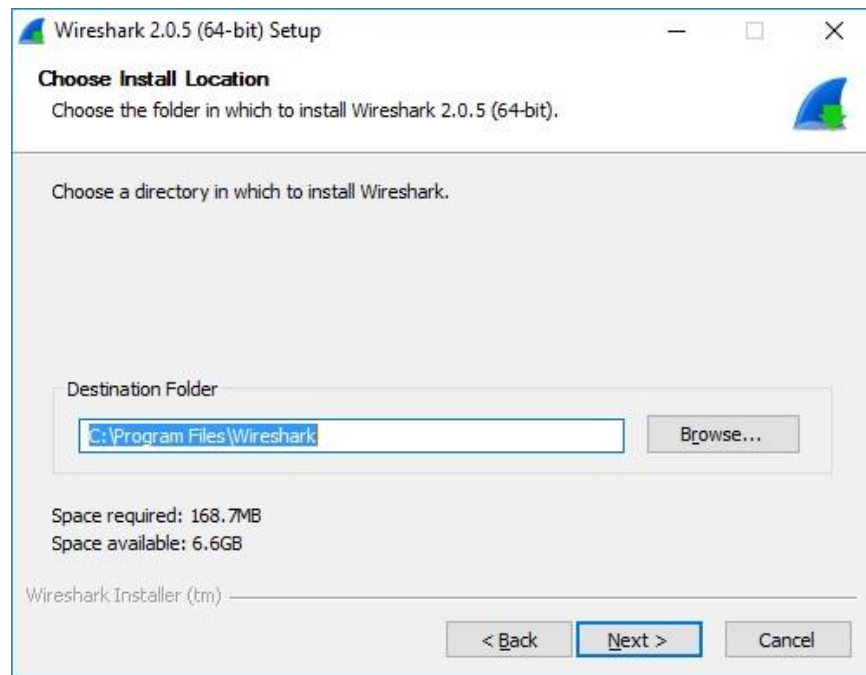
- Si es la primera vez que instala Wireshark, o si lo hace después de haber completado el proceso de desinstalación, navegue hasta el asistente para instalación de Wireshark. Haga clic en **Siguiente**.



- d. Continúe avanzando por el proceso de instalación. Haga clic en **I Agree** (Acepto) cuando aparezca la ventana del acuerdo de licencia.
- e. Guarde la configuración predeterminada en la ventana Elegir componentes y haga clic en **Siguiente**.
- f. Elija las opciones de método abreviado que desee y, a continuación, haga clic en **Siguiente**.

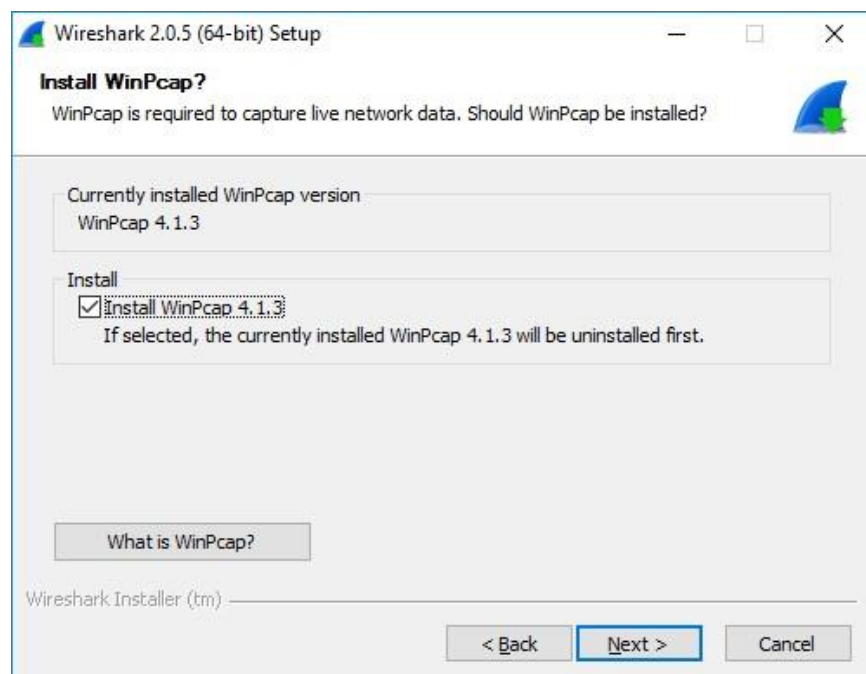


- g. Puede cambiar la ubicación de instalación de Wireshark, pero, a menos que tenga un espacio en disco limitado, se recomienda mantener la ubicación predeterminada.



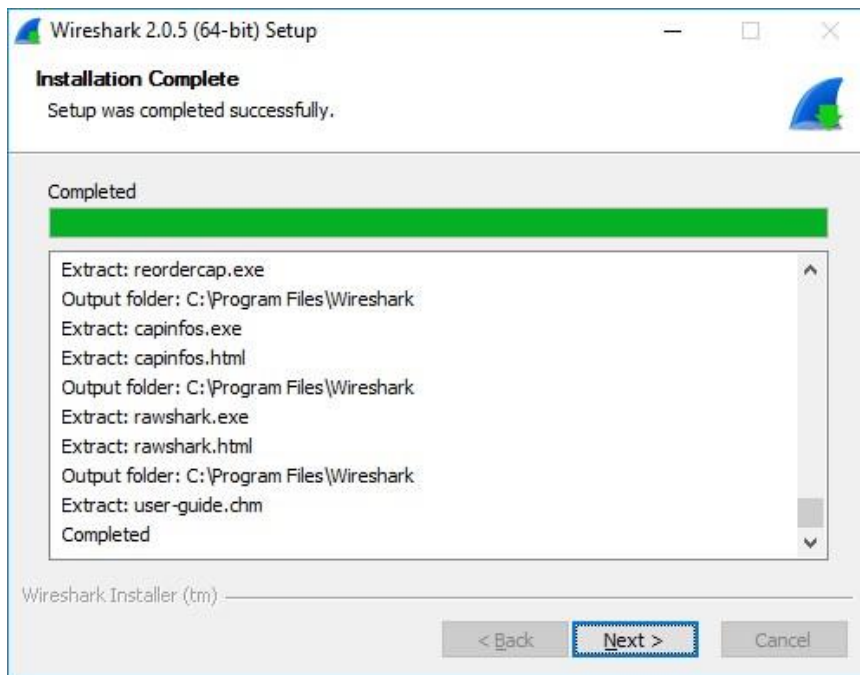
- h. Para capturar datos de la red activa, WinPcap debe estar instalado en la PC. Si WinPcap ya está instalado en la PC, la casilla de verificación Instalar estará desactivada. Si la versión de WinPcap que usted tiene instalada es anterior a la versión que viene con Wireshark, recomendamos instalar la versión más reciente. Para ello, haga clic en la casilla de verificación **Install WinPcap x.x.x** (Instalar WinPcap x.x.x, número de versión).

Finalice el asistente de instalación de WinPcap si instala WinPcap.



Nota: Es posible que se le ofrezca instalar USBPcap. La instalación de USBPcap es opcional.

- i. Wireshark comienza a instalar los archivos, y aparece una ventana independiente con el estado de la instalación. Haga clic en **Siguiente** cuando finalice la instalación.



- j. Haga clic en **Finalizar** para completar el proceso de instalación de Wireshark.



Parte 2: Capturar y analizar los datos ARP locales en Wireshark

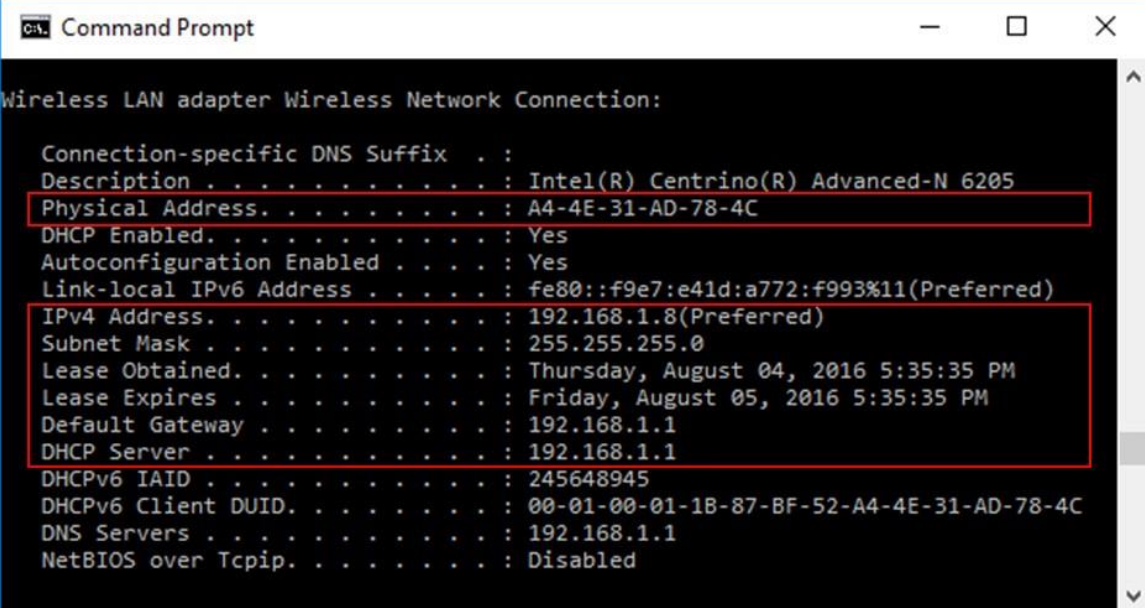
En la parte 2 de este laboratorio, hará ping a otra PC de la LAN y capturará las solicitudes y respuestas ARP en Wireshark. También verá dentro de las tramas capturadas para obtener información específica. Este análisis debe ayudar a aclarar de qué manera se utilizan los encabezados de paquetes para transmitir datos al destino.

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.

- a. Abra una ventana de comandos, escriba **ipconfig /all** y luego presione Intro.

- 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.



```
Command Prompt

Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6205
Physical Address. . . . . : A4-4E-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 5:35:35 PM
Lease Expires . . . . . : Friday, August 05, 2016 5:35:35 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 245648945
DHCPv6 Client DUID. . . . . : 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. Pida a un miembro del equipo la dirección IPv4 de su PC y díglele a esa persona la dirección IPv4 de la PC que usted está usando. En esta instancia, no proporcione su dirección MAC.

Registre las direcciones IPv4 del gateway predeterminado y las otras PC de la LAN.

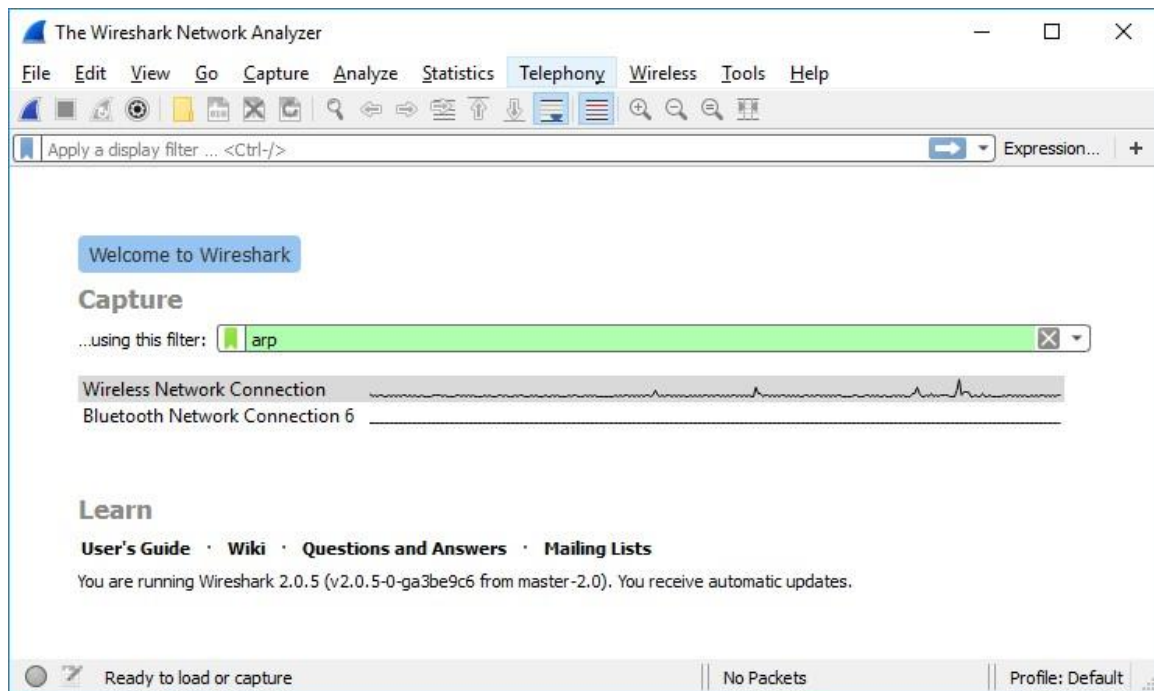
192.168.0.1

Paso 2: Inicie Wireshark y comience a capturar datos.


- a. En su PC, haga clic en **Inicio** y escriba **Wireshark**. Haga clic en **Wireshark Desktop App** cuando aparezca en la ventana de los resultados de la búsqueda.

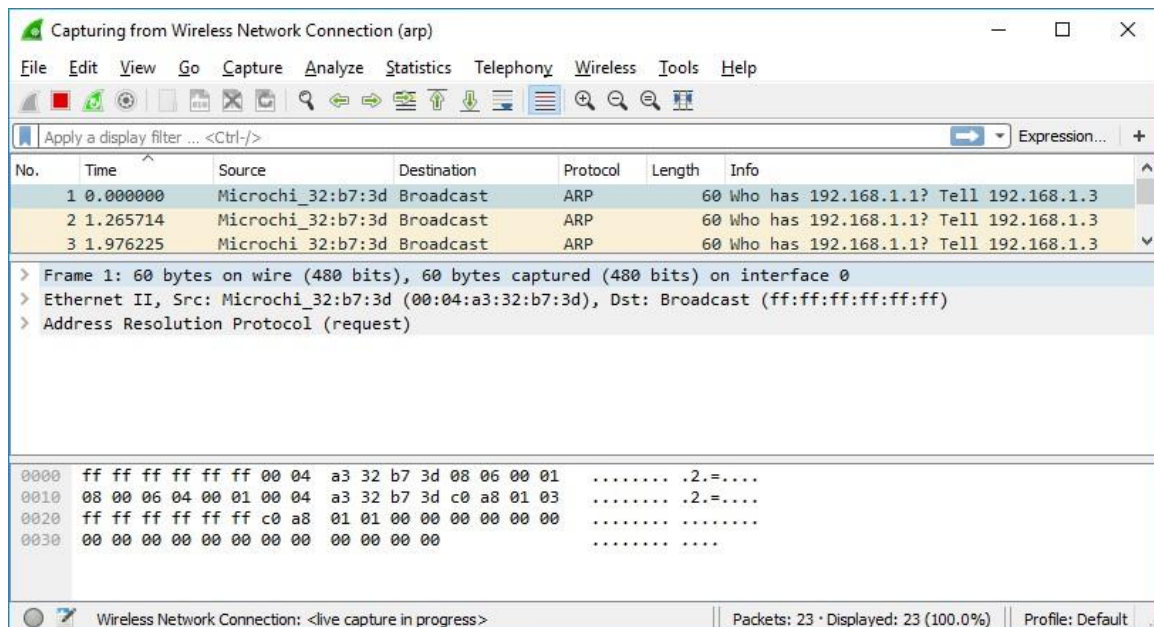
Nota: De manera alternativa, es posible que su instalación de Wireshark también le dé la opción Wireshark Legacy. Esto muestra Wireshark en la GUI anterior, más antigua pero bien conocida. El resto de este laboratorio se realizó con la GUI de Desktop App más nueva.

- 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.

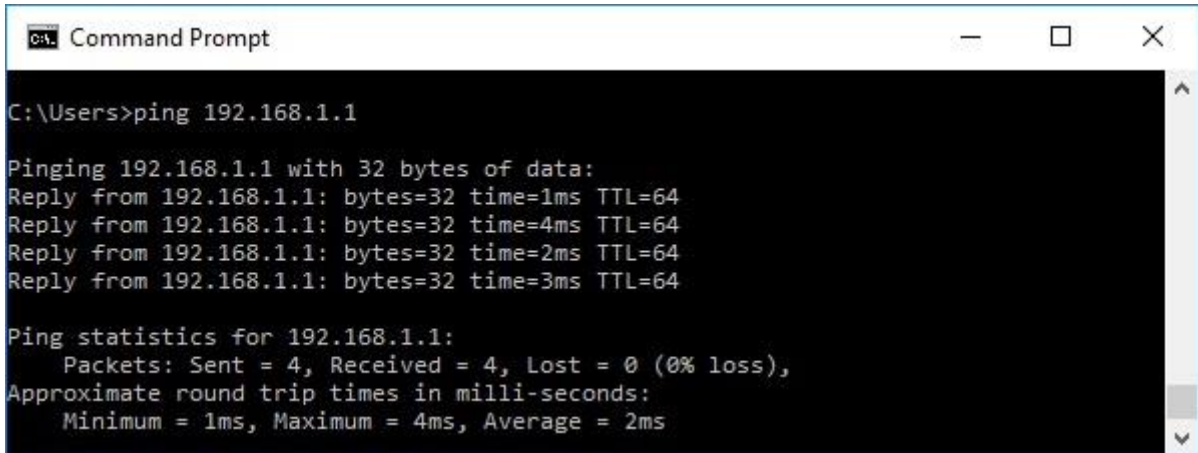


- c. Después de haber seleccionado la interfaz correcta e ingresado la información de filtro, haga clic en

Inicio () para comenzar a capturar datos. La información comienza a desplazarse 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.



- d. Abra una ventana de la línea de comandos. Use el comando **ping** para probar la conectividad con la dirección del gateway predeterminado que identificó en la parte 2, paso 1c.




```
C:\Users>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=4ms TTL=64
Reply from 192.168.1.1: bytes=32 time=2ms TTL=64
Reply from 192.168.1.1: bytes=32 time=3ms 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 = 4ms, Average = 2ms
```

- e. Envíe un comando ping a las direcciones IPv4 de las otras PC de la LAN que le proporcionaron a usted los miembros de su equipo.

Nota: Si la PC del miembro del equipo no responde a sus pings, es posible que se deba a que el firewall de la PC está bloqueando estas solicitudes. Pida ayuda al instructor si es necesario deshabilitar el firewall de la PC.

- f. Detenga la captura de datos haciendo clic en **Stop Capture** () (Detener captura) en la barra de herramientas.

Paso 3: Examine los datos capturados.

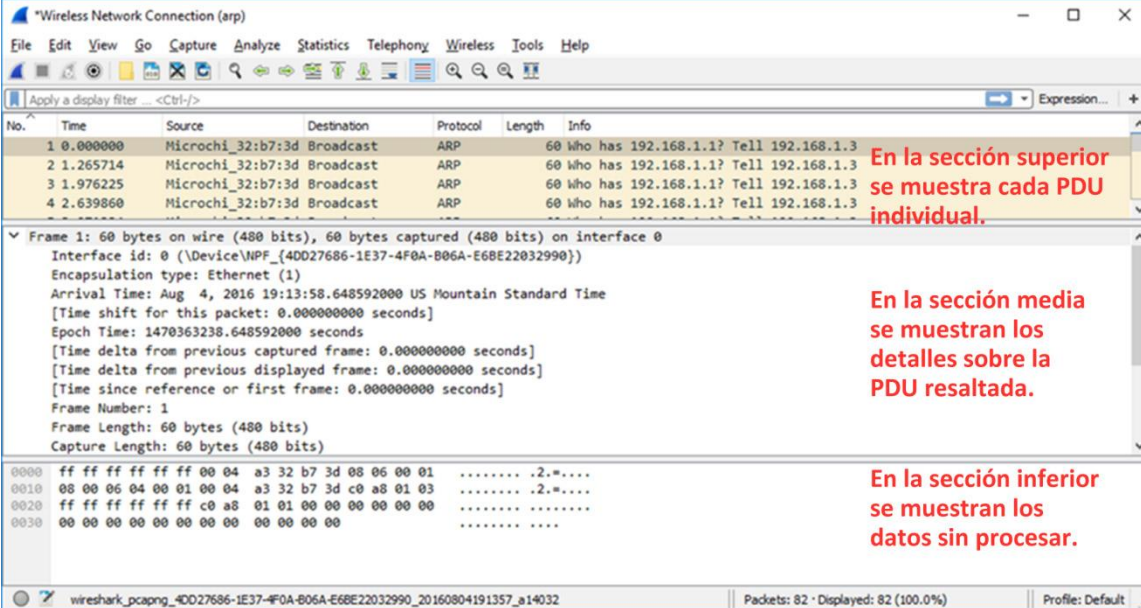
En el paso 3, examine los datos que generaron las solicitudes **ping** de la PC del miembro de su equipo. Los datos de Wireshark se muestra en tres secciones:

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

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.

Laboratorio: Protocolo de resolución de direcciones (ARP)

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

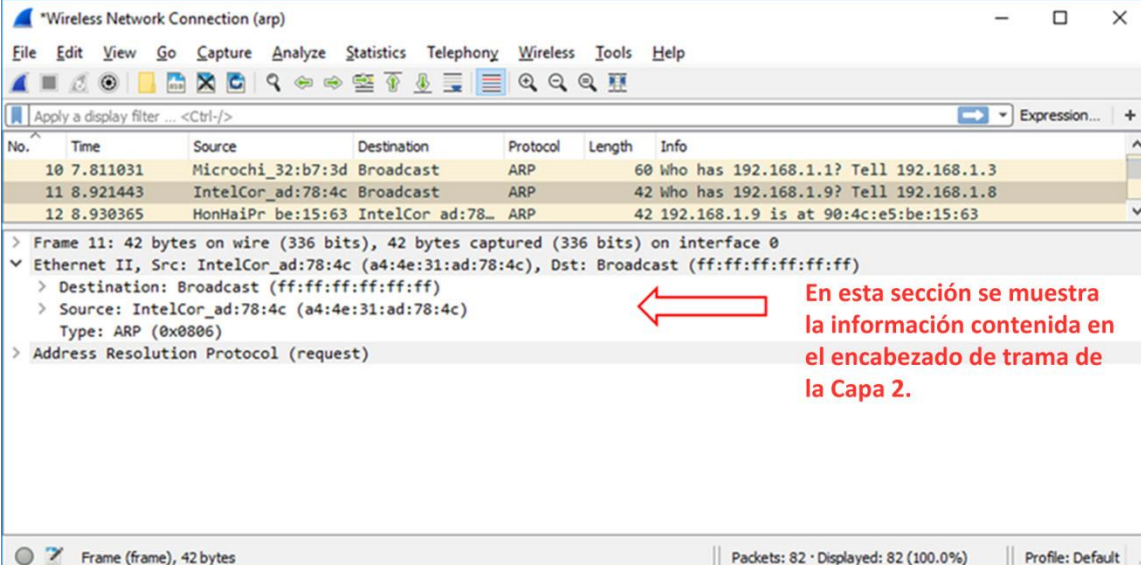


En la sección superior se muestra cada PDU individual.

En la sección media se muestran los detalles sobre la PDU resaltada.

En la sección inferior se muestran los datos sin procesar.

- 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.
- 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.

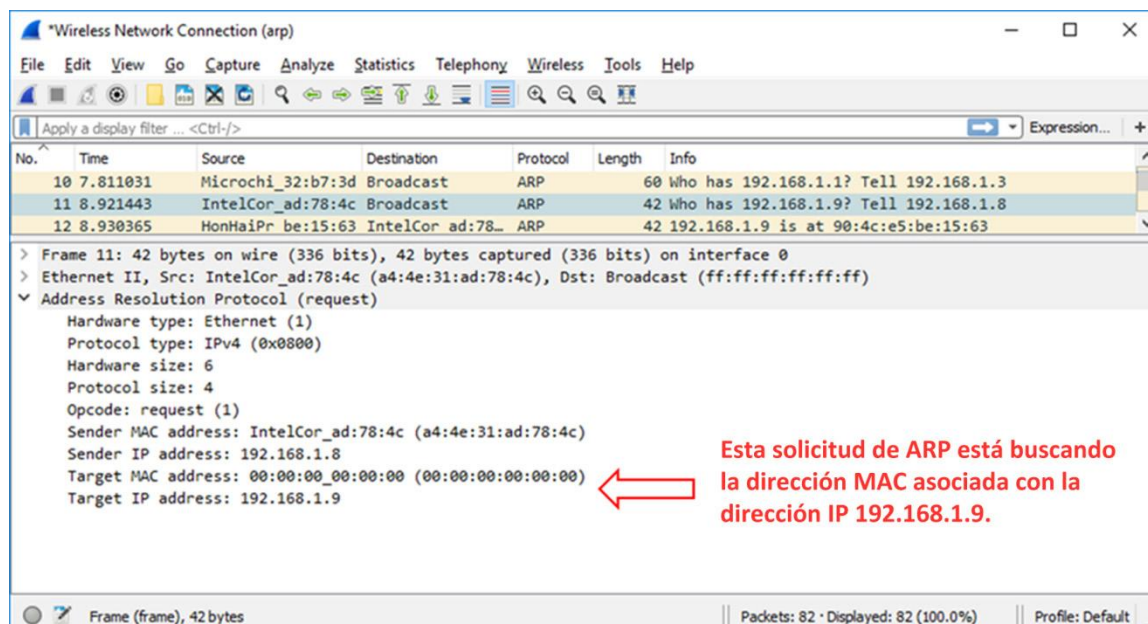


En esta sección se muestra la información contenida en el encabezado de trama de la Capa 2.

Laboratorio: Protocolo de resolución de direcciones (ARP)

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

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.



Esta solicitud de ARP está buscando la dirección MAC asociada con la dirección IP 192.168.1.9.

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

- 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.

¿Cuál es la dirección IPv4 del dispositivo de destino de su solicitud ARP? 192.168.0.7

- 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.

¿La trama de respuesta ARP es una trama de difusión? sí

¿Cuál es la dirección MAC de destino de la trama? e4:ff:18:38:82:6d ¿Es la dirección MAC de su PC? E4-B3-18-38-82-6E

¿Qué dirección MAC es el origen de la trama? E4-B3-18-38-82-6E

- Verifique con el miembro de su equipo que la dirección MAC coincida con la dirección de la PC.

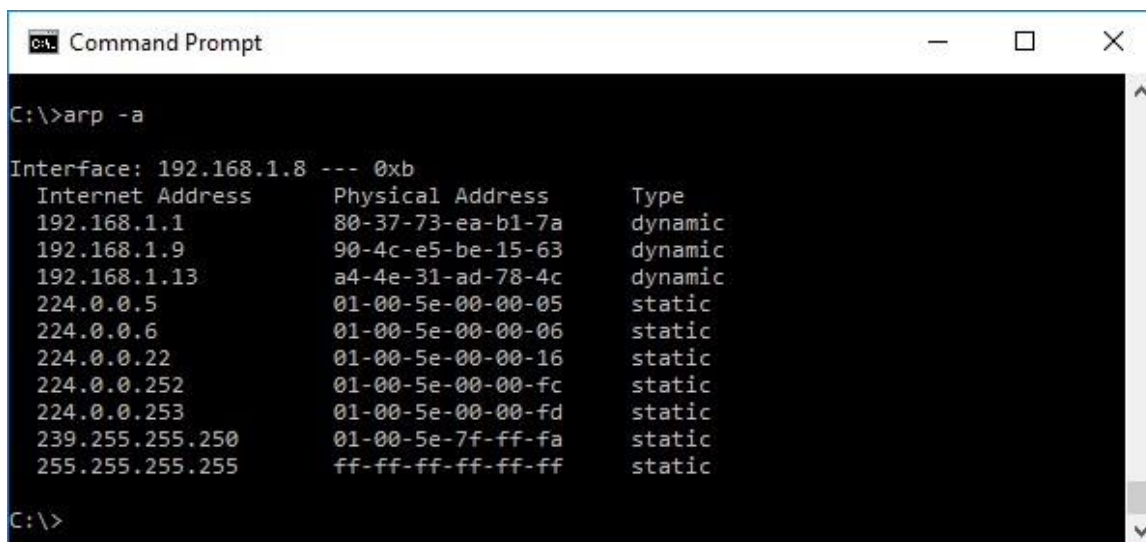
Parte 3: Examine las entradas de la caché ARP en la PC.

Laboratorio: Protocolo de resolución de direcciones (ARP)

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.

Paso 1: Vea las entradas de la caché ARP en una PC con Windows.

- Abra una ventana de línea de comandos en la PC. En la línea de comandos, escriba **arp -a** y presione Enter.



```
C:\>arp -a

Interface: 192.168.1.8 --- 0xb
Internet Address      Physical Address      Type
192.168.1.1           80-37-73-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

C:\>
```

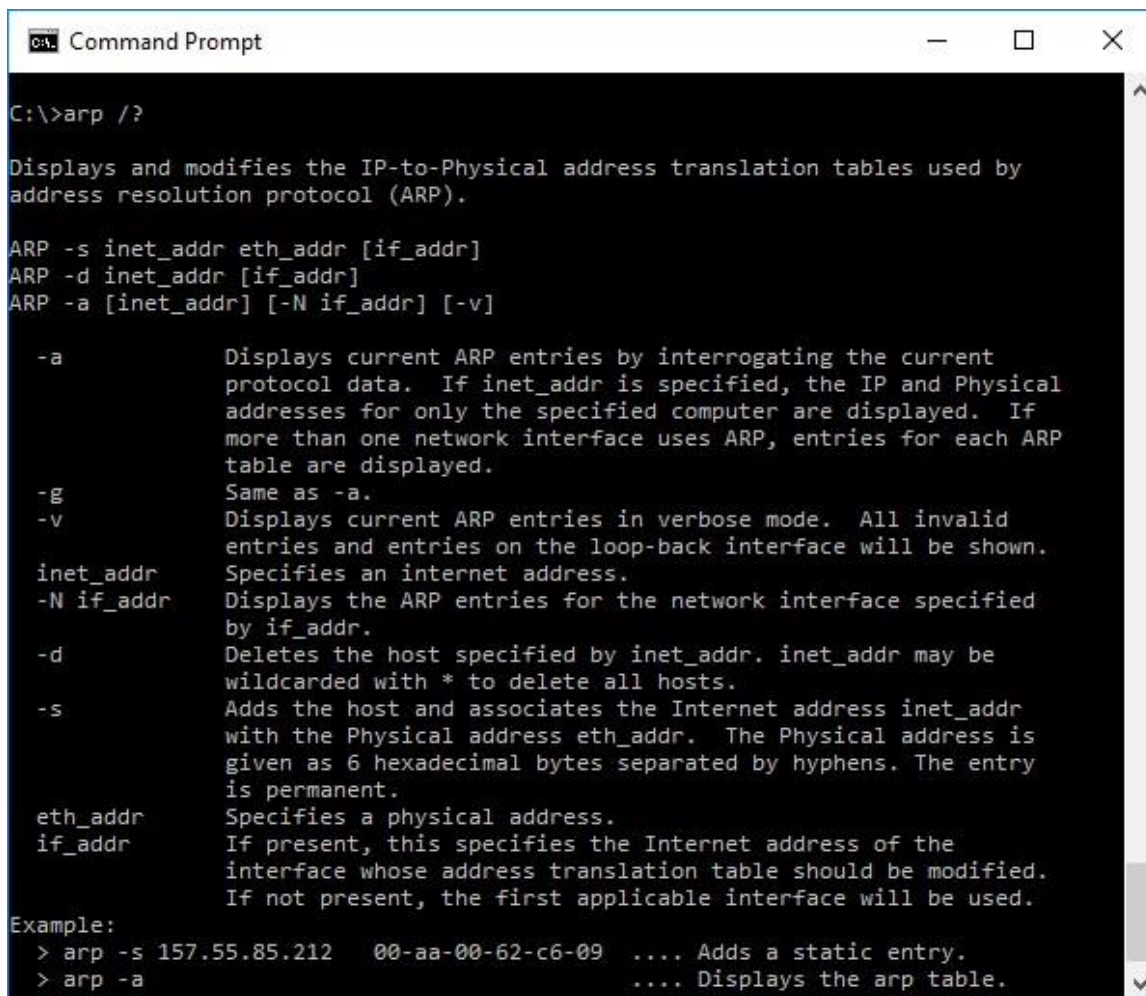
El resultado del comando **arp -a** son las entradas que se encuentran en la caché de la PC. En el ejemplo, la PC tiene entradas para el gateway predeterminado (192.168.1.1) y para dos PC que se encuentran en la misma LAN (192.168.1.9 y 192.168.1.13).

¿Qué produce el **arp -a** en su PC?

Me produce la entrada para el gateway predeterminado que es 192.162.0.1 y el de otra pc que esta conectada a la misma vlan 192.168.0.7

El comando **arp** en la PC con Windows tiene otra función. Escriba **arp /?** en la línea de comando y presione Enter. Las opciones del comando **arp** le permiten ver, agregar y eliminar las entradas de la tabla ARP si es necesario.

Laboratorio: Protocolo de resolución de direcciones (ARP)



```
C:\>arp /?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

-a          Displays current ARP entries by interrogating the current
            protocol data.  If inet_addr is specified, the IP and Physical
            addresses for only the specified computer are displayed.  If
            more than one network interface uses ARP, entries for each ARP
            table are displayed.
-g          Same as -a.
-v          Displays current ARP entries in verbose mode.  All invalid
            entries and entries on the loop-back interface will be shown.
inet_addr  Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified
            by if_addr.
-d          Deletes the host specified by inet_addr.  inet_addr may be
            wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
            with the Physical address eth_addr.  The Physical address is
            given as 6 hexadecimal bytes separated by hyphens.  The entry
            is permanent.
eth_addr   Specifies a physical address.
if_addr    If present, this specifies the Internet address of the
            interface whose address translation table should be modified.
            If not present, the first applicable interface will be used.

Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.
```

¿Qué opción elimina una entrada de la caché ARP? -d

¿Cuál sería el resultado del comando **arp -d ***? Me muestra las funciones de las opciones de arp

Reflexión

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

Permite a los hosts mantener la dirección de hardware del destinatario en la caché

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?

La dirección de destino en el trama sería la del gateway predeterminado, la del mismo router.