Práctica de laboratorio: Observación del protocolo ARP mediante la CLI de Windows, la CLI del IOS y Wireshark

Topología

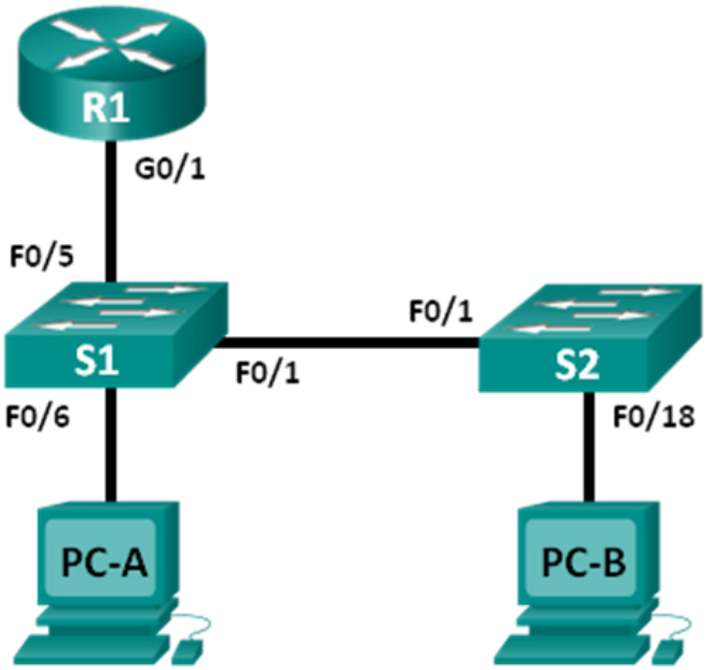


Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.2	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Armar y configurar la red

Parte 2: Utilizar el comando ARP de Windows

Parte 3: Utilizar el comando show ARP del IOS

Parte 4: Utilizar Wireshark para examinar los intercambios ARP

Información básica/Situación

TCP/IP utiliza el protocolo de resolución de direcciones (ARP) para asignar una dirección IP de capa 3 a una dirección MAC de capa 2. Cuando se coloca una trama en la red, debe tener una dirección MAC de destino. Para descubrir dinámicamente la dirección MAC del dispositivo de destino, se transmite una solicitud de ARP en la LAN. El dispositivo que contiene la dirección IP de destino responde, y la dirección MAC se registra en la caché ARP. Cada dispositivo en la LAN mantiene su propio caché ARP, o un área pequeña en RAM que contiene los resultados ARP. Un cronómetro de caché de ARP elimina las entradas ARP que no se han usado por un determinado período de tiempo.

ARP es un excelente ejemplo del equilibrio del rendimiento. Sin caché, ARP debe continuamente solicitar traducciones de direcciones cada vez que se coloca una trama en la red. Esto agrega latencia a la comunicación y puede congestionar la LAN. Por el contrario, los tiempos de espera ilimitados podrían provocar errores con dispositivos que dejan la red o cambiar la dirección de la Capa 3.

Un administrador de red debe estar al tanto del ARP, pero es posible que no interactúe con el protocolo regularmente. ARP es un protocolo que permite que los dispositivos de red se comuniquen con el protocolo TCP/IP. Sin ARP no hay un método eficiente para construir el datagrama de la dirección de destino de la Capa 2. También, ARP es un riesgo de seguridad potencial. La suplantación de identidad de ARP, o envenenamiento de ARP, es una técnica usada por un atacante para inyectar una dirección MAC incorrecta asociada a una red. Un atacante falsifica la dirección MAC de un dispositivo y las tramas son enviadas a un destino equivocado. Configurar manualmente asociaciones ARP estáticas es una manera de impedir la suplantación de identidad de ARP. Por último, se puede configurar una lista de direcciones MAC autorizadas en los dispositivos Cisco para restringir el acceso a la red solo a los dispositivos aprobados.

En esta práctica de laboratorio, utilizará los comandos ARP tanto en los routers Windows como Cisco para visualizar la tabla ARP. También borrará la caché ARP y agregará entradas ARP estáticas.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen de lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte con el instructor.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
- 2 switches (Cisco 2960 con Cisco IOS, versión 15.0(2) [imagen lanbasek9 o comparable])
- 2 PC (Windows 7, Vista o XP con un programa de emulación de terminal instalado, por ejemplo, Tera Term y Wireshark)
- Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología.

Nota: las interfaces Fast Ethernet en los switches Cisco 2960 cuentan con detección automática, y se puede utilizar un cable directo de Ethernet entre los switches S1 y S2. Si utiliza otro modelo de switch Cisco, puede ser necesario usar un cable cruzado Ethernet.

Parte 1: Armar y configurar la red

Paso 1: Tender el cableado de red de acuerdo con la topología

Paso 2: Configurar las direcciones IP de los dispositivos de acuerdo con la tabla de direccionamiento

Paso 3: Verificar la conectividad de red haciendo ping a todos los dispositivos de la PC-B

Parte 2: Usar el comando ARP de Windows

El comando **arp** permite al usuario ver y modificar la caché ARP en Windows. A este comando se accede desde el símbolo del sistema de Windows.

Paso 1: Visualizar la caché ARP

a. Abra una ventana de comandos en la PC-A y escriba **arp**.

```
C:\Users\User1> 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.
```


b. Observe el resultado.

¿Qué comando se usaría para mostrar todas las entradas en la caché ARP?

¿Qué comando se usaría para eliminar todas las entradas de la caché ARP (purgar la caché ARP)?

¿Qué comando se usaría para eliminar la entrada de la caché ARP para 192.168.1.11?

c. Escriba **arp –a** para visualizar la tabla ARP.

```
C:\Users\User1> arp -a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Nota: la tabla ARP está vacía si utiliza Windows XP (como se muestra a continuación).

```
C:\Documents and Settings\User1> arp -a
No ARP Entries Found.
```

d. Haga ping de la PC-A a la PC-B para agregar dinámicamente entradas de la caché ARP.

```
C:\Documents and Settings\User1> ping 192.168.1.2

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
```

¿Cuál es la dirección física para el host con dirección IP 192.168.1.2?

Paso 2: Ajustar las entradas en la caché ARP manualmente

Para eliminar las entradas en la caché ARP, emita el comando **arp –d {inet-addr | *}**. Las direcciones se pueden eliminar de manera individual al especificar la dirección IP, o bien todas juntas con el wildcard *.

Verifique que la caché ARP contenga las entradas siguientes: el gateway predeterminado R1 G0/1 (192.168.1.1), la PC-B (192.168.1.2) y los dos switches (192.168.1.11 y 192.168.1.12).

a. En la PC-A, haga ping a todas las direcciones de la tabla de direcciones.

b. Verifique que todas las direcciones se hayan agregado a la caché ARP. Si la dirección no está en la caché ARP, haga ping a la dirección de destino y verifique que se haya agregado a la caché ARP.

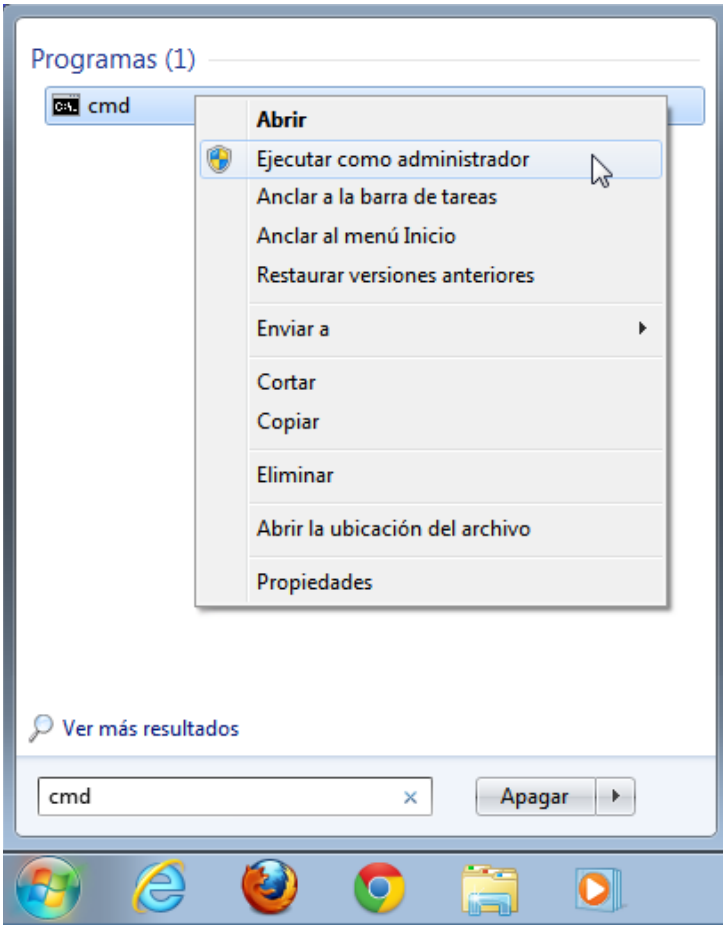
```
C:\Users\User1> arp -a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           d4-8c-b5-ce-a0-c1     dynamic
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.12          0c-d9-96-d2-40-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```



```
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

c. Como administrador, acceda al símbolo del sistema. Haga clic en el ícono **Inicio** y, en el cuadro *Buscar programas y archivo*, escriba **cmd**. Cuando aparezca el ícono **cmd**, haga clic con el botón secundario en él y seleccione **Ejecutar como administrador**. Haga clic en **Sí** para permitir que este programa realice los cambios.

Nota: para los usuarios de Windows XP, no es necesario tener privilegios de administrador para modificar las entradas de la caché ARP.



d. En la ventana del símbolo del sistema Administrador, escriba **arp –d ***. Este comando elimina todas las entradas de la caché ARP. Verifique que todas las entradas de la caché ARP se hayan eliminado; para eso, escriba **arp-a** en el símbolo del sistema.

```
C:\windows\system32> arp –d *
C:\windows\system32> arp –a
No ARP Entries Found.
```

e. Espere unos minutos. El protocolo de descubrimiento de vecinos comienza a llenar la caché ARP nuevamente.

```
C:\Users\User1> arp –a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```


Nota: el protocolo de descubrimiento de vecinos no está implementado en Windows XP.

f. En la PC-A, haga ping a la PC-B (192.168.1.2) y a los switches (192.168.1.11 y 192.168.1.12) para agregar las entradas ARP. Verifique que las entradas ARP se hayan agregado a la caché.

```
C:\Users\User1> arp –a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.12          0c-d9-96-d2-40-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

g. Registre la dirección física del switch S2.

h. Elimine una entrada de caché ARP específica escribiendo **arp –d *inet-addr***. En el símbolo del sistema, escriba **arp –d 192.168.1.12** para eliminar la entrada ARP para el S2.

```
C:\windows\system32> arp –d 192.168.1.12
```

i. Escriba **arp –a** para verificar que la entrada ARP para el S2 se eliminó de la caché ARP.

```
C:\Users\User1> arp –a

Interface: 192.168.1.3 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.2           00-50-56-be-f6-db     dynamic
  192.168.1.11          0c-d9-96-e8-8a-40     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

j. Puede agregar una entrada de caché ARP específica escribiendo **arp –s *inet_addr_mac_addr***. En este ejemplo, se utilizará la dirección IP y la dirección MAC para el S2. Use la dirección MAC registrada en el paso g.

```
C:\windows\system32> arp –s 192.168.1.12 0c-d9-96-d2-40-40
```

k. Verifique que la entrada ARP para el S2 se haya agregado a la caché.

Parte 3: Utilizar el comando show arp del IOS

Cisco IOS también puede mostrar la caché ARP en los routers y switches mediante el comando **show arp** o **show ip arp**.

Paso 1: Mostrar las entradas ARP del router R1

```
R1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1            -   d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2            0   0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3            0   0050.56be.768c  ARPA   GigabitEthernet0/1
R1#
```

Observe que no hay ningún valor de Age (-) para la primera entrada, la interfaz del router G0/1 (el gateway predeterminado de LAN). Age es la cantidad de minutos (min) que la entrada estuvo en la caché ARP y se incrementa para las otras entradas. El protocolo de descubrimiento de vecinos llena las entradas ARP de las direcciones IP y MAC de la PC-A y la PC-B.

Paso 2: Agregar entradas ARP del router R1

Puede agregar entradas ARP a la tabla ARP del router haciendo ping a otros dispositivos.

a. Haga ping al switch S1.

```
R1# ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/4 ms
```

b. Verifique que una entrada ARP para el switch S1 se haya agregado a la tabla ARP del R1.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1              -   d48c.b5ce.a0c1  ARPA   GigabitEthernet0/1
Internet  192.168.1.2              6   0050.56be.f6db  ARPA   GigabitEthernet0/1
Internet  192.168.1.3              6   0050.56be.768c  ARPA   GigabitEthernet0/1
Internet  192.168.1.11             0   0cd9.96e8.8a40  ARPA   GigabitEthernet0/1
R1#
```

Paso 3: Mostrar las entradas ARP del switch S1

```
S1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1             46   d48c.b5ce.a0c1  ARPA   Vlan1
Internet  192.168.1.2              8   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3              8   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11             -   0cd9.96e8.8a40  ARPA   Vlan1
S1#
```

Paso 4: Agregar entradas ARP en el switch S1

Al hacer ping a otros dispositivos, también se puede agregar entradas ARP a la tabla ARP del switch.

a. En el switch S1, haga ping al switch S2.

```
S1# ping 192.168.1.12
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.12, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms
```

b. Verifique que la entrada ARP para el switch S2 se haya agregado a la tabla ARP del S1.

```
S1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1              5   d48c.b5ce.a0c1  ARPA   Vlan1
Internet  192.168.1.2             11   0050.56be.f6db  ARPA   Vlan1
Internet  192.168.1.3             11   0050.56be.768c  ARPA   Vlan1
Internet  192.168.1.11             -   0cd9.96e8.8a40  ARPA   Vlan1
Internet  192.168.1.12             2   0cd9.96d2.4040  ARPA   Vlan1
S1#
```

Parte 4: Utilizar Wireshark para examinar los intercambios ARP

En la parte 4, examinará los intercambios ARP mediante Wireshark para capturar y evaluar el intercambio ARP. También examinará la latencia de red que causan los intercambios ARP entre los dispositivos.

Paso 1: Configurar Wireshark para las capturas de paquetes

a. Inicie Wireshark.

b. Elija la interfaz de red que desea usar para capturar los intercambios ARP.

Paso 2: Capturar y evaluar las comunicaciones del ARP

a. Inicie la captura de paquetes en Wireshark. Utilice el filtro para mostrar solamente los paquetes ARP.

b. Purgue la caché ARP; para eso, escriba el comando **arp –d *** en el símbolo del sistema.

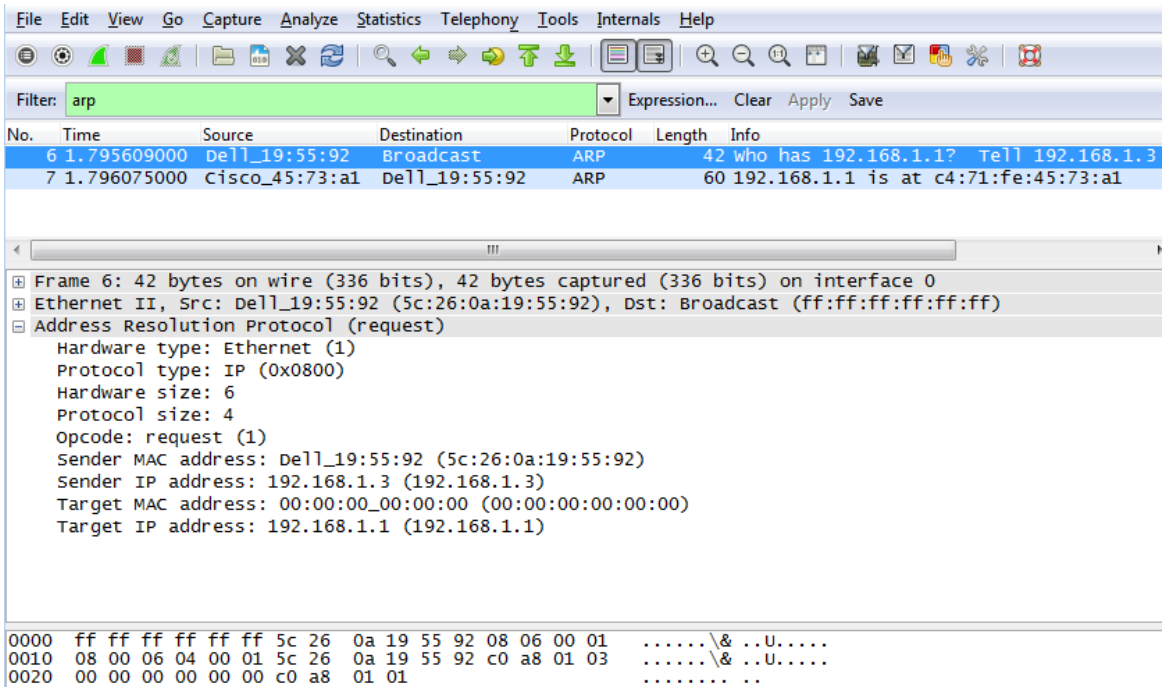
c. Verifique que la caché ARP se haya borrado.

d. Envíe un ping al gateway predeterminado mediante el comando **ping 192.168.1.1**.

e. Después de hacer ping al gateway predeterminado, detenga la captura de Wireshark.

f. Examine las capturas de Wireshark para los intercambios ARP en el panel de detalles del paquete.

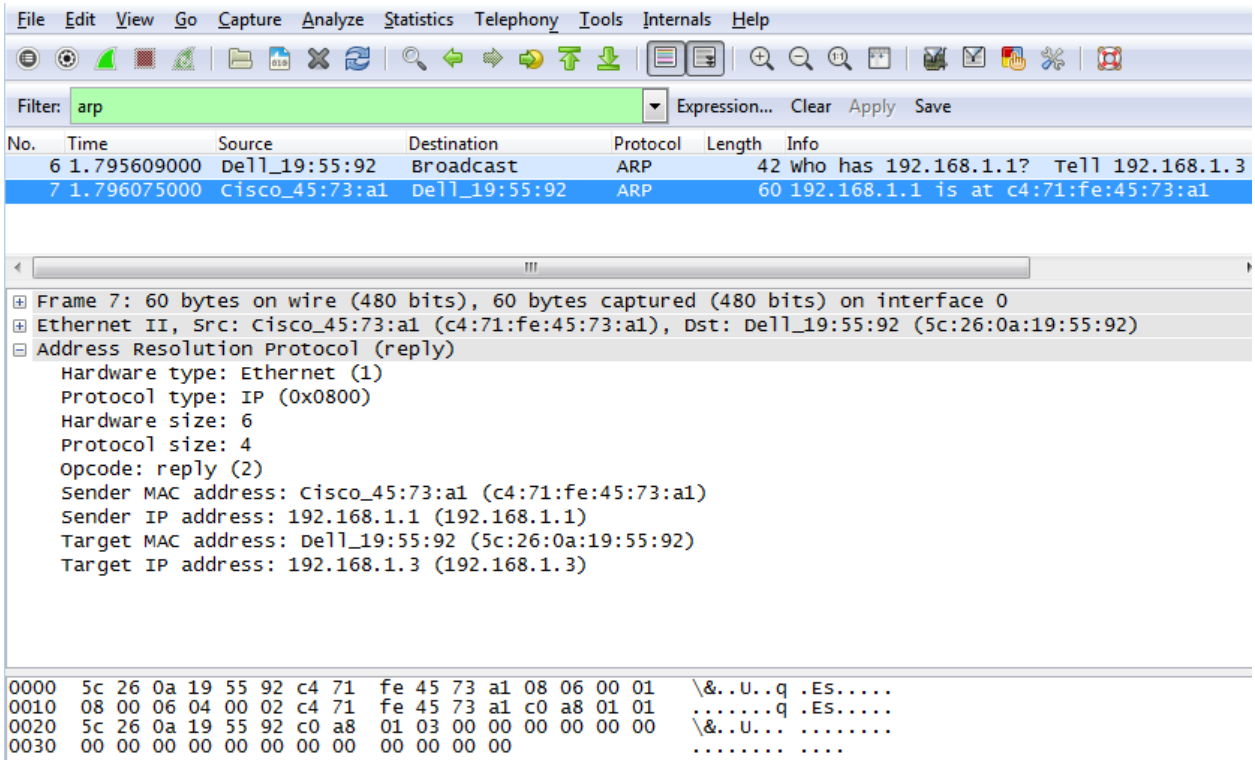
¿Cuál fue el primer paquete de ARP?



Complete la siguiente tabla con información sobre el primer paquete de ARP que se capturó.

Campo	Valor
Dirección MAC del emisor	
Dirección IP del emisor	
Dirección MAC de destino	
Dirección IP de destino	

¿Cuál fue el segundo paquete de ARP?



Complete la siguiente tabla con información sobre el segundo paquete de ARP que se capturó.

Campo	Valor
Dirección MAC del emisor	
Dirección IP del emisor	
Dirección MAC de destino	
Dirección IP de destino	

Paso 3: Examinar la latencia de red que causa el ARP

a. Borre las entradas ARP de la PC-A.

b. Inicie una captura de Wireshark.

c. Haga ping al switch S2 (192.168.1.12). El ping debe ser correcto después de la primera solicitud de eco.

Nota: si todos los pings son correctos, el S1 debe volver a cargarse para observar la latencia de red con el ARP.

```
C:\Users\User1> ping 192.168.1.12
Request timed out.
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
Reply from 192.168.1.12: bytes=32 time=2ms TTL=255
```



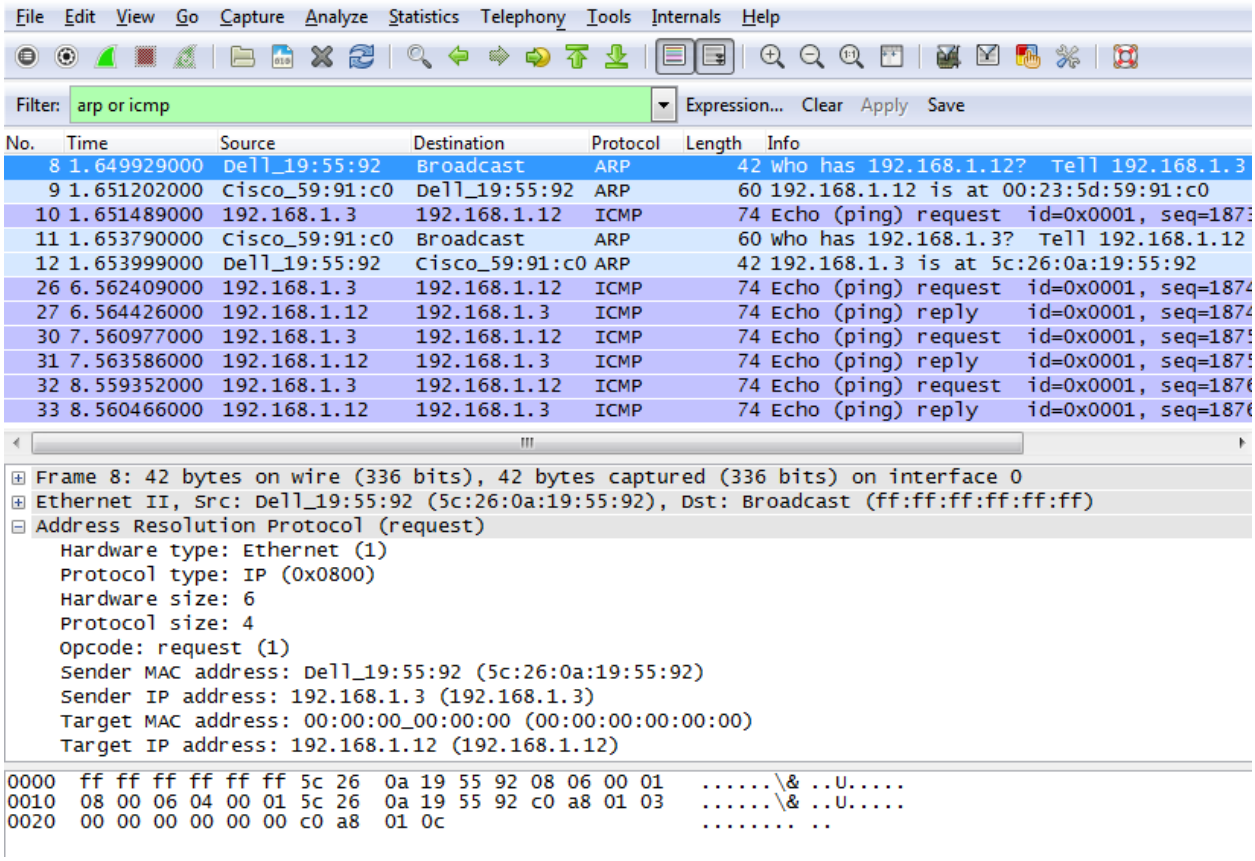
```
Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 3ms, Average = 2ms
```

d. Una vez finalizado el ping, detenga la captura de Wireshark. Utilice el filtro de Wireshark para mostrar solamente los resultados de ARP e ICMP. En Wireshark, escriba **arp o icmp** en el área de entrada **Filter:** (Filtro:).

e. Examine la captura de Wireshark. En este ejemplo, la trama 10 es la primera solicitud de ICMP que se envía de la PC-A al S1. Dado que no hay una entrada ARP para el S1, se envió una solicitud de ARP a la dirección IP de administración del S1 en la que se solicita la dirección MAC. Durante los intercambios ARP, la solicitud de eco no recibió una respuesta antes de agotarse el tiempo de espera de la solicitud. (Tramas 8 a 12)

   Después de que la entrada ARP para el S1 se agregó a la caché ARP, los últimos tres intercambios ICMP fueron correctos, como se muestra en las tramas 26, 27 y 30-33.

   Como se muestra en la captura de Wireshark, ARP es un excelente ejemplo del equilibrio del rendimiento. Sin caché, ARP debe continuamente solicitar traducciones de direcciones cada vez que se coloca una trama en la red. Esto agrega latencia a la comunicación y puede congestionar la LAN.



Reflexión

1. ¿Cómo y cuándo se quitan las entradas ARP estáticas?

2. ¿Por qué desea agregar entradas ARP estáticas en la caché?

3. Si las solicitudes ARP pueden causar latencia de red, ¿por qué no es conveniente tener tiempos de espera ilimitados para las entradas ARP?

Tabla de resumen de interfaces del router

Resumen de interfaces del router				
Modelo de router	**Interfaz Ethernet #1**	**Interfaz Ethernet #2**	**Interfaz serial #1**	**Interfaz serial #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede hacer interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en los comandos de Cisco IOS para representar la interfaz.

