# 华东师范大学软件工程学院实验报告

|  |  |  |
| --- | --- | --- |
| **实验课程**：计算机网络实验 | **年级**：2023级 | **实验成绩**： |
| **实验名称**：APR | **姓名**：陆尚辰 |  |
| **实验编号**：Lab4 | **学号**：10235101545 | **实验日期**：2024.12.13 |
| **指导教师**：刘献忠 | **组号**： | **实验时间**： |

**一、实验目的**

1. 学会通过Wireshark获取ARP消息

2. 掌握ARP数据包结构

3. 掌握ARP数据包各字段的含义

4. 了解ARP协议适用领域

**二、实验内容与实验步骤**

1.获取ARP信息

(1)使用管理员权限打开命令行

输入ipconfig /all，可以获得本地计算机的物理地址

输入netstat –r，可以获得本机路由表

输入arp –a，可以查看ARP cache

输入arp –d，可以清空ARP cache

(2)启动Wireshark，在菜单栏的捕获->选项中进行设置，选择已连接的以太网，设置捕获过滤器为ARP，将混杂模式设为关闭

(3)点击开始

(4)清空ARP cache

2. 作业与分析

(1) 画出你的计算机和本地路由间ARP的请求和应答数据包，标记出请求和应答，为每个数据包给出发送者和接受者的MAC和IP地址。

(2) 什么样的操作码是用来表示一个请求？应答呢？

(3) 一个请求的ARP的报头有多大？应答呢？

(4) 对未知目标的MAC地址的请求是什么值？

(5) 什么以太网类型值说明ARP是更高一层的协议？

(6) ARP应答是广播吗？

**三、实验环境**

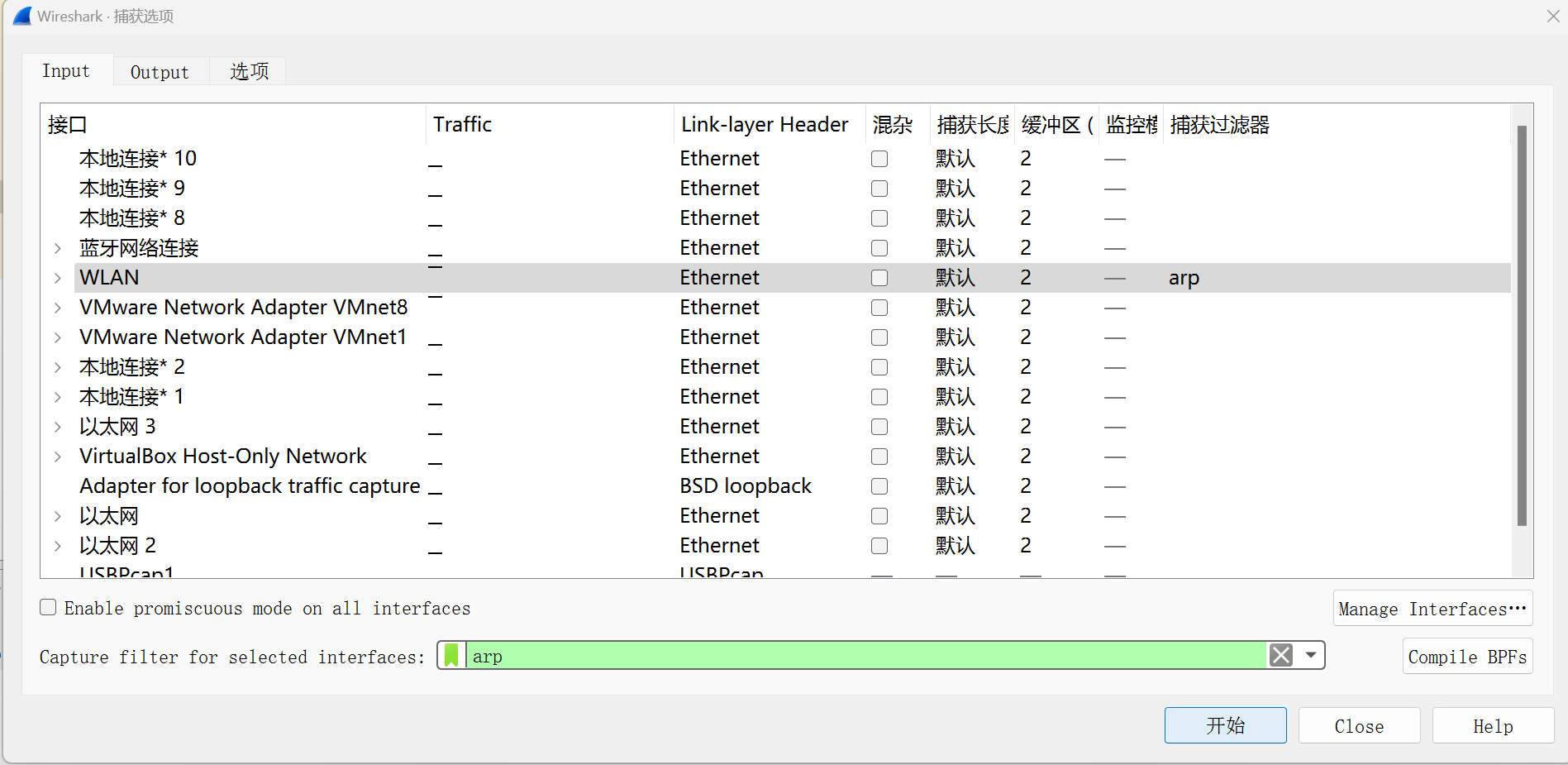
1. Wireshark v2.0.2

2. Windows操作系统

**四、实验过程与分析**

**4.1.捕获数据**

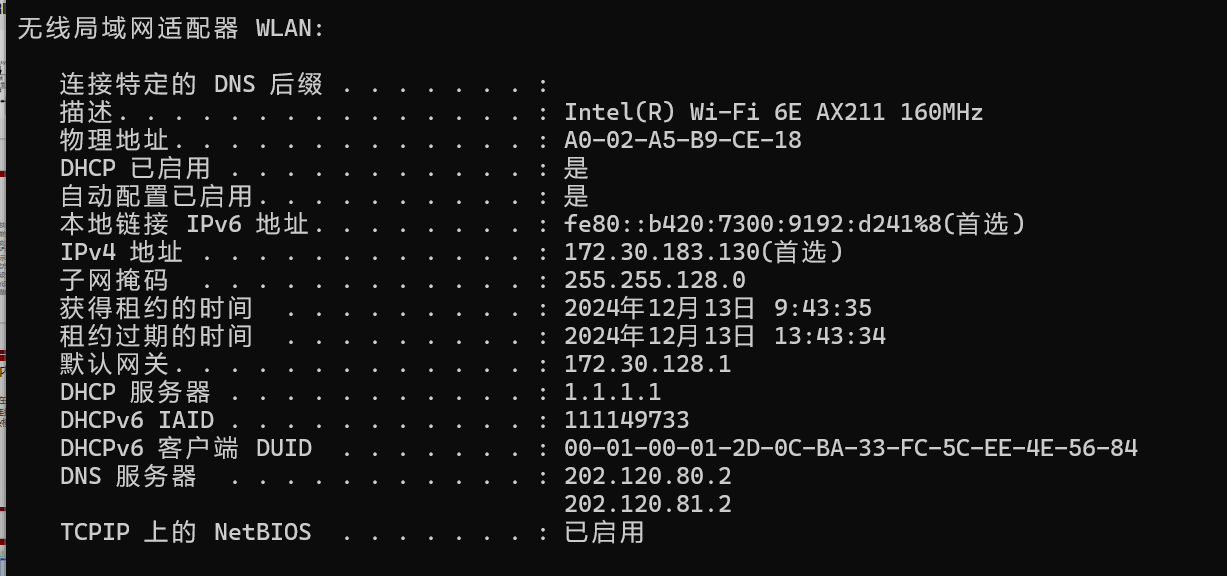
1. 启动Wireshark，在菜单栏的捕获->选项中进行设置，选择已连接的以太网，设置捕获过滤器为ARP，将混杂模式设为关闭。



2.在命令行中输入pconfig -all 命令，获取本机的 IP 地址和 MAC 地址。

MAC地址为：A0-02-A5-B9-CE-18

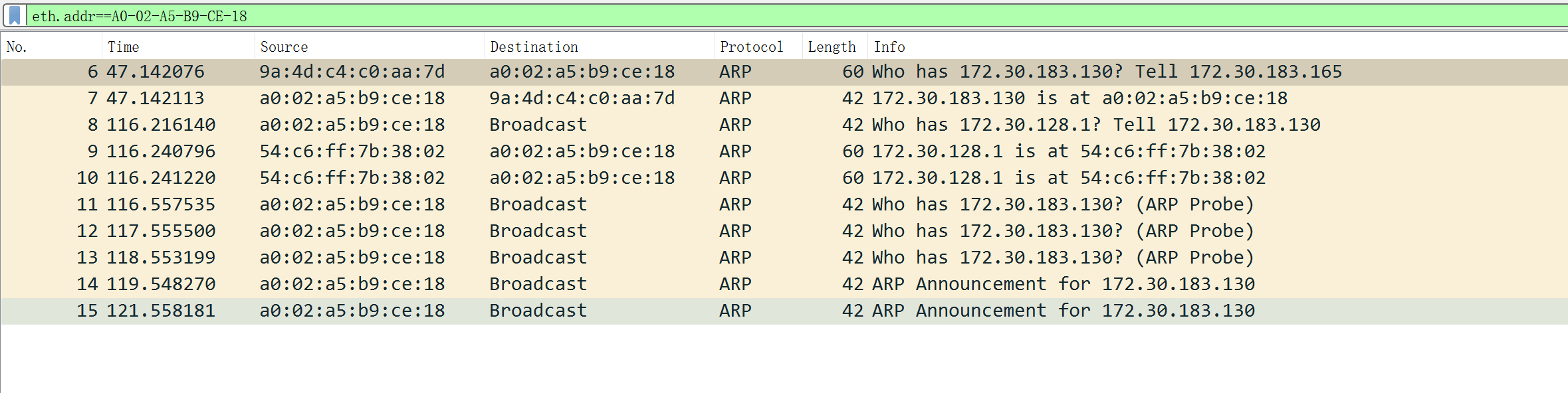
IP地址为：170.30.183.130



3. 在Wireshark中设置捕获过滤器为eth.addr==A0-02-A5-B9-CE-18，

在终端中使用 arp -d 命令（管理员模式下）清除本机的 ARP 缓存。

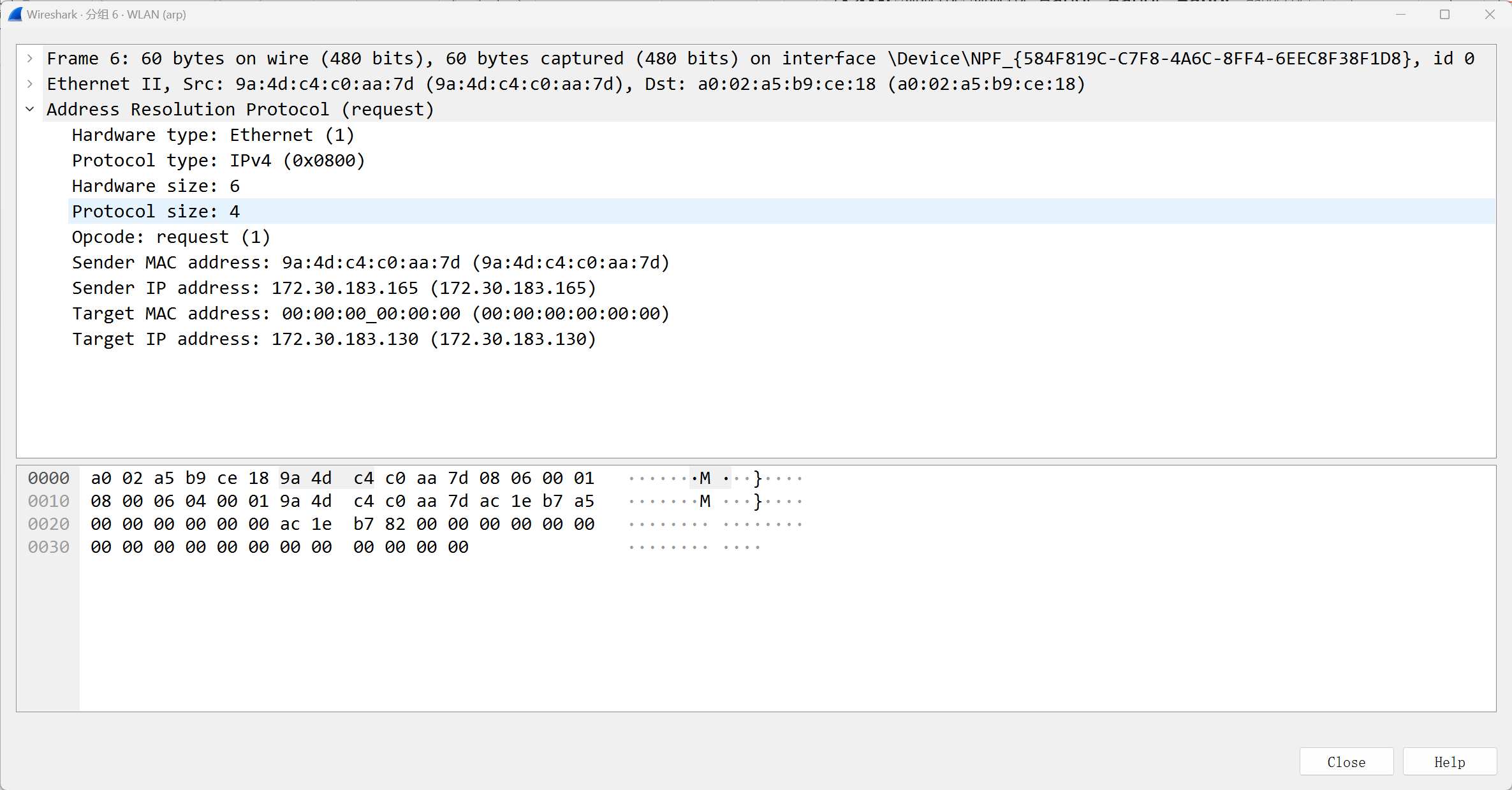
Wireshark中停止捕获，最终得到结果如下：



**4.2.回答问题：**

**1.画出你的计算机和本地路由间ARP的请求和应答数据包，标记出请求和应答，为每个数据包给出发送者和接受者的MAC和IP地址。**

（1）选择一个ARP 请求数据包：



我们可以看到一个长度为28字节的ARP报头，包含如下字段：

Hardware type硬件类型，这里类型为Ethernet (1)，长度为2字节

Protocol type上一层协议类型，为 IPv4（0x0800），长度为2字节

Hardware size硬件长度，为6，长度为1字节

Protocol size协议长度，为4，长度为1字节

Opcode操作类型，为request，长度为 2 字节

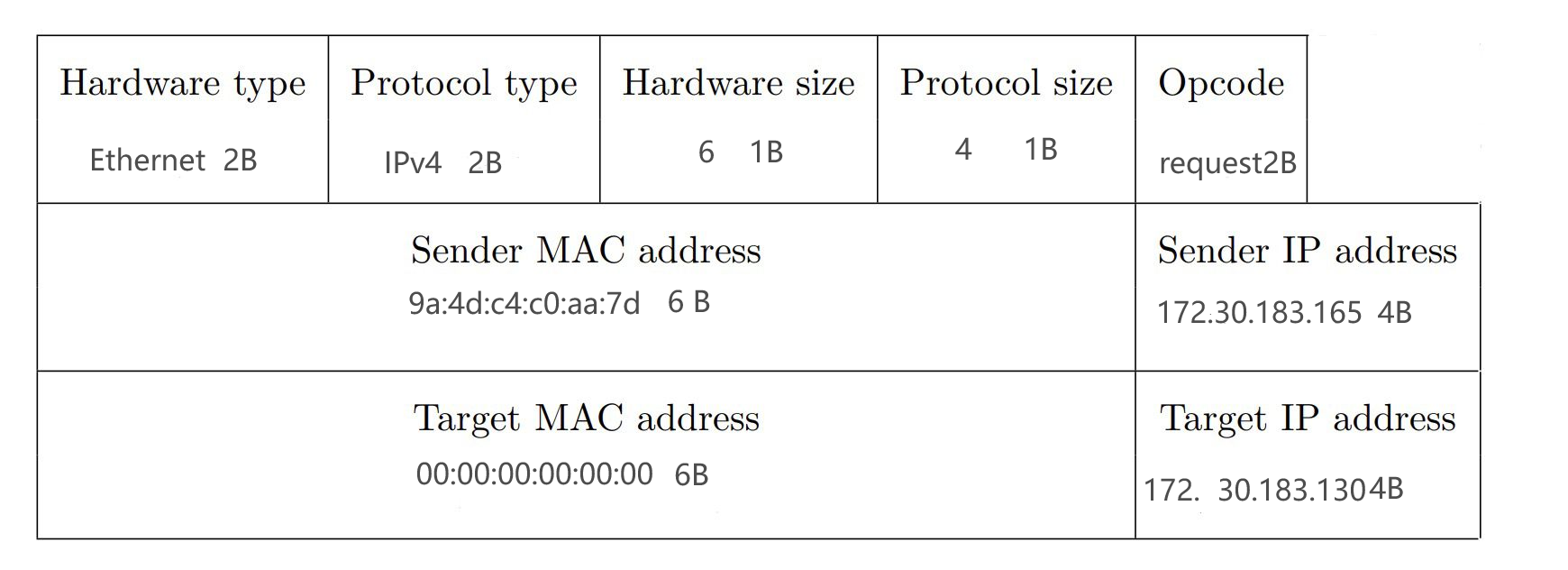
Sender MAC address:发送方源地址9a:4d:c4:c0:aa:7d，长度为 6 字节

Sender IP address发送方IP地址: 172.30.183.165，长度为 4 字节

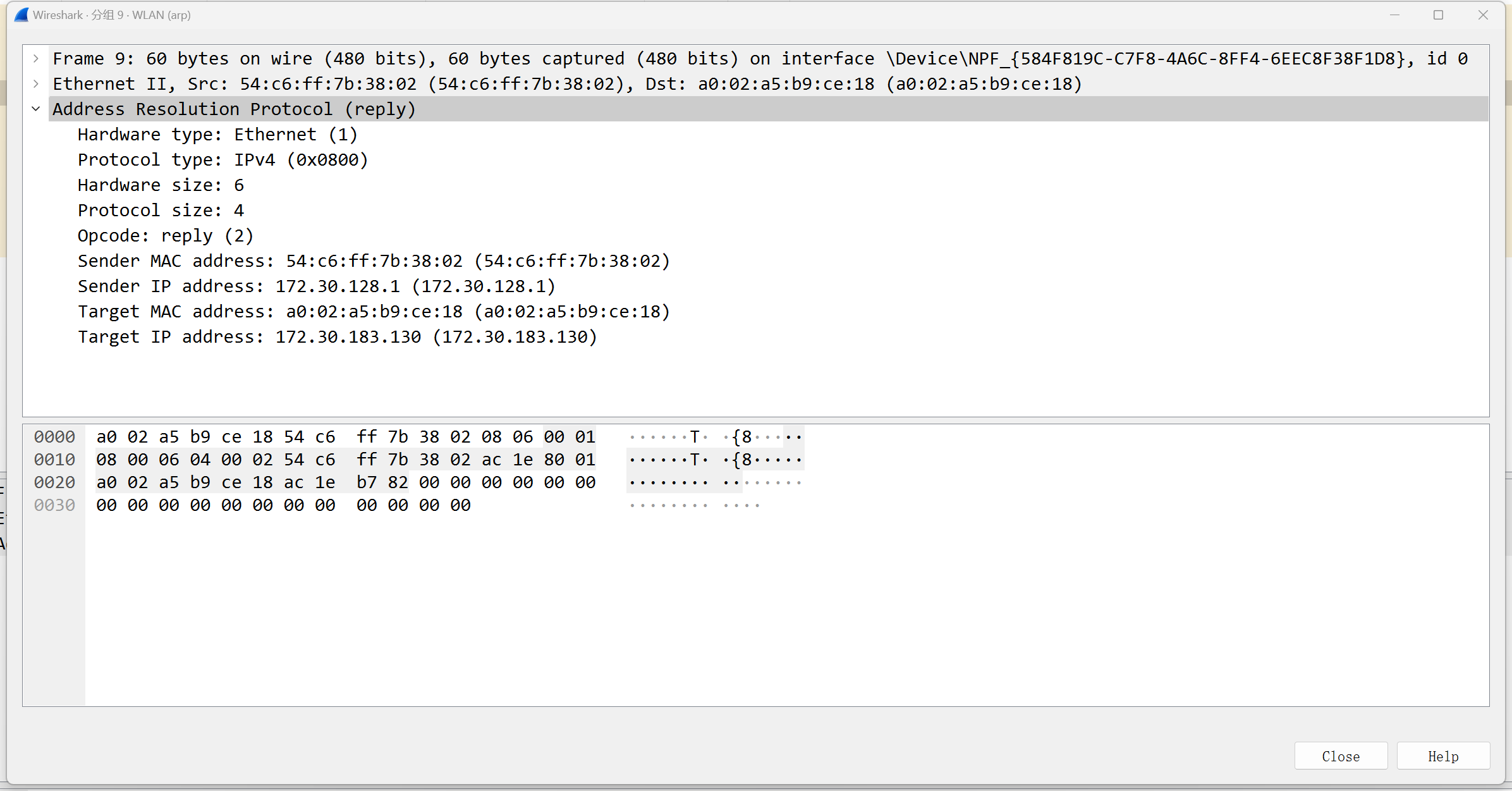
Target MAC address路由器: 00:00:00:00:00:00，长度为 6 字节

Target IP address目标IP地址: 172.30.183.130，长度为 4 字节

由此可以画出APR请求数据包的结构：



（2）选择一个ARP 应答数据包：



同理，我们可以看到一个长度为28字节的ARP报头，包含如下字段：

Hardware type硬件类型，这里类型为Ethernet (1)，长度为2字节

Protocol type上一层协议类型，为 IPv4（0x0800），长度为2字节

Hardware size硬件长度，为6，长度为1字节

Protocol size协议长度，为4，长度为1字节

Opcode操作类型，为reply，长度为 2 字节

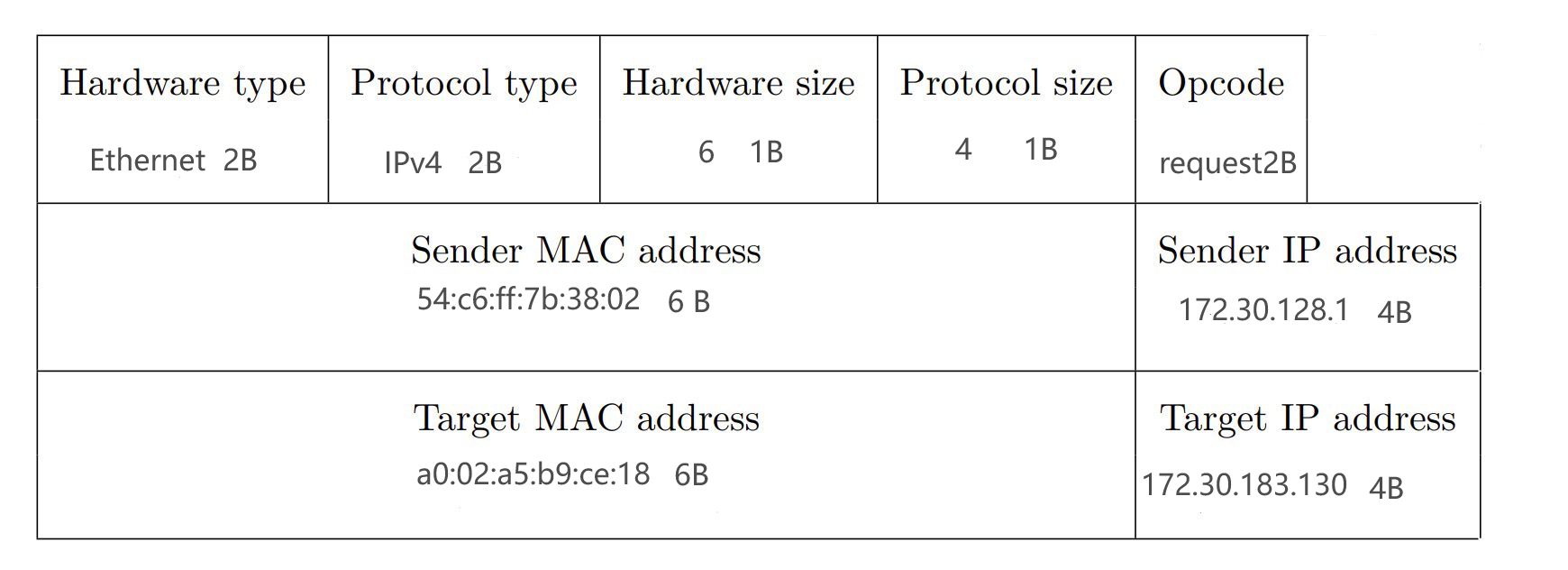
Sender MAC address:发送方源地址54:c6:ff:7b:38:02，长度为 6 字节

Sender IP address发送方IP地址: 172.30.128.1，长度为 4 字节

Target MAC address路由器: a0:02:a5:b9:ce:18，长度为 6 字节

Target IP address目标IP地址: 172.30.183.130，长度为 4 字节

由此可以画出APR应答数据包的结构：



**2.什么样的操作码是用来表示一个请求？应答呢？**

ARP报头中的Opcode字段用来表示ARP请求或应答，

Opcode为1时表示请求（request），

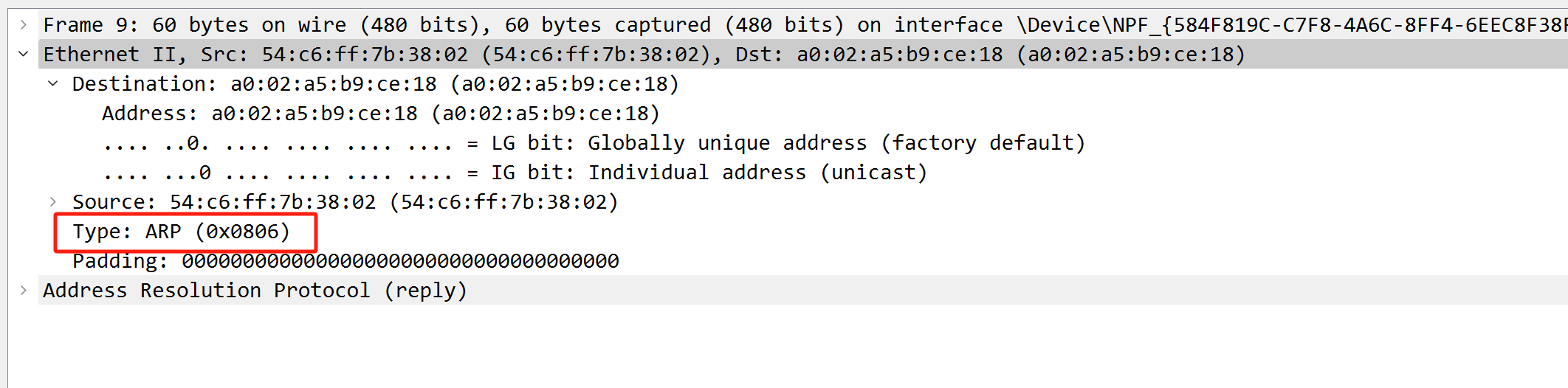
为2时表示应答（reply）。

**3.一个请求的ARP的报头有多大？应答呢？**

由上文分析可知，请求和应答ARP的报头长度均为 28 字节。

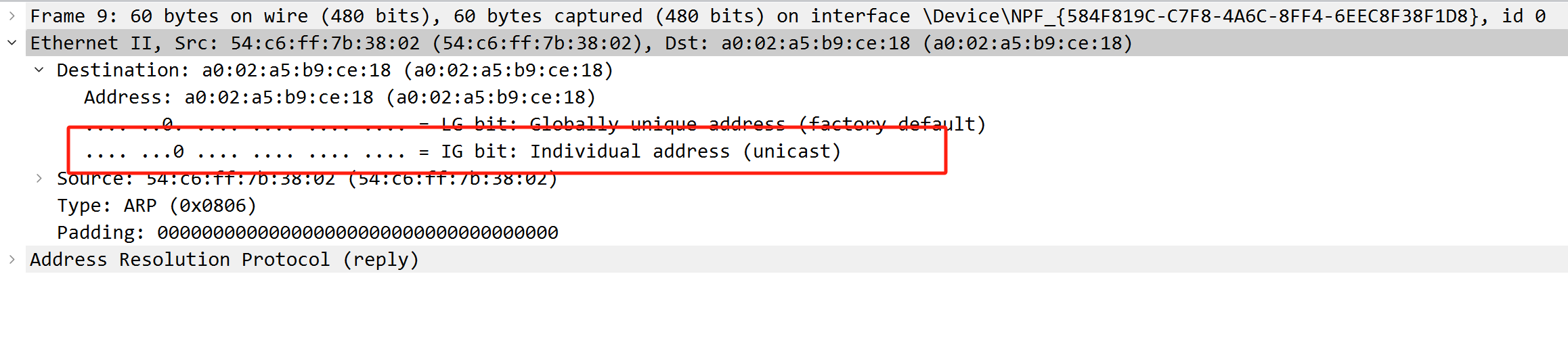
**4.对未知目标的MAC地址的请求是什么值？**

对未知目标的MAC地址的请求为：00:00:00:00:00:00。

**5.什么以太网类型值说明ARP是更高一层的协议？**

由图可知，当以太网类型值为0x0806时，则说明说明 ARP 是更高一层的协议。

**6.ARP应答是广播吗？**



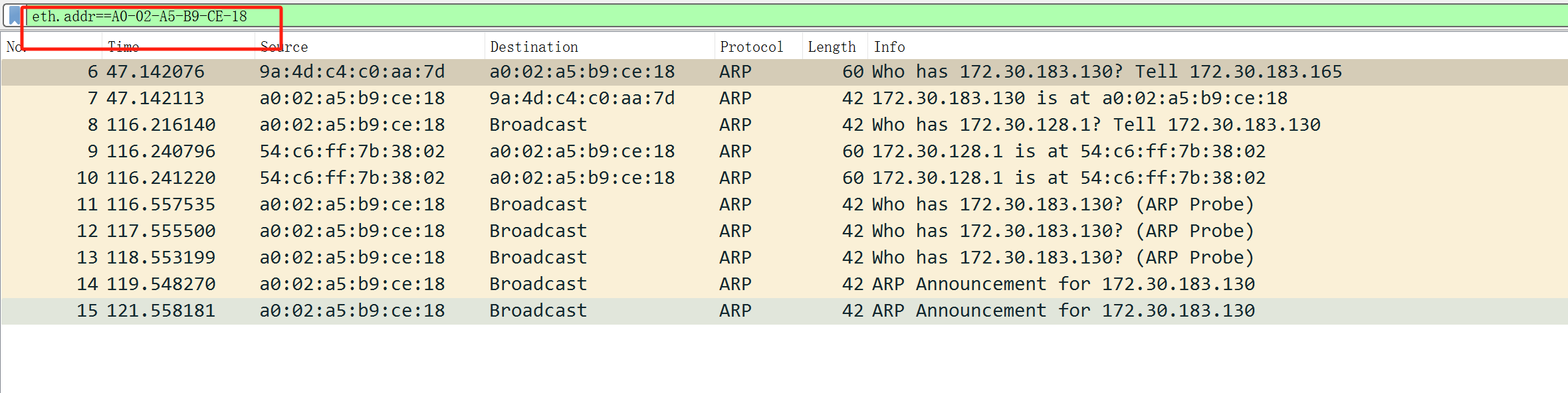
如上图，ARP应答不是广播，是单播。

**五、实验结果总结**

**1.问题分析**

We encourage you to explore ARP on your own once you have completed this lab. One suggestion is to look at other ARP packets that may have been recorded in your trace; we only examined an ARP request by your computer and the ARP reply from the default gateway. To see if there is other ARP activity, make sure to clear any Ethernet address filter that is set. Other ARP packets may exhibit any of the following kinds of behavior for you to explore:

1.ARP requests broadcast by other computers. The other computers on the local network are also using ARP. Since requests are broadcast, your computer will receive their requests.



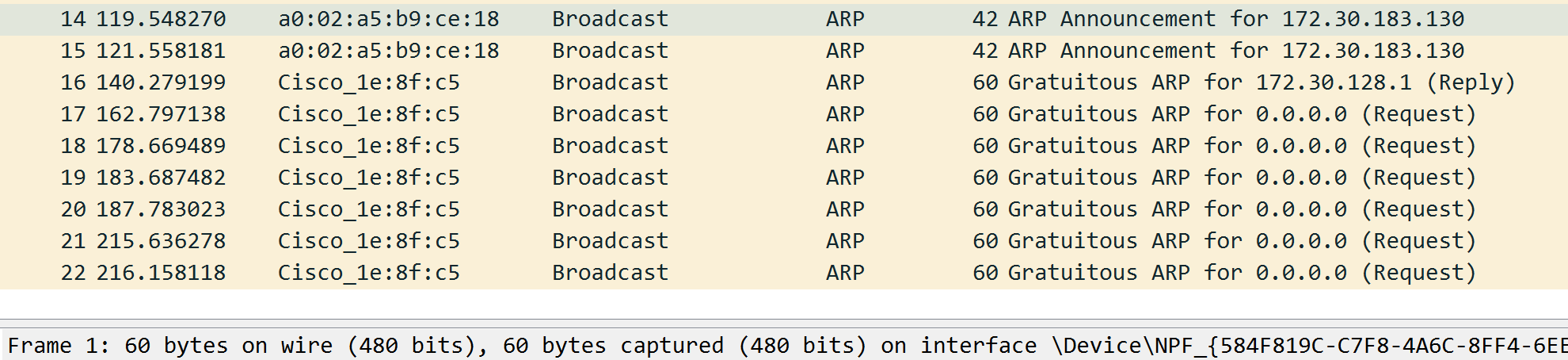
清除筛选后，由于ARP请求为广播，在这里就可以看到其他计算机发送的 ARP 请求。

2.ARP replies sent by your computer. If another computer happens to ARP for the IP address of your computer, then your computer will send an ARP reply to tell it the answer.

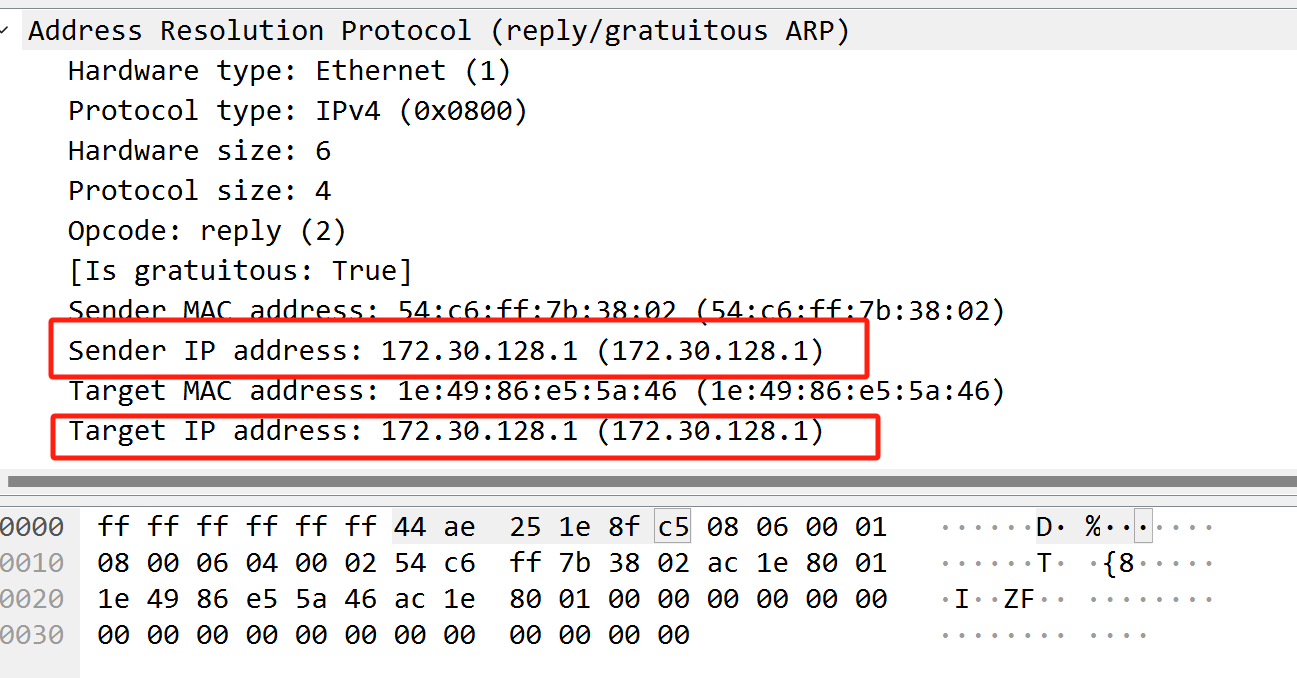
你的计算机发送的ARP回复，告诉别的计算机你的物理地址信息。当你的计算机收到一个 ARP 请求时，这个请求通常是其他计算机在询问 “谁拥有这个 IP 地址，并且请告诉我对应的物理（MAC）地址”。如果这个 IP 地址是你计算机的，那么你的计算机就会发送一个 ARP 回复来告知对方自己的物理地址信息。

3.Gratuitous ARPs in which your computer sends a request or reply about itself. This is helpful when a computer or link comes up to make sure that no-one else is using the same IP address. Gratuitous ARPs have the same sender and target IP address, and they have an Info field in Wireshark that identified them as gratuitous.

我们可以在捕获列表中看到 gratuitous ARP 数据包。



这类报文是自己的计算机发送的 arp 请求和答复，目的是为了确保没有其他人正在使用相同的 IP 地址。这类报文具有相同的发送方和目标 IP 地址。



具体查看可以看到相同的发送方和目标 IP 地址。

4.Other ARP requests sent by your computer and the corresponding ARP reply. Your computer may need to ARP for other hosts besides the default gateway after you flush its ARP cache.

计算机发送的其他 ARP 请求和相应的 ARP 答复，电脑可能需要 ARP 为除默认网关之外的其他主机刷新它的 ARP 缓存，在使用arp -d 命令（管理员模式下）后可以清除本机的 ARP 缓存。

**六、附录**

无