# 华东师范大学软件工程学院实验报告

|  |  |  |
| --- | --- | --- |
| **实验课程**：计算机网络实践 | **年级**：2023级 | **实验成绩**： |
| **实验名称**：Lab2 Ethernet | **姓名**：陆尚辰 |  |
| **实验编号**：Lab2 | **学号**：10235101545 | **实验日期**：2024.11.29 |
| **指导教师**：刘献忠 | **组号**： | **实验时间**： |

**一、实验目的**

1. 学会通过Wireshark获取以太网的帧

2. 掌握以太网帧的结构

3. 分析以太网地址范围

4. 分析以太网的广播帧

**二、实验内容与实验步骤**

**1.获取以太网的帧**

（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icmp，将混杂模式设为关闭,视图选项中勾选是否解析物理地址.然后开始捕获。

（2）点开命令行，重新输入 ping www.baidu.com.

（3）打开Wireshark， 停止捕获

**2.分析以太网帧结构**

理解Ethernet 帧结构，并画一个图，简单的标出Ethernet头部的一些字段的位置和大小 ，以及Ethernet负载的范围。

**3. 分析以太网地址范围**

画一个图,显示你的电脑、路由器和远程服务器的相对位置。标出你的电脑和路由器的以太网地址。标出你的计算机和远程服务器的IP地址。显示以太网和互联网在绘图上的位置。

**4.分析以太网广播帧**

使用分析以太网广播帧broadcast的格式回答下面问题并且上交：

（1）wireshark中以太网广播帧的地址是什么?

（2）以太网地址中哪个比特位是用来确定是单播或多播/广播?

**三、实验环境**

1. Wireshark v2.2.10

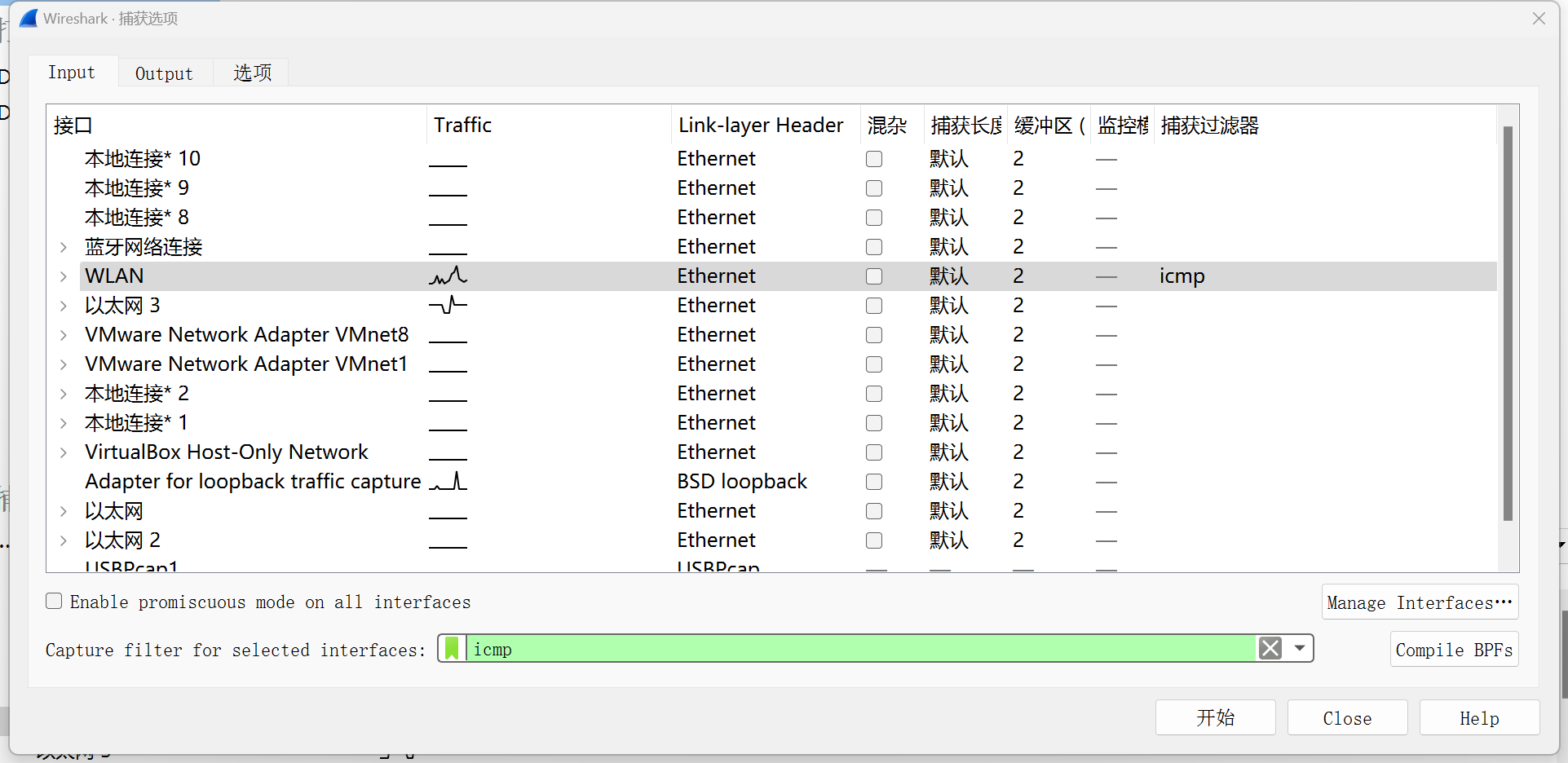
2. Windows操作系统

3. ping

**四、实验过程与分析**

**1.捕获以太网的帧：**

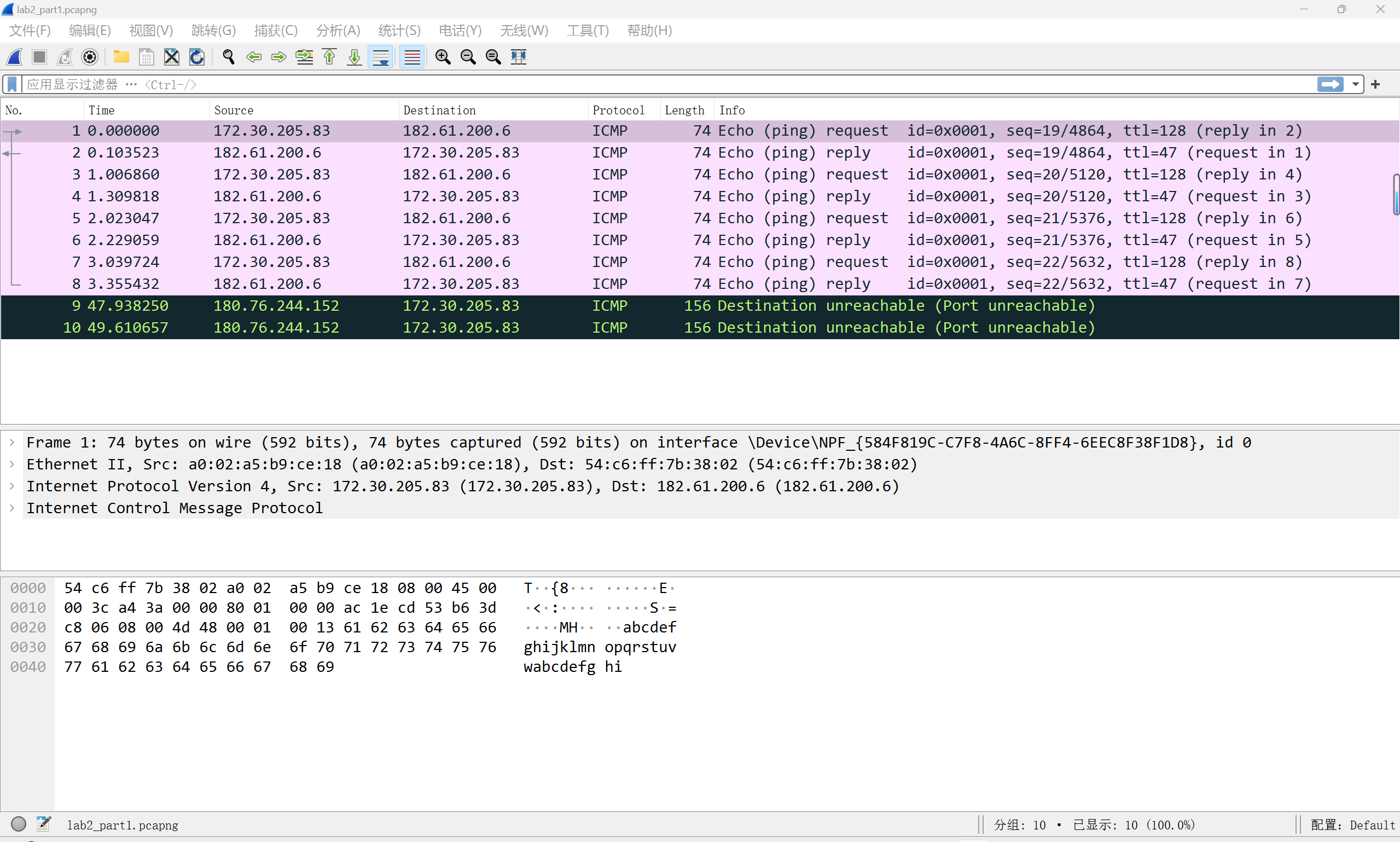
（1）启动Wireshark，在菜单栏的捕获->选项中进行设置，选择已连接的以太网，设置捕获过滤器为icmp，将混杂模式设为关闭,视图选项中勾选是否解析物理地址.然后开始捕获。



（2）win+R打开命令行，输入ping [www.baidu.com](http://www.baidu.com)。计算机就会向远程计算机发送少量ICMP ping请求，每个请求都会引发一个ICMP ping响应。

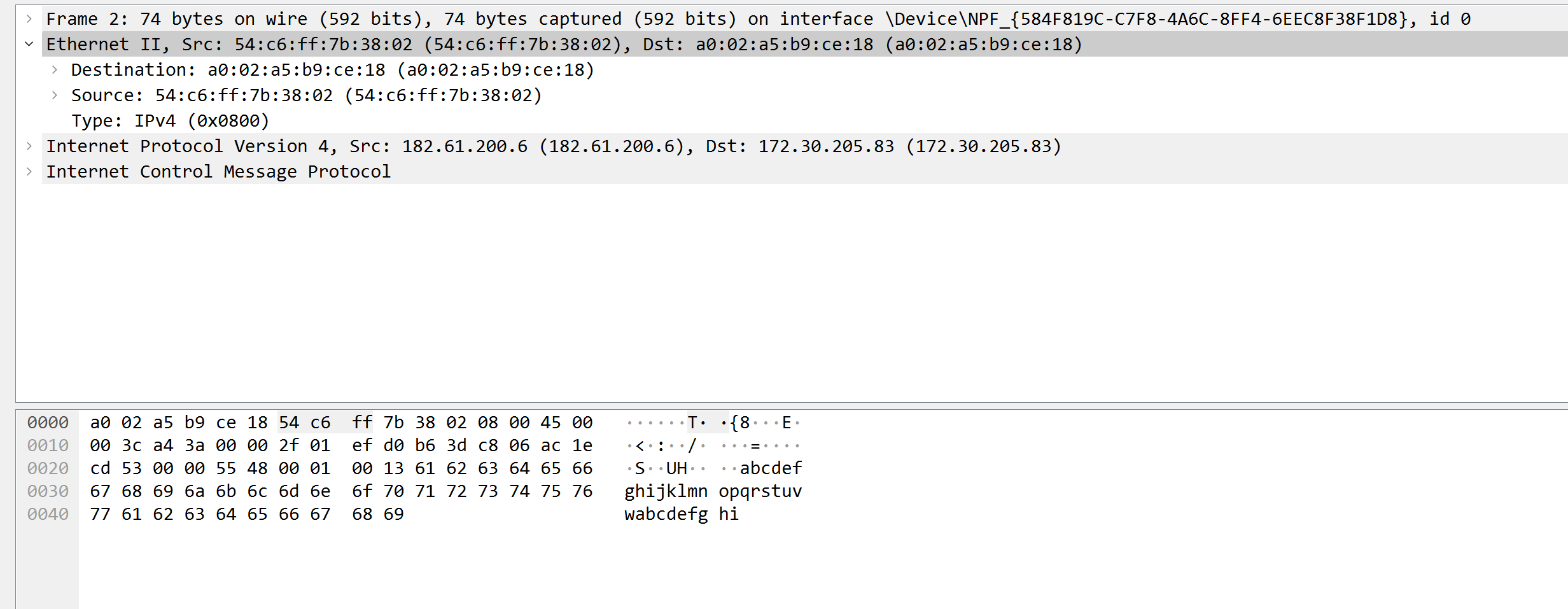


（3）打开wireshark，停止捕获并查看最后结果



**2.分析以太网帧结构**

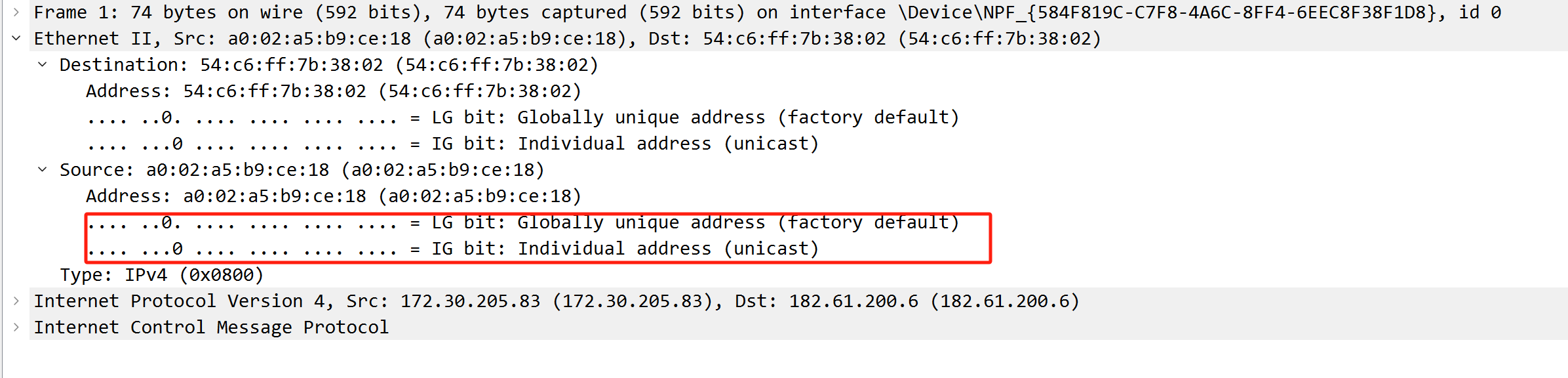
2.1查看Ethernet：



以太网占据了14个字节

分别为本机的MAC地址：54:c6:ff:7b:38:02

路由器的MAC地址：a0:02:a5:b9:ce:18

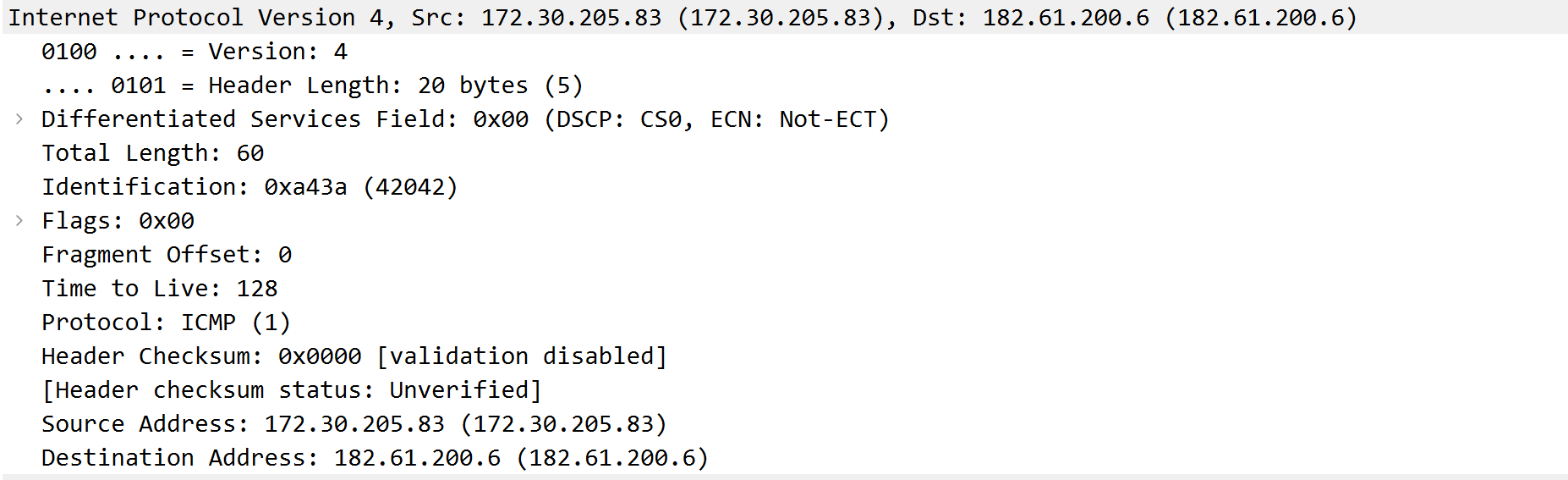


可以看出，MAC地址的第一个字节的第七位是LG位，LG位为0表示这是一个厂家出厂默认的MAC地址。

第八位是IG，IG位为0表示这是一个单播MAC地址。

可以看到以太网头部包括了目的地址 (Destination)、源地址 (Source) 和类型 (Type) 三部分。其中 目的地址和源地址都是 6 个字节，类型是 2 个字节。

2.2查看IP报文：



1.前4位（0100）表示版本号为4。

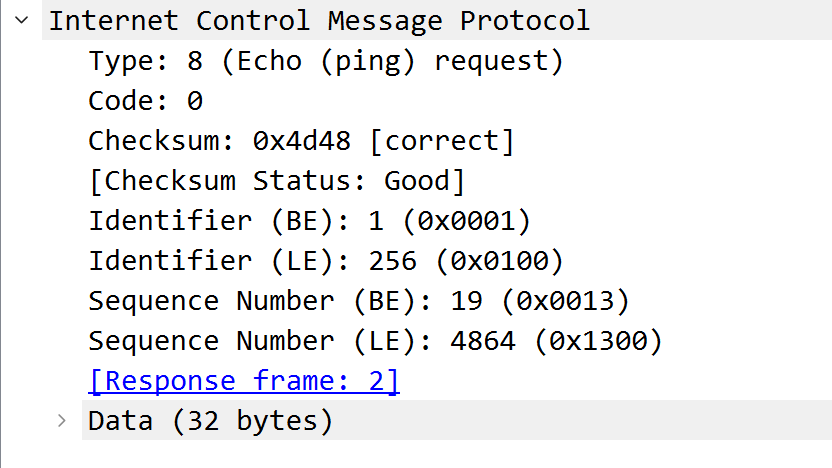
2.接下来4位表示报文的长度为20个字节

3.IP报文的第二个字节为服务类型（服务类型字段声明了数据报被网络系统传输时可以被怎样处理），其值为00000000，全为0表示一般服务。

4.Total Length表示总长度为60字节，即整个数据报的长度为60bytes。

5.头部校验和为0x0000

2.3查看ICMP报文：



1.第一个字节08表示类型，类型为Echo Request。

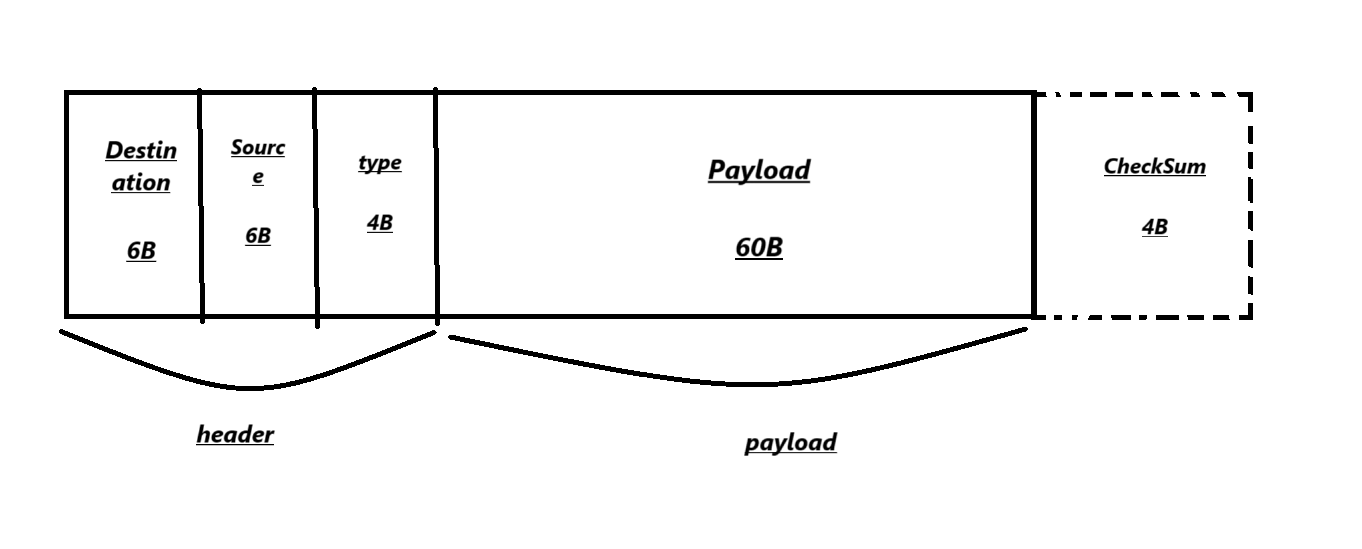
2.第二个字节为00，表示Code。

3.校验和为0x4d48

4.标识码和序列码。

5.后面的32字节是我们发送的数据。

画出的帧结构如下图所示：



**3.分析以太网的地址范围：**

根据上述分析，我们可以得到

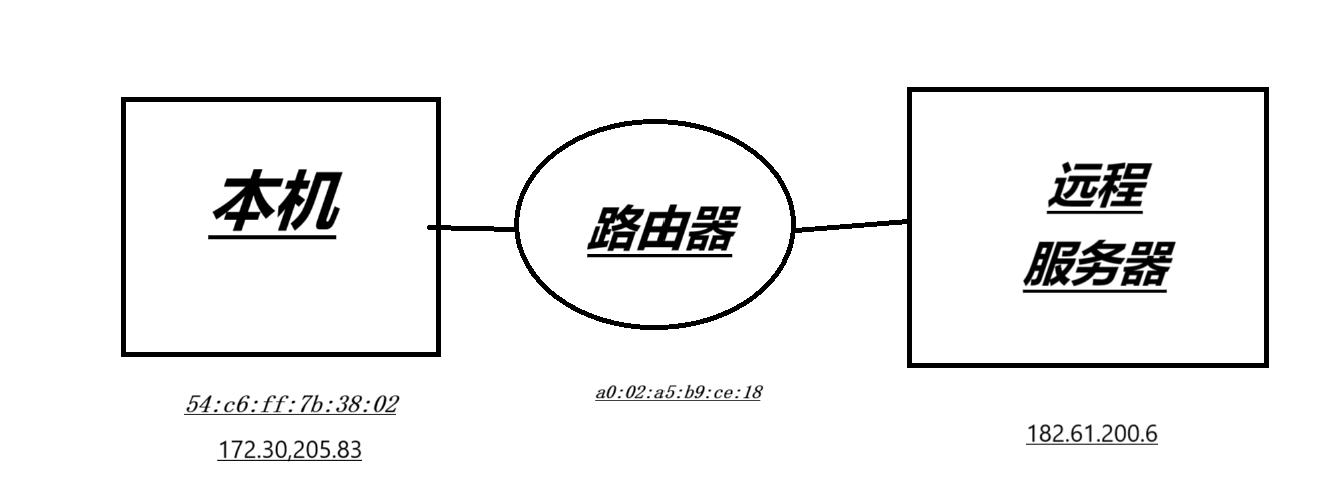
本机MAC地址：54:c6:ff:7b:38:02

本机IP地址：172.30,205.83

路由器MAC地址：a0:02:a5:b9:ce:18

目标IP地址：182.61.200.6

于是可以画出如下关系图：

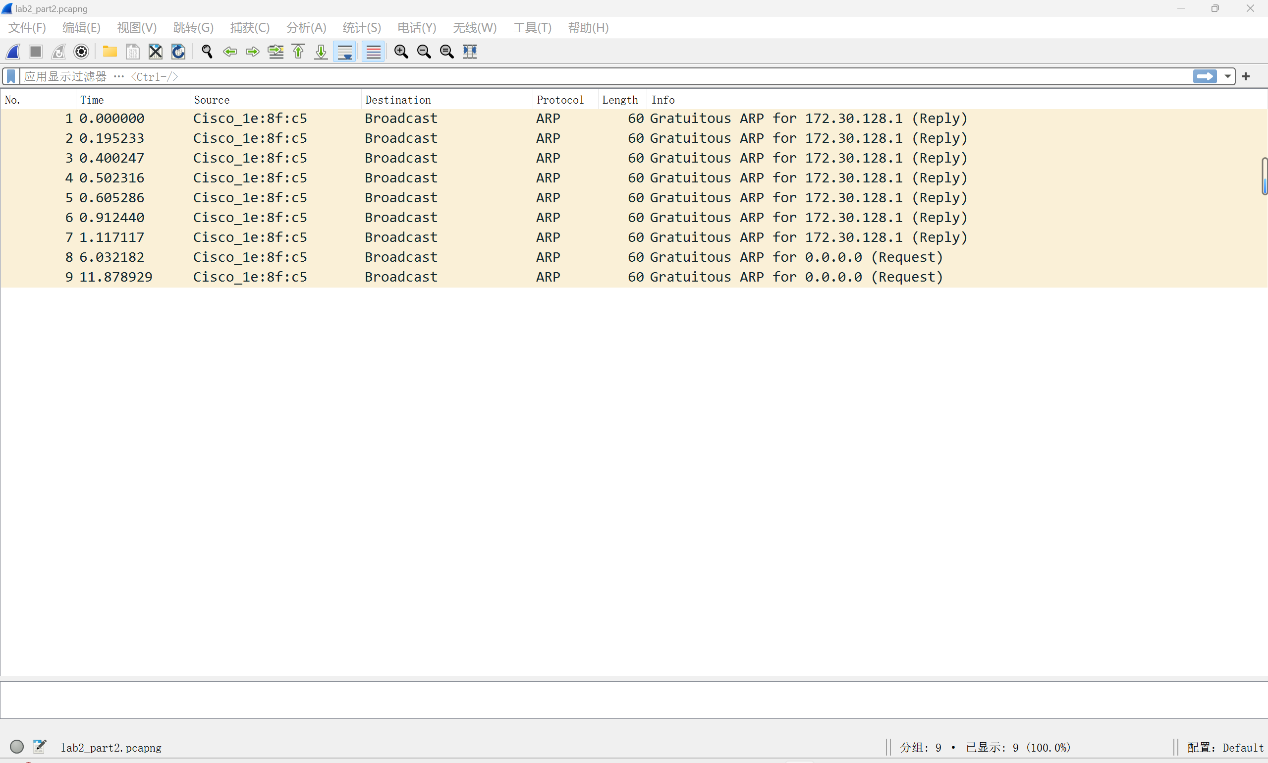


**4.分析以太网的广播帧**

**4.1捕获广播帧**

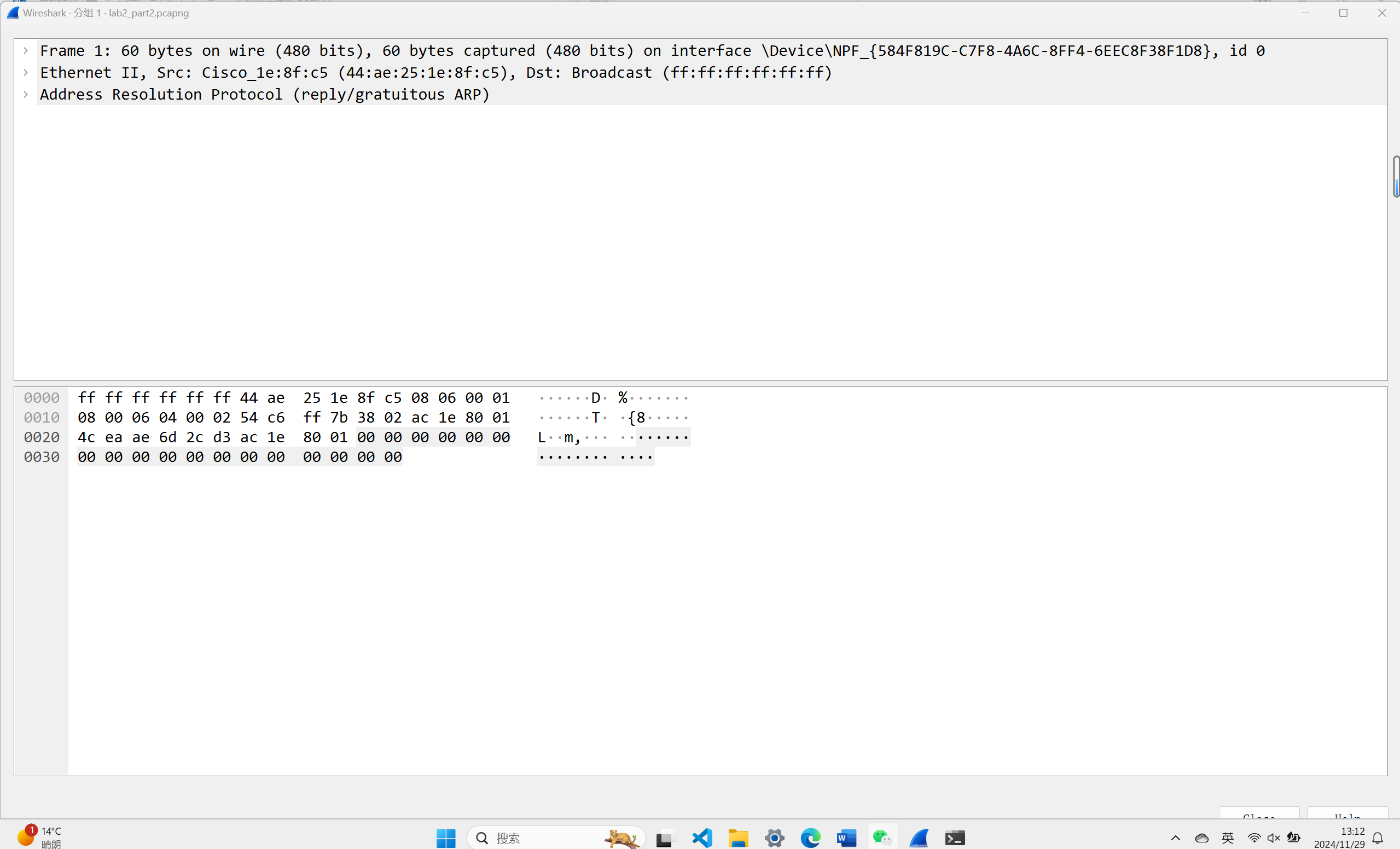
启动 Wireshark，在菜单栏的捕获 → 选项中进行设置，选择已连接的以太网，设置捕获过滤器为 ether multicast，捕获以太网的广播帧。

经过一段时间之后得到如下结果：

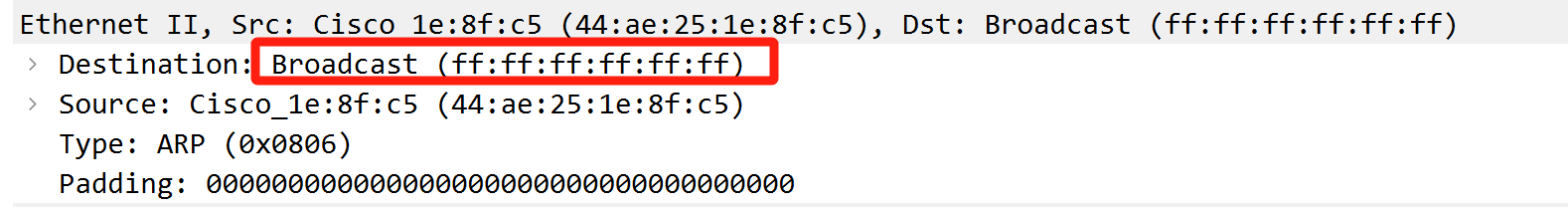


4.2 分析广播帧

打开其中一个，得到如下结果：

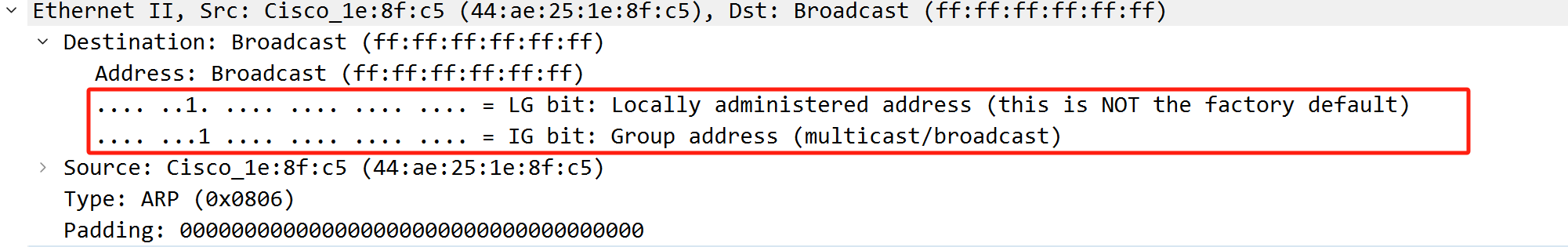


**（1）wireshark中以太网广播帧的地址是什么?**



从上图可以看出，广播帧的地址为 ff:ff:ff:ff:ff:ff。

**（2）以太网地址中哪个比特位是用来确定是单播或多播/广播?**



根据图中信息可以看出，第八位IGbit用于确定是单播还是多播/广播。

**5.问题分析**

**1. How long are the combined IEEE 802.3 and LLC headers compared to the DIX Ethernet headers? （与 DIX 以太网接头相比，IEEE 802.3 和 LLC 接头的组合有多长？）**

1. DIX报头长度为 14 字节。它包含目的 MAC 地址（6 字节）、源 MAC 地址（6 字节）和类型字段（2 字节） 通常为14字节。

2.IEEE 802.3 帧头长度为 14 字节，其中包括目的 MAC 地址（6 字节）、源 MAC 地址（6 字节）和长度字段（2 字节），这里为14字节。

而对于LLC（逻辑链路控制）头，LLC 帧格式包括目的服务访问点DSAP和源服务访问点SSAP，各占 1 字节，在这之后为控制字段，一个字节 。

所以 IEEE 802.3 和 LLC 组合报头长度为17字节。

**2. How does the receiving computer know whether the frame is DIX Ethernet or IEEE 802.3?（接收计算机如何知道帧是 DIX 以太网还是 IEEE 802.3？）**

**ANS：**

在 DIX 以太网帧中，在 MAC 头部之后有一个 2 字节的Type字段。这个类型字段用于标识上层协议。

在 IEEE 802.3 帧中，MAC 头部之后是一个 2 字节的Length字段，它表示数据字段的长度。

根据 Type/Length 字段，如果该字段的值小于或等于 0x600（十进制为 1536），则表示 Length，为IEEE 802.3，否则表示 Type，为 DIX 以太网。

**3. If IEEE 802.3 has no Type field, then how is the next higher layer determined? Use Wireshark to look for the demultiplexing key.（如果 IEEE 802.3 没有 Type 字段，那么如何确定下一个更高的层？）**

IEEE 802.3 中会有LLC报头确定下一个更高的层协议。LLC 头中的 DSAP 字段可以指示上层协议。

**五、实验结果总结**

1. 通过本次实验，我深入理解了 Ethernet 帧结构，清晰地认识到其头部包含目的 MAC 地址（6 字节）、源 MAC 地址（6 字节）、类型字段（2 字节）等关键部分，而负载部分则是紧随头部之后的数据内容，其范围依据帧的总长度和头部长度而定。

2.通过绘制了包含电脑、路由器和远程服务器相对位置的示意图，我对网络设备在不同网络层次中的连接与通信机制有了直观的认识，有助于理解数据在网络中的传输路径和地址转换过程。

3.更具 Wireshark 捕获的数据，我明白了以太网广播帧的地址为FF:FF:FF:FF:FF:FF；了解到以太网地址的第一个字节的最低位（第 8 位）用于确定是单播（为 0）或多播 / 广播（为 1），进一步加深了对以太网地址分类机制的理解。

通过本次实验，不仅在实践操作上熟练掌握了 Wireshark 这一强大的网络分析工具的使用方法，更在理论知识层面深入理解了以太网帧的结构、地址范围以及广播帧的特性。在实验过程中，将理论知识与实际操作紧密结合，使我们对以太网这一基础网络技术有了全面而深入的认识。

**六、附录**

无