

实验报告：Ethernet 实验二

课程名称：计算机网络 年级：大二

上机实践成绩：

实践

指导教师：章玥

姓名：邱吉尔

学号：10235101533

上机实践日期：

2024/11/25

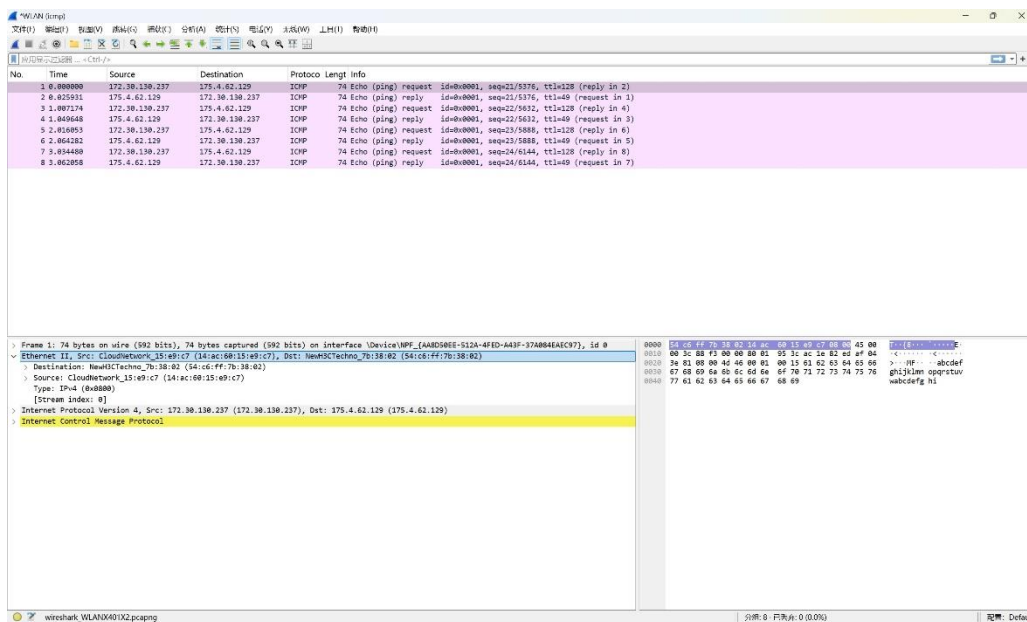
一、目的

- 1、掌握网络抓包工具 Wireshark、网络诊断工具 ping 的用法；
- 2、使用网络诊断工具 ping 触发网络消息；
- 3、使用网络抓包工具 Wireshark 获取并分析以太网数据帧；
- 4、掌握以太网帧的结构；
- 5、分析以太网地址范围；

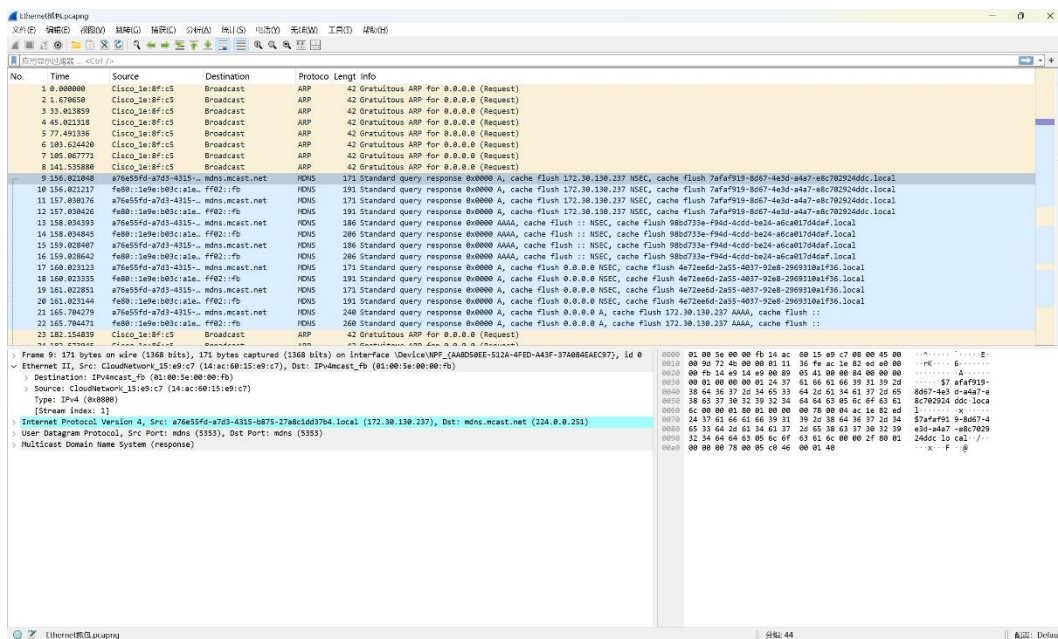
二、实验步骤

1. 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，勾选 Resolve MAC addresses 然后开始捕获。
- ②打开命令行，输入 ping www.bilibili.com.
- ③打开 Wireshark， 停止捕获。

捕获结果如下：

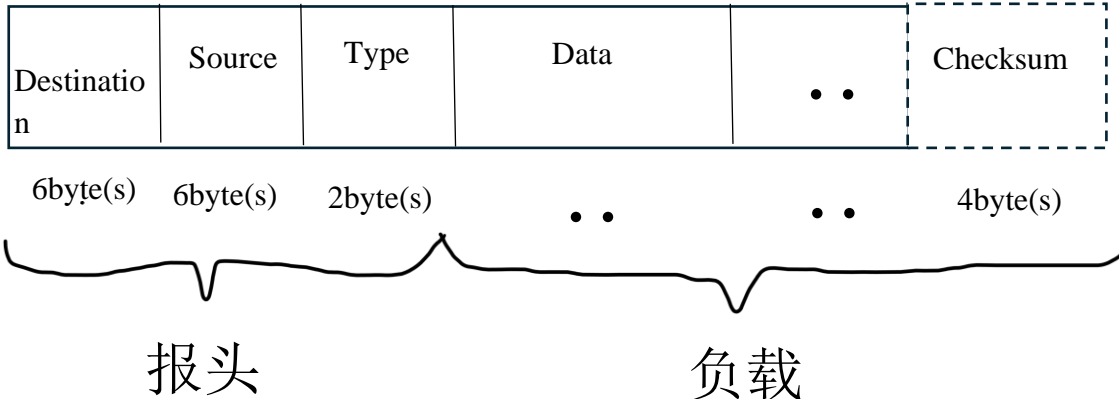


2. 使用“ether multicast”过滤器开始对广播和多播以太网帧进行捕获，等待 30 秒记录背景流量，然后停止捕获。
- 捕获结果如下：



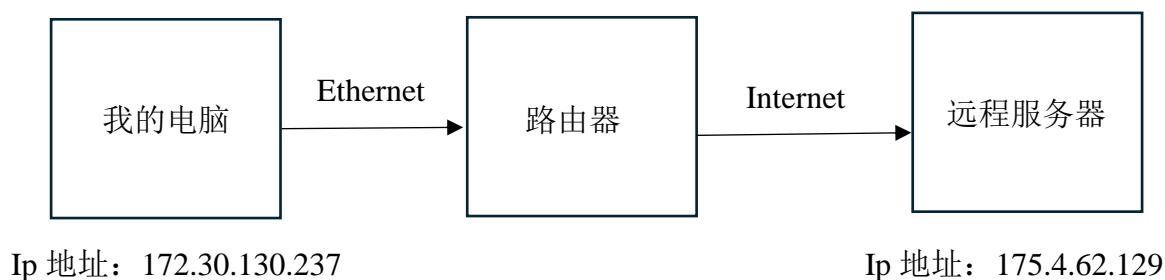
三、实验结果分析

- 1、基于对以太网帧格式的理解，绘制 ping 消息的图形，该图形以字节为单位显示以太网报头字段的位置和大小。图形可以简单地将框架显示为一个细长的矩形。先出现在包中的是最左边的字段，会先通过网络发送。在此图中，显示以太网报头和以太网负载的范围。最后添加一个虚线框来表示 4 字节校验和。



- 2、画一个图,显示你的电脑,路由器和远程服务器的相对位置。标记你的电脑和路由器的以太网地址。标记你的计算机和远程服务器的 IP 地址。同时也在绘图中显示出以太网和其他网络。

以太网地址: 14:ac:60:15:e9:c7 以太网地址: 54:c6:ff:7b:38:02



分析以太网广播帧或多播帧的格式回答下面问题:

- 1、以太网广播帧的地址是什么,以 Wireshark 显示的标准形式写出。

由实验步骤 2 中截图可知，以太网广播帧的地址是 (ff:ff:ff:ff:ff:ff)

```
> Frame 8: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{AA8D50EE-512A-4FED-A43F-37A084EAC97}, id 0
  Ethernet II, Src: Cisco_1e:8f:c5 (44:aa:25:1e:8f:c5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      . . . . . 1 . . . . . = LG bit: Locally administered address (this is NOT the factory default)
      . . . . . 1 . . . . . = IG bit: Group address (multicast/broadcast)
```

- 2、哪几个比特位的以太网地址是用来确定是单播或多播/广播的？

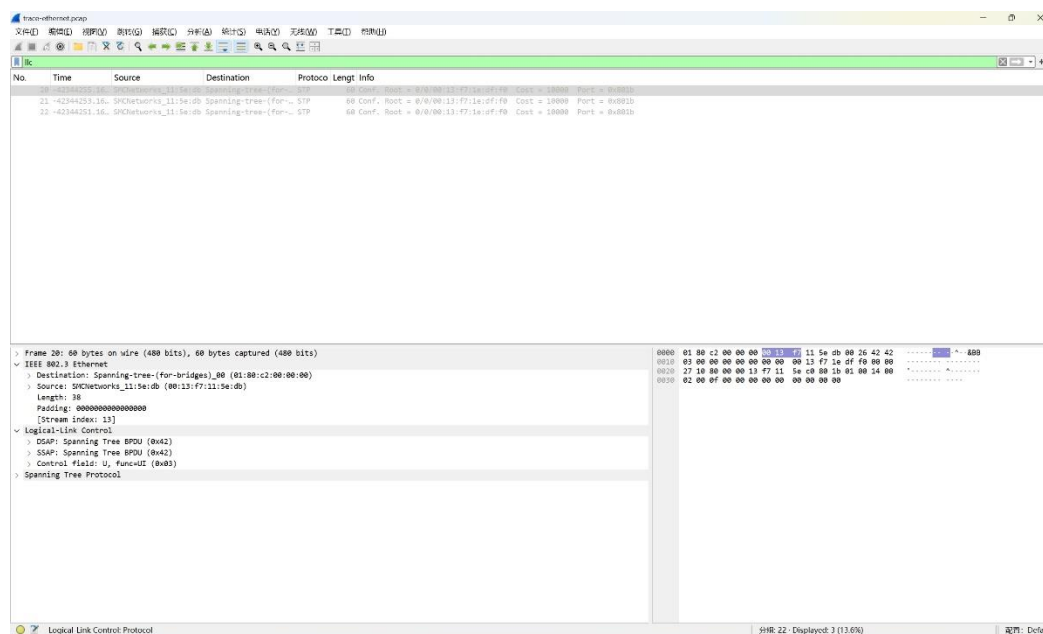
MAC 地址的第一个字节的最低有效位用于指示单播或多播

如果最低有效位是 **0**，则该 MAC 地址是单播地址

如果最低有效位是 **1**，则该 MAC 地址是多播地址

而广播地址是所有 48 位都是 1（即 FF:FF:FF:FF:FF:FF）

IEEE 802.3 数据包分析：（本机未抓取到 802.3 数据包，使用了大夏学堂上的资源）



1.与 DIX 以太网报头相比，IEEE 802.3 和 LLC 组合报头有多长？

您可以使用 Wireshark 解决此问题。 请注意，Trailer / Padding 和 Checksum 可能显示为标头的一部分，但它们位于帧的末尾。

IEEE802.3 总长度为 22Bytes,去除 8Bytes 的 padding，长度应为 14Bytes
LLC 长度为 3Bytes
因此组合报头长度为 17Bytes

2.接收方计算机如何知道该帧是 DIX 以太网还是 IEEE 802.3？ 提示：您可能需要同时使用 Wireshark 查看数据包示例并查找相关文献。

可以通过查看 Type 字段区别帧是 DIX 以太网还是 IEEE 802.3。不同的 Type 字段值可以用来区别这两种帧的类型，当 Type 字段值小于等于 0x05DC 时，帧使用的是 IEEE 802.3 格式。当 Type 字段值大于等于 0x0600 时，帧使用的是 DIX 格式

3. 如果 IEEE 802.3 没有类型字段，那么如何确定下一层？ 使用

Wireshark 查找解复用键。

```
[Stream index: 13]
▼ Logical-Link Control
  ▼ DSAP: Spanning Tree BPDU (0x42)
    0100 001. = SAP: Spanning Tree BPDU
    .... ...0 = IG Bit: Individual
  ▼ SSAP: Spanning Tree BPDU (0x42)
    0100 001. = SAP: Spanning Tree BPDU
    .... ...0 = CR Bit: Command
  ▼ Control field: U, func=UI (0x03)
    000. 00.. = Command: Unnumbered Information (0x00)
    .... ..11 = Frame type: Unnumbered frame (0x3)
```

使用 DSAP 和 SSAP 字段作为解复用键帮助识别数据包的目标协议和源协议

在此抓包中，DSAP 和 SSAP 值为 0x42，表示后续数据包是 **IPX**