华东师范大学软件学院实验报告

实验课程：计算机网络实践	年级：2023 级本科	实验成绩：
实验名称：Lab2 Ethernet	姓名：张梓卫	
实验编号：（2）	学号：10235101526	实验日期：2024/11/29
指导老师：刘献忠	组号：	实验时间：2 课时

目录

一 实验目的

该实验是课程《计算机网络实践》的第二次实验，全名《Ethernet》，目标如下：

- 1. 掌握网络抓包工具 Wireshark 分析以太网数据帧的过程、网络诊断工具 ping 的用法；
- 2. 掌握以太网帧的结构；分析以太网地址范围；分析以太网的广播帧。

二 实验内容与实验步骤

- Step One: Capture a trace. 使用 Wireshark 捕捉 ping 数据包。
- Step Two: Inspect a trace. 在 Wireshark 中查看包。
- Step Three: Ethernet Frame Structure . 辨析并绘制以太网协议头的结构。
- Step Four: Scope of Ethernet Addresses. 绘制一个本地计算机、路由器、远程服务器在以太网中的相对布局图，并表示 IP 地址与 MAC 地址。
- Step Three: Broadcast Frames. 分析以太网广播帧的格式回答下面问题：
- 1. 以太网广播帧的地址是什么, 以标准的形式写在 Wireshark 上显示?
- 2. 那几个比特位的以太网地址是用来确定是单播或多播/广播吗?

三 实验环境

使用 Wireshark v4.2.5, Windows 11 Pro, Wget / Ping Tools 进行实验。
实验报告使用 LaTeX 进行撰写，使用 Vim 编辑器进行文本编辑。

四 实验过程与分析

1 实验环境准备

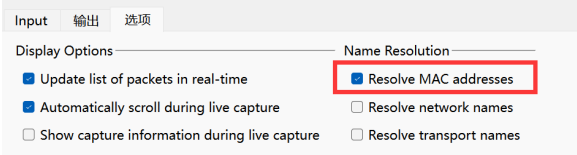

图 1: 开启 Resolve MAC Addresses 选项

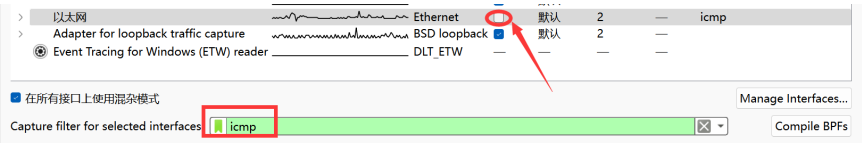

图 2: 开启 ICMP 捕获过滤器

2 发送 ping 请求并捕获

Wireshark 开始捕获后，用命令行向 www.baidu.com 发送 ping 请求。

```
26421 ~ master ≠ ?98 ping www.baidu.com

正在 Ping www.a.shifen.com [180.101.50.188] 具有 32 字节的数据：
来自 180.101.50.188 的回复：字节=32 时间=9ms TTL=51
来自 180.101.50.188 的回复：字节=32 时间=12ms TTL=51
来自 180.101.50.188 的回复：字节=32 时间=9ms TTL=51
来自 180.101.50.188 的回复：字节=32 时间=9ms TTL=51

180.101.50.188 的 Ping 统计信息：
    数据包：已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位)：
    最短 = 9ms，最长 = 12ms，平均 = 9ms
```

由于这里的 ping 请求发送了四次数据包，所以在 Wireshark 中抓包也有四次响应 reply，故我们随意选取一个 reply 进行分析即可。

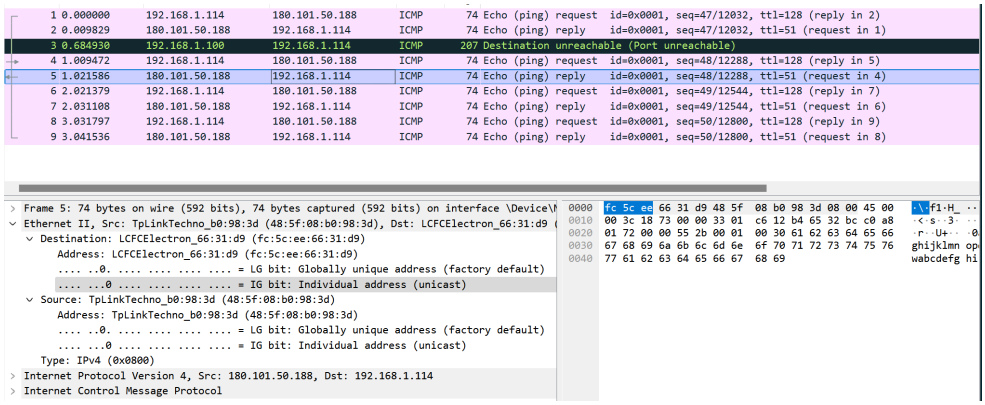

图 3: Wireshark 捕获的 ping 回复包

在 Wireshark 中点击不同的字节，可以对应在左侧看到这部分的内容和意义。要注意的是，大多数跟踪中都没有校验和，即使它确实存在。通常，发送或接收帧的以太网硬件会计算或检查此字段，并添加或删除它。因此，在大多数捕获设置中，操作系统或 Wireshark 根本看不到它。

3 分析以太网帧结构

我们左右对照，逐次点击不同的字段，便可以得出结果，下面是原图中各字段的含义：

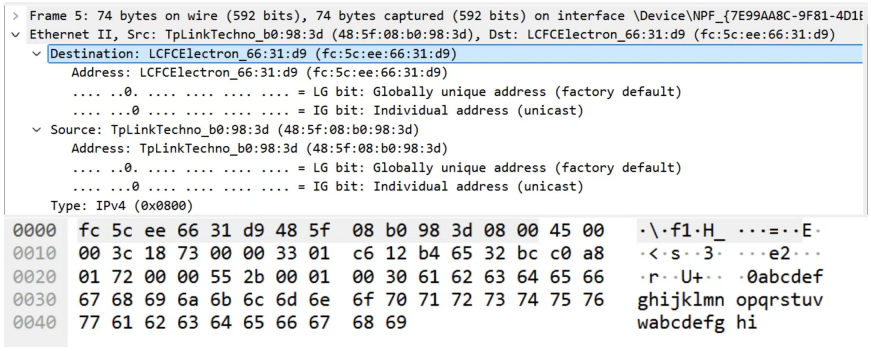

图 4: Combina

现在，我们整理成以下的图片，以在一张图里显示帧结构：

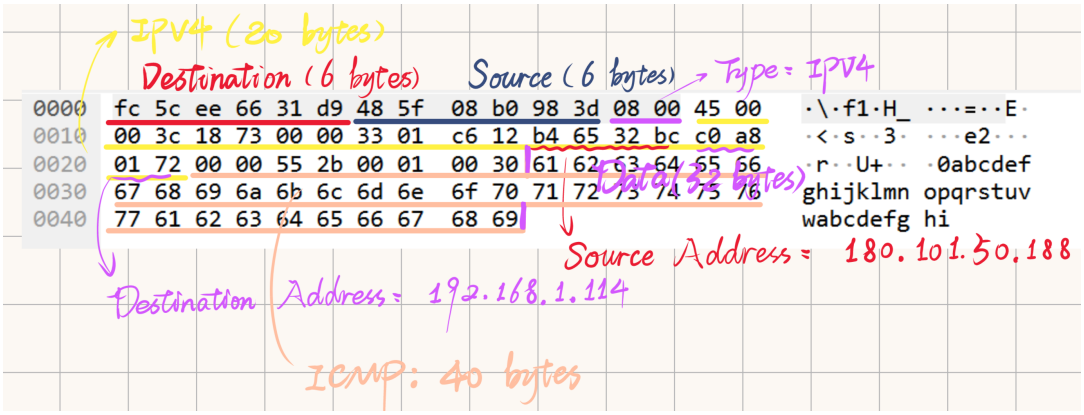

图 5: 帧数据结构

在此图中，可见前 14 个字节为以太网的 Header，其中 Destination 和 Source 各占 6 字节，还剩下 2 字节为 Type 类型，这里是 IPV4.

接踵而至的是 IPV4 数据包，占有 20 个字节，其中体现了 Source Address 和 Destination Address，在此次抓包中，分别是 180.101.50.188 和 192.168.1.114。

后续跟随的是 ICMP 协议，共占 40 字节，其中用紫线分割开的是数据（32 Bytes）。

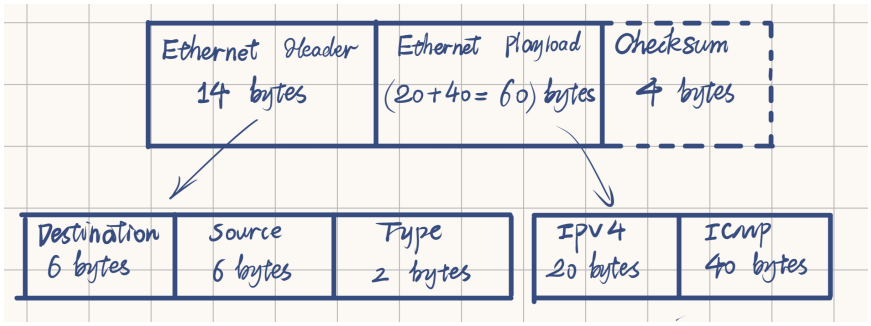

图 6: Structure

4 Scope of Ethernet Addresses

根据实验手册描述：

每个以太网帧都携带一个源地址和目标地址。其中一个地址是您的计算机地址。它是发送帧的源，也是接收帧的目的地。但另一个地址是什么？假设您 ping 了远程互联网服务器，它不能是远程服务器的以太网地址，因为以太网帧只能寻址到一个局域网内。相反，它将是路由器或默认网关的以太网地址，例如 802.11 情况下的 AP。这是将局域网连接到互联网其他部分的设备。相比之下，每个数据包的 IP 块中的 IP 地址确实指示了整个源和目标端点。它们是您的计算机和远程服务器。

据此，以及上面分析获得的两个 IP 地址，可以画出以下的 Scope 图：

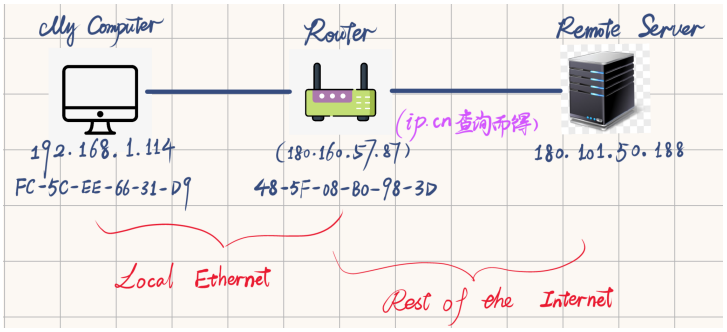

图 7: Scope

5 Broadcast Frames

为捕获以太网广播帧，需要重新抓包，在 Wireshark 中将 Filter 设置为 Ether Multicast，

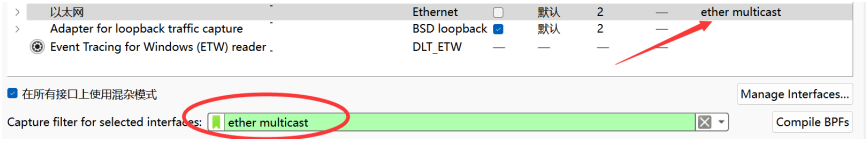

图 8: Ether Multicast

接下来，在命令行中使用 `ipconfig` 命令查询当前的 IP 地址：

图 9: IP Config

然后 ping 本机地址，发送 Broadcast 广播帧：

```
26421  ~  master ≠ ?98  ping 192.168.1.114

正在 Ping 192.168.1.114 具有 32 字节的数据：
来自 192.168.1.114 的回复：字节=32 时间<1ms TTL=128
来自 192.168.1.114 的回复：字节=32 时间<1ms TTL=128
来自 192.168.1.114 的回复：字节=32 时间<1ms TTL=128
来自 192.168.1.114 的回复：字节=32 时间<1ms TTL=128

192.168.1.114 的 Ping 统计信息：
    数据包：已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)，
往返行程的估计时间(以毫秒为单位)：
    最短 = 0ms，最长 = 0ms，平均 = 0ms
```

图 10: Broadcast

进入 Wireshark 查看捕获到的广播帧：

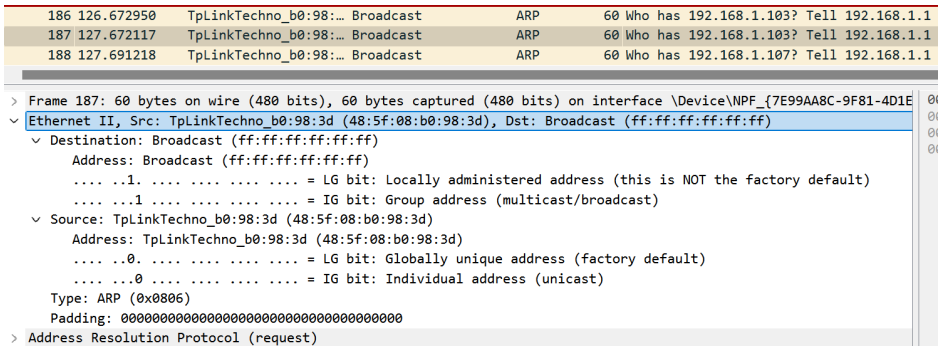

图 11: Wireshark Broadcast

根据 Dst 的内容：`ff:ff:ff:ff:ff:ff`，可以判断这是广播帧广播的地址。
根据下面这张图中提到的 IG bit: Group Address (multicast/broadcast)。
我们可以猜测，是这一位用来确定是单播或多播/广播。
至于为什么可以确定是这一位，可以看到 11 图中，IG bit 在等于 0 和 1 时，后面括号表示了类型。

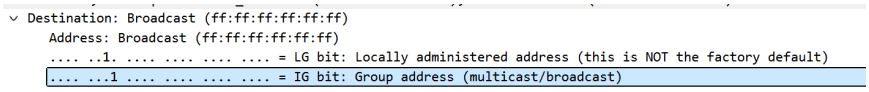

图 12: IG bit

所以，用 Wireshark 格式表达的以太网地址应该为：

```
.......1 ........ ........
```

6 课后思考题

通过解压 lab4stu.rar 获取 trace-ethernet.pcap 文件（在 Lab2 的实验指导手册中，示例图片就是打开了这个）。
用 Wireshark 打开，在上方的过滤器中搜索 llc，如下所示，弹出三个可选项。

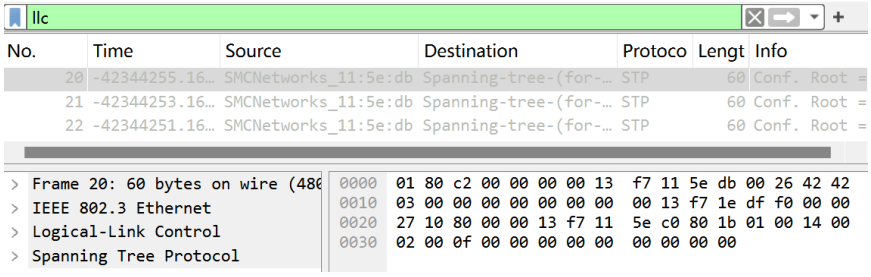

图 13: LLC

6 .1 Question 1

How long are the combined IEEE 802.3 and LLC headers compared to the DIX Ethernet headers? You can use Wireshark to work this out. Note that the Trailer/Padding and Checksum may be shown as part of the header, but they come at the end of the frame.

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。

解答

答：IEEE 802.3 头为 14 个字节，与 DIX 以太网相同。

LLC 又增加了 3 个字节的头，总共有 17 个字节的头。

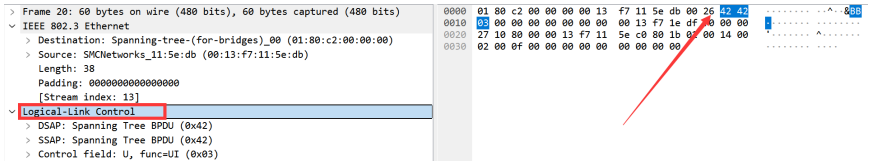

图 14: LLC

6 .2 Question 2

How does the receiving computer know whether the frame is DIX Ethernet or IEEE 802.3? Hint: you may need to both use Wireshark to look at packet examples and read your text near where the Ethernet formats are described.

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。

解答

参考资料：WHAT IS THE DIFFERENCE BETWEEN ETHERNET II AND IEEE 802.3?

如果帧头跟随 Source MAC 地址的 2 Bytes 的值大于 1536(0x600), 则此 Frame 为 Ethernet II。接着比较紧接着的 2 Bytes，如果为 0xFFFF 则为 Novell Ether 类型的 Frame , 如果为 0xAAAA 则为 Ethernet SNAP 格式的 Frame , 如果都不是则为 Ethernet 802.3/802.2 格式的帧。

6 .3 Question 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.

解答

通过 LLC 中的信息确定下一层：读取 DSAP 和 SSAP。

IEEE 802.3 在 IEEE 802.3 报头之后紧接着添加 LLC 报头，以传达下一个更高的层协议。LLC 使用一个称为 DSAP（目的服务接入点）的单一初始字节，而不是 Type 字段中的两个字节。

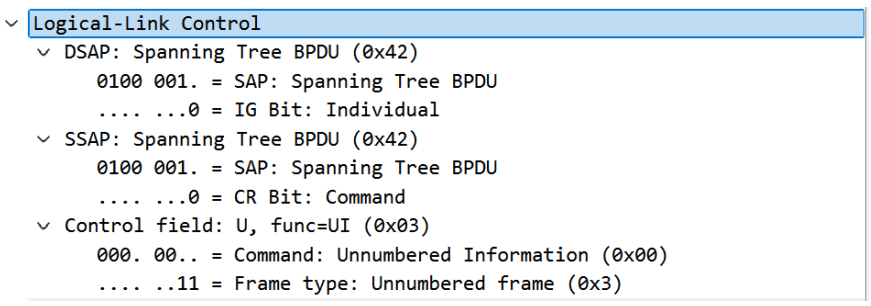

图 15: LLC Demux

五 实验结果总结

实验收获

- 本实验不仅加深了我对以太网帧结构的理解，还通过 Wireshark 工具提供了实践验证。
- 学会了如何通过抓包工具分析网络数据，为后续网络诊断及优化提供了实践基础。
- 通过分析广播帧、多播帧及单播帧的结构和用途，加深了对以太网地址分配和作用范围的理解。

实验不足和改进方向

- 在实验中，由于网络条件的限制，某些情况下捕获的数据量有限，未来可以尝试在更复杂的网络环境中进行类似实验。
- IEEE 802.3 的深入分析中，可以进一步尝试捕获更多类型的帧数据，以验证多种协议下的实际表现。

六 附录

参考资料

- WHAT IS THE DIFFERENCE BETWEEN ETHERNET II AND IEEE 802.3?