Lab1 实验报告

李文彬，1120173001

2020 年 2 月 27 日

1 实验内容

实验报告中记录了根据实验指导进行实现的操作过程，展示实验各关键部分的截图，绘制要求图表，并在相应阶段回答问题。

1.1 实验环境

Macbook pro, macOS Catalina
Wireshark for Mac

2 实验流程

2.1 Step 1：Capture a trace

1. 打开 Wireshark，根据实验指导，在 Wireshark 中 filter 栏输入 “icmp”
2. 打开 Terminal，在终端中输入 ping ”www.baidu.com” 进行抓包
3. 按 “control+c” 快捷键停止 Terminal 中的抓包

2.1.1 过程分析

实验过程中，在 Terminal 中运行 ping www.baidu.com 命令，结果如下

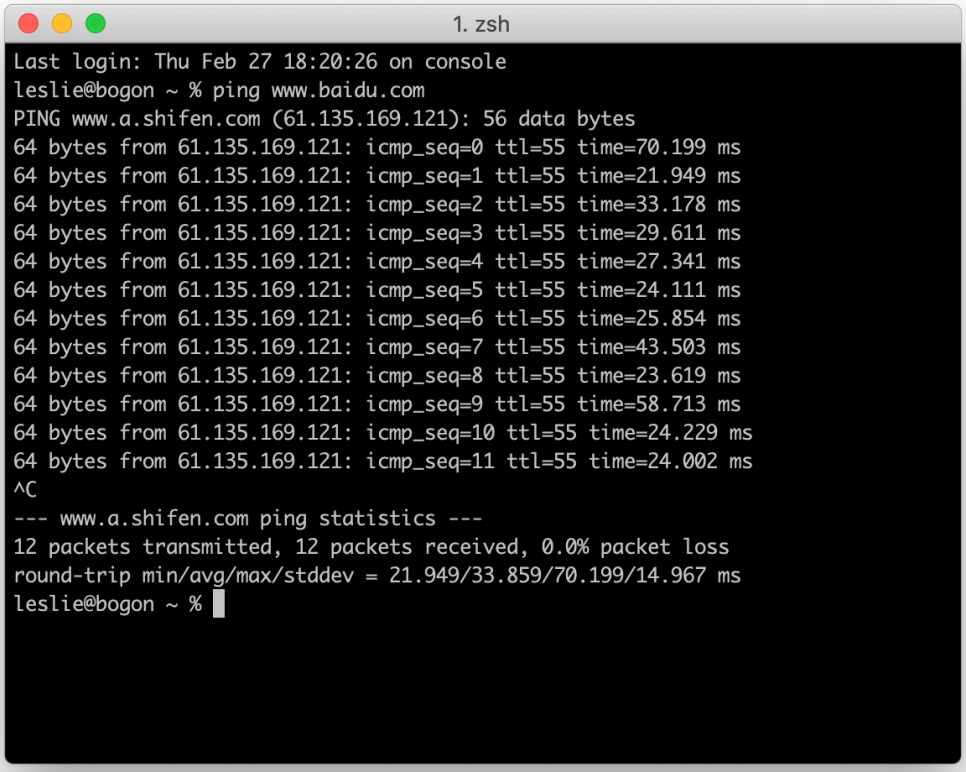

图 1

通过 wireshark 软件捕获 ping 命令后发送接收的包，结果显示如下：

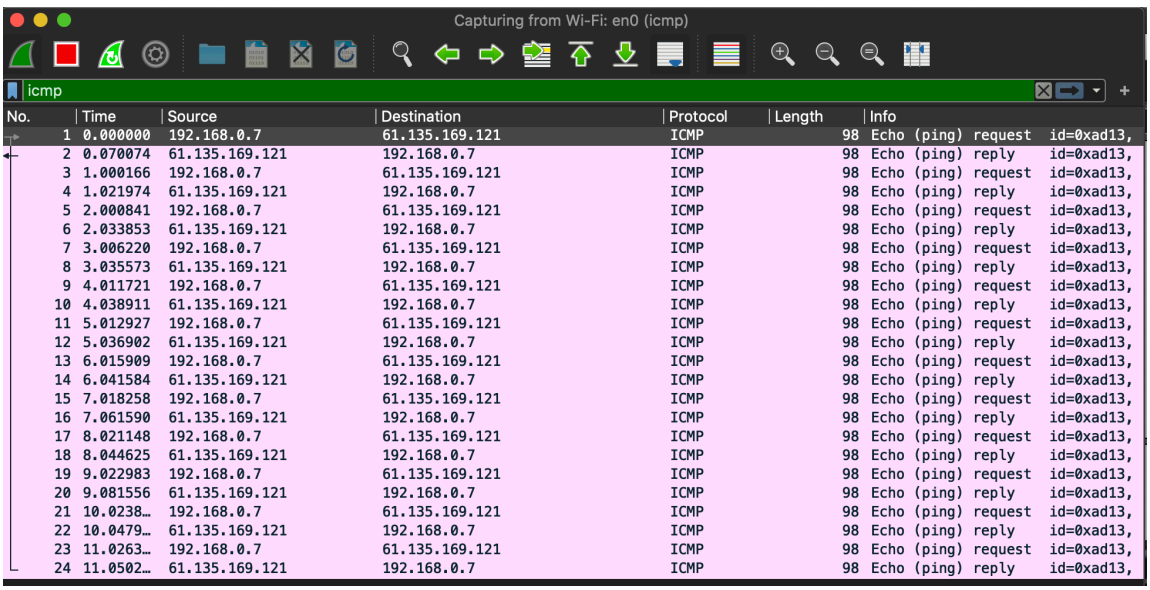

图 2

2.2 Step 2：Ethernet Frame Structure

随机选取图 2 中的一帧，得到 wireshark 的自动进行解析，显示如下:

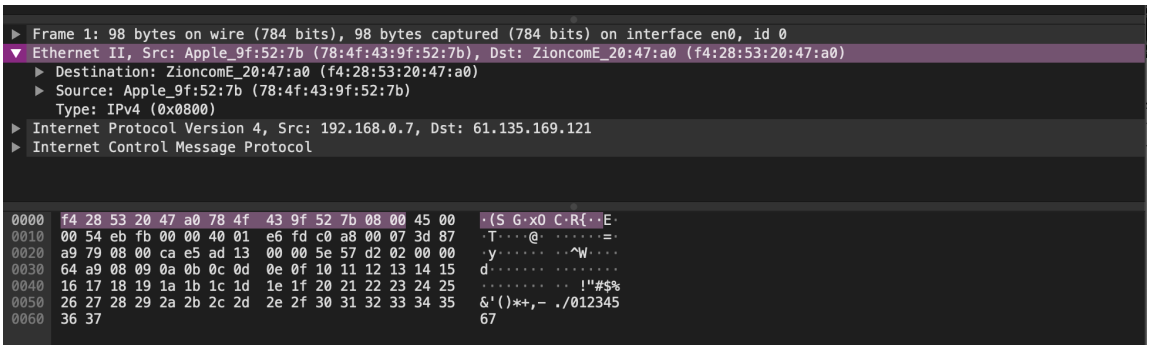

图 3

下部显示的信息共 0x62 字节，与描述 98bytes 匹配（未计算尾部 checksum）。图 3 中选中展开 Ethernet 部分，Wireshark 自动显示其 header 占 14 字节。

2.2.1 Results

根据描述信息可知，实验中采用的是 Ethernet II 协议，由 header、data 和 checksum 组成，Ethernet II 协议的帧结构如下图:

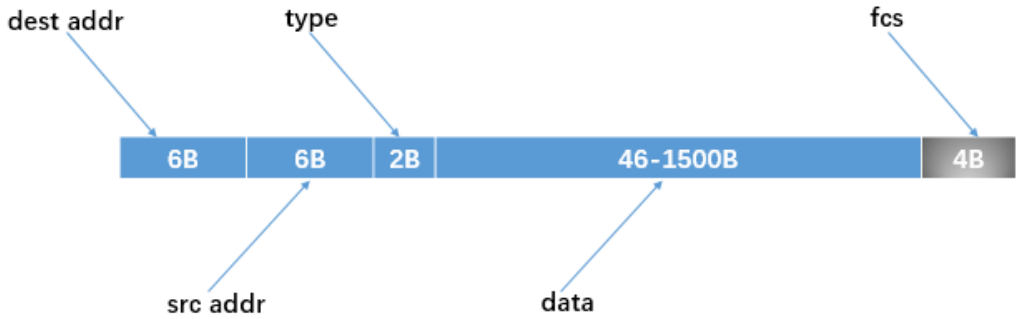

图 4

2.3 Step 3：Scope of Ethernet Addresses

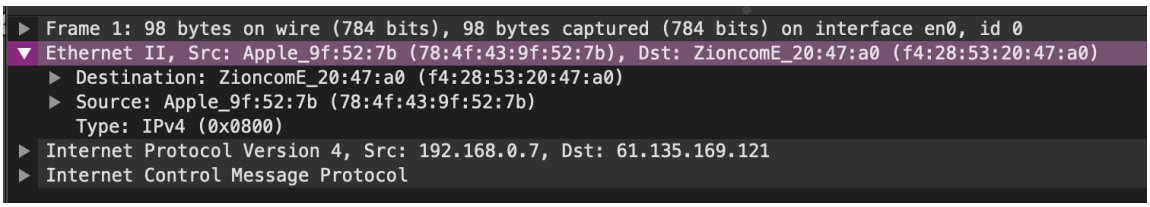

图 5

以上图的 Ethernet frame 为例，src 与 dest 的物理地址分别为（78:4f:43:9f:52:7b）（18:31:bf:4a:be:80），本机 ip 为（192.168.0.7），remote server 的 ip 为（61.135.169.121）。因此 my computer，router 和 remote server 的相对位置如图所示：

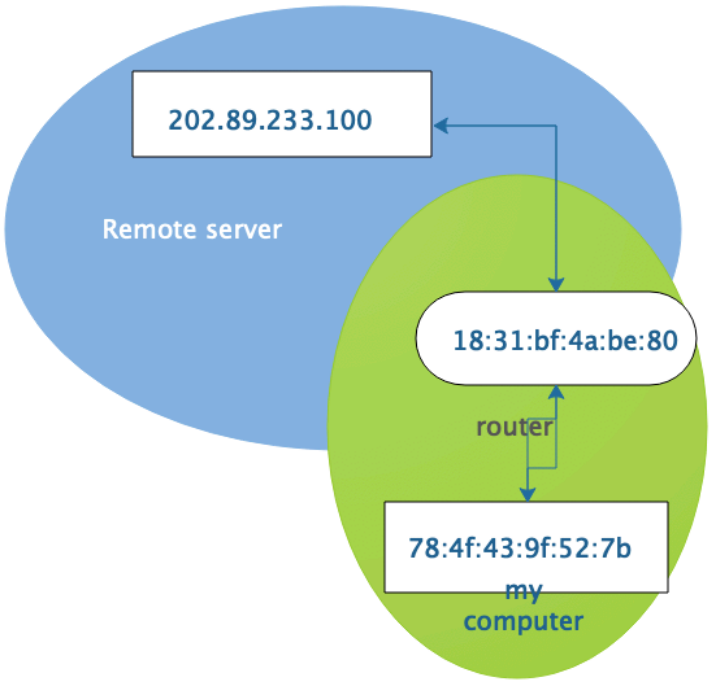

图 6

3 Broadcast Frames

通过如下所示 filter，只显示以太网的多播 multicast 或广播 broadcast 消息。

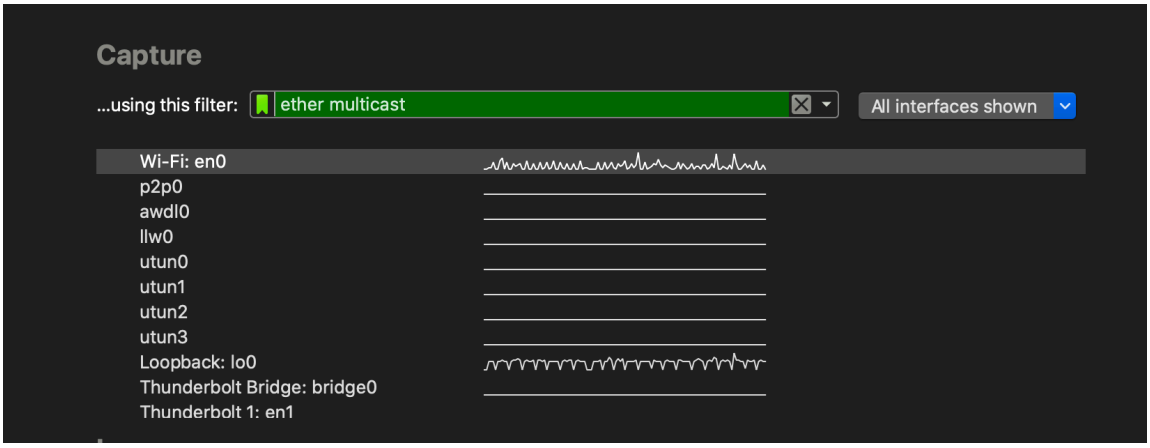

图 7

以下是截获到的 broadcast 和 multicast 样例。

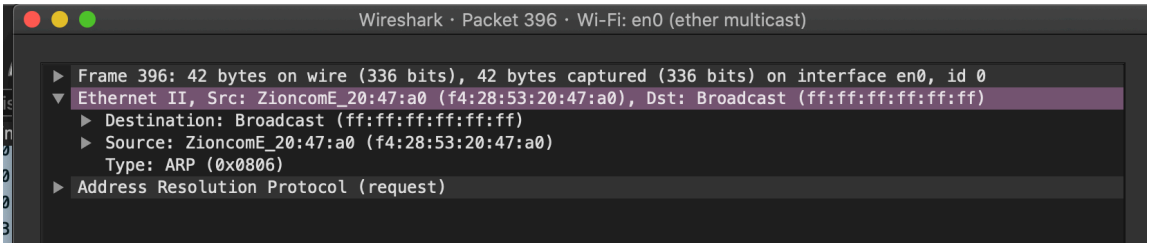

图 8

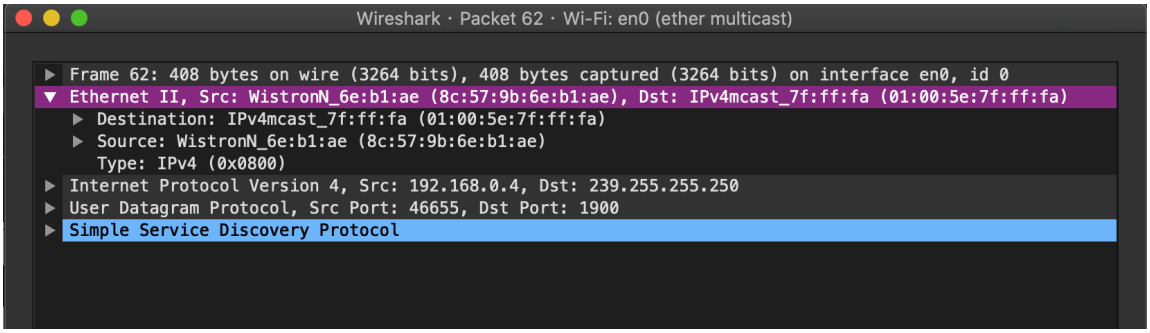

图 9

4 Answering the following question

i What is the broadcast Ethernet address, written in standard form as Wireshark displays it?

图 8 可见，broadcast 的目的地址为（ff:ff:ff:ff:ff:ff），即 48bit 全为 1。

ii whether it is unicast or multicast/broadcast?

分析 multicast 的目的物理地址段，wireshark 软件显示 Group address 标志位为第 8 位，如下图所示，其地址的第一字节为 01H，标识位为 1 表示多播。

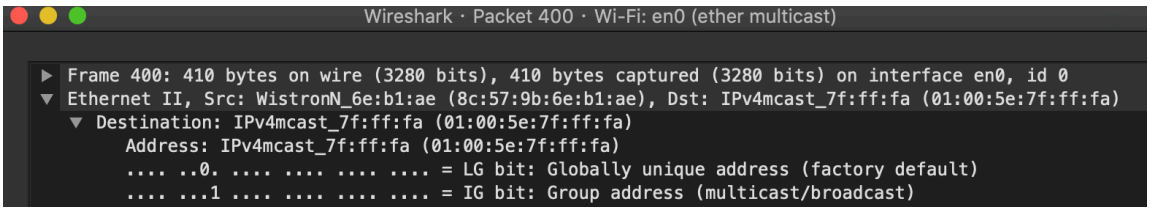

图 10