**计算机网络编程**

**实验报告**

**班级：07111707**

**组长：1120171189 崔程远**

**成员：1120172149 吴沁璇**

**1120172153 张澈**

**1120172163 王晓媛**

**1120172736 张鉴昊**

**1120172765 曾煜瑾**

**1120173326 曾紫飞**

**北京理工大学**

**计算机学院**

**2020年4月**

**第四章 实验1 链路层抓包及协议分析**

**1. 实验目的**

利用WinPap实现网络数据链路层帧捕获，显示分析帧和上层包结构。

**2. 实验内容**

程序运行屏幕输出要点：

首先屏幕显示当前配置的网络适配器，并要求选择捕获适配器编号

按照捕获帧的层次关系显示以下信息：

数据链路层（MAC子层）层结构及各个字段的值

网络层分组的格式及各个字段的值

运输层报文段的格式及各个字段的值

应用层报文格式及各个字段的值

**3. 实验原理**

WinPcap是一个基于Win32平台的，用于捕获网络数据包并进行分析的开源库。它提供了以下功能：捕获原始数据包；在数据包发送给某应用程序前，根据用户指定的规则过滤数据包；将原始数据包通过网络发送出去；收集并统计网络流量信息。

**4. 实验环境**

操作系统：Windows 10

编译器：Visual Studio 2017

环境：WinPcap4.1.3 WpdPack

1. **实验步骤**

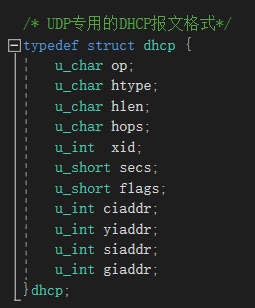
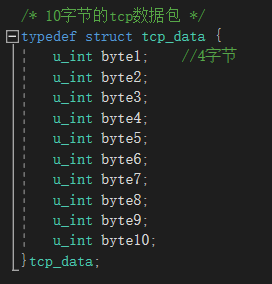
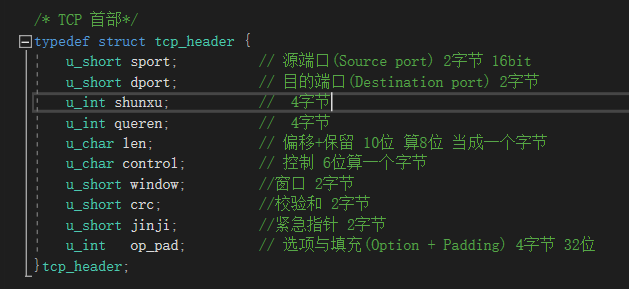
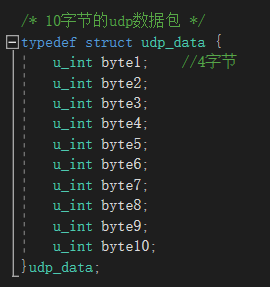
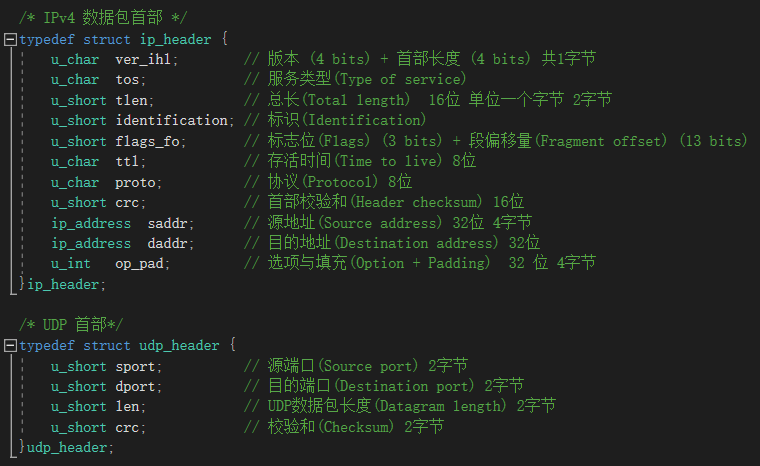
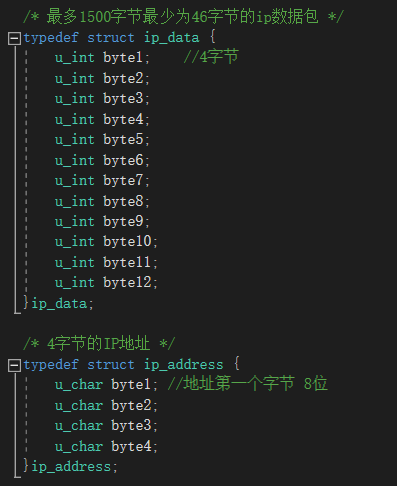
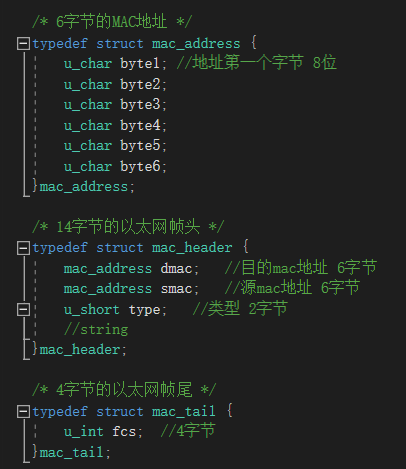
以下是C++代码和具体思路：

1. VS中环境的配置

首先下载WinPcap和WpdPack，然后在vs的项目中添加包含目录和库目录，修改预处理器，添加依赖项。然后就可以进行代码的编写。

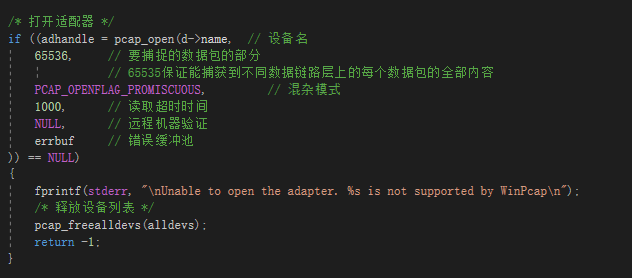
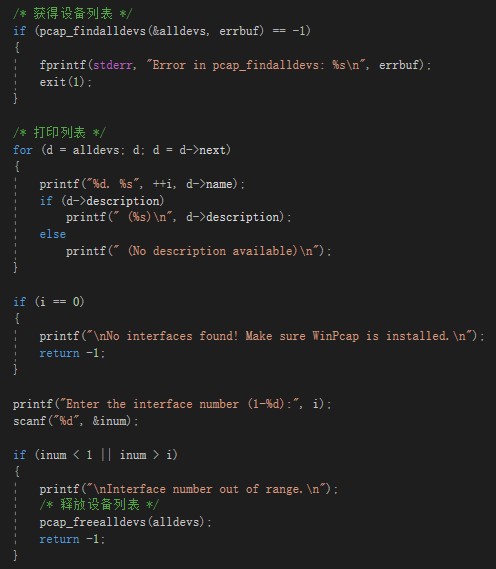
1. 定义数据报头结构

如下图所示，分别定义了以太网帧头、帧尾，IP数据包、IP数据包首部、IP地址、MAC地址，UDP和TCP的数据包和首部，还有应用层的DHCP的报文。根据各个字段的大小用相应的数据类型进行定义。



1. 获得设备并打印设备列表

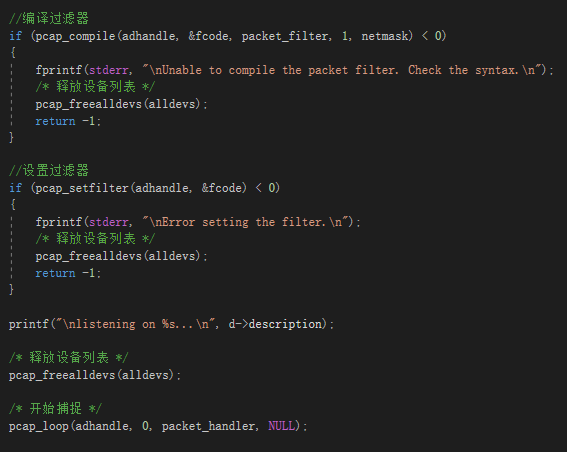
如下图，使用了在WinPacp中文文档给出的函数，来获得设备列表和打印列表设备具体信息。



1. 设置过滤器并调用回调函数

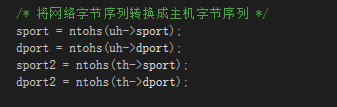
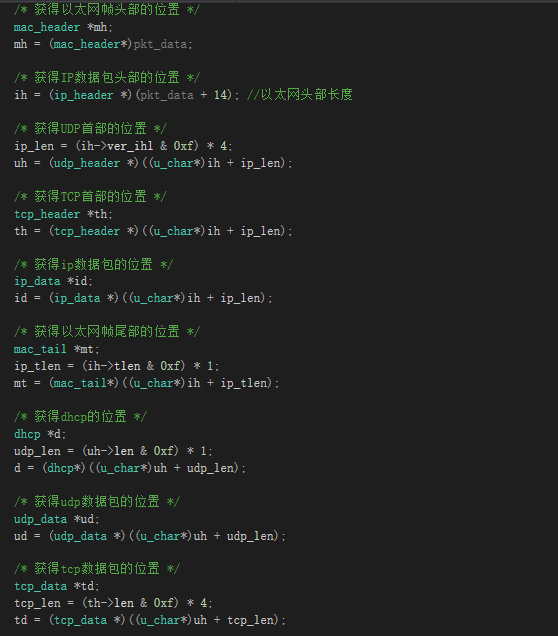
由于捕获的报文信息太多，所以需要设置一个过滤器，用于只处理tcp和udp的报文信息，其他信息都过滤。具体过滤器的设置如下。

1



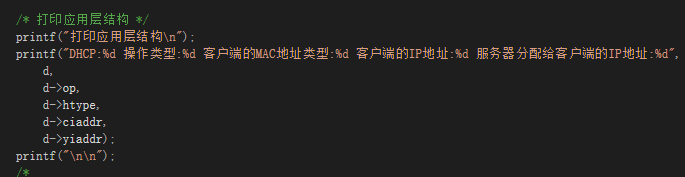
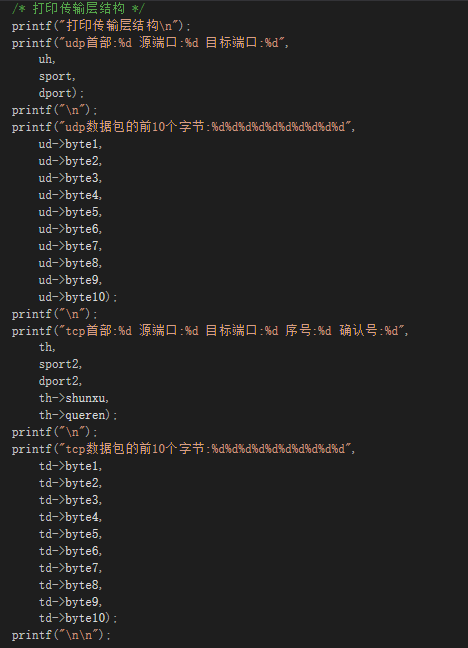
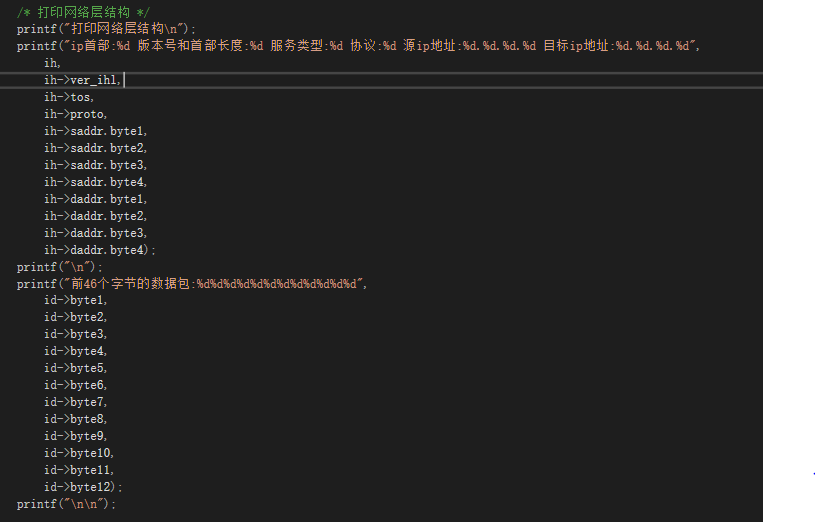
1. 获得各报文具体字段的值

要输出各层结构的值，就要使用之前定义的数据结构用来表示适配器的各个字段。首先将时间戳转换为可识别的格式，然后打印数据包的时间戳和长度。然后根据报文的字段划分将定义的数据结构和获取到的报文的各个字节一一对应，就可以得各字段具体的值。对于上下层结构之间，因为上层的报文首部包含在下层的数据包当中，所以可以通过报文中的数据包长度这一属性和字段的固定长度进行简单的计算，再进行格式的转化，就可以得到上一层结构的报文的首部位置。

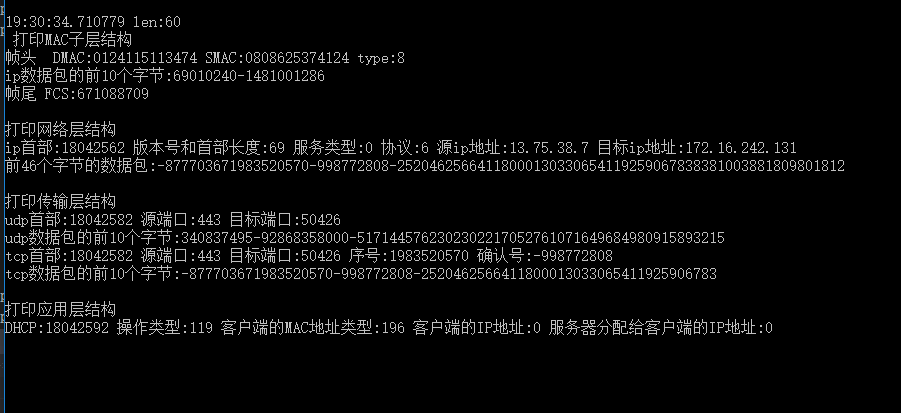
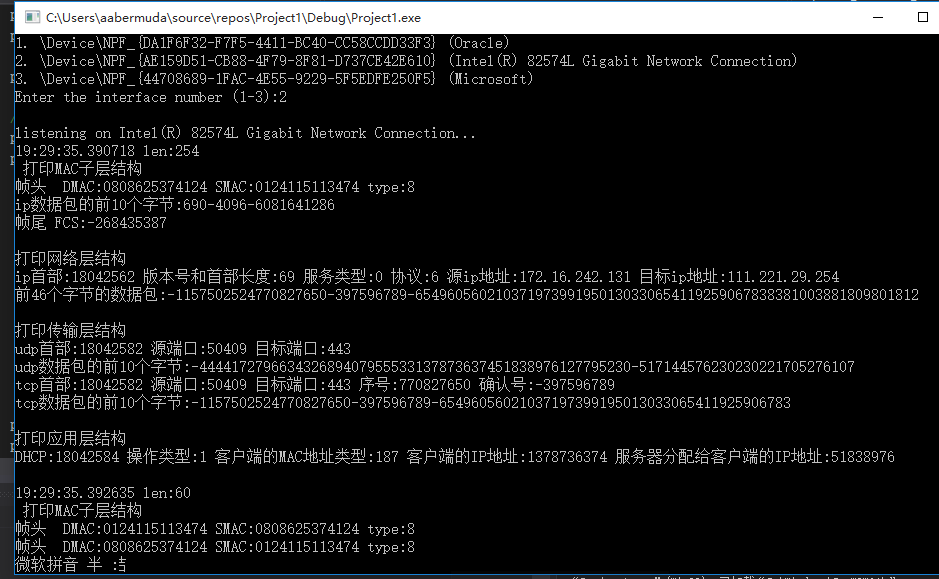
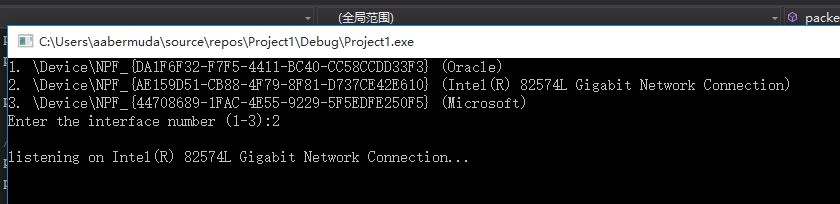
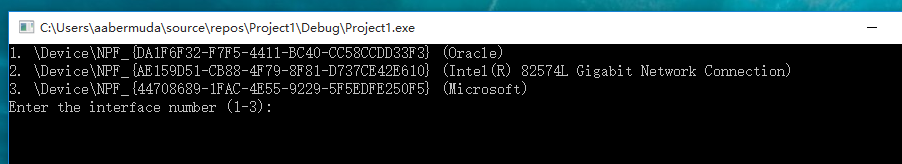


1. 打印各结构的各字段值

最后是打印各个报文的各个字段的具体值。由于在代码编译时，程序必须包含的头文件“pcap.h”和string、ostream之间存在问题导致编译失败，大概是里面有一些重复定义，然而这个问题没能得到解决，所以就只能用printf对结构体的每一项一个个打印出来。



运行结果截图：



如上图所示，选定了2号适配器后，依次打印了各层的结构和格式，以及各个字段的值。由于应用层的协议相对比较复杂，在此只选了DHCP协议进行打印，所得的结果如上图所示。

**6. 实验总结**

本次实验其实说起来并不是很难，主要在于环境的配置和对文档的熟悉，配置winpacp环境就花了很久。好在具体的函数和代码在文档中都给出了示例，所以只需理解了文档中的示例代码，再对对给出的函数加以运用就可以完成这个实验。

本次实验我也遇到了很多的问题，在配置环境上花了不少时间，对报文的各个字段也不熟悉，头文件和源文件的互相包含问题等等。最后还是解决了大部分问题，完成了实验。通过本实验，我更加熟悉了各层之间存在的结构关系，对如何获取高层的报文信息，如何得到每个字段具体值都有了更深的理解，对WinPacp编程也有了一定的认识和了解。