第1节 实验内容说明

本次实验为IP数据报捕获与分析编程实验，要求如下：

（1）了解NPcap的架构。

（2）学习NPcap的设备列表获取方法、网卡设备打开方法，以及数据包捕获方法。

（3）通过NPcap编程，实现本机的IP数据报捕获，显示捕获数据帧的源MAC地址和目的MAC地址，以及类型/长度字段的值。

（4）捕获的数据报不要求硬盘存储，但应以简单明了的方式在屏幕上显示。必显字段包括源MAC地址、目的MAC地址和类型/长度字段的值。

（5）编写的程序应结构清晰，具有较好的可读性。

第2节 实验准备

本次实验需要安装Npcap1.71、npcap-sdk-1.13。

在成功安装后需要对Visual Studio的项目属性配置：

在C/C++中添加附加包含目录：**D:\npcap\Include;**

在预处理器中添加预处理器定义：**WPCAP;HAVE\_REMOTE;**

第3节 实验过程

实现步骤＋流程图

实验流程：

1. 流程图简介

一、

1. 获取设备列表
2. 打开网络接口
3. 捕获数据包

二、数据包分析

1、函数

2、打印显示结果

三、实现效果

完整代码

说明：如果本次实验不是编程实验，则参考书上的实验步骤来编写本节，注意关键处需要添加截图；如果本次实验为编程实验，则本节还需要包含：项目设计思路、关键代码分析。（提交报告时删除此段）

第4节 特殊现象分析

说明：若实验过程有遇到正常实验过程以外的特殊现象并查阅资料弄清楚该现象的成因，可截图说明。如果没有可以省略本节。（提交报告时删除此段）