

****

信息学院软件工程系

《计算机网络》实验报告

**题　　目 实验三 用 PCAP 库侦听并分析网络流量**

**班　　级 软件工程2018级2班**

**姓　　名 卜英乔**

**学　　号 24320182203164**

**实验时间 2020年3月11日**

**2020 年 3 月 17 日**

# 实验目的

本实验是“用 PCAP 库侦听并解析 FTP 口令”实验的第一部分。

用 WinPCAP 或 libPcap 库侦听并分析以太网的帧，记录目标与源 MAC 和 IP 地 址。

基于 WinPCAP 工具包制作程序，实现侦听网络上的数据流，解析发送方与接收 方的 MAC 和 IP 地址，并作记录与统计，对超过给定阈值（如：1MB）的流量进行告警。

# 实验环境

操作系统win10，编程软件visual studio、WinPCAP

# 实验结果

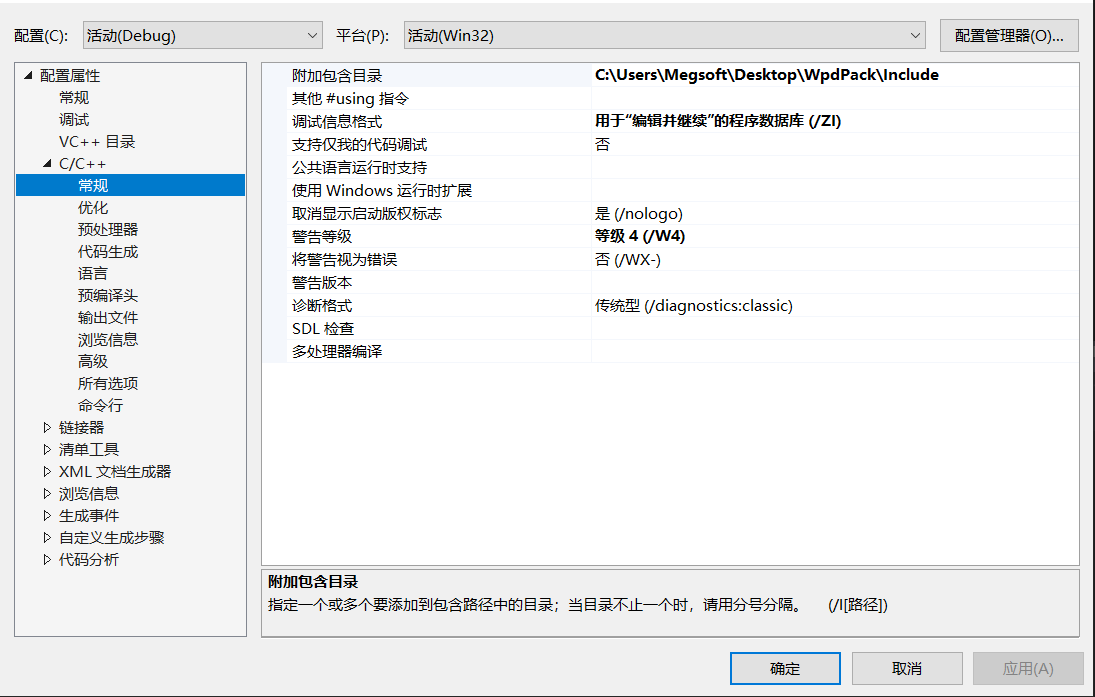
下载winpcap的开发包，网址http://www.winpcap.org/devel.htm，并将其中的Lib文件和Include文件添加到VS studio2013中：

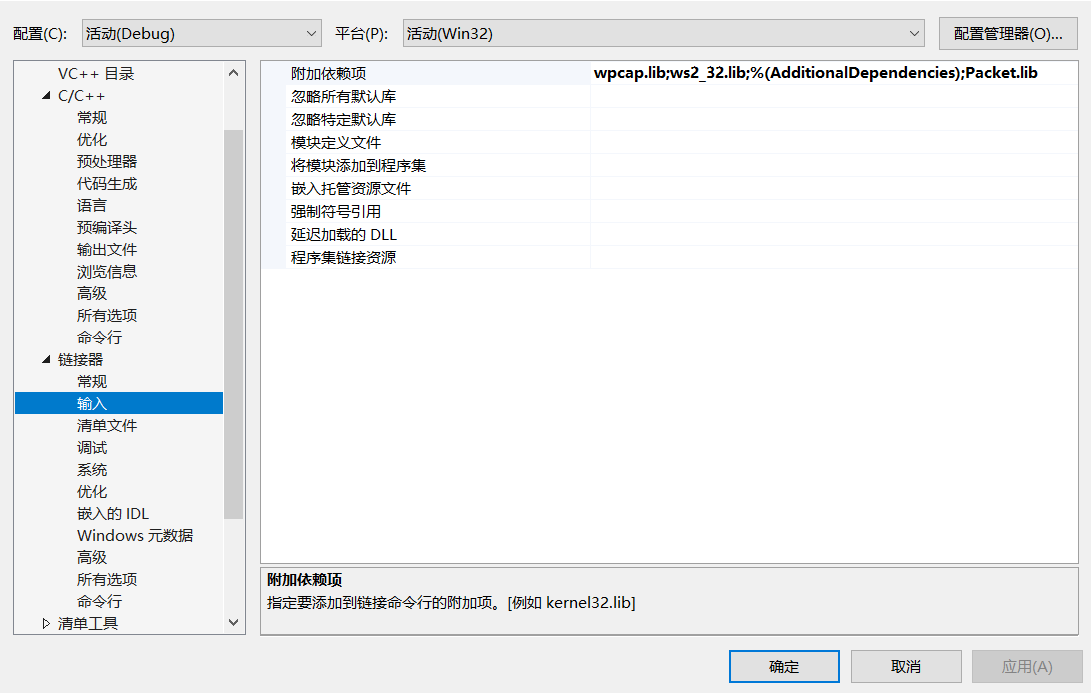
 （1）添加Include文件目录：

     [菜单]“工具->选项->项目和解决方案->c++ 目录”，添加所需“包括文件”目录。

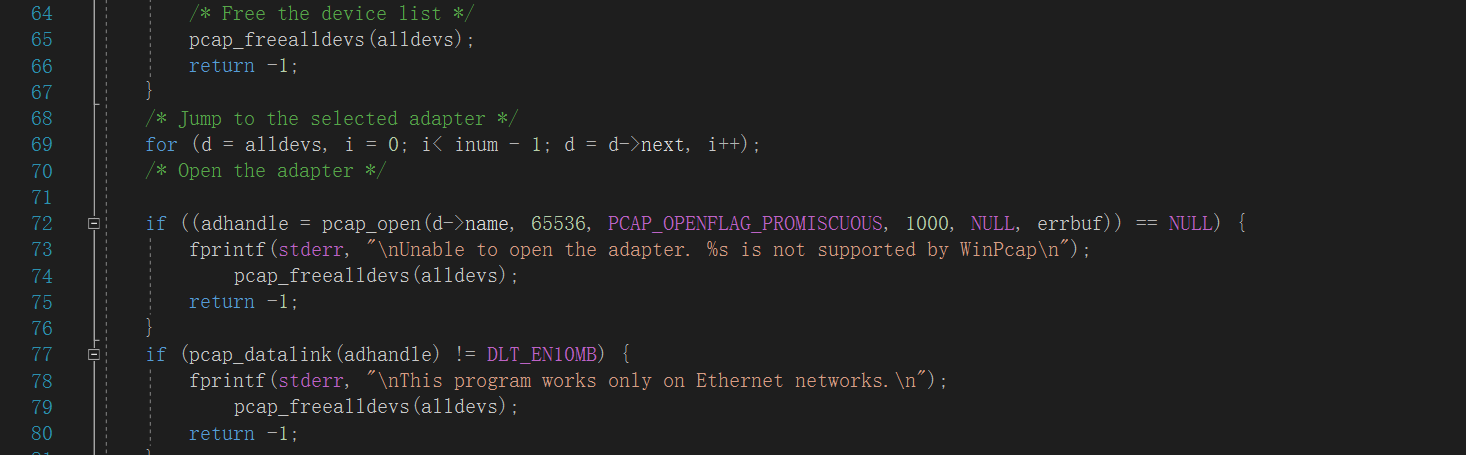
（2）添加Lib文件目录：

    项目->属性->配置属性->连接器->常规->附加库目录”

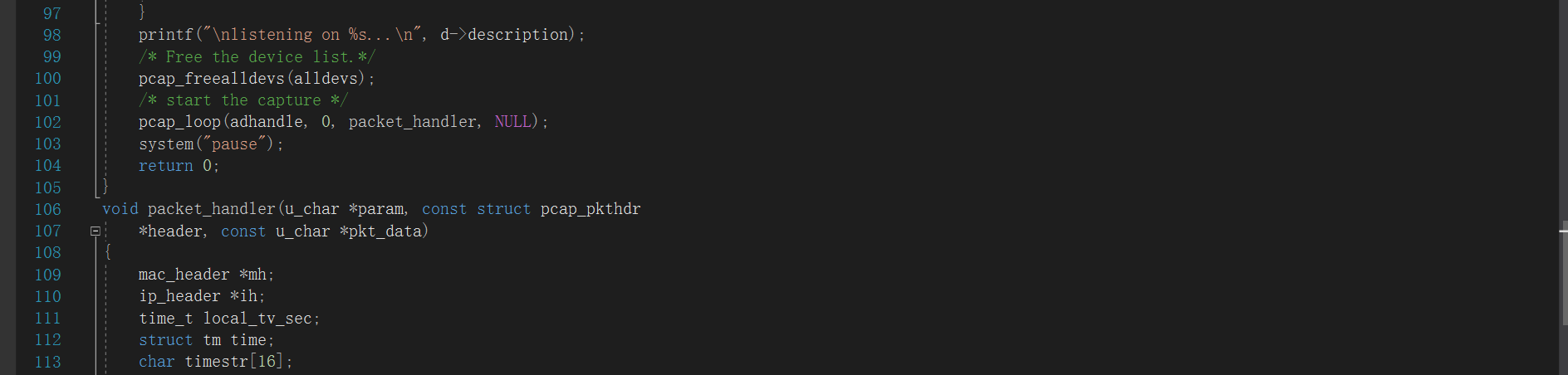
    [菜单]“工具->选项->项目和解决方案->c++ 目录”，选择对应平台，然后添加所需“库文件”目录。还需要添加lib文件到当前项目的输入中，位置：项目-属性，中的“链接器”-“输入”-附加依赖项“中添加lib文件的全名：wpcap.lib.。



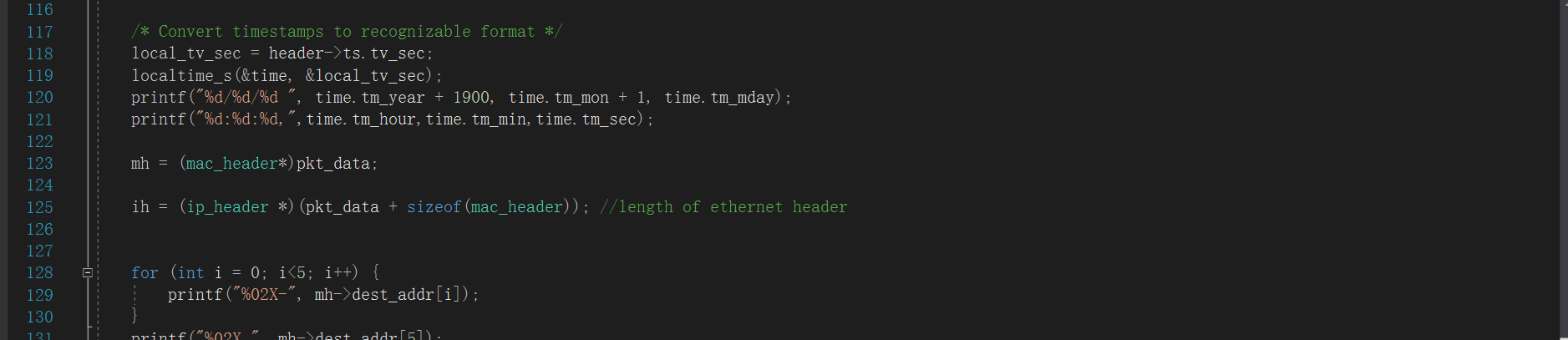
配置好环境后，使用winpcap库中方法进行Free device list、selected adapter等后续功能的编程



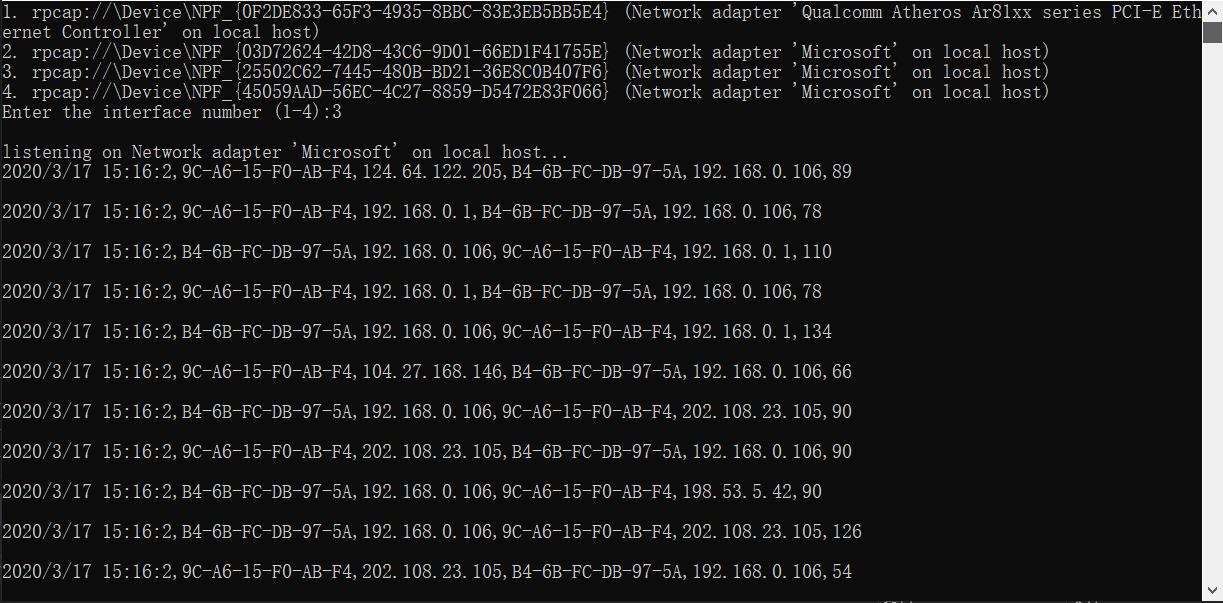
set filter以及捕捉功能



将时间戳转换成可识别的格式



最终运行结果如下：



# 实验总结

通过对于winpcap示例文件的阅读，以及亲自进行网络监听系统的编程，了解了网络监听系统能对网络上的所有数据进行捕获,在功能方面实现对数据包进行分析,查找网络中潜在的危险,对网络故障精确定位,帮助管理员解决网络的故障和性能问题。