实验 5 开发基于 WinPcap 的嗅探器

## 实验目的

通过开发基于 WinPcap 的嗅探器，掌握嗅探器的工作原理，熟悉 WinPcap 的使用，掌握基于 WinPcap 网络嗅探器的开发过程。

## 实验准备

（1）通过 WinPcap 的帮助文档和代码实例熟悉 WinPcap 库的使用方法。

（2）阅读 WinPcap 官方网站上相关开发文档和经典论文。经典论文包括： 

Fulvio Risso, Loris Degioanni, An Architecture for High Performance Network Analysis. Proceeding for the 6th IEEE Symposium on Computers and Communications (ISCC 2001). Hammmamet July 2001 

Loris Degioanni, Mario Baldi, Fulvio Risso, and Gianluca Varenn. Profiling and Optimization of Software-Based Network Analysis Applications. Dipartimento di Automat/ca e Informatica Politecnico vii Torino .April 2004

它们的下载地址分别是：http://www.winpcap.org/docs/iscc01-wpcap.pdf 和 <http://www.winpcap.org/docs/WinPcap-SBAC03.pdf>。

（3）设计程序界面。

## 实验内容

开发出一个简单的 Windows 平台上的 Sniffer 工具，能显示所捕获的数据包并能做简单的分析或统计。主要内容如下：

（1）列出监测主机的所有网卡，选择一个网卡，设置为混杂模式进行监听。

（2）捕获所有流经网卡的数据包，并利用 WinPcap 函数库设置过滤规则。

（3）分析捕获到的数据包的包头和数据，按照各种协议的格式进行格式化显示。

## 实验要求

（1）重点对 TCP、UDP、ARP、RARP、IGMP、ICMP 等数据包进行分析。

（2）所开发的嗅探工具能够根据协议类型、端口、地址等信息对数据包进行过滤。

（3）采用多线程实现。

（4）在实验报告中写出程序关键算法和流程图，根据 WinPcap 常用库函数总结出基于 WinPcap 的嗅探器的程序框架，并附上程序界面或运行结果。