计算机网络实验报告

--捕获数据包，ping篇

学校：哈尔滨工业大学

班级：11403202

学号：1140320206

姓名：霍峻杰

实验3.1

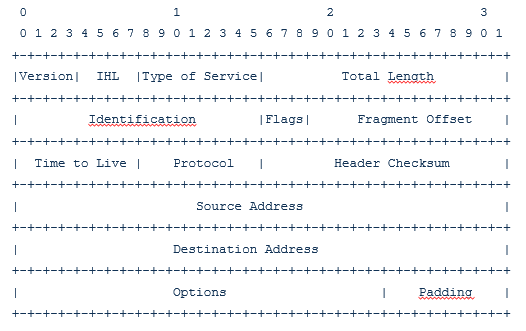
一、实验题目:

用原始套接字实现一个嗅探器，能够识别IP头部字段，源/目的IP地址，协议类型，源端口，目的端口，并根据命令行选项抓取指定报文

二、实验原理：

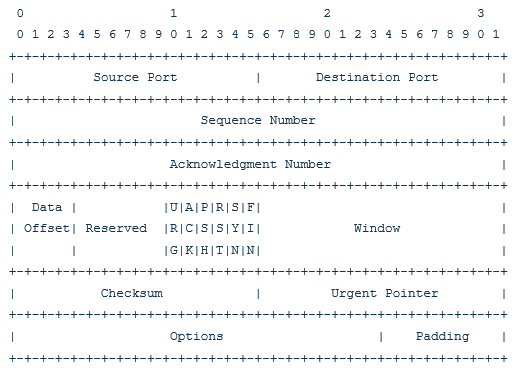
原始套接字的创建和正常的socket创建没有什么区别。TCP/UDP类型的套接字只能访问传输层及以上的数据，而创建好的raw socket可以访问传输层以下的数据，也就是整个数据包。这是因为TCP/IP socket在创建的时候将下层的包头丢弃了，而原始套接字不会丢弃包头。所以我们可以利用它的包头中的信息进行一些操作，比如这个实验要做的数据包嗅探工作。

先来看一下IP头部结构：

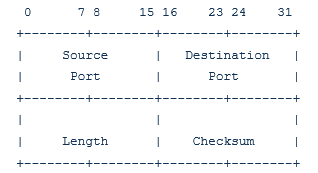


下面是几个传输层协议：

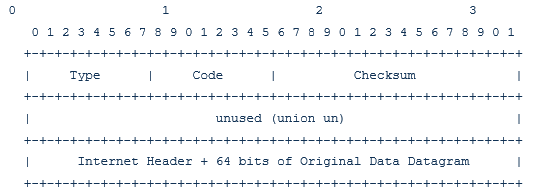
TDP头结构：



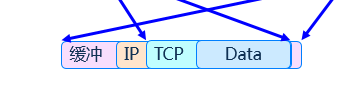
UDP头结构：



ICMP头结构：



数据包是层层封装的，每一层封装都会加一段这一层的头文件，示意图如下：

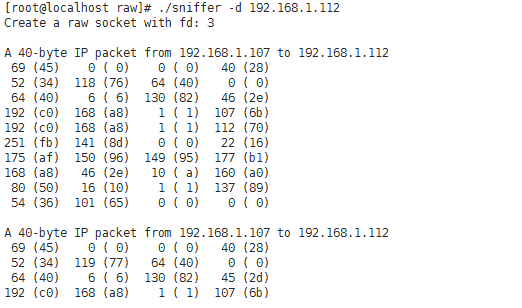


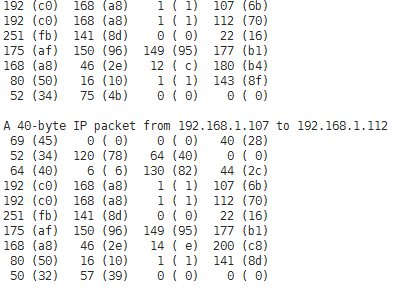
在这个实验我决定学习一些开源项目的选项方式输入参数，而不是用户交互式的输入参数。这就需要用到argc和argv[]参数。我定义了几个选项，分别是”-p“，”-s“，”-sp”，”-d“，”-dp“，对应”协议号“，”源IP“，”源端口“，”目的IP“，”目的端口“。用户可根据需要，填写对应参数，来选择性捕获指定的数据包。其中，前三项包含在ip头部中，可以通过ip头结构进行获取，而端口号则在下一级（传输层）包头中，需要在其中获取端口号（前32位，对应源端口16位，目的端口16位）。

三、实验结果:

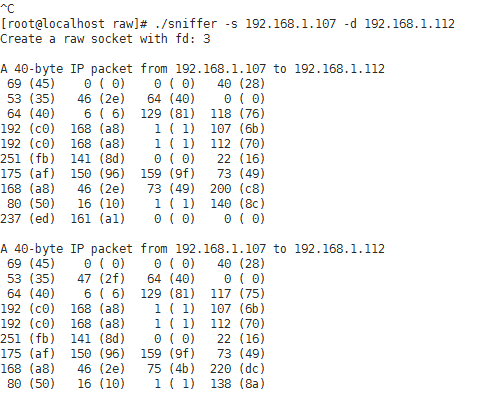
这里我的选项都做了默认设置，用户可以任意指定想捕获的包，用户不一定对所有选项进行设置，当不设置时，会采用默认选项。同时，用户可以用多个选项来将捕获的包进行更详细的捕获。

1. 首先测试 ./sniffer –d 192.168.1.112(虚拟机ip)，嗅探目的ip为192.168.1.112的数据包。

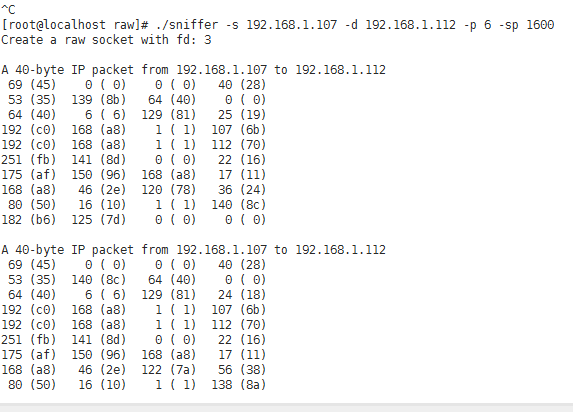




2. 测试 ./sniffer –s 192.168.1.107 –d 192.168.1.112(虚拟机ip)，嗅探源IP为192.168.1.107，目的ip为192.168.1.112的数据包。

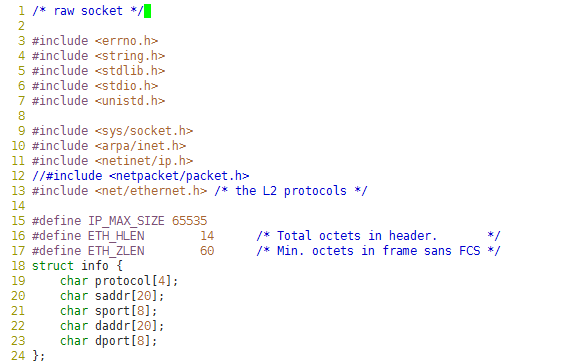


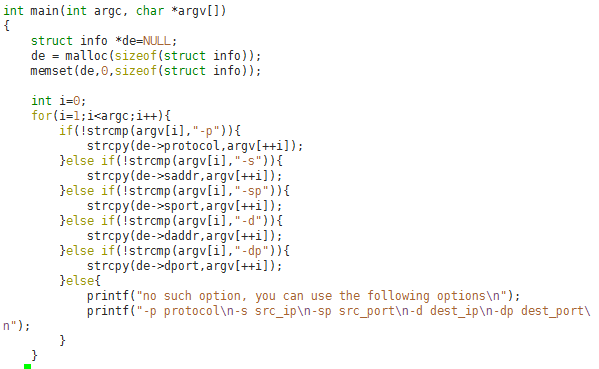
3. 测试./sniffer -s 192.168.1.107 -d 192.168.1.112 -p 6 -sp 1600，嗅探源IP为192.168.1.107，目的ip为192.168.1.112，tcp协议，源端口为1600的数据包。



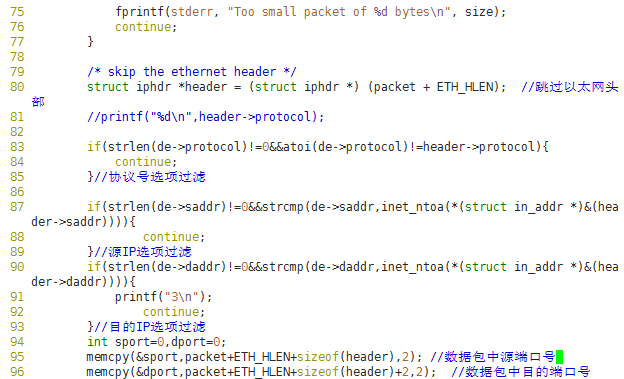
四、实验代码详解

这里源代码注解还是以代码注释的形式给出。

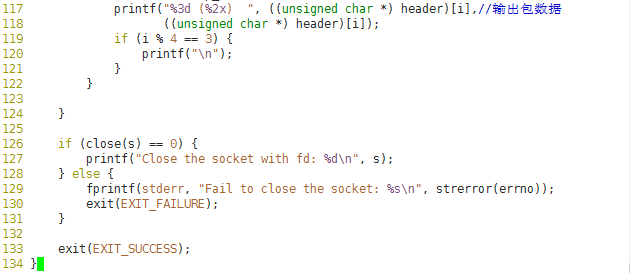












实验3.2

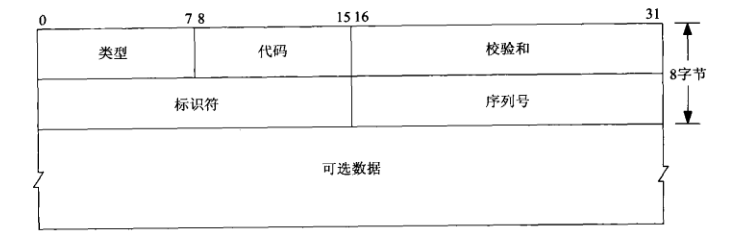
一、实验题目:

实现一个基于ICMP Echo的ping

二、实验原理：

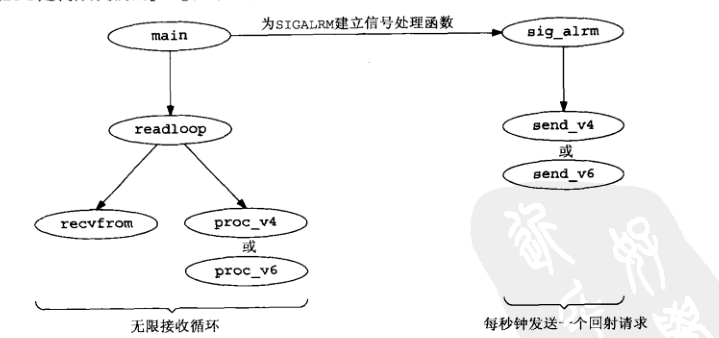
Ping的原理是向请求的IP发送一个ICMP回射请求，目标IP以一个ICMP回射应答进行响应。

ICMP消息格式：



本次实验我是参考教材unix网络编程做的，采用里面的发送附带56字节数据(可选数据)。标识符设置为本进程id，校验返回ICMP是否为此进程的应答ICMP消息。序列号用一个全局变量表示，每次发送序列号自动加1。、

各函数运行调用关系：（摘自教材）

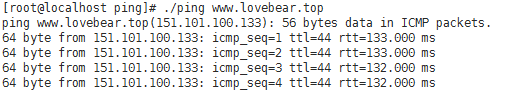


一部分无限循环接收处理收到的ICMP响应消息，另一部分每隔1秒发送一个ICMP包，达到发送后，返回结果被ping程序接受处理响应的过程。

这里面有一个校验和的过程，这个是网际网校验和算法（还有挺多其他的）。

三、实验结果：

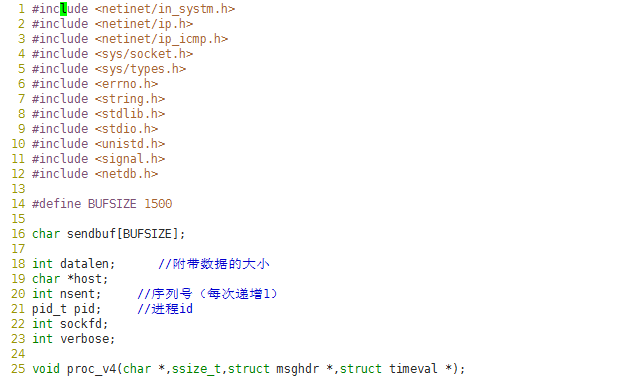
命令 ping [www.lovebear.top](http://www.lovebear.top)

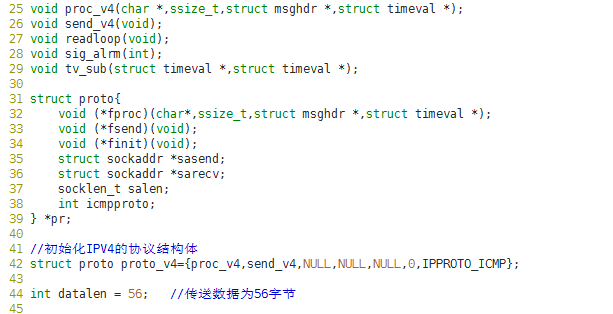


得到正确返回。

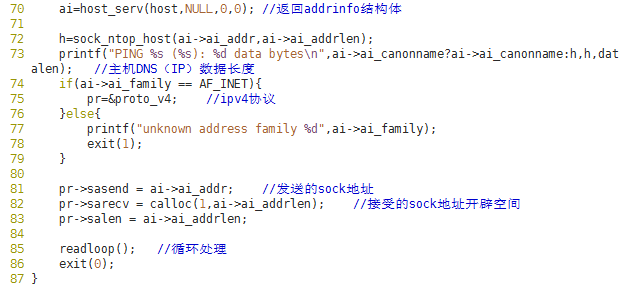
四、实验代码：

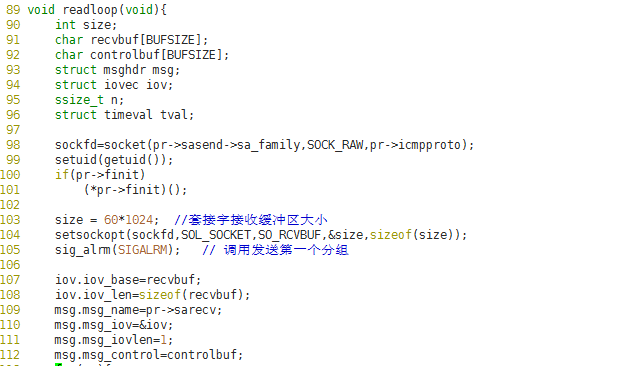
这次的代码详解我还是以注释的形式给出，方便。

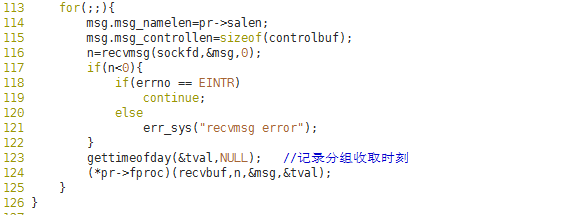


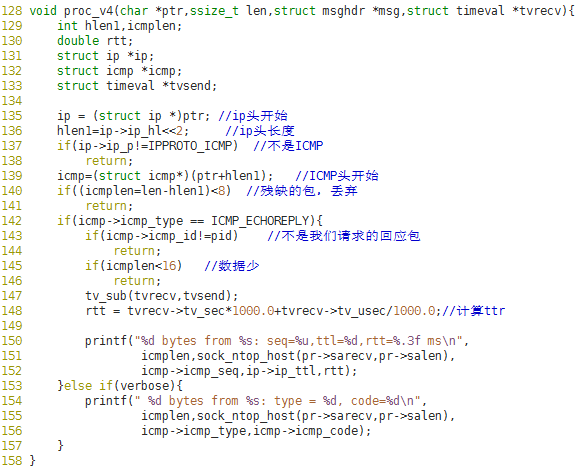














实验总结：

这两个实验让我收获很多，尤其是ping实验，对网络之间的通信协议及方式更加熟知了。同时，还对命令行选项方式有了一个了解，并主动在第一个实验中尝试，但是做到第二个实验，发现还用更好的这种实现方式（getopt函数），觉得我的方法有点笨了，但是总体来说，收获也是可以的。遗憾是，ping主要是借鉴教材的方法，没有思考太多自己的东西，感觉比较遗憾，希望以后的实验可以自己规划好时间，多想一些深层的东西。