《网络协议分析》

项目实践报告

题目：ICMP协议分析

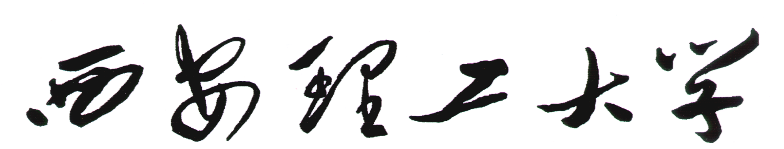
专 业 网络工程

班 级 网络182

学 生 陈正炯

屈致齐

指导教师 张 翔



2021 年 春季 学期

**项目任务**

利用Linux的套接口编程实现对ICMP报文的抓取和分析

主要完成的两大组成部分为：捕获主机发出和接收的数据包，分析数据包中的ICMP报文

1.捕获主机发出和接收的数据报：通过Raw Socket捕获发出和接收的数据包。

2.分析数据包中的ICMP报文：从数据包中获取IP报文且IP报文协议字段为1，从IP报文中获取ICMP报文，根据报文信息对不同种类的ICMP报文进行分析。

**项目任务分工**

陈正炯：捕获主机发出和接收的数据报

屈致齐：分析数据包中的ICMP报文

**评语（教师填写）**

目录

[1.程序总体设计 4](#_Toc76657686)

[1.1 ICMP报文结构 4](#_Toc76657687)

[1.2 ICMP报文概述 4](#_Toc76657688)

[1.3 ICMP报文应用情况 5](#_Toc76657689)

[1.4 抓包原理 5](#_Toc76657690)

[2.程序流程框图 8](#_Toc76657691)

[3.步骤解析 9](#_Toc76657692)

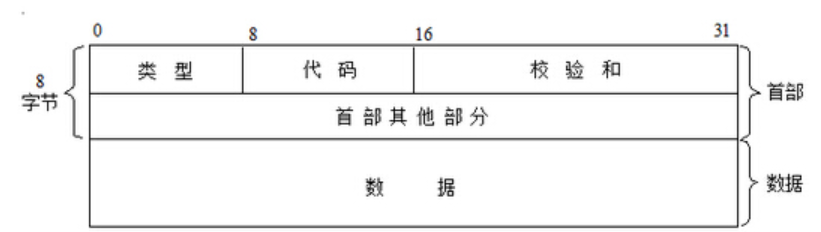
[4.效果展示 10](#_Toc76657693)

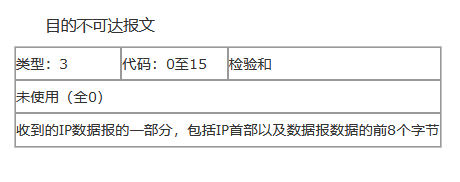
[5.心得体会 14](#_Toc76657694)

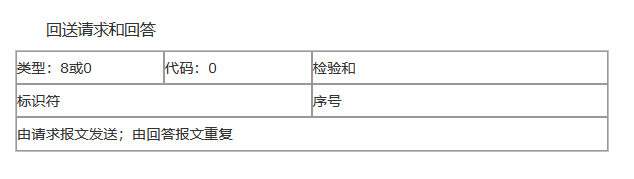
[6.参考文献 15](#_Toc76657695)

# 1.程序总体设计

## 1.1 ICMP报文结构







## 1.2 ICMP报文概述

1. ICMP允许主机或路由报告差错情况和提供有关异常情况。ICMP是因特网的标准协议，但ICMP不是高层协议，而是IP层的协议。通常ICMP报文被IP层或更高层协议（TCP或UDP）使用。一些ICMP报文把差错报文返回给用户进程。

2. ICMP报文作为IP层数据报的数据，加上数据报的首部，组成数据报发送出去。

3. ICMP报文的种类有两种，即ICMP差错报告报文和ICMP询问报文。

## 1.3 ICMP报文应用情况

1. ICMP差错报文：

终点不可达：网络不可达、主机不可达、协议不可达、端口不可达

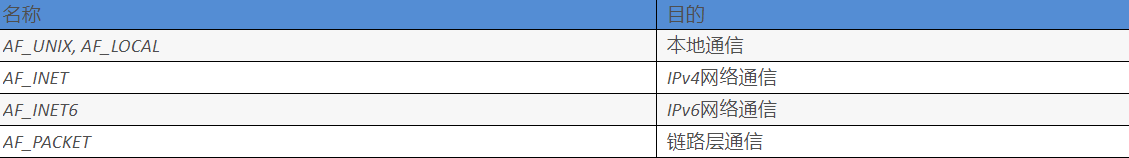
源站抑制、时间超过、参数问题、改变路由

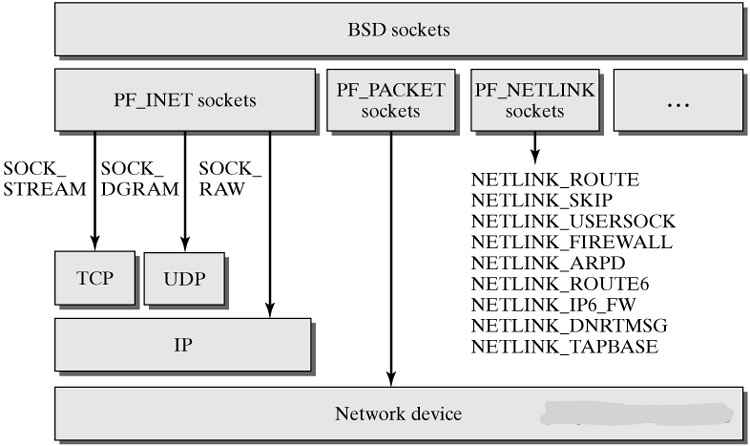
2. ICMP询问报文：

回送请求和回答、时间戳请求和回答、掩码地址请求和回答、路由器询问和通过。

3. Ping：该程序发送一份ICMP回显请求报文给主机并等待返回ICMP回显应答

## 1.4 抓包原理

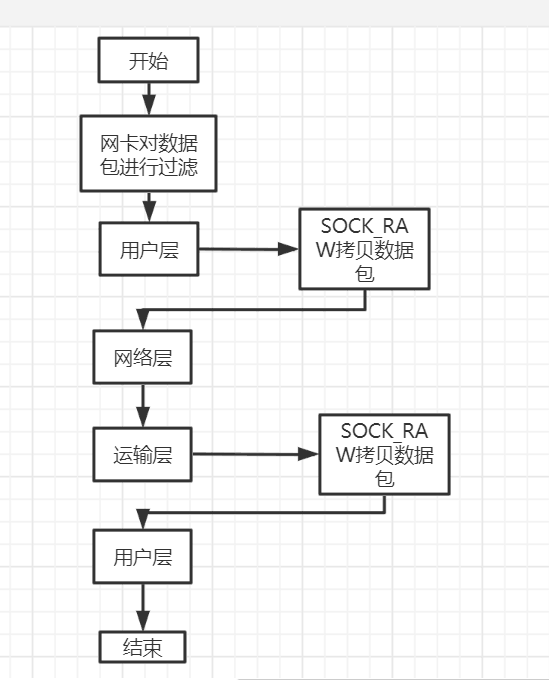




int socket(int domain, int type, int protocol)

domain参数决定了图中所示的第二层通信域, type决定了第三层

的通信模式，protocol决定了第四层真正的通信协议。

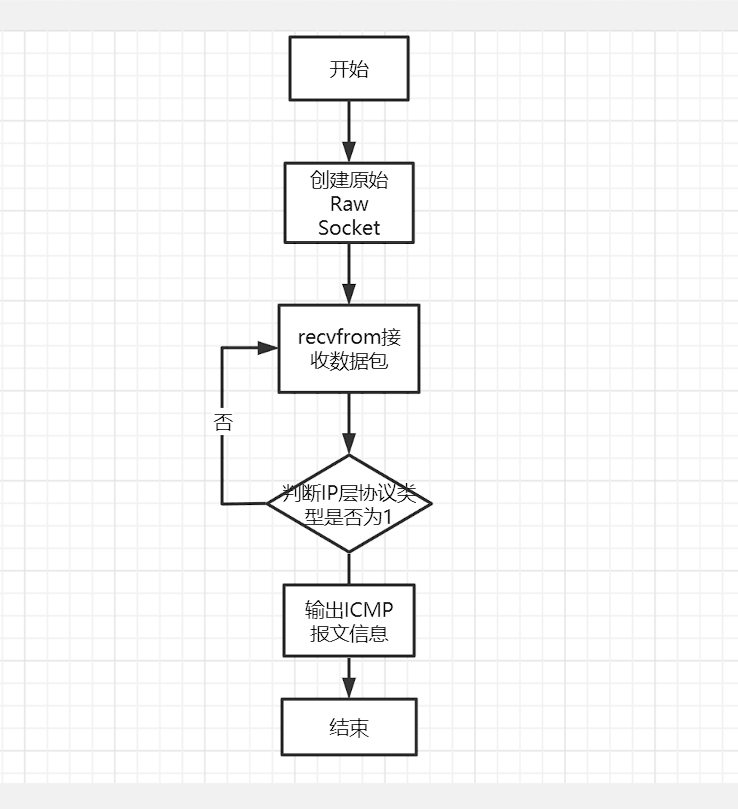


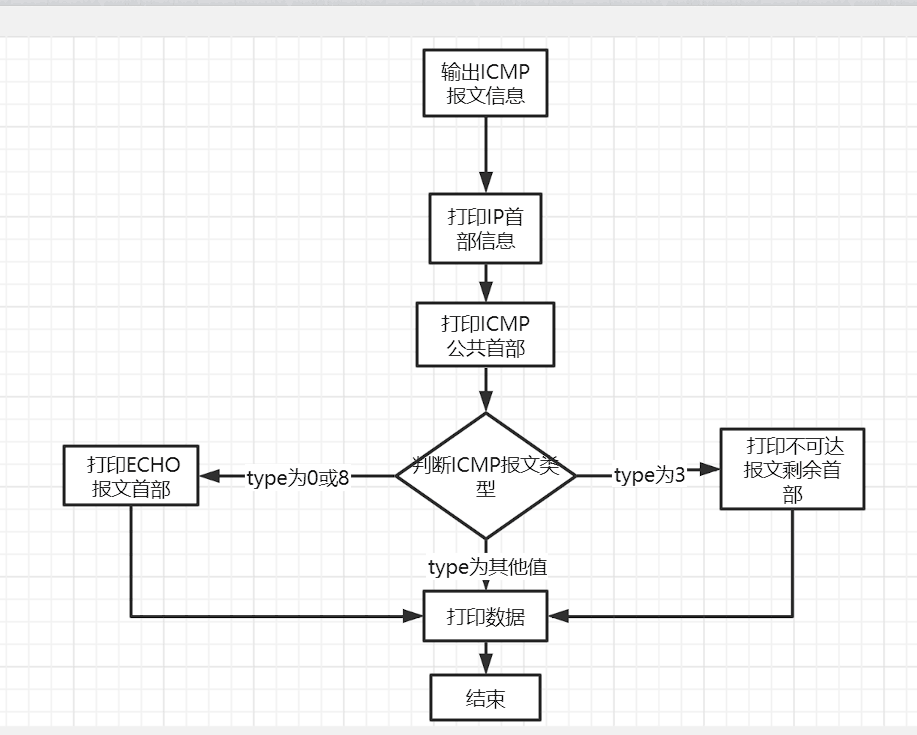
SOCK\_RAW接收数据包的原理, 在没有递交给其他协议处理

器（内核协议处理器）之前，先递交给所有的 Raw

Socket，换句话说，就是 Raw Socket 优先处理。

# 2.程序流程框图





# 3.步骤解析

1. 捕获主机发出和接收的数据报：通过Raw Socket捕获发出和接收的数据包。

sockfd1=socket(PF\_PACKET, SOCK\_RAW, htons( 0x3));

协议地址族以PF开头 地址以AF开头 但目前来说协议簇和地址簇都是一一对应的,SOCK\_RAW原始套接字 需要ROOT权限 0x3即

nr1 = recvfrom(sockfd1, buf1, BUF\_SIZE, 0, (struct sockaddr\*)&from1, &len1);

ip1 = (struct ip\*)(buf1+14);

icmp1 = (struct icmp\*)((char\*)ip1 + iphlen1);

1. 分析数据包中的ICMP报文：从数据包中获取IP报文且IP报文协议字段为1，从IP报文中获取ICMP报文，根据报文信息对不同种类的ICMP报文进行分析

printIp (const struct ip \*ip, int len)

打印IP头部及相关信息

printIcmp (struct icmp\* icmp, int len)

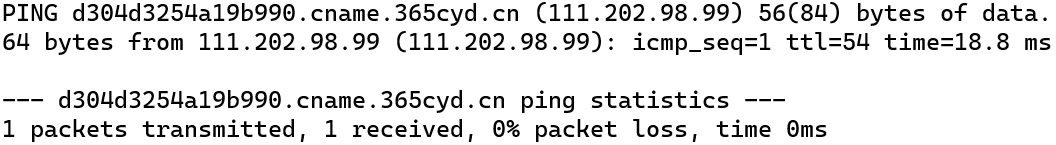
打印ICMP头部及相关信息

printData (const unsigned char\* data, int len, int cols = 16)

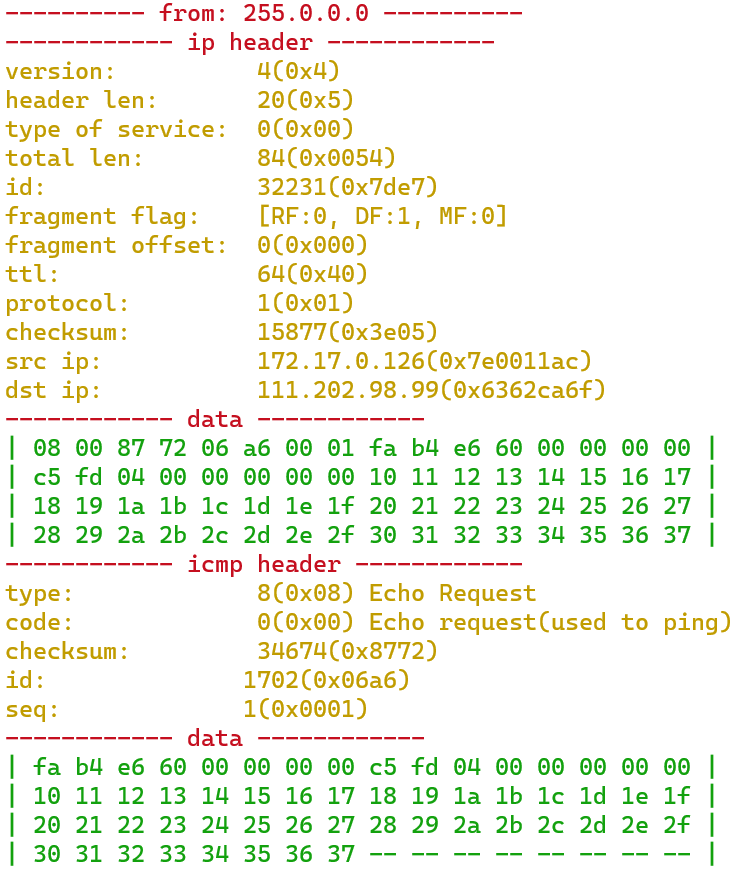
打印剩余数据信息

# 4.效果展示

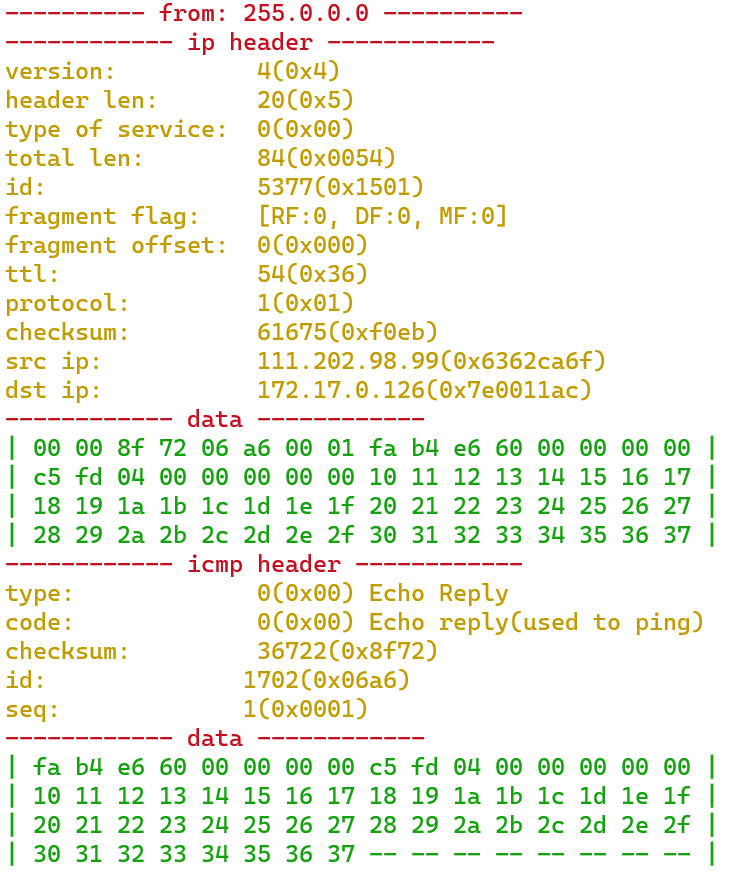
1. ping [www.xaut.edu.cn](http://www.xaut.edu.cn) -c 1



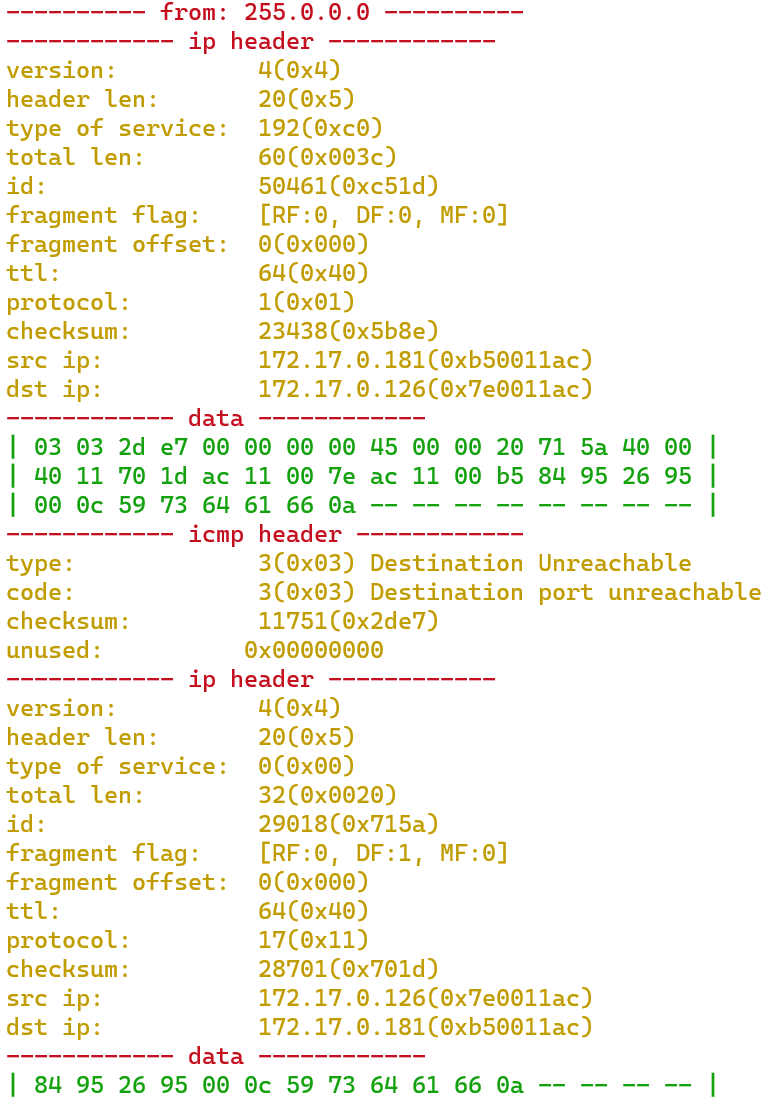
发送报文



应答报文



1. 不可达报文



# 5.心得体会

陈正炯：本次协议分析所遇到的最大困难在于如何捕获本机发出的数据包,刚开始时只是用socket(AF\_INET, SOCK\_RAW, IPPROTO\_ICMP)捕获发往主机的ICMP报文,但是只是实现了单向捕获,经过查阅资料,了解到了一个已经过时的技术socket(PF\_PACKET, SOCK\_RAW, htons(ETH\_P\_ALL))可以捕获

发往本机mac的所有类型（IP、ARP、RARP）的数据帧，并接收从本机发出的所有类型的数据帧.只是头文件已经失效,所以 直接用0x3代替.

由于时间限制,并未查到用什么技术来代替,所以只能用这种过时的技术实现.另,本来是想用QT做个界面的,但是由于打印函数已经写好了,QT想要实现将数据显示在窗口似乎要重写打印函数,工作量有点大,只能放弃.其次,对各个协议的首部长度及ICMP不同类型报文的结构有了更加深刻的认知.在捕获到保护以太帧结构的数据包后,利用地址+14可以得到IP首部的地址,这种方法比较巧妙.总之,本次协议分析课设,我即复习了网络编程的知识,又对ICMP协议理解的更加深刻,包含对ping命令的理解,还是做出了点自己的东西的.

屈致齐：本次网络协议分析课设，主要是针对单个协议报文的具体分析，在获取数据包的过程中有诸多困难，但幸好都得到解决。在拿到数据包以后，我对于几类出现频繁的报文类型进行了switch选择输出对应信息，在实现的过程中对于icmp报文也有了更加清晰的认识。多个类型经过查找有部分已经弃用，所以我们最后决定只对常用具体的几个类型进行简单分析。在整体实现过程中也遇到了很多问题，通过查阅书籍资料，网络查找，组内验证才将功能实现。对于地址位置，数据结构体，ip和icmp有了更多认识，也深刻意识到学以致用的重要性。对于网络协议在今后会多学习多抓包多了解。

# 6.参考文献

1. **Jeffery L.Carrell,Laura A.Chappell,Ed Tittel,James Pyles 《Guide to TCP/IP,Fourth Edition》,北京,清华大学出版社**
2. **Stevents,W.R. Fenner B,Rudoff, A.M 《UNIX网络编程卷一》,北京,人民邮电出版社**