计算机网络 LAB2:　RAW SOCKET 编程与以太网帧分析

计算机科学与技术系　161220071 李杨

实验要求：

1 编写一个抓包程序 raw_socket，抓取 ip 数据包和 arping 数据包。

2.编一个 ping 程序 raw_socket_ping

实验目的：

初步解 raw socket 封装和发送以太网帧的功能，在了解 icmp 包的结构的基础上，实现 ICMP 包的发送和接收。

数据结构说明：以下皆为调用的已封装好了的结构体

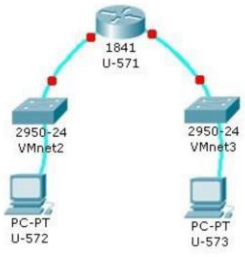
Struct ifreq：用来保存某个接口信息，在 get_local_ip 函数里面使用了这个结构体，目的是获得本地的 ip 地址.

Struct ockaddr_in:这是网络通信常用的结构体，在 get_local_ip 和 call 函数里使用，IPv4 专用 socket 地址,保存目的地址

Structicmp：使用的 Linux 中 ICMP 数据结构(<netinet/ip_icmp.h>)，用来对 icmp 的设置以及发送与接收

Struct timeval：查询获取系统时间的结构体，用来获取每次收发包所用的时间

环境配置：



vmnet2 为子网 2，vmnet3 为子网 3 配置如图所示。

程序设计的思路以及流程：

Raw_socket 程序（抓包）：

按照给定的程序样例，通过 socket 函数建立连接，并通过 recvfrom 函数从（已连接）套接口上接收数据，并捕获数据发送源的地址，进而可以打印得到收发端的 MAC 地址，易知 buffer 的前 12 位为 mac 地址，所以对第十三,十四位进行判断，由信息可知，ip、arp、rarp 的类型分别 0800,0806,8035，所以可以直接对第十四位进行判断, 从而判断出数据包的类型, 然后依次打印出各个数据段的内容。

Raw_socket_ping 程序（ping）：

现在可以先初步搭一个框架出来：检测参数、取（转换）目标 IP 地址、发报文、接收报文、打印信息。使用 gethostbyname ()函数来通过主机名获得 ip 地址(要发当然需要知道目标 IP 地址)。要实现发送报文的函数，首先得有报文才行，所以要先实现一个设置 ICMP 报文的函数。即 seticmp 函数，这里还要再单独实现一个计算校验和的函数，这样的话，就差 rtt 的值不知道了，所以再单独写一个 getrtt 的函数，用来获取时间间隔。这样的话，一个 icmp 包就包装完成了，下面就是发送了，这里使用 sendto 函数，就可以将存放在 buf 里面的报文往 sockfd 写数据。接着就是收取包了，recvfrom 读取 sockfd 上的数据，buf 和 len 参数分别指定度缓冲区的位置和大小。ICMP 数据报是封装 IP 报文里发送的，IP 协议是无连接的，不可靠的协议。所以每次读取数据都要获取发送端的 socket 地址，即参数 src_addr 所指的内容，addlen 参数则指定该地址的长度。

当调用 recvfrom 时，需要设置 addlen 参数指向一个整数，该整数包含 addr 所指向的套接字缓冲区的字节长度。返回时，该整数设为该地址的实际字节长度

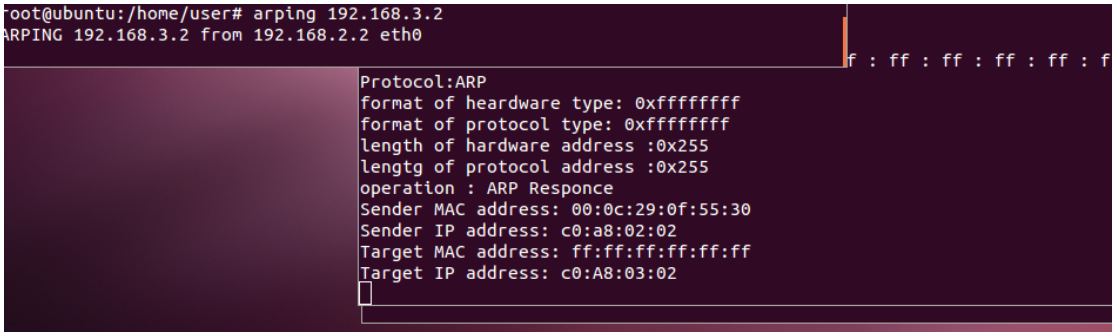
GetRtt 用来获取两个时间戳的差，结果保存在第一个参数所指空间处。

Unpack 函数用来 ip 和 icmp 报头。最后将每个函数整合起来，就可以完成 ping 程序了。由于要打印本地 ip 地址，所以在每次 unpack 打印数据时，调用一次 get_local_ip 函数，来获得本地的 ip 地址。

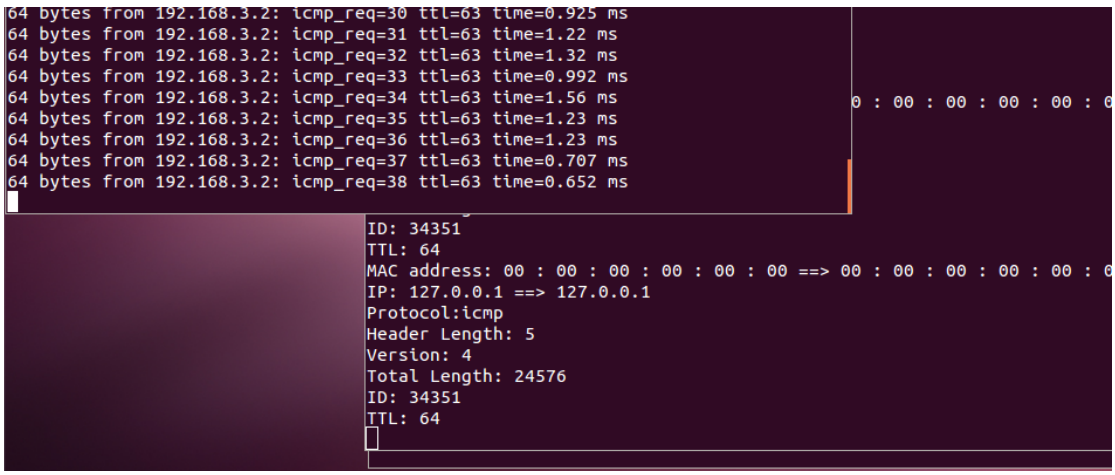
运行结果：

Raw_socket:

Arping:



Ping：



Raw_socket_ping:

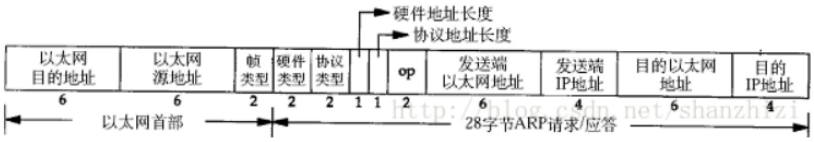
```
root@ubuntu:/home/user/exp# ./raw_socket_ping 192.168.3.2
PING 192.168.3.2(192.168.3.2) 64 bytes of data.
64 bytes from 192.168.3.2 to 192.168.2.2 : icmp_seq =1 ttl=63 time=0.8 ms
64 bytes from 192.168.3.2 to 192.168.2.2 : icmp_seq =2 ttl=63 time=3.2 ms
64 bytes from 192.168.3.2 to 192.168.2.2 : icmp_seq =3 ttl=63 time=3.2 ms
64 bytes from 192.168.3.2 to 192.168.2.2 : icmp_seq =4 ttl=63 time=0.8 ms
64 bytes from 192.168.3.2 to 192.168.2.2 : icmp_seq =5 ttl=63 time=0.8 ms
64 bytes from 192.168.3.2 to 192.168.2.2 : icmp_seq =6 ttl=63 time=1.4 ms
64 bytes from 192.168.3.2 to 192.168.2.2 : icmp_seq =7 ttl=63 time=0.8 ms
```

参考资料：

ARP 结构的参考：

ARP数据报的格式如下图所示（该图出自[TCPIP]）：

ARP数据报格式



注意到源MAC地址、目的MAC地址在以太网首部和ARP请求中各出现一次，对于链路层为以太网的情况是多余的，但如果链路层是其它类型的网络则有可能是必要的。硬件类型指链路层网络类型，1为以太网，协议类型指要转换的地址类型，0x0800为IP地址，后面两个地址长度对于以太网地址和IP地址分别为6和4（字节），op字段为1表示ARP请求，op字段为2表示ARP应答。

网址：https://blog.csdn.net/shanzhizi/article/details/9995489

RARP 结构的参考：

RARP的分组格式与ARP分组基本一致。

他们之间主要的差别是RARP的op（操作字段）请求操作代码为3，应答操作代码为4。

ARP与RARP的请求都以广播方式传送，而他们的应答一般都是单播传送的。

Ip 结构以及 iphdr 结构体详解：
https://blog.csdn.net/beginning1126/article/details/14057087

、

ICMP 协议的报文格式相关资料：
https://blog.csdn.net/u011784495/article/details/71743516

ICMP 消息类型：

ICMP消息类型	用途说明
回显请求	Ping工具通过发送ICMP回显消息检查特定节点的IPv4连接以排查网络问题。类型值为0
回显应答	节点发送回显答复消息响应ICMP回显消息。类型值为8
重定向	路由器发送“重定向”消息，告诉发送主机到目标IPv4地址更好的路由。类型值为5
源抑制	路由器发送“源结束”消息，告诉发送主机它们的IPv4数据报将被丢弃——因为路由器上发生了拥塞。于是，发送主机将以较低的频度发送数据报。类型值为4
超时	这个消息有两种用途。第一，当超过IP生存期时向发送系统发出错误信息。第二，如果分段的IP数据报没有在某种期限内重新组合，这个消息将通知发送系统。类型值为11
无法到达目标	路由器和目标主机发送“无法到达目标”消息，通知发送主机它们的数据无法传送。类型值为3

时间间隔的计算：
https://blog.csdn.net/u011006622/article/details/52459188
使用第二种方法。