计算机网络实验报告

**实验三**

**子网划分、静态路由与NAT**

学号：1412200065

姓名：刘博

时间：2016.4.2

1. **实验目的：**
   1. 了解如何配置一个包含多个子网的网络环境；
   2. 学会NAT的组网方式；并为以后组网要求打下基础；
2. **网络拓扑配置：**

|  |  |  |  |
| --- | --- | --- | --- |
| 节点名 | 虚拟设备名 | IP | 子网掩码 |
| Router 0 | router0 | eth0 210.28.130.166 | 255.255.255.0 |
| eth1 192.168.2.1 | 255.255.255.128 |
| eth2 192.168.2.129 | 255.255.255.224 |
| Router 1 | router1 | eth0 210.28.130.100 | 255.255.255.0 |
| eth1 192.168.3.1 | 255.255.255.0 |
| PC 0 | pc0 | eth0 192.168.2.2 | 255.255.255.128 |
| PC 1 | pc1 | eth0 192.168.2.3 | 255.255.255.128 |
| PC 2 | pc2 | eth0 192.168.3.2 | 255.255.255.0 |
| PC3 | pc3 | eth0 192.168.2.130 | 255.255.255.224 |

1. **路由规则配置：**
   1. Pc0：

sudo ifconfig eth0 192.168.2.2 netmask 255.255.255.128

route add default gw 192.168.2.1

* 1. Pc1：

sudo ifconfig eth0 192.168.2.3 netmask 255.255.255.128

route add default gw 192.168.2.1

* 1. Pc3：

sudo ifconfig eth0 192.168.2.130 netmask 255.255.255.224

route add default gw 192.168.2.129

* 1. router0：

sudo ifconfig eth0 210.28.130.166 netmask 255.255.255.0

sudo ifconfig eth1 192.168.2.1 netmask 255.255.255.128

sudo ifconfig eth2 192.168.2.129 netmask 255.255.255.224

echo 1 > /proc/sys/net/ipv4/ip\_forward

ip route add 192.168.3.0/24 via 210.28.130.100

* 1. router1：

sudo ifconfig eth0 210.28.130.100 netmask 255.255.255.0

sudo ifconfig eth1 192.168.3.1 netmask 255.255.255.0

echo 1 > /proc/sys/net/ipv4/ip\_forward

ip route add 192.168.2.0/24 via 210.28.130.166

* 1. Pc2：

sudo ifconfig eth0 192.168.3.2 netmask 255.255.255.0

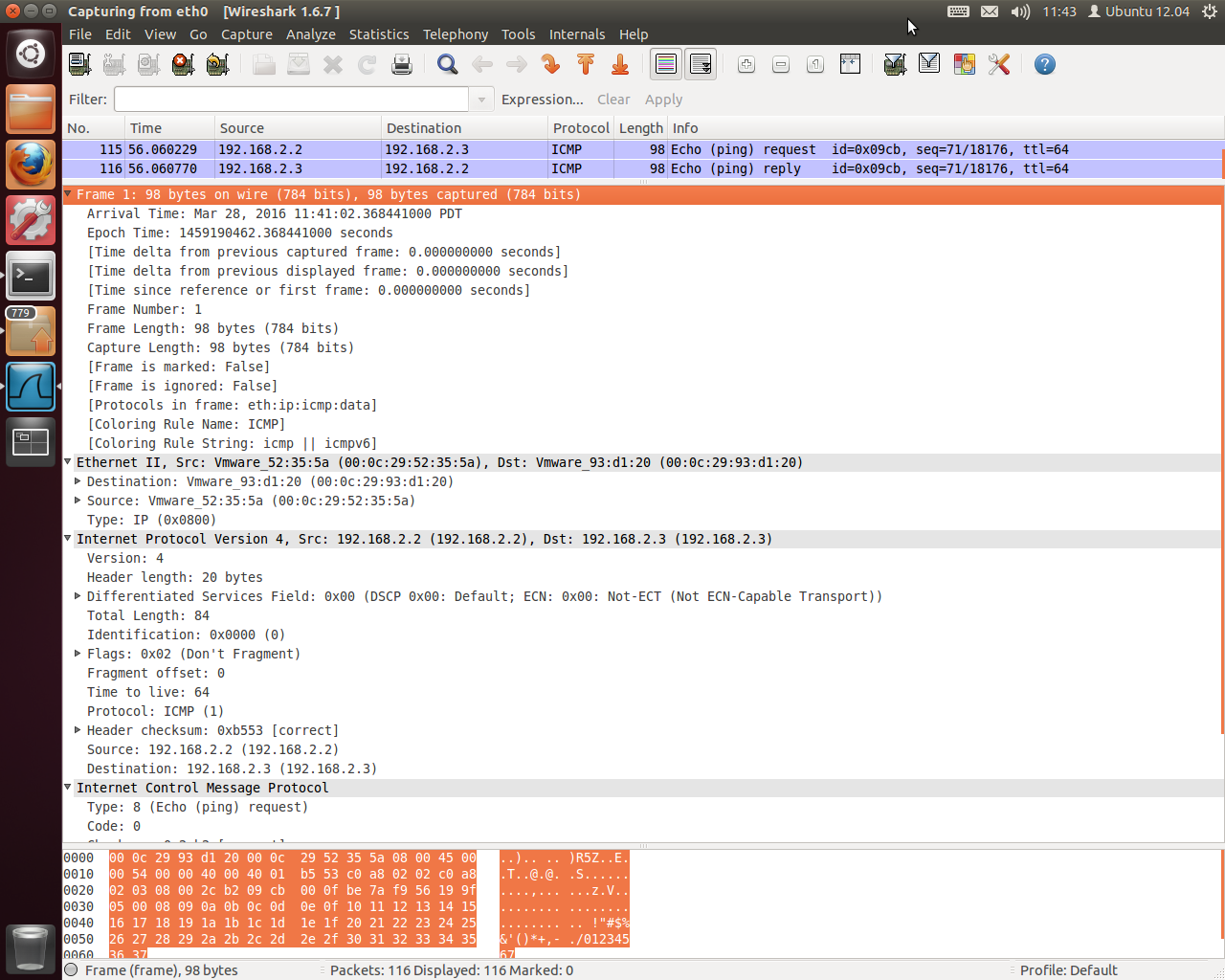
route add default gw 192.168.3.1

1. **NAT设置命令：**

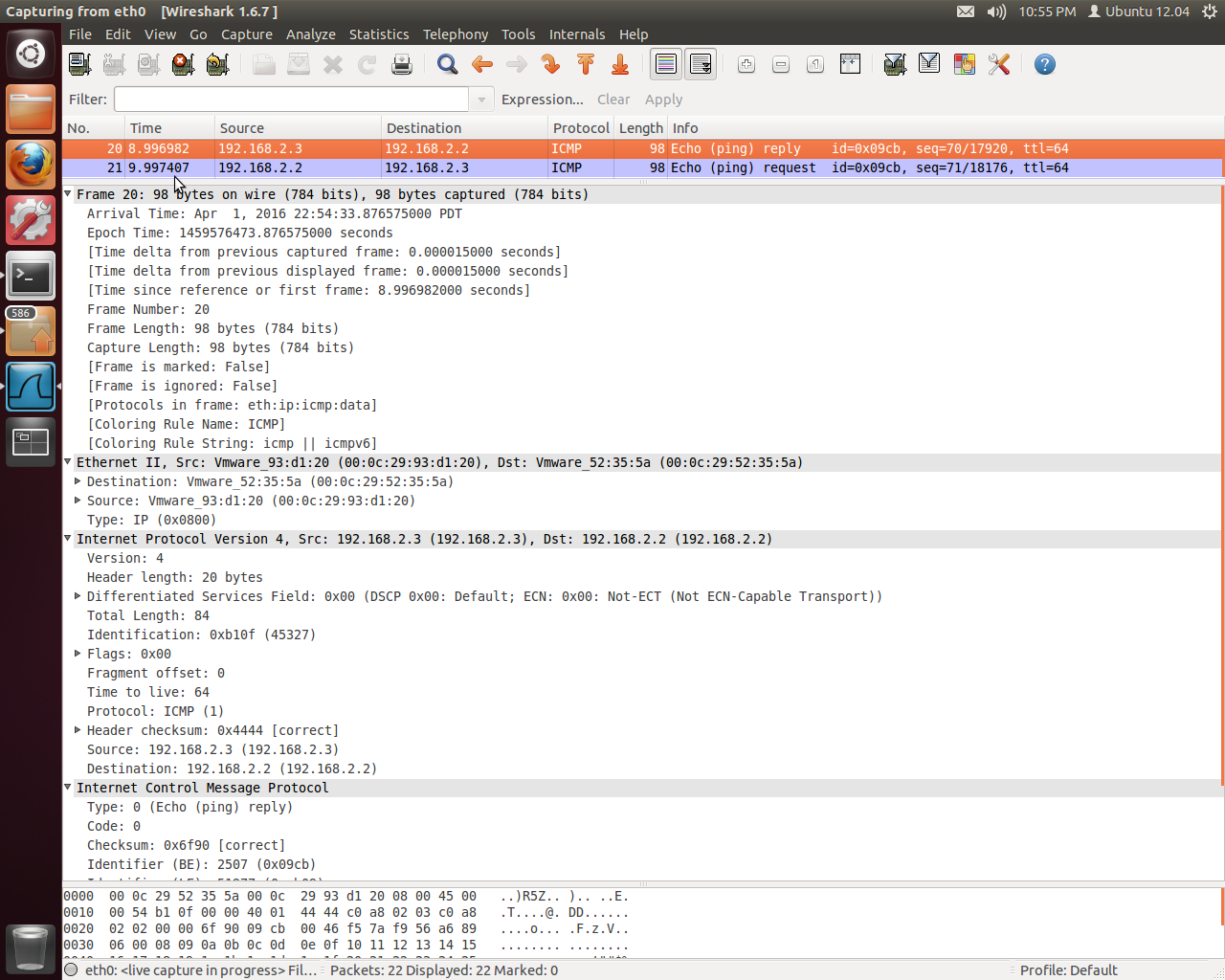
**sudo iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.0/24 -j SNAT --to 210.28.130.166**

1. **数据包截图：**

Pc0(192.168.2.2) ping Pc1(192.168.2.3):

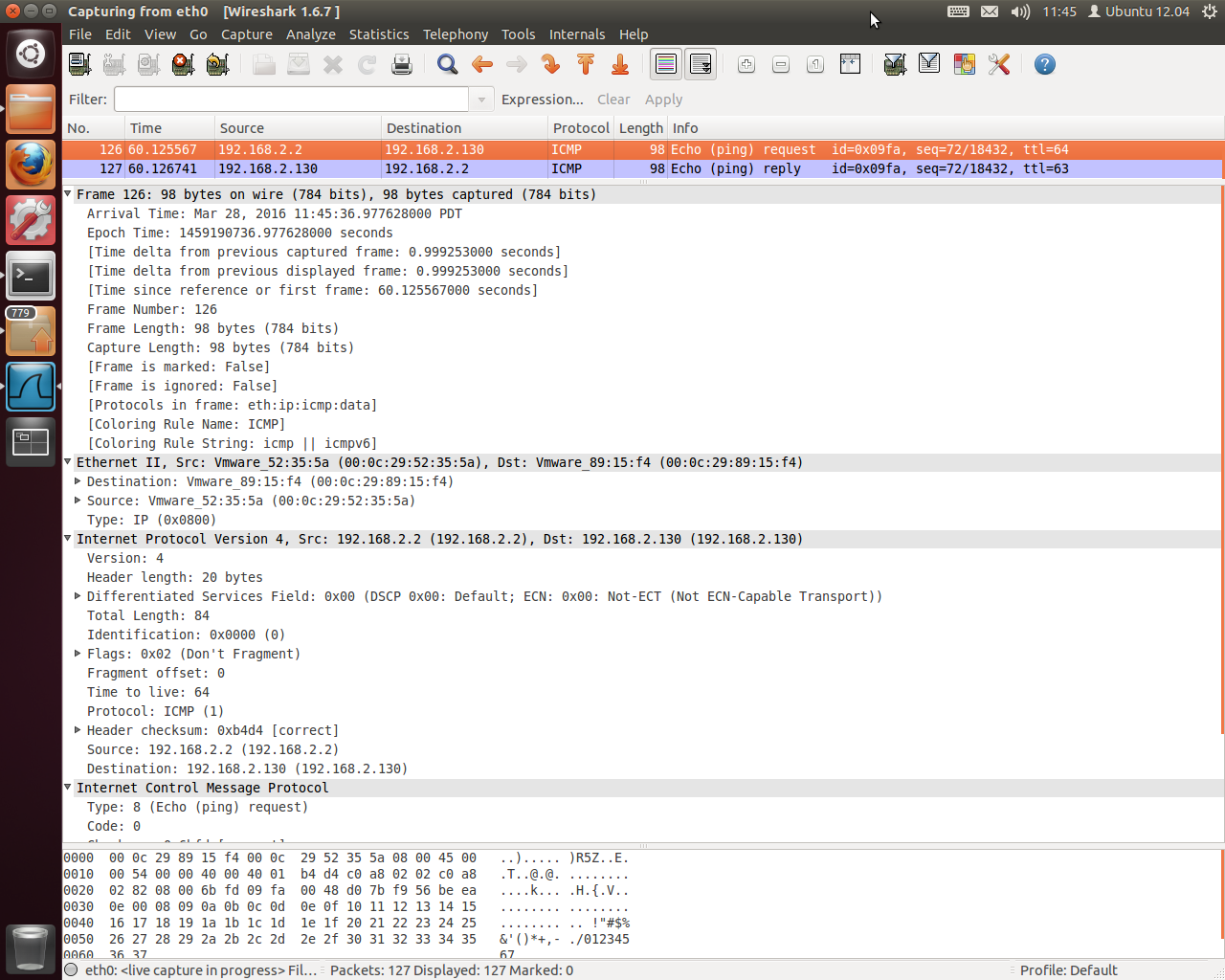


(图为在PC0上的截图)

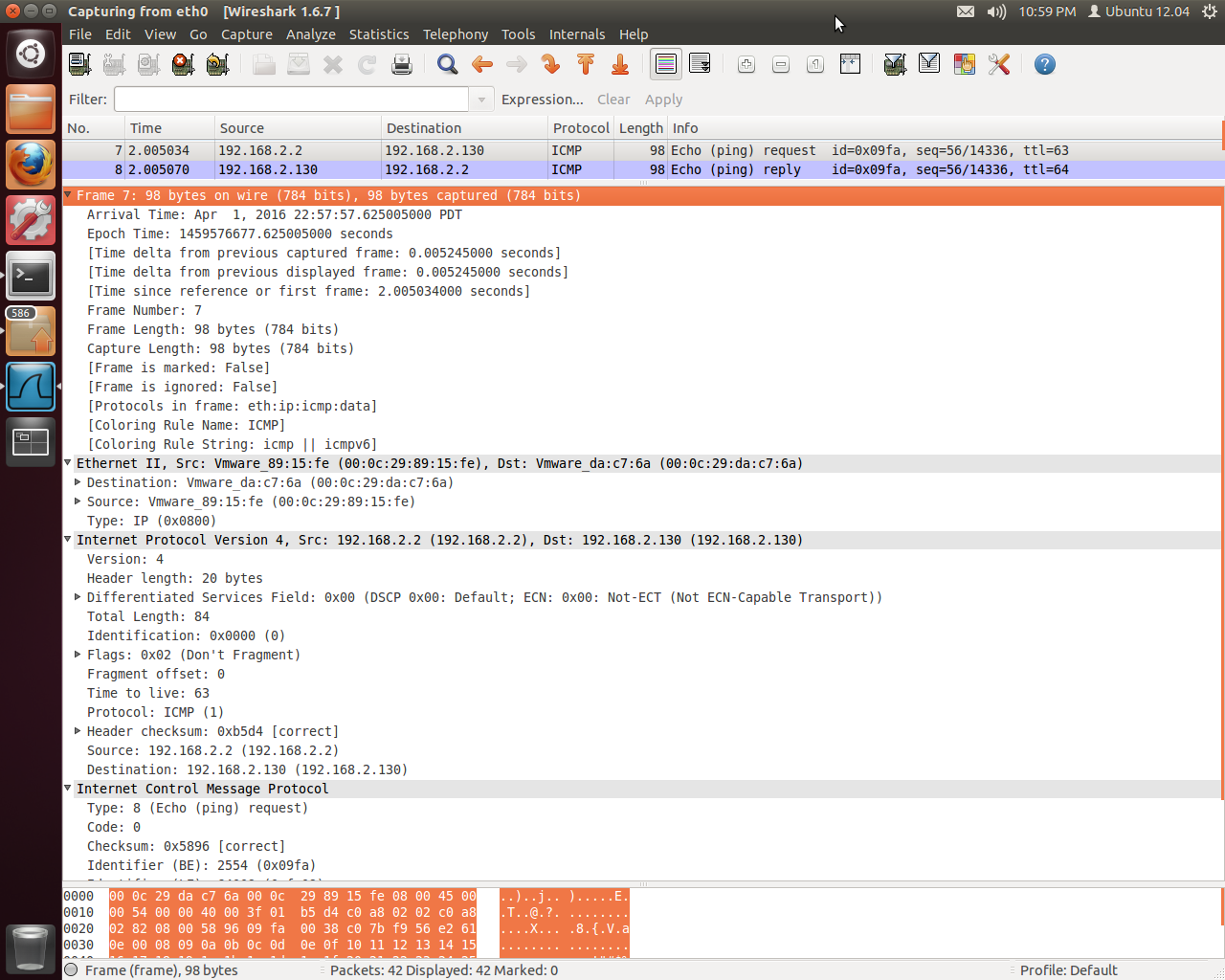


(图为在PC1上的截图)

Pc0(192.168.2.2) ping Pc3(192.168.2.130):

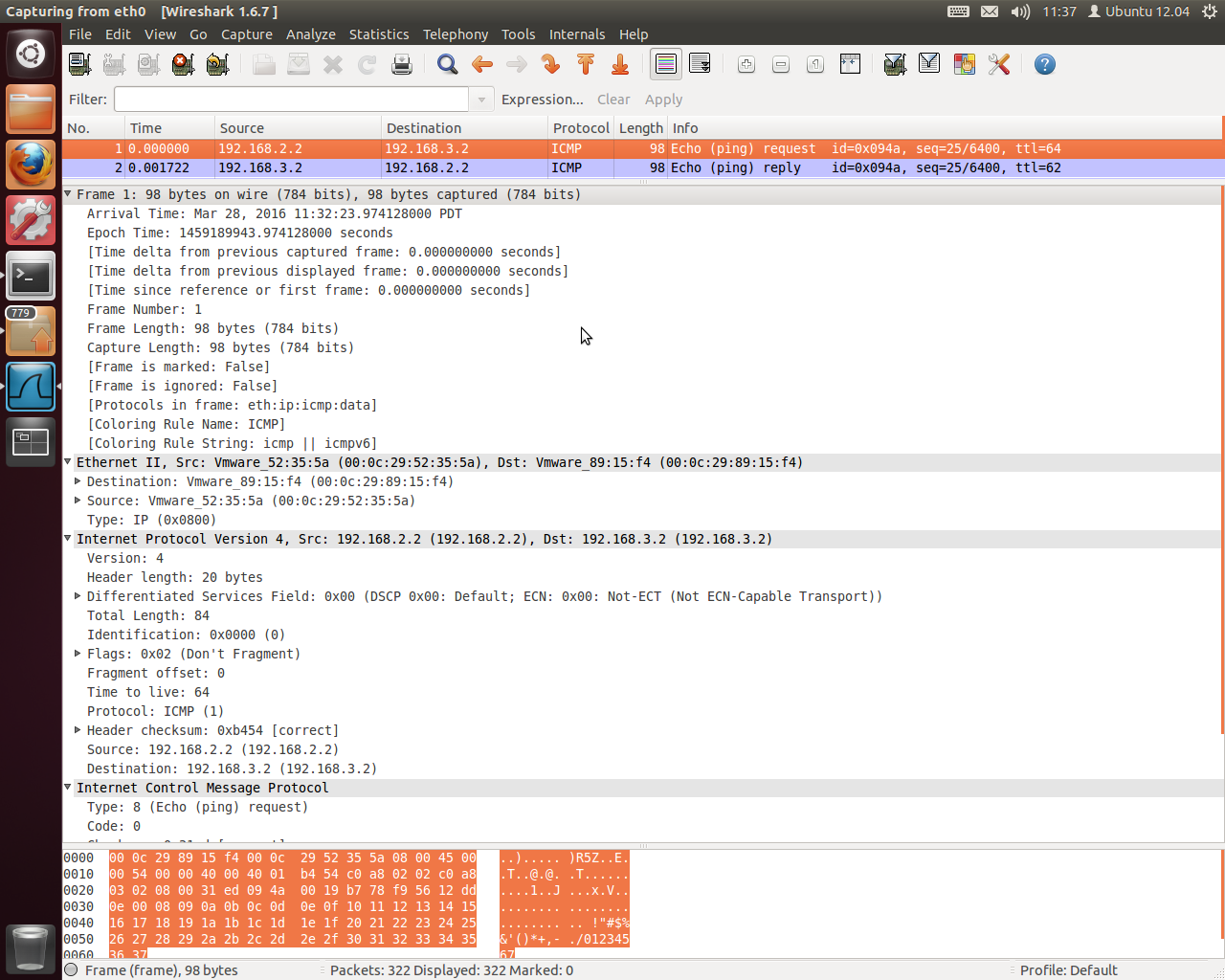


(图为在PC0上的截图)

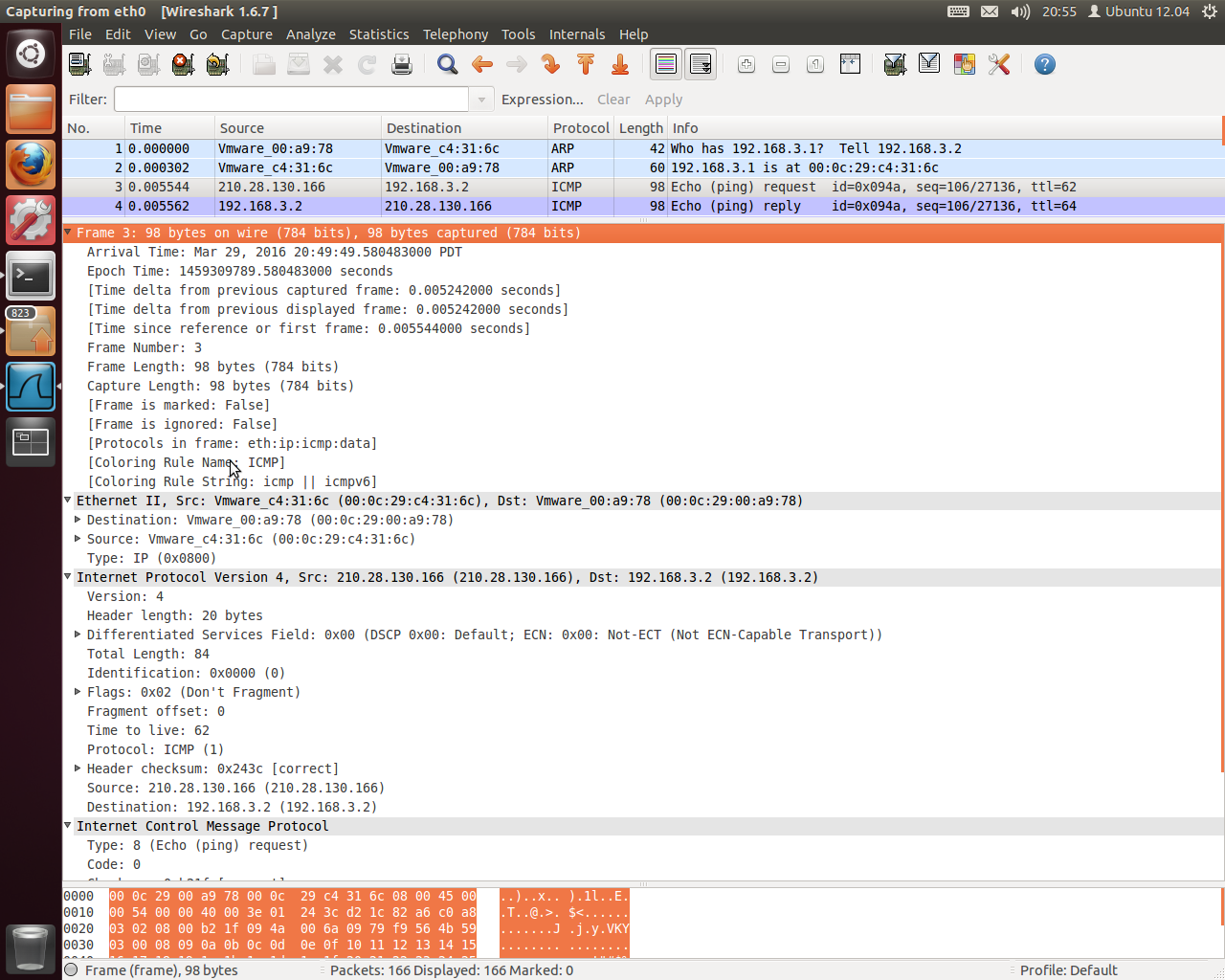


(图为在PC3上的截图)

Pc0(192.168.2.2) ping Pc2(192.168.3.2):



(图为在PC0上的截图)



(图为在PC2上的截图)

1. **协议报文分析：**

PC0 ping PC2：

1.由于PC0与PC2不在一个子网内，所以PC0 ping PC2时就会直接向其默认网关进行发送，即PC0将数据报完整的发到switch0（192.168.2.1）中，然后等待回应；

2.当switch0收到来自PC0的请求后，会自动的转发给所在的路由（router0），等待router0进行转发；

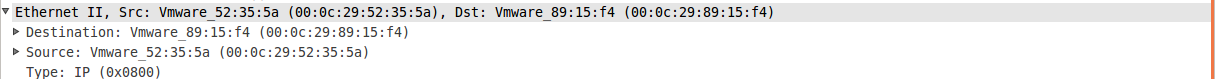
3.Router0接收到来自switch0的数据报后，通过分析得到其目的IP地址是PC2（192.168.3.2）与自己所在的子网（192.168.2.0/24）不一致，所以router0判定其不在自己所在的子网当中，所以router0将其发送到自己的默认网关（210.28.130.166）中，由网关进行转发；

4.当router0的网关接受到来自router0的数据报后会根据路由表进行比较，最后判定该IP应该由router1的网关（210.28.130.100）进行转发，于是将该数据包发送至router1的网关；

5.Router1的网关收到数据报后，会根据路由表进行比较，比较后发现目的IP属于switch2所在的子网内，于是将其发送到switch2（192.168.3.1），由switch2进行转发；

1. Switch2收到包后，将其转发到PC2中，数据报的传送完成。
2. 对于截图进行分析：
   1. 对于PC0上的wireshark截图：

1.以太网帧：

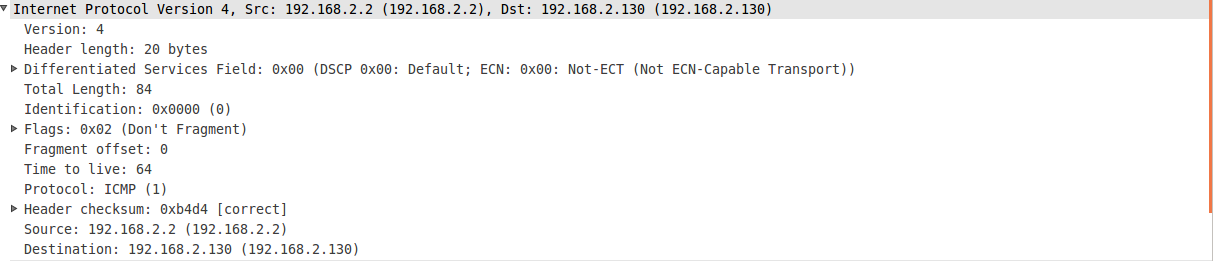


目的Mac地址：00：0c：29：89：15：f4；

源Mac地址：00：0c：29：52：35：5a；

数据报类型：0x0800（IP协议）；

2.IP数据报：



IP version（版本号）：4（发送IPV4数据报）；

IP头长度：20字节；

总长度：84字节；

生存期：64s；

协议类型：ICMP

头部检验和：0xb4d4；

源IP地址：192.168.2.2；

目的IP地址：192.168.2.130

3.ICMP协议报文：

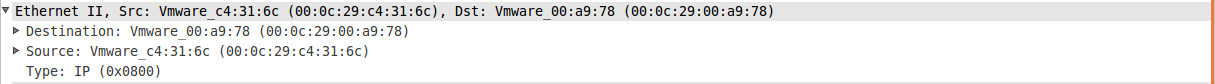
C:\Users\kirito\Desktop\ICMP.png

ICMP type：8（ECHO）表示ping的请求报文；

ICMP code：0；

* 1. 对于PC2上的wireshark截图：

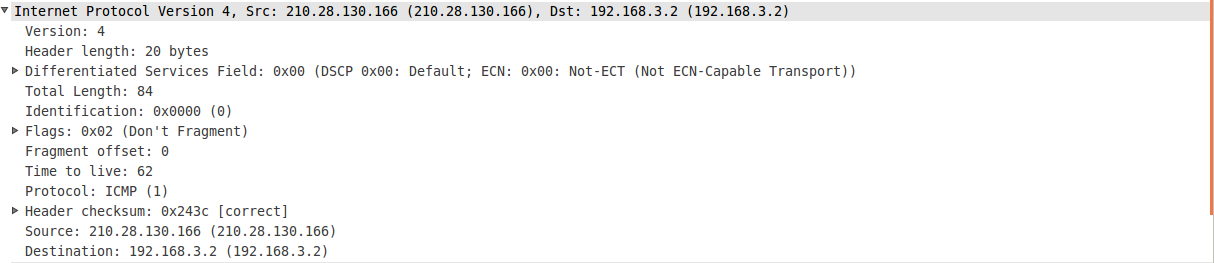
1.以太网帧：



目标Mac地址：00：0c：29：00：a9：78；

源Mac地址：00：0c：29：c4：31：6c；

协议类型：0x0800（IP协议）；



IP version（版本号）：4（发送IPV4数据报）；

IP头长度：20字节；

总长度：84字节；

生存期：62s；

协议类型：ICMP

头部检验和：0x243c；

源IP地址：210.28.130.166；

目的IP地址：192.168.3.2；

**\*\*NAT命令作用：**

**在这里体现了NAT命令的作用，本来对于PC0 ping PC2来说，目的地址是PC2（192.168.3.2），源地址是PC0（192.168.2.2），但是通过NAT协议地址转换，在router0转发时将源地址（192.168.2.2）改成了路由网关的地址（210.28.130.166），所以在PC2的wireshark上的截图就会将210.28.130.166当成发送该数据报的源地址，而在PC0上源地址则是192.168.2.2；**

3.ICMP协议报文：

C:\Users\kirito\Desktop\ICMP.png

ICMP type：8（ECHO）表示ping的请求报文；

ICMP code：0；

**7. 关于子网划分的规则：**

由于switch0下有80台主机，所以我们可以为其分配128个地址，也就是掩码设置为255.255.255.128，这样在switch0所在的子网中，主机IP地址是192.168.2.0，广播IP地址是255.255.255.128，其他的（192.168.2.0/25）126个IP地址划分给switch0进行分配。

同样，对于switch1，我们可以为他分配64个IP地址，也就是将掩码设置为255.255.255.224，这样主机地址是192.168.2.224，广播地址是255.255.255.255，其他的（192.168.2.0/27）30个IP地址分配给该子网内的主机。