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：

a) 了解如何配置一个包含多个子网的网络环境；

b) 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

3. 路由规则配置：

a) Pc0：

```
sudo ifconfig eth0 192.168.2.2 netmask 255.255.255.128
route add default gw 192.168.2.1
```

b) Pc1：

```
sudo ifconfig eth0 192.168.2.3 netmask 255.255.255.128
route add default gw 192.168.2.1
```

c) Pc3：

```
sudo ifconfig eth0 192.168.2.130 netmask 255.255.255.224
route add default gw 192.168.2.129
```

d) 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
route add default gw 210.28.130.166
ip route add 192.168.3.0/24 via 210.28.130.100
```

e) 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
route add default gw 210.28.130.100
ip route add 192.168.2.0/24 via 210.28.130.166

f) Pc2：

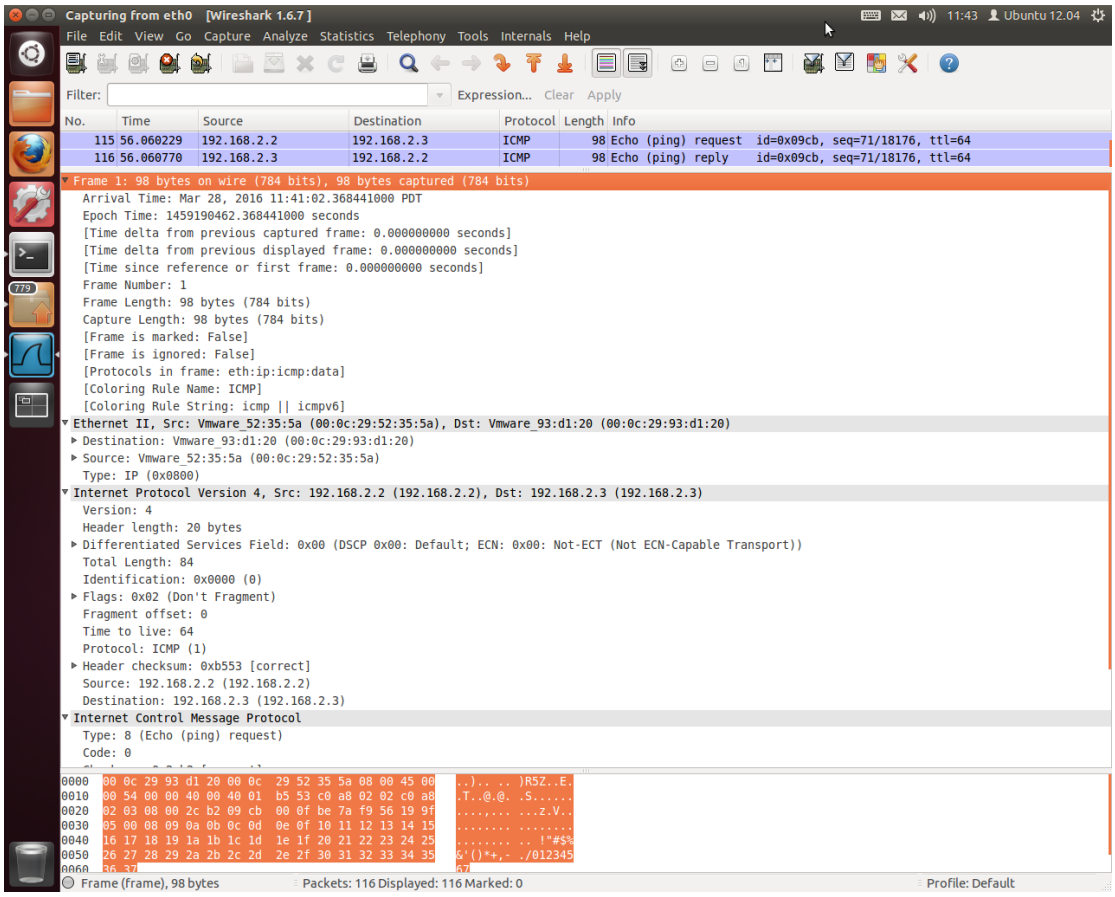
sudo ifconfig eth0 192.168.3.2 netmask 255.255.255.0
route add default gw 192.168.3.1

4. NAT 设置命令：

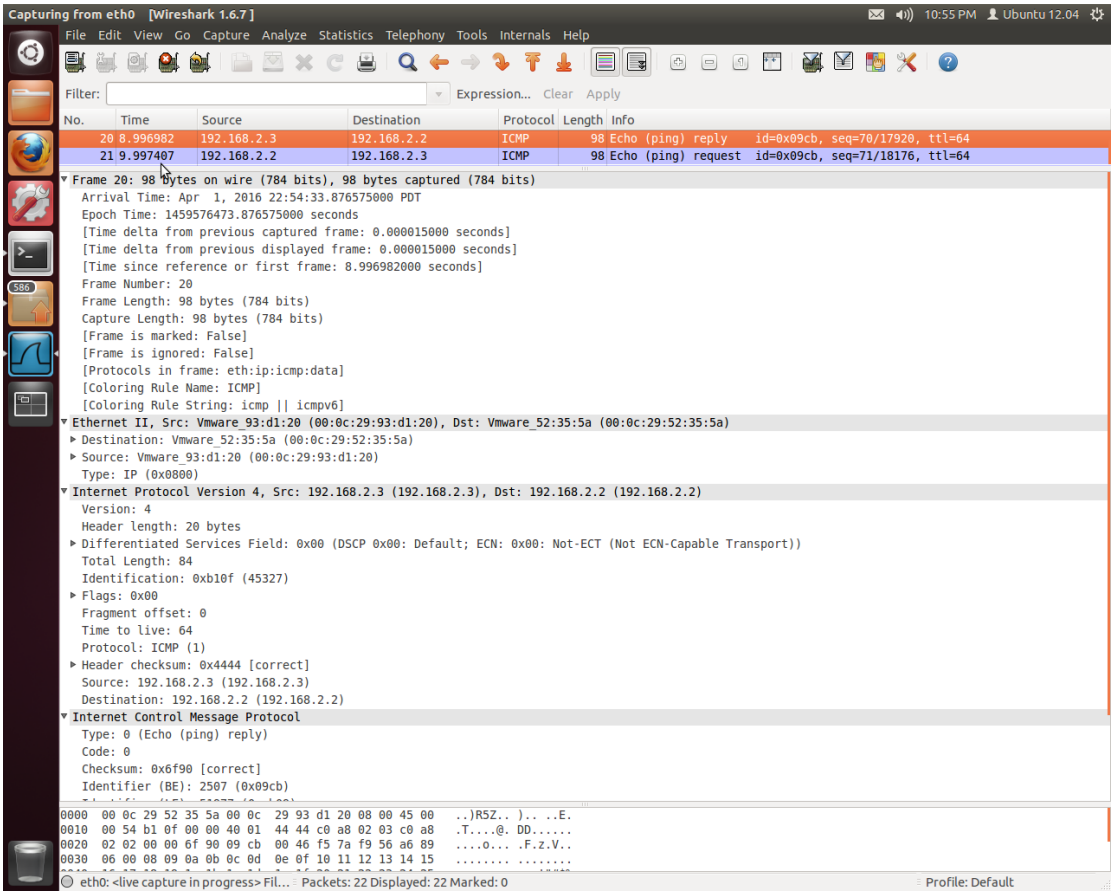
sudo iptables -t nat -A POSTROUTING -o eth0 -s 192.168.2.0/24 -j SNAT --to 210.28.130.166

5. 数据包截图：

Pc0(192.168.2.2) ping Pc1(192.168.2.3):

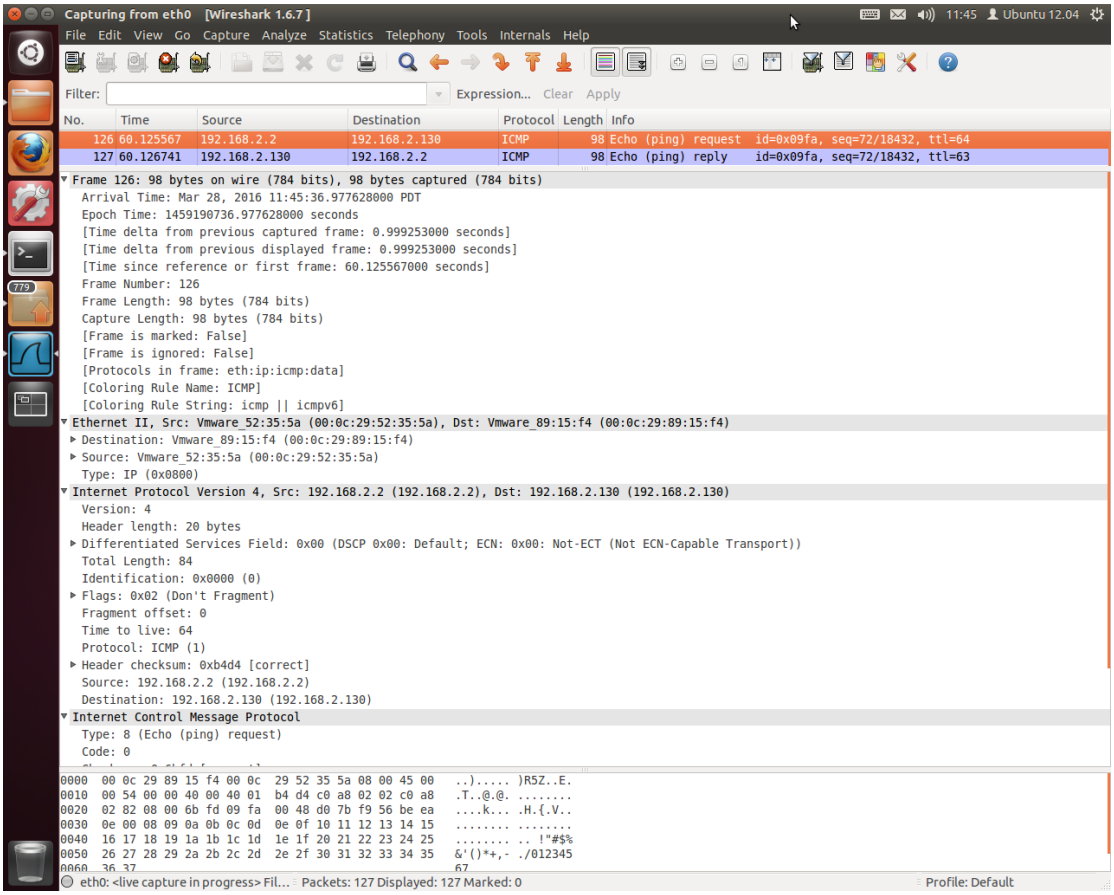


(图为在 PC0 上的截图)

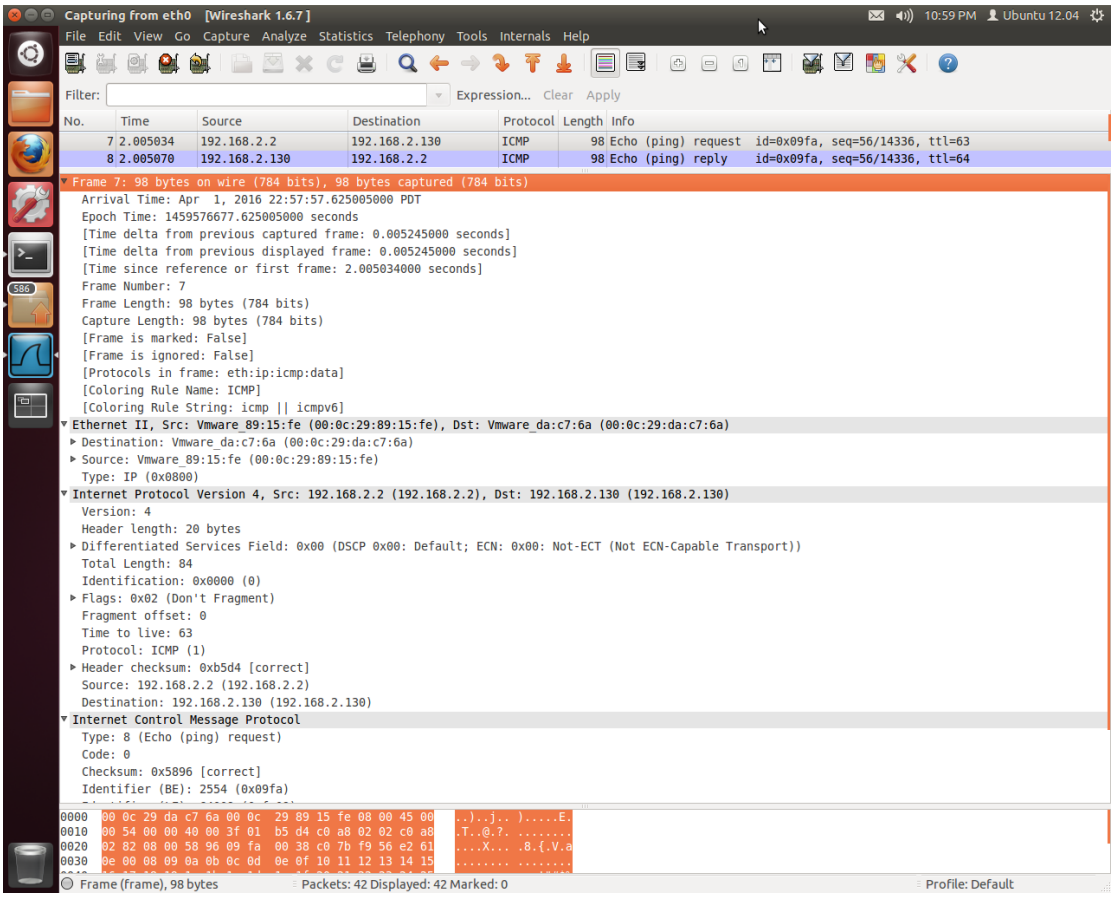


(图为在 PC1 上的截图)

Pc0(192.168.2.2) ping Pc3(192.168.2.130):

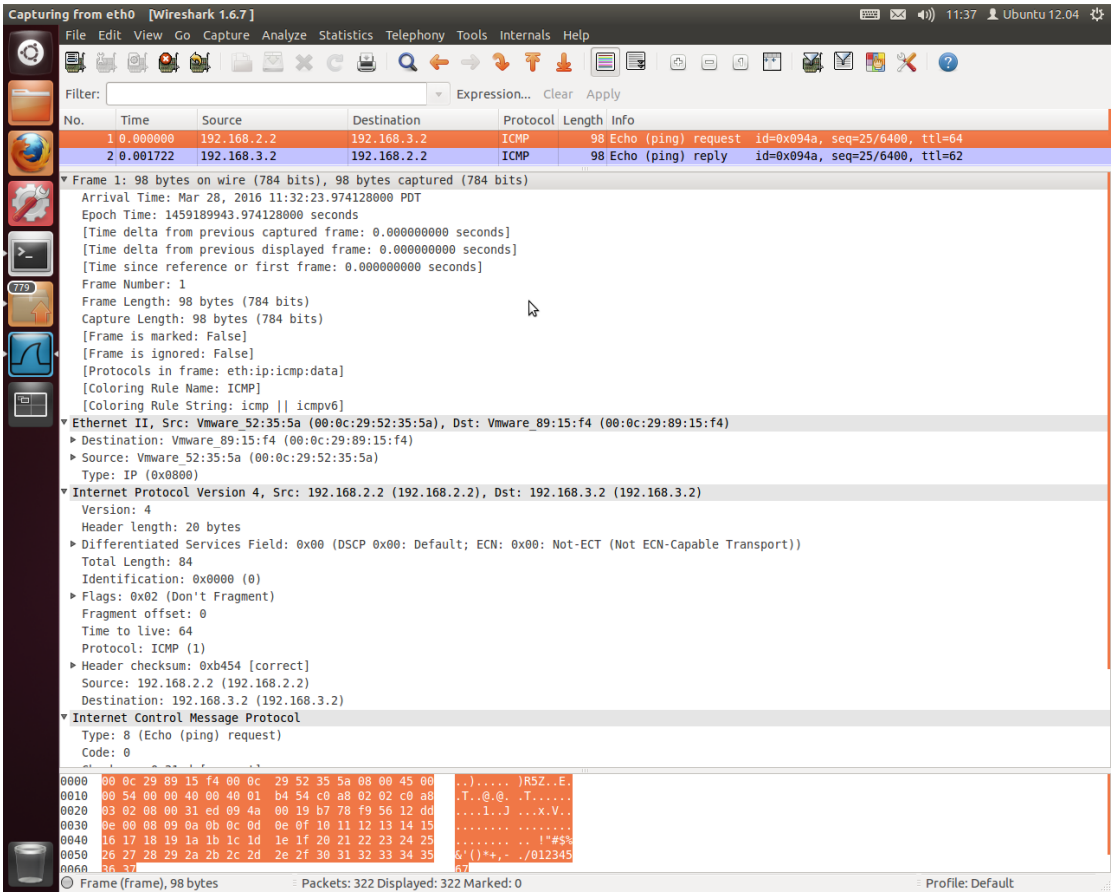

Capturing from eth0 [Wireshark 1.6.7]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length Info
126 60.125567 192.168.2.2 192.168.2.130 ICMP 98 Echo (ping) request id=0x09fa, seq=72/18432, ttl=64
127 60.126741 192.168.2.130 192.168.2.2 ICMP 98 Echo (ping) reply id=0x09fa, seq=72/18432, ttl=63
Frame 126: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Arrival Time: Mar 28, 2016 11:45:36.977628000 PDT
Epoch Time: 1459190736.977628000 seconds
[Time delta from previous captured frame: 0.999253000 seconds]
[Time delta from previous displayed frame: 0.999253000 seconds]
[Time since reference or first frame: 60.125567000 seconds]
Frame Number: 126
Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Vmware_52:35:5a (00:0c:29:52:35:5a), Dst: Vmware_89:15:f4 (00:0c:29:89:15:f4)
Destination: Vmware_89:15:f4 (00:0c:29:89:15:f4)
Source: Vmware_52:35:5a (00:0c:29:52:35:5a)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.2.130 (192.168.2.130)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 84
Identification: 0x0000 (0)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 64
Protocol: ICMP (1)
Header checksum: 0xb4d4 [correct]
Source: 192.168.2.2 (192.168.2.2)
Destination: 192.168.2.130 (192.168.2.130)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
0000 00 0c 29 89 15 f4 00 0c 29 52 35 5a 08 00 45 00 ..).....)R5Z..E.
0010 00 54 00 00 40 00 40 01 b4 d4 c0 a8 02 02 c0 a8 .T..@.@. ....
0020 02 82 08 00 6b fd 09 fa 00 48 d0 7b f9 56 be ea ....k... .H.{.V..
0030 0e 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 ....
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 .... !"#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
0060 36 37 67
eth0: <live capture in progress> Fil... Packets: 127 Displayed: 127 Marked: 0
Profile: Default

(图为在 PC0 上的截图)

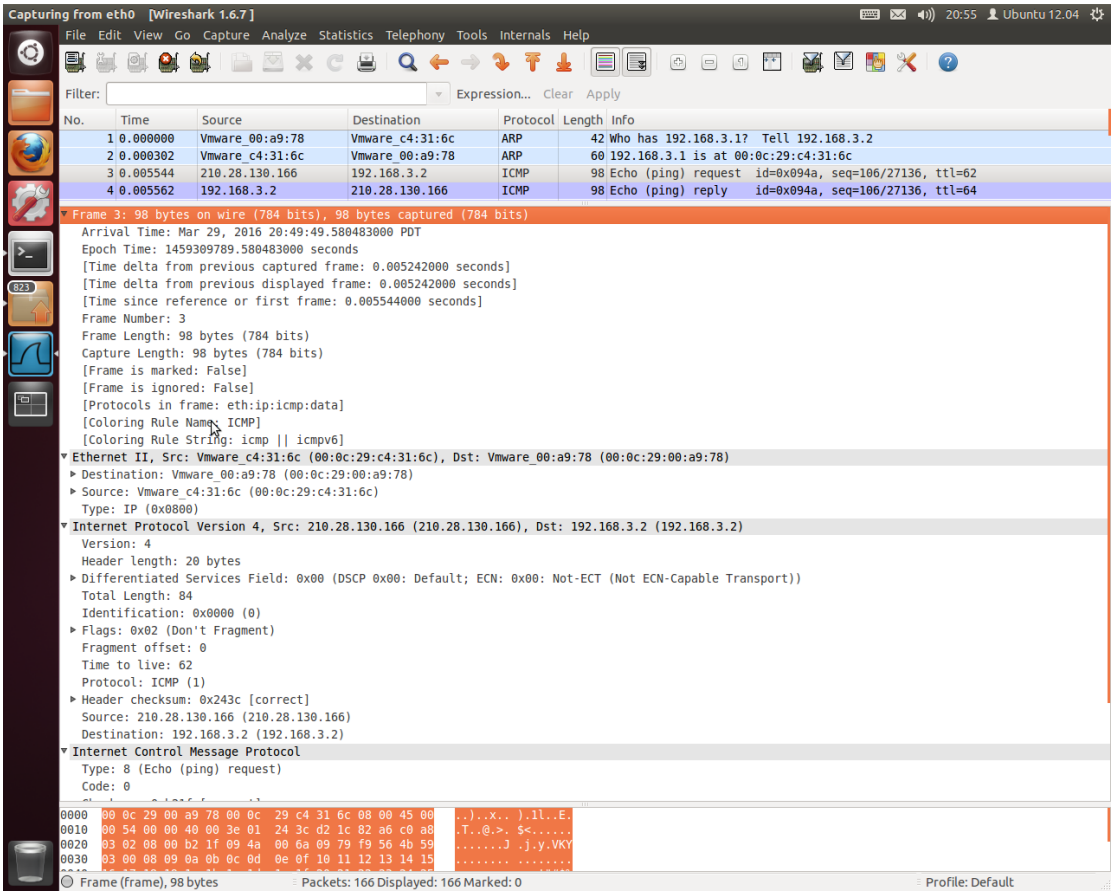

Capturing from eth0 [Wireshark 1.6.7]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Length Info
7 2.005034 192.168.2.2 192.168.2.130 ICMP 98 Echo (ping) request id=0x09fa, seq=56/14336, ttl=63
8 2.005070 192.168.2.130 192.168.2.2 ICMP 98 Echo (ping) reply id=0x09fa, seq=56/14336, ttl=64
Frame 7: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Arrival Time: Apr 1, 2016 22:57:57.625005000 PDT
Epoch Time: 1459576677.625005000 seconds
[Time delta from previous captured frame: 0.005245000 seconds]
[Time delta from previous displayed frame: 0.005245000 seconds]
[Time since reference or first frame: 2.005034000 seconds]
Frame Number: 7
Frame Length: 98 bytes (784 bits)
Capture Length: 98 bytes (784 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ip:icmp:data]
[Coloring Rule Name: ICMP]
[Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: Vmware_89:15:fe (00:0c:29:89:15:fe), Dst: Vmware_da:c7:6a (00:0c:29:da:c7:6a)
Destination: Vmware_da:c7:6a (00:0c:29:da:c7:6a)
Source: Vmware_89:15:fe (00:0c:29:89:15:fe)
Type: IP (0x0800)
Internet Protocol Version 4, Src: 192.168.2.2 (192.168.2.2), Dst: 192.168.2.130 (192.168.2.130)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 84
Identification: 0x0000 (0)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 63
Protocol: ICMP (1)
Header checksum: 0xb5d4 [correct]
Source: 192.168.2.2 (192.168.2.2)
Destination: 192.168.2.130 (192.168.2.130)
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x5896 [correct]
Identifier (BE): 2554 (0x09fa)
0000 00 0c 29 da c7 6a 00 0c 29 89 15 fe 08 00 45 00 ..)..j..).....E.
0010 00 54 00 00 40 00 3f 01 b5 d4 c0 a8 02 02 c0 a8 .T..@.?. ....
0020 02 82 08 00 58 96 09 fa 00 38 c0 7b f9 56 e2 61 ....X... .8.{.V.a
0030 0e 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 ....
Frame (frame), 98 bytes Packets: 42 Displayed: 42 Marked: 0
Profile: Default

(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)

6. 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；

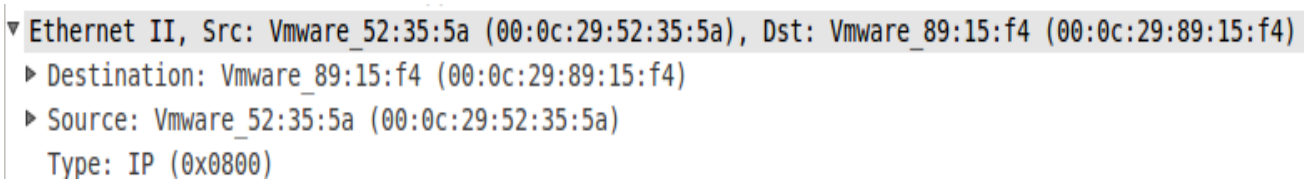
5.Router1 的网关收到数据报后，会根据路由表进行比较，比较后发现目的 IP 属于 switch2 所在的子网内，于是将其发送到 switch2（192.168.3.1），由 switch2 进行转发；

7. Switch2 收到包后，将其转发到 PC2 中，数据报的传送完成。

8. 对于截图进行分析：

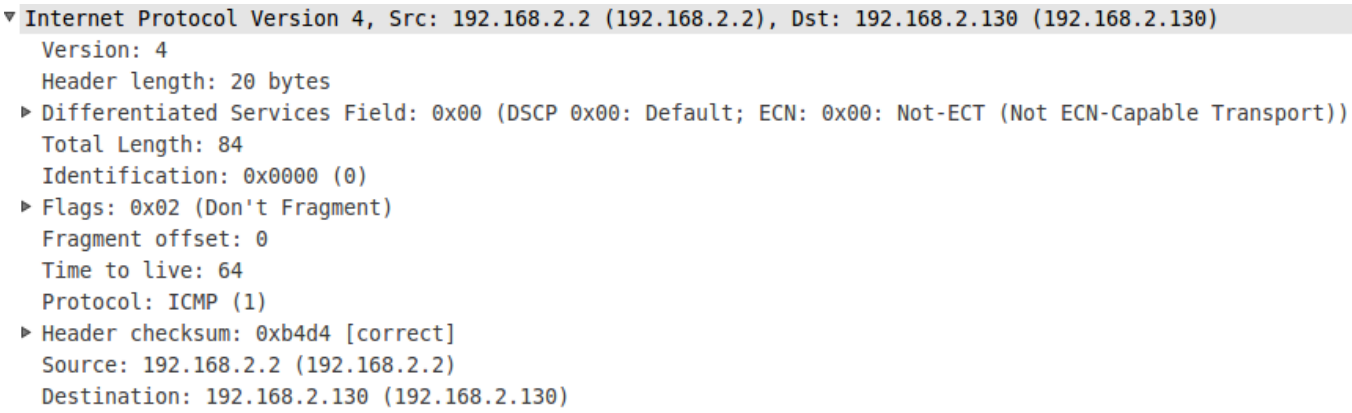
a) 对于 PC0 上的 wireshark 截图：

1.以太网帧：



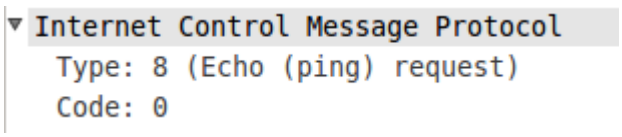
目的 Mac 地址：00：0c：29：89：15：f4；
源 Mac 地址：00：0c：29：52：35：5a；
数据报类型：0x0800（IP 协议）；

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：



ICMP type：8（ECHO）表示 ping 的请求报文；
ICMP code：0；

b) 对于 PC2 上的 wireshark 截图：

1.以太网帧：

```
▼ Ethernet II, Src: Vmware_c4:31:6c (00:0c:29:c4:31:6c), Dst: Vmware_00:a9:78 (00:0c:29:00:a9:78)
  ▶ Destination: Vmware_00:a9:78 (00:0c:29:00:a9:78)
  ▶ Source: Vmware_c4:31:6c (00:0c:29:c4:31:6c)
    Type: IP (0x0800)
```

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）；

```
▼ Internet Protocol Version 4, Src: 210.28.130.166 (210.28.130.166), Dst: 192.168.3.2 (192.168.3.2)
    Version: 4
    Header length: 20 bytes
  ▶ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 84
    Identification: 0x0000 (0)
  ▶ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 62
    Protocol: ICMP (1)
  ▶ Header checksum: 0x243c [correct]
    Source: 210.28.130.166 (210.28.130.166)
    Destination: 192.168.3.2 (192.168.3.2)
```

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：

```
▼ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
```

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。