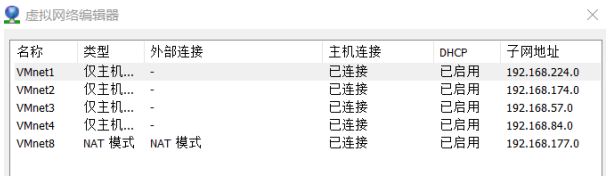
计算机网络实验一

一．实验目的

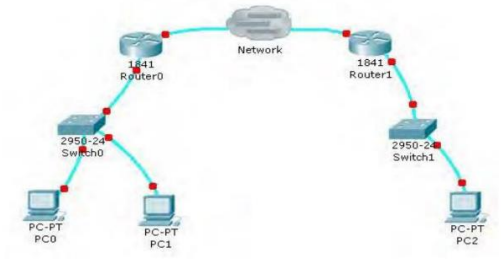
1. 熟悉基本网络工具集的使用
2. 初步了解 PDU 观测工具 Wireshark
3. 加深对子网、子网掩码、网关、路由器、交换机等网络概念的理解
4. 学习路由规则，体会“下一跳”的概念，理解数据包传送过程的转发机制
5. 进一步学习虚拟机、linux 平台以及使用命令行

二．拓扑结构搭建

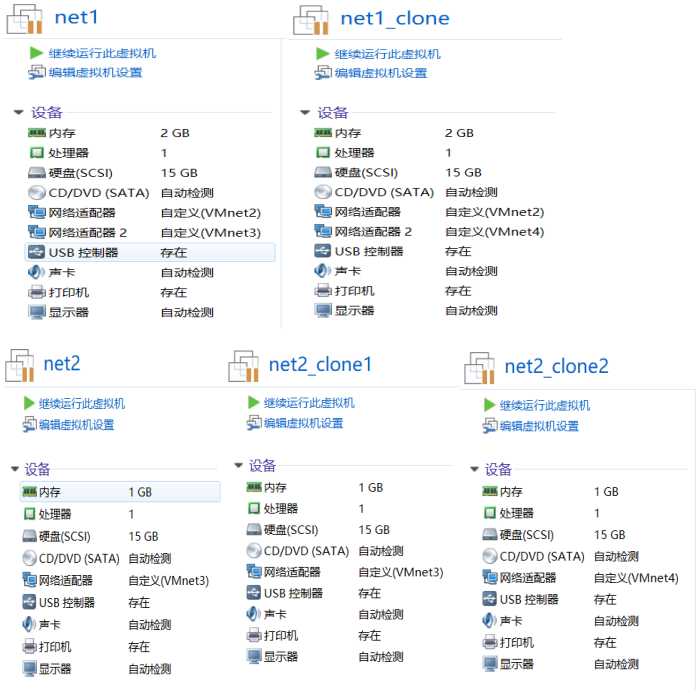
VMware Workstation 提供了七个虚拟交换机，选取其中的三个 vmvet2、vmvet3、vmvet4 作为本次实验的虚拟交换机，在设置中给虚拟交换机自动分配了 ip 如下



然后根据拓扑结构图如下



设 net1 和 net1_clone 为路由器，net2、net2_clone1、net2_clone2 为终端，设置网络适配器如下图



三．网络拓扑配置

节点名	虚拟设备名	ip	netmask
Router0	net1	ens33:192.168.174.1	255.255.255.0
		ens38:192.168.57.1	255.255.255.0
Router1	net1_clone	ens33:192.168.174.2	255.255.255.0
		ens38:192.168.84.1	255.255.255.0
PC1	net2	ens33:192.168.57.2	255.255.255.0
PC2	net2_clone1	ens33:192.168.57.3	255.255.255.0
PC3	net2_clone2	ens33:192.168.84.2	255.255.255.0

三．路由规则配置

（1）通过 ifconfig -a|less 查看虚拟机的网络设备

（2）然后设置 ip：

net1:

```
sudo ifconfig ens33 192.168.174.1 netmask 255.255.255.0
sudo ifconfig ens38 192.168.57.1 netmask 255.255.255.0
```

net1_clone:

```
sudo ifconfig ens33 192.168.174.2 netmask 255.255.255.0
sudo ifconfig ens38 192.168.84.1 netmask 255.255.255.0
```

net2:

```
sudo ifconfig ens33 192.168.57.2 netmask 255.255.255.0
```

net2_clone1:

```
sudo ifconfig ens33 192.168.57.3 netmask 255.255.255.0
```

net2_clone2:

```
sudo ifconfig ens33 192.168.84.2 netmask 255.255.255.0
```

（3）其次需要设置终端的网关

net2:

```
sudo route add default gw 192.168.57.1
```

net2_clone1:

```
sudo route add default gw 192.168.57.1
```

net2_clone2:

```
sudo route add default gw 192.168.84.1
```

(4)最后设置路由器的路由规则并允许转发

net1:

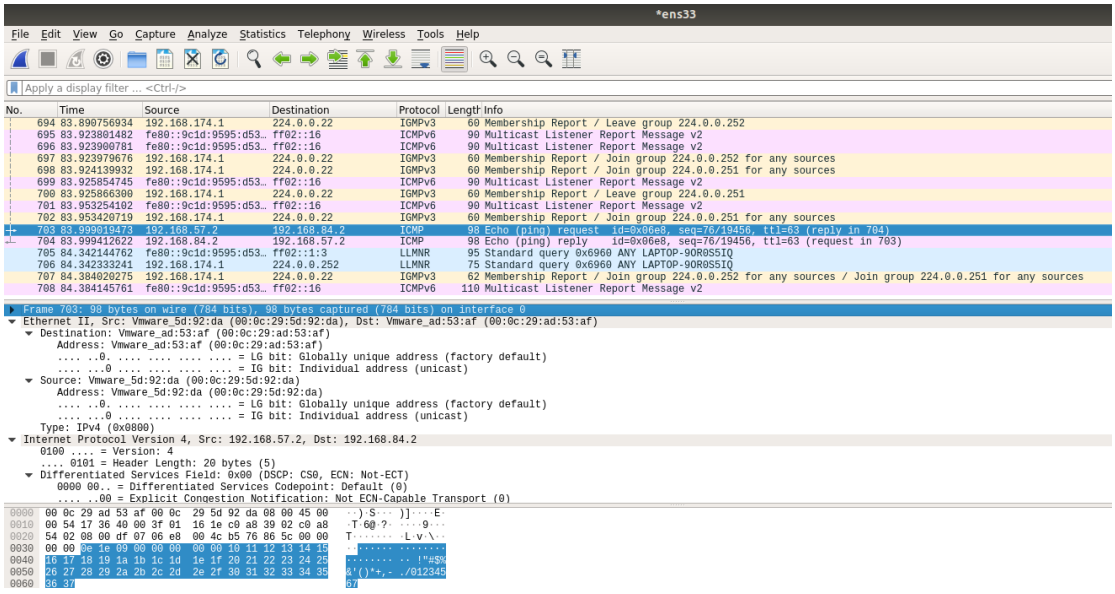
```
sudo ip route add 192.168.84.0/24 via 192.168.174.2
```

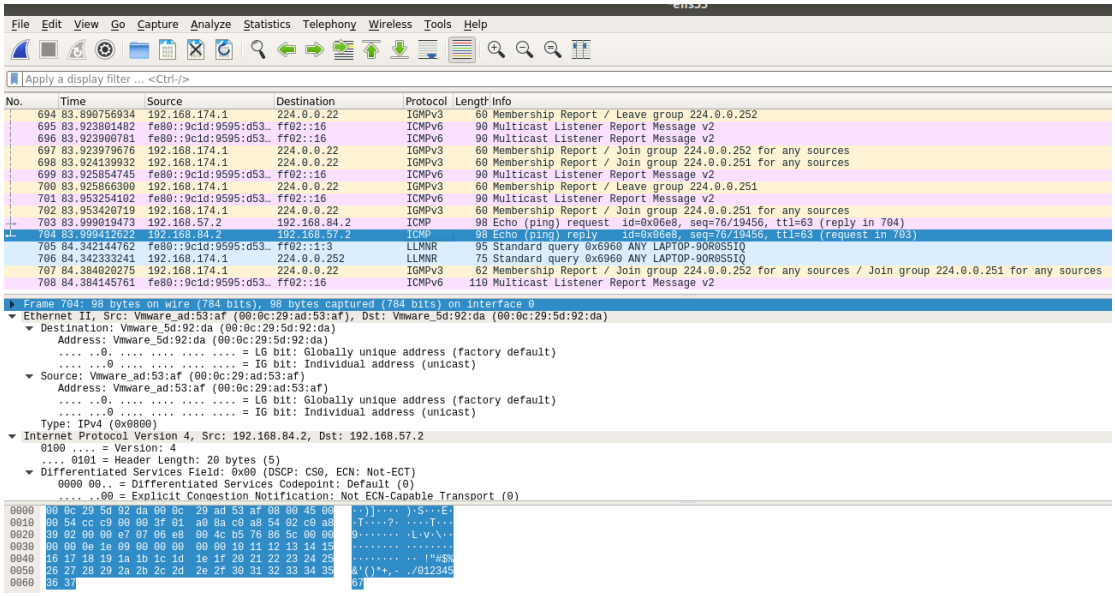
```
sudo su
echo 1 > /proc/sys/net/ipv4/ip_forward
exit

net1_clone:
sudo ip route add 192.168.57.0/24 via 192.168.174.1
sudo su
echo 1 > /proc/sys/net/ipv4/ip_forward
exit
```

然后在终端如 net2：ping 192.168.84.2
然后在路由器 net1： sudo wireshark 即可抓包

四．数据包截图

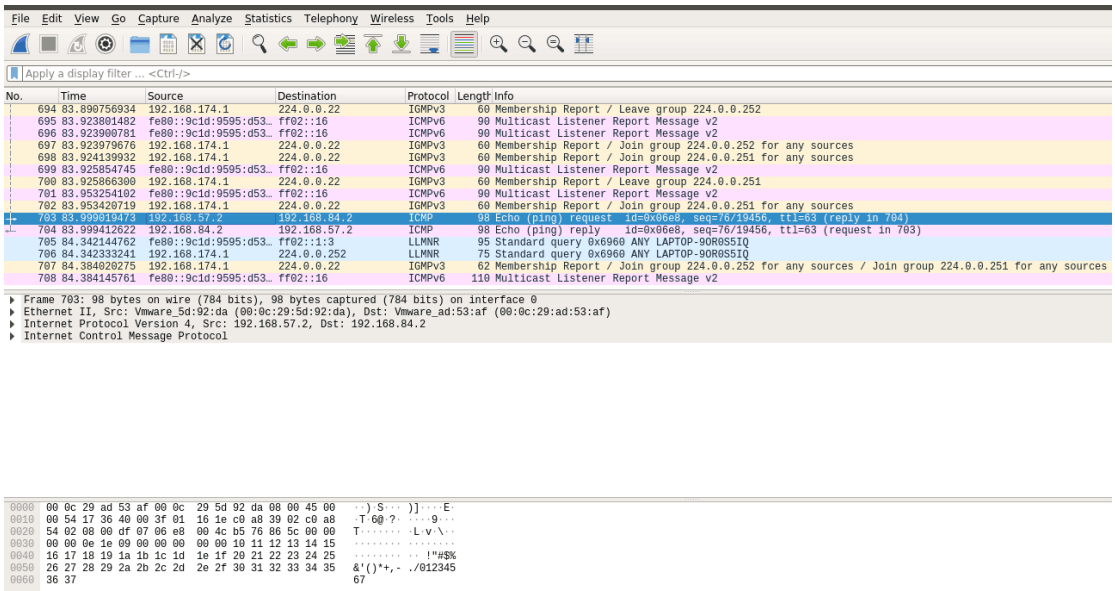
两条记录分别是从 net2 发送到 net2_clone2 的数据包、从 net2_clone2 返回应答的数据包





五．协议报文分析

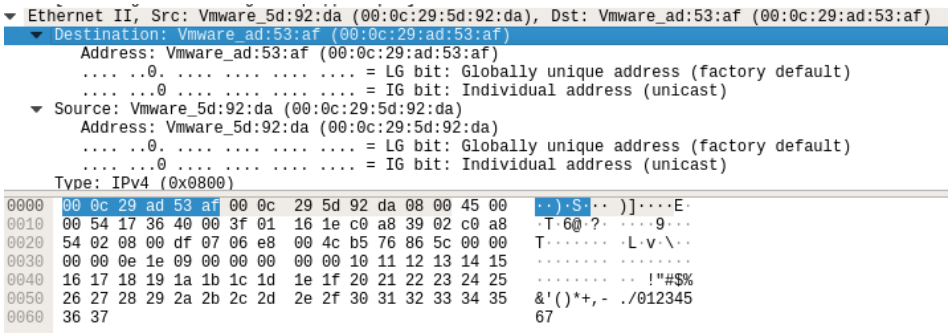
接下来以 net2 to net2_clone2 为例，对抓取的数据包进行字段分析：



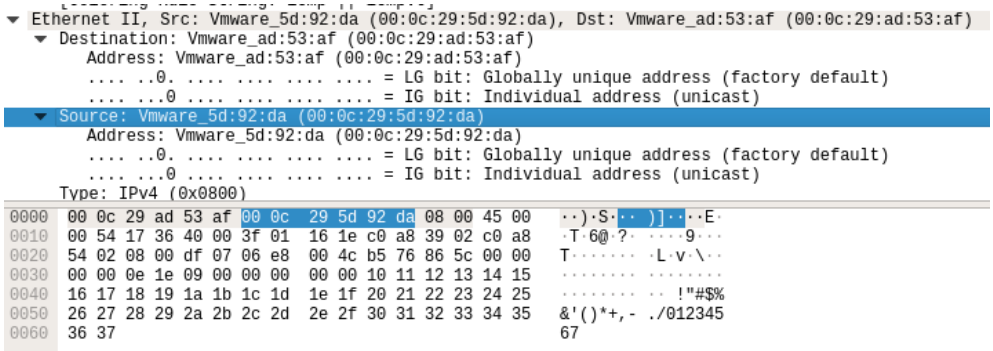
Frame:所抓的包为一个帧，帧号为 703，帧大小为 98bytes

Ethernet:以太网，有线局域网技术，属于链路层

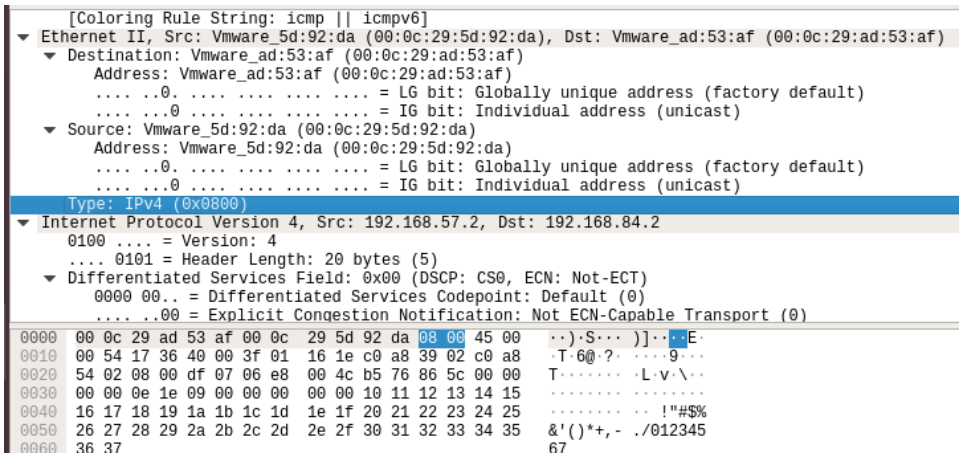
Internet protocol：IP 协议，网络层，ipv4，源 ip 为 192.168.57.2，目的 ip 为 192.168.84.2



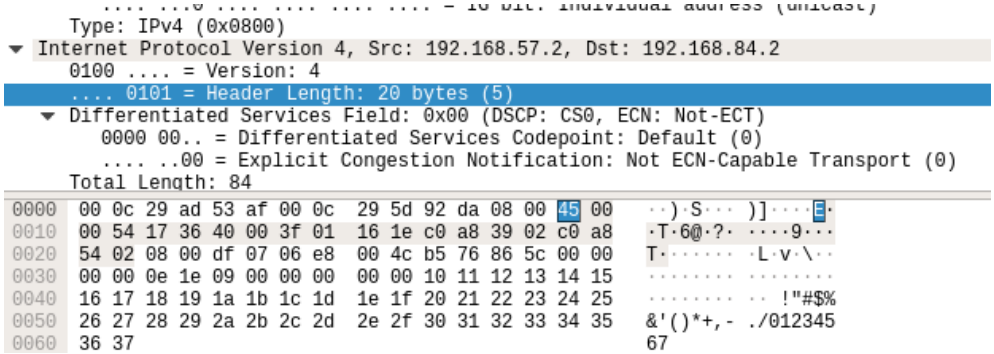
目的地的 MAC 地址：00：0c:29:ad:53:af



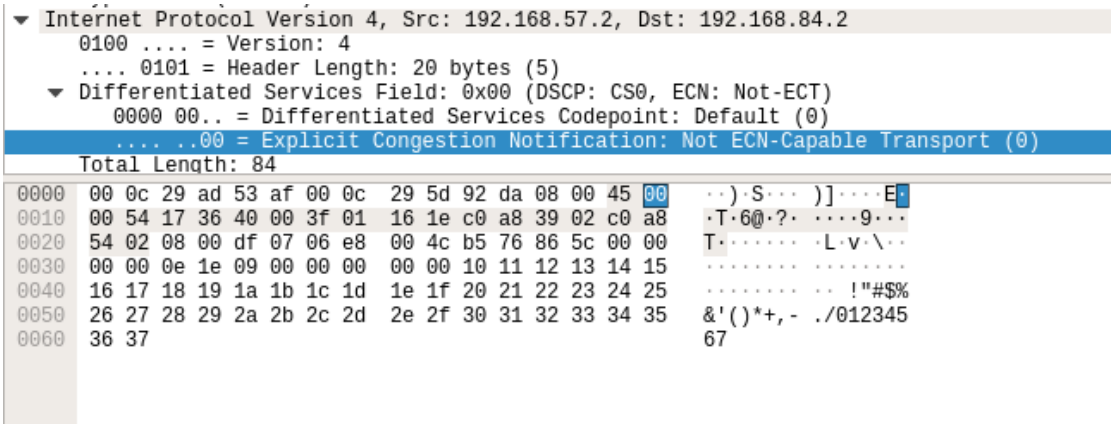
源 MAC 地址:00：0c:29:5d:92:da



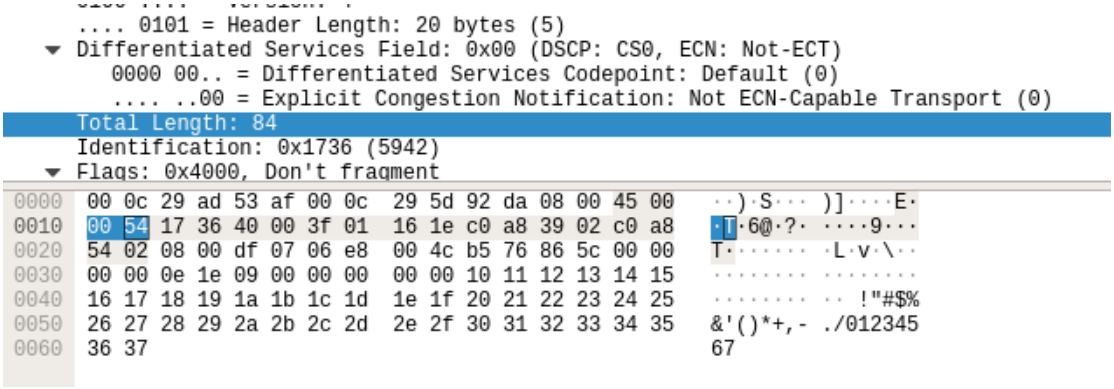
协议类型为 ipv4（0x0800）



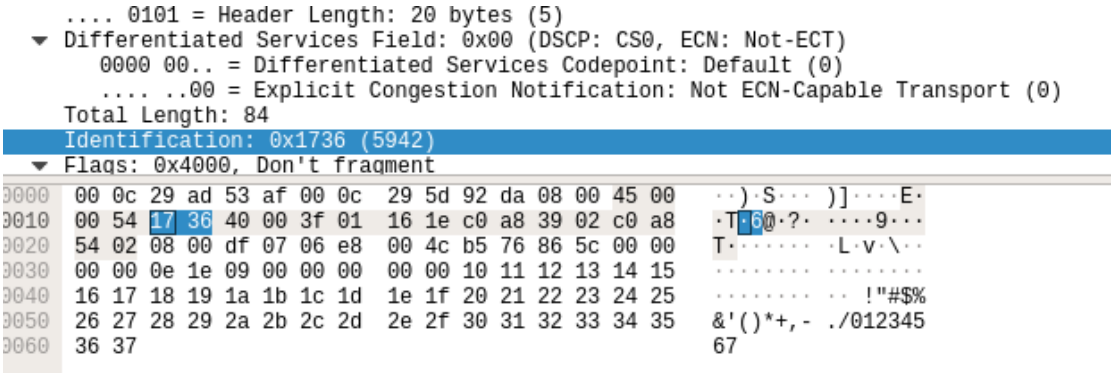
Ip 协议版本 4，20 bytes(5)



00 表示 explicit congestion notification:not ecn-capable transport 即明确的阻塞指示



总长度为 0x54



鉴别号 0x1736

```
    Identification: 0x1736 (5942)
  ▼ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 63
0000  00 0c 29 ad 53 af 00 0c  29 5d 92 da 08 00 45 00   ··)·S··· )]····E·
0010  00 54 17 36 40 00 3f 01  16 1e c0 a8 39 02 c0 a8   ·T·6@·?· ····9···
0020  54 02 08 00 df 07 06 e8  00 4c b5 76 86 5c 00 00   T······ ·L·v·\··
0030  00 00 0e 1e 09 00 00 00  00 00 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
```

标志 flag 为 0x4000

```
  ▼ Flags: 0x4000, Don't fragment
      0... .... .... .... = Reserved bit: Not set
      .1.. .... .... .... = Don't fragment: Set
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 63
    Protocol: ICMP (1)
    Header checksum: 0x161e [validation disabled]
0000  00 0c 29 ad 53 af 00 0c  29 5d 92 da 08 00 45 00   ··)·S··· )]····E·
0010  00 54 17 36 40 00 3f 01  16 1e c0 a8 39 02 c0 a8   ·T·6@·?· ····9···
0020  54 02 08 00 df 07 06 e8  00 4c b5 76 86 5c 00 00   T······ ·L·v·\··
0030  00 00 0e 1e 09 00 00 00  00 00 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
```

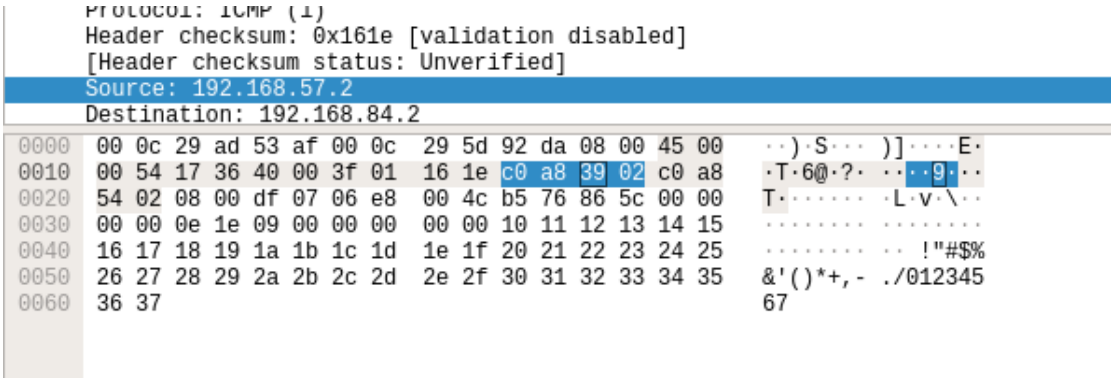
生存期为 0x3f

```
      ..0. .... .... .... = More fragments: Not set
      ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 63
    Protocol: ICMP (1)
    Header checksum: 0x161e [validation disabled]
0000  00 0c 29 ad 53 af 00 0c  29 5d 92 da 08 00 45 00   ··)·S··· )]····E·
0010  00 54 17 36 40 00 3f 01  16 1e c0 a8 39 02 c0 a8   ·T·6@·?· ····9···
0020  54 02 08 00 df 07 06 e8  00 4c b5 76 86 5c 00 00   T······ ·L·v·\··
0030  00 00 0e 1e 09 00 00 00  00 00 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
```

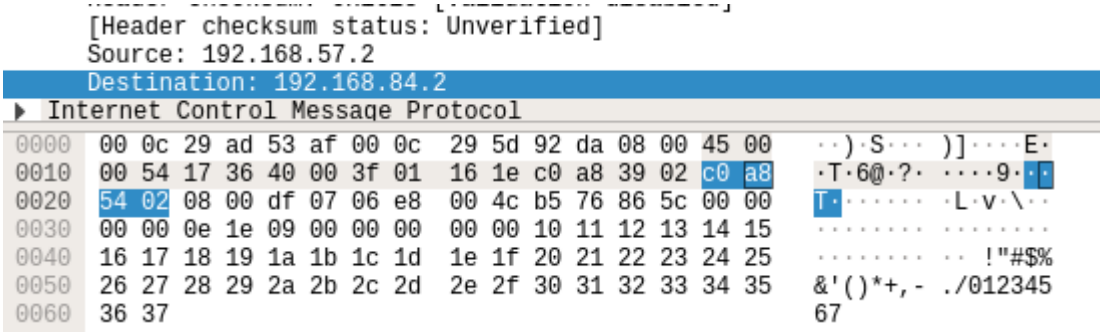
协议名称

```
    Time to live: 63
    Protocol: ICMP (1)
    Header checksum: 0x161e [validation disabled]
    [Header checksum status: Unverified]
0000  00 0c 29 ad 53 af 00 0c  29 5d 92 da 08 00 45 00   ··)·S··· )]····E·
0010  00 54 17 36 40 00 3f 01  16 1e c0 a8 39 02 c0 a8   ·T·6@·?· ····9···
0020  54 02 08 00 df 07 06 e8  00 4c b5 76 86 5c 00 00   T······ ·L·v·\··
0030  00 00 0e 1e 09 00 00 00  00 00 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
```

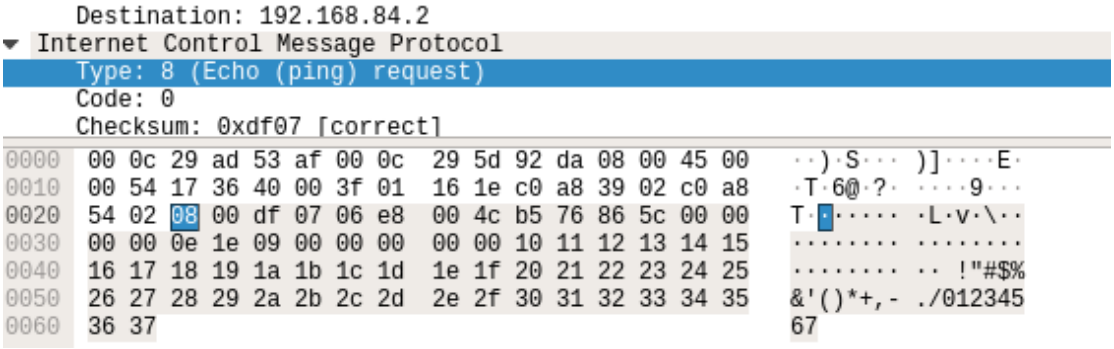
头部校验和校验状态



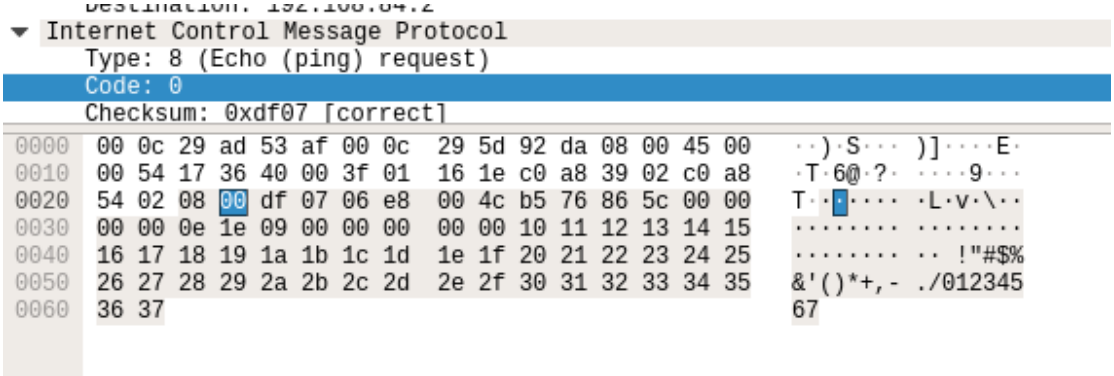
源 ip



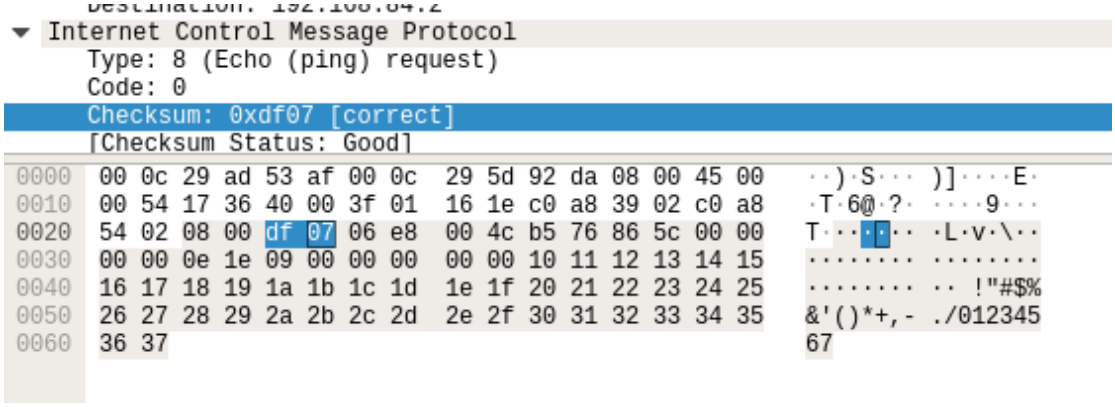
目的 ip



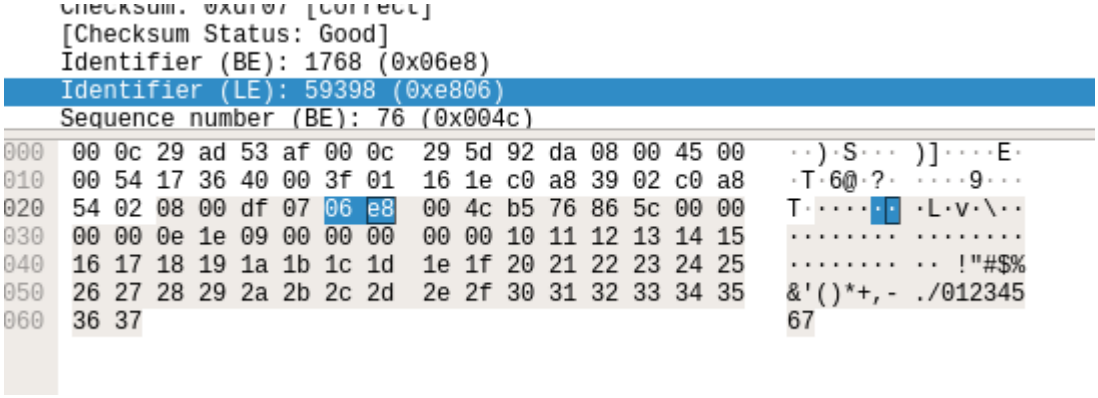
类型：8



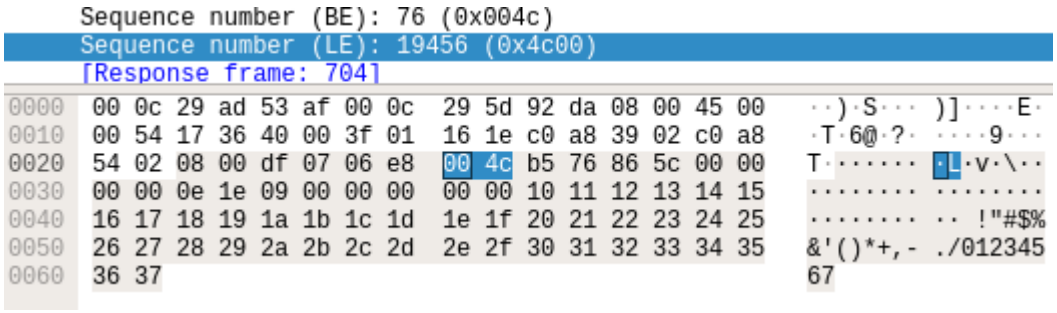
编码：0



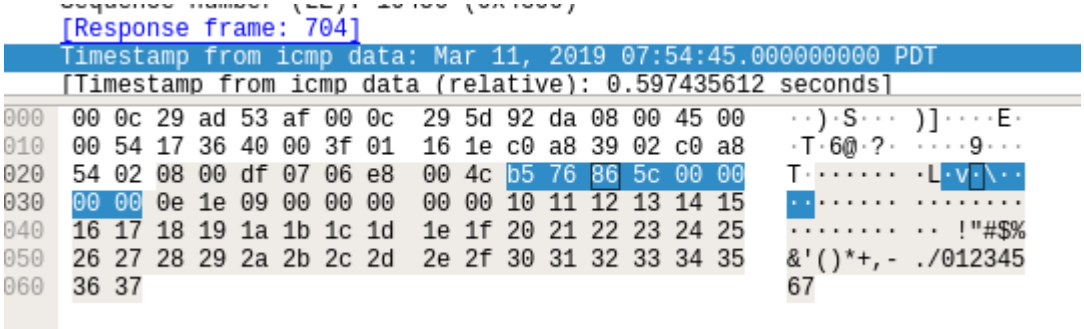
校验和为 0xdf07



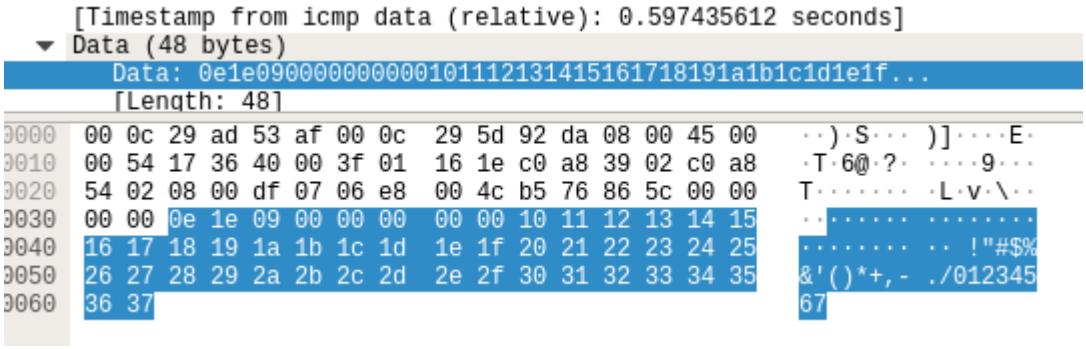
校验者：0xe806



Sequence number：0x4c00



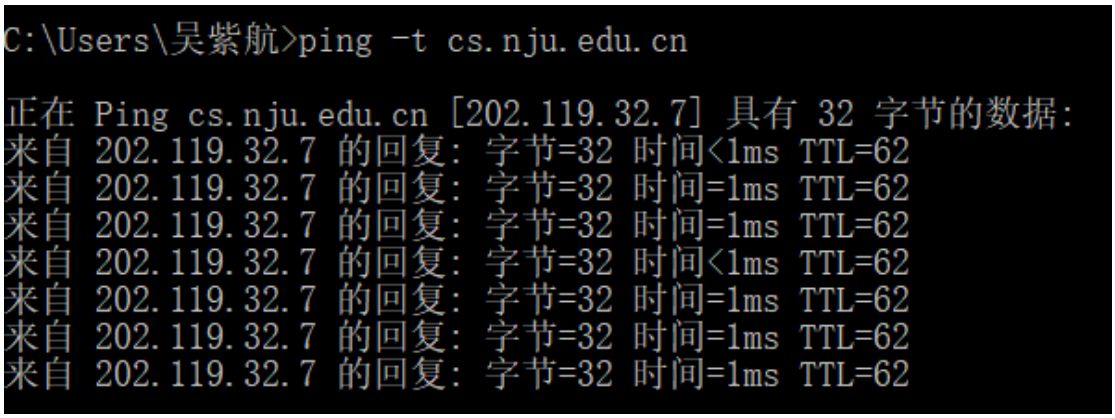
Icmp 数据时间标记 3 月 11 日，2019 年 7 点 54 分 45 秒

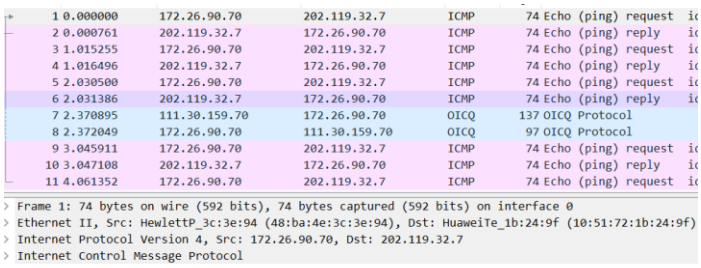


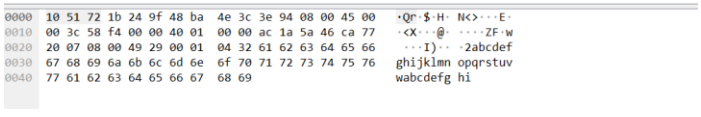
数据包具体的内容

六. Ping 系主页

（1）ping cs.nju.edu.cn 的抓包截图

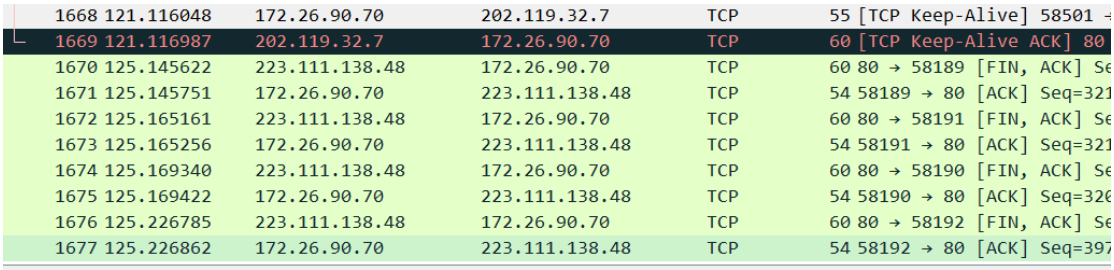






简要说明：帧号 1,74 字节，以太网 2，源 MAC 为 48：ba:4e:3c:3e:94,目的 MAC 为：10：51：72：1b:24:9f,互联网协议版本 4，ipv4，源 ip：172.26.90.70 目的 ip：202.119.32.7

（2）登陆 www.nju.edu.cn 时候的抓包截图



1668	121.116048	172.26.90.70	202.119.32.7	TCP	55 [TCP Keep-Alive] 58501 →
1669	121.116987	202.119.32.7	172.26.90.70	TCP	60 [TCP Keep-Alive ACK] 80
1670	125.145622	223.111.138.48	172.26.90.70	TCP	60 80 → 58189 [FIN, ACK] Se
1671	125.145751	172.26.90.70	223.111.138.48	TCP	54 58189 → 80 [ACK] Seq=321
1672	125.165161	223.111.138.48	172.26.90.70	TCP	60 80 → 58191 [FIN, ACK] Se
1673	125.165256	172.26.90.70	223.111.138.48	TCP	54 58191 → 80 [ACK] Seq=321
1674	125.169340	223.111.138.48	172.26.90.70	TCP	60 80 → 58190 [FIN, ACK] Se
1675	125.169422	172.26.90.70	223.111.138.48	TCP	54 58190 → 80 [ACK] Seq=320
1676	125.226785	223.111.138.48	172.26.90.70	TCP	60 80 → 58192 [FIN, ACK] Se
1677	125.226862	172.26.90.70	223.111.138.48	TCP	54 58192 → 80 [ACK] Seq=397

```
> Frame 1668: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface 0
> Ethernet II, Src: HewlettP_3c:3e:94 (48:ba:4e:3c:3e:94), Dst: HuaweiTe_1b:24:9f (10:51:72:1b:24:9f)
> Internet Protocol Version 4, Src: 172.26.90.70, Dst: 202.119.32.7
> Transmission Control Protocol, Src Port: 58501, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
> Data (1 byte)
```

```
0000  10 51 72 1b 24 9f 48 ba  4e 3c 3e 94 08 00 45 00   ·Qr·$·H· N<>···E·
0010  00 29 57 a8 40 00 80 06  00 00 ac 1a 5a 46 ca 77   ·)W·@··· ····ZF·w
0020  20 07 e4 85 00 50 34 46  5a ff 44 98 e1 ed 50 10    ····P4F Z·D···P·
0030  08 03 f0 fa 00 00 00                               ·******
```

简要说明：帧号 1688，55 字节，以太网 2，源 MAC 为 48：ba:4e:3c:3e:94,目的 MAC 为：10：51：72：1b:24:9f,互联网协议版本 4，ipv4，源 ip：172.26.90.70 目的 ip：202.119.32.7