创新源于实践

《计算机网络原理》

课程实验教学手册

信息工程学院《计算机网络原理》课程组

实验情况一览表

实验序号	实验名称	实验性质	学时	必做/选做	页码
实验一	网线制作	验证性	2	必做	4-6
实验二	交换机路由器基本配置	验证性	2	必做	7-9
实验三	VLAN 的基本配置	设计性	2	必做	10-12
*实验四	对等网的组建与测试	设计性	2（课下完成）	必做	13-15
实验五	常用网络测试命令	验证性	2	必做	16-18
实验六	静态路由和动态路由	设计性	2	必做	19-21
实验七	网络地址转换	综合性	2	必做	22-24
实验八	TCP/IP 协议分析	验证性	2	必做	25-27
实验九	WWW、FTP 服务器配置	综合性	2	必做	28-30

实验八

<table>
<tr><td rowspan="4">实验基本信息</td><td colspan="2">实验名称：TCP/IP 协议分析</td></tr>
<tr><td>实验时间：　　年　　月　　日</td><td>实验地点：　　实验室</td></tr>
<tr><td colspan="2">实验目的：
（1）了解 TCP/IP 的主要协议和协议层次结构；
（2）分析 ICMP 报文格式和协议内容并了解其应用；
（3）通过分析 ARP 协议的解析过程理解其工作原理。</td></tr>
<tr><td colspan="2">实验要求：
初步了解 TCP/IP 的主要协议和协议的层次结构；通过在位于同一网段和不同网段的主机之间执行 Ping 命令，截获报文，分析 ARP 协议报文结构，并分析 ARP 协议在同一网段内和不同网段间的解析过程;通过分析上述截获报文分析 ICMP 报文。</td></tr>
<tr><td>实验前的预习情况</td><td colspan="2"></td></tr>
</table>

实验过程描述

1、命令行窗口（以管理员身份运行），创建以自己学号后 4 位命名的文件夹，进入该文件夹，看 arp 缓存信息

C:\1101\ arp -a

结果（截图）。

```
C:\Users\durq>cd\

C:\>md 1101

C:\>cd 1101

C:\1101>arp -a

接口: 10.196.199.198 --- 0x13
  Internet 地址         物理地址              类型
  10.196.192.1          2c-9d-1e-b0-dd-38     动态
  10.196.199.1          2c-9d-1e-b0-dd-38     动态
  10.196.199.2          2c-9d-1e-b0-dd-38     动态
  10.196.199.3          2c-9d-1e-b0-dd-38     动态
  10.196.199.4          2c-9d-1e-b0-dd-38     动态
  10.196.199.5          2c-9d-1e-b0-dd-38     动态
  10.196.199.6          2c-9d-1e-b0-dd-38     动态
  10.196.199.7          2c-9d-1e-b0-dd-38     动态
  10.196.199.8          2c-9d-1e-b0-dd-38     动态
  10.196.199.9          2c-9d-1e-b0-dd-38     动态
  10.196.199.10         2c-9d-1e-b0-dd-38     动态
  10.196.199.11         2c-9d-1e-b0-dd-38     动态
  10.196.199.12         2c-9d-1e-b0-dd-38     动态
  10.196.199.13         2c-9d-1e-b0-dd-38     动态
  10.196.199.14         2c-9d-1e-b0-dd-38     动态
```

显示当前主机的 ARP 缓存内容

2、清空 ARP 缓存，再进行查看（截图）

```
C:\1101>arp -d

C:\1101>arp -a

接口: 10.196.199.198 --- 0x13
  Internet 地址         物理地址              类型
  10.196.192.1          2c-9d-1e-b0-dd-38     动态
  224.0.0.22            01-00-5e-00-00-16     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

只显示网关 MAC 地址，及两个组播地址及其 MAC 地址。

3、运行 WireShark，开始截获数据报文；在命令行窗口中执行 ping 命令（ping 邻座同学）。执行完之后，停止报文截获。

Ping 命令截图

```
C:\1101>ping 10.196.208.167

正在 Ping 10.196.208.167 具有 32 字节的数据:
来自 10.196.208.167 的回复: 字节=32 时间=1ms TTL=128
来自 10.196.208.167 的回复: 字节=32 时间<1ms TTL=128
来自 10.196.208.167 的回复: 字节=32 时间<1ms TTL=128
来自 10.196.208.167 的回复: 字节=32 时间<1ms TTL=128

10.196.208.167 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 1ms, 平均 = 0ms
```

4　再次查看 ARP 缓存信息：

结果（截图并解释）。

```
C:\1101>arp -a

接口: 10.196.199.198 --- 0x13
  Internet 地址         物理地址              类型
  10.196.192.1          2c-9d-1e-b0-dd-38     动态
  10.196.208.167        f8-b1-56-d5-5a-ed     动态
  10.196.215.35         f4-39-09-22-e6-e1     动态
  224.0.0.22            01-00-5e-00-00-16     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
```

ping 对方 IP 后，如果对方跟本机在同一个网段内，可以通过 arp -a 显示对方的 MAC 地址；如果对方跟本机不在同一个网段内，arp -a 显示网关的 MAC 地址。

解释：

5、抓取报文分析

Broadcast	ARP	42 Who has 10.196.208.167? Tell 10.196.199.198
HewlettP 22:e6:8b	ARP	60 10.196.208.167 is at f8:b1:56:d5:5a:ed

（1）与所 ping 地址相关的有__2__个 ARP 报文。

（2）在所有报文中，ARP 报文中 ARP 协议树的 Opcode 字段有两个取值 1、2，两个取值分别表达什么信息？

```
156 17.416669    HewlettP_22:e6:8b    Broadcast            ARP         42 Who has 10.196.208.167? Tell 10.196.199.198
157 17.417204    Dell_d5:5a:ed        HewlettP_22:e6:8b    ARP         60 10.196.208.167 is at f8:b1:56:d5:5a:ed

Frame 156: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: HewlettP_22:e6:8b (f4:39:09:22:e6:8b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: HewlettP_22:e6:8b (f4:39:09:22:e6:8b)
  Sender IP address: 10.196.199.198
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 10.196.208.167
```

```
157 17.417204    Dell_d5:5a:ed      HewlettP_22:e6:8b    ARP      60 10.196.208.167 is at f8:b1:56:d5:5a:ed
> Frame 157: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Dell_d5:5a:ed (f8:b1:56:d5:5a:ed), Dst: HewlettP_22:e6:8b (f4:39:09:22:e6:8b)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Dell_d5:5a:ed (f8:b1:56:d5:5a:ed)
    Sender IP address: 10.196.208.167
    Target MAC address: HewlettP_22:e6:8b (f4:39:09:22:e6:8b)
    Target IP address: 10.196.199.198
```

解释：1 表示……，2 表示……

（3）选中第一条 ARP 请求报文和第一条 ARP 应答报文，将 ARP 请求报文和 ARP 应答报文中的字段信息填入表 8-1。

表 8-1 ARP 请求报文和 ARP 应答报文的字段信息

字段项	ARP 请求数据报文	ARP 应答数据报文
链路层 Destination 项	Ff:ff:ff:ff:ff:ff	F4:39:……
链路层 Source 项	F4:39:……	F4:39:09:……
网络层 Sender MAC Address		
网络层 Sender IP Address		
网络层 Target MAC Address		
网络层 Target IP Address		

6、分析如果 PCA、PCB 在同一网段，表 8-1 中 ARP 请求报文的 Target MAC Address 是什么？如果不在同一网段，Target Mac Address 应是什么？

答：*****

7、分析截获的 ARP 请求报文，其封装在 MAC 中时，Destination 地址是多少？帧中类型字段的值是多少？

答：*****

8、分析截获的 ICMP 报文。

```
icmp && ip.dst==10.196.208.167 || ip.src==10.196.208.167
```

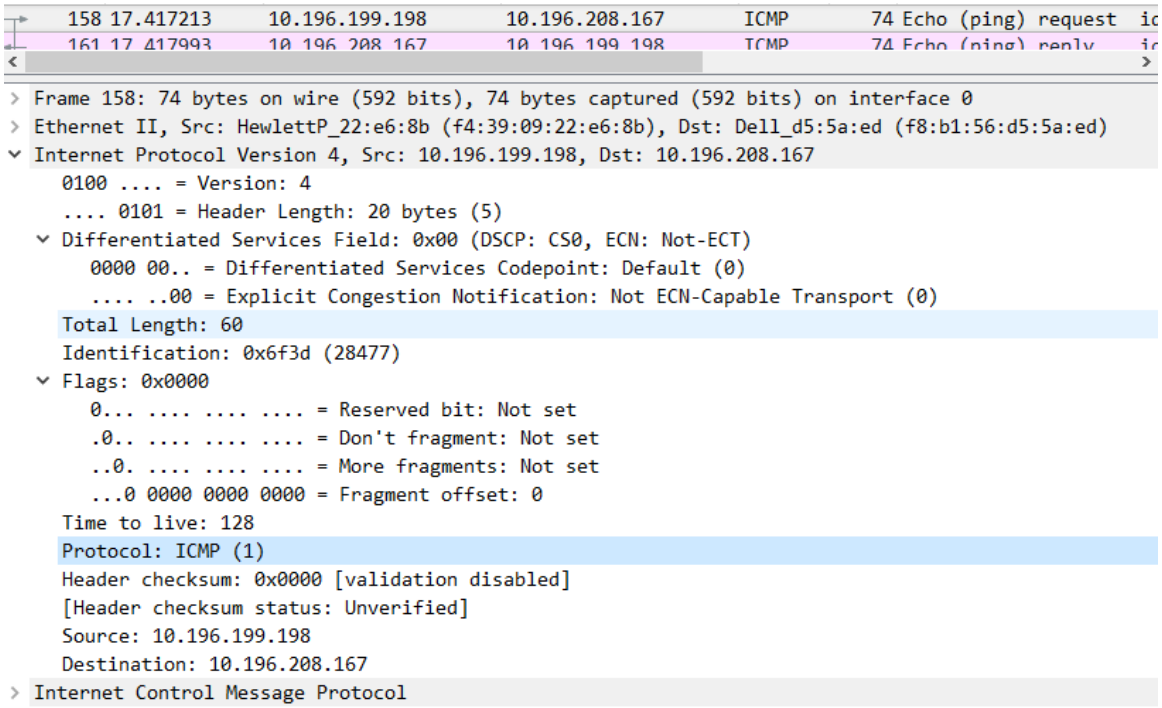
No.	Time	Source	Destination	Protocol	Length	Info
158	17.417213	10.196.199.198	10.196.208.167	ICMP	74	Echo (ping)
161	17.417993	10.196.208.167	10.196.199.198	ICMP	74	Echo (ping)
184	18.418776	10.196.199.198	10.196.208.167	ICMP	74	Echo (ping)
185	18.419397	10.196.208.167	10.196.199.198	ICMP	74	Echo (ping)
194	19.422038	10.196.199.198	10.196.208.167	ICMP	74	Echo (ping)
195	19.422742	10.196.208.167	10.196.199.198	ICMP	74	Echo (ping)
200	20.425105	10.196.199.198	10.196.208.167	ICMP	74	Echo (ping)
201	20.425848	10.196.208.167	10.196.199.198	ICMP	74	Echo (ping)

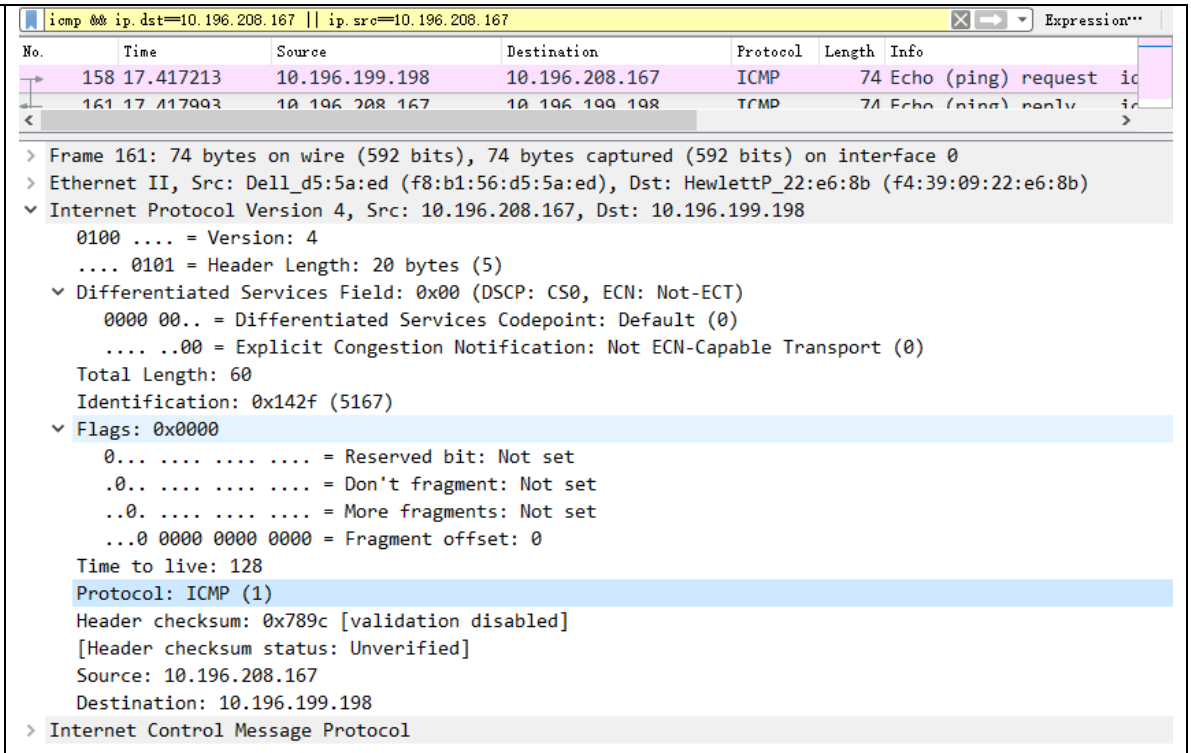
共有 8 个 ICMP 报文，分别属于哪些种类？对应的种类和代码字段分别是什么？

答：****

9、分析第 1 个 ICMP 报文的 IP 协议部分，填写下面表格。

询问请求报文		询问应答报文	
IP 字段名	字段值	IP 字段名	字段值
首部长度			
总长度			
标识			
NF			
MF			
片偏移			
协议			
SRC			
DST			





10、分析第 1 个 ICMP 报文的帧首部与尾部信息，填写下面表格

此报文文类型		
此报文的基本信息（数据报文列表窗口中的 I 项的内容）		
Ethernet Ⅱ协议树中	Source 字段值	
	Destination 字段值	
	类型字段值	
	FCS 字段值	
Internet Protocol 协议树中	Source 字段值	
	Destination 字段值	

11、重复步骤 3（截图）。

12、比较步骤 11 结果与步骤 3 结果，步骤 11 中截获的报文信息，少了什么报文？简述 ARP Cache 的作用。

答：

13、分析步骤 8 截获的 MAC 帧，与发送方发送的数据帧相比较，看少了哪些字段？为什么？

回答问题	1、 在网络课程学习中， ETHERNETII 规定了以太网 MAC 层的报文格式分为 7 字节的前导符，1 字节的起始符，6 字节的目的 MAC 地址，6 字节的源 MAC 地址，2 字节的类型、数据字段和 4 字节的数据校验字段。对于选中的报文，缺少哪些字段，为什么? 2、ARP 协议工作在哪一层?作用是什么?
实验成绩	教师签名：