《计算机网络》实验一

1）题目“ IEEE 802.3 以太网帧封装”

题目内容：编写程序实现 IEEE 802.3 以太网帧封装。

2）要求：

1. 要求画出界面，以太网帧的数据部分、~~源 MAC 地址和目的 MAC 地址~~均从界面输入；
2. 计算后的校验和字段和封装后的结果可以从界面上输出；
3. ~~生成多项式 G（X）=$X^8+X^2+X^1+1$；~~

（或者生成多项式 G(X)=$X^{32}+X^{26}+X^{23}+X^{22}+X^{16}+X^{12}+X^{11}+X^{10}+X^8+X^7+X^5+X^4+X^2+X^1+1$;）

4. 使用的操作系统、语言和编译环境不限，但必须在实验报告中注明

按 802.3 标准的帧结构如下表所示（802.3 标准的 Ethernet 帧结构由 7 部分组成）

表 1 802.3 标准的帧结构

前导码	帧前定界符	目的地址	源地址	长度字段	数据字段	校验字段
7B	1B	(6B)	(6B)	(2B)	(长度可变)	(4B)

实验二 ARP 地址解析协议分析实验

【实验目的】

1、掌握 ARP 协议的作用和格式。
2、理解 IP 地址与 MAC 地址的对应关系。
3、掌握 ARP 命令。

【实验学时】

2 学时

【实验环境】

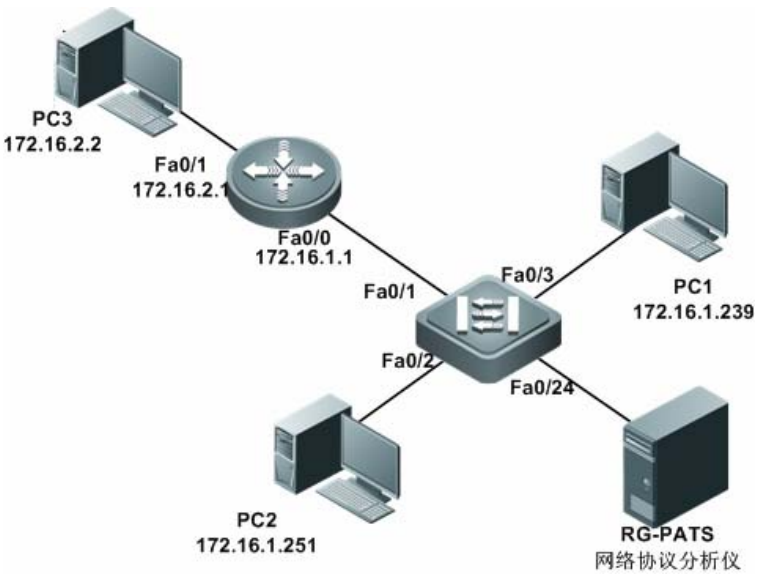

图 3-12 实验拓扑图

【实验内容】

1、学习 ARP 协议的工作原理。
2、掌握 ARP 协议的作用和使用方法。
3、理解 IP 地址与 MAC 地址的对应关系。
4、学习使用 ARP 命令。

【实验流程】

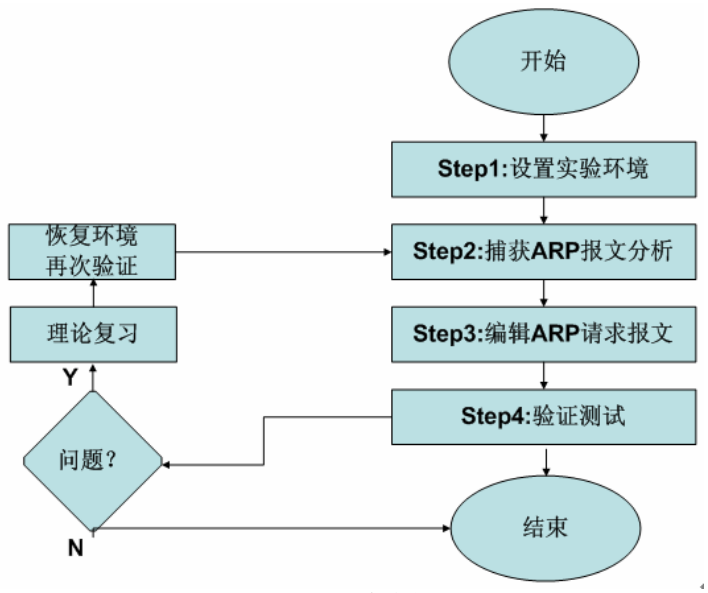

图 3-13 实验流程图

【实验原理】

以太网中的两个节点进行通信时，很容易获知本机和目标主机的 IP 地址，而通常不知道目标主机的 MAC 地址，但是在以太网中进行通信时，在数据链路层对数据进行封装和解封装的过程中都需要利用到 MAC 地址。ARP 协议的功能就在于获取到 IP 地址所对应的 MAC 地址。

1、ARP 报文格式

当某台主机需要获知某 IP 地址对应的 MAC 地址时，主机封装 ARP 请求报文并将目的地址配置为广播地址发送出去，这样，处于同一网段中的所有主机都能够收到此 ARP 请求报文，主机收到 ARP 请求报文后，如果发现请求的 IP 地址与自己相符，则针对发送者单播发送 ARP 应答报文，其中包含自己的 MAC 地址。如果主机收到 ARP 请求报文后，发现请求的 IP 地址与自己不相符，则将请求包丢弃，不做处理。

下图为 ARP 请求或应答报文格式。

图 3-14 ARP 协议的分组格式

字段说明：

- 硬件类型：表示硬件类型，例如：1 表示以太网；
- 协议类型：表示要映射的协议类型，例如 0x0800 表示 IP 地址；
- 硬件长度：指明硬件地址长度，单位是字节，MAC 是 48 位，6 个字节；
- 协议长度：高层协议地址的长度，对于 IP 地址，长度是 4 个字节；
- 操作码：共有二种操作类型，1 表示 ARP 请求，2 表示 ARP 应答；
- 发送方 MAC：6 个字节的发送方 MAC 地址；
- 发送方 IP：4 个字节的发送方 IP 地址；
- 目标 MAC：6 个字节的目的物理地址，当数据包为 ARP 请求时，目的 MAC 地址项留空，为全 0，当数据包为 ARP 应答包时，目的 MAC 地址为目标 IP 地址对应的 MAC 地址；
- 目的 IP：4 个字节的目的 IP 地址，当数据包为 ARP 请求包时，目的 IP 地址为待解析的 IP 地址。

2、ARP 工作过程

当处于同一网段中的计算机 A 要和计算机 B 进行通信时，首先计算机 A 要得到计算机 B 的 IP 地址和 MAC 地址的映射关系，工作过程如下：

- 计算机 A 检查自己的高速缓存中的 ARP 表，判断 ARP 表中是否存有计算机 B 的 IP 地址与 MAC 地址的映射关系。如果找到，则完成 ARP 地址解析；如果没有找到，则转至 2）。
- 计算机 A 广播含有自身 IP 地址与 MAC 地址映射关系的 ARP 请求包，请求解析计算机 B 的 IP 地址对应的 MAC 地址。
- 包括计算机 B 在内的网络中所有计算机接收到计算机 A 的 ARP 请求信息。
- 计算机 B 向计算机 A 发送单播 ARP 应答报文，通告自己的 IP 地址与 MAC 地址的对应关系，并保存计算机 A 的 IP 和 MAC 的对应关系。
- 计算机 A 收到计算机 B 的 ARP 应答信息后，将计算机 B 的 IP 地址与 MAC 地址

的映射关系存入自己的 ARP 缓存表中，从而完成对计算机 B 的 ARP 地址解析。

当处于不同网段的计算机 A 要和计算机 B 进行通信时，由于数据会先交给计算机 A 所在网络的网关，因此计算机 A 此时需要对网关的 IP 地址做 ARP 请求。

3、ARP 缓存和 ARP 命令

为减少广播通信量和提高 ARP 解析速度，每台主机都有 ARP 高速缓存，用于存放解析过的 MAC 和 IP 的映射关系。ARP 缓存表是可以通过命令查询的。在命令提示符下，输入“arp -a”可以查看 ARP 缓存表中的内容，输入“arp-d”可清除 ARP 缓存。

【实验步骤】

步骤一：设定实验环境

1、参照实验拓扑连接网络拓扑；

2、配置 PC 机及路由器 IP 地址；

```
RA(config)#interface FastEthernet 0/0
RA(config-if)#ip address 172.16.1.1 255.255.255.0
RA(config)#interface FastEthernet 0/1
RA(config-if)#ip address 172.16.2.1 255.255.255.0
```

3、在交换上配置端口镜像

```
S3750#
S3750#configure terminal
S3750(config)#monitor session 1 destination interface FastEthernet 0/24
S3750(config)#monitor session 1 source interface FastEthernet 0/1 – 10 both
```

步骤二：捕获 ARP 报文并进行分析

1、在主机 PC1 中用命令 arp –a 可以查看 ARP 缓存表中的 ARP 记录，用 arp –d 命令删除 ARP 缓存中的记录，如下图所示。

```
G:\Documents and Settings\Administrator>arp -a

Interface: 172.16.1.239 --- 0x2
  Internet Address      Physical Address      Type
  172.16.1.1            00-d0-f8-b5-14-8d     dynamic
  172.16.1.137          00-11-85-c7-71-fb     dynamic

G:\Documents and Settings\Administrator>arp -d
```

图 3-15 查看 ARP 缓存表

2、在 PC1 中开启协议分析仪进行数据包捕获。

3、在 PC1 中用命令 ping172.16.1.253。

4、捕获 ARP 报文进行分析。

捕获的 ARP 请求报文如下图所示

图 3-16 ARP 请求报文

捕获的 ARP 应答报文如下图所示。

图 3-17 ARP 应答报文

在 ARP 请求报文的数据帧头中，源物理地址为发送请求的主机地址为：00-1b-fc-a6-ae-e2，目的物理地址是广播地址：ff-ff-ff-ff-ff-ff，协议类型为 0806，表示上层协议为 IP 协议。

- 在 ARP 请求报文中，各字段含义与值如下：
- 硬件类型：0001，表示硬件类型为以太网。
- 协议类型：0800，表示需映射地址为 IP 地址。
- 硬件长度：6，表示硬件地址长度为 6 字节。
- 协议长度：4，表示协议地址长度为 4 字节。
- 操作码：1，表示此 ARP 报文为 ARP 请求报文。
- 源物理地址：00-1b-fc-a6-ae-e2，为发送 ARP 请求主机的物理地址。
- 源 IP 地址：172.16.1.239，为发送 ARP 请求主机的 IP 地址。
- 目标物理地址：00-00-00-00-00-00，为待解析的物理地址。
- 目标 IP 地址：172.16.1.253，为待解析的 IP 地址。

在 ARP 应答报文中的数据帧头中，源物理地址为发送 ARP 应答报文的物理地址：00-1e-8c-a6-d6-4a，目的物理地址为发送 ARP 请求报文的主机的物理地址：00-1b-fc-a6-ae-e2，协议类型为 0806，表示上层协议为 IP 协议。

在 ARP 应答报文中，各字段含义与值如下：

- 硬件类型：0001，表示硬件类型为以太网。
- 协议类型：0800，表示需映射地址为 IP 地址。

- 硬件长度：6，表示硬件地址长度为 6 字节。
- 协议长度：4，表示协议地址长度为 4 字节。
- 操作码：2，表示此 ARP 报文为 ARP 应答报文。
- 源物理地址：00-1e-8c-a6-d6-4a，为发送 ARP 应答报文主机的物理地址。
- 源 IP 地址：172.16.1.253，为发送 ARP 应答报文主机的 IP 地址。
- 目标物理地址：00-1b-fc-a6-ae-e2，为发送 ARP 请求的主机的物理地址。
- 目标 IP 地址：172.16.1.239，为发送 ARP 请求的主机的 IP 地址。

在 PC1 中用命令 arp –d 删去 ARP 缓存中的 ARP 记录。

在 PC1 上开启协议分析仪捕获 ARP 包进行分析。

在 PC1 上 ping PC3 地址 172.16.2.2。

对捕获的数据包进行分析。

从捕获到的数据可以看到，网关 172.16.1.1 返回 ARP 应答信息。可见当一台主机要和非本网段的主机进行通信时，需要对网关进行 ARP 解析。并且在向目标主机发送报文时，目标物理地址填入的是本网段网关的物理地址。

步骤三：编辑发送 ARP 报文请求报文（同网段）

1、在命令提示符下运行：arp –d，清空 ARP 高速缓存。

2、编辑并发送 ARP 报文，如下图所示。

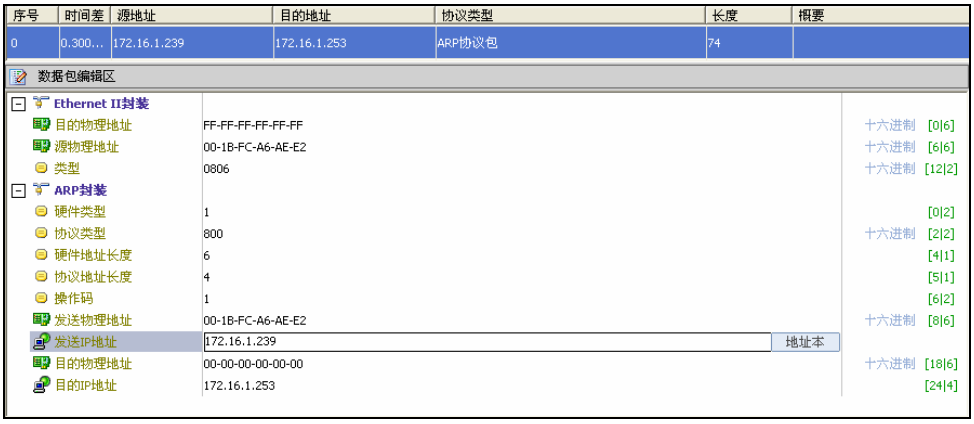

图 3-18 编辑 ARP 报文

- 目的物理地址：FF-FF-FF-FF-FF-FF，ARP 请求为广播报文，目的地址为广播地址；
- 源物理地址：00-1B-FC-A6-AE-E2，发送端物理地址；
- 类型：0806，上层协议是 IP；
- 硬件类型：1，以太网；
- 协议类型：800；
- 硬件类型：0001，表示硬件类型为以太网；
- 协议类型：0800，表示需映射地址为 IP 地址；

- 硬件长度：6，表示硬件地址长度为 6 字节；
- 协议长度：4，表示协议地址长度为 4 字节；
- 操作码：2，表示此 ARP 报文为 ARP 应答报文；
- 源物理地址：00-1e-8c-a6-d6-4a，为发送 ARP 应答报文主机的物理地址；
- 源 IP 地址：172.16.1.253，为发送 ARP 应答报文主机的 IP 地址；
- 目标物理地址：00-1b-fc-a6-ae-e2，为发送 ARP 请求的主机的物理地址；
- 目标 IP 地址：172.16.1.239，为发送 ARP 请求的主机的 IP 地址。

3、在 PC1 上开启协议分析软件，进行数据包捕获分析，捕获报文如下图所示。

图 3-19 采集 ARP 报文

从上图中可以看到，当编辑 ARP 请求报文发送给目的端后，目的端会发送操作码为 2 的 ARP 应答报文，通告自己的 MAC 地址和 IP 地址对应关系。

4、在 PC1 中用命令 arp –a 可以查看到 ARP 缓存中的 PC2 的 ARP 记录，如下图所示。

```
G:\Documents and Settings\Administrator>arp -a

Interface: 172.16.1.239 --- 0x2
  Internet Address      Physical Address      Type
  172.16.1.1            00-d0-f8-b5-14-8d     dynamic
  172.16.1.253          00-1e-8c-a6-d6-4a     dynamic
```

图 3-20 查看 ARP 缓存

步骤四：编辑发送 ARP 报文请求报文（不同网段）

1、在命令提示符下运行：arp –d，清空 ARP 高速缓存。

2、在 PC1 上编辑并发送 ARP 请求，目标地址为 PC3 主机的地址，如下图所示。

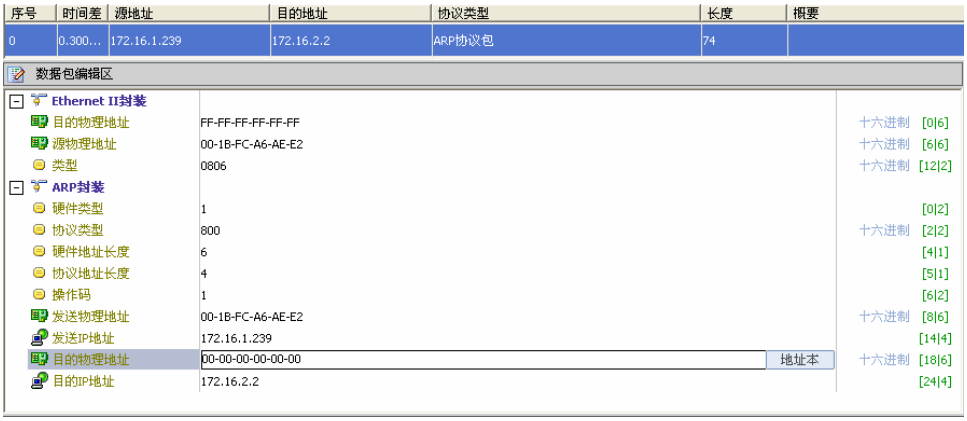

图 3-21 编辑 ARP 报文

在上图中，ARP 请求的目的 IP 地址为不同网段的 PC3 的 IP172.16.2.2。

3、在 PC1 上开启协议分析软件，进行数据包捕获分析，如下图所示。

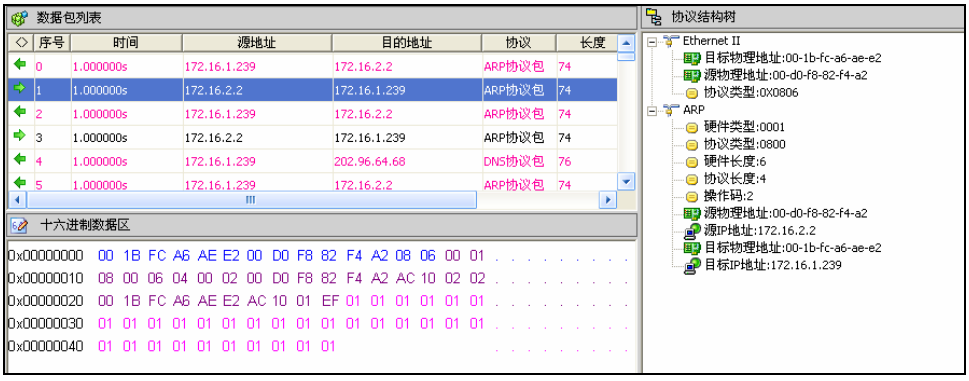

图 3-22 采集 ARP 报文

从上图中可以看到，当主机请求非本网段的 IP 地址对应的 MAC 地址时，应答报文中的源物理地址为 00-d0-f8-82-f4-a2，说明网关代替 PC3 对主机发送了 ARP 应答报文。这是因为，ARP 请求报文为广播发送，无法扩散到其他网段，网关代替目标主机进行了 ARP 应答。当主机需要发送数据到其他网段时，需要在目的 MAC 地址的字段中填入网关 MAC 地址，先将数据发送给网关，再由网关发送到其他网段。

【思考问题】

结合实验过程中的实验结果，问答下列问题：

1、观察实验过程中捕获网络上的多个 ARP 请求帧，观察这些帧的以太网目的地址是否相同，分析其原因。

2、观察实验过程中捕获网络上的多个 ARP 应答帧，观察这些帧的以太网目的地址是否相同，分析其原因。

3、ARP 缓存的作用？

实验三　以太网链路层帧格式分析

2.1 实验目的

分析 Ethernet V2 标准规定的 MAC 层帧结构，了解 TCP/IP 的主要协议和协议的层次结构。

2.2 实验内容

通过对截获帧进行分析，分析和验证 Ethernet V2 标准的 MAC 层帧结构。

2.3 实验环境

本实验使用了交换机 1 台，PC 机两台，拓扑如下图所示。（实验报告中拓扑图手画）

PC1 172.16.1.239　　PC2 172.16.1.251

255.255.255.0　　255.255.255.0

图 2.1 以太网链路层帧格式分析实验组网图

2.4 实验步骤

步骤 1 按图 2.1 所示连接好设备，正确配置 PC1 和 PC2 的 IP 地址。

步骤 2 在 PC1 上 Windows 命令行窗口，执行命令：ping 172. 16. 1. 251。在 PC2 上运行 Ethereal 截获报文。也可以在 PC2 上进行 ping 命令，PC1 进行截获操作。（截图）

步骤 3 对截获的报文进行分析：

1、列出截获的报文的协议种类。

2、找到发送消息的报文并进行分析，研究主窗口中的数据报文列表窗口和协议树窗口信息，填写表 2.1。

表 2.1 报文分析

Ethernet Ⅱ 协议树中	Source 字段值	
	Destination 字段值	

IP 协议树中	Source 字段值	
	Destination 字段值	
ICMP 协议树中	类型值	
	代码值	

3、在网络课程学习中，802.3 和 Ethernet Ⅱ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？（报告中不写问题，写答案）

2.5 实验总结（不少于 50 字）

实验四　IP 分组分片实验

4.1 实验目的

1、理解 IP 分片过程；
2、掌握 IP 分片是数据报头的变化。

4.2 实验环境

本次实验使用了 1 台交换机（或 1 台路由器），2 台 PC 机，其实验拓扑如下图所示。（拓扑图手画）

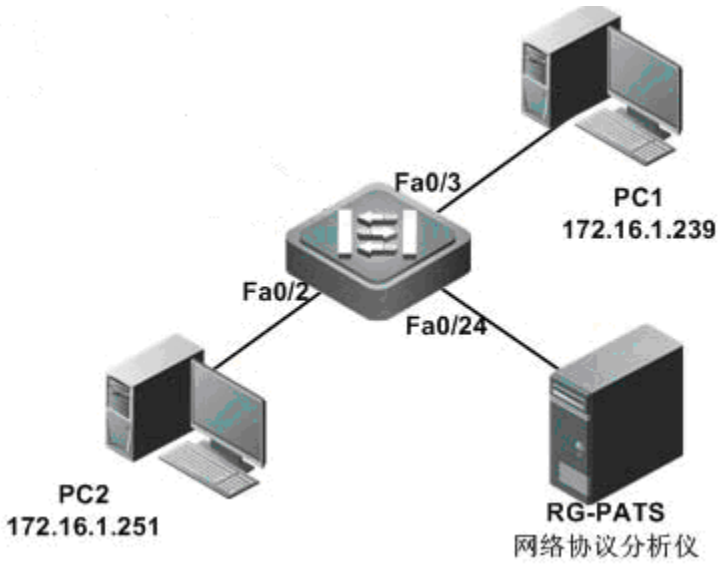

图 5.1 IP 分组分片实验拓扑图

4.3 实验内容

1、掌握 IP 数据包分片过程。
2、掌握 IP 分片报头格式。

4.4 实验步骤

步骤一：设定实验环境

1、配置主机 IP 地址。
2、按照实验拓扑连接网络拓扑。

步骤二：发送大包进行捕获分析

1、在 PC1 上用命令 ping 172.16.1.251 –l 2000 发送 2000 字节的大包到 PC2。

2、在 PC2 上开启协议分析软件，捕获数据包并进行分析，如下图所示。（实验报告中请截图）

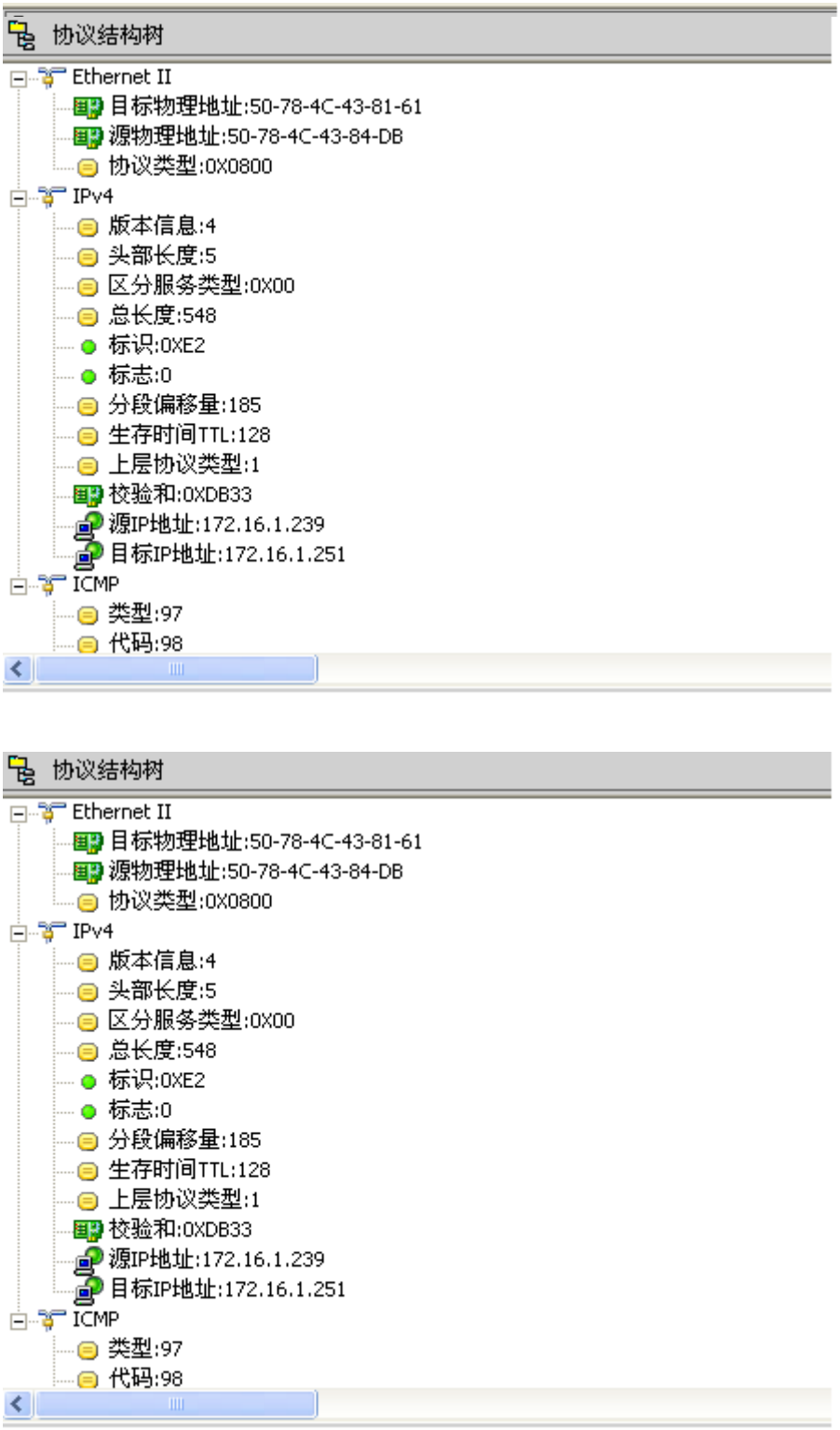

图 5.2 IP 分组第二个分片

从上图是从 PC2 上连续捕获到的两个报文。从报文可以可以看到其中以太网帧头部分均为相同源目的 MAC 地址，其他 IP 报头字段，除和分片有关的标识、标志、分段偏移以及校验和外，其他字段都相同。从协议分析仪中可以看到，捕获报文中：

标识字段：0xE2，标识字段用于和 IP 地址一起唯一标识一个 IP 包，因此，属于同一个 IP 包的分片具有相同的标识字段。

标志：长度为 3 位，第一位保留为以后用，第二位为 1 时，表示此数据包不可分片，第二位为 0 时表示此数据包可以分片。第三位标志此分片是否为最后一个分片，为 1 时表示这个数据包不是最后的分片，如为 0 表示此数据包为最后的分片。所以在第一个分片中，此位为 1，在第二个分片即最后一个分片中，此位为 0。

分段偏移：长度为 13 位，表示这个分片在原数据包中的相对位置，在第一个数据片中的此字段为 0，在第二个数据包中，此分片为 B9，转化为 10 进制数字为 185，表示的偏移位置是 185*8=1480，表示第二个分片偏移量 1480 字节，即第一个分片长度为 1480 字节。在数据目的端，可以根据这三个字段对数据包进行重组。（以上的 4 小段都不用抄）

4.5 实验总结

本实验分析了 IP 分组分片以及对 IP 分组首部进行更改的过程。结合实验过程中的结果，请同学们在实验报告中回答如下问题：

1、在什么情况下会出现数据包分片？

2、数据包进行分片时，第一个数据包的大小是多少，和链路类型是什么关系？（报告中不写问题，直接写答案）