3.2 IP 地址分类与 IP 数据包的组成（IPv4）

实验三 基本报文分析

【实验目的】

1、理解 IP 层的作用以及 IP 地址的分类方法；
2、理解子网的划分和子网掩码的作用；
3、掌握 IP 数据包的组成和网络层的基本功能；

【实验学时】

4 学时

【实验环境】

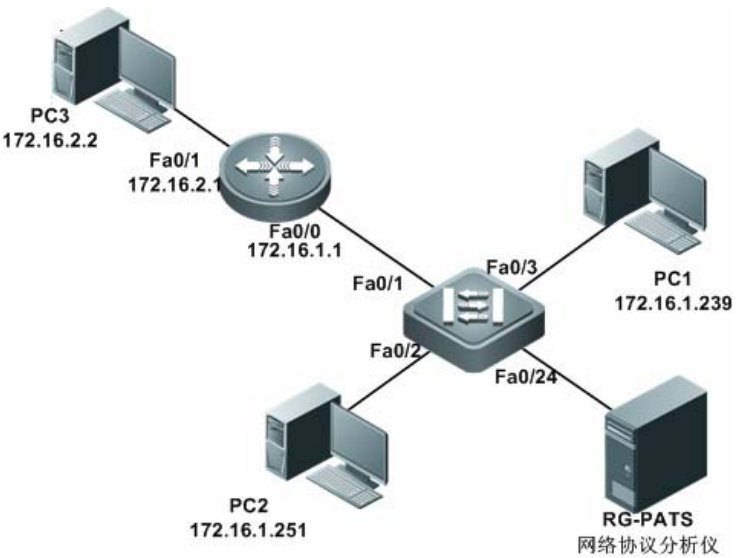

图 3-2 实验拓扑图

【实验内容】

1、学会根据 IP 地址的分类方式区分各类 IP 地址；
2、掌握 IP 数据报的格式、长度以及各字段的功能；
3、学会利用子网掩码确定 IP 地址的网络号、子网号和主机号；
4、学会分析给定数据包的 IP 首部信息；
5、学会手工计算 IP 校验和的方法；

【实验流程】

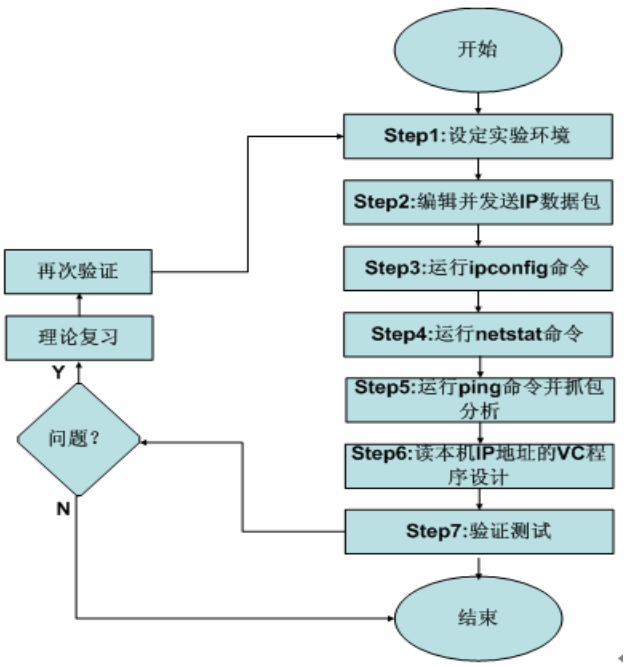

图 3-3 实验流程图

【实验原理】

网际协议 IP 是 TCP/IP 协议栈的心脏，也是网络层中最重要的协议。目前几乎所有的上层网络协议都是基于 IP 协议。在接收数据的时候，网络层接收由数据链路层发送的数据包进行解封装，并把该数据包发送到更高层——传输层，在发送数据的时候，网络层接受由传输层发送的数据包进行 IP 封装，然后把数据报交给下层——数据链路层。

IP 协议处于 TCP/IP 协议栈的网际层，用于管理数据通信中源端和目的端之间的报文传送，是互联网最重要的网际协议。IP 地址是也叫逻辑地址，用于在网络中标识主机。在 IP 网络中，主机之间进行通信时使用 IP 地址来指定接收端的主机地址。

数据进行封装过程中，IP 层负责将数据封装成 IP 包，IPv4 数据包报文格式如下图所示。

图 3-4 IP 报文格式

如上图所示，在 IP 包中，各字段含义如下所述：

- 版本：长度为 4 比特，含义为版本号，对于 IPv4 来说，版本号为 4。
- 报头长度：报头长度字段为 4 比特，用于表示 IP 报头长度，在 IPv4 中，由于选项字段长度可变，因此，报头长度并不固定，报头字节长度为这一字段值的 4 倍。
- 业务类型：业务类型字段长度为 8 比特，主要用于标识 QOS 服务等级。
- 总长度：总长度字段共 16 比特，因此 IP 报的最大长度为 65535 字节。
- 标识符（Identifier）：长度 16 比特。该字段和标识及分段偏移字段联合使用，对大的上层数据包进行分段（fragment）操作。
- 标记（Flags）：长度 3 比特。该字段第一位不使用，第二位是 DF 位，DF 位设为 1 时表明路由器不能对该上层数据包分段。如果一个上层数据包无法在不分段的情况下进行转发，则路由器会丢弃该上层数据包并返回一个错误信息。第三位是 MF 位，当路由器对一个上层数据包分段，则路由器会在除了最后一个分段的 IP 包的包头中将 MF 位设为 1。
- 分段偏移（Fragment Offset）：长度 13 比特。用于指明分片 IP 包在原 IP 包中的偏移量。由于 IP 包在网络上传送的时候不一定能按顺序到达，这个字段保证了目标路由器在接受到 IP 包之后能够还原分段的上层数据包。当某个包含分段的上层数据包的 IP 包在传送时丢失，则整个一系列包含分段的上层数据包的 IP 包都会被要求重传。
- 生存时间（TTL）：长度 8 比特。当 IP 包进行传送时，先会对该字段赋予某个特定的值。当 IP 包经过每一个路由器的时候，路由器会将 IP 包的 TTL 值减少 1。如果 TTL 减少为 0，则该 IP 包会被丢弃。这个字段可以防止由于路由故障而导致 IP 包在网络中不停被转发。
- 协议号（Protocol）：长度 8 比特。标识了上层所使用的协议。
- 报头校验和（Header Checksum）：长度 16 位，由于 IP 包头是变长的，所以提供一个头部校验来保证 IP 包头中信息的正确性。
- 源和目标地址（Source and Destination Addresses）：这两个地段都是 32 比特。标识了这个 IP 包的起源和目标地址。
- 可选项（Options）：这是一个可变长的字段。该字段由起源设备根据需要改写。

【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：利用网络协议分析软件捕获并分析 IP 数据包

1、在某台主机中打开网络协议分析软件，在工具栏中点击“开始”，待一段时间后，点击“结束”，

2、在捕获到数据包中，选择 IP 数据包进行分析，如下图所示。

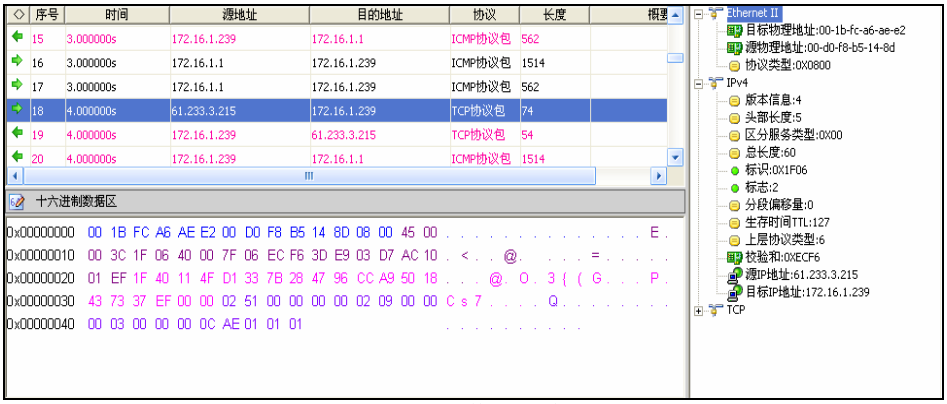

图 3-5 IP 数据包分析

分析捕获到的 IP 数据包，因此在本实验中，只分析数据的的 IP 包头部分。

- 版本信息：4，标识此报文为 IPv4 报文。
- 头部长度：5，标识 IP 报头长度为 5 个 32 比特。在上图中，IP 报头最末端为 01 FF，整个 IP 包头长度为 20 字节，共 160 位，即 32 比特的 5 倍。
- 区分服务类型：0，在此报文中不涉及服务质量的区分。
- 总长度：60，表示总长度为 60 字节。
- 标识：0X1F06，此数据包没有进行分片。
- 标志：2，二进制为 010，表示此数据包不可分片。
- 分段偏移量：0X0000，此数据包没有进行分片。
- 生存时间：127，每经过一个路由器，生存时间减 1，当生存时间减小为 0 时，数据包被丢弃而不被转发。
- 源 IP 地址：此字段显示了数据包的源地址。
- 目的 IP 地址：此字段显示了数据包的目的地址。
- 其他：此包头中，没有选项字段，没有填充字段。IP 报头之后的部分为 IP 包中的数据部分。

步骤三：利用网络协议编辑软件编辑并发送 IP 数据包

1、在主机 PC1 打开网络协议编辑软件，在工具栏选择“添加”，建立一个 IP 数据包。

2、填写“源物理地址”：可以在地址本中找到本机的 MAC 地址，然后左键选择，点击“确定”加入地址。

3、填写“目的物理地址”：可以在地址本中选择 PC2 的 MAC 地址，然后左键选择并单击“确定”加入地址。

4、填写“类型或长度”：该字段值为 0800。

配置完成后，在数据包编辑区中会出现 IP 层各个字段及其默认值，如下图所示。

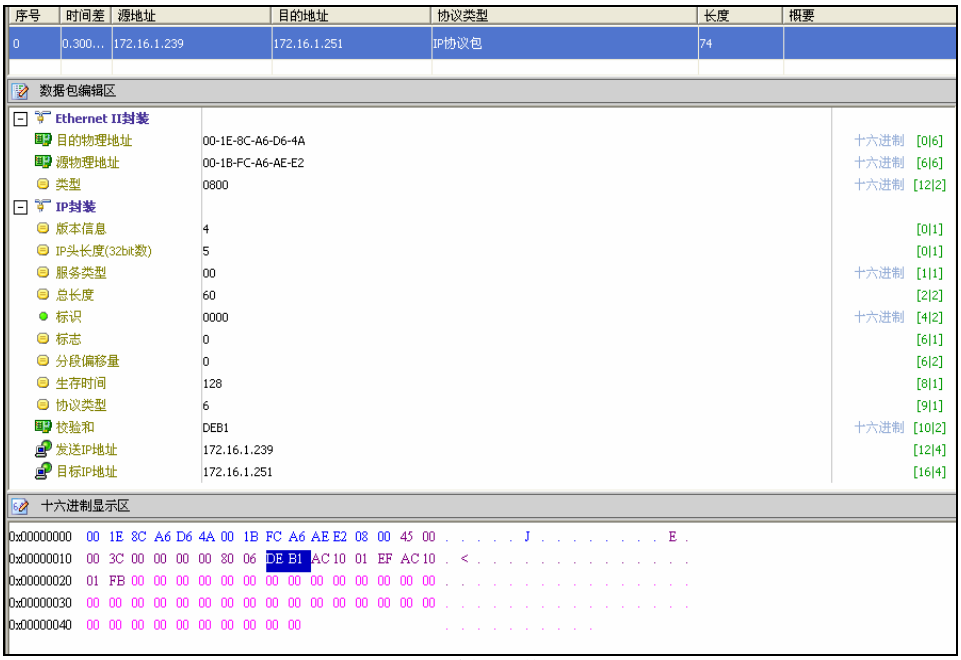

图 3-6 编辑 IP 数据包

填写 IP 协议头信息：

- 版本号和首部长度：版本号为 4，首部长度 5(即 20 个字节)。
- IP 头长度填入 5，如果没有选项，IPv4 包头长度为 20 字节，为 5 个 32 比特长度。
- 服务类型(TOS)：00。
- 总长度：该值为 IP 首部长度加上数据部分的长度：如果没有数据该字段应为 20，否则加上数据的长度，此处可以选用默认值。
- 标识字段：可以采用默认值，或任意值，例如 0。
- 标志字段：可以采用默认值。
- 生存时间：可以采用默认值 128。
- 协议类型：即 IP 携带的上层协议类型(例如：TCP 为 6，UDP 为 17，ICMP 为 1)：本实验填 6，协议分析软件会自动将上层协议设为 TCP。
- 首部校验和：先添 0，等全部字段填完后再计算。
- 源 IP 地址：注意，网络协议编辑软件可以编辑本机发送 IP 数据包，也可以编辑另一台机器发送 IP 数据包，所以，源 IP 地址字段可以填写本机 IP 地址，也可以填

写其它机器的 IP 地址(注意协议分析器的过滤器设置)；

- 目的 IP 地址：从地址本中选择 PC2 的主机的 IP 地址，左键选定，点击确定后"添加"；注意源目的 IP 地址的配置要与源目的 MAC 地址相符。

当上述各字段值均已填写完毕后，可以计算"校验和"，校验和的计算有两种方法

- 方法一：手工计算，首先把校验和字段置为 0，然后对 IP 协议头中的每个 16 比特进行反码求和(整个首部看成是由若干个 16 比特的字组成)，然后取反，结果即校验和的值。
- 方法二：利用网络协议编辑软件提供的工具计算，左键点击工具栏的"校验和"即可。

如果要编辑多个 IP 数据包，可重复上述步骤。

点击工具栏或菜单栏中的"发送"，在弹出的对话框中配置发送次数，然后选择"开始"按钮，发送帧序列，如下图所示。

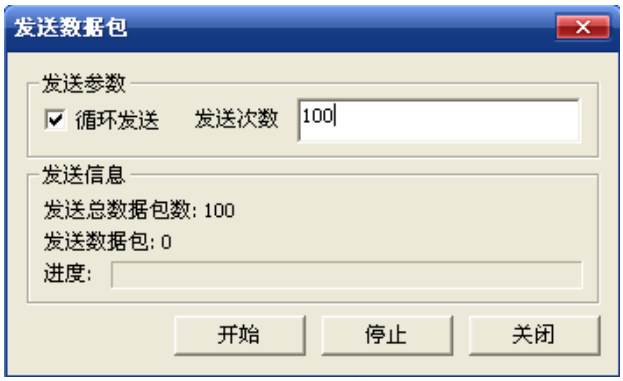

图 3-7 发送 IP 数据包

在 PC2 中用协议分析器截获数据包并分析，捕获到的报文如下图所示。

图 3-6 捕获到的 IP 报文

分析捕获到的数据包的 IPv4 报头部分

- 版本信息：IPv4 报文的版本信息为 4。
- 头部长度：IPv4 报头不含选项和填充字段长度为 20 字节，是 32 比特的 5 倍。

- 总长度：总长度包含 IP 报头长度和 IP 包中的数据长度，协议分析软件将 IP 发送时自动将上层协议选择为 TCP，因此数据内容为 TCP 报头共 20 字节以及 20 字节数据，因此接收到的 IP 报文长度为 60 字节。
- 标识、标识、分段偏移量：均与分片有关。
- 生存时间：由于数据包从源端到目的端没有经过任何路由器的转发，TTL 值不变为 128。
- 校验和：由于发包过程中，标识位和分段偏移修改，因此校验和也和发送的数据稍有不同。
- 源目标地址：源目标地址在 IP 包的发送过程中不做修改。

用同样的方法，在 PC1 中编辑 IP 包，将目的 MAC 地址和目的 IP 地址修改为 PC3 的地址，发送数据包。注意，封装 IP 包发往不同网段的目的主机时，目标 MAC 地址选择网关的 MAC 地址，地址本中找不到不同网段的 IP 地址时，手工输入目的 IP 地址。编辑的数据包如下图所示。

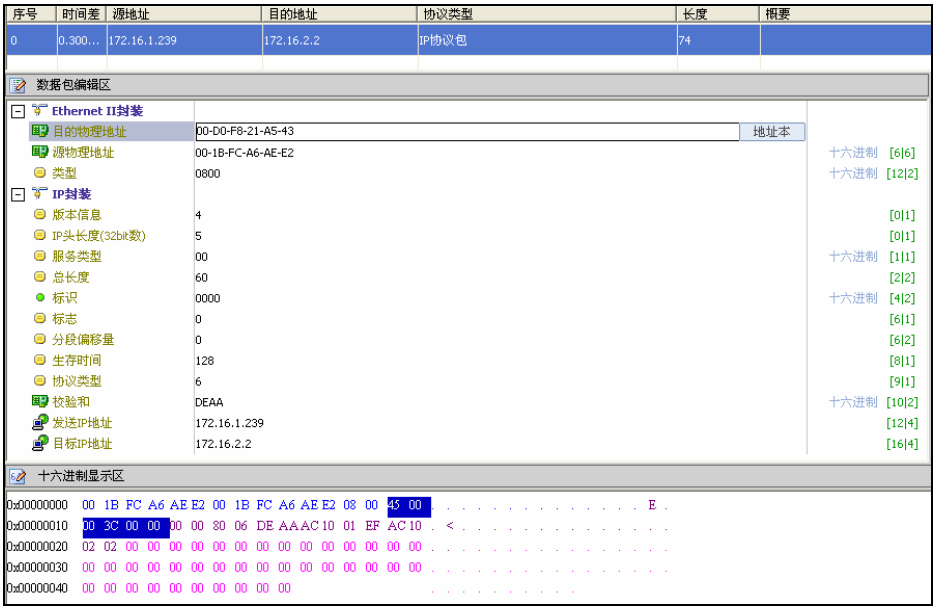

图 3-7 发往不同网段的 IP 包

在 PC3 中用协议分析软件抓包并分析，如下图所示。

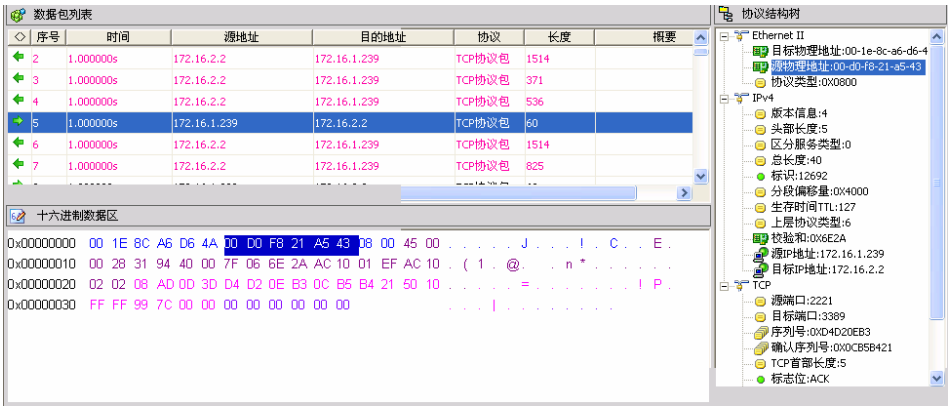

图 3-8 捕获发自不同网段数据包分析

在上图中可以看到，和发往相同网段的数据包并无太多不同，主要区别在于：

- 接受报文中的源目的 MAC 地址与发送的源目的 MAC 地址不同。
- 生存时间：发送数据包的 TTL 值为 128，接受方为 127，因为从拓扑中可以看到数据从 PC1 发送到 PC3，需要经过一个路由器，因此 TTL 值减 1。

步骤四：运行 ipconfig 命令

ipconfig 命令在主机中用于查看本机的网络配置，包括主机的 IP 地址、MAC 地址、网关、DNS 配置等信息。

1、在运行中输入 cmd，出现界面后输入 ipconfig /all；如图：

```
G:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : 97ebd74a16b94e6
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Unknown
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter 本地连接 5:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Attansic L2 Fast Ethernet 10/100 Base-T A
dapter
   Physical Address. . . . . . . . . : 00-1B-FC-A6-AE-E2
   DHCP Enabled. . . . . . . . . . . : No
   IP Address. . . . . . . . . . . . : 172.16.1.239
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.1.1
   DNS Servers . . . . . . . . . . . : 172.16.1.248
                                       202.96.64.68
```

图 3-9 ipconfig 输出信息

2、观察运行结果，获得本机的 IP 地址及子网掩码；

从上图中的显示结果中可以看到，ipconfig /all 命令输出包括主机名称：dqy，节点类型等，以及网络接口上的相关配置。从上图中可以看到网络接口配置为：

- MAC 地址：00-1B-FC-A6-AE-E2
- DHCP：为未启用
- IP 地址：172.16.1.239
- 子网掩码：255.255.255.0
- 默认网关：172.16.1.1
- DNS 服务器：172.16.1.248
- 202.96.64.68

3、分析本主机属于哪一类 IP 地址，网络号、子网号和主机号分别是什么；

步骤五：运行 netstat 命令

netstat 命令用于显示与 IP、TCP、UDP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

1、在命令行界面下运行：netstat –r，显示本机路由表，记录本机的缺省网关的 IP 地址，如下图所示：

```
G:\Documents and Settings\Administrator>netstat -r

IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 1b fc a6 ae e2 ...... Attansic L2 Fast Ethernet 10/100 Base-T Adapter
- Kaspersky Anti-Virus NDIS Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      172.16.1.1     172.16.1.239     20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1      1
      172.16.1.0    255.255.255.0     172.16.1.239     172.16.1.239     20
    172.16.1.239  255.255.255.255        127.0.0.1       127.0.0.1     20
  172.16.255.255  255.255.255.255     172.16.1.239     172.16.1.239     20
        224.0.0.0        240.0.0.0     172.16.1.239     172.16.1.239     20
  255.255.255.255  255.255.255.255     172.16.1.239     172.16.1.239      1
Default Gateway:        172.16.1.1
===========================================================================
```

图 3-10 netstat –r 输出信息

在主机的路由信息输出结果中，第一列为目标网段，第二列为子网掩码，第三列为去往目标网段的网关。第四列为去往目标网段的的接口，第五列为去往目标网段的开销。

2、在命令行界面下运行：netstat –s，查看 IP 协议部分，查看本机已经接收和发送的 IP 报文个数，如图：

```
G:\Documents and Settings\Administrator>netstat -s

IPv4 Statistics

  Packets Received                   = 1488716
  Received Header Errors             = 18
  Received Address Errors            = 54
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 13
  Received Packets Delivered         = 1488684
  Output Requests                    = 1747391
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
  Reassembly Required                = 2
  Reassembly Successful              = 1
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 1
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 2
```

图 3-11 netstat –s 输出结果

从 netstat –s 输出结果中可以查看 TCP、UDP、IP、ICMP 等协议发送和接收的报文数量，上图中给出了 IPv4 报文的接收报文数量、出错数据包的数量等信息。

步骤六：运行 ping 命令

1、在地址本中选择与本主机在同一子网中另一主机的 IP 地址(假设为：172.16.1.251)。

在本机命令行界面下运行：ping 172.16.1.251。

在 ping 的目的地址的主机上用协议分析器一端捕获数据，记录源、目的物理地址及源、目的 IP 地址，捕获到的报文如下图所示。

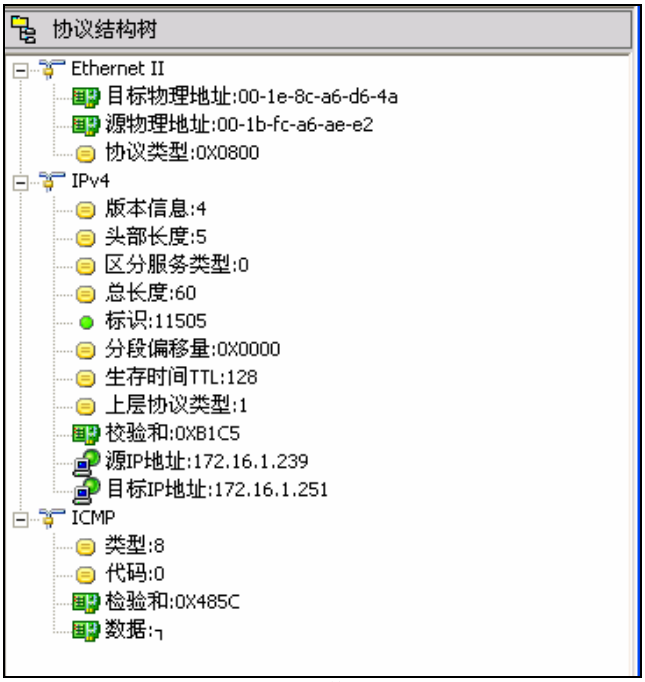

图 3-10 ping 数据包

按照地址本中的记录，分析捕获数据的 MAC 地址与 IP 地址的对应关系；

在 ping 目的主机上通过协议分析器，查看“交互序列图”，了解 PING 程序的会话过程，如下图所示。

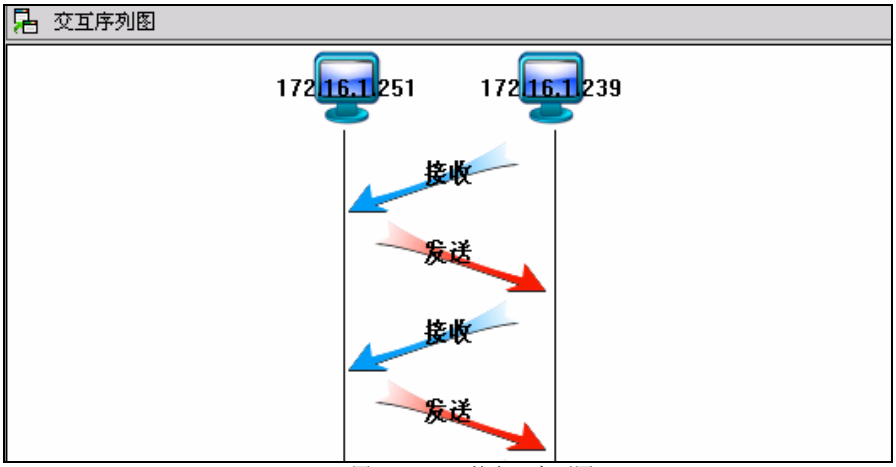

图 3-11 ping 的交互序列图

2、选择与本主机属于不同子网另一主机的 IP 地址(假设为：172.16.2.1)；

在命令行方式下运行：ping 172.16.2.1；

协议分析器端捕获数据，记录源、目的物理地址和源、目的 IP 地址；

分析捕获数据的 MAC 地址与 IP 地址是否具有对应关系。

3、比较上面两个实验的结果，分析二者有何不同？

【思考问题】

结合实验过程中的实验结果，问答下列问题：

1、实验所用主机的 IP 地址、子网掩码、网络号、子网号分别是多少？该主机的 IP 地址属于哪类？

2、IP 数据包在从源主机出发到达目的主机的过程中，IP 首部中的 IP 源地址和目的地址字段是否发生变化？