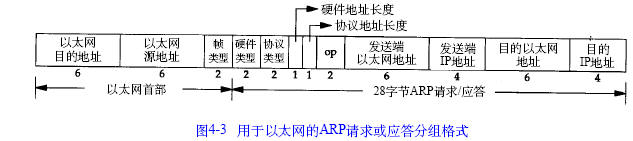
### 实验四：利用分组嗅探器分析数据链路层协议

【实验前需要学习掌握的知识】



以太网报头中的前两个字段是以太网的源地址和目的地址。目的地址为全1的特殊地址是广播地址。电缆上的所有以太网接口都要接收广播的数据帧。

两个字节长的以太网帧类型表示后面数据的类型。对于ARP请求或应答来说，该字段的值为0x0806。

hardware (硬件)和protocol (协议)用来描述ARP分组中的各个字段。例如，一个ARP请求分组询问协议地址（这里是IP地址）对应的硬件地址（这里是以太网地址）。

硬件类型字段表示硬件地址的类型。它的值为1即表示以太网地址。协议类型字段表示要映射的协议地址类型。它的值为0x0800即表示IP地址。它的值与包含IP数据报的以太网数据帧中的类型字段的值相同，这是有意设计的。

接下来的两个1字节的字段，硬件地址长度和协议地址长度分别指出硬件地址和协议地址的长度，以字节为单位。对于以太网上IP地址的ARP请求或应答来说，它们的值分别为6和4。

操作字段指出四种操作类型，它们是ARP请求（值为1）、ARP应答（值为2）、R ARP请求（值为3）和R ARP应答（值为4）。这个字段必需的，因为ARP请求和ARP应答的帧类型字段值是相同的。

接下来的四个字段是发送端的硬件地址（在本例中是以太网地址）、发送端的协议地址（IP地址）、目的端的硬件地址和目的端的协议地址。注意，这里有一些重复信息：在以太网的数据帧报头中和ARP请求数据帧中都有发送端的硬件地址。

对于一个ARP请求来说，除目的端硬件地址外的所有其他的字段都有填充值。当系统收到一份目的端为本机的ARP请求报文后，它就把硬件地址填进去，然后用两个目的端地址分别替换两个发送端地址，并把操作字段置为2，最后把它发送回去。

【实验目的】

了解数据链路层协议构造

【实验内容】

**对数据链路层协议进行捕包分析并回答问题**

**俘获并分析以太网帧**

(1)清空浏览器缓存（在IE窗口中，选择“工具/Internet选项/删除文件”命令）。

(2)启动Ethereal，开始分组俘获。

(3)在浏览器的地址栏中输入：http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-file3.html，浏览器将显示冗长的美国权力法案。

(4)停止分组俘获。首先，找到你的主机向服务器gaia.cs.umass.edu发送的HTTP GET报文的分组序号，以及服务器发送到你主机上的HTTP 响应报文的序号。其中，窗口大体如下。



选择“*Analyze->Enabled Protocols”，*取消对IP复选框的选择，单击OK。窗口如下。



(5)选择包含HTTP GET报文的以太网帧，在分组详细信息窗口中，展开Ethernet II信息部分。根据操作，回答“实验报告”中的1-5题

(6)选择包含HTTP 响应报文第一个字节的以太网帧，根据操作，回答“实验报告”中的6-10题

**ARP分析**

(1)利用MS-DOS命令：arp 或 c:\windows\system32\arp查看主机上ARP缓存的内容。根据操作，回答“实验报告”中的11题。

(2)利用MS-DOS命令：arp-d \* 清除主机上ARP缓存的内容。

(3)清除浏览器缓存。

(4)启动Ethereal，开始分组俘获。

(5)在浏览器的地址栏中输入：http://gaia.cs.umass.edu/ethereal-labs/ HTTP-ethereal-lab-file3.html，浏览器将显示冗长的美国权力法案。

(6)停止分组俘获。选择“*Analyze->Enabled Protocols”，*取消对IP复选框的选择，单击OK。窗口如下。根据操作，回答“实验报告”中的12-15题。



【实验方式】实验指导教师讲解演示，每位同学上机实验，并与指导教师讨论。

【实验地点】学院实验室。

【实验报告】在实验报告中写出各层次捕包实验的实现过程并回答问题，分析并总结实验中遇到的问题，写出实验体会。

在实验的基础上，回答以下问题：

1. 你的主机的48位以太网地址是多少？
2. 是gaia.cs.umass.edu服务器的地址吗？如不是，该地址是什么设备的以太网地址？
3. 给出两种帧类型字段的十六进制值。标志字段的值是1的含义是什么？
4. 在包含“get”以太网帧中，从该帧的起始处开始一共有多少个ASCII字符“G”？
5. 在该以太网帧中CRC字段的十六进制值是多少？
6. 以太网源地址是多少？该地址是你主机的地址吗？是gaia.cs.umass.edu服务器的地址吗？如果不是，该地址是什么设备的以太网地址？
7. 以太网帧的48位目的地址是多少？该地址是你主机的地址吗？
8. 给出两种帧类型字段的十六进制值。标志字段的值是1的含义是什么？
9. 在包含“OK”以太网帧中，从该帧的起始处开始一共有多少个ASCII字符“O”？
10. 在该以太网帧中CRC字段的十六进制值是多少？
11. 写下你主机ARP缓存中的内容。其中每一列的含义是什么？
12. 包含ARP请求报文的以太网帧的源地址和目的地址的十六进制值各是多少？
13. 给出两种帧类型字段的十六进制值。标志字段的值是1的含义是什么？
14. 从ftp://ftp.rfc-editor.org/innotes/std/std37.txt处下载ARP规范说明。在http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html处也有一个可读的关于ARP的讨论网页。根据操作回答：
    1. 形成ARP响应报文的以太网帧中ARP-payload部分opcode字段的值是多少？
    2. 在ARP报文中是否包含发送方的IP地址？
15. 包含ARP回答报文的以太网帧中源地址和目的地址的十六进制值各是多少？

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **计算机网络与通信实验报告（四）** | | | | | | |
| 学 号 | 姓 名 | | 班 级 | | 报告日期 | |
|  |  | |  | |  | |
| 实验内容 | **利用分组嗅探器分析数据链路层协议** | | | | | |
| 实验目的 |  | | | | | |
| 实验预备知识 |  | | | | | |
| 实验过程描述 |  | | | | | |
| 实验结果 |  | | | | | |
| 实验当中问题  及解决方法 | 1、  2、 | | | | | |
| 成绩（教师打分） | 优秀 | 良好 | | 及格 | | 不及格 |