|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **计算机网络与通信实验报告（四）** | | | | | | |
| 学 号 | 姓 名 | | 班 级 | | 报告日期 | |
| 202221139 | 杨涛 | | 2211106 | | 2024.11.4 | |
| 实验内容 | **利用分组嗅探器分析数据链路层协议** | | | | | |
| 实验目的 | 了解数据链路层协议构造，掌握对其进行分析的能力 | | | | | |
| 实验预备知识 | 872729  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。 | | | | | |
| 实验过程描述 | 1. **以太网帧分析**   (1) 清空浏览器缓存。  (2) 启动分组捕获软件，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。  选择“Analyze->Enabled Protocols”，取消对IP复选框的选择，单击OK。  (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。  (6) 选择包含HTTP 响应报文第一个字节的以太网帧。     1. **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。  (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) 启动分组捕获软件，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。 | | | | | |
| 实验结果 | (1)你的主机的48位以太网地址是多少？  bc:6e:e2:8d:f5:13    (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？  不是，这是局域网路由器网关的以太网地址。  (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？    对于IP报文来说，该字段值是0x0800。对于ARP信息来说，以太类型字段的值是0x0806。    LG标志位置1表示：由本地管理的mac地址，而非出厂时默认设置。  IG标志位置1表示：组地址，多播或广播地址。  TCP中也含有标志字段。  URG表示紧急数据  ACK表示确认字段的值有效  PSH表示接收方应立即将数据交给上层  RST表示重建连接  SYN表示连接建立的第一次握手  FIN表示连接拆除的第一次握手  (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”？  包含两个G。    (5)在该以太网帧中CRC字段的十六进制值是多少？  分组被Ethereal捕获时网卡已经把以太网的CRC校验字段给剥除了，故没有显示。  (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？      以太网源地址是a6:9c:cc:1a:46:2d，不是主机地址，也不是目标gaia.cs.umass.edu服务器的地址，是192.168.105.87的动态以太网地址。  (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？    以太网帧的48位目的地址是bc:6e:e2:8d:f5:13，该地址是我的主机地址。  (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？    对于IP报文来说，该字段值是0x0800。对于ARP信息来说，以太类型字段的值是0x0806。    LG标志位置1表示：由本地管理的mac地址，而非出厂时默认设置。  IG标志位置1表示：组地址，多播或广播地址。  TCP中也含有标志字段。  URG表示紧急数据  ACK表示确认字段的值有效  PSH表示接收方应立即将数据交给上层  RST表示重建连接  SYN表示连接建立的第一次握手  FIN表示连接拆除的第一次握手  (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”？  一共有5个O。    (10)在该以太网帧中CRC字段的十六进制值是多少？  分组被Ethereal捕获时网卡已经把以太网的CRC校验字段给剥除了，所以未在软件中出现。  (11)写下你主机ARP缓存中的内容。其中每一列的含义是什么？    A.接口：显示当前ARP表项所属的网络接口.  B.Internet 地址：表示设备的IP地址或多播地址。  C.物理地址：表示与该IP地址相对应的MAC地址。以"01-00-5e"开头的MAC地址通常表示多播地址,MAC地址"ff-ff-ff-ff-ff-ff"表示广播地址。  D.类型：表示条目的类型，有两种：静态：表示该条目是手动添加或永久保存的。动态：表示该条目是 ARP 协议自动生成的，会定期刷新。  (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？    58:69:6c:a6:8f:09和ff:ff:ff:ff:ff:ff  (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？  对于IP报文来说，该字段值是0x0800。对于ARP信息来说，以太类型字段的值是0x0806。    帧类型字段的十六进制值还可以是0x0806，表示数据帧内容为ARP请求或响应类型。  LG标志位置1表示：由本地管理的mac地址，而非出厂时默认设置。  IG标志位置1表示：组地址，多播或广播地址。  TCP中也含有标志字段。  URG表示紧急数据  ACK表示确认字段的值有效  PSH表示接收方应立即将数据交给上层  RST表示重建连接  SYN表示连接建立的第一次握手  FIN表示连接拆除的第一次握手   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？在ARP报文中是否包含发送方的IP地址？     响应报文的opcode字段的值是0x0002。  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？  源地址为本机的mac地址，目的地址为发广播包的主机或路由器的mac地址。 | | | | | |
| 实验当中问题  及解决方法 | 1、执行清楚本机ARP缓存时提示需要进行提升  解决方法：采用管理员方式打开cmd  2、 用Ethereal所捕的以太网帧没有前导码、CRC。  结论：网卡需要做这样的工作，在物理层上要先去掉前导同步码和帧开始定界符，然后对帧进行CRC检验，如果帧校验和错，就丢弃此帧。如果校验和正确，就判断帧的目的硬件地址是否符合自己的接收条件，如果符合，就将帧交“设备驱动程序”做进一步处理。这时我们的捕包软件才能捕到数据。因此，捕包软件捕到的是去掉前导同步码、帧开始分界符和CRC检验之外的数据。  3、抓包时网络流量过大，捕获不完整  解决方法：使用过滤器减少捕获的包数量，或者将抓包分为多个时间段进行，确保数据不丢失。 | | | | | |
| 成绩（教师打分） | 优秀 | 良好 | | 及格 | | 不及格 |