|  |
| --- |
| **实验目的：** 研究以太网协议和 ARP 协议  **实验结果：**  一、以太网协议：  在自己电脑上捕获的数据包：    如下答案均使用官方给出的包  一、你的电脑 48 位的地址是多少？  00:d0:59:a9:3d:68  2.以太网帧中的 48 位目标地址是什么？这是 gaia.cs.umass.edu 的以太网地址吗？（提示：答案是否定的）。那么它是什么?  目标地址： 00:06:25:da:af:73 不是  这是本地的路由器地址，是出子网的链路地址    3.以太网帧上层协议 16 进制值是什么?这对应的上层协议是什么？  16进制：0x0800 说明是IP协议    4.从以太帧的开始，一直到“GET”中的 ASCII“G”出现在以太网帧中为止，有多少字节？  两位16进制数代表一个字节，前三行每一行有16个字节，第四行有7个字节，总共有55个字节，如下图所示：    根据包含 HTTP 响应消息的第一个字节的以太网帧的内容，回答以下问题。  5.这个以太网帧中，以太网源地址的值是多少？这是你的计算机的地址，还是gaia.cs.umass.edu 的地址（提示：答案是否定的）。拥有这个以太网地址的设备是什么？  00:06:25:da:af:73 都不是，  这是Linksys路由器的地址，这是用于进入本地子网的链路地址    6.以太网帧中的目的地址是什么？这是您的计算机的以太网地址吗？  00:d0:59:a9:3d:68 是    7.以太网帧上层协议 16 进制值是什么?这对应的上层协议是什么？  16 进制值：0x800 IP协议  8.从以太帧的开始，一直到“OK”中的 ASCII“O”出现在以太网帧中为止，有多少字节？  有16\*4+4=68个字节    ARP协议：    9.写下计算机 ARP缓存的内容。每个列值的含义是什么？    有三列分别是：Internet地址(也就是IP地址)、  物理地址(也就是MAC地址)、  类型(动态，如果某个表项在一定的时间内没有用到就被删除，静态则永久保存)  10.包含 ARP请求消息的以太网帧中源和目标地址的十六进制值是什么？  对应的源地址为: 00:d0:59:a9:3d:68，  目的地址为: ff:ff:ff:ff:ff:ff广播地址    11.以太网帧上层协议 16进制值是什么?  16进制值：0x0806 ARP协议  12.分析ARP请求   1. ARP 操作码字段 开始从以太网帧的最开始有多少字节？   ARP操作码就是Opcode,距最开始之前20字节的地方     1. 在进行ARP请求的以太网帧的ARP负载部分中，操作码字段的值是多少？   1   1. ARP 消息是否包含发送方的 IP 地址？   包含     1. 在 ARP 请求中从哪里看出我们要查询相应 IP 的以太网地址?   Target MAC address字段    13. 到响应 ARP 请求的而发送 ARP 回复  a)ARP 操作码字段开始从以太网帧的最开始有多少字节？  20 个字节，如下图所示：    B)在进行 ARP 响应的以太网帧的 ARP 负载部分中，操作码字段的值是多少？  操作码字段:0x0002,用于应答。  C)在响应 ARP 中从哪里看出现早期 ARP 请求的答案?  Target MAC address 为 00:d0:59:a9:3d:68  Target IP address 为 192.168.1.105  这两项与之前的ARP Sender MAC address， Sender IP address 对应    14.包含 ARP 回复消息的以太网帧中源地址和目标地址的十六进制值是多少？  source address ： 00:06:25:da:af:73  destination address ： 00:d0:59:a9:3d:68 .    15.在作者抓包结果中，他有两台电脑，一台运行 wireshark 进行抓包，一台没有，那么为什么运行 wireshark 那台电脑发送 ARP 请求得到了应答，另外一台电脑的 ARP 请求没有得到应答?(没有相应第 6 帧的 ARP 的请求)？  因为 ARP 请求信息是广播的，所有该网段内的电脑均可收到，而 ARP 回复是单播的，只有请求的那台电脑才能收到，因此抓不到另外一台电脑的 ARP 请求。  **问题及收获：**  学到了以太网帧中请求消息的目标地址不是访问网址的IP地址而是离开子网的链路地址，响应消息的源地址是进入子网的链路地址；  学会了通过计算十六进制数的个数来得到数据的字节数；  学到了ARP请求消息是采用广播的方式传送，响应消息是采用单播的形式传送； |