山东大学 计算机 学院

计算机网络 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：202000130143 | 姓名： 郑凯饶 | | 班级： 2020级1班 |
| 实验题目：ARP | | | |
| 实验学时：2 | | 实验日期： 2022-5-24 | |
| 实验目的：  研究以太网协议以及ARP协议（通过IP地址获取远程主机的MAC地址） | | | |
| 硬件环境：  Dell Latitude 5411  Intel(R) Core(TM) i5-10400H CPU @ 2.60GHz(8GPUs),~2.6GHz | | | |
| 软件环境：  Windows 10 家庭中文版64位（10.0，版本18363）  Wireshark-win64-3.6.2 | | | |
| 实验步骤与内容：   1. 问题： 2. 本机48位物理地址。 3. 目标地址。是gaia.cs.umass.edu的以太网地址吗？ 4. 给出以太网帧上层协议的16进制值。对应什么协议？ 5. 以太帧开始直到“GET”中“G”出现为止，有多少字节？ 6. 以太网源地址，拥有该地址的设备是什么？ 7. 目的地址，是本机地址？ 8. 上层协议。 9. 以太网帧中直到“OK”中“O”出现之前有多少字节？ 10. 记录arp缓存内容，每个列值的含义？ 11. 包含arp请求的源和目标地址的16进制值。 12. 上层协议。 13. A）以太网帧开始至arp操作码字段有多少字节？B）arp请求的负载部分，操作码的值是多少？C）是否包含发送方的IP地址？D）arp请求中哪里指明我们要查询相应IP的以太网址？ 14. A）同上B）同上C）响应MAC 15. 同（10） 16. 作者运行wireshark的电脑发送的ARP请求获得了回复，而另一台却没有？解释原因。 17. 阐述基本方法     ARP报文格式：  在这里插入图片描述   1. 实验结果展示与分析   （禁用IPV4）     1. Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68) 2. Destination: LinksysG\_da:af:73 (00:06:25:da:af:73)不是，主机与gaia.cs.umass.edu服务器不在同一子网，应为路由器的MAC地址。 3. Type: IPv4 (0x0800) 4. 54B      1. Source: LinksysG\_da:af:73 (00:06:25:da:af:73)，不是，是主机所在在子网的路由设备。 2. Destination: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)，是。 3. Type: IPv4 (0x0800) 4. 67B 5. 如下图     （10）Source: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)  Address: Broadcast (ff:ff:ff:ff:ff:ff)  （11） Type: ARP (0x0806)  （12）A)第21B开始B) Opcode: request (1)C) Sender IP address: 192.168.1.105 D）Target IP address: 192.168.1.1    （13）A)第21B开始B) Opcode: reply (2)C) Sender MAC address: LinksysG\_da:af:73 (00:06:25:da:af:73)    （14）Destination: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)  Address: LinksysG\_da:af:73 (00:06:25:da:af:73)  （15）可能是对应IP不存在，或者发生丢包  EX-1：网络无法访问  EX-2：120s | | | |
| 结论分析与体会：  这次实验我们实践了ARP协议，也了解了许多针对ARP的攻击，如泛洪攻击、ARP欺骗等等，攻击往往利用了ARP的动态特性，这既是ARP的优点也是它的弊端。至此，我们已经知道数据包是如何传输的（在IP协议的引导下，通过链路层进行传送），希望进行更多网络编程实践。 | | | |