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：

（1） 本机 48 位物理地址。

（2） 目标地址。是 gaia.cs.umass.edu 的以太网地址吗？

（3） 给出以太网帧上层协议的 16 进制值。对应什么协议？

（4） 以太帧开始直到“GET”中“G”出现为止，有多少字节？

（5） 以太网源地址，拥有该地址的设备是什么？

（6） 目的地址，是本机地址？

（7） 上层协议。

（8） 以太网帧中直到“OK”中“O”出现之前有多少字节？

（9） 记录 arp 缓存内容，每个列值的含义？

（10）包含 arp 请求的源和目标地址的 16 进制值。

（11）上层协议。

（12）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？

（13）A）同上 B）同上 C）响应 MAC

（14）同（10）

（15）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。

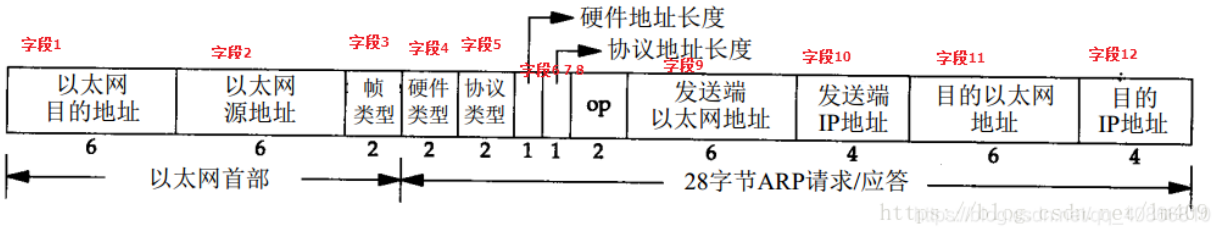
2. 阐述基本方法

①ARP（Address Resolution Protocol）即地址解析协议， 用于实现从 IP 地址到 MAC 地址的映射，即询问目标IP对应的MAC地址。

②在网络通信中，主机和主机通信的数据包需要依据OSI模型从上到下进行数据封装，当数据封装完整后，再向外发出。所以在局域网的通信中，不仅需要源目IP地址的封装，也需要源目MAC的封装。

③一般情况下，上层应用程序更多关心IP地址而不关心MAC地址，所以需要通过ARP协议来获知目的主机的MAC地址，完成数据封装。

ARP 报文格式：



3. 实验结果展示与分析

（禁用 IPV4）

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.1
2	0.001018	LinksysG_da:af:73	AmbitMic_a9:3d:…	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	0.001028	AmbitMic_a9:3d:68	LinksysG_da:af:…	0x0800	62	IPv4
4	2.962850	AmbitMic_a9:3d:68	LinksysG_da:af:…	0x0800	62	IPv4
5	8.971488	AmbitMic_a9:3d:68	LinksysG_da:af:…	0x0800	62	IPv4
6	13.542974	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1
7	17.444423	AmbitMic_a9:3d:68	LinksysG_da:af:…	0x0800	62	IPv4
8	17.465902	LinksysG_da:af:73	AmbitMic_a9:3d:…	0x0800	62	IPv4
9	17.465927	AmbitMic_a9:3d:68	LinksysG_da:af:…	0x0800	54	IPv4
10	17.466468	AmbitMic_a9:3d:68	LinksysG_da:af:…	0x0800	686	IPv4
11	17.494766	LinksysG_da:af:73	AmbitMic_a9:3d:…	0x0800	60	IPv4
12	17.498935	LinksysG_da:af:73	AmbitMic_a9:3d:…	0x0800	1514	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

```
0000  00 06 25 da af 73 00 d0  59 a9 3d 68 08 00 45 00   ··%··s·· Y·=h··E·
0010  02 a0 00 fa 40 00 80 06  bf c8 c0 a8 01 69 80 77   ····@··· ·····i·w
0020  f5 0c 04 22 00 50 65 14  99 a7 ac a5 3f b4 50 18   ···"·Pe· ····?·P·
0030  fa f0 7e 4f 00 00 47 45  54 20 2f 65 74 68 65 72   ··~O··GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 48 54 54 50 2d 65 74   eal-labs /HTTP-et
0050  68 65 72 65 61 6c 2d 6c  61 62 2d 66 69 6c 65 33   hereal-l ab-file3
0060  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1··
0070  48 6f 73 74 3a 20 67 61  69 61 2e 63 73 2e 75 6d   Host: ga ia.cs.um
0080  61 73 73 2e 65 64 75 0d  0a 55 73 65 72 2d 41 67   ass.edu· ·User-Ag
0090  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00a0  20 28 57 69 6e 64 6f 77  73 3b 20 55 3b 20 57 69    (Window s; U; Wi
00b0  6e 64 6f 77 73 20 4e 54  20 35 2e 31 3b 20 65 6e   ndows NT  5.1; en
00c0  2d 55 53 3b 20 72 76 3a  31 2e 30 2e 32 29 20 47   -US; rv: 1.0.2) G
00d0  65 63 6b 6f 2f 32 30 30  33 30 32 30 38 20 4e 65   ecko/200 30208 Ne
00e0  74 73 63 61 70 65 2f 37  2e 30 32 0d 0a 41 63 63   tscape/7 .02··Acc
00f0  65 70 74 3a 20 74 65 78  74 2f 78 6d 6c 2c 61 70   ept: tex t/xml,ap
0100  70 6c 69 63 61 74 69 6f  6e 2f 78 6d 6c 2c 61 70   plicatio n/xml,ap
```

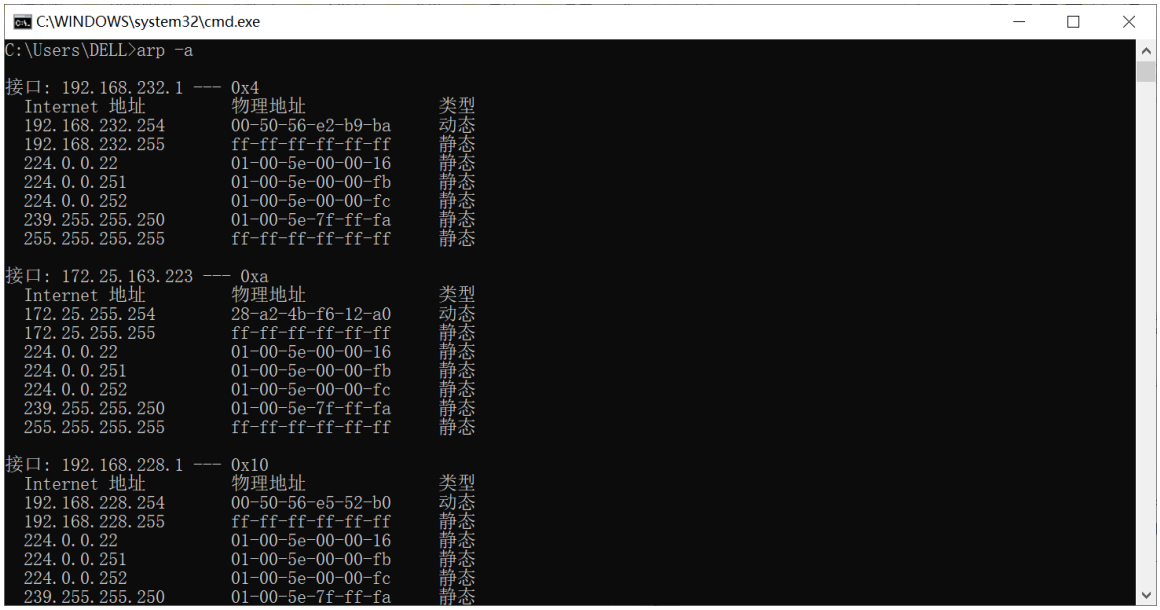
（5） Source: LinksysG_da:af:73 (00:06:25:da:af:73)，不是，是主机所在在子网的路由设备。

（6） Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)，是。

（7） Type: IPv4 (0x0800)

（8） 67B

（9） 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

```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    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)

```
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
Sender IP address: 192.168.1.1
```

（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

3.2 ARP缓存时间

在ARP缓存表中，动态ARP和静态ARP：

动态ARP：动态ARP条目随着时间推移自动添加或删除，每一个动态ARP缓存项目都设置了生存时间（TTL），TTL为0时此项目就会从ARP表中删除，

Linux默认60秒：

```
[root@localhost ~]# cat /proc/sys/net/ipv4/neigh/ens33/gc_stale_time
60
```

Windows默认120秒：

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters（如下不存在，需要创建）

（1）ArpCacheLife：定义arp老化时间，默认120秒

（2）ArpCacheMinReferencedLife：定义arp最大老化时间，默认10分钟

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。