暨南大学本科实验报告专用纸

课程名称 计算机网络实验 成绩评定

实验项目名称 地址解析协议（ARP） 指导老师 某某某

实验项目编号 2 实验项目类型 综合类 实验地点 N117

学生姓名 某某 学号 xxxxxxxx

学院 网络空间安全学院 系 专业 网络空间安全

实验时间 2020 年 10 月 14 日 晚 上～ 2020 年 10 月 14 日 晚 上

（一）实验目的

1. 掌握 ARP 协议的报文格式
2. 掌握 ARP 协议的工作原理
3. 理解 ARP 高速缓存的作用
4. 掌握 ARP 请求和应答的实现方法
5. 掌握 ARP 缓存表的维护过程

（二）实验环境

图 1：实验环境（该实验采用网络结构二，本机为主机 B）

（三）实验原理

1. 关于ARP协议

ARP 协议（地址解析协议）是“Address Resolution Protocol”的缩写。所谓“地址解析”就是主机在发送帧前将目的逻辑地址转换成目的物理地址的过程。在使用 TCP/IP 协议的以太网中，ARP 协议完成将 IP 地址映射到 MAC 地址的过程。

<table>
<tr><td colspan="2">硬件类型（16 位）</td><td>协议类型（16 位）</td></tr>
<tr><td>硬件地址长度
（8 位）</td><td>协议地址长度
（8 位）</td><td>操作码（16 位）</td></tr>
<tr><td colspan="3">发送端硬件地址
（例如，对以太网是 6 字节）</td></tr>
<tr><td colspan="3">发送端逻辑地址
（例如，对 IP 是 4 字节）</td></tr>
<tr><td colspan="3">目的端硬件地址
（例如，对以太网是 6 字节）
（在请求帧中不填入）</td></tr>
<tr><td colspan="3">目的端逻辑地址
（例如，对 IP 是 4 字节）</td></tr>
</table>

图 2: ARP 报文格式

2. 关于 ARP 高速缓存

在真正的协议实现中，并不是每次发送 IP 报文前都需要发送 ARP 请求报文来获取目的 MAC 地址。在大多数的系统中都存在着一个 ARP 缓存表，记录着一段时间内曾经获取过的 MAC 地址和 IP 地址的映射关系。

发送 IP 数据报前先对 ARP 缓存表进行查找，查看目的 MAC 地址是否存在于缓存表中，如果存在，则不需要发送 ARP 请求报文而直接使用此地址进行 IP 数据包的发送。如果不存在，则发送 ARP 请求报文，在收到 ARP 应答报文之后，使用应答报文中的目的 MAC 地址发送 IP 数据包，并将目的 MAC 地址存于 ARP 缓存表中供以后使用。

另外，ARP 缓存表采用老化机制，在一段时间内如果表中的某一项没有使用，就会被删除，这样可以大大减少 ARP 缓存表的长度，加快查询速度。

3. ARP 的运行过程

数据包传输过程可分为如下步骤：

- 发送端知道目的端的 IP 地址。
- IP 要求 ARP 创建一个 ARP 请求报文，其中包含了发送方的物理地址、发送方的 IP 地址和目的端的 IP 地址。目的端的物理地址用 0 填充。

- 将报文传递到数据链路层，并在该层中用发送方的物理地址作为源地址，用物理广播地址作为目的地址，将其封装在一个帧中。
- 因为该帧中包含了一个广播目的地址，所以同一链路中的每个主机或路由器都接收到这个帧。所有接收到该帧的主机都将其传递到 ARP 层进行处理。除了目的端主机以外的所有主机都丢弃该报文。
- 目的端主机用一个包含其物理地址的 ARP 应答报文做出响应，并对该报文进行单播。
- 发送方接收到这个应答报文，这样它就知道了目标主机的物理地址。

（四）实验步骤

练习1 领略真实的 ARP（同一子网）

各主机打开工具区的“拓扑验证工具”，选择相应的网络结构，配置网卡后，进行拓扑验证，如果通过拓扑验证，关闭工具继续进行实验，如果没有通过，请检查网络连接。本练习将主机 A、B、C、D、E、F 作为一组进行实验。

1. 主机 A、B、C、D、E、F 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ARP、ICMP）。
2. 主机 A、B、C、D、E、F 在命令行下运行“arp -d”命令，清空 ARP 高速缓存。
3. 主机 A ping 主机 D（172.16.1.4）。

   主机 B ping 主机 C（172.16.1.3）。

   主机 E ping 主机 F（172.16.0.3）。
4. 主机 A、B、C、D、E、F 停止捕获数据，并立即在命令行下运行“arp -a”命令察看 ARP 高速缓存。

思考问题：

1) ARP 高速缓存表由哪几项组成？

状态、硬件类型、协议类型、硬件地址长度、协议地址长度、接口号、队列号、尝试、超时、硬件地址、协议地址。

2) 结合协议分析器上采集到的 ARP 报文和 ARP 高速缓存表中新增加的条目，简述 ARP 协议的报文交互过程以及 ARP 高速缓存表的更新过程。

1. ARP 模块接收来自上层的协议 IP 的数据报后提取其目的的 IP 地址。
2. 主机 A 检查自己的高速缓存中的 ARP 表判断 ARP 表中是否存有主机 B 的 IP 地址与 MAC 地址的映射关系。如果找到则完成 ARP 地址解析如果没有找到则转至 3。

3. 主机 A 广播含有自身 IP 地址与 MAC 地址映射关系的请求信息包请求解析主机 B 的 IP 的地址与 MAC 地址映射关系。
4. 主机 A 等待接收 ARP 应答。
5. 如果主机 A 没有收到 ARP 应答则停止发送数据报，如果收到 ARP 应答执行 6。
6. 主机 A 收到主机 B 的响应信息使用应答中的物理地址 MAC 作为数据报的 mac 地址并将主机 B 的 IP 地址与 MAC 地址的映射关系存入自己的 ARP 表中从而完成主机 B 的 ARP 地址解析。

练习2 编辑并发送 ARP 报文（同一子网）

本练习将主机 A、B、C、D、E、F 作为一组进行实验。

1. 在主机 E 上启动协议编辑器，并编辑一个 ARP 请求报文。其中：

   MAC 层：

   - 目的 MAC 地址：设置为 FFFFFF-FFFFFF
   - 源 MAC 地址：设置为主机 E 的 MAC 地址
   - 协议类型或数据长度：0806

   ARP 层：

   - 发送端硬件地址：设置为主机 E 的 MAC 地址
   - 发送端逻辑地址：设置为主机 E 的 IP 地址（172.16.0.2）
   - 目的端硬件地址：设置为 000000-000000
   - 目的端逻辑地址：设置为主机 F 的 IP 地址（172.16.0.3）

2. 主机 A、B、C、D、F 启动协议分析器，打开捕获窗口进行数据捕获并设置过滤条件（提取 ARP 协议）。
3. 主机 B、E、F 在命令行下运行“arp -d”命令，清空 ARP 高速缓存。主机 E 发送已编辑好的 ARP 报文。
4. 主机 A、B、C、D、F 停止捕获数据，分析捕获到的数据，进一步体会 ARP 报文交互过程。

思考问题：

1) 哪些主机收到了 ARP 请求包，哪个主机给出了 ARP 响应包？

主机 A、B、C、D、F 都收到 ARP 请求包，主机 E 给出了 ARP 响应包。

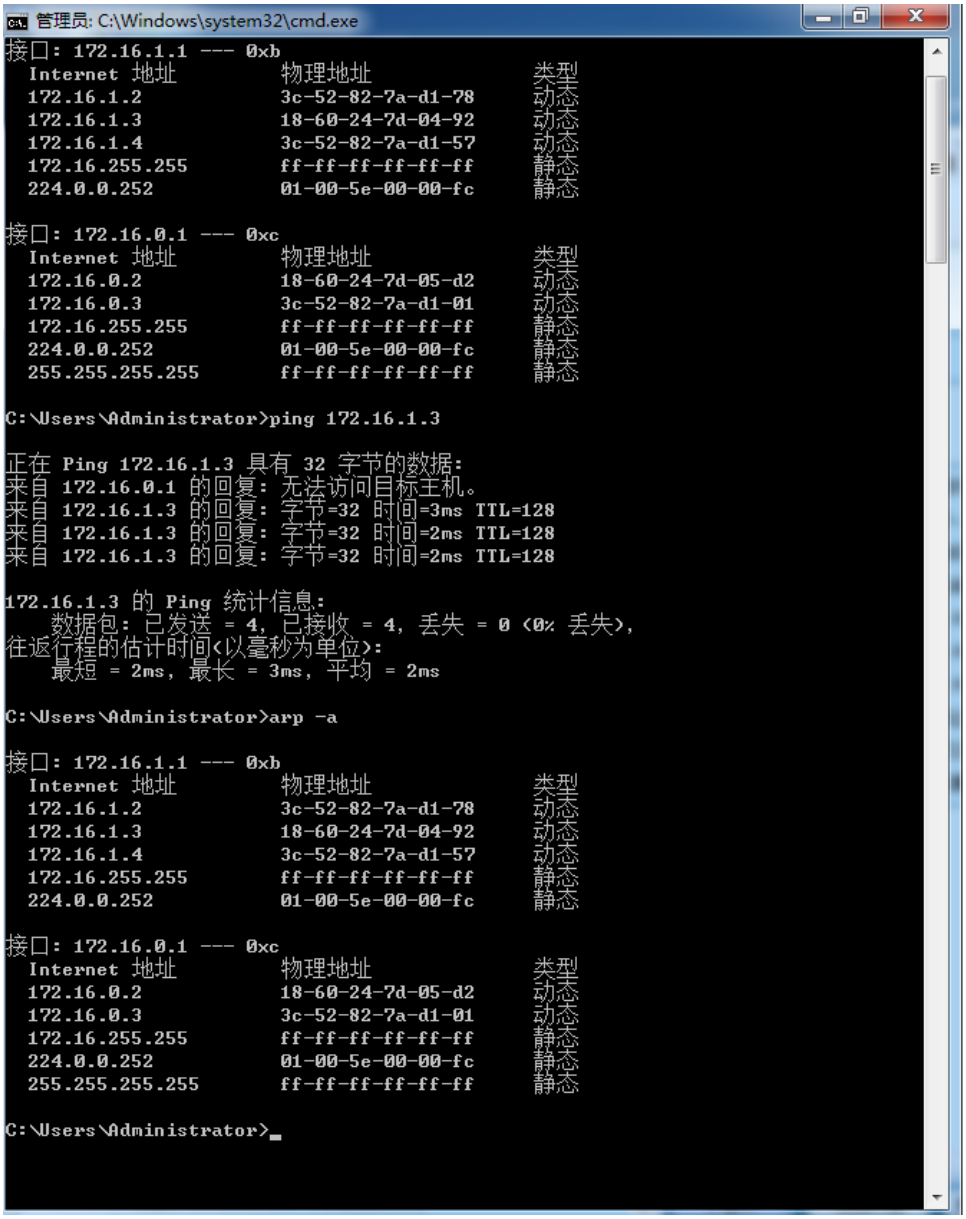
2) 主机 A、C、D 是否收到 ARP 请求包，为什么？

主机 A、C、D 都收不到请求包，因为他们和主机 E 不在同一个网段（被主机 B 隔离了），每一个网段都是独立的广播域。

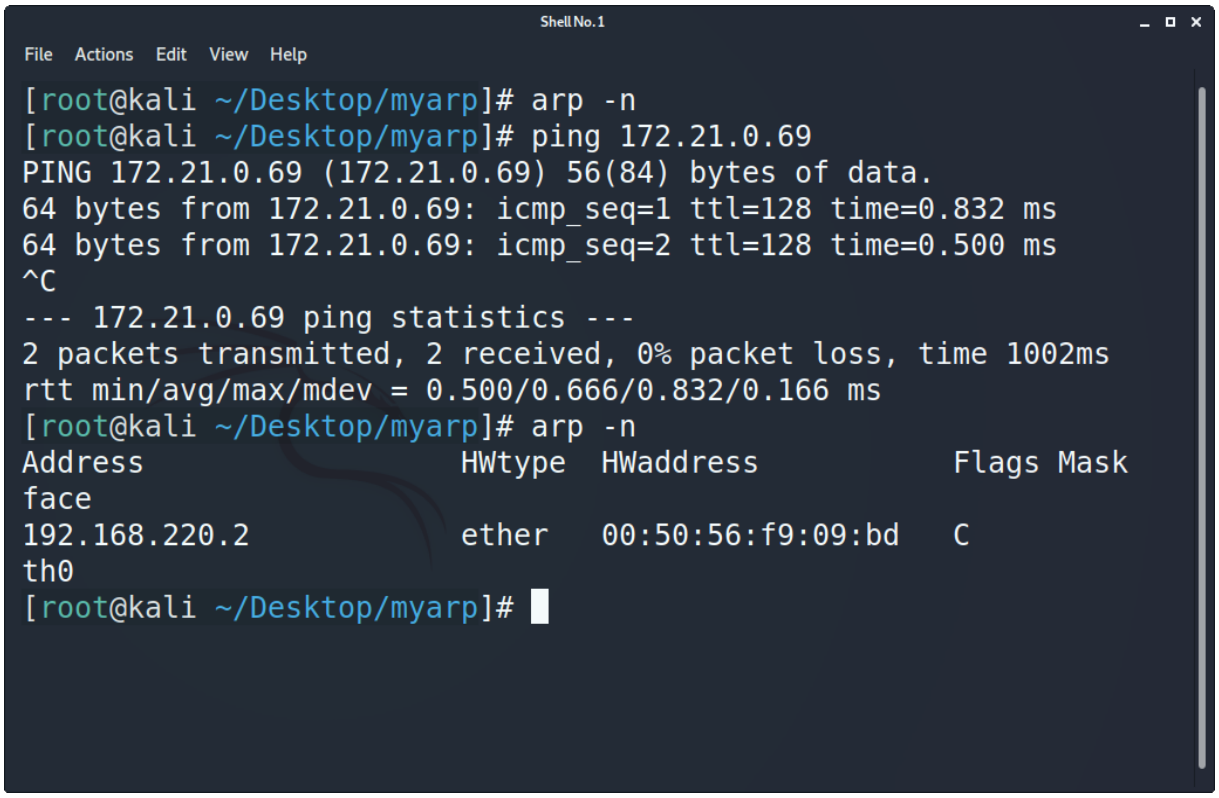
（五）实验结果与分析

练习1 领略真实的 ARP（同一子网）

由于实验是时候图片拍得不是很全，有些实验我在自己的设备又做了一次作为补充分析的材料。

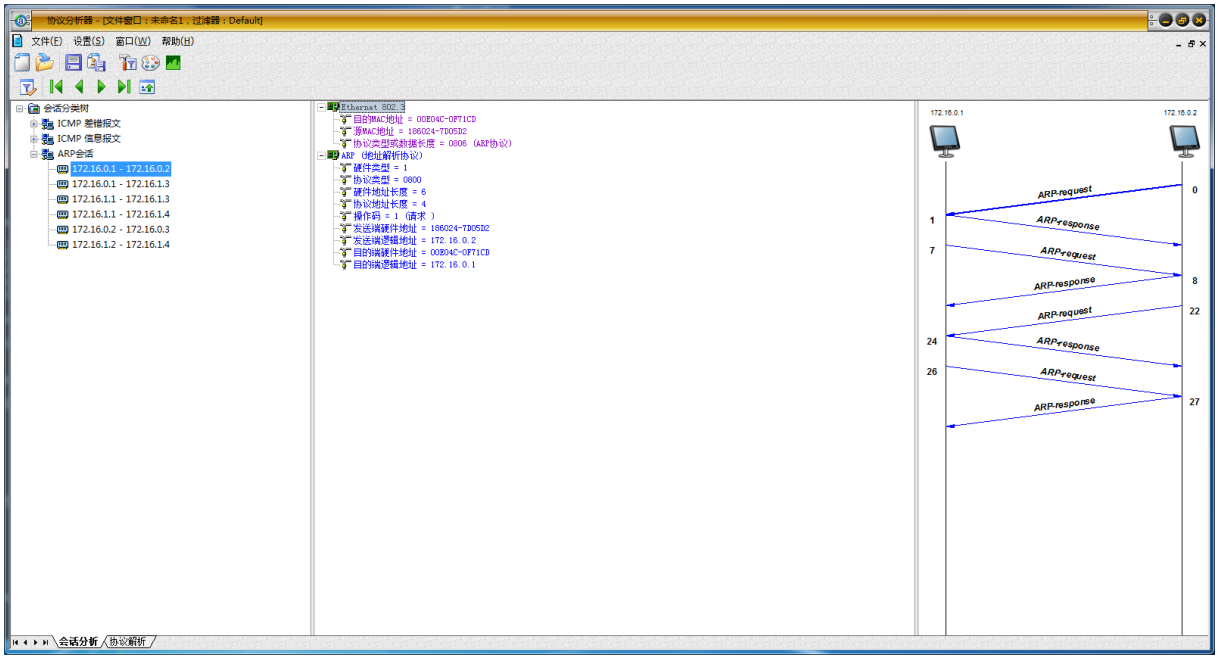


分析：正如实验原理所述，因为本机是 B 主机，所以有两个网卡，充当路由的角色。实验时先用 arp -d 命令清除 arp 缓存中记录的 MAC 地址，由于局域网内多台主机使用 ping 命令，且 B 主机又充当路由的角色，所以 arp 缓存会记录通信过的 IP-MAC 地址映射。当然，过一段时间后又会清除掉，因为有可能接口主机发生变动。这里的缓存又中分了动态和静态两种，静态指固定不变的，因为这些 IP 地址都有特殊含义，而其他主机的 IP-MAC 映射都是动态的，当 TTL=0 时他们会被删除。



分析：Linux 也差不多，清缓存后再 ping 某个 IP，然后查看 arp 缓存记录。

练习2 编辑并发送 ARP 报文（同一子网）



分析：主机 B 先运行 arp -d 命令清空 arp 缓存，主机 E 以太网协议帧的类型设置为 0806 表示这是个 ARP 请求包，同时把目的地址设置为 FFFFFF-FFFFFF 进行广播，询问 IP 地址为 172.16.0.3 的主机的 MAC 地址，ARP 协议包把目的端硬件地址设置为 000000-000000，其余都如实设置。结果只有主机 B、F 收到了主机 E 的 ARP 数据包，因为主机 B 把主机 A、C、D 隔离了，所以他们收不到 ARP 数据包。

（六）附录：借用 PF_PACKET 实现简单的 ARP 报文发送和接收

关于 arping 的一些测试网络说明

- arping IP。发送 arp 数据包得到 IP 的物理地址。
- arping -i eth1 -c 1 IP。-i 可指定网卡，-c 可指定发送的报文数量，Linux 默认是一直发送。
- arping -c 1 MAC。查看某个 MAC 地址的 IP，要在同一子网才查得到。

参考《TCP/IP 详解卷一：协议》第二版第四章

简述

1. 获得局域网其他主机的 MAC 地址主要靠 ARP 协议，Linux 也提供了 libnet 小型库用于收发包括 arp 请求包在内的各种网络编程相关的数据包。

2. 小程序的大体思路如下：

   1) 为数据报分配空间，创建相应的结构体 req。

   2) 创建 PF_PACKET 原始套接字，发送套接字为 reqfd，接收套接字为 recvfd。

   3) 填写链路层通用结构体 reqsa。

   4) get_ifi() 获取本机网络接口数据，填写要发送的 ARP 数据报 req 结构体，sendto() 发送。

   5) 循环 recvfrom() 接收 ARP 响应，滤掉经由本地接口的其他 ARP 数据报。

   6) 另外，把一些函数的检错环节重新封装在 wrap.h，函数名使用开头大写的方式（而不是像 C++ 那些使用下划线命名），既可以使代码逻辑更清晰，又可以在用 vim 写的过程中查看 man page(vim 命令不区分大小写)。

3. ARP 协议涉及到不少网络攻击方式，常见的有 ARP 欺骗、ARP 泛洪攻击等等。

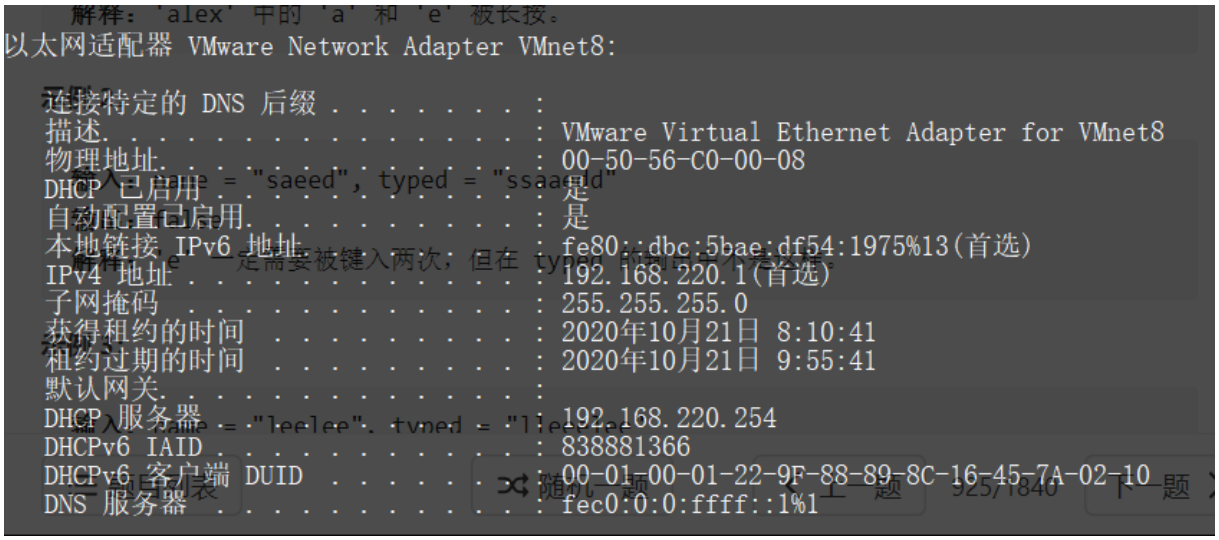


图 3: 同网段下的另一台主机的相关信息

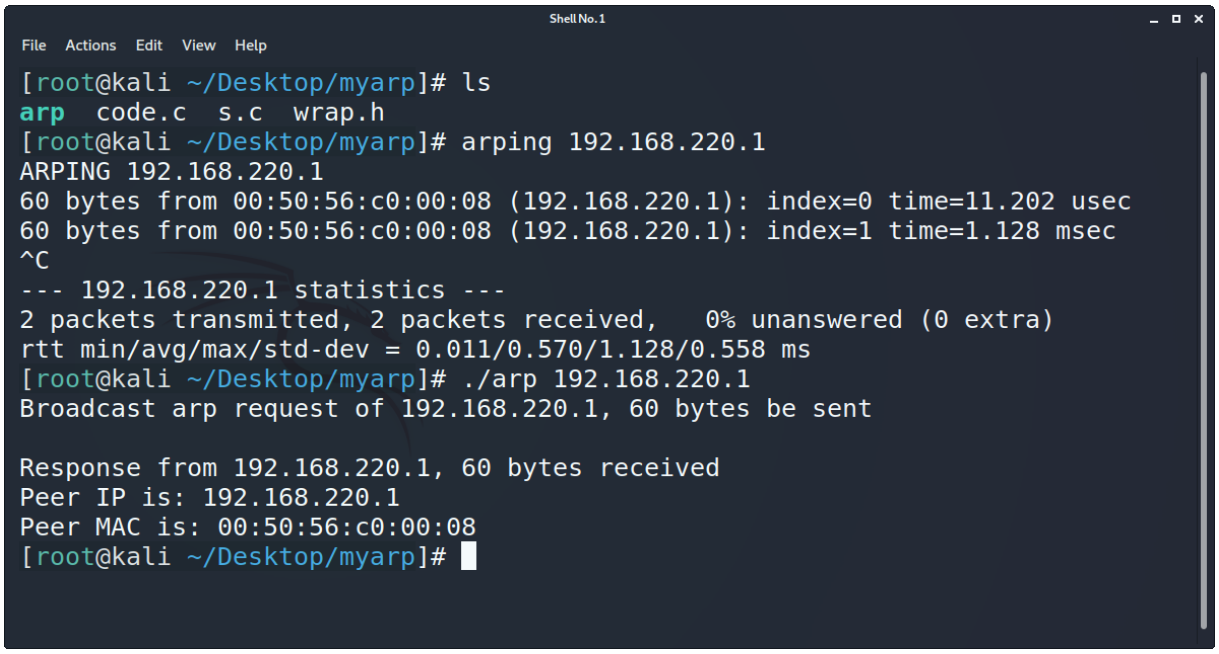


图 4: 利用 arping 命令和小程序分别发送 arp 包获得 192.168.220.1 主机的 MAC 地址