# 以太网完整协议（一）_yundanfengqing_nuc的专栏-CSDN博客_以太网协议

一、以太网中数据帧结构

以太网是目前最流行的一种局域网组网技术（其他常见局域网组网技术还有令牌环局域网、无线局域网、ATM局域网），以太网技术的正式标准是IEEE 802.3标准，它规定了在以太网中传输的数据帧结构，如下图所示。

| 前同步码 | SFD | 目的地址 | 源地址 | 长度/类型 | 数据和填充 | CRC |
|---|---|---|---|---|---|---|
| 7 字节 | 1 字节 | 6 字节 | 6 字节 | 2 字节 | 46 字节~1500 字节 | 4 字节 |

在物理层上看，一个完整的以太网帧有7个字段，事实上，前两个字段并不能算是真正意义上的以太网数据帧，它们是以太网在物理层上发送以太网数据时添加上去的。为了实现底层数据的正确阐述，物理层使用7个字节前同步码（0和1交替的56位（55-55-55-55-55-55-55-55））实现物理层帧输入/输出同步；使用1个字节的SFD（帧首定界符，固定为10101011）标识帧的开始。上图中剩下的5个字段是真正的以太网数据，其中包含了目的地址和源地址，它们都是6字节长度（通常每个网卡都有1个6个字节MAC地址，以在以太网中唯一地标识自己）。网卡接收数据时，通过将目的地址字段和自身的MAC地址做比较，判断是否接收该数据包。通常，将这里的6字节目的地址按照下面的格式来书写，如：00-01-02-03-04-05。这6个字节在以太网中是按照从左到右的顺序发送的，同时对每个字节来说，最先发送的是最低位bit0，最后是最高位bit7。

在以太网帧中，目的地址可以分为三类：单播地址、多播地址和广播地址。单播地址通常与一个具体网卡的MAC地址相对应，它要求第一个字节的bit0（即最先发出去的位）必须是0；多播地址则要求第一个字节的bit0为1，这样，在网络中多播地址不会与任何网卡的MAC相同，多播数据可以被很多个网卡同时接收；广播地址的所有48位全为1（即FF-FF-FF-FF-FF-FF），同一局域网中的所有网卡可以接收广播数据包。

上图中的长度/类型具有两个意义，当这两个字节的值小雨1518时，那么它就代表其后数据字段的长度；如果这两个字节的值大于1518，则表示该以太网帧中的数据属于哪个上层协议（例如0x800，代表IP数据包；0x806，代表ARP数据包等。）

在使用网卡进行数据包的发送与接收时，网卡已为我们完成了物理层的所有工作，驱动程序要做的是，在发送数据时，将目的地址、源地址、类型/长度、数据和填充这些值写入网卡，网卡自动计算其CRC并添加在数据帧尾部，同时对数据帧进行物理层的封装，最后将数据帧发送出去；在接收数据时，网卡会自动检测并接收数据包，验证校验和并把上述四个字段的值放在内部SRAM中供控制器读取。

TCP/IP协议有自己的地址：32bit的IP地址（网络地址），网络层发送数据包时只知道目的地址的IP地址，而底层接口（如以太网驱动程序）必须知道对方的硬件地址才能将数据发送出去。

二、ARP协议

ARP的功能是在32bit的IP地址和采用不同网络技术的硬件地址之间提供动态映射，为上层将底层的物理地址差异屏蔽起来，这样上层的因特网协议就可以灵活地使用IP地址进行通信了。ARP协议的基本功能是使用目标主机的IP地址，查询其对应的MAC地址，以保证底层链路上数据包通信的进行。为了实现在网络接口物理地址与IP地址间的转换，ARP协议中引入了ARP缓存表的概念。ARP缓存表中记录了一条一条的<IP地址，MAC地址>对，他们是主机最近运行获得的关于周围其他主机的IP地址到物理地址的绑定，当需要发送IP数据包时，ARP层根据目的IP地址来查找ARP缓存表，并将匹配的MAC地址装入以太网帧首部，最后发送以太网数据。

ARP缓存表的建立与ARP数据包是密切相关的。在以太网中，ARP数据包和IP数据包是两个独立的部分，它们都封装在以太网帧中发送。ARP数据包的种类有两种：一是ARP请求包，它是通过以太网广播的方式发送的，用于向具有某个IP地址的主机发送请求，希望该主机返回其MAC地址；二是ARP应答包，收到ARP请求的主机会比对该数据包中的IP地址与自己的IP地址是否符合，若是，则该主机向源主机返回一个ARP应答包。向源主机报告自己的MAC地址。源主机通过提取ARP应答包中的相关字段来更新ARP缓存表。在Windows控制台上输入arp -a，可以查看操作系统中使用的ARP缓存表。

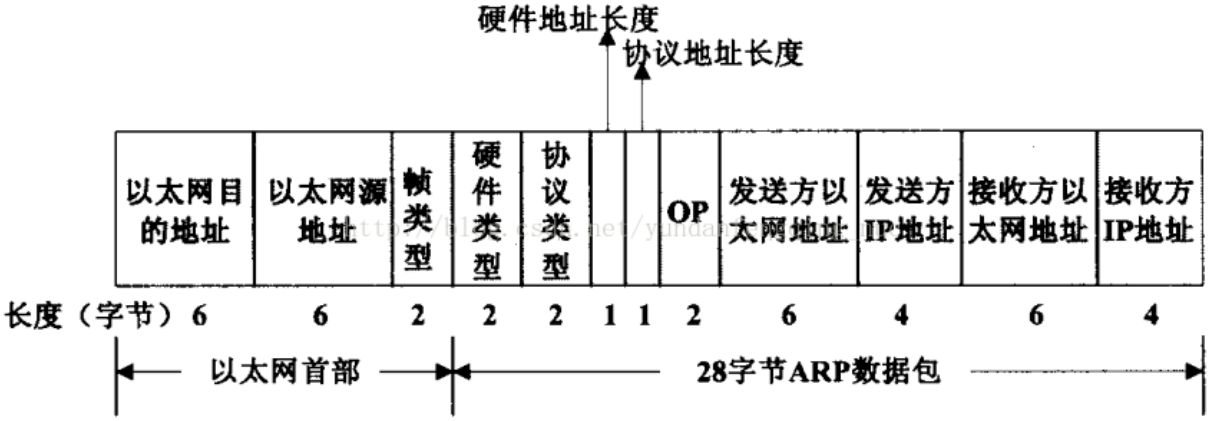
举一个简单的例子来看看ARP的功能。假如我们的主机（192.168.1.11）需要向开发板（192.168.1.37）发送一个IP数据包，当发送数据时，主机会在自己的ARP缓存表中寻找是否有目标IP地址。如果找到了，也就知道了目标MAC地址为（04-02-35-00-00-01），此时，主机直接把目标MAC地址写入以太网首部发送就可以了；如果在ARP缓存表中没有找到相对应的IP地址，此时比较不幸，我们的数据需要被延迟发送，随后主机会先在网络上发送一个广播（ARP请求，以太网目的地址为FF-FF-FF-FF-FF-FF），广播的ARP请求表示同一网段内所有主机将会收到这样一条信息：“192.168.1.37的MAC地址是什么？请回答”。网络IP地址为192.168.1.37（开发板）的主机接收到这个帧后，它有义务做出这样的回答（ARP应答）：“192.168.1.37的MAC地址是（04-02-35-00-00-01）”。这样，主机就知道了开发板的MAC地址，先前被延时的数据包就可以被发送了，此外，主机将这个地址对保存在缓存表中，以便后续数据包发送时使用。

ARP协议的核心就是对ARP缓存表的操作。发送数据包时，查找缓存表以得到目的MAC地址，此外，ARP还需要不断地处理ARP请求包和ARP应答包，以保证缓存表中各个表项的有效性。ARP的实质就是对缓存表的建立、更新、查询等操作。

2.2 ARP报文

要在源主机上建立关于目标主机的IP地址与MAC地址对应表项，则源主机和目的主机的基本信息交互式必须的，简单地说就是，源主机如何告诉目的主机：我需要你的MAC地址；而目的主机如何回复：这就是我的MAC地址。这时ARP报文（ARP数据包）就派上用场了。

ARP请求和ARP应答都是被组装在一个ARP数据包中发送的，ARP包的组成结构如下图所示。需要注意的是：ARP包时被封装在以太网帧中发送的，所以在图中也列出了以太网帧头部。




以太网帧头部中的前两个字段是以太网的MAC地址和源MAC地址，目的地址为全1的特殊地址是以太网广播地址。在ARP表项建立前，源主机只知道目的主机的IP地址，并不知道其MAC地址，所以在数据链路上，源主机只有通过广播的方式将ARP请求数据包发送出去，同一网段上的所有以太网接口都会接收到广播的数据包。

两个字节长的以太网帧类型表示帧中数据的类型。对于ARP包来说，该字段值为0x0806；对IP包来说，该字段的值为0x0800。接下来就是ARP数据包部分了，第一个硬件类型字段表示发送方想要知道的硬件接口类型，对于以太网MAC地址，它的值为1.协议类型字段表示要映射的协议地址类型，它的值为0x0800时，即表示要映射为IP地址，该值与以太网数据帧头中的类型字段的值使用相同的一组值。

接下来的两个单字节长度的字段，称为硬件地址长度和协议地址长度，它们分别指出硬件地址和协议地址的长度，长度单位为字节。对于以太网上ARP请求或应答来说，它们的值分别为6和4，代表MAC地址的长度和IP地址的长度。在ARP协议包中流出硬件地址长度和协议地址长度字段可以使得ARP协议在任何网络中被使用，而不仅仅只在以太网中。

操作字段op指出ARP数据包的类型，它们可以使ARP请求（值为1）、ARP应答（值为2）。

接下来的四个字段是发送端的以太网MAC地址、发送端的IP地址、目的端的以太网MAC地址和目的端的IP地址。

注意，这里有一些重复信息：在以太网的数据帧头部中和 ARP 数据包中都有发送端的以太网 MAC 地址。对于一个 ARP 请求包来说，除接收方以太网地址外的所有字段都应该被填充相应的值。当接收方主机收到一份给自己的 ARP 请求报文后，它就把自己的硬件地址填进去，然后将该请求数据包的源主机信息和目的主机信息交换位置，并把操作字段 op 置为 2，最后把该新构建的数据包发送回去，这就是 ARP 应答。

ARP 和 IP 是两个相互独立的协议，它们都属于网络层上的协议，从分层结构上看，ARP 应该处于更底层，因为没有 ARP 提供的映射功能，IP 数据包无法在以太网上发送。