

# 以太网帧格式及ARP协议简介

[基于FPGA的以太网相关文章导航，点击查看。](#)

---

在以太网中，一个主机和另一个主机进行通信，必须要知道目的主机的MAC地址（**物理地址**），只要知道目的主机的IP地址，就可以通过ARP协议获取目的主机的MAC地址。

## 1、ARP协议简介

ARP（Address Resolution Protocol），即地址解析协议，是根据IP地址（逻辑地址）获取MAC地址的一种TCP/IP协议。在以太网通信中，数据是以“帧”的格式进行传输的，帧格式里面包含目的主机的MAC地址。

源主机的应用程序知道目的主机的IP地址，却不知道目的主机的MAC地址。而目的主机的MAC地址直接被网卡接收和解析，当解析到目的MAC地址非本地MAC地址时，则直接丢弃该包数据，因此在通信前需要先获得目的MAC地址，而ARP协议正是实现了此功能。

下图是OSI七层网络模型，ARP处于第二层，ICMP处于第三层，UDP协议处于第四层。

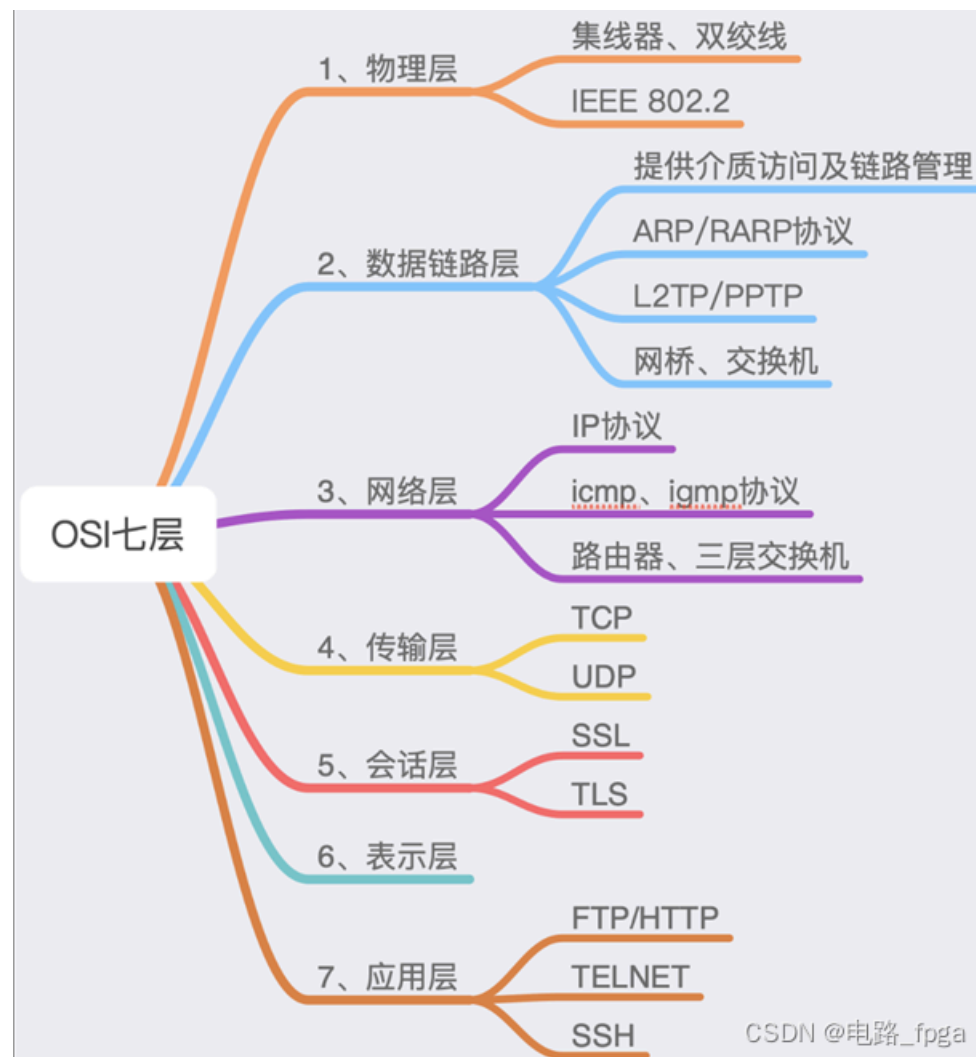


图1 OSI七层模型

ARP协议的基本功能是通过目的主机IP地址，获取目的主机的MAC地址，以保证通信的顺利进行。MAC地址在网络中表示网卡的ID，每个网卡都需要并有且仅有一个MAC地址。在获取到目的MAC地址之后，将目的MAC地址更新至ARP缓存表中，称为ARP映射。下次通信时，可以直接从ARP缓存表中获取，而不用重新通过ARP获取MAC地址。但一般ARP缓存表会有过期时间，过期后需要重新通过ARP协议进行获取。

ARP映射是指将IP地址和MAC地址映射起来，分为静态映射和动态映射。

静态映射指手动创建一张ARP表，把IP地址和MAC地址关联起来。手动绑定之后，源主机在通信之前，可以从ARP表中找到IP地址对应的MAC地址。但存在局限性，因为MAC地址可能会变化，比如：主机可能更换NIC（网络适配器），改变物理地址；要避免类似问题出现，必须定期维护更新ARP表，会比较麻烦且影响网络性能。

动态映射指使用ARP协议来获取相对应的物理地址，此过程是自动完成的，故被称为动态映射。已经设计出用于实现动态映射协议的有ARP和RARP（逆地址解析协议）两种，ARP把IP地址映射为物理地址，RARP把物理地址映射为IP地址。RARP应用较少。

ARP协议分为ARP请求和ARP应答，源主机查询目的MAC地址的报文称为ARP请求，目的主机响应源主机并发送包含本地MAC地址的报文称为ARP应答。

当主机需要找出这个网络中的另一个主机的物理地址时，它就可以发送一个ARP请求报文，ARP请求报文包含了发送方的MAC地址和IP地址以及接收方的IP地址。因为不知道接收方的物理地址，用48'hff\_ff\_ff\_ff\_ff表示，称为广播地址。ARP请求如下图所示：



图2 ARP请求示意图

上图中ARP发送的是广播地址，所以该局域网内的所有电脑都会接收到该协议并且解析。将解析出的IP地址与自身IP地址对比，如果一致，就会把自身的IP和MAC地址打包，通过ARP应答格式回复主机A。如果不是自身IP地址，则不做任何处理。

主机B的IP地址是192.168.133.140，因此主机B会通过ARP应答将自身的IP地址和MAC发送给主机B，如下图所示。由于主机B可以从主机A发送的ARP请求中获取主机A的IP地址和MAC地址，所以主机B发出的ARP应答是单播数据包，只有主机A会接收到。

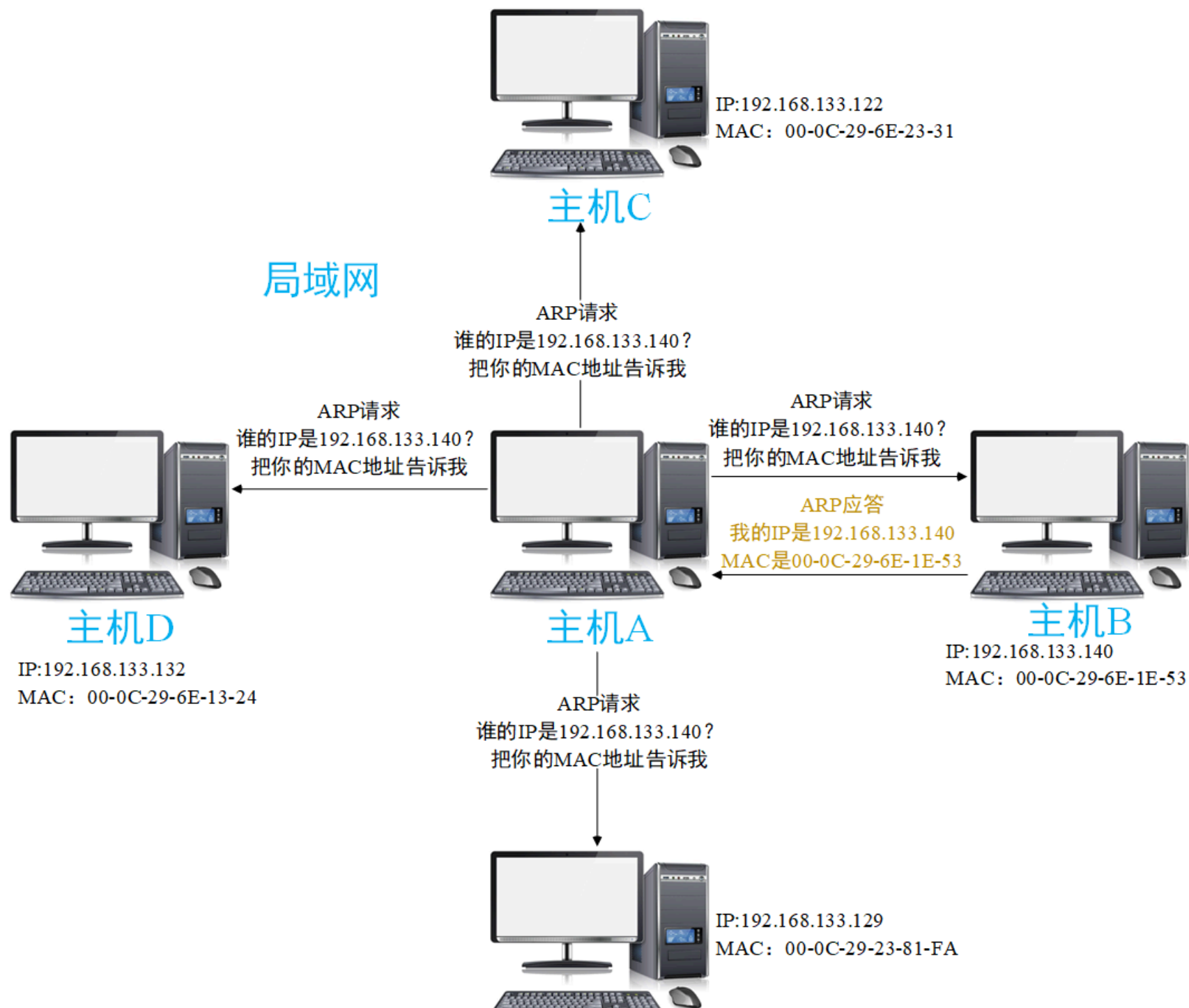


图3 ARP应答示意图

主机A解析收到的ARP应答报文中的目的MAC地址，将目的MAC地址和目的IP地址更新至ARP缓存表中。当再次和主机B通信时，直接从ARP缓存表中获取主机B的IP地址和MAC地址，就不用重新发起ARP请求报文。ARP缓存表中的数据有过期时间（一般为20分钟），过期之后需要重新发起ARP请求以获取目的MAC地址。

## 2、以太网帧格式

ARP协议通过以太网传输，就必须按照以太网规定的格式进行传输，本节讲解以太网的帧格式。

下图就是以太网传输一帧数据的格式，即 **以太网帧格式**，主要分为前导码、帧起始符、以太网帧头、以太网数据、CRC校验五个部分。

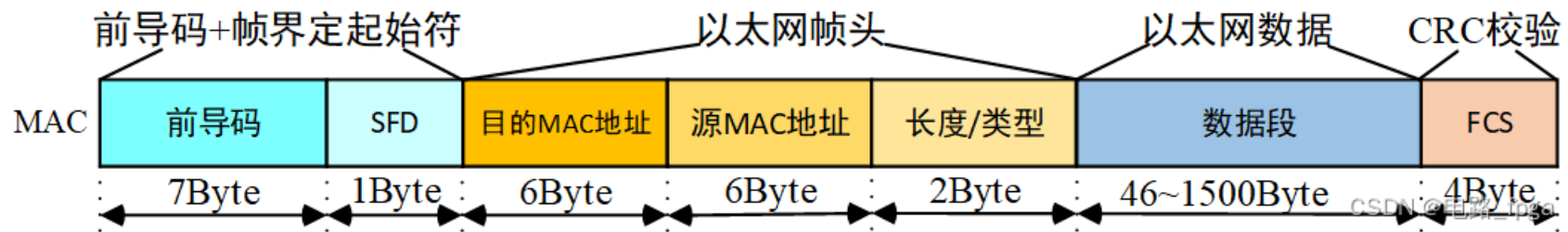


图4 以太网帧格式

**前导码（Preamble）**：7个字节的8'h55，也就是0、1交替出现，标志开始传输数据。

**帧起始符（SFD, Start Frame Delimiter）**：1个字节8'hd5表示一帧数据的开始。

14个字节的以太网帧头包括6个字节的**目的MAC地址**，6个字节的**源MAC地址**，2个字节的长度或者协议类型。

**目的MAC地址**：占用6个字节。MAC地址分为单播地址、组播地址和广播地址。单播地址：第一个字节的最低位为0，比如00-00-00-11-11-11，表示唯一的设备；组播地址：第一个字节的最低位为1，比如01-00-00-11-11-11，表示同属一组的多个设备；**广播地址为FF-FF-FF-FF-FF-FF，表示同一网段中的所有设备**。在ARP请求时，一般使用广播地址，因为源主机不知道目的主机的MAC地址。而ARP应答时，一般使用单播，因为源主机可以通过目的主机发送的ARP请求解析出目的主机的MAC地址。

主机对以太网的帧数据解析时，首先就会解析以太网帧头的目的MAC地址，如果该MAC地址为广播地址或者与自身的MAC地址一致，则继续解析该数据包，否则舍弃该数据包，不在往下解析。

**源MAC地址**：表示发送端的物理地址，占用6字节。

长度/类型：当这两个数据小于1536时，表示以太网数据段的长度，也就是以太网数据段有多少个字节的数据。如果这两个字节的值大于1536，表示该以太网中的数据属于哪个上层协议，例如0x0800代表IP协议、0x0806 代表ARP协议等。

数据段：以太网中的数据段长度最小46个字节，最大1500个字节。考虑多个计算机的数据帧排队等待时间、网络I/O控制器缓存区资源以及网络最大的承载能力等各种因素决定数据段传输的字节不能太大。

上层协议全部包含在以太网的数据段之中，包括后文的ARP协议、ICMP协议、UDP协议等等。

帧检验序列（FCS，Frame Check Sequence）：为确保正确传输数据，在数据的尾部加入4字节的循环冗余校验码（CRC校验）来检测数据是否传输错误。**CRC数据校验从以太网帧头开始，不包含前导码和帧起始界定符。**在网络通信系统中应用最广泛的是CRC-32标准。

网络设备和组件在接收一帧之后，需要短暂的时间来恢复并为接收下一帧做准备的时间，这段时间被称为帧间隙（IFG，Interpacket Gap）。IFG的最小值是96 bit time，也就是传输96字节所需要的时间，具体时间长度根据PHY的时钟周期有关。

### 3、ARP协议

前文对以太网帧格式进行了讲解，本小节对ARP协议的格式进行讲解，下图是以太网ARP数据包的格式，由图可知ARP存在于以太网数据包的数据段。ARP数据长度固定为28字节，由于以太网每次最少传输46字节数据，所以需要填充18字节的0，这18字节的0也要进行CRC校验。

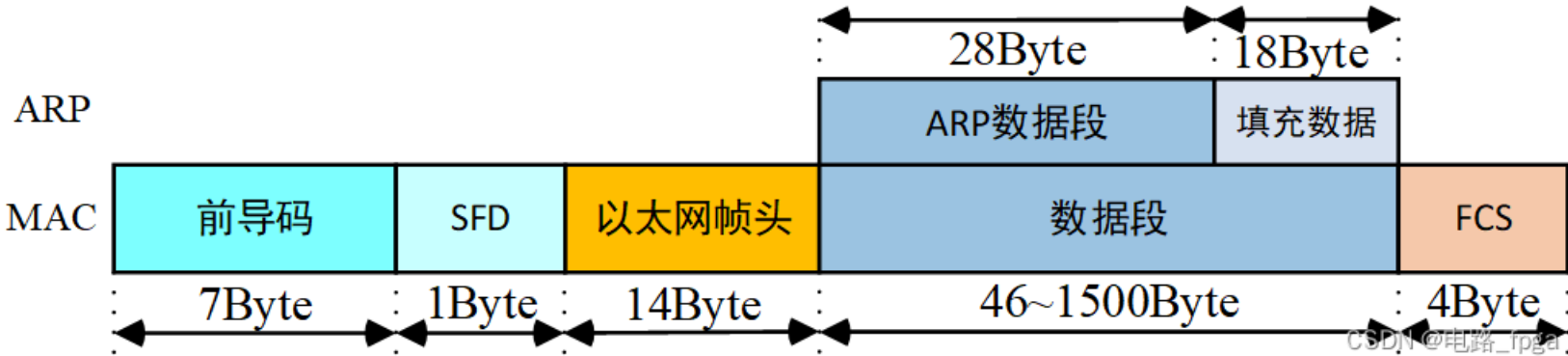


图5 ARP数据包格式

如果数据端是ARP数据，那么以太网帧头的最后两字节必须是0x0806，表示后续的是ARP协议数据包。

下图是28字节ARP数据包的构成，包括2字节的硬件类型、2字节的协议类型、1字节的硬件地址(MAC地址)长度、1字节的协议地址(IP协议地址)长度，6字节的源MAC和目的MAC地址，4字节的源IP和目的IP地址。



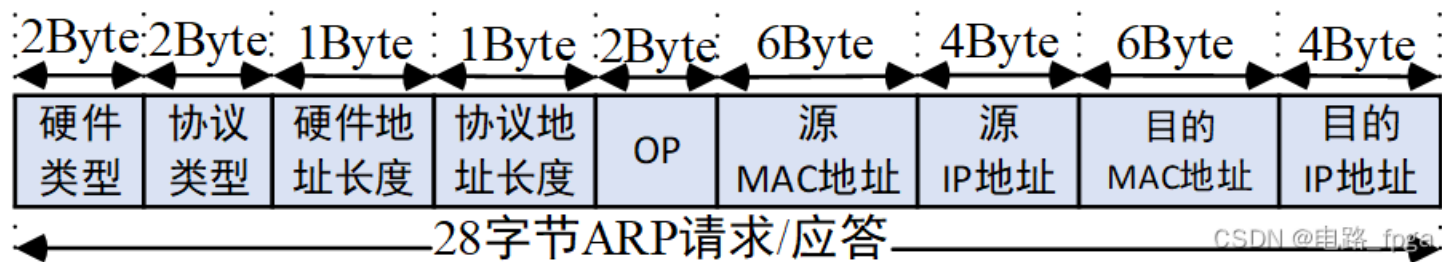


图6 ARP数据报构成

硬件类型 (Hardware type) : 为1表示以太网地址。

协议类型 (Protocol type) : ARP协议的上层协议为IP协议, 值为0x0800。

硬件地址长度 (Hardware size) : MAC地址的长度, 以字节为单位, 该值为6。

协议地址长度 (Protocol size) : IP地址的长度, 以字节为单位, 该值为4。

**OP (Opcode)** : 操作码, 表示该数据包为ARP请求或ARP应答。**1表示ARP请求, 2表示ARP应答。**

源MAC地址: 发送端的硬件地址。

源IP地址: 发送端的协议 (IP) 地址, 如 192.168.1.102。

目的MAC地址: 接收端的硬件地址, 在ARP请求时由于不知道接收端MAC地址, 理论上该字段为广播地址, 即48'hff\_ff\_ff\_ff\_ff。但实际上通过ILA抓取ARP请求数据可知, 该地址为0, 可能是目的主机不会解析该数据吧, 具体值是多少也就无所谓了。

目的IP地址: 接收端的协议 (IP) 地址, 如 192.168.1.10。

对以太网帧格式和ARP数据格式的讲解就到这里了, 下图是整合两者得到的ARP数据包格式。

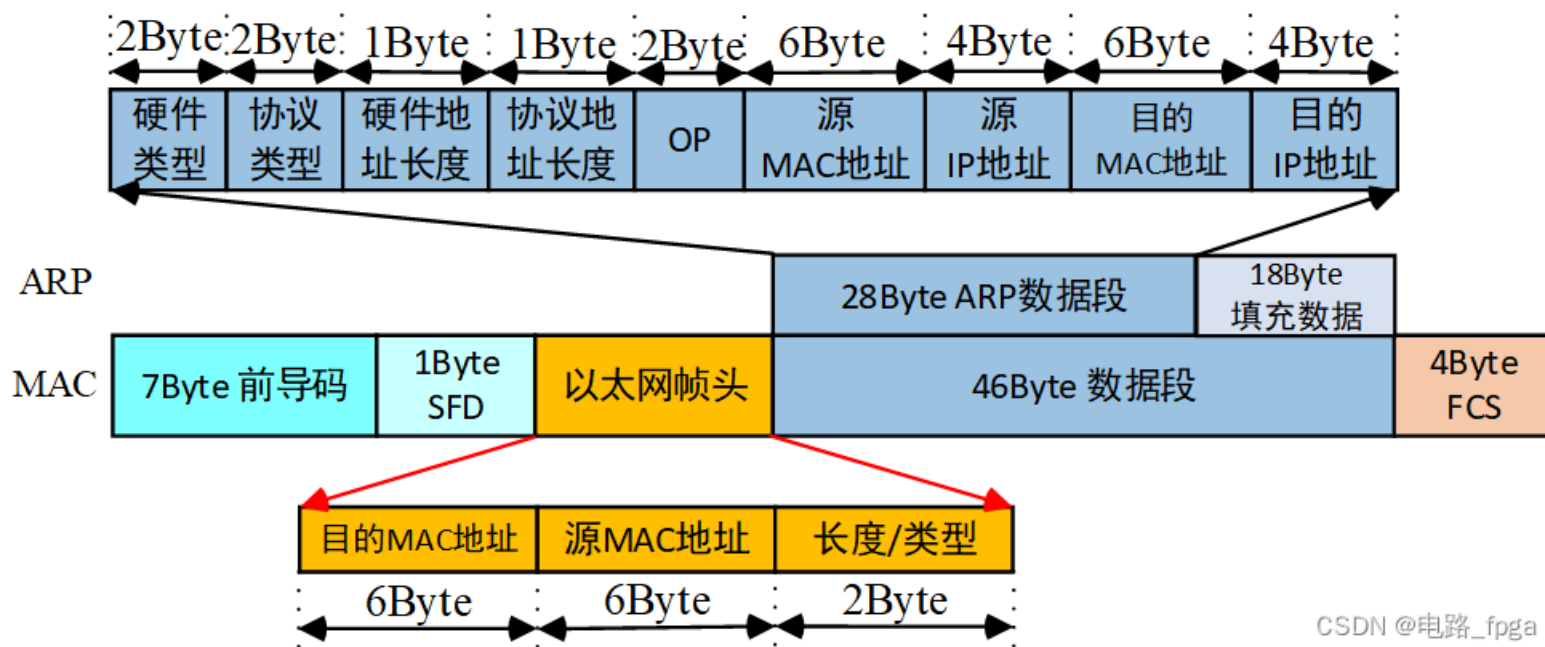


图7 ARP数据包格式

#### 4、总结

本文对以太网帧格式、ARP数据格式做了简要讲解，为后文 **FPGA** 实现ARP协议的解析和发送做基础，其实ICMP、UDP协议原理也都大体类似，稍微复杂一点。

解析ARP数据包，首先需要根据目的MAC地址，确认该数据包是不是发送给开发板的，如果是则继续解析，不是则丢弃。然后根据长度/类型，判断该数据包是否为ARP数据包，如果是则继续解析。

ARP数据段主要注意OP编码，确定接收到的是ARP请求还是ARP应答。然后解析出源主机的MAC地址和源主机的IP地址，作为后续ARP应答的目的MAC地址和目的IP地址。最后对接收到的数据进行CRC校验，确认接收数据无误。

如果接收到ARP请求，则应该向源主机发送ARP应答数据包，将开发板的MAC地址和IP地址发送给源主机，便于后续通信。

**您的支持是我更新的最大动力！将持续更新工程，如果本文对您有帮助，还请多多点赞👍、评论💬和收藏★！**