以太网数据包 TCP、IP、ICMP、UDP、ARP 协议头结构详解

以太网首部

目地 MAC 地址（8 字节）
源 MAC 地址（8 字节）
类型（2 字节）

1、IP 头的结构

版本（4 位）	头长度（4 位）	服务类型（8 位）	封包总长度（16 位）
封包标识（16 位）		标志（3 位）	片断偏移地址（13 位）
存活时间（8 位）	协议（8 位）	校验和（16 位）	
来源 IP 地址（32 位）			
目的 IP 地址（32 位）			
选项（可选）		填充（可选）	
数据			

（1）字节和数字的存储顺序是从右到左，依次是从低位到高位，而网络存储顺序是从左到右，依次从低位到高位。

（2）版本：占第一个字节的高四位。头长度：占第一个字节的低四位。

（3）服务类型：前 3 位为优先字段权，现在已经被忽略。接着 4 位用来表示最小延迟、最大吞吐量、最高可靠性和最小费用。

（4）封包总长度：整个 IP 报的长度，单位为字节。

（5）存活时间：就是封包的生存时间。通常用通过的路由器的个数来衡量，比如初始值设置为 32，则每通过一个路由器处理就会被减一，当这个值为 0 的时候就会丢掉这个包，并用 ICMP 消息通知源主机。

（6）协议：定义了数据的协议，分别为：TCP、UDP、ICMP 和 IGMP。定义为：

```
#define PROTOCOL_TCP        0x06

#define PROTOCOL_UDP        0x11
```

```
#define PROTOCOL_ICMP      0x06

#define PROTOCOL_IGMP      0x06
```

（7）检验和：校验的首先将该字段设置为 0，然后将 IP 头的每 16 位进行二进制取反求和，将结果保存在校验和字段。

（8）来源 IP 地址：将 IP 地址看作是 32 位数值则需要将网络字节顺序转化位主机字节顺序。转化的方法是：将每 4 个字节首尾互换，将 2、3 字节互换。

（9）目的 IP 地址：转换方法和来源 IP 地址一样。

在网络协议中，IP 是面向非连接的，所谓的非连接就是传递数据的时候，不检测网络是否连通。所以是不可靠的数据报协议，IP 协议主要负责在主机之间寻址和选择数据包路由。

2、ICMP 协议的头结构

类型（8 位）	代码（8 位）	校验和（8 位）
类型或者代码		

（1）类型：一个 8 位类型字段，表示 ICMP 数据包类型。（2）代码：一个 8 位代码域，表示指定类型中的一个功能。如果一个类型中只有一种功能，代码域置为 0。（3）检验和：数据包中 ICMP 部分上的一个 16 位检验和。

3、TCP 协议的头结构

来源端口（2 字节）			目的端口（2 字节）		
序号（4 字节）			确认序号（4 字节）		
头长度（4 位）			保留（6 位）		
URG	ACK	PSH	RST	SYN	PIN
窗口大小（2 字节）			校验和（16 位）		
紧急指针（16 位）			选项（可选）		
数据					

（1）TCP 源端口（Source Port）：16 位的源端口包含初始化通信的端口号。源端口和 IP 地址的作用是标识报文的返回地址。（2）TCP 目的端口（Destination Port）：16 位的目的端口域定义传输的目的。这个端口指明报文接收计算机上的应用程序地址接口。

（3）序列号（Sequence Number）：TCP 连线发送方向接收方的封包顺序号。

（4）确认序号（Acknowledge Number）：接收方回发的应答顺序号。

（5）头长度（Header Length）：表示 TCP 头的双四字节数，如果转化为字节个数需要乘以 4。

（6）URG：是否使用紧急指针，0 为不使用，1 为使用。

（7）ACK：请求/应答状态。0 为请求，1 为应答。

（8）PSH：以最快的速度传输数据。

（9）RST：连线复位，首先断开连接，然后重建。

（10）SYN：同步连线序号，用来建立连线。

（11）FIN：结束连线。如果 FIN 为 0 是结束连线请求，FIN 为 1 表示结束连线。

（12）窗口大小（Window）：目的机使用 16 位的域告诉源主机，它想收到的每个 TCP 数据段大小。

（13）校验和（Check Sum）：这个校验和和 IP 的校验和有所不同，不仅对头数据进行校验还对封包内容校验。

（14）紧急指针（Urgent Pointer）：当 URG 为 1 的时候才有效。TCP 的紧急方式是发送紧急数据的一种方式。

4、UDP 协议的头结构

源端口（2 字节）	目的端口（2 字节）
封报长度（2 字节）	校验和（2 字节）
数据	

（1）源端口（Source Port）：16 位的源端口域包含初始化通信的端口号。源端口和 IP 地址的作用是标识报文的返回地址。（2）目的端口（Destination Port）：6 位的目的端口域定义传输的目的。这个端口指明报文接收计算机上的应用程序地址接口。（3）封包长度（Length）：UDP 头和数据的总长度。（4）校验和（Check Sum）：和 TCP 和校验和一样，不仅对头数据进行校验，还对包的内容进行校验。

5、ARP 报头结构

硬件类型		协议类型
硬件地址长度	协议长度	操作类型
发送方的硬件地址（0-3 字节）		

源物理地址（4-5 字节）	源 IP 地址（0-1 字节）
源 IP 地址（2-3 字节）	目标硬件地址（0-1 字节）
目标硬件地址（2-5 字节）	
目标 IP 地址（0-3 字节）	

（1）硬件类型字段指明了发送方想知道的硬件接口类型，以太网的值为 1；（2）协议类型字段指明了发送方提供的高层协议类型，IP 为 0800（16 进制）；（3）硬件地址长度和协议长度指明了硬件地址和高层协议地址的长度，这样 ARP 报文就可以在任意硬件和任意协议的网络中使用；（4）操作字段用来表示这个报文的类型，ARP 请求为 1，ARP 响应为 2，RARP 请求为 3，RARP 响应为 4；（5）发送方的硬件地址（0-3 字节）：源主机硬件地址的前 3 个字节；（6）发送方的硬件地址（4-5 字节）：源主机硬件地址的后 3 个字节；（7）发送方 IP（0-1 字节）：源主机硬件地址的前 2 个字节；（8）发送方 IP（2-3 字节）：源主机硬件地址的后 2 个字节；（9）目的硬件地址（0-1 字节）：目的主机硬件地址的前 2 个字节；（10）目的硬件地址（2-5 字节）：目的主机硬件地址的后 4 个字节；（11）目的 IP（0-3 字节）：目的主机的 IP 地址。

ARP 的工作原理如下：

1. 首先，每台主机都会在自己的 ARP 缓冲区(ARP Cache)中建立一个 ARP 列表，以表示 IP 地址和 MAC 地址的对应关系。

2. 当源主机需要将一个数据包要发送到目的主机时，会首先检查自己 ARP 列表中是否存在该 IP 地址对应的 MAC 地址，如果有，就直接将数据包发送到这个 MAC 地址；如果没有，就向本地网段发起一个 ARP 请求的广播包，查询此目的主机对应的 MAC 地址。此 ARP 请求数据包里包括源主机的 IP 地址、硬件地址、以及目的主机的 IP 地址。

3. 网络中所有的主机收到这个 ARP 请求后，会检查数据包中的目的 IP 是否和自己的 IP 地址一致。如果不相同就忽略此数据包；如果相同，该主机首先将发送端的 MAC 地址和 IP 地址添加到自己的 ARP 列表中，如果 ARP 表中已经存在该 IP 的信息，则将其覆盖，然后给源主机发送一个 ARP 响应数据包，告诉对方自己是它需要查找的 MAC 地址；

4. 源主机收到这个 ARP 响应数据包后，将得到的目的主机的 IP 地址和 MAC 地址添加到自己的 ARP 列表中，并利用此信息开始数据的传输。如果源主机一直没有收到 ARP 响应数据包，表示 ARP 查询失败