IP协议及ICMP协议简介

基于FPGA的以太网相关文章导航，点击查看。

以前常常看见“为什么我的电脑ping不同 FPGA ?“，当时也没有了解过以太网协议，也不知道是什么含义。其实就是ICMP协议的查询功能，用来检测网络是否畅通。ICMP协议主要功能就是确认IP包是否成功到达目的地址，通知在发送过程中IP包被丢弃的原因。

新搭建好的网络需要先通过一个简单的测试来验证网络是否畅通。但是IP协议并不提供可靠传输，如果丢包，IP协议并不能通知传输层是否丢包以及丢包的原因，就需要 ICMP协议 来完成这样的功能。

ICMP大致分为差错报文和查询报文两种，差错报文又分为目的不可达，数据报超时等。常见的ICMP查询报文：回送请求或回答、时间戳请求或回答、路由器询问和通告、信息请求或回答、地址掩码请求或回答。

其中ping指令就与回送请求或回答有关。本文也只对回显请求或应答格式进行详细讲解。

1、IP报文

ICMP报文位于IP报文的数据段，下图是以太网的ICMP数据报文格式，IP协议位于以太网帧数据段，而ICMP位于IP数据段，在讲解ARP协议时对前导码、帧起始符、以太网帧头、FCS都做了详细讲解。所以本文需要对IP首部(至少20字节)、ICMP首部(至少8字节)、ICMP数据端做详细介绍。

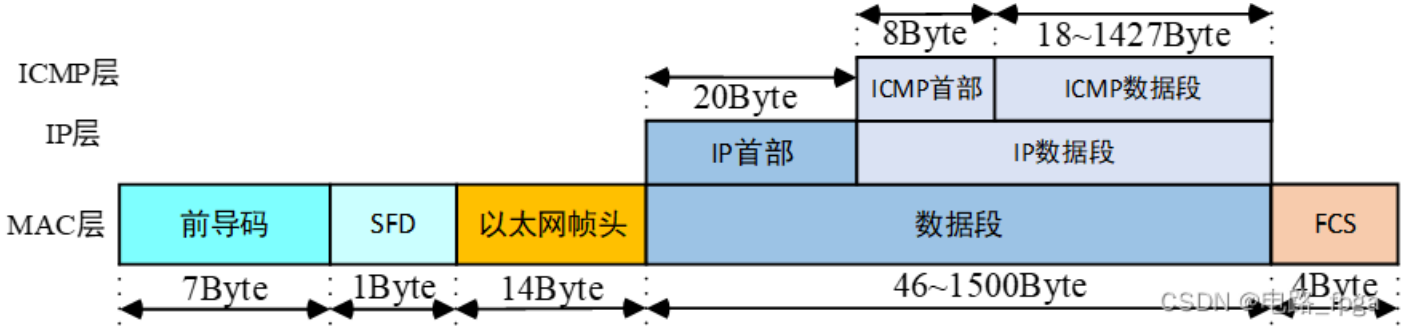

图1 ICMP的报文格式

首先是IP首部，其组成如下所示，这是IP首部最短的组成方式，也是最常见的方式。

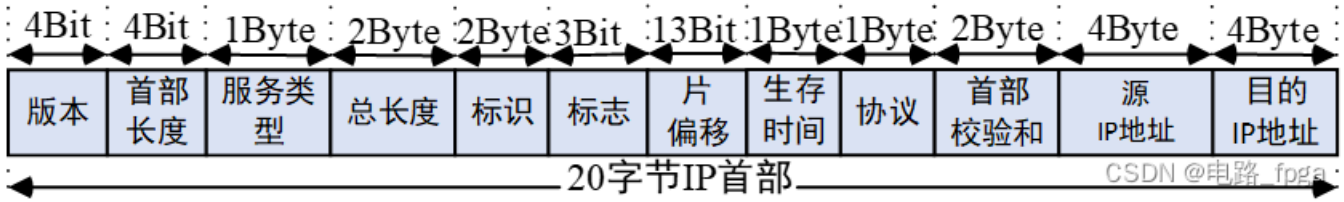

图2 IP首部组成

更常见的是如下图所示方式进行排列。

图3 IP报文格式

常见的就20个字节的IP首部，从左往右，从上往下开始发送数据。

版本（Version）：4位数据表示IP版本号，为4时表示IPv4，为6时表示IPv6，IPv4使用较多。

首部长度（IHL，Internet Header Length）：**4位数据表示IP首部一共有多少个32位（4个字节）数据。** 没有可选字段的IP首部长度为20个字节，故首部长度为5。

服务类型（TOS，Type of service）：8位服务类型被划分成两个子字段：3位优先级字段和4位TOS字段，最后一位固定为0。**服务类型为0时表示一般服务。**

总长度（Total Length）：**16位IP数据报总长度包括IP首部和IP数据部分，以字节为单位。** 利用IP首部长度和IP数据报总长度可以计算出IP数据报中数据内容的起始位置和长度。

标识字段（Identification）：16位标识字段，用来标识主机发送的每一份数据报。**每发送一份报文它的值就会加1。**

标志字段（Flags）：3位标志字段的第1位是保留位，第2位表示禁止分片（1表示不分片，0允许分片），第3位标识更多分片，通常为010不分片。

片偏移（Fragment Offset）：13位片偏移，在接收方进行数据报重组时用来标识分片的顺序。

生存时间（TTL，Time To Live）：8位生存时间防止丢失的数据包在无休止的传播，**一般被设置为64或者128。**

协议（Protocol）：8位协议类型表示此数据报所携带上层数据使用的协议类型，**ICMP为1，TCP为6，UDP为17。**

首部校验和（Header Checksum）：16位首部校验和，**该字段只校验数据报的首部，不包含数据部分；**

源IP地址（Source Address）：32位发送端的IP地址。

目的IP地址（Destination Address）：32位接收端的IP地址。

可选字段：是数据报中的一个可变长度的可选信息，选项字段以32bit为界，不足时插入值为0的填充字节，保证IP首部始终是32bit的整数倍。

前文对IP首部的各个参数含义做了详细讲解，通过下图的数据来讲解首部校验和的计算规则。

首部校验和的计算规则为：首先假设16位检验和为0，然后将IP首部按照16位分成多个单元，把所有单元相加，如果得到的低16位数据出现进位，则把低16位数据与高16位数据相加，相加后如果低16位还有进位，则继续把低16位与高16位数据相加，然后低16位数据取反得到首部校验和。

图4 IP首部数据

例如上图发送总长度为500个字节的IP数据报，发送端IP地址为192.168.1.189，接收端IP地址为192.168.1.10，则IP首部数据如下：

按照上述提到的 IP 首部校验和的方法计算 IP 首部校验和，即：

16’h4500 + 16’h01f4 + 16’h0000 + 16’h4000 + 16’h4001 + 16’h0000(计算时为0) + 16’hc0a8 + 16’h01bd + 16’hc0a8 + 16’h010a = 32’h00024b0c（低16位出现进位）。

16’h0002 + 16’h4b0c = 32’h00004b0e（低16位未出现进位）。

16’h0000 + 16‘h4b0e = 32’h00004b0e（低16位未出现进位）

最终得到校验码check_sum = ~16‘h4b0e = 16’b4f1

其实第一次相加低16位可能出现进位，取相加后的低16位与高16位相加结果也可能出现进位，相加结果的高低位相加两次后就不可能出现进位了，所以在程序设计时，就直接把第一次的计算结果的高16位数据与低16位数据相加两次后得到的低16位数据取反，得到首部校验和，省去判断进位的步骤，简化代码。

IP首部的讲解就到此结束了。

2、ICMP报文

一帧ICMP的报文格式如下图所示，包含IP首部、ICMP首部、ICMP数据三部分，前文已经对IP首部做了详细讲解，本小节对ICMP首部进行讲解。

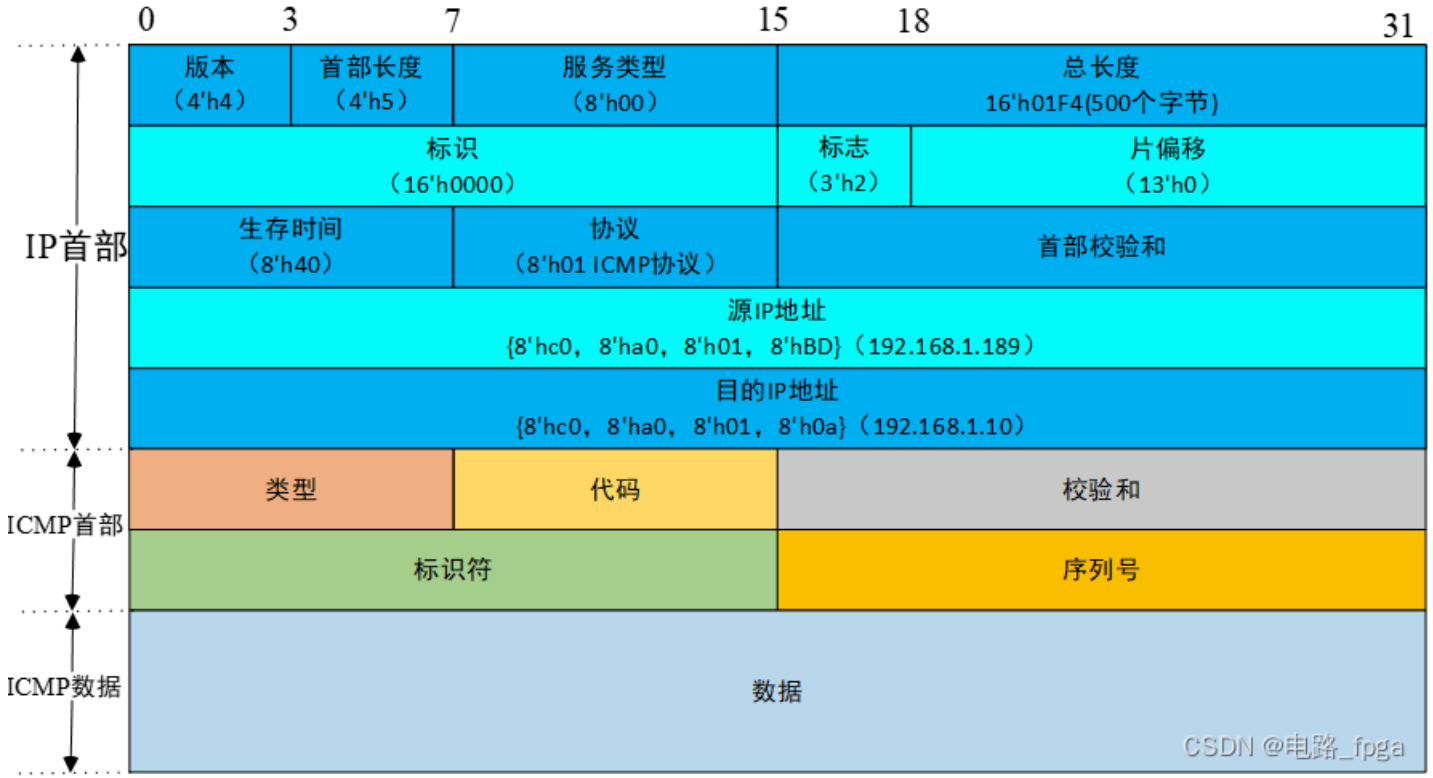

图5 一帧ICMP报文

下图是ICMP报文的首部和数据格式，注意ICMP首部的组成与该报文的类型和功能有关，下图是回显请求或应答的格式，ICMP其余功能可以查看ICMP报文格式获取，链接为RFC 777 - Internet Control Message Protocol (ietf.org)和RFC 777 - Internet Control Message Protocol (ietf.org)。

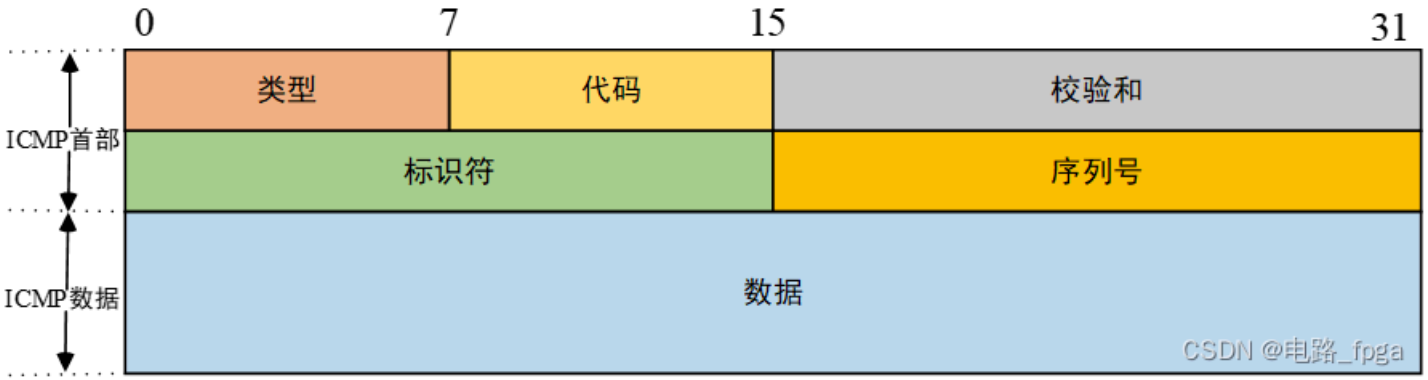

图6 ICMP数据报格式

ICMP首部总共8个字节，所以可以通过IP首部的总长度和IP首部长度、ICMP首部长度计算出ICMP数据长度。

类型(type)：8位数表示错误类型的差错报文或者查询类型的报告报文。通常与代码结合使用

代码(code)：占用8位数据，根据ICMP差错报文的类型，进一步分析错误的原因。下表就是代码和类型部分组合的含义，后文主要使用回显请求和回显应答。

表1 部分报文类型与代码对应的含义

种类	类型	代码	报文含义
查询报文	0	0	回显应答(ping应答)
查询报文	8	0	回显请求(ping请求)
差错报文	3	0	网络不可达
差错报文	3	1	主机不可达
差错报文	3	2	协议不可达
差错报文	3	3	端口不可达
差错报文	3	7	目的主机未知
差错报文	12	0	坏的IP首部
差错报文	12	1	缺少必须选项

校验和(checksum)：16 位校验和的计算方法与IP首部校验和计算方法一致，**该校验和需要对ICMP首部和ICMP数据做校验。**

标识符(Identifier)：16位标识符对每一个发送的数据报进行标识。

序列号(Sequence number)：16位对发送的每一个数据报文进行编号。

标识符和序列号其实是为了区分相同类型的不同两个数据报，比如主机A向主机B发送了两个回显请求，然后主机B针对两个回显请求分别做了回显应答。

回显应答的标识符和序列号必须与回显请求中的标识符和序列号保持一致， 这样主机A收到回显应答后，才知道主机B响应的是哪一个回显请求，进而对比回显应答数据与回显请求的数据是否一致，一致则表示ping成功，否则失败。

数据（Data）：要发送的ICMP数据，**注意回显应答数据段的数据必须与回显请求数据段的数据保持一致**，否则ping失败。

3、总结

本文对IP首部和ICMP数据报的组成以及校验和的计算做了相对详细的讲解，最终ICMP的数据格式如下图所示。

注意ICMP属于IP协议，所以以太网帧头的长度/类型为16'h0800，然后就是跟IP首部内容，由于ICMP位于IP的数据段，所以IP首部的协议类型为8'd1。之后需要把ICMP回显请求报文的标识符、序列号、ICMP数据保存，便于ICMP回显应答时使用。

同时可以计算出数据段的校验和，便于后续发送回显应答时ICMP校验和的计算。

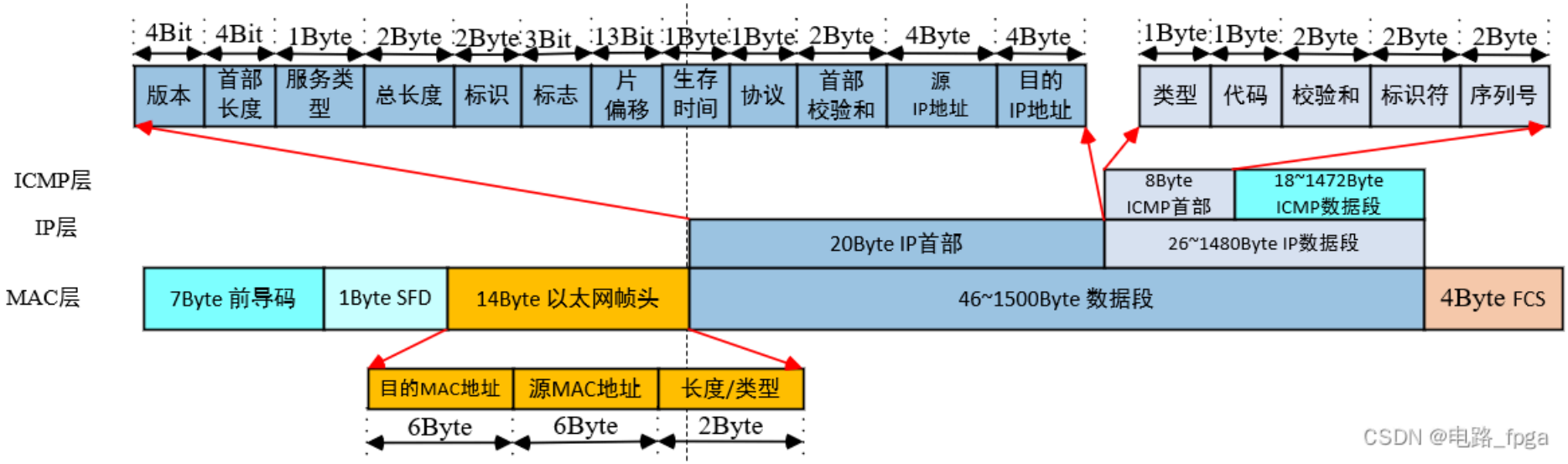

图7 ICMP数据报格式

后文通过FPGA实现ICMP的回显请求检测及回显应答功能。

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⭐！