ICMP协议是一个网络层协议。

一个新搭建好的网络，往往需要先进行一个简单的测试，来验证网络是否畅通；但是IP协议并不提供可靠传输。如果丢包了，IP协议并不能通知传输层是否丢包以及丢包的原因。

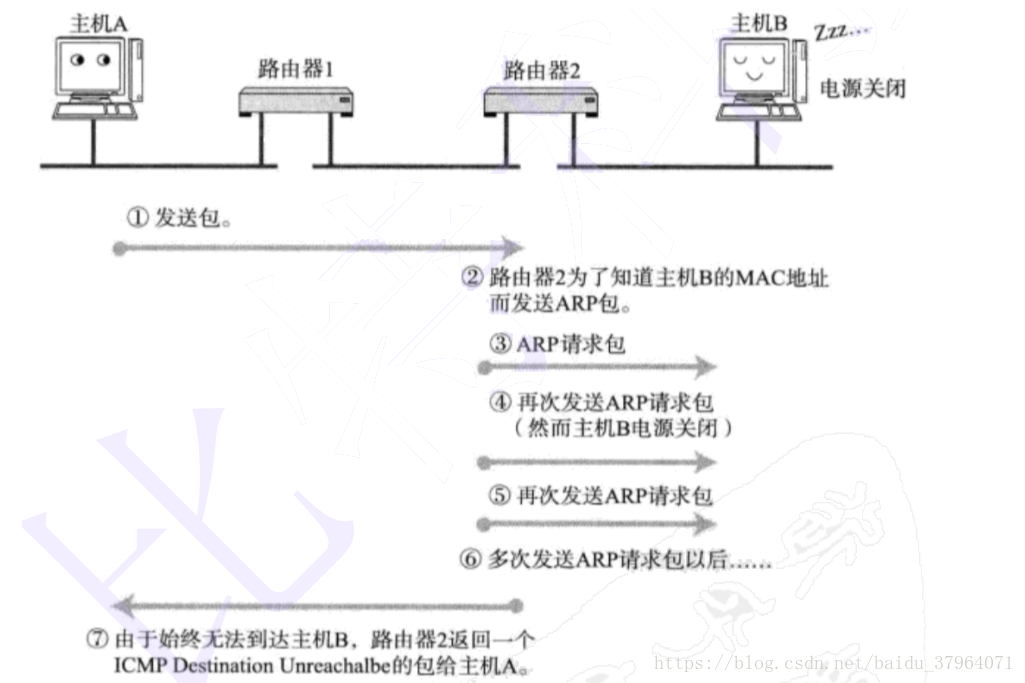
所以我们就需要一种协议来完成这样的功能–ICMP协议。

ICMP协议的功能

ICMP协议的功能主要有：

1. 确认IP包是否成功到达目标地址

2. 通知在发送过程中IP包被丢弃的原因

如下图所示：

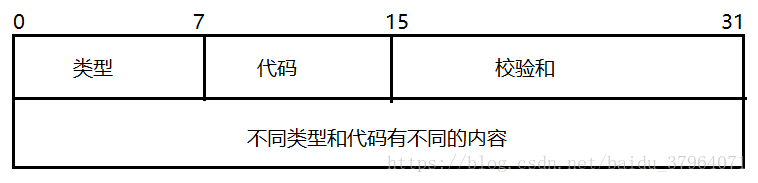
我们需要注意几点：

1.ICMP是基于IP协议工作的，但是它并不是传输层的功能，因此仍然把它归结为网络层协议

2. ICMP只能搭配IPv4使用，如果是IPv6的情况下, 需要是用ICMPv6

ICMP的报文格式

ICMP报文包含在IP数据报中，IP报头在ICMP报文的最前面。一个ICMP报文包括IP报头（至少20字节）、ICMP报头（至少八字节）和ICMP报文（属于ICMP报文的数据部分）。当IP报头中的协议字段值为1时，就说明这是一个ICMP报文。ICMP报头如下图所示。

如下图：

字段说明：

|  |  |
| --- | --- |
| 类型 | 说明 |
| 类型 | 占一字节，标识ICMP报文的类型，从类型值来看ICMP报文可以分为两大类。第一类是取值为1~127的差错报文，第2类是取值128以上的信息报文 |
| 代码 | 占一字节，标识对应ICMP报文的代码。它与类型字段一起共同标识了ICMP报文的详细类型 |
| 校验和 | 这是对包括ICMP报文数据部分在内的整个ICMP数据报的校验和，以检验报文在传输过程中是否出现了差错（其计算方法与在我们介绍IP报头中的校验和计算方法是一样的） |

ICMP大概分为两类报文：

一类是通知出错原因 ；一类是用于诊断查询

类型及含义如下：

|  |  |
| --- | --- |
| 类型（十进制） | 内容 |
| 0 | 回送应答 |
| 3 | 目标不可达 |
| 4 | 原点抑制 |
| 5 | 重点向或改变路由 |
| 8 | 回送请求 |
| 9 | 路由器公告 |
| 10 | 路由器请求 |
| 11 | 超时 |
| 17 | 地址子网请求 |
| 18 | 地址子网应答 |

常见的ICMP报文

相应请求

我们用的ping操作中就包括了相应请求（类型字段值为8）和应答（类型字段值为0）ICMP报文。

过程：

一台主机向一个节点发送一个类型字段值为8的ICMP报文，如果途中没有异常（如果没有被路由丢弃，目标不回应ICMP或者传输失败），则目标返回类型字段值为0的ICMP报文，说明这台主机存在。

目标不可达，源抑制和超时报文

这三种报文的格式是一样的。

（1）目标不可到达报文（类型值为3）在路由器或者主机不能传递数据时使用。

例如：我们要连接对方一个不存在的系统端口（端口号小于1024）时，将返回类型字段值3、代码字段值为3的ICMP报文。

常见的不可到达类型还有网络不可到达（代码字段值为0）、主机不可达到（代码字段值为1）、协议不可到达（代码字段值为2）等等。

（2）源抑制报文（类型字段值为4，代码字段值为0）则充当一个控制流量的角色，通知主机减少数据报流量。由于ICMP没有回复传输的报文，所以只要停止该报文，主机就会逐渐恢复传输速率。

（3）无连接方式网络的问题就是数据报会丢失，或者长时间在网络游荡而找不到目标，或者拥塞导致主机在规定的时间内无法重组数据报分段，这时就要触发ICMP超时报文的产生。

超时报文（类型字段值为11）的代码域有两种取值：代码字段值为0表示传输超时，代码字段值为1表示分段重组超时。

时间戳请求

时间戳请求报文（类型值字段13）和时间戳应答报文（类型值字段14）用于测试两台主机之间数据报来回一次的传输时间。

传输时，主机填充原始时间戳，接受方收到请求后填充接受时间戳后以类型值字段14的报文格式返回，发送方计算这个时间差。

(有些系统不响应这种报文)