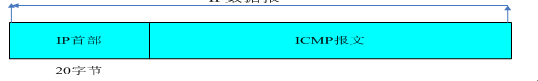
<https://blog.csdn.net/tigerjibo/article/details/7356936>



**一.概述：**

1.   ICMP允许主机或路由报告差错情况和提供有关异常情况。ICMP是因特网的标准协议，但ICMP不是高层协议，而是IP层的协议。通常ICMP报文被IP层或更高层协议（TCP或UDP）使用。一些ICMP报文把差错报文返回给用户进程。

2.   ICMP报文作为IP层数据报的数据，加上数据报的首部，组成数据报发送出去。

3.   ICMP报文的种类有两种，即ICMP差错报告报文和ICMP询问报文。

**二.ICMP报文的格式**



1.   类型：占8位

2.   代码：占8位

3.   检验和：占16位

说明：ICMP所有报文的前4个字节都是一样的，但是剩下的其他字节则互不相同。

4.   其它字段都ICMP报文类型不同而不同。

1>  ICMP报文的前4个字节是统一的格式，共有三个字段：即类型，代码和检验和。

2>  8位类型和8位代码字段一起决定了ICMP报文的类型。

类型8，代码0：表示回显请求(ping请求)。

类型0，代码0：表示回显应答(ping应答)

类型11，代码0：超时

3>16位的检验和字段：包括数据在内的整个ICMP数据包的检验和；其计算方法和IP头部检验和的计算方法一样的。

ICMP报文具体分为查询报文和差错报文(对ICMP差错报文有时需要做特殊处理，因此要对其进行区分。如：对ICMP差错报文进行响应时，永远不会生成另一份ICMP差错报文，否则会出现死循环)

**三.ICMP差错报文(56字节)**

1.   ICMP差错报告报文共有5种

1>  终点不可达：终点不可达分为:网络不可达，主机不可达，协议不可达，端口不可达，需要分片但DF比特已置为1，以及源路由失败等六种情况，其代码字段分别置为0至5。当出现以上六种情况时就向源站发送终点不可达报文。

说明：

端口不可达：UDP的规则之一是：如果收到UDP数据报而且目的端口与某个正在使用的进程不相符，那么UDP返回一个ICMP不可达报文。

2>  源站抑制：当路由器或主机由于拥塞而丢弃数据报时，就向源站发送源站抑制报文，使源站知道应当将数据报的发送速率放慢。

3>  时间超过：当路由器收到生存时间为零的数据报时，除丢弃该数据报外，还要向源站发送时间超过报文。当目的站在预先规定的时间内不能收到一个数据报的全部数据报片时，就将已收到的数据报片都丢弃，并向源站发送时间超过报文。

4>  参数问题：当路由器或目的主机收到的数据报的首部中的字段的值不正确时，就丢弃该数据报，并向源站发送参数问题报文。

5>  改变路由（重定向）路由器将改变路由报文发送给主机，让主机知道下次应将数据报发送给另外的路由器。

说明:

以下几种情况都不会导致产生ICMP差错报文

1>ICMP差错报文（但是，ICMP查询报文可能会产生ICMP差错报文）

2>目的地址是广播地址或多播地址的IP数据报

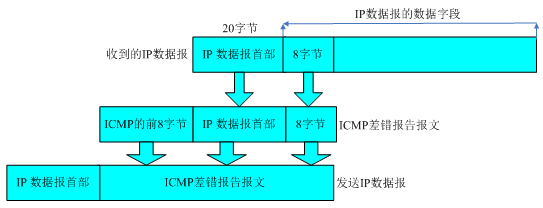
3>作为链路层广播的数据报

4>不是IP分片的第一片

5>源地址不是单个主机的数据报。即源地址不能为零地址、环回地址、广播地址或多播地址。

这些规则是为了防止过去允许ICMP差错报文对广播分组响应所带来的广播风暴。

2.所有的ICMP差错报告报文中的数据字段都具有同样的格式。将收到的需要进行差错报告IP数据报的首部和数据字段的前8个字节提取出来，作为ICMP报文的数据字段。再加上响应的ICMP差错报告报文的前8个字节，就构成了ICMP差错报告报文。提取收到的数据报的数据字段的前8个字节是为了得到运输层的端口号（对于TCP和UDP）以及运输层报文的发送序号（对于TCP）。



注：一下情况不发送ICMP差错报告报文

**三.ICMP询问报文（40字节）**



1.ICMP询问报文有四种回送请求和回答，时间戳请求和回答，掩码地址请求和回答，以及路由器询问和通过。

1>ICMP回送请求报文是由主机或路由器向一个特定的目的主机发出的询问。收到此报文的机器必须给源主机发送ICMP回送应答报文。这种询问报文用来测试目的站是否可达以及了解其有关状态。

2>ICMP时间戳请求允许系统向另一个系统查询当前的时间。该ICMP报文的好处是它提供了毫秒级的分辨率，而利用其他方法从别的主机获取的时间只能提供秒级的分辨率。请求端填写发起时间，然后发送报文。应答系统收到请求报文时填写接收时间戳，在发送应答时填写发送时间戳。大多数的实现是把后面两个字段都设成相同的值。

3>主机使用ICMP地址掩码请求报文可向子网掩码服务器得到某个接口的地址掩码。系统广播它的ICMP请求报文。ICMP报文中的标识符和序列号字段由发送端任意选择设定，这些值在应答中将被返回，这样，发送端就可以把应答与请求进行匹配。

4>主机使用ICMP路由器询问和通过报文可了解连接在本网络上的路由器是否正常工作。主机将路由器询问报文进行广播（或多播）。收到询问报文的一个或几个路由器就使用路由器通过报文广播其路由选择信息

**四.Ping程序**

1.概述

1>Ping程序是为了测试另一台主机是否可达。该程序发送一份ICMP回显请求报文给主机，并等待返回ICMP回显应答。

2>Ping程序还能测出到这台主机的往返时间，以表明该主机离我们有多远。

2.我们将发送回显请求的ping程序为客户，而称被ping的主机为服务器。

3.ICMP回显请求和回显应答报文格式：



1>Unix系统在实现ping程序时把ICMP报文中的标识符字段置成发送进程的ID号。这样即使在同一台主机上同时运行了多个ping程序实例，ping程序也可以识别出返回的信息。

2>序列号从0开始，每发送一次新的回显请求就加1。ping程序打印出返回的每个分组的序列号，允许我们查看是否有分组丢失，失序或重复。.

3>ping程序通过在ICMP报文中存放发送请求的时间值来计算往返时间。当应答返回时，用当前时间减去存放在ICMP报文中的时间值，即是往返时间。

4>当返回ICMP回显应答时，要打印出序列号和TTL，并计算往返时间。TTL位于IP首部的生存时间字段。ping程序通过在ICMP报文数据段中存放发送请求的时间值来计算往返时间。当应答返回时，用当前时间减去存放在ICMP报文中的时间值，即是往返时间。