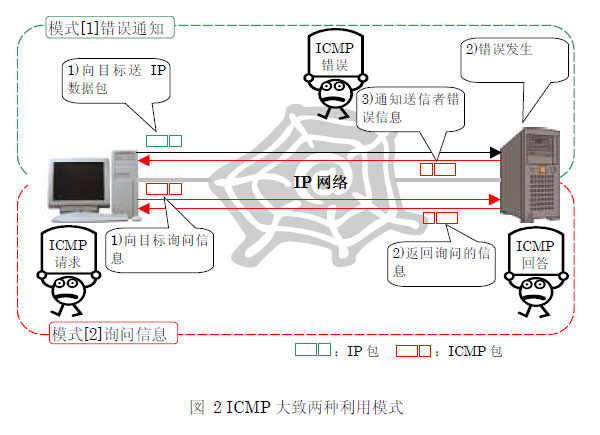
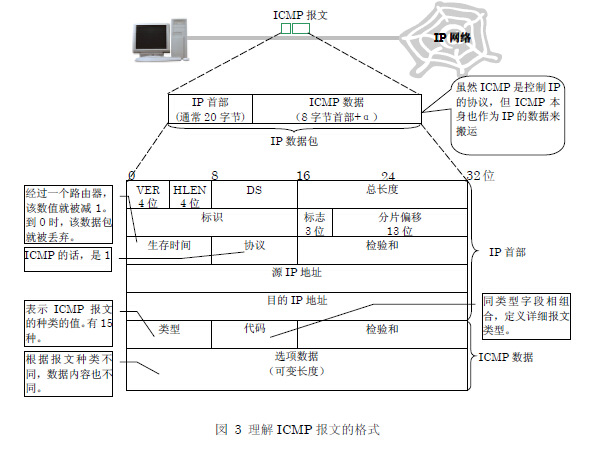
原文地址：<https://www.cnblogs.com/iiiiher/p/8513748.html>

**ICMP的用途**



1. 向发送者报告错误信息
2. 发送者向目标询问信息
3. 目标返回信息给发送者

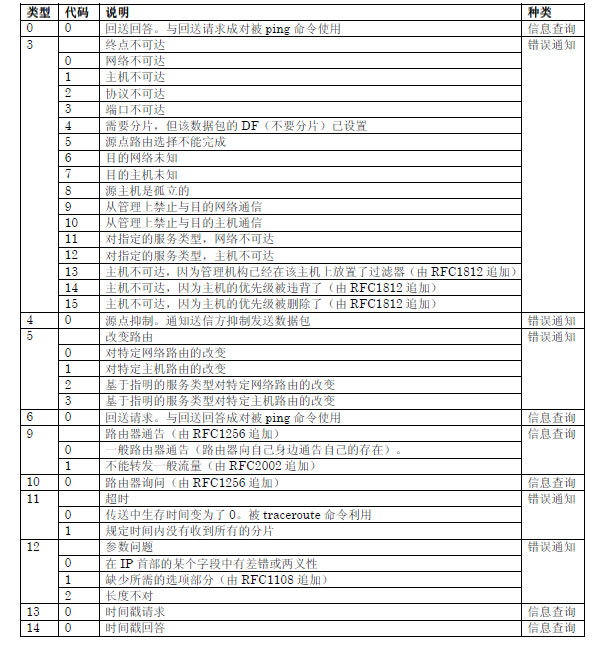
**ICMP报文与IP报文**



ICMP报文基于IP报文

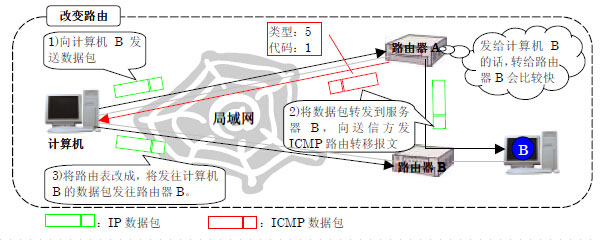
**ICMP类型与代码**

类型与代码确定了ICMP报文的功能



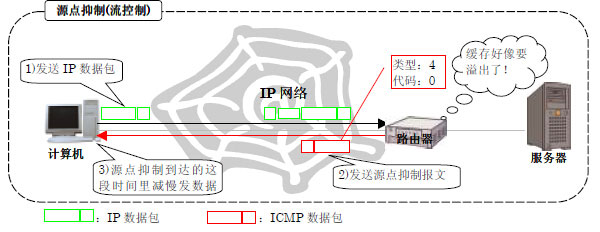
**ICMP实现之改变路由**

路由器A发送ICMP报文告诉发送方“将IP报文发送给 路由器B 会更快”



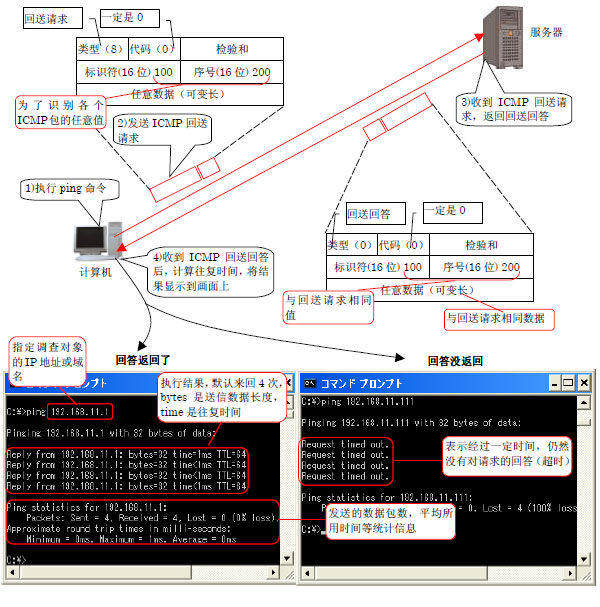
**ICMP实现之源点抑制**

数据包集中到达某一路由器后，数据包因为来不及被处理，有可能被丢弃的情况。这时候，向送信方发送的是ICMP 源点抑制报文，用来使送行方减慢发送速度



**ICMP实现之ping命令**

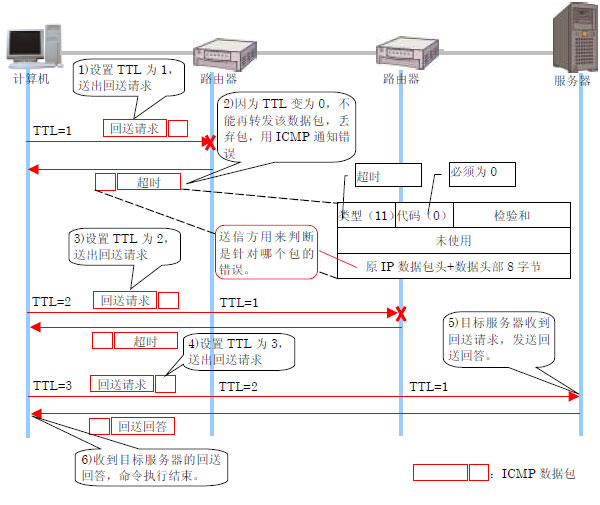
ping 命令用来在IP 层次上调查与指定机器是否连通，调查数据包往复需要多少时间



目标服务器发出回送请求（类型是8，代码是0）。标识符和序号字段分别是16 位的字段，这两个字段里填入任意的值。对于标识符，应用程序执行期间送出的所有报文里填入相同的值。对于序号，每送出一个报文数值就增加1。而且，回送请求的选项数据部分用来装任意数据。这个任意数据用来调整ping 的交流数据包的大小。

**ICMP实现之traceroute命令**

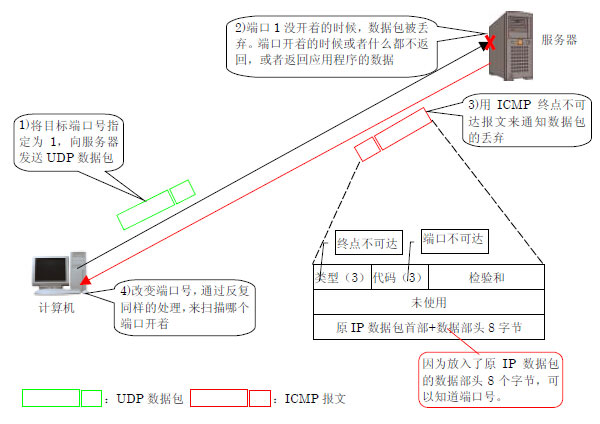
为了调查到通信方的路径现在是怎么样的，使用的是traceroute 命令



traceroute的原理是每次将TTL加1，来获取报文经过的路由

**ICMP实现之端口扫描**

主要是扫描UDP的端口，TCP不需要，因为TCP能连接上就证明端口开着



**ICMP和安全的关系**

ICMP具有较多的安全漏洞，为此一些服务器会禁止一些ICMP功能（如：ping）

ICMP数据包攻击示例：

利用ping 的原理，攻击者向某个网络发送ping，发送源则是被工具的服务器，网络内的计算机会向服务器发送ping会送

