1，概述

ICMP（Internet Control Message Protocol）Internet控制报文协议。它是TCP/IP协议簇的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

2，简介

ICMP协议是一种**面向无连接的协议**，**用于传输出错报告控制信息**。它是一个非常重要的协议，它对于网络安全具有极其重要的意义。 [3] 它**属于网络层协议**，**主要用于在主机与路由器之间传递控制信息**，包括报告错误、交换受限控制和状态信息等。当遇到IP数据无法访问目标、IP路由器无法按当前的传输速率转发数据包等情况时，会自动发送ICMP消息。

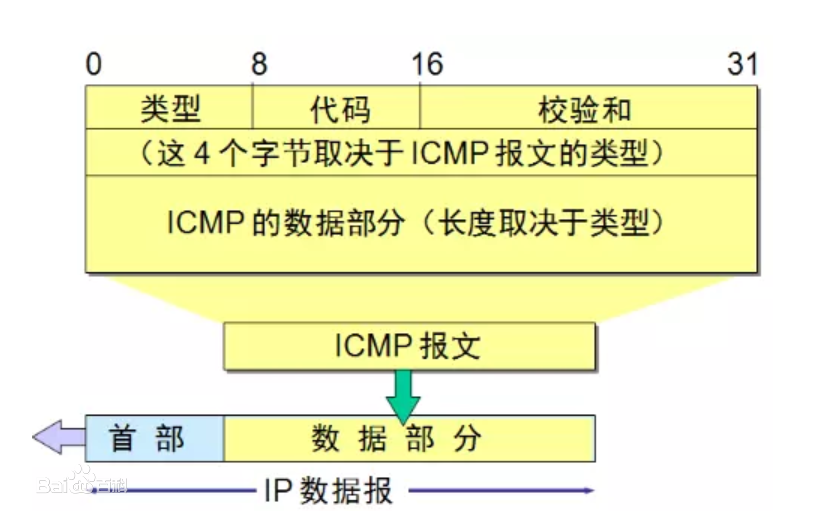
ICMP 是 TCP/IP 模型中网络层的重要成员，与 IP 协议、ARP 协议、RARP 协议及 IGMP 协议共同构成 TCP/IP 模型中的网络层。ping 和 tracert是两个常用网络管理命令，ping 用来测试网络可达性，tracert 用来显示到达目的主机的路径。ping和 tracert 都利用 ICMP 协议来实现网络功能，它们是把网络协议应用到日常网络管理的典型实例。 [1]

**从技术角度来说，ICMP就是一个“错误侦测与回报机制”**，其目的就是让我们能够检测网路的连线状况﹐也能确保连线的准确性。当路由器在处理一个数据包的过程中发生了意外，可以通过ICMP向数据包的源端报告有关事件。

其功能主要有：侦测远端主机是否存在，建立及维护路由资料，重导资料传送路径（ICMP重定向），资料流量控制。ICMP在沟通之中，主要是透过不同的类别(Type)与代码(Code) 让机器来识别不同的连线状况。

ICMP 是个非常有用的协议﹐尤其是当我们要对网路连接状况进行判断的时候。

3，数据报格式



数据报文结构

**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类型

4，ping和tarcert