ICMP 协议介绍

ICMP 出现的背景

IP 协议完成了数据在各主机间的递交，但是，IP 协议是一种无连接的不可靠的数据交付，IP 协议不提供任务错误校验和恢复机制。因此，设计了 ICMP 协议弥补上诉缺陷。

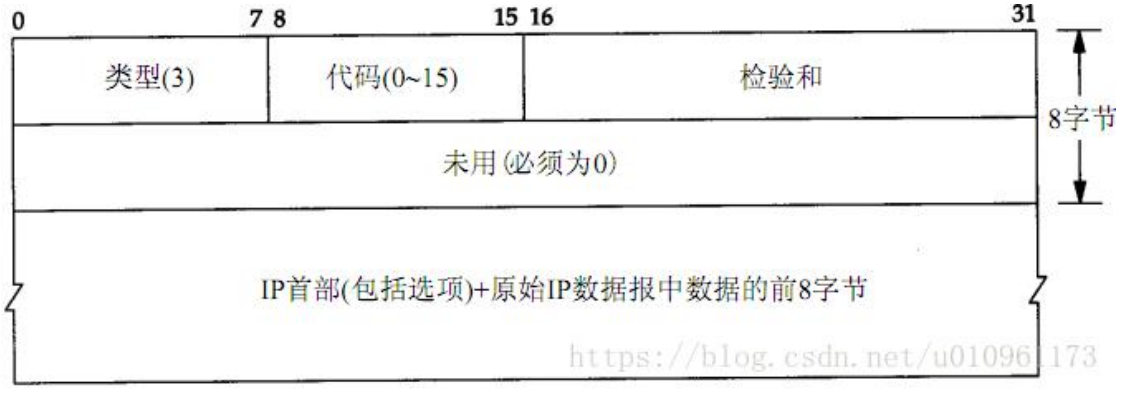
ICMP 报文

ICMP 封装在 IP 报进行传输。ICMP 报文本身被封装在 IP 数据报的数据区中，而这个 IP 数据报又被封装在帧数据中。在 IP 数据报报头中的协议（Protocol）字段设置成 1，表示该数据是 ICMP 报文。

ICMP 报文格式

各种类型的 ICMP 报文由下图所示。由报文中的类型字段和代码字段共同决定了 ICMP 报文的类型：

类　型	代　码	描　述	查　询	差　错
0	0	回显应答(Ping应答，第7章)	•	
3		目的不可达		
	0	网络不可达		•
	1	主机不可达		•
	2	协议不可达		•
	3	端口不可达		•
	4	需要进行分片但设置了不分片比特		•
	5	源站选路失败		•
	6	目的网络不认识		•
	7	目的主机不认识		•
	8	源主机被隔离（作废不用）		•
	9	目的网络被强制禁止		•
	10	目的主机被强制禁止		•
	11	由于服务类型 TOS，网络不可达		•
	12	由于服务类型 TOS，主机不可达		•
	13	由于过滤，通信被强制禁止		•
	14	主机越权		•
	15	优先权中止生效		•
4	0	源端被关闭（基本流控制，11.11节）		•
5		重定向		•
	0	对网络重定向		•
	1	对主机重定向		•
	2	对服务类型和网络重定向		•
	3	对服务类型和主机重定向		•
8	0	请求回显（Ping请求，第7章）	•	
9	0	路由器通告	•	
10	0	路由器请求	•	
11		超时：		
	0	传输期间生存时间为0（Traceroute，第8章）		•
	1	在数据报组装期间生存时间为0		•
12		参数问题：		
	0	坏的IP首部（包括各种差错）		•
	1	缺少必需的选项		•
13	0	时间戳请求	•	
14	0	时间戳应答	•	
15	0	信息请求（作废不用）	•	
16	0	信息应答（作废不用）	•	
17	0	地址掩码请求	•	
18	0	地址掩码应答	•	



（1）类型（Type）字段，长度是 1 字节，用于定义报文类型。

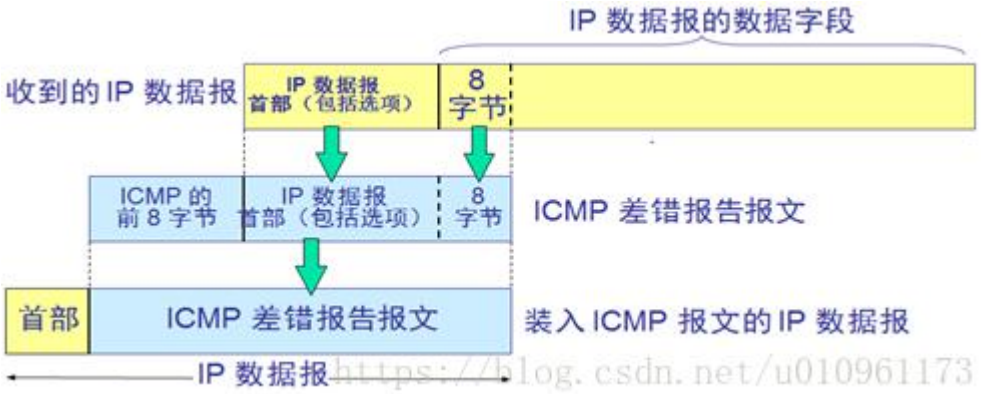
（2）代码（Code）字段，长度是 1 字节，表示发送这个特定报文类型的原因。

（3）校验和（Checksum）字段，长度是 2 字节，用于数据报传输过程中的差错控制。与 IP 报头校验和的计算方法类似，不同的是其是对整个 ICMP 报文进行校验。

（4）报头的其余部分，其内容因不同的报文而不同。

（5）数据字段，其内容因不同的报文而不同。对于差错报告报文类型，数据字段包括 ICMP 差错信息和触发 ICMP 的整个原始数据报，其长度不超过 576 字节。

ICMP 报文包含：ICMP 首部（8 字节）+IP 数据报首部+IP 数据报数据区的前 8 个字节。具体如下图：



IP 包首部要被传回的原因，因为 IP 首部中包含了协议字段，使得 ICMP 可以知道如何解释后面的 8 个字节。而 IP 首部后面的 8 字节（UDP 的首部或者 TCP 首部，UDP 和 TCP 首部的 8 个字节分别包含了 16 位的目的端口号和源端口号），根据源端口号就可以把差错报文与某个特定的用户进程关联。

ICMP 报文类型

从功能上划分，ICMP 报文可分为 2 大类：ICMP 差错报文和 ICMP 查询报文。

差错报告报文包括：目的不可达、源主机消亡、超时、参数问题、重定向。

查询报文包括：回应请求和应答（ping）、信息请求和应答（已弃用）、时间戳和时间戳应答、地址掩码请求和应答、路由器通告和请求。