

# 协议分析 —— I CMP 协议解码详解

本文档属商业机密文件，所有内容均为成都科来软件有限公司独立完成，属科来软件内部机密信息，未经成都科来软件有限公司做出明确书面许可，不得为任何目的、以任何形式或手段（包括电子、机械、复印、录音或其他形式）对本文档的任何部分进行复制、修改、存储、引入检索系统或者传播。

© 2009 科来软件 保留所有权利

技术支持部

科来软件

电话：86-28-85120922

传真：86-28-85120911

网址：<http://www.colasoft.com.cn>

邮件：[support@colasoft.com.cn](mailto:support@colasoft.com.cn)

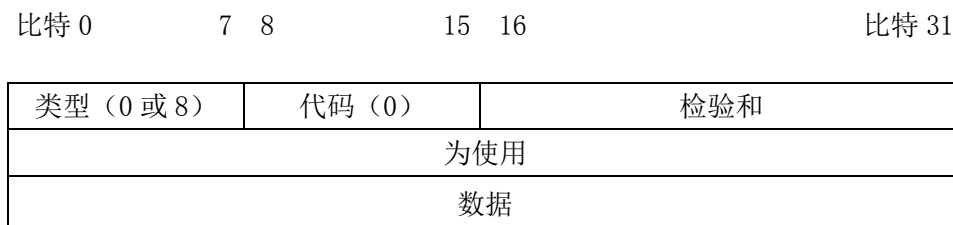
# 协议分析 — ICMP 协议解码详解

## 一、 ICMP 协议简介

ICMP 全称 Internet Control Message Protocol，中文名为因特网控制报文协议。它工作在 OSI 的网络层，向数据通讯中的源主机报告错误。ICMP 可以实现故障隔离和故障恢复。

网络本身是不可靠的，在网络传输过程中，可能会发生许多突发事件并导致数据传输失败。网络层的 IP 协议是一个无连接的协议，它不会处理网络层传输中的故障，而位于网络层的 ICMP 协议却恰好弥补了 IP 的缺陷，它使用 IP 协议进行信息传递，向数据包中的源端节点提供发生在网络层的错误信息反馈。

ICMP 的报头长 8 字节，结构如图 1 所示。



(图 1 ICMP 报头结构)

- **类型**：标识生成的错误报文，它是 ICMP 报文中的第一个字段；
- **代码**：进一步地限定生成 ICMP 报文。该字段用来查找产生错误的原因；
- **校验和**：存储了 ICMP 所使用的校验和值；
- **未使用**：保留字段，供将来使用，起值设为 0；
- **数据**：包含了所有接受到的数据报的 IP 报头。还包含 IP 数据报中前 8 个字节的数据；

ICMP 协议提供的诊断报文类型如表 1 所示。

| 类型 | 描述                                 |
|----|------------------------------------|
| 0  | 回应应答 (Ping 应答，与类型 8 的 Ping 请求一起使用) |
| 3  | 目的不可达                              |
| 4  | 源消亡                                |
| 5  | 重定向                                |
| 8  | 回应请求 (Ping 请求，与类型 0 的 Ping 应答一起使用) |
| 9  | 路由器公告 (与类型 10 一起使用)                |
| 10 | 路由器请求 (与类型 9 一起使用)                 |
| 11 | 超时                                 |
| 12 | 参数问题                               |

解

|    |                     |
|----|---------------------|
| 13 | 时标请求（与类型 14 一起使用）   |
| 14 | 时标应答（与类型 13 一起使用）   |
| 15 | 信息请求（与类型 16 一起使用）   |
| 16 | 信息应答（与类型 15 一起使用）   |
| 17 | 地址掩码请求（与类型 18 一起使用） |
| 18 | 地址掩码应答（与类型 17 一起使用） |

（表 1 ICMP 诊断报文类型）

ICMP 提供多种类型的消息为源端节点提供网络层的故障信息反馈，它的报文类型可以归纳为以下 5 个大类：

- 诊断报文（类型 8，代码 0；类型 0，代码 0）；
- 目的不可达报文（类型 3，代码 0-15）；
- 重定向报文（类型 5，代码 0-4）；
- 超时报文（类型 11，代码 0-1）；
- 信息报文（类型 12-18）。

## 二、详细解码

使用科来网络分析系统捕获数据包，我们得到ICMP回显报文的信息，如图1所示，

工程 1 - 科来网络分析系统 [停止]

文件(F) 编辑(E) 查看(V) 工程(E) 工具(T) 窗口(W) 帮助(H)

新建 打开 保存 向后 向前 向上 开始 停止 报表 设置 适配器 过滤器 网络配置 日志设置 名字表 过滤器表 选项

概要统计 端点 协议 会话 数据包 日志 图表

数据包: 10

| 编号 | 绝对时间            | 源             | 目标            | 协议   | 大小 | 概要              |
|----|-----------------|---------------|---------------|------|----|-----------------|
| 1  | 11:25:24.711698 | 192.168.0.92  | 192.168.0.90  | ICMP | 78 | 回显              |
| 2  | 11:25:29.871104 | 192.168.0.92  | 192.168.0.90  | ICMP | 78 | 回显              |
| 3  | 11:25:41.335575 | 192.168.0.92  | 192.168.0.208 | ICMP | 78 | 回显              |
| 4  | 11:25:41.335780 | 192.168.0.208 | 192.168.0.92  | ICMP | 78 | 回显应答 192.168... |

数据包: 编号:000001 长度:78 捕获长度:74 时间戳:2006-05-31 11:25:24.711698  
目标:00:14:85:CA:F4:F7 源:00:14:85:CA:F5:22 协议:0x0800  
版本:4 头长:5 DSCP:0000 0000 总长:60 标识:0x6EE4 标志:000... 段偏移:0 生

ICMP - 因特网控制消息协议 [34/40]

- 类型: 8 (回显) [34/1]
- 代码: 0 [35/1]
- 校验和: 0x425C (正确) [36/2]
- 标识: 0x0400 [38/2]
- 序列号: 0x0700 [40/2]
- 回显数据: 32 字节 [42/32]

FCS - 帧校验序列:

FCS: 0x627AB756 (计算出的)

```

0000  00 14 85 CA F4 F7 00 14 85 CA F5 22 08 00 45 00 00 3C 6E E4 00 00 80 01 49  .....".E.<n....I
0019  D6 CD A8 00 5C 00 A8 00 5A 08 00 42 5C 04 00 07 00 61 62 63 64 65 66 67 68  ....\...Z..E....abcdefgh
0032  69 6A 6B 6C 6D 6E 6F 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  ijklmnopqrstuvwabcdefghi
  
```

寻求帮助, 请按 F1

(图 1 科来网络分析系统抓取的 ICMP 回显报文)

我们详细介绍在图 1 中的解码信息，

- 类型：8，表示是一个 ICMP 回显请求报文；
- 代码：0，表示网络不可达；
- 校验和：表示 ICMP 的 0x425C；使用 IP 校验和的算法。
- 标识：0x0400
- 序列号：0x0700，每一个 ICMP 回显报文都有一个序列号且是递增的
- 数据：表示是一个 32 字节的数据

注：以上是一个 ICMP 回送报文，可以看出了和前面列出的 ICMP 报文有点不一样。因为 ICMP 有几种类型的报文（目标不可达报文，重定向报文，超时报文，回送请求和回送应答报文），每一种报文都相对都有一些区别，这里我们就不在特别介绍。

成都科来软件有限公司

[www.colasoft.com.cn](http://www.colasoft.com.cn)