Network Working Group
Request for Comments: 792

J. Postel
ISI

September 1981

Updates: RFCs 777, 760
Updates: IENs 109, 128

RFC792- Internet 控制信息协议（ICMP）
（RFC792 INTERNET CONTROL MESSAGE PROTOCOL）

目录

1.介绍

在被称为 Catenet 的系统中，IP 协议被用作主机到主机的数据报服务。网络连接设备称为网关。这些网关通过网关到网关协议（GGP）相互交换用于控制的信息。通常，网关或目的主机将和源主机通信，例如，为报告在数据报过程中的错误。为了这个目的才使用了 ICMP，它使用 IP 做为底层支持，好象它是一个高层协议，而实际上它是 IP 的一部分，每一种 IP 模块必须实现 ICMP。

ICMP 消息在以下几种情况下发送：当数据报不能到达目的地时，当网关的已经失去缓存功能，当网关能够引导主机在更短路由上发送。

IP 并非设计为绝对可靠，这个协议的目的是为了当网络出现问题的时候返回控制信息，而不是使 IP 协议变得绝对可靠，并不保证数据报或控制信息能够返回。一些数据报仍将在没有任何报告的情况下丢失。上层协议必须使用自己的差错控制程序来判断通信是否正确。

ICMP 信息通常报告在处理数据报过程中的错误。若要避免信息无限制地返回，对于 ICMP 消息不会单独成包发送，而且 ICMP 信息只在处理数据报偏移量为 0 时发送。

2.消息格式

ICMP 消息以基本 IP 头发送。数据的第一个字节是 ICMP 类型域；此域的值决定了了其余数据的格式。任何标记为"未使用"的域都是为以后的扩展保留的，在传送过程中必须全部是 0。除非在个别的格式之下，包头域如下格式：

·版本：4
·IHL：Internet 头长度大小以 32 位字为单位。
·服务类型：0
·总长度：包头长度和数据长度。
·标识符（Identification）、标志（Flags）、段偏移量：在分段时使用。
·生存周期：以秒计，此域在每台机器处理数据报时减少，此值必须大于要传送它的网关所

消耗的时间。

·协议：ICMP = 1

·包头校验码：16 位数据反码和再取反而得。为计算校验码，此域应该为 0。在将来可以会取代这一域。

·源地址：创建 ICMP 信息的网关或主机地址，除非说明，它可以是任何网关地址。

·目的地址：信息要发送到的网关或主机地址。

3.目的不可达信息

IP 域：目的地址，发送原始数据报数据的网络地址

ICMP 域：

·类型：3

·代码：

0 = 网络不可达；

1 = 主机不可达；

2 = 协议不可用；

3 = 端口不可达；

4 = 需要段和 DF 设置；

5 = 源路由失败；

·校验码：16 位数据（从 ICMP 类型开始）的反码和再取反而得。为计算校验码，校验码域应该为零。这些零在以后会被校验码取代。

·Internet 包头+源数据报：

Internet 包头加上源数据的头 64 位而得。此数据用于主机匹配信息到相应的进程。如果高层协议使用端口号，应该假设其在源数据的头 64 个字节之中。

·说明：

相应于网关的路由表，如果在目的域中指定的网络不可达，如网络距离为无限远，网关会向发送源数据的主机发送目的不可达消息。而且，在一些网络中，网关有能力决定目的主机是否可达。如果目的地不可达，它将向发送源数据的主机发送不可达信息。

在目的主机，如果 IP 模块因为指定的协议模块和进程端口不可用而不能提交数据报，目的主机将向发送源数据的主机发送不可达信息。

另外一种情况是当数据报必须被分段传送，而"不可分段"位打开，在这种情况下，网关必须抛弃此数据报，并向发送源数据的主机发送不可达信息。

代码 0，1，4 和 5 由网关发送，而代码 2 和 3 由主机发送。

4.超时信息

IP 域：

目的地址：从源数据报数据中得到。

ICMP 域：

·类型：11

·代码：

0 = 传送超时；

1 = 分段级装超时。

·校验码：16 位数据（从 ICMP 类型开始）的反码和再取反而得。为计算校验码，校验码域应该为零。这些零在以后会被校验码取代。

·Internet 包头+64 位源数据报数据：Internet 包头加上源数据的头 64 位而得。此数据用于主机匹配信息到相应的进程。如果高层协议使用端口号，应该假设其在源数据的头 64 个字节之中。

·说明：

如果网关在处理数据报时发现生存周期域为零，此数据报必须抛弃。网关同时必须通过超时信息通知源主机。

如果主机在组装分段的数据报时因为丢失段未能在规定时间内组装数据，此数据报必须抛弃。网关发送超时信息。

如果段零不可用则不用发送超时信息。

代码 0 由网关发送，代码 1 由主机发送。

5.参数问题消息

IP 域：

目的地址：从源数据中得到。

ICMP 域：

·类型：12

·代码：

0 = 指针指向错误。

·校验码： 16 位数据（从 ICMP 类型开始）的反码和再取反而得。为计算校验码，校验码域应该为零。这些零在以后会被校验码取代。

·指针：

如果 code = 0，指向有问题的字节。

·Internet 包头+64 位源数据报数据：Internet 包头+64 位源数据报数据：Internet 包头加上源数据的头 64 位而得。此数据用于主机匹配信息到相应的进程。如果高层协议使用端口号，应该假设其在源数据的头 64 个字节之中。

·说明：

如果网关或主机在处理数据报时发现包头参数有错误以至不能完成工作，它必须抛弃此数据报。一个潜在的原因可以是变量的错误。网关或主机将通过参数问题消息通知源主机，此消息只有在消息被抛弃时才被发送。

指针指向发现错误的数据报包头字节（可能是选项的中间）。例如，1 表示服务类型有错误，如果有选项的话，20 表示第一个选项的类型有错误。

代码 0 可能从主机或网关接收到。

6.源拥塞消息

IP 域：

目的地址：源数据报数据的地址和源网络。
ICMP 域：
·类型：4
·代码： 0
·校验码： 16 位数据（从 ICMP 类型开始）的反码和再取反而得。为计算校验码，校验码域应该为零。这些零在以后会被校验码取代。
·Internet 包头+64 位源数据报数据： Internet 包头+64 位源数据报数据：Internet 包头加上源数据的头 64 位而得。此数据用于主机匹配信息到相应的进程。如果高层协议使用端口号，应该假设其在源数据的头 64 个字节之中。
·说明：
如果没有缓冲容纳，网关会抛弃数据报，如果网关这样做了，它会发送源拥塞消息给发送主机。如果接收的数据报太多无法处理，目的主机也会发送相应的消息给发送主机。此消息要求发送发减少发送速率，网关会给每个抛弃的消息返回源拥塞消息，在接到此消息后，发送主机应该减少发送速率，直到不再接收到网关发送的源拥塞消息为止。在此之后，源主机可以再增加发送速率，直到接收到目的主机的源拥塞消息为止。
网关或主机不会等到已经超过限度后再发送此消息，而是接近自己的处理极限时就发送此消息，这意味着，引发源拥塞消息的数据报仍然可以处理。
代码 0 可能会从主机或网关接收到。
7.重定向消息

IP 域：
目的地址：源数据报数据的地址和源网络。
ICMP 域：
·类型： 5
·代码：
0 = 重定向网络的数据报；
1 = 重定向主机的数据报；
2 = 重定向网络和服务类型的数据报；
3 = 重定向网络和主机类型的数据报。
·校验码：
16 位数据（从 ICMP 类型开始）的反码和再取反而得。为计算校验码，校验码域应该为零。这些零在以后会被校验码取代。
·网关 Internet 地址：
应该发送网关地址（其在源数据报数据的 internet 目的网络域中指定）。
·Internet 包头+64 位源数据报数据：
Internet 包头加上源数据的头 64 位而得。此数据用于主机匹配信息到相应的进程。如果高层协议使用端口号，应该假设其在源数据的头 64 个字节之中。
·说明：
网关在下面情况下发送重定向消息。网关（G1）从网关相连的网络上接收到数据报，它检查路由表获得下一个网关（G2）的地址（X）。如果 G2 和指定的接收主机在同一网络上，重定向消息发出，此消息建议发送主机直接将数据报发向网关 G2，因为这更近，同时网关 G1 向前继续发送此数据报。
因为在数据报中的 IP 源路由和目的地址域是可选的，所以即使有更好的路由有时也无法发现。
代码 0，1，2 和 3 可能会从网关发送。
8.回送或回送响应消息

IP 域：
地址：
回送消息的源地址是回送响应消息的目的地址。若要形成一个回送响应消息，应该将源和目的地址交换，将类型代码更改为 0，重新计算机校验码。
ICMP 域：
·类型：
8 代表回送消息；
0 代表回送响应消息。
代码：0
·校验码：
16 位数据（从 ICMP 类型开始）的反码和再取反而得。为计算校验码，校验码域应该为零。这些零在以后会被校验码取代。
·标识符：如果代码=0，帮助匹配回送和回送响应的代码可以为 0。
·序列码：如果代码=0，帮助匹配回送和回送响应的序列码可以为 0。
·说明：
回送消息中接收到的消息应该在回送响应消息中返回。标识符和序列码由回送发送者使用帮助匹配回送请求的响应。
代码 0 可能会从主机或网关接收到。
9.时间戳和时间戳响应消息

IP 域：
地址：
时间戳消息的源地址是时间戳响应消息的目的地址。若要形成一个时间戳响应消息，应该将源和目的地址交换，将类型代码更改为 14，重新计算机校验码。
ICMP 域：
·类型：
13 代表时间戳消息；
14 代表时间戳响应消息。
·代码：0
·校验码：
16 位数据（从 ICMP 类型开始）的反码和再取反而得。为计算校验码，校验码域应该为零。这些零在以后会被校验码取代。
·标识符：如果代码=0，帮助匹配时间戳和时间戳响应的代码可以为 0。
·序列码：如果代码=0，帮助匹配时间戳和时间戳响应的代码可以为 0。
·说明：
接收到的时间戳附加在响应里返回，时间是以百万分之一称为单位计算，并以标准时午夜开始计时。原时间戳是发送方发送前的时间。接收时间戳是回送者接收到的时间，传送时间是回送者发送的时间。
如果时间以百万分之一秒计无效，或者不能以标准时提供，可以在时间戳的高字节填充入数据以表示这不是标准数据。标识符和序列码由发送者匹配请求的响应。
代码 0 可能会从主机或网关接收到。
信息请求或信息响应消息

IP 域：
地址：

信息请求消息的源地址是信息响应消息的目的地址。若要形成一个信息响应消息，应该将源和目的地址交换，将类型代码更改为 16，重新计算机校验码。

ICMP 域：

·类型：

15 代表信息请求消息；

16 代表信息响应消息。

·代码： 0

·校验码：

16 位数据（从 ICMP 类型开始）的反码和再取反而得。为计算校验码，校验码域应该为零。这些零在以后会被校验码取代。

·标识符：如果代码=0，帮助匹配信息请求和信息响应的代码可以为 0。

·序列码：如果代码=0，帮助匹配信息请求和信息响应的代码可以为 0。

·说明：

此消息可以在 IP 包头中以源网络地址发送，但同时目的地址域为 0（这表示此网络内）。响应 IP 模块应该发送完全指定地址的响应。发送此消息是主机寻找到自己所在网络号码的一种方法。标识符和序列码由发送者匹配请求的响应。

代码 0 可能会从主机或网关接收到。

10.消息类型总结

0 回送响应

3 目的不可达

4 源拥塞

5 重定向

8 回送

11 超时

12 参数问题

13 时间戳

14 时间戳响应

15 信息请求

16 信息响应

11. 参考资料

[1] Postel, J. (ed.), "Internet Protocol - DARPA Internet Program Protocol Specification," RFC 791, USC/Information Sciences Institute, September 1981.

[2] Cerf, V., "The Catenet Model for Internetworking," IEN 48, Information Processing Techniques Office, Defense Advanced Research Projects Agency, July 1978.

[3] Strazisar, V., "Gateway Routing: An Implementation Specification", IEN 30, Bolt Beranek and Newman, April 1979.

[4] Strazisar, V., "How to Build a Gateway", IEN 109, Bolt Beranek and Newman, August 1979.

[5] Mills, D., "DCNET Internet Clock Service," RFC 778, COMSAT Laboratories, April 1981.

制信息协议（ICMP）

1

1