

RFC 792 : Internet Control Message Protocol

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 4 Janvier 2008

Date de publication du RFC : Septembre 1981

<http://www.bortzmeyer.org/792.html>

Protocole auxiliaire d'IP depuis le début, ICMP est toujours un des protocoles essentiels de l'Internet. Sa version pour IPv4 est normalisé dans ce RFC.

Un très vieux RFC que notre RFC 792¹. À l'époque, on parlait encore du Catenet (le terme Internet n'était pas universellement adopté), les RFC étaient très courts, sans table des matières et sans sections numérotées, et la fameuse section Sécurité n'était pas obligatoire (alors qu'elle aurait été intéressante pour ICMP, protocole non connecté, sans aucune authentification, même faible).

ICMP est une partie intégrante d'IP (RFC 791). Même s'il est situé dans une couche au dessus (les paquets ICMP sont encapsulés dans l'IP), la mise en œuvre d'ICMP est obligatoire pour toute machine IP. IPv6 a d'ailleurs repris exactement le même modèle dans le RFC 4443.

À quoi sert ICMP ? À signaler les problèmes et à obtenir quelques informations sur les autres machines.

Un paquet ICMP comporte un champ de huit bits, le "*Message Type*" et notre RFC liste, par exemple, les types suivants :

- "*Destination Unreachable*", par lequel un routeur peut signaler à la machine source que la destination n'est pas joignable.
- "*Time Exceeded*", par lequel un routeur signale que le temps maximum de séjour dans le réseau (en fait, un nombre de routeurs traversés) est dépassé. C'est ce type qu'utilise traceroute, qui envoie des paquets avec un TTL de 1, puis 2, puis 3, et déduit des ICMP "*Time Exceeded*" reçus qu'on a atteint le routeur n° 1, 2, 3, etc.

1. Pour voir le RFC de numéro NNN, <http://www.ietf.org/rfc/rfcNNN.txt>, par exemple <http://www.ietf.org/rfc/rfc792.txt>

- "Echo", qui permet de réclamer une réponse (qui sera un paquet ICMP de type "Echo Reply"). Ce mécanisme est surtout utilisé par la commande ping. C'est aussi un exemple d'un cas où un paquet ICMP ne sert pas qu'à signaler des erreurs. On notera que le RFC comporte d'ailleurs une bogue (souvent répétée depuis) en affirmant qu'on n'envoie jamais un paquet ICMP en réponse à un paquet ICMP. C'est faux ("Echo" est un bon exemple), et la formulation correcte est qu'on n'envoie jamais un paquet ICMP en réponse à un paquet ICMP d'erreur.
- "Source Quench", qui permet de dire à la source de ralentir son débit. Il n'est plus utilisé car il serait trop facile de s'en servir pour un déni de service (RFC 1812, section 4.3.3.3).
- "Timestamp", qui permet de demander à une autre machine l'heure (qui arrivera dans un "Timestamp Reply"). Il n'a jamais été très utilisé, en comparaison de protocoles comme daytime (RFC 867) ou time (RFC 868) ou bien sûr comme NTP (RFC 1305).

D'autres types ont été depuis rajoutés dans le registre IANA (<http://www.iana.org/assignments/icmp-parameters>).

"Destination Unreachable" nécessite de donner d'avantage d'informations (beaucoup de choses peuvent aller mal !) et les paquets de ce type ont donc un champ "Code" de huit bits dont voici certaines valeurs possibles :

- "Network Unreachable", lorsque le routeur n'a pas de route vers ce réseau.
- "Host Unreachable" lorsqu'une machine ne répond pas. Ce code est typiquement utilisé par le dernier routeur, lorsque la machine de destination ne répond pas aux requêtes ARP.
- "Fragmentation needed and DF set" est utilisé lorsque le paquet a une taille supérieure à la MTU du lien et que le bit DF ("Do not fragment") est mis dans l'en-tête IP. C'est l'utilisation de ces paquets ICMP qui permet la découverte de la MTU du chemin (RFC 1191).

traceroute affiche ces codes lorsque la réponse n'est pas "Time exceeded", avec des lettres suivies d'un point d'exclamation (pour citer la documentation, "*!H, !N, or !P (host, network or protocol unreachable), !S (source route failed), !F (fragmentation needed), !X (communication administratively prohibited), [...] or !num ζ (ICMP unreachable code ;num ζ)*")

ICMP a évolué par la suite, notamment par la possibilité d'inclure des messages structurés dans les paquets (RFC 4884).

Un des plus gros problèmes que rencontre ICMP aujourd'hui, est que beaucoup de coupe-feux administrés par des ignorants bloquent la totalité des paquets ICMP. Cette erreur vient en général d'une mauvaise compréhension des problèmes de sécurité (comme le ping of death, mal nommé puisqu'il n'est pas spécifique à ping, ou à ICMP). Le résultat est que certains protocoles comme la découverte de la MTU du chemin fonctionnent mal (cf. RFC 4821).