RFC 7279 : An Acceptable Use Policy for New ICMP Types and Codes

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 13 juin 2014

Date de publication du RFC : Mai 2014

https://www.bortzmeyer.org/7279.html

Voici un court RFC sur un protocole peu connu mais indispensable au bon fonctionnement de l'Internet : ICMP. Plus précisément, ce RFC se penche sur la création de nouveaux types et codes ICMP : quand est-ce une bonne idée ?

ICMP est normalisé dans le RFC 792 [1] pour IPv4 et dans le RFC 4443 pour IPv6. Il sert de protocole de signalisation pour IP, transportant des informations sur l'état du réseau et les éventuels problèmes rencontrés. Les messages ICMP ont un champ nommé "*Type*" qui indique la catégorie du message et, lorsque le message nécessite davantage d'analyse, un champ "*Code*". Ainsi, pour IPv6, un paquet ICMP dont le champ "*Type*" vaut 1 indique que la destination souhaitée n'est pas joignable, et le "*Code*" indique la raison <https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml#icmpv6-parameters-codes-2> (par exemple, 0 indique que le routeur ne connait pas de route vers cette destination). La liste de ces types et codes n'est pas figée et on pouvait toujours en ajouter des nouveaux (par exemple celui du RFC 6743) ou en retirer (cf. RFC 6633). Un registre IANA donne la liste actuelle (pour IPv4 <https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml> et pour IPv6 <https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml>).

Il n'existait pas de politique formelle quant à l'enregistrement de nouveaux types et codes. Chaque demande était évaluée sans référence à une règle commune. La section 2 de notre RFC introduit une politique. Deux cas sont estimés acceptables :

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

— Le nouveau type sert à indiquer à l'émetteur du paquet qu'un problème dans la transmission est survenu en aval. L'examen du message ICMP doit permettre à l'émetteur de savoir si le paquet a été transmis ou pas. C'est par exemple le cas, pour les types existants, de "*Destination unreachable*" (type 3 en IPv4 et 1 en IPv6), de "*Time exceeded*" (utilisé par traceroute, type 11 en IPv4 et 3 en IPv6), de "*Packet too big*" (type 2 en IPv6, malheureusement trop souvent filtré, ce qui explique les problèmes de "*Path MTU discovery*" fréquents avec IPv6).
— Le nouveau type sert à obtenir ou à transmettre des informations sur un nœud du réseau, obtenir ou transmettre des paramètres du réseau, ou découvrir des machines situées sur le lien. C'est par exemple le cas, pour les types existants, de "*Echo (request or reply)*" (dont dépend la commande ping, types 0 et 8 en IPv4, 128 et 129 en IPv6), des messages de sollicitation ou d'annonce du routeur (types 9 et 10 en IPv4, 133 et 134 en IPv6), des messages de résolution d'adresse IP en adresse MAC (types 135 et 136 en IPv6, cf. RFC 4861).

La section 2.1 de notre RFC classe tous les types existants en indiquant de quel cas ils relèvent. Attention, cette classification couvre aussi les types abandonnés et qui ne doivent plus être utilisés (RFC 6918).

Ces cas limitatifs excluent donc l'usage d'ICMP pour faire un protocole de routage complet. D'abord, du point de vue architecture, ICMP n'a pas été prévu pour cela. Ensuite, il n'a aucun mécanisme d'authentification et il permet des usurpations triviales. D'autre part, et malheureusement, il est souvent filtré.

Il existe au moins un protocole de routage mis en œuvre sur ICMP : RPL (RFC 6550). C'est une exception et elle ne devrait pas être généralisée (RPL ne fonctionne pas au niveau de tout l'Internet mais uniquement dans des réseaux locaux).

Certaines applications utilisent ICMP de manière créative, par exemple en provoquant délibérement des conditions d'erreur, pour récolter, via les messages ICMP d'erreur, des informations sur le réseau. C'est notamment le cas de traceroute, qui envoie des paquets avec un TTL délibérement trop bas, pour provoquer l'envoi de messages "*Time exceeded*". Cela ne pose pas de problème philosophique : ces applications utilisent les types ICMP existants, elles ne changent pas le protocole.

Notre RFC note également que, si on veut étendre ICMP parce qu'il est actuellement trop limité, il existe un mécanisme standard pour mettre de l'information structurée dans les messages ICMP, mécanisme décrit dans le RFC 4884. Par exemple, ce mécanisme permet d'indiquer dans les messages ICMP des informations sur les interfaces réseaux utilisées par le paquet d'origine (RFC 5837).

La section 3 résume les choses importantes à savoir sur la place d'ICMP : originellement prévu pour signaler les erreurs, il a été vite étendu pour faire des diagnostics (style ping). Il fait partie intégrante d'IP (ce n'est pas une option : une machine IP doit gérer ICMP). Bien que ses messages soient encapsulés dans IP, il n'est pas considéré comme un protocole au-dessus d'IP mais comme un composant d'IP. Et le RFC rappelle que son nom est trompeur : le « Protocole des Messages de Contrôle de l'Internet » ne contrôle nullement l'Internet, son rôle est plus modeste mais indispensable.