RFC 5837 : Extending ICMP for Interface and Next-hop Identification

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 25 avril 2010

Date de publication du RFC : Avril 2010

https://www.bortzmeyer.org/5837.html

Depuis les débuts d'IP, les routeurs envoient des messages ICMP à l'émetteur lorsqu'ils ne peuvent pas transmettre un datagramme. Ces messages, normalisés dans les RFC 792 [1] et RFC 4443, donnent un certain nombre d'informations sur le datagramme original mais ne contiennent pas les informations internes au routeur comme l'interface réseau par lequel le datagramme original est arrivé, ou bien l'adresse IP du routeur auquel il aurait été transmis. Ce RFC normalise des extensions pour transmettre cette information.

Donc, quand un routeur reçoit un datagramme qu'il ne peut pas ou ne veut pas faire suivre, il renvoie un message ICMP (RFC 1812, notamment la section 4.3). Parfois, l'interface réseau sur laquelle a été reçue le datagramme original (celui dont la non-transmission a nécessité l'émission d'un message ICMP) est identifiée par l'adresse IP source du message ICMP. Mais pas toujours (section 2 du RFC). Pour que cela marche, en effet, il faut que le routeur aie envoyé le message ICMP par l'interface où le datagramme original avait été reçu **et** que cette interface soit « numérotée » (aie une adresse IP en propre). Mais le routage peut être asymétrique (auquel cas le message ICMP sort par une autre interface que celle où le datagramme IP était entrée) et les interfaces n'ont pas forcément une adresse IP.

IPv6 fournit d'autres possibilités (RFC 4443) pour la sélection de l'adresse IP source du message d'erreur. Mais, dans les deux cas, IPv4 ou IPv6, il n'existe pas de moyen fiable d'indiquer l'interface d'entrée du datagramme original. D'où l'extension de notre RFC. Celle-ci permet d'indiquer le nom de l'interface (identique au `ifName` du RFC 2863), ses adresses IP, etc.

Pour cela, cette extension repose sur le concept de messages ICMP structuré, défini dans le RFC 4884.

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

La section 3 donne des exemples d'application de cette extension. Par exemple, elle peut être utilisée par traceroute pour améliorer l'information donnée à l'utilisateur (section 3.1). Malheureusement, je ne connais pas encore de mise en œuvre de traceroute qui utilise cette extension.

Même des informations a priori complètement opaques (comme le numéro - `ifIndex` - de l'interface où le routeur avait reçu le datagramme original) peuvent être utiles, par exemple pour voir si deux paquets étaient entrés par la même interface.

Comme cette extension permet également d'identifier quelle aurait été l'interface de **sortie** du datagramme original (s'il avait été transmis), elle peut servir à déboguer des problèmes de filtrage spécifiques à une interface, ou bien à résoudre les problèmes de MTU (section 3.2).

L'extension est formellement décrite dans la section 4. Elle a la forme d'un **objet** (RFC 4884), le "*Interface Information Object*". Cet objet porte le numéro de classe 2 dans le registre IANA <https://www.iana.org/assignments/icmp-parameters> (cf. section 7). Il est joint aux paquets ICMP comme `Time Exceeded` ou `Destination Unreachable`. Le sous-type (section 4.1, "*c-type*" dans le RFC 4884) identifie le rôle de l'interface du routeur et quelles informations sont incluses (par exemple, le cinquième bit du sous-type indique si l'objet comprend l'information sur l'adresse IP de l'interface considérée). Quels sont les rôles possibles pour l'interface à propos de laquelle l'objet d'information est envoyé ? Par exemple, les deux premiers bits du sous-type à zéro indiquent que l'interface est celle d'entrée du datagramme originel. Le premier bit à 1 et le second à zéro indiquent que l'objet décrit au contraire l'interface de sortie (enfin, celle qui aurait été utilisée si le paquet avait été transmis).

Les sections suivantes décrivent le format des sous-objets d'information. Par exemple, si une adresse IP est présente (bit 5 du sous-type), son format figure en section 4.2 (la famille, IPv4 ou IPv6, puis l'adresse elle-même). Si le nom de l'interface est présent (bit 6 du sous-type), le format de ce nom est décrit par la section 4.3 (un octet pour la longueur, puis le nom en UTF-8, suivant la description de la MIB-II, dans le RFC 2863, par exemple `eth1` ou `Ethernet0/3`).

Pour aider à la compréhension, la section 4.4 donne des exemples détaillés de paquets utilisant cette extension ICMP. Si vous n'avez pas compris mes explications, les exemples de cette section rendront tout cela plus clair.

Ces paquets ICMP étendus permettent de transmettre des informations d'un réseau à un autre, peut-être en traversant les frontières d'un espace d'adressage particulier. Si un routeur sur un réseau interne émet ces paquets ICMP, et qu'ils passent par un routeur NAT pour atteindre la machine de gestion, que va t-il se passer ? Les adresses IP contenues dans le paquet ICMP peuvent n'avoir plus aucun sens. La section 5 s'attaque à ce problème, déjà abordé dans le RFC 5508. La règle est simple : toute « traduction » de l'objet d'information est interdite. Le routeur NAT doit laisser passer cet objet intact ou le retirer mais jamais le modifier. Le destinataire du message ICMP et de l'objet qu'il contient est donc averti que les adresses IP de l'objet peuvent concerner un autre domaine d'adressage et peuvent donc ne pas être pertinentes.

Quels autres problèmes peut poser cette extension ICMP ? Comme elle distribue davantage d'information qu'avant, il existe des risques de confidentialité. Avant, un routeur ne révelait pas quelle était l'interface d'entrée ou de sortie du datagramme qu'il n'avait pas routé. Désormais, il peut le faire et certains administrateurs réseau peuvent estimer que cette information ne doit pas sortir. La section 6, sur la sécurité, leur donne raison en spécifiant que la diffusion de cette information devrait être configurable, par exemple pour permettre de ne pas diffuser certains points.

Enfin, dernier avertissement, rien n'authentifie le contenu des paquets ICMP. Il ne faut donc pas se fier aveuglément au contenu des ces objets d'information.

Je n'ai pas d'informations sur les implémentations de ce RFC. Peut-être faudra t-il attendre.