RFC 5881 : BFD for IPv4 and IPv6 (Single Hop)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 juin 2010

Date de publication du RFC : Juin 2010

https://www.bortzmeyer.org/5881.html

Le protocole de détection BFD, normalisé dans le RFC 5880 [1], permet plusieurs applications. La plus évidente est la détection de la panne d'une machine voisine et c'est celle que normalise notre RFC 5881.

Traditionnellement, la détection de la panne d'un voisin se faisait lorsqu'il arrêtait d'envoyer certains messages, par exemple les paquets `Hello` pour un voisin OSPF. Mais cette méthode est souvent lente. BFD (RFC 5880) spécifie un mécanisme générique de détection, indépendant des protocoles de routage et du lien physique. BFD permet plusieurs applications dont, pour notre RFC 5881, la connectivité avec un voisin immédiat (« immédiat » au sens IP, pas forcément au sens physique). Cette application fonctionne avec IPv4 ou IPv6, mais sur des sessions BFD séparées.

Si la fonction d'écho de BFD est employée, la section 2 note qu'il faut penser à désactiver les filtres du RFC 2827, incompatibles avec la façon dont cette fonction marche.

À quoi ressemblent les paquets de cette application ? Comme indiqué en section 4, ce sont des paquets UDP utilisant le port 3784 - et 3785 pour la fonction d'écho. BFD emploie IP de manière assez... créative et nécessite donc des précautions particulières, notamment pour éviter que des paquets de redirection ("*ICMP redirect*") soient envoyés. Ainsi, la section 4 prévient que l'adresse IP source, paradoxalement, ne devrait pas être une adresse légale du sous-réseau utilisé (ni, en IPv6, une adresse locale au lien). Mettre en œuvre BFD, sur certains systèmes d'exploitation, peut donc être difficile, puisque ce protocole nécessite de court-circuiter pas mal de fonctions normales d'IP.

La section 5 précise les TTL à utiliser. Si on ne se sert pas des fonctions d'authentification de BFD, il faut limiter les risques d'usurpation en mettant un TTL de 255, la valeur maximale. Comme le TTL est diminué par chaque routeur, la réception d'un paquet avec ce TTL prouvera que le paquet vient bien du lien local (cf. section 9 et RFC 5082).

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5880.txt`