RFC 5880 : Bidirectional Forwarding Detection

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/5880.html

Le tout nouveau protocole BFD est un protocole très générique de test de la liaison entre deux routeurs, de manière à ce qu'ils puissent déterminer qu'ils sont encore capables de se passer des paquets. Son originalité est d'être indépendant du type de liaison physique, ainsi que des protocoles de routage.

Les routeurs ont toujours besoin de savoir si les autres routeurs sur le même réseau sont joignables, afin de pouvoir calculer une route alternative. Certaines liaisons physiques fournissent très rapidement une indication en cas de panne (SONET), d'autres peu ou pas du tout (Ethernet). Les routeurs utilisent donc en général une fonction du protocole de routage, comme la fonction `Hello` de OSPF. Le principe est de s'envoyer des messages régulièrement. Si on n'a pas entendu un routeur voisin depuis deux ou trois périodes, c'est qu'il est en panne (section 1 du RFC). Mais ces mécanismes ne fonctionnent que s'il y a un protocole de routage (ce n'est pas toujours le cas, il existe des routes statiques), ils ne testent que la communication entre les "*control engines*" des routeurs, la partie qui gère les protocoles de routage, pas la communication entre les "*forwarding engines*", la partie qui commute effectivement les paquets (ces deux parties sont souvent radicalement séparés sur un routeur et peuvent donc tomber en panne séparement). Enfin, ces mécanismes sont typiquement trop lents à détecter les pannes.

D'où BFD, présenté dans la section 2 de notre nouveau RFC. BFD est une fonction du "*forwarding engine*" pour être sûr qu'il teste la capacité des routeurs à transmettre les paquets, et pour survivre au redémarrage d'un protocole de routage. Il ne dépend pas de fonctions du lien physique comme la diffusion, pour pouvoir fonctionner sur tous les types de liens physiques.

La section 3 décrit le fonctionnement du protocole. Comme les autres systèmes de type `Hello`, chaque routeur BFD envoie périodiquement à ses voisins des paquets pour dire « Tout va bien ». Lorsqu'on ne les reçoit plus, on sait que le routeur est planté. La durée entre deux paquets est modifiable dynamiquement, afin de garantir un temps de détection de panne aussi court que possible, sans pour autant trop surcharger le réseau par des paquets `Hello`.

BFD a deux modes de fonctionnement (section 3.2), asynchrone, où chaque routeur envoie ses paquets `Hello` sans se préoccuper de l'autre et synchrone ("*Demand mode*", cf. section 6.6) où le routeur n'envoie rien par défaut, il attend une sollicitation « Tu es toujours là ? ». En outre, BFD dispose d'une fonction `Echo` où le routeur qui reçoit un paquet BFD répond aussitôt. Cette fonction est utilisable avec les deux modes. Elle peut être coûteuse en nombre de paquets mais elle teste réellement tout le chemin à travers le "*forwarding plane*" (la machinerie qui commute et transmet les paquets) du routeur cible. La même section 3.2 discute les avantages et les inconvénients de chaque mode, ainsi que ceux d'une utilisation de la fonction `Echo` (sur cette fonction, voir aussi les sections 5 et 6.4, qui précise notamment qu'`echo` est asymétrique, elle peut être activée dans une direction seulement).

Les paquets BFD sont envoyés dans le contexte d'une **session** et l'établissement de cette session nécessite un mécanisme de contrôle. Le format des paquets qui le réalisent est exposé en section 4. Un paquet BFD a plusieurs champs (section 4.1) dont deux **discriminateurs**, des nombres qui identifient les sessions à bord des deux routeurs (chaque paquet comprend le discriminateur mis par la source et, s'il est connu, celui pertinent pour la destination ; le discriminateur identifie la session, pas le routeur). Une authentification simple est possible (sections 4.2 à 4.4 et 6.7).

Une fois le format défini, que doivent faire les deux routeurs pour envoyer et traiter correctement les paquets BFD ? C'est l'objet de la section 6. D'abord, il faut décider de lancer le service. Un des routeurs le sollicite, il est **actif** (l'autre est **passif**). L'actif envoie des paquets de contrôles, informant de son désir de commencer une session, et indiquant le discriminateur (cf. section 6.3). Des paramètres comme le mode (synchrone ou asynchrone) et le rythme d'envoi de paquets (section 6.8.2) sont alors négociés. L'envoi de paquets continue alors, selon les paramètres sélectionnés. La session est considérée comme en panne s'il n'y a pas de réponse.

La machine à états du protocole (très simple) est décrite en section 6.2.

Enfin, en pratique, l'expérience du déploiement d'autres protocoles justifie qu'une section, la 7, soit consacréee aux problèmes opérationnels. Par exemple, les paquets BFD circulant directement sur la couche 2, sans passer par un protocole de couche 3 (ce qui sera sans doute un cas courant), risquent d'être bloqués par certains pare-feux et il faut donc veiller à la configuration de ceux-ci. Il y a aussi un problème analogue pour tous les mécanismes de "*shaping*". Limiter le rythme de transmission des paquets BFD (qui doivent normalement être considérés comme du trafic temps réel) pourrait interférer avec leur fonction de détection des pannes.

Autre question pratique de grande importance, la sécurité. Si tout se passe bien, BFD deviendra une partie essentielle de l'infrastructure réseau. Une attaque contre BFD pourrait donc avoir des effets très étendus, par exemple en réalisant une DoS si un attaquant peut bloquer la réception des paquets BFD. D'où la section 9 sur la sécurité. Ainsi, pour ne citer qu'un exemple, si on fait passer BFD sur un protocole de couche 3 comme IP, un paquet BFD imité, avec une fausse adresse IP source, serait trivial à fabriquer et à envoyer au routeur victime. Lorsque les routeurs parlant BFD sont adjacents (situés sur le même réseau physique), il faut donc mettre le TTL à la valeur maximale et vérifier qu'elle n'a pas été décrémentée (technique GTSM, décrite dans le RFC 5082 [1]).

Et les implémentations ? Les routeurs Juniper l'ont depuis longtemps (version 8.3 de JunOS), ainsi que les Brocade et les Cisco. Pour les deux premiers, BFD fonctionne aussi en "*multi-hop*", cf. RFC 5883. Voici par exemple sur un Brocade :

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc5082.txt`

```
telnet@ro=1#show bfd neighbors bgp
Total Entries:8 R:RxRemote(Y:Yes/N:No)H:Hop(S:Single/M:Multi)
....
```

Il y a aussi une implémentation dans Linux avec kbfd <http://kbfd.sourceforge.net/> et une autre libre, OpenBFDd <https://github.com/JakeMont/OpenBFDD>. Merci à Ludovic Boué pour ses précisions.