RFC 7086 : Host Identity Protocol-Based Overlay Networking Environment (HIP BONE) Instance Specification for REsource LOcation And Discovery (RELOAD)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 17 janvier 2014

Date de publication du RFC : Janvier 2014

https://www.bortzmeyer.org/7086.html

Le protocole pair-à-pair RELOAD, spécifié dans le RFC 6940 [1], définit un certain nombre d'éléments minimum pour créer un réseau pair-à-pair mais pas la totalité. Il doit être complété par des descriptions d'un "*overlay*" particulier, un réseau utilisant RELOAD. Ce RFC est la spécification d'un "*overlay*" basé sur HIP <https://www.bortzmeyer.org/hip-resume.html>.

HIP est normalisé dans le RFC 7401 et le cadre pour construire des "*overlays*" avec HIP est dans le RFC 6079. Ce RFC 7086 combine donc RELOAD et HIP BONE pour faire des réseaux pair-à-pair. À noter que tout RELOAD n'est pas utilisé : le "*Forwarding and link management layer*" de RELOAD (section 6.5 du RFC 6940 est complètement remplacé par HIP (section 3 de notre RFC).

Définir une classe d'instances RELOAD nécessite de spécifier les identificateurs utilisés pour les machines ("*Node ID*" dans RELOAD). Dans le cas de HIP, les "*Node ID*" peuvent être de deux types (section 4 de notre RFC) :

— Les identificateurs HIP classiques, les ORCHID (RFC 7343), qui ont l'avantage de pouvoir s'utiliser dans les API existantes, puisqu'ils ont la forme d'une adresse IPv6, dans un préfixe dédié,
— Des identificateurs RELOAD complets, qui permettent d'avantage de machines ($2\hat{\{\}}128$ au lieu de $2\hat{\{\}}100$) mais qui ne sont plus compatibles avec les applications existantes.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6940.txt

Il faut aussi définir la correspondance entre les messages RELOAD et les messages HIP (section 5). Les messages RELOAD sont transportés dans des messages HIP de type `DATA` (RFC 6078) **mais** certains services assurés par des parties du message RELOAD sont déplacés vers HIP. Ainsi, le "*forwarding header*" de RELOAD (qui sert à contrôler l'envoi vers la destination finale) est remplacé par des fonctions HIP comme les listes `Via` (RFC 6028) qui permettent de mieux contrôler le routage, et le "*security block*" de RELOAD se déplace vers des extensions HIP comme les certificats du RFC 6253.

Normalement, les messages RELOAD sont sécurisés par l'utilisation de TLS (RFC 5246). Mais HIP peut déjà tout chiffrer. Plus besoin de TLS, donc, remplacé par le chiffrement HIP du RFC 6261.

Dans tout système pair-à-pair, le recrutement et l'arrivée de nouveaux pairs sont des points délicats (section 8). Ici, on utilise les mécanismes de RELOAD, avec quelques détails différents. Par exemple, les certificats échangés contiennent des HIT (condensat d'un HI, d'un identificateur HIP) et pas des URI RELOAD. Ces HIT sont placés dans le champ `subjectAltName` du certificat (RFC 6253).

Il a aussi fallu étendre un peu la définition du document de configuration initial (section 11 du RFC 6940 et section 10 de notre RFC). Récupéré par les pairs, ce document contient les informations nécessaires pour rejoindre l'"*overlay*". L'élément XML `<bootstrap-node>` contient désormais un HIT.

Ce nouveau type d'"*overlay*" est désormais noté dans le registre IANA `<https://www.iana.org/assignments/reload/reload.xhtml#overlay-link-protocols>`.

Il existe apparemment au moins une mise en œuvre de ce RFC mais je n'ai pas eu l'occasion de l'essayer.