RFC 5826 : Home Automation Routing Requirements in Low Power and Lossy Networks

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 7 avril 2010

Date de publication du RFC : Avril 2010

https://www.bortzmeyer.org/5826.html

L'≪ Internet des objets ≫ est un terme à la mode, pour désigner l'interconnexion d'équipements qui ne sont pas habituellement considérés comme des ordinateurs mais qui ont néanmoins une adresse IP et une connexion (souvent indirecte) à l'Internet. Dans un environnement de type domotique, par exemple, cela concerne le grille-pain et le réfrigérateur lorsqu'ils veulent échanger des recettes. Mais, s'ils sont trop éloignés l'un de l'autre et qu'ils ne peuvent communiquer que via le presse-purée ? C'est ici que rentre en jeu notre RFC, troisième document du groupe de travail ROLL <http://tools.ietf.org/wg/roll> de l'IETF, groupe de travail qui vise à définir des protocoles de routage permettant au grille-pain et au réfrigérateur de découvrir que le presse-purée est volontaire pour router leurs paquets IP. Ce document est le cahier des charges des futurs protocoles de ROLL.

Bien sûr, les exemples cités plus haut sont des cas trop faciles, car le grille-pain et le réfrigérateur disposent tous les deux de tellement d'énergie que les protocoles classiques de routage peuvent être utilisés. Mais si on prend des équipements non reliés au réseau électrique comme une alarme incendie planquée dans le plafond, la télécommande de la télévision, le compteur d'eau, etc, la situation devient plus délicate, on entre vraiment dans le monde des ≪ "*Low power and lossy networks*" ≫ qui ont donné leur nom au groupe ROLL. Ces engins ne peuvent plus communiquer que par radio et la portée de leurs émetteurs est souvent limitée (notamment afin d'économiser les batteries). Le routage est donc nécessaire, certaines machines relayant les communications des autres. D'autre part, la réception sera souvent mauvaise (le spectre hertzien est très encombré et la seule mise en route du four à micro-ondes peut perturber le réseau). Les pertes de paquets seront donc fréquentes. Le problème ressemble donc beaucoup à celui décrit dans le RFC 5548 [1] (qui était davantage tourné vers l'extérieur, notre RFC 5826 visant la maison, alors que le RFC 5867 vise les immeubles de bureaux).

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5548.txt

Pour allêcher le lecteur, la section 2 donne quelques exemples d'applications domotiques, chacune illustrant un ou deux points précis des exigences qui pèseront sur le protocole. À noter que beaucoup de ces exemples reprennent sans nuance le discours habituel des vendeurs de solution domotiques, qui font miroiter le côté "*high-tech*" de leurs gadgets, sans jamais se demander s'ils sont réellement utiles et si le même objectif ne pouvait pas être atteint autrement. C'est ainsi que le contrôle de l'air conditionné (section 2.2) est présenté comme permettant de réduire la consommation énergétique, sans même mentionner la possibilité de supprimer complètement ce gouffre d'énergie absurde qu'est l'air conditionné ! Bel exemple d'écoblanchiment.

L'exemple des systèmes d'alarme (section 2.8) est particulièrement détaillé. Comme certains des capteurs ont un rôle vital (par exemple les détecteurs de fumée), il n'est pas question de tirer inutilement sur leur batterie en leur faisant assurer des tâches de routage pour des équipements moins vitaux. Le protocole de routage doit donc permettre d'exclure de la corvée de routage certains systèmes.

Après ce voyage dans le Disneyland de la domotique, la section 3 liste les exigences concrètes :

— Routage prenant en compte les contraintes, notamment de limitation de la consommation d'énergie de l'appareil (section 3.1). Les protocoles de routage actuels sur l'Internet ignorent complètement ce facteur.
— Possibilité de mobilité, certains des équipements se déplacent en effet souvent (section 3.2). Certains équipements sont fixes mais arrêtés relativement souvent alors que d'autres, lorsqu'ils « disparaissent » à la vue du routage, réapparaissent à un autre endroit.
— Passage à l'échelle (section 3.3), le chiffre envisagé étant de centaines (!) d'équipements actifs dans une maison. Cela semble incroyable aujourd'hui, où la domotique est souvent un luxe de riche, tout juste bon à permettre au milliardaire de la Silicon Valley d'impressionner ses visiteurs en leur infligeant une démo de ses derniers gadgets à chaque "*party*". Mais ce chiffre pourrait être atteint dans des maisons plus ordinaires si la tendance actuelle à la multiplication du nombre d'appareils électriques se poursuit (regardez le nombre de prises de courant qu'il faut aujourd'hui, sans compter les appareils sur pile ou batterie). En mettant une limite arbitraire à « au moins 250 appareils », le RFC n'interdit quand même pas de stocker l'adresse des appareils sur un seul octet...
— Convergence rapide (section 3.4) après un changement. Les équipements de la maison vont bouger et être allumés et éteints fréquemment. Les changements dans le routage seront donc fréquents et ne doivent pas bloquer le réseau pendant plusieurs minutes. Le RFC met des limites quantitatives : 0,5 secondes maximum si les nœuds du réseau n'ont pas bougé et 4 secondes s'ils se sont déplacés.
— Autoconfiguration, car les utilisateurs n'auront pas envie d'être l'administrateur réseaux de leur propre mauson. Tout devra marcher tout seul (section 3.5).
— Stabilité (section 3.6) ce qui implique une forme de mémoire : si un équipement est souvent en panne, il faut pouvoir s'en souvenir, pour ne pas le choisir comme routeur.

Bien sûr, un tel réseau à la maison, dont la taille et la complexité serait à peu près celle de l'Internet de 1975, poserait des problèmes de sécurité. C'est l'objet de la section 5. Les réseaux à la maison rendent beaucoup de solutions de sécurité irréalistes. Par exemple, difficile d'exiger d'une machine devant économiser chaque milliwatt d'énergie de faire des calculs cryptographiques compliqués à chaque paquet. Le RFC insiste donc sur la nécessité de développer des solutions de sécurité légères.

Autre problème de sécurité, l'auto-configuration. Elle rend difficile la mise en œuvre de politiques de sécurité et notre RFC 5826 demande donc des mécanismes permettant de refuser l'accès à une machine inconnue.