RFC 6550 : RPL: IPv6 Routing Protocol for Low power and Lossy Networks

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 mars 2012

Date de publication du RFC : Mars 2012

https://www.bortzmeyer.org/6550.html

Il y a beaucoup d'intérêt en ce moment pour un (largement mythique) « Internet des objets » qui mèle des fantasmes domotiques éculés (le réfrigérateur qui commande tout seul des bières à Carrefour via l'Internet, lorsqu'il est vide), l'arrivée massive d'ordinateurs qui ne sont pas considérés comme des ordinateurs ("*smartphones*", tablettes, télévisions connectées), la connexion à des réseaux TCP/IP d'équipements très modestes, et la diffusion de plus en plus large d'étiquettes RFID. Pour les ordinateurs (un "*smartphone*", bien plus puissant que l'ordinateur qu'embarquait les vaisseaux Apollo, mérite tout à fait ce titre), un des enjeux de l'Internet des objets est le routage des paquets IP. Ces « objets » ont des ressources électriques limitées, et sont souvent connectés par des liens radio de qualité médiocre. Les protocoles de routage traditionnels ne sont pas très adaptés à cette situation. Le groupe de travail ROLL <http://tools.ietf.org/wg/roll> de l'IETF travaille sur ce problème et vient de produire son protocole « officiel », RPL ("*Routing Protocol for LLNs*" où un LLN est un "*Low power and Lossy Network*", un réseau où mêmes les routeurs ont peu de courant et où pas mal de paquets se perdent en route). Le groupe ROLL a déjà produit plusieurs RFC détaillant les demandes de ces LLNs : RFC 5867 [1], RFC 5826, RFC 5673 et RFC 5548. Il a également normalisé l'algorithme de distribution utilisé par RPL, Trickle (RFC 6206).

Un exemple de LLNs est un groupe de capteurs dispersés un peu partout dans un bâtiment industriel : ce sont des petites machines par rapport au "*smartphone*" typique, fonctionnant sur batteries ou sur piles, ils doivent faire attention à leur consommmation électrique. Connectés par radios, ils n'ont en général pas la possibilité de parler directement aux gros routeurs de la salle machines, située à des dizaines de mètres. Certains des objets doivent donc tenir le rôle de routeur, relayant les communications de leurs camarades (la distinction entre routeur et machine terminale est d'ailleurs assez floue dans RPL). Il leur faut donc un protocole de routage pour trouver les chemins possibles et les protocoles

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5867.txt

existants comme OSPF n'ont jamais été conçus pour ce genre de missions (par exemple, OSPF émet des messages même lorsqu'il n'y a pas de changements, ce qui peut vider une batterie rapidement). Le « public » visé est donc composé de machines avec des processeurs 16bits, quelques ko de RAM et de Flash, dans des réseaux où il peut y avoir des milliers de tels engins.

RPL est la solution technique à ce problème du routage. Je préviens tout de suite mes fidèles lecteurs que ce RFC est **très** long et que je n'ai pas tout suivi, loin de là. Il n'y aura donc pas ici de cours sur RPL mais juste la mise en évidence de certains points intéressants (si vous ne lisez qu'une partie du RFC, la section 3 est une description de haut niveau de RPL). Notez qu'il existe d'autres protocoles de routage répondant à peu près à ce cahier des charges, notamment Babel (RFC 8966).

Pour distribuer l'information sur les routes et les routeurs, RPL utilise l'algorithme Trickle (RFC 6206).

RPL essaie de construire un graphe acyclique, qui est lui-même divisé en sous-graphes acycliques, chacun enraciné dans une et une seule destination (RPL les nomme **DODAG** pour "*Destination-Oriented Direct Acyclic Graphs*"). Tout le trafic pour une destination donnée a ainsi la garantie de l'atteindre, sans boucler. Le graphe est orienté : les informations de routage indiquent si le paquet progressera « vers le haut » ou bien « vers le bas » et cette orientation joue un rôle essentiel dans la prévention des boucles (section 11.2). L'annexe A décrit en détail un exemple de fonctionnement.

Pour optimiser les routes, RPL est paramétré avec une fonction nommée OF (pour "*Objective Function*"). Des concepts comme celui de distance sont définis par cette fonction. Des réseaux différents peuvent utiliser des OF différents (une qui cherche le chemin le plus court, une qui cherche à ne pas utiliser comme routeur les machines n'ayant pas de connexion au courant électrique, etc), même s'ils utilisent tous RPL. Ces fonctions sont enregistrées à l'IANA <https://www.iana.org/assignments/rpl/rpl.xml> (section 20.5). La section 14 décrit les règles auxquelles doivent obéir ces fonctions.

RPL nécessite des liens bidirectionnels. Ce n'est pas toujours évident d'avoir de tels liens dans le monde des ondes radio. RPL doit donc tester la bidirectionnalité des liens avec un potentiel routeur, par exemple en utilisant le protocole du RFC 5881. Comme tout bon protocole TCP/IP, RPL peut fonctionner sur un grand nombre de modèles de réseaux physiques (cf. RFC 3819). Les communications du protocole RPL utiliseront ensuite des paquets ICMP (RFC 4443) de type 155 <https://www.iana.org/assignments/icmpv6-parameters>.

Conçu pour des réseaux de machines ayant peu de capacités, et qu'on ne peut pas aller toutes configurer à la main, RPL a par défaut peu de sécurité. Dans le mode de base, n'importe quelle machine peut se joindre au réseau et se faire désigner comme routeur. Dans le mode « pré-installé », les machines doivent connaître une clé pour joindre le réseau. Dans le mode de sécurité maximale, dit « authentifié », il y a deux clés, une pour devenir un nœud ordinaire, et une pour devenir un routeur. (Voir la section 10 pour tous les détails sur la sécurité.)

RPL est un protocole de **routage** ("*routing*"), c'est-à-dire de construction de routes. Il ne change pas le modèle de transmission ("*forwarding*") d'IP, celui que suivent les nœuds une fois les routes connues. Néanmoins, la section 11 donne quelques conseils intéressants sur la façon dont les machines peuvent limiter les problèmes lors de la transmission des paquets. Par exemple, une machine peut faire partie de plusieurs réseaux RPL (on dit « plusieurs **instances** RPL ») et elle doit faire attention en routant des paquets entre deux instances car les protections contre les boucles ne s'appliquent plus. Une solution possible est d'ordonner les instances (on peut transmettre les paquets destinés à un réseau seulement vers un réseau dont le numéro d'instance est supérieur).

L'ingénieur réseaux qui devra installer et configurer un réseau utilisant RPL peut aller regarder tout de suite la section 18 : elle explique la gestion de ces réseaux et les paramètres qu'on peut avoir à configurer, dans l'esprit du RFC 5706. Évidemment, c'est toujours préférable lorsqu'il n'y a rien à configurer et que cela marche tout seul (RFC 1958, section 3.8). C'est particulièrement vrai pour le type de réseaux auxquels est destiné RPL, des réseaux composés de nombreuses machines planquées un peu partout. Néanmoins, si on veut configurer, il y a quelques boutons à tourner comme le choix du numéro d'instance RPL (section 18.2.3) qui permet d'avoir plusieurs réseaux RPL différents dans un même endroit.

Enfin, la section 19 est la traditionnelle section sur la sécurité. Comme résumé au début de cet article, RPL offre forcément peu de sécurité : les réseaux ad hoc pour lesquels il est prévu ne s'y prêtent guère (difficulté à configurer chaque machine, par exemple pour y indiquer une clé, ou bien ressources limitées des machines, ce qui limite l'usage de la cryptographie). RPL fournit néanmoins des mécanismes de sécurité mais il est à parier qu'ils ne seront pas souvent déployés.

Comme souvent de nos jours, une bonne partie des efforts du groupe de travail a été dépensé en discussions sur les différentes brevets plombant le protocole. Il a finalement été décidé de foncer mais les juristes peuvent regarder les différentes prétentions à l'appropriation qui pèsent sur RPL <http://datatracker.ietf.org/ipr/search/?option=document_search&id_document_tag=18975>.

Quelles implémentations sont disponibles ? Selon le groupe de travail, elles seraient déjà plus de dix, mais je n'ai pas de liste. Ce qui est sûr, c'est que deux tests d'interopérabilité ont déjà eu lieu, sous la houlette de l'IPSO et du consortium Zigbee. La section 16 intéressera certainement les implémenteurs car elle récapitule les choses importantes qu'il faut savoir pour que toutes les mises en œuvre de RPL coopèrent.

Un résumé de synthèse sur RPL est « "*"The Internet of Things" takes a step forward with new IPv6 routing protocol*" <http://blogs.cisco.com/news/internet-of-things/> », écrit par un employé de Cisco (entreprise qui a fondé l'alliance IPSO <http://www.ipso-alliance.org/> en septembre 2008).