RFC 6606 : Problem Statement and Requirements for 6LoWPAN Routing

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 mai 2012

Date de publication du RFC : Mai 2012

https://www.bortzmeyer.org/6606.html

Il y en a, des RFC produits par le groupe de travail 6lowpan <http://tools.ietf.org/wg/6lowpan>, qui a pour tâche de normaliser des protocoles pour les LowPAN ("*Low-Power Wireless Personal Area Network*"), ces réseaux de toutes petites machines, limitées en puissance de calcul et en électricité (réseaux de capteurs industriels, par exemple). Parmi les questions soulevées par les LowPAN, le routage. Les liens radio 802.15.4 entre les machines ont une portée limitée et la communication entre deux machines quelconques du LowPAN nécessite parfois une transmission par un ou plusieurs routeurs intermédiaires. Les normes des couches basses, comme IEEE 802.15.4 ne spécifient pas de mécanisme pour gérer ce routage. Ce RFC 6606 [1] est le cahier des charges pour les protocoles de routage du LowPAN, protocoles qui seront établis par d'autres groupes comme Roll <http://tools.ietf.org/wg/roll>, qui travaille sur un problème plus général que celui des seuls LowPAN et a normalisé le protocole RPL dans le RFC 6550. Notez qu'il y a eu d'autres RFC proches comme le RFC 5826 qui se focalise sur le cas particulier de la domotique, ou le RFC 5673, pour les réseaux industriels.

Pour réviser les caractéristiques des machines d'un LowPAN, le mieux est de lire le RFC 4919. Pour savoir comment IPv6 (le 6 dans le nom du groupe 6lowpan <http://tools.ietf.org/wg/6lowpan>) fonctionne sur un LowPAN, c'est le RFC 4944. Un point important à garder en tête avant d'étudier le routage est que ce dernier consomme des ressources (courant électrique, par exemple) et qu'il faut donc limiter cette fonction aux machines les mieux pourvues.

La norme de couche 2 IEEE 802.15.4, sur laquelle s'appuient les LowPAN ne dit pas comment les topologies sont établies puis maintenues. Et elle ne spécifie pas de protocole de routage. Dans un LowPAN, on distingue traditionnellement deux formes de « routage », une en couche 2, le "*mesh under*"

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6606.txt

(brièvement mentionné dans le RFC 4944 : tout le LowPAN est un seul réseau IP), et une en couche 3 (la seule qu'on devrait normalement appeler « routage »), le "*route over*". Le groupe Roll cité plus haut ne travaille que sur le "*route over*" (le « vrai » routage) mais notre RFC 6606 couvre les deux formes. Pour le routage, l'IETF a déjà des tas de protocoles (comme OSPF). Mais aucun ne convient aux LowPAN, en raison de leurs caractéristiques propres (notamment les faibles ressources en processeur et en puissance électrique, et le problème spécifique posé par l'hibernation).

Le RFC 4919 formulait déjà des exigences spécifiques pour les protocoles de routage du LowPAN : minimisation de la consommation de ressources, et acceptation des machines qui hibernent pendant la majorité du temps. Ce RFC 6606 reprend et détaille ces exigences.

Notez que, dans un LowPAN typique, les adresses allouées aux machines n'ont aucune chance de suivre la topologie du réseau. Il n'y a donc pas de possibilité de router par préfixe IP, d'agréger des préfixes adjacents, etc.

Il y a beaucoup de sortes de LowPAN, d'autant plus qu'on en est aux débuts et qu'on ne sait pas encore tout. La section 4 détaille les caractéristiques des différents types de LowPAN qui peuvent avoir une influence sur les algorithmes de routage. Par exemple, le nombre de machines est un des principaux (un algorithme d'inondation n'est envisageable que dans les petits réseaux). Or, un LowPAN peut aller de deux machines (cas de capteurs dans le corps humain, les "*Body Area Network*") à des millions de machines (grande usine).

Et c'est à partir de la section 5 qu'on en arrive aux exigences explicites pour l'algorithme de routage. Elles sont numérotées Rn, de R1, à R18 mais, rassurez-vous, je ne les expliquerai pas toutes.

R1 est liée à la taille des machines du LowPAN. Elle exige un mécanisme de routage qui convienne à ces toutes petites machines. Par exemple, certaines auront si peu de mémoire qu'il faudra limiter la table de routage à 32 entrées. Le système de routage doit donc permettre de stocker une table partielle, ou fortement résumée (voir aussi R10). Pour donner une idée des contraintes, certaines machines auront entre 4 et 10 ko de mémoire vive, et seulement 48 à 128 ko de mémoire Flash, pour stocker le code du programme de routage. Un MICAz <http://www.scribd.com/doc/91069327/Micaz-Datasheet-t> a 4ko/128ko, un TIP700CM <http://www.gobizkorea.com/blog/ProductList.do?blogId=maxfor&group_code=999999999&group_name=All> 10ko/48ko. Il faudra donc des algorithmes simples, pour que le code tienne dans ces mémoires.

L'exigence **R2** porte sur la consommation électrique : il faut un mécanisme qui la limite. Par exemple, un paquet de diffusion va potentiellement réveiller toutes les machines du lien, les forçant à traiter ce paquet. Il faut donc les éviter. Même si le temps de processeur est à économiser, il faut se rappeler que la principale cause de consommation d'électricité, de loin, est la radio. Celle du TR1000 <http://www.rfm.com/products/spec_sheet.php?record=TR1000> consomme 21 mW en transmission et 15 mW en réception.

Le LowPAN fonctionnant sur 802.15.4, il doit tenir compte des caractéristiques de celui-ci. Par exemple, **R3** demande que les paquets de contrôle du protocole de routage tiennent dans une seule trame 802.15.4 pour éviter toute fragmentation. D'autre part, 802.15.4 a des caractéristiques de taux de pertes et de latence qui peuvent éliminer certains algorithmes (**R4** et **R5** pour les détails).

Les machines d'un LowPAN étant typiquement peu fiables (déplacement, extinction, panne), les protocoles de routage doivent se préparer à trouver des routes alternatives (exigence **R6**). Le RFC demande moins de deux secondes de convergence si le destinataire d'un paquet s'est déplacé et seulement 0,5 seconde si seul l'expéditeur a bougé (voir aussi le RFC 5826).

Les liens radio ayant souvent des caractéristiques asymétriques, **R7** demande que les protocoles de routage fonctionnent quand même dans ces conditions. Cela veut dire, par exemple, que le coût d'un lien doit être une paire {coût aller, coût retour}.

Chaque machine, dans un LowPAN, a droit à un sommeil fréquent (99 % de sommeil n'est pas impossible), pour économiser sa batterie (des capteurs industriels doivent parfois tenir cinq ans sans changement de batterie). **R8** en tire les conséquences en rappelant que le routage doit marcher même si certains nœuds hibernent. Et le calcul des coûts de routage doit inclure celui de la consommation électrique (il faut éviter de choisir comme routeurs les machines limitées en énergie).

La taille des LowPAN variant considérablement, le protocole de routage doit marcher aussi bien pour un réseau urbain de plusieurs millions de machines (RFC 5548) que pour un réseau de 250 machines dans une maison (RFC 5826). Rappelez-vous les contraintes de taille mémoire : pas question de stocker une table de routage d'un million d'entrées en mémoire !

Les machines se déplacent, dans un LowPAN. Dans les environnements industriels, il faut que le réseau fonctionne malgré des déplacements jusqu'à 35 km/h (RFC 5673). Aujourd'hui, on en est loin mais, en tout cas, **R12** exige des protocoles qui gèrent des réseaux qui changent, avec des machines qui bougent.

Et la sécurité, problème très crucial et très difficile pour les LoWPAN (un réseau sans-fil est toujours plus vulnérable) ? Non seulement un attaquant qui viserait le routage pourrait sérieusement perturber les communications entre les machines, mais il pourrait indirectement vider la batterie de certaines, réalisant ainsi une attaque par déni de service très efficace. L'exigence **R14** impose donc aux protocoles de routage candidats de fournir des services de confidentialité, d'authentification et de vérification de l'intégrité des messages. C'est beaucoup, vous trouvez ? Et pourtant cela ne protège pas contre tout (par exemple contre une machine authentifiée, mais malveillante). De toute façon, il ne faut pas se faire d'illusion : compte-tenu du coût élevé (en processeur et donc en énergie électrique) de la plupart des techniques de sécurité (notamment de la cryptographie à clé publique), le routage des LowPAN restera très peu protégé. Le RFC n'espère qu'un compromis raisonnable (un peu de sécurité, si ça ne coûte pas trop cher).

Il semble donc, note le RFC, que cela exclut IPsec, alors qu'il serait une solution élégante au problème, car il est bien trop consommateur de ressources et trop compliqué du point de vue de la gestion des clés.

À noter que 802.15.4 dispose de mécanismes de sécurité propres. S'ils sont activés, des protocoles comme NDP deviennent relativement sûrs. (La section 6 est également à lire, si on s'intéresse à la sécurité.)

Enfin, après la sécurité, la gestion : le RFC 5706 impose de la prendre en compte dès la conception du protocole. L'exigence **R18** demande donc que le futur protocole de routage des LowPAN soit gérable (test de l'état de la table de routage, compteurs d'erreurs, etc).