

# RFC 6568 : Design and Application Spaces for 6LoWPANs

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 mai 2012

Date de publication du RFC : Avril 2012

<https://www.bortzmeyer.org/6568.html>

---

Vous ne connaissez pas encore le terme de LowPAN? Ce n'est pas grave, c'est encore assez rare. Un LowPAN est un "*Low-Power Wireless Personal Area Network*". En gros, c'est un ensemble de petites machines (très petites : pas des ordinateurs), disposant de peu de puissance électrique, connectées souvent sans fil, et cherchant à communiquer. Le groupe de travail IETF 6lowpan <<http://tools.ietf.org/wg/6lowpan>> établit des normes de communication pour ces LowPAN, en utilisant IPv6 (d'où le 6 au début de son nom). Ce document est son quatrième RFC. Il explique les principes de base de son travail, à travers des scénarios d'utilisation des LowPAN.

Un LowPAN typique va être, dans une exploitation agricole, l'ensemble des capteurs qui mesurent l'humidité, et des actionneurs qui déclenchent l'arrosage. La section 1 explique les douleurs du LowPAN : machines ayant peu de ressources (processeur, mémoire, courant), et connectées par des liens lents et sujets aux parasites et aux coupures (WiFi, CPL). En général, on veut en prime que ces machines soient peu chères. Résultat :

- Certaines machines du LowPAN peuvent n'avoir qu'un CPU 8-bits de 10 MHz. (Des plus chanceuses auront des CPU ARM de 32 bits à 50 MHz.)
- Certaines n'auront que quelques kilo-octets de RAM et quelques dizaines de kilo-octets de ROM. Plus élaboré, le IMote <[http://www.ieee.org/Archive/Intel\\_mote.pdf](http://www.ieee.org/Archive/Intel_mote.pdf)> a 64 ko de RAM et une Flash de 512 ko.
- Fonctionnant souvent sur batterie, ces machines devront se limiter à une consommation de 10 à 30 mA pour la radio, limitant la puissance à 3 dBm et donc la portée à entre 30 et 100 mètres.
- La capacité de ces liens radio peut être entre 20 et 250 kb/s.

Bref, on est très loin des ordinateurs portables ou même des "*smartphones*". Et c'est pourtant dans ces machines qu'il va falloir faire tenir le code réseau. Deux bonnes lectures sur ces environnements si différents des machines sur lesquelles l'Internet a commencé : le RFC 4919<sup>1</sup> décrit plus en détail le monde des LowPAN, le RFC 4944 normalise l'utilisation d'IPv6 sur IEEE 802.15.4.

---

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc4919.txt>

Il existe en fait beaucoup de LowPAN différents. Suivant le document « *The Design Space of Wireless Sensor Networks* » <<http://wsn.cse.wustl.edu/images/8/8c/Wsn-design04.pdf>>, la section 2 du RFC explique les axes sur lesquels se différencient les LowPAN : déploiement conçu dès le début ou bien incrémental, taille du réseau (10 machines ou 1000?), connectivité permanente ou intermittente (ce qui est courant lorsque les machines se déplacent), etc.

Bien, maintenant, assez de précautions, place au cœur du RFC, la section 3. Elle expose une partie des scénarios d'usage des LowPAN. Par exemple, en section 3.1, figure un usage souvent cité, la surveillance de bâtiments industriels. L'idée est que les capteurs dispersés un peu partout dans les bâtiments deviennent communicants. Au lieu d'être relevés manuellement par un humain faisant sa ronde, ils transmettront d'eux-mêmes les résultats des mesures. De très nombreuses mesures peuvent être envisagées, comme les vibrations d'une machine (trop intenses, elles indiquent un problème) ou la température dans les entrepôts (attention à conserver la chaîne du froid). Les communications sans-fil sont ici cruciales car certaines parties de l'usine peuvent être difficiles à atteindre pour les câbles.

Comme exemple précis de ce type de surveillance, le RFC cite les salles de stockage d'un hôpital. Les globules rouges doivent être stockés entre 2 et 6°, les plaquettes entre 20 et 24°, et le plasma à -18°. Les capteurs de température sont disposés tous les 25 mètres environ, chaque emballage a une étiquette et des nœuds 6LowPAN sont placés dans les palettes. Par rapport aux axes de classification cités plus haut, on a un cas de déploiement planifié, avec un réseau de taille moyenne mais très dense, et peu de déplacements. Le débit attendu est faible mais les données peuvent être urgentes (alerte de réchauffement, par exemple). Les exigences de sécurité sont élevées. 6LowPAN peut-il convenir? Oui, analyse cette section.

Autre cas, celui de la surveillance d'un bâtiment, pour veiller à son intégrité (section 3.2). Par exemple, un pont est construit et est truffé de capteurs et de machines LowPAN qui relèvent les capteurs et transmettent à un contrôleur. Le RFC part d'un pont de 1 000 m de long, avec 10 piliers. Chaque pilier a 5 capteurs pour mesurer le niveau de l'eau sur le pont et 5 autres qui mesurent les vibrations. Les machines LowPAN ne sont pas gênées par les murs du bâtiment, comme dans l'exemple précédent, et peuvent se voir à 100 m de distance. Tout est placé manuellement (attention à ne pas avoir un pilier dans la LoS) et ne bouge pas.

Le réseau est cette fois de petite taille, très statique. Mais sa sécurité est vitale. Dans ce cas simple, 6LowPAN convient bien (il faut juste faire attention aux placements des engins sur les piliers).

Pas d'article ou de document sur les LowPAN sans l'inévitable bla-bla sur la domotique et ses promesses d'un monde merveilleux où le réfrigérateur détectera la fin proche du stock de bières et en commandera d'autres. C'est le rôle ici de la section 3.3. Après la santé et les transports, où des vies humaines sont en jeu, cette section se penche sur le confort de l'occidental rose moyen, qui veut que sa maison high-tech s'occupe de tout pendant qu'il regarde le match de foot à la télé.

Il y a beaucoup de choses à mesurer dans une maison, la température, l'humidité, l'état des portes (ouvert ou fermé), la vidéo-surveillance (pendant qu'on est dans les délires de mauvaise science-fiction, transformons la maison en bunker avec caméra braquée sur les quartiers sensibles). En combinant avec l'idée de « *Smart Grid* » (réseau de distribution électrique doté de capacités de mesure et de transmission de l'information), on peut aussi imaginer de connecter ces informations avec celle du réseau électrique.

Du point de vue technique, les murs de la maison feront souvent obstacle aux communications sans fil. Le réseau devra donc permettre le routage, pour le cas où la machine qu'on veut joindre n'est pas

directement visible (« *Multi-hop routing* »). Les fonctions de ce réseau de gadgets ne sont pas vitales, cette fois. Par contre, l'ergonomie est cruciale, le réseau devra être très simple à administrer.

Autre scénario d'usage, en section 3.4, l'assistance médicale. L'idée est de mettre les capteurs sur et dans le patient, de manière à pouvoir surveiller son état à tout moment. Pour une personne âgée à la maison, on peut imaginer quelques capteurs portés à même le corps et qui mesurent des choses comme les battements cardiaques, et d'autres capteurs dans la maison, captant les mouvements, par exemple pour pouvoir donner l'alerte en cas de chute. Les enjeux de sécurité, notamment de protection de la vie privée, sont très importants. Si le LowPAN est ici de petite taille, et que la mobilité est limitée, les contraintes de bon fonctionnement sont essentielles, puisqu'une vie humaine peut être en jeu.

Un scénario dans un univers plus technique est celui de l'automobile (section 3.5). Les nœuds LowPAN peuvent être inclus dans la route au moment de sa construction et surveiller les véhicules qui passent. Cela pose un sacré problème de durée de vie puisque les nœuds vont devoir durer autant que la route (typiquement, dix ans, avant la première réfection sérieuse qui permettra de les changer). Malgré cela, avec le temps, la densité des capteurs diminuera, au fur et à mesure des pannes. Les machines LowPAN de la route seront nombreuses mais statiques, celles des véhicules peu nombreuses mais très mobiles.

Enfin, le dernier exemple est un peu plus vert, puisqu'il concerne l'agriculture (section 3.6), celle qui, selon Jared Diamond <<https://www.bortzmeyer.org/gunsgermsteels.html>>, est à la base de la force des empires. L'idée est de mesurer à distance, via de nombreux capteurs, l'humidité, la température et l'état du sol, de manière à appliquer l'irrigation ou les pesticides au bon moment. Le RFC prend l'exemple d'une vigne de bonne taille (dans les huit hectares) où 50 à 100 machines de contrôle piloteront des centaines de capteurs. La principale difficulté, pour ces derniers, sera de résister à des conditions hostiles dehors (humidité, poussière, hommes et machines qui passent en permanence et font courir des gros risques aux fragiles capteurs), etc. Heureusement, les exigences de sécurité sont cette fois bien plus basses.

En parlant de sécurité, la section 4 y est entièrement consacrée. Elle rappelle que les machines d'un LowPAN sont souvent exposées dehors, et donc physiquement accessibles à un éventuel attaquant. Les méthodes de sécurisation doivent tenir compte de cela. La communication entre les machines du LowPAN est souvent par radio, médium qui n'offre aucune sécurité, permettant à l'attaquant de capter tout le trafic, voire d'injecter de fausses données. La cryptographie devient alors nécessaire.

Mais les machines d'un LowPAN ont des ressources, notamment d'énergie, très limitées. Elles sont donc vulnérables aux attaques par déni de service : des requêtes répétées et hop, la batterie est à plat. À cause de cela, les techniques de sécurité adoptées doivent être légères et ne pas abuser des ressources très limitées de ces petits engins. Par exemple, IPsec est probablement exagéré pour ces environnements, en raison des calculs qu'il entraîne. Cela doit évidemment s'adapter à l'usage envisagé : le nœud LowPAN qui allume une lampe n'a pas les mêmes contraintes de sécurité que celui qui contrôle un stimulateur cardiaque.