RFC 5867 : Building Automation Routing Requirements in Low Power and Lossy Networks

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 12 juin 2010

Date de publication du RFC : Juin 2010

https://www.bortzmeyer.org/5867.html

Nouveau « cahier des charges » du groupe de travail ROLL <http://tools.ietf.org/wg/roll> de l'IETF, ce RFC décrit les exigences du protocole de routage des réseaux difficiles (peu de courant et beaucoup de parasites), pour le cas des immeubles de bureaux. Le cas de la maison avait été traité dans le RFC 5826 [1].

Les immeubles de bureaux sont remplis de systèmes techniques complexes, collectivement dénommés HVAC (pour "*Heating, Ventilation and Air Conditioning*", même s'il faut ajouter les ascenseurs, les alarmes incendie, l'éclairage, etc). Ces systèmes tendent de plus en plus à être informatisés, puis à communiquer entre eux, ou bien avec une centrale de contrôle. Les exigences particulières de cet environnement (par exemple le fait que certains appareils fonctionnent sur batterie et ne doivent donc pas gaspiller l'énergie) font que les mécanismes de routage IP traditionnels ne sont pas forcément adaptés.

Autrefois, de tels systèmes étaient connectés, comme le rappelle le RFC, par un lien pneumatique, maintenant, c'est un réseau informatique local, qui doit pouvoir être partitionné en sous-réseaux, reliés par des routeurs. Notre RFC se penche donc sur le futur protocole de routage.

J'ai parlé d'une centrale de contrôle. En fait, il s'agit d'un système de contrôle bien plus complexe, en général dénommé FMS (pour "*Facility Management System*", en Europe, on dit plutôt BMS pour "*Building Management System*", et GTB en français) et qui a la lourde responsabilité de piloter des immeubles allant jusqu'au gratte-ciel de cent étages et de cent mille mètres carrés de surface totale (à noter que le RFC, suivant les mœurs du BTP états-unien, utilise encore les pieds carrés...) ou bien à des immeubles très complexes comme le Pentagone.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5826.txt

La section 3 du RFC décrit l'organisation générale d'un FMS. En 3.2, on découvre le bestiaire qui peuple un immeuble de bureaux (capteurs, contrôleurs, etc). En 3.3, les méthodes utilisées pour l'installation de cet équipement. Le réseau informatique traditionnel est installé en commençant par le câblage, puis les équipements actifs, puis enfin les terminaux. Le FMS, au contraire, croît à partir d'équipements installés immédiatement, puis connectés petit-à-petit et ensuite reliés aux systèmes centraux, voire au réseau informatique « normal » (voir aussi section 5.6). Les raisons de cette méthode sont en bonne partie organisationnelles : tous les corps de métier n'accèdent pas au bâtiment en même temps. D'autre part, certains systèmes de sécurité (comme la détection incendie) doivent être en place très tôt dans la vie de l'immeuble, avant qu'on ne branche l'électricité partout. Le système de détection du feu ne peut donc pas compter sur des serveurs DNS ou DHCP déjà en place.

Enfin, la section 3.4, très détaillée et où le lecteur informaticien qui n'a pas d'expérience du bâtiment apprendra bien des choses, explique les problèmes spécifiques liés à la densité des machines. Par exemple, la tendance actuelle à la vidéo-surveillance a nettement accru le nombre de caméras, et celles-ci sont inégalement réparties. Autrefois, de tels systèmes utilisaient des réseaux fermés mais, aujourd'hui, c'est de plus en plus souvent un bête réseau IP qui connecte les caméras. (Elles posent d'autres problèmes, comme le débit de données important qu'elles fournissent, par rapport aux équipements FMS traditionnels.)

Tiens, à propos de capacité nécessaire, quelles sont les caractéristiques du trafic des équipements de l'immeuble ? La section 4 analyse quantitativement (200 octets pour un message typique au contrôleur, envoyé toutes les minutes..., 30 % des paquets restent sur le réseau local et 70 % ont besoin d'être routés...) et qualitativement (lors d'une coupure de courant, le plus dur est la reprise, lorsque les machines alimentées par batterie vont tout à coup essayer de transmettre les données qu'elles avaient stockées) le trafic sur le réseau du FMS.

Puis le cœur de notre RFC, la section 5, expose le cahier des charges proprement dit. Comme l'installation est souvent faite par des non-informaticiens (des électriciens, par exemple), tout le réseau doit pouvoir être auto-configurable, sans aucune action humaine (section 5.1.1). Le routage doit pouvoir commencer tout de suite (section 5.1.2), sans intervention d'un administrateur réseaux.

Le réseau doit pouvoir fonctionner pour des immeubles de cent mille mètres carrés. Le RFC demande que les protocoles marchent avec des réseaux de deux mille machines, dont la moitié routent des paquets pour le compte des autres (section 5.2.1). Un sous-réseau (par exemple une pièce) doit accepter 255 machines. Et chaque machine doit pouvoir parler directement à n'importe quelle autre, en pair-à-pair. Par exemple, si les tours de refroidissement sont sur le toit et le refroidisseur dans le sous-sol, vue sa taille, ils doivent néanmoins pouvoir se parler (section 5.2.2).

La plupart des machines dans l'immeuble sont fixes, accrochés au mur ou dans un faux plafond. Il n'y a donc pas d'énormes exigences de mobilité (section 5.3). Toutefois, les équipements mobiles se répandent et le RFC ajoute donc quelques demandes pour eux :

— Possibilité d'exclure les engins en déplacement des fonctions de routeur (section 5.3.1),
— Moins de cinq secondes après un déplacement pour pouvoir parler sur le réseau à nouveau, si on est restés sur le même sous-réseau (et dix autrement),

Les équipements de l'immeuble sont souvent très limités dans leurs ressources matérielles. La section 5.4 liste donc les règles à suivre pour ne pas les épuiser :

— Le logiciel doit pouvoir tourner sur un processeur 8-bits avec 128 ko de mémoire flash (section 5.4.1), et sur 256 ko si la machine sert à router les paquets (avec seulement 8 ko de RAM),
— Un capteur typique doit pouvoir durer cinq ans avec une batterie de 2000 mAh (pour un transmetteur de 25 ma et une émission par minute, section 5.4.3). Le logiciel doit donc absolument être économe et ne pas provoquer des émissions inutiles. Le RFC demande de garder un message (et de retransmettre) pendant au moins 20 secondes si le destinataire ne répond pas (il peut être en train de dormir pour économiser sa batterie).

Il existe aussi des exigences pour la sélection des routes. Ainsi, le RFC demande que les applications prioritaires (alarme incendie, par exemple) puissent prendre le pas sur les autres (section 5.7.7).

Enfin, le cahier des charges se conclut par une longue section sur la sécurité (section 5.8). D'abord, s'il y a une configuration de la sécurité, celle-ci doit pouvoir être faite via le réseau (beaucoup d'équipements seront en effet peu accessibles). Cette configuration par le réseau est délicate à réaliser mais nécessaire puisque le même équipement peut être installé dans des immeubles aux règles de sécurité très variables (petite entreprise banale vs. bâtiment Seveso). Idéalement, toute communication devrait être chiffrée, puisqu'on ne peut pas espérer qu'il n'y ai jamais de méchant indiscret sur le trajet. Mais, d'un autre côté, les équipements installés dans l'immeuble ont souvent des moyens limités et la cryptographie coûte cher. Le RFC demande donc simplement que les deux arguments, de sécurité et d'économie, soient pris en considération.

Une autre règle sur le chiffrement (section 5.8.3) est que les protocoles développés par le groupe ROLL **doivent** inclure le chiffrement mais cela n'implique pas que l'implémentation le permette, ni que le responsable sécurité l'active obligatoirement.

Un cahier des charges tourne toujours facilement à la « lettre au Père Noël », où on accumule des dizaines de demandes toutes plus irréalistes que les autres. La valeur d'un bon cahier des charges n'est donc pas dans les demandes mais plutôt dans ce que les auteurs ont eu le courage d'écarter. Pour ce RFC, ces exigences non retenues ont fini dans l'annexe A : intéressantes idées mais qui ne sont pas considérées par le groupe de travail ROLL comme obligatoires. Par exemple, la section A.3.5 dit que cela serait sympa si le protocole de routage permettaient à certains routeurs, les plus limités en mémoire, de ne garder qu'une partie des routes. La A.4.1 voudrait bien imposer une limite basse de capacité à 20 Kb/s...

Merci à Nicolas Riou pour sa relecture (mais, bien évidemment, les erreurs sont de moi).