RFC 7368 : IPv6 Home Networking Architecture Principles

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 1 novembre 2014

Date de publication du RFC : Octobre 2014

https://www.bortzmeyer.org/7368.html

Le projet Homenet <https://tools.ietf.org/wg/homenet> de l'IETF est très ambitieux. Il s'agit de définir une architecture et des protocoles pour des réseaux IPv6 à la maison. Non seulement tout doit marcher « tout seul » (on ne peut pas demander à M. Michu de lire le RFC, ou même la documentation) mais en outre le groupe de travail Homenet prévoit deux innovations principales par rapport aux réseaux IPv4 des maisons actuelles : un inter-réseau à la maison (plusieurs réseaux séparés par des routeurs) et pas de NAT, la plaie des communications actuelles. Ce premier RFC du groupe de travail Homenet <https://tools.ietf.org/wg/homenet> décrit l'architecture générale envisagée.

La tendance générale dans les maisons modernes est à la prolifération des équipements électroniques. Si toutes les maisons ne connaissent pas encore la situation de la célèbre Maison qui tweete <https://twitter.com/Maisonquitweet>, il n'y a pas de doute que les vingt dernières années ont vu un changement de modèle avec le passage de « à la maison, un ordinateur et un seul, connecté au réseau » à « deux ou trois dizaines d'équipements électroniques dont beaucoup sont connectés au réseau, au moins de temps en temps ». Entre les "*smartphones*", les compteurs intelligents, l'Arduino qui arrose les plantes, la "*box*", le PC du joueur de jeu vidéo, les tablettes de tout le monde, et la télé connectée <http://www.brennancenter.org/analysis/im-terrified-my-new-tv-why-im-scared-turn-thing>, on atteint vite un nombre de machines connectées bien supérieur à la totalité de l'Arpanet du début. Il y a bien longtemps qu'il n'y a plus assez d'adresses IPv4 <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html> pour tout ce monde. L'architecture typique aujourd'hui (pas réellement documentée, car jamais vraiment réfléchie et étudiée) est d'un réseau à plat (pas de séparation des machines, tout le monde est sur la même couche 2), avec numérotation des équipements avec les adresses IPv4 privées du RFC 1918 [1] et connexion à l'Internet via un unique FAI. Homenet vise au contraire des réseaux IPv6 (IPv4 peut continuer à tourner sur un réseau Homenet mais à côté, car Homenet ne prévoit rien de particulier pour lui), non gérés (M. Michu...) et connectés à plusieurs FAI, pour la résilience, pour compenser les faiblesses ou manques d'un FAI par un autre (bridage de YouTube, par exemple...) ou tout simplement

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1918.txt

parce que des tas d'offres de connectivité sont disponibles (pensez au "*smartphone*" qui a le choix entre la 3G et le WiFi).

Homenet ne sera pas un protocole unique. L'idée du projet est d'analyser ce qui existe, de réutiliser autant que possible les protocoles existants et testés, et d'identifier ce qui manque, pour pouvoir ensuite l'ajouter. Homenet se focalise sur la couche 3 et quelques services indispensables, comme la résolution de noms. Les protocoles physiques sous-jacents sont tous acceptés, du moment qu'IPv6 peut tourner dessus.

L'explosion du nombre d'équipements connectés est déjà largement une réalité (donnant naissance à des slogans plus ou moins pipeau comme « Internet des objets »). Le routage interne (plusieurs réseaux à la maison, séparés par des routeurs) est par contre encore embryonnaire. Mais Homenet vise le futur (ce qui explique aussi pourquoi les questions liées à IPv4 ne sont pas abordées, cf. section 3.2.3). À noter qu'il existe déjà une description du routeur IPv6 idéal pour la maison, dans le RFC 7084.

Comme tout document d'architecture, le RFC Homenet commence avec de la terminologie (section 1.1). Ainsi, la **frontière** ("*border*") est l'endroit où on change de domaine administratif et où on applique donc les règles de sécurité (filtrage, par exemple). Chaque réseau derrière une frontière se nomme un royaume ("*realm*"). Le CER ("*Customer Edge Router*") est le routeur qui est à la frontière. Il peut y en avoir plusieurs (un point important de Homenet, qui avait été chaudement discuté, est que Homenet doit gérer le cas où il y a plusieurs FAI). Homenet prévoit plusieurs routeurs à la maison et le réseau des invités ("*guest network*") est un réseau interne conçu pour les visiteurs et n'ayant pas forcément accès à tous les services du réseau de la maison (pour pouvoir fournir un accès WiFi à vos invités sans qu'ils puissent fureter dans votre collection de "*sex tapes*" sur le NAS). Si FQDN est bien connu, Homenet utilise aussi le sigle LQDN ("*Locally Qualified Domain Name*", un nom qui n'a de signification que local).

Attaquons maintenant le problème de créer des "*homenets*". La section 2 fait le point des différences entre IPv4 et IPv6 qui vont avoir un impact sur le réseau à la maison (ou dans le petit bureau d'une petite organisation). Premièrement (section 2.1), IPv6 permet d'avoir plusieurs réseaux à la maison. C'est possible également en IPv4, mais uniquement avec des adresses privées, on a rarement des préfixes IPv4 assez grands pour les découper finement. En revanche, IPv6 permettrait de faire plus facilement des réseaux multiples, par exemple pour séparer le réseau des invités, ou bien pour avoir un réseau de l'employeur, étendu à la maison via un VPN, mais séparé du réseau personnel. Une autre raison pour le multi-réseaux est que les technologies de couche 1 et de couche 2 deviennent de plus en plus hétérogènes, notamment en raison de l'apparition de techniques dédiées aux objets limités (peu de puissance électrique, peu de capacités de calcul, etc). Des écarts de trois ordres de grandeur (de 1 Mb/s à 1 Gb/s) sont courants aujourd'hui et tendent à s'élargir. Pour éviter d'aligner Ethernet sur le plus grand dénominateur commun de ces réseaux limités (RFC 7102), il faut bien partitionner en plusieurs réseaux IP et router entre eux.

Cela implique d'avoir un préfixe IPv6 plus général qu'un /64. Le /64 permet un nombre colossal d'adresses mais ne permet qu'un seul préfixe, donc qu'un seul réseau, en tout cas tant qu'on garde l'auto-configuration sans état du RFC 4862. C'est pour cela que le RFC 6177 recommande d'allouer à M. Michu des préfixes suffisants pour tous ses usages, y compris futurs.

Donc, avoir plusieurs réseaux IP à la maison serait très bien. Mais ce n'est pas trivial. Il faut allouer ces préfixes (rappelons que le réseau à la maison n'est **pas** géré, M. Toutlemonde ne va pas installer un logiciel d'IPAM et concevoir un plan d'adressage). Et les mécanismes existants pour le réseau sans configuration (comme le mDNS du RFC 6762) ne fonctionnent pas en multi-réseaux (ils dépendent de la diffusion, qui s'arrête au premier routeur rencontré).

Deuxième propriété importante d'IPv6, la possibilité d'avoir des adresses uniques au niveau mondial et donc l'élimination du NAT (section 2.2). C'est à la fois une chance formidable de retrouver la communication directe de bout en bout qui a fait le succès de l'Internet, et aussi un risque car tout trafic sur l'Internet n'est pas souhaitable, et beaucoup d'engins connectés ont une sécurité... abyssale (imprimantes ou caméras <http://www.shodanhq.com/> avec des mots de passe par défaut, et jamais changés <http://www.lemouv.fr/diffusion-des-milliers-d-objets-connectes-vous-mettent-a-poil-sur-i
Une connectivité de bout en bout nécessite une meilleure sécurité des machines, ou alors des pare-feux IPv6 protégeant le réseau. S'agissant de ces pare-feux, notre RFC Homenet note qu'il faut distinguer adressabilité et joignabilité <http://fr.wiktionary.org/wiki/joignabilit%C3%A9>. IPv6 fournit l'adressabilité (toute machine, si humble soit-elle, a une adresse IP unique) mais on ne souhaite pas forcément la joignabilité (je ne veux pas que le voisin se connecte à ma caméra IP).

À noter qu'il existe un débat très chaud à l'IETF concernant les recommandations à faire pour la politique de sécurité par défaut d'un pare-feu à la maison. Les RFC 4864 et RFC 6092 discutent des mérites comparés des politiques « bloquer tout par défaut, sauf quelques exceptions » et « autoriser tout par défaut, avec quelques exceptions ».

Bien sûr, une des nouveautés les plus spectaculaires d'IPv6 est la disponibilité d'un grand nombre d'adresses. Mais on oublie souvent une autre nouveauté, le fait qu'avoir plusieurs adresses IP n'est plus un bricolage spécial, mais devient la norme (section 2.3). Cela entraine des questions nouvelles comme « quelle adresse IP source choisir pour les connexions sortantes ? » (RFC 6724).

IPv6 permet de disposer d'adresses purement locales (section 2.4 de notre RFC), attribuées sans référence à un registre central, les ULA ("*Unique Local Addresses*", RFC 4193 et RFC 7084 pour leur usage dans les CER). Comme M. Michu n'a typiquement pas d'adresses IP à lui, les adresses externes de sa maison ou de sa petite association seront sans doute des adresses attribuées par le FAI. Pour la stabilité, il est donc recommandé d'y ajouter des ULA, qui permettront aux machines locales de se parler en utilisant toujours les mêmes adresses, même en cas de changement de FAI. Comme toutes les adresses privées, les ULA isolent des changements extérieurs. Par contre, elles n'impliquent pas de faire du NAT, même pas du NAT IPv6 (RFC 6296). La machine est censée utiliser son ULA lorsqu'elle communique avec le réseau local et une adresse publique lorsqu'elle communique avec l'extérieur (c'est le comportement par défaut si le RFC 6724 a été implémenté correctement sur la machine). Homenet déconseille donc toute forme de NAT IPv6, même celle du RFC 6296 (pourtant bien meilleure techniquement que le NAT d'IPv4).

Un autre avantage des ULA est que les machines qui n'ont pas besoin de communiquer avec l'extérieur (une imprimante, par exemple), n'ont pas besoin d'adresse publique et peuvent donc se contenter de l'ULA.

Dans les réseaux IPv4, on voit parfois des équipements exposer leur adresse IPv4 à l'utilisateur, par exemple pour pouvoir la changer manuellement. Les adresses IPv6 étant plus longues, plus difficiles à mémoriser et plus aléatoires d'apparence, cette pratique est déconseillée pour Homenet (section 2.5). Pas touche aux adresses !

Enfin, dernier point spécifique à IPv6, le fait que certains réseaux seront peut-être seulement en IPv6. Si on part de zéro aujourd'hui (déploiement "*greenfield*" en anglais), il n'y a guère de raison de mettre de l'IPv4. Ne faire que de l'IPv6 simplifie le réseau et sa gestion, par contre cela implique que chaque machine sache tout faire en IPv6 (par exemple, il existe des systèmes qui ont une gestion d'IPv6 complète, sauf pour les résolveurs DNS qui doivent être accessibles en IPv4). Évidemment, même si le réseau local peut être entièrement IPv6, il faudra encore, pendant un certain temps, communiquer avec des machines purement IPv4 et donc déployer des solutions de coexistence comme celle du RFC 6144.

Sur ce, la section 2 du RFC Homenet est terminée. Vous savez désormais ce qu'il faut savoir d'important sur IPv6, place aux principes d'architecture de Homenet en section 3. Comment construire des réseaux IPv6 à la maison avec les techniques IPv6 ? Et ce avec des engins variés, connectés en une topologie quelconque, sans configuration manuelle ou, en tout cas, sans qu'elle soit obligatoire ? La section 3.1 pose les principes de base :

— Autant que possible, réutiliser des protocoles existants. Homenet est ambitieux mais conservateur.
— Imposer le moins de changements possibles aux machines, routeurs ou machines terminales.

Les topologies (façons dont les réseaux qui forment le "*homenet*" sont connectés) doivent pouvoir être quelconques (section 3.2). Les utilisateurs vont sans doute connecter sans réfléchir et on ne veut pas leur imposer des règles comme « ne pas faire de boucles » ou « le réseau doit avoir une topologie strictement arborescente ». Le réseau doit continuer à fonctionner tant qu'il n'est pas physiquement partitionné. Par exemple, si deux commutateurs sont connectés en une boucle, le commutateur doit le détecter (en voyant son adresse MAC à l'extérieur) et réparer tout seul. Le réseau doit pouvoir être dynamique : il doit accepter non seulement l'ajout ou le retrait de machines mais également les changements dans la connectivité. Le RFC 7084 donne des idées de configurations qui doivent fonctionner. Parmi les propriétés d'un réseau qui ont une particulière importance :

— La présence ou non de routeurs internes (très rare à l'heure actuelle),
— Présence de plusieurs réseaux physiques interconnectés uniquement via l'Internet,
— Gestion du CER ("*Customer Edge Router*") par l'utilisateur ou par le FAI (le RFC ne mentionne pas le cas plus compliqué où l'utilisateur doit utiliser le CER du FAI mais peut configurer certains aspects),
— Nombre de FAI (presque toujours un seul aujourd'hui mais cela pourrait changer, notamment pour avoir davantage de résilience),
— Et nombre de CER (il n'y en a pas forcément qu'un seul par FAI).

Le cas le plus commun aujourd'hui est un seul FAI, un seul CER, pas de routeurs internes. Le cas le plus simple dans le RFC est celui de la section 3.2.2.1 : un seul FAI, un seul CER mais des routeurs internes. (Les sections suivantes présentent des cas plus compliqués.)

Le "*multi-homing*" présente des défis spécifiques. Une partie du groupe de travail Homenet aurait préféré travailler sur des réseaux ayant un seul FAI, où la plus grande partie des services permettant de faire fonctionner le "*homenet*" aurait été fournie par le FAI. Cela simplifiait nettement le problème mais au prix d'une grosse perte d'indépendance pour l'utilisateur. Sans surprise, cette position était surtout défendue par les gens qui travaillent pour les FAI, ceux qui travaillent pour les fabriquants de routeurs préférant du "*multi-homing*", avec plein de routeurs partout. Le "*multi-homing*" reste relativement simple s'il n'y a qu'un seul CER, connecté aux différents FAI. Des fonctions comme la sélection d'un FAI en fonction de l'adresse IP source peuvent être entièrement gérées dans le CER. S'il y a plusieurs CER, il faut que chaque machine choisisse le bon CER de sortie. « Bon » au sens qu'il doit être cohérent avec l'adresse IP source (utilisation des adresses du préfixe du FAI) pour éviter le filtrage par les techniques anti-usurpation dites BCP 38 <https://www.bortzmeyer.org/bcp38.html> (RFC 2827 et RFC 3704). La question du "*multi-homing*" est récurrente à l'IETF et mène souvent à des solutions assez complexes, peut-être trop pour le "*homenet*". Par exemple, une solution possible serait de faire tourner les protocoles de routage sur toutes les machines, de façon à ce que même les machines terminales apprennent les routes et sachent quel routeur contrôle quel réseau. Le RFC 7157 décrit une solution plus simple (qui évite la traduction d'adresses du RFC 6296, déconseillée pour le projet Homenet). Il y a aussi d'utiles techniques qui sont entièrement dans les machines terminales, sans mettre en jeu le réseau, comme SHIM6 (RFC 5553), MPTCP (RFC 6824) ou les globes oculaires heureux du RFC 6555.

Parmi les pièges du "*multi-homing*", le RFC note que certains des FAI peuvent ne pas fournir une connectivité complète. Un exemple est celui du télé-travailleur où le réseau local est "*multihomé*" vers l'Internet et vers le réseau de l'employeur, via un VPN, et où le réseau de l'employeur ne donne pas accès à tout l'Internet. Homenet ne fournit pas de solutions à ce sous-problème. (Un autre cas où il se pose, plus polémique et non cité par le RFC, est celui où l'un des FAI bride, filtre ou censure, en violation de la neutralité <https://www.bortzmeyer.org/neutralite.html>.)

Le réseau à la maison doit évidemment être entièrement auto-configuré, puisqu'on ne souhaite pas que M. Toutlemonde soit obligé de devenir administrateur réseaux (section 3.3). C'est plus facile à dire qu'à faire. Par exemple, il faut éviter que n'importe quelle machine qui se trouve passer dans les environs puisse rejoindre le réseau alors que sa présence n'est pas souhaitée. L'utilisateur doit donc avoir un moyen simple de tenir à distance les importuns et donc de dire « cette machine est bienvenue ». Il y a d'intéressants problèmes d'interface utilisateur ici... Un exemple d'un moyen simple est la pression quasi-simultanée de deux boutons, un sur la nouvelle machine qui arrive et un sur le routeur.

En parlant de sécurité et de « eux » et « nous », il faudra bien que le "*homenet*" soit conscient de l'étendue de son royaume afin, par exemple, d'appliquer des politiques de sécurité différentes entre les communications internes et externes. Sans compter les frontières à l'intérieur même de la maison, comme entre le réseau des enfants et l'extension virtuelle du réseau de l'entreprise de Maman. Comme souvent, le RFC demande que cela soit automatique, mais avec possibilité de changement manuel si on a une configuration très spéciale.

Et l'adressage (section 3.4) ? Ah, c'est une question compliquée. D'abord, le "*homenet*" sera dépendant de ce que lui aura alloué le ou les FAI. Espérons qu'ils suivent les politiques du RFC 6177 et lui donnent donc assez d'adresses et en tout cas plus que le pauvre /64 que certains FAI distribuent aujourd'hui à leurs abonnés, et qui ne leur permet pas d'avoir facilement plusieurs réseaux à la maison. Le RFC 6177 n'imposant plus une longueur unique aux allocations, le "*homenet*" récupérera peut-être un /60, un /56 ou un /48 (notre RFC recommande un /56 ou plus général). Le protocole de récupération du préfixe sera sans doute celui du RFC 3633. Il permet au "*homenet*" de solliciter une certaine longueur de préfixe, mais sans garantie que le FAI ne lui enverra pas un préfixe plus spécifique. Là encore, la délégation de préfixe peut échouer (si la liaison avec le FAI est coupée) et le "*homenet*" doit donc pouvoir fonctionner seul, y compris pour son adressage. Une nouvelle raison d'utiliser les ULA. Rappelez-vous que ce RFC est juste une architecture, il ne définit pas en détail les protocoles utilisés, mais il note ici qu'il faudra sans doute une et une seule méthode de délégation de préfixe, pour que tous les routeurs du réseau local soient d'accord sur les adresses à utiliser.

Il est préférable que les préfixes utilisés en interne soient stables, et notamment survivent au redémarrage des routeurs. Cela implique un mécanisme de stockage permanent des données sur les routeurs, ainsi que, de préférence, un moyen de tout remettre à zéro s'il y a une reconfiguration significative.

À propos de stabilité, il faut noter que, bien qu'elle facilite nettement le fonctionnement du réseau, elle a aussi des inconvénients en terme de vie privée. Si le préfixe alloué à un client du FAI reste stable, il aura à peu près le même effet qu'une adresse IPv4 fixe : les machines avec qui communique le client pourront voir que plusieurs requêtes viennent de la même maison. Le NAT (en IPv4) ou les extensions de vie privée (en IPv6, cf. RFC 8981) n'aident pas contre cette indiscrétion.

La section 3.5 discute ensuite de la question du routage interne. En effet, une des nouveautés du projet Homenet est de considérer qu'il y aura des routeurs internes et donc du routage à faire entre les différents réseaux de la maison. Là encore, tout doit se configurer tout seul donc il faudra problablement choisir un protocole de routage dynamique, de préférence un protocole existant et déjà testé, mais qui tient compte des exigences particulières de Homenet (par exemple le peu de ressources matérielles des routeurs internes).

Que des gros problèmes compliqués, non ? Chacun d'entre eux a déjà de quoi distraire une équipe d'ingénieurs pendant un certain temps. Mais ce n'est pas fini. La section 3.6 s'attaque à la sécurité. Le problème est difficile car on ne veut évidemment pas que les voisins récupèrent les selfies qu'on a laissés sur l'appareil photo connecté <http://www.slate.fr/story/91907/celebgate-mes-photos-intimes-sur-in
mais on veut également une grande simplicité de configuration (voire zéro configuration), ce qui va

généralement mal avec la sécurité. La disparition souhaitée du NAT ajoute en outre une nouvelle composante au problème. Il sera difficile d'éviter une réflexion sur la sécurité des machines (abyssalement basse, aujourd'hui), la protection offerte par le réseau ayant ses limites (surtout si on veut que chaque brosse à dents puisse communiquer sur l'Internet). L'un des buts d'Homenet est de rétablir le principe des communications de bout en bout (RFC 2775). Mais cela ne signifie pas "*open bar*" pour tout le trafic et notre RFC distingue donc bien le fait d'être mondialement adressable (adresse IPv6 unique) et celui d'être mondialement joignable (n'importe quel "*script kiddie*" peut tenter une attaque sur la brosse à dents IP). Le RFC 4864 proposait un modèle de sécurité fondé sur un pare-feu protégeant le périmètre, considérant qu'on ne pouvait pas espérer que toutes les machines soient sécurisées. La polémique se concentre évidemment sur la politique par défaut de ce pare-feu. On sait bien que très peu de gens changeront cette politique donc elle a une importance cruciale. Un blocage par défaut ("*default deny*") ferait retomber dans les problèmes du NAT où des tas d'applications (serveur auto-hébergé, pair-à-pair) sont interdites, sauf à déployer des techniques d'ouverture de pare-feu comme UPnP ou le PCP du RFC 6887. Le RFC 6092 ne suivait donc pas cette approche du « interdit par défaut », et recommandait que, même si elle était choisie, il soit facile de revenir à un mode d'autorisation par défaut, celui qui permet l'innovation et le déploiement de nouveaux services. La question continue à susciter d'innombrables discussions à l'IETF et il est clair qu'il n'existe pas de consensus entre les partisans du « interdit par défaut » et ceux du « autorisé par défaut ».

Par contre, il est certain que, comme indiqué plus haut, tout trafic n'est pas souhaitable. Le principe fondateur de connectivité de bout en bout, c'est « deux machines qui le souhaitent doivent pouvoir communiquer directement », pas « je dois supporter n'importe quel trafic qu'un crétin quelconque veut m'envoyer ». Par exemple, comme indiqué plus haut, on peut souhaiter isoler le trafic du réseau des invités. Filtrer à la frontière sera donc toujours nécessaire.

Est-ce que le NAT ou les pare-feux actuels assurent cette fonction de manière satisfaisante ? Pour le NAT, clairement non <https://www.bortzmeyer.org/nat-et-securite.html>. Pour les pare-feux, la religion actuelle des pare-feux (auditeurs ignorants qui vous reprochent de ne pas avoir de pare-feu devant un serveur Internet public, managers qui croient qu'ils ont traité les problèmes de sécurité en installant une boîte noire très chère marquée en gros "*Firewall*"...) ne peut pas masquer les innombrables problèmes de sécurité qui affectent les utilisateurs pourtant situés derrière un pare-feu (distribution de "*malware*" par le courrier, par exemple). Une des plus grosses faiblesses de la religion du pare-feu est qu'elle suppose que les méchants sont uniquement à l'extérieur : résultat, la compromission d'une seule machine à l'intérieur suffit à annuler l'effet du pare-feu. Donc, la situation actuelle n'est pas satisfaisante. Néanmoins, pour un réseau typique, on peut difficilement se passer aujourd'hui du pare-feu. Autant on peut sécuriser un serveur Internet sérieux, géré par des professionnels, autant on ne peut pas compter sur les innombrables objets connectés : la plupart d'entre eux ont zéro sécurité (serveur Web d'administration activé par défaut, avec un mot de passe identique pour toutes les machines et jamais changé, et un CGI écrit en bash pour faire bonne mesure). Il est donc nécessaire que la sécurité soit assurée en dehors de ces machines, par un pare-feu. Donc, avoir cette fonction de protection, ainsi que la politique « tout interdit sauf ce qui est autorisé » (même si elle n'est pas activée par défaut) est utile, comme demandé par le RFC 7084. Cela ne doit pas faire oublier qu'il faut aussi pouvoir permettre aux machines du réseau de communiquer, lorsqu'elles en ont besoin.

Autre grande question des systèmes répartis, le nommage (section 3.7). Il ne fait pas de doute que Jean-Michu Toutlemonde préférera des noms parlants et surtout stables, aux adresses IPv6. À chaque changement de FAI, le préfixe IPv6, et donc les adresses, changera, alors que les noms resteront. Il faut donc des noms et, comme toujours dans le projet Homenet, que ces noms puissent être attribués sans administration explicite (à part éventuellement la saisie du nom dans une interface simple ; les autres machines devront s'attribuer un nom unique automatiquement). D'autre part, il faudra pouvoir découvrir des services (par exemple, une imprimante, ou bien un NAS), typiquement via une interface graphique qui affichera tous les services trouvés dans le réseau. Les protocoles existants à cette fin (comme celui du RFC 6763) sont typiquement mono-réseau et fonctionnent en criant à la cantonade « Y a-t-il une

imprimante dans la salle ? » Avec les "*homenets*" composés de plusieurs réseaux, il faudra une autre approche.

En parlant de découverte de service, il est important de faire une distinction entre **résolution** ("*lookup*") et **découverte** ("*discovery*"). La première consiste à trouver les informations (comme l'adresse IP) à partir d'un nom connu et existant. La seconde à trouver des noms (s'il y en a) correspondant à un certain critère. Homenet va avoir besoin d'un service de noms fournissant ces deux fonctions. Il est évidemment souhaitable, en application du principe qu'Homenet doit réutiliser autant que possible les protocoles existants, que cela soit le DNS (ou une variante comme celle du RFC 6762). Notre RFC voudrait même en plus qu'on puisse utiliser DNSSEC (RFC 4033) ce qui est très souhaitable pour la sécurité, mais tout en gardant cette absence de configuration, ce qui va être difficile.

D'autre part, on voudrait pouvoir utiliser un espace de nommage public, celui des noms de domaine, mais tout en gardant l'aspect « zéro configuration ». La question « un espace de noms ou plusieurs » n'est pas tranchée par ce RFC. Si on veut accéder aux engins de la maison depuis l'extérieur, il faudra bien utiliser l'espace public et unique (celui d'aujourd'hui, là où se trouvent les noms comme `www.potamochère.fr`, qui marchent sur toute la planète). Si les noms dans cet espace public dépendent du FAI (par exemple `jean-jacques.michu.free.fr`), l'utilisateur dépendra de son FAI. Le RFC souhaite donc qu'Homenet fonctionne avec des noms de domaine personnels, qui assurent à l'utilisateur son indépendance. Même dans le cas où on a des noms mondiaux, le RFC demande qu'on puisse avoir en plus un espace de noms purement local, qui ne fonctionne que sur le "*homenet*" (de la même façon qu'il recommande des adresses IPv6 publiques **et** des ULA). Le TLD `.local` ne convient pas forcément à cet usage car il est lié à un protocole particulier (le mDNS du RFC 6762). Il faudra donc un nouveau TLD pour les "*homenets*" multi-réseaux (ou bien attendre une éventuelle extension de mDNS, dont le RFC ne parle pas). Une fois le nouveau TLD défini (`.sitelocal` ? `.home` ?), les noms dans ce TLD seront des ALQDN ("*Ambiguous Local Qualified Domain Name*"), des noms ambigus car plusieurs réseaux pourront utiliser le même (par exemple Jean-Jacques Michu et Jennifer Michu auront tous les deux un `michu.sitelocal`). Ces noms sont casse-gueule car on ne peut jamais exclure qu'un utiliseur ne mémorise un tel nom lorsqu'il est sur un des réseaux et l'utilise après sur un autre réseau où cela ne marchera pas ou, pire, où cela l'entrainera sur un autre service que celui attendu. Une façon de résoudre le problème est d'avoir des ULQDN ("*Unique Locally Qualified Domain Name*") où le deuxième composant du nom (avant `.sitelocal`) serait une chaîne de caractères unique, par exemple en condensant l'ULA. Cela peut être généré automatiquement, et survivre aux redémarrages. Ainsi, on peut obtenir un nom unique, avec quasiment aucun risque de collisions, sans faire appel à un registre central. Cela résoudrait le problème de l'accès depuis l'extérieur. Mais le RFC oublie de dire que ces noms ne seront pas très conviviaux... (`04619d3973addefca2be3.sitelocal` ?). Et si on ne faisait pas appel à un TLD comme `.sitelocal` mais qu'on utilisait simplement des noms courts comme `pc-jean-jacques` ou `printer` ? Le problème de ces noms est le risque de collision <`http://www.iab.org/documents/correspondence-reports-documents/2013-2/iab-statement-dotless-domains-considered-harmful`> avec, par exemple, un TLD délégué (que se passe-t-il si l'ICANN délègue `.printer` ?)

Enfin, parmi les autres innombrables détails qui compliquent le déploiement d'un joli système de nommage pour le "*homenet*", le RFC note que ce système doit continuer à fonctionner même si le réseau est déconnecté de l'Internet (et ne peut donc pas joindre les serveurs racine du DNS). Cela va à l'opposé de l'approche de la plupart des « objets intelligents » qu'on vend au gogo aujourd'hui et qui sont presque tous dépendants d'un "*cloud*" lointain à qui ils envoient systématiquement toutes les données. Et il y a le problème des engins mobiles qui peuvent être connectés à un "*homenet*" puis se déplacer pour un autre. On voudrait évidemment qu'ils gardent le même nom, mais ce n'est pas évident (DNS dynamique du RFC 2136 ?).

Pour terminer cette longue liste de problèmes à résoudre, la section 3.8 du RFC traite des problèmes divers. Par exemple, la gestion opérationnelle du réseau. Comme on veut un réseau sans administrateur et qui s'organise tout seul, cette activité de gestion doit être facultative. Mais il peut y avoir des tâches

optionnelles, par exemple pour l'utilisateur avancé, ou pour celui qui a des exigences de sécurité fortes et veut donc durcir la configuration par défaut. Au minimum, même si l'utilisateur ne change rien, il aura peut-être envie de regarder (en mode « lecture seule ») son réseau, voir les machines connectées, le trafic (un seul ado abonné à Netflix à la maison peut sérieusement stresser le réseau, croyez-moi), les pannes, l'état de certains services (« NAS plein à 98 % », merci BitTorrent).

Enfin, pour clore le RFC, la section 3.9 revient sur les problèmes qui sont déjà résolus par IPv6 et sur ceux qu'il faudra résoudre. Le principe d'Homenet est de réutiliser, **autant que possible**, les protocoles existants de la famille IPv6. Mais il faudra bien développer de nouveaux protocoles pour les cas qui sortent du possible actuel. Le routage de base est, selon le RFC, bien traité à l'heure actuelle (bientôt OSPF à la maison...) Le cas du "*multi-homing*" avec plusieurs routeurs de sortie est plus compliqué, et nécessitera sans doute des extensions aux protocoles de routage.

À noter que Homenet a un futur protocole de distribution d'information, HNCP ("*Home Networking Control Protocol*", pas encore de RFC publié), qui pourra servir de base à des mécanismes de distribution des routes.

Autre problème pas vraiment résolu, les protocoles de résolution (RFC 6762) et de découverte de services (RFC 6763) ne fonctionnent que sur un réseau où la diffusion à tous est possible. Dans un environnement multi-réseaux comme Homenet, il faudra utiliser leurs extensions, actuellement en cours de développement.

Dernier problème ouvert, pour les ambitieux qui ont des idées : découvrir automatiquement les frontières du réseau, où se termine la maison et où commence le monde extérieur. On l'a dit, Homenet est un projet très ambitieux, régulièrement critiqué comme trop ambitieux et traitant trop de choses à la fois.

Quelques bons articles à lire :

- Sur l'automatisation de la maison, les excellents et très concrets exposés de Nathalie Trenaman <http://www.ripe.net/internet-coordination/press-centre/publications/speakers/nathalie-trenaman> comme "*IPv6 at Home*" <https://www.netnod.se/sites/default/files/IPv6%20at%20home-Trenaman.pdf>.
- Un article généraliste sur la maison qui tweete <http://mondeactechno.blog.lemonde.fr/2014/05/16/la-premiere-maison-francaise-qui-tweete/> et l'exposé de son architecte à la Journée du Conseil Scientifique de l'AFNIC <https://www.afnic.fr/medias/documents/JCSA/2014/00-Tutoriel-2-Spiquel-Objets-connectes-JCSA-2014.pdf>.
- Un article de synthèse <http://thingsonip.blogspot.fr/2012/04/home-networks-by-magic.html> très bien fait et très rigolo.
- Un très bon interview <http://www.geekpage.jp/en/blog/2013/cisco-homenet.php> stratégique de Mark Townsley, président du groupe de travail Homenet. « "*The homenet working group focuses on home networks with IPv6. The task of the working group includes producing an architecture document that outlines how to construct home networks involving multiple routers and subnets, i.e. multi-homing with IPv6.*" » Il insiste sur les oppositions à Homenet et sur les contestations dans le groupe de travail, entre ceux qui voulaient que le réseau à la maison soit une simple extension de celui du FAI et ceux qui voulaient un réseau autonome « "*The limit from the operator[Caractère Unicode non montré [2]]s perspective seems to be that the user can have one two or maybe three routers with one ISP connection and a backup or VPN connection, and thats about it. [...] There has always been this tug-of-war between what the operator will provide as a supported configuration and what the users will make happen on their own if the ISP doesn[Caractère Unicode non montré]t provide it. We[Caractère Unicode non montré]re seeing a bit of that in the Working Group now.*" ».
- Une excellente présentation générale <https://ripe67.ripe.net/presentations/195-townsley-ip pdf>, du même auteur.

Et, côté mise en œuvre, le projet Hnet <http://www.homewrt.org/>.

2. Car trop difficile à faire afficher par LaTeX