RFC 7381 : Enterprise IPv6 Deployment Guidelines

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 26 octobre 2014

Date de publication du RFC : Octobre 2014

https://www.bortzmeyer.org/7381.html

Le déploiement d'IPv6 continue, trop lentement, mais il continue et de plus en plus d'organisations font désormais fonctionner ce protocole. Ce document est une série de conseils sur le passage à IPv6 au sein d'une organisation (le RFC dit « "*enterprise*" » mais je ne vois pas de raison de traduire par « entreprise », ce qui limiterait arbitrairement aux organisations privées prévues pour faire gagner de l'argent à leurs actionnaires). Les précédents RFC de conseils sur le déploiement d'IPv6 ciblaient des organisations spécifiques (comme les opérateurs réseaux dans le RFC 6036 [1]), celui-ci s'adresse à toute organisation qui dispose d'un réseau et d'administrateurs pour s'en occuper (les particuliers, ou toutes petites organisations sans administrateurs réseaux, ne sont pas traités).

Bref, vous êtes l'heureux titulaire du titre d'administrateur réseaux dans une organisation qui est pour l'instant encore attardée et qui n'utilise que le protocole du siècle dernier, IPv4. Votre mission, que vous l'acceptiez ou pas, est de passer à IPv6, sachant en outre que vous n'avez probablement pas le droit d'abandonner complètement IPv4. Que faire ? Le RFC 4057 décrivait ces réseaux d'organisation, qui se distinguent du réseau SOHO par la présence d'administrateurs réseaux compétents et dévoués. Il s'agit donc de réseaux **gérés**, contrairement au réseau de la maison de M. Toutlemonde. Le, la ou les administrateurs réseau doivent gérer un réseau interne, comprenant des serveurs, des postes de travail, des imprimantes, et parfois des routeurs internes. Ce réseau est connecté à l'Internet via au moins un routeur. Plusieurs serveurs sont prévus pour être accessibles de l'extérieur, par exemple le serveur de courrier. Donc, pour résumer le cahier des charges :

— Déployer IPv6 sans casser IPv4, qui doit continuer à fonctionner,
— Perturber le moins possible le service. L'utilisateur professionnel veut que ça continue à marcher, les changements techniques indispensables (comme le passage à IPv6) doivent pouvoir être ignorés dans le cadre de son travail.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6036.txt

La pénurie d'adresses IPv4 <https://www.bortzmeyer.org/epuisement-adresses-ipv4.html> a des conséquences même sur ceux qui s'obstinent à ne pas déployer IPv6. Par exemple, comme le note le RFC 6302, les serveurs Internet, face au déploiement de techniques comme le CGN, ne peuvent plus se contenter de journaliser l'adresse IP source de leurs clients, ils doivent aussi noter le port source. D'autre part, même si on croit pouvoir se passer d'IPv6, certains réseaux ont déjà de l'IPv6 sans le savoir (parce qu'il est activé par défaut sur beaucoup de systèmes) et cela a des conséquences de sécurité (cf. RFC 6104 pour un exemple et le RFC 7123 pour une vision plus générale de ce problème).

Notre RFC propose **trois phases** pour l'opération de déploiement :
— Préparation et détermination,
— Phase interne,
— Phase externe.
Les deux dernières ne sont pas forcément exécutées dans cet ordre. Par exemple, si on gère un site Web et que beaucoup de clients potentiels ont déjà IPv6, il est logique de commencer par la phase externe, doter ce site d'une connectivité IPv6. En outre, bien des applications de gestion, comme celles de comptabilité sont affreusement archaïques et n'auront pas IPv6 de si tôt, ce qui relativise l'urgence de la phase interne. D'un autre côté, bien des systèmes d'exploitation ont IPv6 par défaut, et le RFC 7123 note que cela pose des problèmes de sécurité qui mériteraient peut-être une attention immédiate, et donc une priorité à la phase interne. Autre cas où la phase interne doit sans doute passer en premier : si l'espace d'adressage du RFC 1918 commence à ne plus suffire ou bien si une fusion/acquisition a mené à assembler deux réseaux qui utilisaient les mêmes préfixes, entraînant un grand désordre et l'envie, chez l'administrateur réseaux, de se reconvertir comme affineur de fromage dans l'Hérault, ou de déployer IPv6. Comme le notait le RFC 6879, la fusion/acquisition de deux organisations est souvent une bonne occasion pour passer à IPv6, car fusionner deux réseaux IPv4 en adressage privé est toujours long et compliqué. Bref, chaque organisation va devoir déterminer ses priorités et décider de commencer, après la première phase de préparation, par la phase interne ou par l'externe. Autrefois, il y avait aussi la catégorie « c'est bien compliqué tout cela, est-ce que ça en vaut la peine ? » mais sa taille diminue. Certaines objections techniques qui étaient valables à une époque (RFC 1687) ont depuis été traitées.

Donc, maintenant, au travail, avec la première phase, Préparation & Détermination (section 2 du RFC). Le RFC recommande de nommer un « chef de projet professionnel ». Ce qui est sûr est qu'il faut gérer le projet sérieusement, car c'est après tout un changement important dans l'infrastructure, avec plein d'interdépendances. La phase de Préparation & Détermination va, entre autres, servir à décider si on priorise la Phase Interne ou la Phase Externe. La première phase découvrira sans doute des problèmes inattendus et elle se fera donc en plusieurs itérations (« zut, ce plan ne marchera pas, il faut en trouver un autre »).

D'abord, l'inventaire de l'existant. Il faut faire la liste des matériels en déterminant pour chacun s'il est prêt pour IPv6. Il y aura du matériel déjà prêt (au sens où il fait déjà tourner un système capable d'IPv6), du matériel qui pourra recevoir une mise à jour logicielle, et du matériel qu'il faudra remplacer car aucun système avec IPv6 n'existe pour ce matériel. Par exemple, les routeurs (sauf le bas de gamme) sont probablement prêts, mais les objets connectés (genre caméras ou imprimantes) ne le sont souvent pas.

Après le matériel, le logiciel. Il faut faire le tour des applications pour déterminer lesquelles passeront en IPv6 sans problèmes. Si certains logiciels ne sont pas prêts, il faut demander au vendeur. Je suis toujours surpris que les vendeurs expliquent leur manque d'IPv6 par l'argument « aucun client ne l'a demandé ». Parfois, bien sûr, le vendeur ment mais, parfois, les clients semblent effectivement d'une timidité maladive et n'osent pas dire aux vendeurs, même gentiment « excusez-nous de vous demander pardon, mais pourrions-nous avoir de l'IPv6 un jour, s'il vous plait ? »

Lorsque l'application est développée/maintenue en interne, c'est l'occasion de se pencher sur les pratiques de codage. Est-ce que les applications ne sont pas d'un trop bas niveau <https://www.

bortzmeyer.org/network-high-level-programming.html>, intégrant des détails non pertinents comme la taille de l'adresse IP ? Parmi les RFC dont la lecture peut être utile aux programmeurs à ce stade, citons le RFC 4038 sur le rapport entre les applications et IPv6, le RFC 6724 sur la sélection de l'adresse IP source, et le RFC 6555, sur l'algorithme des globes oculaires heureux, si utile lorsqu'on a à la fois IPv4 et IPv6. Un autre point important, mais non mentionné par ce RFC, est que le cycle de vie d'un logiciel développé en interne est long : ce qui est programmé aujourd'hui sera toujours en service dans de nombreuses années. Il faut donc adopter des bonnes pratiques de programmation (programmation réseau de haut niveau, valable aussi bien pour IPv4 que pour IPv6) aujourd'hui, même si la migration vers IPv6 semble lointaine.

C'est l'occasion d'aborder la question cruciale de la formation. Aujourd'hui, il existe encore des écoles ou universités qui enseignent IP sans parler d'IPv6, ou en le réduisant à deux heures de cours à la fin de l'année, dans un fourre-tout « divers sujets ». C'est consternant et cela veut dire que la formation à IPv6 dépendra surtout du technicien lui-même, ou bien de son employeur (section 2.3 du RFC).

Autre gros morceau dans la phase de préparation et détermination, la question de la sécurité. Évidemment, on veut que le réseau soit aussi sûr en IPv6 qu'en IPv4. Au passage, j'ai fait un long exposé à ce sujet <https://www.bortzmeyer.org/ipv6-securite.html>. Je ne suis pas d'accord avec l'approche du RFC. Le RFC note qu'IPv6 n'est pas intrinsèquement plus sûr qu'IPv4 juste parce qu'il est plus récent, ce qui est du bon sens. Mais il prend ensuite une approche unilatérale, en notant qu'il existe beaucoup de failles de sécurité dans le code IPv6 car il n'a guère été testé au feu. C'est exact mais le RFC oublie de dire que c'est la même chose pour les attaquants : leurs programmes sont rarement adaptés à IPv6. Mon expérience est que les attaquants et les défenseurs sont aussi peu préparés à IPv6 et que, en pratique, la sécurité des deux protocoles est à peu près équivalente. Le RFC, comme le font souvent les professionnels de la sécurité, pessimistes par profession, ne voit que les faiblesses de la défense. En tout cas, tout le monde est d'accord pour dire que la formation (paragraphe précédent...) est essentielle.

Le RFC tord le cou à quelques mythes comme quoi la sécurité d'IPv6 serait meilleure (il oublie les mythes inverses, tout aussi répandus). Par exemple, IPv6 ne rend pas impossible le balayage d'un réseau, juste parce qu'il a davantage d'adresses. Le RFC 7707 décrit plusieurs techniques de balayage qui sont faisables avec IPv6 (et qui sont effectivement mises en œuvre dans des outils existants <https://www.bortzmeyer.org/hacking-ipv6.html>). Mais s'il est vrai qu'IPv6 n'empêche pas le balayage, ce nouveau RFC, dans son analyse trop rapide, oublie de dire que le balayage est bien plus facile et rapide en IPv4, comme le montre la disponibilité d'outils (comme massscan <http://blog.erratasec.com/2013/09/masscan-entire-internet-in-3-minutes.html>) qui balaient tout l'Internet IPv4 en quelques heures ! De même, notre nouveau RFC rappelle qu'IPv6 n'a pas de sécurité cryptographique par défaut (contrairement à une légende répandue par des zélotes d'IPv6 au début, cf. RFC 6434 pour l'enterrement de cette légende). Pire (et, là, ce RFC 7381 est gravement en tort) : la section 2.4.1 explique que c'est une bonne chose pour la sécurité qu'il n'y ait pas de chiffrement car il faut pouvoir espionner le trafic de ses utilisateurs, un argument vraiment incroyable à l'ère post-Snowden.

Le RFC est plus raisonnable par la suite en notant que certaines pratiques de sécurité relèvent plus de la magie que de la raison. Par exemple, les ULA en IPv6 (RFC 4193) ou les adresses privées en IPv4 (RFC 1918) n'apportent aucune sécurité en elles-même, contrairement à ce que croient naïvement certains administrateurs réseau <https://www.bortzmeyer.org/nat-et-securite.html>.

Notre RFC fait le point sur les failles de sécurité qui sont spécifiques à IPv6 :

— Les adresses de protection de la vie privée (RFC 8981) ne la protègent que partiellement mais, surtout, compliquent la vie de l'administrateur réseaux, en limitant la traçabilité des machines. Si un journal montre que 2001:db8:1:1:c144:67bd:5559:be9f s'est connecté au serveur LDAP, comment savoir quelle machine était 2001:db8:1:1:c144:67bd:5559:be9f puisque, s'il utilisait le RFC 8981, il a pu changer d'adresse souvent, sans que cela soit enregistré quelque

part ? Une solution possible est d'utiliser un logiciel qui écoute le réseau et stocke dans une base de données les correspondances entre adresses MAC et adresses IPv6 (un logiciel comme ndpmon <http://ndpmon.sourceforge.net/>, donc). Si on contrôle complètement les machines terminales, on peut aussi interdire les extensions « vie privée ». On peut enfin forcer l'usage de DHCP en demandant au routeur d'envoyer toutes les annonces avec le bit M (qui indique que DHCP est disponible, RFC 4861, section 4.2) et qu'aucun préfixe ne comporte le bit A (ce qui interdira l'auto-configuration sans état, RFC 4861, section 4.6.2). Cela suppose que toutes les machines ont un client DHCP v6, ce qui n'est pas gagné aujourd'hui. Pire : on sait qu'aujourd'hui le comportement des différents système en présence des bits M et A varie énormément.

— Et les en-têtes d'extension ? Leur analyse est difficile <https://www.bortzmeyer.org/analyse-pcap-ip html> et, résultat, certains systèmes de sécurité ne savent pas les traiter, permettant ainsi au méchant d'échapper à la détection ou au filtrage, simplement en ajoutant des en-têtes au paquet IPv6 (RFC 7113 pour un exemple).
— La fragmentation est une source classique de casse-tête. Elle existe aussi en IPv4 mais IPv6 la restreint à la source, les routeurs intermédiaires ne peuvent pas fragmenter. Du point de vue sécurité, la principale question liée à la fragmentation est le fait que, au nom d'une sécurité mal comprise, certains réseaux bloquent le protocole ICMP, malgré le RFC 4890, gênant ainsi la détection de MTU et empêchant donc de facto la fragmentation. Autres problèmes liés à la fragmentation, mais qui ne sont pas spécifiques à IPv6, le risque d'utilisation de fragments pour échapper à la détection (RFC 6105 pour un exemple), et le réassemblage de fragments qui se recouvrent (RFC 5722).
— Pour la résolution d'adresses IP en adresses MAC, IPv6 utilise NDP et plus ARP. Le RFC classe cela comme « une importante différence » mais, en fait, du point de vue de la sécurité, les deux protocoles sont très proches. Ils fonctionnent en diffusant à tous l'adresse convoitée, et ils font une confiance absolue à la première réponse reçue. Aucune authentification n'existe (IPv6 a des solutions, mais très peu déployées, cf. RFC 3971 et RFC 3972).
— Enfin, dernier problème qu'on n'avait pas avec de l'IPv4 pur, un réseau double-pile, IPv4 et IPv6, augmente la surface d'attaque en offrant davantage de possibilités au méchant. Au minimum, il faut faire attention à ce que les politiques de sécurité soient les mêmes en IPv4 et en IPv6 afin d'éviter (je l'ai déjà vu), un pare-feu strict en IPv4 mais très laxiste en IPv6.

Maintenant, le routage. Un grand réseau interne va probablement utiliser un IGP. Lequel ? Plusieurs protocoles gèrent IPv6 (RIPng, IS-IS, OSPF). A priori, pour faciliter la vie des techniciens, il est logique d'utiliser le même protocole de routage en IPv4 et en IPv6. Petit piège dans le cas d'OSPF : OSPF v2 (pour IPv4) et OSPF v3 (pour IPv6) sont proches mais ne sont pas exactement le même protocole (le RFC oublie qu'OPSF v3 peut désormais gérer IPv4, cf. RFC 5838, mais il est vrai que c'est très peu fréquent).

Et l'adressage (section 2.6) ? Il est évidemment radicalement différent en IPv4 et en IPv6. En IPv4, l'essentiel du travail sur l'adressage a pour but d'économiser les quelques adresses qu'on détient, pour tout faire fonctionner malgré la pénurie. En IPv6, ce problème disparait et on peut donc se concentrer sur un plan d'adressage propre. Le document à lire pour faire de jolis plans d'adressage en IPv6 est le RFC 5375.

L'une des décisions à prendre sera d'utiliser des adresses PA ou PI. Les premières sont attribuées par l'opérateur réseau qui nous connecte à l'Internet. Pas de formalités particulières à remplir, elles sont typiquement allouées en même temps que la connectivité est mise en place. Leur inconvénient est qu'on dépend de l'opérateur : le "*multi-homing*" va être plus difficile, et, si on change d'opérateur, on est parti pour une pénible renumérotation (RFC 5887). En outre, il peut être difficile d'obtenir la taille de préfixe souhaitée, malgré le RFC 6177 : certains opérateurs ne fileront qu'un /56, voire un /60. Les secondes adresses, les adresses PI, résolvent ces problèmes mais les obtenir nécessite d'affronter la bureaucratie des RIR. Pour les réseaux internes, notre RFC recommande un /64 pour les réseaux des utilisateurs, et un /127 pour les interconnexions point-à-point, comme dit dans le RFC 6164. IPv6 ne nécessite pas les masques de longueur variable, très communs en IPv4 pour essayer de grappigner quelques malheureuses adresses. Utiliser, par exemple, un /80 pour un Ethernet de plusieurs machines utilisateur

empêcherait d'utiliser l'auto-configuration (RFC 4862) sans gain utile, et au risque de perturber les futures réorganisations du réseau.

Une fois le plan d'adressage fini, il reste à distribuer les adresses aux machines. Autrefois, on n'utiliisait que SLAAC, parce que c'était la seule possibilité. Le RFC note, avec un très grand optimisme, que DHCP est désormais une alternative mûre (en fait, bien des machines clientes n'ont pas encore de client DHCP, voilà pourquoi je trouve le RFC trop optimiste). Pour le réseau fermement administré, DHCP a l'avantage de garder trace de la correspondance entre adresse MAC et adresse IP, en un point central. Pour faire l'équivalent avec SLAAC, il faudrait un logiciel de supervision comme ndpmon <http://ndpmon.sourceforge.net/> cité plus haut. Autre avantage de DHCP, le serveur DHCP est l'endroit logique où faire des mises à jour dynamiques du DNS pour refléter les changements d'adresses IP. Dernier mot sur le DNS : il est déconseillé de mettre des données pour les ULA dans le DNS mondial.

La phase de Préparation et de Détermination se termine avec une analyse des outils disponibles pour l'administrateur réseaux. Il arrive en effet trop souvent que l'outil utilisé, par exemple, pour le déploiement de nouvelles versions de logiciels, ne soit finalement pas compatible IPv6. S'il a été écrit dans les dix dernières années, cela montre une grande incompétence de la part de son auteur mais ça arrive. Parmi les erreurs faites par les programmeurs, le manque de place pour la représentation des adresses, que ce soit en forme texte (RFC 5952) ou sous leur forme binaire. Ceci dit, tant que le réseau est en double-pile, certaines fonctions (par exemple l'interrogation des agents SNMP) peuvent continuer à se faire en IPv4.

S'il est logique de commencer par la phase Préparation & Détermination, le choix de la phase suivante dépend, comme on l'a vu, des caractéristiques propres à l'organisation dont on gère le réseau. Le RFC commence par la phase externe (section 3) mais ce n'est que l'ordre de présentation, pas forcément l'ordre recommandé.

Donc, la phase externe : il s'agit de migrer en IPv6 les composants du réseau visibles de l'extérieur. Il va évidemment falloir obtenir une connectivité IPv6 d'un opérateur réseau. Il est **fortement** recommandé d'utiliser de l'IPv6 natif, plus simple à déboguer et évitant les problèmes comme la taille de MTU <https://www.bortzmeyer.org/mtu-et-mss-sont-dans-un-reseau.html>. Mais, si cela n'est pas possible (dans certaines régions du monde, il est très difficile de trouver un opérateur qui sache faire de l'IPv6), il faudra se résigner à utiliser un tunnel, par exemple vers Hurricane Electric <https://www.bortzmeyer.org/ipv6-he.html>, qui fournit un service stable et pro. Si les adresses utilisées sont des adresses PA, ledit opérateur s'occupera du routage externe. Si ce sont des PI, l'opérateur pourra parfois les router pour le compte du client, et le client devra parfois faire du BGP lui-même. Évidemment, l'obtention d'un préfixe PI va dépendre des règles du RIR local. Par exemple, en Europe, le RIPE-NCC n'impose plus d'être "*multihomé*" pour avoir un préfixe PI.

Notre RFC ne traite pas des problèmes spécifiques à chaque service. Par exemple, cela aurait pu être l'occasion d'expliquer que, si annoncer une adresse IPv6 pour un serveur HTTP peut présenter un risque (pour les clients qui croient avoir une connectivité IPv6 alors qu'elle est imparfaite, cf. RFC 6556), en revanche, mettre des adresses IPv6 à ses serveurs DNS n'en présente aucun, puisque les clients DNS mettent en œuvre depuis longtemps un algorithme de test et de sélection des différents serveurs d'une zone. Cela explique sans doute que, selon le rapport ODRIF <https://www.ssi.gouv.fr/agence/rayonnement-scientifique/lobservatoire-de-la-resilience-de-linternet-francais/>, il y ait beaucoup plus de zone sous `.fr` avec du DNS IPv6 que de zones avec un serveur Web IPv6. (Notez que Google fait, curieusement, le contraire : leurs sites Web sont IPv6 depuis longtemps mais leurs zones DNS non.)

Il faudra évidemment penser à la sécurité. Le RFC rappelle que, si on filtre, il ne faut **surtout pas** bloquer stupidement tout ICMP, indispensable à certaines fonctions d'IPv6 (voir le RFC 4890 pour une

discussion détaillée, que notre RFC résume en donnant la liste minimale des types de messages ICMP qui doivent être autorisés).

Il y a des règles de sécurité générales, qui s'appliquent à IPv6 aussi bien qu'à IPv4 : attention aux applications (pensez à mettre bash à jour, par exemple...), mettez en place des mécanismes contre l'usurpation d'adresses (RFC 2827), protégez les routeurs (RFC 6192), etc. Et il y a quelques règles spécifiques d'IPv6 comme les attaques contre le cache NDP (RFC 6583) : il est recommandé de limiter le rythme des requêtes NDP et de bloquer le trafic entrant sauf vers les adresses publiques.

La supervision doit aussi faire l'objet d'une grande attention. Notre RFC recommande de surveiller séparément IPv4 et IPv6, pour être averti si un des deux protocoles défaille. Prenons l'exemple d'un serveur HTTP. Si vous testez son bon fonctionnement avec curl ou wget, vous ne serez pas prévenu si IPv4 ou IPv6 est en panne. En effet, ces deux programmes passent automatiquement aux adresses IP suivantes si l'une d'elles ne fonctionne pas. Il faut donc un test explicitement limité à IPv4 et un limité explicitement à IPv6. Avec Icinga et le check_http <https://www.monitoring-plugins.org/doc/man/check_http.html> des "*monitoring plugins*" <https://www.monitoring-plugins.org/>, cela peut être :

```
define service{
        use                             generic-service
        hostgroup_name                  WebServers
        service_description             HTTP4
        check_command                   check_http!-4
        }

define service{
        use                             generic-service
        hostgroup_name                  WebServers
        service_description             HTTP6
        check_command                   check_http!-6
        }
```

Il reste la phase interne (section 4) qui, rappelez-vous, peut être faite avant, après ou en même temps que la phase externe, selon les caractéristiques de votre réseau et vos choix. Il s'agit cette fois de migrer en IPv6 le réseau interne, ses applications métier, ses commutateurs, ses postes de travail... A priori, comme il y a peu de chances que toutes les applications et systèmes IPv4 soient prêts demain à migrer, le réseau interne va rester mixte pendant longtemps. Pour la connectivité, la règle habituelle s'applique : « double-pile quand on peut, tunnel quand on n'a pas le choix ». La double-pile (IPv4 **et** IPv6 sur tous les équipements) est la solution la plus simple pour la gestion du réseau. Le tunnel, fragile et faisant dépendre IPv6 d'IPv4, sert pour les cas où on est coincé à n'utiliser que des systèmes antédiluviens.

En interne également, on va se poser la question de la sécurité. Les gestionnaires de réseaux d'organisations sont souvent peu satisfaits des adresses IP « vie privée » du RFC 8981, car elles rendent difficile la traçabilité (« 2001:db8:1:1:c144:67bd:5559:be9f a fait des accès répétés au serveur LDAP, c'est qui, déjà, 2001:db8:1:1:c144:67bd:5559:be9f ? ») Ou bien on force l'utilisation de DHCP, ou bien on utilise un outil comme ndpmon qui garde trace des correspondances entre adresses MAC et adresses IP.

Comme pour les ARP et DHCP d'IPv4, les techniques de base du réseau IPv6 (les RA de NDP, et DHCP) n'offrent aucune sécurité et il est trivial, par exemple, d'envoyer des « RAcailles », des faux RA (RFC 6104). Il est donc très recommandé de déployer des techniques comme celles du RFC 6105. Vérifiez auprès de votre fournisseur de commutateurs qu'elles sont disponibles ! Dans le futur, les techniques issues du projet SAVI ("*Source Address Validation Improvement*", cf. RFC 6959) aideront peut-être.

Pour assurer le bon fonctionnement du réseau interne, une des questions qui perturbent le plus les administrateurs d'un réseau IPv6 est le choix du mécanisme principal de configuration des machines terminales. SLAAC (RFC 4862) ou DHCP (RFC 8415) ? Il n'y a pas de réponse simple, chacune des deux solutions ayant ses avantages et ses inconvénients. SLAAC est certainement plus simple et plus rapide à déployer mais DHCP permet davantage de contrôle, ce qui est en général apprécié dans les réseaux d'organisations. En pratique, malheureusement, il faudra sans doute les deux car aucun des deux mécanismes ne permet de tout faire. Par exemple, DHCP n'a pas d'option pour indiquer les routeurs à utiliser (il faudra donc compter sur les RA de SLAAC, ou sur une configuration statique). Et SLAAC ne permet pas d'indiquer les serveurs NTP. Si les deux protocoles, DHCP et SLAAC, permettent désormais d'indiquer les résolveurs DNS, aucun des deux n'est encore suffisant pour tous les usages et, en pratique, il est difficile de choisir.

Autre question essentielle, la résilience face aux pannes. Cela passe par la redondance des équipements comme les routeurs. NDP permet aux machines de maintenir une liste de routeurs disponibles et de passer à un autre en cas de panne (RFC 4861, section 7.3). Par défaut, la bascule se fait en 38 secondes (RFC 4861, section 10), ce qui est bien trop long dans beaucoup de cas. Il est donc souvent préférable d'utiliser des techniques comme VRRP (RFC 5798).

Autre problème à regarder de près pendant la phase Interne, les machines terminales, de l'ordinateur de bureau à la machine à café connectée, en passant par l'imprimante et la caméra de vidéo-surveillance. Les ordinateurs ont quasiment tous IPv6 aujourd'hui (mais pas forcément activé par défaut). Mais certaines fonctions peuvent manquer (adresses privées du RFC 8981, client DHCPv6, client RA qui comprend les résolveurs DNS du RFC 8106...) Il est également possible que des algorithmes comme la bonne sélection de l'adresse source (RFC 6724) ou les globes oculaires heureux (RFC 6555) soient manquants ou désactivés. Or, sans eux, l'utilisation d'un système double-pile (IPv4 **et** IPv6) est bien plus pénible. Il faut donc s'assurer de bien connaître le comportement par défaut des systèmes qu'on utilise sur les réseaux locaux.

Quant aux autres engins, non considérés comme des ordinateurs, il est malheureusement fréquent, en 2014, qu'ils n'aient toujours pas IPv6 (alors même qu'ils sont souvent bâtis sur des systèmes, comme Linux, qui ont IPv6 depuis longtemps). Enfin, le dernier gros problème de la phase interne sera les systèmes utilisés dans l'infrastructure de l'organisation (le système de téléphonie, par exemple) qui ne sont pas toujours prêts pour IPv6. Là encore, il est essentiel que les clients se fassent entendre et tapent sérieusement sur les vendeurs les plus attardés.

On a parlé à plusieurs reprises de réseaux double-pile car c'est l'approche la plus réaliste aujourd'hui. Pourra-t-on un jour simplifier sérieusement le réseau en supprimant enfin le bon vieil IPv4 et en ayant à nouveau un réseau mono-protocole, entièrement IPv6 ? C'est bien le but à long terme, dit avec optimisme la section 5 de notre RFC. Atteindre ce but ne nécessite même pas que tout l'Internet soit entièrement passé en IPv6. Il existe des techniques permettant aux machines d'un réseau purement IPv6 de parler avec les derniers survivants de l'ère IPv4 (cf. par exemple RFC 6144). Au début, une bonne partie du trafic devra passer par ces relais ou des traducteurs NAT64. Mais au fur et à mesure que le reste de l'Internet devient accessible en IPv6 (RFC 6883), ces techniques deviennent naturellement de moins en moins utilisées.

Tous les conseils ci-dessus étaient génériques, s'appliquant à toutes sortes d'organisations. La section 6 traite maintenant des cas particuliers de certaines organisations. Par exemple, les gens dont le métier est de distribuer du contenu sur l'Internet (par exemple via un CDN) ont intérêt à lire les RFC 6883 et RFC 6589.

Un autre cas particulier, qui permettra de finir sur une note optimiste, est celui des campus universitaires. Ils sont aujourd'hui très souvent passés à IPv6. Les NREN ont en général IPv6 depuis le début des

années 2000. L'intérêt pour les techniques nouvelles, et la mission de recherche et d'éducation, faisait des universités l'endroit logique pour les premiers déploiements. C'est évidemment souvent le département d'Informatique qui était le premier à migrer ses machines et ses services vers IPv6. Le réseau Eduroam est également accessible avec IPv6 puisqu'il repose sur 802.1x (qui est indifférent à la version du protocole IP utilisée) et non pas sur ces horribles portails captifs (dont un des inconvénients est d'être limité à un protocole).

La grande majorité des universités qui ont déployé IPv6 n'utilise pas d'ULA, ni traduction d'adresses. Presque toujours, elles utilisent des adresses PA fournies par le NREN.