

Image: iStock

## Dossier IPv6

en collaboration avec **Boll Engineering**

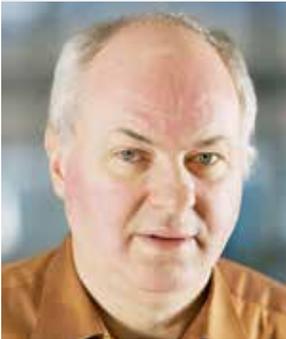
## En route vers l'IPv6

**cgr-y.ch.** La migration d'IPv4 vers IPv6 est au point mort en Suisse. Un temps au top du classement établi par Akamai des pays les plus avancés dans cette transition, la Suisse a reculé. Cédant sa première place à la Belgique et doublé par les USA ainsi que la Grèce. Or les adresses IPv4 deviennent de plus en plus rares. Tandis qu'avec l'avènement de l'Internet des objets, toujours plus d'appareils ayant besoin de leur propre IP viennent se connecter au réseau: selon Gartner, on dénombre déjà 20 milliards d'appareils IoT dans trois ans. La demande en nouvelles adresses IP va donc prendre l'ascenseur. Créé dans les années 90, le protocole IPv6 a le potentiel d'y répondre, avec ses adresses de 128 bits au lieu de 32 bits pour l'IPv4. La transition n'a toutefois rien d'une mince affaire, notamment car ce protocole nécessite des composants hardware compatibles. Et l'investissement a de quoi rendre les entreprises frileuses. Dans ce dossier, Walter Benz, Product Manager pour A10 Networks chez Boll, conseille ainsi de migrer progressivement. Il sera dans ce cas important d'assurer la communication entre les infrastructures reposant sur deux différentes normes. Quant aux nouveaux projets, ils devront dès le début être mis en œuvre en IPv6.

# IPv4 et IPv6: l'immense défi

La transition de l'IPv4 à l'IPv6 impose des tâches énormes aux entreprises et aux fournisseurs d'accès. Une plate-forme intégrée offrant des technologies de traduction et de tunneling très variées garantit la coexistence des deux univers et permet une transition sans heurts.

## L'AUTEUR



**Walter Benz**  
Product Manager pour  
A10 Networks,  
BOLL

Une pénurie d'adresses affecte Internet, en particulier en ce qui concerne les adresses IPv4. L'espace d'adresses IPv4 offre certes de la place à plusieurs milliards de participants et cela a toujours été suffisant jusqu'à présent. Mais le problème se pose à nouveau de manière urgente: les fournisseurs d'accès Internet ne reçoivent plus de nouvelles adresses IPv4 de la part des organes officiels chargés de les attribuer et, sur le marché gris, les quelques blocs d'adresses restants sont négociés à des prix exorbitants. A tel point que les petits fournisseurs ne peuvent plus se les permettre.

A l'avenir, la pénurie d'adresses deviendra encore plus critique. La population des appareils mobiles augmente à un rythme effréné et exige des connexions parfaitement stables et disponibles à tout moment pour certains services tels que le streaming. L'Internet des objets se propage à un rythme exponentiel; le nombre de 20 milliards d'appareils IoT prévu par Gartner à l'horizon 2020 sont pratiquement déjà atteints. Et chaque appareil individuel a besoin de sa propre adresse IP.

Avec IPv6, une nouvelle version de protocole Internet est disponible depuis 1998 et ses 340 sextillions d'adresses possibles devraient offrir une capacité suffisante pour tous les nouveaux appareils et pour toujours. Mais dans la pratique, l'introduction d'IPv6 est toutefois compliquée et coûteuse. Elle implique des investissements dans du nouveau matériel compatible IPv6 et des modifications de configuration complexes. C'est la raison pour laquelle on recommande généralement une introduction échelonnée. Les systèmes actuels peuvent par exemple continuer sur IPv4, alors que les nouveaux projets sont dès le départ mis en œuvre sur une base IPv6.

## Deux univers

Mais l'infrastructure IPv6 n'est pas basée intrinsèquement sur la communication avec l'environnement IPv4 actuel: IPv4 et IPv6

sont deux univers complètement différents. Une coexistence des deux protocoles n'est possible que s'il existe une passerelle qui traduit le trafic IPv6 en temps réel vers l'univers IPv4.

Ceci est particulièrement pertinent pour les fournisseurs d'accès: alors que l'infrastructure interne du serveur peut être migrée assez facilement vers IPv6 et que l'accès backbone IPv6 est déjà pris en charge, les appareils des clients ne sont souvent pas compatibles IPv6 ou ne sont pas configurés pour ce dernier – de nombreux clients ne sont pas en mesure d'effectuer eux-mêmes les modifications nécessaires. Les clients privés et les petites entreprises ne disposent pas de leur propre service informatique.

Mais même les organisations plus importantes avec une propre infrastructure de réseau sont tributaires d'une solution associant IPv4 et IPv6. Une grande partie des appareils IoT actuels – du capteur simple au système domotique complet – ne sont par ailleurs pas compatibles IPv6, ce qui est particulièrement critique, en particulier compte tenu de la longue période d'utilisation de ces appareils.

## Des technologies pour la transition

Afin de mettre en place des infrastructures IP convergentes, dans lesquelles IPv4 et IPv6 coexistent sans problème, diverses technologies sont disponibles.

- Le Server Load Balancing with Protocol Translation (SLB-PT) permet de rendre les serveurs, qu'ils soient basés sur IPv4 ou IPv6, accessibles à tous les clients externes, peu importe si ces clients viennent eux-mêmes de l'univers IPv4 ou IPv6. La traduction entre les protocoles est transparente, les clients et les utilisateurs ne remarquent rien.
- NAT64/DNS64 permet aux clients IPv6 d'accéder aux infrastructures de serveur IPv4 et à leurs contenus.
- Le tunneling permet de guider le trafic IPv4 via une connexion IPv6 – ou inversement. Les paquets de l'un des protocoles sont respectivement encapsulés dans des paquets de l'autre protocole. Le trafic IPv6 peut ainsi accéder à l'Internet IPv6 via un routeur – qui ne maîtrise lui-même pas la transmission IPv6.
- DS-Lite est une variante de tunneling qui suscite un intérêt croissant. Avec DS-Lite, les appareils uniquement compatibles IPv4 peuvent accéder à Internet dans un réseau purement IPv6 via «Softwires». Les procédures LW4o6 et 6rd offrent des possibilités comparables.
- Avec un Carrier-Grade NAT (CGN), les fournisseurs d'accès peuvent faire un pied de nez à la pénurie d'adresses IPv4. Les clients ne reçoivent pas d'adresse IPv4 publique, mais une adresse privée qui leur est attribuée par le mécanisme CGN.





Ainsi, une seule adresse publique chez le fournisseur peut être répartie entre 100 clients et plus – la réserve d'adresses IPv4 dure plus longtemps. Ce qui est important dans tout cela, c'est que les clients restent clairement identifiables comme la loi l'exige.

- Les passerelles de la couche Application garantissent que les protocoles tels que FTP, H.323 ou DNS restent fonctionnels. Certains déploiements NAT traditionnels ne le garantissent pas.

#### Une solution intégrée offre des avantages

Les meilleures conditions pour une migration sans heurt vers IPv6 sont obtenues avec une plate-forme intégrée qui maîtrise toutes les méthodes de traduction et de tunneling courantes et permet par ailleurs d'utiliser diverses méthodes en parallèle. Sur cette base, on peut migrer progressivement vers IPv6 au rythme souhaité sans que les différents clients ou serveurs soient laissés de côté.

Des méthodes telles que CGN nécessitent une puissance de calcul élevée et exigent que les systèmes sous-jacents soient extrêmement performants. Il est recommandé d'utiliser pour cela du matériel dédié, de préférence un appareil spécialement conçu pour la transition IPv4/IPv6.

L'avantage en termes de coûts et d'intégration entrent encore plus en ligne de compte si la plate-forme offre des fonctionnalités supplémentaires telles que le SSL-Offloading avec support matériel (termination des connexions clients cryptées) et SSL-Bridging (contrôle des données cryptées en vue de détecter un code erroné) ainsi que des fonctions de sécurité telles que la lutte contre les attaques DDoS ainsi que DNS-Application-Firewall et Web-Application-Firewall. Ceci est valable notamment lorsque ces fonctions sont exploitées simultanément avec une fonctionnalité Application-Delivery-Controller sur différentes partitions d'un même matériel. Il n'y a alors pas lieu d'investir dans plusieurs produits différents qui ne fonctionnent pas encore parfaitement ensemble et qui coûtent globalement nettement plus cher. Un autre avantage d'une solution

intégrée – comme le propose par exemple la société A10 Networks qui travaille dans le domaine Application Networking, Server Load Balancing et Application Delivery – est le management unique.

#### Un système performant est nécessaire

La condition de base pour une solution complètement intégrée est une plate-forme matérielle très performante, qui autorise réellement l'exploitation parallèle de toutes les fonctions. Tous les fabricants ne répondent pas à cette condition – la densité de puissance par unité de rack peut être très différente d'un produit à l'autre. Pour les infrastructures de réseau dynamiques modernes selon le modèle du Software-defined Networking ou de la Network Function Virtualization, un appareil virtuel peut aussi être envisagé – l'idéal étant que le fournisseur propose les deux variantes.

*«Avec un Carrier-Grade NAT (CGN), les fournisseurs d'accès peuvent faire un pied de nez à la pénurie d'adresses IPv4»*

*Walter Benz, Product Manager pour A10 Networks, BOLL*

#### INFO

Les Server Load Balancer (SLB) et ADCs (solutions pour Application Delivery et Application Networking) sont envisagés lorsque des applications doivent être mises à disposition plus rapidement, avec une meilleure qualité et de manière sécurisée. Pour cela, des systèmes innovants prennent en charge des fonctionnalités de sécurité et de réseau élargies telles que:

- Web Application Firewall (WAF)
- DNS Application Firewall (protection des infrastructures DNS)
- Lutte contre les DDoS (protection contre les attaques Distributed-Denial-of-Service multicouches)
- Application Access Management (des fonctions d'authentification intégrées garantissent que les serveurs Backend ne recevront aucun flux de données indésirable ou non authentifié)
- Réduction du trafic de données (par ex. compression du protocole HTTP et du Traffic Caching)
- SSL-Offloading (termination des connexions clients cryptées)
- SSL-Bridging (contrôle des données cryptées en vue de détecter un code erroné)
- Software Defined Networking (SDN)

# Délai de grâce pour les adresses IPv4 limitées

Les adresses IPv4 libres deviennent rares. Christoph Tobler, responsable informatique du groupe Leucom, explique dans une interview, comment le fournisseur d'accès de Suisse orientale a résolu le problème avec la technologie Carrier-Grade Network Address Translation (CGN). Interview: George Sarpong

**« Nous avons migré quelque 3000 clients – au pas de course, en deux mois seulement! »**

*Christoph Tobler, Responsable IT chez Leucom*

## A quel défi avez-vous été confronté?

Christoph Tobler: Nous avons le même problème que tous les fournisseurs d'accès Internet: les adresses IPv4 deviennent rares. Notre réserve se tarit lentement mais sûrement. Acheter des adresses sur le marché ou reprendre une société qui possède encore des adresses disponibles serait certainement très coûteux. Nous avons dû trouver une autre solution.

## Quelles alternatives avez-vous envisagées?

De toute évidence, une migration vers IPv6 s'impose naturellement. Nous aurions ainsi un nombre astronomique d'adresses à disposition. Mais la migration serait relativement difficile – et tout ce dont nous avons besoin ne pourrait pas encore être mis en œuvre. Nous avons donc longuement réfléchi et opté pour la technologie Carrier-Grade NAT.

## Comment ça marche?

Avec un Carrier Grade NAT, le fournisseur n'attribue pas au client une adresse IPv4 publique mais une adresse IPv4 privée. La passerelle CGN traduit alors l'adresse privée en adresse publique pour l'accès à Internet, plusieurs clients se partageant l'une des rares adresses publiques. Ainsi, la réserve des adresses IPv4 disponibles sera suffisante pendant encore longtemps.

## Où en êtes-vous dans l'introduction de cette technologie?

Notre solution CGN est en service depuis bientôt six mois et fonctionne de manière parfaitement stable. En premier lieu, nous avons procédé à la migration vers le CGN des clients avec les abonnements les moins chers, que nous avons lancés à la fin 2016. Ensuite, ce fut le tour des abonnements à prix moyen – nous avons procédé avec prudence avec une migration par tranches de 100 clients, puis plus tard de 500 clients. Nous avons ainsi recueilli des feedback et procédé aux adaptations nécessaires. A ce jour, nous avons migré quelque 3000 clients – au pas de course, en deux mois seulement!

## Les clients sont-ils satisfaits?

C'est l'une de nos principales préoccupations, que la transition soit transparente pour nos clients dans la mesure du possible. Le fait que nous travaillions avec un CGN ne doit pas entraîner de changements chez le client. Dans la pratique, cela a parfaitement fonctionné: il y a eu des réclamations chez seulement 1% des clients migrés. La plupart du temps des webcams ou serveurs NAS qui



*Christoph Tobler, Responsable IT chez Leucom*

n'étaient plus accessibles depuis Internet. Pour de tels cas, nous offrons encore la possibilité d'activer une adresse IP publique.

## Comment avez-vous eu l'idée de sélectionner cette solution?

Un de nos partenaires exploite déjà un CGN avec succès depuis un an sur la base de son infrastructure Cisco. Mais j'ai fait d'autres recherches et je suis tombé sur A10 Networks. Le produit Thunder CGN m'a convaincu: il est spécialement conçu pour un CGN et est évolutif, car il offre aussi des fonctionnalités pour la migration vers IPv6. L'assistance du fabricant et distributeur Boll Engineering m'a particulièrement convaincu. Dès le départ, nous avions également un technicien à disposition en plus du vendeur. Nous avons eu des discussions ouvertes et l'alchimie a fonctionné.

## Comment votre infrastructure CGN est-elle configurée?

Aujourd'hui, nous exploitons deux appareils Thunder CGN et nous pouvons passer de l'un à l'autre en cas de panne. Le deuxième appareil prend alors automatiquement en charge le routage de l'unité en panne. Les deux se trouvent actuellement à Zurich, où la connexion Backbone se fait. A l'avenir, un troisième appareil est prévu à Frauenfeld en fonction des besoins. En ce qui concerne la puissance, nous n'aurons pas besoin de l'augmenter avant longtemps: la charge CPU est actuellement de 5%. Cela laisse encore beaucoup de marge pour des clients supplémentaires.