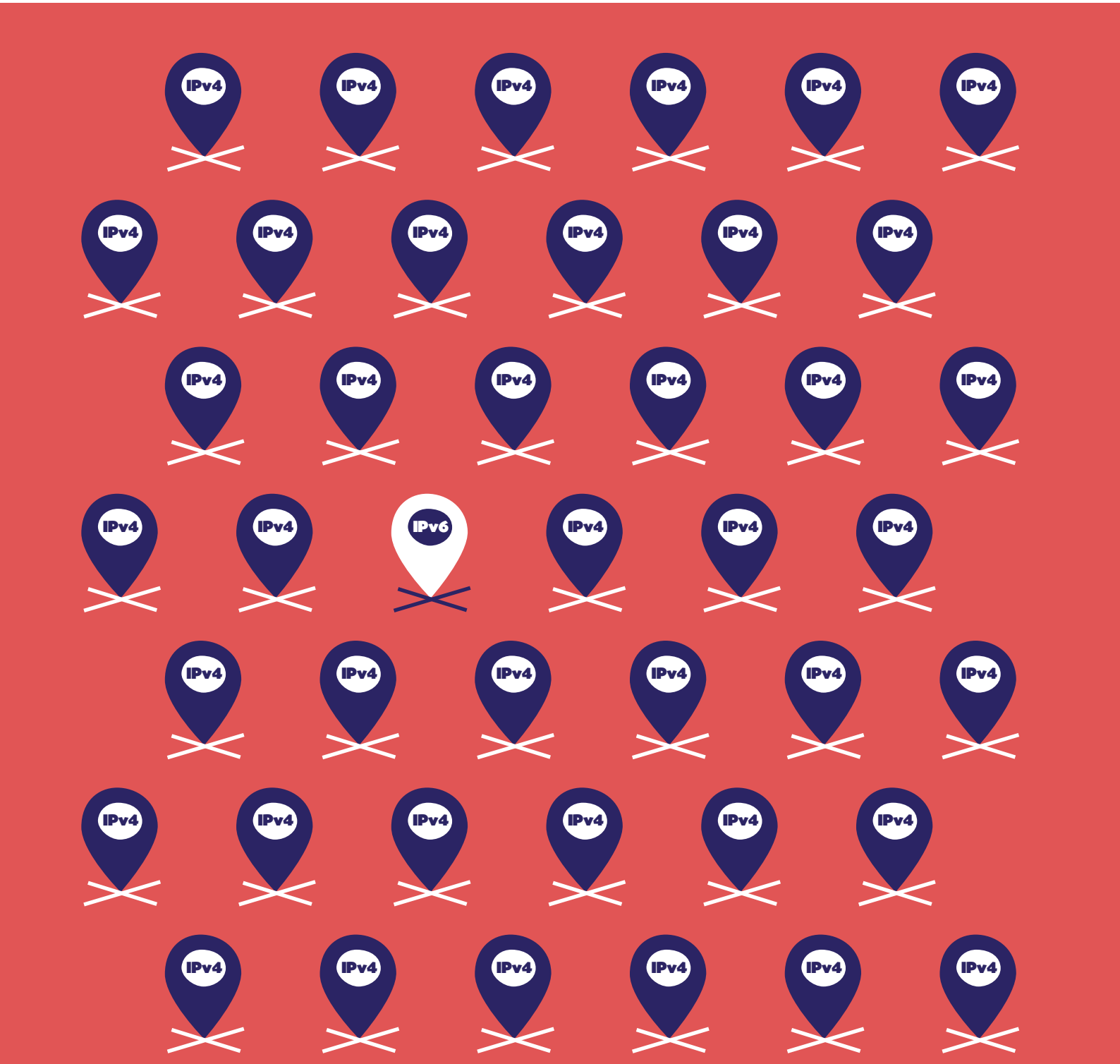
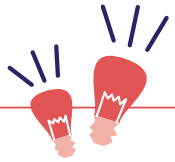
ENTREPRISES :
POURQUOI PASSER À IPv6 ?





Ce document a été réalisé par la task-force IPv6 co-pilotée par l'Arcep et Internet Society France.

L'Arcep et Internet Society France ont mis en place une task-force dédiée à IPv6 et ouverte à l'ensemble des acteurs de l'écosystème internet (opérateurs, hébergeurs, entreprises, secteur public, etc.). Elle a pour objectif de favoriser l'accélération de la transition vers le protocole IPv6 en permettant aux participants d'aborder des problèmes spécifiques et de partager les bonnes pratiques.

Inscrivez-vous à la task-force IPv6

Ce document ne représente pas une prise de position de l'Arcep mais reflète les travaux des participants à la task-force.

Décembre 2020

UNE PÉNURIE D'IPv4 PUBLIQUES ?

IPv4 et IPv6, pour *Internet Protocol* version 4 ou version 6, sont des protocoles utilisés sur internet pour permettre d'identifier chaque terminal sur le réseau (ordinateur, téléphone, serveur, etc.). Les adresses IP publiques sont « routables » sur internet, c'est-à-dire que leur réseau a la capacité d'acheminer le trafic depuis et vers les machines qu'elles représentent. Ces adresses publiques sont donc uniques mondialement.

Le protocole IPv4, utilisé sur internet depuis 1983, offre un espace d'adressage de près de 4,3 milliards d'adresses IPv4. Or le succès d'internet, la diversité des usages et la multiplication des objets connectés ont eu comme conséquence directe l'épuisement des adresses IPv4 effectif pour la région Europe et Moyen-Orient depuis le 25 novembre 2019. Le protocole IPv6 offre une quasi-infinité d'adresses : 667 millions d'IPv6 pour chaque millimètre carré de surface terrestre.

Les protocoles IPv4 et IPv6 ne sont pas compatibles : un équipement ne disposant que d'adresses IPv4 ne peut pas dialoguer avec un équipement ne disposant que d'adresses IPv6. La migration d'internet vers IPv6 s'impose donc.

Du fait de la complexité actuelle d'internet et de l'incompatibilité entre les protocoles IPv4 et IPv6, cette migration ne peut être effectuée en un seul jour. IPv6 doit être déployé progressivement, d'abord en parallèle d'IPv4, puis, quand tous les acteurs auront migré, en remplacement total d'IPv4.

POURQUOI FAUT-IL PASSER À IPv6 ?

Car le stock d'adresses d'IPv4 est épuisé depuis fin 2019 en Europe et qu'à terme, certains services pourraient ne plus être accessibles en IPv4 !

→ Si je reste en IPv4 sur mon réseau local ?
Certains services en ligne pourraient être inaccessibles totalement ou partiellement, pour vos employés.

→ Si mon site web reste en IPv4 ?
Certains internautes pourraient avoir des problèmes pour accéder à votre site, en fonction de ses fonctionnalités (par exemple si deux personnes cherchent à accéder à un site nécessitant une authentification avec la même adresse IPv4 partagée, la connexion de la seconde personne peut, dans certains cas, déconnecter la première). On pourrait aussi imaginer qu'un jour le référencement par certains moteurs de recherche dépende de l'accessibilité de votre site en IPv6.

La transition vers IPv6 est donc la seule solution pérenne pour le fonctionnement d'internet et est donc cruciale pour le fonctionnement du système d'informations (SI) de votre entreprise.

Pour les grandes entreprises, la transition vers IPv6 peut être aussi nécessaire si vous commencez à manquer d'adresses IP privées[1] utilisées pour votre SI.

[1] *RFC 1918 : 10.0.0.0/8 ; 172.16.0.0/12 et 192.168.0.0/16 soit 21,78 millions d'IPv4*
RFC 6598 : 100.64.0.0/10 soit 4,19 millions d'IPv4
RFC 4193 : fd00::/8

Par ailleurs, pour les grandes entreprises, la transition vers IPv6 peut simplifier le système d'adressage en permettant d'avoir beaucoup plus d'adresses à sa disposition que ce soit pour aller sur internet ou pour accueillir de nouveaux services ou de nouvelles applications déployées en mode virtuel.

Sur un plan plus technique, IPv6 est un prérequis à l'usage de la technologie de *segment routing* SRv6[2]. Cette dernière devient un maillon important de simplification de l'architecture réseau chez de nombreux opérateurs et devrait permettre à des grandes entreprises de se séparer des millefeuilles protocolaires courants (comme MPLS[3] et VxLAN[4]+EVPN[5] en *backbone* et *datacenter*). La simplification technique permise par le développement de cette technologie SRv6 pourrait ainsi permettre une réduction des coûts d'exploitation pour les entreprises.

Si l'on s'intéresse aux fournisseurs de solutions *cloud* de tout type, de plus en plus migrent vers IPv6 et certaines solutions de type temps réel comme de la softphonie en *cloud* requièrent un minimum de traitement intermédiaire. Il est ainsi probable qu'IPv6 devienne une recommandation chez de nombreux éditeurs.

La transition vers IPv6 est donc une nécessité, même si la phase de déploiement peut engendrer des coûts pour l'entreprise, en particulier pour les grandes entreprises.

DANS QUEL DÉLAI EST-IL POSSIBLE DE MIGRER MON ENTREPRISE VERS IPv6?

VOUS ÊTES UNE PME ?

Le passage à IPv6 est relativement simple et prend généralement peu de temps car la majorité des équipements sont déjà compatibles. Mais il est nécessaire de faire un audit de vos équipements réseau et sécurité pour s'en assurer.

Dans certains cas, le passage peut être effectué par votre opérateur et donc être transparent pour votre entreprise. N'hésitez pas à lui demander conseil.

Dans d'autres cas, il est nécessaire de configurer les différents équipements réseau et sécurité en IPv6 ou sur votre *front end* avec un *load balancer*[6] ou un *reverse-proxy*[7] qui fera la conversion entres les flux externes IPv6 natifs et vos applications restées en IPv4 avant de les convertir plus tard en IPv6 nativement.

Enfin, afin d'améliorer la maîtrise de votre réseau en prévision d'un éventuel changement de fournisseur (le préfixe IPv6 restant la propriété de l'opérateur), il est utile de maîtriser l'usage de la translation de préfixe NPTv6.

VOUS ÊTES UNE GRANDE ENTREPRISE ?

Un projet doit être mis sur place par les équipes SI. Le projet devra aussi impliquer les équipes métiers de votre entreprise qui utilisent différents équipements, applications spécifiques, etc.

L'ampleur de ce projet dépendra de l'organisation et de l'architecture réseau de votre entreprise. De même si vos sites distants sont connectés avec un service géré par un opérateur, il faudra soit demander à votre opérateur de fournir de l'IPv6 soit prévoir d'encapsuler IPv6 au sein du réseau IPv4 géré par l'opérateur.

Le projet devra suivre un séquencement articulé autour du besoin primaire (faire du B2C en IPv6, résoudre des problèmes de manque IPv4 interne chez des grands comptes, etc.). Il sera utile de solliciter séquentiellement les différentes entités concernées et de déployer IPv6 progressivement sur le périmètre visé.

[2] *SRv6 (Segment Routing over IPv6) : nouveau type d'en-tête de routage IPv6, constitué d'une liste d'adresses IPv6 identifiant les segments à traverser, ainsi que d'un compteur indiquant le nombre de segments restant à parcourir afin de pouvoir identifier le prochain segment à visiter.*
[3] *MPLS (MultiProtocol Label Switching) : mécanisme de transport de données basé sur la commutation de labels, qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie.*
[4] *VxLAN (Virtual eXtensible Local Area Network) : technologie de virtualisation réseau ayant des fonctionnalités semblables au VLAN et qui encapsule une trame Ethernet dans un datagramme UDP, dans le but d'isoler un plus grand nombre de machines virtuelles.*
[5] *EVPN (Ethernet VPN) : technologie pour transporter le trafic Ethernet de couche 2 en tant que réseau privé virtuel utilisant des protocoles de réseau étendu.*
[6] *Load balancer : équipement qui a pour tâche de répartir une charge de travail entre plusieurs serveurs.*
[7] *Reverse-proxy : serveur frontal permettant à un utilisateur d'internet d'accéder à des serveurs internes.*

QUELLES SONT LES ENTREPRISES QUI ONT DÉJÀ DÉPLOYÉ IPv6 ?

➔ **Des milliers de PME**, grâce soit une action volontaire de leur part soit à une activation en IPv6 de leur opérateur.

➔ **De nombreuses grandes entreprises** ont lancé un projet IPv6, mais rares sont celles qui ont terminé entièrement la transition.

IPv6 CHEZ EDF

S'il est très difficile de se représenter l'infini, l'inverse l'est tout autant pour percevoir que l'adressage privé IPv4 utilisé dans le réseau interne d'une entreprise a lui une fin : 18 millions d'IP, dont on peut arriver à bout.

Beaucoup de groupes ont été confrontés à ce problème par le passé, et ont souvent choisi d'utiliser en interne des adresses IPv4 publiques existantes sur internet. Une pratique qui atteint aujourd'hui ses limites à l'heure où l'on s'interconnecte avec de plus en plus de fournisseurs *cloud* en allant jusqu'à annoncer leurs véritables adresses IP publiques sur le réseau interne ; ou encore en autorisant les télétravailleurs à joindre des applications SaaS directement sans repasser par le VPN (*split tunneling*). Les solutions de SD-WAN* mettent également en avant ce type de délestage à l'échelle des campus (*local breakout*). Tout cela sans compter certains flux temps réel comme la voix qui doivent subir le minimum de traitement intermédiaire avant de partir vers le *cloud*.

Face à cette problématique d'une pénurie annoncée sur l'adressage interne, nous avons choisi d'étudier la possibilité d'y répondre via IPv6 plutôt que par les « bidouilles » de recouvrement d'adressage IPv4 ; se basant sur le fait que l'implémentation du protocole semblait mature ou proche de l'être dans un grand nombre de solutions.

Les adresses IP concernent l'ensemble du système d'information de l'entreprise, il faut donc être très méthodique dans l'implémentation du *dual-stack*, et celle du retrait d'IPv4 sur certaines portions du SI.

Notre objectif à terme est de pouvoir se passer d'IPv4 sur les réseaux tertiaires des campus, grands consommateurs d'IP, qui ont l'avantage de fonctionner autour d'un écosystème bureautique plutôt homogène basé sur des solutions bien connues du marché. On peut donc profiter d'un facteur de mise à l'échelle.

L'ordre d'implémentation consiste à remonter dans les couches du

**SD-WAN (Software-Defined Wide Area Network) : technologie de transport de paquets IP séparant la partie matérielle et logicielle du réseau, qui permet un contrôle et un déploiement centralisé et automatisé sur des équipements hétérogènes.*

SI par le bas : réseau (*backbone*, campus et *data center*), puis système (socle d'OS) et enfin application tant côté client que serveur (navigateur, *middleware*, appli monolithique…).

Peu d'environnements disposent d'un écosystème de qualification intégral, les serveurs de qualifications sont souvent sur des réseaux de production dans des espaces dédiés, etc. Impossible donc de qualifier tant que la production sous-jacente n'est pas prête, et ainsi de suite…

Le d*ual-stack* doit atteindre en priorité les services d'infrastructure, les consommateurs de bande passante et flux temps réel (DNS, DHCP**, proxy, annuaire, messagerie, téléphonie/ collaboration, NAS***, impression, déploiement de mises à jour…) avant de s'attaquer aux applications métiers.

Il est important de faire du bout en bout sur des périmètres-pilotes restreints afin de qualifier progressivement chaque type d'élément et de capitaliser, pour être à terme en mesure d'industrialiser le déploiement horizontalement en élargissant le périmètre.

Il ne faut cependant pas cibler un passage global interne au *dual-stack*, au-delà des campus et des services d'infrastructure, notre stratégie cible un passage progressif des frontaux d'applications en *dual-stack*. Pas d'urgence donc à migrer les *backends*, d'autant qu'ils sont extrêmement nombreux et hétérogènes.

Nous utiliserons de la translation DNS64/NAT64 en entrée de *data center* afin de joindre les applications IPv4 à partir de clients IPv6. Un autre prérequis majeur au retrait d'IPv4 est que la totalité des utilisateurs puissent communiquer sur IPv6, il faut donc qu'il soit déployé sur l'ensemble des campus avant d'entamer le retrait de v4.

Peu de retours existent en dehors d'entreprises dont l'IT est le cœur de métier et il est extrêmement difficile d'estimer le cout de déploiement et le surcoût d'exploitation liés au *dual-stack*. De plus l'ensemble des impacts ne peuvent pas être identifiés en amont. Faire transiter de l'IPv6 est une chose, adapter tout l'écosystème amont et aval en est une autre.
La seule adaptation du SIEM**** qui corrèle les logs de l'entreprise sera un défi, et ce fut probablement l'un des points les plus faciles à identifier.

Le projet vise aussi à permettre l'accès aux sites web publics en IPv6.

Pour conclure, les usages à venir tels que les microservices / containers et l'internet des objets vont sans doute faire exploser les besoins d'adressage dans les années à venir.
Il convient donc de s'atteler au plus tôt, afin de préparer le SI à cette transition qui risque d'être longue et douloureuse.

** *DHCP (Dynamic Host Configuration Protocol) : protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une machine.*
*** *NAS (Network Attached Storage) : serveur de stockage de fichiers, autonome et relié à un réseau*
**** *SIEM (Security Information and Event Management) : système de gestion des événements de sécurité informatique.*

IPv6 CHEZ SCHNEIDER ELECTRIC

Nous menons actuellement chez Schneider Electric une réflexion autour de la mise en place d'IPv6 sur notre réseau d'entreprise. Les caractéristiques de notre réseau, qui sont importantes en particulier dans le contexte d'IPv6, sont sa taille et la multitude de ses points de présence.

Schneider Electric a la particularité d'être une grande industrie et non une entreprise IT, même si nous sommes en train de nous tourner davantage vers du service et du logiciel.

Chez Schneider, le volet produits et services est le plus avancé en IPv6 : pratiquement tous nos produits IoT ont une double pile IPv4 et IPv6. En effet, tous les produits livrés à nos clients sont déjà IPv6-*ready*. Par ailleurs, une grande partie des développeurs et des ingénieurs travaillent depuis une bonne dizaine d'années en IPv6 et certains ont même contribué aux travaux de l'IETF sur le sujet.

Il y a également toute la partie IT de Schneider pour délivrer des services à nos 120 000 employés. Notre réseau d'entreprise est uniquement raccordé en IPv4 et des problèmes commencent à apparaître pour cette raison. Ces problèmes concernent :

→ **Une impossibilité d'accès aux ressources disponible en IPv6-*only* :** en effet, des succursales de Schneider en Asie ont signalé qu'elles étaient dans l'incapacité d'accéder à des ressources internet uniquement disponibles en IPv6. De plus, notre serveur proxy officiel n'est pas compatible IPv6, ce qui rend la résolution du problème encore plus complexe.

→ **Des brèches de sécurité :** des problèmes de sécurité ont émergé dans des labs ou plus généralement dans des zones du réseau où il y a des développeurs qui, pour des besoins spécifiques, n'utilisent pas l'accès internet dédié de Schneider, mais commencent à connecter dans le LAN des box internet qui ont de l'IPv6 activé. Ces box annoncent donc des routes en IPv6 sur ce LAN. Même si le LAN n'est pas IPv6-*ready*, les *switchs* et les dispositifs de routage qui gèrent déjà IPv6 véhiculent ces annonces de routes en IPv6. Par conséquent, les piles IPv6 des postes de travail voient arriver de l'IPv6 et répondent à ces requêtes, créant ainsi des brèches de sécurité. Ceci a notamment été constaté au niveau de notre succursale en Australie.

Ceci amène une réflexion plus globale : avec la taille et la dimension internationale de nos activités, comment un déploiement d'IPv6 sur notre réseau d'entreprise pourrait résoudre les problèmes que nous rencontrons ?

Actuellement, nous ne sommes pas encore confrontés à une pénurie d'adresses IPv4. En termes d'utilisation, la moitié d'un /10 est allouée et diffusée sur l'ensemble du monde, en prenant en compte toutes les filiales acquises ces dernière années. Penser à une migration vers IPv6 ou une compatibilité IPv6 pourrait s'avérer une tâche fastidieuse. Nous cherchons ainsi un mode de compatibilité progressif à mettre en place.

Par ailleurs, plusieurs de nos serveurs web sont uniquement en IPv4 et nous nous posons donc la question suivante : à quel moment faudra-t-il faire le pas pour lancer une présence en IPv6 pour nos serveurs ? De plus, beaucoup d'équipements sur les sites R&D ne sont pas compatibles IPv6 et nous sommes obligés de maintenir une pile IPv4 ou utiliser une passerelle pour continuer à utiliser ses équipements. Dans le cadre de notre migration vers SD-WAN, Cisco SDWAN Viptela ne supporte pas bien IPv6 et nous ne sommes pas aidés par nos fournisseurs de service qui ne fournissent pas de l'IPv6 sur cette technologie.

Une solution envisageable pour avoir accès aux services en IPv6 serait de tout laisser en IPv4 en interne et de s'appuyer sur un proxy qui gère IPv6.

Il n'y a pas de doute sur l'importance de la mise en place d'IPv6. Par contre, le manque d'information sur la façon avec laquelle il faut procéder nous pose problème. Beaucoup d'entreprises réfléchissent à faire la transition mais peu ont sauté le pas. Ceci rend la démarche de l'Arcep avec la task-force intéressante pour pouvoir échanger entre entreprises concernées par IPv6.

IPv6 CHEZ DIGDEO

1. LE PARI DE DIGDEO : EN FINIR AVEC LES RÉSEAUX NAT EN IPv4

DigDeo, SSLL en infogérance, hébergement, logiciels libres, vient de fêter ses 10 ans. DigDeo prône l'automatisation avec l'Infrastructure As Code, la méthode DevSecOps, la sécurité renforcée pour tous et des applications clients performantes. Cette approche par l'automatisation permet de réduire les coûts pour les clients, limiter les actions manuelles des équipes d'ingénieurs, accélérer les développements et améliorer la traçabilité notamment pour simplifier les audits de sécurité ISO 27001.

Le point de départ est d'abord une mauvaise expérience de la gestion des IPv4 par certains grands groupes français, avec des adresses avec plusieurs niveaux de NAT successifs, qui rendent très difficile la gestion, le débugage ou la résolution des problèmes avec les *firewall*s au sein d'un système d'information. Il s'agit souvent du résultat de fusion de réseaux successifs sans remise à plat.

Assez vite après sa création, DigDeo s'est déclaré LIR auprès RIPE pour avoir des adresses IPv4 et IPv6, mais le nombre d'adresses IPv4 était insuffisant pour pouvoir faire un *cloud* de « bonne taille ». Nous nous sommes d'abord rattachés à un AS d'un prestataire, sans AS en propre, pour bénéficier d'un réseau bien connecté et de solutions de DDoS. **Nous avons affirmé dès 2012 avoir la volonté de bannir complètement le NAT IPv4**. Un objectif : **une adresse IP doit être unique,** IPv6 répond à ce besoin. Fini l'équipement en 172.16.0.1 naté en 192.168.0.1 quand le flux remonte vers une DMZ et est encore naté en 10.42.42.1 pour tel prestataire, car il a des conflits d'adressage en 172 et 192 déjà utilisés en interne.

Nous avons tenu cet engagement et nous sommes satisfaits du résultat. Nous utilisons des adresses IPv4 privées, par exemple pour certains VPN en plus de l'IPv6. Dans ce cas, seul le NAT IPv4 de translation adresses privé / adresse publique est possible.

Ainsi quand nous déployons l'infrastructure d'un client, par défaut, tous les serveurs ont au moins une IPv6 : c'est la norme chez Digdeo. L'IPv4 publique est devenue optionnelle avec des machines *dual-stack* seulement pour les équipements exposés sur internet (serveur web, *firewall*, l*oad balancer*). Ainsi les serveurs de base de données de type MySQL ou PostgreSQL, qui ne sont pas exposés sur internet, ne sont qu'en IPv6, pour économiser les IPv4 publiques. Tous les réseaux de SI hébergés qui étaient IPv4 NATés ont été basculés en IPv6-*only*. Enfin, DigDeo vient de mettre en place un réseau d'administration en IPv6-*only* qui nous permet un découpage idéal à la vue de la quantité d'IP possibles en IPv6.

2. LE RETOUR DES CLIENTS SUR L'ADOPTION D'IPv6

Le passage à IPv6 a permis de résoudre les problèmes de NAT pour le personnel devant accéder à des ressources *backend* : développeurs, contributeurs, administrateurs. Nous avons poussé certains clients à demander à leur fournisseur d'accès à internet d'activer IPv6 sur leur *firewall* : cela a fonctionné pour deux tiers des clients, le dernier tiers considérant cela trop compliqué principalement par peur de la nouveauté et le risque de toucher à une installation qui marche.

En première étape, nous demandons aux clients d'activer seulement IPv6 au niveau du WAN avec NAT46 pour gérer la translation IPv4 vers IPv6. Souvent les équipements *firewall* ne sont pas au point où l'équipe en charge ne veut pas toucher à cela, dans ce cas nous préconisons d'avoir un premier réseau en *dual-stack* vers les postes du personnel devant accéder au *backend* pour commencer. Globalement, les personnes habilitées aux *backends* sont satisfaites de pouvoir accéder au serveur sans redirection de ports et sans VPN grâce à IPv6.

Les clients ont aussi vu des logiciels propriétaires (des logiciels de téléphonie sur IP notamment) qui ne supportaient pas le NAT IPv4 fonctionner à nouveau grâce à la bascule en IPv6.

Le résultat est probant sur nos serveurs DNS faisant autorité pour nos domaines et ceux de nos clients : il y a plus de requêtes DNS en IPv6 (54%) qu'en IPv4 (46%) tous flux confondus.

La plupart de nos clients se posent la question d'avoir une IPv6 publique et donc attaquable. Nous les rassurons sur le fait que nous supprimons la translation d'adresses mais que nous conservons le *firewall* : « ce n'est pas parce qu'on n'a pas de NAT qu'on n'a pas de règles *firewall* ». Avec le même principe qu'en IPv4 avec une règle par défaut qui interdit des flux IPv6 d'entrer, le niveau de « protection » est équivalent à l'IPv4 avec un NAT qui cache le réseau interne.

3. ET LA TRANSITION VERS IPv6 AU SIÈGE DE DIGDEO ?

DigDeo dispose deux accès *dual-stack* IPv4 et IPv6. Nous souhaitons faire une bascule franche pour le siège sans passer par le *dual-stack*. Cette transition vers IPv6-*only* ou *dual-stack* n'a pas encore été faite en raison de plusieurs obstacles :

→ **Certains équipements ne font pas d'IPv6-*only*,** notamment des bornes Wi-Fi, une imprimante et des caméras de surveillance.

→ **Le manque d'expérimentation sur le *dual* WAN IPv6 :** étant donné qu'il y a deux accès à internet, les postes doivent avoir deux IPv6, avec une dans chacun des sous-réseaux mais la gestion au niveau de la priorisation des flux et la bascule en cas de coupure d'un WAN au niveau du *firewall* nécessite encore un peu d'étude avant une bascule franche.

Comme il y a moins d'urgence sur un réseau interne à supprimer l'IPv4 (merci la RFC 1918 de nous en donner autant) notre raison pas trop avouable est que nous attendons que nos équipements non compatibles IPv6 ne fonctionnent plus pour passer sur des équipements IPv6-*ready*.

Le fait de passer directement en IPv6-*only* demandera moins de travail, par rapport à une étape en *dual-stack* pour le siège. Pour les serveurs, le *dual-stack* est la bonne solution mais avec les contraintes d'avoir une entrée DNS (plus pratique qu'une IPv6 dictée par téléphone par exemple), de gestion de deux réseaux différents (configuration, transit, *peering*), superviser les équipements et leurs services en IPv4 et IPv6. Globalement tous les freins concernant les réseaux, logiciels, configurations, méthodes pour l'IPv6 ont été levés depuis pas mal d'années en interne, nous faisons tourner des productions conséquentes en IPv6 **et finalement ce n'est pas plus compliqué que l'IPv4.**

4. ACCÉLÉRER LA TRANSITION VERS IPv6

L'avenir se dessine en *dual-stack* côté infrastructure et côté résidentiel. Les nouveaux acteurs de type fournisseurs d'accès internet mobile, domestique ou pro n'auront d'autre choix que payer au prix fort des IPv4 ou alors assumer une position IPv6-*only* en contrepartie de services disruptifs introuvables ailleurs. Ce type d'action coup de poing fera faire des pics de demandes en connectivité IPv6 de la part du grand public ou des entreprises. Ces acteurs-là seront un des moteurs pour l'IPv6-*only* et ils vont arriver de manière fracassante à la manière de la saga de cet été entre Epic Games contre Apple et Google.

Nous ne sommes pas non plus à l'abri que des acteurs mondiaux décident d'en finir avec IPv4, si les moteurs de recherche privilégient les sites en IPv6 dans leur classement après avoir poussé les sites à être rapides, responsive et sécurité avec SSL / TLS, une forte demande en connectivité et configuration IPv6 arrivera d'un coup. Apple a déjà exigé depuis 2016 que toutes les applications soient compatibles avec un réseau d'accès IPv6-*only* et donc naturellement avec le NAT64 et DNS64.

Si j'imagine assez mal la fin de l'internet IPv4, je suis persuadé qu'il faut que chaque service sur internet soit disponible en *dual-stack* pour permettre à tout terminal qu'il soit IPv4 ou IPv6-*only* ou *dual-stack* de pouvoir bénéficier du même service avec une qualité égale peu importe le protocole disponible.

Les professionnels doivent être prêts, le *dual-stack* IPv4 et IPv6 est une nécessité sur internet.

IPv6 AU SEIN DE L'OLYMPIQUE LYONNAIS

L'OL Groupe compte environ 550 salariés, avec environ 150 personnes du côté sportif et le reste des effectifs pour les services administratifs et support. L'OL est donc une PME mais qui peut compter plus de 2500 personnes les jours de matchs.

Le réseau est assez étendu pour permettre les échanges entre terminaux sur le stade, les communications des journalistes, etc. Le réseau doit être dimensionné pour permettre à près de 60 000 personnes de communiquer en même temps pendant un match.

La transition vers IPv6 a été intégrée dans le projet global de construction du nouveau stade de l'OL. Une nouvelle infrastructure a alors été mise en place (serveurs, réseaux, déploiement d'applications spécifiques, etc.). Lors de la construction de ce nouveau stade, les équipements ont été remplacés et le dimensionnement de tout le réseau a évolué : cœur de réseau, *switchs* d'accès, *firewalls*, infrastructures serveurs, stockage, terminaux métiers dans les stades, etc.

Ce projet a été l'occasion de déployer IPv6. La transition vers IPv6 a été motivée par la connaissance de la migration vers ce protocole par les équipes, plutôt que par un besoin technique. Cette transition a vocation à préparer l'avenir. Les coûts ont été intégrés dans le projet global. Le réseau a été basculé en double pile (*dual-stack*) sur tout le périmètre. IPv6 est en production depuis janvier 2016.

Lors de la refonte du site, il est aussi devenu accessible en IPv6 pour les clients externes. L'éditeur Atos a expliqué qu'on ne lui demandait généralement pas d'IPv6. Les sites hébergés en interne ne sont par contre pas tous en IPv6. Le *firewall* de l'applicatif web a nécessité un peu de du travail pour fonctionner en IPv6. L'IPv6 permet d'atténuer les problèmes du NAT IPv4 pour les gros services comme Google, Facebook, Instagram, etc.

Cette transition n'a pas entrainé de changement important au quotidien pour les utilisateurs.

Le Wi-Fi invité n'est pas encore en IPv6 car la solution de portail captif retenue est une solution française qui ne supporte pas IPv6. IPv4 pour le Wi-Fi permet ainsi de faire du NAT en utilisant 1 seule adresse publique pour 10 000 personnes.

Nous n'avons pas vraiment eu de difficultés techniques pour effectuer cette transition. La difficulté a plutôt été de convaincre les constructeurs et intégrateurs IT car IPv6 n'était pas encore habituel en 2015/2016. Les acteurs du monde de l'industrie et du bâtiment ne connaissaient pas IPv6 : il a été nécessaire de vérifier avec eux les documentations des équipements sur la compatibilité IPv6 et leur demander d'activer IPv6. Les différents acteurs disaient « c'est la première fois qu'on nous demande de l'IPv6 » mais cela ne devrait donc plus être le cas maintenant.

Les avantages ne sont pas visibles immédiatement mais, comme l'internet est en pénurie d'adresses IPv4 publiques, les difficultés vont apparaître dans 2 ou 3 ans. Le plus tôt sera donc le mieux pour s'attaquer à la transition, surtout pour les entreprises qui ont des refontes massives de leurs réseaux et applications à faire. Il n'y aura plus de choix dans quelques années quand les grosses plateformes de *cloud* comme Azure ou AWS vont avoir des difficultés à récupérer des IP publiques pour les services qu'ils proposent. Les développeurs vont s'arracher les cheveux quand ils seront obligés de mettre du NAT pour mettre une application web sur le *cloud*.

Les gains techniques ne sont pas forcément très visibles. Passer en IPv6 permet de s'affranchir du NAT. Certains voient malheureusement encore cela comme un désavantage car ils considèrent le NAT comme un élément de sécurité, alors qu'un *firewall* offre autant de sécurité mais permet d'éviter les translations de ports et les règles de NAT. Le changement des adresses est parfois un frein, mais il suffit de prendre l'habitude, les adresses IPv6 permettent de mettre plus d'informations dans la structure de l'IPv6. Par exemple, nous utilisons un octet dans l'adressage IPv6 qui correspond directement au numéro de VLAN, ce qui permet de vérifier rapidement et simplement si une machine est dans le bon VLAN.

Le plus tôt sera le mieux pour basculer en IPv6 !

QUELLES PARTIES DE L'INFRASTRUCTURE DE MON ENTREPRISE BASCULER EN IPv6 ?

La transition vers IPv6 peut se concrétiser de différentes façons pour une entreprise :

➔ rendre les services de votre entreprise qui sont exposés sur internet accessibles en IPv6 : site web, VPN, mail, etc. ;

➔ s'assurer que les applications « internes » hébergées à l'extérieur fonctionnent en IPv6 ;

➔ permettre à l'entreprise d'accéder à internet en IPv6 depuis ses postes internes. Si votre entreprise utilise un proxy, il n'est pas forcément nécessaire de passer tous les postes en IPv6 ; il faut seulement que le proxy ait accès à la partie IPv6 d'internet (en plus de celle IPv4) ;

➔ basculer le réseau interne de l'entreprise (trafic vers des sites internes et trafic entre les postes de l'entreprise et le proxy) en IPv6. Le passage de l'intranet en IPv6 peut être fait dans un second temps, à condition que les échanges avec le réseau internet puissent se faire en IPv6 ;

➔ offrir IPv6 sur le service d'accès réseau Wi-Fi invité ;

➔ demander IPv6 à ses clients, fournisseurs, partenaires, etc. ;

➔ intégrer systématiquement IPv6 dans ses appels d'offres et demander l'activation d'IPv6 ;

➔ etc.

FAUT-IL DÉPLOYER LES ORDINATEURS ET SERVEURS EN DOUBLE PILE OU EN IPv6-*ONLY* (EN INTERNE) ?

Il existe 2 façons d'effectuer la transition d'IPv4 vers IPv6 :

➔ la migration en double pile (*dual-stack*)[8] consiste à conserver en parallèle les deux protocoles IPv4 et IPv6, en affectant une adresse IPv4 et une adresse IPv6 à un équipement du réseau ;

➔ la migration en IPv6-*only*[9] consiste à remplacer complètement le protocole IPv4 par le protocole IPv6.

[8] Double pile (dual-stack) : consiste à affecter une adresse IPv4 et une adresse IPv6 à un équipement du réseau.
[9] IPv6-only : la box ou le terminal n'est connecté(e)s au réseau que via une adresse IPv6.

Voici des éléments de comparaison de ces deux procédés de transition :

	DOUBLE PILE (*DUAL-STACK*)	**IPv6-*ONLY***
Accès IPv4/IPv6	• Accès à la fois à IPv4 et à IPv6, permettant une migration en douceur	• Pas d'accès en IPv4 : des mécanismes de traduction d'adresses comme le NAT64+DNS64 ou des *reverse proxys* spécialisés sont nécessaires pour accéder aux ressources IPv4-*only*
Configuration	• Nécessite de configurer à la fois IPv4 et IPv6	• Nécessite que l'ensemble des postes possèdent de l'IPv6 avant d'entamer le retrait d'IPv4 (exemple typique lors de la dépendance à la téléphonie SIP) • Configuration plus simple
Sécurité	• Différences de politiques de sécurité *au niveau des firewalls* • Différences de services disponibles sur les serveurs double pile • Définition des règles des IPS/IDS doublées	• Une seule configuration de sécurité

Si vous souhaitez garantir une connectivité en IPv6 mais que votre réseau interne est encore en IPv4, une solution transitoire peut consister à utiliser un *load balancer* ou un *reverse proxy* (pour les serveurs) ou alors un *proxy* (pour l'accès à internet de l'entreprise) qui s'assurera de la conversion en attendant que vos applications soient migrées en IPv6 natif.

QUELS SONT LES « SCÉNARIOS DE SORTIE » D'IPv4 PLAUSIBLES ?

Le scénario de sortie d'IPv4 n'est pas connu et est très difficile à prévoir à ce jour. Si l'on essaie malgré tout d'imaginer les différentes étapes d'un tel scénario, on arrive par exemple à une séquence telle que celle-ci :

1. La quasi-totalité des offres d'accès internet grand public commercialisées proposent de l'IPv6 activé par défaut en plus de l'IPv4.

2. La quasi-totalité des offres d'accès internet grand public, pro et entreprise proposent de l'IPv6 activé par défaut. Une connectivité IPv4 est toujours proposée.

3. Une part non négligeable des sites web sont hébergés en IPv6 uniquement, malgré des poches de résistances à l'IPv6 pour l'accès proposés par quelques entreprises à ses salariés. Ces sites ne sont plus accessibles depuis une entreprise qui bloque l'IPv6.

4. Une part non négligeable des offres des fournisseurs d'accès à internet ne proposent plus de connectivité IPv4. Il n'est plus possible de consulter des sites web hébergés en IPv4 uniquement.

5. La majorité des sites web abandonnent IPv4, devenu inutile. IPv4 n'est plus utilisé sur internet, mais peut continuer à être utilisé pour des réseaux privés.

VOUS AVEZ DÉCIDÉ DE DÉPLOYER IPv6 DANS VOTRE ENTREPRISE

Pour vous accompagner dans la mise en œuvre de cette transition, la task-force poursuivra ses travaux avec la réalisation d'un guide méthodologique sur « Comment déployer IPv6 ? » qui sera prochainement disponible. Plusieurs acteurs d'internet proposent des méthodologies dans lesquelles sont décrites les étapes d'analyse, de formation, d'architecture, de configuration, de tests, de mise en œuvre de la sécurisation d'IPv6, de la gestion d'exception pour les équipements qui ne peuvent pas être convertis en IPv6 et de l'évolution de la politique d'achat qui doit alors permettre d'acquérir uniquement de nouveaux équipements fonctionnant en IPv6.

RESSOURCES UTILES SUR LE DÉPLOIEMENT D'IPv6 :

→ Le MOOC Objectif IPv6 disponible sur la plateforme Fun MOOC

→ Le livre « IPv6 Théorie et Pratique » réalisé par l'association G6

→ Le livre Deploying IPv6 Networks, écrit par Ciprian Popoviciu (payant ; ISBN : 978-1587052101)

→ Le livre IPv6 Fundamentals, Cisco Press écrit par Graziani (payant ; ISBN : 978-1-58714-477-6)

→ Rapport MR-276 du Broadband Forum