TRANSITION VERS IPv6
L'Arcep publie un compte-rendu de la réunion de lancement de la task-force IPv6 en France

Paris, le 18 décembre 2019

Dans la continuité de ses ateliers relatifs à la transition vers le protocole IP♥6, l'Arcep a créé une task-force, co-pilotée avec Internet Society France, pour accélérer la transition vers IPv6 en associant l'ensemble des acteurs d'internet qui le souhaitent (opérateurs, hébergeurs, entreprises, secteur public, etc.).

Dans un contexte d'annonce de pénurie d'adresses IPv4 désormais atteinte, l'Arcep a accueilli dans ses locaux une cinquantaine d'acteurs le 15 novembre 2019, pour lancer la task-force et organiser des groupes de travail multi parties prenantes :

- Le premier groupe de travail s'est intéressé aux **impacts de la pénurie d'IPv4**. Les ateliers de travail se sont focalisés sur les alternatives en cas de non transition vers IPv6, les solutions techniques pour la transition ainsi que les problèmes de compatibilité avec IPv6 des équipements, logiciels ou applications. Une *keynote* du RIPE NCC (le registre régional d'adresses IP qui alloue les IPv4 pour l'Europe et le Moyen-Orient) a précédé ce groupe de travail et a permis d'apporter une vision régionale de la situation actuelle de la pénurie d'IPv4 et d'illustrer l'urgence d'accélérer la transition vers IPv6.
- Le second groupe de travail a permis de traiter **les enjeux de la sécurité d'IPv6**. Les échanges ont abordé la sécurisation du réseau local, les problématiques d'anonymisation et de vie privée ainsi que les problématiques de filtrage. Une *keynote* de l'ANSSI (l'Agence nationale de la sécurité des systèmes d'information) a introduit ce groupe de travail en mettant l'accent sur l'intérêt de repenser la sécurité avec IPv6.

Le compte-rendu des travaux de ces groupes est publié ce jour. D'ici à la prochaine réunion de la task-force IPv6 prévue au printemps 2020, les participants approfondiront ensemble certains des axes de travail identifiés.

Contact presse
Anne-Lise Lucas
Anne-Lise.LUCAS@arcep.fr
Tél. : 01 40 47 71 37

Les documents associés

Les vidéos de la réunion de lancement de la task-force IPv6

• Ouverture de l'atelier par **Loïc Duflot**, directeur Internet, Presse, Poste et Utilisateur à l'Arcep et par **Nicolas Chagny**, président de l'Internet Society France

• Présentation du baromètre de la transition vers IPv6 en France par **Aurore Tual**, cheffe d'unité internet ouvert, **Samih Souissi** et **Vivien Gueant**, chargés de mission à l'Arcep

• Keynote de **Xavier Le Bris**, RIPE NCC

• Intervention de **Sébastien Soriano**, président de l'Arcep

• Keynote d'**Arnaud Ebalard**, ANSSI

A propos de l'Arcep

L'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse, arbitre expert et neutre au statut d'autorité administrative indépendante, est l'architecte et le gardien des réseaux d'échanges internet, télécoms fixes, mobiles et postaux en France.

Compte-rendu de la réunion de lancement de la task-force IPv6 en France

Les différents ateliers ont permis d'identifier des propositions d'actions concrètes visant à en accélérer la transition.

Le tableau en annexe expose en détail les différents points qui ont émergé de chaque groupe de travail.

1. Groupe de travail : Quels impacts de la pénurie d'IPv4 ?

a. Le contexte et les enjeux

- Nécessité de garder IPv4, tant que la transition vers IPv6 n'est pas finalisée au niveau des différents maillons de la chaine technique d'internet ;
- Problèmes générés par les alternatives en cas de non transition (achat d'IPv4 ou partage d'adresses IPv4) ;
- Existence de diverses options pour faire la transition : IPv6 dans un réseau *IPv4-Only*, *dual-stack*[1] ou IPv4 dans un réseau *IPv6-only* ;
- Problèmes de compatibilité IPv6 de certains équipements, applications, logiciels, services, etc. ;
- Différences de gestion entre IPv4 et IPv6, notamment dans les fonctionnalités déployées et en termes de performances ;
- Besoin de renforcer l'exemplarité de l'État dans la transition vers IPv6.

b. Les axes de travail

- Communiquer auprès des entreprises pour les inciter à effectuer leur transition vers IPv6 ;
- Inclure l'activation d'IPv6 dans les appels d'offres, au-delà de la compatibilité IPv6 ;
- Avoir des retours d'expérience d'entreprises qui ont réalisé la migration d'IPv4 vers IPv6 (au moins en *dual-stack*) pour estimer les coûts, les bénéfices, les conditions techniques, etc. ;
- A partir des retours d'expériences, rédiger un guide de développement interne pour le déploiement d'IPv6 ;
- Identifier les différentes catégories d'applications, équipements ou logiciels pour lesquels des dysfonctionnements dus au *Carrier Grade NAT* (CGN)[2] sont observés ;
- Recenser les différentes catégories d'applications, équipements et logiciels qui posent des problèmes de compatibilité avec IPv6.

[1] Double pile IP : consiste à affecter une adresse IPv4 et une adresse IPv6 à un équipement du réseau.

[2] *Carrier Grade NAT* : mécanisme de traduction d'adresse réseau (*Network Address Translation* ou NAT) à grande échelle, utilisé notamment par des FAI dans le but de diminuer la quantité d'adresses IPv4 utilisées.

2. Groupe de travail : Quels enjeux de la sécurité d'IPv6 ?

a. Le contexte et les enjeux

- Existence de plusieurs aspects de sécurisation du réseau IPv6 similaires en IPv4 mais IPv6 nécessite de repenser la sécurité ;
- Faible disponibilité des compétences et méconnaissance des offres de sécurité IPv6 existantes ;
- Présence de plusieurs référentiels et RFC non mis à jour ;
- Prise en considération nécessaire des enjeux d'anonymisation et la protection de la vie privée lors de la mise en place d'IPv6 ;
- Manque de connaissance des bonnes pratiques en termes de filtrage IPv6.

b. Les axes de travail

- Recenser les RFC et les formations sécurité IPv6 à jour ;
- Compiler les ressources existantes du RIPE ainsi que les initiatives d'Internet Society et les mettre à jour ;
- Lister les problèmes de *privacy* occasionnés par IPv6 et discuter des différentes contremesures ;
- Émettre des recommandations sur la façon avec laquelle le filtrage IPv6 doit s'effectuer.

Pour rappel, cette restitution ne constitue en rien une prise de position de l'Arcep sur la pertinence, la faisabilité ou la priorité des axes de travail. Elle décrit uniquement les informations remontées par les différents participants à la task-force IPv6. Les priorités des actions à mettre en place se feront en concertation avec la communauté des participants.

Annexe : Restitution des groupes de travail

Groupe de travail	Atelier	Contexte et enjeux	Axes de travail proposés par les participants
Quels impacts de la pénurie d'IPv4 ?	**Les alternatives en cas de non transition : achat d'IPv4 et partage d'adresses**	• Nécessité de garder IPv4 pour tous les acteurs encore plusieurs années, qu'IPv6 soit proposé ou pas. • Nécessité de solutions pour absorber la croissance, après avoir optimisé la ressource. • Achat / Location d'IPv4 : risques de blocage de certains services utilisant la localisation (vidéo à la demande, services financiers, services de l'Etat etc.). • Partage d'IPv4 : problématiques pour identifier l'abonné ; nombreux usages dégradés par le CGN.	• Communiquer auprès des entreprises pour les inciter à effectuer leur transition vers IPv6. • Développer les formations à IPv6 : ○ Formations pour les ingénieurs mais aussi pour les managers ; ○ Formations dans les écoles d'ingénieurs : orienter davantage sur IPv6 et sur des études de cas concrets. • Inclure l'activation d'IPv6 dans les appels d'offres, au-delà de la compatibilité IPv6. • Édicter des bonnes pratiques pour les règles anti-spam pour IPv6, afin de favoriser la transition vers IPv6 du mail. • Identifier les différentes catégories d'applications, équipements, logiciels, etc. pour lesquels des dysfonctionnements sont observés avec les CGN.
	Quel(s) choix pour la transition : IPv6 dans un réseau *IPv4-Only*, *dual-stack* ou IPv4 dans un réseau *IPv6-only* ?	• Nécessité de la solution *dual-stack* pour permettre la transition, la durée de cette étape étant liée à la transition des applications, logiciels, etc. • Nécessité de l'IPv6 pour certains réseaux d'entreprises afin d'assurer leur croissance (dont des réseaux internes d'entreprises). • Besoin de montrer les intérêts d'IPv6 : offrir des services en *bêta-test* en IPv6, proposer un support au moins équivalent à celui en IPv4.	• Accompagner la transition grâce à des retours d'expérience d'entreprises qui ont réalisé la migration vers IPv6 (au moins en *dual-stack*) pour estimer les coûts, les bénéfices, les conditions techniques, etc. • Accélérer la transition des logiciels : la migration doit être suffisamment importante pour que les logiciels aient intérêt à déployer IPv6, ce qui implique une qualité de service suffisante d'IPv6. • Favoriser la formation et la montée en compétences : notamment pour les jeunes ingénieurs. Le *dual-stack* est une solution pour permettre la montée en compétences.
	Compatibilité IPv6 des équipements, applications, logiciels, etc.	• Plusieurs problèmes de compatibilité IPv6 identifiés : ○ Certaines applications et logiciels métiers pour les entreprises gèrent mal (ou ne gèrent pas) IPv6 ; ○ Certaines plateformes de service (notamment voix) ne sont pas compatibles avec IPv6 ; ○ Certains équipements ont des fonctionnalités ne supportant pas IPv6. • Manque de parité fonctionnelle entre v4 et v6 : ○ Plusieurs équipements compatibles (ou partiellement compatibles) ne sont pas capables de gérer IPv6 avec la même qualité qu'IPv4 ; ○ Certains logiciels sont peu performants avec IPv6. • Problèmes du Wifi en IPv6. • Besoin de renforcer l'exemplarité de l'Etat sur la transition vers IPv6.	• Identifier et recenser les différentes catégories d'applications, équipement, logiciels, etc. qui posent problème et leur maturité par rapport à IPv6, par catégorie technique. • Définir les bonnes pratiques et apporter des conseils (y compris organisationnels) pour garantir la compatibilité avec IPv6, par catégorie technique : ○ Effectuer un inventaire structuré sur la parité v4/v6 en indiquant les derniers maillons résistants ; ○ Mettre à disposition des retours d'expériences dans un guide de développement interne pour le déploiement d'IPv6 ; ○ Donner des éléments sur la gestion de projet de la transition vers IPv6 : Quoi faire en amont ? Quelle est la réglementation en vigueur ? Qui impliquer? Quand? • Encourager la prise de compte de la compatibilité IPv6 dans les marchés publics en s'inspirant du plan France numérique 2012.

Groupe de travail	Atelier	Contexte et enjeux	Axes de travail proposés par les participants
Quels enjeux de la sécurité d'IPv6 ?	**Sécurisation du réseau local (entreprise, data center)**	• Existence de plusieurs aspects de sécurisation du réseau IPv6 similaires en IPv4. Cependant, IPv6 nécessite de repenser la sécurité. • Méconnaissance des offres de sécurité IPv6 existantes. • Présence de plusieurs référentiels et RFC non mis à jour. • Faible disponibilité des compétences sur la sécurité IPv6.	• Recenser les principaux problèmes des acteurs entreprises / hébergeurs : ○ Faire de comparatifs de la sécurité v4 vs. v6. • Recenser les RFC et les formations de sécurité à jour ; • Collecter, analyser et compiler les ressources existantes du RIPE ainsi que les initiatives d'Internet Society (Deploy 360, etc.) et les mettre à jour.
	Anonymisation et vie privée	• Présence d'un biais d'identification et de localisation quand l'adresse MAC est disponible dans l'adresse IPv6. • Problèmes de *tracking* en ligne en IPv6 : ○ NAT66 : Est-ce la solution à mettre en place systématiquement ? ○ DoH : Est-ce un moyen supplémentaire de *tracker* les utilisateurs ? • Existence de solutions de *privacy* : extension de *privacy* (rfc4941), identifiants d'interface opaque (rfc7217), adresses CGA (rfc3972), etc. Laquelle privilégier ? • Manque d'information sur la façon avec laquelle les équipements obsolètes, non maîtrisables ou non maîtrisés (IoT, tablette ou mobiles dont l'OS n'est plus supporté) doivent être traités.	• Lister les différents problèmes de *privacy* générés par IPv6. • Discuter des différentes contre-mesures et des bonnes pratiques à mettre en œuvre. • Spécifier les maillons de la chaine où les efforts doivent se porter : équipement de terminaison ou intermédiaire (routeur, serveur DHCP, etc.) ? ○ Analyser les risques couverts en fonction des cas et spécifier les risques résiduels.
	Problématiques du filtrage IPv6 (box, interconnexion)	• Existence de plusieurs pratiques en termes de filtrages IPv6 et absence de consensus sur la façon avec laquelle ce filtrage doit être effectué : ○ Sécurité au niveau du périphérique pour ne pas avoir un *firewall* IPv6 vs. besoin d'un *firewall* vu la difficulté pour certains objets connectés à se protéger et rester à jour contre les failles de sécurité ; ○ Existence de mécanismes de *privacy* pour limiter la traçabilité d'une adresse IPv6. Toutefois, il ne s'agit pas d'un mécanisme de sécurité. Le fait que les IPv6 soient difficiles à trouver ou non permanentes n'est pas gage de sécurité et de protection ; ○ Volonté de certains acteurs de suivre le modèle de sécurité accompagnant le NAT en bloquant le trafic IPv6 entrant non sollicité par défaut via un *firewall*.	• Émettre des recommandations sur le filtrage IPv6, notamment les suivantes : ○ Possibilité d'augmenter le niveau de sécurité connu aujourd'hui sur IPv4 en combinant : - Une IPv6 qui change régulièrement parmi les adresses inutilisées du /64 ; - Un *firewall* qui bloque par défaut les flux entrants. ○ Activer le *firewall* correspondant uniquement sur le protocole TCP et UDP, certains souhaitant que le *firewall* ne bloque pas d'autres protocoles afin de permettre de futures innovations. ○ Permettre une désactivation simple du *firewall* avec la possibilité de le désactiver : - Entièrement ; - Périphérique par périphérique ; - Port par port ; - IPv6 par IPv6.