

L'état d'internet en France

ÉDITION

2018

3. Accélérer la transition vers IPv6



*Carence en adresses IP,
prenez en urgence
vos IPv6*



1. LA TRANSITION VERS IPv6 : UNE NÉCESSITÉ TOUJOURS PLUS PRESSANTE

L'IPv4, pour *Internet Protocol version 4*, est utilisé depuis 1983 pour permettre à internet de fonctionner : chaque terminal sur le réseau internet (ordinateur, téléphone, serveur...) possède une adresse IPv4. Le protocole IPv4 est techniquement limité à 4,3 milliards d'adresses⁴⁰, dont une grande partie est inutilisable pour l'adressage internet : non seulement 593 millions d'IPv4 sont destinées à des usages particuliers (réseaux privés...), mais surtout l'attribution a été réalisée de façon inefficace vers la fin des années 1980, aux débuts de l'internet, certaines entreprises ayant reçu des blocs de 18 millions d'IPv4 alors qu'elles n'étaient ni FAI, ni hébergeurs.

Les spécifications d'IPv6 ont été finalisées en 1998. Elles intègrent des fonctionnalités pouvant renforcer la sécurité par défaut et optimiser le routage. Surtout, IPv6 offre une quasi-infinité d'adresses : 667 millions d'IPv6 pour chaque millimètre carré de surface terrestre⁴¹ (!). Dans le contexte actuel de diversification des usages et de multiplication des objets connectés, la transition vers ce nouveau protocole apparaît comme un enjeu majeur de compétitivité et d'innovation.

Cette transition représente aussi l'évolution la plus importante depuis la création d'internet. En effet, contrairement aux évolutions logicielles qui sont rétro-compatibles avec les anciennes versions (les logiciels développés pour Windows 7 peuvent fonctionner sous Windows 10), l'IPv6 est totalement incompatible avec l'IPv4. Comme cela a été le cas le 1^{er} janvier 1983 pour la migration vers IPv4, on pourrait penser que la transition vers IPv6 aurait pu être effectuée brutalement en un seul jour (le *flag day*). Mais la taille, l'hétérogénéité et la complexité de l'internet d'aujourd'hui rendent impossible la mise en place d'un tel processus. La transition vers le protocole IPv6 se réalise donc progressivement, d'abord en parallèle d'IPv4 (phase de cohabitation), puis, quand tous les acteurs auront migré, en remplacement total d'IPv4 (phase d'extinction).

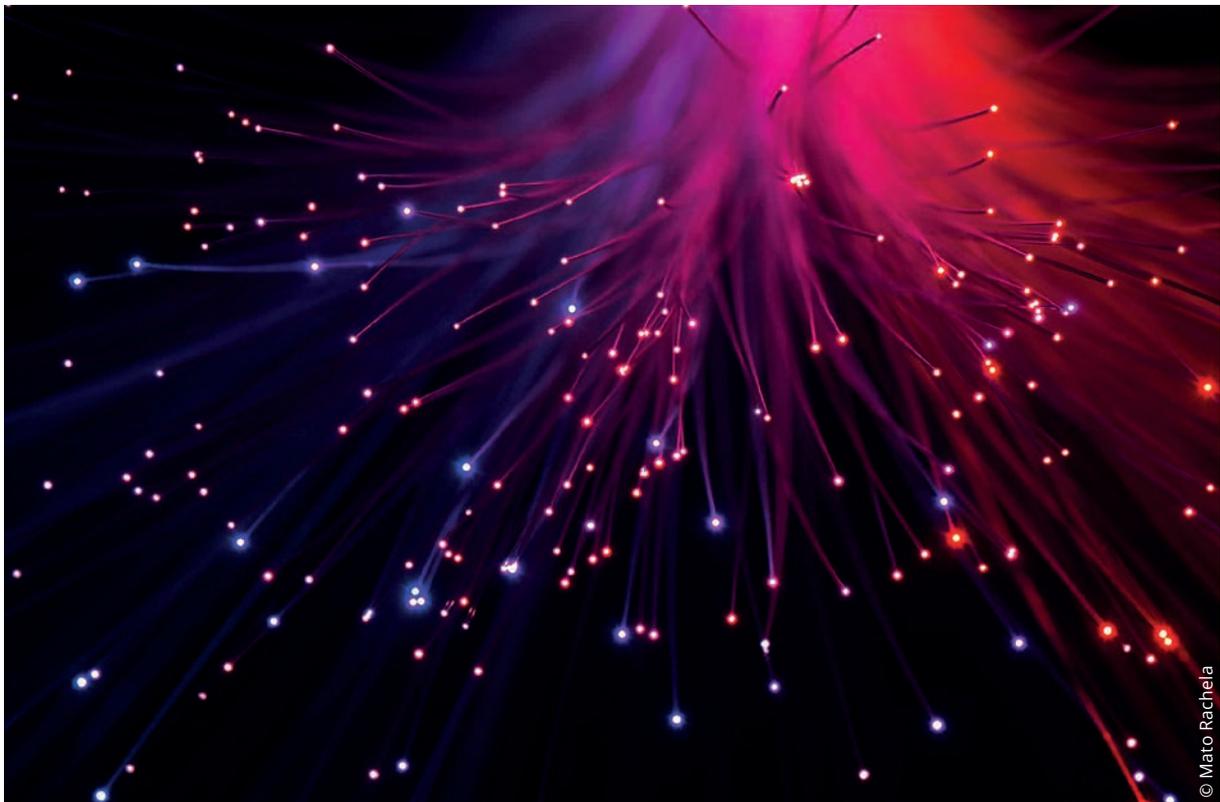
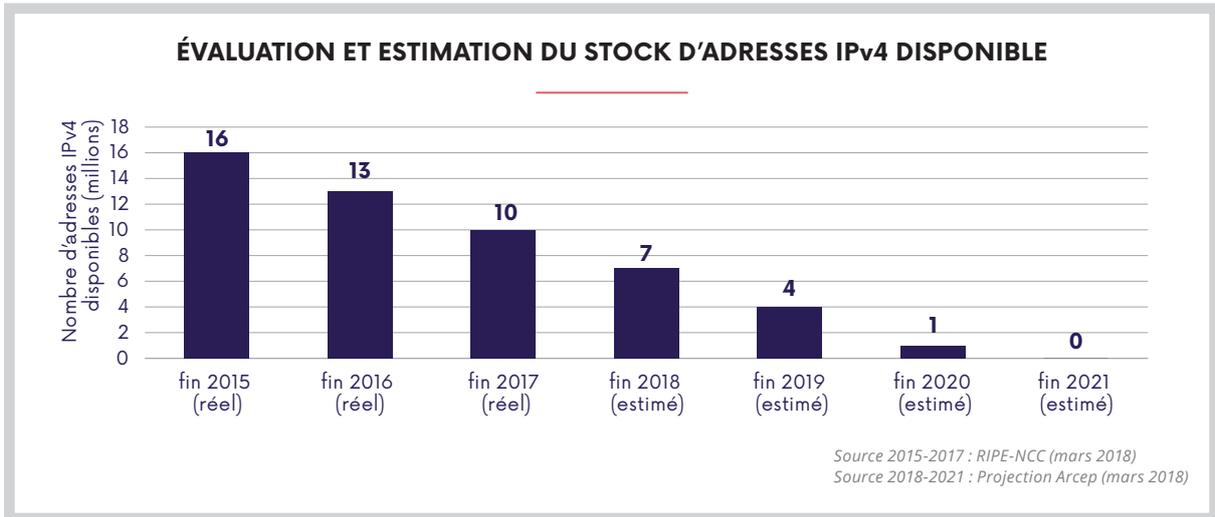
La transition vers le protocole IPv6 a démarré en 2003. Cependant, en 2018, internet est encore au début de la phase de cohabitation. Comme expliqué, IPv4 reste nécessaire tant que toute la chaîne technique n'aura pas migré entièrement vers IPv6. Dans le cas contraire, un site qui ne serait pas en mesure d'avoir une adresse IPv4 ne sera pas accessible aux clients des FAI qui ne proposent pas d'IPv6 ; l'IPv4 reste nécessaire pour communiquer avec l'internet IPv4. Or la date de fin de

⁴⁰ Les adresses IPv4 sont codées sur 32 bits. Au maximum 2^{32} , soit 4 294 967 296 adresses peuvent donc être attribuées simultanément en théorie.

⁴¹ Les adresses IPv6 sont codées sur 128 bits. Au maximum 2^{128} (soit environ $3,4 \times 10^{39}$) adresses peuvent donc être attribuées simultanément en théorie.

disponibilité de l'IPv4 en Europe approche. Estimée à fin 2021, elle entraîne d'ores et déjà une augmentation significative du prix des adresses IPv4, devenues les ressources rares de l'internet du XXI^e siècle. Ce prix élevé

érige une barrière à l'entrée significative à l'encontre des nouveaux acteurs du marché et augmente le risque de voir se développer un internet scindé en deux, IPv4 d'un côté et IPv6 de l'autre.



Pour répondre à la pénurie des adresses IPv4, certains mécanismes de substitution ont été mis en place par les FAI. Les équipements *Carrier-grade NAT* (CGN) permettent par exemple de partager une adresse IPv4 entre plusieurs clients. Cependant, ils entraînent aussi avec eux plusieurs effets négatifs qui rendent complexe le maintien d'IPv4 et quasi impossible un certain nombre usages comme le pair-à-pair⁴², l'accès à distance à des fichiers partagés

sur un NAS⁴³ ou à des systèmes de contrôle de maison connectée, certains jeux en réseau...

L'Arcep a remis au Gouvernement en juin 2016 un rapport élaboré avec le concours de l'Afnic comportant plusieurs leviers d'actions de nature à accompagner et à accélérer la transition vers IPv6. Elles sont exposées dans le schéma ci-après.



⁴² Ou *peer-to-peer*.

⁴³ *Network Attached Storage*, un serveur de stockage en réseau.



LIMITATION DE L'USAGE DES CGN ET TRANSITION VERS IPv6 : L'EXEMPLE BELGE

Gregory MOUNIER, Centre Européen de lutte contre la cybercriminalité (EC3), **EUROPOL**⁴⁴



Commissaire Adeline CHAMPAGNAT, Conseiller à la délégation en charge de la lutte contre les cybermenaces, **DIRECTION CENTRALE DE LA POLICE JUDICIAIRE**



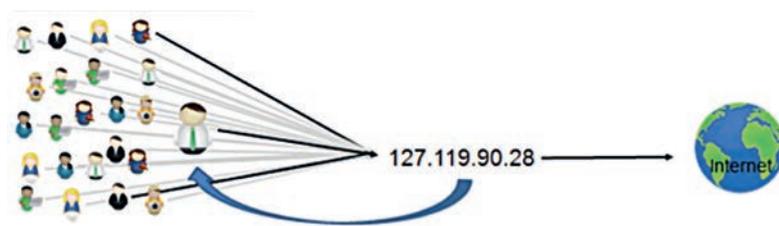
Le CGN est un mécanisme qui permet de traduire une adresse IP interne privée en une adresse externe publique visible sur internet. Ainsi, les FAI peuvent partager une adresse IP publique entre plusieurs milliers d'utilisateurs simultanément et ainsi faire face à la pénurie d'adresse IPv4. Outre que cette pratique, qui concerne plus de 90 % des opérateurs mobiles, pose un certain nombre de problèmes techniques, elle a aussi des conséquences négatives importantes en termes de sécurité publique. En effet, lorsque des services d'enquêtes poursuivent des investigations sur un délit ou un crime facilité par l'internet, l'une des premières traces digitales disponibles est une

tification d'un abonné prendra beaucoup de temps : l'opérateur peut fournir aux enquêteurs une liste de tous les abonnés qui utilisaient la même adresse IP, mais cette liste peut comprendre plusieurs milliers de noms. La non-conformité des opérateurs avec la loi porte ainsi atteinte à la vie privée de nombreuses personnes qui pourraient être citées en procédure alors même que les enquêteurs ne s'intéressent qu'à un seul suspect.

Dans ce contexte, seule une transition quasi-totale à l'IPv6 peut constituer une réponse pérenne à ce problème. Les techniques de CGN étaient censées être des solutions temporaires en attendant que la

deux rapports en 2017 critiquant l'utilisation abusive du CGN par les opérateurs et dénonçant les effets négatifs de ces pratiques sur la sécurité des citoyens européens.

Pour pallier l'absence de stockage du port source par les plateformes internet, la Belgique a invité les FAI basés sur son territoire à signer en 2012 un code de bonne conduite volontaire dans lequel ils s'engagent à réduire le ratio d'abonnés par adresse IP globale à 16/1. Après cinq années de pratique, les services répressifs belges reçoivent en moyenne seulement quatre abonnés utilisant la même adresse IP, ce qui réduit grandement l'impact négatif du CGN sur les enquêtes criminelles.



adresse IP. Les FAI sont alors légalement obligés de fournir aux enquêteurs l'identité de l'abonné utilisant cette adresse. Lorsque celle-ci est derrière un CGN, les FAI ont techniquement besoin qu'on leur fournisse non seulement la date, l'heure et les adresses IP de connexion et de destination, mais aussi le numéro de port source. Malheureusement, les fournisseurs de service ne conservent que rarement le port source. Ainsi, le CGN rend les enquêtes plus difficiles car l'iden-

transition à l'IPv6 atteint un seuil critique et que l'ensemble du trafic internet passe en IPv6. Malheureusement, force est de constater que depuis les années 2000, la transition est très lente. On peut légitimement se demander si la technologie CGN n'est pas graduellement devenue, pour certains opérateurs, un substitut à l'IPv6, une manière de prolonger indéfiniment la durée de vie de l'IPv4 et d'éviter d'investir dans la modernisation des réseaux. Le Parlement européen a d'ailleurs adopté

Autre conséquence inattendue, la Belgique a le plus fort taux d'adoption d'IPv6 au monde avec plus de 52 % d'utilisateurs en IPv6, et cela depuis 2013, juste après l'adoption du code de bonne conduite. Il est donc permis de penser que la décision de limiter volontairement le nombre d'abonnés par adresse IP publique, a incité les opérateurs basés en Belgique à n'utiliser les CGN qu'en cas de dernier recours, mais également à investir de manière plus importante dans la transition IPv6.

Les institutions européennes ont décidé de s'inspirer de l'exemple belge en invitant fin 2017⁴⁵ les états européens à proposer l'adoption de codes de conduite aux opérateurs pour limiter l'utilisation des CGN et le nombre d'abonnés par adresse IP publique. Cette mesure part du principe que la technologie CGN freine l'adoption de l'IPv6.

⁴⁴ Europol et son Centre Européen de lutte contre la Cybercriminalité (EC3) collaborent avec les autorités compétentes des États membres de l'Union européenne (UE), les institutions européennes et RIPE NCC pour accélérer la transition vers l'IPv6.

⁴⁵ <http://data.consilium.europa.eu/doc/document/ST-15748-2017-INIT/en/pdf>, p. 14 et 15.

2. L'OBSERVATOIRE ARCEP OU LE CHOC DE TRANSPARENCE AU SERVICE D'UNE ACCÉLÉRATION DE LA TRANSITION

Dans le cadre des actions préconisées dans son rapport de juin 2016, l'Arcep a mis en place depuis décembre 2016 un observatoire de la transition vers IPv6 annuel, qui vise à mieux informer l'utilisateur sur le sujet dans une optique de régulation par la data. En effet, cet observatoire, dont les résultats sont présentés ci-dessous, dresse l'état des lieux de la transition en France ainsi que les prévisions de déploiement des FAI de plus de un million d'abonnés⁴⁶ à un an et à trois ans. Sa prochaine édition sera à nouveau enrichie (cf. section 2.2).

2.1. Les résultats à fin 2017

Le 18 décembre dernier, l'Arcep a publié l'édition 2017 de son observatoire de la transition vers IPv6 en France. Cette édition est marquée par deux enrichissements majeurs :

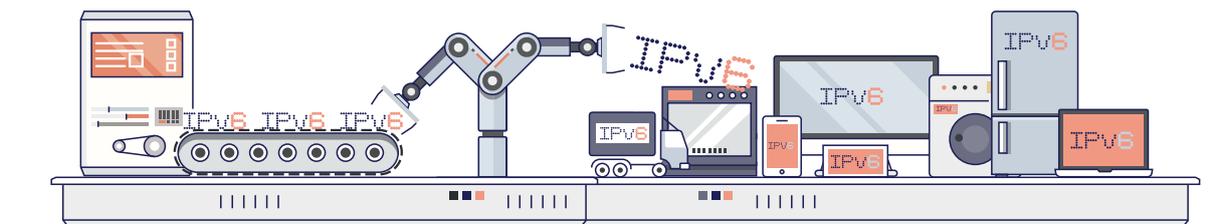
- outre les données produites et mises à disposition par des tiers (Cisco, Google, ANSSI, World IPv6 Launch), l'observatoire est dorénavant enrichi de données que l'Arcep a recueillies directement auprès des principaux opérateurs en France ;
- l'état des lieux actuel et les évolutions passées de l'adoption du protocole IPv6 sont maintenant complétés par les prévisions de déploiement à court et moyen terme anticipées par les opérateurs.

L'observatoire expose trois types d'informations liées à IPv6 : le taux de clients compatibles (ou *IPv6-ready*), le taux de clients activés et le taux d'utilisation d'IPv6. Le schéma ci-après indique l'endroit du réseau où ces taux sont mesurés ou calculés. En cas de doute sur la signification exacte de ces indicateurs, le lecteur pourra se référer au schéma explicatif présenté dans l'observatoire Arcep⁴⁷.

Les résultats confirment la progression du taux d'utilisation d'IPv6 en France, qui atteint 20,4 % fin 2017. Free est l'opérateur le plus avancé dans la transition, avec 35 % de taux d'utilisation à fin 2017 (contre 24 % fin 2016). L'évolution la plus forte concerne néanmoins Orange, dont le taux d'utilisation a doublé en un an, passant de 16 % fin 2016 à 33 % fin 2017.

Concernant les plans de transition au niveau du réseau fixe des différents opérateurs en France :

- fin 2018 : Free envisage d'activer IPv6 sur l'intégralité de son parc. Orange projette d'activer IPv6 pour 50 % à 60 % de clients d'ici un an. Bouygues Telecom envisage de généraliser la migration pour obtenir 25 % à 35 % de clients activés. SFR projette quant à lui que moins de 10 % de ses clients seront activés à cet horizon ;
- fin 2020 : Orange envisage d'atteindre 70 % à 80 % de clients activés en IPv6. Bouygues Telecom projette d'activer 75 à 85 % de ses clients. SFR, de son côté, envisage d'avoir atteint entre 10 % et 20 % de clients activés.



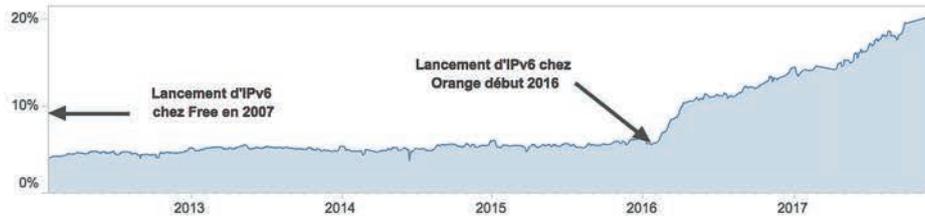
⁴⁶ Ou plus précisément, les FAI de plus d'un million d'abonnés *gérant leur plan d'adressage IP*.

⁴⁷ <https://www.arcep.fr/index.php?id=13726>

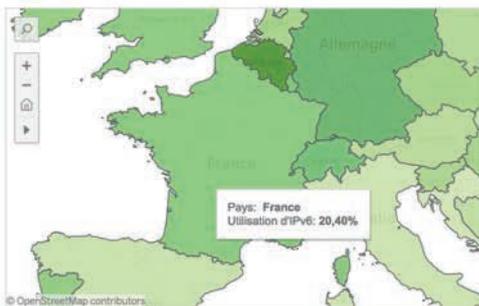
OBSERVATOIRE DE LA TRANSITION VERS IPv6 EN FRANCE

Au 18 décembre 2017

Evolution du taux d'utilisation d'IPv6 en France, tel qu'observé par Google
Source : Cisco - 6Lab



Etat de la transition IPv6 dans le monde au 07/12/2017
Source: Cisco - 6Lab



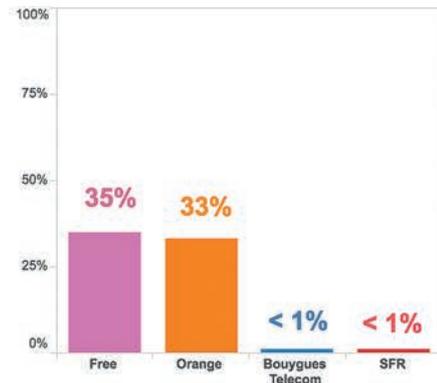
Choix de l'indicateur
Utilisation d'IPv6

Utilisation d'IPv6 :
Taux d'utilisation d'IPv6, tel qu'observé par Google.

Contenus IPv6 :
Taux de sites web accessibles en IPv6 parmi les sites web les plus visités dans chaque pays.

Intermédiaires IPv6 :
Taux d'intermédiaires techniques (par ex. transitaires) empruntés utilisant IPv6, pour chaque pays.

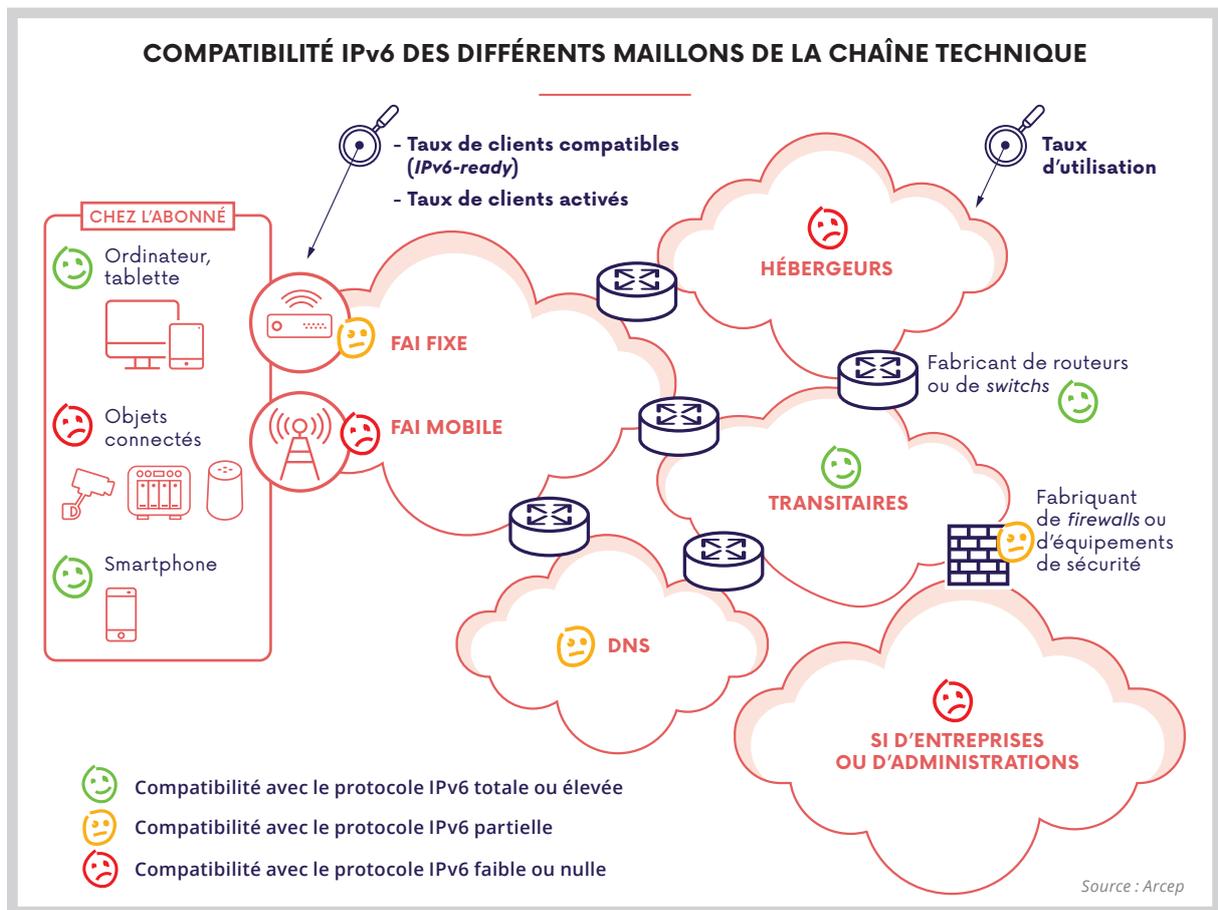
Taux d'utilisation d'IPv6 sur les principaux réseaux en France au 08/11/2017
Source: World IPv6 Launch / Apnic



Prévisions des taux de clients du réseau fixe activés en IPv6 pour les principaux opérateurs en France*
Source: Données recueillies par l'Arcep auprès des opérateurs



* Projections, chiffres susceptibles d'évoluer.



2.2. Les enrichissements à venir

Début 2018, la décision de l'Arcep n° 2018-0268 en date du 15 mars 2018 relative à la mise en place d'enquêtes dans le secteur des communications électroniques a été complétée dans le but :

- d'établir un questionnaire qui clarifie davantage la différence entre les clients *IPv6-ready* et les clients activés en IPv6, et spécifie les chiffres par technologies d'accès et par nature du réseau ;
- de faire évoluer le périmètre de la collecte pour inclure, au-delà des opérateurs gérant leur plan d'adressage IP et ayant plus d'un million d'abonnés, les hébergeurs et les opérateurs gérant leur plan d'adressage IP et possédant entre 10 000 et un million d'abonnés qui auront accepté de contribuer à l'enrichissement de l'observatoire.

Le rôle des hébergeurs est en effet primordial dans la transition. Afin d'assurer un fonctionnement de bout en bout du protocole IPv6, celle-ci doit concerner simultanément tous les maillons de la chaîne technique sur internet. Or comme l'indique le schéma ci-dessus, les hébergeurs représentent encore l'un des principaux goulots d'étranglement.

En parallèle, d'autres données viendront enrichir les futures publications de l'observatoire. Dorénavant, l'Arcep suivra notamment le pourcentage des sites du top 50⁴⁸ qui sont compatibles IPv6. En deux ans, de mars 2016 à mars 2018, ce pourcentage est passé de 22 % à 34 %⁴⁹. À titre de comparaison, le pourcentage de sites du top 50 qui sont accessibles en https est passé de 22 % à 76 % durant la même période⁵⁰ : une augmentation bien supérieure qui peut être entre autres attribuée à la pression mise sur les sites par plusieurs acteurs (les moteurs de recherche qui dégradent le classement des sites http, les navigateurs qui indiquent des alertes de sécurité sur un site en http, etc.).

⁴⁸ Source listant les sites du top 50 : classement Médiamétrie.

⁴⁹ Selon des tests effectués par les services de l'Arcep en mars 2016 et mars 2018.

⁵⁰ Selon des tests également effectués par les services de l'Arcep en mars 2016 et mars 2018.

LA VISION D'UN HÉBERGEUR



Jérémy MARTIN,
Directeur Technique,
[FIRSTHEBERG.COM/TECH CRÉA SOLUTIONS](https://firstheberg.com/tech)

[FIRSTHEBERG.COM](https://firstheberg.com)

Le 17 avril 2018, le RIPE NCC, l'organisme qui alloue les IP pour l'Europe, a alloué sa dernière plage IPv4 neuve. Le RIPE alloue maintenant les IPv4 qui lui ont été retournées, mais la pénurie totale d'IPv4 devrait arriver début 2021. Avec une demande croissante pour un nombre d'IPv4 fixes, le coût de location d'une IPv4 va doubler d'ici à deux ans.

À l'heure actuelle, FirstHeberg propose une adresse IPv4 et une plage IPv6 dédiée pour chaque serveur loué. D'ici 2020, FirstHeberg proposera une offre plus abordable, sans IPv4 dédiée. En effet, FirstHeberg considère qu'à partir de 2020, pour des raisons financières, un petit site web pourrait être contraint de n'avoir qu'une adresse IPv6. Ainsi, si toutes les boxes ne sont pas activées en IPv6 d'ici là ou si de nombreuses entreprises continuent de refuser de migrer leur SI en IPv6, internet sera malheureusement scindé en

deux : ces petits sites web ne seront en effet pas accessibles par un client qui n'a pas d'adresse IPv6. Une option « adresse IPv4 dédiée » payante sera donc toujours proposée par FirstHeberg, au moins jusqu'en 2030. Elle sera particulièrement nécessaire pour ceux qui ont absolument besoin d'un site visible par les clients IPv6 et les clients IPv4.

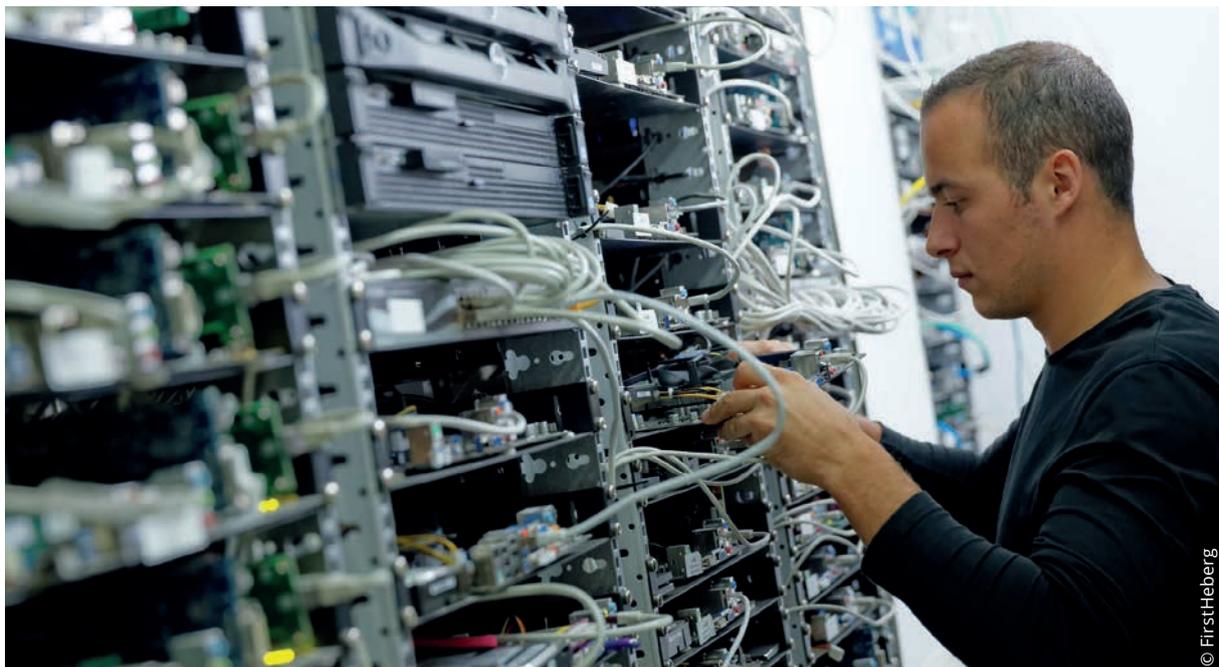
Il est clair que l'implémentation de l'IPv6 doit être portée par une vision politique,



« DANS LA TRANSITION
VERS IPv6,
LA CONTRAINTE POLITIQUE
EST NÉCESSAIRE. »

afin d'inciter très concrètement les acteurs à implémenter ce protocole et à l'utiliser (grâce éventuellement à des contreparties financières).

Par ailleurs, une date de mise à disposition obligatoire et légale de l'IPv6 pourrait faire son effet, sous réserve que l'État accompagne la transition des petites structures. Une échéance à l'horizon 2023 est tout à fait envisageable pour une couverture à 100 %. L'Europe pourrait aider en fixant dès aujourd'hui une date éloignée où les opérateurs devront éteindre l'IPv4, ce qui forcerait la migration des derniers récalcitrants. En effet, dans la transition vers IPv6, la contrainte politique est nécessaire pour éviter les défaillances de TPE et PME, notamment celles dont le *business model* est basé sur la fourniture de prestations réseaux, par manque de stock d'adresse IPv4.



© FirstHeberg



L'ENSEIGNEMENT D'IPv6, LE LEVIER FONDAMENTAL DE LA TRANSITION



Bruno STEVANT,
Enseignant-chercheur et responsable des activités
formation à l'association G6, **INSTITUT MINES-TÉLÉCOM**



Le déploiement d'IPv6 se généralise chez les opérateurs et dans les réseaux d'entreprise. 20 % du trafic internet est aujourd'hui en IPv6. Afin d'être opérationnels, les ingénieurs réseaux nouvellement diplômés doivent être compétents dans la mise en œuvre du nouveau protocole IP ainsi que dans la gestion d'un réseau double pile IPv4/IPv6. Les formations en réseau dans les universités et écoles d'ingénieurs doivent donc couvrir les aspects théoriques d'IPv6 mais aussi et surtout permettre aux étudiants de pratiquer IPv6. Or, aujourd'hui encore, trop peu d'universités offrent de l'IPv6 sur leur réseau et encore moins une formation adaptée au nouveau protocole.

Au sein de l'IMT, IPv6 était un sujet de recherche depuis plus de 15 ans. À mesure que cette technologie est passée de la R&D à la production, nous

avons fait le choix d'intégrer IPv6 dans nos enseignements de formation initiale et continue. Grâce au déploiement d'IPv6 sur les réseaux de l'IMT, des salles de travaux pratiques jusqu'aux réseaux des résidences étudiantes, nos élèves utilisent le nouveau protocole au quotidien. Forte de cette expérience, et en coopération

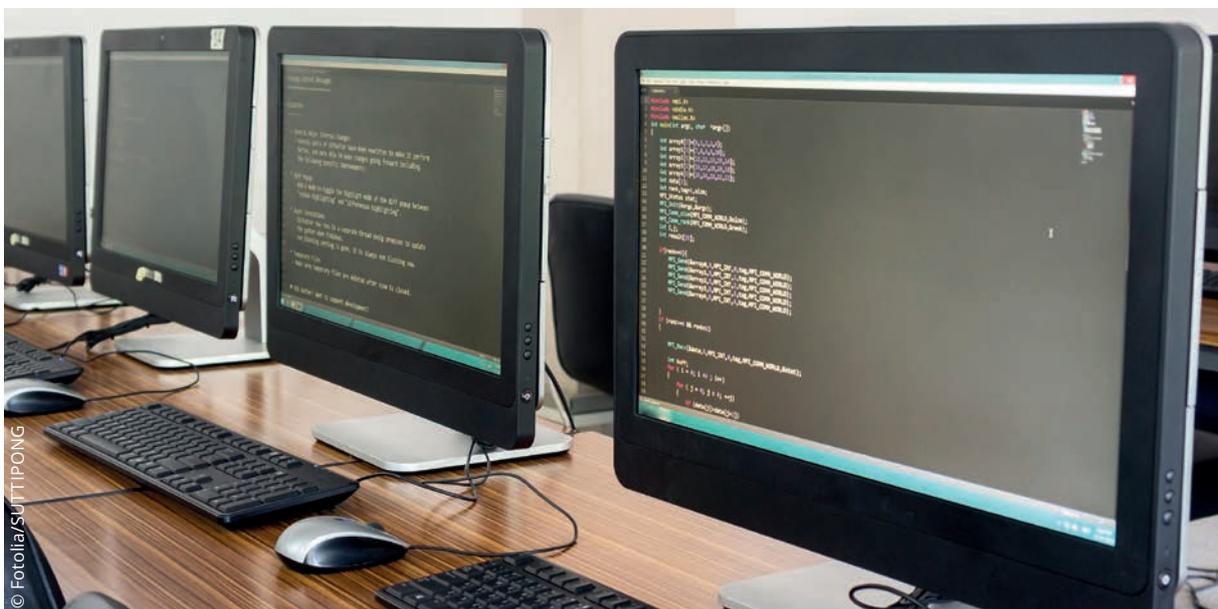
avec l'Association G6 (Association pour la promotion et le développement d'IPv6) et l'université de la Réunion, l'IMT a lancé en 2015 sur la plateforme France Université Numérique le premier MOOC (cours en ligne massivement ouvert) sur IPv6.

Après trois sessions, le MOOC Objectif IPv6 totalise plus de 15 000 inscrits et a délivré environ 1 000 attestations de participation. Ce succès montre l'intérêt pour une formation de qualité sur IPv6.

Il est donc important que les formations autour des réseaux et de l'internet, du niveau technicien au niveau ingénieur, évoluent pour intégrer les aspects théoriques et pratiques du protocole IPv6 et que les formateurs l'enseignent non pas comme une technologie du futur mais comme le standard actuel des réseaux.



« AUJOURD'HUI ENCORE,
TROP PEU D'UNIVERSITÉS
OFFRENT [...] UNE FORMATION
ADAPTÉE AU NOUVEAU
PROTOCOLE. »



3. LA FÉDÉRATION DE L'ÉCOSYSTÈME AUTOUR D'UN ATELIER IP♥6

Dans le cadre de la mise en place d'espaces d'échanges visant à fédérer la communauté, l'Arcep a décidé d'organiser, en partenariat avec l'Internet Society France (ISOC), un atelier de travail dédié au partage d'expériences individuelles et de bonnes pratiques utiles à la transition vers IPv6.

Celui-ci s'inscrira dans la dynamique du forum de la gouvernance d'internet (ou *Internet Governance Forum* – IGF) de l'ISOC, organisé autour d'un événement principal⁵¹ et de plusieurs ateliers satellites (RGPD, cybersécurité, IPv6, etc.). L'atelier « IP♥6 », qui se tiendra le mercredi 10 octobre dans les locaux de l'Arcep, donnera lieu à des groupes de travail multi parties prenantes (FAI, hébergeurs, organismes de formation, organismes publics, etc.) qui échangeront sur des thèmes concrets liés à la transition d'IPv4 vers IPv6, notamment :

- l'enseignement d'IPv6 : comment s'assurer que la majorité des cours et exercices réalisés par les étudiants concernent IPv6, et non IPv4 ? Comment diffuser des contenus utiles aux ingénieurs et techniciens réseaux afin qu'ils puissent se former à IPv6 ? ;

- l'exemplarité de l'État : quels sont les principaux points de blocage qui entravent le déploiement d'IPv6 au sein des services en ligne de l'État ? Comment les surmonter ? ;
- la préparation de la fin d'IPv4 : comment donner de la visibilité aux acteurs concernant la fin de l'utilisation d'IPv4 ? Quelle solution pour inciter les retardataires à démarrer au plus vite leur transition vers IPv6 ?

Les inscriptions à l'atelier sont d'ores et déjà ouvertes sur le site internet de l'ISOC⁵². L'Arcep encourage vivement tous les acteurs de l'écosystème à participer, quel que soit le stade de leur avancement dans la transition vers IPv6. Les participants qui le souhaitent pourront profiter de cet événement à forte visibilité pour annoncer leurs avancées particulières, passées ou à venir, en matière de transition vers IPv6.



⁵¹ L'événement principal de l'IGF aura lieu le 5 juillet 2018, de 9 h à 20 h, à l'Université Paris Descartes. Inscriptions sur <https://www.isoc.fr>.
⁵² <https://www.weezevent.com/ateliers-de-l-avenir-numerique-internet-6>

Lexique

Les définitions énoncées ci-dessous sont uniquement utilisées dans le cadre du présent rapport pour en faciliter sa lecture.

Agent dans la box : outil de mesure de QoS et/ou QoE installé directement dans la box des FAI.

Android : système d'exploitation mobile développé par Google.

ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) : service gouvernemental français à compétence nationale chargé de la sécurité et de la défense des systèmes d'information.

API (Application Programming Interface) : interface de programmation applicative qui permet à deux systèmes de s'interopérer et de communiquer sans qu'ils aient été conçus initialement dans cet objectif. Plus précisément, ensemble normalisé de classes, de méthodes ou de fonctions à travers lequel un logiciel offre des services à d'autres logiciels.

ARN (Autorité de Régulation Nationale) : l'organisme ou les organismes chargés par un État membre du BEREC de la régulation des communications électroniques.

BEREC (Body of European Regulators for Electronic Communications) : instance européenne indépendante créée par le Conseil de l'Union européenne et le Parlement européen qui rassemble les régulateurs des communications électroniques des vingt-huit États membres de l'Union européenne.

Câble ou « réseaux câblés » : réseaux de communications électroniques constitués d'un cœur de réseau en fibre optique et d'une terminaison en câble coaxial. Historiquement conçus pour diffuser des services de télévision, ces réseaux permettent depuis plusieurs années d'offrir également des services de téléphonie et d'accès à l'internet grâce à l'utilisation de la bande passante non mobilisée par les flux de télévision.

CDN (Content Delivery Network) : réseau de diffusion de contenu sur internet.

CDN interne : CDN situé directement dans le réseau des FAI.

CGN (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.

[Adaptateurs] CPL (Courants Porteurs en Ligne) : équipement qui permet de transporter internet par le réseau électrique à l'intérieur d'une habitation à la place d'un câble Ethernet ou du Wi-Fi.

Cross-traffic : dans le chapitre 1, le *cross-traffic* fait référence au trafic généré pendant un test de QoS et/ou QoE par une autre application que celle réalisant le test, sur le même terminal ou sur un autre terminal connecté à la même box. Le *cross-traffic* diminue le débit disponible pour le test.

Crowdsourcing : dans le chapitre 1, les outils de *crowdsourcing* font référence aux dispositifs qui centralisent des mesures de QoS et/ou QoE réalisées par des utilisateurs réels.

Débit : quantité de données numériques transmises par unité de temps. Le débit s'exprime souvent en bits par seconde (bit/s) et ses multiples Mbit/s, Gbit/s, Tbit/s, etc. Il convient de distinguer la vitesse à laquelle les données peuvent être :

- envoyées depuis un ordinateur, un téléphone ou tout autre équipement terminal connecté à l'internet, comme pendant l'envoi de photographies vers un site d'impression en ligne : on parle alors de débit montant ;
- reçues depuis un équipement terminal connecté à l'internet, comme lors du visionnage d'une vidéo en ligne ou du chargement d'une page web : on parle de débit descendant.

DGCCRF (Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes) : service de l'administration française qui a pour objet de veiller au bon fonctionnement des marchés, au bénéfice des consommateurs et des entreprises.

DNS (Domain Name System): mécanisme de traduction des noms de domaine internet en adresses IP.

DPI (Deep Packet Inspection): équipement d'infrastructure de réseau consistant à analyser le contenu des paquets IP afin de les prioriser, les filtrer ou en tirer des statistiques.

Ethernet (câble): nom usuel du connecteur RJ45 supportant le protocole de communication de paquets Ethernet.

FAI: Fournisseur d'Accès à Internet.

FCA (Fournisseurs de Contenu et d'Applications): fournisseurs du contenu (pages web, blogs, vidéos) et/ou des applications (moteurs de recherche, applications VoIP) sur internet.

FCC (Federal Communications Commission): agence indépendante du gouvernement des États-Unis chargée de réguler les télécommunications ainsi que les contenus des émissions de radio et de télévision.

FTC (Federal Trade Commission): agence indépendante du gouvernement des États-Unis chargée de l'application du droit de la consommation et du contrôle des pratiques commerciales anticoncurrentielles.

FttH ou « réseaux fibrés » (Fiber to the Home): réseau de communications électroniques à très haut débit en fibre optique jusqu'à l'abonné, c'est-à-dire pour lequel la fibre optique se termine dans le logement ou le local de l'abonné.

HTTP (Hypertext Transfer Protocol): protocole de communication client-serveur développé pour le World Wide Web.

HTTPS (HTTP Secured): protocole HTTP sécurisée par l'usage des protocoles SSL ou TLS.

ICMP: protocole utilisé pour véhiculer des messages de contrôle et d'erreur. Il peut servir à mesurer la latence *via* la commande « ping » intégrée à tous les systèmes d'exploitation.

INC (Institut National de la Consommation): établissement public à caractère industriel et commercial placé sous la tutelle du ministre chargé de la consommation au service des consommateurs et des associations qui les représentent.

iOS: système d'exploitation mobile développé par Apple pour ses appareils mobiles.

IP (Internet Protocol): protocole de communication qui permet un service d'adressage unique pour l'ensemble des terminaux utilisés sur internet. IPv4 (IP version 4) est le protocole utilisé depuis 1983. IPv6 (IP version 6) est son successeur.

IPv6-Ready: qui est compatible avec le protocole IPv6, mais sur lequel IPv6 n'est pas nécessairement activé par défaut.

ISOC (Internet Society): association de droit américain à vocation internationale visant à promouvoir et coordonner le développement des réseaux informatiques dans le monde.

IXP (Internet Exchange Point) ou GIX (Global Internet Exchange): infrastructure physique permettant aux FAI et FCA qui y sont connectés d'échanger du trafic internet entre leurs réseaux grâce à des accords de *peering* public.

LAN (Local Area Network): réseau local. Pour un particulier, il s'agit du réseau constitué de la box du FAI et de tous les périphériques qui y sont connectés en Ethernet ou en Wi-Fi.

Latence: délai nécessaire à un paquet de données pour passer de la source à la destination à travers un réseau. La latence est exprimée en millisecondes.

Mesure de débit en *monothread* : mesure du débit avec une unique connexion TCP.

Mesure de débit en *multithread* : mesure du débit avec plusieurs connexions TCP en parallèle.

NAS (*Network Attached Storage*) : serveur de fichiers autonome, relié à un réseau dont la principale fonction est le stockage de données.

ONT (*Optical Network Termination*) : équipement du réseau FttH Gpon situé chez le client. Un ONT peut-être externe à la box (cas le plus fréquent) ou intégré dans une cage SFP.

OS (*Operating System*) : système d'exploitation. Logiciel qui permet de faire fonctionner un périphérique, comme Windows, Mac OS, Linux, Android ou iOS.

OTT (*over-the-top*) : qualifie les services de communications électroniques fournis par des FCA sur internet

Peering : désigne l'échange de trafic internet entre deux pairs (ou *peers*). Un lien de *peering* peut être gratuit ou payant (pour celui qui envoie le plus de trafic vers son pair). Le *peering* peut par ailleurs être public, lorsqu'il est réalisé à un IXP (*Internet Exchange Point*), ou privé, lorsqu'il s'effectue dans le cadre d'un PNI (*Private Network Interconnect*), c'est-à-dire d'une interconnexion directe entre deux opérateurs.

Politique de *peering* (ou *peering policy*) : désigne un document de référence, généralement public, contenant les stratégies des opérateurs en matière d'interconnexion.

QoE (*Qualité d'Expérience*) : dans le cadre du chapitre 1, qualité de l'expérience de l'utilisateur sur internet lors d'usages donnés. Elle est mesurée par des indicateurs dits « d'usage » comme le temps de téléchargement de pages web ou la qualité de la lecture de vidéo en *streaming*.

QoS (*Qualité de Service*) : dans le cadre du chapitre 1, qualité de service du réseau internet mesurée par des indicateurs dits « techniques » comme le débit montant ou descendant, la latence ou la gigue. Il arrive souvent que le terme QoS soit utilisé pour désigner à la fois la qualité de service au sens de la présente définition et la qualité d'expérience.

QUIC (*Quick UDP Internet Connection*) : QUIC est un protocole expérimental transportant les données sur de l'UDP, développé et utilisé par Google dans le but de diminuer le temps de chargement des pages web.

Formation RDPI (*Formation de Règlement des Différends, de Poursuite et d'Instruction de l'Arcep*) : formation de l'Arcep composée de quatre membres du collège de l'Autorité dont le président qui statue sur les décisions en matière d'enquête prises sur le fondement des articles L. 5-9 et L. 32-4 du code des postes et des communications électroniques, sur les décisions de règlement des différends ainsi que sur les décisions ayant trait à l'exercice des poursuites dans le cadre de la procédure de sanction (ouverture, mise en demeure, notification des griefs ou non-lieu à poursuivre, mesures conservatoires).

SI (*Système d'Information*) : ensemble organisé de ressources qui permet de collecter, stocker, traiter et diffuser de l'information.

Slow start (*démarrage lent*) : algorithme du protocole TCP qui consiste à augmenter progressivement le débit au cours du téléchargement.

Sonde matérielle : outil de mesure de QoS et/ou QoE qui prend souvent la forme d'un boîtier à connecter à la box du FAI *via* un câble Ethernet. La sonde matérielle teste généralement de manière passive et automatique la ligne internet.

TCP (*Transmission Control Protocol*) : protocole de transport fiable, en mode connecté, développé en 1973. En 2018, la majeure partie du trafic sur internet utilise le protocole TCP, au-dessus du protocole IPv4 ou IPv6.

Testeur web : outil de mesure de QoS et/ou QoE accessible depuis un site internet.

Tier 1 : réseau capable de joindre tous les réseaux internet par une interconnexion directe (*peering*) sans avoir de transitaire. En 2018, 18 opérateurs sont *Tier 1* : AT&T, CenturyLink/Level 3, Cogent Communications, Deutsche Telekom AG, Global Telecom & Technology, Hurricane Electric, KPN International, Liberty Global, NTT Communications, Orange, PCCW Global, Sprint, Tata Communications, Telecom Italia Sparkle, Telxius/Telefónica, Telia Carrier, Verizon Enterprise Solutions, Zayo Group.

TRAI (Telecom Regulatory Authority of India) : l'Autorité de régulation des communications électroniques en Inde.

Transitaire : opérateur de transit.

Transit : bande passante vendue par un opérateur à un opérateur client, qui permet d'accéder à la totalité de l'internet dans le cadre d'un service contractuel et payant.

UDP (User Datagram Protocol) : protocole de transport simple, sans connexion (aucune communication préalable n'est requise) qui permet de transmettre rapidement de petites quantités de données. Le protocole UDP s'utilise au-dessus du protocole IPv4 ou IPv6.

UFC-Que choisir (Union Fédérale des Consommateurs) : association ayant pour objet d'informer, de conseiller et de défendre les consommateurs.

VPN (Virtual Private Network) : connexion inter-réseau permettant de relier deux réseaux locaux différents par un protocole de tunnel.

WAN (Wide Area Network) : dans le chapitre 1, le réseau WAN désigne le réseau internet par opposition au réseau LAN.

xDSL (Digital Subscriber Line) : réseau de télécommunications physique à haut débit utilisant la paire de cuivre du téléphone. La norme ADSL2+ et VDSL2 sont les normes xDSL les plus utilisées en France.

Zero-rating : pratique tarifaire consistant à ne pas décompter du forfait data du client final le volume de données consommé par une ou plusieurs applications particulières.

4G box : box qui offre une connexion internet haut débit *via* le réseau 4G.

802.11ac : standard de transmission sans fil de la famille Wi-Fi, normalisé par l'*Institute of Electrical and Electronics Engineers* (IEEE) en 2014. En 2018, 802.11ac est le Wi-Fi normalisé le plus performant.

