TOME 3

L'état d'internet en France

RAPPORT D'ACTIVITÉ 2019

arcep

République française - juin 2019

L'état d'internet en France

RAPPORT D'ACTIVITÉ

arcep

SOMMAIRE

ASSURER LE BON FONCTIONNEMENT D'INTERNET 08

1. AMÉLIORER LA MESURE DE LA QUALITÉ DE SERVICE 10

1. Les biais potentiels de la mesure de la qualité de service 10
2. Les travaux amorcés en 2018 sur la caractérisation de l'environnement utilisateur 11
3. Vers des méthodologies de mesures plus transparentes et robustes 12
4. L'importance du choix de la mire de test 17
5. Comment maximiser la fiabilité de son test de qualité de service ? 20
6. Le suivi par l'Arcep de la qualité de l'internet mobile 20

2. SUPERVISER L'INTERCONNEXION DE DONNÉES 23

1. Évolution de l'architecture internet 23
2. État de l'interconnexion en France 27

3. ACCÉLÉRER LA TRANSITION VERS IPv6 34

1. Accélération de la pénurie d'IPv4 : IPv6, une transition indispensable 34
2. Baromètre de la transition vers IPv6 en France 35
3. La co-construction avec l'écosystème pour accélérer la transition vers IPv6 41

VEILLER À L'OUVERTURE D'INTERNET 47

4. GARANTIR LA NEUTRALITÉ D'INTERNET 48

1. L'Arcep s'engage au niveau européen 48
2. Travaux en cours 49
3. Analyse des pratiques observées 57
4. La coopération européenne pour une application cohérente du règlement 59

5. CONTRIBUER À L'OUVERTURE DES TERMINAUX 61

1. Travaux de l'Arcep 61
2. Bilan réglementaire 62
3. Analyse des pratiques observées 63

Lexique 66

Annexe 1 : Mise en place d'une interface de programmation applicative (API) dans les box 71

Annexe 2 : Mires (serveurs) proposées par les différents outils de test de qualité de service 74

Annexe 3 : Fiabilisation du test de qualité de service 79

L'Arcep établit le bilan de santé 2019 d'internet

L'Arcep ausculte le patient sur les composantes qui relèvent de ses missions : qualité du service, interconnexion des données, transition vers le protocole IPv6, neutralité des réseaux et ouverture des terminaux. L'enjeu ? Veiller à ce qu'internet se développe comme un « bien commun ».

Devenu outil incontournable du quotidien des Français, internet est un bien collectif et une « infrastructure de libertés » : liberté d'expression et de communication, liberté d'accès au savoir et de partage, mais aussi liberté d'entreprise et d'innovation.

Évaluer la santé d'internet, c'est évaluer sa capacité de résistance aux risques et aux menaces qui pèsent aujourd'hui sur ce bien commun : polémiques répétées sur les données personnelles ou les fausses nouvelles *(fake news),* diffusions de contenus haineux sur les réseaux sociaux, cyber-attaques, impacts environnementaux du numérique, remise en cause de la neutralité de l'internet, concentration autour d'un nombre réduit de plateformes numériques, ou encore inégalités d'accès. Veiller à la santé d'internet, c'est en garantir l'accessibilité, le bon fonctionnement et l'ouverture.

L'Arcep, architecte et gardien des réseaux d'échanges, prend sa part au diagnostic. Ce rapport propose une présentation didactique de l'état des réseaux et des chantiers entrepris pour garantir au mieux la capacité d'échange des utilisateurs. Pour chacune des composantes, l'Arcep identifie les symptômes, et établit une prescription pour soigner le patient internet, ou lui proposer des remèdes préventifs.

Le présent document constitue le tome 3 du rapport annuel de l'Arcep : il se concentre sur les composantes de la santé d'internet qui relèvent directement des missions de l'Autorité. Les questions liées à la résilience, à la sécurité ne sont pas abordées ici ; mais le lecteur qui souhaiterait prolonger l'exercice du bilan de santé sur ces autres composantes pourra par exemple se reporter aux travaux pilotés par l'ANSSI sur le sujet.

L'état des déploiements des réseaux, autre aspect de la bonne santé d'internet en France, est pour sa part détaillé dans un autre rapport intitulé « La régulation de l'Arcep au service des territoires connectés », tome 2 du rapport annuel.

Et demain ?

Internet évolue en permanence… Pour être à l'écoute des évolutions technologiques des réseaux, l'Arcep a entamé un cycle de réflexion intitulé « Réseaux du futur ». Les premiers résultats de cette réflexion, notamment sur la virtualisation des réseaux, sont disponibles sur le site de l'Autorité… et nourriront probablement un jour le présent rapport.

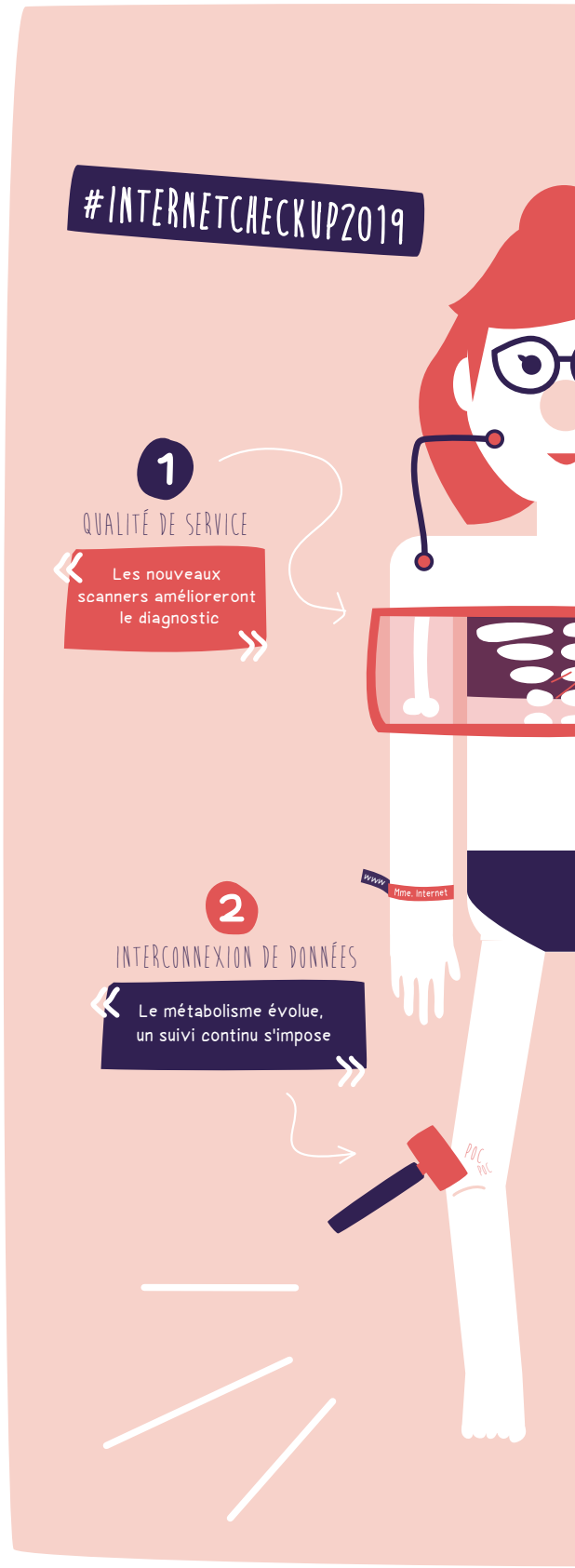
Le bilan de santé d'internet 2019 par l'Arcep

1 QUALITÉ DE SERVICE

Pour pouvoir améliorer la qualité de service d'internet, encore faut-il pouvoir la mesurer. Les comparateurs d'aujourd'hui sont si peu homogènes qu'il est impossible pour les utilisateurs de faire de la performance un réel critère de choix de fournisseur d'accès. Pour remédier à cela, l'Arcep a souhaité perfectionner le scanner : la mise en place d'une API dans les box déclinant la « carte d'identité de l'accès » de chaque terminal permettra un bien meilleur diagnostic, avec une information fiable sur les paramètres de chaque mesure. Fruit d'une concertation avec l'ensemble des acteurs de l'écosystème, cette API est complétée par un Code de conduite. Progressivement adopté par les acteurs de la mesure, il permet de gagner en fiabilité, en transparence et en lisibilité des résultats.

2 INTERCONNEXION DE DONNÉES

L'interconnexion constitue le fondement d'internet : elle permet à tous les réseaux de communiquer entre eux et de ne faire qu'un à nos yeux. Cet écosystème en constante évolution peut être le terrain de tensions ponctuelles. C'est la qualité de service perçue par l'utilisateur qui est alors menacée. L'Arcep exerce donc un suivi vigilant du marché, et publie dans son baromètre annuel de l'interconnexion en France des données issues de sa collecte d'information. Une étude du métabolisme de ce marché et de ses évolutions, de grande valeur pour les acteurs du secteur. Quand la situation l'exige, l'Arcep peut aussi se faire « gendarme » et régler les différends entre les acteurs.



3 TRANSITION VERS IPv6

Le rythme d'acquisition des derniers blocs d'adresse IPv4 s'est encore intensifié cette année. Conséquence : la fin d'IPv4 est dorénavant annoncée pour juin 2020. Accélérer la transition vers IPv6 n'est plus une option, c'est une nécessité. Pourtant, les déploiements de l'IPv6 prévus par les opérateurs fixes et mobiles risquent de ne pas permettre de répondre à la pénurie d'adresses IPv4. Afin d'activer l'écosystème sur le sujet, l'Arcep organisera, au second semestre de 2019, la première réunion de travail de la « Task-Force IPv6 ». Ces réunions semestrielles permettront de partager les expériences des différents acteurs et de définir des actions à mettre en place pour accélérer la transition vers IPv6 en France. Pour cela, l'Arcep étudie la mise en place d'une plateforme en ligne permettant l'échange entre tous les participants à la « Task-Force ».

4 NEUTRALITÉ DU NET

Deux ans après l'entrée en vigueur du règlement sur l'internet ouvert en Europe, c'est l'heure du premier bilan ! La mise en pratique du principe de neutralité du net par les régulateurs nationaux a permis de constater que les lignes directrices, qui peuvent nécessiter encore quelques clarifications, ont globalement fait leurs preuves. En France, l'application « Wehe » arrivée fin 2018 fait désormais partie, avec la plateforme « J'alerte l'Arcep », de l'arsenal des outils que l'Autorité mobilise au quotidien pour détecter des gestions de trafic contraires au principe de neutralité du net. Le pays bénéficie d'un bilan positif en matière de neutralité du net. Toutefois, l'Autorité veille à ce que les fournisseurs d'accès continuent d'ajuster leurs pratiques en conformité avec le cadre réglementaire. Enfin, la neutralité technologique du règlement internet ouvert permet à l'Arcep d'accompagner sereinement l'arrivée de la 5G et de ses innovations.

5 OUVERTURE DES TERMINAUX

Avec l'entrée en vigueur du règlement européen sur la neutralité du net, l'Arcep peut exercer sa protection sur les réseaux. Pourtant, au bout de la chaîne, il existe un maillon faible : les terminaux. Le sujet a gagné en visibilité depuis quelques mois. En Europe, Android a été sanctionné pour son abus de position dominante sur le marché des systèmes d'exploitation mobiles. Le règlement européen "Platform-to-business", adopté début 2019, apporte plus de transparence sur les pratiques des plateformes en ligne vis-à-vis de leurs clients entreprises. Mais si l'Arcep se félicite de ces premières avancées pour la liberté d'innovation et la liberté de choix des utilisateurs, le règlement "Platform-to-business" ne permet pas encore d'assurer la neutralité des terminaux. Dans son rapport consacré à la question, publié en février 2018, l'Arcep émet onze propositions concrètes pour assurer un internet ouvert "de bout en bout".

Assurer le bon fonctionnement d'internet

1. AMÉLIORER LA MESURE DE LA QUALITÉ DE SERVICE
2. SUPERVISER L'INTERCONNEXION DE DONNÉES
3. ACCÉLÉRER LA TRANSITION VERS IPv6

1 Améliorer la mesure de la qualité de service

« Les nouveaux scanners amélioreront le diagnostic »

5
outils de mesure de qualité de service se sont déclarés conformes au Code de conduite de l'Arcep

Comment se porte la qualité de service de l'internet en France ? S'il suffit qu'un corps soit à 37°C pour considérer qu'il est à la « bonne » température, la mesure et l'analyse de la capacité des réseaux à véhiculer dans de bonnes conditions un trafic internet est plus complexe : en effet il est nécessaire de mesurer plusieurs indicateurs (débit, latence, gigue, etc.) pour réaliser une telle évaluation, mais la mesure en elle-même est également complexe.

1. LES BIAIS POTENTIELS DE LA MESURE DE LA QUALITÉ DE SERVICE

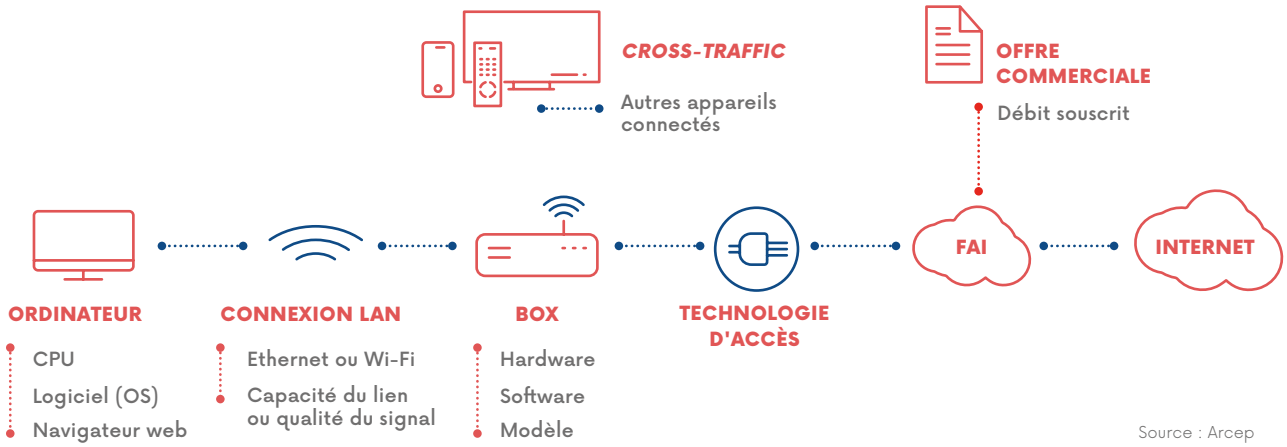
Aujourd'hui, les utilisateurs peuvent facilement faire remonter leurs mesures de la qualité de service de leur accès internet via des outils de test dits *« en crowdsourcing »*.

Néanmoins, un grand nombre de caractéristiques techniques ou d'usage ont une influence sur la mesure et il est très difficile de savoir si une mauvaise qualité mesurée est due au réseau d'accès du fournisseur d'accès à internet (FAI), à la qualité du Wi-Fi et/ou à l'utilisation parallèle d'autres appareils connectés au réseau local lors du test.

« L'environnement utilisateur » est le premier facteur qui peut affecter le résultat d'une mesure lors d'un test. Le schéma ci-dessous récapitule les caractéristiques principales de l'environnement utilisateur pouvant avoir une influence sur le résultat.

D'autres caractéristiques (emplacement et capacité de la mire de test, méthodologie de mesure de l'outil de test) peuvent également être facteurs de biais lors de la mesure de la qualité de service. Elles sont explicitées dans la suite du chapitre.

CARACTÉRISTIQUES DE L'ENVIRONNEMENT UTILISATEUR



Source : Arcep

2. LES TRAVAUX AMORCÉS EN 2018 SUR LA CARACTÉRISATION DE L'ENVIRONNEMENT UTILISATEUR

La caractérisation de l'environnement d'un utilisateur sur un accès fixe est primordiale pour établir un diagnostic précis d'un problème de qualité de service. Les possibilités de caractérisation varient en fonction du type de l'outil de test utilisé. Certaines sondes matérielles[1] sont par exemple en mesure de caractériser la connexion LAN[2] voire d'estimer le *cross-traffic*[3] sur le réseau local. À l'inverse, s'il est vrai que les testeurs web[4] sont rapidement déployables à grande échelle, ils ne permettent de caractériser qu'un nombre très faible d'éléments (navigateur web utilisé, etc.). En tout état de cause, quel que soit l'outil, il n'est pas à même de caractériser tous les paramètres définissant l'environnement utilisateur et impactant la mesure de qualité de service.

Afin de pouvoir mieux caractériser l'environnement utilisateur, l'Arcep a animé en 2018 un chantier de co-construction avec des acteurs issus d'un large spectre de l'écosystème de la métrologie en *crowdsourcing*[5] :

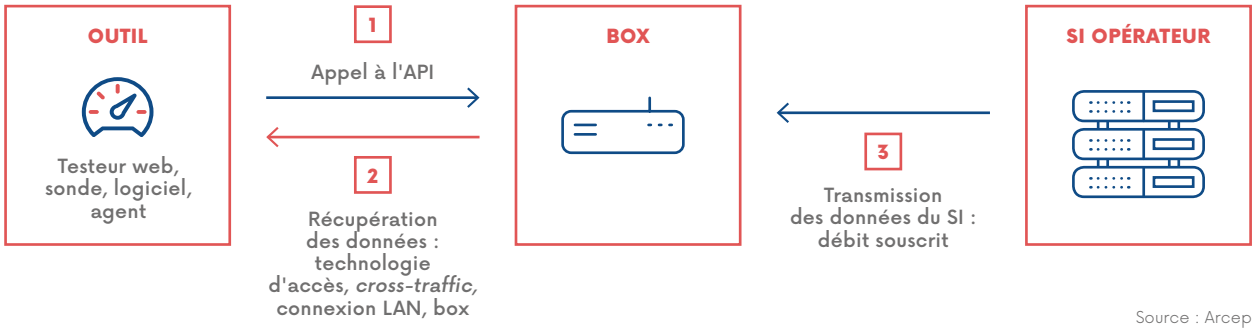
- des outils de mesure : ASSIA, Case on IT, Cedexis, Directique, Ip-label, M-Lab, Ookla, nPerf, QoSi, SamKnows, V3D ;
- des FAI : Bouygues Telecom, Free, Orange, SFR ;
- des acteurs académiques et de la recherche : CNES, Inria ;
- des organismes de protection des consommateurs : INC, UFC Que-Choisir, qui ont également développé leurs propres outils.

En décembre 2018, ces travaux ont permis, à l'issue d'une série de groupes de travail, de converger vers la définition et mise en place d'une interface de programmation applicative (API) implémentée directement dans les box des opérateurs et accessible aux outils déclarant se conformer au Code de conduite de la qualité de service publié par l'Arcep[6]. Cette interface permettra de transmettre les informations qui constituent la « carte d'identité de l'accès ».

Afin de stabiliser le périmètre de cette API, l'Arcep a mis en consultation publique le 23 avril 2019 un projet de décision précisant les modalités de son déploiement.

Cette API est une interface logicielle qui sera implémentée dans chaque box permettant la transmission, au moment de l'exécution d'une mesure de la qualité de service internet par le client d'un accès xDSL, câble ou FttH, ainsi que les box d'accès fixe supportant la technologie 5G des informations telles que la technologie d'accès, le débit souscrit par le consommateur, ou la qualité du Wi-Fi. L'API permet ainsi de caractériser l'environnement utilisateur sans dégrader l'expérience utilisateur.

FONCTIONNEMENT DE L'API « CARTE D'IDENTITÉ DE L'ACCÈS »



Source : Arcep

L'outil de mesure utilisé par le client (testeur web, sonde, logiciel installable, agent dans la box) envoie une requête à l'API située dans la box. Le test de mesure de la qualité de service internet est lancé par l'outil de mesure immédiatement après cette requête.

L'API répond à l'outil de mesure en lui transmettant les spécifications techniques qui caractérisent l'environnement de l'utilisateur lors du test de mesure de la qualité de service internet. La plupart des informations transmises sont disponibles nativement dans la box : technologie, informations sur la connexion LAN et WAN et compteur d'octets permettant de détecter le *cross-traffic*.

Les autres spécifications, comme le débit souscrit par l'utilisateur (non disponible nativement), sont transférées du système d'information des opérateurs à la box. Cette implémentation laisse la liberté aux opérateurs de choisir le moyen de transmission et offre aux outils de mesure de la qualité de service internet une interface unique pour collecter les informations de caractérisation.

Les informations principales remontées par l'API ont été arrêtées en co-construction avec l'écosystème :

- métadonnées : version de l'API, horodatage ;
- informations concernant le modèle de la box et la version du logiciel intégré à la box ;
- débits souscrits par le consommateur ;
- type de connexion internet : FttH, ADSL, VDSL, etc. ;
- débits réels entre la box et l'équipement côté opérateur et entre la box et l'équipement terminal ;

1. Voir lexique.
2. Voir lexique.
3. Voir lexique.
4. Voir lexique.
5. L'Autorité invite les acteurs non cités qui souhaiteraient participer à la démarche de co-construction à la contacter.
6. Édition 2018 du Code de conduite de la mesure de la qualité de service internet : https://www.arcep.fr/uploads/tx_gspublication/code-de-conduite-qs-internet-2018_FR.pdf

- type de connexion entre l'équipement terminal et la box : Wi-Fi, Ethernet, CPL ;
- spécifiquement pour le Wi-Fi : la génération du Wi-Fi (802,11n, 802,11ac, etc.) et de la puissance reçue du signal Wi-Fi ;
- information sur le *cross-traffic :* nombre complet d'octets utilisés sur la box entre le début et la fin du test de qualité de service.

La liste exhaustive des paramètres est disponible à l'annexe 1 du rapport, qui reprend l'annexe 1 du projet de décision mis en consultation publique par l'Autorité.

Le projet de décision de l'Autorité mis en consultation publique prévoit une phase de test de l'API. Puis, à la suite de plusieurs échéances intermédiaires, le projet de décision prévoit que les opérateurs implémentent et activent par défaut l'API, dans un délai de 28 mois, sur 95 % des box du parc concerné par la mise en place de l'API, et sur 100 % des box mises à disposition auprès des nouveaux clients sur le marché de détail grand public fixe. Un comité de suivi du développement de l'API sera mis en place pour réunir les parties prenantes afin de faire vivre le projet le plus agilement possible.

3. VERS DES MÉTHODOLOGIES DE MESURE PLUS TRANSPARENTES ET ROBUSTES

3.1. Présentation du Code de conduite de l'Arcep

Outre les caractéristiques de l'environnement utilisateur, les méthodologies de mesure sont également des facteurs ayant une forte influence sur le résultat des mesures de qualité de service. L'Arcep avait identifié en 2017 le besoin d'une plus grande transparence des méthodologies de mesure. Elle a publié en décembre 2018 un Code de conduite à destination des acteurs de la mesure. Ce Code de conduite porte sur deux aspects : d'une part, inviter les outils à accompagner la publication des résultats par une explication claire des choix méthodologiques réalisés afin que toute personne tierce soit en mesure d'analyser les résultats présentés ; d'autre part, indiquer les bonnes pratiques essentielles à l'obtention de mesures robustes. Cette approche permet d'inciter les acteurs à un niveau minimum de transparence et de robustesse, à la fois pour les protocoles de test, mais aussi pour la présentation des résultats.

Le Code de conduite se structure en deux grandes parties :

- la première partie concerne les protocoles de test, les mires de test et les méthodologies de mesure des débits descendants et montants, de la latence, du temps de téléchargement des pages web et de la qualité du *streaming* vidéo ;
- la seconde partie concerne les publications agrégées, dont un engagement général sur la mise en place d'algorithmes visant à exclure les mesures erronées, manipulées ou non pertinentes. Par ailleurs, pour garantir la représentativité statistique, les outils respectant le Code de conduite s'engagent à publier la période couverte, le nombre de mesures et les facteurs susceptibles d'introduire un biais significatif dans l'analyse des catégories comparées.

Chaque partie présente les modalités permettant d'assurer la transparence des choix réalisés et un premier niveau de robustesse des pratiques mises en œuvre :

- **les critères de transparence :** en ce qui concerne les protocoles de test, les outils doivent par exemple indiquer les différents paramètres du protocole de mesure qui permettent d'analyser si le test est ou non représentatif des usages les plus fréquents sur internet. Un exemple concret : un outil de test de qualité de service qui utilise le port 8080 ou le port 8443, des ports principalement utilisés par les outils de test de débit eux-mêmes, est par principe moins représentatif qu'un outil qui utilise les ports 80 ou 443, utilisés pour accéder aux pages web. En ce qui concerne les publications agrégées, les outils doivent par exemple rendre public le nombre de mesures sous-jacentes ;
- **les critères de robustesse :** en ce qui concerne les protocoles de test, par exemple, pour mesurer le débit, le critère de robustesse impose un test de plus de 7 secondes ou un téléchargement de plus de 100 Mo de données. Pour mesurer la latence, un critère de robustesse impose de ne pas utiliser le protocole ICMP pour mesurer la latence, ICMP étant un protocole non représentatif d'un cas d'usage réel, qui peut remonter une latence non représentative de la réalité observée avec le protocole TCP ou UDP. En ce qui concerne les publications agrégées, les outils doivent par exemple avoir mis en place des algorithmes efficaces de traitement des données afin de présenter des résultats les plus fiables possibles.

Le Code de conduite de la qualité de service internet, version 2018, fixe un niveau minimum de transparence et de robustesse qui sera amené à évoluer périodiquement afin de renforcer les critères présentés, mais aussi de les compléter par des éléments relatifs à d'autres catégories thématiques. Les évolutions se feront en concertation avec les acteurs impliqués. Ce Code de conduite apportera également prochainement des précisions sur la mesure de la qualité de service d'internet via des réseaux mobiles.

3.2. Les premiers outils qui commencent à adopter le Code de conduite de la qualité de service internet

Le Code de conduite a été publié par l'Arcep le 20 décembre 2018 et dès début 2019, plusieurs outils s'y déclaraient conformes.

Les outils de test de qualité de service fixe qui se sont déclarés conformes au Code de conduite de la qualité de service internet :

- nPerf, développé par nPerf ;
- Speedtest UFC-Que Choisir, développé par UFC-Que Choisir ;
- DébiTest 60 : le testeur de connexion de 60 millions de consommateurs, développé par QoSi ;
- 4GMark, développé par QoSi ;
- IPv6-test : le test de qualité de service IPv4 et IPv6, développé par IPv6-test.

Les outils de test de qualité de service mobile qui se sont déclarés conformes le Code de conduite de la qualité de service internet :

- nPerf, développé par nPerf ;
- DébiTest 60 : le testeur de connexion de 60 millions de consommateurs, développé par QoSi ;
- 4GMark, développé par QoSi.

PAROLE À...

Martin Thierry, Ingénieur d'études, Centre d'essais comparatifs, Institut National de la consommation (INC)

Comparer la qualité de sa connexion avec DébiTest 60, l'outil collaboratif de l'INC

Paradoxalement, plus les réseaux à très haut débit, fixes et mobiles, s'étendent, plus les insatisfactions sur leurs performances se font entendre. Accéder à un réseau de qualité est primordial, quelles que soient les zones du territoire français. Or l'écart entre les promesses des opérateurs et le ressenti des consommateurs reste important et atteint parfois des proportions inacceptables sur certaines zones rurales, montagneuses et insulaires voire absurdes quand le haut d'une rue bénéficie d'un bon débit ADSL et le bas de cette rue d'un débit anémique.

Toutes ces difficultés liées à l'accessibilité et aux performances des réseaux sont ressenties comme une inégalité insupportable et incompréhensible par les consommateurs. Dans ce contexte, ces derniers ont encore plus besoin d'outils orientés QoE pour mieux comprendre ces limitations « *géo-technologiques* » ainsi que d'outils dédiés à la collecte de l'expérience terrain. En ce dernier domaine, l'INC salue les efforts des élus et de l'AFUTT dans la remontée des attentes et des insatisfactions des citoyens ainsi que les initiatives de l'Arcep avec sa plateforme de signalement « J'alerte l'Arcep » et de l'Agence du numérique avec « France Mobile ».

Pour sa part, l'INC a sorti en 2018 son service collaboratif DébiTest 60. Véritable boîte à outils de mesure, il permet d'évaluer les performances des connexions internet fixes et mobiles et d'objectiver ce sentiment confus que l'on « nous ment » sur la qualité des réseaux et des connexions. DébiTest 60 propose ainsi au consommateur une comparaison des performances de sa connexion avec celles des autres utilisateurs, des cartes de performances et une approche pédagogique à même de mieux l'instruire sur les comportements de ses connexions. Aujourd'hui, l'INC s'est engagé dans la construction d'indicateurs de fiabilité de l'information restituée par ses cartes de performances et dans une réflexion sur la déontologie minimale qui engagerait les acteurs de la mesure en *crowdsourcing*.

Vincent Néguier, fondateur, IPv6-test

Mesurer la qualité de service d'internet en IPv6

Il y a environ dix ans, les premiers rapports commençaient à s'inquiéter sur la diminution alarmante du nombre de blocs IPv4 non alloués et sur la nécessité d'une solution à long terme au manque d'adresses disponibles pour un monde de l'IoT connecté en 5G.

Cette solution existait déjà et il s'agit bien sûr du protocole IPv6. Mais, la connectivité IPv6 pour une entreprise n'était alors pas une évidence, encore moins pour un particulier, et rares étaient les sites web qui disposaient d'une adresse IPv6.

C'est dans ce contexte que nous avons lancé en 2010 ipv6-test.com, une plateforme d'évaluation technique de la connectivité IPv6. Le site permet de tester divers aspects de sa connexion : de la comparaison de sa bande passante v4/v6 à la détection de certaines problèmes de configuration ou de sécurité.

Les données anonymes collectées depuis le lancement du site permettent de mettre en lumière une évolution significative de la politique des grands acteurs du net en France et dans le monde vis-à-vis du protocole IPv6.

Nos chiffres pour la France montrent que plus de 99 % des adresses IPv6 testées sont désormais natives, quand à l'époque près de 20 % utilisaient des protocoles de transition tels que 6to4 ou Teredo. Ce changement, ajouté aux efforts des fournisseurs de transit et des points d'échange, a permis d'arriver aujourd'hui à des performances identiques en IPv6 et en IPv4 sur nos tests de bande passante, alors que IPv6 était à la traîne d'environ 20 % en moyenne sur l'année 2010.

On retrouve cette tendance à l'échelle mondiale, avec des chiffres similaires. On dénombre 99 % d'adresses IPv6 natives en 2019 contre 74 % en 2010, et l'écart de performances de 25 % constaté en 2010 est maintenant résorbé.

La décennie 2010 a été celle de la transition vers IPv6. Si celle-ci s'est faite parfois trop lentement, les rouages sont maintenant bien huilés et il n'y a plus aucune raison de vouloir s'en passer.

Renaud Keradec, CEO/CTO et fondateur, nPerf SAS

La fausse simplicité du *crowdsourcing*

Chez nPerf, on s'est rendu compte que vus de l'extérieur, les outils de tests de débit paraissent souvent assez simples et à la portée de n'importe quel développeur.

Pourtant, il n'en est rien. Bien que simple en apparence, un test de débit est très complexe à mettre en œuvre pour assurer sa fiabilité. C'est un ensemble de maillons (de l'applicatif qui mesure le débit au serveur qui le fournit) reliés par un système d'information intelligent qui doit en permanence savoir où est l'utilisateur, chez quel opérateur et lui indiquer sur quel serveur (actuellement disponible) il doit effectuer son test sans craindre d'être limité par la connectivité de celui-ci. À cela s'ajoute bien évidemment la performance de l'algorithme de mesure qui se doit d'exploiter au maximum les capacités de l'ordinateur ou du smartphone de l'utilisateur pour mesurer le débit de façon fiable et précise. Enfin, pour être valable dans le monde entier, le test doit s'appuyer sur un réseau mondial de serveurs. C'est un véritable travail d'horloger !

Ensuite, vient la phase d'analyse, de filtrage et de compilation des millions de mesures collectées pour en extraire des tendances générales et générer des cartographies. On est en plein dans le big data !

Au-delà de la difficulté technologique, fédérer une communauté autour d'un outil aussi technique est un véritable challenge. Il faut proposer un outil ergonomique et attrayant suffisamment précis pour convaincre les technophiles mais aussi facile d'accès pour ne pas rebuter le grand public. On est en recherche constante de l'équilibre entre la mesure utile pour l'analyse des données et le confort d'utilisation de l'outil.

Bref, tout cela nécessite un véritable savoir-faire qui fait notre fierté. Notre détermination a permis à une petite entreprise française comme la nôtre d'acquérir, petit à petit, une renommée mondiale.

Fabien Renaudineau, directeur général, QoSi

La donnée, un outil indispensable à la régulation du secteur

La donnée est aujourd'hui devenue un élément incontournable des stratégies industrielles de tout l'écosystème télécom et un outil indispensable à la régulation du secteur.

Expert indépendant de la mesure de la qualité des réseaux, s'appuyant entre autre sur le *crowdsourcing*, nous avons acquis la conviction qu'une démarche de mesure isolée, quelle que soit la méthode employée, a une portée limitée et donne des résultats très en-deçà du potentiel offert par une démarche globale avec un écosystème désormais mature sur ces sujets.

C'est pourquoi chez QoSi, nous nous efforçons d'associer à notre démarche un nombre de contributeurs toujours plus important – qu'ils soient des grands comptes privés (entreprises), publics (collectivités et administrations territoriales), associations de consommateurs ou encore des médias –.

Ce sont leurs apports qui renforcent la robustesse de notre plateforme et consolident la pertinence des mesures et des données recueillies.

En 2019, c'est cette démarche collective et collaborative, dont nous sommes devenus les agrégateurs, qui est mise au service de la politique de régulation par la donnée de l'Arcep.

Antoine Autier, responsable adjoint du service des études, UFC-QueChoisir

Pour une description encore plus précise de la qualité de l'internet sur le territoire

Au-delà de l'outil d'information individuel qu'offrent aux consommateurs les tests de qualité de l'internet, l'UFC-Que Choisir considère qu'ils doivent également, idéalement, permettre d'alimenter les débats publics concernant l'aménagement numérique du territoire.

C'est cette double exigence qui a mené l'année dernière notre association à lancer son Observatoire de la qualité de l'internet fixe, en retenant deux grands axes : coupler des tests de performance (débits, latence) et d'usages (navigation web, lecture d'une vidéo en *streaming)* d'une part, et différencier les résultats selon la zone géographique d'autre part.

Après un an de tests, les résultats du terrain mettent en évidence le traitement différencié des consommateurs en termes d'accès à internet selon leur lieu d'habitation. Ils soulignent aussi tout l'intérêt à bien saisir que des différences minimes de débits en ADSL peuvent avoir des impacts considérables sur l'expérience utilisateur. A contrario, de gros différentiels de débits sur le très haut débit (en lien avec les différentes technologies utilisées), sont loin d'avoir des effets significatifs sur les usages courants.

Pour que les outils de mesure de la qualité puissent permettre de tirer des enseignements forts, structurants, il est nécessaire qu'ils soient robustes techniquement, suffisamment souples pour s'adapter aux évolutions des réseaux, et suffisamment pertinents pour décrire la capacité de ces réseaux à délivrer du débit. À cet égard, le développement en cours d'une API, sous l'égide de l'Arcep, permettant de connaître au mieux l'environnement dans lequel un test de qualité est réalisé pour limiter les biais, constitue une démarche précieuse.

Afin de pouvoir notamment mobiliser cette API, l'UFC-Que Choisir vient de faire évoluer son dispositif technique en l'ouvrant à tous *(speed test* en ligne ainsi qu'une extension aux navigateurs web à télécharger pour tester les usages). En perspective : des résultats plus nombreux, plus affinés, encore plus probants, pour une description encore plus précise de la qualité de l'internet sur le territoire.

POUR ALLER PLUS LOIN

FOCUS SUR LES TESTS MONO-CONNEXION / MULTI-CONNEXIONS

Certains outils de test de qualité de service sont uniquement mono-connexion (ou *mono-thread* en anglais), d'autres remontent le débit mesuré en additionnant les débits de multiples connexions simultanées *(multi-thread* en anglais). Certains laissent enfin le choix à l'utilisateur de réaliser un test *mono-* ou *multi-thread.*

Les deux types de mesure du débit sont pertinents et répondent à un objectif différent.

- le mode **multi-connexions** permet d'estimer la **capacité** du lien au moment de la mesure en déterminant, à cet instant, le débit maximum du lien en utilisant plusieurs flux en parallèle ;
- le mode **mono-connexion** permet de remonter un **débit représentatif d'une utilisation d'internet.** La majorité des usages utilisant une ou deux connexions simultanées pour transférer les données, le mode mono-connexion permet d'être plus proche du ressenti réel, surtout si le débit est un débit moyen incluant la période de *« slow start »,* c'est-à-dire la période située juste après l'établissement du *« handshake »,* où la connexion TCP monte en débit. À l'opposé, d'autres outils remontent le débit en régime établi, une fois le régime nominal atteint. Enfin, certains remontent un débit basé sur le 70e centile (durée moyenne sur la meilleure période représentant 30 % de la durée totale du test), proche du débit crête.

Il arrive régulièrement que les tests réalisés en mode multi-connexions affichent un débit plus élevé que ceux en mono-connexions, ce qui s'explique par plusieurs raisons :

- **latence :** plus la latence est élevée, plus une connexion TCP met du temps à monter en débit. Un test mono-connexion va monter en débit seize fois plus lentement qu'un test multi-connexion qui utilise seize connexions TCP : plus la latence est élevée, plus le débit moyen d'un test mono-connexions va baisser ;
- **limitation de la taille de fenêtre d'acquittement TCP** (c'est-à-dire le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception). Cette fenêtre n'est limitante que sur les systèmes d'exploitation les plus anciens. Par exemple, dans certains cas Microsoft Windows 7 limite cette fenêtre à 255 Ko par connexion TCP. Avec une latence bout en bout de 30 ms, le débit sera alors limité à 68 Mbit/s pour un test mono-connexion et 1088 Mbit/s pour un test de qualité de service qui additionne le débit de 16 connexions simultanées ;
- **gigue :** une connexion avec une gigue qui ne permet pas de garantir que les paquets arrivent dans l'ordre va dégrader fortement le débit : quand les paquets arrivent dans le désordre, TCP ne peut pas identifier le débit de la connexion, conséquence, le débit peut être divisé par dix[1] ;
- **saturation d'un lien d'un LAG :** l'agrégation de liens (LAG) est une technique utilisée dans les réseaux informatiques, permettant le regroupement de plusieurs liens réseau et de les utiliser comme s'il s'agissait d'un seul. Les LAG Ethernet sont presque toujours implémentés pour répartir les paquets en scrutant leurs en-têtes *(IP headers).* De cette façon, une session TCP donnée, disposant toujours des mêmes éléments considérés en en-têtes pour chaque sens (adresses MAC, adresses IP, ports), verra ses paquets tous transmis par le même lien physique. Un test de qualité de service mono-connexion utilisera donc toujours le même lien physique qui peut être saturé, alors qu'un test multi-connexions utilisera plusieurs liens physiques, réduisant le risque de contention. Un exemple fictif concret : vous avez une connexion 1 Gbit/s. La collecte de votre opérateur récupère les flux de votre région par un lien 100 Gbit/s, constitué d'un LAG de 10 liens 10 Gbit/s. Le lien est chargé à 97 % au moment où vous réalisez le test, il y a donc 3 Gbit/s disponible sur l'ensemble du LAG. En partant du principe théorique que le LAG est parfaitement équilibré (chaque lien est chargé exactement à 97 %, donc chaque lien à 300 Mbit/s disponible), un test de qualité de service mono-connexion affichera un débit 300 Mbit/s là où un test de qualité de service multi-connexions affichera 1 Gbit/s, en utilisant plusieurs liens du LAG simultanément ;
- **saturation d'un cœur du processeur du terminal :** un test de qualité de service mono-connexion peut ne pas exploiter tous les cœurs d'un processeur au maximum, contrairement à un test multi-connexions. Une machine équipée d'un processeur quatre cœurs pourrait avoir une limitation de débit liée au processeur plus faible en mono-connexion, comparé au même test en multi-connexions.

Le débit d'un test de qualité de service mono-connexion est proche de celui d'un test multi-connexions, si :

- la latence de bout en bout est faible (inférieure à 15 ms) ;
- le système d'exploitation possède une pile TCP/IP moderne (cas des différents systèmes d'exploitation récents, comme Microsoft Windows 8 et ultérieur, macOS 10.9 et ultérieur, Ubuntu 11.10 et ultérieur) ;
- les paquets arrivent systématiquement dans l'ordre où ils ont été émis ;
- la connexion est éloignée de toute saturation aussi bien chez le fournisseur d'accès à internet que l'hébergeur et les éventuels prestataires entre l'hébergeur et le fournisseur d'accès à internet ;
- le processeur du terminal utilisé sait gérer le débit sans saturer un seul cœur du microprocesseur ;
- le débit de la connexion internet est inférieur à 1 Gbit/s. Pour les débits supérieurs à 1 Gbit/s, le temps de montée en débit peut entraîner un écart significatif entre test de qualité de service mono-connexion et multi-connexions.

Un débit mono-connexion fortement inférieur au débit multi-connexions montre un problème qui impacte négativement la qualité d'expérience. Il est toutefois impossible, sans une étude précise, de définir si ce problème est lié à l'ordinateur utilisé pour le test, aux équipements utilisés sur le réseau local du client, au fournisseur d'accès à internet, aux éventuels prestataires entre l'hébergeur et le fournisseur d'accès à internet ou l'hébergeur.

1. Source :
https://www.semanticscholar.org/paper/Packet-reordering-in-high-speed-networks-and-its-on-Feng-Ouyang/4acaee5f78578273071f23832ca799278126149d

4. L'IMPORTANCE DU CHOIX DE LA MIRE DE TEST

Le choix de la « mire de test », c'est-à-dire le serveur avec lequel le test de qualité de service réalise les mesures de débit descendant, de débit montant et de latence est important. C'est aussi un facteur qui conditionne le résultat de la mesure.

4.1. Impact de la bande passante entre une mire et internet

Une mire doit avoir suffisamment de bande passante disponible pour ne pas être un facteur limitant. En particulier, c'est le cas quand la capacité de la mire est inférieure ou égale à celle de la ligne testée.

Pour donner un exemple concret : un test sur une ligne FttH qui permettrait un débit de 1 Gbit/s sera limité à 500 Mbit/s si deux clients FttH effectuent simultanément ce même test sur une mire qui serait connectée à internet avec seulement 1 Gbit/s.

Le Code de conduite 2018 contient ainsi un ensemble de critères de transparence minimum sur les mires utilisées par les outils de mesure, critères qui devraient être renforcés dans les prochaines versions du Code de conduite en concertation avec l'écosystème.

Le Code de conduite 2018 ne contient pas de critère fixant une bande passante minimum pour les mires (fixer un minimum de 10 Gbit/s réduirait considérablement le choix ou aurait un impact financier potentiellement assez élevé). Toutefois, il préconise d'exclure des publications les mesures pour lesquelles les mires se sont avérées être un facteur limitant.

D'autres critères de robustesse devraient être ajoutés dans la prochaine version du Code de conduite.

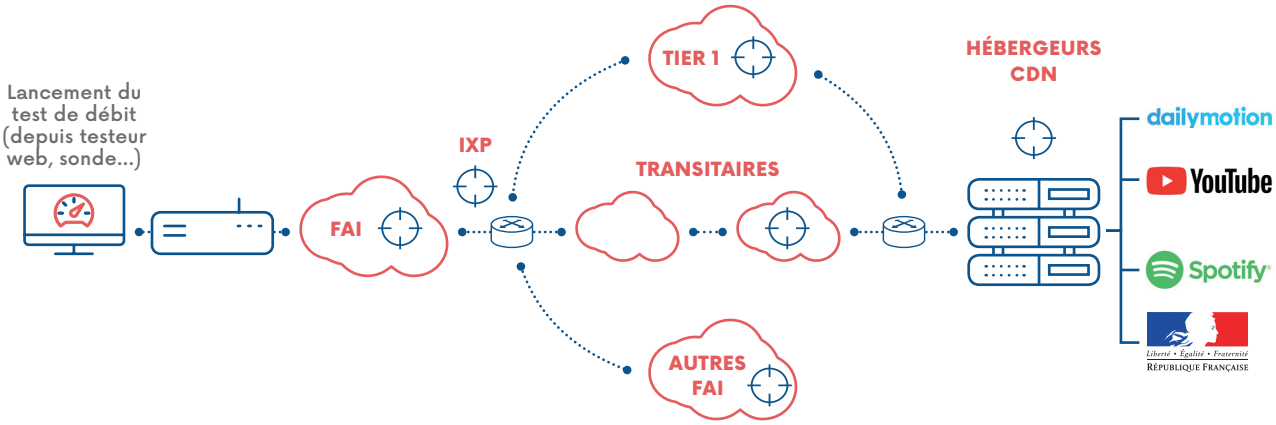
POUR ALLER PLUS LOIN

ZOOM SUR LES MIRES ANYCAST

Certains outils proposent pour certaines mires d'exploiter le protocole « Anycast ». Anycast est une technique d'adressage où le réseau identifie le serveur le « plus proche » du point de vue de la topologie globale du réseau. Il y a donc plusieurs serveurs physiques derrière une mire accessible en Anycast. Cela permet au réseau de sélectionner le serveur le plus proche du client.

Par exemple, un habitant de Nice utilise la mire Anycast de son fournisseur d'accès à internet qui possède trois serveurs physique : Paris, Lyon et Marseille. Si le choix est réalisé en fonction de la distance géographique, c'est Marseille qui est choisi. Toutefois, si pour joindre le serveur de Marseille le client doit passer par Lyon, dans ce cas-là, le réseau sélectionnera le serveur de Lyon, plus proche au niveau réseau du client que le serveur de Marseille.

IMPACT DE LA LOCALISATION DES MIRES DE TEST



Mires de test : serveurs potentiels vers lesquels sont effectuées les mesures de qualité de service

Source : Arcep

4.2. Impact de la localisation des mires de test

La localisation de la mire est primordiale pour la latence et les tests de débit mono-connexion à très haut débit. La localisation est moins importante pour un test de qualité de service multi-connexions, la latence impactant peu le débit.

Comme explicité sur le schéma « Impact de la localisation des mires de test », les mires de test peuvent être localisées à différents endroits :

- dans le réseau du FAI de l'utilisateur : le résultat du test ne dépend que du FAI mais il est très peu représentatif d'un usage réel des services internet, souvent hébergés au delà de ce simple réseau ;
- dans le réseau d'un autre FAI directement interconnecté (par *peering*) avec le FAI de l'utilisateur : le test prend non seulement en compte le réseau du FAI de l'utilisateur mais également la qualité du réseau et de l'interconnexion avec un autre FAI ; ce test est le plus souvent très peu représentatif d'un usage réel des services internet ;
- à un point d'échange internet (IXP, pour *internet Exchange Point*) : le réseau testé ne dépend pratiquement que du FAI et se rapproche d'un usage réel, une partie du trafic internet passant par les IXP ;
- dans le réseau d'un transitaire : le test n'est pertinent que si le transitaire échange beaucoup de trafic avec le FAI de l'utilisateur ; il est à noter que les observatoires réalisés par des transitaires (comme celui d'Akamai) représentent uniquement la qualité de service vers un point précis de l'internet ;
- dans le réseau d'un *Tier 1*[7] : le réseau testé va au-delà des seules performances du réseau du FAI ; les mesures sont encore plus représentatives d'un usage réel que lorsque les mires sont placées à un IXP ;
- au plus proche des serveurs des FCA : le réseau testé est celui emprunté de bout en bout jusqu'à un hébergeur donné ; les tests sont donc très représentatifs *d'un usage en particulier* (l'observatoire de Netflix par exemple, donne uniquement une mesure de la qualité vers son service).

L'emplacement géographique est trompeur. Prendre le serveur géographiquement le plus proche de son domicile ne signifie pas que le serveur est proche d'un point de vue réseau. Par exemple, un habitant de Nice peut penser pertinent d'utiliser un serveur hébergé dans sa ville. Toutefois, il est tout à fait possible qu'il soit nécessaire de passer par Paris pour joindre ce serveur si ce dernier n'est pas hébergé sur le réseau de son fournisseur d'accès à internet.

Quelles sont les mires proposées par les différents outils de test de qualité de service ?

L'Arcep liste, à titre illustratif, les mires de tests utilisées par différents outils en annexe 2 du rapport.

L'Arcep met à disposition des utilisateurs un script de tests permettant de vérifier les débits de certaines des mires de test de qualité de service, dans le but de sélectionner une mire qui ne soit pas le facteur limitant pour le test de qualité de service. Le script est disponible ici : https://github.com/ARCEP-dev/testDebitMire

POUR ALLER PLUS LOIN

IMPACT DU PORT TCP UTILISÉ PAR LA MIRE DE TEST

Il s'agit encore d'un aspect important pour la représentativité des tests. De nombreux usages sur internet utilisent le port TCP 443. Un test de qualité de service qui utilise le même port sera plus représentatif d'un usage réel qu'un test utilisant un port différent. En effet, les choix techniques pour acheminer le trafic peuvent être différents en fonction du port.

Quatre ports TCP sont utilisés par les différents outils de test de qualité de service :

- port 80 : port du trafic HTTP utilisé pour l'accès non chiffré aux pages web ;
- port 443 : port utilisé par HTTPS (HTTP avec une couche de chiffrement au travers le plus souvent du protocole TLS) ;
- port 8080 : le trafic transporté sur ce port est majoritairement du trafic lié à des tests de débit. Aujourd'hui, le trafic du port 8080 est généralement chiffré, ce qui n'était pas le cas il y a quelques années ;
- port 8443 : ce port qui est le pendant chiffré du port 8080.

7. *Les Tier 1* sont les réseaux capables de joindre tous les réseaux internet par une interconnexion directe ; voir lexique.

PAROLE À...

Isabelle Chrisment, professeure, Telecom Nancy, Université de Lorraine

BetterNet : vers une cartographie collaborative d'internet

Parallèlement à la croissance exponentielle du trafic internet, les services proposés aux utilisateurs ont augmenté en complexité. Les acteurs intermédiaires se sont multipliés et ont défini de nouvelles solutions pour améliorer la performance d'accès à ces services. Des systèmes de distribution de contenus (CDN) ont ainsi été mis en place. Des entités qui fournissent des services multimédia OTT *(Over-The-Top),* c'est-à-dire hors offre du fournisseur d'accès à internet, ont déployé leurs propres serveurs de cache pour améliorer la qualité de services offerte. De nouveaux protocoles, comme QUIC, se sont développés pour permettre d'accéder plus rapidement aux applications web. L'environnement local utilisateur est devenu également de plus en plus complexe (pare-feux, NAT, réseaux sans fil, box internet…). Pour afficher une seule page web, un navigateur doit souvent interagir avec plusieurs serveurs car les différentes parties d'une page web sont souvent distribuées à travers l'internet. La performance de chargement d'une application web ne dépend donc plus strictement du seul fournisseur d'accès mais d'autres facteurs et stratégies déterminés par les fournisseurs de contenus.

Il convient donc d'analyser finement l'impact de cette complexité sur la qualité d'expérience telle que perçue par l'utilisateur final afin d'améliorer les protocoles et les applications, et éventuellement détecter des comportements qui pourraient être biaisés par des acteurs intermédiaires. Le traitement est dit « neutre » si tous les paquets de données sont traités sans distinction de leur type, origine ou destination, à chaque nœud du réseau. La neutralité est imposée par la loi en Europe mais a été remise en question dernièrement aux États-Unis, par exemple.

Dans le cadre du projet BetterNet, nous proposons donc de construire un observatoire scientifique et technique collaboratif pour mesurer et améliorer l'accès aux services internet à partir de l'expérience utilisateur. BetterNet est un *Inria Project Lab* (IPL) impliquant plusieurs équipes de recherche Inria (Diana, Dionysos, MiMove, Resist, Spirals), l'entreprise ip-label et le laboratoire Triangle (ENS-Lyon/CNRS) et l'Arcep.

Afin de concevoir, intégrer, valider et améliorer des méthodes de mesure nouvelles ou existantes, nous avons ainsi développé une plateforme de mesure qui fédère différents outils développés au sein d'Inria :

- APISENSE® (https://apisense.io) et son application Android Bee qui offrent une solution distribuée de *mobile crowdsensing* pour collecter des mesures quantitatives (en provenance de capteurs physiques) et/ou qualitatives (via des interactions utilisatrices) sur le terrain en favorisant une démarche participative et respectueuse de l'intimité des participants ;
- Hostview qui permet de récupérer des mesures sur le trafic réseau annoté avec les retours des utilisateurs sur la qualité de l'expérience. Une version mobile de Hostview a été développée et intégrée à l'application mobile Bee afin qu'un utilisateur puisse aisément participer à la collecte ;
- ACQUA qui est une application Android permettant de mesurer régulièrement les performances de l'accès internet (débit, délai, taux de pertes de paquets, etc.) et de prédire la qualité d'expérience utilisateur à partir de ces mesures.

Les données collectées sont ensuite stockées au sein du Laboratoire Haute Sécurité (https://lhs.inria.fr) pour être ensuite analysées et agrégées avant d'être restituées aux utilisateurs et autres acteurs de l'internet. Elles leur permettront ainsi d'être informés sur l'évolution de l'usage de l'internet et de ses performances. Ce travail devrait conduire à l'amélioration des modèles et métriques définis.

Nous travaillons également sur le développement d'outils de métrologie pour mesurer si un comportement biaisé peut être observé, au niveau par exemple du traitement des paquets ou par le choix des données mises en cache près des utilisateurs pour une meilleure qualité de service. Il s'agira donc pour les différents types d'acteurs réseau de définir un comportement neutre ou équitable, ainsi que les métriques associées, et de mettre en place des techniques de mesure correspondantes. Ce travail se complète d'un effort de traduction culturelle (au plus grand nombre) des mesures effectuées, en produisant des cartes associant mesures, démographie et géographie, et en étudiant les effets de ces cartes (et d'autres, produites par divers organismes comme l'Arcep) sur nos représentations du monde contemporain.

5. COMMENT MAXIMISER LA FIABILITÉ DE SON TEST DE QUALITÉ DE SERVICE ?

Un utilisateur pourrait souhaiter maximiser la fiabilité de son test de qualité de service. Dans ce cas, un certain nombre de paramètres doit être pris en compte pour s'affranchir des biais liés notamment à l'environnement utilisateur et aux mires de test et pouvant impacter la mesure. Ces paramètres sont détaillés dans l'annexe 3 de ce rapport.

POUR ALLER PLUS LOIN

CLÉ USB BOOTABLE

Les logiciels installés sur une machine semblent également avoir une importance lors d'un test de qualité de service. Pour réaliser un test de qualité de service qui fait abstraction des logiciels installés, le lecteur expert peut suivre la démarche disponible sur le site de l'Arcep[8] pour créer une USB bootable et réaliser un test de qualité de service qui fait abstraction des logiciels installés.

L'outil de mesure développé par le BEREC

Au mois de septembre 2018, le BEREC a démarré le développement de son outil *open source* de mesure de qualité de service internet. Cet outil sera constitué d'une application mobile (sur Android et iOS), d'un testeur web et d'une version installable (sur Windows, Mac et Linux).

Au-delà de la mesure des indicateurs habituels (débit, latence, etc.), cet outil pourra mesurer certains indicateurs d'usage tel que la qualité de la navigation web ou du streaming vidéo ainsi que des indicateurs liés à la neutralité du net comme le blocage de ports, la détection de proxy ou la manipulation DNS.

La fin du développement de l'outil est prévue pour fin 2019. Son adoption se faisant sur base volontaire, les autorités de régulation nationales pourraient implémenter l'outil sur leur territoire après une adaptation aux besoins nationaux (traduction de l'interface utilisateur, mise en place de serveurs de tests locaux, ajout d'indicateurs de test supplémentaires, etc.).

Cet outil pourrait devenir à terme un nouveau dispositif de diagnostic de l'Arcep sur les volets de qualité de service et de neutralité du net.

6. LE SUIVI PAR L'ARCEP DE LA QUALITÉ DE L'INTERNET MOBILE

Si les cartes de couverture mobile des opérateurs, réalisées à partir de simulations numériques des opérateurs et vérifiées par l'Arcep, donnent une information nécessaire sur l'ensemble du territoire, elles présentent des visions simplifiées de disponibilité des services mobiles ; ces cartes sont complétées par les données relatives à la qualité de service. Réalisées en conditions réelles, elles n'offrent pas une vision exhaustive du territoire, mais permettent de connaître de façon précise le niveau de service proposé par chaque opérateur dans tous les lieux mesurés.

Depuis 1997, l'Arcep mène, chaque année, une campagne d'évaluation de la qualité des services mobiles des opérateurs métropolitains. Les mesures réalisées visent à évaluer la performance des réseaux des opérateurs de manière strictement comparable, et ce dans différentes situations d'usage (en ville, en zone rurale, dans les transports, etc.) et pour les principaux services utilisés (appels, SMS, chargement de page web, *streaming* vidéo, téléchargement de fichiers, etc.). Cette enquête s'inscrit dans la stratégie de régulation par la donnée de l'Arcep et permet d'éclairer les utilisateurs. Pour l'année 2018, plus d'un million de mesures en 2G, 3G et 4G ont été réalisées sur l'ensemble du territoire, dans tous les départements (à l'intérieur et à l'extérieur des bâtiments) et dans les transports (TER, Transiliens, RER, métros, TGV, routes).

En 2017, l'Arcep a lancé son outil cartographique et interactif monreseaumobile.fr, qui permet de visualiser l'ensemble des données de cette enquête de qualité de service. « Mon réseau mobile » apporte une information sur mesure aux consommateurs en permettant de visualiser simplement, en un point donné, quel opérateur sera susceptible de leur proposer la meilleure qualité de service. Depuis juillet 2018, les territoires d'outremer ont également rejoint l'outil.

8. www.arcep.fr/demarches-et-services/consommateurs/comment-creer-une-cle-usb-bootable-pour-mesurer-sa-vitesse-de-connexion.html

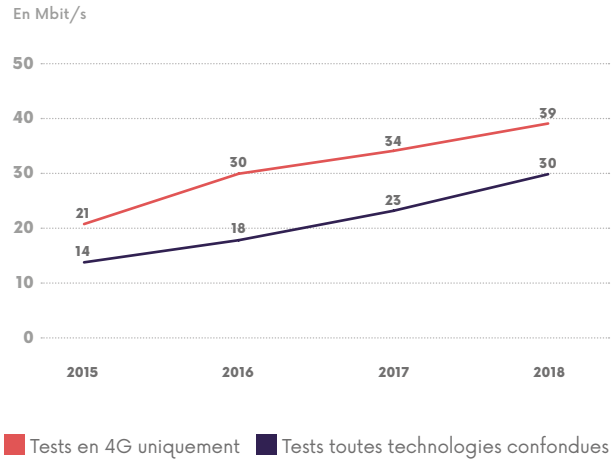
Avec l'explosion des usages de données, le *smartphone* est devenu le principal moyen d'accès à internet[9] ; ainsi la consommation sur les réseaux mobiles double chaque année, pour atteindre 6,8 Go[10] par mois par client avec une carte SIM active en 4G. Par ailleurs ces utilisateurs 4G représentent plus de 90 % du volume total d'échange de données mobiles.

La 4G est donc le fer de lance des investissements des opérateurs, afin de suivre cette explosion des usages. L'enquête annuelle menée par l'Arcep permet de mesurer la progression de la qualité de service des réseaux de chacun des opérateurs.

6.1. Le débit moyen en mobilité en France métropolitaine s'établit à 30 Mbit/s

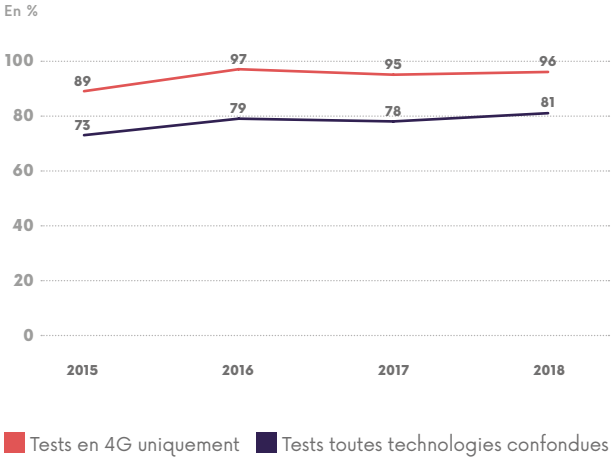
Le débit moyen mesuré par l'Arcep continue à progresser. En particulier, et pour la première fois, le débit moyen en téléchargement mesuré en France métropolitaine, toutes technologies confondues, tout opérateur confondu et toutes zones confondues (rurales, intermédiaires et denses) atteint 30 Mbit/s. En 4G uniquement, les débits continuent également à croître, et s'établissent en moyenne à 39Mbit/s. Par ailleurs, l'écart de performance entre le débit descendant moyen en 4G uniquement et celui en 2G/3G/4G tend à se réduire avec la généralisation de la 4G sur le territoire.

MOYENNE DES DÉBITS DESCENDANTS MESURÉS PAR L'ARCEP EN FRANCE MÉTROPOLITAINE



Source : Arcep

PART DES PAGES WEB CHARGÉES EN MOINS DE 10 SECONDES EN FRANCE MÉTROPOLITAINE



Source : Arcep

Concernant la navigation web, en 2018, 81 % des pages web mesurées par l'Arcep – parmi un échantillon des 30 sites les plus consultés en France – étaient chargées en moins de 10 secondes. La 4G apporte également un gain très important sur cet indicateur puisque le taux de pages web chargées en moins de 10 secondes uniquement en 4G s'établit quant à lui à 96 %[11]. Il apparaît ainsi que la 4G apporte une nette amélioration de la qualité des services de données des opérateurs, ce qui favorise d'autant plus le développement des usages en mobilité.

9. Baromètre du numérique 2018.
10. Observatoire des marchés des communications électroniques au 3e trimestre 2018.
11. Mesures de l'Arcep disponibles en *open data* : https://static.data.gouv.fr/resources/monreseaumobile/20181019-104845/2018-10-lieuxdevie-arcepqos2018.csv

6.2. Enrichissement de Mon réseau mobile

En décembre 2018, l'Arcep a publié une feuille de route sur son outil « Mon réseau mobile » pour répondre aux attentes des territoires qui souhaitent effecteur leurs propres mesures et recourir à des solutions de type *crowdsourcing.* L'Arcep a donné une nouvelle impulsion à sa démarche de régulation par la data et d'ouverture à l'intelligence collective en publiant un « kit du régulateur » mis à disposition des collectivités pour organiser des mesures en environnement maîtrisé en complément de celles effectuées par l'Arcep lors de ses campagnes de mesures. Ce « kit du régulateur » est destiné aux collectivités et à tous les acteurs qui souhaitent mener des mesures comparables répondant à leurs propres besoins, par exemple dans des zones géographiques inexplorées. Il permettra la réalisation de mesures en environnement maîtrisé, isolant ainsi les nombreux facteurs externes susceptibles d'avoir une influence sur les résultats et d'en fausser la pertinence, tels que le type de mobile utilisé, l'horaire du test ou encore le fait de tester à l'intérieur ou l'extérieur d'un bâtiment. En facilitant la réutilisation de ses protocoles et en les rendant plus compréhensibles, l'Arcep souhaite encourager les initiatives visant à compléter sa propre action.

En ce qui concerne les applications de mesure de l'expérience mobile, comme des tests via des applications basées sur le *crowdsourcing,* l'Arcep a également publié une version préliminaire de son « Code de conduite de la qualité d'expérience mobile » qui traite des spécificités liées aux réseaux mobile et qui a pour objectif d'assurer un niveau minimal d'exigence en termes de pertinence, de présentation et de transparence des mesures. Il s'agit de proposer une démarche de co-construction qui permet de s'assurer que les mesures produites en complément viennent effectivement enrichir ses publications, dès lors que l'Arcep publie d'ores et déjà des informations dans le cadre de la mission qui lui est dévolue par la loi. Pour être reconnus par l'Arcep, les outils de mesure (tels que les applications de *crowdsourcing)* devront suivre le Code de conduite. L'Arcep échangera avec les acteurs concernés pour affiner le Code de conduite, avec l'objectif que ceux qui le respectent puissent se faire connaître rapidement des collectivités locales. Il s'agit pour l'Autorité d'accompagner les élus locaux dans leur recours à des outils pertinents qui produisent des mesures qui viendront enrichir les cartes de couverture. Les données collectées dans ce cadre pourront par ailleurs être publiées sur « Mon réseau mobile ».

J'alerte l'Arcep

Lancée en octobre 2017, la plateforme « J'alerte l'Arcep » est à disposition de chaque citoyen, de chaque entreprise ou de chaque collectivité qui souhaite remonter du terrain tout problème lié à l'internet mobile, à l'internet fixe ou aux services postaux. En une année, plus de 34 000 signalements ont été transmis à l'Arcep. De ces signalements, 62 % concernent un problème lié à qualité et la disponibilité des services fixes ou mobiles. 1,2 % concernent un problème lié à la neutralité du net.

Ces remontées constituent un élément important dans la capacité de diagnostic de l'Arcep. En effet, elles permettent de quantifier et identifier les difficultés rencontrées par les utilisateurs afin d'orienter ses actions vers les solutions les plus appropriées possible. S'agissant de la qualité de service d'internet, ces signalements ont permis de confirmer les orientations stratégiques de l'Autorité relatives à la construction d'outils permettant de fiabiliser et de comparer plus efficacement les mesures. Les signalements liés aux questions de neutralité du net ont permis à l'Autorité d'identifier dans des temps très brefs des signaux faibles correspondant à de possibles infractions au principe de neutralité d'internet et de favoriser une remédiation rapide.

L'Arcep travaille pour améliorer « J'alerte l'Arcep » et notamment ses typologies et sous-typologies. La partie « qualité de service », qui représente une majorité des signalements, est particulièrement concernée. C'est aussi en accroissant les précisions demandées sur certains cas que l'Arcep sera en mesure de mieux étudier certains sujets futurs.

2

Superviser l'interconnexion de données

« Le métabolisme évolue, un suivi continu s'impose »

53 %
du trafic vers les clients des principaux FAI en France provient de quatre fournisseurs de contenu : Netflix, Google, Akamai et Facebook

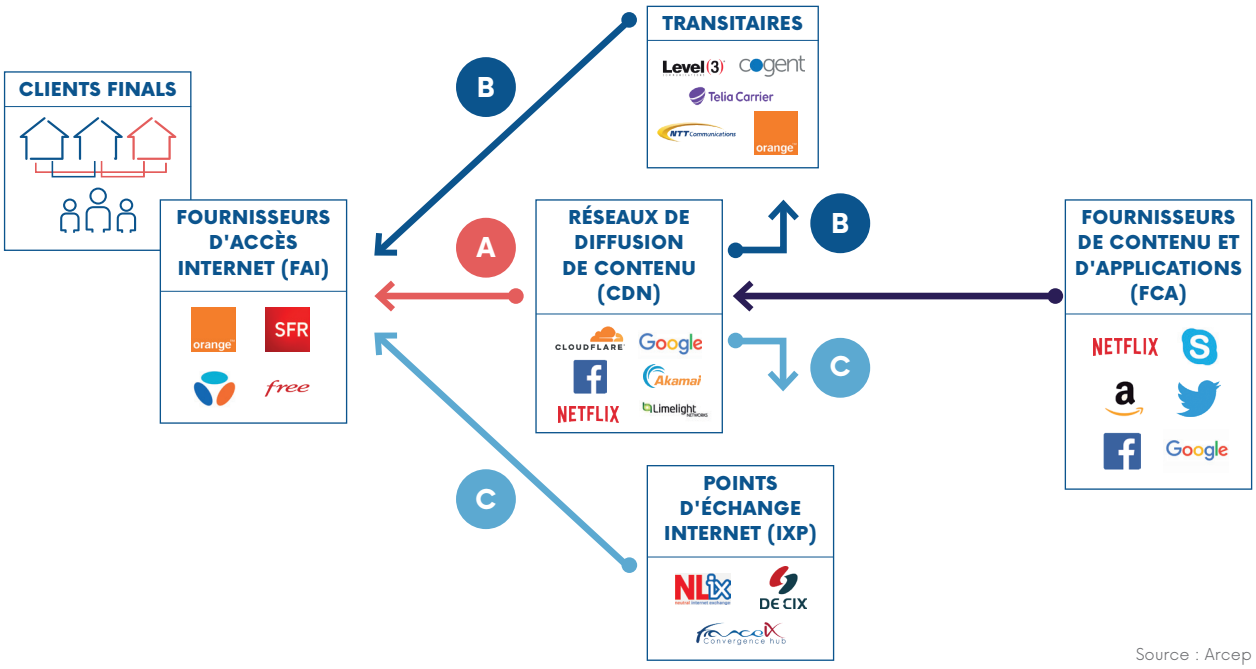
1. ÉVOLUTION DE L'ARCHITECTURE INTERNET[1]

De nombreux acteurs interagissent dans l'écosystème internet : fournisseurs de contenu et d'applications (FCA), hébergeurs, transitaires, point d'échanges internet (IXP), fournisseurs d'accès internet (FAI), etc.

Avec l'augmentation de la quantité de données à acheminer sur internet, un nouveau type d'acteurs a vu le jour : les CDN (ou réseaux de diffusion de contenu), qui se spécialisent dans la livraison de volumes de trafic importants vers plusieurs FAI, grâce à des serveurs cache au plus proche des clients finals. Ces acteurs récupèrent les données à partir d'un FCA et peuvent avoir des accords de *peering* directement avec les FAI (A), passer par un transitaire (B), ou par un IXP (C) pour acheminer ces données jusqu'au client final (voir schéma ci-dessous).

INTERCONNEXION DES CDN AVEC LES AUTRES ACTEURS D'INTERNET

Ce schéma est uniquement à titre illustratif et n'indique pas les vraies relations d'interconnexion entre les exemples d'acteurs indiqués.



Source : Arcep

1. N.B. : pour plus de précisions sur les termes techniques, l'Arcep invite le lecteur à se référer au baromètre de l'Arcep sur l'interconnexion de données en France : https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/linterconnexion-de-donnees/barometre-de-linterconnexion-de-donnees-en-france.html

Les avantages perçus par les FCA de l'utilisation de plateformes CDN sont notamment :

- l'amélioration de la qualité du service et de l'expérience pour l'internaute ;
- la connectivité internationale (comme avec un transitaire) ;
- l'intermédiation technique et commerciale (comme avec un transitaire) ;
- le rôle d'offreur alternatif aux transitaires contribuant globalement à faire diminuer les frais d'acheminement.

Comme indiqué par l'Arcep dans l'édition 2018 de son rapport sur l'état d'internet en France[2], l'architecture d'internet est en constante évolution et plusieurs scénarios d'intégration verticale peuvent être observés. Ainsi, la tendance actuelle est à la convergence entre les différents acteurs. Par exemple, d'un côté les CDN déploient leur propre infrastructure à travers le monde et les FCA mettent en place leur propre infrastructure réseau et plateformes CDN au plus près de l'utilisateur.

De nouveaux acteurs (CDN ou gros FCA) peuvent ainsi faire en partie abstraction des intermédiaires habituels pour l'acheminement du trafic.

Une autre tendance majeure est l'arrivée des CDN internes (ou CDN *on-net).* Ces serveurs sont gérés par l'entité qui les possède (FCA, CDN ou FAI) mais sont installés au niveau du réseau même du FAI. Afin d'améliorer leur qualité de service en se rapprochant au plus près du client final, les FCA effectuent des partenariats avec les FAI afin que leur contenu soit hébergé dans des serveurs cache placés à l'intérieur du réseau des opérateurs. Ces CDN internes peuvent être ceux de l'opérateur qui les héberge ou appartenir à des tiers. Ils permettent aux FCA/CDN de ne plus avoir besoin d'héberger leur infrastructure, les opérateurs réalisant l'opération pour eux. Du côté des opérateurs le gain est de ne plus avoir à transporter depuis un point d'interconnexion (Paris ou Marseille par exemple) les flux jusqu'à l'utilisateur final.

En France, Google et Netflix sont les deux principaux acteurs à mettre en place des CDN internes aux réseaux des principaux FAI en France.

2. https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-2018_conf050618.pdf

PAROLE À...

Sylvie LaPerrière, négociatrice stratégique au service interconnexions et infrastructure mondiale, Google

L'interconnexion et l'investissement en infrastructure au service de la qualité de service et de la compétitivité

Une étude récente d'Analysys Mason[1] met en exergue les investissements réalisés par les fournisseurs de services en ligne *("online service providers")* dans les infrastructures : entre 2014 et 2018, ces acteurs auraient investi plus de 300 milliards de dollars dans les infrastructures internet, soit 75 milliards par an, le double des investissements annuels sur la période 2011-2013. En Europe, ces investissements ont crû de 68 % par rapport à la même période.

Cette tendance est particulièrement avérée pour Google, l'infrastructure étant un domaine clé d'investissements pour nous. Google a investi 47 milliards de dollars en capex entre les années calendaires 2016 et 2018. Nous continuons à étendre notre infrastructure en 2019, y compris dans le déploiement de câbles sous-marins en propre, notamment sous-marin transatlantique baptisé Dunant, qui atterrira sur la côte française atlantique d'ici fin 2020[2] en partenariat avec Orange[3].

Dunant sera le premier câble sous-marin à relier les États-Unis et la France depuis plus de 15 ans !

« L'infrastructure est un domaine clé d'investissement pour Google »

Sur le plan de l'interconnexion, Google continue de proposer une politique de *peering* ouverte[4] destinée à promouvoir au maximum les liens directs avec les opérateurs au bénéfice des utilisateurs. En France, des liens de *peering* sont en place avec les principaux opérateurs français.

Par ailleurs, toujours dans l'esprit de favoriser un *peering* ouvert, Google soutient depuis son origine le point d'échange France IX[5] qui compte désormais une présence à Marseille et qui s'est hissé parmi les principaux *hubs* européens. Plus récemment, courant 2017, nous avons rejoint RezoPole et le point d'échange LyonIX[6].

Ces investissements permettent de proposer aux utilisateurs français une excellente qualité de service, tant pour les services tels que Google ou YouTube en ce qui concerne le grand public, que pour tous les services Google Cloud pour les entreprises françaises. Ce second domaine est crucial dans un contexte où le recours au *cloud* – et aux technologies qui vont de pair : analyse de données, *machine learning,* etc. – est un véritable enjeu de compétitivité pour les entreprises.

1. http://www.analysysmason.com/Consulting/content/reports/Online-service-providers-Internet-infrastructure-Dec2018/ (décembre 2018)
2. https://www.blog.google/products/google-cloud/delivering-increased-connectivity-with-our-first-private-trans-atlantic-subsea-cable/
3. https://www.orange.com/fr/Press-Room/communiques/communiques-2018/Orange-et-Google-s-associent-pour-un-nouveau-cable-sous-marin-a-travers-l-Ocean-Atlantique
4. https://peering.google.com/#/options/peering
5. www.franceix.net
6. https://www.rezopole.net/fr/news-rezopole/tag/google

PAROLE À…

Nicolas Pisani, Responsable relations opérateurs – Europe du Sud, Akamai

Akamai, un acteur majeur du marché de l'interconnexion

QUEL EST VOTRE AVIS GÉNÉRAL SUR LE MARCHÉ DE L'INTERCONNEXION EN FRANCE ?

La France représente pour Akamai l'un des premiers pays européens en termes de volumétrie de trafic. Cette position peut s'expliquer par un bon développement du marché des « OTT » ainsi que par une accélération du déploiement du très haut débit.

En France, comme dans tous les autres pays, Akamai entretient de bonnes relations avec les FAI. Notre philosophie consiste à collaborer étroitement avec eux afin de mettre en place des architectures d'interconnexion évolutives et fiables.

Cela étant dit, le marché français se distingue des autres marchés européens au moins pour deux raisons.

D'une part, les coûts d'interconnexion restent assez élevés chez certains FAI français par rapport à d'autres pays où les fournisseurs d'accès préfèrent appliquer une « stratégie de contenu » donnant la priorité à un partenariat technique garantissant performance et fiabilité.

D'autre part, le marché de l'interconnexion est fortement concentré à Paris. L'appétence des fournisseurs de services internet pour l'hébergement des CDN au sein de leur réseau dans d'autres villes reste limitée, malgré l'impact très positif de ces architectures distribuées, sur les performances et les coûts d'acheminement du trafic vers les abonnés.

QUELLE EST LA VALEUR DES RÉSEAUX DE DISTRIBUTION DE CONTENU SUR LE MARCHÉ ACTUEL DE L'INTERCONNEXION ? QUELS SONT LES ÉLÉMENTS QUI DIFFÉRENCIENT AKAMAI DES AUTRES ACTEURS ?

Lorsqu'il est question de diffusion de contenu, il semble important de différencier les détenteurs (plateformes UGC, plateformes VOD…) des agrégateurs tels qu'Akamai, qui fournissent un service de diffusion mais ne possèdent ni ne contrôlent les contenus.

Les agrégateurs permettent aux FAI de recevoir et de distribuer une multitude de sources de contenu populaires tout en minimisant le nombre d'accords d'interconnexion à établir et gérer. Il s'agit d'un bénéfice important pour les FAI dans la mesure où cette consolidation des sources de trafic contribue à optimiser leurs coûts d'interconnexion.

De plus, et même si la consommation de contenu s'avère être de plus en plus locale, l'existence de CDN minimise considérablement la quantité de trafic transportée sur les réseaux internationaux, ce qui permet une meilleure performance et une plus grande efficacité de l'internet global. Avec des pointes de trafic à plus de 80 Tbit/s, si notre plateforme s'arrêtait brusquement à l'échelle mondiale ou même européenne, l'internet serait probablement congestionné.

Plus généralement, les services disponibles sur internet (IPTV, e-Commerce, e-Banking, réseaux sociaux,…) nécessitent de s'appuyer sur des infrastructures distribuées offrant robustesse, performance, capacité extrême de montée en charge et sécurité.

L'utilisation d'un CDN comme Akamai est le seul moyen de couvrir ces quatre besoins fondamentaux tout en maîtrisant ses coûts.

Le succès d'Akamai réside dans la puissance et l'étendue de son infrastructure, ses relations étroites avec plus de 1 200 FAI dans le monde et sa capacité à fournir à ses clients des services associés à la distribution, tels que des solutions de sécurité, d'optimisation des ressources, d'analyse des performances, et plus récemment de gestion des identités et des accès clients (CIAM).

QUELLES SONT LES FUTURES ORIENTATIONS STRATÉGIQUES D'AKAMAI ?

Akamai investit dans la virtualisation, l'automatisation et, plus généralement dans l'industrialisation de sa plateforme mondiale. À titre d'exemple, nous avons commencé à déployer des *clusters* standardisés capables de générer jusqu'à plusieurs Tbit/s de trafic. Akamai a également fait évoluer son modèle en déployant son propre *backbone* international au cours des deux dernières années, alors que tout le trafic entre les infrastructures d'Akamai était auparavant acheminé via l'internet public. Enfin, Akamai a déployé ses propres centres de données aux États-Unis et est sur le point de faire de même en Europe.

L'objectif de ces différents axes de développement est double. D'une part, augmenter continuellement le niveau de qualité de service offert à nos clients et, d'autre part, optimiser notre structure de coûts afin de rester compétitifs dans un marché soumis à une forte concurrence.

2. ÉTAT DE L'INTERCONNEXION EN FRANCE

Grâce à la collecte d'information sur l'interconnexion et l'acheminement de données qu'elle réalise, l'Arcep dispose de données techniques et tarifaires sur l'interconnexion du premier semestre de 2012 au second semestre de 2018. Par souci de confidentialité, la publication des résultats[3] ne porte que sur des données agrégées.

Afin de pérenniser ces publications relatives à l'interconnexion de données, l'Arcep a mis en place en décembre 2018 un baromètre dédié. Ce baromètre sera mis à jour sur une base annuelle à chaque publication du rapport sur l'état d'internet[4].

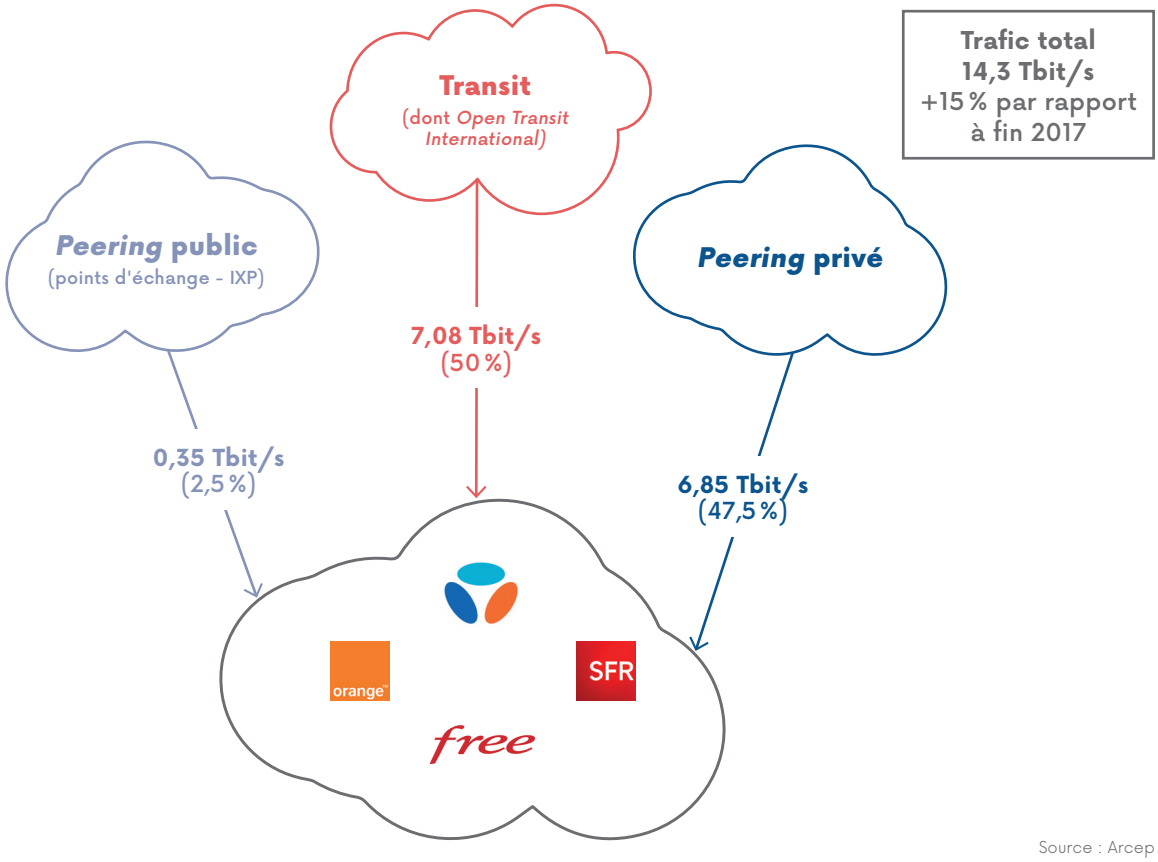
2.1. Trafic entrant

Le trafic entrant vers les quatre principaux FAI en France à l'interconnexion est passé de plus 12 Tbit/s à fin 2017 à 14,3 Tbit/s à fin 2018, marquant ainsi une augmentation de 15 % en un an. Le trafic provient pour la moitié des liens de transit. Ce taux de transit assez élevé est dû en grande partie au trafic de transit entre Open Transit International (OTI), Tier 1 appartenant à Orange, et le Réseau de *Backbone* et de Collecte Internet d'Orange (RBCI), qui permet d'acheminer le trafic vers les clients finals de ce FAI.

Les autres FAI, n'ayant pas d'activité de transitaire, font davantage appel au *peering*.

On remarque aussi une légère diminution du taux de *peering* au profit du transit. Cette évolution est due notamment à l'augmentation de la quantité de trafic provenant des CDN internes (Cf. 2.5. Répartition du trafic par mode d'interconnexion).

RÉPARTITION DU TRAFIC ENTRANT (AU 95E CENTILE) SUR LE RÉSEAU DES PRINCIPAUX FAI EN FRANCE (FIN 2018)

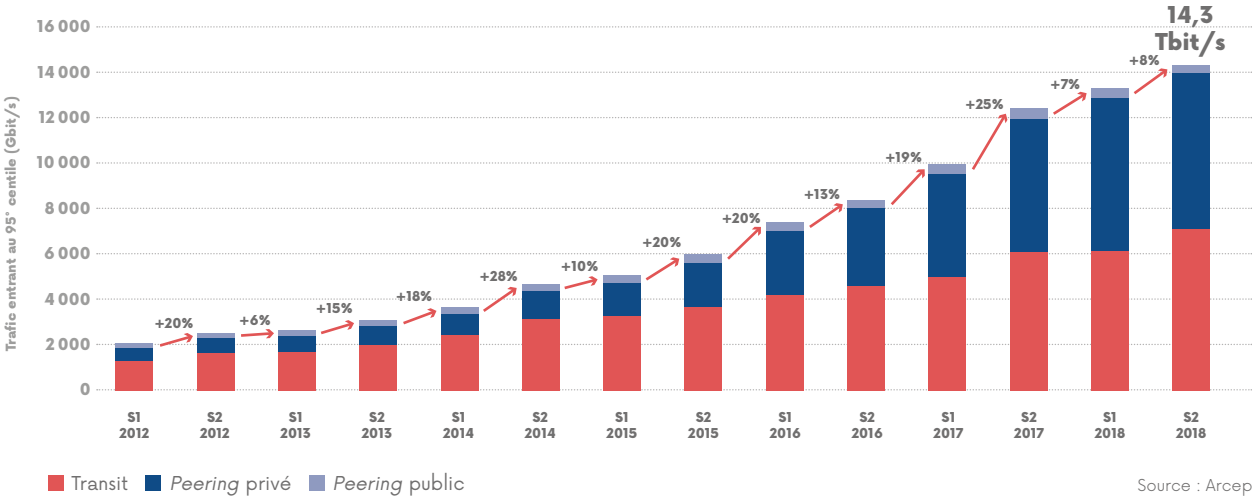


Source : Arcep

3. Résultats issus des réponses des différents acteurs à la collecte d'informations sur les conditions techniques et tarifaires de l'interconnexion et de l'acheminement de données, dont le périmètre est explicité dans les décisions de l'Arcep n° 2014-0353 et n° 2017-1492-RDPI qui modifient la décision n° 2012-0366 de l'Autorité.

4. https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/interconnexion-de-donnees/barometre-de-linterconnexion-de-donnees-en-france.html

ÉVOLUTION DU TRAFIC ENTRANT VERS LES PRINCIPAUX FAI EN FRANCE ENTRE S1-2012 ET S2-2018

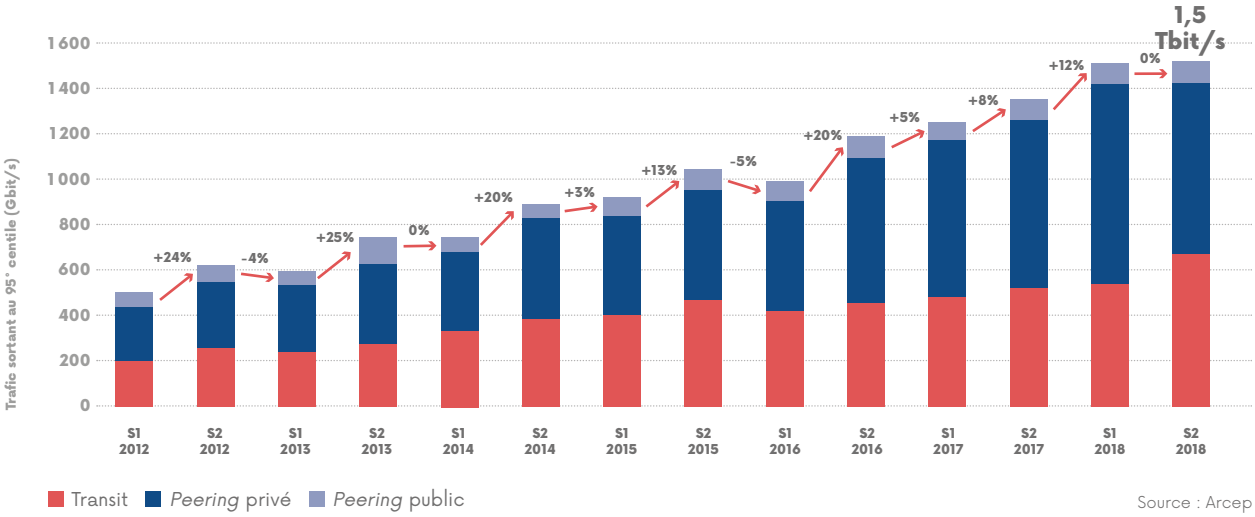


Source : Arcep

2.2. Trafic sortant

À mi-2018, le trafic sortant du réseau des quatre principaux FAI en France dépasse les 1,5 Tbit/s, soit une augmentation de 12 % par rapport à fin 2017. Entre 2012 et 2018, ce trafic a triplé. Par ailleurs, l'augmentation du trafic sortant est plus significative au second semestre de chaque année.

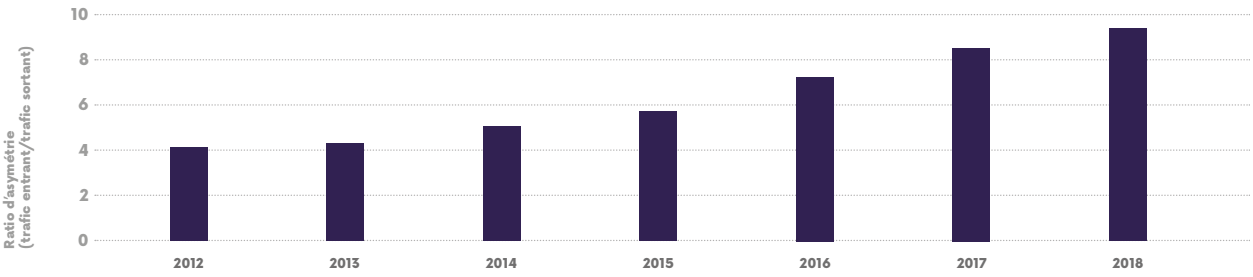
ÉVOLUTION DU TRAFIC SORTANT VERS LES PRINCIPAUX FAI EN FRANCE ENTRE S1-2012 ET S2-2018



Source : Arcep

Le trafic sortant est bien inférieur au trafic entrant. Par ailleurs, le taux d'asymétrie entre ces deux types de trafic est passé de 1/4 en 2012 à plus de 1/9 en 2018. Cette augmentation est due essentiellement à l'augmentation du contenu multimédia consulté par les clients *(streaming* vidéo et audio, téléchargement de contenu de grande taille, etc.).

ÉVOLUTION DU TAUX D'ASYMÉTRIE ENTRE LE TRAFIC ENTRANT ET LE TRAFIC SORTANT POUR LES PRINCIPAUX FAI EN FRANCE ENTRE 2012 ET 2018

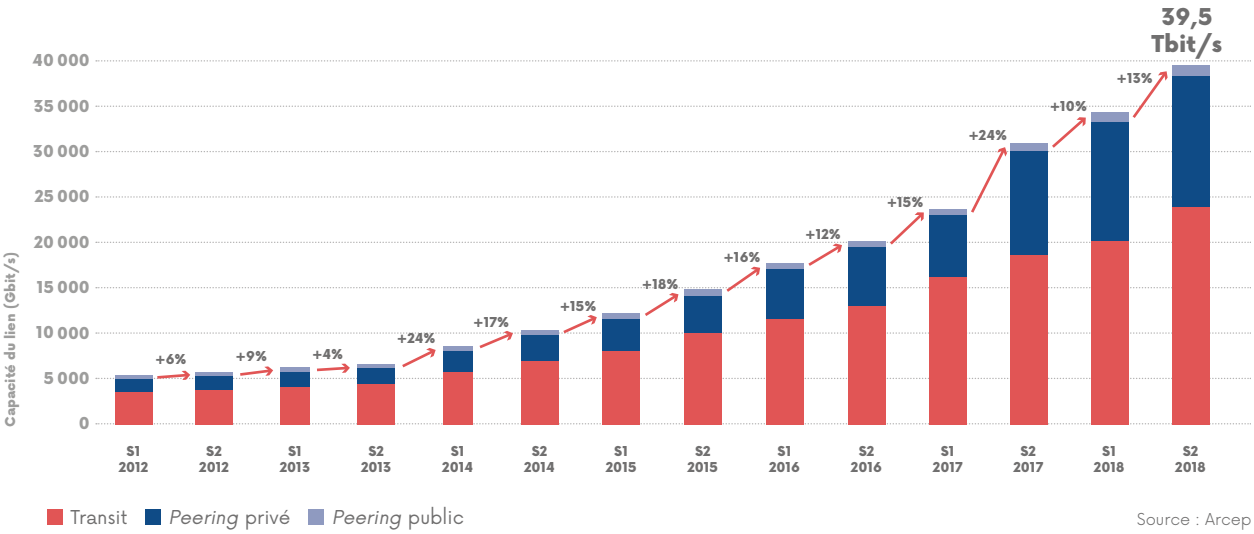


Source : Arcep

2.3. Évolution de la capacité installée

Une augmentation du même ordre de grandeur que le trafic entrant a été observée pour les capacités installées. À fin 2018, elles sont estimées à 39,5 Tbit/s, soit un facteur de 2,8 par rapport au trafic entrant. Ce ratio n'exclut pas l'existence de cas ponctuels de congestion, qui peuvent se manifester au niveau d'un ou de plusieurs lien(s) particulier(s) en fonction de leur état à un instant donné.

ÉVOLUTION DES CAPACITÉS DES INTERCONNEXIONS DES PRINCIPAUX FAI EN FRANCE ENTRE S1-2012 ET S2-2018



Source : Arcep

2.4. Évolution des modalités d'interconnexion

Peering vs Transit

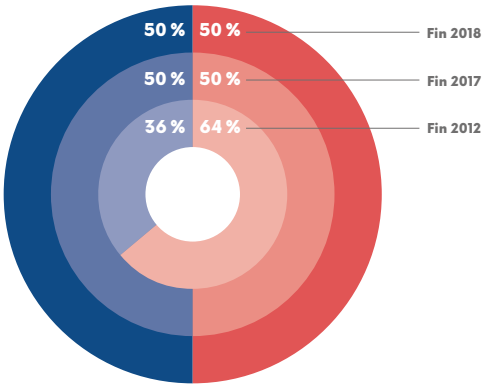
Généralement, la part de *peering* augmente d'une façon régulière. Cette croissance est principalement due à l'augmentation des capacités installées en *peering* privé entre les FAI et les principaux fournisseurs de contenu.

Cependant, entre fin 2017 et fin 2018, la part de *peering* n'a pas augmenté (50 %). Cette situation est due essentiellement à la substitution d'une partie du trafic de *peering* avec du trafic provenant des CDN internes.

Le trafic issu du *peering* public reste globalement stable : sa part relative (4 % à fin 2017, pour 2,5 % à fin 2018) diminue au profit du *peering* privé (46 % à fin 2017, pour 47,5 % à fin 2017).

ÉVOLUTION DES PARTS DE *PEERING* ET DE TRANSIT DES PRINCIPAUX FAI EN FRANCE

(en proportion du trafic entrant)



Peering Transit

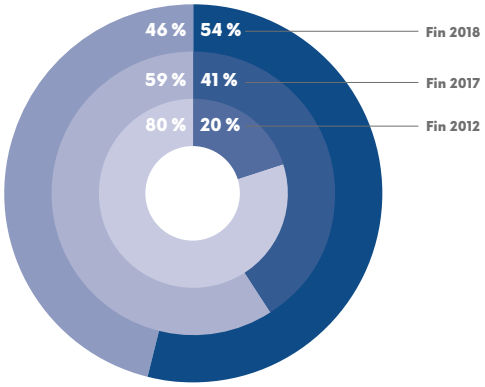
Source : Arcep

Peering gratuit vs *peering* payant

La part du *peering* payant est passée de 41 % à fin 2017 à 54 %. Cette évolution est due essentiellement à l'augmentation du trafic au niveau des liens de *peering* privé, dont une part importante est payante notamment dans le cas d'une grande asymétrie de trafic. Le *peering* entre les acteurs de taille comparable reste pour sa part généralement gratuit.

ÉVOLUTION DES PARTS DE *PEERING* GRATUIT ET PAYANT POUR LES PRINCIPAUX FAI EN FRANCE

(en proportion du trafic entrant)



Peering gratuit *Peering* payant

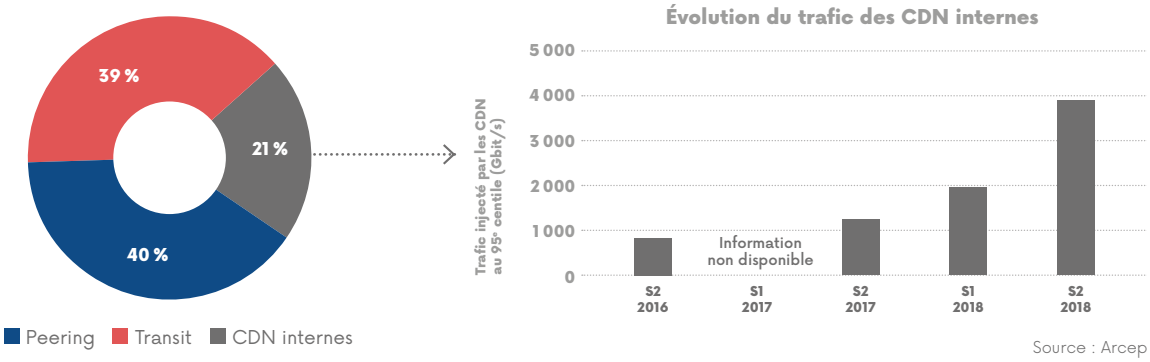
Source : Arcep

2.5. Répartition du trafic par mode d'interconnexion

À fin 2017, le trafic provenant des CDN internes était d'environ 1,2 Tbit/s. À fin 2018 ce trafic a triplé pour atteindre 3,8 Tbit/s soit 21 % du trafic total vers les clients finals des principaux FAI. Ce taux – en hausse par rapport à fin 2017 (9 %) – varie fortement d'un FAI à l'autre : chez certains opérateurs ce trafic ne constitue même pas 1 % du trafic vers les utilisateurs finals alors que pour d'autres, il constitue plus du tiers du trafic entrant injecté dans leurs réseaux.

Par ailleurs, le ratio de trafic entrant/sortant varie entre 1/5 et 1/20 en fonction de l'opérateur. Autrement dit, les données disponibles au niveau des CDN internes sont consultées entre 5 et 20 fois en moyenne.

RÉPARTITION DU TRAFIC ENTRE LES DIFFÉRENTS MODES D'INTERCONNEXION (FIN 2018)

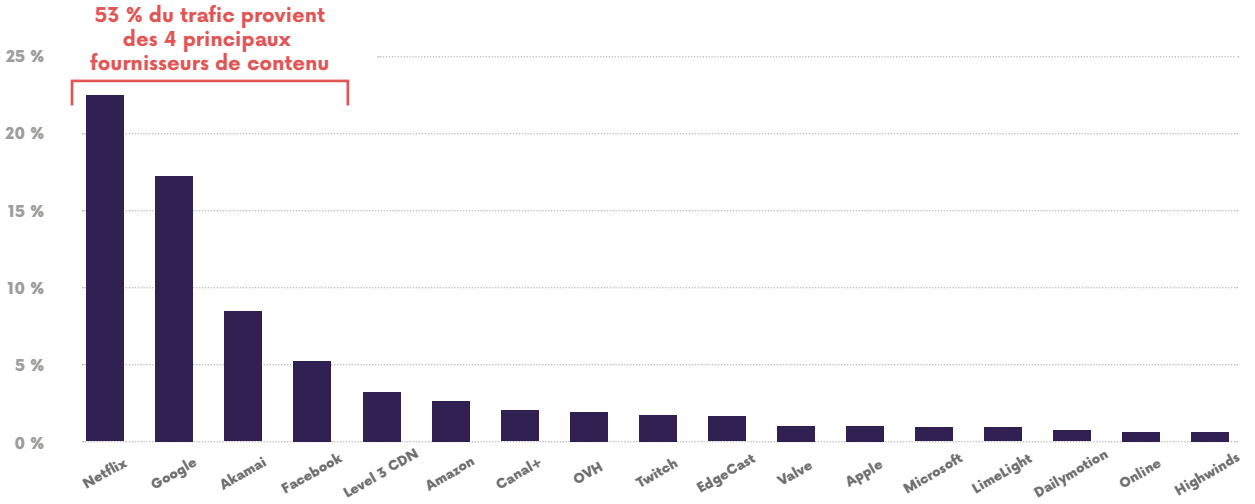


Source : Arcep

2.6. Décomposition du trafic selon l'origine

Plus de la moitié (53 %) du trafic vers les clients des principaux FAI en France provient de quatre fournisseurs : Netflix, Google, Akamai et Facebook. Ceci indique une concentration de plus en plus nette du trafic entre un petit nombre d'acteurs dont la position sur le marché des contenus est renforcée.

DÉCOMPOSITION DU TRAFIC EN FRANCE SELON L'ORIGINE POUR LES PRINCIPAUX OPÉRATEURS EN FRANCE (FIN 2018)



Source : Arcep

2.7. Évolution des tarifs

Les fourchettes de tarifs de transit et de *peering* n'ont pas connu d'évolution depuis l'année dernière.

Le transit se négocie toujours entre 10 centimes d'euro HT et plusieurs euros HT par mois et par Mbit/s. Quant au *peering* payant, il se situe dans une fourchette comprise entre 25 centimes d'euro HT et plusieurs euros HT par mois et par Mbit/s[5].

Dans la majorité des cas, les CDN internes sont gratuits. Néanmoins, il arrive que ceux-ci soient payants dans le cadre plus large de la prestation de *peering* payant que le FCA a contracté par ailleurs avec le FAI.

5. Les fourchettes de tarifs ne reflètent que les tarifs que les acteurs ayant répondu au questionnaire payent pour les prestations de transit, *peering* ou CDN internes.

PAROLE À...

Theresa Bobis, directrice régionale Europe du Sud, DE-CIX

Marseille, nouveau hub d'interconnexion, du numérique et du cloud

Les flux de trafic mondial traditionnels évoluent et se dirigent dorénavant vers le sud. C'est pourquoi DE-CIX a choisi d'établir, il y a plusieurs années, ses points d'échange internet dans le sud de l'Europe - notamment « DE-CIX Marseille » en 2015. Marseille est l'une des principales stations d'atterrissage européennes pour un grand nombre de câbles sous-marins internationaux et de voies de transit pour internet. En s'établissant ici, DE-CIX peut fournir des installations d'interconnexion neutres à l'intersection des principales routes sous-marines de la Méditerranée et des hubs continentaux européens.

En effet, la ville constitue une passerelle vers l'Europe de l'Ouest reliant les opérateurs du Moyen-Orient, d'Afrique et de l'Asie-Pacifique aux principaux nœuds d'interconnexion européens qui permettent d'accéder à l'internet mondial. Contrairement à la plupart des marchés dans lesquels DE-CIX investit, celui-ci est davantage influencé par l'augmentation de la demande d'acteurs géographiquement éloignés plutôt que par l'augmentation de la demande locale. Marseille est étroitement liée aux marchés d'Afrique, d'Asie et du Moyen-Orient. Ce sont d'ailleurs ces marchés qui consomment le plus de bande passante à l'échelle mondiale. Alors que la croissance de la demande mondiale en bande passante a ralenti au cours des cinq dernières années, chacune de ces régions a conservé une croissance annuelle de plus de 40 %. Et ce n'est pas près de s'arrêter. La demande en bande passante ne cesse de croître entre ces régions.

En s'établissant à Marseille, DE-CIX fournit des installations d'interconnexion neutres à l'intersection des principales routes sous-marines de la Méditerranée et des hubs continentaux européens. D'ici 2022, les capacités pourraient plus que quadrupler entre l'Europe et le Moyen-Orient, et être multipliées par six entre l'Europe et l'Afrique.

À Marseille, c'est tout un écosystème de l'interconnexion qui se développe. Ainsi, les clients de DE-CIX bénéficient d'économies d'échelle renforcées grâce à l'accès à plus de 130 partenaires d'interconnexion présents au campus MRS d'Interxion qui connaît un essor rapide. Le lancement des services Microsoft Azure dans la région France-Sud alimentera également la demande et les opportunités concernant l'environnement l'IXP. Pour les clients ayant besoin d'une connectivité permanente vers Francfort ou Paris, plusieurs opérateurs sont disponibles à Marseille. Leurs tarifs sont comparables à ceux proposés sur les grands marchés européens. Le service *DE-CIX GlobePEER Remote* de Marseille à Francfort offre une autre option de connectivité pour les clients qui ont besoin d'accéder au marché de Francfort – l'un des plus grands écosystèmes d'interconnexion dans le monde – mais qui préfèrent conserver leur localisation à Marseille.

La croissance de la demande provenant du Moyen-Orient et d'Afrique vers l'Europe indique que les opérateurs et fournisseurs de contenu européens devront se rapprocher de la périphérie du réseau pour s'adapter à ces marchés en forte croissance. Ce mouvement est déjà en cours, transformant Marseille en l'un des plus importants hubs européens de bande passante et d'interconnexion. Avec peu d'écosystèmes d'interconnexion prometteurs sur la route sous-marine vaste et très peuplée entre Singapour et l'Europe, Marseille continuera à être une destination attrayante pour les réseaux du bassin méditerranéen et cela pour les décennies à venir.

PAROLE À...

Bertrand Yvain, associé-fondateur, HOPUS

Interconnectés autrement : notre vision HOPUS pour le développement des réseaux

L'évolution des usages de l'internet se traduit par l'augmentation des débits et de l'interactivité. Ces deux besoins conduisent naturellement les fournisseurs de contenu et d'applications, moteurs de cette évolution par leur innovation, à se rapprocher des clients finals. Les différentes formes de convergence des acteurs de l'écosystème internet visent à accroître la performance et la fiabilité des réseaux, aussi bien en termes de bande passante que de latence. Ces changements s'illustrent par la part croissante qu'occupe le *peering,* en particulier payant, dans les interconnexions. Les transitaires sont de moins en moins pertinents pour les échanges de données fortement asymétriques, à une échelle locale. Cependant, la multiplication des accords de *peering* constitue une charge accrue sur le plan technique, commercial, et juridique.

HOPUS a pour mission de faciliter ces échanges, notamment à travers son réseau IP, hybride entre *peering* et transit. Ce réseau consiste en un intermédiaire, visant l'excellence technique et proposant une relation commerciale claire et prévisible, basée sur la distinction des trafics entrant et sortant. Ainsi, les acteurs raccordés payent pour le trafic qu'ils émettent et reçoivent une compensation pour la prise en charge de celui qu'ils reçoivent. Nous pensons que ce modèle économique permet d'accompagner sainement la croissance des réseaux. Il constitue également une forme d'arbitrage privé, permettant aux acteurs les moins puissants d'accéder aux bénéfices du *peering* privé et facilitant l'émergence de nouveaux fournisseurs de contenu et d'applications.

Durant les vingt dernières années, nous avons assisté à une transition de l'écosystème internet. Alors composé principalement d'acteurs intégrés, à la fois fournisseurs d'accès et de contenu, il voyait principalement des échanges symétriques. Désormais, l'essentiel du trafic provient d'acteurs spécialisés : fournisseurs de contenu et d'applications, hébergeurs, ou réseaux de diffusion de contenu. Leur trafic est à la fois en forte croissance et très nettement asymétrique. C'est un défi pour la construction des réseaux et l'occupation des capacités installées. La difficulté à le relever s'illustre par des congestions et des tensions entre les différents acteurs, qui mettent à mal la neutralité des réseaux.

« Le débit n'est plus le seul critère de qualité perçue. La latence est critique. »

Une des vertus de notre pratique commerciale est d'assurer un traitement égal à tous nos membres. La rémunération que chacun peut recevoir se justifie par des engagements de qualité quant à l'acheminement du trafic reçu. La reconnaissance de cette valeur nous paraît être la clef qui ouvre les vannes pour les débits toujours plus importants : réseaux 5G, internet des objets, multiplication des offres de *streaming,* etc.

La nature des contenus a également évolué. Ils étaient statiques, monolithiques et parfois consultés hors-ligne. La généralisation des terminaux mobiles et la place croissante donnée à l'interactivité les a rendus composites, dynamiques et personnalisés. Ces caractéristiques font que le débit n'est plus le seul critère de qualité perçue. La latence est critique pour rendre fluides les interactions avec les usagers. L'existence même des différents types de distribution de contenu l'illustre bien. L'amélioration de la latence est un axe fondamental du développement du réseau HOPUS, notamment par l'établissement de points de présence distribués au plus près des usagers. Elle profite directement à tous les types d'acteurs, sensibles à la satisfaction de leurs usagers.

La spécificité de la relation commerciale entretenue avec les membres nous interdit de faire appel à des transitaires, dont la logique n'est pas compatible avec nos engagements. Le réseau HOPUS n'est donc pas joignable par tout l'internet mais constitue une matrice fermée de réseaux connectés. C'est un avantage supplémentaire pour garantir la sécurité des échanges et se protéger des attaques par déni de service. Il s'ajoute au dimensionnement des circuits et à l'arsenal des outils désormais nécessaires à la bonne gestion des réseaux.

L'offre HOPUS se démarque des acteurs usuels de l'internet par son principe de fonctionnement. La rupture n'est pas technologique, mais une invitation à une nouvelle forme de coopération. Cinq ans d'existence de notre modèle alternatif confortent sa pertinence à soutenir l'évolution du marché, en tant que forme complémentaire dans la gestion des interconnexions.

3 Accélérer la transition vers IPv6

« La carence en IP s'accentue, prenez de toute urgence vos IPv6 »

2020

Selon les estimations actuelles de l'Arcep, le stock en adresses IPv4 sera épuisé en 2020

1. ACCÉLÉRATION DE LA PÉNURIE D'IPv4 : IPv6, UNE TRANSITION INDISPENSABLE

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, etc.) est adressable par une adresse IPv4. Le protocole IPv4, utilisé sur internet dès ses débuts, offre un espace d'adressage de près de 4,3 milliards d'adresses IPv4[1]. Or le succès d'internet, la diversité des usages et la multiplication des objets connectés ont eu comme conséquence directe l'épuisement progressif des adresses IPv4, certaines régions du monde étant touchées plus que d'autres. Les quatre principaux opérateurs français (Bouygues Telecom, Free, Orange, SFR) ont déjà affecté entre 88 % et 99 % des adresses IPv4 qu'ils possèdent, à fin juin 2018[2].

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 terrestre[3].

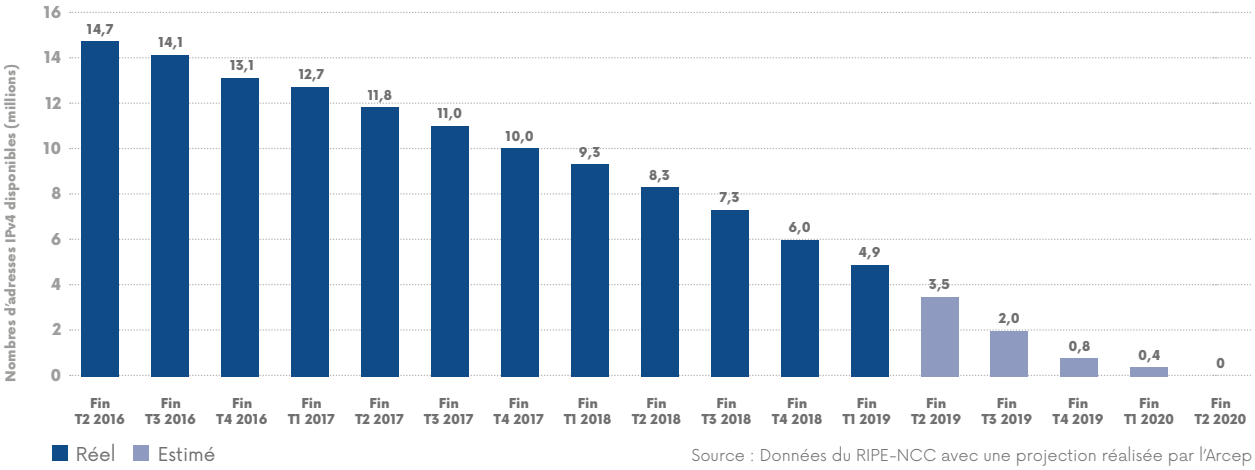
Du fait de la complexité actuelle d'internet, la migration d'IPv4 vers IPv6 ne peut se réaliser que progressivement, d'abord en parallèle d'IPv4 (phase de cohabitation), puis, quand tous les acteurs auront migré, en remplacement total d'IPv4 (phase d'extinction). La transition vers le protocole IPv6 a démarré en 2003. Cependant, en 2018, internet n'en est encore qu'au début de la phase de cohabitation[4].

La lenteur de la migration peut d'une part provoquer le dysfonctionnement de certaines catégories de services sur internet (systèmes de contrôle de maison connectée, jeux en réseau, etc.) du fait de systèmes de partage d'adresse IPv4 entre plusieurs clients mis en place pour faire face à la pénurie. D'autre part, elle est susceptible d'ériger une barrière à l'entrée à l'encontre des nouveaux acteurs du marché. En effet, IPv4 reste nécessaire tant que toute la chaîne technique d'internet n'aura pas migré entièrement vers IPv6. Dans le cas contraire, un site web 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. Or la date de fin de disponibilité des adresses IPv4 en Europe approche.

Dans l'édition 2018 de son rapport sur l'état d'internet en France, l'Arcep a estimé que l'épuisement du stock d'adresses IPv4 serait effectif fin 2021. Le rythme des acquisitions des derniers blocs d'IPv4 s'accélère et l'Arcep estime actuellement que cet épuisement est susceptible de se produire vers la fin du second trimestre de 2020[5].

1. Les adresses IPv4 sont codées sur 32 bits. Au maximum 232, soit 4 294 967 296 adresses peuvent donc être attribuées simultanément en théorie.
2. Données recueillies par l'Arcep auprès de FAI conformément à la décision n° 2018-0268 de l'Autorité en date du 15 mars 2018.
3. Les adresses IPv6 sont codées sur 128 bits. Au maximum 2 128 (soit environ 3,4 × 1 038) adresses peuvent donc être attribuées simultanément en théorie.
4. L'Arcep précise que les constats et travaux évoqués concernent uniquement le réseau internet et ne s'appliquent pas à l'interconnexion privée entre deux acteurs, notamment l'interconnexion des réseaux de deux opérateurs pour la terminaison d'appel vocal en mode IP.
5. Données du RIPE-NCC avec une projection réalisée par l'Arcep.

ÉVALUATION ET ESTIMATION DU STOCK D'ADRESSES IPv4 DISPONIBLES[6]



Source : Données du RIPE-NCC avec une projection réalisée par l'Arcep

L'Arcep a remis au Gouvernement en juin 2016 un rapport élaboré avec le concours de l'Afnic décrivant l'état d'IPv6 en France et proposant plusieurs leviers d'actions dans l'objectif d'accompagner et d'accélérer la transition. Depuis, elle publie chaque année son baromètre de la transition vers IPv6, dans une optique de régulation par la donnée. Elle a également amorcé une démarche de co-construction avec l'écosystème internet en France afin de fédérer la communauté et permettre d'accélérer cette transition.

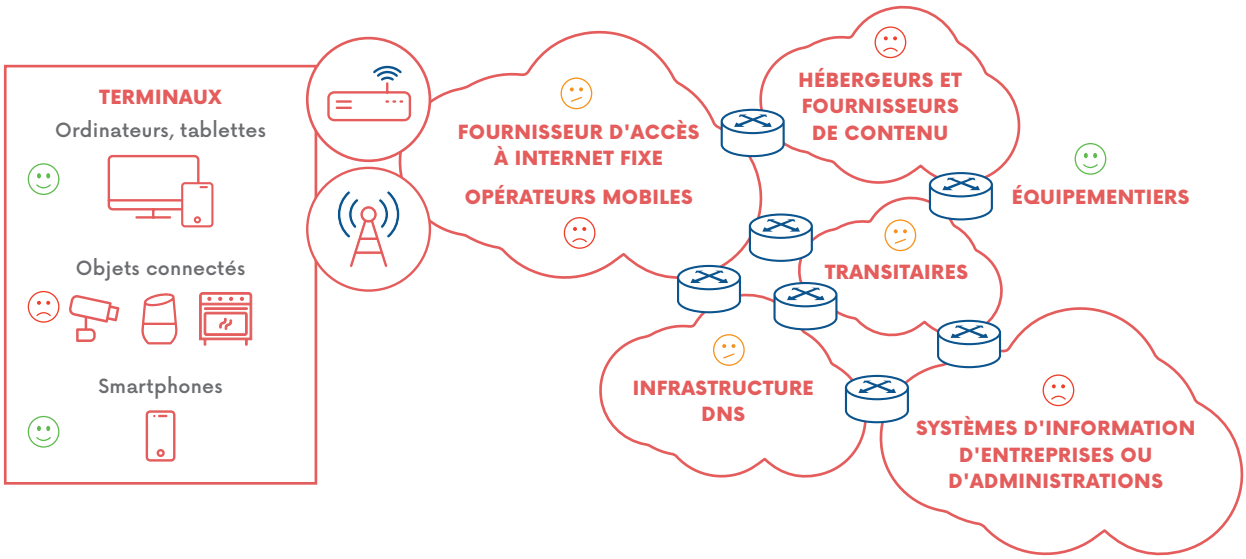
2. BAROMÈTRE DE LA TRANSITION VERS IPv6 EN FRANCE

Comme recommandé dans son rapport de juin 2016, l'Arcep publie un baromètre annuel de la transition vers IPv6 depuis décembre 2016. L'objectif est de mieux informer les utilisateurs sur ce sujet. Ce baromètre, qui compile à la fois des données produites et mises à disposition par des tiers (Cisco, Google et Afnic) et des données recueillies par l'Arcep directement auprès des principaux opérateurs français, donne un aperçu des progrès réalisés en France, ainsi que des prévisions de déploiement sur un et trois ans. L'Arcep a publié l'édition 2018 de ce baromètre le 10 octobre 2018.

L'Arcep a utilisé un certain nombre d'indicateurs différents pour évaluer l'état du déploiement d'IPv6 en France pour les différentes parties prenantes impliquées dans la transition. Comme exposé ci-après, les parties prenantes se trouvent à différentes étapes de la transition.

6. Simulation effectuée avec une interpolation polynomiale et en prenant pour hypothèse l'attribution de 1 024 adresses IPv4 par LIR jusqu'au dernier million d'adresses IPv4 disponible, puis 256 IPv4 par LIR jusqu'à épuisement. Avec les données RIPE du 2 avril 2019, la simulation donne une date de fin d'IPv4 le 17 juillet 2020.

ÉTAT D'AVANCEMENT DE LA TRANSITION VERS IPv6 AU NIVEAU DES DIFFÉRENTS MAILLONS DE LA CHAÎNE TECHNIQUE



Migration vers IPv6 totale ou élevée — Migration vers IPv6 partielle — Migration vers IPv6 faible ou nulle

Source : Arcep

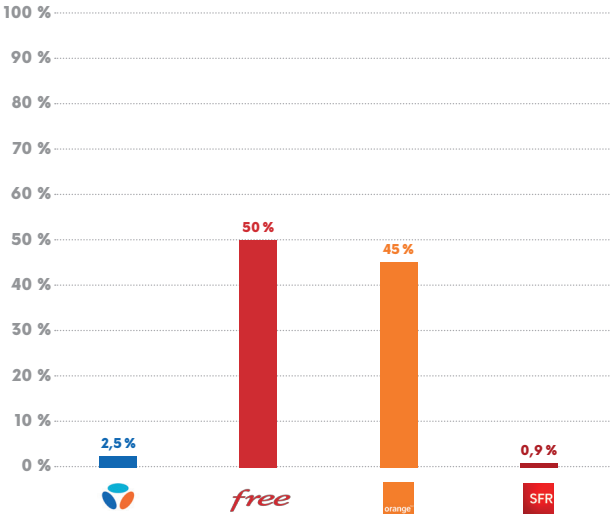
Les résultats confirment la progression du taux d'utilisation d'IPv6 en France qui a atteint 23 % au mois d'octobre 2018. Le baromètre montre en détail l'état de la transition au niveau de chaque acteur de l'écosystème.

2.1. Fournisseurs d'accès à internet fixe

Les schémas suivants exposent la situation actuelle du déploiement d'IPv6 ainsi que les prévisions au niveau du réseau fixe des principaux opérateurs en France.

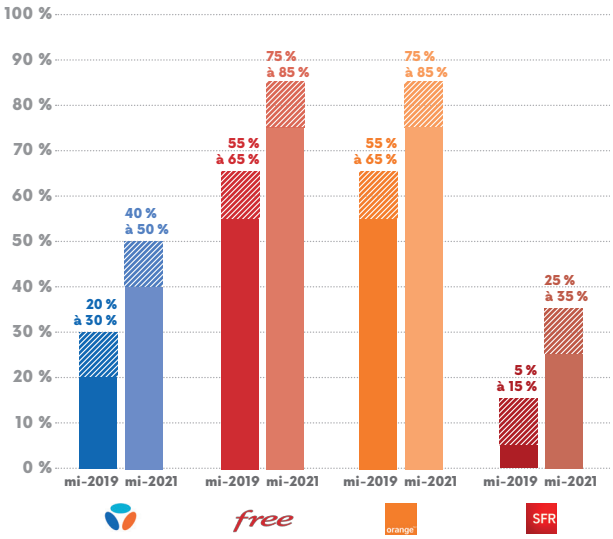
Alors que l'épuisement des adresses IPv4 est prévu au deuxième trimestre de 2020, certains acteurs n'envisagent pas un déploiement de l'IPv6 sur leurs réseaux fixes qui permettrait de répondre à la pénurie à moyen terme, ce qui, comme indiqué plus haut, apparaît problématique.

TAUX DE CLIENTS DU RÉSEAU FIXE ACTIVÉS EN IPv6 DES PRINCIPAUX OPÉRATEURS EN FRANCE



Source : Données à fin juin 2018, recueillies par l'Arcep auprès des opérateurs concernant leur réseau propre.

PRÉVISIONS DES TAUX DE CLIENTS DU RÉSEAU FIXE ACTIVÉS EN IPv6 DES PRINCIPAUX OPÉRATEURS EN FRANCE

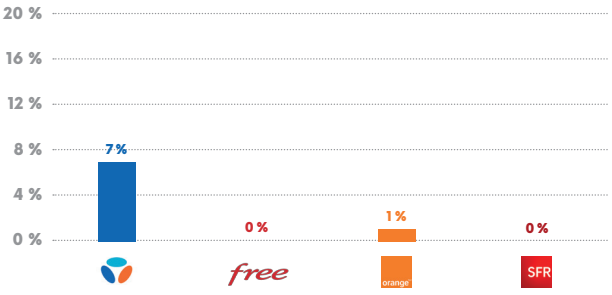


Source : Données recueillies par l'Arcep mi-2018, auprès des opérateurs concernant leur réseau propre. Chiffres susceptibles d'évoluer.

2.2. Opérateurs mobiles

Les schémas suivants exposent la situation actuelle du déploiement d'IPv6 ainsi que les prévisions au niveau du réseau mobile des principaux opérateurs en France.

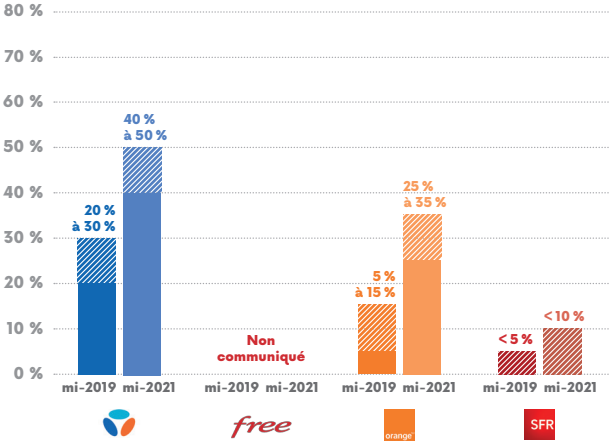
TAUX DE CLIENTS DU RÉSEAU MOBILE ACTIVÉS EN IPv6 DES PRINCIPAUX OPÉRATEURS EN FRANCE



Source : Données à fin juin 2018, recueillies par l'Arcep auprès des opérateurs concernant l'APN par défaut du smartphone des offres voix+data.

De façon encore plus marquée que sur les réseaux fixes, le rythme des déploiements futurs de l'IPv6 de la part des opérateurs mobiles risque fort de ne pas permettre de répondre au problème de pénurie générale d'adresses IPv4.

PRÉVISIONS DES TAUX DE CLIENTS DU RÉSEAU MOBILE ACTIVÉS EN IPv6 DES PRINCIPAUX OPÉRATEURS EN FRANCE



Source : Données recueillies par l'Arcep mi-2018 auprès des opérateurs concernant l'APN par défaut du smartphone des offres voix+data. Chiffres susceptibles d'évoluer.

Plus particulièrement :

- si 100 % des clients SFR sont déjà compatibles sur le xDSL et le FttH (0 % sur le câble), moins de 1 % d'entre eux sont activés – c'est-à-dire émettent et reçoivent effectivement en IPv6 –. Les activations à venir, bien qu'en hausse par rapport aux dernières annonces de l'opérateur, demeurent très insuffisantes (25-30 % à mi-2021). Une grande majorité des clients n'activant pas IPv6 manuellement, l'Arcep invite SFR à réaliser cette activation par défaut comme la plupart des autres opérateurs. Quant aux réseaux mobiles : SFR prévoit moins de 10 % de clients activés à mi-2021 ;
- l'Arcep note les efforts de déploiement de Bouygues Telecom sur les réseaux mobiles, mais regrette la chute des prévisions de migration sur les réseaux fixes : 40 à 50 % de clients activés sont prévus à horizon mi-2021, contre 75 à 85 % annoncés à fin 2020 dans le précédent baromètre ;
- sur les réseaux fixes, les taux actuels de clients activés de Free et Orange sont relativement élevés (respectivement 50 % et 45 %), mais les projections sur le même indicateur à mi-2021 ne permettent pas d'achever la transition à moyen terme (entre 75 et 85 % pour les deux FAI). Sur les réseaux mobiles, le taux de clients activés prévu par Orange à mi-2021 est en hausse mais demeure limité (25-35 %) ; l'Arcep regrette que Free Mobile n'ait pas été en mesure de lui transmettre des prévisions.

2.3. Hébergeurs web

Les hébergeurs de sites web représentent encore l'un des principaux goulots d'étranglement dans la migration vers IPv6 : sur les principaux sites visités par les Français selon le classement Alexa, seuls 26 % sont accessibles en IPv6[7]. On considère un site comme accessible en IPv6 lorsqu'il dispose d'un enregistrement IPv6 (« AAAA ») au niveau du serveur DNS.

Le taux de pages web accessibles en IPv6 (contenus IPv6) est, quant à lui, significativement plus élevé (61 %)[8]. La raison en est que les petits fournisseurs de contenu proposent souvent des sites web (au nombre de pages consultées généralement faible) non compatibles avec IPv6.

26 %
des sites les plus visités en France sont accessibles en IPv6

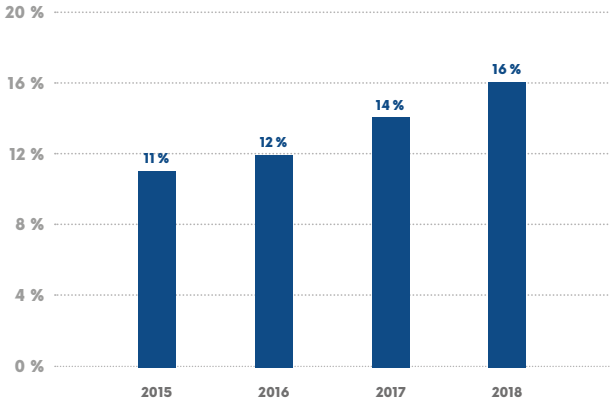
61 %
des pages web les plus visitées sont accessibles en IPv6

Source : Cisco 6lab au 28/09/2018 (6lab.cisco.com). Données sur le top 731 d'Alexa en France (www.alexa.com/topsites/countries).

7. Cisco 6lab au 08/10/2018 (http://6lab.cisco.com). Données sur le Top 731 d'Alexa en France www.alexa.com/topsites/countries
8. Ibidem.

Le taux de sites disponibles en IPv6 est uniquement de 16 % lorsque l'on considère les 3 millions de sites web en .fr, .re .pm .yt .tf et .wf[9]. Ce pourcentage est en augmentation depuis 2015, mais le rythme de cette évolution semble loin de pouvoir permettre une transition complète vers l'IPv6 d'ici le troisième trimestre de 2020.

ÉVALUATION DU TAUX DES SITES WEB ACCESSIBLE EN IPv6 SUR LES NOMS DE DOMAINE .FR, .RE, .PM, .YT, .TF ET .WF



Source : données Afnic à juillet 2018.

Pour plus d'information sur l'état de déploiement d'IPv6, le baromètre de la transition vers IPv6 est disponible sur le site de l'Arcep.[10]

Afin de tenir compte du retour d'expérience des acteurs sur la collecte d'information mise en place, la décision de l'Arcep n°2019-0287 en date du 12 mars 2019 relative à la mise en place d'enquêtes dans le secteur des communications électroniques a été mise à jour. Les principales modifications concernant la collecte d'informations pour le baromètre de la transition vers IPv6 ont consisté à :

- inclure les opérateurs disposant d'un nombre d'abonnement actifs entre 5 000 et 3 000 000 sur les marchés de détail grand public (fixe ou mobile) afin de permettre à l'Arcep d'améliorer sa connaissance de la transition au niveau de tous les opérateurs concernés ;
- spécifier pour le réseau mobile le nombre de clients IPv6-ready et activés par technologie et avoir plus d'information sur le partage d'adresse IPv4 afin d'améliorer la précision des informations publiées et mieux détecter les goulots d'étranglement éventuels ;
- simplifier le questionnaire pour les hébergeurs afin de demander que les informations qui alimenteraient le baromètre de la transition vers IPv6.

Ces évolutions permettront d'améliorer la qualité de l'information publiée par l'Arcep et de garantir une meilleure transparence sur les avancées de la transition. L'édition 2019 de ce baromètre sera publiée au second semestre 2019.

9. Données Afnic, juillet 2018.
10. https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/transition-ipv6/barometre-annuel-de-la-transition-vers-ipv6-en-france.html

PAROLE À…

Nicolas Guillaume, secrétaire général, AOTA

IPv6 : pour que toutes les innovations se développent en Europe

Selon plusieurs projections, le stock d'adresses IPv4 sera épuisé en Europe courant 2020, autant dire demain. Il est indispensable d'agir dès maintenant pour permettre à toutes les innovations de se développer et ne pas freiner la concurrence sur le marché des télécoms entre ceux qui auront des ressources IPv4 suffisantes et les nouveaux entrants.

À tel point qu'Apple a rappelé, dès l'été 2016, à sa communauté de développeurs qu'elle refuserait dans ses magasins d'applications toute application qui ne soit pas en mesure de ne fonctionner qu'en IPv6.

Autrefois leader en matière de pénétration d'IPv6, grâce notamment à l'action d'envergure de Free ou à plus petite échelle de Nerim, notre pays apparaît désormais à la traîne en termes d'adoption effective.

Si sur les réseaux fixes la migration vers IPv6 est engagée de longue date, la situation sur les réseaux mobiles est clairement en retrait.

Les prestataires d'hébergement et fournisseurs de services ne semblent pas encore avoir pris la pleine mesure des enjeux. De grandes plateformes de *cloud* ne proposent toujours pas de solutions IPv6 satisfaisantes par exemple. Twitter, pour ne citer que lui, n'offre pas d'interface IPv6 pour ses services. L'État lui-même n'est pas le meilleur exemple en la matière : le service d'impôts en ligne n'est toujours accessible qu'en IPv4.

Si bien que dans de nombreuses situations, des abonnés, pourtant en IPv6 sur l'accès, sont rebasculés par les réseaux en IPv4, pour être en mesure de joindre des services, effectuer des démarches administratives, ou dialoguer avec des utilisateurs finals dont les infrastructures ne savent pas gérer IPv6.

Nous assistons à une forte inertie du secteur de l'hébergement. En cause : l'attentisme de leurs clients professionnels pour lesquels il n'y a aucune incitation à privilégier IPv6. L'exemple type du serpent qui se mord la queue : les opérateurs constatent que bien que produit en IPv6, le trafic de leurs abonnés reste essentiellement IPv4. Les hébergeurs expliquent qu'il n'y a aucune raison d'inciter leurs clients à basculer sur IPv6 parce que ces derniers traitent essentiellement du trafic IPv4.

« Un changement de paradigme s'impose en privilégiant une approche concertée entre plusieurs acteurs à intérêts a priori divergents. »

On le voit, toute action purement sectorielle, sans approche concertée impliquant l'ensemble des parties prenantes, ne peut que déboucher sur des demi-succès… ou semi-échecs.

Pourtant, le « marché entreprises » est un facteur clé de succès pour une migration massive et effective vers IPv6. Ce n'est que parce que la couche services saura gérer nativement et efficacement IPv6 que les hébergeurs pourront basculer en IPv6 et que le trafic des FAI pourra devenir majoritairement IPv6. Les derniers acteurs récalcitrants, notamment sur le marché mobile, seront alors incités, de fait, à migrer vers IPv6.

Un changement de paradigme s'impose donc, en privilégiant une approche concertée entre plusieurs acteurs à intérêts a priori divergents.

Si le législateur peut intervenir pour créer des formes de « contraintes incitatives », l'Arcep pourrait préciser les conditions techniques nominales d'une interconnexion en mode IP, en privilégiant des signaux économiques incitant à un raccordement principal en IPv6.

L'État pourrait donner l'exemple, en privilégiant dans la commande publique des acteurs en mesure de proposer, pour l'accès un raccordement produit en IPv6, et pour les services (*cloud,* hébergement, développement d'applications) des solutions en mesure de ne fonctionner qu'en IPv6, avec bascule en IPv4 uniquement à titre temporaire.

Les opérateurs de proximité adhérents de l'AOTA souhaitent plus que jamais jouer un rôle essentiel pour accompagner les pouvoirs publics et l'Arcep dans cet effort collectif de migration effective vers IPv6 natif. Comment ? En accompagnant localement leurs clients – dont beaucoup de collectivités publiques qui doivent aussi donner l'exemple – et en les aidant à monter en compétence par des actions concrètes.

PAROLE À…

Cédric Schroerer, responsable infrastructures, Orne THD

Le déploiement d'IPv6 comme un accélérateur de croissance

Le déploiement d'IPv6 répond à deux problèmes majeurs que nous connaissions : la contrainte technique du CGNAT[1] faute d'adresses IPv4 suffisantes pour chacun de nos abonnés, et la multiplication des équipements dans les foyers.

En attendant l'IPv6, la guerre faisait rage sur nos routeurs CGNAT où les nouvelles connexions des uns déconnectaient celles des autres, impactant tous les services indifféremment. En plus de ternir notre image, notre équipe technique était saturée de problèmes issus du NAT. Des abonnés résignés étaient retournés sur des lignes ADSL préférant la stabilité au débit. Il fallait donc éliminer ce problème rapidement et définitivement.

La difficulté provenait du *provisioning*[2] de nos modems câbles. Ayant un parc hétérogène, avec un mélange de Cisco, de Technicolor, eux-mêmes subdivisés en plusieurs modèles… il était compliqué de dire à tous nos modems câbles « allez chercher vos /56 ». Il nous fallait à la fois de l'aide de nos équipementiers et de l'éditeur de notre solution de *provisioning*.

Point positif, nous avons gardé les *firmwares* d'origine du constructeur. Ainsi nos modems étaient déjà prêts pour l'IPv6 depuis le début… sans le savoir. Notre *provisioning* avec la norme DOCSIS nécessitait malgré tout de connaître les bons paramètres afin de dire au modem d'initier ses configurations DHCPv6-PD et SLAAC spontanément après son démarrage. Mais la difficulté provient d'un manque de documentation : l'IPv6 est géré sur le modem… mais personne ne sait comment le contrôler.

Les bons paramètres obtenus, tous nos modems commencent à émettre des requêtes pour obtenir de la connectivité IPv6. A l'aide d'un dhcp6-relay sur nos CMTS, nous redirigeons ces requêtes sur nos serveurs de *provisioning*. Mais rien ne passe. Il s'avère que notre solution logicielle de *provisioning,* pourtant changée il y a quelques mois, ne gère pas IPv6 (ou de façon très brouillonne), et son éditeur ne semble pas très préoccupé par le sujet.

« Nous avons compensé la lacune de notre SI avec un logiciel open-source et détourné nos requêtes DHCPv6 dessus. Une solution stable et transparente. »

L'idée m'est alors venue de tout simplement… installer un serveur DHCPv6 open-source connu (ISC). Après quelques lignes de configuration plus tard, nos CMTS renvoient les requêtes vers ce petit serveur, et c'est un succès ! Les modems prennent tous un bloc /56 pour les équipements du foyer et 3 IPv6 /128 (la patte *provisioning,* MTA/SIP et WAN) en quelques minutes à peine, et très vite le trafic IPv6 monte en flèche. Tout le parc était migré en quelques minutes !

Nous avons donc compensé la lacune de notre SI avec un logiciel *open-source* et détourné nos requêtes DHCPv6 dessus. Cette solution est stable et transparente.

Les effets sur notre clientèle se sont fait sentir dès le lendemain : la fluidité et la stabilité des connexions ont été confirmées par nos clients les plus regardants sur la qualité du service. Parallèlement les souscriptions augmentent.

Côté support technique, les appels et les emails se sont nettement calmés, permettant à nos techniciens d'agir enfin précisément et efficacement sur les problématiques d'un réseau câble. En effet, avant, difficile de savoir si les coupures provenaient d'un routeur qui coupait la session ou du modem câble qui bagotte, malgré des valeurs excellentes en bout de prise. Nos agents en régie ont eux aussi de l'IPv6 pour remonter sur n'importe quel modem sans le moindre proxy ou NAT. Ce sont maintenant des pare-feux qui régissent la sécurité qu'offraient les anciennes plages IPv4 privées, aussi bien au sein du foyer de chaque abonné que sur notre réseau opérateur.

OrneTHD a réussi son déploiement d'IPv6 chez tous ses abonnés grand public et professionnels. Nous espérons que d'autres déploiements similaires suivront.

1. Voir lexique.
2. Voir lexique.

3. LA CO-CONSTRUCTION AVEC L'ÉCOSYSTÈME POUR ACCÉLÉRER LA TRANSITION VERS IPv6

3.1. Atelier IP♥6

Le 10 octobre dernier, l'Arcep a organisé, en partenariat avec l'internet Society France, un atelier de travail dédié au partage d'expériences et de bonnes pratiques utiles à la transition vers IPv6. Réservé aux acteurs de l'écosystème – FAI, hébergeurs, organismes de formation, organismes publics, entreprises, etc. –, l'atelier était inscrit dans la dynamique du Forum de la gouvernance d'internet (ou *Internet Governance Forum*- IGF), organisé autour d'un événement principal et de plusieurs ateliers, aussi appelés Ateliers de l'Avenir Numérique (RGPD, cyber-sécurité, IPv6, etc.).

Grâce à un format original (à mi-chemin entre une réunion multilatérale et une conférence), l'atelier IP♥6 a donné lieu à des groupes de travail multi-parties prenantes qui ont échangé sur des thèmes concrets liés à la transition d'IPv4 vers IPv6. Cet événement s'est articulé autour de deux sessions de trois ateliers en parallèle :

- la première session a abordé la transition vers IPv6 du point de vue des différents acteurs impliqués : FAI et constructeurs de terminaux, hébergeurs ainsi qu'organismes publics et entreprises. Les ateliers de travail ont permis de recenser les problèmes spécifiques à chaque type d'acteur ainsi que les pistes d'actions pour prévenir ou répondre à ces problèmes ;
- la seconde a permis de traiter des sujets plus transverses intrinsèquement liés à la transition vers IPv6 : qualité de service et sécurité d'IPv6, enseignement d'IPv6 et préparation de la fin d'IPv4. Les discussions ont mis en exergue les problèmes communs à tous les maillions de la chaîne technique ainsi que les éventuelles solutions à mettre en place.

3.2. Restitution de l'atelier[11]

Les résultats de ces ateliers sont résumés dans le tableau suivant[12] :

Principaux problèmes détectés	Pistes d'actions émergeant de l'écosystème
- Difficultés de fonctionnement liés aux CGN, ou aux sites internet, applications et objets connectés qui ne sont pas compatibles. - Manque de rentabilité d'IPv6 à court terme et manque de visibilité sur le retour sur investissement à plus long terme (manque de visibilité sur le coût de la transition ou de la non-transition). - Manque de formation du personnel et de compétence du support en IPv6. - Manque d'intérêt sur IPv6 et faible demande de la part des clients. - Problèmes de qualité de service liés à la dégradation du trafic au niveau de certains équipements et des problèmes d'interconnexion en IPv6. - Manque de connaissance sur la sécurité d'IPv6 et faible maturité des solutions techniques. - Manque de retours d'expérience sur la migration vers IPv6. - Complexité du maintien du Dual-Stack[13].	- Créer une Task Force IPv6 et un espace d'échange pour permettre le partage d'une manière régulière des retours d'expérience sur le déploiement d'IPv6 et les problèmes qui peuvent être rencontrés. - Promouvoir les acteurs qui proposent de l'IPv6 (par exemple via le baromètre de l'Arcep consacré à cette question) et inciter les acteurs à communiquer sur leurs offres IPv6 au grand public (obligation pour les FAI d'informer le client final de la présence d'IPv6 et d'IPv4/v6 fixes ou de la présence de CGN). - Effectuer des campagnes de sensibilisation auprès des acteurs de l'écosystème internet ainsi qu'auprès des directeurs des systèmes d'information et des comités de direction afin d'inclure IPv6 dans les appels d'offres. - Améliorer le catalogue de formations IPv6 et émettre des recommandations sur les architectures et la mise en place d'IPv6. - Définir au niveau national un calendrier de la transition : planning ou stratégie nationale de transition. - Labelliser les équipements et les terminaux pour garantir leur compatibilité IPv6 et leur bon fonctionnement et standardiser un certain nombre d'indicateurs IPv6 afin de suivre l'évolution du déploiement du protocole et d'évaluer l'impact d'IPv6 sur la qualité de service. - Établir un code de conduite limitant le partage d'adresse IPv4 au niveau des CGN. - Mettre en place des dispositions incitatives pour encourager les acteurs à choisir IPv6. - Émettre des recommandations communes / prévoir des actions coercitives pour accélérer la transition vers IPv6.

3.3. Les suites de l'atelier : mise en place d'une Task-Force IPv6 et d'une plateforme d'échange

Dans la continuité de l'atelier IP❤6, l'Arcep a décidé d'initier la création d'une Task-Force IPv6, co-pilotée avec Internet Society, qui associe les acteurs qui le souhaitent (opérateurs, hébergeurs, entreprises, secteur public, etc.). Objectifs : permettre aux participants d'aborder des problèmes spécifiques et partager les bonnes pratiques afin d'accélérer la transition vers IPv6.

La Task-Force se réunira deux fois par an à partir du second semestre de 2019. Les personnes qui ont un retour d'expérience à partager ou bien qui ont l'intention de mettre en place IPv6 sont invitées à faire part à l'Arcep de leur intérêt via le formulaire suivant : https://www.arcep.fr/la-regulation/grands-dossiers-internet-et-numerique/lipv6/suivi-de-la-fin-de-lipv4/appel-a-candidature-task-force-ipv6-en-france.html. En parallèle des réunions semestrielles, l'Arcep et Internet Society étudient la mise en place d'une plateforme en ligne permettant l'échange entre les différents acteurs, en vue d'alimenter les travaux de la Task-Force.

Les priorités des actions à mettre en place seront établies en concertation avec la communauté des participants à la Task-Force.

11. https://www.arcep.fr/uploads/tx_gspublication/compte_rendu-atelier-IPv6-fev2019.pdf
12. Cette restitution n'est pas une prise de position de l'Arcep sur la pertinence, la faisabilité ou la priorité des actions. Elle décrit uniquement les informations remontées par les différents acteurs de l'écosystème ayant participé aux ateliers. Un travail de priorisation des actions à mettre en place pourra être mené en tant que de besoin par l'Arcep en concertation avec la communauté des participants.
13. Double pile IP : consiste à affecter une adresse IPv4 et une adresse IPv6 à un équipement du réseau.

PAROLE À…

Franck Pflieger, président de l'IPv6 Council Martinique, gérant de GALACTUS Technologie et fondateur de l'association ASPIK

IPv6 dans les Antilles-Guyane : un facteur essentiel de la transformation numérique, gage d'un nouvel essor économique

IPv6 est un moyen de garantir le développement de l'innovation sur internet. Il est par conséquent gage d'un nouvel essor économique.

De plus, IPv6 est une brique essentielle de l'IoT, base de la transformation numérique des industries, des entreprises et des services publics.

Depuis plus de quinze ans, GALACTUS Technologie organise aux Antilles et en Guyane des ateliers sur des thématiques liées aux technologies d'avant-garde, tel qu'IPv6. Ces ateliers ont abouti, entre autres, à la création de l'association ASPIK, une association industrielle composée de plus de 40 membres (opérateurs de télécommunication, groupes industriels et sociétés de services). Active dans les départements de la Martinique, de la Guadeloupe et de la Guyane, cette association poursuit un triple objectif :

- favoriser les échanges de compétences liées aux métiers de la cybersécurité, de la transformation numérique et de tous métiers liés aux innovations technologiques aux Caraïbes ;
- développer la coopération des métiers de l'informatique dans les Caraïbes ;
- et promouvoir la place des femmes dans le secteur du numérique.

« Saint-Barthélemy est dans le Top 5 des territoires dans lesquels IPv6 est le plus déployé ; Saint-Martin dans le Top 30. »

En juin 2016, ASPIK a organisé le premier événement IPv6 en Martinique. Une étape importante, puisque depuis ce séminaire, les différents participants, opérateurs mobiles et fixes, sociétés de services ont des objectifs concrets de développement de la technologie IPv6 au sein de leur entreprise.

Par ailleurs, le Forum IPv6 accueille la Martinique depuis 2016. L'IPv6 Council Martinique s'est constitué à cette occasion. Objectif du Forum IPv6 : promouvoir le déploiement et l'adoption du nouvel internet à l'aide du protocole IPv6.

Pour reprendre les mots de Latif Ladid, président du Forum IPv6, *« L'IPv6 Council Martinique a été créé pour étendre la communauté internet à une voix forte. Il œuvrera en faveur de l'accès égal au savoir et à l'éducation sur les technologies internet de nouvelle génération et à la dynamique de déploiement IPv6 ».*

Ces initiatives portent leurs fruits. Depuis plusieurs mois, on constate, notamment sur le site d'Akamai[1], que Saint–Barthélemy est dans le Top 5 des pays dans lesquels l'IPv6 est le plus déployé ; Saint-Martin fait partie du Top 30… Une belle revanche sur l'ouragan Irma.

Afin d'accélérer encore plus la transition vers IPv6 dans la région, un prochain atelier sur l'IPv6 sera organisé en Guadeloupe du 18 au 22 novembre 2019 avec la présence des équipes de l'Arcep et de l'*Internet Society France*[2].

1. https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp
2. https://galactus.fr/ipv6_event/

PAROLE À...

François Contat, chef du laboratoire de la sécurité des réseaux et des protocoles, ANSSI
Arnaud Ebalard, expert du laboratoire de la sécurité des réseaux et des protocoles, ANSSI

IPv6 : un changement de paradigme à anticiper et à maîtriser

LA TRANSITION VERS IPv6 EST-ELLE INÉLUCTABLE ?

Oui, d'ailleurs la plupart des acteurs majeurs de l'internet sont aujourd'hui totalement compatibles avec IPv6. IPv4 a perduré grâce à des palliatifs qui atteignent aujourd'hui leurs limites. La place de plus en plus importante des objets connectés ou encore la pénurie d'adresses IPv4 concourent à la nécessité de prendre en compte rapidement IPv6 et d'y participer.

QU'EST-CE QU'IPv6 CHANGE CONCRÈTEMENT POUR L'ACCÈS INTERNET RÉSIDENTIEL DU CITOYEN ?

Pour l'utilisateur final, l'apparition d'IPv6 sur son accès résidentiel constitue un changement de paradigme, important à comprendre et anticiper. Les solutions techniques permettant de limiter la pénurie d'adresses IPv4 comme la translation d'adresse réseau (NAT) rendaient, jusqu'à présent, les équipements connectés difficilement accessibles depuis l'extérieur de son domicile. L'activation d'IPv6 se traduit par la fourniture automatique d'adresses accessibles depuis internet, à l'ensemble des équipements du réseau (télévision, caméra, ampoule ou interrupteur connectés, console de jeu, etc.), ce qui les expose au monde extérieur. Sans précaution particulière de la part de l'opérateur et de l'utilisateur, le réseau domestique privé en IPv4 devient un lieu exposé au public en IPv6.

QUELS SONT LES CHANGEMENTS POUR UNE ENTREPRISE OU UN FOURNISSEUR D'ACCÈS À INTERNET ?

Les grandes entreprises bénéficieront d'avantages importants lors du passage à IPv6. Actuellement, elles doivent travailler avec un espace d'adressage privé limité. Cet aspect d'IPv4 ainsi que les mesures de contournement associées (la NAT notamment) ont un coût humain et matériel important, notamment lors d'évolutions du réseau, de l'intégration de nouvelles filiales, etc. L'arrivée, avec IPv6, d'espaces quasi illimités d'adresses locales uniques (ULA) constitue un outil permettant de conserver une infrastructure interne stable et surtout évolutive.

Pour les fournisseurs d'accès internet, la transition de leur réseau à IPv6 est déjà effective. Leur principal défi aujourd'hui concerne la mise en œuvre de moyens techniques temporaires, la NAT à grande échelle par exemple (CG-NAT), devant permettre aux clients IPv4 de continuer à croître malgré la pénurie effective d'adresses publiques. L'autre aspect important concerne le maintien, durant un temps long, des mécanismes de transition entre les deux versions du protocole. D'un point de vue sécurité, le changement de paradigme pour les clients, nécessitera un accompagnement par les opérateurs pour éviter de subir les effets de l'ouverture des réseaux résidentiels et de l'augmentation du nombre d'équipements non supervisés. Ceci dans un contexte où les attaques en déni de service (DoS) sont incessantes et pour lesquelles ces équipements peuvent être utilisés comme moyen d'attaque.

IPv6 AMÉLIORE-T-IL INTERNET ?

IPv6 a été conçu pour gommer les défauts visibles d'IPv4 (espace d'adressage limité, aspects liés à la fragmentation, taille des tables de routage, etc.) et devrait donc permettre d'accompagner la croissance d'internet. Par exemple, la table de routage IPv6 est aujourd'hui dix fois plus petite que celle d'IPv4. En outre, le besoin en traduction d'adresse devient marginal en IPv6 et permet d'alléger la consommation de ressources dans les équipements et infrastructures qui y ont recours, comme par exemple dans les réseaux mobiles. Finalement, la croissance du nombre d'équipements sur les réseaux, et la facilité d'y accéder permises par IPv6, constituent des défis majeurs en terme de sécurité qui sont liés au déploiement du protocole ; d'autant plus lorsqu'une part importante de ces nouveaux équipements n'est pas supervisée. Ainsi, même si les scans deviennent plus complexes à mettre en œuvre pour les attaquants sur des réseaux IPv6 du fait de l'espace d'adressage étendu ou des mécanismes de randomisation d'adresse, il n'est pas certain que cela suffise à protéger totalement le réseau.

QUELS SONT LES POINTS D'ATTENTION PARTICULIERS LORS DE LA TRANSITION VERS IPv6 ?

Lors du passage à IPv6, il est nécessaire de décliner de façon adaptée les moyens de protection (pare-feu, IDS), de suivi du réseau, services et équipements (syslog, SNMP, etc.) mis en place précédemment pour IPv4. Il convient également de prendre en compte les spécificités du protocole. Par exemple, pour les réseaux locaux sur lesquels un administrateur a déployé du DHCP *snooping* ou des mécanismes anti-*spoofing*, une solution spécifique doit être mise en place.

Veiller à l'ouverture d'internet

4.
GARANTIR LA NEUTRALITÉ D'INTERNET

5.
CONTRIBUER À L'OUVERTURE DES TERMINAUX

4

Garantir la neutralité d'internet

« Le bilan de santé est positif, le régime doit être maintenu pour prévenir une éventuelle rechute »

56000
tests ont été effectués à ce jour en France avec l'application Wehe

Depuis 2016, le législateur européen protège la neutralité du net, en reconnaissant dans son règlement sur l'internet ouvert[1] notamment :

- le droit des utilisateurs « d'accéder aux informations et aux contenus et de les diffuser, d'utiliser et de fournir des applications et des services et d'utiliser les équipements terminaux de leur choix, quel que soit le lieu où se trouve l'utilisateur final ou le fournisseur, et quels que soient le lieu, l'origine ou la destination de l'information, du contenu, de l'application ou du service, par l'intermédiaire de leur service d'accès à l'internet » ;
- le devoir des fournisseurs d'accès internet de traiter « tout le trafic de façon égale et sans discrimination, restriction ou interférence, quels que soient l'expéditeur et le destinataire, les contenus consultés ou diffusés, les applications ou les services utilisés ou fournis ou les équipements terminaux utilisés ».

En France, c'est l'Arcep qui est chargée de sa mise en œuvre, et veille à son respect par les fournisseurs d'accès à internet (FAI).

1. L'ARCEP S'ENGAGE AU NIVEAU EUROPÉEN

L'année 2018 a été l'année du bilan sur l'application du règlement internet ouvert n° 2015/2120 et sur la mise en œuvre des lignes directrices publiées par le BEREC pour éclairer les autorités de régulation nationales (ARN) dans le suivi de la mise en œuvre du règlement. Ce bilan, réalisé dans le cadre de la coopération régulière entre les ARN, s'est appuyé sur les contributions reçues lors d'une consultation publique des différents acteurs du secteur. Il a fait l'objet d'un avis du BEREC à destination de la Commission européenne publié en décembre 2018[2]. Cet avis dresse un bilan sur l'application du principe de neutralité du net en Europe et détermine une liste des clarifications possibles à apporter au cadre législatif actuel. L'objectif est ainsi de réduire le risque d'une interprétation divergente de la législation en vigueur par l'ensemble des acteurs qui participent au fonctionnement de l'internet en France et en Europe. Au sein du BEREC, l'Arcep contribue activement aux discussions sur les éventuelles clarifications à apporter aux lignes directrices du règlement internet ouvert.

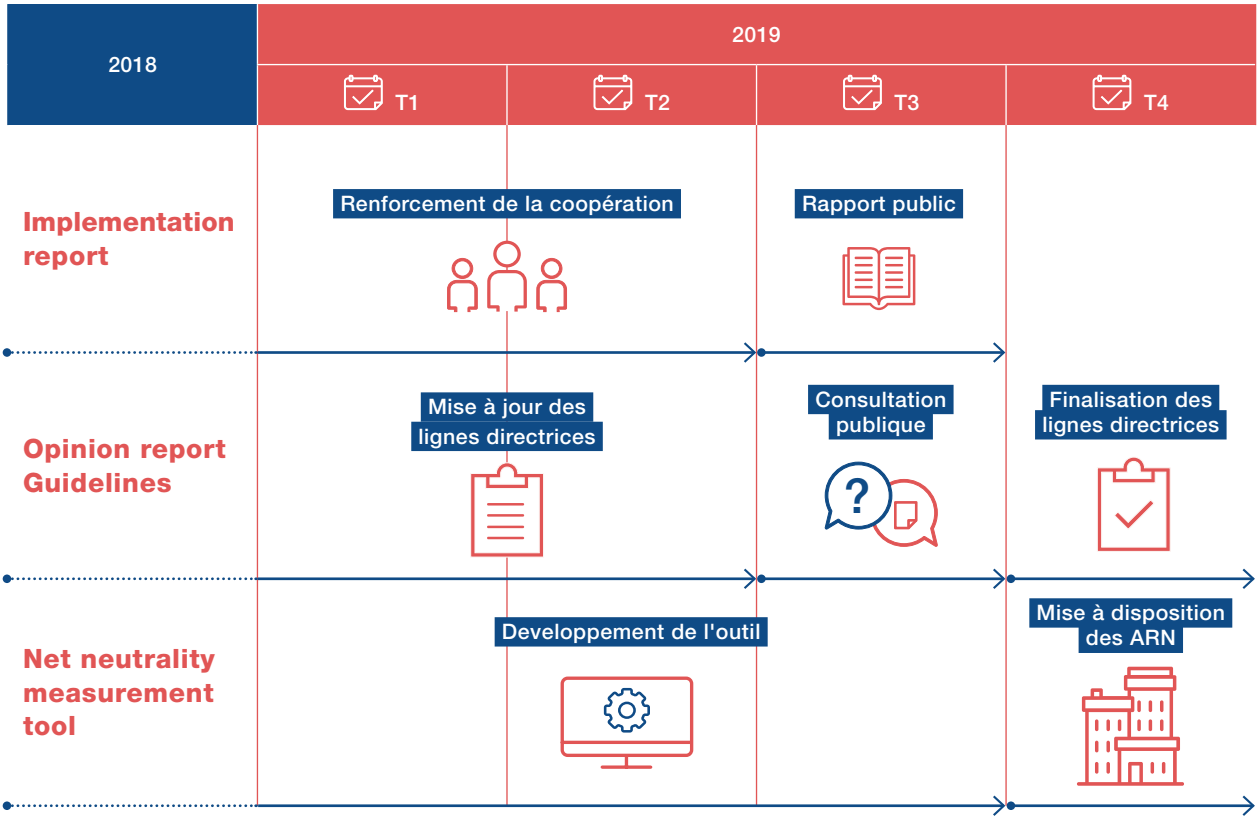
Un des points d'attention pour l'Arcep et les autres ARN porte sur l'application de la neutralité du net aux offres dites de *zero-rating*[3]. Les offres de *zero-rating* proposées dans les différents États membres portent principalement sur des applications ou des catégories d'application de musique, vidéo en ligne ou de réseaux sociaux populaires. Ces pratiques ne sont pas interdites *per se* par le règlement européen, mais peuvent engendrer un traitement discriminatoire au profit d'applications ou de catégories d'applications. La consommation d'une application à prix nul crée une incitation économique à son utilisation au risque que cette consommation orientée se fasse au détriment des applications concurrentes. Il apparaît donc souhaitable de clarifier les modalités d'évaluation par les ARN de ces offres et de leurs impacts sur le marché et les droits des utilisateurs finals. Ces pratiques feront d'ailleurs l'objet d'un premier examen par la Cour de Justice de l'Union Européenne (CJUE) suite aux questions préjudicielles posées par le juge hongrois. La réponse apportée par la Cour à ces questions permettra de clarifier les modalités d'examen des offres de *zero-rating* prévues par les lignes directrices.

L'avis du BEREC aborde également la question de la différenciation de qualité de service par classes d'accès. Les lignes directrices permettent en effet aux FAI de fournir différents services d'accès à internet qui se distinguent par des caractéristiques techniques telles que le volume de données accessible ou le débit internet, sous certaines conditions. Cette question est suivie de près par l'Arcep afin de favoriser l'innovation dans les réseaux sans risque de créer un internet à deux vitesses.

1. https://www.arcep.fr/fileadmin/reprise/textes/communautaires/reglement-UE-2015_310-Net-Neutralite-251115.pdf
2. L'avis du BEREC publié le 6 décembre 2018 sur l'évaluation de l'application du règlement européen n° 2015/2120 et des lignes directrices du BEREC sur la neutralité d'internet : https://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/8317-berec-opinion-for-the-evaluation-of-the-application-of-regulation-eu-20152120-and-the-berec-net-neutrality-guidelines
3. Voir lexique.

Enfin, les réflexions menées au BEREC ont porté sur l'adéquation du principe de neutralité du net avec les avancées technologiques de la 5G. Les acteurs du secteur manifestent régulièrement leurs interrogations quant à la compatibilité du principe de neutralité du net avec l'arrivée de la 5G. Le BEREC conclut dans son avis que le règlement internet ouvert est technologiquement neutre et s'applique donc sans obstacle majeur à la technologie 5G, de la même façon qu'il s'est appliqué aux technologies antérieures 2G, 3G et 4G. Il indique notamment considérer que le règlement internet ouvert laisse une marge de manœuvre importante pour l'implémentation des technologies 5G telles que le *network slicing* ou le *mobile edge computing*. Il affirme enfin ne pas avoir reçu d'exemple concret où le développement de la 5G est susceptible d'être freiné par le règlement internet ouvert.

CALENDRIER DE TRAVAIL DU BEREC EN MATIÈRE DE NEUTRALITÉ DE L'INTERNET



2. TRAVAUX EN COURS

2.1. Un nouvel outil de diagnostic

Dans la continuité de ce qui était annoncé dans le rapport sur l'état d'internet en France 2018, l'Arcep s'est attaché à enrichir la détection des pratiques, en accompagnant le développement d'un outil issu de la recherche universitaire capable de détecter des pratiques de gestion de trafic. Cette fonctionnalité, délicate à mettre en œuvre techniquement est absente des outils jusqu'alors disponibles sur le marché.

Cet outil appelé Wehe, développé par la Northeastern University, est disponible pour tous les consommateurs *via* une application mobile sur Android et iOS. L'outil mesure et compare les temps de parcours du trafic pour certains services. L'outil évalue, au niveau des couches réseau, la différence entre le temps de parcours du trafic réel et celui d'un trafic similaire mais « brouillé ». Si les résultats pour une même source s'avèrent sensiblement différents de manière répétée et concordante, et que le problème n'est pas conjoncturel mais bien structurel, il est possible de soupçonner une intervention de l'opérateur sur le trafic. L'utilisateur pourra le cas échéant décider d'informer l'Autorité, qui sera alors en mesure d'approfondir les signalements transmis. Ce nouvel outil distribué s'inscrit dans la démarche de *crowdsourcing* de l'Autorité. Il participe en effet à l'*empowerment* du consommateur, faisant de chacun un participant intégral de la régulation à même de venir contribuer au faisceau d'indices déclenchant les actions de l'Autorité.

PAROLE À…

Dave Choffnes, directeur de recherche, Northeastern University

Wehe : l'outil de détection de bridage en crowdsourcing

Dans une lutte constante qui oppose les intérêts commerciaux des opérateurs à ceux des fournisseurs de contenu et à la liberté des utilisateurs d'accéder à internet sans restrictions artificielles, la neutralité de l'internet est devenue le cri de ralliement pour garantir un internet libre et ouvert aux générations futures.

Les lois constituent un pas important vers la neutralité du net, mais elles ne se suffisent pas à elles seules. En effet, les réglementations sans mécanisme d'audit ne sont pas garanties. Auparavant, les régulateurs et les utilisateurs finals n'avaient pas à disposition d'outils fiables et indépendants pour détecter les potentielles violations à la neutralité d'internet. Un outil comme Wehe permet de donner un moyen supplémentaire afin d'offrir plus de transparence aux utilisateurs sur la politique de leur fournisseur d'accès à internet et de suivre l'application des règlements en vigueur. Avec l'Arcep, nous poursuivons ce double objectif : fournir une application que tout internaute peut utiliser pour détecter de potentielles violations de la neutralité du net et mettre à disposition des tableaux de bord permettant aux utilisateurs et aux régulateurs de consulter les données remontées par l'outil dans le monde entier.

Notre application Wehe a été installée par plus de 125 000 utilisateurs dans le monde. Depuis janvier 2018, les utilisateurs ont effectué collectivement plus de 1 000 000 tests de neutralité du réseau pour plus de 2 700 réseaux de 183 pays différents. Nous avons officiellement lancé notre application en France en novembre 2018. À ce jour, les Français ont effectué plus de 56 000 tests – un record après les États-Unis ! – Les résultats remontés par l'application sont régulièrement mis à jour sur https://dd.meddle.mobi/globalStats.html. Les résultats pour la France sont consultables sur https://dd.meddle.mobi/StatsFrance.html.

QUEL BILAN POUVONS-NOUS TIRER DES RÉSULTATS ?

Au 26 janvier 2019, Wehe avait détecté une limitation ou un blocage de 30 FAI dans sept pays. La quasi-totalité des cas de limitation détectée affectent les services de diffusion vidéo, et majoritairement Youtube (25 cas). Wehe a également détecté un bridage des tests vidéo de l'application Skype chez deux FAI situés aux États-Unis : Sprint et Boost Mobile (également propriété de Sprint).

Par ailleurs, le débit de bridage détecté le plus courant est de 1,5 Mbps (12 cas). Ce débit correspond généralement à celui offert par les FAI dont les abonnements prévoient la diffusion de vidéo bloquée en basse résolution.

« En France, Wehe n'a détecté jusqu'à présent aucun bridage. »

Pour la grande majorité des réseaux fixes testés (les tests sont réalisés en connectant l'application mobile au réseau fixe via Wi-Fi), Wehe n'a détecté aucune différenciation. La quasi-totalité des bridages détectés sont donc sur des réseaux mobiles. De plus, la grande majorité des cas proviennent de fournisseurs d'accès à internet aux États-Unis, où il est légalement possible de passer outre la neutralité du net (au moment de la rédaction de cet article).

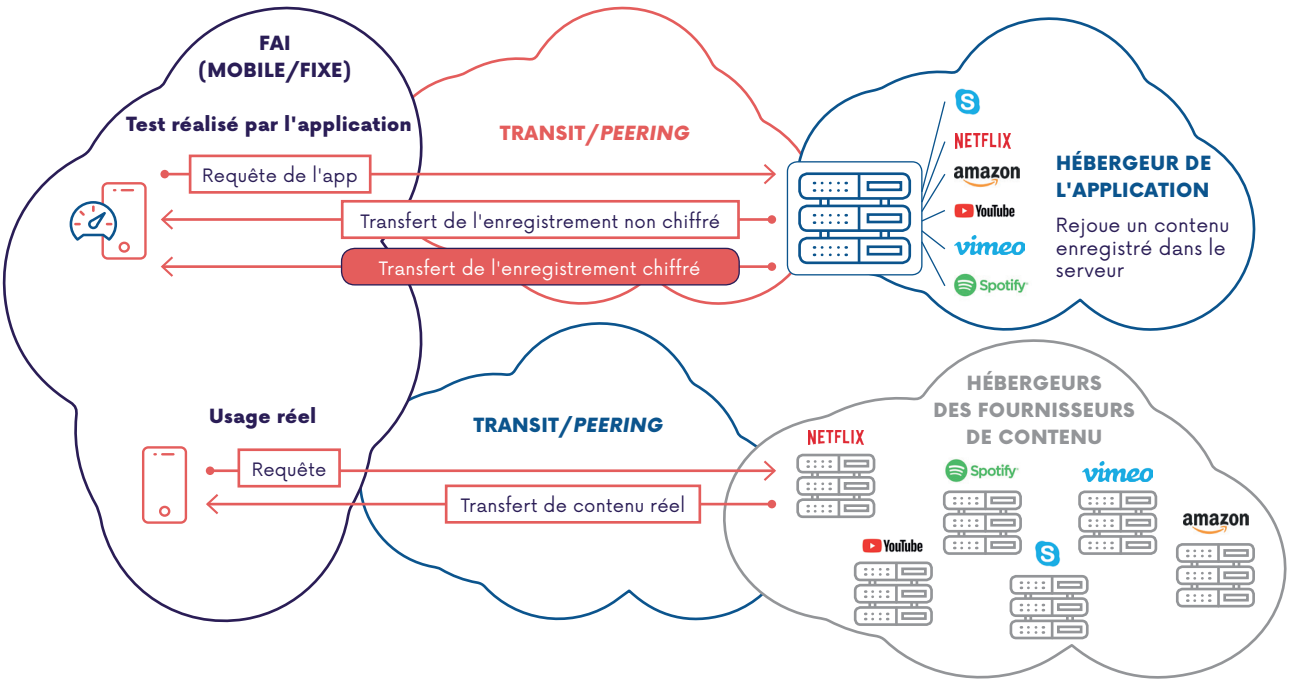
Wehe a aussi détecté un phénomène de "bridage retardé", dans lequel un FAI (T-Mobile US dans ce cas précis) donne un débit non bridé à une application pour les premiers mégaoctets échangés, puis bride ensuite la connexion. Bien que cela puisse réduire les délais de démarrage de la vidéo, cette technique entraîne également une certaine inefficacité lors du transfert de données car le FAI détruit des paquets lorsque le bridage démarre.

En France, Wehe n'a détecté jusqu'à présent aucun bridage. Cela semble indiquer que les FAI français sont respectueux de l'interdiction des pratiques basées sur la différenciation de contenu (pour les applications populaires testées). Toutefois, il n'est pas possible d'être catégorique sur le fait qu'ils respectent entièrement le règlement européen en matière de neutralité de l'internet.

QUELLES ÉVOLUTIONS POUR WEHE ?

Les travaux sur le projet Wehe se poursuivent. Pour offrir une portée mondiale à notre outil, nous étendons notre infrastructure, nous intégrons plus d'applications afin de tester la différenciation sur plus de contenus, nous effectuons des recherches pour mieux comprendre l'impact des atteintes à la neutralité du net… Enfin, nous cherchons également à travailler avec d'autres régulateurs, dans d'autres juridictions, en nous appuyant sur notre expérience fructueuse avec l'Arcep.

FONCTIONNEMENT DE L'APPLICATION DE DETECTION WEHE



Source : Arcep

Concrètement, le partenariat entre la Northeastern University et l'Arcep s'est matérialisé par plusieurs avancées majeures dans les briques principales de l'outil : fiabilisation de la détection de faux positifs, développement de la détection automatique des règles de *Deep Packet Inspection* (DPI) en cas de bridage détecté, possibilité de signaler les tests positifs à l'Arcep via un bouton « J'alerte l'Arcep », mise en place d'un tableau de bord en ligne de suivi des tests réalisés en France, diversification des serveurs hébergeant l'application (notamment avec deux serveurs en France hébergés par l'Arcep et par K-net que nous remercions), refonte du design des applications Android et iOS, traduction de l'interface en français, etc.

À ce jour les résultats remontés par l'application ne permettent pas de suspecter une quelconque gestion de trafic contraire à la neutralité des réseaux sur les flux observés en France.

2.2. Préparer l'arrivée de la 5G

L'Arcep a pour mission de veiller au respect de la neutralité de l'internet en France. Elle est aussi en charge du développement et du déploiement de la 5G sur le territoire. Pour certains, 5G et neutralité de l'internet sont incompatibles mais qu'en est-il vraiment ? Pour démystifier les idées reçues, l'Arcep a synthétisé les débats dans un document *ad hoc*[4].

L'Arcep a par ailleurs organisé dans le cadre du Forum sur la gouvernance de l'internet qui s'est tenu à Paris en novembre 2018 un atelier thématique sur le sujet.

Enfin, l'Arcep a contribué aux travaux du BEREC sur le sujet qui ont conclu, notamment, que le règlement internet ouvert laisse une marge de manœuvre importante pour l'implémentation des technologies 5G telles que le *network slicing* ou le *mobile edge computing.*

4. https://www.arcep.fr/uploads/tx_gspublication/ARCEP_BD_5G_nov2018.pdf

5G ET NEUTRALITÉ DU NET : AMIS OU ENNEMIS ?

Pour certains, 5G et neutralité de l'internet sont incompatibles mais qu'en est-il vraiment ? Pour démystifier les idées reçues, l'Arcep a synthétisé les débats dans un document *ad hoc*.

LES PROMESSES DE LA 5G, LA PROCHAINE GÉNÉRATION DE RÉSEAU MOBILE

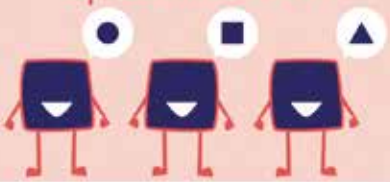
Débits

La 5G offrira des débits inédits pour utiliser au mieux des applications toujours plus datavores.

Instantanéité

La 5G réduira la latence pour des services en temps réels (robots, chirurgie...).

Spécialisation



Avec la 5G, il sera possible d'adopter différentes qualités de service en fonction de certains usages.

Virtualisation

La virtualisation d'un nombre important de composants réseaux et les réseaux logiciels seront synonymes de flexibilité pour les réseaux 5G.

Sobriété énergétique

La 5G permettra entre autres d'émettre uniquement à l'endroit et au moment où cela est nécessaire, en adaptant la puissance à l'usage.

Fiabilité

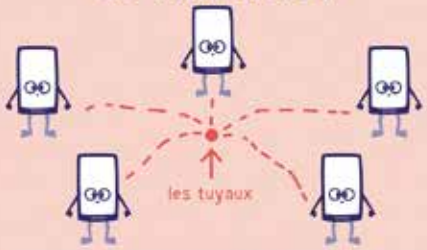
La 5G offrira une fiabilité accrue pour des communications critiques et de nouvelles applications, notamment sur les réseaux publics.

QUE FAIT LE RÉGULATEUR ?

- Il encourage l'innovation et les investissements dans le secteur ;
- Il autorise des expérimentations et délivre les autorisations d'utilisation de fréquences qui comportent des obligations

NEUTRALITÉ DU NET : ASSURER LA NON-DISCRIMINATION SUR LE NET

Les valeurs fondamentales de l'internet

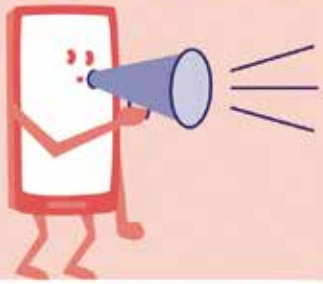


La neutralité du net c'est comprendre que l'intelligence est dans le réseau, sans contrôle centralisé.

Les droits des utilisateurs

La neutralité du net garantit que chaque utilisateur peut accéder à tous les contenus et services de son choix, via le terminal de son choix.

Liberté d'expression et d'information



La neutralité du net garantit les libertés de chaque utilisateur en tenant compte de celles des autres.

Innovation sans permission

La neutralité du net laisse les fournisseurs de contenus offrir leur service sans que les fournisseurs d'accès contrôlent ce qu'ils font.

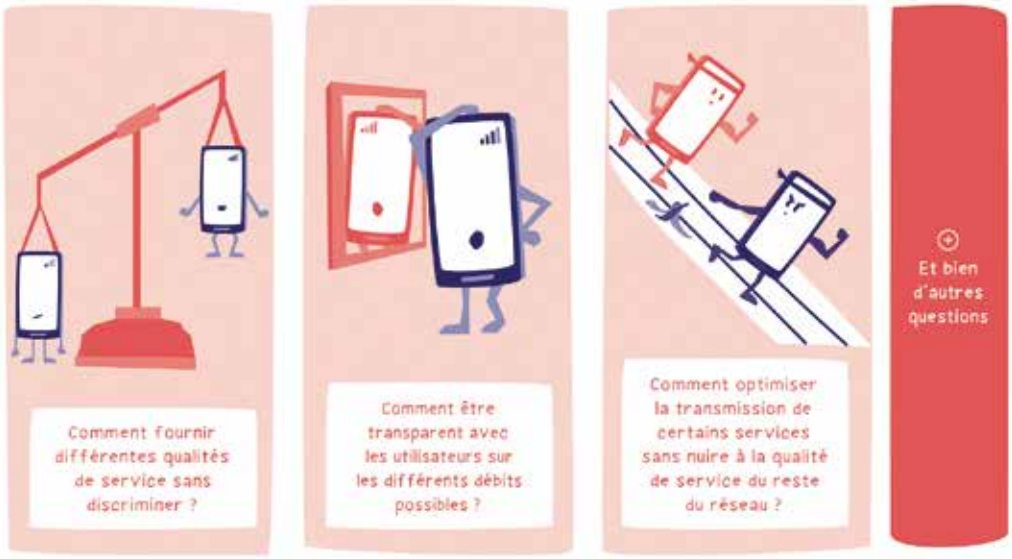
QUE FAIT LE RÉGULATEUR ?

- Il fait appliquer le principe de neutralité du net et sanctionne ceux qui ne le respecteraient pas ;
- Il co-construit des outils de détection : plateformes, applications pour détecter les gestions de trafic...

L'INNOVATION ET LA NON-DISCRIMINATION EN PRATIQUE :

la 5G ouvre la voie à de nouvelles applications...

... et de nouvelles relations à inventer



QUI A DIT QUOI ?

Panorama des opinions en quelques citations

BEREC (Groupe des régulateurs européens des télécoms)
Le Berec considère que le Règlement européen sur l'internet ouvert laisse une grande place à la mise en oeuvre des technologies 5G, comme le «network slicing», «5QI», et le «Mobile Edge Computing» par exemple. A ce jour, le Berec n'a pas connaissance d'exemples concrets de déploiements de la 5G entravés par le Règlement.

FCC
(Régulateur américain des télécoms)
Un autre impact négatif pour le consommateur des précédentes règles de la FCC sur la neutralité du net a été la baisse de l'innovation. Nous avons basculé d'un formidable cadre prônant l'innovation ouverte à une approche de contrôle à l'effet paralysant.

GSMA (GSM Association) **et ETNO**
(Europeans Telecommunications Network Operators)
Les pays européens doivent concilier le besoin d'un internet ouvert avec les règles qui encouragent l'innovation. L'industrie des télécoms alerte sur le fait que les lignes directrices actuelles sur la neutralité du net, comme publiées par le BEREC, créent des incertitudes significatives sur la rentabilité des investissements des opérateurs.

EDRI
(European Digital Rights)
Nous craignons beaucoup que la standardisation en cours de la 5G sape le niveau actuel de protection de la neutralité du net en Europe.

TRAI
(Régulateur indien des télécoms)
L'optimisation des performances du réseau, en conformité avec la neutralité du net, offre un cadre propice pour concevoir, construire et déployer les objets connectés et leurs mécanismes de communication afin de minimiser la charge sur le réseau, en étant proactif sur l'amélioration de l'efficacité et du débit de leurs données. C'est aussi un gage d'avantages concurrentiels.

PAROLE À...

Pieter Nooren, *senior scientist,* TNO

Neutralité du net et 5G

TNO[1] a réalisé une étude[2] indépendante sur la 5G et la neutralité de l'internet. Objectif : fournir une base solide au débat public. Cette étude offre un cadre analytique qui aide à structurer les discussions entre les décideurs, les régulateurs et les opérateurs de téléphonie mobile. Elle repose sur trois cas dont les conditions d'utilisation nécessitent des exigences de connexion spécifiques avec la 5G : la réalité virtuelle dans les médias et le divertissement, les communications d'urgence dans le cadre de la sécurité publique et la conduite automatisée. Ensemble, ils recouvrent des combinaisons différentes d'exigences spécifiques pour les réseaux 5G : des courts délais (latence), une bande passante élevée et une fiabilité élevée de la connectivité.

LA 5G S'APPUIE SUR DES TECHNOLOGIES NOUVELLES ET EXISTANTES

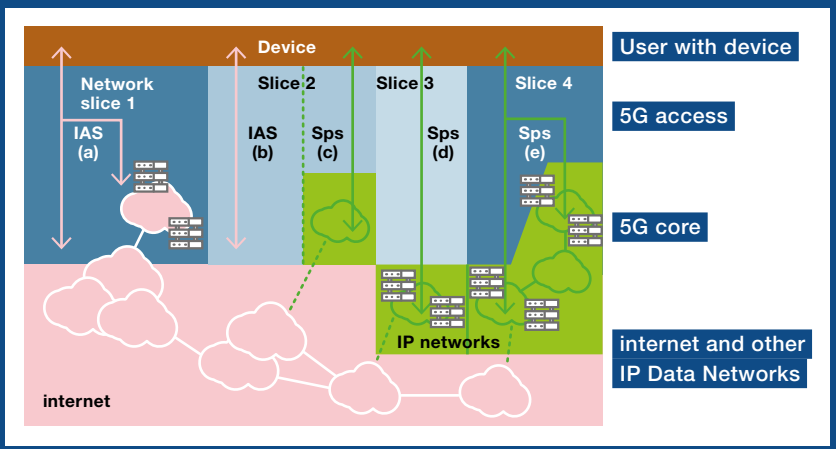
La 5G permet des débits de données plus élevés, des capacités de réseau importantes et l'utilisation d'un nombre supérieur de périphériques que la 4G. La 5G permet aussi aux opérateurs de téléphonie mobile de fournir une connexion adaptée à des secteurs, des groupes d'utilisateurs et des applications spécifiques à partir d'avancées technologiques telles que le *network slicing,* le *Mobile Edge Computing* ou encore la différenciation de qualité de service.

L'IMPORTANCE DE LA NEUTRALITÉ TECHNOLOGIQUE

La neutralité technologique est un principe bien établi auquel adhèrent le règlement et les lignes directrices qui fixent les règles en matière de neutralité de l'internet en Europe. Ces règles examinent les modalités d'utilisation de la technologie 5G, et non la technologie 5G en elle-même. Ainsi, les règles européennes de neutralité du net n'interdisent aucune des possibilités de la 5G, ni même les technologies de différenciation des flux de trafic et des applications en cours de développement.

La question centrale dans l'évaluation de la conformité de la 5G aux règles de neutralité du net est de savoir si les services et applications reposant sur cette technologie respectent les règles applicables aux services d'accès internet ou aux services dits spécialisés. L'étendue de ces règles détermine la marge de manœuvre des opérateurs de téléphonie mobile et des fournisseurs de contenus et d'applications (y compris ceux issus d'intégration verticale) dans l'utilisation des technologies de la 5G. La technique du *network slicing* en est un parfait exemple, dont l'utilisation peut prendre des formes multiples (cf. le schéma ci-dessous).

Dans les architectures 5G qui utilisent la technologie du *network slicing,* une *slice* peut être utilisée soit pour fournir exclusivement un service d'accès internet (*slice* 1), soit pour fournir exclusivement un service spécialisé (*slices* 3 et 4), soit pour fournir les deux. Ainsi, l'utilisation de la technologie du *network slicing* est soumise aux dispositions relatives aux services d'accès à internet et/ou à celles relatives aux services spécialisés. Une évaluation globale n'est donc plus possible à partir de la seule mise en conformité des *slices* avec la neutralité du net. En effet, l'évaluation des cas d'espèce dépendent non seulement de la technologie 5G utilisée, mais également de l'articulation retenue entre les services, les applications et l'architecture du réseau. Ces conclusions pour le *network slicing* sont également valables pour d'autres technologies clés de la 5G, telles que la différenciation de la qualité de service. *In fine,* les opérateurs de téléphonie mobile, les fournisseurs de contenu et d'applications, ainsi que les autorités de régulation nationales, devront procéder à une analyse plus approfondie pour déterminer si un type particulier de connexion est conforme aux règles de neutralité du net.



1. https://www.tno.nl/en/about-tno/organisation/
2. 5G and Net Neutrality: a functional analysis to feed the policy discussion, P.A. Nooren, N.W. Keesmaat, A.H. van den Ende, A.H.J. Norp, TNO 2018 R10394, 13 April 2018.

3. ANALYSE DES PRATIQUES OBSERVÉES

Dans la continuité des pratiques identifiées l'année passée, l'Arcep s'est d'abord penchée sur la liberté de choix et d'utilisation des terminaux dans les offres mobiles des FAI. Plusieurs restrictions potentielles avaient été identifiées depuis 2017, en particulier l'impossibilité d'utiliser le mode modem (interdiction totale d'usage ou limitation du volume de données alloué à cette modalité), ainsi que sur l'impossibilité d'utiliser certaines classes de terminaux dans certaines offres d'accès internet.

Suite à l'action de l'Arcep, les opérateurs ont supprimé les clauses limitant l'utilisation du mode modem et interdisant l'utilisation des cartes SIM dans tout terminal mobile. L'Arcep continue d'effectuer un suivi renforcé de la situation.

En début d'année 2018, suite à de nombreuses sollicitations publiques et à des remontées importantes sur la plateforme « J'alerte l'Arcep », l'Autorité a souhaité disposer d'éléments d'information complémentaires sur les causes de la mauvaise qualité de certains services particuliers sur le réseau de Free. Ces problèmes de débits et d'accessibilité récurrents semblaient toucher plusieurs services en ligne populaires, au premier rang desquels Netflix. Au vu des éléments obtenus par la formation compétente de l'Autorité en début d'année, il est apparu que l'interconnexion du réseau de Free avec le reste de l'internet pouvait être un élément d'explication. Contrairement aux autres FAI de grande taille, l'accès de Free à l'essentiel du trafic mondial repose en grande partie sur un seul transitaire, dont certains liens connaissaient des saturations de capacité très régulières. En conséquence, sans qu'il soit forcément question de gestion de trafic, les services les plus sensibles en bande passante tels que le *streaming* vidéo pouvaient connaître des problèmes de qualité dans ces moments de saturation, quel que soit par ailleurs le débit théorique dont bénéficiait l'accès internet du client final. La qualité de service perçue *in fine* par le consommateur dépend de l'ensemble des intervenants de la chaîne technique entre le client final et le contenu qu'il consomme (FAI, transitaires, fournisseurs de contenus, etc.). La presse s'était d'ailleurs fait écho au printemps 2018 de l'établissement d'une interconnexion directe entre Free et Netflix. Aujourd'hui, l'Arcep constate une attrition des signalements qu'elle reçoit, signe d'une amélioration de la situation pour le client final. Comme évoqué dans le chapitre 2, les modalités d'interconnexion entre les acteurs sont variées (transit, mais aussi relations directes telles que le *peering* gratuit ou payant) et permettent de répondre à différents types de besoins.

L'Arcep s'est également intéressée aux offres de Wi-Fi en vol proposées par les compagnies aériennes. Cette interaction a été l'occasion pour l'Arcep de rappeler que le règlement s'applique non seulement aux offres des FAI traditionnels, mais aussi à ce type d'offres d'accès considérées comme publiquement disponibles par l'Arcep. Le sujet des offres de Wi-Fi en vol étant par nature transnational, la question a été également évoquée, à l'initiative de l'Arcep, dans le cadre des travaux du groupe d'experts du BEREC. Ceux-ci confirment que ce type d'offres peut être défini comme publiquement disponibles et de fait sujettes aux dispositions du règlement européen sur l'internet ouvert.

Enfin, suite à plusieurs signalisations sur la plateforme « J'alerte l'Arcep », les services de l'Arcep examinent la question des blocages de port. L'accès à un service ou à une application en ligne s'effectue au moyen d'un port, dont le blocage empêche de fait l'accès au service. Cette restriction d'accès est une pratique qui pourrait être incompatible avec le règlement internet ouvert dès lors qu'elle ne serait pas justifiée par l'une des exceptions visées au règlement.

L'Arcep met à disposition des utilisateurs finals un petit script de tests permettant de vérifier si un port TCP est opérationnel dans le sens sortant, bloqué ou bien disponible mais avec un débit réduit. Le script est disponible ici : https://github.com/ARCEP-dev/disPorts

L'objectif de ce script est de mieux informer les utilisateurs sur les blocages de port mis en place par leurs FAI et d'alimenter les réflexions de l'Arcep sur ce sujet.

POUR ALLER PLUS LOIN

QULS SONT LES « PORTS » EXPLOITÉS LORS D'UNE CONNEXION ?

Les protocoles TCP et UDP sont les deux principaux protocoles exploités sur internet pour transporter des flux au moyen du protocole IP. Schématiquement, à chaque connexion sur internet émanant d'une application est associée une session UDP ou TCP identifiée à partir d'un « numéro de port ». Ainsi, à chaque extrémité de la connexion TCP (émetteur et récepteur) est associé un numéro de port sur 16 bits (de 1 à 65 535) assigné à l'application émettrice ou réceptrice. On parle alors respectivement de port source et destination.

Si les ports source sont le plus souvent choisis de manière aléatoire, ce sont les ports destination qui permettent sur un serveur supportant de multiples applications, le routage du flux vers la bonne application. Ceux-ci sont donc relativement standardisés.

Afin que le service soit accessible, le port correspondant doit être « ouvert », c'est-à-dire que les équipements impliqués dans le transit des flux ne doivent pas bloquer l'acheminement des paquets réseau associés à ce port. Tout blocage/bridage sur ce port peut ainsi affecter le service en question.

PAROLE À...

Benjamin Bayart et Oriane Piquer-Louis, co-présidents de la Fédération FDN

La neutralité du net comme liberté individuelle

Les textes européens qui protègent la neutralité du net la définissent comme la liberté pour les utilisateurs finals de faire un certain nombre de choses : consulter et mettre à disposition du contenu, utiliser et mettre à disposition des applications, etc. Cette liberté se traduit en une interdiction faite aux intermédiaires techniques, en particulier les opérateurs du réseau, de s'opposer à son exercice, le gardien de cette liberté étant, de manière un peu étrange, le régulateur économique du secteur.

Le volet le mieux compris pour l'instant est celui qui porte sur les chamailleries commerciales entre acteurs économiques du réseau : le fournisseur d'accès qui veut privilégier sa plateforme de vente de vidéo par rapport à celles des autres, ou privilégier ses accords commerciaux et publicitaires, au détriment du libre marché et de la concurrence, et donc au détriment de la liberté du citoyen d'accéder aux contenus de son choix. Bien que l'analyse sur ce volet soit maîtrisée par les régulateurs nationaux, la défense des libertés laisse encore à désirer (le *zero-rating* reste, pour le moment, toléré dans trop de cas).

Un autre volet reste pour l'heure complètement négligé : le droit à une connexion symétrique. Cette symétrie est présente, littéralement, à chaque mot utilisé par le législateur européen pour décrire la neutralité du net. Chaque mot qui place l'internaute dans une situation (mettons, consommateur) est accompagné de son symétrique (ergo, producteur). L'intention est évidente, non seulement le libre choix de ce que l'on consomme, mais aussi, mais surtout, le droit de proposer, en tant qu'internaute, tout ce qui est proposable.

La formulation n'est pas que l'internaute peut souscrire l'abonnement dont il a envie, et que Netflix a le droit de diffuser les abonnements qu'il souhaite. La formulation est limpide : l'internaute a le droit de diffuser. Ce n'est pas un droit limité à certains acteurs économiques, c'est un droit essentiel du citoyen européen, protégé, qui est une conséquence logique des libertés fondamentales en Europe.

Cet élément clef, la symétrie dans le rapport au réseau, est pourtant encore trop souvent mis à mal. Pour s'en convaincre et comprendre le problème, il suffit de faire un rapide parallèle avec d'autres réseaux.

« La neutralité du net permet d'exercer une liberté d'accéder mais aussi une liberté de diffuser qui lui est symétrique. »

Premier exemple : l'adressage. Sans adresse IP publique et fixe, un accès à internet ressemble à un accès téléphonique sans numéro de téléphone : on peut appeler, mais on ne peut pas être appelé. La limitation est évidente. Non seulement ces pratiques sont courantes dans l'accès fixe, mais elles sont la norme dans les accès mobiles. En ce sens, le déploiement de l'IPv6 auquel l'Arcep pousse est un progrès (pour fournir des adresses publiques à tous les accès), mais il restera encore à faire comprendre que l'adresse IP devrait être aussi fixe que le numéro de téléphone, ou devrait pouvoir l'être.

Second exemple : les ports et services. Beaucoup de ports sont bloqués, en entrée, quand ce n'est pas en sortie, par un bon nombre d'opérateurs. Les ports de transport du mail, nécessaires pour héberger un serveur de messagerie, sont l'exemple le plus ancien. Le prétexte du blocage est d'ailleurs relativement bon : nombre d'ordinateurs sont équipés de systèmes d'exploitation mal sécurisés, et sont utilisés comme relais dans des botnets, soit pour inonder la planète de spams, soit pour mener des attaques. Reste que les opérateurs le font sans discernement, en intervenant de manière autoritaire dans ce que leurs abonnés ont le droit de transporter ou non. En supposant que les gens sont inaptes à faire une chose, on s'assure qu'ils le sont : ils n'ont aucune opportunité d'apprendre à faire autrement. Interdisez à quelqu'un de se tenir debout, de peur qu'il ne tombe, et il ne saura jamais marcher.

La neutralité du net permet donc d'exercer une liberté d'accéder, mais aussi une liberté de diffuser, qui lui est symétrique. Il est important que les régulateurs européens sortent un peu de leur carapace de régulation économique, pour prendre en main leur rôle de protecteur de ces libertés essentielles au XXIe siècle.

Protéger ces libertés peut passer pour la lubie de quelques idéalistes d'un réseau hippie fantasmé. C'est en fait le seul outil connu pour s'affranchir de la toxicité des plateformes hyper-centralisatrices dont les pratiques sont tant décriées, mais aussi tant confortées par nos choix politiques.

4. LA COOPÉRATION EUROPÉENNE POUR UNE APPLICATION COHÉRENTE DU RÈGLEMENT

Durant l'année écoulée, les ARN européennes ont échangé sur leurs différentes enquêtes nationales. L'année 2018 a été surtout marquée par le nombre d'offres de *zero-rating* portées à la connaissance des régulateurs nationaux (27 pays sur 28 au total). De plus, certaines ARN ont collectivement constaté plusieurs limites à la liberté de choix et d'utilisation par l'utilisateur final de son équipement terminal. Plusieurs autorités ont également échangé sur les pratiques de blocage de port identifiées et ont discuté les arguments de sécurité avancés par les différents FAI pour justifier de telles pratiques. Enfin, les ARN ont aussi partagé leurs analyses sur les services spécialisés de téléphonie et de télévision sur IP.

L'Arcep se félicite de participer à cette coopération européenne qui contribue à une application cohérente du règlement et des lignes directrices au profit de chaque utilisateur final (internautes et fournisseurs de contenu, d'applications ou de services).

FEUILLE DE ROUTE DE L'ARCEP POUR L'APPLICATION DU RÈGLEMENT INTERNET OUVERT

ÉTAPE 1

Diagnostic

- Outils réglementaires
- Espace de signalement
- Plateformes de détection
- Veille
- Coopération internationale

ÉTAPE 2

Analyse et mise en conformité

La loi pour une République numérique a confié à l'Arcep les pouvoirs nécessaires pour assurer le respect du règlement.

ÉTAPE 3

Reporting

Arcep
Rapport annuel national
(annuel)

BEREC
Rapport consolidé européen
(annuel)

PAROLE À...

Thomas Lohninger, directeur général, epicenter.works

Vers une coopération renforcée en Europe pour garantir la neutralité du net

Il y a deux ans et demi, l'Union européenne a adopté une législation visant à protéger la neutralité de l'internet. L'objectif était de protéger l'internet ouvert en tant que moteur de l'innovation et de mettre en place un marché unique européen des télécommunications qui protège le droit des utilisateurs finals. Pour contribuer à la discussion sur le cadre européen de la neutralité du net, notre ONG, epicenter.works, a publié un rapport basé sur une enquête des pratiques de prix différenciés dans l'Espace Économique Européen (EEE), sur la lecture de près de 800 pages cumulées des rapports annuels des régulateurs européens, sur les principales décisions de neutralité du réseau prises par les régulateurs et sur l'analyse économique de l'impact des offres de *zero-rating* sur le prix du volume des données mobiles.

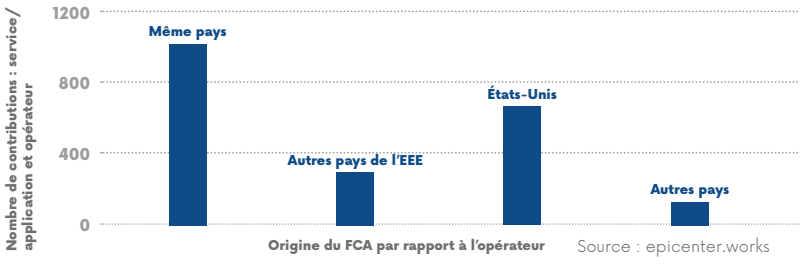
Grâce aux lignes directrices du BEREC sur la neutralité de l'internet, la mise en œuvre des textes et la supervision opérée par les autorités de régulation nationales (ARN) se sont faites de manière harmonisée. Cependant, cela n'a eu lieu que dans les cas où les ARN prennent soin d'évaluer la situation dans leurs pays. Comme le montrent leurs rapports annuels, les ARN ont des priorités différentes. Par exemple, dans des domaines comme le blocage des ports de réseau – une pratique très facile à détecter et assez simple à réglementer – les ARN ont adopté des approches différentes qui limitent la fourniture de services transfrontaliers. Les ARN doivent publier des rapports annuels sur leurs activités de contrôle, mais très peu respectent les critères du BEREC qui imposent la publication d'un minimum d'informations. Il est particulièrement préoccupant que seules huit ARN aient communiqué des chiffres sur la disponibilité continue de services d'accès à internet avec des niveaux de qualité suffisants.

Notre rapport[1] se concentre sur les pratiques commerciales de prix différenciés. Depuis l'entrée en vigueur du règlement, ces offres se sont étendues à tous les pays de l'Union Européenne, à l'exception de deux États membres. Nous avons répertorié 186 offres de ce type dans l'EEE. Bien que les lignes directrices du BEREC prévoient une évaluation au cas par cas de chaque offre, selon les rapports 2017 et 2018 d'implémentation de du BEREC, seules 17 ARN ont engagé des évaluations formelles, et aucune d'entre elles n'a encore décidé d'interdire de telles pratiques commerciales. Ces évaluations ne respectent pas, pour la plupart, les critères des lignes directrices du BEREC.

113 offres échouent dans la diffusion d'informations sur les modalités de leurs accès en itinérance dans l'EEE ont pu être identifiées. 67 % des offres de différenciation tarifaire ne délivrent pas d'informations à l'intention des fournisseurs de contenu et d'applications (FCA) qui souhaitent y adhérer (offres fermées). De plus, pour celles qui procurent de telles informations (offres ouvertes), le temps de réponse apportés aux demandes des FCA intéressés est très variable. Deux ont répondu en un jour, cinq en une semaine, une en un mois et dix ne nous ont jamais répondu. Notre étude montre donc que la pratique de prix différenciés, même ouverte à tous les FCA, peut être en réalité discriminatoire. À notre connaissance, ce fait n'a pas encore été évalué par les ARN.

Lors de la révision du cadre réglementaire actuel, le BEREC doit veiller à ce que les ARN puissent examiner ce type d'offres afin de limiter leurs effets sur les droits des utilisateurs finals. *In fine,* l'Europe doit donc non seulement s'assurer de la compatibilité de la 5G avec la neutralité de l'internet, mais aussi restaurer la confiance des consommateurs dans les régulateurs avec la mise à jour des lignes directrices.

Relations géographiques entre opérateurs et services/applications à prix différenciés



Source : epicenter.works

1. Notre rapport complet sur la situation de la neutralité de l'internet en Europe et l'analyse de l'ensemble des données sous-jacentes à l'adresse : https://epicenter.works/document/1522

5 Contribuer à l'ouverture des terminaux

« Le diagnostic fait désormais consensus mais la pathologie reste vivace »

4,3 milliards d'euros

C'est le montant de l'amende infligée par la Commission européenne à Google pour abus de position dominante sur le marché des systèmes d'exploitation en favorisant son moteur de recherche et son navigateur Chrome.

Le règlement européen sur l'internet ouvert accorde des droits aux utilisateurs : le droit d'accéder et de diffuser des informations et des contenus en ligne. Mais ce règlement ne concerne que les fournisseurs d'accès à internet qui ne sont qu'un maillon de la chaîne d'accès à internet. Situés à l'extrémité de cette chaîne les smartphones, les assistants vocaux, les voitures connectées et autres terminaux accompagnés de leur système d'exploitation se révèlent être le maillon faible de l'ouverture d'internet. Après les premiers éléments de diagnostic mis dans le débat public par l'Arcep en 2017, l'année 2018 aura été marquée par une prise de conscience des acteurs institutionnels, qui se sont ainsi saisis du sujet.

1. TRAVAUX DE L'ARCEP

Après son diagnostic sur l'influence des équipements terminaux dans l'ouverture d'internet, l'Arcep mobilise les acteurs pour une plus grande liberté de choix.

En février 2018, l'Arcep a complété son analyse sur les terminaux commencée un an plus tôt en publiant un rapport complet intitulé « Terminaux, maillon faible de l'ouverture d'internet », présenté lors d'une conférence organisée le 15 février 2018. Cette conférence a été l'occasion d'interpeller chacun sur le rôle des équipements terminaux dans l'ouverture d'internet et les actions à envisager.

Pour aider les utilisateurs face aux restrictions auxquelles ils sont confrontés dans la pleine utilisation de leurs smartphones, l'Arcep a publié deux fiches pratiques.

Les difficultés liées au transfert des données et des contenus vers un nouvel équipement, et en particulier vers un nouveau système d'exploitation, peuvent décourager les consommateurs souhaitant changer d'environnement. C'est pourquoi l'Arcep a publié une première fiche expliquant comment les utilisateurs peuvent conserver leurs données lorsqu'ils migrent vers un nouveau smartphone[1].

Par ailleurs, les systèmes d'exploitation des smartphones orientent souvent les utilisateurs dans leurs choix en mettant en avant des contenus et services particuliers (applications installées par défaut, moteur de recherche, magasin d'application…). Ainsi, une seconde fiche vise à guider les utilisateurs dans la configuration de leur smartphone pour leur permettre de tirer le meilleur profit de l'offre de services et de contenus, mais aussi pour identifier les limites qui s'imposent à leur liberté de choix[2].

Tout au long de l'année, l'Arcep a contribué sur le sujet notamment lors de *l'Internet Governance Forum,* espace de dialogue créé sous l'égide des Nations Unies, qui se déroulait en novembre 2018 à l'UNESCO, en organisant une table ronde regroupant des acteurs de la société civile (Mozilla, Epicenter) ainsi que des régulateurs internationaux (TRAI, CRTC). Par ailleurs, l'Arcep a suivi l'évolution du marché et des pratiques tout au long de l'année.

L'Arcep souhaite pérenniser ce travail de veille et de communication au travers d'un observatoire des terminaux collaboratif regroupant les entités publiques qui seraient intéressées par le sujet.

1. https://www.arcep.fr/demarches-et-services/consommateurs/terminaux-portabilite-donnees.html
2. https://www.arcep.fr/demarches-et-services/consommateurs/terminaux-personnalisation-api.html

2. BILAN RÉGLEMENTAIRE

Sur le plan réglementaire, l'année écoulée marque une étape importante puisque les premiers jalons de la régulation des terminaux que l'Arcep appelle de ses vœux y ont été posés.

Dès avril 2018, la Commission européenne proposait le règlement *Platform-To-Business* qui a pour objectif d'apporter transparence, prévisibilité et équité aux entreprises qui dépendent des plateformes en ligne et des moteurs de recherche. Ce règlement prévoit en effet que les plateformes, y compris les magasins d'applications, devront désormais annoncer plus en amont tout changement contractuel pouvant avoir un impact sur les développeurs et, en cas de suspension ou terminaison de l'accès de leurs applications au magasin d'application, expliquer les raisons qui sous-tendent cette décision et offrir un mécanisme de recours aux développeurs. C'est un premier pas vers la résolution rapide des différends entre développeurs et plateformes que l'Arcep préconisait dans son rapport de février 2018. Quant aux systèmes d'exploitation, s'ils ne sont pas appréhendés en tant que tels par le texte, celui-ci permettra néanmoins aux entreprises utilisatrices d'être informées des traitements différenciés que la plateforme est susceptible de mettre œuvre entre ses propres services et ceux d'entreprises concurrentes en ce qui concerne l'accès aux fonctionnalités du système d'exploitation. Un Observatoire européen a également été mis en place permettant de contrôler la bonne mise en œuvre du règlement. Cette surveillance du marché est en ligne avec ce que le BEREC, organe des régulateurs européens des télécoms, recommandait dans son rapport sur l'impact des contenus et des terminaux sur le fonctionnement des marchés de communications électroniques, publié également en 2018. Pour autant, si la transparence permise par ce règlement pourrait mettre en exergue certains des problèmes que rencontrent les développeurs, il n'offre pas aux utilisateurs la liberté de choix que leur permettrait la « neutralité des terminaux ».

La seconde contribution européenne à l'« ouverture des terminaux » est la décision de la Direction Générale à la concurrence concernant le système d'exploitation Android. En effet, constatant que Google abusait de sa position dominante sur le marché des systèmes d'exploitation pour favoriser son moteur de recherche et son navigateur Chrome, la Commission a sanctionné Google pour pratiques abusives. L'entreprise a été condamnée à verser une amende de 4,3 milliards d'euros et à mettre fin à ces pratiques. En conséquence, Google est désormais contraint d'assouplir les règles permettant aux fabricants de téléphones de développer des variantes du système *Android ;* Google doit de plus permettre aux fabricants de préinstaller son Play Store sans devoir préinstaller Chrome et Google Search également ; Google avait annoncé proposer désormais cette option moyennant l'achat d'une licence pouvant aller jusqu'à 40$ par téléphone. C'est ainsi que Wiko propose depuis avril 2019 un smartphone Android offrant le moteur de recherche Qwant par défaut au lieu de Google Search[3]. Enfin, Google devrait prochainement présenter aux utilisateurs européens d'Android la possibilité d'installer un le moteur de recherche et un navigateur en supplément de ceux déjà installés[4]. Aptoide a également porté plainte devant la Commission européenne contre le géant américain, l'accusant d'utiliser l'antivirus Google Play Protect pour supprimer à tort son magasin d'application alternatif des téléphones Android. Enfin, une plainte a été déposée par Spotify devant la Commission européenne en mars 2019, cette fois au sujet du magasin d'applications d'Apple. Spotify accuse en effet Apple de profiter de son intégration verticale pour favoriser son service Apple Music, notamment en exonérant ce service de la taxe de 30 % auxquels sont soumis les services en ligne tiers proposant leur abonnement via l'Apple Store.

3. https://fr.wikomobile.com/shop/smartphone-view2-pro-qwant/
4. https://www.blog.google/around-the-globe/google-europe/presenting-search-app-and-browser-options-android-users-europe/

Une ouverture similaire est prônée par l'autorité Australienne de la Concurrence et de la Consommation qui, dans son rapport préliminaire *« Digital Platforms Inquiry »,* publié en décembre 2018, estime nécessaire que lorsque plusieurs moteurs de recherche ou navigateurs sont proposés, aucun choix ne soit présélectionné par défaut.

Enfin, à l'été 2018, l'application du RGPD[5] a été l'occasion d'une mise en exergue des restrictions pesant sur les choix offerts aux utilisateurs lors de la configuration de leurs terminaux et qui pouvaient, *in fine*, peser sur leur consentement au traitement de leurs données. Les députés Eric Bothorel et Cédric Villani ont ainsi déposé un amendement, adopté par la représentation nationale, qui a permis de renforcer le choix des utilisateurs en matière de services et d'applications disponibles, notamment lors de la configuration initiale de leur terminal[6].

3. ANALYSE DES PRATIQUES OBSERVÉES

Malgré les avancées notables observées depuis la publication du rapport, de nouvelles pratiques observées en 2018 soulignent le besoin persistant d'une régulation plus forte des terminaux.

Plusieurs pratiques observées sur le marché des systèmes d'exploitation illustrent la façon dont une application peut être discriminée, à commencer par le biais des mécanismes de gestion de batterie. Afin d'allonger l'autonomie des terminaux et pour limiter l'impact des logiciels espions, le système d'exploitation Android contient un mécanisme visant à éteindre certaines applications exécutées en arrière-plan. Certains constructeurs de terminaux sont allés plus loin en ajoutant une surcouche logicielle qui sélectionne un faible nombre d'applications populaires pouvant continuer à être utilisées en toutes circonstances. Les autres applications sont en revanche automatiquement éteintes lorsque celles-ci fonctionnent en arrière-plan, la surcouche interférant ainsi avec le fonctionnement d'un champ plus large d'applications que ne le prévoit la base Android. Or, ces extinctions d'applications peuvent être perçues par les utilisateurs comme des dysfonctionnements des applications elles-mêmes. Victimes de ces pratiques, des développeurs d'applications ont créé le projet DontKillMyApp, qui propose un classement des constructeurs les plus « tueurs » d'applications et indiquent aux utilisateurs comment modifier le paramétrage de leur terminal lorsque cela est possible.

De nouvelles pratiques sont également observées au niveau des magasins d'applications. Par exemple, fin 2018, la société Kaspersky s'est vu empêcher de mettre à jour son application Safe Kids sur iPhone (une application de contrôle parental qui permet de bloquer l'utilisation de certaines applications) au motif qu'elle accède au profil de configuration des téléphones Apple pour son fonctionnement. Ce blocage étant survenu peu de temps après qu'Apple ait inclus une application similaire dans iOS (Screen Time), Kaspersky a déposé plainte en mars 2019 auprès des autorités russes pour concurrence déloyales. Ces restrictions, mêmes lorsqu'elles peuvent être justifiées par des motifs de sécurité, peuvent avoir des effets de bord en termes de diversité de choix offert aux consommateurs. Ainsi, suite à certains abus, Google a annoncé en mars 2019 vouloir restreindre l'accès à la fonctionnalité d'envoi de SMS aux seules applications de messageries SMS.

Or, cette fonctionnalité était par exemple utilisée par l'Organisation Mondiale de la Santé pour véhiculer des données sur les zones vaccinées contre la polio en Somalie en l'absence de couverture 2G ; les développeurs se sont plaints de difficultés à obtenir un traitement au cas par cas approprié des restrictions d'accès. Toutefois, certaines applications ont su exploiter leur popularité pour s'affranchir des conditions imposées par les magasins d'applications. Le jeu mobile Fortnite n'est par exemple pas disponible sur le Play Store, ce qui n'a pas empêché des millions d'utilisateurs de l'installer sur leur téléphone Android depuis sa sortie en 2018. Une telle possibilité reste toutefois restreinte aux utilisateurs Android, Apple n'autorisant pas le téléchargement d'application depuis d'autres sources que son App Store. De même, d'autres applications telles que Netflix et Spotify, si elles sont toujours présentes sur le Play Store et l'App Store, tentent de s'affranchir des marges prélevées par les magasins d'applications. Spotify empêche ainsi ses clients de s'abonner *via* l'App Store, ce qui contraint les utilisateurs à souscrire leur abonnement *via* le site web. La même pratique est observée par Netflix pour contourner le prélèvement de marges par l'App Store et le Play Store.

Les navigateurs web peuvent également constituer un moyen pour les acteurs verticalement intégrés de favoriser leurs propres services, au détriment de la liberté de choix des consommateurs. Par exemple, Chrome empêche l'installation d'extensions permettant de télécharger les vidéos depuis YouTube mais les autorise lorsqu'il s'agit de télécharger des vidéos de services concurrents, ces téléchargements limitant les revenus liés au visionnage de vidéos pour ces services

Néanmoins, certaines évolutions sont en ligne avec les recommandations de l'Arcep. Constatant que les assistants vocaux (pour l'essentiel développés par Google, Amazon, et Apple) s'appuient sur des logiciels de reconnaissance vocale entraînés sur d'importantes bases de données, Mozilla a lancé fin 2017 son projet *« Common Voice »* pour permettre à de nouveaux acteurs de développer des algorithmes similaires. L'organisation a ainsi incité des milliers de volontaires à lire des textes pour enrichir une base de données ouverte et permettant l'entraînement de modèles de reconnaissance vocale par des entreprises alternatives. La base de données est devenue multi-langue le 28 février 2019.

5. Règlement général sur la protection des données du 27 avril 2016.

6. Article 28 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles : https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte#JORFARTI000037086002

PAROLE À…

Stefano Quintarelli, entrepreneur et ancien parlementaire italien

Pourquoi nous ne possédons pas notre terminal

Imaginons que vous êtes propriétaire d'un appartement dans une grande résidence dont les règles sont strictes et changent régulièrement. Vous faites appel à un kinésithérapeute spécialisé dans le type de soins dont vous avez besoin. Mais lorsqu'il vient chez vous pour une consultation, le gardien de votre résidence l'empêche d'entrer. Il invoque plusieurs motifs pour expliquer ce refus : le kinésithérapeute refuse de lui verser 30 % de ses gains et, de plus, il est vêtu d'une façon que le gardien juge inappropriée. Le gardien vous explique que vous ne pouvez recourir qu'à un kinésithérapeute figurant sur une liste qu'il a établi. De nombreux kinésithérapeutes figurent sur cette liste, mais pas celui que vous voulez. Le gardien vous explique que la règle ne sert pas à contrôler ce que vous faites chez vous ou à soutirer de l'argent aux kinésithérapeutes, mais plutôt à éviter que quelqu'un de mal intentionné entre chez vous – vous comprenez au passage que vous ne pourrez pas inviter qui vous voulez –.

Votre domicile n'est, en réalité, le vôtre que dans la limite des règles imposées par le gardien. Vous remarquerez cela le jour où vous essayerez de faire appel à un maçon (autre que celui recommandé par la compagnie de gardiennage) pour enlever la cheminée qu'on vous oblige à garder et qui prend de la place au milieu de votre salon. Le gardien vous expliquera alors que vous ne pouvez pas, car la résidence a un accord avec un vendeur de bûches et que peut-être un jour vous pourriez vous en servir.

Si vous n'appréciez pas ces règles, le gardien vous explique que vous êtes libre de déménager dans un autre immeuble, mais vous y perdriez beaucoup : les souvenirs associés aux décennies passées dans l'appartement, les meubles faits sur mesure, etc. Potentiellement, vous devriez acheter un nouvel appartement sans avoir la certitude de vendre l'actuel. Au final, changer d'immeuble vous coûterait trop cher en temps et en argent, et vous vous résignez à rester…

« La neutralité des terminaux, c'est s'assurer qu'un opérateur de plateforme ne pourra altérer vos décisions en restreignant votre liberté de choix »

Le principe de « neutralité » implique que ceux qui gèrent l'accès aux ressources ne peuvent pas utiliser ce privilège pour interférer dans les choix des utilisateurs, les modifier ou les limiter. Ce principe est maintenant établi et respecté sur les réseaux de télécommunication car définit dans un Règlement européen.

Mais ce n'est pas encore le cas pour les terminaux, ces outils avec lesquels nous nous tenons informés, établissons et maintenons nos liens sociaux et professionnels. Avec le temps, nos terminaux deviennent, pour nous tous, notre principale interface avec le monde. Mais nous ne « possédons » pas notre terminal, tout comme dans le cas de cet appartement en résidence, il n'est pas vraiment le nôtre, nos choix sont limités par des fonctionnalités techniques et des engagements contractuels désavantageux (avez-vous déjà lu les conditions générales d'utilisation de votre smartphone ?).

La neutralité des terminaux étend et complète le principe de la neutralité du net pour assurer que, tout comme votre opérateur télécom, un opérateur de plateforme ne pourra altérer vos décisions en restreignant votre liberté de choix. Bien sûr, une personne appréciant les conditions du gardien sera libre de continuer de suivre ce fonctionnement et les contraintes associées. Elle pourrait même payer un supplément pour cela. Mais une personne préférant suivre une voix alternative doit pouvoir le faire, que ce soit en tant qu'habitant de l'immeuble ou en tant que kinésithérapeute.

C'est pour garantir la neutralité des terminaux qu'en 2015, lorsque je siégeais au Parlement italien, j'ai proposé une loi pour garantir la neutralité des réseaux et des terminaux. Cette proposition a été validée par toutes les commissions du Sénat en 2017 mais le vote final a été repoussé et la législature a pris fin ; ce texte n'a ainsi jamais pu être mis en œuvre en Italie. Une telle loi est pourtant toujours nécessaire en Europe.

PAROLE À...

Maryant Fernández Pérez, *Senior Digital Policy Officer,* BEUC

Contrôlons-nous nos appareils électroniques? Une loi européenne pourrait le rendre possible!

Internet est omniprésent dans nos vies. Et pour y accéder, nous avons inévitablement besoin de terminaux. Mais quand nous les utilisons, nous sommes restreints dans nos usages. Par exemple, est-ce que vous pouvez désinstaller toutes les applications préinstallées dans votre tablette ? Est-ce que votre décision d'avoir un navigateur différent de celui qui est préinstallé est toujours respectée ? Afin de résoudre ces problèmes, au sein du Bureau européen des unions de consommateurs (BEUC) nous demandons à l'Union européenne (UE) de garantir la neutralité des terminaux au cours de son prochain mandat législatif.

Si l'Europe arrivait à adopter une loi sur la neutralité des terminaux, ce serait une victoire très importante pour les consommateurs. Grâce à une telle loi, les consommateurs pourraient par exemple avoir plus de liberté lorsqu'ils utilisent leurs smartphones, assistants vocaux, véhicules connectés, accéder à plus d'applications ou de services. De nouvelles entreprises pourraient quant à elles accéder aux marchés pertinents pour fournir des applications plus respectueuses de notre vie privée, par exemple.

Que ce soit un smartphone, une tablette, des haut-parleurs, des assistants vocaux ou d'autres appareils connectés, les consommateurs doivent pouvoir utiliser leurs terminaux de manière neutre et sans discrimination.

Ceci n'est pas toujours le cas. Légiférer sur la neutralité des terminaux serait la suite logique des règles européennes sur la neutralité du net, par lesquelles l'UE a fait preuve de son leadership mondial. Depuis 2016, les consommateurs peuvent bénéficier d'un internet ouvert, où les fournisseurs d'accès doivent traiter le trafic internet « de façon égale et sans discrimination, restriction ou interférence ». Les législateurs devraient désormais garantir l'accès à l'internet ouvert à tous les niveaux de la chaîne d'accès à internet, au-delà des seuls fournisseurs d'accès.

Une loi européenne sur la neutralité des terminaux devrait d'une part établir des définitions et des obligations claires pour les différents acteurs économiques qui sont derrière nos terminaux. D'autre part, elle devrait assurer une bonne application des règles pertinentes. Par ailleurs, cette loi devrait garantir que les consommateurs ont le droit d'utiliser des logiciels, d'accéder aux contenus et aux services de leur choix sans aucune condition discriminatoire ; de désinstaller de leurs terminaux les applications, services et contenus qui ne les intéressent pas, tout en sauvegardant la fonctionnalité essentielle et la sécurité du dispositif, entre autres.

Finalement, cette législation pourrait compléter le règlement européen *Platform to Business (P2B)* et le droit de la concurrence.

D'une part, le règlement P2B introduit déjà des obligations de transparence, de nouvelles exigences concernant les mécanismes de règlement des différends et interdit certaines pratiques déloyales. Le règlement P2B ne s'applique qu'aux relations entre les entreprises, mais nous espérons que les consommateurs en tireront aussi des bénéfices.

D'autre part, le droit de la concurrence peut régler certains problèmes mais ceci ne suffit pas pour assurer la neutralité des terminaux. Par exemple, la neutralité comme une forme de non-discrimination pourrait être un élément constitutif d'un remède pour que le marché soit compétitif, comme dans l'affaire *Android.* Toutefois, toute restriction à la neutralité des terminaux ne peut être traitée que lorsqu'elle est liée à un abus de position dominante. Le droit de la concurrence peut établir des principes, mais la vraie solution doit être inscrite dans la loi au niveau européen.

Nous félicitons le travail de l'Arcep, ainsi que les efforts fournis par d'autres autorités compétentes pour défendre les consommateurs et promouvoir une innovation concurrentielle dans ce domaine. Ceci est une première étape pour réussir à obtenir la neutralité des terminaux. Le BEUC a déjà soutenu une initiative similaire en Italie avec notre membre italien Altroconsumo. Il est temps d'assurer la neutralité des terminaux en Europe !

Lexique

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

A

AES-NI *(Advanced Encryption Standard New Instructions)* : Jeu d'instructions intégrées dans tous les microprocesseurs récents dont le but est d'accélérer les opérations de chiffrement et de déchiffrement utilisant l'*Advanced Encryption Standard* (AES) comme les échanges utilisant le protocole HTTPS.

Afnic (Association française pour le nommage internet en coopération) : association loi de 1901 qui a pour mission de gérer les domaines internet nationaux de premier niveau de France (.fr), La Réunion (.re), Terres australes et antarctiques françaises (.tf), Mayotte (.yt), Saint-Pierre-et-Miquelon (.pm) et Wallis-et-Futuna (.wf).

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, utilisant le noyau Linux.

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) : organisme chargé chargé par un État membre du BEREC de la régulation des communications électroniques.

B

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.

C

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

D

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.

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.

***Dual-Stack* (Double pile IP) :** consiste à affecter une adresse IPv4 et une adresse IPv6 à un équipement du réseau.

E

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

F

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.

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.

H

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

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

I

IAD *(Integrated Access Device)* : passerelle domestique, communément appelée box internet qui permet de connecter téléphone, ordinateurs et box TV.

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 utilisé 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.

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.

L

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.

Linux : au sens large, désigne tout système d'exploitation fondé sur le noyau Linux. Le noyau Linux est utilisé sur du matériel informatique allant des téléphones portables (exemple : Android) aux super-ordinateurs en passant par les PC (exemple : Ubuntu).

Live-USB : clé USB qui permet d'amorcer un système d'exploitation situé sur la clé USB, sans utiliser le disque de l'ordinateur. N'importe quelle clé USB peut être transformée en Live-USB.

M

macOS : système d'exploitation développé par Apple pour ses ordinateurs.

Mémoire vive : mémoire informatique dans laquelle sont traitées les informations par un appareil informatique. Sur un ordinateur un manque de mémoire vive va entraîner un fort ralentissement de celui-ci, le système utilisant le disque, beaucoup plus lent, pour combler le manque de mémoire vive.

Mire de test (pour les tests de qualité de service) : un serveur qui ne stocke pas de données, mais qui est en mesure de délivrer des données à très haut débit, afin de permettre de mesurer le débit.

O

ONT *(Optical Network Termination)* : équipement d'un réseau FttH situé chez le client. Un ONT peut être intégré ou externe à la box.

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

P

***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.

***Provisioning* (provisionnement) :** désignant l'allocation automatique de ressources. Par exemple une solution de *provisioning* peut allouer automatiquement les IPv4 et IPv6 aux clients.

Q

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.

R

RGPD (Règlement général sur la protection des données) : règlement n° 2016/679 de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel.

S

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.

T

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.

Test de débit mono-connexion : *(mono-thread* en anglais) test mesurant le débit *via* une seule connexion, ce qui permet de remonter un débit représentatif d'une utilisation d'internet.

Test de débit multi-connexions : *(multi-thread* en anglais) test mesurant le débit en additionnant les débits de multiples connexions simultanées, ce qui permet d'estimer la capacité du lien.

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.

TLS *(Transport Layer Security)* : permet de chiffrer les échanges sur internet et d'authentifier le serveur.

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.

U

Ubuntu : système d'exploitation GNU/Linux basé sur la distribution Linux Debian. Ubuntu est l'un des systèmes d'exploitation composés de logiciels libres les plus utilisés en France.

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.

V

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

W

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

Websocket : protocole réseau qui permet de créer des canaux de communication *full-duplex* par-dessus une connexion TCP pour les navigateurs web. Il est utilisé par de nombreux tests de débit car il permet de meilleures performances que HTTP.

Wehe : application Android et iOS, développée par la Northeastern University en partenariat avec l'Arcep pour détecter des pratiques de gestion de trafic contraires au principe de neutralité du net.

Wi-Fi : protocoles de communication sans fil régis par les normes du groupe IEEE 802.11.

Windows : système d'exploitation propriétaire, développé par Microsoft, qui équipe la majorité des ordinateurs en France.

X

xDSL *(Digital Subscriber Line)* : technologies de communications électroniques utilisées sur les réseaux en cuivre qui permettent aux opérateurs de fournir un accès internet à haut ou très haut débit. Les normes ADSL2+ et VDSL2 sont les normes xDSL les plus utilisées en France pour les accès grand public.

Z

***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 fixe via le réseau 4G.

Annexes

Annexe 1

Mise en place d'une interface de programmation applicative (API) dans les box

1. PARAMÈTRES PRINCIPAUX

Les paramètres principaux sont transmis par l'IAD (pour *Integrated Access Device*) à un outil de mesure de qualité de service à la suite d'une requête effectuée une seule fois lorsqu'un utilisateur réalise un test de mesure de la qualité de service internet.

CONDITION DE PRÉSENCE	ARBRE JSON	NOM DU PARAMÈTRE	UNITÉ	DÉTAIL DU PARAMÈTRE	FORMAT / LISTE DE VALEURS ACCEPTÉES
Obligatoire	Root	ApiVersion		Version de l'API	Entier positif de 64 bits
Obligatoire	TimeStamp	ApiCallTime		Horodatage correspondant à l'heure à laquelle l'API est requêtée	Entier positif de 64 bits
Obligatoire	Gateway	Model		Nom de l'IAD (« box ») du client	texte
Obligatoire	Gateway	HardwareVersion		Version hardware (comme rev3)	texte
Obligatoire	Gateway	SoftwareVersion		Version du logiciel	texte
Obligatoire	Subscription Speed	DownloadMin	Kbit/s	Débit minimum descendant contractuel	Entier positif de 64 bits
Obligatoire	Subscription Speed	UploadMin	Kbit/s	Débit minimum montant contractuel	Entier positif de 64 bits
Obligatoire	Subscription Speed	DownloadMax	Kbit/s	Débit maximum descendant contractuel	Entier positif de 64 bits
Obligatoire	Subscription Speed	UploadMax	Kbit/s	Débit maximum montant contractuel	Entier positif de 64 bits
Obligatoire	Subscription Speed	DownloadNormally	Kbit/s	Débit « normalement disponible » descendant contractuel (s'il existe)	Entier positif de 64 bits
Obligatoire	Subscription Speed	UploadNormally	Kbit/s	Débit « normalement disponible » montant contractuel (s'il existe)	Entier positif de 64 bits
Obligatoire	WAN	Technology		Technologie WAN utilisée par l'IAD (« box »)	["FttH"; "ADSL"; "VDSL"; "Gfast"; "cable"; "satellite"; "2G/3G"; "4G"; "5G"]
Obligatoire si la technologie WAN est FttH	WAN/SpeedOnt	Download	Kbit/s	FttH uniquement : débit descendant Ethernet entre l'ONT et l'IAD. Facultatif : Si détection d'un CPL sur le port WAN : débit brut remonté par le CPL.	Entier positif de 64 bits
Obligatoire si la technologie WAN est FttH	WAN/SpeedOnt	Upload	Kbit/s	FttH uniquement : débit montant Ethernet entre l'ONT et l'IAD Facultatif : Si détection d'un CPL sur le port WAN : débit brut remonté par le CPL.	Entier positif de 64 bits

CONDITION DE PRÉSENCE	ARBRE JSON	NOM DU PARAMÈTRE	UNITÉ	DÉTAIL DU PARAMÈTRE	FORMAT / LISTE DE VALEURS ACCEPTÉES
Obligatoire si la technologie WAN est FttH	WAN/SpeedOnt	Duplex		FttH uniquement : mode Ethernet entre l'ONT et l'IAD	["half";"full"]
Obligatoire si la technologie WAN est xDSL	WAN/ SpeedSynchro	Download	Kbit/s	xDSL uniquement : débit de synchronisation descendant	Entier positif de 64 bits
Obligatoire si la technologie WAN est xDSL	WAN/ SpeedSynchro	Upload	Kbit/s	xDSL uniquement : débit de synchronisation montant	Entier positif de 64 bits
Obligatoire	WAN	Aggregation		Présence d'une agrégation de deux accès WAN active Exemple : xDSL + 4G	["yes";"no"]

Note : concernant les débits commerciaux souscrits par le client :
- le « débit minimum » n'est à remplir que si l'accès possède un débit minimum ;
- le « débit normalement disponible » n'est à remplir que si l'accès possède un débit normalement disponible ;
- le « débit maximum » est à remplir systématiquement en FttH avec le débit contractuel. Pour le xDSL il n'est à remplir que si l'accès possède un débit maximum.

CONDITION DE PRÉSENCE	ARBRE JSON	NOM DU PARAMÈTRE	UNITÉ	DÉTAIL DU PARAMÈTRE	FORMAT / LISTE DE VALEURS ACCEPTÉES
Obligatoire	LAN	Connection Type		Technologie pour joindre l'IAD utilisée par le terminal requêtant l'API. Note : La détection du CPL sur le LAN est facultative.	["wifi";"Ethernet";"cpl" ; "other"]
Obligatoire	LAN/ SpeedLan	Download	Kbit/s	Débit descendant sur le LAN (Ethernet / Wi-Fi / CPL) négocié par le terminal requêtant l'API. CPL : débit brut remonté par le CPL connecté sur le port Ethernet d'où provient la requête de l'API.	Entier positif de 64 bits
Obligatoire	LAN/ SpeedLan	Upload	Kbit/s	Débit montant sur le LAN (Ethernet / Wi-Fi / CPL) négocié par le terminal requêtant l'API.	Entier positif de 64 bits
Obligatoire si la connexion LAN est Ethernet	LAN/ SpeedLan	Duplex		Ethernet *half-duplex* ou *full-duplex*	["half";"full"]
Obligatoire si la connexion LAN est Wi-Fi	LAN/Wi-Fi	Ieee		Norme Wi-Fi IEEE 802.11 négociée entre l'IAD et le terminal requêtant l'API.	Entier positif (802.11a=>1 802.11b=> 2 802.11g=> 3 802.11n=> 4 802.11ac=>5 802.11ax=>6)
Obligatoire si la connexion LAN est Wi-Fi	LAN/Wi-Fi	RadioBand		Bande radio Wi-Fi utilisée par le terminal requêtant l'API. Bloc de fréquence de 2,4 GHz ou bloc de fréquence de 5 GHz.	Entier positif : Bande 2,4 Ghz => 2 Bande 5 Ghz => 5
Obligatoire si la connexion LAN est Wi-Fi	LAN/Wi-Fi	RSSI	dBm	Mesure de la puissance d'un signal radio reçu. C'est le Rssi du terminal requêtant l'API.	Entier positif de 64 bits

Note : certains adaptateurs CPL[1] ne peuvent pas être détectés par l'IAD, de même que les connexions Wi-Fi initiées depuis un point d'accès tiers connecté en Ethernet à l'IAD.

1. 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.

2. PARAMÈTRES LIÉS AU *CROSS-TRAFFIC*

Ces paramètres sont spécifiques au *cross-traffic.* Ils sont récupérés par l'outil de mesure de qualité de service à la suite de **deux requêtes** effectuées :

- immédiatement après que le client a lancé le test de mesure de la qualité de service internet ;
- immédiatement après que l'outil de mesure a terminé la mesure de la qualité de service internet.

L'outil détermine la présence de *cross-traffic* si le nombre d'octets sur l'interface WAN est significativement supérieur au nombre d'octets générés par le test de mesure de la qualité de service en lui-même.

CONDITION DE PRÉSENCE	ARBRE JSON	NOM DU PARAMÈTRE	UNITÉ	DÉTAIL DU PARAMÈTRE	FORMAT / LISTE DE VALEURS ACCEPTÉES
Obligatoire	Root	APIVersion		Version de l'API	Entier positif de 64 bits
Obligatoire	ByteCounter	Download	octets	Relevé du compteur de trafic descendant (internet => IAD) du port WAN	Entier positif de 64 bits
Obligatoire	ByteCounter	Upload	octets	Relevé du compteur de trafic montant (IAD => internet) du port WAN	Entier positif de 64 bits
Obligatoire	TimeStamp	APICallTime		Horodatage correspondant à l'heure à laquelle l'API est requêtée	Entier positif de 64 bits
Obligatoire	TimeStamp	LastUpdate		Horodatage de la dernière mise à jour du compteur du port WAN (le compteur est relevé en temps réel alors LastUpdate = ApiCallTime)	Entier positif de 64 bits

Dans le cas où l'IAD ne peut pas remonter l'information d'un compteur du nombre d'octets sur le port WAN, il conviendra d'utiliser le compteur de paquets multiplié par la MTU *(Maximum Transmission Unit)* afin de fournir une approximation.

Annexe 2

Mires (serveurs) proposées par les différents outils de test de qualité de service

L'Arcep a fait le maximum pour que cette information soit exacte au moment de la publication du document mais il est, par exemple, possible que des évolutions des mires utilisées par les outils soient survenues entre temps.

NPERF

SPONSOR, TEL QU'AFFICHÉ SUR NPERF	VILLE	RÉGION OU PAYS	IPV6	CAPACITÉ DE LA CONNEXION	PORT UTILISÉ	NOM DE L'HÉBERGEUR	AS
SFR	Courbevoie	Île-de-France	IPv4 uniquement	10 Gbit/s	443	SFR	AS15557
Orange	Paris	Île-de-France	IPv4 ou IPv6	10 Gbit/s	443	Orange	AS3215
Orange	Puteaux	Île-de-France	IPv4 ou IPv6	10 Gbit/s	443	Orange	AS3215
Orange	Lyon	Auvergne-Rhône-Alpes	IPv4 ou IPv6	10 Gbit/s	443	Orange	AS3215
Orange	Rennes	Bretagne	IPv4 ou IPv6	10 Gbit/s	443	Orange	AS3215
Bouygues Telecom	Anycast	Île-de-France (Paris) Hauts-de-France (Lille) Auvergne-Rhône-Alpes (Lyon) Région SUD (Marseille) Nouvelle-Aquitaine (Bordeaux)	IPv4 ou IPv6	10 Gbit/s	443	Bouygues Telecom	AS5410
RRT	Compiègne	Hauts-de-France	IPv4 uniquement	10 Gbit/s	443	Renater	AS2200
OVH	Gravelines	Hauts-de-France	IPv4 ou IPv6	10 Gbit/s	443	OVH	AS16276
OVH	Roubaix	Hauts-de-France	IPv4 ou IPv6	10 Gbit/s	443	OVH	AS16276
OVH	Strasbourg	Grand Est	IPv4 ou IPv6	10 Gbit/s	443	OVH	AS16276
DataPacket	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s	443	DataCamp	AS60068
Leonix	Paris	Île-de-France	IPv4 ou IPv6	10 Gbit/s	443	Leonix Telecom	AS50628
Wibox	Saint-Denis	Île-de-France	IPv4 uniquement	10 Gbit/s	443	Altitude Infrastructure	AS49594
Phibee Telecom	Aubervilliers	Île-de-France	IPv4 ou IPv6	10 Gbit/s	8443	Phibee Telecom	AS8487
SHPV France	Toulouse	Occitanie	IPv4 ou IPv6	6 Gbit/s	443	SHPV France	AS41652
Online	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	4 Gbit/s	443	Scaleway – Online	AS12876
Proceau	Paris	Île-de-France	IPv4 uniquement	1 Gbit/s	8443	Proceau	AS43424

SPONSOR, TEL QU'AFFICHÉ SUR NPERF	VILLE	RÉGION OU PAYS	IPV6	CAPACITÉ DE LA CONNEXION	PORT UTILISÉ	NOM DE L'HÉBERGEUR	AS
AppliWave	Vitry-sur-Seine	Île-de-France	IPv4 ou IPv6	1 Gbit/s	443	AppliWave	AS200780
Ikoula	Reims	Grand Est	IPv4 ou IPv6	1 Gbit/s	8443	Ikoula	AS21409
Azylis	Besançon	Bourgogne-Franche-Comté	IPv4 uniquement	1 Gbit/s	443	Azylis	AS207151
Rezopole	Lyon	Auvergne-Rhône-Alpes	IPv4 ou IPv6	1 Gbit/s	443	Rezopole	AS199422
Muona	Lyon	Auvergne-Rhône-Alpes	IPv4 uniquement	1 Gbit/s	443	Muona	AS50818
iDruide	Limonest	Auvergne-Rhône-Alpes	IPv4 uniquement	1 Gbit/s	443	DCforData	AS197685
AOC Telecom	Clermont-Ferrand	Auvergne-Rhône-Alpes	IPv4 uniquement	100 Mbit/s	443	AOC Telecom	AS202328
Célinéo	Lucé	Centre-Val de Loire	IPv4 uniquement	1 Gbit/s	443	CM'IN – Célinéo	AS39271
System-Net	Montpellier	Occitanie	IPv4 uniquement	1 Gbit/s	443	System-Net	AS60427

SPEEDTEST UFC-QUE CHOISIR

Le test utilise une seule mire, composée de deux serveurs à 10 Gbit/s en réparation de charge, qui écoutent sur le port 443 avec une connexion chiffrée.

VILLE	RÉGION	IPV6	CAPACITÉ DE LA CONNEXION	PORT UTILISÉ	NOM DE L'HÉBERGEUR	AS
Saint-Denis	Île-de-France	IPv4 uniquement	20 Gbit/s	443	Zayo France	AS8218

LES TESTS DE DÉBIT FIXE DÉVELOPPÉS PAR QOSI (DÉBITEST 60 / 4GMARK / NETGMARK ZD-NET)

Voici les mires proposées par QoSi pour les tests fixes. Elles écoutent toutes sur le port 8443 et le trafic est chiffré.

VILLE	RÉGION	IPV6	CAPACITÉ DE LA CONNEXION	PORT UTILISÉ	NOM DE L'HÉBERGEUR	AS
Roubaix	Hauts-de-France	IPv4 uniquement	1 Gbit/s	8443	OVH	AS16276
Vitry-sur-Seine ou Saint-Ouen-l'Aumône	Île-de-France	IPv4 uniquement	1 Gbit/s	8443	Scaleway – Online	AS12876

LES TESTS DE DÉBIT MOBILE DÉVELOPPÉS PAR QOSI (4GMARK / DÉBITEST 60 / KICAPTE / TU CAPTES ? / GIGALIS)

SPONSOR, TEL QU'AFFICHÉ SUR L'APPLICATION	VILLE	RÉGION OU PAYS	IPV6	CAPACITÉ DE LA CONNEXION	PORT UTILISÉ	NOM DE L'HÉBERGEUR	AS
SFR	Courbevoie	Île-de-France	IPv4 uniquement	10 Gbit/s	80	SFR	AS15557
Orange France	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s	80	Hivane	AS34019
Bouygues Telecom	Nanterre	Île-de-France	IPv4 uniquement	10 Gbit/s	443	Bouygues Telecom	AS540
Mediactive Network	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s	80	Mediactive Network	AS197133
OneProvider Paris	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	1 Gbit/s	443	Scaleway – Online	AS12876
OneProvider Paris2	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	1 Gbit/s	443	Scaleway – Online	AS12876
OneProvider Paris3	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	1 Gbit/s	443	Scaleway – Online	AS12876
OVH 5GMARK	Roubaix	Hauts-de-France	IPv4 uniquement	1 Gbit/s	443	OVH	AS16276
Ikoula	Reims	Grand Est	IPv4 uniquement	1 Gbit/s	443	Ikoula	AS21409
Adeli	Saint-Trivier-sur-Moignans	Auvergne-Rhône-Alpes	IPv4 uniquement	1 Gbit/s	443	Adeli	AS43142

IPv6-TEST

Voici les mires proposées par IPv6-test. La migration est en cours vers le port 443.

SPONSOR, TEL QU'AFFICHÉ SUR IPV6-TEST	VILLE	RÉGION OU PAYS	IPV6	CAPACITÉ DE LA CONNEXION	PORT UTILISÉ	NOM DE L'HÉBERGEUR	AS
LaFibre.info	Paris	Île-de-France	IPv4 et IPv6	10 Gbit/s	443 ou 80	Bouygues Telecom	AS5410
OVH	Limbourg	Allemagne	IPv4 et IPv6	100 Mbit/s	443 ou 80	OVH	AS16276
ZeelandNet	Zélande	Pays-Bas	IPv4 et IPv6	1 Gbit/s	80 unique-ment	ZeelandNet	AS15542
ServerHouse	Portsmouth	Royaume-Uni	IPv4 et IPv6	1 Gbit/s	80 unique-ment	ServerHouse	AS21472
EBOX	Longueuil	Canada	IPv4 et IPv6	1 Gbit/s	80 unique-ment	EBOX	AS174

SPEEDTEST.NET D'OOKLA

Voici les mires proposées par SpeedTest.net d'Ookla en France. Elles écoutent toutes sur le port 8080 et le trafic est chiffré. Sur les applications mobiles, un mode *Legacy* permet de faire le test en HTTP sur le port 80 si les *websockets* sur le port 8080 sont bloqués.

SPONSOR, TEL QU'AFFICHÉ SUR SPEEDTEST	VILLE	RÉGION OU PAYS	IPV6	CAPACITÉ DE LA CONNEXION	PORT UTILISÉ	NOM DE L'HÉBERGEUR	AS
Orange	Paris	Île-de-France	IPv6 uniquement*	10 Gbit/s	8080	Hivane	AS34019
Naitways	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s	8080	Naitways	AS57119
SFR	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s	8080	SFR	AS15557
SiriusHD	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s	8080	Scaleway – Online	AS12876
fdcservers.net	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s	8080	Cogent	AS174
Interoute VDC	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s	8080	GTT – Interoute	AS8928
Cloudwatt	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s	8080	Cloudwatt	AS60940
Leonix Telecom	Paris	Île-de-France	IPv6 uniquement*	10 Gbit/s	8080	Leonix Telecom	AS50628
Stella Telecom	Courbevoie	Île-de-France	IPv4 uniquement	10 Gbit/s	8080	Stella Telecom	AS16211
ONLINE	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	10 Gbit/s	8080	Scaleway – Online	AS12876
TestDebit.info	Massy	Île-de-France	IPv6 uniquement*	10 Gbit/s	8080	Bouygues Telecom	AS5410
Wibox	Val-de-Reuil	Normandie	IPv4 uniquement	10 Gbit/s	8080	Altitude Infrastructure	AS49594
LaFibre.info	Douai	Hauts-de-France	IPv6 uniquement*	10 Gbit/s	8080	Bouygues Telecom	AS5410
Orange	Lyon	Auvergne-Rhône-Alpes	IPv6 uniquement*	10 Gbit/s	8080	Rezopole	AS199422
LaFibre.info	Lyon	Auvergne-Rhône-Alpes	IPv6 uniquement*	10 Gbit/s	8080	Bouygues Telecom	AS5410
Via Numérica	Archamps	Auvergne-Rhône-Alpes	IPv4 uniquement	10 Gbit/s	8080	Via Numérica	AS44494
LaFibre.info	Bordeaux	Nouvelle-Aquitaine	IPv6 uniquement*	10 Gbit/s	8080	Bouygues Telecom	AS5410
TestDebit.info	Marseille	Région Sud	IPv6 uniquement*	10 Gbit/s	8080	Bouygues Telecom	AS5410
CCleaner	Paris	Île-de-France	IPv4 uniquement	1 Gbit/s	8080	Scaleway	AS12876
HarryLafranc	Paris	Île-de-France	IPv4 uniquement	1 Gbit/s	8080	Hexatom	AS51269
Télécom ParisTech	Paris	Île-de-France	IPv6 uniquement*	1 Gbit/s	8080	Renater	AS1712
Host-Heberg	Paris	Île-de-France	IPv4 uniquement	1 Gbit/s	8080	OVH	AS16276
Ozone	Courbevoie	Île-de-France	IPv4 uniquement	1 Gbit/s	8080	Nomotech – Ozone	AS39886
Vianet	Le Havre	Normandie	IPv4 uniquement	1 Gbit/s	8080	velia.net	AS29066
Eurafibre	Lille	Hauts-de-France	IPv4 uniquement	1 Gbit/s	8080	Eurafibre	AS35625

SPONSOR, TEL QU'AFFICHÉ SUR SPEEDTEST	VILLE	RÉGION OU PAYS	IPV6	CAPACITÉ DE LA CONNEXION	PORT UTILISÉ	NOM DE L'HÉBERGEUR	AS
ePlay TV	Roubaix	Hauts-de-France	IPv6 uniquement*	1 Gbit/s	8080	OVH	AS16276
Techplus. europe	Roubaix	Hauts-de-France	IPv4 uniquement	1 Gbit/s	8080	OVH	AS16276
Ikoula	Reims	Grand Est	IPv6 uniquement*	1 Gbit/s	8080	Ikoula	AS21409
Hexanet	Reims	Grand Est	IPv4 uniquement	1 Gbit/s	8080	Hexanet	AS34863
RIV54	Saulnes	Grand Est	IPv4 uniquement	1 Gbit/s	8080	Vialis	AS42487
Orne THD	Rombas	Grand Est	IPv6 uniquement*	1 Gbit/s	8080	Orne THD	AS41114
Vialis	Woippy	Grand Est	IPv4 uniquement	1 Gbit/s	8080	Vialis	AS42487
Regie Talange	Talange	Grand Est	IPv4 uniquement	1 Gbit/s	8080	Vialis	AS42487
REFO Falck	Falck	Grand Est	IPv4 uniquement	1 Gbit/s	8080	Vialis	AS42487
Enes	Hombourg-Haut	Grand Est	IPv4 uniquement	1 Gbit/s	8080	Vialis	AS42487
Fibragglo	Forbach	Grand Est	IPv4 uniquement	1 Gbit/s	8080	Vialis	AS42487
La Regie	Reichshoffen	Grand Est	IPv4 uniquement	1 Gbit/s	8080	SFR	AS15557
AS Dienstleistungen	Strasbourg	Grand Est	IPv4 uniquement	1 Gbit/s	8080	OVH	AS16276
Rocho DataCenter	Chambéry	Auvergne-Rhône-Alpes	IPv6 uniquement*	1 Gbit/s	8080	OVH	AS16276
Axione	Pau	Nouvelle-Aquitaine	IPv4 uniquement	1 Gbit/s	8080	Axione	AS31167
Orange	Marseille	Région Sud	IPv4 uniquement	1 Gbit/s	8080	Jaguar Network	AS30781
SEACOM	Marseille	Région Sud	IPv6 uniquement*	1 Gbit/s	8080	SEACOM	AS37100
DFOX	Nice	Région Sud	IPv4 uniquement	1 Gbit/s	8080	Scaleway – Online	AS12876
VistaWAN.com	Nice	Région Sud	IPv4 uniquement	1 Gbit/s	8080	Scaleway – Online	AS12876

* Le test est réalisé avec le protocole IPv6 pour tous les clients avec une connectivité IPv6. Il n'est pas possible de forcer le protocole IPv4 sur ces mires. Les clients avec une connectivité IPv4 sans connectivité IPv6 font eux leur test en IPv4.

Annexe 3

Fiabilisation du test de qualité de service

Cette annexe permet d'éclairer l'utilisateur sur les paramètres à prendre en compte afin de fiabiliser son test de qualité de service ou test de débit. Les informations de cette page sont données à titre purement indicatif et ne visent pas l'exhaustivité. Certains outils de mesure de la qualité de service peuvent avoir des prérequis différents. Aussi, vous êtes invités à vous référer aux indications proposées par l'éditeur de l'outil utilisé.

Débit inférieur à 100 Mbit/s : presque toutes les machines équipées de 4 Go de mémoire vive ou plus semblent en mesure de faire des tests à moins de 100 Mbit/s. Seule l'utilisation de Windows XP semble être à éviter dans ce cadre.

Débit entre 100 et 300 Mbit/s, la configuration minimum recommandée inclut :

- Windows 10 et Live-USB Linux : 6 Go de mémoire vive minimum macOS et Linux : 4 Go de mémoire vive minimum ;
- carte réseau qui permet de gérer 1 Gbit/s ;
- câble réseau Ethernet équipé de 4 paires, soit 8 fils (les câbles Ethernet avec 4 fils sont limités à 100 Mbit/s) ;
- processeur équipé du jeu d'instruction dédiées au chiffrement matériel AES : AES-NI *(Advanced Encryption Standard New Instructions).* AES-NI équipe a priori les PC Intel Core-i7 depuis 2011, les PC Intel Core-i5 depuis 2012, les PC AMD depuis 2013, les PC Intel Core-i3 depuis 2014, les PC Intel Pentium et Intel Celeron depuis 2016 ;
- un antivirus qui ne fait pas d'inspection de trafic HTTPS. Certains antivirus proposent une case à décocher pour ne plus faire d'inspection de trafic HTTPS ;
- désactiver les extensions dans le navigateur web qui peuvent dégrader le débit. Certaines extensions entraînent une limitation du débit soit directement soit indirectement via une augmentation de la charge du processeur ;
- spécifiquement pour les tests mono-connexion, il est conseillé de privilégier lorsque cela est possible les systèmes d'exploitation les plus récents (à titre d'exemple, les systèmes d'exploitation Windows 7 ou plus anciens peuvent limiter le débit à cause d'une fenêtre de réception TCP[2] trop faible dans certains cas).

Débit entre 300 Mbit/s et 1 Gbit/s, en plus des prérequis de la section pour un débit de 100 à 300 Mbit/s, la configuration minimum recommandée inclut :

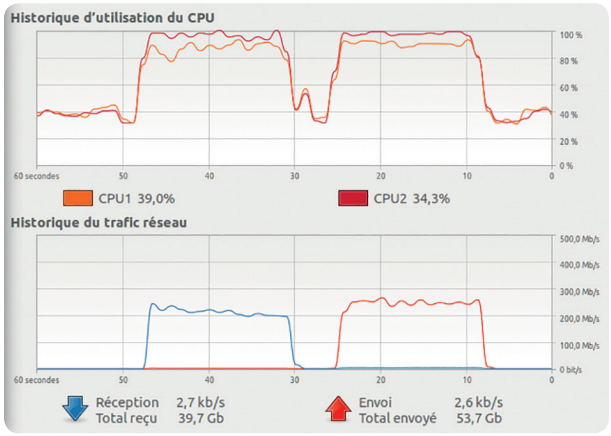
- Windows 10 et Live-USB Linux : 8 Go de mémoire vive minimum macOS et Linux : 6 Go de mémoire vive minimum ;
- un système d'exploitation 64 bits moderne :
  - Windows : Windows 8.1 minimum,
  - Mac OS : Mac OS 10.9 minimum,
  - Ubuntu : Ubuntu 14.04 minimum.
- sélectionner une mire (serveur de test) connecté à internet en 10 Gbit/s ;
- afficher la charge du processeur pendant le test et vérifier que le pourcentage d'utilisation du processeur ne dépasse pas 70 % pendant le test.

Débit supérieur à 1 Gbit/s : il semble aujourd'hui complexe de faire des tests de débit fiables pour les lignes à 10 Gbit/s dans un navigateur web. De plus, à la connaissance des services de l'Arcep pratiquement aucune mire de test n'est connectée avec un lien de plus de 10 Gbit/s à l'internet.

Démarche à suivre pour connaître le pourcentage d'utilisation du processeur pendant un test de qualité de service :

- Windows : cliquer sur le bouton droit sur la barre des tâches et cliquer sur « Gestionnaire des tâches » dans l'onglet « Performance », choisir « Processeur » ;
- macOS : lancer le « Moniteur d'activité ». Dans l'onglet « Processeur », il doit rester au minimum 30 % d'inactif ;
- Ubuntu : lancer l'application « Moniteur système » et cliquer sur l'onglet « Ressources ».

Le graphique représente la charge moyenne du processeur sur un intervalle de temps. Afin de garantir que le test de qualité de service ne soit pas limite, il faut que le pourcentage d'utilisation du processeur ne dépasse pas 70 % pendant le test.



2. Quantité de données reçues susceptibles d'être transférées en une seule fois sur une connexion. L'expéditeur ne peut envoyer que cette quantité de données, puis il doit attendre un accusé de réception et une mise à jour de la fenêtre de la part de l'hôte receveur.

Exemple de démarche à suivre pour vérifier que le processeur est équipé du jeu d'instruction dédié au chiffrement matériel AES :

AES-NI *(Advanced Encryption Standard New Instructions)* permet d'accélérer le traitement :

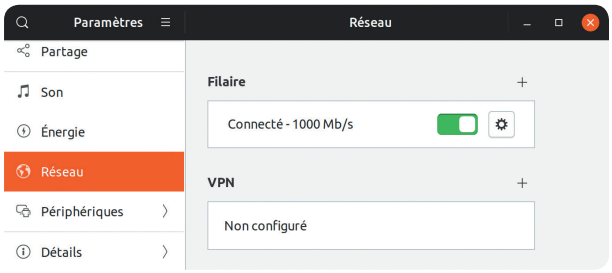
- Windows : Télécharger et lancer CPU-Z (https://www.cpuid.com/softwares/cpu-z.html). Dans l'onglet « CPU », la ligne « Instructions » doit contenir les 3 lettres « AES » ;
- macOS : Télécharger et lancer MacCPUID (https://software.intel.com/en-us/download/download-maccpuid). Dans l'onglet « Features », vérifier que « AES » est supporté ;
- Ubuntu : Lancer le Terminal et écrire « lscpu ». Les 3 lettres « AES » doivent être présente sur le dernier paragraphe.

L'absence des 3 lettres « AES » signifie que le processeur n'embarque pas cette technologie, ce qui peut dégrader les tests de débit.

Spécification	Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz				
Famille	0X6	Modèle	0XE	Temp.	40°C
Famille ét.	0X6	Modèle ét.	0X8E	Stepping	10
Instructions	HT, MMX, SSE(1, 2, 3, 3S, 4.1, 4.2), AVX(1, 2), FMA(3) AES, CLMUL, RdRand, SGX, VT-x, x86-64				

Démarche à suivre pour vérifier que le débit du câble Ethernet est bien à 1 Gbit/s :

- Windows 10 : Dans le menu « Démarrer », lancer « Paramètres », cliquer sur « Réseau et internet » puis « Afficher vos propriétés réseau ». La « Vitesse de connexion » doit afficher 1 Gbit/s.
- macOS : Lancer « Utilitaire de réseau », dans l'onglet « Infos », sélectionner l'interface réseau Ethernet. Le « Débit de la liaison » doit afficher 1 Gbit/s.
- Ubuntu : Lancer « Paramètres », dans l'élément « Réseau », le débit filaire doit afficher 1 000 Mbit/s.



Ce document a été réalisé par l'Arcep

DIRECTION « INTERNET ET UTILISATEURS »
Loïc Duflot, *directeur*

Unité « Internet ouvert »
Pierre Dubreuil, Vivien Guéant, Emmanuel Leroux
et **Samih Souissi,** *chargés de mission*

DIRECTION « ÉCONOMIE, MARCHÉS ET NUMÉRIQUE »
Stéphane Lhermitte, *directeur*

Unité « Analyse économique et intelligence numérique »
Anaïs Le Gouguec, *cheffe de l'unité*
Nisrynne Nahhal et **Vincent Toubiana,** *chargés de mission*

DIRECTION « MOBILE ET INNOVATION »
Anne Laurent, *directrice*

Unité « Couverture et investissements mobiles »
Guillaume Decorzent, *chef de l'unité*
Arnaud Comerzan, *chargé de mission*

DIRECTION « COMMUNICATION ET PARTENARIATS »
Clémentine Beaumont, *directrice*
Anne-Lise Lucas, *chargée de mission*

DIRECTION « AFFAIRES JURIDIQUES »
Elisabeth Suel, *directrice*

Unité « Infrastructures et réseaux ouverts »
Agate Rossetti, *cheffe de l'unité*
Annabel Gandar et **Mélissa Nobileau,** *chargées de mission*

Un grand merci à...

Toutes les personnes consultées, auditionnées ou ayant participé à la démarche de co-construction de l'Arcep sur la qualité de service d'internet ou à l'atelier IP❤6 pour leur dynamisme et leur contribution précieuse au présent rapport.

Publication
Arcep
14, rue Gerty Archimède - 75012 Paris
01 40 47 70 00 - com@arcep.fr

Design
Agence Luciole

Impression
Corlet Imprimeur
ZI, rue Maximilien Vox,
Condé-sur-Noireau,
14110 Condé-en-Normandie

Crédits photos
Pages 6 et 7 : Kiblind,
pages 15, 21, 24, 35, 38
et 62 : IStock/Getty Images,
page 41 : Florence Gaty /
Internet Society,
pages 52 à 55 : Kiblind

Juin 2019

L'ARCEP, LES RÉSEAUX COMME BIEN COMMUN

Les réseaux d'échanges internet, télécom fixes, mobiles et postaux, constituent une **« infrastructure de libertés ».** Liberté d'expression et de communication, liberté d'accès au savoir et de partage, mais aussi liberté d'entreprise et d'innovation, enjeu clé pour la compétitivité du pays, la croissance et l'emploi. Parce que le plein exercice de ces libertés est essentiel dans une société ouverte, innovante et démocratique, les institutions nationales et européennes veillent à ce que les réseaux d'échanges se développent comme un **« bien commun »,** quel que soit leur régime de propriété, c'est-à-dire qu'ils répondent à des exigences fortes en termes d'accessibilité, d'universalité, de performance, de neutralité, de confiance et de loyauté.

À cette fin, les institutions démocratiques ont jugé qu'une intervention étatique indépendante était nécessaire pour veiller à ce qu'aucune force, qu'elle soit économique ou politique, ne soit en situation de contrôler ou de brider la capacité d'échange des utilisateurs (consommateurs, entreprises, associations, etc.).

L'Autorité de régulation des communications électroniques et des postes (Arcep), arbitre expert et neutre au statut d'autorité administrative indépendante, est **l'architecte** et le **gardien** des réseaux d'échanges en France.

Architecte des réseaux, l'Arcep crée les conditions d'une organisation plurielle et décentralisée des réseaux. Elle garantit l'ouverture du marché à de nouveaux acteurs et à toutes les formes d'innovation, et veille à la compétitivité du secteur à travers une concurrence favorable à l'investissement. L'Arcep organise le cadre d'interopérabilité des réseaux, afin qu'ils apparaissent comme un seul aux yeux des utilisateurs malgré leur diversité, simples d'accès et non cloisonnés. Elle coordonne la bonne articulation public/privé dans le cadre de l'intervention des collectivités territoriales.

Gardien des réseaux, l'Arcep s'assure du respect des principes essentiels pour garantir la capacité d'échange des utilisateurs. Elle veille à la fourniture du service universel, et accompagne les pouvoirs publics pour étendre la connectivité sur l'ensemble du territoire. Elle assure la liberté de choix et la bonne information des utilisateurs, et protège contre les atteintes possibles à la neutralité de l'internet.

L'Autorité lutte plus généralement contre toutes les formes de silos qui pourraient menacer la liberté d'échanger sur les réseaux, et s'intéresse à ce titre aux nouveaux intermédiaires que sont les grandes plateformes internet.