ÉDITION 2020

TOME 3

RAPPORT D'ACTIVITÉ

L'état d'internet en France

arcep

République française - juin 2020

RAPPORT D'ACTIVITÉ

L'état d'internet en France

arcep

SOMMAIRE

ÉDITO

Allions générosité d'internet et exigence environnementale

La crise sanitaire et le confinement de la population en France nous ont rappelé à quel point les réseaux sont indispensables à la vie du pays. Cette crise inédite a aussi confirmé combien les réseaux sont et doivent rester un « bien commun ». Garantir l'accessibilité, le bon fonctionnement et l'ouverture d'internet est plus que jamais nécessaire.

Par
Sébastien Soriano,
président de l'Arcep

La mobilisation exemplaire des équipes des opérateurs et de l'ensemble de leurs sous-traitants a assuré sur le terrain le fonctionnement et la maintenance des réseaux. Je tiens une fois encore à saluer cette mobilisation. Au-delà, les infrastructures ont aussi montré leur résilience et ont permis aux opérateurs de maîtriser les risques potentiels de congestion. Cela est le fruit d'un modèle de déploiement des infrastructures qui a montré toute sa solidité. L'orientation de la régulation en faveur de l'investissement dans les infrastructures, 10,4 milliards d'euros l'an dernier, a montré toute sa pertinence, aussi bien dans la fibre que dans la 4G.

La responsabilité collective des acteurs et utilisateurs est intrinsèquement liée à l'idée même de bien commun. C'est ce qui a permis que le plus grand nombre puisse continuer d'avoir accès à des réseaux performants. Dès le début de la crise, l'ensemble des acteurs se sont rapidement organisés pour prévenir une éventuelle congestion des réseaux. Le Gouvernement et l'Arcep ont mis en place avec les opérateurs un dialogue permanent pour anticiper les risques. Les grands fournisseurs de contenu et de services ont, de leur propre initiative ou dans le cadre d'un dialogue avec les pouvoirs publics, diminué leur empreinte sur les réseaux. Les utilisateurs ont aussi été invités par l'Arcep, le Gouvernement et les opérateurs à adopter des réflexes pouvant contribuer à lisser la charge sur les réseaux.

Sans que l'on sache vraiment si tout cela est derrière nous, ce bouleversement inédit qu'est la crise sanitaire nous permet d'ores et déjà de tirer quelques enseignements, en dehors du besoin évident et impérieux de connectivité.

Tout d'abord, le cadre réglementaire de la neutralité du net en Europe a une fois encore donné les preuves de toute sa capacité d'adaptation et sa pertinence. Plus encore, elle montre un chemin. Lorsqu'il s'agit de gouvernance des biens communs, la loi de la multitude sera toujours plus porteuse que la loi du plus fort. Les régulateurs européens membres du BEREC[*] et la Commission européenne ont rappelé ces principes pendant la crise. L'Arcep a veillé à la pleine application de ce principe dans les conditions particulières de la période et continuera à être le gardien de la neutralité d'internet.

Cette période et les différents événements qui l'ont jalonnée ont aussi pu nous amener à réfléchir à un cadre plus clair en la matière. Au-delà de l'obligation de non-discrimination imposée aux opérateurs, l'impact majeur des grands fournisseurs de contenus et de services sur les réseaux mérite l'attention. Le dialogue entre ces acteurs et les opérateurs pour améliorer la gestion des réseaux a parfois semblé à géométrie variable, lors du lancement de nouveaux services, de l'ouverture de certaines options ou de la mise en ligne de mises à jour de certains jeux vidéo particulièrement courus par exemple. Il serait bon de pouvoir instaurer un mécanisme de dialogue pour permettre aux opérateurs d'anticiper de tels événements. Par ailleurs, l'efficacité des mesures d'optimisation apportées par les fournisseurs de services en ligne (réduction du format vidéo) sur leur consommation en bande passante sera à évaluer. Entendons-nous bien, l'innovation sans permission doit rester la règle pour tous, mais la poignée de grands OTT* dont les usages structurent le dimensionnement des réseaux devrait s'obliger à un dialogue systématique.

Bien qu'éloigné des sujets portés par l'Arcep, le développement de solutions de traçage des contacts grâce au numérique pour lutter contre l'épidémie a aussi confirmé tout l'enjeu de l'internet ouvert au-delà des seuls opérateurs télécoms. Eu égard au rôle décisif joué par les deux plus grands fournisseurs de systèmes d'exploitation (OS*) mobiles, il apparaît toujours plus indispensable de pouvoir questionner ces acteurs sur leurs choix technologiques et les entraves qu'ils imposent aux développeurs d'applications. Est-il vraiment acceptable que des acteurs privés puissent, par leurs décisions techniques, influer sur les choix faits par un État démocratique comme le nôtre en matière de santé publique ? C'est la question que cette crise sanitaire invite à se poser, indépendamment des débats de fond sur l'outil lui-même. L'extension du principe d'internet ouvert aux OS, que l'Arcep propose aux pouvoirs politiques depuis 2018, apparaît plus que jamais d'actualité.

Enfin, la période que nous avons traversée nous a confirmé combien il était urgent de poser la question environnementale au centre de nos actions. L'Arcep s'engage fermement dans cette voie, à travers le lancement de la plateforme de travail « pour un numérique soutenable », dans le prolongement de la dynamique engagée l'an passé dans le cadre du cycle « Réseaux du futur ».

Pour la première fois, le rapport sur l'état d'internet en France de l'Arcep consacre un chapitre entier à la question environnementale. Y figurent notamment le rappel des connaissances chiffrées disponibles sur l'empreinte carbone du numérique et l'exposé des premières actions mises en place par l'Arcep pour mesurer l'impact environnemental d'un secteur qui représente aujourd'hui environ 3 % des émissions mondiales de gaz à effet de serre.

Pour autant, gardons-nous d'un contresens. La nécessaire sobriété du numérique ne doit pas s'entendre comme la limitation des échanges en ligne. La crise a montré combien ces échanges étaient cruciaux à la vie de la Nation et nulle autorité ne pourrait s'ériger en juge des bons ou des mauvais usages dans la démocratie. La profusion d'internet doit rester une source inépuisable de vitalité, d'expression et d'innovation. Le défi qui nous attend est autrement plus fin : c'est en décortiquant les chaînes techniques des différents usages que l'on pourra responsabiliser chaque maillon et veiller à une limitation globale de l'empreinte environnementale du numérique, dans une logique d'éco-conception.

Ce rapport sur l'état d'internet en France, qui constitue le tome 3 du rapport d'activité de l'Arcep, donne des clés pour comprendre le bon fonctionnement d'internet, avant et pendant la crise, en présentant l'évolution des principales composantes d'internet sur l'année 2019 : qualité de service, interconnexion des données, transition vers IPv6, neutralité d'internet, ouverture des terminaux et rôle des plateformes.

Outre les enjeux déjà mentionnés, l'actualité des réseaux télécoms soulève de nombreuses questions de société : souveraineté, inclusion numérique, vie privée, etc. Ces enjeux, qui ne relèvent pas directement du périmètre d'action de l'Arcep, ne sont pas étudiés en détail dans ce rapport. Les travaux de l'Autorité en matière d'accessibilité et de couverture sont présentés dans les tomes 1 et 2 de son rapport d'activité.

Rappelons enfin que l'action de l'Arcep ne serait rien sans la mobilisation pleine et entière de l'ensemble des parties intéressées, à qui nous avons voulu donner l'occasion de s'exprimer dans ce rapport. Qu'ils en soient remerciés.

* Voir lexique.

Les réseaux pendant la crise sanitaire

Le présent rapport sur l'état d'internet porte un regard sur les activités de l'Arcep et les événements survenus en 2019. Néanmoins, la crise sanitaire et le confinement du printemps 2020 ont eu de forts impacts sur les usages des réseaux, et l'Arcep propose dans ce chapitre une synthèse de ses observations à date et les premiers enseignements tirés de cette période.

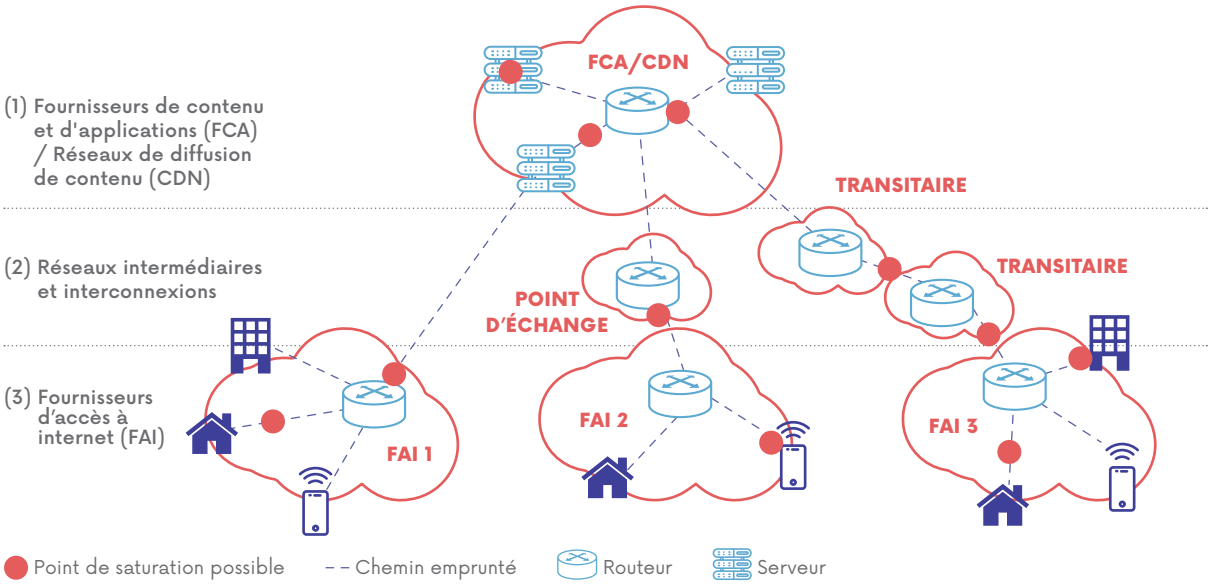
L'Arcep se concentre ici sur les thématiques abordées dans le rapport, et n'abordera donc pas, pour importantes qu'elles soient, les questions liées à l'inclusion numérique soulevées dans le cadre de cette crise.

La volumétrie du trafic internet varie, en règle générale, très sensiblement au cours de la journée et en fonction du jour de la semaine. En temps normal en effet, le trafic internet connaît un pic le soir, du fait d'usages relativement consommateurs en bande passante (vidéo notamment), et durant les week-ends. Ce sont ces pics d'utilisation qui déterminent le dimensionnement des réseaux. La crise sanitaire du Covid-19 a illustré le besoin et la nécessité pour les citoyens français de rester connectés à leur environnement professionnel, personnel et culturel depuis leur domicile. Ce basculement de nombreux usages au sein des foyers a entraîné une forte augmentation du trafic, de 30 % pendant le confinement selon les premières estimations[1], mais aussi une modification importante du profil de trafic, avec le pic de trafic habituellement constaté en soirée, étalé sur toute la journée.

Cette situation a posé un certain nombre de questions sur le fonctionnement d'internet, liées à des thèmes abordés dans ce rapport : le dimensionnement des réseaux était-il suffisant pour supporter l'augmentation de trafic liée à la crise ? Quels étaient les principaux risques de congestion ? Quelles ont été les bonnes pratiques à adopter pour qu'internet continue à fonctionner ? Comment garantir le respect de la neutralité du net dans cette situation exceptionnelle ?

LE DIMENSIONNEMENT DES RÉSEAUX ÉTAIT-IL SUFFISANT POUR SUPPORTER L'AUGMENTATION DE TRAFIC LIÉE À LA CRISE ? QUELS ÉTAIENT LES PRINCIPAUX RISQUES DE CONGESTION ?

SCHÉMA SIMPLIFIÉ DES POINTS POSSIBLES DE SATURATION DES RÉSEAUX



Source : Arcep

1. Étude Netscout à partir des données des fournisseurs d'accès à internet français.

Un utilisateur qui se connecte à internet pour accéder à un contenu ou un service particulier (par exemple navigation web, visioconférence, *streaming* vidéo, téléchargement, etc.) peut faire face à une indisponibilité de ce service ou contenu, voire de plusieurs services à la fois. Cette indisponibilité peut être due à une surcharge au niveau du réseau ou du système d'information d'un maillon de la chaîne technique qui permet d'acheminer le trafic du serveur hébergeant le contenu au terminal de l'utilisateur.

Des saturations peuvent parfois survenir au niveau du réseau local (LAN) du domicile de l'utilisateur final, par exemple à cause d'une sursollicitation du Wi-Fi[2]. Au-delà de ces limitations au niveau de l'utilisateur final, cette partie se focalise sur les risques de congestion qui peuvent avoir lieu au niveau des différents acteurs de la chaîne d'internet. D'une façon plus simple, et comme indiqué dans le schéma, les problèmes de congestion peuvent ainsi survenir à 3 niveaux : au niveau du fournisseur de contenu et d'applications (FCA) ou du réseau de diffusion de contenu (CDN) (1), au niveau des réseaux intermédiaires et interconnexions (2) et au niveau du réseau du fournisseur d'accès à internet (FAI) (3).

- Au niveau du FCA/CDN (1), des congestions peuvent tout d'abord se situer au niveau des serveurs, quand un service est bien plus sollicité que normalement. Cette saturation peut être liée à une limitation matérielle (processeur, mémoire, carte réseau, etc.) ou à une limitation logicielle (dépassement du nombre maximum d'utilisateurs simultanés, de fichiers ouverts, de ports TCP ouverts, etc.). De nombreux autres points de congestion sont possibles au niveau du FCA/CDN : les liens, les équipements d'agrégation, de collecte, de *firewall*[3] et de routage peuvent limiter le trafic, si on dépasse leur capacité (physique ou souscrite) en octets par seconde ou paquets par seconde.
- Au niveau des réseaux intermédiaires et des interconnexions (2), des congestions peuvent survenir au niveau des liens s'ils ne sont pas suffisamment dimensionnés par rapport au trafic qui y circule. Cette congestion peut se manifester en général au niveau d'un lien de *peering* privé, d'un lien de *peering* public (au niveau d'un IXP), entre un FCA et un transitaire, entre deux transitaires ou entre un transitaire et un FAI. Selon le point de congestion, la saturation peut impacter un ou plusieurs services et un ou plusieurs acteurs. Les acteurs d'internet prévoient en général un surdimensionnement et une redondance des interconnexions pour faire face à des événements exceptionnels comme les grandes manifestations sportives. La situation liée à la crise Covid-19 était inédite et a provoqué une montée en charge importante pour les réseaux.
- Au niveau du réseau du FAI (3), des congestions peuvent avoir lieu à différents niveaux : au niveau de l'accès qu'il soit fixe ou mobile, au niveau du réseau de transport/collecte du FAI ou au niveau du cœur du réseau du FAI. En effet, quand un client souscrit une connexion internet fixe, le débit ne lui est pas dédié de bout en bout (hors offre spécifique) : à chaque point du réseau, une capacité plus importante est partagée entre les différents utilisateurs, en partant du principe que tous les utilisateurs n'utilisent pas leur connexion au débit maximum simultanément[4]. Le dimensionnement est aussi réalisé de façon à ne pas saturer, mais une situation inhabituelle peut potentiellement entraîner des congestions. Par ailleurs, des saturations de l'accès internet mobile peuvent survenir au niveau d'une cellule notamment quand plusieurs utilisateurs qui y sont connectés sollicitent des services qui consomment beaucoup de bande passante (*streaming* vidéo, visioconférence, téléchargement, etc.).

Lors de la crise, des saturations sont apparues au niveau de nombreux fournisseurs de contenu, perturbant l'accès à plusieurs services (services de visioconférences, *e-learning*, etc.). Des tensions très locales sur l'accès à internet mobile ont aussi été constatées ponctuellement.

Au-delà du réseau internet, des congestions peuvent aussi apparaître sur le réseau voix. Cela a été constaté dans les premiers jours de confinement : en effet, la forte augmentation des appels téléphoniques avait entraîné des saturations ponctuelles et temporaires sur le réseau voix. Le redimensionnement des interconnexions concernées par les opérateurs a permis d'améliorer rapidement la situation.

Grâce, d'une part, aux capacités et performances des réseaux de télécommunications, et d'autre part à la mobilisation des différents acteurs de l'écosystème, les réseaux en France n'ont pas connu de congestion majeure durant la période de confinement liée au Covid-19 entre mars et mai 2020. Pour autant, au-delà de cette crise, l'augmentation des usages se poursuit sur le long terme et nécessite une montée en débit des infrastructures au travers du déploiement de la fibre et de la 5G.

2. Voir partie suivante sur l'optimisation des usages.
3. Voir lexique.
4. La norme GPON permet par exemple de mettre un maximum de 128 clients sur un arbre proposant 2488 Mbit/s descendants et 1244 Mbit/s montants. Plusieurs dizaines d'arbres GPON sont ensuite concentrés et souvent connectés au réseau par un lien 10 Gbit/s.

QUELLES ONT ÉTÉ LES BONNES PRATIQUES POUR QU'INTERNET CONTINUE À FONCTIONNER ?

La mobilisation exceptionnelle de tous les acteurs de l'écosystème (opérateurs, fournisseurs de contenu et d'applications, utilisateurs finals et institutions publiques) a permis de faire face à l'intensité inédite des besoins numériques durant la crise.

Tout d'abord, les entreprises télécoms et le tissu de PME, d'acteurs locaux et associations qui les entourent ont travaillé de concert pour maintenir et assurer le fonctionnement continu des réseaux. En plus de la mobilisation de leurs équipes sur le terrain, les opérateurs ont également multiplié les gestes commerciaux à destination de leurs clients confinés : données mobiles supplémentaires offertes, communications téléphoniques gratuites, accès libre aux chaînes de télévision payantes, augmentation du débit sur certaines offres, etc.

Suite à un dialogue proactif initié par le Gouvernement ou de leur propre initiative, les fournisseurs de contenu et d'applications ont également contribué à l'effort collectif. Les « grands » utilisateurs des réseaux, telles les les plateformes de *streaming* vidéo ou encore les plateformes de jeux en ligne, ont réduit la charge de leurs contenus en circulation en limitant la bande passante requise par leurs services, en diminuant la qualité de leurs vidéos ou encore en programmant les téléchargements et les mises à jour de leurs services en période de faible affluence. Le dialogue mis en place entre Disney et les opérateurs a aussi permis d'anticiper le lancement de la plateforme de *streaming* vidéo Disney+. En effet, à la différence d'autres FCA, l'architecture retenue par Disney ne reposait pas sur son propre CDN mais sur le recours à des CDN tiers, pouvant ainsi saturer un lien d'interconnexion partagé avec de multiples autres contenus en cas de pic d'utilisation lié au lancement de la plateforme. Le redimensionnement de certaines interconnexions a donc pu être nécessaire pour prévenir d'éventuels risques de congestion des réseaux.

MOBILISATION DES ACTEURS DE L'ÉCOSYSTÈME DURANT LA CRISE SANITAIRE

Source : Arcep

Cette situation illustre la nécessité d'un dialogue proactif entre les opérateurs et les principaux fournisseurs de contenu et d'applications pour favoriser l'anticipation des événements pouvant avoir un impact sur la charge des réseaux.

De même, les utilisateurs finals ont également pu contribuer à l'effort collectif pour les réseaux, en adaptant leurs usages notamment guidés par les recommandations du Gouvernement et de l'Arcep sur les bonnes pratiques à suivre par exemple en matière de télétravail[5] ou encore les recommandations de l'Arcep pour améliorer la qualité de son Wi-Fi[6]. Ainsi, les utilisateurs finals qui ont suivi ces recommandations ont basculé certains de leurs usages de la 4G au Wi-Fi, optimisé l'utilisation de leur Wi-Fi (par exemple en utilisant des répéteurs Wi-Fi), séquencé leurs usages numériques dans la journée et reporté aux heures creuses les usages lourdement consommateurs en bande passante.

Durant toute la crise, le Gouvernement et l'Arcep ont opéré un suivi quotidien de l'évolution des réseaux télécoms. Ainsi, en complément des dispositifs directement dédiés à la gestion opérationnelle de la crise, les opérateurs ont transmis au Gouvernement et à l'Arcep tous les jours puis de façon plus espacée les données relatives à l'état de leurs réseaux. De plus, la résilience des réseaux télécoms étant aussi une question transnationale, les régulateurs européens dont l'Arcep ont activement contribué au suivi de l'état des réseaux européens au sein du BEREC. Enfin, l'Arcep et le Gouvernement ont aussi ouvert, dès les premiers jours de la crise, un dialogue avec les opérateurs pour s'assurer du respect du principe de neutralité de net malgré les conditions exceptionnelles.

COMMENT GARANTIR LE RESPECT DE LA NEUTRALITÉ DU NET DANS CETTE SITUATION EXCEPTIONNELLE ?

Pour répondre à cette demande exceptionnelle et démultipliée de connectivité, les fournisseurs d'accès à internet ont rapidement émis l'hypothèse de devoir prioriser l'acheminement dans leurs réseaux de certains contenus jugés essentiels (notamment le télétravail, l'enseignement à distance ou encore la télémédecine) afin d'assurer leur fonctionnement continu. Parfois présentée comme la solution pour contenir l'augmentation des flux en circulation en période de crise, cette dernière n'est pas si simple en pratique, notamment lorsqu'il est question de distinguer des flux similaires (exemple : la visioconférence du *streaming* vidéo) ou encore lorsque des services sont détournés de leurs usages premiers (exemple : le recours à des plateformes de jeux vidéo à des fins d'enseignement pédagogique). Si à situation exceptionnelle, mesure exceptionnelle, qu'en est-il de la validité de cette pratique au regard du règlement internet ouvert ?

Selon l'article 3 du règlement internet ouvert, les FAI sont tenus de traiter tout le trafic de façon égale et non discriminatoire quelles que soient la nature et l'origine des données en circulation dans leurs réseaux. Le traitement différencié de certains contenus est donc strictement encadré par le règlement internet ouvert, mais peut toutefois s'inscrire dans l'une des trois exceptions explicitement prévues par ce dernier : l'obligation de respecter une autre disposition légale, la nécessité pour un FAI de préserver la sécurité de son réseau et enfin le risque d'une congestion imminente. C'est dans le cadre légal de cette dernière exception que l'Arcep a ouvert un dialogue proactif avec les opérateurs sur les éventuelles mesures de gestion de trafic envisagées par ces deniers en lien avec la crise sanitaire.

Au regard du règlement internet ouvert, les fournisseurs d'accès à internet pouvaient, si besoin, prendre des mesures exceptionnelles de gestion de trafic afin de réduire les effets d'une congestion imminente survenant dans leurs réseaux. Toutefois, bien qu'exceptionnelles, ces mesures doivent aussi respecter certaines conditions : permettre de résorber le phénomène de congestion, être les moins contraignantes possible à l'égard du trafic en circulation, traiter de manière égale les catégories de trafic équivalentes et ne pas être appliquées plus longtemps que nécessaire. Ces critères permettent d'assurer la pérennité d'un traitement non discriminatoire entre fournisseurs de contenus similaires, y compris lors de la mise en œuvre de mesures exceptionnelles de gestion de congestion par les FAI.

La question de la résilience des réseaux de télécommunication s'est également posée au niveau européen. Dans une déclaration conjointe[7], la Commission européenne et le BEREC ont rappelé la possibilité pour les opérateurs de recourir à de telles mesures exceptionnelles de gestion de trafic en cas de congestion imminente. Ainsi, malgré la gravité et la dureté de la crise sanitaire, le règlement internet ouvert a montré sa capacité à s'appliquer en toutes circonstances.

5. Bonnes pratiques sur l'utilisation d'internet en télétravail publiées par l'Arcep : https://www.arcep.fr/demarches-et-services/utilisateurs/teletravail-et-connexion-internet.html
6. Cinq astuces pour améliorer la qualité de son signal Wi-Fi : https://www.arcep.fr/demarches-et-services/utilisateurs/comment-ameliorer-la-qualite-de-son-wifi.html
7. Déclaration conjointe de la Commission européenne et du BEREC sur la manière de faire face à la demande accrue de connectivité des réseaux due à la pandémie liée au Covid-19 : https://berec.europa.eu/eng/document_register/subject_matter/berec/others/9236-joint-statement-from-the-commission-and-the-body-of-european-regulators-for-electronic-communications-berec-on-coping-with-the-increased-demand-for-network-connectivity-due-to-the-covid-19-pandemic

PARTIE 1

Assurer le bon fonctionnement d'internet

CHAPITRE 1

Améliorer la mesure
de la qualité d'internet

CHAPITRE 2

Superviser l'interconnexion
de données

CHAPITRE 3

Accélérer la transition vers IPv6

CHAPITRE 1

Améliorer la mesure de la qualité d'internet

À RETENIR

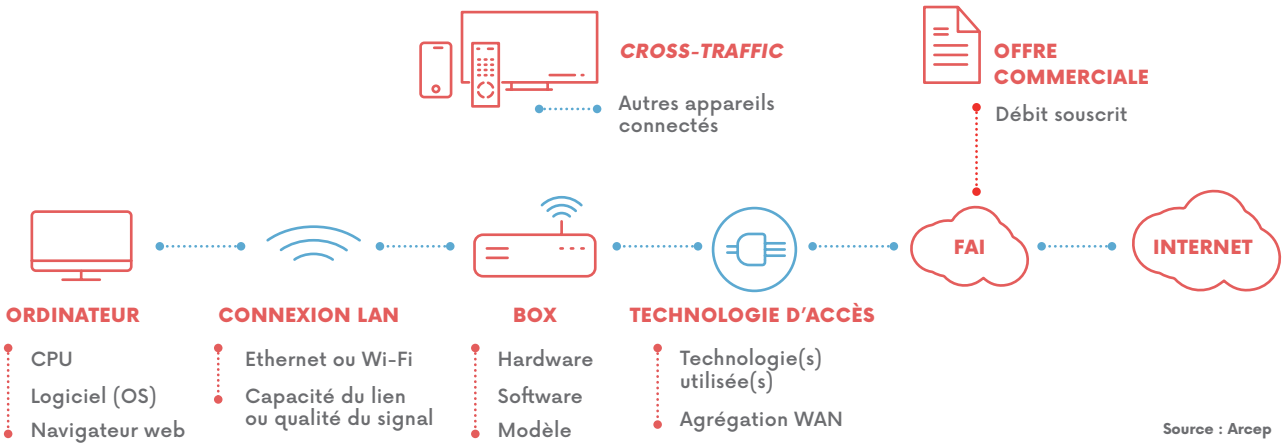
Le 16 janvier 2020
marque le début du calendrier de déploiement dans les box de l'API « carte d'identité de l'accès », qui sera accessible aux outils respectant le Code de conduite de l'Arcep. Objectif : améliorer la mesure de la qualité d'internet.

47 %
des signalements
reçus sur la plateforme « J'alerte l'Arcep » concernent un problème lié à qualité et la disponibilité des services fixes ou mobiles.

La qualité du service de données mobiles a fait un bond conséquent depuis 2018 : le débit moyen en France métropolitaine atteint **45 Mbit/s** en 2019 (+50 % en un an).

Si les offres internet, notamment FttH, évoluent régulièrement pour proposer toujours plus de débit, les usages évoluent également et pour certains sont sensibles au débit disponible. De nombreux clients souhaitent donc mesurer la qualité de service dont ils disposent à domicile, mais aussi en mobilité.

CARACTÉRISTIQUES DE L'ENVIRONNEMENT UTILISATEUR



Source : Arcep

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 (QoS) 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 de la page précédente 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. Les biais potentiels sont développés dans les sections suivantes.

2. LA MISE EN PLACE DE L'API DANS LES BOX POUR CARACTÉRISER L'ENVIRONNEMENT UTILISATEUR

Alors que sur les réseaux mobiles les applications de test de débit sont à même d'identifier l'environnement utilisateur (technologie radio, intensité du signal, etc.), sur les réseaux fixes, la mesure de la qualité de service est particulièrement complexe : il est à ce jour quasi impossible techniquement pour un outil de mesure (souvent appelé « *speed test* ») de connaître avec certitude la technologie d'accès (cuivre, câble, fibre, etc.) sur laquelle a été réalisé un test. Ce manque de caractérisation de la mesure, qui ne permet pas d'isoler des facteurs susceptibles de modifier fortement les résultats, rend les données difficilement exploitables, voire, dans certains cas, induit en erreur le consommateur.

Dans ce contexte, l'Arcep a lancé en début d'année 2018 un vaste chantier sollicitant toutes les parties prenantes afin de résoudre les difficultés de mesure de la qualité de service des réseaux fixes. Cette démarche de co-construction[1] initiée par l'Arcep implique une vingtaine d'acteurs dont des outils de mesure en *crowdsourcing*, des opérateurs, des organismes de protection des consommateurs et des acteurs académiques. Pour permettre aux acteurs de la mesure de mieux caractériser l'environnement utilisateur, l'écosystème a convergé vers la mise en place d'une *Application Programming Interface* (API) implémentée directement dans les box des opérateurs et accessible aux outils de mesure qui respectent le Code de conduite publié par l'Arcep[2]. Cette interface logicielle permettra de transmettre les informations qui constituent la « carte d'identité de l'accès ».

Une consultation publique a été menée au printemps dernier sur ce projet ; les dix-sept contributions reçues et publiées[3] par l'Arcep ont permis d'ajuster, en concertation avec les acteurs de l'écosystème, les modalités de mise en œuvre de l'API. L'Arcep a adopté la décision correspondante fin octobre 2019[4] et le Gouvernement a homologué cette décision par un arrêté publié au *Journal Officiel* le 16 janvier 2020[5].

L'API « carte d'identité de l'accès » a pour objectif de caractériser l'environnement de la mesure. Cette API sera accessible à des outils de mesure en *crowdsourcing* utilisés par les usagers pour évaluer le débit ou plus généralement la qualité de service de leurs accès internet. Sollicitée uniquement lorsque l'utilisateur initie un test de débit, et sous son contrôle, l'API renseignera l'outil de mesure sur une série d'indicateurs techniques, tels que le type de box, la technologie d'accès à internet, les débits montants ou descendants contractuels. La liste exhaustive des indicateurs remontés est détaillée dans l'annexe 1 du présent rapport.

Opérateurs et box concernés, paramètres techniques remontés, calendrier de mise en place, spécifications techniques d'implémentation sont précisés dans la décision de l'Arcep.

Les modalités de fonctionnement de l'API prennent pleinement en compte les questions de respect et de protection de la vie privée des utilisateurs. D'abord, les données recueillies par l'API ne sont évidemment pas transmises à l'Arcep. Ensuite, aucune donnée liée à l'identification de l'utilisateur (identifiant, nom, localisation, etc.) n'est transmise par l'API aux outils de mesure. Enfin, l'API n'est sollicitée que lors d'un test de débit initié par l'utilisateur lui-même et ne répond pas aux sollicitations depuis internet. Questionnée dans le cadre de cette démarche, la CNIL a pu s'assurer que le dispositif répondait dans son principe aux exigences en matière de protection des données personnelles tout en insistant sur l'importance du rôle de conseil de l'Arcep, notamment au travers du « Code de conduite de la qualité de service internet », vis-à-vis des outils de mesure exploitant l'API.

Les résultats obtenus, désormais qualifiés, seront un nouveau pas dans l'amélioration de la mesure de la qualité de service des réseaux fixes.

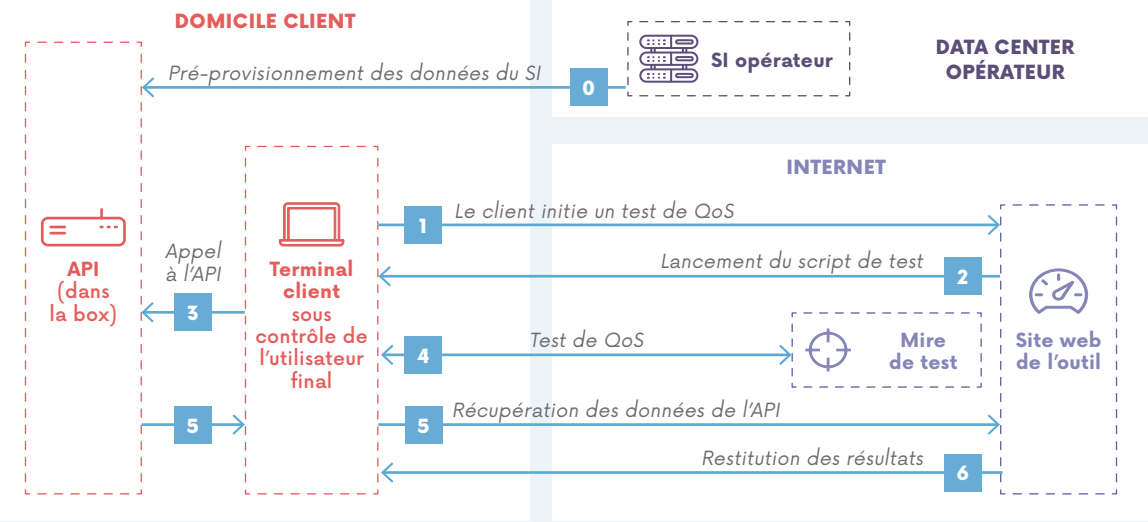
1. La démarche de co-construction de l'API est décrite dans le rapport 2018 sur l'état d'internet en France : https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-2018_conf050618.pdf#page=11
2. Édition 2018 du Code de conduite de la qualité de service internet : https://www.arcep.fr/uploads/tx_gspublication/code-de-conduite-qs-internet-2018_FR.pdf
3. Réponses reçues à la consultation publique : https://www.arcep.fr/uploads/tx_gspublication/reponses_consultation_publique_api_box-oct2019.zip
4. Décision n° 2019-1410 de l'Arcep en date du 10 octobre 2019 : https://www.arcep.fr/uploads/tx_gsavis/19-1410.pdf
5. Arrêté du 8 janvier 2020 homologuant la décision n° 2019-1410 de l'Arcep : https://www.arcep.fr/fileadmin/cru-1582218129/reprise/textes/arretes/2020/arr-08012020-homolog-2019-1410-api-box.pdf

PLUS D'INFORMATIONS SUR L'API « CARTE D'IDENTITÉ DE L'ACCÈS »

Comment fonctionne l'API ?

Le schéma suivant décrit de façon simplifiée le fonctionnement de l'API lorsqu'un client initie un test de QoS avec un outil de test ayant accès à l'API.

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



Ce schéma est simplifié : pour une meilleure lisibilité, les flux vers internet (flèches 1, 2, 4 et 6) passent par la box mais ne sont pas représentés ici.

Source : Arcep

Quels sont les outils de mesure qui ont accès à l'API ?

L'API sera accessible aux outils de mesure qui se sont déclarés conformes au « Code de conduite de la qualité de service internet » publié par l'Arcep.

Les travaux sur le Code de conduite sont abordés dans la section suivante.

Quelles sont les box concernées par l'API ?

Les opérateurs qui ont plus d'un million de clients et qui remplissent les conditions décrites dans la décision de l'Arcep auront l'obligation d'implémenter l'API dans la majorité des modèles de box xDSL, câble, FttH et 5G fixe proposées aux clients à partir du 17 juillet 2021.

L'Arcep encourage également à implémenter l'API dans les autres modèles de box.

L'API est-elle accessible depuis internet ?

Non, l'API est accessible uniquement depuis le réseau local de l'utilisateur final et ne répond pas aux requêtes provenant d'internet. De plus, un système de restriction d'accès est mis en place, afin que seuls les outils autorisés puissent accéder à l'API.

Quand l'API sera-t-elle disponible ?

En juillet 2022, l'API « carte d'identité de l'accès » sera implémentée et activée dans la quasi-totalité des box du parc concerné par la décision de l'Arcep après plusieurs phases de démonstrations et d'implémentations.

CALENDRIER DE DÉPLOIEMENT DE L'API

Source : Arcep

LA PAROLE À...

LAURENCE PAUMARD

*Responsable qualité de service internet fixe - **Orange***

VERS DES PUBLICATIONS QoS ÉQUITABLES, PERTINENTES ET PARLANTES

La mesure du débit internet de bout en bout ou des temps de navigation, à la maison, dépend d'une chaîne complète : du terminal utilisé par le client, plus ou moins performant, jusqu'au serveur internet, en passant par le réseau de l'opérateur et la fiabilité de l'outil de mesure commercial lui-même. Plus le débit est élevé, comme avec la fibre, plus le maillon côté client est prépondérant dans la valeur obtenue et éclipse les autres performances.

Il est donc très pertinent de caractériser l'environnement utilisateur dans la mesure de bout en bout : c'est même la condition *sine qua non* à toute interprétation de résultats !

Les outils de mesure actuellement disponibles sur le marché n'ont connaissance ni des caractéristiques de la ligne mesurée, ni de l'environnement à domicile, à la main du client : la technologie de son accès, le débit qu'il a choisi s'il a une offre fibre, son choix de mesurer en Wi-Fi ou en filaire, la présence ou non d'un usage simultané dans son foyer... Autant d'éléments structurants qui induisent des débits mesurés très différents : ce contexte de la mesure, non maîtrisé, ignoré, et variable d'un opérateur à l'autre, introduit des biais dans les comparaisons globales entre opérateurs. Il nous paraît nécessaire de débiaiser ces publications, pour les rendre équitables, pertinentes et parlantes.

C'est pourquoi Orange participe activement au chantier multipartite de l'Arcep qui vise à caractériser l'environnement utilisateur. La solution retenue, une API en interaction avec la box, à développer par chaque opérateur, permettra d'enrichir une mesure de bout en bout avec les paramètres cités.

Mais nous serons très vigilants sur l'utilisation qui en sera faite, sur deux plans : le contrôle de l'accès à ces données, pour les protéger, et leur utilisation effective dans les statistiques et les interprétations par les outils de mesure notamment. Le Code de conduite devra intégrer ces exigences. Nous travaillons déjà en ce sens avec l'Arcep.

ADRIEN d'USSEL

*Responsable performance réseau - **Bouygues Telecom***

LA QoE DOIT ÊTRE AU CŒUR DES MESURES DE *CROWDSOURCING*

Dans l'environnement du fixe, la mesure de la qualité de service est un sujet particulièrement complexe. Nous confondons trop souvent les mesures relatives à la QoS, comme le débit et la latence, avec l'expérience vécue par le client au quotidien (QoE).

L'enjeu principal des opérateurs est d'offrir la meilleure qualité d'expérience à chaque client au sein de chaque foyer. Cela passe évidemment par une bonne connectivité et stabilité de l'accès mais cette qualité « technique » n'est qu'un fragment de ce qu'il faut accomplir pour maintenir une performance élevée toute l'année. La qualité d'un opérateur ne peut donc pas s'évaluer sur un test de débit car, même si cela permet *a minima* de vérifier la conformité de son accès avec son offre commerciale, cela ne reflète pas nécessairement la qualité réelle des services internet utilisés au quotidien par nos clients. La qualité du fixe est la conjoncture de la performance et couverture du Wi-Fi, de la qualité des services TV et *replay*, de la stabilité des box mais également de la disponibilité et de la définition de services OTT comme la VOD et le *gaming*.

Le vrai enjeu pour l'écosystème du *crowdsourcing* est donc de mesurer l'expérience que vit chacun d'entre nous le soir, à l'heure de charge dans chaque foyer, pour ses services favoris. La qualité d'un réseau fixe s'évalue particulièrement en fin de journée lorsque l'on rentre chez soi et que toute la famille se connecte au Wi-Fi de la box. C'est à ce moment-là qu'il est nécessaire d'évaluer la qualité des services vidéo, web, *gaming*...

La démarche animée par l'Arcep de développer une API au sein des box pour permettre de partager des données techniques et commerciales, lorsqu'un « test *crowdsourcing* » est réalisé, est donc essentielle. Elle permettra de caractériser au mieux l'environnement de l'utilisateur, d'être plus précis dans les résultats et d'enrichir progressivement la démarche de régulation par la donnée. Elle permettra également de corriger les comparaisons parfois trop rapides et de prendre en compte les spécificités de chaque foyer pour informer sur les performances et éviter les biais dans les résultats. Cette API est donc une première étape importante qui doit être suivie par une transition forte des acteurs du *crowdsourcing* vers des tests de QoE afin d'informer le grand public sur la qualité des services réels au quotidien.

Sollicités par l'Arcep, Free et SFR n'ont pas souhaité s'exprimer dans cette rubrique.

3. VERS DES MÉTHODOLOGIES DE MESURE PLUS TRANSPARENTES ET ROBUSTES

3.1. Présentation du Code de conduite 2018 de l'Arcep et outils conformes

À l'instar des 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[6] 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.

Ce Code de conduite se structure en deux grandes parties :

- la première concerne le protocole de test de l'outil de mesure, c'est-à-dire à la fois les méthodologies de mesure des différents indicateurs (débit, latence, temps de chargement des pages web et qualité du *streaming* vidéo) et les mires de test ;
- la seconde 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.

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

En ce qui concerne la qualité de service fixe, les outils de test qui se sont déclarés conformes à la version 2018 du Code de conduite de la qualité de service internet sont :

- 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 ;
- 5GMark, développé par QoSi ;
- IPv6-test : le test de qualité de service IPv4 et IPv6, développé par IPv6-test.

En ce qui concerne la qualité de service mobile, les outils de test qui se sont déclarés conformes à la version 2018 du Code de conduite de la qualité de service internet sont :

- nPerf, développé par nPerf ;
- DébiTest 60 : le testeur de connexion de 60 Millions de consommateurs, développé par QoSi ;
- 5GMark, développé par QoSi.

L'OUTIL DE MESURE DÉVELOPPÉ PAR LE BEREC (L'ORGANE DES RÉGULATEURS EUROPÉENS DES TÉLÉCOMS)

Au cours de l'année 2019, le BEREC a mené et finalisé les travaux de développement de son outil *open source* de mesure de qualité de service internet. Cet outil est 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 permet de 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. Le code source de l'outil est disponible sur Git Hub depuis décembre 2019 : https://github.com/net-neutrality-tools/nntool.

Actuellement, cet outil est mis à disposition des autorités de régulation nationales (ARN) des différentes États membres qui peuvent l'adopter, sur base volontaire. Les ARN pourraient implémenter l'outil sur leur territoire après une adaptation aux besoins nationaux (traduction de l'interface utilisateur, mise en place de serveurs de test 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. Édition 2018 du Code de conduite de la qualité de service internet : https://www.arcep.fr/uploads/tx_gspublication/code-de-conduite-qs-internet-2018_FR.pdf

3.2. Vers une nouvelle version du Code de conduite

Le Code de conduite de la qualité de service internet, dans sa version 2018, a fixé un niveau minimal de transparence et de robustesse. Comme indiqué lors de sa publication, ce Code de conduite est évolutif et a vocation à être mis à jour régulièrement afin de non seulement renforcer les critères déjà présents, mais aussi de les compléter par des éléments relatifs à d'autres catégories thématiques.

À la suite de cette première version, l'Arcep a poursuivi en 2019 sa démarche de co-construction pour alimenter la nouvelle version du Code de conduite. L'Arcep a ainsi relancé un cycle de travail avec les acteurs impliqués dans la mesure de la QoS (FAI, outils de mesure, organismes de protection des consommateurs et acteurs académiques).

Afin d'accompagner progressivement la montée en compétence de l'écosystème de mesure de la QoS, plusieurs axes seront renforcés dans la nouvelle version du Code de conduite.

D'abord, l'Arcep travaille avec l'ensemble de l'écosystème pour renforcer les exigences de transparence ou de robustesse des protocoles de test. Voici quelques exemples de pistes de réflexion dans le cadre des travaux pour cette nouvelle version du Code de conduite :

- la pertinence d'afficher une valeur médiane, notamment pour la latence. En effet, la médiane pourrait, dans certains cas, être plus pertinente pour refléter l'expérience utilisateur, notamment dans le cas où il existe des valeurs extrêmes dans les résultats mesurés impactant la représentativité de la moyenne ;
- le besoin de préciser d'autres facteurs impactant la mesure, notamment l'utilisation et les caractéristiques du Wi-Fi, le modèle et la version du système d'exploitation et du navigateur web qui peuvent avoir une forte influence sur la mesure de QoS ;
- le besoin d'introduire une capacité minimale pour les mires de test, afin d'éviter que le test soit limité par ces mires ;
- l'intérêt de préciser la capacité pour les mires de test de réaliser des tests en IPv6, le protocole utilisé pouvant impacter la mesure de débit (cf. section suivante sur les mires de test).

De plus, ce Code de conduite mettra aussi l'accent sur un certain nombre de biais de mesure à expliciter dans les publications agrégées des outils de mesure.

Cette nouvelle version du Code de conduite, qui visera également à mieux prendre en compte les spécificités de la mesure de la qualité de service d'internet sur des réseaux mobiles, sera publiée à l'été 2020.

L'Autorité invitera les acteurs de mesure qui le souhaitent à se déclarer conformes au Code de conduite 2020 et dressera le bilan des acteurs de la mesure qui se seront déclarés.

Par ailleurs, les travaux pour améliorer encore les pratiques et renforcer le Code de conduite se poursuivront lors de la mise en place effective de l'API. La prise en compte des fonctionnalités proposées par cette API aux outils de mesure permettra en effet de fiabiliser non seulement les tests de QoS mais aussi les publications agrégées. Ces évolutions se feront bien évidemment en concertation avec les acteurs impliqués.

LES LIGNES DIRECTRICES QoS DU BEREC*

Comme le prévoit l'article 104 du nouveau Code des communications électroniques européen (CCEE), le BEREC vient de publier des lignes directrices détaillant les indicateurs de qualité de service pour les services d'accès à internet et les services de communications interpersonnelles accessibles au public.

Ces lignes directrices ont notamment pour objectif de guider les autorités de régulation nationales dans le choix des indicateurs de qualité de service que les fournisseurs de ces services doivent publier afin que les utilisateurs finals disposent de données complètes, fiables, faciles à exploiter et actualisées sur la qualité de leurs services.

Les lignes directrices du BEREC abordent également les indicateurs pertinents pour les utilisateurs finals en situation de handicap, les méthodes de mesure de la QoS applicables, les questions liées à la publication des informations ainsi que les mécanismes de certification de la qualité.

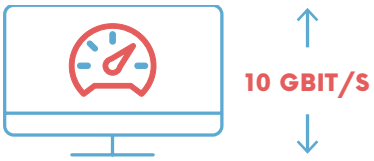
Conformément au CCEE qui prévoit que les services de communications interpersonnelles « *over-the-top* » (OTT) constituent désormais une catégorie des services de communications électroniques, les lignes directrices du BEREC intègrent des indicateurs pour ces services parmi lesquels les services de messagerie en ligne.

Dans le cadre de la transposition du code européen, les compétences de l'Arcep devraient être étendues à ces acteurs au regard des obligations qui leur sont désormais applicables, et au contrôle desquelles l'Arcep devrait être chargée de veiller.

* Lignes directrices QoS du BEREC - BoR (20) 53 : https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/9043-berec-guidelines-detailing-quality-of-se_0.pdf

LES TESTS DE DÉBIT À 10 GBIT/S, UN DÉFI POUR LES OUTILS DE LA MESURE DE QoS

La grande majorité des tests de débit fixe sont réalisés dans un navigateur web.



Toutefois, un navigateur web est un logiciel complexe reposant sur un ensemble de composants tels, par exemple, qu'une *sandbox* (mécanisme de sécurité informatique se basant sur l'isolation de composants logiciels). Un test de débit consomme donc en principe beaucoup plus de ressources dans un navigateur que s'il est exécuté directement sur le système d'exploitation.

Les débits proposés par les connexions internet évoluant beaucoup plus rapidement que la puissance des microprocesseurs de nos ordinateurs, aujourd'hui les clients équipés de connexion 10 Gbit/s ne mesurent plus le débit de leur connexion à internet, mais la puissance de leur microprocesseur. En effet, seuls des PC très puissants peuvent réaliser des tests à 10 Gbit/s dans un navigateur web, sans saturer leur microprocesseur.

Les connexions à 10 Gbit/s nécessitent également une mire de test disposant de plus de 10 Gbit/s vers internet, ce qui est très rare à ce jour.

Face à ces nouveaux défis à relever, plusieurs solutions émergent, telle l'utilisation d'un outil de mesure de la QoS qui s'exécute directement sur le système d'exploitation.

D'autres acteurs militent pour ne plus mesurer la capacité de la connexion mais la qualité d'expérience (QoE), car l'augmentation de débit vers des serveurs de test de débit ne permet pas forcément de juger de la qualité ressentie. Dans certains cas, il pourrait en effet être possible d'avoir une meilleure QoE sur une ligne FttH 100 Mbit/s que sur une ligne FttH 10 Gbit/s. En effet, la latence, les pertes de paquets, la taille des *buffers*, la capacité à transporter les paquets dans l'ordre ou les relations d'interconnexion sont aussi très importantes dans la qualité d'expérience, ces paramètres ne dépendant pas de la capacité du lien.

LA PAROLE À...  JEAN-FRANÇOIS GIORGI

Développeur indépendant

NSPEED - MESURE DES DÉBITS DES CONNEXIONS 10 GBIT/S

Les tests de débits existants à destination des utilisateurs profanes en technologie des réseaux rencontrent des soucis pour mesurer correctement le débit d'une connexion internet de plusieurs gigabits par seconde (Gbit/s) :

- utilisation de technologies web qui limitent les performances et qui ne permettent pas de savoir les conditions locales d'utilisation, comme la performance du processeur de la machine ;
- utilisation d'un serveur de test unique : le test utilise un chemin précis sur internet et pas forcément la partie terminale (boucle locale). Pour des connexions multi-gigabits le serveur et/ou son interconnexion à internet sont donc souvent les maillons limitants.

L'outil NSpeed est né de ce constat, notamment suite aux difficultés de mesure que rencontrent les abonnés des connexions à 8 Gbit/s proposées par Free. Les utilisateurs n'ont aucune information ou méthode simple pour savoir où se situe le problème, s'ils n'arrivent pas à mesurer le débit maximum.

L'autre souci est le manque de transparence de ces applications, aucune n'est en *open source*.

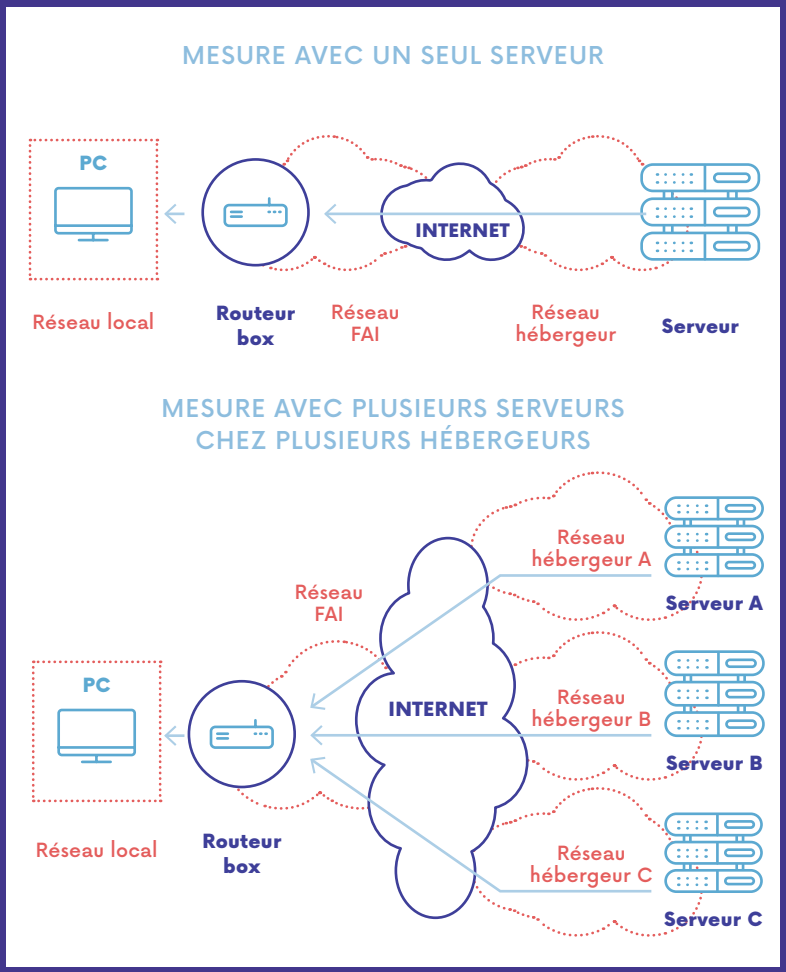
L'outil NSpeed propose une approche différente :

- utiliser HTTP en version 1.1, 2 et 3 avec ou sans chiffrement. Les versions 1.1 et 2 utilisent TCP*, la version 3 utilise UDP* ;
- utiliser autant de serveurs que l'on souhaite, positionnés partout dans le monde ;
- utiliser des serveurs spécifiques à NSpeed ou n'importe quel serveur web du monde permettant de télécharger un fichier et/ou d'en envoyer un. L'intérêt des serveurs spécifiques à NSpeed est d'avoir plus d'informations sur ce qui se passe côté serveur notamment la charge réseau, processeur et le *cross-traffic*.

Le logiciel NSpeed se présente pour la plupart des systèmes d'exploitation sous forme d'un fichier binaire unique exécutable qui ne nécessite aucune installation. Il suffit de le télécharger et de l'exécuter.

Le logiciel NSpeed est aussi un serveur NSpeed qui propose des fichiers fictifs qui peuvent être téléchargés non seulement par le logiciel NSpeed lui-même, mais aussi par n'importe quel logiciel utilisant le protocole HTTP. Le serveur NSpeed permet aussi d'envisager de faire des tests de débits *peer to peer* directement entre internautes.

Le projet NSpeed est développé en langage Go et son code source librement disponible sur le site https://nspeed.app. Nous lançons un appel à contribution à ceux qui ont des compétences en développement logiciel pour faire évoluer le produit.



* Voir lexique.

4. L'IMPACT 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 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.

L'Arcep travaille ainsi avec l'ensemble de l'écosystème pour ajouter dans le Code de conduite 2020 un ensemble de nouveaux critères de transparence minimum sur les mires utilisées par les outils de mesures, afin que l'utilisateur soit informé de la bande passante de chaque mire proposée en France par l'outil de test de la qualité de service utilisé.

Le Code de conduite 2020 pourrait également recommander une capacité minimale pour la mire de test afin de réduire le nombre de mesures où celle-ci est l'élément limitant.

4.2. Impact de la localisation des mires de test

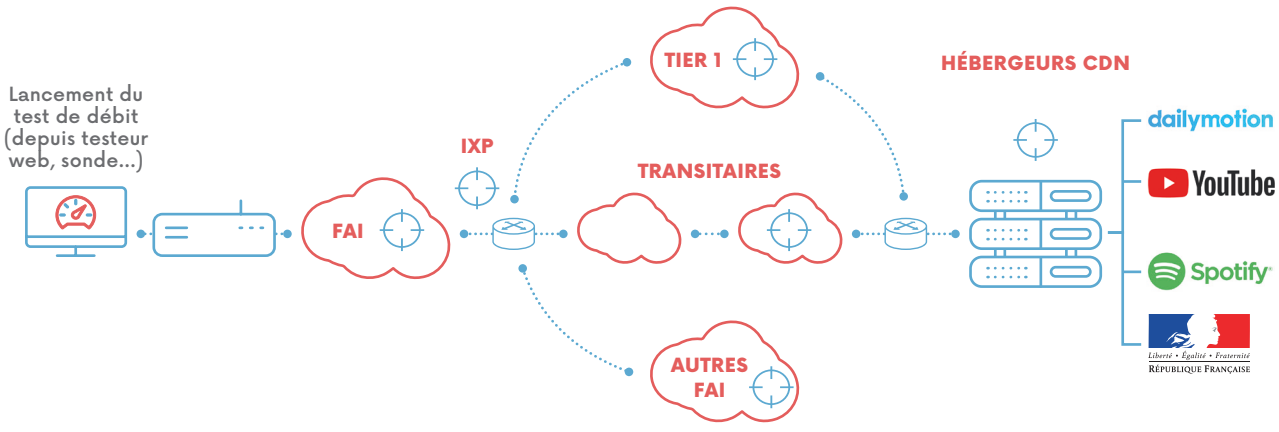
La localisation de la mire est primordiale pour le calcul de la latence car celle-ci dépend principalement du trajet parcouru par l'information entre le client et la mire[7]. La localisation influe également sur la montée en débit et donc sur le débit moyen. La localisation est moins importante pour les outils qui affichent le débit en régime établi.

Comme explicité sur le schéma ci-dessous, 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 l'observatoire d'Akamai) représentent uniquement la qualité de service vers un point précis de l'internet ;
- dans le réseau d'un *Tier 1*[8] : 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 fournisseurs de contenu et d'applications : 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.

IMPACT DE LA LOCALISATION DES MIRES DE TEST



Source : Arcep

7. Outre la latence liée à la technologie d'accès, la majorité du trajet entre un client et un serveur se fait par des fibres optiques.
8. Les *Tier 1* sont les réseaux capables de joindre tous les réseaux internet par une interconnexion directe (voir lexique).

L'IMPACT DU CONTRÔLE DE CONGESTION SUR LA MESURE DE LA QoS

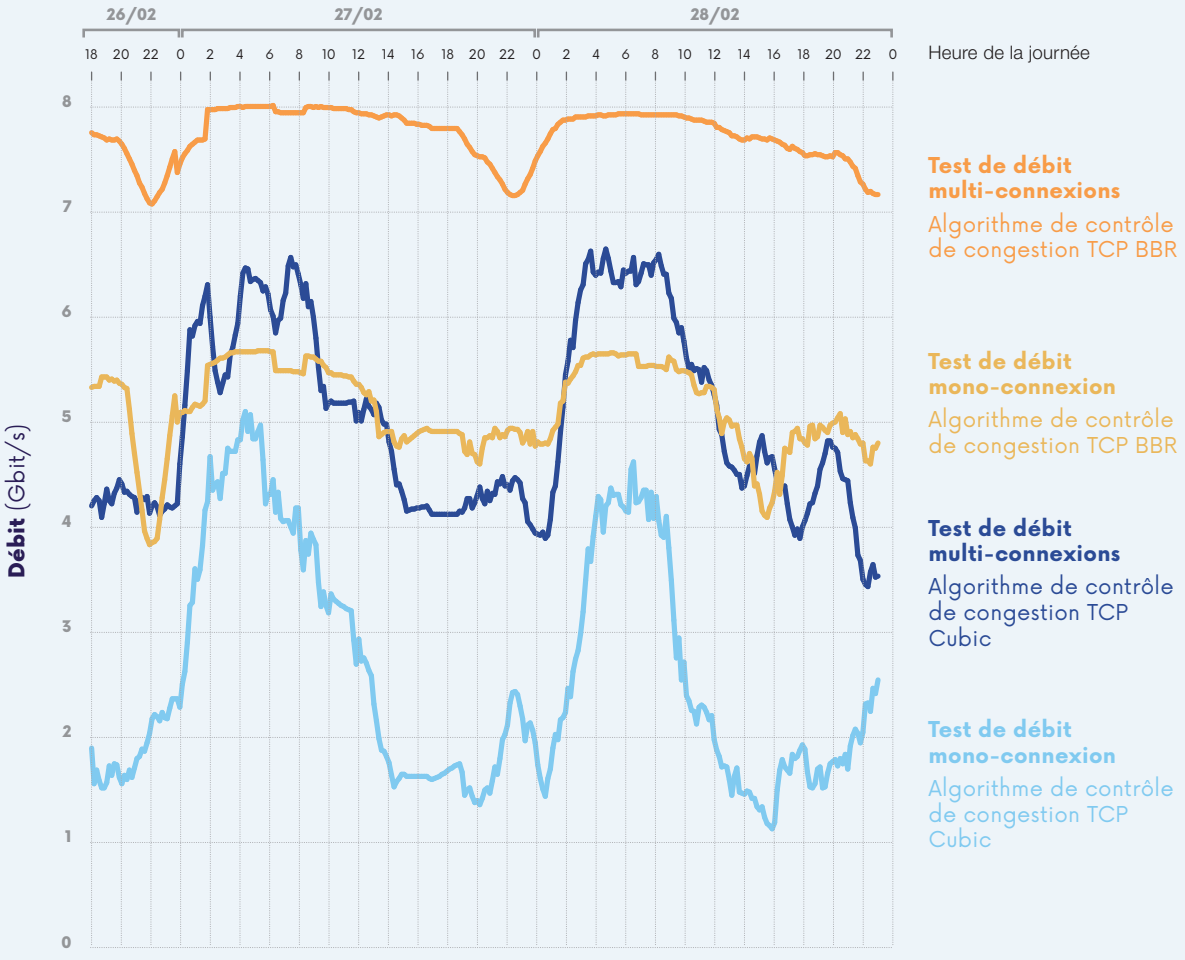
Les outils de test de qualité de service font des choix techniques qui ont des effets importants sur les résultats de mesure. Certains sont uniquement mono-connexion (ou *mono-thread* en anglais), d'autres remontent le débit mesuré en additionnant les débits de multiples connexions simultanées (*multi-thread* en anglais), d'autres encore laissent le choix à l'utilisateur de réaliser un test mono- ou multi-connexions. 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.

Les résultats des mesures de la QoS dépendent aussi des caractéristiques techniques des serveurs de mire, et notamment de leurs algorithmes d'évitement de congestion TCP. Ces algorithmes sont utilisés côté émetteur de données pour décider de la vitesse d'envoi des paquets. Il existe de nombreux algorithmes d'évitement de congestion TCP et ces algorithmes évoluent. Aujourd'hui la majorité de l'internet utilise TCP Cubic créé en 2006, qui s'appuie sur la perte de paquets comme signal pour réduire le débit. C'est toujours l'implémentation TCP par défaut sous Linux, Android et MacOS.

Google a développé en 2016 TCP BBR (*Bottleneck Bandwidth and Round-trip propagation time*), qui utilise un modèle différent se basant sur la bande passante maximale et le temps d'aller-retour. Cette approche permet à TCP BBR de proposer un débit plus élevé et une latence plus faible que ceux offerts par les algorithmes s'appuyant sur la perte de paquets, comme TCP Cubic. Aujourd'hui, certains grands acteurs de l'internet commencent à déployer BBR sur leurs serveurs.

Comme illustré ci-dessous, les mesures de débit descendant varient fortement selon la combinaison des choix entre le mode mono- ou multi-connexions et l'algorithme de congestion :

DÉBIT DESCENDANT SUR UNE LIGNE FttH 8 GBIT/S, EN FONCTION DU TYPE DE TEST RÉALISÉ



Les traits correspondent à la moyenne mobile sur 2 heures. Tests réalisés par Yann G. (Breizh29) sur une Freebox Delta avec un client iPerf3.7 sous Ubuntu 19.10 avec le protocole IPv6, sur la commune Ergué-Gabéric (Finistère). Mire de test : lille.testdebit.info située sur le réseau Bouygues Telecom à Lille (Nord).

QUELLES SONT LES MIRES PROPOSÉES PAR LES DIFFÉRENTS OUTILS DE TEST DE QUALITÉ DE SERVICE ?

L'Arcep liste, à titre illustratif, en annexe 2 du présent rapport les mires de test utilisées par différents outils. Les caractéristiques présentées pour chaque mire de test sont les suivantes :

Sponsor : c'est le nom de la mire affichée sur l'outil de mesure de la qualité de service. Attention, ce nom ne permet pas toujours de savoir quel est le réseau qui héberge la mire.

Ville / Région : localisation de la mire.

Protocole IPv4 / IPv6 : certaines mires sont « IPv4 uniquement » ce qui empêche la réalisation d'un test en IPv6. Les tests réalisés sur des connexions où IPv6 est natif et IPv4 transporté sur IPv6 montrent un léger gain de débit avec le protocole IPv6, quand on le compare au protocole IPv4. Réaliser le test en IPv6 est utile puisqu'aujourd'hui, 62 % des pages web les plus visitées en France sont accessibles en IPv6*. Choisir une mire « IPv4 uniquement » permet à un utilisateur de vérifier également la qualité de service qu'il obtient en IPv4.

Capacité de la connexion : la mire doit offrir suffisamment de débit pour ne pas être le facteur limitant dans la mesure de débit (il est souvent conseillé d'utiliser une mire qui offre au minimum le double du débit présumé de votre connexion).

Port utilisé : 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 est le pendant chiffré du port 8080.

Nom de l'hébergeur et AS *(Autonomous System)* : permet d'identifier le réseau hébergeant la mire. Chaque AS identifie un réseau (au niveau routage). Certaines sociétés peuvent avoir plusieurs numéros d'AS pour segmenter leurs activités (les relations d'interconnexion des différents AS pouvant être différentes).

* Source : 6lab Cisco au 28/10/2019, données sur le top 730 Alexa en France.

TUTORIEL

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

L'Arcep précise sur son site internet[1] la configuration minimale (mémoire vive, processeur, carte réseau, câble réseau, etc.) nécessaire pour un test fiable. Toutefois, ce premier niveau de précaution méthodologique ne permet pas de s'affranchir des logiciels installés sur une machine qui peuvent aussi impacter le débit. Pour réaliser un test de qualité de service qui fait abstraction des logiciels installés, le lecteur expert peut suivre la démarche ci-dessous qui repose sur la création d'une clé USB bootable et la réalisation un test sous Linux. Le tutoriel détaillé est disponible sur le site de l'Arcep[2].

Le prérequis est un PC avec au minimum 8 Go de mémoire vive et une clé USB de 4 Go minimum dont le contenu peut être effacé. Attention, tout le contenu de la clé USB utilisé sera perdu.

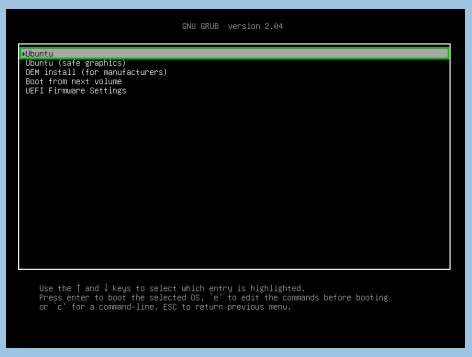
Les étapes sont les suivantes :

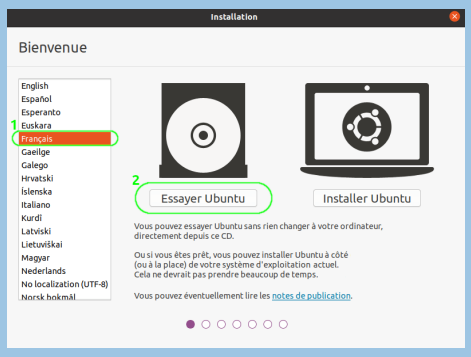
1. Créer la clé USB bootable :

- Télécharger une distribution Linux performante, par exemple « Ubuntu Desktop »[3].
- Télécharger un logiciel qui va permettre de créer la clé USB, par exemple « Rufus »[4].
- Lancer Rufus, insérer votre clé USB puis sélectionner le fichier « ubuntu-desktop-amd64.iso ».
- Cliquer sur « Démarrer » pour lancer la création de la clé USB.

2. Redémarrer votre ordinateur sur la clé USB :

- Mettre l'ordinateur sous tension ou le redémarrer et appuyer sur la touche pour afficher le menu de *boot,* avant le chargement de Windows. Si deux modes de démarrage sont proposés (soit « UEFI » soit « BIOS » ou « legacy »), sélectionner le mode « UEFI ».
- En mode « UEFI », un écran avec un fond noir s'affiche. Sélectionner « Ubuntu », puis sur l'écran de bienvenue sélectionner « Français », puis cliquer sur « Essayer Ubuntu ».





3. Réaliser un test de qualité de service

Il suffit de lancer Firefox, puis de lancer votre outil de test de la qualité de service.

Pour suivre le pourcentage d'utilisation du processeur, lancer l'application « Moniteur système » et cliquer sur l'onglet « Ressources ». Afin de garantir que le test de qualité de service ne soit pas limité, il faut que le pourcentage d'utilisation d'un cœur du processeur ne dépasse pas 70 %.

1. Comment fiabiliser un test de débit ? : https://www.arcep.fr/demarches-et-services/utilisateurs/comment-fiabiliser-un-test-de-debit.html
2. Tutoriel pour la création d'une clé USB bootable : https://www.arcep.fr/demarches-et-services/utilisateurs/creation-dune-clef-usb-bootable-pour-realiser-un-test-de-debit-fiable.html
3. Lien pour télécharger « Ubuntu Desktop » : https://ubuntu.com/download/desktop
4. Lien pour télécharger « Rufus » : https://rufus.ie

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

Si les cartes de couverture mobile, 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, les mesures de qualité de service 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 2019, 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), dans les transports (TER, Transiliens, RER, métros, TGV, routes) et dans une cinquantaine de zones touristiques.

En 2017, l'Arcep a lancé son outil cartographique et interactif monreseaumobile.fr, qui permet de visualiser les cartes de couverture mobile des opérateurs ainsi que l'ensemble des données de cette enquête de qualité de service. Depuis juillet 2018, les territoires d'outre-mer y figurent également.

Ces mesures permettent de mesurer la progression de la qualité de service des différents réseaux alors que le smartphone est devenu le principal moyen d'accès à internet, rendant ainsi compte des efforts d'investissement des opérateurs sur leur réseau.

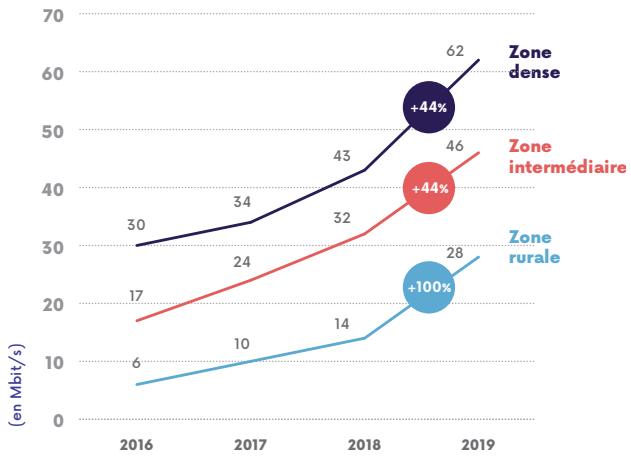
5.1. Le débit moyen en France métropolitaine s'établit à 45 Mbit/s, contre 30 Mbits/s en 2018

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, tous opérateurs confondus et toutes zones confondues (rurales, intermédiaires et denses) atteint 45 Mbit/s, contre 30 Mbits/s en 2018.

Cette progression est particulièrement marquée en zone rurale, où le débit a doublé en un an, traduisant des efforts d'investissement des opérateurs y compris dans les zones moins denses. Pour autant, les performances en zones rurales restent encore en retrait par rapport aux zones denses.

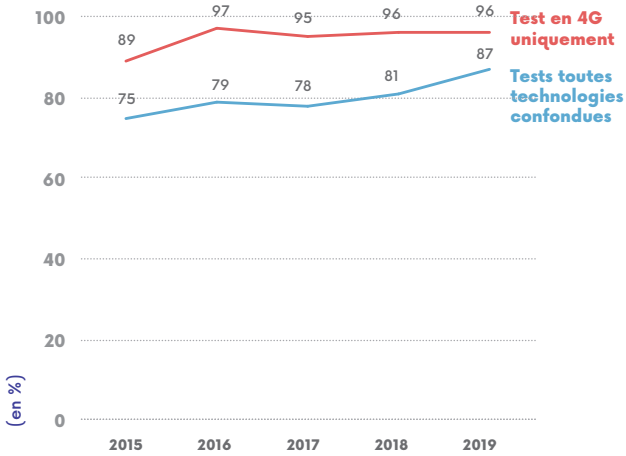
Concernant la navigation web, en 2019, 87 % des pages web mesurées par l'Arcep – parmi un échantillon des 30 sites les plus consultés en France – étaient chargées en moins de 10 secondes. La 4G apporte également un gain très important sur cet indicateur puisque le taux de pages web chargées en moins de 10 secondes uniquement en 4G s'établit quant à lui à 96 % : la généralisation de la 4G sur l'ensemble des sites des opérateurs, prévue par le *New Deal* mobile, apporte ainsi une nette amélioration de la qualité des services de données des opérateurs.

DÉBITS DÉSCENDANTS MOYENS (MOYENNE TOUS OPÉRATEURS) EN FRANCE MÉTROPOLITAINE



Source : Arcep

NAVIGATION WEB (MOYENNE TOUS OPÉRATEURS) : TAUX DE PAGES CHARGÉES EN MOINS DE 10 SECONDES EN FRANCE MÉTROPOLITAINE



Source : Arcep

5.2. Outre-mer, la qualité de service connaît également un bond conséquent

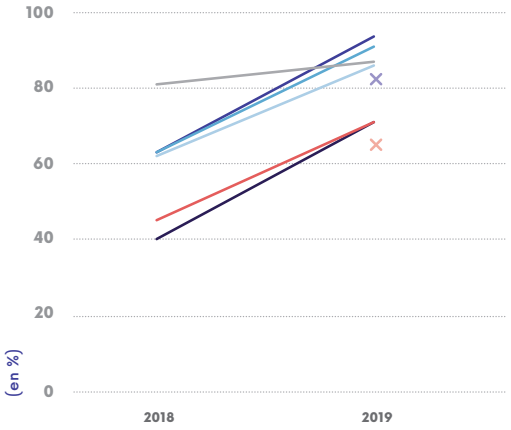
Les résultats en nette amélioration entre 2018 et 2019 traduisent les efforts de déploiement de la 4G en Outre-mer.

La qualité du service de données mobiles a en effet fait un bond conséquent : les débits moyens doublent dans presque tous les territoires, et la qualité de la navigation web s'améliore en moyenne de moitié. Ces performances se rapprochent voire, dans certains cas, dépassent celles rencontrées en Métropole.

DÉBITS DESCENDANTS MOYENS (MOYENNE TOUS OPÉRATEURS)

Source : Arcep

NAVIGATION WEB (MOYENNE TOUS OPÉRATEURS) : TAUX DE PAGES CHARGÉES EN MOINS DE 10 SECONDES



Source : Arcep

5.3. L'enrichissement de « Mon réseau mobile »

Depuis fin 2018, l'Arcep a engagé des travaux pour faire évoluer « Mon réseau mobile ».

En premier lieu, l'Arcep a publié un « Kit du régulateur » pour répondre aux attentes des territoires qui souhaitent effectuer leurs propres mesures, notamment pour identifier leurs besoins de couverture dans le cadre du *New Deal* mobile. Ce Kit comprend des modèles de cahiers des charges techniques, pouvant être réutilisés simplement dans le cadre de marchés relatifs à la sélection d'un prestataire pour réaliser une campagne de mesures sur le terrain. De premiers acteurs, tels que SNCF et certaines collectivités territoriales, se sont saisis de ce document pour faire réaliser leurs propres mesures de connectivité. L'Arcep a engagé des discussions avec ces acteurs et depuis avril dernier, « Mon réseau mobile » s'est enrichi des données de mesure de plusieurs territoires : le Cher, les Hauts-de-France, les Pays de la Loire et l'Auvergne-Rhône-Alpes. Sont également accessibles des données de mesures sur le réseau SNCF. Il continuera à s'enrichir en intégrant les mesures de qualité de service mobile réalisées conformément au « Kit du régulateur ».

L'Arcep a également publié un Code de conduite à destination des acteurs qui proposent des applications de mesure de l'expérience mobile, comme des tests de débit en *crowdsourcing* que chacun peut réaliser sur son téléphone. Ce document a pour objectif d'assurer un niveau minimal d'exigence en matière de pertinence, de présentation et de transparence des mesures. À l'heure actuelle, trois acteurs ont déclaré leurs outils conformes au Code de conduite (QoSi, nPerf et 60 Millions de consommateurs). Les solutions proposées par ces acteurs ont été adoptées par certains territoires tels que les Hauts-de-France ou l'Ille-et-Vilaine.

Enfin, plus récemment, l'Arcep a adopté une décision visant à durcir le seuil de fiabilité des cartes de couverture transmises par les opérateurs de 95 % à 98 %. En effet, l'Arcep vérifie la fiabilité de ces cartes, établies par modélisation informatique, au moyen d'enquêtes sur le terrain (environ 2 millions de mesures en 2018). Jusqu'à présent, une carte est considérée comme fiable par l'Arcep si son taux de fiabilité, correspondant au taux de succès d'un test donné dans les zones que les opérateurs déclarent couvrir, est supérieur ou égal à 95 %. L'Autorité a fixé ce seuil à 98 %. Plus précisément, la décision prévoit la fixation d'un seuil de fiabilité « global » des cartes à 98 %. En complément, il est proposé de décliner cette exigence localement, à 98 % pour toute zone de plus de 1 000 km² et à 95 % pour toute zone de plus de 100 km².

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. L'Arcep a dressé le bilan le bilan 2019 de son action au profit des consommateurs et de sa plateforme de signalement « J'alerte l'Arcep »*. En 2019, plus de 20 000 signalements ont été transmis à l'Arcep. De ces signalements, 47 % concernent un problème lié à qualité et la disponibilité des services fixes ou mobiles.

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. Par exemple, pour répondre au décalage ressenti par les utilisateurs entre les informations publiées sur les outils cartographiques de l'Arcep (notamment « Mon réseau mobile ») et la réalité du terrain, l'Arcep a relevé ses seuils d'exigence pour disposer de cartes plus fiables (de 95 % à 98 %). Les signalements sont aussi une source utile aux services de l'Autorité pour identifier les infractions potentielles au règlement internet ouvert et son principe de neutralité du net (cf. chapitre 4 de ce rapport).

En 2019, l'Arcep a travaillé à l'amélioration de son outil pour notamment préciser ses typologies et sous-typologies. La partie « qualité de service », qui représente une majorité des signalements, a été particulièrement scrutée. C'est aussi en accroissant les précisions demandées sur certains cas que l'Arcep sera en mesure de mieux étudier certains sujets futurs. « J'alerte l'Arcep » évoluera dans le courant de l'année 2020, en particulier pour permettre de signaler directement depuis les outils tiers : Mon réseau mobile (https://www.monreseaumobile.fr/), Ma connexion internet (https://maconnexioninternet.arcep.fr/), etc.

* Bilan 2019 des actions de l'Arcep vis-à-vis des consommateurs et de la plateforme « J'alerte l'Arcep » : https://www.arcep.fr/actualites/les-communiques-de-presse/detail/n/regulation-par-la-data-4.html

CHAPITRE 2

Superviser l'interconnexion de données

À RETENIR

Le trafic entrant vers les principaux FAI en France à l'interconnexion **a augmenté de 29 %** en un an pour atteindre 18,4 Tbit/s à fin 2019.

Les capacités installées à l'interconnexion pour les principaux FAI sont en moyenne **2,7 fois supérieures** au trafic entrant.

55 % du trafic vers les clients des principaux FAI en France provient de quatre fournisseurs : Netflix, Google, Akamai et Facebook.

L'interconnexion[1] constitue le fondement d'internet. Elle désigne la relation technico-économique qui s'établit entre différents acteurs pour se connecter et échanger mutuellement du trafic. Elle garantit le maillage global du réseau et permet aux utilisateurs finals de communiquer entre eux[2].

1. ÉVOLUTION DE L'ARCHITECTURE D'INTERNET

À ses débuts, internet s'est structuré d'une manière hiérarchique avec des fournisseurs d'accès internet (FAI) qui, afin d'assurer à leurs clients une connectivité mondiale, font appel à des transitaires pour les interconnecter aux fournisseurs de contenu et d'applications (FCA) et aux autres FAI. Ces transitaires et surtout les *Tier 1* jouent dans ce contexte un rôle central pour garantir l'acheminement du trafic. Les acteurs internet ont ainsi toujours été dépendants de ces acteurs dans leurs échanges.

Cependant, en l'espace de quelques années, avec l'augmentation de la quantité de trafic et le besoin de rapprocher le contenu du client final notamment pour améliorer la qualité de service et d'expérience de l'utilisateur final, l'architecture d'internet a connu des évolutions et plusieurs alternatives au transit ont vu le jour. Ces alternatives, qui permettent aux FAI et aux FCA de s'affranchir du moins pour partie des transitaires, prennent plusieurs formes :

- L'émergence et la croissance des réseaux de distribution de contenu (CDN), qui substituent au transport longue distance le stockage rapproché des données, dans des serveurs cache. Ainsi des acteurs CDN peuvent faire en partie abstraction de la chaîne de valeur habituelle pour l'acheminement du trafic.
- Le déploiement de réseaux internationaux en propre notamment par les gros FCA, qui leur permet de développer eux-mêmes et de posséder une infrastructure de transport longue distance, mais aussi d'améliorer leur connectivité.
- Le développement du *peering* (autre que celui entre *Tier 1*) :
  - certains FCA s'affranchissent des transitaires pour venir s'interconnecter directement aux FAI. Les point d'échange (IXP) ont facilité le développement de ce type d'interconnexion directe ;
  - les FAI s'interconnectent de plus en plus entre eux au niveau national ou régional, là encore en grande partie grâce à des interconnexions directes ou au niveau de points d'échange.

Par ailleurs, le marché du transit reste fortement concurrentiel, avec des prix qui varient en fonction des routes, selon le nombre d'acteurs présents et les quantités de données échangées. Ainsi, les liaisons transatlantiques, qui sont nombreuses et fortement utilisées, sont parmi les moins chères du monde, à l'inverse des liaisons avec l'Afrique par exemple. Le tarif constaté des prestations de transit a également diminué régulièrement au cours du temps, du fait de la combinaison de l'augmentation des volumes de trafic, de la baisse des coûts unitaires des équipements et de la pression concurrentielle. À titre d'exemple, selon le cabinet d'études Telegeography[3], le prix moyen du transit à la fin 2018, toutes routes confondues, avoisine 0,5 € par Mbit/s par mois en Europe de l'Ouest et aux États-Unis soit 10 fois moins qu'à fin 2011. Il atteint environ 2,5 € par Mbit/s par mois à São Paulo (Brésil), contre 30 € par Mbit/s par mois à fin 2011. Ces prix continuent à baisser de façon spectaculaire notamment là où la concurrence est la plus forte.

1. Les termes techniques liés à l'interconnexion employés ci-après sont définis dans le baromètre de 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.
2. L'Arcep tient à préciser que le présent rapport concerne uniquement l'interconnexion de données dans le réseau internet et ne s'applique pas à l'interconnexion des réseaux de deux opérateurs pour la terminaison d'appel vocal.
3. https://global-internet-map-2018.telegeography.com

Ainsi, même si les volumes de trafic globaux poursuivent une croissance très forte, permettant aux volumes de transit de continuer de progresser, ces deux tendances précédentes, que sont la forte concurrence et l'apparition d'alternatives au transit, font craindre depuis quelques années l'arrivée à maturité du marché mondial du transit qui entraîne une stabilisation de la croissance et des revenus des transitaires.

Les transitaires cherchent à s'adapter selon deux modalités principales :

- La consolidation. Le marché de transit a surtout connu ce phénomène durant la dernière décennie, avec plusieurs rachats dont le dernier en date est celui de Level 3 par Centurylink en 2016.
- La diversification. Il s'agit principalement de la fourniture de services de CDN et de sécurité à valeur ajoutée, par exemple des solutions anti-DDoS. Cette diversification se fait soit par développement interne soit par rachat d'entreprises spécialisées dans ces activités (notamment, rachat de Bigravity par Tata Communications en 2011 ou de Streamroot par Centurylink en 2019).

Le marché de l'interconnexion en France s'inscrit dans cette tendance mondiale. En effet, les résultats issus de la collecte d'information sur l'interconnexion de données montrent une augmentation du taux de *peering* par rapport au transit, une augmentation du taux de trafic provenant des CDN internes aux réseaux des FAI ainsi qu'une concentration du trafic entre un petit nombre d'acteurs.

LA PAROLE À... DAVE SCHAEFFER

*Fondateur et PDG - **Cogent Communications***

LA DYNAMIQUE DU TRANSIT

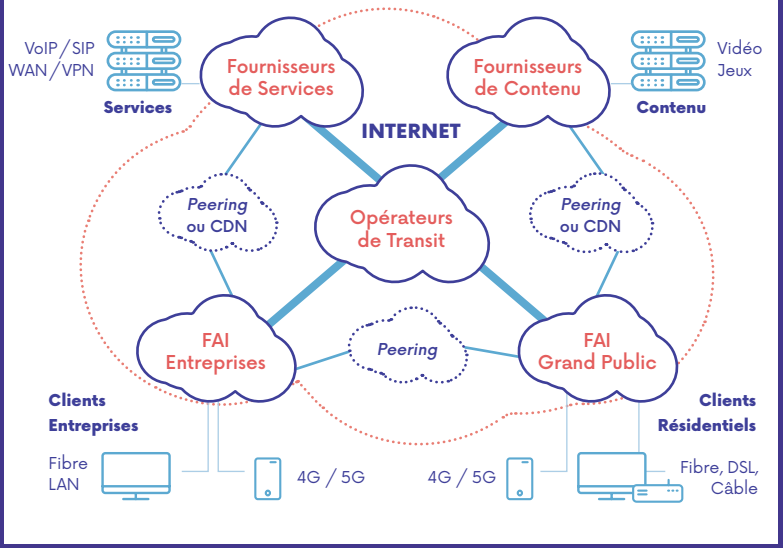
Depuis sa création, internet s'est développé comme un réseau de réseaux interconnectés : passant de quelques-uns en 1996 à plus de 65 000 systèmes autonomes (AS) actifs aujourd'hui à travers le monde. Une couche de transit est très vite devenue nécessaire : se connecter localement à un transitaire (ou à plusieurs pour des raisons de redondance) est incontestablement plus efficace que d'établir des liens directs avec des milliers de réseaux dans le monde. Le transit est au cœur d'internet. Alors que le *peering*, les CDN ou d'autres initiatives d'interconnexion directe se sont développés au cours des années, le transit s'est avéré le moyen le plus efficace de faire face à l'augmentation de trafic, à un rythme de 45 % par an sur les 20 dernières années sur le réseau de Cogent, et constitue une solution de « dernier recours » très appréciée lorsque tous les autres moyens d'interconnexion sont défaillants.

En effet, les CDN et autres méthodes pour rapprocher le contenu et les applications des utilisateurs finals jouent un rôle important dans l'écosystème internet, mais ils restent moins répandus que le transit, car le capital important nécessaire pour établir et faire fonctionner ces nœuds en périphérie n'est pas utilisé efficacement. Aujourd'hui, le transit fournit une connectivité adéquate, dans une couche neutre du réseau, pour prendre en charge toutes les applications OTT tout en restant indépendant de celles-ci. Par exemple, les réseaux WAN* des entreprises multisites ont tendance à migrer des VPN* MPLS* coûteux et peu pratiques à des solutions SD-WAN* flexibles et permettant de maîtriser les coûts, reposant sur un accès internet à chaque site : ceci est possible uniquement parce que la qualité de l'interconnexion entre FAI, souvent *via* des réseaux de transit, est équivalente sinon supérieure à celle des réseaux privés traditionnels.

Le transit joue un rôle unique dans l'écosystème de la connectivité internet, tout en étant un marché concurrentiel. Les progrès technologiques dans le transport ou le traitement continuent à faire baisser sans cesse le prix de la bande passante. L'idée fondatrice de Cogent était que la bande passante deviendrait une commodité, tout comme l'électricité ou l'eau, et que, par conséquent, les opérateurs internet devaient agir comme des entreprises de services publics et produire la bande passante en grande quantité, à moindre coût unitaire. Cette vision est devenue une réalité et, avec son réseau de 150 000 km de fibre optique, plus de 7 000 AS connectés à travers le monde, et un volume de trafic de plus de 625 pétaoctets qui transitent sur son réseau tous les jours, Cogent est l'un des plus importants fournisseurs de transit au monde. Internet est le seul réseau qui compte, et le transit est la pierre angulaire d'internet.

* Voir lexique.

RÔLE DU TRANSIT DANS L'ÉCOSYSTÈME D'INTERNET



LA PAROLE À... JORG DEKKER

*Responsable des services internet - **Telia Carrier***

FAIRE FACE À L'ÉVOLUTION DE L'ARCHITECTURE INTERNET

Remplir sa mission de responsabilité sociale de l'internet

Le réseau global IP de Telia Carrier, AS1299, représente près de 60 % des routes internet mondiales. Être leader dans son domaine implique de nombreuses responsabilités. Chez Telia Carrier, nous nous engageons chaque jour pour chaque client, partout dans le monde, et l'un de ces engagements comprend la sécurité et la stabilité du routage internet. Dans le monde des entreprises, on parle de responsabilité sociale. Dans notre écosystème internet, on parle alors de RPKI (*Resource Public Key Infrastructure*) et Telia Carrier est le premier dans la catégorie des fournisseurs de services *Tier 1* à l'avoir mis en œuvre à l'échelle mondiale, en février 2020, pour ses *peers* et ses clients.

RPKI est un mécanisme qui permet aux propriétaires de ressources IP de s'assurer de fournir une liste valide des routes autorisées au reste du monde. Ce mécanisme aide à la validation et au filtrage des annonces BGP* de chaque fournisseur, empêchant ainsi les détournements de trafic (annonce illégitime d'adresse étrangère ou de numéro d'AS, intentionnellement ou non) et les fuites (annonce illégitime d'une route reçue d'un *peer* vers un autre). Bien qu'il ne s'agisse pas d'une nouvelle technologie, RPKI a connu un démarrage difficile, comme l'IPv6, avec un faible taux d'adoption auprès des propriétaires de ressources IP et des opérateurs. Suite à l'implémentation RPKI de Telia Carrier à l'échelle mondiale et l'enthousiasme unanime de nos clients, qu'ils soient fournisseurs de contenu ou FAI, nous pensons que beaucoup d'autres nous rejoindront sur le même chemin en 2020.

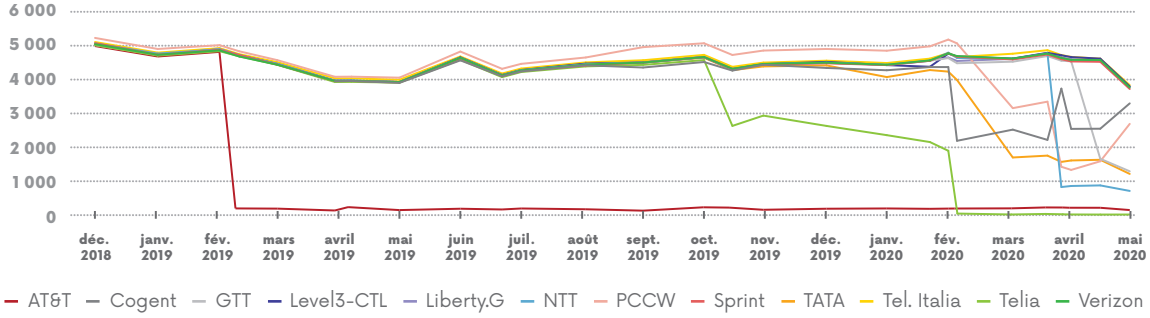
Toujours surfer sur la vague de la croissance

L'AS1299 représente plus de 2 000 clients ainsi qu'une trentaine de *peers*. Le trafic total de 60 Tbit/s est réparti sur 150 équipements de périphérie, cumulant près de 10 000 sessions BGP. En 2019, Telia Carrier aura déployé plus de 10 000 nouveaux ports 100 Gbit/s. Accroître son agilité tout en diminuant ses coûts, tout cela à l'échelle mondiale, n'est pas nouveau dans le monde des opérateurs. Ce qui change vraiment aujourd'hui est non seulement le besoin de planifier l'appétit constant pour la capacité à la demande, illimitée et de haute qualité requise pour la 5G, le *streaming*, les jeux et les connexions 100 % disponibles, mais aussi d'agir rapidement et soutenir ses utilisateurs dans toutes les situations.

La normalisation en cours de technologies cohérentes 400 Gbit/s encourage de nouvelles architectures IP sur DWDM* simplifiées et partiellement décorrélées. Notre ambition est maintenant d'utiliser cette vague comme référence dans des systèmes optiques ouverts sur plusieurs continents. En février 2020, nous avons commencé le déploiement de notre nouvelle architecture réseau avec une densité inégalée, de 1 Gbit/s jusqu'à 400 Gbit/s, avec une technologie de routage à l'échelle du *cloud*. La valeur des logiciels s'est accrue, les cycles matériels sont devenus plus courts et la normalisation en cours du 400 Gbit/s est sur le point de révolutionner enfin le marché des réseaux optiques.

* Voir lexique.

NOMBRE DE ROUTES IPv4 INVALIDES



Source : CAIDA https://www.caida.org/publications/papers/2020/filter_not_filter/filter_not_filter.pdf

2. ÉTAT DE L'INTERCONNEXION EN FRANCE

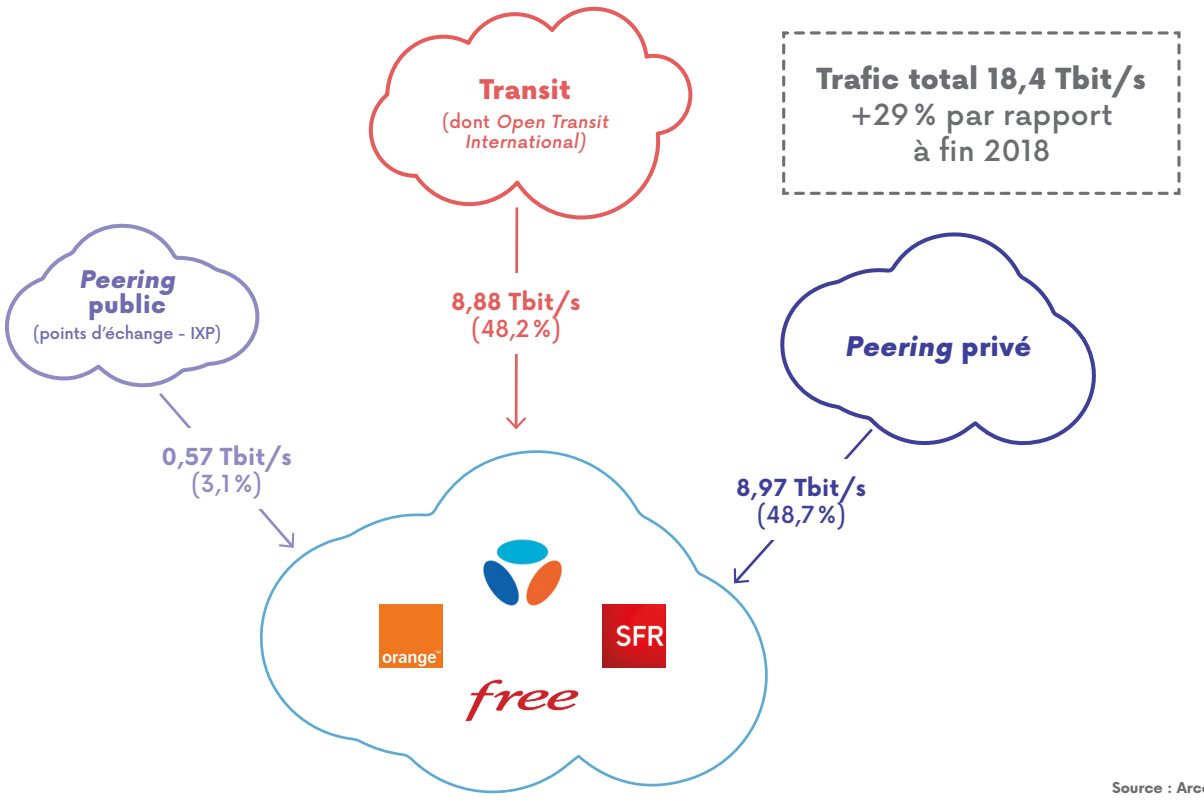
Grâce à la collecte d'information sur l'interconnexion et l'acheminement de données qu'elle réalise, l'Arcep dispose de données techniques et tarifaires sur l'interconnexion du premier semestre de 2012 au second semestre de 2019. Par souci de confidentialité, la publication des résultats[4] ne porte que sur des données agrégées.

2.1. Trafic entrant

Le trafic entrant vers les quatre principaux FAI en France à l'interconnexion est passé de plus 14,3 Tbit/s à fin 2018 à 18,4 Tbit/s à fin 2019, marquant ainsi une augmentation de 29 % 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.

Ce taux de transit est beaucoup moins élevé chez les autres FAI qui, n'ayant pas en parallèle une activité de transitaire, font davantage appel au *peering*.

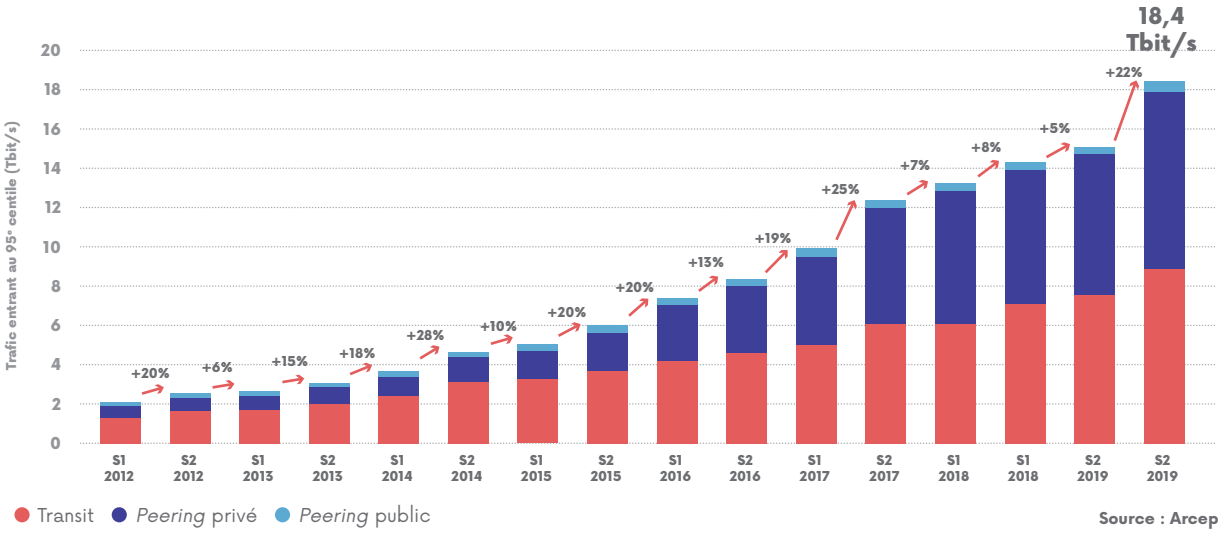
RÉPARTITION DU TRAFIC ENTRANT À L'INTERCONNEXION (AU 95E CENTILE) SUR LE RÉSEAU DES PRINCIPAUX FAI EN FRANCE (FIN 2019)



Source : Arcep

4. Résultats issus des réponses des différents opérateurs 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 la décision 2017-1492-RDPI (https://www.arcep.fr/uploads/tx_gsavis/17-1492-RDPI.pdf).

ÉVOLUTION DU TRAFIC ENTRANT À L'INTERCONNEXION VERS LES PRINCIPAUX FAI EN FRANCE ENTRE S1-2012 ET S2-2019

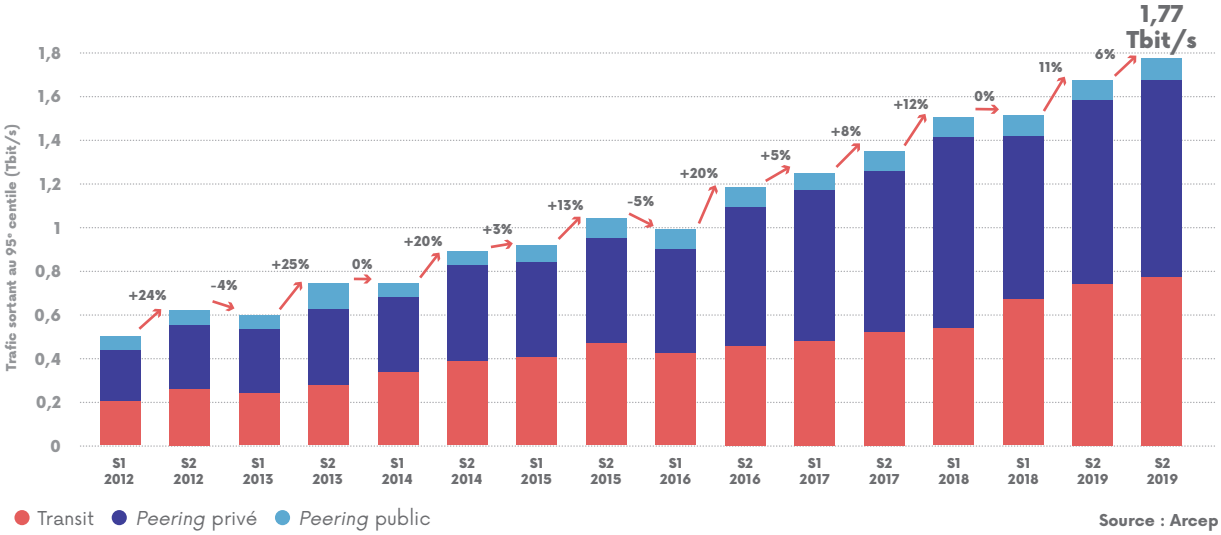


Source : Arcep

2.2. Trafic sortant

À fin 2019, le trafic sortant du réseau des quatre principaux FAI en France à l'interconnexion atteint environ 1,8 Tbit/s, soit une augmentation de 17 % par rapport à fin 2018. Entre 2012 et 2019, ce trafic a été multiplié par quatre.

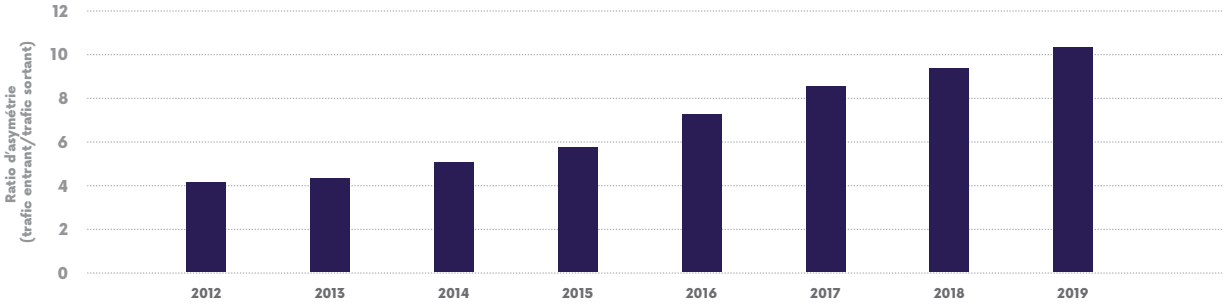
ÉVOLUTION DU TRAFIC SORTANT À L'INTERCONNEXION DES PRINCIPAUX FAI EN FRANCE ENTRE S1-2012 ET S2-2019



Source : Arcep

Le trafic sortant est bien inférieur au trafic entrant. Par ailleurs, le taux d'asymétrie entre ces deux trafics est passé de 1/4 en 2012 à plus de 1/10 en 2019. Cette augmentation est due notamment 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 TRAFIC ENTRANT ET TRAFIC SORTANT À L'INTERCONNEXION POUR LES PRINCIPAUX FAI EN FRANCE ENTRE 2012 ET 2019

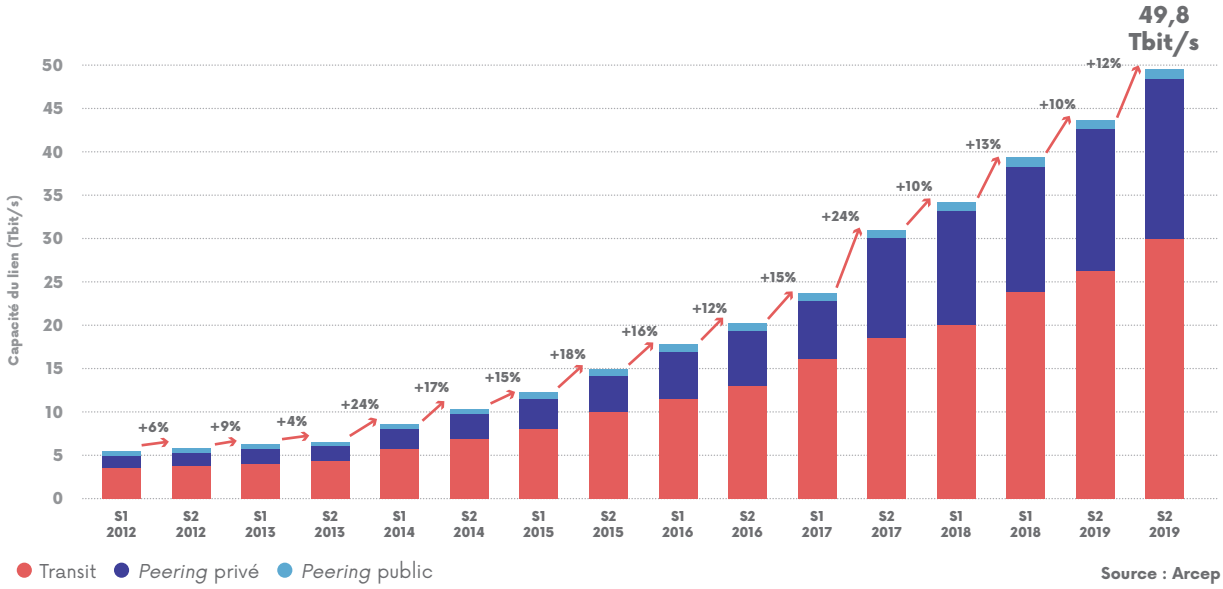


Source : Arcep

2.3. Évolution des capacités installées

Les capacités installées à l'interconnexion ont connu une augmentation du même ordre de grandeur que le trafic entrant. Les capacités installées à fin 2019 sont estimées à 49,8 Tbit/s, soit un facteur de 2,7 par rapport au trafic entrant. Ce ratio n'exclut pas l'existence d'épisodes de congestion, qui peuvent survenir entre deux acteurs sur un ou des lien(s) particulier(s) en fonction de leur état à un instant donné, notamment lors de pics d'utilisation.

ÉVOLUTION DES CAPACITÉS DES INTERCONNEXIONS DES PRINCIPAUX FAI EN FRANCE ENTRE S1-2012 ET S2-2019



Source : Arcep

2.4. Évolution des modalités d'interconnexion

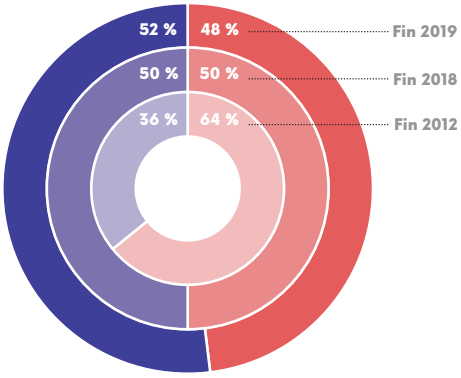
***Peering* vs transit**

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.

La part de *peering* a augmenté légèrement pour passer de 50 % à fin 2018 à environ 52 % à fin 2019. Cette croissance est due cette année à une hausse du trafic en *peering* privé ainsi qu'en *peering* public à moindre échelle. La part relative du *peering* privé passe de 47,5 % fin 2018 à 48,7 % fin 2019 et celle du *peering* public de 2,5 % fin 2018 à 3,1 % fin 2019.

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

(en proportion du trafic entrant)



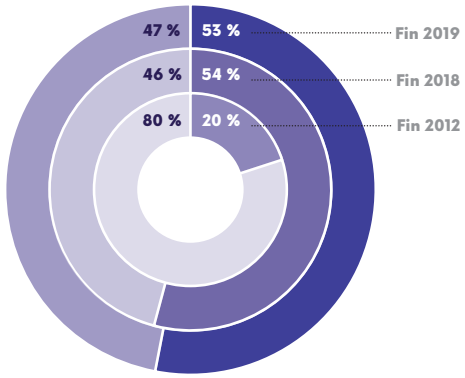
Source : Arcep

***Peering* gratuit vs *peering* payant**

La part du *peering* payant est restée relativement stable (54 % fin 2018 et 53 % à fin 2019). Cette situation s'explique par l'augmentation concomitante, d'une part, du trafic en *peering* privé, dont une proportion importante est payante notamment dans le cas d'une grande asymétrie de trafic, et d'autre part, du *peering* entre les acteurs de taille comparable et du *peering* public, qui sont généralement gratuits.

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

(en proportion du trafic entrant)



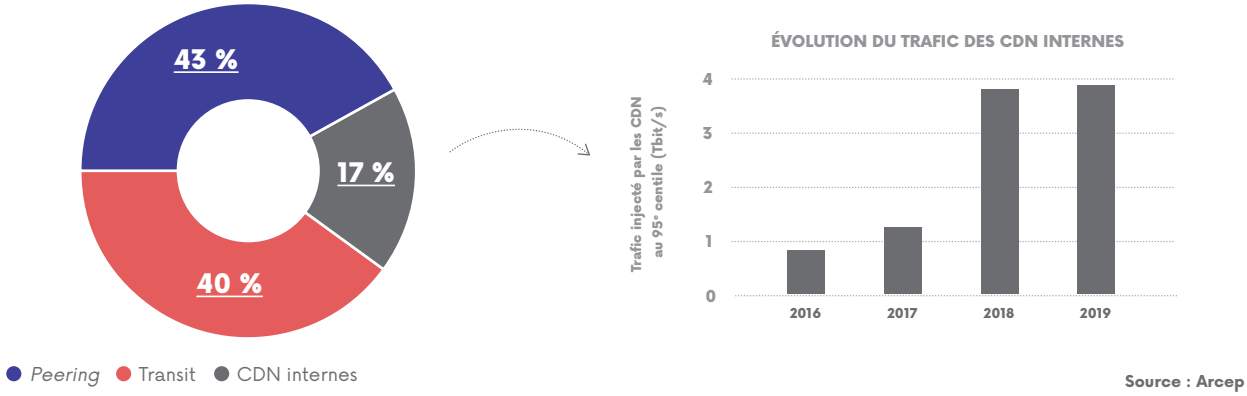
Source : Arcep

2.5. Répartition du trafic par mode d'interconnexion

Entre fin 2018 et fin 2019, le trafic provenant des CDN internes vers les clients des principaux FAI en France a très légèrement augmenté pour atteindre environ 3,9 Tbit/s. Le taux de trafic provenant des CDN internes (17 %) est en baisse par rapport à l'année dernière (21 %), ce qui confirme que le *peering* et le transit restent des modes d'interconnexion largement utilisés par les opérateurs. Ce taux 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 1/14 en fonction de l'opérateur. Autrement dit, les données disponibles au niveau des CDN internes sont consultées entre 5 et 14 fois en moyenne.

RÉPARTITION ENTRE LES DIFFÉRENTS MODES D'INTERCONNEXION DU TRAFIC VERS LES CLIENTS DES PRINCIPAUX FAI EN FRANCE (FIN 2019)

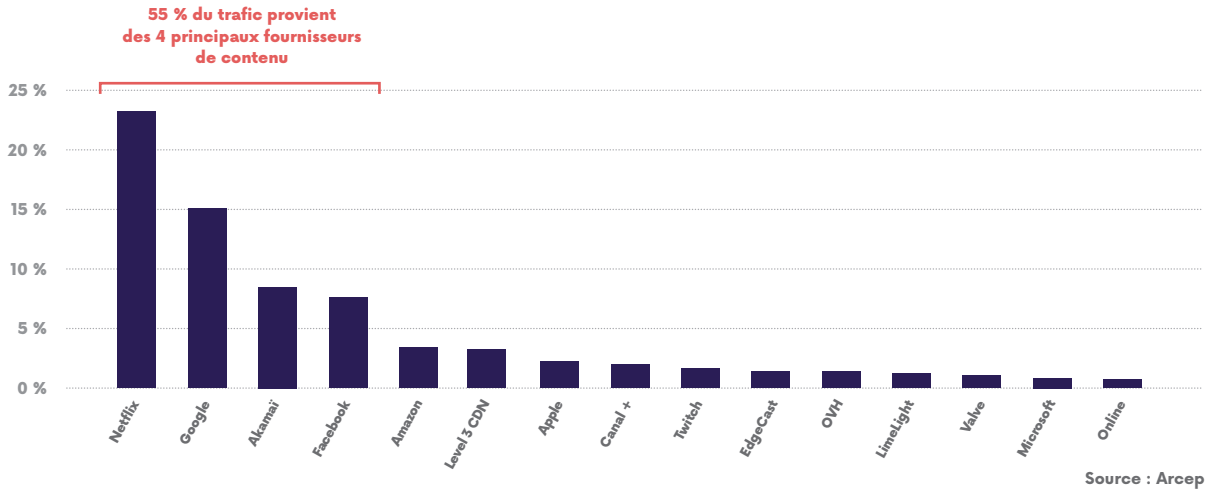


Source : Arcep

2.6. Décomposition du trafic selon l'origine

Plus de la moitié du trafic (55 %)[5] 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. Par ailleurs, l'écart se creuse entre le volume de trafic provenant de Netflix et celui des autres fournisseurs de contenu.

DÉCOMPOSITION SELON L'ORIGINE DU TRAFIC VERS LES CLIENTS DES PRINCIPAUX FAI EN FRANCE (FIN 2019)



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. D'après les données recueillies, les prestations de transit se négocient entre moins de 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[6].

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. Pour information, le trafic provenant des quatre principaux fournisseurs de contenu était de 53 % à fin 2018.
6. Les fourchettes de tarifs ne reflètent que les tarifs payés par les acteurs ayant répondu au questionnaire pour les prestations de transit, *peering* ou CDN internes.

LA PAROLE À... GINA HASPILAIRE

*Vice-présidente - **Netflix Open Connect***

DIFFUSION DU CONTENU NETFLIX : L'INTERCONNEXION ET L'ENCODAGE VIDÉO AU SERVICE D'UN *STREAMING* EFFICACE

Les FAI et les FCA ont une relation de symbiose. Les FAI créent des réseaux robustes pour fournir un accès à internet aux foyers, entreprises et écoles. Les FCA créent et fournissent les services internet qui rendent cet accès à internet important. Chez Netflix, nous avons conçu un système qui réduit simultanément les coûts d'exploitation des FAI, permet une expérience de meilleure qualité pour nos abonnés et minimise l'impact du *streaming* sur l'environnement. Nous le faisons de trois manières :

1- *Netflix Open Connect* : plus c'est proche, mieux c'est

Netflix Open Connect s'associe à plus d'un millier de FAI, notamment en France, afin de diffuser efficacement le trafic Netflix. Netflix fournit gratuitement ses propres serveurs cache, appelés *Open Connect Appliances* (OCA) aux FAI, et a déployé plus de 13 511 de ces serveurs dans 142 pays. Les FAI installent les OCA dans leurs réseaux, permettant au contenu d'être distribué localement. Cela permet de réduire les coûts du FAI en minimisant le trafic circulant *via* du transit, des liaisons louées et/ou des infrastructures de longue distance. Rapprocher le contenu des utilisateurs permet de réduire les liens, routeurs et autres équipements nécessaires. Si un FAI ne souhaite pas prendre d'OCA, Netflix propose d'établir un *peering* directement avec les FAI à un emplacement d'interconnexion mutuellement acceptable.

Open Connect est un partenariat entre Netflix et les FAI. Nous travaillons ensemble pour fournir des solutions de déploiement personnalisées qui peuvent amener jusqu'à 100 % du trafic Netflix à proximité du client final d'un FAI. Et ce sont les FAI qui déterminent les routes annoncées aux OCA déployés.

Par ailleurs, la mise à jour du contenu des OCA s'effectue en dehors des heures de pointe, quand le volume de trafic est à son plus bas niveau, minimisant ainsi l'impact de cette opération sur les réseaux. Étant donné que les réseaux sont établis et généralement facturés en fonction du pic d'utilisation plutôt que par octet, les FAI ne supportent pas de coûts supplémentaires pour l'utilisation de la capacité du réseau aux heures creuses. Ce « prépositionnement » du contenu est unique à Netflix.

Enfin, nous augmentons l'efficacité en préchargeant le contenu populaire sur des disques SSD au sein de l'OCA afin de limiter les accès au contenu à partir des disques durs, qui nécessitent plus d'énergie électrique. Cette approche nous permet de gérer plus de trafic à partir d'un seul appareil tout en optimisant la consommation électrique du *data center*.

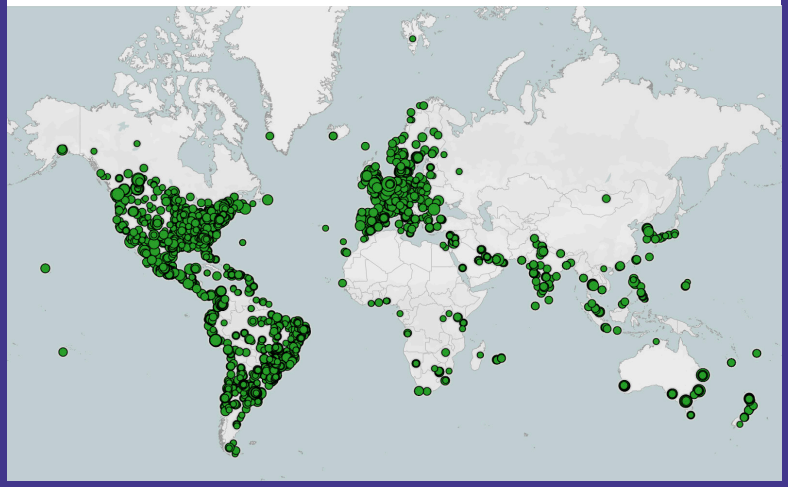
2- *Open Connect Appliances* : une efficacité énergétique fournie gratuitement

La quantité de débit par watt que chaque OCA est capable de fournir a augmenté de plus de 100 % tandis que les OCA sont devenus plus petits. Cela permet aux opérateurs d'obtenir un débit considérablement plus élevé tandis que le besoin de ressources du *data center* diminue ou reste stable.

3- Encodage vidéo : une meilleure qualité avec moins de données

Les encodages vidéo Netflix fournissent une vidéo de haute qualité avec moins de données. Nous avons récemment annoncé AV1[1], un nouveau codage qui peut réduire de 20 % la bande passante requise pour la vidéo de haute qualité sur les appareils mobiles. Nous ajustons également la quantité de données nécessaires pour une vidéo scène par scène afin que les scènes simples nécessitent moins de données que celles complexes.

CARTE DES DÉPLOIEMENTS DES OCA



1. https://netflixtechblog.com/netflix-now-streaming-av1-on-android-d5264a515202

LA PAROLE À... SAMUEL TRIOLET

*Directeur et fondateur - **LyonIX/Rezopole***

IMPACTS TECHNICO-ÉCONOMIQUES DES IXP

Avant 2001, l'interconnexion des réseaux lyonnais, se faisait à Paris.

Outre les aspects techniques comme une mauvaise latence / un manque de résilience / la centralisation *de facto* sur Paris, ce manque d'échange en local avait surtout un impact économique sur la filière IT et plus généralement pour tous les acteurs économiques.

Résultat, on comptait très peu de *data centers*, d'opérateurs locaux, de fibres locales. Et les entreprises hébergeaient leurs données à Paris ou ailleurs à l'étranger.

Bon nombre d'acteurs, y compris des locaux, raillèrent initialement la démarche de créer un IXP à Lyon : « *À Lyon, c'est inutile et ça ne marchera jamais !* ».

Une attention particulière fut portée sur la neutralité de l'entité porteuse de l'IXP pour favoriser la coopération, le *peering*, entre acteurs parfois concurrents, ce qui se concrétisa par l'utilisation du modèle associatif.

Sans capital de départ, des subventions étaient nécessaires et en 2006, le Grand Lyon et la région Rhône-Alpes ont validé leur soutien via des subventions. C'est encore 20 % du budget en 2019.

Dès ses débuts, LyonIX a permis aux différents acteurs connectés, y compris les grands comptes privés et publics, non seulement d'échanger du trafic IP en local, mais également de s'acheter et de vendre tous types de services télécom sur une place de marché évidente et neutre. On parle alors d'IXP/NAP*.

En plus du *peering* et des interconnexions VLAN*, les membres peuvent héberger leur matériel télécom dans les baies de LyonIX, augmentant encore l'aspect stratégique de l'IXP lyonnais.

LyonIX se doit d'être innovant et a déployé RPKI* dès 2014 puis une plateforme VXLAN* EVPN* 100 Gbs en 2018. Étant depuis le début cantonné à l'échelle d'un IXP régional, les interconnexions avec d'autres IXP (8 français et 5 étrangers) ont été favorisées et font de LyonIX l'IXP le plus interconnecté à ses pairs en Europe.

Fin 2019, on comptait 100 acteurs connectés dans 21 baies sur 7 POP*. Une équipe de 9 salariés assure le bon fonctionnement 24/7 et anime le territoire avec des événements, plus de 20 par an ; le réseau des machines a assurément besoin d'un réseau humain.

La véritable raison d'être d'un IXP local serait-elle technique ? L'objectif de gain de quelques dizaines de millisecondes ou la gratuité du *peering* suffisent-ils à motiver les acteurs ?

L'intérêt est bien sûr technique mais aussi à chercher ailleurs sur des aspects économiques, d'emploi, d'écosystème, de start-up, d'économie du libre et de sécurité par la résilience qu'apporte l'IXP.

Si des pans entiers de l'IT moderne partent dans le *cloud* lointain, il reste intéressant d'avoir des offres proposées localement. Cela évite aussi la « fuite de devise » et la destruction d'emplois locaux. On notera que pour accéder aux offres *cloud*, un réseau télécom local performant est nécessaire. Le réseau est non délocalisable.

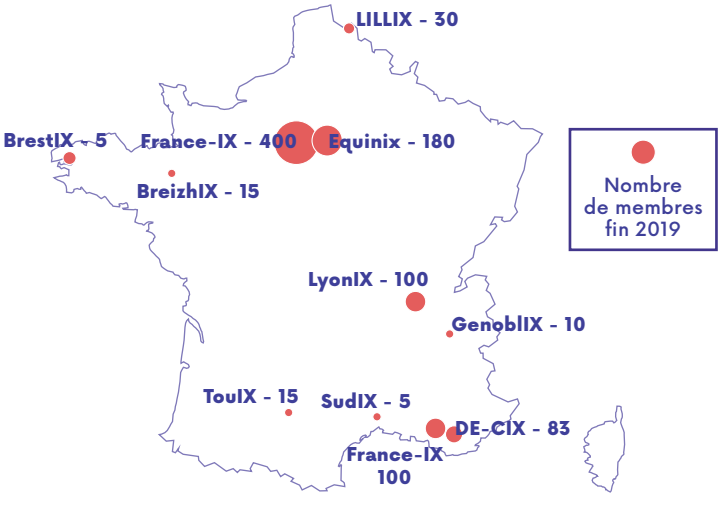
Enfin, à l'aube de la 5G, tous les acteurs du numérique se rendent comptent désormais de l'importance d'être au plus près de l'activité humaine, avec de nouveaux usages qui vont exploser autour du *edge computing* et de l'intelligence artificielle (IA).

Premier bilan, 18 ans après la création de LyonIX : près de 15 *data centers* existent à Lyon, plus de 25 opérateurs locaux et régionaux vendent leurs services aux entreprises. Et tous ces acteurs sont évidemment connectés sur LyonIX.

Les IXP régionaux… inutiles ?

* Voir lexique.

CARTE DES IXP EN FRANCE MÉTROPOLITAINE



CHAPITRE 3

Accélérer la transition vers IPv6

À RETENIR

Le 15 novembre 2019,
l'Arcep et Internet Society France lancent la task-force IPv6. Objectif : favoriser l'accélération de la transition vers IPv6 par l'ensemble de l'écosystème d'internet.

La pénurie d'IPv4 est annoncée **le 25 novembre 2019.**
Conséquence : internet ne cessera pas de fonctionner mais cessera de grandir. La transition vers IPv6 est la seule solution pérenne.

Pourtant, seulement **27 % des sites web** les plus visités en France sont aujourd'hui accessibles en IPv6.

L'IPv4 et l'IPv6, pour *Internet Protocol* version 4 ou version 6, sont des protocoles utilisés sur internet pour permettre d'identifier chaque terminal sur le réseau (ordinateur, téléphone, serveur, etc.). Les adresses IP publiques sont enregistrées et routables sur internet, elles sont donc uniques mondialement. IPv4 et IPv6 ne sont pas compatibles : un équipement ne disposant que d'adresses IPv4 ne peut pas dialoguer avec un équipement ne disposant que d'adresses IPv6. La transition ne se fait pas en remplaçant le protocole IPv4 par IPv6, mais en rajoutant IPv6 en plus d'IPv4[1].

1. LA FIN D'IPv4, LA TRANSITION INDISPENSABLE VERS IPv6

Le protocole IPv4, utilisé sur internet depuis 1983, offre un espace d'adressage de près de 4,3 milliards d'adresses IPv4[2]. 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 ont déjà affecté plus de 90 % des adresses IPv4 qu'ils possèdent, à fin juin 2019[3].

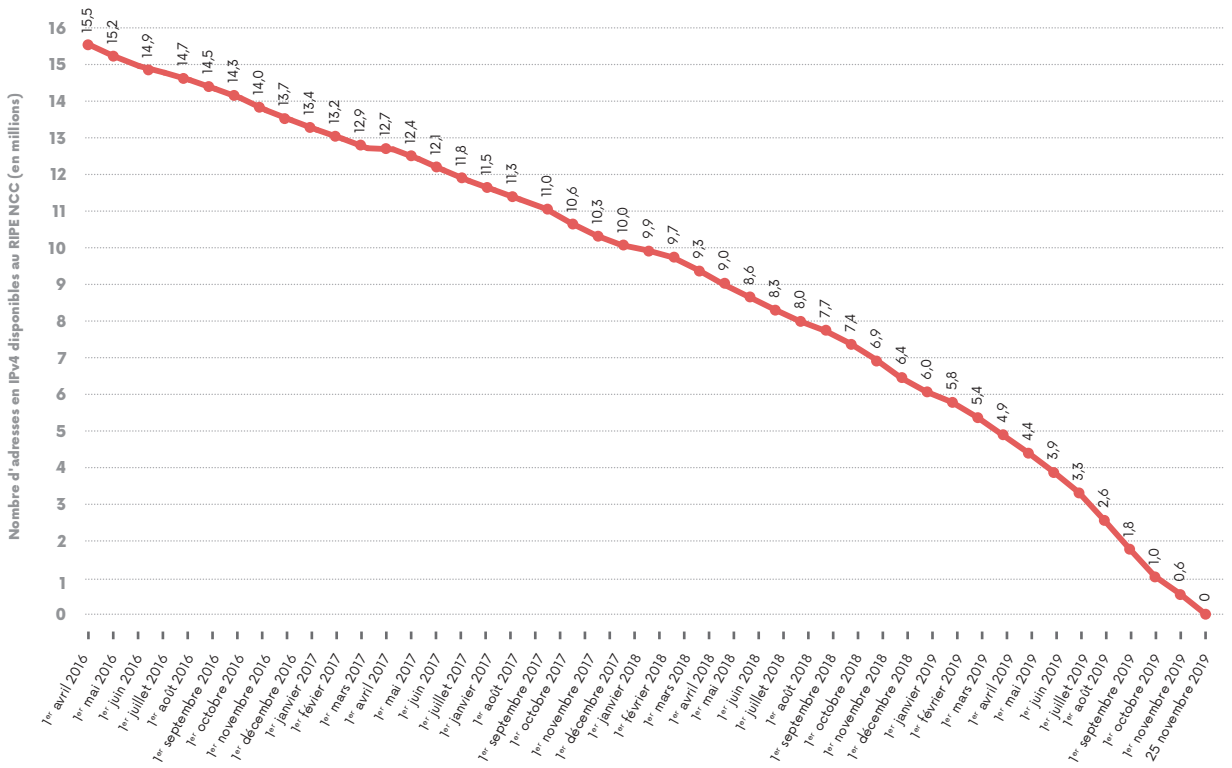
Les spécifications d'IPv6 ont été finalisées en 1998. Elles intègrent des fonctionnalités pouvant renforcer la sécurité par défaut et optimiser le routage. Surtout, IPv6 offre une quasi-infinité d'adresses : 667 millions d'IPv6 pour chaque millimètre carré de surface terrestre[4].

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 2019, internet n'en est encore qu'au début de la phase de cohabitation[5].

Dans l'édition 2019 de son rapport sur l'état d'internet en France, l'Arcep a estimé que l'épuisement du stock d'adresses IPv4 serait effectif vers la fin du second trimestre de 2020, mais le rythme des acquisitions des derniers blocs d'IPv4 s'est accéléré et l'épuisement des adresses IPv4 s'est produit fin 2019. Au 25 novembre 2019, le RIPE NCC (le registre régional qui alloue les adresses IP pour l'Europe et le Moyen-Orient) a en effet annoncé la pénurie d'IPv4, après avoir effectué l'attribution du dernier /22 IPv4 à partir des dernières adresses restantes.

1. Dans certains cas, notamment sur les réseaux mobiles, IPv6 est déployé à la place d'IPv4. Dans ce cas-là, des mécanismes de traduction de protocoles sont mis en place sur le réseau (NAT64 et DNS64) et sur le terminal (464XLAT).
2. Les adresses IPv4 sont codées sur 32 bits. Au maximum 2^{32}, soit 4 294 967 296 adresses peuvent donc être attribuées simultanément en théorie.
3. Données recueillies par l'Arcep auprès de FAI conformément à la décision n° 2019-0287 de l'Autorité en date du 12 mars 2019 (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038383523&categorieLien=id).
4. Les adresses IPv6 sont codées sur 128 bits. Au maximum 2^{128} (soit environ $3{,}4 \times 10^{38}$) adresses peuvent donc être attribuées simultanément en théorie.
5. 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.

HISTORIQUE D'ÉPUISEMENT DES ADRESSES IPv4



Source : données RIPE NCC

Une liste d'attente existe, permettant de récupérer des adresses IPv4 rendues au RIPE NCC, même si peu d'adresses le sont en pratique. Le RIPE NCC explique que ces attributions, nécessairement limitées, ne pourront pas répondre aux besoins d'adresses IPv4 pour les réseaux aujourd'hui.

Faire perdurer internet en IPv4 ne l'empêchera pas de fonctionner, mais l'empêchera de grandir, en raison des risques que présentent les solutions permettant de continuer le fonctionnement d'internet sur IPv4 malgré le manque d'adresses :

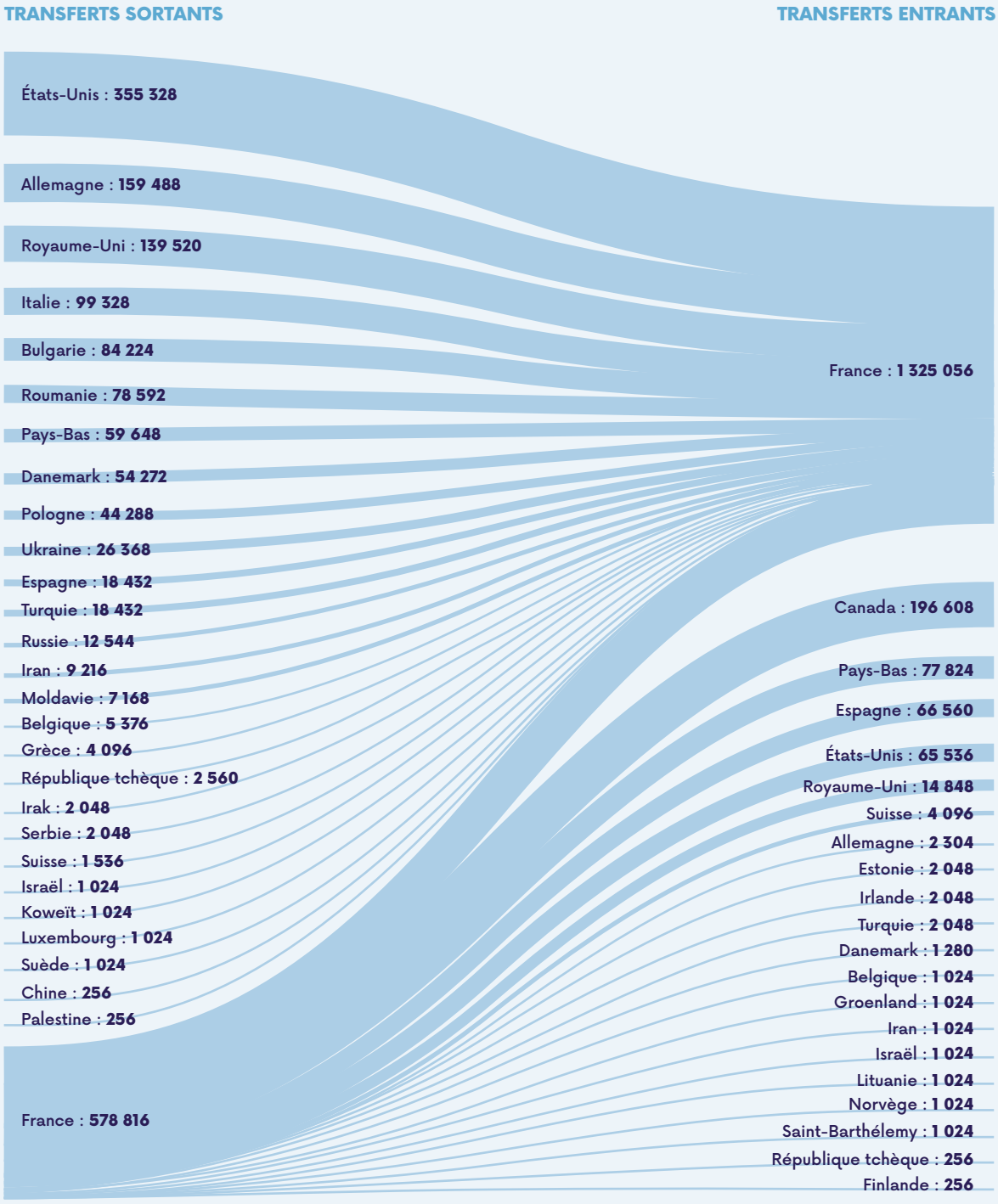
- Le partage d'adresses IPv4 entre plusieurs clients peut provoquer le dysfonctionnement de certaines catégories de services sur internet (systèmes de contrôle de maison connectée, jeux en réseau, etc.). En plus, ce partage augmente le risque de se voir refuser l'accès à un service, par exemple quand l'IP est mise sur liste noire à cause du comportement frauduleux d'un autre colocataire de la même adresse IPv4. Un autre effet collatéral du partage d'IPv4 est de rendre difficile l'identification d'un suspect sur la base de son adresse IP pour les enquêtes judiciaires, obligeant parfois les enquêteurs à ouvrir des enquêtes sur des personnes qui n'ont pour seul tort que de partager la même adresse IPv4 qu'un suspect.
- L'achat d'adresses IPv4 est possible sur un marché secondaire, mais le prix des adresses est susceptible d'ériger une barrière à l'entrée significative à l'encontre des nouveaux acteurs. Par ailleurs, les adresses IPv4 achetées sur le marché secondaire peuvent bloquer certains services bancaires ou de vidéo à la demande tant que la mise à jour de la géolocalisation des adresses n'est pas effective.

Ces pratiques **augmentent le risque de voir se développer un internet scindé en deux, IPv4 d'un côté et IPv6 de l'autre.** Par exemple, certains hébergeurs proposent désormais des offres IPv6-*only* et les sites hébergés sur ces serveurs ne sont alors pas accessibles aux clients d'opérateurs IPv4-*only*.

TRANSFERT D'ADRESSES IPv4 EN FRANCE

Le graphique montre le nombre d'adresses IPv4 importées, exportées et transférées à l'intérieur de la France, ainsi que les pays de provenance ou de destination jusqu'à mars 2020.

NOMBRE D'ADRESSES IPv4 IMPORTÉES, EXPORTÉES ET TRANSFÉRÉES EN FRANCE



Source : RIPE NCC, mars 2020

LA PAROLE À...  MARCO HOGEWONING

RIPE NCC

L'ÉPUISEMENT DES ADRESSES IPv4

En novembre 2019, le RIPE NCC a attribué les derniers blocs d'adresses IPv4 en sa possession. Aujourd'hui, quatre des cinq Registres internet régionaux n'ont que très peu, voire aucun bloc d'adresses IPv4 à allouer aux FAI ou aux autres opérateurs de réseau importants. Par conséquent, la plupart des entreprises cherchent des solutions alternatives : l'achat d'adresses IPv4 sur le marché secondaire, l'adoption de solutions techniques comme le NAT* qui permet de partager une adresse IP entre plusieurs utilisateurs, ou le déploiement du protocole IPv6.

Le marché IPv4

En 2012, la communauté RIPE a développé une politique pour satisfaire au besoin de transférer les adresses non utilisées entre les membres du RIPE NCC. C'est ainsi qu'un marché secondaire s'est développé.

Suite à une demande importante et à une pénurie de ressources, l'IPv4 est devenue chère : les prix actuels varient entre 18 et 24 $ par adresse. Au-delà de l'augmentation du coût de développement de réseaux, un effet de bord de cette monétisation est une augmentation des tentatives de fraude, de vol et de détournement.

Solutions techniques

Des solutions techniques telles que le NAT existent depuis des décennies. Employé à l'origine dans des réseaux privés, le NAT est utilisé aujourd'hui dans les réseaux publics, notamment par des opérateurs mobiles.

Si le NAT a été dimensionné pour satisfaire la demande actuelle, l'équipement nécessaire est coûteux, il peut augmenter la latence et réduit souvent la résilience du réseau en introduisant des goulots d'étranglement ou même des points de défaillance uniques.

De plus, Europol a alerté sur le fait que l'utilisation à grande échelle de la traduction d'adresse de réseau nuit à sa capacité d'enquêter sur les crimes en ligne. De même, le NAT entrave les systèmes de détection de fraude des banques. Des centaines de milliers d'internautes pourraient être touchés lorsqu'un individu avec qui ils partagent leur adresse IP est bloqué par des services internet pour comportement abusif.

Plusieurs gouvernements étudient actuellement les options juridiques pour réduire le nombre d'utilisateurs pouvant partager la même adresse ou ont pu inciter l'industrie à réduire son recours au NAT.

L'adoption du protocole IPv6

Le déploiement du protocole IPv6 chez les FAI, les hébergeurs et les fournisseurs de contenu augmente lentement mais sûrement. Le taux d'activation d'IPv6 dépasse les 50 % dans quelques pays, alors que bon nombre des fournisseurs de contenu parmi les plus importants – notamment Google, Facebook ou Netflix – ont déjà commencé à remplacer IPv4 avec IPv6, non seulement en offrant tous leurs services à la fois en IPv4 et en IPv6, mais surtout en réduisant au strict minimum le recours à IPv4 dans leurs systèmes internes.

Toutefois, le taux d'activation d'IPv6 reste très faible dans de nombreux pays, même dans ceux où la pénurie d'IPv4 rend impossible de connecter tout citoyen ou tout foyer.

La situation en France

Il y a plus de 83 millions d'adresses IPv4 aujourd'hui en France, pour une population d'un peu plus de 65 millions d'habitants, ce qui met l'Hexagone dans une position relativement favorable par rapport à beaucoup d'autres pays.

481 blocs IPv4 ont été transférés à l'intérieur de, vers ou depuis la France depuis 2012, soit plus de 14 millions d'adresses. Certains de ces transferts ont eu lieu suite à d'importantes opérations de fusion ou d'acquisition. Si on exclut ceux-ci, environ 136 000 adresses ont été transférées à l'intérieur du pays, 444 000 adresses importées et 1,9 million d'adresses exportées.

En ce qui concerne IPv6, seuls 38 % des réseaux français (AS) affichent des préfixes IPv6. Même si cela dépasse la moyenne mondiale (27 %), cette proportion reste bien en deçà d'autres pays comme l'Allemagne (56 %)[1], ce qui suggère que des efforts supplémentaires seront nécessaires pour compléter le déploiement IPv6.

La suite

Les incidences de la pénurie IPv4 sont réelles, et les mesures temporaires pour y remédier sont insoutenables à long terme. Les sociétés et les économies migrent vers internet. Des milliards de personnes n'ont toujours pas accès à internet. Les technologies nouvelles et émergentes, telles que l'internet des objets, ne font qu'augmenter les exigences imposées à internet. La transition vers IPv6 est la seule solution à long terme capable d'assurer cette future croissance, et d'assurer que les citoyens, les entreprises ou les gouvernements à travers le monde puissent bénéficier pleinement du potentiel de la transformation numérique.

1. http://v6asns.ripe.net/v/6

* Voir lexique.

Face à cette pénurie annoncée et aux risques encourus, la transition vers un nouveau protocole de communication sur internet apparaît comme un enjeu majeur de compétitivité et d'innovation.

Dans le rapport élaboré avec le concours de l'Afnic décrivant l'état d'IPv6 en France remis au Gouvernement en juin 2016, l'Arcep proposait plusieurs leviers d'action 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 de permettre d'accélérer cette transition.

LA TRANSITION VERS IPv6 DANS LE VISEUR DU BEREC

Face à l'épuisement des adresses IPv4 et à ses conséquences, le BEREC a intégré le sujet de la transition vers IPv6 dans son programme de travail de 2020. Un *workshop* interne entre experts des différentes ARN sera organisé au second semestre de 2020 afin de discuter de la situation actuelle de la transition vers IPv6 en Europe, de partager les bonnes pratiques et d'aborder le rôle que peut avoir le régulateur pour accélérer cette transition.

MOOC OBJECTIF IPv6 : UN EXEMPLE DE FORMATION AU SERVICE DE LA TRANSITION VERS IPv6

Le MOOC Objectif IPv6 est une plateforme de formation gratuite et sous licence *Creative Commons* permettant l'acquisition des compétences-clés pour la mise en œuvre et la gestion d'un réseau IPv6 opérationnel. Il a été conçu par des enseignants-chercheurs des écoles membres de l'Institut Mines-Télécom et de l'Université de La Réunion, ainsi que des professionnels des réseaux. Hébergé sur la plateforme Fun MOOC*, il a attiré plus de 2 000 inscrits issus de 60 pays dans sa session 5, ouverte du 6 juin au 9 septembre 2019.

Ce cours a pour objectif d'aider le participant **à évoluer vers la mise en œuvre d'IPv6** dans une approche orientée vers **l'opérationnel :**

- après un exposé des concepts en vidéo, un **support de cours complet** détaille notamment la mise en œuvre opérationnelle ;
- des **travaux pratiques** permettent de mettre en application le protocole IPv6 dans un réseau fonctionnel virtualisé sur un poste ;
- des **exercices** d'approfondissement permettent des **études de cas réels** rencontrés sur le terrain.

Le MOOC Objectif IPv6 s'adresse aussi bien aux étudiants, professionnels ou amateurs intéressés par les évolutions d'internet. Il décrit un protocole et des mécanismes des réseaux informatiques. Il n'est pas nécessaire de maîtriser le protocole IPv4. Des rappels sur des détails précis sont donnés au besoin tout au long du cours.

Ce MOOC permet à la personne qui le suit :

- d'expliquer les différents types d'adresses IPv6, **leur notation et leurs usages** ;
- de créer un plan d'adressage IPv6 **en tenant compte des évolutions du réseau** ;
- de mettre en application les mécanismes **nécessaires à un réseau IPv6 opérationnel** ;
- de planifier la gestion **d'un réseau IPv6** (détecter les pannes, assurer le bon fonctionnement et la sécurité) ;
- d'expliquer le besoin d'interopérabilité **des réseaux et services entre IPv6 et IPv4** ;
- d'appliquer des solutions **dans différents contextes d'interopérabilité.**

La prochaine session du MOOC IPv6, disponible à l'automne 2020, voit une partie de son cours mis à jour, avec de nouvelles vidéos et de nouveaux thèmes adaptés aux débutants et aux décideurs, mais aussi aux experts réseaux IPv4 voulant se former pour gérer une mise en place du protocole IPv6 dans leur entreprise.

* Plateforme Fun Mooc : https://www.fun-mooc.fr

LA PAROLE À...  STÉPHANE BORTZMEYER

Afnic

LA TRANSITION VERS IPv6 POUR LES NULS

Si vous lisez les publications de l'Arcep, ou si vous avez déjà regardé un article parlant de l'internet d'aujourd'hui, vous avez sans doute déjà vu mentionné « IPv6 ». Et, plus précisément, vous avez lu qu'il y avait un problème avec « la migration vers IPv6 ». Cette migration, et la lenteur gastéropodesque avec laquelle elle se fait, est en effet un des grands échecs de l'internet, et qui mérite qu'on se penche dessus.

Toutes les données qui circulent sur l'internet sont découpées en petites unités nommées « paquets », et qui doivent respecter un certain format, normalisé pour que toute machine connectée à l'internet puisse communiquer avec toute autre. Ce format se nomme IP, pour *Internet Protocol*. Ce format a évolué dans le temps, trois premières versions ont été testées sans succès avant que ne soit adoptée la quatrième version, IPv4 (pour « IP version 4 ».) IPv4 a une sérieuse faiblesse, la place réservée pour indiquer les adresses des machines ne permet qu'un maximum de quatre milliards d'adresses. Cela peut sembler beaucoup mais cela ne fait même pas une adresse par être humain, alors qu'aujourd'hui beaucoup d'humains ont plusieurs machines connectées à l'internet et donc besoin de plusieurs adresses IP.

La pénurie d'adresses IPv4 se fait sentir depuis plusieurs années, menant à des manœuvres plus ou moins honnêtes, comme le récent détournement d'adresses IPv4 de la ville du Cap (et de nombreux autres acteurs sud-africains), sans compter des vols d'adresses pour lesquels le registre africain AFRINIC a porté plainte. Comme le disait ma grand-mère, *« quand le foin manque dans l'écurie, les chevaux se battent ».*

Le problème est identifié depuis longtemps et, en 1995 (soit une éternité en temps internet), la version 6 d'IP, « IPv6 », a été créée, résolvant ce problème. (Ne me demandez pas où est passée la version 5.) Ainsi, mon blog personnel a l'adresse 204.62.14.153 en IPv4 et 2605:4500:2:245b::42 en IPv6.

Il ne restait plus qu'à faire migrer tout l'internet vers cette nouvelle version, de la même façon qu'on est passé de MS-DOS à Windows 3 puis Windows 95, puis… (jusqu'à Windows 10 aujourd'hui.) Mais, et c'est là qu'il y a un problème, la migration qui, dans les visions les plus optimistes, devait prendre quelques années, n'est toujours pas achevée. Si tous les systèmes d'exploitation savent faire de l'IPv6 depuis le siècle dernier, si les gros hébergeurs de contenu, comme Google et Facebook, ont IPv6 depuis longtemps, si les nombreux hébergeurs français, comme OVH ou Gandi, proposent de l'IPv6 à leurs clients, il n'y a pas encore une couverture complète en IPv6. Certains FAI n'ont toujours pas IPv6, et certains sites web restent en IPv4 seul.

Pourquoi donc ce retard, après tant d'années ? Alors que, depuis 1995, on a changé d'ordinateur, d'ordiphone, de version du navigateur et de version d'Android plusieurs fois ? Tout le monde, et son chat, a une opinion à ce sujet. Écartons tout de suite l'hypothèse comme quoi il y aurait un problème technique. IPv6 n'est pas un nouveau protocole, juste une nouvelle version, et le changement n'a rien d'effrayant, surtout dans un secteur où on est habitué à des changements bien plus disruptifs et fréquents. Certes, IPv6 n'est pas compatible avec IPv4 mais c'est souvent le cas dans les migrations : le protocole HTTPS (la version sécurisée du web) n'est pas compatible avec HTTP et la migration a pourtant été faite bien plus vite, en réponse aux problèmes de sécurité du HTTP traditionnel.

Et donc, si ce n'est pas un problème technique, c'est quoi ? Avant tout, il s'agit d'un problème de prise de décision. Pour un acteur de l'internet, migrer son réseau, ses serveurs, ses applications, vers IPv6, ce n'est pas un exploit technique, ce n'est pas très compliqué, mais ce n'est pas à coût nul non plus. Et, si chaque dépense est évaluée en fonction des bénéfices financiers qu'elle rapportera, le calcul est vite fait : IPv6 est utile collectivement (car il supprime le problème de pénurie) mais n'a guère d'intérêt financier individuel, pour chaque acteur. Comme l'internet n'a pas de Direction (avec un grand D) qui pourrait aboyer *« tout le monde passe à IPv6 et plus vite que cela ! »*, comme tout dépend de décisions locales, il est extrêmement difficile de réaliser les migrations qui sont utiles à tous, mais pas à chacun.

L'étude des problèmes de la migration vers IPv6 ne nous dit donc rien sur la technique, ou sur la gestion des réseaux informatiques. En revanche, elle nous renseigne beaucoup sur nos processus de décision. Comme en écologie, on constate que les décisions fondées sur un gain financier pour l'opérateur qui décide mènent à des situations peu souhaitables pour la collectivité.

TUTORIEL

COMMENT CONNAÎTRE LA RÉPARTITION DES FLUX IPv4/IPv6 SUR UN SERVEUR ?

Plusieurs outils peuvent être utilisés pour faire du *monitoring* réseau, mais ce tutoriel se base sur Munin pour un serveur Linux.

Munin est un système de *monitoring open source*, simple à mettre en place, intégré dans presque toutes les distributions Linux. Il est plutôt utilisé pour superviser d'un à quelques dizaines de serveurs, mais il peut aussi être utilisé sur un PC bureautique.

L'architecture de Munin est constituée d'un processus serveur appelé Munin-master, récupérant les informations toutes les 5 minutes sur un ou plusieurs PC où Munin-node est installé.

Munin-master permet de générer une série de graphiques mis à disposition sur une interface web. Les graphiques peuvent représenter l'utilisation du processeur, de la mémoire, du réseau, la température de la carte-mère ou du processeur…

Munin-node est à installer sur chaque serveur poste Linux à analyser. Des nombreux plugins sont disponibles pour Munin-node : celui décrit ci-dessous permet de créer un graphique d'usage d'IPv6 et IPv4. Les données sont celles de toutes les interfaces réseaux de la machine analysée, si elle en dispose de plusieurs.

Pour élaborer des statistiques IPv6, il faut récupérer le code du plugin Munin IPv6, disponible sur GitHub[1] et le placer dans un fichier nommé /usr/share/munin/plugins/ipv6_ et rendre le script exécutable :

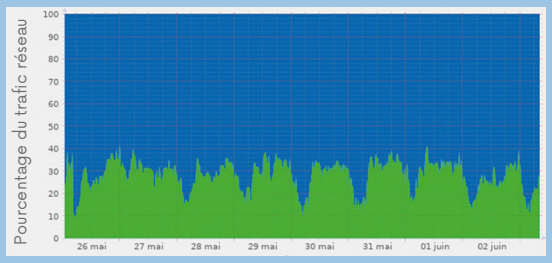
- **chmod +x /usr/share/munin/plugins/ipv6_**

Pour activer le plugin, il est nécessaire de créer deux liens : un pour le graphique exprimé en pourcentage et un pour celui exprimé en Mbit/s (ou Gbit/s) :

- **ln -s /usr/share/munin/plugins/ipv6_ /etc/munin/plugins/ipv6_total**
- **ln -s /usr/share/munin/plugins/ipv6_ /etc/munin/plugins/ipv6_percent**

Voici un exemple des graphiques produits par ce plugin IPv6[2] :

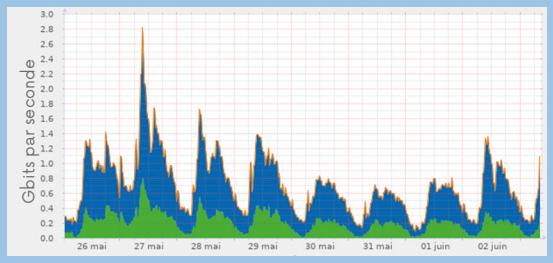
RÉPARTITION DES PROTOCOLES IPv4 ET IPv6 – PAR SEMAINE



	Actuel	Minimum	Moyenne	Maximum
% IPv6	27,64	5,19	28,32	50,44
% IPv4	72,35	49,55	71,67	94,80

Dernière mise à jour : Mercredi 3 juin 2020 08:30:23

TRAFIC RÉSEAU PAR PROTOCOLE IP – PAR SEMAINE



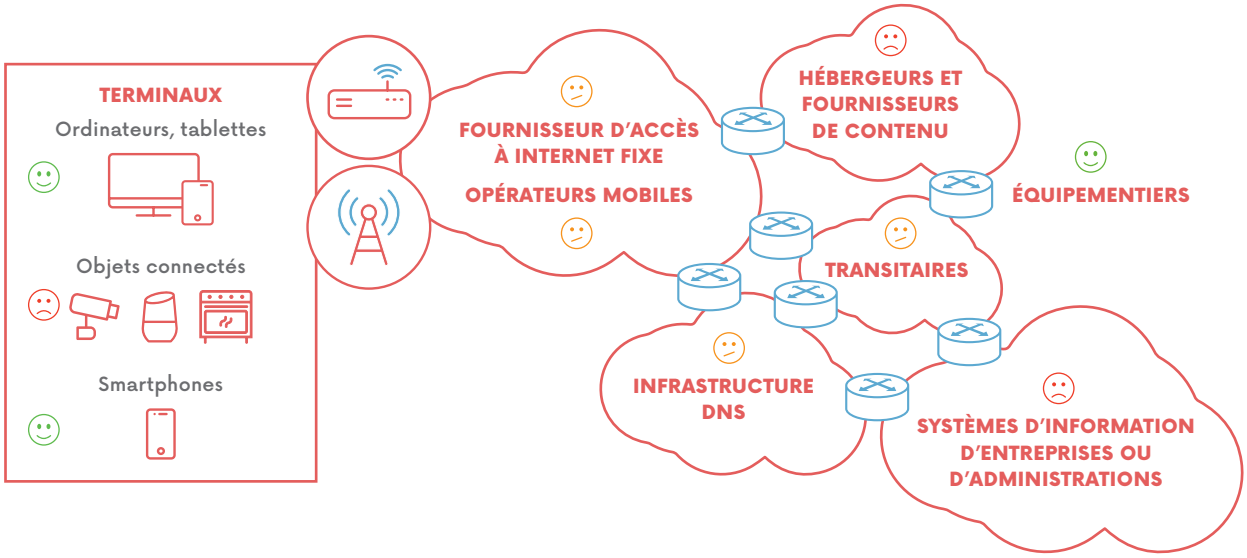
	Actuel	Minimum	Moyenne	Maximum
IPv6 bps	304,15 M	8,61 M	210,29 M	864,46 M
IPv4 bps	793,40 M	58,95 M	499,13 M	2,35 G
Total bps	1,10 G	76,32 M	709,42 M	3,16 G

Dernière mise à jour : Mercredi 3 juin 2020 08:30:18

1. Plug-in IPv6 pour Munin : https://github.com/MorbZ/munin-ipv6/blob/master/ipv6_
2. Graphiques extraits de https://fr.archive.ubuntu.com/stats/stats_server.html

2. BAROMÈTRE DE LA TRANSITION VERS IPv6 EN FRANCE

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

Le baromètre annuel de la transition vers IPv6 a pour objectif 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[6], donne un aperçu de l'état du déploiement d'IPv6 en France pour les différentes parties prenantes impliquées dans la transition. L'Arcep a publié l'édition 2019 de ce baromètre le 15 novembre 2019.

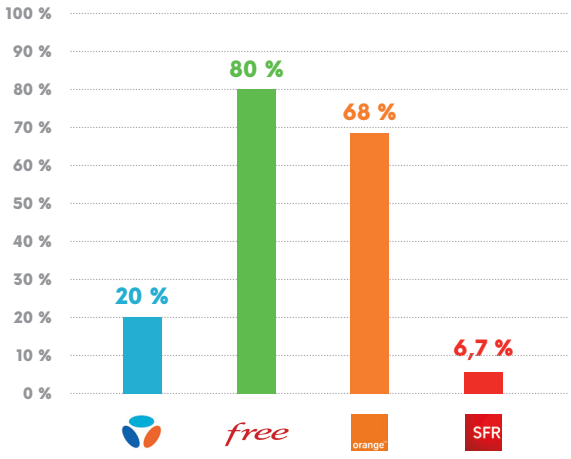
L'édition 2019 du baromètre a été enrichie par rapport aux éditions précédentes grâce, d'une part, à l'élargissement de la collecte d'informations 2019 (notamment aux opérateurs ayant entre 5 000 et 3 millions d'abonnements actifs sur les marchés de détail grand public), et d'autre part, à l'ajout de données exclusives fournies par l'Afnic, notamment sur l'hébergement. Comme exposé ci-après, les parties prenantes se trouvent à différentes étapes de la transition.

Les résultats confirment la progression du taux d'utilisation d'IPv6 en France qui est de plus de 38 % en mars 2020. La France qui se situait l'année dernière à la moyenne du classement européen, se situe aujourd'hui en quatrième position derrière la Belgique, l'Allemagne et la Grèce en termes d'utilisation d'IPv6[7]. 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.

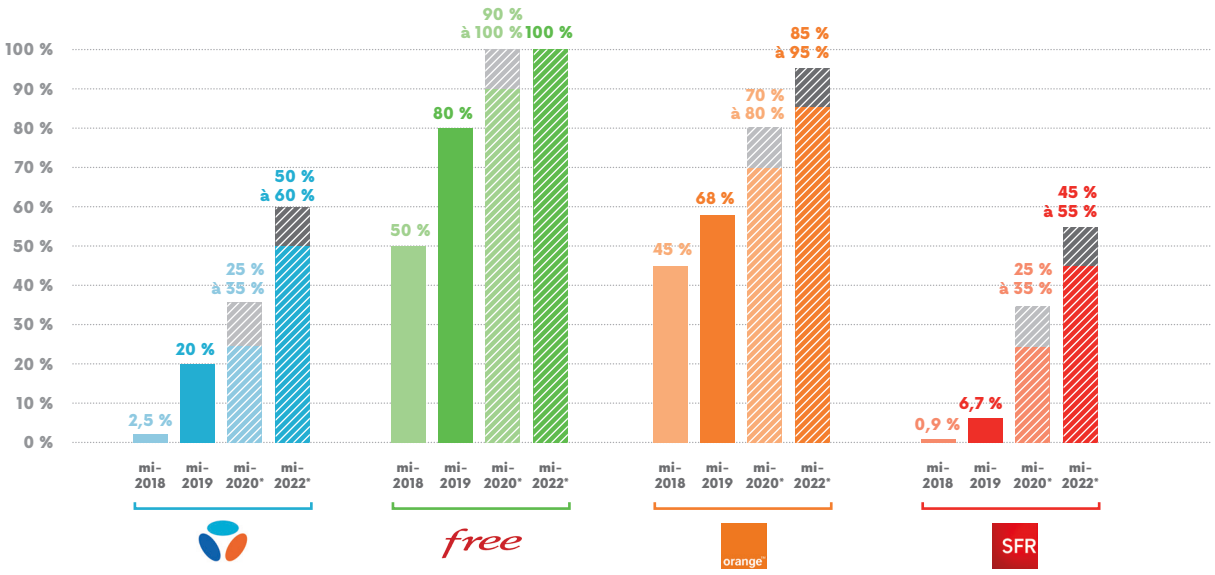
RÉSEAU FIXE : TAUX DE CLIENTS ACTIVÉS EN IPv6



Source : données à fin juin 2019, recueillies par l'Arcep auprès des opérateurs

6. Décision n° 2019-0287 de l'Arcep relative à la mise en place d'enquêtes dans le secteur des communications électroniques (https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038383523&categorieLien=id)
7. Cisco 6lab au 28/10/2019 (https://6lab.cisco.com/stats/index.php?option=users)

RÉSEAU FIXE : ÉVOLUTION DU TAUX DE CLIENTS ACTIVÉS EN IPv6



* **Chiffres susceptibles d'évoluer**

Source : données à fin juin 2019, recueillies par l'Arcep auprès des opérateurs

Sur le réseau fixe, en ce qui concerne les principaux opérateurs télécom en France, des progrès peuvent être constatés même si les opérateurs doivent encore poursuivre leurs efforts :

- À fin juin 2019, 100 % des clients SFR sont déjà compatibles IPv6 sur le xDSL, 60 % en FttH et 0 % sur le câble. Des progrès sur l'activation en FttH sont à noter, même si le nombre de clients activés, c'est-à-dire qui émettent et reçoivent effectivement en IPv6, reste très faible (moins de 7 % des clients toutes technologies confondues). Les activations à venir demeurent également insuffisantes (entre 25 % et 35 % à mi-2020 et entre 45 % et 55 % à mi-2022). Une grande majorité des clients n'activant pas IPv6 manuellement, SFR est encouragé à réaliser cette activation par défaut comme la plupart des autres opérateurs.
- Les efforts de déploiement de Bouygues Telecom sont observés (environ 20 % de clients activés à mi-2019 contre 2,5 % à mi-2018) bien que la compatibilité en IPv6 reste très faible. Les prévisions demeurent également très insuffisantes (entre 50 % et 60 % à mi-2022) pour faire face à la pénurie. Bouygues Telecom est encouragé à augmenter le nombre de clients IPv6-*ready* et à poursuivre les efforts de déploiement d'IPv6 sur leur réseau fixe.
- Sur les réseaux fixes, les taux à fin juin 2019 de clients activés de Free et d'Orange sont relativement élevés (environ respectivement 80 % et 68 %) et ont progressé. Les projections à mi-2022 sont encourageantes (100 % pour Free et entre 85 % et 95 % pour Orange) mais la pénurie rend nécessaire une accélération de la transition encore plus prononcée.
- Free a déployé un nouveau *firmware* sur la très grande majorité de ses box en mai 2019 et supprimé la possibilité de désactiver IPv6, augmentant ainsi significativement l'utilisation d'IPv6 en France.

Comme indiqué précédemment, afin d'améliorer le suivi de la transition vers IPv6, l'Arcep a élargi la collecte d'informations aux opérateurs ayant entre 5 000 et 3 millions de clients grand public sur le marché fixe. Au global, le nombre d'opérateurs ayant entamé leur transition reste faible, même si l'on peut souligner les initiatives de certains opérateurs tels que Coriolis, K-Net et OVH Télécom qui poursuivent leur transition vers IPv6 engagée depuis plusieurs années et Orne THD qui a déjà migré l'intégralité de ses clients. Plus d'informations sont disponibles dans le baromètre IPv6[8].

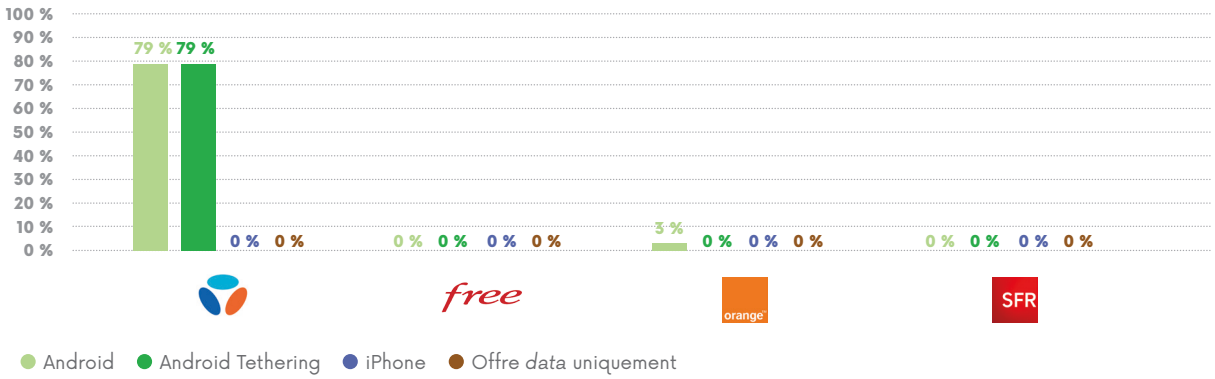
Alors que l'Europe connaît désormais une pénurie d'IPv4, certains acteurs n'envisagent pas un déploiement d'IPv6 sur leurs réseaux fixes, ce qui, comme indiqué plus haut, apparaît problématique.

8. Baromètre Arcep IPv6 2019, « Les opérateurs ayant entre 5 000 et 3 millions de clients sur le réseau fixe » : https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_Barometre_2019_de_la_transition_vers_IPv6.pdf#page=9

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.

RÉSEAU MOBILE : TAUX DE CLIENTS ACTIVÉS EN IPv6



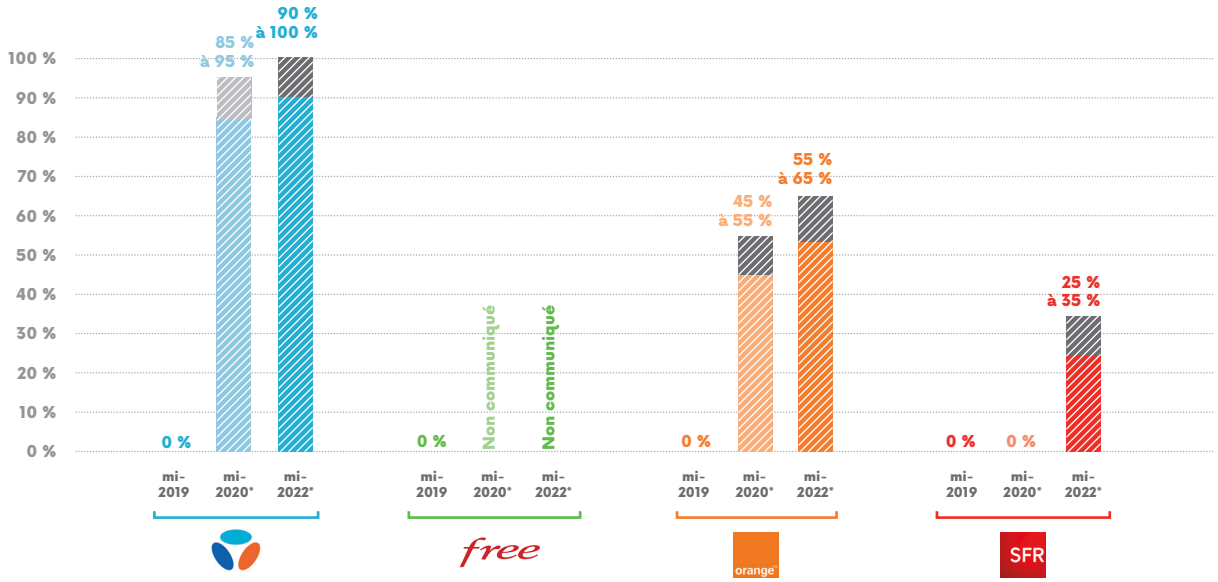
Source : données à fin juin 2019, recueillies par l'Arcep auprès des opérateurs

ANDROID : ÉVOLUTION DU TAUX DE CLIENTS ACTIVÉS EN IPv6

* **Chiffres susceptibles d'évoluer**

Source : données à fin juin 2019, recueillies par l'Arcep auprès des opérateurs

iPHONE :
ÉVOLUTION DU TAUX DE CLIENTS ACTIVÉS EN IPv6



* **Chiffres susceptibles d'évoluer**

Source : données à fin juin 2019, recueillies par l'Arcep auprès des opérateurs

Sur le réseau mobile, l'Arcep s'inquiète du retard dans le déploiement d'IPv6 et invite les opérateurs à prendre les mesures nécessaires pour faire face à la pénurie d'IPv4 :

- Bouygues Telecom poursuit ses efforts de déploiement sur les réseaux mobiles, avec 79 % de clients Android activés.
- Les prévisions d'Orange sur Android sont à noter (entre 15 % et 25 % à mi-2020 et entre 45 % et 55 % à mi-2022), même si l'opérateur est invité à augmenter le nombre de terminaux dans lesquels IPv6 est activé.
- Bouygues Telecom et Orange ont mené un déploiement remarquable sur les iPhone en septembre 2019 (respectivement 68 % et 30 % fin octobre 2019).
- Malgré les efforts prévus par SFR pour 2022, le déploiement programmé reste, selon l'Autorité, insuffisant en termes d'objectif et de rythme.
- Il est particulièrement regrettable que Free Mobile n'ait pas été en mesure de transmettre des prévisions.
- Les opérateurs sont invités à entamer le déploiement d'IPv6 sur l'intégralité de leurs offres, notamment « *data* uniquement » et entreprises.

Parmi les opérateurs ayant entre 5 000 et 3 millions de clients, Zeop est l'unique opérateur mobile qui a commencé à activer IPv6 sur son réseau[9].

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 ralentir la transition vers IPv6.

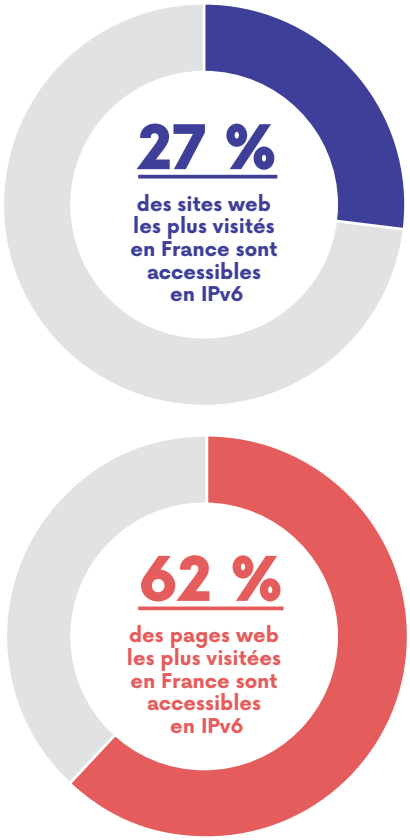
2.3. Hébergeurs web

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 27 % sont accessibles en IPv6[10]. 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 (62 %)[11]. 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.

Le taux de sites disponibles en IPv6 est uniquement de 15,5 % lorsque l'on considère les 3,5 millions de sites web en .fr, .re, .pm, .yt, .tf et .wf[12]. Ce pourcentage est en augmentation depuis 2015, mais le rythme de cette évolution semble loin de pouvoir permettre une transition complète dans les prochaines années.

Même si plusieurs hébergeurs proposent IPv6 dans leurs offres, le taux de sites web accessibles en IPv6 est très faible pour tous les acteurs du Top 10 car il n'est pas activé par défaut. Parmi les acteurs du Top 10, seul 1&1 IONOS et Cloudflare ont plus des trois quarts des sites avec de l'IPv6, ce qui en fait des exemples à suivre.

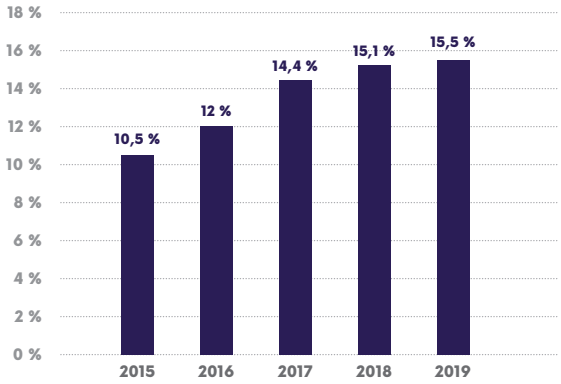
9. Baromètre Arcep de la transition vers IPv6 en France 2019 : https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_Barometre_2019_de_la_transition_vers_IPv6.pdf#page=13
10. Cisco 6lab au 28/10/2019 (https://6lab.cisco.com). Données sur le Top 730 d'Alexa en France www.alexa.com/topsites/countries
11. *Ibidem*
12. Données Afnic, septembre 2019.



Source : 6lab Cisco au 28/10/2019 (6lab.cisco.com)
Données sur le top 730 d'Alexa en France

ÉVOLUTION DU TAUX DES SITES WEB ACCESSIBLES EN IPv6

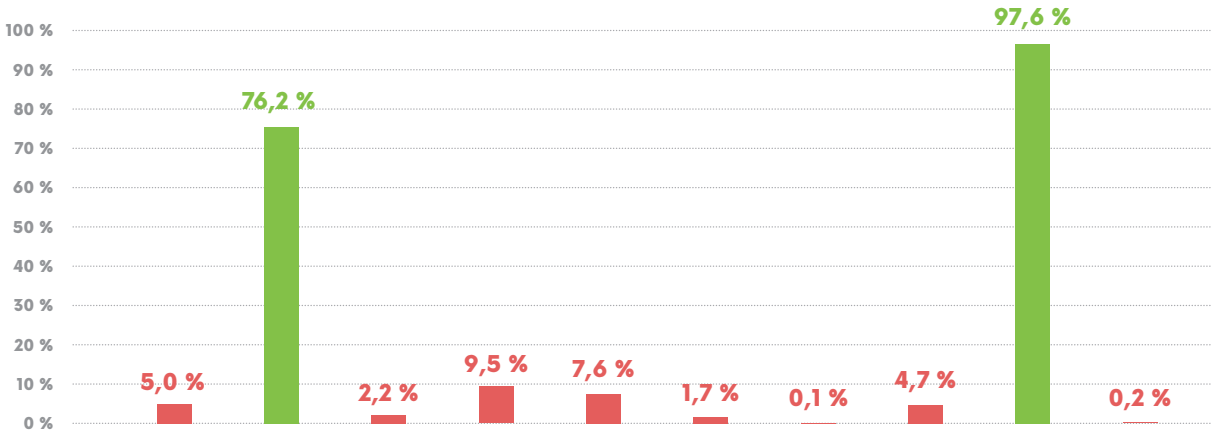
sur les noms de domaine .fr, .re, .pm, .yt, .tf et .wf



Source : données Afnic à septembre 2019

TAUX DE SITES WEB ACCESSIBLES EN IPv6

sur les noms de domaine .fr, .re, .pm, .yt, .tf et .wf



	OVHcloud	1&1 IONOS	Gandi	Scaleway	Amazon	Adista	Register.it	Google	Cloudflare	o2switch
Nombre de noms de domaine	1 248 335	373 111	224 634	80 063	80 063	53 934	46 804	44 893	40 715	35 487

Source : données Afnic à février 2020

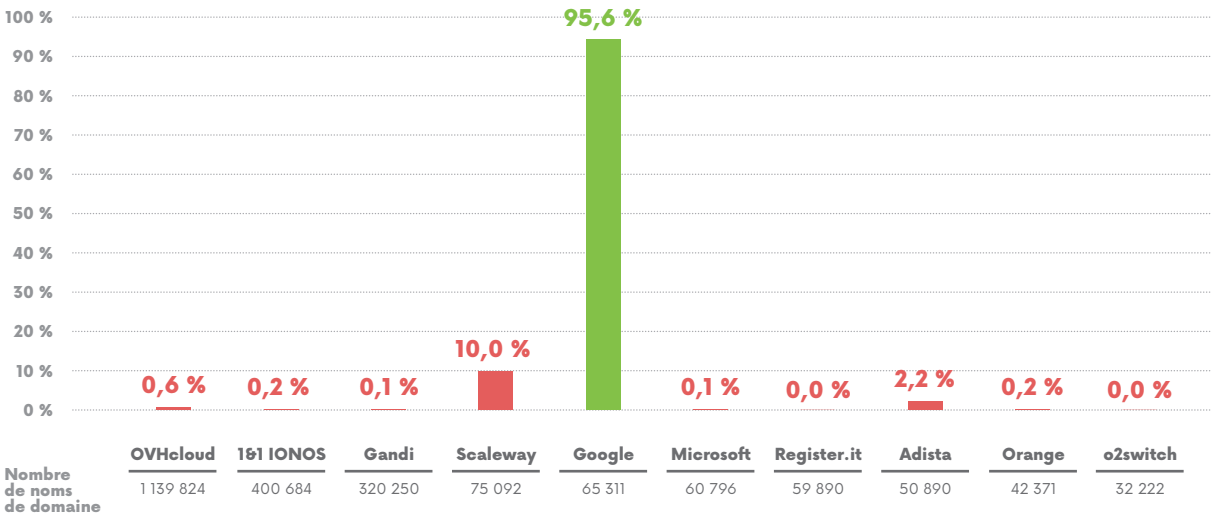
2.4. Hébergeurs mail

La transition des hébergeurs mail connaît également un très fort retard : seuls 5,8 % des serveurs mail sont à ce jour adressés en IPv6 sur l'intégralité des .fr, .re, .pm, .yt, .tf et .wf[13] (contre 5,2 % à mi-2018). Il est à noter qu'un certain nombre d'entre eux comportent un niveau de redondance en IPv6 inférieur à celui atteint en IPv4, et est donc susceptible de poser des problèmes de résilience.

Le taux d'hébergement mail est alarmant puisque le retard sur ce maillon de la chaîne d'internet, s'il n'est pas comblé dans les prochaines années, pourrait obliger à conserver plus longtemps IPv4, avec des coûts inhérents. Seul Google se démarque avec plus de 95 % de noms de domaines en IPv6 pour le mail.

TAUX D'HÉBERGEMENT MAIL ACCESSIBLES EN IPv6

sur les noms de domaine .fr, .re, .pm, .yt, .tf et .wf



Source : données Afnic à février 2020

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[14].

Afin d'améliorer la qualité de l'information qu'elle publie et de garantir une meilleure transparence sur les avancées de la transition, l'Arcep fait évoluer son enquête annuelle[15]. Les principales modifications ont consisté à :

- affiner les indicateurs demandés afin d'améliorer la précision des informations publiées et mieux détecter les goulots d'étranglement éventuels ;
- remplacer le questionnaire pour les hébergeurs par une analyse des données fournies par l'Afnic pour permettre un état des lieux plus complet de l'avancement de ces acteurs ;
- ajouter un questionnaire pour les principaux opérateurs sur le marché « entreprises » afin de connaître l'avancement de la transition sur ce marché.

L'exemplarité de l'État dans la transition vers IPv6 étant un des leviers importants pour accélérer la migration, la présentation d'indicateurs de l'avancement de cette transition pour les différents sites web et services en ligne de l'État dans la prochaine édition du baromètre est à l'étude.

La prochaine édition de ce baromètre sera publiée au second semestre 2020.

13. Données Afnic, septembre 2019.
14. https://www.arcep.fr/cartes-et-donnees/nos-publications-chiffrees/transition-ipv6/barometre-annuel-de-la-transition-vers-ipv6-en-france.html
15. Décision n° 2020-0305 de l'Arcep en date du 26 mars 2020 relative à la mise en place d'enquêtes dans le secteur des communications électroniques : https://www.arcep.fr/uploads/tx_gsavis/20-0305.pdf

LA PAROLE À...  JOAQUIM DOS SANTOS

*Directeur de la Recherche & Développement - **IKOULA***

MICROSERVEURS IPv6, SANS SUPPORT D'IPv4

Vous le savez déjà : l'une des ressources qu'internet utilise pour son développement - à savoir les adresses IPv4 - est maintenant épuisée. Vous me direz qu'on peut toutefois encore en acheter, ou même en demander aux instances officielles, si l'on est prêt à attendre que d'autres les libèrent... Mais concrètement, que fait un hébergeur comme IKOULA pour pallier cette pénurie ?

Cela fait maintenant plusieurs années que le monde de l'hébergement compose avec cette menace. Chez IKOULA par exemple, nous avons décidé il y a quelques années déjà de fournir un (petit) *slash* d'IPv6 (65536), pour accompagner chaque serveur dédié possédant une adresse IPv4 automatiquement configurée. Les questions étaient alors nombreuses : quelles adresses fournir à nos clients ? Combien ? Comment faciliter la transition dans les esprits de 127.0.0.1 à ::1 ? Comment aider à comprendre et à manipuler des adresses telles que 2a00:0c70:abba:fa00:de00:ca00:7833:547b ?

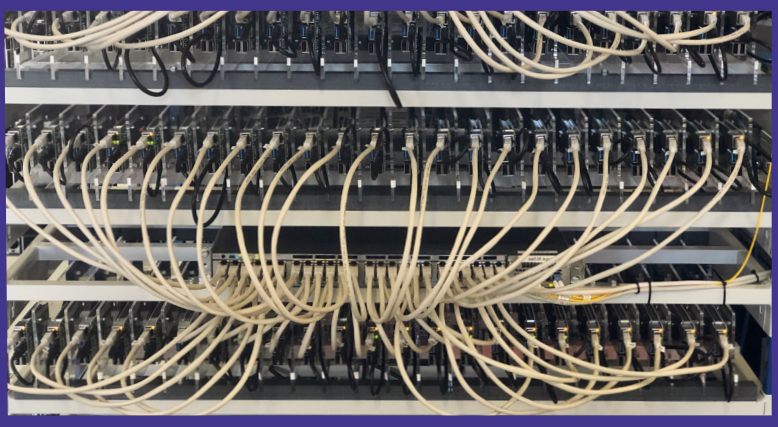
Au début, nous avions décidé de « calquer » les adresses IPv6 reçues sur l'adresse IPv4 configurée. Par exemple, une adresse IPv4 du type 213.246.53.53 se voyait attribuer 2a00:c70:1:213:246:53:53:0/112. Hélas, l'accueil ne fut pas à la hauteur de nos ambitions, même si cela aida plusieurs clients à mettre en place certains services et à tirer le meilleur de ce fameux /112. Quelques bugs et effets de bord sont également apparus au fil du temps, dont l'un des plus mémorables fut le traitement spécifique des caractères [et] des adresses IPv6 par un *parser* smtp/http, qu'il a fallu adapter...

L'annonce du RIPE en avril 2018 est tombée au moment où nous menions chez IKOULA une réflexion sur ce que certains appellent les microserveurs. Nous cherchions alors un moyen de répondre à plusieurs besoins : réduire l'empreinte carbone et l'espace occupé par nos serveurs, mais aussi faciliter leur manipulation au quotidien par les équipes techniques, et bien entendu - avant tout même – créer pour nos clients une offre à la pointe de la technologie et ultra compétitive ! Certains membres de nos équipes, passionnés par l'architecture ARM, avaient même débuté de leur côté des tests sur le tout nouveau Raspberry Pi 4 et ses 4 Go de mémoire vive. Tous les éléments étaient donc réunis pour faire naître une offre *full* IPv6, avec une unique adresse /128, sans *dual-stack* et sans support IPv4.

Certains éléments ont dû être repensés, tels que le support sur lequel fixer ces Raspberry, mais aussi l'ajout de disques HD/SSD à ces machines (car pas de stockage distribué ni de *boot* sur le réseau), le *bootstrap*, ou encore la configuration du système d'exploitation. Côté réseau « pur », au final, très peu de modifications à faire, IKOULA étant déjà préparé depuis longtemps à l'arrivée de l'IPv6.

Mais l'histoire ne s'arrête pas là, car internet dans son ensemble n'est PAS joignable directement depuis une adresse IPv6, et inversement ! Nous avons donc mis en place *via* des logiciels libres un mécanisme de transition – le NAT64 – qui permet de donner un accès internet en IPv4 à une machine (en l'occurrence nos Raspberry), qui n'a PAS d'adresse IPv4 et seulement une adresse IPv6. Dans le détail, il est composé de deux éléments : le NAT64, pour translater/nater la requête originale vers internet en IPv4 en utilisant une IPv4 source, et le DNS64, pour répondre une adresse IPv6 spécialement « calculée » pour tout nom de domaine n'ayant PAS d'enregistrement AAAA (enregistrements présents si le nom de domaine possède une adresse IPv6).

Cette offre a connu un succès certain à son lancement auprès de nos clients, qui peuvent depuis quelques mois aller encore plus loin, grâce à l'ajout en option d'une adresse IPv4.



L'ARCEP INTRODUIT UNE OBLIGATION DE COMPATIBILITÉ IPv6 DANS LES AUTORISATIONS D'UTILISATION DE FRÉQUENCES

L'Arcep a introduit une obligation de support d'IPv6 pour les opérateurs qui se verront attribuer des fréquences 5G dans la bande 3,4-3,8GHz en France métropolitaine* : *« Le titulaire est tenu de rendre son réseau mobile compatible avec le protocole IPv6 à compter du 31 décembre 2020 »*. L'objectif, tel que précisé dans les motifs, est d'assurer l'interopérabilité des services et ne pas freiner l'utilisation de services uniquement disponibles en IPv6, dans un contexte d'augmentation du nombre de terminaux et d'une pénurie d'adresses IPv4 au RIPE NCC.

L'Arcep a également proposé dans sa consultation publique relative à l'attribution de nouvelles fréquences (700 MHz et 3,5 GHz) pour les réseaux mobiles à La Réunion et Mayotte une obligation de support d'IPv6.

* Décision relative aux modalités et aux conditions d'attribution d'autorisations d'utilisation de fréquence dans la bande 3,4-3,8 GHz : https://www.arcep.fr/uploads/tx_gsavis/19-1386.pdf

3. LA MISE EN PLACE D'UNE TASK-FORCE DÉDIÉE À IPv6 RASSEMBLANT L'ÉCOSYSTÈME D'INTERNET

3.1. Lancement de la task-force IPv6

L'Arcep a mis en œuvre la première des pistes d'action identifiées lors des ateliers IP♥6 de 2018 en créant une task-force dédiée à IPv6. Cette task-force, co-pilotée avec Internet Society France, est ouverte à l'ensemble des acteurs de l'écosystème internet (opérateurs, hébergeurs, entreprises, secteur public, etc.). Elle a pour objectif de favoriser l'accélération de la transition vers le protocole IPv6 en permettant aux participants d'aborder des problèmes spécifiques et de partager les bonnes pratiques.

La réunion de lancement a eu lieu le 15 novembre 2019 et a réuni une cinquantaine d'acteurs qui ont participé à des groupes de travail multiparties prenantes sur deux thèmes :

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

3.2. Restitution du lancement de la task-force[16]

Les différents ateliers lors de la réunion de lancement de la task-force IPv6 ont permis d'identifier des propositions d'actions concrètes visant à en accélérer la transition sur les deux thématiques traitées[17].

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

Les enjeux	Les axes de travail
- Nécessité de garder IPv4, tant que la transition vers IPv6 n'est pas finalisée au niveau des différents maillons de la chaîne technique d'internet ; - Problèmes générés par les alternatives en cas de non-transition (achat d'IPv4 ou partage d'adresses IPv4) ; - Existence de diverses options pour faire la transition : IPv6 dans un réseau IPv4-*only*, *dual-stack* ou IPv4 dans un réseau IPv6-*only* ; - Problèmes de compatibilité IPv6 de certains équipements, applications, logiciels, services, etc. ; - Différences de gestion entre IPv4 et IPv6, notamment dans les fonctionnalités déployées et en termes de performances ; - Besoin de renforcer l'exemplarité de l'État dans la transition vers IPv6.	- Communiquer auprès des entreprises pour les inciter à effectuer leur transition vers IPv6 ; - Inclure l'activation d'IPv6 dans les appels d'offres, au-delà de la compatibilité IPv6 ; - Avoir des retours d'expérience d'entreprises qui ont réalisé la migration d'IPv4 vers IPv6 (au moins en *dual-stack*) pour estimer les coûts, les bénéfices, les conditions techniques, etc. ; - À partir des retours d'expériences, rédiger un guide de développement interne pour le déploiement d'IPv6 ; - Identifier les différentes catégories d'applications, équipements ou logiciels pour lesquels des dysfonctionnements dus au *Carrier Grade* NAT (CGN) sont observés ; - Recenser les différentes catégories d'applications, équipements et logiciels qui posent des problèmes de compatibilité avec IPv6.

2. Groupe de travail : Quels enjeux de sécurité pour IPv6 ?

Les enjeux	Les axes de travail
- Existence de plusieurs aspects de sécurisation du réseau IPv6 similaires en IPv4 mais IPv6 nécessite de repenser la sécurité ; - Faible disponibilité des compétences et méconnaissance des offres de sécurité IPv6 existantes ; - Présence de plusieurs référentiels et RFC non mis à jour ; - Prise en considération nécessaire des enjeux d'anonymisation et la protection de la vie privée lors de la mise en place d'IPv6 ; - Manque de connaissance des bonnes pratiques en termes de filtrage IPv6.	- Recenser les RFC[18] et les formations sécurité IPv6 à jour ; - Compiler les ressources existantes du RIPE ainsi que les initiatives d'Internet Society et les mettre à jour ; - Lister les problèmes de *privacy* occasionnés par IPv6 et discuter des différentes contremesures ; - Émettre des recommandations sur la façon dont le filtrage IPv6 doit s'effectuer.

3.3. Les suites des travaux de la task-force

Les priorités quant aux actions à mettre en place s'établiront en concertation avec la communauté des participants. Le premier axe de travail identifié à l'issue de la première réunion de la task-force est d'encourager les entreprises à effectuer leur transition vers IPv6. L'Autorité, en partenariat avec Internet Society France, réunira la task-force deux fois par an pour approfondir ensemble certains des axes de travail identifiés.

Afin de faciliter les échanges au sein de l'écosystème, l'Arcep et Internet Society France travaillent également à la mise en place d'une plateforme en ligne.

Les personnes qui souhaitent partager un retour d'expérience ou mettre en place IPv6 sont invitées à faire part à l'Arcep de leur intérêt pour rejoindre la task-force via le formulaire suivant : https://www.arcep.fr/la-regulation/grands-dossiers-internet-et-numerique/lipv6/suivi-epuisement-adresses-ipv4/appel-a-candidatures-pour-former-une-task-force-ipv6-en-france.html

16. Compte-rendu de la réunion de lancement de la task-force IPv6 : https://www.arcep.fr/actualites/les-communiques-de-presse/detail/n/transition-vers-ipv6-2.html
17. Pour rappel, cette restitution ne constitue en rien une prise de position de l'Arcep sur la pertinence, la faisabilité ou la priorité des axes de travail. Elle décrit uniquement les informations remontées par les différents participants à la task-force IPv6. Les priorités des actions à mettre en place se feront en concertation avec la communauté des participants.
18. Voir lexique.

LA PAROLE À...  JEAN-CHARLES BISECCO

*Architecte réseaux - **EDF***

LA TRANSITION IPv6 AU SEIN DU GROUPE EDF

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

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

Face à cette problématique d'adressage interne, nous avons choisi d'étudier la possibilité d'y répondre via IPv6 plutôt que par les « bidouilles » de recouvrement d'adressage IPv4 ; se basant sur le fait que l'implémentation du protocole semblait mature ou proche de l'être dans un grand nombre de solutions. Afin de gagner du temps, nous avons tout de même ratifié l'usage interne du bloc 100.64/10 et ses 4 millions d'IPv4.

L'IP concerne l'ensemble du système d'information de l'entreprise, il faut être méthodique dans le séquencement de l'implémentation du *dual-stack*, et celle du retrait d'IPv4 sur certaines portions du SI.

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

L'ordre d'implémentation consiste à remonter dans les couches du SI par le bas : réseau (*backbone*, campus et *data center*), puis système (socle d'OS) et enfin application tant côté client que serveur (navigateur, *middleware*, appli monolithique…).

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

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

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

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

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

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

Le projet vise enfin évidement à offrir les sites web publics en *dual-stack*. Les entreprises devraient travailler à migrer les flux entre bornes Wi-Fi et contrôleur en IPv6, ainsi qu'à fournir du *dual-stack* sur leur réseau invité pour se faire la main ; les microservices/containers et l'internet des objets vont sans doute faire exploser les besoins d'adressage dans les années à venir.

* Voir lexique.

TUTORIEL

LES ACCÈS IPv6-*ONLY* ET LE MÉCANISME DE NAT64/DNS64

Certains opérateurs proposent à leurs clients un accès à internet en IPv6, sans proposer d'accès en IPv4. Aujourd'hui, ce type d'accès se trouve principalement sur le mobile, où la majorité des offres proposant une connectivité IPv6 sont de type IPv6-*only*.

Comment l'accès aux ressources IPv4-*only* d'internet est-il possible sans IPv4 ?

Comme aujourd'hui une partie importante d'internet est accessible uniquement en IPv4, la solution utilisée, pour plus de 99 % du trafic IPv4-*only*, est le NAT64/DNS64. Le résolveur DNS ne va pas renvoyer une adresse IPv4 pour les sites internet en IPv4, mais une IPv6 spéciale : c'est une IPv6 qui pointe vers une plateforme NAT64, placée sur le réseau de l'opérateur. La plateforme NAT64 permet de faire communiquer la pile réseau IPv6 du client avec internet IPv4. La plateforme va faire une traduction d'adresse classique (NAT) à l'exception près que l'IPv4 privée est remplacée par une adresse IPv6. La plateforme NAT64 récupère l'IPv4 de destination codée dans l'IPv6 : afin d'acheminer le trafic au niveau de l'accès IPv6-*only*, le NAT64 génère une IPv6 construite à partir du préfixe réservé 64 :ff9b ::/96 suivit des 32 bits de l'adresse IPv4.

Afin de pouvoir utiliser la plateforme NAT64, il est nécessaire d'utiliser un résolveur DNS spécifique, de type DNS64. Si vous ne parvenez pas à configurer le DNS64 proposé par votre opérateur, il existe des services DNS64 publics hébergés en France proposés par deux acteurs : Cloudflare DNS[1] et Google Public DNS[2].

Voici quelques illustrations du comportement d'un résolveur DNS64 :

Type de site	Nom de domaine	Résolveur DNS classique[3]	Résolveur DNS64
Dual-stack	www.orange.fr	2a01:c9c0:a3:8::70 193.252.148.70	2a01:c9c0:a3:8::70 193.252.148.70
IPv4-*only*	www.sfr.fr	80.125.163.172	64:ff9b::507d:a3ac 80.125.163.172
IPv4-*only*	www.bouyguestelecom.fr	23.38.100.155	64:ff9b::1726:649b 23.38.100.155
Dual-stack	www.free.fr	2a01:e0c:1::1 212.27.48.10	2a01:e0c:1::1 212.27.48.10
IPv4-*only*	www.ovh.com	198.27.92.1	64:ff9b::c61b:5c01 198.27.92.1
IPv4-*only*	www.ionos.fr	217.160.86.38	64:ff9b::d9a0:5626 217.160.86.38
IPv4-*only*	www.gandi.net	151.101.1.103	64:ff9b::9765:167 151.101.1.103
IPv4-*only*	www.scaleway.com	212.47.255.70	64:ff9b::d42f:e146 212.47.255.70

Comment accéder à une ressource IPv4 littérale, qui, par définition, n'utilise pas de résolveur DNS ?

C'est un cas rare sur internet, mais certains services utilisent des IPv4 littérales (exemple : http://46.227.16.8/), alors que la bonne pratique est d'utiliser systématiquement des noms de domaine. Dans ce cas, le DNS64 n'est d'aucune utilité car aucune résolution DNS n'est effectuée. Pour ne pas avoir de régression, des mécanismes tels que 464XLAT (RFC 68779[4]) et/ou CLAT ont été intégrés aux systèmes d'exploitation (Android depuis Android 4.3, iOS depuis iOS 12.0, Windows10 depuis 2017, Linux en utilisant clatd[5]) pour que les applications disposent en apparence d'une adresse IPv4 fonctionnelle, alors que l'hôte ne dispose que d'adresses IPv6.

1. DNS64 Cloudflare DNS : 2606:4700:4700::64 et 2606:4700:4700::6400
2. DNS64 Google Public DNS : 2001:4860:4860::6464 et 2001:4860:4860::64
3. Seul la première IPv4 et première IPv6 renvoyée ont été conservées. Ces résolutions DNS sont celles observées le 14 avril 2020 et peuvent avoir été modifiées depuis.
4. RFC 6877 : 464XLAT *Combination of Stateful and Stateless Translation* https://tools.ietf.org/html/rfc6877
5. Clatd, une implémentation de 464XLAT CLAT pour Linux : https://github.com/toreanderson/clatd

PARTIE 2

Veiller à l'ouverture d'internet

CHAPITRE 4

Garantir la neutralité d'internet

CHAPITRE 5

Terminaux et plateformes, maillons structurants de l'accès à internet

CHAPITRE 4

Garantir la neutralité d'internet

À RETENIR

450 millions de citoyens européens
sont protégés par le règlement européen internet ouvert adopté en 2015 et les lignes directrices relatives à la mise en œuvre de ce règlement.

18 mois de travail
ont été nécessaires aux autorités de régulation européennes afin de réviser les lignes directrices du règlement internet ouvert. Elles ont été publiées le 16 juin 2020.

En France, l'Arcep s'est dotée de plusieurs outils pour assurer le respect du principe de neutralité du net : l'application Wehe a été utilisée plus de **115 000 fois** et **146 signalements** ont été remontés via la plateforme J'alerte l'Arcep.

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. LA NEUTRALITÉ D'INTERNET AU-DELÀ DE LA FRANCE

Le règlement européen garantit l'accès à un internet ouvert à plus de 450 millions de citoyens européens, répartis sur 27 États membres. Le retrait du Royaume-Uni de l'Union européenne pourrait modifier la situation pour 66 millions de Britanniques. Le gouvernement britannique a en effet déposé un *Open Internet Access* (*Amendment etc.*) *EU Exit Regulations* 2018 qui assure la continuité du principe de neutralité du net, mais uniquement jusqu'à l'aboutissement du processus de sortie du Royaume-Uni, soit le 31 décembre 2020.

La neutralité du net progresse dans certains pays. En Inde, le régulateur, la *Telecom Regulatory Authority of India* (TRAI), a adopté en novembre 2017 une série de recommandations visant à la renforcer. Depuis juillet 2019, ces recommandations conditionnent ainsi l'obtention ou le maintien d'une licence pour les opérateurs télécoms indiens. De même, la Corée du Sud, au travers de son régulateur, le *Korea Communications Commission* (KCC), impose aux opérateurs le respect des lignes directrices relatives à la neutralité du net depuis 2011. Enfin, d'autres États sont aussi sur le point d'intégrer ou de renforcer le principe de neutralité du net dans leurs propres corpus juridiques : on peut noter, par exemple, l'adoption prochaine en Suisse d'un texte législatif ou encore la rédaction au Mexique de lignes directrices sur la neutralité du net.

1. Règlement (UE) 2015/2120 du Parlement européen et du Conseil du 25 novembre 2015 établissant des mesures relatives à l'accès à un internet ouvert : https://www.arcep.fr/fileadmin/reprise/textes/communautaires/reglement-UE-2015_310-Net-Neutralite-251115.pdf

LA PAROLE À...

DAVE CHOFFNES

*Professeur associé - **Northeastern University***

LA NEUTRALITÉ DU NET AUX ÉTATS-UNIS AUX NIVEAUX FÉDÉRAL ET ÉTATIQUE

En 2017, la *Federal Communication Commission* (FCC), le régulateur américain, a renoncé à tout contrôle réglementaire des fournisseurs d'accès à internet (FAI). Par son ordonnance, la FCC a mis fin à la protection de la neutralité du net aux États-Unis, permettant aux FAI de bloquer et de gérer le trafic internet à leur guise, et obligeant les fournisseurs de contenu à payer pour leur priorisation.

Bien que l'ordonnance indique que la FCC reste en retrait, elle instaure deux exigences importantes : les FAI doivent être transparents quant à leurs violations de la neutralité du net et aucun État fédéré ne peut instaurer la neutralité du net sur son territoire. De fait, aucun rapport d'audit ou d'application de l'obligation de transparence n'est effectué. Dans une récente affaire devant la Cour d'appel fédérale, le tribunal a rejeté l'interdiction d'exemption, insinuant que les États fédérés peuvent promulguer une loi sur la neutralité du net.

Malgré le renversement de l'interdiction d'exemption, il n'y a actuellement aucune mise en application de la neutralité du net aux États-Unis alors que les violations du principe de neutralité du net augmentent. Grâce à notre projet Wehe, nous avons constaté que presque tous les fournisseurs de services cellulaires limitent les applications de *streaming* vidéo à de faibles résolutions. La manière dont ils différencient le *streaming* vidéo conduit souvent à un traitement inégal entre les différents fournisseurs de contenu vidéo. De plus, ce traitement différencié change au fil du temps, entraîne une inefficience du réseau et est activé en permanence (sans lien avec une surcharge du réseau).

Toutefois, un espoir subsiste pour les lois sur la neutralité du net dans les États fédérés, notamment après le récent jugement annulant la préemption de la FCC sur ce sujet. Cependant, les législatures ont été lentes – y compris dans mon État d'origine, le Massachusetts –, malgré une proposition de loi et le soutien écrasant du public. Les élections de novembre 2020 sont peut-être le meilleur moyen de faire respecter la neutralité du net aux États-Unis, avec la possibilité pour les nouveaux élus de promulguer des lois permanentes sur la neutralité du net.

JINNY KWAK

*Directrice en chef du CCDI - **KCC***

LES ENJEUX DE LA NEUTRALITÉ DU NET À L'ÈRE DE LA 5G EN CORÉE DU SUD

Le principe de neutralité du net en Corée du Sud repose sur des lignes directrices créées en 2011 et sur des normes de gestion du trafic raisonnables de 2013. Ce principe interdit le blocage et la discrimination du trafic et impose une obligation de transparence sur la gestion de trafic. L'amendement de 2016 à l'*Enforcement Decree of the Telecommunications Business Act* et la déclaration de 2017 sur l'interdiction de pratiques inégales ou discriminatoires envers des FCA ont enrichi cette réglementation *ex post*.

Préalablement à l'arrivée de la 5G, la Commission des communications coréenne (KCC) a formé en 2018 un Comité de 48 membres sur la Coexistence et le Développement d'Internet (CCDI) et a lancé un débat sur la nécessité de réviser le principe de neutralité du net, en raison de l'arrivée du *network slicing* avec la 5G.

Trois axes ont été discutés : un premier relatif à l'application flexible du principe de neutralité d'internet à la technologie 5G. Sous cet angle, les services de santé et de sécurité, qui nécessitent une latence ultra faible (télémédecine et voitures autonomes) seraient qualifiés de services gérés (équivalents européens des services spécialisés).

Le deuxième axe suppose de renforcer la réglementation existante. Cette vision est partagée par plusieurs FCA qui craignent qu'un assouplissement du principe de neutralité du net favorise les grands FCA et étende la domination des opérateurs au marché des contenus. Ces FCA soutiennent le renforcement des règles de gestion du trafic.

Le dernier axe envisage la disparition du principe de neutralité du net, à l'exception de l'obligation de transparence. Cette approche, selon les opérateurs qui la soutiennent, permettrait l'émergence de services innovants et le partage raisonnable avec les principaux FCA de la charge financière liée à leur important trafic.

Suite à la commercialisation de la 5G en avril 2019, les opérateurs ont fourni des contenus B2C tels que la réalité augmentée et la réalité virtuelle. La KCC continuera de surveiller le développement des services de la 5G et coopérera avec le ministère des Sciences et des technologies de l'information et de communication pour décider si le principe de neutralité du net doit évoluer.

LA PAROLE À...

ROBERT WELLS

*Conseiller juridique - **Ofcom**[1]*

LA NEUTRALITÉ DU NET AU ROYAUME-UNI DANS LE CONTEXTE DU BREXIT

Alors que le Royaume-Uni a quitté l'Union européenne fin janvier, sa réglementation sur la neutralité du net reste identique à celle en vigueur dans l'UE, car la législation européenne continue à s'appliquer au Royaume-Uni le temps de la transition, jusqu'au 31 décembre 2020. Passée cette période, la réglementation européenne relative à la neutralité du net sera convertie en loi britannique, avec de légères modifications, telles que la suppression de toute référence au droit ou aux institutions européennes ou leur replacement par des équivalents nationaux. Les fondements de la loi resteront inchangés, en particulier les droits des utilisateurs finaux, les restrictions sur les mesures de gestion de trafic, et les conditions selon lesquelles les services spécialisés sont fournis.

À partir de 2021, et selon les négociations sur les futures relations économiques entre le Royaume-Uni et l'Union européenne, le parlement britannique pourrait décider de modifier ou de remplacer la loi, bien que nous n'ayons pas connaissance d'un tel projet à ce jour. Néanmoins, comme toute autorité réglementaire nationale, l'Ofcom continue à examiner l'impact des évolutions technologiques sur les règles existantes, ainsi que l'éventuelle nécessité de les réviser. Nous prévoyons de continuer à échanger avec nos homologues européens, afin de nourrir notre réflexion collective sur ce sujet.

En attendant, l'Ofcom continue à veiller au respect des règles en vigueur. Au cours des dernières années, nous avons examiné plusieurs offres de *zero-rating* et nous avons pris des sanctions envers certaines pratiques de gestion de trafic. Dans l'ensemble, les offres de *zero-rating* observées sur le marché britannique n'ont pas suscité de préoccupations importantes. Avec notre programme de détection, et maintenant que tous les opérateurs respectent les règles relatives à la gestion de trafic, nous espérons consacrer moins de temps à l'application de la loi et plus de temps à réfléchir à des questions politiques, telles que l'articulation entre la neutralité du net et les nouvelles technologies émergentes, notamment la 5G, le *network slicing* et le *mobile edge computing*.

1. *Office of communications:* régulateur des télécommunications au Royaume-Uni.

SIDHARTH DEB

Conseiller politique et parlementaire

APAR GUPTA

*Directeur exécutif - **Internet Freedom Foundation***

LA DÉMOCRATISATION DE LA NEUTRALITÉ DU NET EN INDE

Suite à la mobilisation d'un mouvement de plus d'un million de personnes, le ministère des Télécommunications en Inde a réformé en juillet 2018 les licences des FAI. Il enjoint aux FAI de respecter techniquement le principe de neutralité du net. Parallèlement à l'adoption d'une loi en février 2016[1] interdisant les offres de *zero-rating*, cette réforme contribue au bon fonctionnement d'internet en Inde.

Toutefois, sans application effective, la victoire est partielle. Postérieurement à cette réforme, on a observé que les FAI discriminaient le trafic. Pourquoi ? Une asymétrie d'information permet aux FAI de ne pas rendre de comptes. Notre mécanisme de *crowsourcing*, hébergé sur SaveTheInternet.in[2], a remonté 307 signalements aux autorités compétentes entre janvier et mai 2019[3]. En janvier 2020, la *Telecom Regulatory Authority of India* (TRAI) a lancé une consultation publique sur des questions telles que la gestion de trafic raisonnable et les mécanismes de contrôle et de détection des infractions.

Or plusieurs représentants de l'industrie proposent d'instaurer une gestion du trafic par catégorie d'application et d'adapter la neutralité du net aux futurs réseaux 5G. Plus préoccupant encore, ils incitent la TRAI à ignorer les outils de détection destinés aux utilisateurs en donnant des raisons comme l'hétérogénéité des environnements utilisateurs.

Selon nous, la neutralité du net doit être centrée sur l'individu. Ainsi, la gestion du trafic devrait être « *aussi agnostique que possible par rapport aux applications* »[4]. De plus, les autorités devraient voir dans la neutralité du net un dispositif structurant le déploiement de technologies comme la 5G.

Les régulateurs doivent réduire cette asymétrie d'information. Disposer d'un outil de diagnostic serait un prérequis. À cet égard, la TRAI pourrait bénéficier des échanges avec ses homologues, tels que le BEREC ou l'Arcep. Une application mobile comme Wehe pourrait être profitable car internet se développe surtout sur le mobile en Inde. Dans ce contexte, les autorités indiennes doivent assumer leur rôle et créer des outils pour responsabiliser les FAI.

1. *Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016*
2. https://savetheinternet.in
3. https://internetfreedom.in/net-neutrality-in-india-needs-to-find-its-bearings
4. Voir publications du Pr. VAN SCHEWICK

En revanche, depuis décembre 2017, le régulateur américain des télécoms, la *Federal Communications Commission* (FCC) a renversé les règles existantes en adoptant un texte intitulé « *Restoring internet freedom* ». Entré en vigueur en juin 2018, ce décret revient sur des dispositions centrales de l'*Open Internet Order* de 2015, qui interdisaient notamment aux fournisseurs de services internet (FAI) de bloquer, de brider ou de faire de la priorisation payante. En réaction, plusieurs États fédérés, en particulier la Californie et l'État de Washington, ont décidé de réinstaurer localement la neutralité du net, en contradiction avec la décision de la FCC, et s'exposant ainsi à des poursuites judiciaires. En octobre 2019 et en février 2020, la Cour d'appel fédérale a confirmé la décision de la FCC, laissant toutefois libre les États fédérés d'adopter leurs propres lois sur ce sujet.

Par ailleurs, au-delà du principe de neutralité, la liberté d'accès à internet, reste menacée dans de nombreux pays. En Russie, même si le principe de neutralité du net est protégé par la loi depuis 2016, l'accès à de vastes étendues d'internet est occasionnellement bloqué. Cette pratique est aussi présente en Chine où l'accès à internet est filtré par le « *Grand Firewall Chinois* » ou encore reconditionné par le « *Grand Canon of China* », supprimant *de facto* la portée d'un principe de neutralité d'accès aux contenus ou aux applications. Le principe de neutralité du net pourrait également souffrir de la déconnexion de réseaux internet locaux de l'internet mondial privant les utilisateurs finals d'un accès complet à internet, comme en Russie en décembre dernier. Ce principe pourrait aussi souffrir de coupures partielles ou totales d'internet (*shutdowns*) de plus en plus fréquentes et mises en œuvre par des autorités nationales ou locales. À titre d'exemple, le nombre de *shutdowns* survenus en Inde en 2019 est en nette augmentation, bien que la Cour suprême indienne ait rendu un arrêt relatif à ces pratiques et que le principe de neutralité du net soit protégé dans ce pays.

5G ET NET NEUTRALITÉ EN EUROPE : ASSURER L'INNOVATION TOUT EN PRÉSERVANT LA NEUTRALITÉ DES RÉSEAUX

La technologie 5G promet l'arrivée de nouveaux services grâce à des capacités décuplées, notamment en matière de débit, de latence, de virtualisation, de différenciation de qualité de services, ou encore de fiabilité. Certains acteurs du secteur s'interrogent encore sur la compatibilité de la technologie 5G avec le principe de neutralité, mais qu'en est-il vraiment ?

Dans son avis publié en décembre 2018, le BEREC a rappelé que le règlement internet ouvert et ses lignes directrices sont technologiquement neutres et s'appliquent donc sans obstacle majeur à la technologie 5G, de la même façon qu'ils se sont appliqués aux technologies antérieures 2G, 3G et 4G. Ainsi, le cadre législatif en vigueur laisse une marge de manœuvre importante au déploiement des innovations promises par la 5G, telles que le *network slicing*, la différenciation de classes de qualité de service ou encore le *mobile edge computing*.

Pour démystifier les idées reçues, l'Arcep a d'ailleurs synthétisé les débats sur ce sujet dans un document *ad hoc*, publié sur son site*. L'Arcep continuera de suivre avec attention le développement des cas d'usages de la 5G et restera à l'écoute des acteurs sur leurs interrogations quant à la compatibilité de ces usages avec le principe de neutralité du net.

* https://www.arcep.fr/uploads/tx_gspublication/ARCEP_BD_5G_planche_FR-2019.pdf

LA PAROLE À... FELICIA ANTHONIO

*Coordinatrice de la campagne #KeepItOn - **Access Now***

LES COUPURES D'INTERNET : LA NOUVELLE NORME MONDIALE

Internet est indispensable à notre quotidien : il promeut les droits et stimule les économies. Or des gouvernements à travers le monde coupent l'accès à internet. L'ONG internationale Access Now, avec la coalition #KeepItOn, lutte contre ces coupures d'internet depuis 2011.

En 2016, pas moins de 75 coupures[1] ont été recensées. En 2019, ce nombre a triplé, avec près de 213 cas[2]. Entre 2016 et 2019 le projet « *Shutdown Tracker optimization* »[3] a recensé plus de 590 coupures de réseau. Dans la majorité des cas, les autorités perturbent les communications pendant d'importants événements nationaux, tels que les élections, les manifestations ou les crises. Ces coupures durent de plus en plus longtemps, affectent plus d'individus et visent des groupes vulnérables.

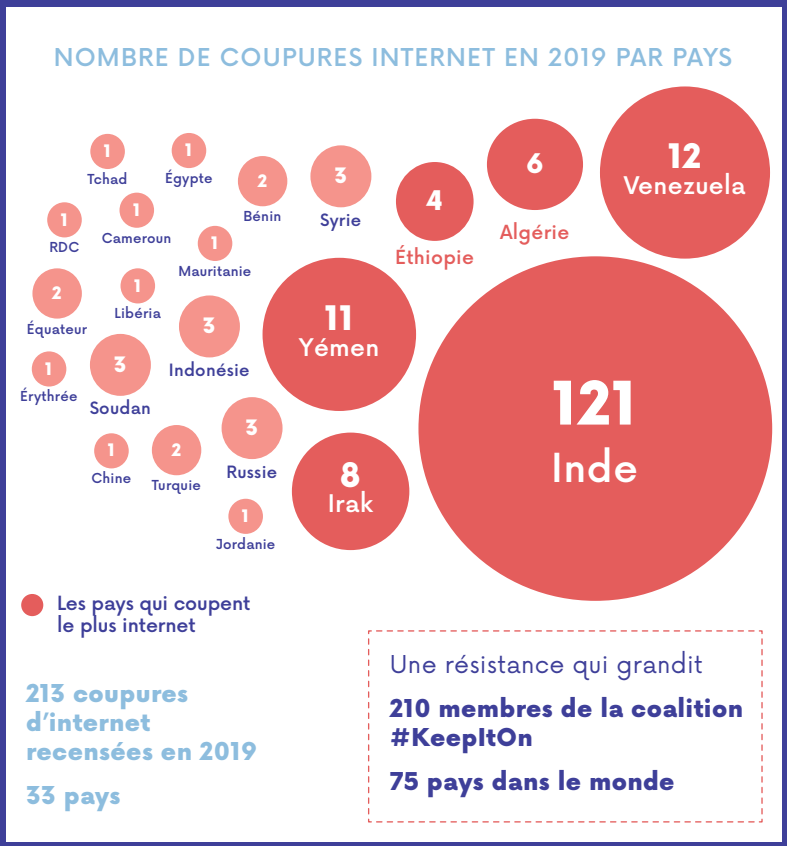
Cette pratique est une atteinte aux droits fondamentaux ainsi qu'une menace économique. Les gouvernements justifient cette répression par la nécessité de combattre les « *fake news* », de garantir la sécurité nationale ou d'empêcher la fraude aux examens. En réalité, pendant ces coupures, les internautes sont incapables de s'informer ou de s'exprimer librement, tandis que les PME perdent des revenus et, parfois, se voient contraintes de cesser leur activité.

Comment peuvent agir les FAI ?

Mettant en œuvre les coupures ordonnées par les gouvernements, les FAI[4] sont au cœur de cette crise. Ils peuvent les freiner en exigeant que ces ordres soient écrits et émanent d'une autorité légale. Ils devraient également avertir les clients concernés de l'étendue, de l'ampleur, de la durée et des motifs de la perturbation.

Les opérateurs devraient travailler avec les entreprises, les autorités et la société civile afin de dissuader les gouvernements d'ordonner des perturbations et devraient y mettre fin dès que possible. Défenseurs, journalistes et militants de la société civile peuvent s'exprimer publiquement lorsque les FAI ne le peuvent pas. Les FAI devraient s'associer aux défenseurs qui poursuivent les gouvernements en justice, pour contester ces mesures arbitraires et excessives, qui contreviennent aux intérêts des entreprises et aux droits de l'homme.

1. https://accessnow.org/kio-2018-report
2. www.accessnow.org/keepiton-2019-report
3. https://www.accessnow.org/keepiton
4. https://accessnow.org/telco-action-plan



2. LA PARTICIPATION DE L'ARCEP AUX CHANTIERS EUROPÉENS

Dans la continuité du bilan dressé en 2018, l'Arcep et ses homologues européens au sein du BEREC ont travaillé en 2019 sur les clarifications à apporter aux lignes directrices relatives à la mise en œuvre du règlement internet ouvert. Sur la base du bilan dressé fin 2018 par le BEREC[2], l'enjeu de ces révisions est de réduire le risque d'une interprétation divergente de ces textes par l'ensemble des acteurs qui participent au fonctionnement d'internet en France et en Europe. Après une coopération active entre les autorités de régulation nationales (ARN), une première version révisée des lignes directrices a été soumise à consultation publique en octobre 2019. Suite aux différentes contributions (opérateurs télécoms, équipementiers, associations, universités et membres de la société civile), les lignes directrices révisées ont été finalisées et publiées le 16 juin 2020. Elles conservent la structure des lignes directrices précédentes, elle-même calquée sur la structure du règlement internet ouvert. Les clarifications apportées, dont les principales sont résumées ci-après, reflètent les conclusions communes auxquelles sont parvenus les régulateurs européens.

Les offres de *zero-rating* sont des offres où le volume de données consommées par une ou plusieurs applications particulières n'est pas décompté du forfait *data* du client final. Ces pratiques ne sont pas interdites *per se* par le règlement européen, mais elles peuvent engendrer un traitement discriminatoire au profit d'applications ou de catégories d'applications. La consommation à prix nul de certaines applications crée une incitation économique pouvant à terme réduire la liberté de choix de l'utilisateur final. Ainsi, les lignes directrices révisées précisent les critères d'évaluation de ces offres, en particulier l'examen du caractère ouvert ou fermé d'un programme de *zero-rating* à l'intégration de nouvelles applications, et répertorient ces critères dans une méthodologie d'analyse à disposition des ARN.

Les lignes directrices révisées précisent aussi les conditions dans lesquelles les FAI peuvent créer différentes classes de qualité de service d'accès à internet afin de mettre en place des offres spécifiques, notamment à destination des entreprises. Des garde-fous encadrent la commercialisation de ces offres afin que les ARN soient en mesure de s'assurer que ni la qualité générale des services d'accès à internet, ni les droits des utilisateurs finals ne soient restreints. Cette évolution permet de favoriser l'innovation tout en limitant le risque de créer un internet à deux vitesses.

Les travaux ont également porté sur l'adéquation des critères définissant un « service spécialisé »[3] avec l'essor de l'internet des objets et des services *machine to machine*. Ces derniers présentent en effet des besoins spécifiques, notamment en matière de fiabilité, de sécurité et de contraintes énergétiques, qui pourraient ne pas être assurés par des offres classiques de services d'accès à internet. Afin de répondre à ces attentes, les lignes directrices révisées clarifient la notion de « niveau de qualité spécifique », propre à la définition des services spécialisés, en y intégrant de nouveaux critères d'examen en sus de la latence, la gigue et la perte de paquets. L'introduction de ces services reste conditionnée à la capacité des FAI à démontrer la nécessité d'un tel niveau de qualité spécifique.

CADRE DE RÉGULATION EN MATIÈRE DE NEUTRALITÉ DE L'INTERNET

NOVEMBRE 2015
Règlement (UE 2015/2120) du Parlement européen et du Conseil établissant des mesures relatives à l'accès à un internet ouvert

JUIN 2016
Consultation publique sur les lignes directrices du BEREC pour la mise en œuvre par les régulateurs nationaux du règlement internet ouvert

AOÛT 2016
Rapport de la consultation publique sur les lignes directrices du BEREC BoR (16)128

AOÛT 2016
Adoption des lignes directrices du BEREC pour la mise en œuvre par les régulateurs nationaux du règlement internet ouvert BoR (16)127

MARS 2018
Consultation publique du BEREC sur l'évaluation de l'application du règlement internet ouvert et des lignes directrices du BEREC BoR (18) 33

DÉCEMBRE 2018
Avis du BEREC à destination de la Commission européenne sur l'évaluation de l'application du règlement internet ouvert et des lignes directrices du BEREC BoR (18) 244

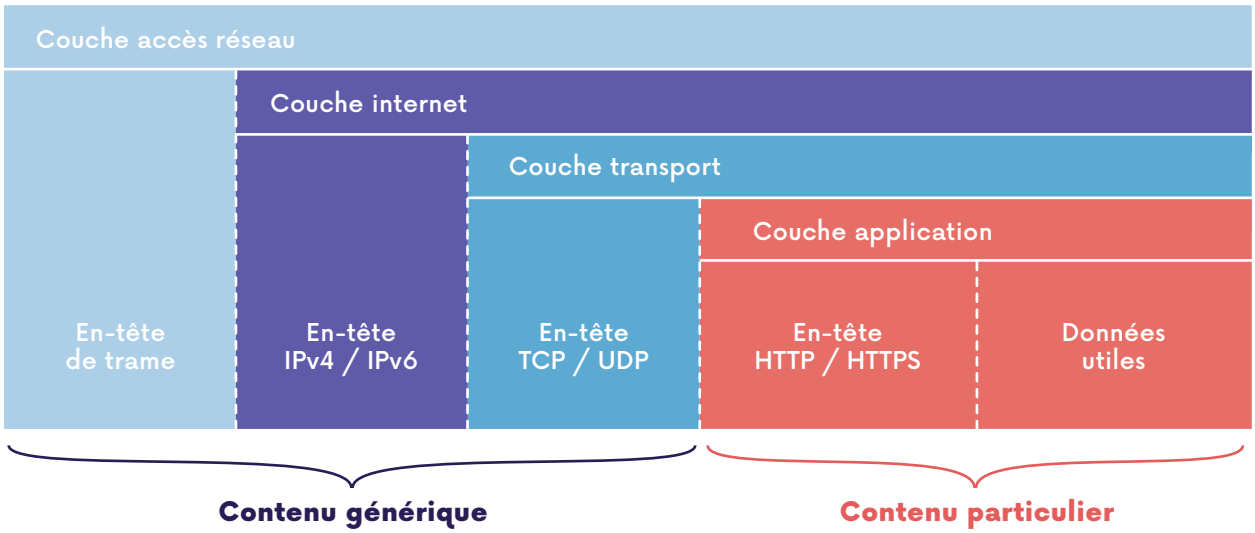
OCTOBRE 2019
Consultation publique sur les lignes directrices révisées du BEREC pour la mise en œuvre par les régulateurs nationaux du règlement internet ouvert BoR (19) 180

JUIN 2020
Rapport de la consultation publique sur les lignes directrices révisées du BEREC BoR (20) 111

JUIN 2020
Adoption des lignes directrices révisées du BEREC pour la mise en œuvre par les régulateurs nationaux du règlement internet ouvert BoR (20) 112

2. 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 du net : 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.

SCHÉMA SYNTHÉTIQUE DU CONTENU GÉNÉRIQUE ET PARTICULIER DES DONNÉES DE COMMUNICATIONS ÉLECTRONIQUES



Source : Arcep

La révision des lignes directrices a aussi permis à l'Arcep et ses homologues d'échanger sur différentes pratiques pouvant affecter la neutralité des services d'accès à internet. Ainsi, les ARN se sont intéressées à l'arrivée de nouveaux services additionnels (par exemple des services de contrôle parental ou de filtrage de contenu) offerts par un FAI en parallèle d'un service d'accès à internet. De manière plus générale, les ARN se sont aussi interrogées sur les modalités de mise en œuvre des mesures de gestion de trafic dans le réseau d'un FAI. Les lignes directrices révisées clarifient l'étendue du contrôle des ARN sur l'ensemble de ces questions dès lors que ces pratiques présenteraient un risque pour la neutralité des services d'accès à internet.

A également été abordée la question de l'accès par les FAI aux noms de domaine (ou aux URL) à des fins de gestion de trafic ou à des fins de facturation[4]. Or le règlement internet ouvert permet aux FAI d'accéder qu'aux informations contenues dans l'en-tête du paquet IP et dans l'en-tête du protocole de la couche transport (par exemple l'en-tête TCP ou l'en-tête UDP) dont les noms de domaine et URL sont exclus. Par ailleurs, dans une lettre rendue publique[5], le Comité européen de la protection des données (EDPB/CEPD) qui a été saisi pour avis, précise que le nom de domaine et l'URL peuvent être qualifiés de données à caractères personnels et à ce titre sont protégés par les dispositions de la directive « vie privée et communications électroniques »[6] ainsi que du règlement général sur la protection des données[7]. Ainsi, les FAI qui utiliseraient le nom de domaine ou les URL à des fins de catégorisation de trafic ou de facturation s'exposeraient non seulement à une violation potentielle du règlement internet ouvert, mais aussi à une possible violation de la protection des données à caractère personnel de leurs clients.

Enfin, les lignes directrices sur les modalités de définition du point de terminaison du réseau[8] ne sont pas sans effet sur l'étendue de la protection offerte aux utilisateurs finals par le règlement internet ouvert. Ces nouvelles lignes directrices ont vocation à orienter les ARN dans le choix de la localisation du point de terminaison, en prenant en compte le degré de complémentarité technique qui existe entre la box des opérateurs et leurs offres d'accès à internet. Ainsi, le point de terminaison du réseau devra permettre le bon équilibre entre, d'une part, le bon fonctionnement des réseaux et, d'autre part, la liberté des utilisateurs dans le choix de leur terminal. Les discussions relatives à cette question ont été l'occasion pour l'Autorité de rappeler la nécessité d'étendre l'application du principe de neutralité aux terminaux afin de renforcer la liberté de l'utilisateur final dans le choix et l'utilisation de son terminal.

4. Sous-entendue ici la question pour les FAI d'accéder aux noms de domaine et aux URL dans le cadre des pratiques commerciales permises par l'art. 3.2 du règlement internet ouvert.
5. Lettre de l'EDPB en date du 3 décembre 2019 relative à la demande d'orientation du BEREC sur la révision de ses lignes directrices sur la neutralité d'internet (Ref. OUT2019-0055) : https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2019-0055_berecnetneutrality2.pdf
6. Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques
7. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE
8. BEREC *Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies,* BoR (20)46 : https://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/9033-berec-guidelines-on-common-approaches-to_0.pdf

LA PAROLE À...  CLÉMENCE SCOTTEZ

*Chef du service des affaires économiques - **CNIL***

PROTECTION DES DONNÉES PERSONNELLES ET ANALYSE DES COMMUNICATIONS ÉLECTRONIQUES PAR LES FOURNISSEURS D'ACCÈS À INTERNET

La neutralité du net et la protection des données personnelles sont au service d'un enjeu sociétal commun. Celui d'offrir aux citoyens un cadre permettant de s'exprimer librement en ligne, sans craindre une forme de discrimination ou de surveillance de leurs communications électroniques par les opérateurs fournissant l'accès à ces services.

C'est dans cet esprit que la Directive 2002/58/CE dite « vie privée et communications électroniques » ou *ePrivacy* complète et précise le cadre général posé par le Règlement Général sur la Protection des Données (RGPD). Elle rappelle que les données de communications électroniques présentent une sensibilité particulière en ce qu'elles *« permettent de tirer des conclusions précises sur la vie privée des personnes intervenant dans la communication électronique »*[1]. Elle tire de ce constat un principe général d'interdiction d'intercepter, stocker ou surveiller ces données, assorti d'exceptions très encadrées, et circonscrit le rôle des opérateurs à l'acheminement des communications sur les réseaux.

Plus précisément, ladite directive permet aux opérateurs de traiter ces données uniquement afin de garantir la sécurité de leurs services (art. 4), d'acheminer la communication (art. 5.1), ou encore, s'agissant des données de trafic, de facturer leurs clients (art. 6). Tout traitement réalisé par les opérateurs ne répondant pas à ces finalités précises nécessite le recueil du consentement du ou des utilisateurs concernés, conformément aux articles 5 et 6 de la directive précitée. Rappelons que ce consentement doit répondre aux exigences du RGPD en vertu de l'article 2(f) de la directive ; l'accord de l'utilisateur doit donc être spécifique et éclairé quant à la finalité visée et non contraint (par exemple, il ne peut conditionner la conclusion d'un contrat de fourniture d'accès à internet). Le traitement doit de manière plus générale répondre aux principes de transparence, de loyauté (nécessité d'informer sur les caractéristiques du traitement, son objectif, etc.), être limité à la finalité préalablement annoncée à l'utilisateur et ne porter que sur des données nécessaires à l'atteinte de cette finalité.

C'est sur la base de ces principes, notamment de « minimisation », que le Comité Européen de la Protection des Données (CEPD) a répondu aux interrogations du BEREC relatives aux problématiques de protection des données posées par le règlement 2015/2120, s'agissant notamment des dispositifs de « *zero-rating* ». Le CEPD relève ainsi que la notion de « *contenu particulier* », dont la surveillance par les opérateurs est interdite par l'article 3(3) du règlement 2015/2120, peut être assimilée à celle de « *communication* », définie par la directive ePrivacy (art. 2) comme *« toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public »*. À cet égard, le CEPD rappelle que les adresses URL et les noms de domaine ne sont pas des « *données relatives au trafic* » dans la mesure où elles ne sont pas nécessaires à l'acheminement d'une communication sur un réseau de communications électroniques. Il s'agit en revanche de données de « *communication* », c'est-à-dire des informations matérialisant le contenu échangé ou consulté par les utilisateurs. Le traitement de ces informations à des fins de facturation dans le cadre des dispositifs de « *zero-rating* » requiert donc de collecter le consentement de tous les utilisateurs dont le contenu des communications serait ainsi inspecté (par exemple, l'émetteur et le destinataire d'un courriel).

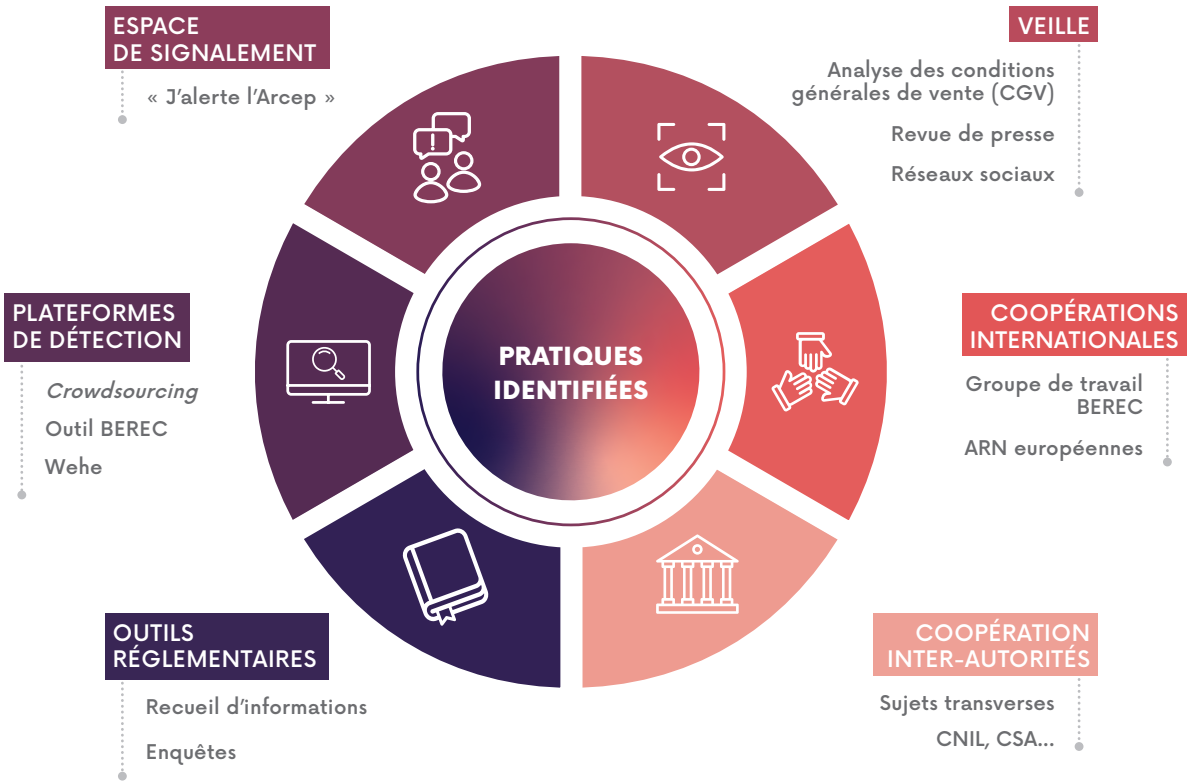
De manière plus générale, le CEPD relève que les dispositifs consistant à traiter les noms de domaine ou les URL induisent une forme de surveillance des réseaux susceptible de porter atteinte aux droits fondamentaux à la vie privée et à la protection des données personnelles des utilisateurs consacrés par les articles 7 et 8 de la Charte des droits fondamentaux de l'UE. Au-delà du recueil du consentement des utilisateurs concernés, le CEPD encourage donc les opérateurs à faire appel à des techniques moins intrusives afin de gérer du trafic et à mettre en commun leurs efforts pour développer des techniques standardisées et interopérables plus respectueuses des données personnelles des utilisateurs.

1. Considérant 2 de la proposition de règlement

3. LE DÉVELOPPEMENT DE LA BOÎTE À OUTILS DE L'ARCEP

Afin de veiller à la neutralité du net, l'Arcep s'est dotée d'une boîte à outils lui permettant de disposer d'une vue d'ensemble des pratiques du marché sur les quatre pierres angulaires du règlement sur l'internet ouvert : les pratiques commerciales, les gestions de trafic, les services spécialisés et les obligations de transparence.

LA BOÎTE À OUTILS DE L'ARCEP EN MATIÈRE DE NEUTRALITÉ DU NET



Source : Arcep

Dans le cadre de la mission de surveillance, les services de l'Autorité s'attachent à vérifier de manière continue les conditions de vente des offres des FAI. Cette action a permis de déceler dans les conditions générales de certains opérateurs des clauses contraires à la neutralité du net. En 2019, ce travail de veille a porté sur l'ensemble des offres d'accès à internet des FAI, notamment celles commercialisées par les opérateurs ultramarins ou par des entreprises de secteurs autres que celui des communications électroniques (cf. section suivante).

En complément, l'Autorité dispose d'outils réglementaires permettant de recueillir auprès des FAI des informations sur les règles de gestion de leurs réseaux.

Fin 2017, une plateforme de signalement « J'alerte l'Arcep » est venue enrichir la boîte à outils de l'Autorité. Grâce à cette plateforme, les utilisateurs finals peuvent informer l'Autorité de situations problématiques. Au cours de l'année passée, 146 signalements relatifs à la neutralité du net ont été déposés sur le site « J'alerte l'Arcep ». En particulier, les signalements déposés par les utilisateurs finals ont permis à l'Autorité d'identifier rapidement de possibles infractions au principe de neutralité d'internet et de favoriser une résolution rapide des difficultés soulevées, détaillées dans la section suivante.

Par ailleurs, l'Arcep échange régulièrement avec ses homologues européens sur leurs différentes problématiques rencontrées au niveau national. Ce mécanisme de coopération renforcée entre ARN a permis à l'Autorité de se projeter dans des cas concrets très variés, de confronter la régulation au regard des nouvelles technologies et usages et de mieux appréhender des situations nationales similaires à celles décrites par ses homologues. À nouveau, l'année écoulée a été marquée par les interrogations relatives à la conformité des offres commerciales de *zero-rating* avec le règlement internet ouvert, comme en témoignent les différentes questions préjudicielles sur ce sujet portées devant la Cour de justice de l'Union européenne.

En 2019, l'Arcep s'est aussi rapprochée d'autorités de régulation françaises, en particulier la Commission nationale de l'informatique et des libertés (CNIL) dans le cadre des discussions relatives à l'étendue des données de transport accessibles aux FAI. Cette coopération inter-autorités permet de croiser les compétences respectives de chacun afin de faire progresser l'analyse réglementaire sur des sujets communs et transversaux.

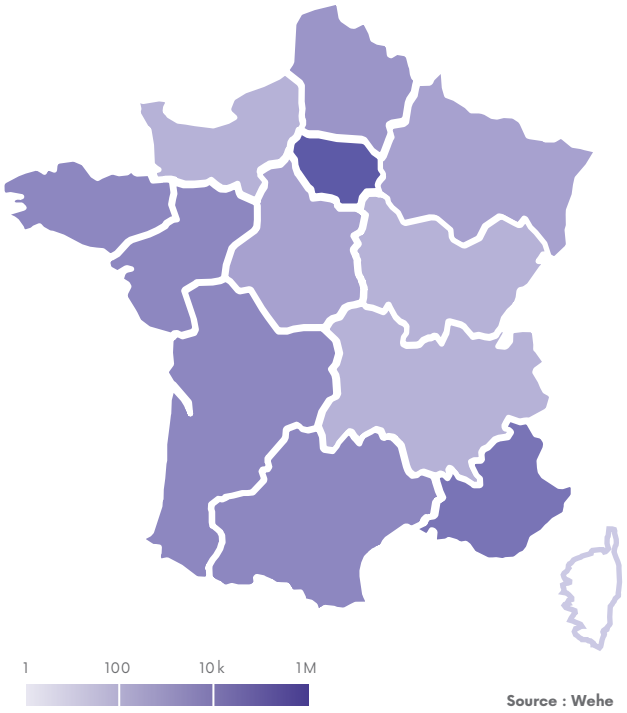
Enfin, l'Arcep met à la disposition du grand public depuis novembre 2018 un outil de détection Wehe. Développé par la *Northeastern University* et fondé sur un code en *open source,* cet outil de mesure compare les temps de parcours du trafic pour certains

services. Le test s'effectue en deux étapes. Premièrement, l'outil simule l'utilisation d'un service dans le réseau d'un FAI afin de mesurer comment celui-ci traite le trafic réel issu de ce service. Deuxièmement, l'outil simule à nouveau le même trafic mais en remplaçant le contenu par un contenu chiffré invisible pour le FAI. En cas de dissemblance entre les deux simulations, il est possible de soupçonner l'existence d'une mesure de gestion de trafic mise en œuvre par le FAI. Depuis son lancement, l'outil Wehe a été utilisé par les utilisateurs finals près de 115 000 fois et, à ce jour, aucune différenciation n'a été détectée *via* l'application.

Disponible sous Android et iOS, l'outil est disponible en français afin d'être le plus largement accessible pour les utilisateurs finals français. Toutefois, les applications testées ne reflétaient pas nécessairement les services les plus usités par les internautes français. Grâce au partenariat avec la *Northeastern University,* la liste des services testés a donc été récemment mise à jour afin de correspondre aux services les plus communs en France.

Dans la continuité des premiers travaux menés en 2018, l'Arcep a souhaité que l'outil Wehe soit doté d'une fonctionnalité supplémentaire de détection des blocages de ports logiciels. En effet, l'accès à certains services ou applications en ligne s'effectue au moyen d'un port logiciel[9] spécifique dont un éventuel blocage, bridage ou priorisation pourrait affecter les modalités d'accès au dit service par l'utilisateur final. Le test, en cours de développement, permettra aux utilisateurs finals de contrôler plusieurs ports logiciels fréquemment utilisés. En cas de dysfonctionnement, les utilisateurs finals sont invités à relayer leurs difficultés directement *via* la nouvelle plateforme « J'alerte l'Arcep » afin que l'Autorité puisse examiner au cas par cas les incompatibilités potentielles avec le règlement internet ouvert.

LOCALISATION DES TESTS WEHE EN FRANCE MÉTROPOLITAINE - 2019



Source : Wehe

DIFFÉRENTS *REPLAYS* TESTÉS PAR L'APPLICATION WEHE

Source : Arcep

9. Voir lexique.

PREMIÈRES QUESTIONS PRÉJUDICIELLES POUR LA COUR DE JUSTICE DE L'UNION EUROPÉENNE

En 2019, la Cour de justice de l'Union européenne (CJUE) a été saisie de plusieurs questions préjudicielles relatives aux modalités d'application des dispositions du règlement internet ouvert.

Fin 2018 et début 2019, la Cour de Budapest a saisi la CJUE de questions préjudicielles portant sur des offres de *zero-rating* proposées par l'opérateur national Telenor (Affaires jointes C-807/18 et C-39/19). L'opérateur hongrois propose en effet des offres commerciales où l'accès à certains services en ligne n'est pas décompté du volume de données prévu dans les contrats et n'est pas bridé ou bloqué une fois ce volume de données épuisé, contrairement aux autres services en ligne.

La CJUE a également été saisie en novembre 2019 d'une question préjudicielle, déposée par le Tribunal administratif de Cologne (Allemagne), relative aux modalités de gestion en itinérance des offres de *zero-rating* de l'opérateur allemand Vodafone (Affaire C-854/19). L'opérateur Vodafone propose des *pass* afin que les services visés ne soient pas décomptés du volume de données prévu au contrat. Mais, à l'étranger, cette politique tarifaire n'est plus valide et les services normalement non décomptés sont alors décomptés du volume de données contractuellement consenti à l'utilisateur final.

Ces questions préjudicielles devraient faire l'objet d'un premier examen par la CJUE en 2020, offrant ainsi une grille d'analyse complémentaire à celle détaillée par les lignes directrices révisées.

4. ÉTAT DES LIEUX DES PRATIQUES OBSERVÉES

Dans la continuité des travaux lancés en 2018, l'Autorité s'est intéressée à la question des blocages de port. L'accès à un service ou à une application en ligne s'effectue au moyen d'un port logiciel, dont le blocage empêche de fait l'accès au service. L'Autorité s'est donc penchée sur les différents cas signalés sur la plateforme « J'alerte l'Arcep ». Les premiers signalements étaient relatifs au blocage de flux HTTPS sur un port donné par un opérateur mobile, empêchant ainsi pour les utilisateurs l'accès à certains services. L'Arcep s'est fait l'écho des difficultés rencontrées par les utilisateurs auprès de l'opérateur concerné, qui a convenu de mettre en place un mécanisme préservant la liberté de choix des usagers.

Afin de mieux informer les utilisateurs finals, l'Arcep met à leur disposition un 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. Ce dispositif sera renforcé par le lancement prochainement du nouveau test de priorisation de port de l'outil Wehe, précédemment évoqué.

Durant l'année 2019, la formation compétente de l'Autorité s'est penchée sur le respect de la neutralité du net par les offres de Wi-Fi en vol proposées par les compagnies aériennes. Ce sujet étant par nature transnational, la question a également resurgi dans le cadre des travaux du groupe d'experts sur la neutralité du net du BEREC. Le groupe d'experts du BEREC a confirmé que les offres de Wi-Fi en vol pouvaient être définies comme publiquement accessibles et *de facto* soumises aux dispositions du règlement internet ouvert. Ces services d'accès à internet en vol sont ainsi soumis au règlement internet ouvert au même titre que les offres fournies par des fournisseurs d'accès à internet traditionnels. Placée sous le sceau du dialogue proactif, l'action de l'Arcep a permis une meilleure prise en compte des dispositions du règlement internet ouvert par les compagnies aériennes dans le déploiement de leurs offres d'accès à internet en vol. Ainsi Air France a adapté ses offres afin de les rendre les plus neutres possible compte tenu de la singularité des contraintes techniques d'un service internet en vol.

La formation compétente de l'Autorité s'est également intéressée aux offres de Wi-Fi dans les trains. Proposées aux passagers, ces offres d'accès à internet, également considérées comme publiquement accessibles, sont soumises aux dispositions du règlement internet ouvert. Au dernier trimestre 2019, l'Autorité a donc interrogé la SNCF afin de disposer d'informations complémentaires sur le respect du principe de neutralité du net dans son offre d'accès à internet, ainsi que les informations transmises aux usagers. À ce jour, l'Arcep poursuit l'examen de ces offres et compte sur la mobilisation de la SNCF pour s'assurer du respect du principe de neutralité du net dans les offres de Wi-Fi dans les trains.

L'Autorité est également attentive aux différents signalements reçus sur de possibles pratiques contraires à la neutralité du net, remontés notamment sur la plateforme « J'alerte l'Arcep ». Ces alertes ont amené l'Autorité à examiner la conformité de différents services d'accès à internet, comme récemment des offres proposées dans des hôpitaux. Elles ont aussi permis la résolution rapide d'un problème d'accès à plusieurs sites internet (dont la plateforme « J'alerte l'Arcep » elle-même) depuis le réseau d'un petit opérateur.

Enfin, l'Arcep a examiné la conformité de l'ensemble des offres d'accès à internet proposées en outre-mer au principe de neutralité du net. Début 2020, l'Arcep s'est rapprochée des opérateurs ultramarins afin de dresser un état des lieux sur cette question et d'inviter les opérateurs à entrer dans un dialogue proactif avec les services de l'Autorité.

NEUTRALITÉ DU NET ET SERVICES PMR OPÉRÉS SUR UN RÉSEAU 4G GRAND PUBLIC

Historiquement, les réseaux *Private Mobile Radiocommunication* (PMR) sont des réseaux de radiocommunication privés sécurisés, essentiellement axés sur des services de phonie et de mini-messagerie. Ils s'adressent à des entreprises qui ont des besoins forts en matière de disponibilité, de confidentialité ou de couverture de zone spécifique.

Le fonctionnement de ces réseaux repose historiquement sur des technologies spécifiques (TETRA par exemple), mais les entreprises sont progressivement invitées à migrer vers des offres modernisées. Deux approches potentiellement complémentaires sont envisagées pour répondre aux nouveaux usages attendus : soit un réseau PMR est déployé sur une infrastructure 4G ad hoc complètement distincte du réseau 4G à destination du grand public, soit un réseau PMR est déployé sous la forme d'un service distinct au sein même d'une infrastructure 4G grand public. La première solution assure à l'exploitant une autonomie dans le déploiement de son réseau PMR, mais présente l'inconvénient d'imposer des coûts d'exploitation plus élevés. La seconde solution permet de mutualiser les coûts d'exploitation, mais nécessite potentiellement que le service PMR bénéficie d'une préemption ponctuelle sur les autres services exploités concomitamment sur le réseau 4G grand public.

Introduire une préemption des services PMR sur un réseau 4G grand public revient à prioriser ces services sur le fonctionnement général du réseau, y compris les services d'accès à internet. Cette seconde solution peut donc affecter la qualité des services d'accès à internet. L'Arcep a donc analysé cette pratique au regard des dispositions du règlement internet ouvert et a conclu que la mise en place d'un service PMR est possible du point de vue du règlement sous réserve qu'il réponde à un véritable besoin de disponibilité/sécurité et que ni la qualité générale d'internet, ni celle des autres services activés sur le réseau (notamment la VoLTE*) n'en pâtissent. Enfin, les cas de priorisation des services PMR devront rester très exceptionnels.

* Voir lexique.

CHAPITRE 5

Terminaux et plateformes, maillons structurants de l'accès à internet

À RETENIR

Le 19 février 2020, le Sénat a adopté à l'unanimité **(342 voix pour 0 voix contre)** la proposition de loi visant à garantir le libre choix du consommateur dans le cyberespace. Elle confierait à l'Arcep des pouvoirs afin d'assurer la neutralité des terminaux et d'établir l'interopérabilité des plateformes.

Le 24 février 2020, Bruno Le Maire, ministre de l'Économie et des Finances, et Cédric O, secrétaire d'État chargé du Numérique, ont mis en place **une équipe interministérielle** à laquelle participent les principales autorités françaises, dont l'Arcep, afin de faire des propositions d'intervention à l'égard des plateformes numériques.

Dans une communication présentée en février 2020, **la Commission européenne** indique étudier les modalités d'une régulation *ex ante* dont la mise en place permettra d'assurer que les marchés dominés par des plateformes structurantes restent ouverts et contestables.

Le règlement européen sur l'internet ouvert accorde des droits aux utilisateurs, tels que le droit d'accéder et de diffuser des informations et contenus en ligne. Mais il ne s'impose qu'aux fournisseurs d'accès à internet. Situés à une extrémité de la chaîne d'accès à internet, les smartphones, assistants vocaux, les voitures connectées et autres terminaux accompagnés de leur système d'exploitation se révèlent être un maillon faible de l'ouverture d'internet.

L'Arcep a établi ce constat dans son rapport[1] de 2018 et a émis une série de propositions pour garantir un internet ouvert, c'est-à-dire pour rendre sa liberté de choix à l'utilisateur, en particulier :

- réguler « par la *data* », et rendre l'information transparente et comparable pour les utilisateurs, particuliers et professionnels ;
- veiller à la fluidité des marchés, et à la liberté de passer d'un environnement à l'autre ;
- lever certaines restrictions imposées artificiellement par les acteurs-clés des terminaux aux utilisateurs et aux développeurs de contenu et services.

Après la publication de ce rapport, l'Arcep a poursuivi ses travaux de veille et de communication en partenariat avec une diversité d'acteurs tout au long de l'année 2019. Au-delà des composantes physiques des terminaux, le faible nombre de plateformes numériques qui structurent l'accès à internet est un sujet qui a pris de l'importance.

1. NEUTRALITÉ DES TERMINAUX : AVANCÉE DES TRAVAUX

Un premier outil d'ouverture des terminaux consiste à donner aux utilisateurs les moyens de faire des choix éclairés. Sans attendre la mise en place d'une régulation plus avancée, l'Arcep a ainsi publié en 2019 deux fiches pratiques à destination des utilisateurs finals pour les guider dans l'utilisation de leurs terminaux. La première[2] explique comment les utilisateurs peuvent conserver leurs données lorsqu'ils migrent vers un nouveau smartphone grâce aux mécanismes de portabilité des données mis en avant par le RGPD. Il est en effet possible de porter d'un système à l'autre ses contacts, mais aussi ses photos, ses historiques de messagerie, ses calendriers, ou encore certaines applications. La seconde fiche pratique[3] 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. Elle indique par exemple comment paramétrer certaines options par défaut (navigateur, moteur de recherche, ou choix d'applications) et aide ainsi les utilisateurs à reprendre le contrôle sur leur smartphone.

Pour approfondir son diagnostic, l'Arcep a également souhaité interroger les Français sur leur liberté de choix sur leur smartphone lors de l'édition 2019 du Baromètre du numérique[4]. S'agissant des systèmes d'exploitation, 99 % des interrogés fonctionnent avec l'un des deux systèmes dominants (Android ou iOS). Trois

1. https://www.arcep.fr/uploads/tx_gspublication/rapport-terminaux-fev2018.pdf
2. https ://www.arcep.fr/demarches-et-services/utilisateurs/terminaux-portabilite-donnees.html
3. https://www.arcep.fr/demarches-et-services/utilisateurs/terminaux-personnalisation-api.html
4. https://www.arcep.fr/actualites/les-communiques-de-presse/detail/n/equipements-et-usages-du-numerique.html

quarts des utilisateurs accordent de l'importance à la possibilité de portabilité de leurs données, indispensable pour passer d'un système à l'autre et pourtant limitée à ce jour. Dans son rapport, l'Arcep constatait que la série d'applications préinstallées avec lesquelles les smartphones sont généralement vendus constituent une contrainte imposée. L'enquête montre effectivement que le navigateur préinstallé est largement privilégié : moins de 20 % des détenteurs de smartphone utilisent un autre navigateur que celui préinstallé, et deux tiers d'entre eux n'ont pas testé d'autres navigateurs. En revanche, lorsqu'ils ont effectué ce test, ils sont une majorité (55 %) à en changer. Le baromètre conforte ainsi l'analyse de l'Arcep et ses propositions pour garantir la liberté de choix des utilisateurs au niveau des terminaux.

Enfin, l'Arcep a contribué à l'étude[5] HADOPI/CSA « Assistants vocaux et enceintes connectées » en concentrant son analyse sur les limites additionnelles engendrées par ces terminaux spécifiques qui sont amenés à prendre une part croissante dans les usages. L'évolution vers des terminaux toujours plus intelligents – notamment des assistants vocaux à la maison et des ordinateurs de bord dans la voiture – laisse entrevoir un risque de limitation toujours plus grand. En effet, les conditions d'affichage (écran petit, voire inexistant) et le passage de l'essentiel de l'interaction par le canal audio limitent les possibilités d'accéder à une information exhaustive et entraînent une sélection des informations présentées trop imparfaitement maîtrisée par l'utilisateur sans que la transparence adéquate sur les choix effectués par le terminal soit toujours faite.

L'année 2019 a été riche en actualités sur le sujet de la neutralité des terminaux. À la suite de sa condamnation par la Direction générale à la Concurrence de la Commission européenne pour abus de position dominante sur le marché des systèmes d'exploitation, en 2018, Google a été contraint de proposer à ses utilisateurs Android le choix de navigateurs par défaut alternatifs. L'interface de choix implémentée a toutefois fait l'objet de nombreuses critiques. Duck Duck Go a notamment accusé Google de profiter du design de l'interface de choix pour mettre en avant son propre navigateur. Google a également fait l'objet de virulentes critiques concernant les enchères organisées pour permettre à des moteurs de recherche alternatifs d'être proposés aux utilisateurs d'Android. Cette situation met en avant la difficulté d'implémenter *a posteriori* des remèdes comportementaux efficaces.

Outre-Atlantique, la décision américaine d'interdire à Huawei toute relation commerciale avec les entreprises américaines a contraint le constructeur à ne plus pouvoir proposer les services de Google (Search, Youtube, Chrome, Play Store, kits pour développeurs, etc.) sur ses terminaux. En réponse, Huawei a choisi de développer ses propres services[6], ce qui pourrait à terme conduire à une plus forte concurrence sur les marchés des systèmes d'exploitation et produits associés, mais aussi à la création d'un troisième écosystème fermé avec des problématiques similaires à celles observées pour les deux autres.

La question des conditions d'accès aux magasins d'applications par les développeurs d'applications est également restée au cœur de l'actualité en 2019. En effet, à la suite de la plainte de Spotify, la Commission européenne a ouvert une enquête concernant les tarifications appliquées sur l'Apple Store. Spotify accuse Apple de profiter de son intégration verticale pour exonérer son application Apple Music des 30 % de commissions appliquées sur son magasin d'applications, lui donnant ainsi un avantage concurrentiel sur les autres applications de *streaming* musical. Les 30 % de commission appliqués sur le PlayStore de Google font aussi l'objet de critiques. Le jeu à succès Fortnite développé par Epic n'est par exemple toujours pas disponible sur le Play Store, Google ayant refusé[7] d'accéder à la demande d'exception tarifaire de l'entreprise.

Par ailleurs, le sujet de l'accès à certaines fonctionnalités des terminaux fait toujours débat. La question de l'accès à la puce NFC des terminaux Apple est par exemple en discussion auprès de la Commission européenne, qui étudie si la restriction de cet accès aux applications tierces constitue un abus de position dominante.

Enfin, une lettre ouverte[8] signée par Privacy International et plus de 50 autres organisations a été publiée, demandant à Google de prendre des mesures contre les pratiques de pré-installations de logiciels sur les appareils Android. Les signataires mettent notamment en cause les constructeurs de terminaux bénéficiant d'accès privilégiés aux fonctionnalités sans en informer les utilisateurs.

Le sujet de l'ouverture et de la neutralité des terminaux a fait l'objet de réflexions au sein de différentes institutions. Au niveau européen, le *Center on Regulation in Europe* (CERRE) s'est penché sur le sujet en publiant un rapport en mars 2019[9]. Ce rapport a constaté que les structures de marché propres aux systèmes d'exploitation sont propices aux comportements abusifs, ce qui peut conduire à restreindre la liberté de choix des consommateurs. Le rapport propose en conséquence l'interdiction de certaines pratiques telles que la pré-installation d'applications ou l'activation de fonctionnalités par défaut, lorsque ces pratiques sont liées à des fins purement commerciales.

En France, une proposition de loi a été déposée au Sénat[10], visant à instaurer un principe de liberté de choix du consommateur dans l'usage de leurs terminaux. Cette proposition de loi conférerait à l'Arcep des outils de contrôle et de sanction visant à assurer la bonne mise en œuvre de ce principe. Elle vise notamment à interdire, sur les terminaux, des pratiques telles que l'impossibilité de supprimer des applications préinstallées, l'impossibilité d'installer des magasins d'applications alternatifs, ou encore la restriction de manière injustifiée de l'accès aux fonctionnalités des équipements terminaux par les développeurs. La proposition de loi a été adoptée à l'unanimité au Sénat.

5. https://www.csa.fr/Informer/Collections-du-CSA/Thema-Toutes-les-etudes-realisees-ou-co-realisees-par-le-CSA-sur-des-themes-specifiques/Les-autres-etudes/Etude-HADOPI-CSA-Assistants-vocaux-et-enceintes-connectees
6. https://consumer.huawei.com/en/press/news/2020/huawei-revealed-huawei-appgallery-vision
7. https://www.theverge.com/2019/12/9/21003553/google-play-store-fortnite-epic-games-30-percent-cut-dispute
8. https://privacyinternational.org/advocacy/3320/open-letter-google
9. https://cerre.eu/publications/device-neutrality-missing-link-fair-and-transparent-online-competition
10. http://www.senat.fr/espace_presse/actualites/202002/libre_choix_du_consommateur_dans_le_cyberespace.html

2. LES PLATEFORMES NUMÉRIQUES STRUCTURANTES

Si la liberté de choix des consommateurs peut être limitée par des restrictions liées à leurs terminaux, le positionnement et les actions de certaines plateformes numériques peuvent également être de nature à restreindre cette liberté de choix. Le sujet de la prédominance de ces plateformes, pouvant être qualifiées de « structurantes », a fait l'objet de nombreuses réflexions et initiatives. Au niveau français, la proposition de loi visant à garantir le libre choix du consommateur dans le cyberespace prévoit par exemple des dispositions telles que l'interopérabilité pour faire partager les effets de réseaux dont profitent les principales plateformes. Des initiatives visant à limiter la puissance de ces plateformes ont également été lancées dans d'autres pays européens, par exemple par le ministère de l'Économie allemand et l'Autorité de la concurrence hollandais. L'Italie et la Pologne ont notamment rédigé, au côté de l'Allemagne et la France, une lettre ouverte destinée à la vice-présidente Margrethe Vestager invitant la Commission à mettre en place un cadre de régulation spécifique destiné à encadrer le pouvoir de certains acteurs systémiques du numérique. Enfin, plusieurs rapports, dont les rapports Crémer[11] (diligenté par la DG Concurrence de la Commission européenne), Furman[12] (à la demande des autorités britanniques) et Scott-Morton[13] (centre Stigler à Chicago) ou encore le rapport de l'Autorité de la concurrence et de la protection des consommateurs australienne[14] ont mis en évidence la place prédominante prise par certains acteurs numériques. Ces travaux soulignent que les préoccupations autour de l'importance de ces plateformes ne sont plus seulement économiques et concurrentielles mais également d'ordre sociétal.

L'Arcep suit avec attention les travaux réalisés concernant les pratiques de régulation de la diffusion de contenus haineux et fausses informations. L'Arcep a notamment participé à la mission « Régulation des réseaux sociaux – Expérimentation Facebook » qui avait pour objectif d'émettre des recommandations pour la création d'un cadre français de responsabilisation des réseaux sociaux. Le rapport de la mission, publié en mai 2019[15], a conclu à la légitimité d'une intervention publique de régulation et a proposé des pistes de réflexion. Cette intervention doit reposer sur une logique de responsabilisation accrue des réseaux sociaux fondée sur une régulation *ex ante*, tout en assurant un équilibre avec une politique répressive, indispensable pour lutter efficacement contre les auteurs des abus.

Dans le prolongement des États généraux du numérique, l'Arcep a contribué aux réflexions autour de l'identification des grands acteurs qui seraient soumis à cette régulation *ex ante* nouvelle. L'Arcep a ainsi d'abord proposé une définition des opérateurs de « plateformes numériques structurantes » qui seraient les opérateurs de plateforme en ligne ou les fournisseurs de système d'exploitation, qui, en particulier du fait de leur activité d'intermédiation dans l'accès aux services et contenus d'internet, et de par leur importance, sont en mesure de limiter de manière significative la capacité des utilisateurs à exercer une activité économique ou à communiquer en ligne. En complément, l'Arcep a proposé un faisceau d'indices permettant de caractériser une plateforme comme étant « structurante », ainsi qu'une articulation possible des régulations *ex ante* et *ex post*. Aujourd'hui, l'Arcep poursuit ses réflexions et s'intéresse aux outils et remèdes dont il pourrait être pertinent que la puissance publique dispose pour réguler efficacement les acteurs contrôlant les carrefours d'internet.

Au niveau européen et dans le cadre de la publication de l'agenda du *Digital Services Act,* la Commission européenne a indiqué étudier la possibilité d'implémenter une régulation *ex ante* à un certain nombre d'acteurs du secteur numérique. Après une consultation publique et une étude d'impact prévues à l'été 2020, la Commission européenne devrait présenter en fin d'année les résultats de ses réflexion. L'objectif de ces travaux consiste à étudier les modes de régulations *ex ante* pouvant garantir le caractère contestable, l'équité et l'innovation des marchés numériques, dont les bienfaits pourront aller au-delà des considérations économiques. À ce sujet, le Gouvernement français a mis en place[16] une équipe réunissant des représentants des principales autorités françaises compétentes, dont l'Arcep, en matière de régulation des plateformes numériques pour continuer à travailler sur les orientations fixées par la Commission européenne dans le cadre du *Digital Services Act.*

11. https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf
12. https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel
13. https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure---report-as-of-15-may-2019.pdf?la=en&hash=B2F11FB118904F2AD701B78FA24F08CFF1C0F58F
14. https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report
15. https://www.economie.gouv.fr/remise-rapport-mission-regulation-des-reseaux-sociaux
16. https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=5FA62C31-70A4-4392-8526-EFC6F85FD8AD&filename=2043%20CP%20groupe%20de%20travail%20num%C3%A9rique.pdf

LA PAROLE À...

SOPHIE PRIMAS

Présidente de la Commission des affaires économiques du Sénat

LE SÉNAT A ADOPTÉ LA NEUTRALITÉ DES TERMINAUX

La domination économique presque sans partage des quelques entreprises qui régissent nos vies en ligne est déplorée à longueur d'articles et de rapports, mais le logiciel de la régulation économique peine à se mettre à jour. Si, outre-Atlantique, le démantèlement est mis en avant comme l'alpha et l'oméga, il nous semble que l'économie numérique a ses particularités qui exigent d'imaginer de nouvelles régulations de ce qu'il est désormais convenu d'appeler les plateformes « structurantes ». C'est ce que propose le Sénat à travers la proposition de loi visant à garantir le libre choix du consommateur dans le cyberespace, adoptée à l'unanimité le 19 février dernier.

Elle consacre, entre autres mesures, le principe de « libre choix » de l'utilisateur sur son smartphone ou sur tout terminal, autrement appelé « neutralité des terminaux ». Il faut ici rendre hommage aux travaux précurseurs de l'Arcep depuis le début des années 2010, sur lesquels le Sénat a pu s'appuyer. Une autorité de régulation serait en charge de vérifier si les pratiques portant atteinte à ce libre choix – comme l'impossibilité sur un terminal de désinstaller une application ou les pratiques discriminatoires à l'encontre d'applications tierces – sont justifiées ou non. Elle devrait accompagner les acteurs pour éviter l'apparition de pratiques dommageables plutôt que de les sanctionner *a posteriori.* Le Sénat propose ainsi une régulation agile, pro-innovation et qui rend le pouvoir à l'utilisateur.

Alors que des négociations sont engagées au niveau européen, les sénateurs proposent d'agir au niveau national, sans attendre, pour une raison simple : le coût de l'attente nous semble trop élevé. Plus nous attendons, plus nous risquons de laisser les géants asphyxier la concurrence et l'innovation, et enfermer les consommateurs à leur insu dans leurs écosystèmes. Il est urgent de rendre le pouvoir au consommateur.

DIANE COYLE

*Professeure de politique publique - **Université de Cambridge***
Membre du Comité d'experts de la concurrence numérique au Royaume-Uni

LA RÉGULATION *EX ANTE* DES PLATEFORMES NUMÉRIQUES

L'opinion selon laquelle les marchés numériques, dominés par un petit nombre d'acteurs, ne fonctionnent pas aussi bien qu'ils le pourraient, est largement répandue. Les préoccupations vont de la concurrence ou l'absence de choix pour les consommateurs à la toxicité des « fausses informations » en ligne.

La crise économique actuelle signifie probablement que ces entreprises riches en liquidités se retrouveront dans une position encore plus dominante. Cependant, il est difficile d'améliorer la concurrence et le choix des consommateurs sur ces marchés. L'une des raisons est la présence d'effets de réseau : plus il y a d'utilisateurs sur une plateforme numérique, plus ils en bénéficient tous, et plus celle-ci devient importante. Les marchés numériques sont donc toujours susceptibles d'être des marchés où le vainqueur remporte tout. C'est pour cela que notre rapport, le *Furman Review*, au Royaume-Uni, a conclu que la régulation *ex ante* des acteurs concernés devrait être renforcée, de même que la politique de concurrence qui examine leur comportement *ex post*.

Actuellement, il existe peu de règles régissant les types de comportement ou les conséquences spécifiques aux plateformes numériques. Il s'agit notamment des traitements préférentiels qu'une plateforme donnerait à ses propres services, au détriment de ceux fournis par des tiers, ou des modifications fréquentes et inopinées des conditions générales et des interfaces de programmation (« API »). Nous avons recommandé qu'une unité spéciale dédiée aux marchés numériques soit créée pour introduire et mettre en application un code de conduite pour les plateformes dotées d'un pouvoir de marché important. Le gouvernement britannique a créé un groupe de travail au sein de l'Autorité de la concurrence nationale (la CMA) à cette fin.

Nous avons aussi appelé à une réglementation spécifique des données, l'un des principaux vecteurs de concentration et de barrières à l'entrée. La mobilité et l'interopérabilité des données seront essentielles pour stimuler la concurrence. Il s'avérera peut-être nécessaire d'imposer un accès plus ouvert à certaines données détenues par les géants du numérique. L'objectif serait non seulement d'ouvrir les marchés davantage à la concurrence, mais cela pourrait aussi devenir une nécessité sociale en cette période de crise économique sans précédent. De nombreuses personnes se demandent en effet pourquoi quelques grandes entreprises peuvent conserver toute la valeur des masses de données fournies gratuitement par leurs utilisateurs, et exigent qu'elles soient aussi utilisées pour la société dans son ensemble.

PARTIE 3

Agir face au défi environnemental du numérique

CHAPITRE 6

Intégrer l'empreinte environnementale des réseaux à la régulation

CHAPITRE

6

Intégrer l'empreinte environnementale des réseaux à la régulation

À RETENIR

Le cadre prospectif du chantier « Réseaux du futur » a permis à l'Arcep d'initier une réflexion afin d'apprécier les effets de diverses évolutions des réseaux et de leurs usages sur l'empreinte carbone du numérique et donné lieu à la publication d'une note **le 21 octobre 2019.**

L'organe des régulateurs européens des télécoms, le BEREC, a mis en place **le 6 mars dernier** trois nouveaux groupes d'experts, dont un dédié au développement durable, que l'Arcep co-préside.

Le 6 avril 2020, l'Arcep ajoute un volet environnemental à son outil de collecte d'informations auprès des opérateurs télécoms afin de mieux comprendre les enjeux environnementaux du secteur et informer les pouvoirs publics ainsi que les utilisateurs sur l'impact de leurs usages.

Dès 2018, à l'occasion de son cycle de réflexion sur « les Réseaux du futur », l'Arcep, entourée d'un Comité scientifique, a initié une réflexion afin d'apprécier les effets de diverses évolutions des réseaux et de leurs usages sur l'empreinte carbone du numérique. Après la publication en octobre 2019 d'une première note sur le sujet, l'Arcep désire contribuer à la réflexion sur la préservation de l'environnement.

1. ÉTAT DES LIEUX

L'impact du numérique sur l'environnement est un sujet d'attention croissant. Le baromètre du numérique publié par l'Arcep en 2019 souligne cette prise de conscience sociétale et montre que si les Français conçoivent positivement le rôle du numérique dans leur quotidien, ils sont de plus en plus réservés quant à l'impact environnemental de celui-ci. En effet, 38 % de la population française perçoit le numérique comme une chance pour l'environnement contre 53 % en 2008. Disposés à changer leur comportement pour 69 % d'entre eux, 45 % des Français s'estiment encore insuffisamment informés sur l'impact du numérique sur l'environnement[1].

Selon les sources[2], le numérique représente aujourd'hui 3 à 4 % des émissions de gaz à effet de serre (GES) dans le monde soit une empreinte équivalente au transport aérien. Si cette part demeure modeste comparativement à d'autres secteurs, la croissance annuelle de la consommation de numérique[3] (volume de données, terminaux, etc.) doit nous interroger[4].

2. LES PREMIERS TRAVAUX DE L'ARCEP À L'OCCASION DU CHANTIER « RÉSEAUX DU FUTUR »

En 2018, à l'occasion de son cycle de réflexion sur « les Réseaux du futur », l'Arcep, entourée d'un Comité scientifique, a initié une réflexion afin d'apprécier les effets de diverses évolutions des réseaux et de leurs usages sur l'empreinte carbone du numérique. Pour ce faire, l'Autorité a auditionné des experts de la société civile, des industriels ainsi que des acteurs publics pour tenter d'identifier les principales problématiques liées à l'empreinte carbone du numérique et apporter des premiers éléments de réponse.

Ces travaux ont permis de dresser plusieurs constats dont les principaux peuvent être repris ici[5].

En premier lieu, si la consommation électrique des réseaux est la source majeure d'émission de GES des opérateurs, les émissions de GES du numérique concernent toute la chaîne de valeur, des centres de données aux terminaux. Ces derniers sont la cause

1. CREDOC, Enquête sur les « Conditions de vie et les Aspirations », juin 2019.
2. Shiftproject, Lean ICT : « Pour une sobriété numérique », octobre 2018 ; GreenIT, « Empreinte environnementale du numérique mondiale », septembre 2019.
3. Si l'on se réfère au dernier rapport du « Shift Project », la croissance annuelle des émissions en GES du numérique est de l'ordre de 8 à 9 %.
4. Si l'on en reste aux émissions en GES du numérique, dans une audition au Sénat le 29 janvier 2020, Hugues Ferreboeuf, chef de projet au Shift Project, indiquait notamment que le rythme actuel de croissance de ces émissions pourrait entraîner un triplement de son empreinte globale d'ici à 2025 par rapport à 2015.
5. Pour le détail, voir la note « L'empreinte carbone du numérique », Arcep, 21 octobre 2019, disponible ici : https://www.arcep.fr/uploads/tx_gspublication/reseaux-du-futur-empreinte-carbone-numerique-juillet2019.pdf

principale de l'impact énergétique du numérique. En effet, les équipements terminaux (smartphones, tablettes, écrans, enceintes connectées, etc.) sont, selon les sources, responsables de plus de la moitié des émissions de GES du numérique, en particulier durant leur phase de production qui représente environ 80 % des émissions qui leur sont associées. À noter qu'aux émissions de GES s'ajoute la consommation en ressources (terres rares et eau notamment) que génère la production d'équipements terminaux. Concernant les opérateurs télécoms en particulier, ces derniers peuvent être incités à améliorer l'efficacité énergétique des réseaux et des centres de données pour limiter leur facture énergétique. En effet, une estimation grossière situe la facture énergétique des opérateurs français de quelques dizaines à plusieurs centaines de millions d'euros[6] en fonction de leur taille et du prix d'achat de l'électricité. Par exemple, pour les opérateurs mobiles, la consommation énergétique représenterait de l'ordre de 15 à 20 % des coûts d'exploitation[7].

En second lieu, les nouveaux usages et leur massification, permis entre autres par l'amélioration des réseaux et des équipements, augmentent la consommation de données, ce qui s'apparente à un « effet rebond[8] » c'est-à-dire qu'une évolution technologique qui s'avère permettre une réduction des émissions de GES à usage constant est susceptible de produire en fait un accroissement global des émissions en raison de la multiplication des usages qu'elle permet. Ce phénomène contribue donc à une hausse de la consommation énergétique. Il ressort de certains échanges organisés par les services de l'Arcep dans la préparation du rapport « L'empreinte carbone du numérique » que dans le cas particulier des réseaux mobiles, dont la consommation électrique est largement dépendante de leur utilisation, la consommation électrique d'une antenne en pic de trafic peut être jusqu'à trois fois supérieure à sa consommation au repos. Les équipements situés dans le cœur de réseau des opérateurs voient aussi leur consommation énergétique croître avec le trafic. À l'inverse, les améliorations technologiques peuvent contribuer à une amélioration de l'efficacité énergétique et à une réduction de la consommation par unité de trafic. Concernant l'utilisation des réseaux fixes par exemple, un acteur a indiqué que la fibre consomme en moyenne un peu plus de 0,5 watts (W) par ligne, soit trois fois moins que l'ADSL (1,8 W) et quatre fois moins que le RTC (2,1 W) sur le réseau d'accès[9]. La façon dont ces deux phénomènes se combinent déterminera *in fine* l'évolution de la consommation énergétique totale.

Enfin, si certains acteurs de la chaîne (opérateurs de réseaux ou de *data centers* par exemple) sont incités à limiter leur empreinte (notamment pour limiter les coûts liés à leurs infrastructures)[10], l'empreinte environnementale liée à la consommation de services numériques reste invisible pour la plupart des utilisateurs. Par exemple, l'énergie monopolisée par le numérique est principalement utilisée par les consommateurs (20 %), la production et l'utilisation des *data centers* (19 %), la production et l'utilisation des réseaux (16 %) et par la production (uniquement) des ordinateurs (17 %), smartphones (11 %) et télévisions (11 %)[11]. Il existe donc un réel besoin d'information des citoyens et des entreprises sur la base de référentiels métrologiques partagés entre les parties prenantes.

6. Estimation faite sur la base des bilans RSE des opérateurs et du coût de l'accès régulé à l'électricité.
7. https://www.mobileworldlive.com/ict-ee-18-news/global-ict-energy-efficiency-summit-paves-way-for-5g
8. L'effet rebond désigne l'augmentation de consommation liée aux différentes innovations technologiques (baisse des coûts, amélioration de l'efficacité énergétique, etc.). Il est pour la première fois mis en évidence par W. Stanley Jevons (« paradoxe de Jevons ») puis actualisé par les économistes Daniel Khazzoom et Leonard Brookes (« postulat de Khazzoom-Brookes »). Il représente un « paradoxe » dans la mesure où toute évolution d'un usage ou d'une technologie qui s'avère améliorer l'efficacité énergétique d'une activité devrait impliquer, *a priori,* une réduction de l'impact énergétique total de cette activité. Cependant, si cette amélioration engendre (ou se produit) en parallèle d'une baisse du coût de production du service considéré, cette baisse de coût permet alors de produire une plus grande quantité du bien ou service pour un prix inférieur et a pour effet d'en stimuler la demande.
9. Les consommations énergétiques de ces technologies filaires dépendant assez peu des usages qui en sont faits, ces évolutions se traduisent donc par des gains de consommation en valeur absolue.
10. Les incitations ne portent en revanche pas forcément sur la totalité de l'empreinte environnementale du numérique (notamment les phases de production et de recyclage d'équipements).
11. Voir note 7.

3. UNE VOLONTÉ DU RÉGULATEUR D'AGIR FACE AU DÉFI ENVIRONNEMENTAL

Fort de ces premiers constats l'Arcep propose d'établir une démarche, s'appuyant en particulier sur la régulation par la donnée, qui viserait à fournir à l'utilisateur final les informations pertinentes sur les impacts énergétiques associés aux usages du numérique. Définie en tant qu'objectif de la régulation à l'article L. 32-1 du CPCE[12], la protection de l'environnement est en effet un sujet sur lequel l'Arcep, qui souhaite poser le débat sur des bases objectives et sans *a priori*, désire approfondir son action afin notamment d'étendre la prise de conscience amorcée et de transmettre une information fiable et compréhensible aux utilisateurs finals. Cette démarche pourrait déboucher sur un « baromètre vert » du numérique. En ce sens, l'Arcep engage une première collecte d'informations sur l'impact environnemental des télécoms (réseaux, terminaux) auprès des opérateurs. Les indicateurs collectés portent sur les émissions de gaz à effet de serre produits par les principaux opérateurs de télécommunications et sur la consommation électrique des box et décodeurs audiovisuels utilisés par leurs clients.

Par ailleurs, l'Autorité a contribué début 2020 à la publication d'une note rédigée en collaboration avec les autres régulateurs sectoriels français visant à témoigner de leur prise de conscience et de leur rôle à jouer quant au défi climatique. Dans le même sens, la collaboration entre l'Arcep et l'ADEME devrait également se renforcer *via* une étude conjointe sur le sujet et des travaux communs dans le cadre de la mise en œuvre de la loi Économie circulaire imposant aux fournisseurs d'accès à internet d'informer leurs abonnés sur leur consommation et les émissions de gaz à effet de serre associées.

L'Arcep a par ailleurs proposé à ses homologues européens de traiter du sujet dans le cadre des travaux du BEREC dans les mois et années à venir après que d'autres régulateurs télécoms nationaux l'aient contacté à la suite de la publication de sa note Réseaux du futur « empreinte carbone du numérique ». Dans ce sens, les régulateurs européens, au sein du BEREC, ont mis en place le 6 mars dernier trois nouveaux groupes d'experts, dont un dédié au développement durable, avec notamment pour objectif d'étudier l'impact environnemental des réseaux télécoms au sens large et d'envisager les pistes permettant de le réduire. Anaïs Aubert, de l'Arcep, co-préside ce groupe d'experts avec Dr. Panos Karaminas, responsable de la gestion des programmes à l'office du BEREC.

Ces ambitions sont cohérentes avec la tendance amorcée au niveau européen puisque la Commission européenne a fait de l'empreinte carbone du numérique un sujet d'attention dans le cadre du Pacte vert pour l'Europe (*Green Deal*) qui devrait être publié dans les prochains mois. Elle a ainsi annoncé, dans le cadre de sa stratégie numérique, l'objectif de neutralité carbone à l'horizon 2030 des réseaux de télécommunications et des centres de données. Le *Radio Spectrum Policy Group* (RSPG) a également intégré dans ses travaux pour 2020 et 2021 une dimension environnementale. Le sous-groupe RSPG dédié à la question prévoit d'aborder trois sujets : l'inclusion des facteurs environnementaux dans les autorisations d'utilisation des fréquences, la protection des services météorologiques notamment dans les bandes millimétriques et l'accès aux fréquences pour les opérateurs d'énergie.

QUELQUES PREMIÈRES SOLUTIONS POUR LIMITER SON EMPREINTE ENVIRONNEMENTALE NUMÉRIQUE :

1. Choisir le réseau le moins énergivore en fonction de ses usages

- Sur le fixe par exemple, la fibre est moins énergivore que le cuivre
- Basculer son téléphone en mode Wi-Fi une fois chez soi (plutôt que de rester en 3G ou 4G)
- Télécharger ses contenus consommés en mobilité en avance chez soi sur réseau fixe (via Wi-Fi)

2. Adopter une certaine forme de sobriété dans ses usages numériques

- Éteindre sa box lorsque l'on est absent ou la nuit
- Télécharger uniquement des applications ou des vidéos qui nous intéressent vraiment
- Réduire les qualités d'image vidéo si possible
- Limiter les pièces jointes et nettoyer périodiquement sa boîte mail

3. Optimiser la durée de vie de ses objets connectés

- Ne changer de smartphone que lorsqu'il n'est plus fonctionnel (même chose pour tous les autres terminaux : ordinateurs, écrans, tablettes, etc.)
- Préférer les terminaux recyclés et recycler son téléphone en fin de vie.

12. Conjointement avec les ministres chargées de la Santé et de l'Environnement.

LA PAROLE À...

ARNAUD LEROY

*Président - **ADEME***

L'INTERNET ET LA TRANSITION ÉCOLOGIQUE

Je suis heureux de pouvoir signer ce billet sur un sujet qui interpelle de manière croissante nos contemporains, en France comme dans bon nombre de pays. L'internet et par extension l'activité numérique dans son ensemble interrogent : est-ce seulement accélérateur positif de transition ou il y a-t-il aussi des effets négatifs à cette dématérialisation apparente ?

En effet, ce secteur symbolise les paradoxes qui agitent la mise en œuvre de la transition écologique. La récente loi sur l'économie circulaire pose d'ailleurs un jalon important dans le questionnement de la société sur l'impact en émissions de gaz à effet de serre des pérégrinations sur internet à un moment où les émissions du secteur explosent.

Le confinement a démontré le besoin d'avoir des infrastructures réseaux qui fonctionnent en période de crise, car les flux de données représentent, aujourd'hui plus que jamais, un enjeu majeur dans notre société. Ces données, qui nous permettent de rester en contact, de garder une activité professionnelle, de nous informer, d'éduquer nos enfants et de nous distraire, ne doivent pas pour autant représenter un risque d'aggraver l'empreinte carbone de nos activités.

Il est donc nécessaire de continuer à améliorer l'efficacité énergétique des réseaux, comme c'est le cas avec le déploiement de la fibre optique, d'informer les usagers des émissions de gaz à effet de serre liées à leurs consommations de services numériques, et de proposer des solutions à toutes les parties prenantes visant une « sobriété » numérique.

Si l'évolution actuelle des technologies réduit la taille et la consommation en énergie des terminaux, on note un transfert d'impact aux phases pour lesquelles les données sont moins fiables : l'extraction des matières premières non renouvelables, le traitement de fin de vie et l'usage d'internet.

HUGUES FERREBOEUF

*Chef de projet et co-auteur du rapport « Lean ICT : Pour une sobriété numérique » - **The Shift Project***

NUMÉRIQUE ET ENVIRONNEMENT : UNE ARDENTE OBLIGATION DE CONGRUENCE

La transition numérique en cours se double d'une envolée de l'empreinte carbone des services, terminaux et infrastructures qui la rendent possible, sans pour autant concrétiser pour l'instant les espoirs d'accélération de la décarbonation des secteurs sur lesquels elle porte, ce qui est très préoccupant.

Les raisons principales de cette situation ne sont pas technologiques mais systémiques[1] et y remédier implique de faire évoluer vers plus de sobriété les pratiques des consommateurs et des offreurs, significativement et rapidement, face à l'urgence environnementale. De tels changements ne pourront se produire au rythme et avec l'amplitude nécessaires que s'ils sont facilités, voire provoqués, par une régulation adaptée.

The Shift Project considère donc l'implication de l'Arcep sur ce sujet comme non seulement bienvenue mais totalement nécessaire, au titre de la mobilisation de son expertise sectorielle pour éclairer des choix politiques et en tant que maître d'œuvre des mécanismes de régulation.

Afin de garantir une efficacité à la mesure des enjeux, il sera essentiel d'établir une cohérence forte entre les choix découlant de la prise en compte de la contrainte environnementale et ceux effectués en référence à d'autres principes (neutralité d'internet…) ou à l'occasion du déploiement de nouvelles technologies (5G, IoT).

Enfin, compte tenu de l'existence du duopole américano-chinois dans le secteur, il est évidemment indispensable que des leviers d'action similaires soient définis et mis en œuvre à l'échelle européenne, ce qui passe par une sensibilisation et une mobilisation des régulateurs.

1. Rapport « Lean ICT : Pour une sobriété numérique », The Shift Project, 2018

Lexique

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

A

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).

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.

Anycast : technique d'adressage et de routage permettant de rediriger les données vers la mire de test la plus proche.

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 au travers duquel un logiciel offre des services à d'autres logiciels.

ARN (Autorité de Régulation Nationale) : organisme chargé par un État membre du BEREC de la régulation des communications électroniques.

AS (*Autonomous System*) : ensemble de réseaux IP intégrés à internet et sous le contrôle d'une seule entité, par exemple un fournisseur d'accès à internet.

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-sept États membres de l'Union européenne.

BGP *(Border Gateway Protocol):* protocole d'échange de route utilisé notamment sur le réseau internet.

***Buffer* :** mémoire-tampon, zone de mémoire virtuelle ou de disque dur d'un ordinateur utilisée pour stocker temporairement des données.

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 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.

CPU (*Central Processing Unit*) : processeur ou microprocesseur d'un ordinateur, chargé de l'exécution des instructions des programmes.

***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 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 internet, comme lors du visionnage d'une vidéo en ligne ou du chargement d'une page web : on parle de débit descendant.

DHCP *(Dynamic Host Configuration Protocol):* protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une machine.

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

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

DWDM *(Dense Wavelength Division Multiplexing):* multiplexage en longueur d'onde permettant de faire circuler plusieurs signaux sur une seule fibre.

E

EDPB (*European Data Protection Board*) : organe européen indépendant dont les objectifs sont de garantir l'application cohérente du RGPD et de promouvoir la coopération entre les autorités de protection des données de l'Union européenne.

[câble] Ethernet : nom usuel du connecteur RJ45 supportant le protocole de communication de paquets Ethernet.

EVPN *(Ethernet VPN)* : technologie pour transporter le trafic Ethernet de couche 2 en tant que réseau privé virtuel utilisant des protocoles de réseau étendu.

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.

***Firewall* :** pare-feu, il s'agit d'un dispositif matériel ou logiciel de sécurité qui permet de filtrer et de bloquer les flux en fonction de la politique de sécurité en place.

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, ordinateur et box TV.

ICMP *(Internet Control Message Protocol)* : 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.

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 activé : qui émet et reçoit effectivement du trafic en IPv6, soit grâce à une activation de la part du client, soit grâce ou une activation effectuée par l'opérateur.

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 *via* 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).

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.

Mires 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.

MPLS *(MultiProtocol Label Switching)*: mécanisme de transport de données basé sur la commutation de labels, qui sont insérés à l'entrée du réseau MPLS et retirés à sa sortie.

N

NAP (*Network Access Point*) : point d'interconnexion offrant une place de marché dans laquelle les utilisateurs peuvent vendre et/ou acheter de la capacité de trafic à d'autres acteurs présents.

NAS *(Network Attached Storage)*: serveur de stockage de fichiers, autonome et relié à un réseau.

NAT *(Network Adress Translation)*: mécanisme de traduction d'adresses réseau permettant de faire correspondre des adresses IP à d'autres adresses IP, notamment utilisé pour limiter le nombre d'IPv4 publiques utilisées.

O

OS (*Operating System*) : système d'exploitation. Logiciel qui permet de faire fonctionner un périphérique, comme Windows, macOS, 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.

Point de terminaison du réseau : le point physique auquel un utilisateur obtient l'accès à un réseau de communications électroniques public.

POP (*Point of Presence*) : point de présence physique d'un opérateur.

Port logiciel : à chaque connexion sur internet émanant d'une application est associée à une session UDP ou TCP, elle–même identifiée au moyen d'un « numéro de port », c'est-à-dire une adresse codée sur 16 bits.

Puce NFC (*Near-Field Communication*) : technologie de communication sans fil à courte portée et à haute fréquence, permettant l'échange d'informations entre des périphériques jusqu'à une distance d'environ 10 cm dans le cas général.

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

RFC (*Requests For Comments*) : documents officiels décrivant les aspects et spécifications techniques d'internet ou de différents matériels informatiques.

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.

RPKI (*Resource Public Key Infrastructure*) : infrastructure à clés publiques conçue pour sécuriser l'infrastructure de routage d'internet.

S

***Sandbox* :** mécanisme de sécurité informatique se basant sur l'isolation de composants logiciels.

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

Service spécialisé : service(s) de communications électroniques distinct(s) des services d'accès à l'internet qui nécessite(nt) des niveaux de qualité spécifiques.

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

SIEM *(Security Information and Event Management) :* Système de gestion des événements de sécurité informatique.

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.

***Shutdown* :** perturbation(s) intentionnelle(s) des communications électroniques en les rendant inaccessibles ou indisponibles, pour une population et/ou à un emplacement spécifique (par exemple au niveau national ou local).

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)* : 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) : 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 2019, 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.

V

VoLTE *(Voice over TLE) :* principale technique de transport de la voix sur les réseaux de téléphonique mobile 4G LTE.

VLAN (*Virtual Local Area Network*) : réseau local virtuel regroupant un ensemble de machines de façon logique et non physique. Ce concept permet de créer plusieurs réseaux indépendants ne pouvant pas, par défaut, communiquer entre eux.

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

VXLAN (*Virtual eXtensible Local Area Network*) : technologie de virtualisation réseau ayant des fonctionnalités semblables au VLAN et qui encapsule une trame Ethernet dans un datagramme UDP, dans le but d'isoler un plus grand nombre de machines virtuelles.

W

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

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 : quatrième génération des standards pour la téléphonie mobile. Elle est définie par les normes *release 8* du 3GPP.

5G : cinquième génération des standards pour la téléphonie mobile. Elle est définie par les normes *release 15* du 3GPP.

Annexes

ANNEXE 1

Paramètres communiqués par l'API pour caractériser l'environnement utilisateur

Les paramètres ci-dessous sont extraits de la décision adoptée par l'Arcep fin octobre 2019[1] et dont l'arrêté d'homologation a été publié au *Journal Officiel* le 16 janvier 2020.

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
Facultatif	Gateway	Model		Nom de l'IAD (« box ») du client	texte
Facultatif	Gateway	SoftwareVersion		Version du logiciel	texte
Obligatoire lorsque défini et existant	SubscriptionSpeed	DownloadMin	Kbit/s	Débit minimum descendant contractuel	Entier positif de 64 bits
Obligatoire lorsque défini et existant	SubscriptionSpeed	UploadMin	Kbit/s	Débit minimum montant contractuel	Entier positif de 64 bits
Obligatoire	SubscriptionSpeed	DownloadMax	Kbit/s	Débit maximum descendant contractuel	Entier positif de 64 bits
Obligatoire	SubscriptionSpeed	UploadMax	Kbit/s	Débit maximum montant contractuel	Entier positif de 64 bits
Obligatoire lorsque défini et existant	SubscriptionSpeed	DownloadNormally	Kbit/s	Débit « normalement disponible » descendant contractuel (s'il existe)	Entier positif de 64 bits
Obligatoire lorsque défini et existant	SubscriptionSpeed	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»;»other»]
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
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		Technologie WAN secondaire active « *no* » : absence d'agrégation ou agrégation non activée.	[«no»;»ftth»;»adsl»;«vdsl»; »gfast»;»cable»;»satellite»; »2g»;»3g»;»4g»;»5g»;»other»]

Note : le « débit maximum » est à remplir systématiquement avec les technologies WAN FttH, câble et satellite avec le débit contractuel. Pour les autres technologies WAN, il n'est à remplir que si l'accès possède un débit maximum.

1. https://www.arcep.fr/uploads/tx_gsavis/19-1410.pdf

Condition de présence	Arbre JSON	Nom du paramètre	Unité	Détail du paramètre	Format / liste de valeurs acceptées
Obligatoire	Lan	ConnectionType		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	DownloadMax	Kbit/s	Débit maximal théorique de l'interface. Ethernet/CPL : capacité du port Ethernet coté box d'où provient la requête de l'API. Wi-Fi : débit maximum théorique proposé par le Wi-Fi de la box.	Entier positif de 64 bits
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	UploadMax		Débit maximal théorique de l'interface. Ethernet/CPL : capacité du port Ethernet coté box d'où provient la requête de l'API. Wi-Fi : débit maximum théorique proposé par le Wi-Fi de la box.	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/Wifi	IeeeMax		Norme Wi-Fi IEEE 802.11 la plus élevée, supportée par la box.	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/Wifi	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/Wifi	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/Wifi	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
Facultatif	Miscellaneous	Other[1…n]		Autres paramètres que l'opérateur souhaite transmettre aux outils de mesure.	

Note : certains adaptateurs CPL[2] 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.

2. 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 ait lancé le test de mesure de la qualité de service internet ;
- immédiatement après que l'outil de mesure ait 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.

Optionnellement, un compteur pour le *cross-traffic* LAN peut être mis en place. Il permet de détecter la présence de *cross-traffic* ayant un impact côté LAN.

Condition de présence	Arbre JSON	Nom du paramètre	Unité	Détail du paramètre	Format / liste de valeurs acceptées
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
Obligatoire	Wan/ByteCounter	Download	Octets	Relevé du compteur de trafic descendant (internet => IAD) du port WAN	Entier positif de 64 bits
Obligatoire	Wan/ByteCounter	Upload	Octets	Relevé du compteur de trafic montant (IAD => internet) du port WAN	Entier positif de 64 bits
Facultatif	Lan/ByteCounter	Download	Octets	Relevé du compteur de trafic descendant (IAD => Terminal utilisateur) du port LAN	Entier positif de 64 bits
Facultatif	Lan/ByteCounter	Upload	Octets	Relevé du compteur de trafic montant (Terminal utilisateur => IAD) du port LAN	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 ou LAN, il conviendra d'utiliser le compteur de paquets multiplié par la MTU (*Maximum Transmission Unit*) afin de fournir une approximation.

Si le trafic « hors internet » (essentiellement le trafic TV/VoD) est à l'extérieur du débit internet, avec une bande passante dédiée, alors les compteurs de *cross-traffic* ne remontent que les octets liés au trafic internet.

Si le trafic « hors internet » impacte le débit maximum sur internet, ce qui correspond à une enveloppe globale utilisée pour l'un ou l'autre, alors les compteurs de *cross-traffic* remontent les octets sur le port WAN, en incluant le trafic TV/VoD.

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.

1. NPERF

Sponsor, tel qu'affiché sur nPerf	Ville	Région	IPv6 (web, application windows)	IPv6 (application Android / iOS)	Capacité de la connexion affichée	Port utilisé	Nom de l'hébergeur	AS
RRT	Compiègne	Hauts-de-France	IPv4 uniquement	IPv4 uniquement	10 Gbit/s	443	Renater	AS2200
Orange	Paris	Île-de-France	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Orange	AS3215
Orange	Puteaux	Île-de-France	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Orange	AS3215
Orange	Rennes	Bretagne	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Orange	AS3215
Orange	Lille	Hauts-de-France	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Orange	AS3215
Orange	Strasbourg	Grand-Est	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Orange	AS3215
Orange	Lyon	Auvergne-Rhône-Alpes	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Orange	AS3215
Orange	Marseille	Région Sud	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Orange	AS3215
Orange	Bordeaux	Nouvelle-Aquitaine	IPv4 ou IPv6	IPv4 uniquement	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	IPv4 uniquement	10 Gbit/s	443	Bouygues Telecom	AS5410
Bouygues Telecom	Paris	Île-de-France	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Bouygues Telecom	AS5410
Bouygues Telecom	Lille	Hauts-de-France	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Bouygues Telecom	AS5410
Bouygues Telecom	Lyon	Auvergne-Rhône-Alpes	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Bouygues Telecom	AS5410
Bouygues Telecom	Marseille	Région Sud	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Bouygues Telecom	AS5410
Bouygues Telecom	Bordeaux	Nouvelle-Aquitaine	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	Bouygues Telecom	AS5410

Sponsor, tel qu'affiché sur nPerf	Ville	Région	IPv6 (web, application windows)	IPv6 (application Android / iOS)	Capacité de la connexion affichée	Port utilisé	Nom de l'hébergeur	AS
Phibee Telecom	Aubervilliers	Île-de-France	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	8443	Phibee Telecom	AS8487
Online	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	IPv4 uniquement	4 Gbit/s	443	Scaleway – Online	AS12876
Wangarden	Pontoise	Île-de-France	IPv4 uniquement	IPv4 uniquement	1 Gbit/s	443	Scaleway – Online	AS12876
SFR	*Anycast*	Île-de-France (Courbevoie) Auvergne-Rhône-Alpes (Vénissieux)	IPv4 uniquement	IPv4 uniquement	10 Gbit/s	443	SFR	AS15557
SFR	Courbevoie	Île-de-France	IPv4 uniquement	IPv4 uniquement	10 Gbit/s	443	SFR	AS15557
SFR	Vénissieux	Auvergne-Rhône-Alpes	IPv4 uniquement	IPv4 uniquement	10 Gbit/s	443	SFR	AS15557
OVH	Gravelines	Hauts-de-France	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	OVH	AS16276
OVH	Roubaix	Hauts-de-France	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	OVH	AS16276
OVH	Strasbourg	Grand-Est	IPv4 ou IPv6	IPv4 uniquement	10 Gbit/s	443	OVH	AS16276
Axialys	Courbevoie	Île-de-France	IPv4 uniquement	IPv4 uniquement	1 Gbit/s	443	Axialys	AS16363
Corexpert	Paris	Île-de-France	IPv4 uniquement	IPv4 uniquement	5 Gbit/s	443	Amazon AWS	AS16509
Ikoula	Reims	Grand-Est	IPv4 ou IPv6	IPv4 uniquement	1 Gbit/s	8443	Ikoula	AS21409
Eurafibre	Douai	Hauts-de-France	IPv4 uniquement	IPv4 uniquement	20 Gbit/s	8443	Eurafibre	AS35625
Videofutur	Paris	Île-de-France	IPv4 uniquement	IPv4 uniquement	10 Gbit/s	443	Reunicable	AS37002
CMIN	Lucé	Centre-Val de Loire	IPv4 uniquement	IPv4 uniquement	1 Gbit/s	443	CMIN	AS39271
SHPV France	Toulouse	Occitanie	IPv4 ou IPv6	IPv4 uniquement	4 Gbit/s	443	SHPV France	AS41652
Proceau	Paris	Île-de-France	IPv4 uniquement	IPv4 uniquement	1 Gbit/s	8443	Proceau	AS43424
Alsatis	Paris	Île-de-France	IPv4 uniquement	IPv4 uniquement	10 Gbit/s	443	Alsatis	AS48072
Muona	Lyon	Auvergne-Rhône-Alpes	IPv4 uniquement	IPv4 uniquement	1 Gbit/s	443	Muona	AS50818
Metro Optic	Paris	Île-de-France	IPv4 uniquement	IPv4 uniquement	1 Gbit/s	443	Metro Optic	AS57902
DataPacket	Paris	Île-de-France	IPv4 uniquement	IPv4 uniquement	10 Gbit/s	443	DataCamp	AS60068
System-Net	Montpellier	Occitanie	IPv4 uniquement	IPv4 uniquement	1 Gbit/s	443	System-Net	AS60427
Rezopole	Lyon	Auvergne-Rhône-Alpes	IPv4 ou IPv6	IPv4 uniquement	1 Gbit/s	443	Rezopole	AS199422
AOC Telecom	Clermont-Ferrand	Auvergne-Rhône-Alpes	IPv4 uniquement	IPv4 uniquement	200 Mbit/s	443	AOC Telecom	AS202328
Neyrial	Cébazat	Auvergne-Rhône-Alpes	IPv4 uniquement	IPv4 uniquement	1 Gbit/s	443	Neyrial informatique	AS203352
Telicity	Bordeaux	Nouvelle-Aquitaine	IPv4 uniquement	IPv4 uniquement	10 Gbit/s	443	Telicity	AS204355
Alpesys	Grenoble	Auvergne-Rhône-Alpes	IPv4 uniquement	IPv4 uniquement	10 Gbit/s	8443	Alpesys	AS206120
Azylis	Besançon	Bourgogne-Franche-Comté	IPv4 uniquement	IPv4 uniquement	1 Gbit/s	443	Azylis	AS207151

2. SPEEDTEST UFC-QUE CHOISIR

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

3. LES TESTS DE DÉBIT FIXE DÉVELOPPÉS PAR QOSI (5GMARK / DÉBITEST 60 / NETGMARK ZD-NET)

Nom de domaine	Ville	Région	IPv6	Capacité de la connexion	Port utilisé	Nom de l'hébergeur	AS
dedi3.5gmark.com	Saint-Ouen-l'Aumône	Île-de-France	IPv4 uniquement	1 Gbit/s	8443	Scaleway – Online	AS12876
dedi5.5gmark.com	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	2,5 Gbit/s	8443	Scaleway – Online	AS12876
dedi6.5gmark.com	Saint-Ouen-l'Aumône	Île-de-France	IPv4 uniquement	1 Gbit/s	8443	Scaleway – Online	AS12876
paris.4gmark.com	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	400 Mbit/s	8443	Scaleway – Online	AS12876
paris2.4gmark.com	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	400 Mbit/s	8443	Scaleway – Online	AS12876
paris3.4gmark.com	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	400 Mbit/s	8443	Scaleway – Online	AS12876

4. LES TESTS DE DÉBIT MOBILE DÉVELOPPÉS PAR QOSI (5GMARK / BECOVER+ / DÉBITEST 60 / GIGALIS / KICAPTE / QOSBEE / TU CAPTES ? / RÉSOMÈTRE)

Sponsor, tel qu'affiché sur l'application	Ville	Région	IPv6	Capacité de la connexion supposée	Port utilisé	Nom de l'hébergeur	AS
Bouygues Telecom	Nanterre	Île-de-France	IPv6 uniquement*	10 Gbit/s	443	Bouygues Telecom	AS540
Orange Montsouris	Paris	Île-de-France	IPv6 uniquement*	10 Gbit/s	443	Orange	AS3215
Orange Lyon	Lyon	Auvergne-Rhône-Alpes	IPv6 uniquement*	10 Gbit/s	443	Orange	AS3215
Azure Network	Paris / Marseille	Île-de-France / Région Sud	IPv6 uniquement*	600 Mbit/s	443	Microsoft Corporation	AS8068
OneProvider Paris	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	400 Mbit/s	443	Scaleway – Online	AS12876
OneProvider Paris2	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	400 Mbit/s	443	Scaleway – Online	AS12876
Dedibox Paris3	Saint-Ouen-l'Aumône	Île-de-France	IPv4 uniquement	1 Gbit/s	443	Scaleway – Online	AS12876
SFR	Courbevoie	Île-de-France	IPv4 uniquement	10 Gbit/s	80	SFR	AS15557
OVH 5GMARK	Roubaix	Hauts-de-France	IPv4 uniquement	1 Gbit/s	443	OVH	AS16276
QoSi.eu	Roubaix	Hauts-de-France	IPv6 uniquement*	1 Gbit/s	443	OVH	AS16276
AWS	Paris	Île-de-France	IPv6 uniquement*	1 Gbit/s	443	Amazon Web Services	AS16509
Azure Akamai	multiples localisations	multiples localisations	IPv6 uniquement*	1 ou 10 Gbit/s**	443	Akamai International	AS20940
Ikoula	Reims	Grand-Est	IPv6 uniquement*	1 Gbit/s	443	Ikoula	AS21409
Adeli	Saint-Trivier-sur-Moignans	Auvergne-Rhône-Alpes	IPv6 uniquement*	1 Gbit/s	443	Adeli	AS43142
Mediactive Network	Paris	Île-de-France	IPv6 uniquement*	10 Gbit/s	80	Mediactive Network	AS197133

* 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.

** En fonction de la solution de diffusion de contenu Akamai utilisée.

5. IPv6-TEST

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 uniquement	ZeelandNet	AS15542
ServerHouse	Portsmouth	Royaume-Uni	IPv4 et IPv6	1 Gbit/s	80 uniquement	Server House	AS21472
EBOX	Longueuil	Canada	IPv4 et IPv6	1 Gbit/s	80 uniquement	EBOX	AS174

6. SPEEDTEST.NET D'OOKLA

Sponsor, tel qu'affiché sur Speedtest	Ville	Région	IPv6	Capacité de la connexion descendante**	Capacité de la connexion montante**	Port utilisé	Nom de l'hébergeur	AS	ID***
fdcservers.net	Paris	Île-de-France	IPv4 uniquement	2 Gbit/s	10 Gbit/s ou +	8080	Cogent	AS174	6027
Orange	Lyon	Auvergne-Rhône-Alpes	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Orange	AS3215	24394
Orange	Rennes	Bretagne	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Orange	AS3215	23282
Orange	Strasbourg	Grand-Est	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Orange	AS3215	29543
Orange	Lille	Hauts-de-France	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Orange	AS3215	29544
Orange	Puteaux	Île-de-France	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Orange	AS3215	23884
Orange	Paris	Île-de-France	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Orange	AS3215	24215
Orange	Bordeaux	Nouvelle-Aquitaine	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Orange	AS3215	29542
Orange	Marseille	Région Sud	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Orange	AS3215	29545
GTT.net	Paris	Île-de-France	IPv4 uniquement	4 Gbit/s	2 Gbit/s	8080	GTT	AS3257	24386
LaFibre.info	Lyon	Auvergne-Rhône-Alpes	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Bouygues Telecom	AS5410	2023
LaFibre.info	Douai	Hauts-de-France	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Bouygues Telecom	AS5410	4010
TestDebit.info	Massy	Île-de-France	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Bouygues Telecom	AS5410	2231
LaFibre.info	Bordeaux	Nouvelle-Aquitaine	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Bouygues Telecom	AS5410	21415
TestDebit.info	Marseille	Région Sud	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Bouygues Telecom	AS5410	4036
Sewan	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s ou +	10 Gbit/s ou +	8080	Sewan	AS8399	24130
Vialis	Colmar	Grand-Est	IPv4 uniquement	6 Gbit/s	4 Gbit/s	8080	Vialis	AS12727	24059
ONLINE	Vitry-sur-Seine	Île-de-France	IPv4 uniquement	10 Gbit/s ou +	10 Gbit/s ou +	8080	Scaleway – Online	AS12876	5022
Sirius Media Group	Paris	Île-de-France	IPv4 uniquement	2,5 Gbit/s	2,5 Gbit/s	8080	Scaleway – Online	AS12876	10676
DFOX	Nice	Région Sud	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Scaleway – Online	AS12876	8195
CCleaner	Paris	Île-de-France	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Scaleway – Online	AS12876	16676
SFR	Lyon	Auvergne-Rhône-Alpes	IPv4 uniquement	10 Gbit/s ou +	10 Gbit/s	8080	SFR	AS15557	27852
SFR	Vénissieux	Auvergne-Rhône-Alpes	IPv4 uniquement	10 Gbit/s ou +	5 Gbit/s	8080	SFR	AS15557	30993
SFR	Trappes	Île-de-France	IPv4 uniquement	10 Gbit/s ou +	10 Gbit/s ou +	8080	SFR	AS15557	31993

* 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.

** Capacité de connexion supposée sur internet, hors du réseau de l'opérateur.

*** L'ID est utilisé pour sélectionner le serveur avec l'application en ligne de commande Speedtest CLI.

Sponsor, tel qu'affiché sur Speedtest	Ville	Région	IPv6	Capacité de la connexion descendante**	Capacité de la connexion montante**	Port utilisé	Nom de l'hébergeur	AS	ID***
SFR	Mitry	Île-de-France	IPv4 uniquement	10 Gbit/s ou +	10 Gbit/s ou +	8080	SFR	AS15557	27984
SFR	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s	4 Gbit/s	8080	SFR	AS15557	12746
SFR	Bordeaux	Nouvelle-Aquitaine	IPv4 uniquement	10 Gbit/s ou +	5 Gbit/s	8080	SFR	AS15557	32438
Stella Telecom	Paris	Île-de-France	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Stella Telecom	AS16211	26387
Stella Telecom	Courbevoie	Île-de-France	IPv4 uniquement	1 Gbit/s	200 Mbit/s	8080	Stella Telecom	AS16211	14821
Rocho DataCenter	Chambéry	Auvergne-Rhône-Alpes	IPv6 uniquement*	1 Gbit/s	1 Gbit/s	8080	OVH	AS16276	11457
OVH Cloud	Gravelines	Hauts-de-France	IPv6 uniquement*	3 Gbit/s	10 Gbit/s ou +	8080	OVH	AS16276	25985
ITDATA Telecom	Roubaix	Hauts-de-France	IPv4 uniquement	500 Mbit/s	600 Mbit/s	8080	OVH	AS16276	29243
StreamRadio	Roubaix	Hauts-de-France	IPv4 uniquement	200 Mbit/s	200 Mbit/s	8080	OVH	AS16276	32230
Ikoula	Reims	Grand-Est	IPv6 uniquement*	1 Gbit/s	1 Gbit/s	8080	Ikoula	AS21409	5813
Axione	Paris	Île-de-France	IPv4 uniquement	1 Gbit/s	4 Gbit/s	8080	Axione	AS31167	28308
Keyyo	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s ou +	2 Gbit/s	8080	Keyyo	AS34659	27961
Hexanet	Reims	Grand-Est	IPv4 uniquement	5 Gbit/s	5 Gbit/s	8080	Hexanet	AS34863	17225
Networth Telecom	Clichy	Île-de-France	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Networth Telecom	AS35283	28073
Eurafibre	Lille	Hauts-de-France	IPv4 uniquement	1 Gbit/s	10 Gbit/s ou +	8080	Eurafibre	AS35625	16913
FullSave	Toulouse	Occitanie	IPv6 uniquement*	10 Gbit/s	3 Gbit/s	8080	FullSave	AS39405	29032
Orne THD	Rombas	Grand-Est	IPv6 uniquement*	2 Gbit/s	1 Gbit/s	8080	Orne THD	AS41114	17349
Enes Hag	Hagondange	Grand-Est	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	31081
Regivision	Nilvange	Grand-Est	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	31082
Enes	Hombourg-Haut	Grand-Est	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	21268
Fibragglo	Forbach	Grand-Est	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	16232
RIV54	Saulnes	Grand-Est	IPv4 uniquement	1 Gbit/s	700 Mbit/s	8080	Vialis	AS42487	14372
Regie Talange	Talange	Grand-Est	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	16876
REFO Falck	Falck	Grand-Est	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Vialis	AS42487	21216

Sponsor, tel qu'affiché sur Speedtest	Ville	Région	IPv6	Capacité de la connexion descendante**	Capacité de la connexion montante**	Port utilisé	Nom de l'hébergeur	AS	ID***
Vialis	Woippy	Grand-Est	IPv4 uniquement	1 Gbit/s	200 Mbit/s	8080	Vialis	AS42487	13661
Via Numérica	Archamps	Auvergne-Rhône-Alpes	IPv4 uniquement	10 Gbit/s ou +	2 Gbit/s	8080	Via Numérica	AS44494	3596
Naitways	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s ou +	10 Gbit/s ou +	8080	Naitways	AS57119	16476
ColocationIX 10G	Paris	Île-de-France	IPv4 uniquement	10 Gbit/s ou +	5 Gbit/s	8080	ColocationIX	AS61955	28994
HarryLafranc	Paris	Île-de-France	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	Netrix	AS62000	10176
Mediactive	Paris	Île-de-France	IPv6 uniquement*	10 Gbit/s ou +	10 Gbit/s ou +	8080	Mediactive	AS197133	31895
iBlooPro	Rennes	Bretagne	IPv4 uniquement	10 Gbit/s ou +	1 Gbit/s	8080	Blue Infra	AS201808	31656
Enes	Creutzwald	Grand-Est	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	ENES Creutzwald	AS204645	24052
Telerys	Paris	Île-de-France	IPv6 uniquement*	10 Gbit/s ou +	3 Gbit/s	8080	Telerys	AS205344	31725
Alpesys	Grenoble	Auvergne-Rhône-Alpes	IPv4 uniquement	1 Gbit/s	700 Mbit/s	8080	Alpesys	AS206120	25041
AS208196	Paris	Île-de-France	IPv6 uniquement*	1 Gbit/s	10 Gbit/s ou +	8080	Dorian GALIANA	AS208196	32367
Tubeo	Bitche	Grand-Est	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	CC Pays de Bitche	AS208574	31083
La Regie	Reichshoffen	Grand-Est	IPv4 uniquement	1 Gbit/s	1 Gbit/s	8080	La Regie Reichshoffen	AS208719	14043

Ce document a été réalisé par l'Arcep

Jean Cattan, conseiller du Président
Cécile Dubarry, directrice générale

DIRECTION « INTERNET, PRESSE, POSTES ET UTILISATEURS »

Loïc Duflot, directeur

Unité « Internet ouvert »

Aurore Tual, *cheffe de l'unité*
Samih Souissi, *adjoint à la cheffe d'unité*
Vivien Guéant et Emmanuel Leroux, *chargés de mission*

Unité « Régulation par la donnée »

Pierre Dubreuil, *chef de l'unité*

Unité « Opérateurs et obligations légales »

David Epelbaum, *chef d'unité*
Hélène Bartyzel, *chargée de mission*

DIRECTION « ÉCONOMIE, MARCHÉS ET NUMÉRIQUE »

Stéphane Lhermitte, *directeur*
Laurent Toustou, *conseiller auprès du directeur*

Unité « Analyse économique et intelligence numérique »

Anaïs Aubert, *adjointe à la cheffe d'unité*
Chiara Caccinelli, Arthur Dozias, Adrien Haïdar et Nisrynne Nahhal, *chargés de mission*

DIRECTION « MOBILE ET INNOVATION »

Anne Laurent, *directrice*
Maxime Forest, *directeur adjoint*

Unité « Couverture et investissements mobiles »

Guillaume Decorzent, *chef de l'unité*
Audrey Goffi et Corentin Golly, *chargés de missions*

DIRECTION « COMMUNICATION ET PARTENARIATS »

Clémentine Beaumont, *directrice*
Anne-Lise Lucas, *chargée de mission*

DIRECTION « AFFAIRES JURIDIQUES »

Elisabeth Suel, *directrice*

Unité « Marché mobile et ressources rares »

Aurore Martinat, *cheffe de l'unité*
Annabel Gandar, *adjointe à la cheffe de l'unité*

Unité « Infrastructures et réseaux ouverts »

Rémy Maecker, *adjoint à la cheffe d'unité*
Théotime Gélineau, *chargé 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 la task-force IPv6 pour leur dynamisme et leur contribution précieuse au présent rapport.

Publication
Arcep
14, rue Gerty Archimède - 75012 Paris
Direction de la communication
et des partenariats : com@arcep.fr

Design
Agence Luciole

Crédits photos
p. 20, 30 et 79 : Adobe Stock,
p. 53 : Ikoula

Juin 2020

LE MANIFESTE
L'ARCEP, LES RÉSEAUX COMME BIEN COMMUN

Les réseaux d'échanges internet, télécoms 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.