arcep
autorité de régulation
des communications électroniques
et des postes

RÉPUBLIQUE FRANCAISE

CONSULTATION PUBLIQUE

Du 23 avril au 27 mai 2019

Projet de décision relative à la caractérisation de l'environnement utilisateur dans les mesures de qualité de service d'internet fixe via la mise en place d'une interface de programmation applicative (API) dans les box

Date de publication 23 avril 2019

ISSN n°2258-3106

Avertissement sur la mise en consultation

L'Autorité de régulation des communications électroniques et des postes (Arcep) met en consultation publique un projet de décision relative à la caractérisation de l'environnement utilisateur dans les mesures de qualité de service d'internet fixe via la mise en place d'une interface de programmation applicative (API) dans les box.

L'avis des acteurs du secteur est sollicité sur l'ensemble du présent document et les commentaires doivent être transmis à l'Arcep, de préférence par e-mail à l'adresse qos-internet-fixe@arcep.fr au plus tard le 27 mai 2019. À défaut, ils peuvent être transmis par courrier à l'adresse suivante :

Réponse à la consultation publique sur la mise en place d'une API dans les box
À l'attention de la Direction Internet et Utilisateurs
Autorité de régulation des communications électroniques et des postes
CS 90410
75613 PARIS CEDEX 12

Les acteurs du secteur sont invités à répondre aux questions qui figurent dans ce document de consultation publique mais aussi, plus globalement, à fournir tout élément d'analyse qu'ils estimeraient pertinents à devoir porter à la connaissance de l'Autorité.

L'Arcep, dans un souci de transparence, publiera l'intégralité des commentaires qui lui auront été transmis, à l'exclusion des parties couvertes par le secret des affaires. À cette fin, les contributeurs sont invités à reporter dans une annexe spécialement identifiée les éléments qu'ils considèrent devoir être couverts par le secret des affaires. Toujours dans un souci de transparence, les contributeurs sont invités à limiter autant que possible les passages couverts par le secret des affaires.

L'Autorité pourra déclasser d'office des éléments d'information qui, par leur nature, ne relèvent pas du secret des affaires.

Ce document est disponible en téléchargement sur le site : https://www.arcep.fr

1 Contexte

1.1 Cadre juridique

L'article L. 32-1 du CPCE dispose notamment que :

> « *II. – Dans le cadre de leurs attributions respectives, le ministre chargé des communications électroniques et l'Autorité de régulation des communications électroniques et des postes prennent, dans des conditions objectives et transparentes, des mesures raisonnables et proportionnées en vue d'atteindre les objectifs suivants :* […]
>
> *3° Le développement de l'investissement, de l'innovation et de la compétitivité dans le secteur des communications électroniques ;*
>
> *III. – Dans le cadre de ses attributions et, le cas échéant, conjointement avec le ministre chargé des communications électroniques, l'Autorité de régulation des communications électroniques et des postes prend, dans des conditions objectives et transparentes, des mesures raisonnables et proportionnées en vue d'atteindre les objectifs suivants :* […]
>
> *« 6° La capacité des utilisateurs finals à accéder à l'information et à la diffuser ainsi qu'à accéder aux applications et aux services de leur choix. ».*

L'article L. 36-6 du CPCE dispose que :

> *« Dans le respect des dispositions du présent code et de ses règlements d'application […], l'Autorité de régulation des communications électroniques et des postes précise les règles concernant :* […]
>
> *1° Les droits et obligations afférents à l'exploitation des différentes catégories de réseaux et de services, en application de l'article L. 33-1 ;* […]
>
> *7° Les contenus et les modalités de mise à disposition du public d'informations fiables et comparables relatives à la disponibilité, à la qualité et à la couverture des réseaux et des services de communications électroniques et la détermination des indicateurs et méthodes employées pour les mesurer.* […]
>
> *Les décisions prises en application du présent article sont, après homologation par arrêté du ministre chargé des communications électroniques, publiées au Journal Officiel. »*

L'article L. 33-1, I du CPCE prévoit quant à lui que :

« L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles portant sur :

a) Les conditions de permanence, de qualité, de disponibilité, de sécurité et d'intégrité du réseau et du service qui incluent des obligations de notification à l'autorité compétente des atteintes à la sécurité ou à l'intégrité des réseaux et services ; […]

n) L'information des utilisateurs, dans la mesure où cette information est nécessaire à la mise en œuvre des dispositions du présent code ou des décisions prises en application de celui-ci ; […]*».*

1.2 Objectifs de la décision

La présente décision concerne le processus de mise à disposition d'informations fiables et comparables dans l'objectif d'améliorer la mesure de la qualité de service des réseaux fixes en France.

En effet, les différents travaux de l'Arcep sur la qualité de service des réseaux fixes témoignent de la complexité de la mesure de cette qualité de service dans ce type de réseaux : techniquement, il est à ce jour impossible pour un outil web proposant des tests de mesure de la qualité de service internet de connaître avec certitude la technologie d'accès (cuivre, câble, fibre, etc.) sur laquelle a été réalisée une mesure de la qualité de service internet. Ce manque de caractérisation de la mesure rend les données difficilement exploitables, voire, dans certains cas, peut induire en erreur le consommateur.

L'Arcep a lancé en 2018 un vaste chantier en collaboration avec une vingtaine d'acteurs dont des outils de mesure de la qualité de service internet, des opérateurs et des acteurs académiques afin de résoudre ce problème majeur. En décembre 2018, l'Arcep a annoncé que, à l'issue d'une série de groupes de travail, l'écosystème avait convergé vers la mise en place d'une interface de programmation applicative (API) implémentée directement dans la box des opérateurs.

L'objet de la présente décision est de définir les conditions d'implémentation de cette interface de programmation applicative (API). L'API est une interface logicielle implémentée dans la box permettant la transmission, au moment de l'exécution d'une mesure de la qualité de service internet par le client d'un accès xDSL, câble ou FTTH ainsi que les box d'accès fixe supportant la technologie 5G, des informations qui constituent la « carte d'identité de l'accès », telles que la technologie d'accès, le débit souscrit par le consommateur, ou la qualité du Wi-Fi. L'API permet ainsi de **caractériser l'environnement utilisateur** sur un accès xDSL, câble ou FTTH, sans dégrader l'expérience utilisateur du client du test de mesure quel qu'il soit (testeur web, sonde matérielle, agent dans la box, logiciel installable sur le terminal, etc.).

Afin de garantir le caractère raisonnable et proportionné du dispositif, seul les opérateurs visés par la présente décision sont tenus d'intégrer une telle API dans leurs box.

1.3 Périmètre de la décision

Sont soumis à la présente décision les opérateurs au sens de l'article L. 32 (15°) du CPCE disposant, directement ou à travers des sociétés qu'ils contrôlent ou qui les contrôlent au sens de l'article L. 233-3 du code de commerce, d'un nombre d'abonnements actifs supérieur à 1 000 000 clients, sur les marchés de détail grand public fixe.

Est considéré comme un abonnement actif tout abonnement souscrit par un client sur une ligne activée, c'est-à-dire une ligne sur laquelle le client peut accéder au service.

Les opérateurs de moins de 1 000 000 clients peuvent mettre en place l'API de manière facultative.

Les modèles de box concernés par la mise en place de l'API sont ceux mis à disposition sur le marché de détail grand public fixe pour les technologies xDSL, câble, FTTH ainsi que les box d'accès fixe supportant la technologie 5G, à l'issue d'un délai de 12 mois à compter de la publication de la présente décision au Journal officiel. Ce délai de 12 mois est mis en place pour permettre à un opérateur de gérer son éventuel stock de box non compatible avec l'API.

Les box d'accès fixe ne supportant pas les technologies xDSL, câble, FTTH ou 5G (notamment, celles utilisant la 4G sans supporter la technologie 5G ou le satellite comme moyen d'accès principal à l'internet) peuvent implémenter l'API de manière facultative. Les opérateurs fournissant des offres entreprises peuvent implémenter l'API sur les box mises à disposition des entreprises de manière facultative.

Les modèles de box qui n'ont pas vocation à dépasser 10 000 unités ne sont pas soumis à l'obligation d'implémenter l'API. Cette limite a pour vocation de ne pas faire peser de contraintes sur des box de tests, mises à disposition sur le marché de détail grand public fixe à moins de 10 000 unités.

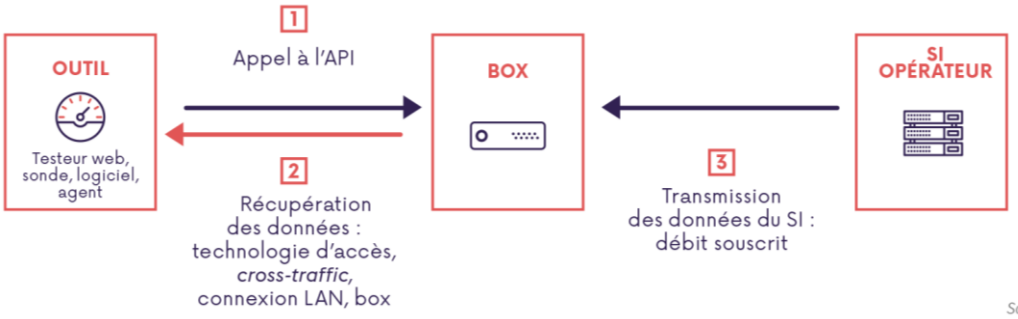
En outre, les modèles de box ne sont plus concernés par la mise en place de l'API après expiration d'un délai de 5 ans à compter du jour de l'arrêt de la mise à disposition sur le marché de détail grand public fixe du modèle de box concerné, ou lorsque le modèle de box est présent en moins de 10 000 exemplaires dans le parc de l'opérateur. Dans ce cas, pour des raisons de coûts engendrés pour les opérateurs et afin de ne pas obliger l'opérateur à maintenir des mises à jour de la box uniquement pour l'API, l'opérateur, à l'expiration de ce délai, peut désactiver l'API des box si le modèle n'est plus concerné par la mise en place de l'API, après en avoir informé l'Arcep, au minimum 3 mois avant la désactivation de l'API.

Les opérateurs concernés communiquent à l'Arcep annuellement une liste des différents modèles de box grand public mises à disposition sur le marché de détail grand public fixe au cours de l'année écoulée prenant en charge l'API ainsi que celles qui ne prennent pas en charge l'API.

Question 1 : Le périmètre opérateurs et box concernés par le projet de décision vous parait-il pertinent ?

2 Le développement de l'API "carte d'identité de l'accès"

2.1 Définition et fonctionnement de l'API



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

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

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

2.2 Objectif de l'API

L'API « carte d'identité de l'accès » est une **nouvelle API**, indépendante d'éventuelles autres API déjà développées par certains opérateurs dans leur box. Elle ne mesure pas le débit et se limite à caractériser l'environnement utilisateur afin de fiabiliser les données remontées par des outils de mesure tiers qui font appel à l'API.

La caractérisation de l'environnement utilisateur présente un **enjeu double** : d'une part, elle est indispensable à la réalisation d'observatoires plus pertinents pour le consommateur, et d'autre part, elle représente un intérêt significatif dans l'établissement d'un diagnostic précis d'un problème de qualité de service. Il est par exemple important de savoir si une mauvaise qualité est due au réseau de l'opérateur, à la qualité du Wi-Fi ou à l'utilisation parallèle d'autres appareils connectés au réseau local lors du test de mesure de la qualité de service internet.

Cette API permet à la fois de remonter des informations fiables, listées à l'annexe 1 de la présente décision, d'une manière sécurisée, dans les conditions définies à l'annexe 2 de la présente décision, et sans dégrader l'expérience utilisateur du client, ce que ne permettent pas d'autres solutions comme un formulaire à remplir par le client avant d'effectuer le test de mesure de qualité de service ou bien une API directement mise en place au niveau du système d'information de l'opérateur. Cette solution a par ailleurs été élaborée en collaboration notamment avec les principaux fournisseurs d'accès à internet en France et les principaux outils de mesure de la qualité de service internet[1].

Question 2 : L'objectif retenu vous parait-il pertinent ?

Question 3 : Les paramètres proposés dans l'Annexe 1 vous paraissent-il pertinents pour la mise en place de l'API? Quel(s) autre(s) paramètre(s) trouvez-vous utiles d'ajouter ou de supprimer ?

[1] La liste complète des participants à la démarche de co-construction de la qualité de service internet est disponible dans l'édition 2018 du rapport sur l'état d'internet en France (page 13) :
https://www.arcep.fr/uploads/tx_gspublication/rapport-etat-internet-2018_conf050618.pdf

2.3 Implémentation de l'API et restriction d'accès à celle-ci (annexe 2)

La démarche de co-construction suivie par l'Arcep avec les principaux opérateurs et acteurs de mesure de la qualité de service en France a permis d'arriver à un consensus en terme d'implémentation de l'API dans les box. Les spécifications d'une restriction d'accès à l'API ont par ailleurs été définies par l'ensemble des participants, à la demande des principaux opérateurs, en vue de satisfaire les besoins exprimés par les opérateurs en termes de sécurité de leurs réseaux. L'annexe 2 de la présente décision détaille en ce sens les modalités d'implémentation de l'API et les modalités de restrictions d'accès à l'API, présentées ci-après.

Afin que les acteurs puissent réaliser des publications sur un nombre suffisant de mesures caractérisées pour être représentatif, l'API est activée par défaut, pour toutes les box compatibles, sans intervention de l'utilisateur.

Une uniformisation du format de sortie est nécessaire et le format JSON (JavaScript Object Notation) a été plébiscité par l'écosystème.

Les outils de mesure de la qualité de service internet qui ont vocation à utiliser l'API sont en HTTPS. Les « contenus mixte actifs » (un script chargé en HTTP sur une page HTTPS) sont bloqués par les navigateurs web. Il est donc nécessaire que l'API écoute en HTTPS, sur le port TCP 443 ou sur le port spécifié par l'opérateur dans l'URL.

Pour des raisons de sécurité et de confidentialité des échanges, l'API ne répond pas sur une connexion HTTP sans couche de chiffrement TLS. L'API n'est accessible que depuis le réseau local (LAN) de l'utilisateur final et ne répond pas aux requêtes qui pourraient provenir d'Internet.

Les principaux navigateurs web désactiveront TLS 1.0 et TLS 1.1 d'ici fin 2020 pour des raisons de sécurité. La connexion HTTPS utilisée pour l'API doit utiliser TLS 1.2 et/ou une version plus récente. Il est déconseillé d'autoriser les connexions HTTPS utilisant TLS 1.0 et/ou TLS 1.1, toutefois, TLS 1.0 et TLS 1.1 sont tolérés, s'ils sont présents suite à une contrainte de l'opérateur.

Les navigateurs web bloquent les certificats n'émanant pas d'une autorité de certification tout comme les certificats expirés. Il est donc nécessaire que l'API utilise un certificat TLS délivré par une autorité de certification. Un certificat TLS a généralement une durée de validité de deux ans maximum. Il est donc nécessaire de régulièrement mettre à jour le certificat, pour ne pas recourir à un certificat expiré, qui bloquerait l'outil de mesure de la qualité de service internet.

Un nom de domaine est nécessaire pour obtenir un certificat TLS reconnu par les navigateurs web. L'API est joignable par un (ou deux) nom(s) de domaine(s) par opérateur (un opérateur correspond à un AS ou « système autonome »). Concrètement, les outils de mesure de la qualité de service internet récupèrent l'AS du client via son adresse IP puis ils récupèrent l'URL à interroger via une table de correspondance AS⇔URL. Il est possible de spécifier un second nom de domaine à interroger pour les AS qui auraient besoin de deux noms de domaines.

Afin de sécuriser l'API et réduire le périmètre d'attaque, un système de restriction d'accès doit être mis en place. La restriction d'accès retenue en concertation avec les différents acteurs impliqués est : CORS + OAuth 2.0 (https://oauth.net/2/) avec un token à validité de 15 minutes.

La mise en œuvre de la présente décision sera suivie par un comité de suivi composé de représentants des opérateurs et des outils de mesure de la qualité de service internet et piloté par l'Arcep.

Question 4 : L'implémentation de l'API et les restrictions d'accès retenues par l'Arcep (détaillées à l'annexe 2) vous paraissent-elles les plus appropriées ? Sinon, quelles modifications proposez-vous ?

3 Calendrier de mise en œuvre

Afin de déployer dans des délais raisonnables cette solution permettant l'information de l'utilisateur sur la qualité de service internet fixe, et pour tenir compte de contraintes techniques, les opérateurs visés par la présente décision sont tenus de mettre en œuvre l'API dans le respect de certaines échéances.

Ainsi, dans un délai de 12 mois suivant la publication de la présente décision, les opérateurs effectuent la démonstration auprès de l'Arcep d'une box de développement avec l'API implémentée conformément aux dispositions de la présente décision.

Dans un délai de 20 mois suivant la publication de la présente décision, les opérateurs implémentent et à activent par défaut l'API sur 5% des box du parc concerné par la mise en place de l'API.

Dans un délai de 24 mois suivant la publication de la présente décision, les opérateurs implémentent et à activent par défaut l'API sur 40% des box du parc concerné par la mise en place de l'API.

Dans un délai de 28 mois suivant la publication de la décision :

- les opérateurs implémentent et à activent par défaut l'API sur 95% des box du parc concerné par la mise en place de l'API ;

- les opérateurs implémentent et à activent par défaut l'API sur 100 % des box mises à disposition auprès des nouveaux clients sur le marché de détail grand public fixe.

Question 5 : Le calendrier retenu vous parait-il réaliste et adapté aux contraintes de développement ? Pour quelles raisons ? Sinon, quelles modifications proposez-vous ?

Question 6 : Les acteurs sont invités à formuler, le cas échéant, d'autres observations ou propositions sur le projet de décision en consultation.

Décide :

Champ d'application

Article 1. La présente décision s'applique à tout opérateur de communications électroniques, au sens de l'article L. 32 (15°) du CPCE, disposant, directement ou à travers des sociétés qu'ils contrôlent ou qui les contrôlent au sens de l'article L. 233-3 du code de commerce, d'un nombre d'abonnements actifs supérieur à 1 000 000 clients, sur les marchés de détail grand public fixe.

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

Article 2. Les opérateurs mentionnés à l'article 1er mettent en place une interface de programmation applicative (API) dans les modèles de box mis à disposition sur le marché de détail grand public fixe à compter d'un délai de 12 mois suivant la publication de la présente décision pour les technologies xDSL, câble, FTTH, ainsi que les modèles de box d'accès fixe supportant la technologie 5G sous réserve que le parc de chacun de ces modèles dépasse 10 000 unités.

Article 3. Les modèles de box mentionnés à l'article 2 ne sont plus concernés par la mise en place de l'API après expiration d'un délai de 5 ans, à compter du jour de l'arrêt de la mise à disposition sur le marché de détail grand public fixe du modèle de box concerné, ou lorsque le modèle de box est présent en moins de 10 000 exemplaires dans le parc de l'opérateur. L'opérateur peut retirer l'API des box si le modèle n'est plus concerné par la mise en place de l'API, après en avoir informé l'Arcep, au minimum 3 mois avant la désactivation de l'API.

Paramètres communiqués par l'API

Article 4. Les opérateurs mentionnés à l'article 1er, lorsqu'ils mettent en place une interface de programmation applicative (API) dans les conditions prévues par l'article 2, implémentent les paramètres définis à l'annexe 1.

Implémentation et restriction d'accès de l'API

Article 5. Les opérateurs mentionnés à l'article 1er, lorsqu'ils mettent en place une interface de programmation applicative (API) dans les conditions prévues par l'article 2, respectent les conditions d'implémentation et de restrictions d'accès définies à l'annexe 2.

Transmission de données à l'Autorité

Article 6. Les opérateurs mentionnés à l'article 1er communiquent à l'Arcep annuellement la liste des différents modèles de box grand public mis à disposition sur le marché de détail grand public fixe au cours de l'année écoulée prenant en charge l'API et celles qui ne prennent pas en charge l'API prévue à l'article 2.

Mise en œuvre de la présente décision

Article 7. Dans un délai de 12 mois suivant la publication de la présente décision, les opérateurs mentionnés à l'article 1er effectuent la démonstration auprès de l'Arcep d'une box de développement comportant une API implémentée conformément aux articles 1 à 5.

Article 8. Dans un délai de 20 mois suivant la publication de la présente décision, les opérateurs mentionnés à l'article 1er implémentent et activent par défaut une API, conformément aux articles 1 à 5, sur 5% des box visées à l'article 2.

Article 9. Dans un délai de 24 mois suivant la publication de la présente décision, les opérateurs mentionnés à l'article 1er implémentent et activent par défaut une API, conformément aux articles 1 à 5, sur 40% des box visées à l'article 2.

Article 10. Dans un délai de 28 mois suivant la publication de la décision, les opérateurs mentionnés à l'article 1er :

- implémentent et activent par défaut une API, conformément aux articles 1 à 5, sur 95% des box des box visées à l'article 2.

- implémentent et à activent par défaut l'API sur 100 % des box mises à disposition auprès des nouveaux clients sur le marché de détail grand public fixe visées à l'article 2.

Exécution

Article 11. La directrice générale de l'Autorité de régulation des communications électroniques et des postes est chargée de l'exécution de la présente décision qui sera publiée au Journal officiel de la République française et sur le site internet de l'Autorité, après son homologation par le ministre chargé des communications électroniques.

Annexe 1 – Paramètres communiqués par l'API

1 Paramètres principaux

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

Condition de présence	Arbre JSON	Nom du paramètre	Unité	Détail du paramètre	Format / liste de valeurs acceptées
Obligatoire	Root	ApiVersion		Version de l'API	Entier positif de 64 bits
Obligatoire	TimeStamp	ApiCallTime		Horodatage correspondant à l'heure à laquelle l'API est requêtée	Entier positif de 64 bits
Obligatoire	Gateway	Model		Nom de l'IAD (« box ») du client	texte
Obligatoire	Gateway	HardwareVersion		Version hardware (comme rev3)	texte
Obligatoire	Gateway	SoftwareVersion		Version du logiciel	texte
Obligatoire	SubscriptionSpeed	DownloadMin	Kb/s	Débit minimum descendant contractuel	Entier positif de 64 bits
Obligatoire	SubscriptionSpeed	UploadMin	Kb/s	Débit minimum montant contractuel	Entier positif de 64 bits
Obligatoire	SubscriptionSpeed	DownloadMax	Kb/s	Débit maximum descendant contractuel	Entier positif de 64 bits
Obligatoire	SubscriptionSpeed	UploadMax	Kb/s	Débit maximum montant contractuel	Entier positif de 64 bits
Obligatoire	SubscriptionSpeed	DownloadNormally	Kb/s	Débit « normalement disponible » descendant contractuel (s'il existe)	Entier positif de 64 bits
Obligatoire	SubscriptionSpeed	UploadNormally	Kb/s	Débit « normalement disponible » montant contractuel (s'il existe)	Entier positif de 64 bits
Obligatoire	Wan	Technology		Technologie WAN utilisée par l'IAD (« box »)	["ftth";"adsl"; "vdsl";"gfast";"cable"; "satellite";"2g/3g";"4g";"5g"]
Obligatoire si la technologie WAN est FTTH	Wan/SpeedOnt	Download	Kb/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	Kb/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	Kb/s	xDSL uniquement : débit de synchronisation descendant	Entier positif de 64 bits
Obligatoire si la technologie WAN est xDSL	Wan/SpeedSynchro	Upload	Kb/s	xDSL uniquement : débit de synchronisation montant	Entier positif de 64 bits
Obligatoire	Wan	Aggregation		Présence d'une agrégation de deux accès WAN active Exemple: xDSL + 4G	["yes";"no"]

Note : concernant les débits commerciaux souscrits par le client :

- Le « débit minimum » n'est à remplir que si l'accès possède un débit minimum ;
- Le « débit normalement disponible » n'est à remplir que si l'accès possède un débit normalement disponible ;
- Le « débit maximum » est à remplir systématiquement en FTTH avec le débit contractuel. Pour le xDSL il n'est à remplir que si l'accès possède un débit maximum.

Condition de présence	Arbre JSON	Nom du paramètre	Unité	Détail du paramètre	Format / liste de valeurs acceptées
Obligatoire	Lan	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	Download	Kb/s	Débit descendant sur le LAN (Ethernet / Wi-Fi / CPL) négocié par le terminal requêtant l'API. CPL : débit brut remonté par le CPL connecté sur le port Ethernet d'où provient la requête de l'API.	Entier positif de 64 bits
Obligatoire	Lan/SpeedLan	Upload	Kb/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	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

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.

Condition de présence	Arbre JSON	Nom du paramètre	Unité	Détail du paramètre	Format / liste de valeurs acceptées
Obligatoire	Root	ApiVersion		Version de l'API	Entier positif de 64 bits
Obligatoire	ByteCounter	Download	octets	Relevé du compteur de trafic descendant (internet => IAD) du port WAN	Entier positif de 64 bits
Obligatoire	ByteCounter	Upload	octets	Relevé du compteur de trafic montant (IAD => internet) du port WAN	Entier positif de 64 bits
Obligatoire	TimeStamp	ApiCallTime		Horodatage correspondant à l'heure à laquelle l'API est requêtée	Entier positif de 64 bits
Obligatoire	TimeStamp	LastUpdate		Horodatage de la dernière mise à jour du compteur du port WAN (le compteur est relevé en temps réel alors LastUpdate = ApiCallTime)	Entier positif de 64 bits

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

Annexe 2 – Implémentation et restriction d'accès de l'API

1 Spécifications de l'implémentation de l'API

- l'API écoute uniquement en HTTPS, sur le port TCP 443 ou sur le port spécifié par l'opérateur dans l'URL. L'API ne répond pas sur une connexion HTTP sans couche de chiffrement TLS ;
- la connexion HTTPS utilisée pour l'API doit utiliser TLS 1.2 et/ou une version plus récente ;
- le certificat TLS est valide, il est donc nécessaire de régulièrement pousser un nouveau certificat, pour ne pas disposer uniquement d'un certificat expiré ;
- l'API écoute uniquement sur le LAN. L'API ne répond pas aux requêtes qui pourraient provenir d'Internet ;
- l'API est activée par défaut sans intervention de l'utilisateur ;
- l'API est joignable par un (ou deux) nom(s) de domaine(s) par opérateur (un opérateur correspond à un AS ou « système autonome ») ;
- le format de sortie de l'API est un fichier JSON (JavaScript Object Notation).

2 Restriction d'accès via CORS

Le « *cross-origin resource sharing* » (CORS) ou « partage des ressources entre origines multiples » (en français, moins utilisé) est un mécanisme qui consiste à ajouter des en-têtes HTTP afin de permettre à une application web d'accéder à des ressources d'un serveur situé sur une autre origine que le site courant. Une application web réalise une requête HTTP multi-origine (*cross-origin*) lorsqu'elle demande une ressource provenant d'un domaine, d'un protocole ou d'un port différent de ceux utilisés pour la page courante.

Techniquement, le nom de domaine de l'outil de mesure de la qualité de service internet doit être présent dans le champ d'en-tête HTTP nommé « *Access-Control-Allow-Origin* » envoyé par le serveur web intégré dans la box. Cela permet de limiter l'accès de l'API aux seuls sites web autorisés : si le nom de domaine n'est pas présent, le navigateur web bloque l'accès à l'API.

Le World Wide Web Consortium explique cependant qu'il n'est pas possible d'intégrer plusieurs nom de domaine dans un même en-tête : "*Note that it is not possible to grant access to multiple specific sites, nor use a partial wildcard match. It is also not possible to specify more than one Access-Control-Allow-Origin header*."[3]

Pour pouvoir donner l'accès à plusieurs outils, il convient de n'envoyer qu'un champ d'en-tête HTTP nommé « *Access-Control-Allow-Origin* » qui contienne le nom de domaine appelant, s'il est autorisé. La liste des noms de domaines autorisés est alors conservée dans le serveur web et n'est pas envoyée en totalité : seul le « *Access-Control-Allow-Origin* » correspondant à la source est envoyé, sous réserve que la source soit dans la liste des noms de domaines autorisés. Si la source n'est pas autorisée, le serveur web ne renvoie aucun champ d'en-tête HTTP nommé « *Access-Control-Allow-Origin* » et le navigateur web bloque la requête.

[3] https://www.w3.org/wiki/CORS_Enabled

3 Restriction d'accès via OAuth 2.0 avec un token à validité de 15 minutes

Le token est un identifiant utilisé par un outil pour accéder à l'API valable 15 minutes. Chaque outil à son propre token, permettant ainsi de retirer les accès à un outil sans impacter les autres.

Le token informe l'API que le porteur du token a été autorisé à accéder à l'API et ils permettent d'associer à chaque accédant un champ d'action.

Il est envisagé d'avoir un schéma d'autorisation serveur à serveur pour obtenir le token d'accès, c'est-à-dire que l'outil de mesure obtiendrait le token auprès des opérateurs sans action nécessaire de l'utilisateur. L'outil utiliserait alors ce token pour accéder à l'API.

Ce mécanisme nécessite la mise en place d'une infrastructure à clés publiques (PKI[4]) pour renouveler les tokens et transférer ces informations entre acteurs de manière sécurisée, en utilisant de la cryptographie asymétrique.

Le serveur d'autorisation OAuth 2.0 peut être directement sur l'IAD ou en central, selon le choix de l'opérateur et les outils de mesure de la qualité de service internet doivent savoir gérer les deux cas.

[4] Public Key Infrastructure

Annexe 3 - Fiabilité de la restriction d'accès à l'API

Un Code de conduite a été établi en concertation avec les opérateurs et les outils de mesure. Il s'agit d'un document à destination des acteurs de la mesure de la qualité des réseaux internet, aussi bien fixes que mobiles, qui regroupe des bonnes pratiques qui incitent les acteurs, d'une part, à accentuer la transparence des choix méthodologiques réalisés, afin que toute personne tierce soit en mesure d'analyser les résultats présentés et, d'autre part, à abandonner les pratiques les plus sujettes à caution, en termes de protocole de test comme de publication des résultats[5].

Afin de mieux fiabiliser la restriction définie en annexe 2, les outils de mesure devraient mettre en place les mesures de sécurité suivantes:

- le nom de domaine de l'outil de mesure doit être signé par DNSSEC, afin de protéger contre le *cache poisoning* ;
- le champ DNS *Certification Authority Authorization* (CAA) doit être déclaré pour limiter les autorités de certification (CA) qui sont autorisées à délivrer des certificats pour le nom de domaine ;
- un appel au site en HTTP doit contenir uniquement une redirection vers le même site en HTTPS ;
- les échanges HTTPS ne doivent pas gérer des versions inférieures à TLS 1.2 ;
- les en-têtes *HTTP Strict Transport Security* (HSTS) doivent être envoyés sur le domaine principal.

[5] La version 2018 du code de conduite a été publiée par l'Arcep le 20 décembre 2018 à l'adresse Internet https://www.arcep.fr/uploads/tx_gspublication/code-de-conduite-qs-internet-2018_FR.pdf