

Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 7679
STD 81
RFC rendue obsolète : 2679
Catégorie : Norme
ISSN : 2070-1721

G. Almes, Texas A&M
S. Kalidindi, Ixia
M. Zekauskas, Internet2
A. Morton, Ed., AT&T Labs
janvier 2016
Traduction Claude Brière de L'Isle

Métrique de délai unidirectionnel pour les métriques de performance IP (IPPM)

Résumé

Le présent mémoire définit une métrique pour le délai unidirectionnel de paquets sur les chemins de l'Internet. Il s'appuie sur les notions introduites et discutées dans le document cadre sur la métrique des performances IP (IPPM, *IP Performance Metrics*) la RFC 2330 dont le lecteur est supposé familier. Le présent mémoire rend obsolète la RFC 2679.

Statut de ce mémoire

Le présent document est une norme de l'Internet.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Plus d'informations sur les normes de l'Internet sont disponibles à la Section 2 de la [RFC5741].

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à <http://www.rfc-editor.org/info/rfc7679>

Notice de droits de reproduction

Copyright (c) 2014 IETF Trust et les personnes identifiées comme auteurs du document. Tous droits réservés.

Le présent document est soumis au BCP 78 et aux dispositions légales de l'IETF Trust qui se rapportent aux documents de l'IETF (<http://trustee.ietf.org/license-info>) en vigueur à la date de publication de ce document. Prière de revoir ces documents avec attention, car ils décrivent vos droits et obligations par rapport à ce document. Les composants de code extraits du présent document doivent inclure le texte de licence simplifié de BSD comme décrit au paragraphe 4.e des dispositions légales du Trust et sont fournis sans garantie comme décrit dans la licence de BSD simplifiée.

Table des Matières

1. Introduction.....	2
1.1 Motivation.....	2
2. Questions générales concernant le temps.....	3
3. Définition d'un singleton pour délai unidirectionnel.....	3
3.1 Nom de la métrique.....	3
3.2 Paramètres de la métrique.....	4
3.3 Unités de la métrique.....	4
3.4 Définition.....	4
3.5 Discussion.....	4
3.6 Méthodologies.....	5
3.7 Erreurs et incertitudes.....	5
3.8 Rapport de métrique.....	7
4. Définition d'échantillons de délai unidirectionnel.....	8
4.1 Nom de la métrique.....	8
4.2 Paramètres de la métrique.....	9
4.3 Unités de la métrique.....	9
4.4 Définition.....	9
4.5 Discussion.....	9
4.6 Méthodologies.....	9
4.7 Erreurs et incertitudes.....	10
4.8 Rapport de métrique.....	10
5. Définitions de statistiques pour délai unidirectionnel.....	10
5.1 Type-P-One-way-Delay-Percentile.....	10

5.2 Type-P-One-way-Delay-Median.....	10
5.3 Type-P-One-way-Delay-Minimum.....	11
5.4 Type-P-One-way-Delay-Inverse-Percentile.....	11
6. Considérations sur la sécurité.....	11
7. Changements depuis la RFC 2679.....	12
8. Références.....	13
8.1 Références normatives.....	13
8.2 Références pour information.....	13
Remerciements.....	14
Adresse des auteurs.....	14

1. Introduction

Le présent mémoire définit une métrique pour le délai unidirectionnel des paquets sur les chemins de l'Internet. Il s'appuie sur les notions introduites et discutées dans le document cadre IPPM, [RFC2330] dont le lecteur est supposé familier, avec sa récente mise à jour [RFC7312].

Le présent mémoire est destiné à être parallèle par sa structure au document qui l'accompagne pour la perte de paquet ("Métrique de perte de paquet unidirectionnelle pour IPPM") [RFC7680].

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119]. Bien que la [RFC2119] ait été écrite en vue des protocoles, les mots clés sont utilisés dans ce document pour des raisons similaires. Ils sont utilisés pour assurer que les résultats des mesures de deux mises en œuvre différentes sont comparables et pour noter les instances où une mise en œuvre pourrait perturber le réseau.

Chaque fois qu'un terme technique du document cadre IPPM est utilisé pour la première fois dans ce mémoire, il sera marqué avec une astérisque en queue. Par exemple, "terme*" indique que "terme" est défini dans le document cadre.

La structure du document est la suivante :

- o Une métrique analytique de "singleton*", appelée Type-P-One-way-Delay (*délai unidirectionnel de type P*), sera introduite pour mesurer une seule observation de délai unidirectionnel.
- o En utilisant cette métrique de singleton, un "échantillon*" appelée Type-P-One-way-Delay-Poisson-Stream (*flux de Poisson de délai unidirectionnel de type P*) est introduit pour mesurer une séquence de délais singletons envoyés à des instants tirés d'un processus de Poisson, défini au paragraphe 11.1.1 de la [RFC2330].
- o En utilisant cet échantillon, plusieurs "statistiques*" de l'échantillon seront définies et discutées. Cette progression du singleton à l'échantillon et de l'échantillon à la statistique, avec une claire séparation entre eux, est importante.

1.1 Motivation

Comprendre le délai unidirectionnel d'un paquet de Type-P* provenant d'un hôte* de source à un hôte de destination est utile pour plusieurs raisons :

- o Certaines applications ne fonctionnent pas bien (ou pas du tout) si le délai de bout en bout entre les hôtes est grand par rapport à une certaine valeur seuil.
- o Une variation erratique du délai rend difficile (ou impossible) de prendre en charge de nombreuses applications en temps réel.
- o Plus grande est la valeur du délai, plus il est difficile aux protocoles de couche transport de tenir une forte bande passante.
- o La valeur minimum de cette métrique donne une indication du délai dû seulement au délai de propagation et de transmission.
- o La valeur minimum de cette métrique donne une indication du délai qui va probablement être subi lorsque le chemin* traversé est légèrement chargé.
- o Les valeurs de cette métrique au dessus du minimum donnent une indication de l'encombrement présent sur le chemin.

La mesure du délai unidirectionnel au lieu du délai d'aller-retour est motivée par les facteurs suivants :

- o Dans l'Internet d'aujourd'hui, le chemin d'une source à une destination peut être différent du chemin de retour de la destination à la source ("chemins asymétriques"), lorsque des séquences différentes de routeurs sont utilisées pour le chemin vers l'avant et celui en sens inverse. Donc, les mesures d'aller-retour mesurent en fait ensemble les performances de deux chemins distincts. Mesurer chaque chemin indépendamment souligne les différences de performances entre les deux chemins qui peuvent traverser des fournisseurs d'accès Internet différents et même des types de réseaux radicalement

différents (par exemple, des réseaux de recherche par opposition à des réseaux commerciaux, ou des réseaux avec des capacités de liaison asymétriques, ou un accès sans fil par opposition à un réseau filaire).

- o Même lorsque deux chemins sont symétriques, ils peuvent avoir des caractéristiques de performances radicalement différentes dues à une mise en file d'attente asymétrique.
- o Les performances d'une application peuvent dépendre surtout des performances dans une direction. Par exemple, une communication fondée sur TCP va subir une réduction de débit si de l'encombrement se produit dans une direction de sa communication. Les ennuis peuvent être simplifiés si on peut identifier la direction encombrée de la transmission TCP.
- o Dans les réseaux dans lesquels la qualité de service (QS) est activée, le provisionnement dans une direction peut être radicalement différent du provisionnement dans la direction inverse et donc les garanties de QS diffèrent. Mesurer les chemins indépendamment permet la vérification des deux garanties.

Il sort du domaine d'application du présent document de dire précisément comment les métriques de délai seraient appliquées à des problèmes spécifiques.

2. Questions générales concernant le temps

{Commentaire : La terminologie ci-dessous diffère de celle définie par les documents de l'UIT-T (par exemple, G.810, "Définitions et terminologie pour la synchronisation des réseaux" et I.356, "Performances de transfert de cellule de couche ATM dans le RNIS-LB") mais est cohérente avec le document cadre IPPM. En général, ces différences proviennent de la différence de contexte ; les documents de l'UIT-T ont une origine historique dans la téléphonie, tandis que les auteurs du présent document (et du document cadre) viennent du monde de l'informatique. Bien que les termes définis ici n'aient pas d'équivalent direct dans les définitions de l'UIT-T, nous en donnerons après nos définitions une transposition grossière. Cependant, on notera une confusion potentielle : notre définition de "horloge" est la définition des systèmes d'exploitation informatiques qui notent une horloge donnant l'heure, tandis que la définition de l'horloge par l'UIT-T note une référence à une fréquence.}

Chaque fois qu'un instant (c'est-à-dire, un moment historique) est mentionné ici, il est compris comme étant mesuré en secondes (et fractions de secondes) par rapport au temps universel (UTC).

Comme décrit plus complètement dans le document cadre, il y a quatre notions distinctes, mais en relations les unes avec les autres, de l'incertitude d'horloge :

synchronisation* : mesure dans laquelle deux horloges s'accordent sur l'heure qu'il est. Par exemple, l'horloge d'un hôte peut être en avance de 5,4 ms de l'horloge d'un second hôte. {Commentaire : à peu près équivalent à "l'erreur de temps" de l'UIT-T.}

précision* : mesure dans laquelle une certaine horloge s'accorde à l'UTC. Par exemple, l'horloge d'un hôte peut être en retard de 27,1 ms sur l'UTC. {Commentaire : équivalent à peu près à "l'erreur de temps par rapport à l'UTC" de l'UIT-T.}

résolution* : spécification de la plus petite unité par laquelle l'heure de l'horloge est mise à jour. Elle donne la limite inférieure de l'incertitude de l'horloge. Par exemple, l'horloge d'un vieil hôte Unix peut battre seulement une fois toutes les 10 ms, et a donc une résolution de 10 ms. {Commentaire : équivalent très grossièrement à la "période d'échantillonnage" de l'UIT-T.}

biais* : mesure le changement de précision, ou de synchronisation, avec le temps. Par exemple, l'horloge d'un certain hôte peut gagner 1,3 ms par heure et donc être en retard de 27,1 ms sur l'UTC à un moment et seulement de 25,8 ms une heure plus tard. Dans ce cas, on dit que l'horloge de l'hôte a un biais de 1,3 ms par heure par rapport à l'UTC, ce qui nuit à la précision. On peut aussi parler du biais d'une horloge par rapport à une autre, ce qui nuit à la synchronisation. {Commentaire : équivalent à peu près à la "dérive horaire" de l'UIT-T.}

3. Définition d'un singleton pour délai unidirectionnel

3.1 Nom de la métrique

Type-P-One-way-Delay

3.2 Paramètres de la métrique

- o Src, adresse IP d'un hôte
- o Dst, adresse IP d'un hôte
- o T, un instant
- o Tmax, temps d'attente des seuils de perte

3.3 Unités de la métrique

La valeur d'un Type-P-One-way-Delay est soit un nombre réel, soit un nombre indéfini (informellement, infini) de secondes.

3.4 Définition

Pour un nombre réel dT , \gg le *Type-P-One-way-Delay* de Src à Dst à T est $dT \ll$ signifie que Src a envoyé le premier bit d'un paquet de type P à Dst à l'heure du réseau T et que Dst a reçu le dernier bit de ce paquet à l'heure du réseau $T+dT$.

\gg Le *Type-P-One-way-Delay* de Src à Dst à T est indéfini (informellement, infini) \ll signifie que Src a envoyé le premier bit d'un paquet de type P à Dst à l'heure du réseau T et que Dst n'a pas reçu ce paquet (dans le seuil de temps d'attente de perte, Tmax).

Des suggestions sur ce dont on fait rapport et des valeurs de métriques apparaissent au paragraphe 3.8 après la discussion de la métrique, des méthodologies de mesure de la métrique, et de l'analyse des erreurs.

3.5 Discussion

Type-P-One-way-Delay est une métrique analytique relativement simple, et dont on pense qu'elle est une des méthodes de mesure efficaces.

Les problèmes suivants vont se poser en pratique :

- o Les valeurs de délai réelles seront positives. Donc, rapporter une valeur négative comme délai réel n'a pas de sens. Cependant, une valeur individuelle de délai de zéro ou négative peut être utile au titre d'un flux lorsque on essaye de découvrir une distribution d'un flux de valeurs de délai.
- o Comme les valeurs de délai vont souvent être dans la gamme de 100 μ s à 10 ms, il sera important pour Src et Dst de se synchroniser très étroitement. Les systèmes de positionnement mondial (GPS, *Global Positioning System*) donnent un moyen de réaliser la synchronisation à plusieurs dizaines de μ s. L'application ordinaire de NTP peut permettre la synchronisation à plusieurs ms, mais cela dépend de la stabilité et de la symétrie des propriétés de délai chez les agents NTP utilisés, et ce délai est ce qu'on essaye de mesurer. Une combinaison de serveurs NTP fondés sur GPS et d'un ensemble de serveurs NTP de conception et déploiement plus traditionnels devrait donner de bons résultats. Cela a été vérifié dans la [RFC6808], où un système de mesures GPS avait des résultats comparables avec un système synchronisé NTP fondé sur GPS pour le même chemin intercontinental.
- o Une méthodologie devra inclure un moyen de déterminer si une valeur de délai est infinie ou si elle est simplement très grande (et le paquet est déjà arrivé à Dst). Comme noté par Mahdavi et Paxson [RFC2678], de simples limites supérieures (comme la limite théorique supérieure de 255 secondes sur la durée de vie des paquets IP [RFC791]) pourrait être utilisée ; mais une bonne ingénierie, incluant la compréhension des durées de vie des paquets, sera nécessaire en pratique. {Commentaire : Noter que, pour de nombreuses applications de ces métriques, l'inconvénient de traiter un grand délai comme infini peut être nul ou très faible. Un paquet de données TCP, par exemple, qui arrive seulement après plusieurs multiples du délai d'aller-retour pourrait aussi bien avoir été perdu. Voir au paragraphe 4.1.1 de la [RFC6703] l'examen de délais de paquet inhabituels et l'estimation des performances d'application.}
- o Si le paquet est dupliqué sur le ou les chemins de sorte que de multiples copies non corrompues arrivent à destination, le paquet est alors compté comme reçu, et la première copie qui arrive détermine le délai unidirectionnel du paquet.
- o Si le paquet est fragmenté et si, pour une raison quelconque, le réassemblage ne se fait pas, le paquet sera alors réputé perdu.
- o Une méthodologie va inclure un moyen de déterminer si le paquet est formé de façon standard, les critères par défaut pour toutes les définitions de métrique définies à la Section 15 de la [RFC2330], autrement, le paquet sera réputé perdu. Noter que pour l'instant, la définition de paquets formés de façon standard ne s'applique qu'à IPv4, mais voir aussi [IPPM-UPDATES].

3.6 Méthodologies

Comme avec les autres métriques de type P-*, les détails de la méthodologie vont dépendre du type P (par exemple, le numéro de protocole, le numéro d'accès UDP/TCP, la taille, le champ Services différenciés (DS) [RFC2780]).

Généralement, pour un certain Type-P, la méthodologie va procéder comme suit :

- o S'arranger pour que Src et Dst soient synchronisées; c'est-à-dire qu'elles aient des horloges qui soient très étroitement synchronisées l'une avec l'autre et chacune très proche de l'heure réelle.
- o Chez l'hôte Src, choisir les adresses IP de source et de destination, et former un paquet d'essai de Type-P avec ces adresses. Toute portion de "bourrage" du paquet nécessaire pour donner au paquet d'essai une certaine taille devrait être remplie de bits aléatoires pour éviter une situation dans laquelle le délai mesuré serait inférieur à ce qu'il serait autrement du fait des techniques de compression le long du chemin. Voir aussi le paragraphe 3.1.2 de la [RFC7312].
- o Chez l'hôte Dst, s'arranger pour recevoir le paquet.
- o Chez l'hôte Src, placer un horodatage dans le paquet de type P préparé, et l'envoyer vers Dst (idéalement en minimisant le temps avant l'envoi).
- o Si le paquet arrive dans un délai raisonnable, mettre un horodatage aussitôt que possible à la réception du paquet. En soustrayant les deux horodatages, une estimation du délai unidirectionnel peut être calculée. L'analyse d'erreur d'une certaine mise en œuvre de la méthode doit prendre en compte l'étroitesse de la synchronisation entre Src et Dst. Si le délai entre l'horodatage de Src et l'envoi réel du paquet est connu, l'estimation pourra être ajustée en soustrayant cette quantité ; l'incertitude sur cette valeur doit être prise en compte dans l'analyse d'erreur. De même, si le délai entre la réception réelle du paquet et l'horodatage de Dst est connu, l'estimation pourra être ajustée en soustrayant cette quantité ; l'incertitude sur cette valeur doit être prise en compte dans l'analyse d'erreur. Voir "Erreurs et incertitudes" (paragraphe 3.7) pour une discussion plus détaillée.
- o Si le paquet manque à arriver dans un délai raisonnable, Tmax, le délai unidirectionnel est pris comme indéfini (informellement, infini). Noter que le seuil de "raisonnable" est un paramètre de la métrique. Ces points sont examinés en détail dans la [RFC6703], incluant les préférences d'analyse pour allouer un délai indéfini aux paquets qui échouent à arriver avec les difficultés résultant de l'allocation du "délai infini" informel, et une estimation d'une limite supérieure au temps d'attente des paquets en transit. De plus, appliquer une constante spécifique de temps d'attente sur des singletons mémorisés de délai unidirectionnel est conforme à la présente spécification et peut permettre que les résultats servent à une audience plus large que celle du rapport.

Les questions comme le format du paquet, les moyens par lesquels la destination sait quand attendre le paquet d'essai, et les moyens par lesquels Src et Dst sont synchronisées sortent du domaine d'application du présent document. {Commentaire : on prévoit de documenter ailleurs plus en détail les techniques de mise en œuvre de ce travail et on invite d'autres à le faire aussi.}

3.7 Erreurs et incertitudes

La description de toute méthode de mesure spécifique devrait inclure une comptabilité et une analyse des diverses sources d'erreur ou incertitude. Le document cadre donne des lignes directrices générales sur ce point, mais on note ici les spécificités suivantes relatives aux métriques de délai :

- o les erreurs ou incertitudes dues aux incertitudes d'horloges des hôtes de source et destination,
- o les erreurs ou incertitudes dues à la différence entre heure du réseau et heure de l'hôte.

De plus, le seuil de perte peut affecter les résultats. Tout cela est discuté en détail ci-dessous, avec un paragraphe (3.7.3) sur la prise en compte de ces erreurs et incertitudes.

3.7.1 Erreurs ou incertitudes relatives aux horloges

L'incertitude dans une mesure de délai unidirectionnel est relative, en partie, aux incertitudes dans les horloges des hôtes Src et Dst. Dans ce qui suit, on se réfère à l'horloge utilisée pour mesurer quand le paquet a été envoyé de Src comme l'horloge de source, on se réfère à l'horloge utilisée pour mesurer quand le paquet a été reçu par Dst comme horloge de destination ; on se réfère à l'heure observée quand le paquet a été envoyé par l'horloge de source comme Tsource, et on se réfère à l'heure observée quand le paquet a été reçu par l'horloge de destination comme Tdest. En ce qui concerne les notions de synchronisation, précision, résolution, et biais mentionnées dans l'introduction, on note ce qui suit :

- o Toute erreur de synchronisation entre l'horloge de source et l'horloge de destination va contribuer à une erreur de la mesure

du délai. On dit que l'horloge de source et l'horloge de destination ont une erreur de synchronisation de T_{synch} si l'horloge de source est en avance de T_{synch} sur l'horloge de destination. Donc, si on connaît la valeur de T_{synch} exactement, on peut corriger la synchronisation d'horloge en ajoutant T_{synch} à la valeur non corrigée de $T_{\text{dest}} - T_{\text{source}}$.

- o La précision d'une horloge n'est importante que pour identifier l'heure à laquelle un certain délai a été mesuré. La précision en elle-même n'a pas d'importance pour la précision de la mesure du délai. Quand on calcule des délais, on est intéressé seulement par la différences entre les valeurs d'horloges, non par les valeurs elles-mêmes.
- o La résolution d'une horloge ajoute à l'incertitude sur le temps mesuré par elle. Donc, si l'horloge de source a une résolution de 10 ms, cela ajoute alors 10 ms d'incertitude à toute valeur de temps mesurée par elle. On notera la résolution de l'horloge de source par R_{source} , et celle de l'horloge de destination par R_{dest} .
- o Le biais d'une horloge n'est pas tant un problème supplémentaire que la réalisation du fait que T_{synch} est elle-même une fonction du temps. Donc, si on tente de mesurer ou fixer des limites à T_{synch} , cela doit être fait périodiquement. Sur une certaine période de temps, cette fonction peut être approximée comme une fonction linéaire plus des termes d'ordre supérieur ; dans ce cas, une option est d'utiliser la connaissance de la composante linéaire pour corriger l'horloge. En utilisant cette correction, le T_{synch} résiduel est diminué mais reste une source d'incertitude dont il faut tenir compte. On utilise la fonction $E_{\text{synch}}(t)$ pour noter la limite supérieure de l'incertitude de synchronisation. Donc, $|T_{\text{synch}}(t)| \leq E_{\text{synch}}(t)$.

En prenant tous ces éléments, on note que le simple calcul de $T_{\text{dest}} - T_{\text{source}}$ sera court de $T_{\text{synch}}(t) \pm (R_{\text{source}} + R_{\text{dest}})$. En utilisant la notion de $E_{\text{synch}}(t)$, on note que ces problèmes d'horloge introduisent une incertitude totale de $E_{\text{synch}}(t) + R_{\text{source}} + R_{\text{dest}}$. Cette estimation de l'incertitude totale relative à l'horloge devrait être incluse dans l'analyse d'erreur/incertitude de toute mise en œuvre de mesure.

3.7.2 Erreurs ou incertitudes relatives à l'heure du réseau par rapport à l'heure de l'hôte

Comme on a défini le délai unidirectionnel, on va mesurer le temps entre le moment où le paquet d'essai quitte l'interface réseau de Src et celui où il arrive (complètement) à l'interface réseau de Dst : on appelle cela le "temps réseau". Si les mesures de temps sont elles-mêmes effectuées par le logiciel sur Src et Dst, ce logiciel ne peut cependant mesurer directement que le temps entre l'apposition d'un horodatage sur Src juste avant d'envoyer le paquet d'essai et l'apposition d'un horodatage sur Dst juste après avoir reçu le paquet d'essai : on appelle ces deux points les "temps d'hôtes".

On note que certains systèmes effectuent l'horodatage d'hôte sur le matériel d'interface réseau, en tentant de minimiser la différence avec le temps réseau.

Dans la mesure où la différence entre temps réseau et temps d'hôtes est connue avec précision, cette connaissance peut être utilisée pour corriger les mesures de temps d'hôtes, et la valeur corrigée estime plus précisément la métrique désirée (sur le temps réseau).

Cependant, dans la mesure où la différence entre le temps réseau et le temps d'hôte est incertaine, cette incertitude doit être prise en compte par une analyse d'une certaine méthode de mesure. On note H_{source} la limite supérieure de l'incertitude sur la différence entre temps réseau et temps d'hôte sur l'hôte source, et on définit de même H_{dest} pour l'hôte de destination. On note alors que ces problèmes introduisent une incertitude totale de $H_{\text{source}} + H_{\text{dest}}$. Cette estimation de l'incertitude totale réseau par rapport à hôte devrait être incluse dans l'analyse d'erreur/incertitude de toute mise en œuvre de mesure.

3.7.3 Calibrage des erreurs et incertitudes

Généralement, les valeurs mesurées peuvent être décomposées comme suit :

valeur mesurée = vraie valeur + erreur systématique + erreur aléatoire

Si l'erreur systématique (le biais constant des valeurs mesurées) peut être déterminée, elle peut être compensée dans les résultats rapportés.

valeur rapportée = valeur mesurée – erreur systématique

donc : valeur rapportée = vraie valeur + erreur aléatoire

Le but du calibrage est de déterminer l'erreur systématique et l'erreur aléatoire générées par les hôtes eux-mêmes en autant de détail que possible. Au minimum, une limite ("e") devrait être trouvée telle que la valeur rapportée soit dans la gamme (vraie valeur - e) à (vraie valeur + e) au moins dans 95 % des cas. On appelle "e" l'erreur de calibrage pour les mesures. Elle

représente le degré auquel les valeurs produites par l'hôte de mesure sont répétables ; c'est-à-dire, dans quelle mesure un délai réel de 30 ms est rapporté comme 30 ms. {Commentaire : 95 % a été choisi parce que (1) un certain niveau de confiance est souhaitable pour être capable de supprimer les anomalies, qui vont se trouver dans les mesures de toute propriété physique ; (2) un niveau de confiance particulier devrait être spécifié afin que les résultats de mises en œuvre indépendantes puissent être comparés ; et (3) même avec un prototype de mise en œuvre au niveau utilisateur, 95 % est assez lâche pour exclure les anomalies indépendantes.}

De la discussion des deux paragraphes précédents, l'erreur de mesures pourrait être bordée en déterminant toutes les incertitudes individuelles, et en les additionnant pour former : $E_{\text{synch}}(t) + R_{\text{source}} + R_{\text{dest}} + H_{\text{source}} + H_{\text{dest}}$.

Cependant, des limites raisonnables sur l'incertitude relative à l'horloge saisie par les trois premiers termes et l'incertitude relative à l'hôte saisie par les trois derniers termes devraient être possibles par des techniques de conception soigneuses et en calibrant les hôtes à l'aide d'un réseau de laboratoire isolé connu.

Par exemple, les incertitudes relatives à l'horloge sont notablement réduites par l'utilisation d'une source horaire GPS. La somme de $E_{\text{synch}}(t) + R_{\text{source}} + R_{\text{dest}}$ est petite et est aussi limitée pour la durée de la mesure parce que la source horaire est mondiale.

Les incertitudes relatives à l'hôte, $H_{\text{source}} + H_{\text{dest}}$, pourraient être bordées en connectant deux hôtes dos à dos avec une liaison série à haut débit ou un segment de LAN isolé. Dans ce cas, des mesures répétées mesurent le même délai unidirectionnel.

Si les paquets d'essai sont petits, une telle connexion réseau a un délai minimal qui peut être approximé à zéro. Le délai mesuré contient donc seulement les erreurs systématiques et aléatoires des hôtes de mesure. La "valeur moyenne" de mesures répétées est l'erreur systématique, et la variation est l'erreur aléatoire.

Une façon de calculer l'erreur systématique et l'erreur aléatoire à un intervalle de confiance de 95 % est de répéter l'expérience de nombreuses fois – au moins des centaines d'essais. L'erreur systématique sera alors la moyenne. L'erreur aléatoire pourra alors être trouvée en retirant cette erreur systématique des valeurs mesurées. L'intervalle de confiance de 95 % sera dans la gamme du 2,5ème centile au 97,5ème centile de ces déviations de la vraie valeur. L'erreur de calibrage "e" pourra alors être prise comme la plus grande valeur absolue de ces deux nombres, plus l'incertitude relative à l'horloge. {Commentaire : comme décrite, cette limite est relativement lâche car les incertitudes sont ajoutées, et la valeur absolue du plus grand écart est utilisée. Tant que la valeur résultante n'est pas une fraction significative des valeurs mesurées, c'est une limite raisonnable. Si la valeur résultante est une fraction significative des valeurs mesurées, des méthodes plus exactes seront nécessaires pour calculer l'erreur de calibrage.}

Noter que l'erreur aléatoire est une fonction de la charge de mesure. Par exemple, si de nombreux chemins sont mesurés par un hôte, cela peut augmenter les interruptions, la programmation des procès, et les entrées/sorties de disque (par exemple, pour enregistrer les mesures) qui peuvent tous ensemble augmenter l'erreur aléatoire dans les singletons mesurés. Donc, en plus des mesures de charge minimale pour trouver l'erreur systématique, les mesures de calibrage devraient être effectuées avec la même charge de mesures que les hôtes verront sur le terrain.

On rappelle que ce traitement statistique se réfère au calibrage de l'hôte ; il est utilisé pour "calibrer la pile de mesure" et dit comment la pile de mesure reflète la réalité.

En plus du calibrage des hôtes pour un délai unidirectionnel fini, deux vérifications devraient être faites pour s'assurer que les paquets rapportés comme perdus le sont réellement. D'abord, le seuil de perte devrait être vérifié. En particulier, s'assurer que le seuil "raisonnable" est raisonnable : c'est-à-dire qu'il est très peu probable qu'un paquet arrive après la valeur seuil, et donc que le nombre de paquets perdus sur un intervalle n'est pas sensible à la limite d'erreur sur les mesures. Ensuite, on examine la possibilité qu'un paquet arrive à l'interface réseau, mais soit perdu du fait de l'encombrement sur cette interface ou de l'épuisement d'autres ressource (par exemple, des mémoires tampon) chez l'hôte.

3.8 Rapport de métrique

Le calibrage et le contexte dans lesquels la métrique est mesurée DOIVENT être examinés avec attention et DEVRAIENT toujours être rapportés avec les résultats de la métrique. On présente maintenant quatre éléments à examiner : le Type-P du paquet d'essais, le seuil de délai infini (s'il y en a un), le calibrage d'erreur, et le chemin traversé par le paquet d'essais. Cette liste n'est pas exhaustive ; toutes informations supplémentaires qui pourraient être utiles pour interpréter l'applications des métriques devraient aussi être rapportées (voir dans la [RFC6703] une discussion étendue des considérations de rapport pour différentes audiences).

3.8.1 Type-P

Comme noté à la Section 13 du document cadre [RFC2330], la valeur de la métrique peut dépendre du type des paquets IP utilisés pour faire les mesures, ou "Type-P". La valeur du Type-P-One-way-Delay pourrait changer si le protocole (UDP ou TCP), le numéro d'accès, la taille, ou l'arrangement pour un traitement spécial (par exemple, le champ DS IP [RFC2780], la notification d'encombrement explicite (ECN, *Explicit Congestion Notification*) [RFC3168], ou RSVP) change.

Des distinctions de paquet supplémentaires identifiées dans de futures extensions de la définition du Type-P s'appliqueront. Le type P exact utilisé pour faire les mesures DOIT être précisément rapporté.

3.8.2 Seuils de perte

De plus, le seuil (ou la méthodologie pour distinguer) entre un grand délai fini et la perte DOIT être rapporté.

3.8.3 Résultats du calibrage

- o Si l'erreur systématique peut être déterminée, elle DEVRAIT être retirée des valeurs mesurées.
- o On DEVRAIT aussi rapporter l'erreur de calibrage, e , afin que la vraie valeur soit la valeur rapportée plus ou moins e , avec un intervalle de confiance de 95 % (voir le dernier paragraphe).
- o Si possible, les conditions dans lesquelles un paquet d'essai avec un délai fini est rapporté comme perdu du fait de l'épuisement de ressources chez l'hôte de mesure DEVRAIENT être rapportées.

3.8.4 Chemin

Finalement, le chemin traversé par le paquet DEVRAIT être rapporté, si possible. En général, il est impossible de savoir le chemin précis que prend un certain paquet à travers le réseau. Le chemin précis peut être connu pour certains Type-P sur des chemins courts ou stables. Si le Type-P inclut l'option de chemin enregistré (ou chemin enregistré lâche) dans l'en-tête IP, et si le chemin est assez court, et si tous les routeurs* sur le chemin prennent en charge l'enregistrement de chemin (ou la source lâche) le chemin sera alors enregistré précisément. Ceci est impraticable parce que le chemin doit être assez court, de nombreux routeurs ne prennent pas en charge (ou ne sont pas configurés pour) l'enregistrement de chemin, et l'utilisation de ce dispositif dégrade souvent artificiellement les performances observées en retirant le paquet du traitement courant. Cependant, des informations partielles sont quand même un contexte précieux. Par exemple, si un hôte peut choisir entre deux liaisons* (et donc deux chemins séparés de Src à Dst), la liaison initiale utilisée est un contexte précieux. {Commentaire : Par exemple, avec l'établissement NetNow de Merit, une source sur un point d'accès réseau (NAP, *Network Access Point*) peut atteindre une destination sur un autre NAP par l'un ou l'autre de plusieurs différents réseaux centraux.}

4. Définition d'échantillons de délai unidirectionnel

Étant donnée la métrique de singleton Type-P-One-way-Delay, on définit maintenant un échantillon particulier de ces singletons. L'idée de l'échantillon est de choisir un lien particulier des paramètres Src, Dst, et Type-P, puis de définir un échantillon des valeurs du paramètre T. Le moyen pour définir les valeurs de T est de choisir un temps de début T_0 , un temps de fin T_f , et un taux moyen λ , puis de définir un processus de Poisson pseudo aléatoire de taux λ , dont les valeurs tombent entre T_0 et T_f .

L'intervalle de temps entre les valeurs successives de T alors avoir pour moyenne $1/\lambda$.

Noter que l'échantillonnage de Poisson est seulement une des façons de définir un échantillon. La loi de Poisson présente l'avantage de limiter les biais, mais d'autres méthodes d'échantillonnage seront appropriées pour des situations différentes. Par exemple, une distribution de Poisson tronquée peut être nécessaire pour éviter des changements en réaction de l'état du réseau durant les intervalles d'inactivité, voir au paragraphe 4.6 de la [RFC7312]. Parfois, le but est l'échantillonnage avec un biais connu, et la [RFC3432] décrit une méthode pour l'échantillonnage périodique avec des instants de début aléatoires.

4.1 Nom de la métrique

Type-P-One-way-Delay-Poisson-Stream

4.2 Paramètres de la métrique

- o Src, adresse IP d'un hôte
- o Dst, adresse IP d'un hôte

- o T_0 , un instant
- o T_f , un instant
- o T_{max} , seuil d'attente de perte
- o λ , taux en secondes réciproques (ou paramètres pour une autre distribution)

4.3 Unités de la métrique

Une séquence de paires ; les éléments de chaque paire sont :

- o T , un instant,
- o dT , un nombre réel ou indéfini de secondes.

Les valeurs de T dans la séquence sont à accroissement monotone. Noter que T serait un paramètre valide de Type-P-One-way-Delay et que dT serait une valeur valide de Type-P-One-way-Delay.

4.4 Définition

Connaissant T_0 , T_f , et λ , on calcule un processus pseudo aléatoire de Poisson débutant à T_0 ou avant, avec un taux moyen d'arrivée λ , et se terminant à T_f ou après. Ces valeurs de temps supérieures ou égales à T_0 et inférieures ou égales à T_f sont alors choisies. À chacun des instants choisis dans ce procès, on obtient une valeur de Type-P-One-way-Delay. La valeur de l'échantillon est la séquence constituée des paires <instant, délai> résultantes. Si il n'y a aucune de ces paires, la séquence est de longueur zéro et l'échantillon est dit vide.

4.5 Discussion

Le lecteur devrait être familiarisé avec l'exposé en profondeur sur l'échantillonnage de Poisson dans le document cadre [RFC2330], qui inclut les méthodes pour calculer et vérifier le processus pseudo aléatoire de Poisson.

La seule contrainte spécifique de la valeur de λ est de noter les extrêmes. Si le taux est trop fort, la mesure de trafic va perturber le réseau et causer par elle-même de l'encombrement. Si le taux est trop faible, on ne peut pas capturer le comportement de réseau intéressant. {Commentaire : on prévoit de documenter notre expérience et nos suggestions sur λ dans un autre document de "bonnes pratiques actuelles".}

Comme une séquence de nombres pseudo aléatoires est employée, la séquence des instants, et donc la valeur de l'échantillon, n'est pas complètement spécifiée. Des générateurs de nombres pseudo aléatoires de bonne qualité seront nécessaires pour atteindre les qualités désirées.

L'échantillon est défini dans les termes d'un processus de Poisson à la fois pour éviter les effets d'auto synchronisation et pour capturer un échantillon qui soit statistiquement aussi peu biaisé que possible. {Commentaire : on ne prétend pas, bien sûr, que le trafic réel de l'Internet arrive conformément à un processus d'arrivée de Poisson.} Le processus de Poisson est utilisé pour programmer les mesures de délai. Les paquets d'essais ne vont généralement pas arriver à Dst selon une distribution de Poisson car ils sont influencés par le réseau.

Toutes les métriques de singleton de Type-P-One-way-Delay dans la séquence auront les mêmes valeurs de Src, Dst, et Type-P.

Noter aussi que, étant donné un échantillon qui va de T_0 à T_f , et de nouvelles valeurs de temps T_0' et T_f' telles que $T_0 \leq T_0' \leq T_f' \leq T_f$, la sous séquence de l'échantillon dont les valeurs de temps tombent entre T_0' et T_f' sont aussi un échantillon de Type-P-One-way-Delay-Poisson-Stream valide.

4.6 Méthodologies

Les méthodologies découlent directement de :

- o la sélection d'instant spécifiques utilisant le processus d'arrivée de Poisson spécifié, et
- o de la discussion des méthodologies déjà fournies pour la métrique de singleton Type-P-One-way-Delay.

Il faut veiller à traiter correctement les arrivées décalées de paquet d'essais ; il est possible que la source puisse envoyer un paquet d'essai à $TS[i]$, puis en envoyer un second (plus tard) à $TS[i+1]$ tandis que la destination pourrait recevoir le second paquet d'essai à $TR[i+1]$, et ensuite recevoir le premier (plus tard) à $TR[i]$. On peut trouver des métriques pour la remise en ordre dans la [RFC4737].

4.7 Erreurs et incertitudes

En plus des sources d'erreurs et d'incertitudes associées aux méthodes employées pour mesurer les valeurs de singletons qui constituent l'échantillon, on doit veiller à analyser la précision du processus de Poisson par rapport à l'heure du réseau de l'envoi des paquets d'essais. Des problèmes avec ce processus pourraient être causés par plusieurs choses, incluant des problèmes avec les techniques de nombres pseudo aléatoires utilisées pour générer le processus de Poisson d'arrivée, ou avec la gigue dans la valeur de Hsource (mentionnée ci-dessus comme l'incertitude dans la métrique de délai de singleton). Le document cadre montre comment utiliser le test d'Anderson-Darling pour vérifier la précision d'un processus de Poisson sur des trames de temps courtes. {Commentaire : Le but est de s'assurer que les paquets d'essais sont envoyés "assez près" d'un processus de Poisson et d'éviter un comportement périodique.}

4.8 Rapport de métrique

Le calibrage et le contexte pour les singletons sous-jacents DOIT être rapporté avec le flux. (Voir à "Rapporter la métrique" pour Type-P-One-way-Delay au paragraphe 3.8.)

5. Définitions de statistiques pour délai unidirectionnel

Étant donnée l'échantillon de métrique Type-P-One-way-Delay-Poisson-Stream, on offre maintenant plusieurs statistiques de cet échantillon. Ces statistiques sont présentées pour illustrer ce qu'on peut faire. Voir dans la [RFC6703] un exposé supplémentaire sur les statistiques pertinentes pour différentes audiences.

5.1 Type-P-One-way-Delay-Percentile

Étant donné un flux de Poisson de délai unidirectionnel de type P (*Type-P-One-way-Delay-Poisson-Stream*) et un pourcentage X entre 0 % et 100 %, le Xème centile de toutes les valeurs dT dans le flux. En calculant ce centile, les valeurs indéfinies sont traitées comme infiniment grandes. Noter que cela signifie que le centile pourrait donc être indéfini (informellement, infini). De plus, le Type-P-One-way-Delay-Percentile est indéfini si l'échantillon est vide.

Par exemple: supposons qu'on prenne un échantillon et que le résultat soit :

```
Flux1 = <
  <T1, 100 ms>
  <T2, 110 ms>
  <T3, indéfini>
  <T4, 90 ms>
  <T5, 500 ms>
  >
```

Le 50ème centile sera alors 110 ms, car 90 ms et 100 ms sont plus petits, et 500 ms et "indéfini" sont plus grands. Voir au paragraphe 11.3 de la [RFC2330] le calcul des centiles.

Noter que si la possibilité qu'un paquet de délai fini soit rapporté comme perdu est significative, un centile élevé (90ème ou 95ème) pourrait être rapporté comme infini au lieu de fini.

5.2 Type-P-One-way-Delay-Median

Soit un flux Type-P-One-way-Delay-Poisson-Stream, la médiane de toutes les valeurs dT dans le flux. En calculant la médiane, les valeurs indéfinies sont traitées comme infiniment grandes. Comme avec le Type-P-One-way-Delay-Percentile, Type-P-One-way-Delay-Median est indéfini si l'échantillon est vide.

Comme noté dans le document cadre, la médiane diffère du 50ème centile seulement lorsque l'échantillon contient un nombre pair de valeurs, auquel cas la moyenne des deux valeurs centrales est utilisée.

Par exemple, supposons qu'on prenne un échantillon dont le résultat serait :

```
Flux2 = <
  <T1, 100 ms>
  <T2, 110 ms>
  <T3, indéfini>
```

<T4, 90 ms>
>

La médiane serait alors 105 ms, la moyenne de 100 ms et 110 ms, les deux valeurs centrales.

5.3 Type-P-One-way-Delay-Minimum

Soit un flux Type-P-One-way-Delay-Poisson-Stream, le minimum de toutes les valeurs dT dans le flux. En le calculant, les valeurs indéfinies sont traitées comme infiniment grandes. Noter que cela signifie que le minimum pourrait donc être indéfini (informellement, infini) si toutes les valeurs dT sont indéfinies. De plus, le Type-P-One-way-Delay-Minimum est indéfini si l'échantillon est vide.

Dans l'exemple ci-dessus, le minimum serait 90 ms.

5.4 Type-P-One-way-Delay-Inverse-Percentile

Note : cette statistique est déconseillée dans le présent document à cause d'un manque d'utilisation.

Soit un flux Type-P-One-way-Delay-Poisson-Stream et un seuil de durée, la fraction de toutes les valeurs dT dans le flux inférieures ou égales au seuil. Le résultat pourrait aussi bas que 0 % (si toutes les valeurs dT excèdent le seuil) ou aussi élevé que 100 %. Le Type-P-One-way-Delay-Inverse-Percentile est indéfini si l'échantillon est vide.

Dans l'exemple ci-dessus, le centile inverse de 103 ms serait 50 %.

6. Considérations sur la sécurité

Effectuer des mesures sur l'Internet soulève des problèmes de sécurité et de confidentialité. Le présent mémoire ne spécifie pas une mise en œuvre des métriques, de sorte qu'il n'affecte pas directement la sécurité de l'Internet ni des applications qui fonctionnent sur l'Internet. Cependant, les mises en œuvre de ces métriques doivent être conscientes des problèmes de sécurité et de confidentialité.

Il y a deux types de problèmes de sécurité : le dommage potentiel causé par les mesures et le dommage potentiel aux mesures. Les mesures pourraient causer des dommages parce qu'elles sont actives et injectent des paquets dans le réseau. Les paramètres de mesure DOIVENT être choisis avec soin afin que les mesures injectent des quantités minimales de trafic supplémentaire dans les réseaux qu'elles mesurent. Si elles injectent "trop" de trafic, elles peuvent biaiser le résultat de la mesure et dans des cas extrêmes causer de l'encombrement et un déni de service.

Les mesures elles-mêmes pourraient être endommagées par les routeurs qui donneraient au trafic de mesures une priorité différente du trafic "normal" ou par un attaquant qui injecterait du trafic de mesure artificiel. Si les routeurs peuvent reconnaître le trafic de mesure et le traiter séparément, la mesure ne reflètera pas le trafic d'utilisateur réel. Donc, les méthodologies de mesure DEVRAIENT inclure des techniques appropriées pour réduire la probabilité que le trafic de mesure puisse être distingué du trafic "normal".

Si un attaquant injecte des paquets simulant du trafic accepté comme légitime, le taux de perte ou autres valeurs mesurées sera altéré. Des techniques d'authentification, comme les signatures numériques, peuvent être utilisées lorsque approprié pour se garder contre les attaques de trafic injecté.

Lorsque on considère la confidentialité de ceux qui sont impliqués dans les mesures ou ceux dont le trafic est mesuré, les informations sensibles disponibles à des observateurs potentiels sont considérablement réduites lorsque on utilise les techniques actives qui sont mentionnées dans le présent travail. Les observations passives du trafic d'utilisateur pour les besoins des mesures soulèvent de nombreux problèmes de confidentialité. On renvoie le lecteur aux considérations sur la confidentialité décrites dans le cadre pour mesures à grande échelle de performances de haut débit (LMAP, *Large Scale Measurement of Broadband Performance*) [RFC7594], qui couvre les techniques actives et passives.

La collecte des mesures ou l'utilisation des résultats de mesures pour la reconnaissance pour aider à une attaque ultérieure du système est assez courante. L'accès aux résultats de mesures, ou le contrôle des systèmes de mesure pour effectuer la reconnaissance devrait être protégés. Voir à la Section 7 de la [RFC7594] (Considérations sur la sécurité du cadre LMAP) les exigences système qui aident à éviter la compromission du système de mesures.

7. Changements depuis la RFC 2679

Le texte ci-dessus constitue une révision de la RFC 2679, et est maintenant une norme de l'Internet. Cette section retrace les changements par rapport à la [RFC2679].

La [RFC6808] donne le plan d'essais et les résultats qui soutiennent l'avancement de la [RFC2679] sur la voie de la normalisation, conformément au procès de la [RFC6576]. Les conclusions de la [RFC6808] citent quatre modifications mineures :

1. Le paragraphe 6.2.3 de la [RFC6808] affirme que l'hypothèse d'un post traitement pour appliquer un seuil de temps d'attente constant est conforme et que le texte de la RFC devrait être légèrement révisé pour inclure ce point. L'applicabilité du post traitement a été ajoutée dans le dernier élément de la liste du paragraphe 3.6.
2. Le paragraphe 6.5 de la [RFC6808] indique que la statistique Type-P-One-way-Delay-Inverse-Percentile a été ignorée dans les deux mises en œuvre, et qu'elle est donc candidate au retrait ou à être déconseillée dans ce document (cette petite discordance n'affecte pas la candidature à l'avancement). Cette statistique est déconseillée au paragraphe 5.4.
3. L'IETF est arrivée à un consensus sur les directives sur le rapport des métriques dans la [RFC6703], et ce mémoire est référencé dans le présent document pour incorporer l'expérience récente lorsque approprié. Cette référence a été ajoutée dans le dernier élément de la liste du paragraphe 3.6, au paragraphe 3.8, et à la Section 5.
4. Il y a actuellement un erratum avec le statut "Conservé pour la mise à jour du document" (EID 398) pour la [RFC2679], et cette révision mineure et l'ajout de texte ont été incorporés au paragraphe 5.1 du présent document.

Un certain nombre de mises à jour au texte de la [RFC2679] ont été apportées dans le texte ci-dessus pour faire référence aux RFC clés de IPPM qui ont été approuvées après la [RFC2679] et pour répondre aux commentaires des listes de diffusion IPPM qui décrivent les conditions et expérience actuelles.

1. Vers la fin du paragraphe 1.1, il y a une mise à jour d'un exemple de réseau utilisant ATM, une précision de l'effet de TCP sur l'occupation de la file d'attente, et une discussion de l'importance de la mesure du délai unidirectionnel.
2. L'inclusion explicite du paramètre d'entrée du temps d'attente maximum aux paragraphes 3.2 et 4.2, reflétant la reconnaissance de ce paramètre dans les RFC les plus récentes et dans la Recommandation UIT-T Y.1540.
3. Ajout d'une référence à la RFC 6703 dans la discussion de la durée de vie du paquet et des fins de temporisation d'application au paragraphe 3.5.
4. Ajout d'une référence à l'exigence par défaut (que les paquets soient formés de façon standard) provenant de la RFC 2330 comme nouvel élément de la liste du paragraphe 3.5.
5. L'expérience de NTP fondé sur le GPS remplace le "à essayer" au paragraphe 3.5.
6. Remplacé "préséance" par la terminologie à jour (champ DS) aux paragraphes 3.6 et 3.8.1 (avec les références).
7. Ajout d'une directive entre parenthèses sur la minimisation de l'intervalle entre l'apposition de l'horodatage au moment de l'envoi au paragraphe 3.6.
8. Le paragraphe 3.7.2 note que certains systèmes actuels effectuent l'horodatage de l'hôte sur le matériel d'interface réseau.
9. "instrument" a été remplacé par le terme défini "hôte" aux paragraphes 3.7.3 et 3.8.3.
10. Ajout d'une référence à la RFC 3432 concernant l'échantillonnage périodique pendant un échantillonnage de Poisson à la Section 4 et aussi noté qu'une distribution de Poisson tronquée peut être nécessaire avec les réseaux modernes comme décrit dans la mise à jour du cadre IPPM [RFC7312].
11. Ajout d'une référence à la RFC 4737 concernant les métriques de remise en ordre dans la discussion relative aux méthodologies (paragraphe 4.6).
12. Modification du formatage de l'exemple du paragraphe 5.1 pour correspondre à l'original (produit par conversion en XML dans cette version).
13. Précisé les conclusions sur deux points de dommages aux mesures (reconnaissance du trafic de mesure pour un traitement

de priorité inattendu et trafic attaquant qui simule les mesures) dans les "Considérations sur la sécurité" (Section 6).

14. Développement et mise à jour des éléments sur la confidentialité et ajout d'un avertissement sur l'utilisation de mesures pour la reconnaissance dans les "Considérations sur la sécurité" (Section 6).

Le paragraphe 5.4.4 de la [RFC6390] suggère un gabarit commun pour les métriques de performances partiellement déduites de RFC antérieures des groupes de travail IPPM et méthodologie de référencement (BMWG) mais il contient aussi des éléments nouveaux. Toutes les parties normatives de la [RFC6390] sont couvertes, mais pas dans les mêmes noms de section ou orientation. Plusieurs des parties pour information sont couvertes. Conserver l'aspect familier de la littérature IPPM a à la fois de la valeur et minimise les différences inutiles entre cette RFC révisée et les futures ou actuelles RFC IPPM.

La publication de la [RFC6921] suggérerait un domaine où le présent mémoire pourrait faire une mise à jour. Le transfert de paquets sur les réseau plus rapides que la lumière (FTL, *Faster-Than-Light*) pourrait résulter en délais négatifs et en réarrangement de l'ordre des paquets ; cependant, tous deux sont couverts comme possibilités dans le texte actuel et aucune révision n'est jugée nécessaire (on note aussi que la [RFC6921] est une RFC du 1^{er} avril).

8. Références

8.1 Références normatives

- [RFC0791] J. Postel, éd., "Protocole Internet - Spécification du [protocole du programme Internet](#)", STD 5, septembre 1981. DOI 10.17487/RFC0791
- [RFC2119] S. Bradner, "[Mots clés à utiliser](#) dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. (*MàJ par RFC8174*). DOI 10.17487/RFC2119.
- [RFC2330] V. Paxson, G. Almes, J. Mahdavi, M. Mathis, "[Cadre pour la mesure des performances](#) d'IP", mai 1998. (*Information ; MàJ par RFC8468*). DOI 10.17487/RFC2330.
- [RFC2678] J. Mahdavi, V. Paxson, "[Métrique IPPM pour la mesure de la connexité](#)", septembre 1999. (*P.S.*), DOI 10.17487/RFC2678.
- [RFC2679] G. Almes, S. Kalidindi, M. Zekauskas, "[Métrique de délai unidirectionnel pour IPPM](#)", septembre 1999. (*P.S. ; Remplacée par RFC7679*, STD 81), DOI 10.17487/RFC2679.
- [RFC2780] S. Bradner et V. Paxson, "[Lignes directrices pour les allocations](#) par l'IANA des valeurs du protocole Internet et des en-têtes qui s'y rapportent", BCP 37, mars 2000. DOI 10.17487/RFC2780.
- [RFC3432] V. Raisenen et autres, "Mesure des [performances réseau avec des flux périodiques](#)", novembre 2002. (*P.S.*), DOI 10.17487/RFC3432.
- [RFC6576] R. Geib, A. Morton, R. Fardid, A. Steinmitz, "Essais pour l'avancement de la normalisation des métriques de performances IP (IPPM)", mars 2012. (BCP0176), DOI 10.17487/RFC6576.
- [RFC7312] J. Fabini, A. Morton, "Cadre évolué de flux et d'échantillonnage pour les métriques de performance IP (IPPM)", août 2014. (*Information*), DOI 10.17487/RFC7312.
- [RFC7680] G. Almes, et autres, "[Métrique de perte unidirectionnelle](#) pour les performances de IP (IPPM)" janvier 2016. STD 82 ; (*Remplace RFC2680*), DOI 10.17487/RFC7680.

8.2 Références pour information

- [IPPM-UPDATES] Morton, A., Fabini, J., Elkins, N., Ackermann, M., and V. Hegde, "Updates for IPPM's Active Metric Framework: Packets of Type-P and Standard-Formed Packets", Travail en cours, draft-morton-ippm-2330-stdform-typep-02, décembre 2015.
- [RFC3168] K. Ramakrishnan et autres, "Ajout de la [notification explicite d'encombrement](#) (ECN) à IP", septembre 2001. (*P.S.* ; *MàJ par RFC8311*), DOI 10.17487/RFC3168.

- [RFC4737] A. Morton et autres, "Métrieque de remise des paquets dans l'ordre", novembre 2006. (*P.S.*), DOI 10.17487/RFC4737.
- [RFC6390] A. Clark, B. Claise, "Lignes directrices pour la prise en considération des nouveaux développements de mesure de performances", octobre 2011. (BCP0170), DOI 10.17487/RFC6390.
- [RFC6703] A. Morton, G. Ramachandran, G. Maguluri, "Rapport des métriques de performances de réseau IP : Points de vue différents", août 2012. (*Information*), DOI 10.17487/RFC6703.
- [RFC6808] L. Ciavattoni, R. Geib, A. Morton et M. Wieser, "Plan et résultats d'essais pour la prise en charge de l'avancement de la RFC 2679 sur la voie de la normalisation", décembre 2012. (*Information*), DOI 10.17487/RFC6808.
- [RFC6921] R. Hinden, "Considérations sur la conception de la communication plus rapide que la lumière (FTL)", 1^{er} avril 2013 (*Info.*), DOI 10.17487/RFC6921.
- [RFC7594] P. Eardley, et autres, "Cadre pour mesures à grande échelle de performances de haut débit", septembre 2015. (*Info*), DOI 10.17487/RFC7594.

Remerciements

Pour la [RFC2679], des remerciements particuliers sont dus à Vern Paxson de Lawrence Berkeley Labs pour ses commentaires sur les problèmes d'incertitude d'horloge et de statistiques. Merci aussi à Garry Couch, Will Leland, Andy Scherrer, Sean Shapira, et Roland Wittig pour plusieurs suggestions utiles.

Pour le présent document, merci à Joachim Fabini, Ruediger Geib, Nalini Elkins, et Barry Constantine pour le partage de leur expérience des mesures au titre de leur relecture attentive. Brian Carpenter et Scott Bradner ont fourni des retours utiles lors du dernier appel de l'IETF.

Adresse des auteurs

Al Morton (éditeur)
AT&T Labs
200 Laurel Avenue South
Middletown, NJ 07748
United States
téléphone : +1 732 420 1571
mél : acmorton@att.com

Guy Almes
Texas A&M
mél : almes@acm.org

Sunil Kalidindi
Ixia
mél : skalidindi@ixiacom.com

Matt Zekauskas
Internet2
mél : matt@internet2.edu