Équipe d'ingénierie de l'Internet (IETF)
**Request for Comments : 7680**
**STD 82**
RFC rendue obsolète : 2680
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 perte unidirectionnelle pour les métriques de performance IP (IPPM)

**Résumé**
Le présent mémoire définit une métrique pour la perte unidirectionnelle des paquets sur les chemins de l'Internet. Il s'appuie sur les notions introduites et discutées dans le document cadre des métriques de performances IP (IPPM, *IP Performance Metrics*) [RFC2330] dont le lecteur est supposé familier. Le présent document rend obsolète la RFC 2680.

**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/rfc7680



## Table des Matières

# 1. Introduction

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

Le présent mémoire est destiné à être parallèle par sa structure au document qui l'accompagne pour le délai unidirectionnel ("Métrique de délai unidirectionnel pour les métriques de performances IP (IPPM)") [RFC7679] ; le lecteur est supposé être familier avec ce document.

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 :
- Une métrique analytique de "singleton*", appelée Type-P-One-way-Packet-Loss *(perte de paquet unidirectionnelle de type P)* sera introduite pour mesurer une seule observation de transmission ou perte de paquet.
- En utilisant cette métrique de singleton, un "échantillon*" appelé Type-P-One-way-Packet-Loss-Poisson-Stream *(flux de Poisson de perte de paquet unidirectionnelle de type P)* est introduit pour mesurer une séquence de singletons de transmission et/ou perte envoyés à des instants tirés d'un processus de Poisson, comme défini au paragraphe 11.1.1 de la [RFC2330].
- 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 la perte de paquet unidirectionnelle de paquets de Type-P* provenant d'un hôte* de source à un hôte de destination est utile pour plusieurs raisons :
- Certaines applications ne fonctionnent pas bien (ou pas du tout) si la perte de bout en bout entre les hôtes est grande par rapport à une certaine valeur seuil.
- Une perte de paquet excessive peut rendre difficile de prendre en charge certaines applications en temps réel (où le seuil précis de "excessif" dépend de l'application).
- Plus grande est la valeur de la perte de paquets, plus il est difficile aux protocoles de couche transport de tenir une forte bande passante.
- La sensibilité à la perte des applications de temps réel et des protocoles de couche transport devient particulièrement importante lorsque des produits à très forts délais/bandes passantes doivent être pris en charge.

La mesure de la perte unidirectionnelle au lieu de la perte sur l'aller-retour est motivée par les facteurs suivants :

- 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 de routeurs différentes 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).

- Même lorsque deux chemins sont symétriques, ils peuvent avoir des caractéristiques de performances radicalement différentes dues à une mise en file d'attente asymétrique.

- 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.

- 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 perte seraient appliquées à des problèmes spécifiques.

### 1.2. 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.}

## 2. Définition d'un singleton pour perte de paquet unidirectionnelle

### 2.1 Nom de la métrique

Type-P-One-way-Packet-Loss

### 2.2. Paramètres de la métrique

- Src, adresse IP d'un hôte

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

### 2.3 Unités de la métrique

La valeur d'un Type-P-One-way-Packet-Loss est soit zéro (signifiant une transmission réussie du paquet) soit un (signifiant la perte).

### 2.4 Définition

>>*Type-P-One-way-Packet-Loss* de Src à Dst à T est 0<< 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 ce paquet.

>>*Type-P-One-way-Packet-Loss* de Src à Dst à T est 1 << 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 temps d'attente de seuil de perte, Tmax).

### 2.5 Discussion

Donc, Type-P-One-way-Packet-Loss est 0 exactement quand Type-P-One-way-Delay est une valeur finie, et il est 1 exactement quand Type-P-One-way-Delay est indéfini.

Les problèmes suivants vont se poser en pratique :

- o Une méthodologie devra inclure un moyen de distinguer entre une perte de paquet et un très long délai (mais fini). 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, il peut n'y avoir aucun dommage à traiter un grand délai comme une perte de paquet. Un paquet de restitution audio, par exemple, qui arrive seulement après le point où il aurait dû être exécuté, peut tout aussi bien être perdu. Voir au paragraphe 4.1.1 de la [RFC6703] l'examen des délais de paquet anormaux et l'estimation des performances d'applications.}

- o Si le paquet arrive mais est corrompu, il est alors compté comme perdu. {Commentaire : on est tenté de compter le paquet comme reçu car la corruption et la perte de paquet sont des phénomènes en rapport mais distincts. Si l'en-tête IP est corrompu, on ne peut cependant pas être sûr des adresses IP de source ou de destination et on est donc sur un terrain mouvant quant à savoir si le paquet corrompu reçu correspond à un certain paquet d'essai envoyé. De même, si d'autres parties du paquet nécessaires à la méthodologie pour savoir si le paquet reçu corrompu correspond à un certain paquet d'essai envoyé, un tel paquet devrait alors être compté comme perdu. Il ne serait pas cohérent de compter les paquets avec des champs spécifiques de la méthodologie corrompus comme perdus, et de ne pas compter les paquets avec d'autres aspects corrompus dans la même catégorie.} La Section 15 de la [RFC2330] définit le paquet de "forme standard" qui est applicable à toutes les métriques. Noter que pour l'instant la définition de paquets de forme standard ne s'applique qu'à IPv4 (voir aussi [IPPM-UPDATES]).

- 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.

- o Si le paquet est fragmenté et si, pour une raison quelconque, le réassemblage ne se fait pas, le paquet sera alors réputé perdu.

### 2.6 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, une méthodologie possible va procéder comme suit :

- o S'arranger pour que Src et Dst aient des horloges synchronisées l'une avec l'autre. Le degré de synchronisation est un paramètre de la méthodologie et dépend du seuil utilisé pour déterminer la perte (voir ci-dessous).

- 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.

- 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, la perte de paquet unidirectionnelle est prise pour zéro (et prend un horodatage aussitôt que possible à réception du paquet).

- o Si le paquet manque à arriver dans un délai raisonnable, Tmax, la perte de paquet unidirectionnelle est prise pour un. Noter que le seuil de "raisonnable" est ici un paramètre de la métrique.

{Commentaire : la définition de raisonnable est intentionnellement vague et est destinée à indiquer une valeur "Th" si grande que toute valeur dans l'intervalle fermé [Th-delta, Th+delta] soit un équivalent du seuil de perte. Ici, delta englobe toutes les erreurs de synchronisation et d'acquisition d'horloge et d'allocation d'horodatage sur le chemin mesuré. Si il y a une seule valeur, Tmax, après laquelle le paquet doit être compté comme perdu, on réintroduit alors le besoin d'un degré de synchronisation d'horloge similaire à celui utilisé pour le délai unidirectionnel, et virtuellement tous les systèmes pratiques de mesure combinent les méthodes pour le délai et la perte. Donc, si une mesure de perte de paquet paramétrée par une valeur de temporisation spécifique "raisonnable" non énorme est nécessaire, on peut toujours mesurer le délai unidirectionnel et voir quel pourcentage de paquets pour un certain flux excède une certaine valeur de temporisation. Ce point est examiné en détail dans la [RFC6703], incluant les préférences d'analyse pour allouer des délai indéfinis aux paquets qui manquent à arriver avec les difficultés résultant de l'allocation informelle de "délai infini", et une estimation d'une limite supérieure du temps d'attente pour les paquets en transit. De plus, appliquer un temps d'attente constant spécifique aux singletons mémorisés de délai unidirectionnel est conforme à la présente spécification et peut permettre que les résultats servent à plus d'une audience de rapports.}

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.}

### 2.7 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.

Pour la perte, il y a trois sources d'erreur :
- o la synchronisation entre horloges sur Src et Dst ;
- o le seuil de perte de paquet (qui est en relation avec la synchronisation entre les horloges) ;
- o les limites de ressources à l'interface réseau ou du logiciel sur l'instrument de réception.

Les deux premières sources sont en inter relations et pourraient résulter en ce qu'un paquet d'essai avec un délai fini soit rapporté comme perdu. Type-P-One-way-Packet-Loss est 1 si le paquet d'essai n'arrive pas, ou si il arrive et que la différence entre l'horodatage de Src et l'horodatage de Dst est supérieure à la "période de temps raisonnable" ou au seuil de perte. Si les horloges ne sont pas suffisamment synchronisées, le seuil de perte peut n'être pas "raisonnable" - le paquet peut prendre beaucoup moins de temps pour arriver que ce que son horodatage Src n'indique. De même, si le seuil de perte est réglé trop bas, de nombreux paquets peuvent alors être comptés comme perdus. Le seuil de perte doit être assez élevé et les horloges assez bien synchronisées pour qu'un paquet qui arrive soit rarement compté comme perdu. (Voir la discussion des deux paragraphes précédents.)

Comme la sensibilité de la seule mesure de perte de paquet au manque de synchronisation des horloges est moindre que pour le délai, on renvoie le lecteur au traitement des erreurs de synchronisation de la "métrique de délai unidirectionnel pour IPPM" [RFC2330] pour les détails.

La dernière source d'erreur, les limites de ressources, cause l'abandon du paquet par l'instrument de mesure et son classement comme perdu alors qu'en fait le réseau a livré le paquet dans un délai raisonnable.

Les instruments de mesure devraient être calibrés de telle façon que le seuil de perte soit raisonnable pour l'application de la métrique et que les horloges soient assez synchronisées pour que le seuil de perte reste raisonnable.

De plus, les instruments devraient être vérifiés pour s'assurer que la possibilité qu'un paquet arrive à l'interface réseau mais soit perdu à cause de l'encombrement sur l'interface ou autre épuisement de ressources (par exemple les mémoires tampon) sur l'instrument soit faible.

### 2.8 Rapport de métrique

Le calibrage et le contexte dans lesquels la métrique est mesurée DOIVENT être considérés avec attention et DEVRAIENT toujours être rapportés avec les résultats de la métrique. On présente maintenant quatre éléments à prendre en considération : le type P des paquets d'essai, le seuil de perte, le calibrage d'instrument, et le chemin traversé par les paquets d'essai. Cette liste n'est pas exhaustive ; toute information supplémentaire qui pourrait être utile pour interpréter les applications des métriques devrait aussi être rapportée (voir dans la [RFC6703] une discussion extensive des considérations de rapport pour les différentes audiences).

#### 2.8.1 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-Packet-Loss pourrait changer si le protocole (UDP ou TCP), le numéro d'accès, la taille, ou un arrangement pour un traitement spécial (par exemple, le champ DS IP [RFC2780], la notification d'encombrement explicite (ECN, *Explicit Congestion Notification*) [RFC3168], ou RSVP) changent. Des distinctions de paquet supplémentaires identifiées dans de futures extensions de la définition de Type-P s'appliqueront. Le type P exact utilisé pour faire les mesures DOIT être rapporté avec précision.

#### 2.8.2 Seuils de perte

Le seuil, Tmax, entre un grand délai finit et la perte (ou autre méthodologie pour distinguer entre délai fini et perte) DOIT être rapporté.

#### 2.8.3 Résultats du calibrage

Le degré de synchronisation entre les horloges de source et de destination DOIT être rapporté. Si possible, un paquet d'essai qui arrive à l'interface réseau de la destination et est rapporté comme perdu à cause de l'épuisement des ressources à la destination DEVRAIT être rapporté.

#### 2.8.4 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.}

## 3. Définition d'échantillons de perte de paquet unidirectionnelle

Étant donnée la métrique de singleton Type-P-One-way-Packet-Loss, 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 T0, un temps de fin Tf, et un taux moyen lambda, puis de définir un processus de Poisson pseudo aléatoire de taux lambda, dont les valeurs tombent entre T0 et Tf. 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.

### 3.1 Nom de la métrique

Type-P-One-way-Packet-Loss-Poisson-Stream

### 3.2 Paramètres de la métrique

- Src, adresse IP d'un hôte
- Dst, adresse IP d'un hôte
- T0, un instant
- Tf, un instant
- Tmax, seuil d'attente de perte
- lambda, taux en secondes réciproques

### 3.3 Unités de la métrique

Une séquence de paires ; les éléments de chaque paire sont :
- T, un instant,
- L, zéro ou un.

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

### 3.4 Définition

Connaissant T0, Tf, et lambda, on calcule un processus pseudo aléatoire de Poisson débutant à T0 ou avant, avec un taux moyen d'arrivée lambda, et se terminant à Tf ou après. Ces valeurs de temps supérieures ou égales à T0 et inférieures ou égales à Tf sont alors choisies. À chacun des instants choisis dans ce procès, on obtient une valeur de Type-P-One-way-Packet-Loss. La valeur de l'échantillon est la séquence constituée des paires <instant, perte> résultantes. Si il n'y a aucune de ces paires, la séquence est de longueur zéro et l'échantillon est dit vide.

### 3.5 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 lambda 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 lambda 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  Le processus de Poisson est utilisé pour programmer les mesures de pertes. Les paquets d'essais ne vont généralement pas arriver à Dst selon une distribution de Poisson car ils sont influencés par le réseau. Les liaisons à intervalles de temps décrites au paragraphe 3.4 de la [RFC7312] peuvent grandement modifier les caractéristiques de l'échantillon. Le principal souci est que des flux de paquets non biaisés avec des intervalles inter paquets aléatoires soient convertis en une nouvelle distribution après avoir rencontré une liaison à intervalles de temps, éventuellement avec de fortes caractéristiques périodiques à la place.

{Commentaire : on ne prétend pas, bien sûr, que le trafic réel de l'Internet arrive conformément à un processus d'arrivée de Poisson. Il est important de noter que, à l'opposé de cette métrique, les ratios de perte observés par les connexions de transport ne reflètent pas des échantillons non biaisés. Par exemple, les transmissions TCP (1) se produisent en salves, qui peuvent induire des pertes dues au volume de salve qui n'auraient autrement pas été observées, et (2) adaptent leur taux de transmission pour tenter de minimiser le taux de pertes observés sur la connexion.}

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

Noter aussi que, étant donné qu'un échantillon qui va de T0 à Tf, et étant données les nouvelles valeurs T0' et Tf' telles que $T0 \leq T0' \leq Tf' \leq Tf$, les suivants de l'échantillon dont les valeurs tombent entre T0' et Tf' sont aussi des échantillons valides de Type-P-One-way-Packet-Loss-Poisson-Stream.

### 3.6 Méthodologies

Les méthodologies découlent directement de :
- o la sélection d'instants spécifiques utilisant le processus d'arrivée de Poisson spécifié, et
- o de la discussion des méthodologies déjà fournie pour la métrique de singleton Type-P-One-way-Packet-Loss.

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].

### 3.7 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 d'arrivée 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. 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.}

### 3.8 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-Packet-Loss au paragraphe 2.8.)

## 4. Définitions de statistiques pour délai unidirectionnel

Étant donnée la métrique d'échantillon de Type-P-One-way-Packet-Loss-Poisson-Stream, on propose maintenant plusieurs statistiques de cet échantillon. Ces statistiques sont proposées surtout afin d'illustrer ce qui peut être fait. Voir dans la [RFC6703] une discussion des statistiques qui sont pertinentes pour différentes audiences.

### 4.1. Type-P-One-way-Packet-Loss-Ratio

Soit un Type-P-One-way-Packet-Loss-Poisson-Stream, la moyenne de toutes les valeurs L dans la flux est le ratio des pertes sur le total des paquets dans le flux. De plus, le Type-P-One-way-Packet-Loss-Ratio est indéfini si l'échantillon est vide.

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

Flux1 = <
  <T1, 0>
  <T2, 0>
  <T3, 1>
  <T4, 0>
  <T5, 0>
  >

La moyenne des résultats de pertes serait 0,2, le ratio de pertes.

Noter que, comme des chemins Internet en bonne santé devraient fonctionner avec des ratios de perte en dessous de 1 % (en particulier si des produits à fort délai-bande passante doivent être tenus) les tailles d'échantillon nécessaires pourraient être plus grandes que ce qu'on souhaiterait. Donc, par exemple, si on veut discriminer entre diverses fractions de 1 % sur des périodes de une minute, plusieurs centaines d'échantillons par minute pourraient alors être nécessaires. Il en résulterait de plus grandes valeurs de lambda que ce qu'on veut ordinairement.

Noter que bien que le seuil de perte doive être réglé de telle façon que toutes les erreurs de pertes ne soient pas significatives, si la possibilité qu'un paquet qui est arrivé soit compté comme perdu à cause d'un épuisement des ressource est significative comparée au taux de perte qui nous intéresse, Type-P-One-way-Packet-Loss-Ratio sera non signifiant.

## 5. 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 minimes 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. Si un attaquant injecte du trafic artificiel qui est accepté comme légitime, le taux de perte va être artificiellement abaissé. 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". 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.

## 6. Changements depuis la RFC 2680

Le texte ci-dessus constitue une révision de la RFC 2680, et c'est maintenant une norme de l'Internet.

La [RFC7290] donne le plan d'essais et les résultats qui viennent à l'appui de l'avancement de la [RFC2680] sur la voie de la normalisation, conformément au procès de la [RFC6576]. Les conclusions de la [RFC7290] mentionnent quatre modifications mineures à inclure :

1. Au paragraphe 6.2.3 de la [RFC7290] on affirme que l'hypothèse de 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 du paragraphe 2.6.

2. Le paragraphe 6.5 de la [RFC7290] indique que la statistique de Type-P-One-way-Packet-Loss-Average est plus couramment appelée un taux de perte de paquet, de sorte qu'elle est rebaptisée ainsi dans le présent document (cette petite discordance n'affecte pas l'éligibilité à l'avancement du statut). Le changement de nom a été appliqué au paragraphe 4.1.

3. L'IETF a obtenu un consensus sur les directives de rapport de 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 2.6, au paragraphe 2.8, et à la Section 4.

4. Il y a actuellement deux errata avec le statut "Verified" (EID 1528) et "Held for Document Update" (EID 3186) pour la [RFC2680], et ces révisions mineures ont été incorporées à la Section 1 et au paragraphe 2.7.

Un certain nombre de mises à jour du texte de la [RFC2680] ont été mises en œuvre dans le texte pour référencer les RFC clés sur IPPM qui ont été approuvées après la [RFC2680] (voir la Section 3 et le paragraphe 3.6) et pour suivre les commentaires de la liste de diffusion IPPM qui décrivent les conditions et expériences actuelles.

1. Vers la fin du paragraphe 1.1, il y a une mise à jour d'un exemple de réseau utilisant ATM, une clarification de l'effet de TCP sur l'occupation de file d'attente, et une discussion de l'importance de la mesure du délai unidirectionnel.

2. Clarification de la définition de "résolution" au paragraphe 1.2.

3. Inclusion explicite du paramètre d'entrée de temps d'attente maximum aux paragraphes 2.2, 2.4, et 3.2, reflétant la reconnaissance de ce paramètre dans les RFC plus récentes et la Recommandation UIT-T Y.1540.

4. Ajout d'une référence à la RFC 6703 dans la discussion de la durée de vie de paquet et les temporisations d'application au paragraphe 2.5.

5. Remplacement de "préséance" par la terminologie à jour (champ DS) aux paragraphes 2.6 et 2.8.1 (avec référence).

6. Ajout de lignes directrices entre parenthèses sur la minimisation de l'intervalle entre l'apposition de l'horodatage de l'instant d'envoi ou de réception au paragraphe 2.6. Aussi, le texte reconnaît maintenant le processus d'acquisition de l'horodatage et qu'en pratique les systèmes mesurent à la fois le délai et la perte (exigeant dont le paramètre Temps d'attente maximal).

7. Ajout d'une référence à la RFC 3432 concernant l'échantillonnage périodique à côté de l'échantillonnage de Poisson à la Section 3 et aussi noté qu'une distribution de Poisson tronquée peut être nécessaire dans les réseaux modernes, comme décrit dans la mise à jour du cadre IPPM [RFC7312].

8. Reconnaissance que les liaisons à intervalles de temps décrites dans la [RFC7312] peuvent grandement modifier les caractéristiques d'échantillonnage, au paragraphe 3.5.

9. Ajout d'une référence à la RFC 4737 concernant les métriques de réarrangement dans la discussion relative aux méthodologies (paragraphe 3.6).

10. Extension et mise à jour du matériel sur la confidentialité et ajout d'avertissements sur l'utilisation des mesures pour la reconnaissance à la Section 5, "Considérations sur la sécurité".

Le paragraphe 5.4.4 de la [RFC6390] suggère un gabarit commun pour les métriques de performances partiellement dérivées des RFC antérieures du groupe de travail Méthodologie IPPM et de référencement (BMWG) mais il contient aussi quelques nouveaux éléments. Toute la partie normative de la [RFC6390] est couverte, mais pas tout a fait avec les mêmes noms ou les mêmes orientations des paragraphes. Plusieurs des parties pour information sont couvertes. Conserver la présentation familière de la littérature IPPM a de la valeur et minimise les différences inutiles entre cette RFC révisée et les RFC IPPM actuelles et futures.

## 7. Références

### 7.1 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.

[RFC2680] G. Almes, S. Kalidindi, M. Zekauskas, "Métrique de perte de paquet unidirectionnelle pour IPPM", septembre 1999. *P.S. ; Remplacée par* RFC7680). DOI 10.17487/RFC2680.

[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. Raisanen 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.

[RFC7679] G. Almes, et autres, "Métrique de retard unidirectionnel pour les performances de IP (IPPM)" janvier 2016. STD 81 ; DOI 10.17487/RFC7679 *(Remplace* RFC2679)

### 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, "Métrique 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.

[RFC7290] L. Ciavattone, et autres, "Plan et résultats d'essais pour avancer la RFC2680 sur la voie de la normalisation" juillet 2014. DOI 10.17487/RFC7290.

[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 [RFC2680], des remerciements sont dus à Matt Mathis qui a encouragé ce travail et attiré l'attention en de nombreuses occasions sur la signification de la perte de paquet. Merci aussi à Vern Paxson pour ses précieux commentaires sur les projets antérieurs et à Garry Couch et Will Leland 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