Groupe de travail Réseau
Request for Comments : 3432
Catégorie : En cours de normalisation
Traduction Claude Brière de L'Isle

V. Raisanen, Nokia
G. Grotefeld, Motorola
A. Morton, AT&T Labs
novembre 2002

Mesure des performances réseau avec des flux périodiques

Statut de ce mémoire
Le présent document spécifie un protocole Internet en cours de normalisation pour la communauté de l'Internet, et appelle à des discussions et des suggestions pour son amélioration. Prière de se reporter à l'édition actuelle du STD 1 "Normes des protocoles officiels de l'Internet" pour connaître l'état de normalisation et le statut de ce protocole. La distribution du présent mémoire n'est soumise à aucune restriction.

Notice de copyright
Copyright (C) The Internet Society (2002). Tous droits réservés.

Résumé
Le présent mémoire décrit une méthode d'échantillonnage périodique et les métriques pertinentes pour attester des performances des réseaux IP. D'abord, le mémoire explique les motifs de l'échantillonnage périodique et traite de la question de sa valeur comme alternative à l'échantillonnage de Poisson décrit dans la [RFC2330]. Ses avantages incluent l'applicabilité aux mesures actives et passives, la simulation d'un trafic de débit binaire constant (CBR, *constant bit rate*) (typique des communications multimédia, ou presque CBR, comme on le trouve dans la détection d'activité vocale) et plusieurs instances dans lesquelles l'analyse peut être simplifiée. La méthode d'échantillonnage évite la prévisibilité en rendant obligatoire des moments de démarrage aléatoires et des essais de longueur finie. À la suite des descriptions de la méthode d'échantillonnage et des paramètres de métrique d'échantillon sont exposées les méthodes et erreurs de mesure. Finalement, on donne des informations supplémentaires sur les mesures périodiques, y compris les considérations sur la sécurité.

Table of Contents

1. Conventions utilisées dans ce document

Dans le présent document, les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" sont à interpréter comme décrit dans le BCP 14, [RFC2119].

Bien que la RFC2119 ait été écrite en visant les protocoles, les mots clés sont utilisés dans le présent document pour des raisons similaires. Ils sont utilisés pour s'assurer que les résultats des mesures provenant de deux mises en œuvre différentes sont comparables, et pour noter les instances dans lesquelles une mise en œuvre pourrait perturber le réseau.

2. Introduction

Le présent mémoire décrit une méthode d'échantillonnage et des métriques de performances pertinentes pour certaines applications de réseaux IP. Le fil conducteur original de ce travail était la qualité de service des flux périodiques interactifs, comme les conférences multimédia sur IP, mais l'idée d'échantillonnage et de mesures périodiques a une plus large applicabilité. Le trafic interactif multimédia est utilisé ci-dessous comme exemple pour illustrer le concept.

Transmettre des paquets de taille égale (ou des paquets presque de même taille) à travers un réseau à des intervalles réguliers simule un flux multimédia de débit binaire constant (CBR, *constant bit-rate*) ou presque CBR. Ci après, ces paquets sont appelés des flux périodiques. Des cas de "paquets presque de même taille" peuvent se trouver dans des applications qui ont plusieurs méthodes de codage (par exemple, du bruit de confort codé numériquement durant les trous de silence dans la parole).

Dans les paragraphes qui suivent sont présentées une méthodologie et des métriques d'échantillonnage pour les flux périodiques. Les résultats de mesures peuvent être utilisés dans des métriques dérivées telles que de délai moyen et maximum. Le mémoire cherche à formaliser les mesures de flux périodiques pour obtenir des résultats comparables entre des mises en œuvre indépendantes.

2.1 Motivation

Comme noté dans le cadre IPPM [RFC2330], une métrique d'échantillon qui utilise des essais de singletons régulièrement espacés connaît quelques limitations quand on la considère du point de vue général des mesures : seulement une partie du spectre des performances du réseau est échantillonnée. Cependant, certaines applications échantillonnent aussi ce spectre de performances limité et leurs performances peuvent être d'un intérêt critique.

L'échantillonnage périodique est utile pour les raisons suivantes :

* Il est applicable aux mesures passives, aussi bien qu'aux mesures actives.
* Une mesure active peut être configurée pour correspondre aux caractéristiques des flux de support, et simplifie l'estimation des performances de l'application.
* Les mesures de nombreuses dégradations du réseau (par exemple, variation de délai, pertes consécutives, réarrangement de l'ordre des paquets) sont sensibles à la fréquence d'échantillonnage. Lorsque les dégradations elles-mêmes varient dans le temps (et que les variations sont assez rares, donc importantes) une fréquence d'échantillonnage constante simplifie l'analyse.
* L'analyse de domaine de fréquence est simplifiée lorsque les échantillons sont espacés de façon égale.

La simulation des flux CBR avec des flux périodiques encourage les échantillonnages denses de performances réseau, car les flux multimédia typiques ont 10 à 100 paquets à chaque seconde. L'échantillonnage dense permet la caractérisation des phénomènes réseau de courte durée.

3. Méthodologie d'échantillonnage périodique

La RFC cadre [RFC 2330] souligne les problèmes potentiels suivants de l'échantillonnage périodique :

1. Les performances échantillonnées peuvent être synchronisées avec certains autres comportements périodiques, ou les échantillons peuvent être anticipés et les résultats manipulés. L'échantillonnage imprévisible est préféré.

2. Les mesures actives peuvent causer de l'encombrement, et un échantillonnage périodique peut amener des envoyeurs sensibles à l'encombrement à un état synchronisé, produisant des résultats atypiques.

L'échantillonnage de Poisson produit un échantillon non biaisé pour les diverses métriques de performances IP, bien qu'il y ait des situations où d'autres méthodes d'échantillonnage sont avantageuses (comme exposé sous Motivation).

On peut prescrire des méthodes d'échantillonnage périodique qui s'intéressent aux problèmes énumérés ci dessus. La prévisibilité et certaines formes de synchronisation peuvent être atténuées par l'utilisation de temps de démarrage aléatoires et d'une durée de flux limitée sur un intervalle d'essai. Les paramètres d'échantillonnage périodique produisent des biais, et un choix judicieux peut produire un biais connu intéressant. Le trafic total généré par cette méthode d'échantillonnage ou toute autre, devrait être limité pour éviter des effets contraires sur le trafic autre que d'essai (taille de paquet, taux d'envoi des paquets, et durée et fréquence de l'échantillonnage devraient tous être pris en considération).

Les paramètres de configuration de l'échantillonnage périodique sont :

T début d'un intervalle de temps où un échantillon périodique est désiré.

dT durée de l'intervalle pour l'instant de début d'échantillonnage permis.

T0 instant qui DOIT être choisi au hasard dans l'intervalle [T, T + dT] pour commencer à générer les paquets et prendre les mesures.

Tf instant, supérieur à T0, pour arrêter la génération des paquets pour un échantillon (Tf peut se rapporter à T0 si on le désire).

incT durée nominale de l'intervalle entre paquets, de premier bit à premier bit.

T0 peut être tiré d'une distribution uniforme, ou T0 = T + Unif(0,dT). D'autres distributions peuvent aussi être appropriées. Les instants de début dans les intervalles de temps successifs DOIVENT utiliser une valeur indépendante tirée de la distribution. Dans une mesure passive, l'arrivée des flux support d'usager peut avoir un caractère suffisamment aléatoire, ou un instant de début de la mesure rendu aléatoire durant un flux peut être nécessaire pour satisfaire à cette exigence.

Lorsque on désire que les tailles de paquet soient mélangées, les mesures passives possèdent généralement les séquences et statistiques des tailles réellement utilisées, alors que des mesures actives auraient besoin de reproduire la distribution des tailles voulue.

4. Métriques d'échantillon pour flux périodiques

La métrique d'échantillon présentée ici est similaire à la métrique d'échantillon Flux de Poisson de délai unidirectionnel de type P (*Type-P-One-way-Delay-Poisson-Stream*) présentée dans la [RFC2679]. Les singletons définis dans la [RFC2330] et la [RFC2679] sont aussi applicables ici.

4.1 Nom de la métrique

Flux périodique de délai unidirectionnel de type P *(Type-P-One-way-Delay-Periodic-Stream)*

4.2 Paramètres de la métrique

4.2.1 Paramètres généraux de la métrique

Ces paramètres s'appliquent aux paragraphes suivants (4.2.2, 4.2.3, et 4.2.4).

Paramètres que comporte habituellement chaque singleton :

Src	adresse IP d'un hôte.
Dst	adresse IP d'un hôte.
IPV	version IP (IPv4/IPv6) utilisée dans la mesure.
dTloss	intervalle de temps, temps d'attente maximum avant qu'un paquet soit déclaré perdu.
packet size p(j)	nombre désiré d'octets dans le paquet de type P, où j est l'indice de taille.

Paramètres facultatifs :

PktType	tout qualificatif supplémentaire (adresse de transport)
Tcons	intervalle de temps pour consolider les paramètres collectés au point de mesure.

Bien qu'un certain nombre d'applications utilisent une seule taille de paquet (j = 1), d'autres applications peuvent utiliser des paquets de différentes tailles (j > 1). En particulier dans les cas d'encombrement, il peut être utile d'utiliser des paquets plus petits que la taille de paquet maximum ou prédominante dans le flux périodique.

On suppose une topologie où Src et Dst sont séparés des points de mesure.

4.2.2 Paramètres collectés au point de mesure MP(Src)

Paramètres que chaque singleton comporte habituellement :
+ Tstamp(Src)[i], pour chaque paquet [i], c'est l'heure du paquet telle que mesurée à MP(Src).

Paramètres supplémentaires :
+ PktID(Src) [i], pour chaque paquet [i], une identification ou numéro de séquence univoque.
+ PktSi(Src) [i], pour chaque paquet [i], la taille réelle du paquet.

Certaines applications peuvent utiliser des paquets de différentes tailles, soit à cause des exigences de l'application, soit en réponse aux performances IP rencontrées.

4.2.3 Paramètres collectés au point de mesure MP(Dst)

+ Tstamp(Dst)[i], pour chaque paquet [i], l'heure du paquet telle que mesurée à MP(Dst).
+ PktID(Dst) [i], pour chaque paquet [i], une identification ou numéro de séquence univoque.
+ PktSi(Dst) [i], pour chaque paquet [i], la taille réelle du paquet.

Paramètres facultatifs :
+ dTstop, intervalle de temps, utilisé ajouté à l'instant Tf pour déterminer quand arrêter de collecter les mesures pour un échantillon.
+ PktStatus [i], pour chaque paquet [i], le statut du paquet reçu. Les statuts possibles incluent OK, en-tête de paquet corrompu, charge utile de paquet corrompue, dupliqué, fragment. Les critères pour déterminer le statut DOIVENT être spécifiés, si utilisés.

4.2.4 Métriques d'échantillon résultant de la combinaison des paramètres de MP(Src) et MP(Dst)

En utilisant les paramètres ci-dessus, un singleton de délai serait calculé comme suit :
+ Délai [i], pour chaque paquet [i], l'intervalle de temps Délai[i] = Tstamp(Dst)[i] - Tstamp(Src)[i]

Pour les conditions suivantes, il ne sera pas possible de calculer les singletons de délai :
Parasite : il n'y aura pas de temps Tstamp(Src)[i]
Non reçu : il n'y aura pas de Tstamp(Dst)[i]
En-tête de paquet corrompu : il n'y aura pas de Tstamp(Dst)[i]
Dupliqué : seul la première copie non corrompue du paquet reçue à Dst devrait avoir son Délai[i] calculé.

Une métrique d'échantillon pour le délai moyen serait comme suit :

AveDelay = (1/N)Somme (de i = 1 à N, Délai[i])

en supposant que tous les paquets de i = 1 à N ont des singletons valides.

Un singleton de variation de délai [RFC3393] peut aussi être calculé :

+ IPDV[i], pour chaque paquet [i] sauf le premier, la variation de délai entre les paquets successifs serait calculée par :

IPDV[i] = Délai[i] – Délai [i-1]

IPDV[i] peut être négatif, nul, ou positif. Les singletons de délai pour les paquets i et i-1 doivent être calculables sinon IPDV[i] est indéfini.

Un exemple de métrique pour l'échantillon d'IPDV est la gamme :

GammeIPDV = max(IPDV[]) - min(IPDV[])

4.3 Description générale de la procédure de collecte d'un échantillon

En commençant à l'instant T0 ou après, les paquets de type P sont générés par Src et envoyés à Dst jusqu'à l'instant Tf avec un intervalle nominal entre le premier bit des paquets successifs de incT, comme mesuré à MP(Src). incT peut être nominal pour un certain nombre de raisons : une variation de la génération des paquets à Src, des problèmes d'horloge (voir au paragraphe 4.6), etc. MP(Src) enregistre les paramètres ci-dessus pour les seuls paquets qui ont un horodatage entre T0 et Tf inclus qui ont les Src, Dst, et tous autres qualificatifs requis. MP(Dst) enregistre aussi les paquets avec des horodatages entre T0 et (Tf + dTstop).

Facultativement, à l'instant Tf + Tcons (mais éventuellement dans tous les cas) les données provenant de MP(Src) et MP(Dst) sont consolidées pour déduire les résultats de la métrique d'échantillons. Pour empêcher que la collecte des données s'arrête trop tôt, dTcons devrait être supérieur ou égal à dTstop. À l'inverse, pour garder une efficacité raisonnable à la collecte des données, dTstop devrait être un intervalle de temps raisonnable (secondes/minutes/heures) même si dTloss est infini ou extrêmement long.

4.4 Discussion

Cette méthodologie d'échantillonnage est destinée à quantifier les délais et la variation de délai subie par les flux multimédia d'une application. Du fait des définitions de ces métriques, l'état de perte de paquet est aussi enregistré. L'intervalle nominal entre les paquets atteste des variations de performance du réseau sur une échelle temporelle spécifique.

Un certain nombre de facteurs devraient être pris en considération lors de la collecte d'une métrique d'échantillons de Flux périodique de délai unidirectionnel de type P.

+ L'intervalle T0 à Tf devrait être spécifié de façon à couvrir un intervalle de temps assez long pour représenter une utilisation raisonnable de l'application soumise à l'essai, mais pas excessivement longue dans le même contexte (par exemple, un appel téléphonique dure plus de 100 ms, mais moins d'une semaine).

+ L'intervalle nominal entre les paquets (incT) et la ou les tailles de paquet (p(j)) ne devraient pas définir un taux binaire équivalent qui excède la capacité de l'accès de sortie de Src, de l'accès d'entrée de Dst, ou la capacité du ou des réseaux intervenants, si elles sont connues. Il peut y avoir des cas exceptionnels pour tester la réponse de l'application à des conditions de surcharge dans les réseaux de transport, mais ces cas devraient être strictement contrôlés.

+ Les valeurs de délai réel seront positives. Donc, cela n'a pas de sens de faire rapport d'une valeur négative comme délai réel. Cependant, une valeur de délai individuel de zéro ou négative pourrait être utile au titre d'un flux lorsque on essaye de découvrit une distribution des erreurs de délai.

+ Selon la topologie de mesure, les valeurs de délai peuvent être aussi faibles que 100 µs à 10 ms, donc il peut être important pour Src et Dst de se synchroniser très étroitement. Les systèmes GPS fournissent un moyen pour réaliser une synchronisation à quelques dizaines de µs. Les applications ordinaires de NTP peuvent aussi permettre une synchronisation à plusieurs ms, mais cela dépend de la stabilité et de la symétrie des propriétés de délai parmi les agents NTP utilisés, et ce délai est ce qu'on essaye de mesurer.

+ Une méthodologie donnée devra inclure un moyen de déterminer si un paquet a été perdu ou si le délai est simplement très grand (et si le paquet est déjà arrivé à Dst). Le paramètre global de métrique dTloss définit un intervalle de temps tel que les délais supérieurs à dTloss sont interprétés comme des pertes. {Commentaire : pour de nombreuses applications, le traitement de grands délais comme infini/perte sera sans conséquence. Un paquet de données TCP, par exemple, qui arrive seulement après plusieurs multiples du RTT usuel peut aussi bien avoir été perdu.}

4.5 Aspects supplémentaires de méthodologie

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, la préséance).

4.6 Erreurs et incertitudes

La description de toute méthode de mesure spécifique devrait inclure une prise en compte et une analyse des diverses sources d'erreur ou d'incertitude. La RFC cadre [RFC 2330] donne des lignes directrices générales sur ce point, mais on note ici les spécificités suivantes qui se rapportent aux métriques de flux périodiques et de délai :

+ Erreur due à la variation de incT. La raison peut en être une programmation inadéquate du processus, éventuellement due à la charge de CPU.
+ Erreurs ou incertitudes dues à l'incertitude des horloges des points de mesure de MP(Src) et MP(Dst).
+ Erreurs ou incertitudes dues à la différence entre 'heure du réseau' et 'heure de l'hôte'.

4.6.1 Erreurs ou incertitudes sur les horloges

L'incertitude de mesure d'un délai unidirectionnel est en partie en rapport avec les incertitudes des horloges de MP(Src) et MP(Dst). Dans ce qui suit, on se réfère à l'horloge utilisée pour mesurer quand le paquet a été envoyé de MP(Src) comme horloge MP(Src) et on se réfère à l'horloge utilisée pour mesurer quand le paquet a été reçu à MP(Dst) comme horloge MP(Dst). En ce qui concerne les notions de synchronisation, précision, résolution, et biais, on notera que :

+ Toute erreur de synchronisation entre l'horloge MP(Src) et l'horloge MP(Dst) va contribuer à une erreur de la mesure du délai. On dit que l'horloge MP(Src) et l'horloge MP(Dst) ont une erreur de synchronisation de Tsynch si l'horloge MP(Src) est Tsynch en avance sur l'horloge MP(Dst). Donc, si on connaît exactement la valeur de Tsynch, on peut corriger la synchronisation d'horloge en ajoutant Tsynch à la valeur incorrecte de Tstamp(Dst)[i] - Tstamp(Src) [i].
+ La résolution d'une horloge ajoute à l'incertitude sur toute mesure de temps. Donc, si l'horloge MP(Src) 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 source MP(Src) par ResMP(Src) et la résolution de l'horloge MP(Dst) par ResMP(Dst).
+ Le biais d'une horloge n'est pas tant un problème supplémentaire que la réalisation du fait que Tsynch est lui-même une fonction du temps. Donc, si on essaye de mesurer Tsynch ou de le borner, cette mesure ou calcul doit être répétée périodiquement. Sur une certaine période de temps, cette fonction peut être approximée par une fonction linéaire plus quelques termes d'ordre supérieur ; dans ces cas, une option est d'utiliser la connaissance des composants linéaires pour corriger l'horloge. En utilisant cette correction, le Tsynch résiduel est diminué, mais reste une source d'incertitude qui doit être prise en compte. On utilise la fonction Esynch(t) pour noter une borne supérieure de l'incertitude en synchronisation. Donc, $|Tsynch(t)| \leq Esynch(t)$.

Prenant ensemble tous des éléments, on note qu'un calcul simple de Tstamp(Dst)[i] - Tstamp(Src) [i] sera faux de Tsynch(t) +/- (ResMP(SRc) + ResMP(Dst)). En utilisant la notion de Esynch(t), on note que ces problèmes d'horloge introduisent une incertitude totale de Esynch(t) + Rsource + Rdest. Cette estimation de l'incertitude d'horloge totale devrait être incluse dans l'analyse d'erreur/incertitude de toute mise en œuvre de mesures.

4.6.2 Erreurs ou incertitudes sur l'heure du réseau par rapport à l'heure de l'hôte

On voudrait mesurer le temps entre le moment où un paquet est mesuré et horodaté à MP(Src) et celui où il arrive et est horodaté à MP(Dst) ; on se réfère à cela comme à des "heures du réseau". Cependant, si les horodatages sont appliqués par un logiciel à Src et à Dst, ce logiciel peut seulement mesurer directement le temps entre le moment où Src génère le paquet juste avant d'envoyer le paquet d'essai et celui où Dst a commencé à traiter le paquet après avoir reçu le paquet d'essai ; on se réfère à ces deux points par le terme de "heure de l'hôte".

Dans la mesure où la différence entre l'heure du réseau et l'heure de l'hôte est connue avec précision, cette connaissance peut être utilisée pour corriger les mesures de l'heure du réseau. La valeur corrigée estime plus précisément la métrique désirée (d'heure de l'hôte), et vice-versa.

Cependant, dans la mesure où la différence entre heure du réseau et heure de l'hôte est incertaine, cette incertitude doit être pris en compte pour une analyse d'une certaine méthode de mesure. On note par Hsource une borne supérieure de l'incertitude dans la différence entre heure du réseau de MP(Src) et heure de l'hôte sur l'hôte Src, on définit de même Hdest pour la différence entre l'heure de l'hôte sur l'hôte Dst et l'heure du réseau de MP(Dst). On note alors que ces problèmes introduisent une incertitude totale de Hsource + Hdest. Cette estimation de l'incertitude totale de réseau contre hôte devrait être incluse dans l'analyse d'erreur/incertitude de toute mise en œuvre de mesures.

4.6.3 Calibrage

Généralement, les valeurs mesurées peuvent être décomposées comme suit :

valeur mesurée = vraie valeur + erreur systématique + erreur aléatoire

Si l'erreur systématique (le biais constant dans les 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 aléatoire générée par les instruments eux-mêmes aussi en détail que possible. Au minimum, une borne ("e") devrait être trouvée telle que la valeur rapportée soit dans la gamme (vraie valeur - e) à (vraie valeur + e) au moins 95 pour cent du temps. On appelle "e" l'erreur de calibrage pour les mesures. Elle représente le degré auquel les valeurs produites par l'instrument de mesure sont répétables ; c'est-à-dire, à combien près un délai réel de 30 ms est rapporté comme 30 ms. {Commentaire : 95 pour cent a été choisi pour des raisons qui sont exposées dans la [RFC2679], brièvement résumées par : (1) un certain niveau de confiance est souhaitable pour être capable de retirer les excentriques, qu'on va trouver dans la mesure de toute propriété physique ; (2) un niveau de confiance particulier devrait être spécifié afin que les résultats de mises en œuvres indépendantes puissent être comparés.}

De la discussion des deux paragraphes précédents, l'erreur de mesure peut être bornée en déterminant toutes les incertitudes individuelles, et en les ajoutant ensemble pour former :

Esynch(t) + ResMP(Src) + ResMP(Dst) + Hsource + Hdest

Cependant, il devrait être possible d'établir des bornes raisonnables à l'incertitude d'horloge capturée par les trois premiers termes ainsi qu'à l'incertitude relative à l'hôte capturée par les deux derniers termes en utilisant des techniques de conception soigneuses et en calibrant les instruments à l'aide d'un réseau de laboratoire connu et isolé.

Par exemple, les incertitudes d'horloge sont bien réduites par l'utilisation d'une source horaire GPS. La somme de Esynch(t) + ResMP(Src) + ResMP(Dst) est petite, et est aussi bornée par la durée de la mesure à cause de la source horaire mondiale. Les incertitudes relatives à l'hôte, Hsource + Hdest, pourraient être bornées en connectant deux instruments 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 par zéro. Le délai mesuré ne contient donc que l'erreur systématique et aléatoire de l'instrumentation. La "valeur moyenne" de mesures répétées est l'erreur systématique, et la variation est l'erreur aléatoire. Un moyen de calculer l'erreur systématique et l'erreur aléatoire à un niveau de confiance de 95 % est de répéter l'expérience de nombreuses fois – au moins des centaines d'essais. L'erreur systématique sera alors la médiane. L'erreur aléatoire sera alors trouvée en retirant l'erreur systématique des valeurs mesurées. L'intervalle de confiance de 95 % sera la gamme du 2,5ème percentile au 97,5ème percentile de ces écarts de la vraie valeur. L'erreur de calibrage "e" pourra alors être prise comme étant la plus grande valeur absolue de ces deux nombres, plus l'incertitude d'horloge. {Commentaire : telle que décrite, cette borne est relativement lâche car les incertitudes sont ajoutées, et on utilise la valeur absolue du plus grand écart. Tant que la valeur résultante n'est pas une fraction significative de la valeur mesurée, c'est une borne raisonnable. Si la valeur résultante devient une fraction significative des valeurs mesurées, il sera alors nécessaire de calculer l'erreur de calibrage avec des méthodes plus exactes.}

Noter que l'erreur aléatoire est une fonction de la charge de mesure. Par exemple, si de nombreux chemins sont mesurés avec un seul instrument, cela peut augmenter les interruptions, la programmation du processus, et l'entrée/sortie du disque (par exemple, pour enregistrer les mesures) toutes choses qui peuvent 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 ce que les instruments verront sur le terrain.

On souligne encore que ce traitement statistique se réfère au calibrage de l'instrument ; il est utilisé pour "calibrer le mètre" et dire avec quelle précision le mètre reflète la réalité.

4.6.4 Erreurs dans incT

L'intervalle nominal entre les paquets, incT, peut varier durant les mesures actives ou passives. Dans la mesure passive, les en-têtes de paquet peuvent comporter un horodatage appliqué avant la plus grande partie de la pile de protocole, et l'heure d'envoi réelle peut varier à cause de la programmation du traitement. Par exemple, les systèmes H.323 sont obligés d'avoir des paquets prêts pour la pile réseau dans les 5 ms de leur temps idéal. Il peut y avoir une variation supplémentaire de la part du réseau entre la source et le point de mesure de source MP(Src). Les systèmes de mesure active peuvent rencontrer des erreurs similaires, mais à un moindre degré. Ces erreurs doivent être prises en compte dans certains types d'analyse.

4.7 Rapports

Le calibrage et le contexte dans lequel la méthode est utilisée DOIVENT être mûrement réfléchis, et DEVRAIENT toujours être rapportés avec les résultats de la métrique. On va présenter cinq éléments à prendre en considération : le type P des paquets d'essai, le seuil de délai équivalent à la perte, le calibrage d'erreur, le chemin traversé par les paquets d'essai, et les conditions d'environnement à Src, Dst, et dans les réseaux intervenants durant un échantillonnage. Cette liste n'est

pas exhaustive ; toute information supplémentaire qui pourrait être utile pour interpréter les applications des métriques devrait aussi être rapportée.

4.7.1 Type P

Comme il est noté dans le document cadre [RFC 2330], la valeur d'une métrique peut dépendre du type de paquets IP utilisés pour faire la mesure, ou "type P". La valeur du délai unidirectionnel de type P pourrait changer si le protocole (UDP ou TCP), le numéro d'accès, la taille, ou l'arrangement pour un traitement particulier (par exemple, la préséance IP ou RSVP) change. Le type P exact utilisé pour faire les mesures DOIT être rapporté.

4.7.2 Seuil du délai équivalent de perte

De plus, le seuil du délai équivalent à une perte (ou la méthodologie pour déterminer ce seuil) DOIT être rapporté.

4.7.3 Résultats de calibrage

+ Si l'erreur systématique peut être déterminée, elle DEVRAIT être retirée de la valeur mesurée.
+ On DEVRAIT aussi rapporter l'erreur de calibrage, afin que la vraie valeur soit la valeur rapportée plus ou moins, avec un intervalle de confiance de 95 % (voir le dernier paragraphe.)
+ Si possible, les conditions dans lesquelles un paquet d'essai avec un délai fini est rapporté comme perdu dû à l'épuisement des ressources sur l'instrument de mesure DEVRAIenT être rapportées.

4.7.4 Chemin

Le chemin traversé par les paquets DEVRAIT être rapporté, si possible. En général, il est impossible en pratique de savoir le chemin précis qu'un certain paquet prend à travers le réseau. Le chemin précis peut être connu pour certains paquets de type P sur des chemins courts ou stables. Si le type P inclut l'option de chemin enregistré (ou de chemin de source lâche) dans l'en-tête IP, et si le chemin est assez court, et si tous les routeurs sur le chemin acceptent d'enregistrer le chemin (ou la source lâche) le chemin sera alors enregistré avec précision.
Cela peut n'être pas praticable parce que le chemin doit être assez court. De nombreux routeurs ne prennent pas en charge (ou ne sont pas configurés pour) l'enregistrement du chemin, et l'utilisation de ce dispositif diminuerait souvent artificiellement les performances observées en éloignant 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 distincts de Src à Dst) la liaison initiale utilisée est alors un contexte précieux. {Commentaire : par exemple, sur une réalisation commerciale, une Src sur un NAP peut atteindre une Dst sur un autre NAP par un parmi plusieurs cœurs de réseau différents.}

5. Exposé supplémentaire sur l'échantillonnage périodique

La Figure 1 illustre des mesures sur plusieurs niveaux de protocole qui sont pertinents pour le présent mémoire. L'utilisateur se concentre sur l'évaluation de la qualité du transport du point de vue de l'application. Cependant, pour séparer correctement la contribution à la qualité du système d'exploitation et du codec sur un paquet vocal, par exemple, il est utile d'être capable de mesurer la qualité au niveau IP [6]. La surveillance de la couche liaison donne un moyen pour tenir compte des caractéristiques de couche liaison telles que les taux d'erreur binaires.

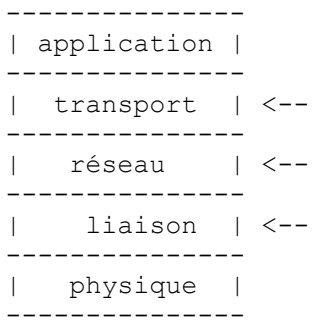

Figure 1 : Différentes possibilités d'effectuer les mesures : vue du protocole.

Ci-dessus, "application" se réfère à toutes les couches au-dessus de L4 et n'est pas utilisé au sens de l'OSI.

En général, les résultats des mesures peuvent être influencés par les exigences/réponses d'applications individuelles à l'égard des problèmes suivants :

+ Paquets perdus : les applications peuvent avoir une tolérance variée aux paquets perdus. Une autre considération est la distribution des paquets perdus (c'est-à-dire. aléatoire ou sporadique).
+ Longs délais : de nombreuses applications vont considérer les paquets retardés plus longtemps qu'une certaine valeur comme équivalent à une perte de paquet (c'est-à-dire, les applications en temps réel).
+ Paquets dupliqués : certaines applications peuvent être perturbées si des paquets dupliqués sont reçus.
+ Réarrangement : certaines applications peuvent être perturbées si des paquets arrivent hors séquence. Cela peut être en plus de la possibilité de dépasser le seuil de "long" délai par suite du déclassement.
+ En-tête de paquet corrompu : la plupart des applications vont probablement traiter un paquet avec un en-tête corrompu comme équivalent à un paquet perdu.
+ Charge utile de paquet corrompue : certaines applications (par exemple, des codecs vocaux numériques) peuvent accepter une charge utile de paquet corrompue. Dans certains cas, la charge utile du paquet peut contenir des corrections d'erreur directe (FEC, *forward error correction*) spécifiques de l'application qui peuvent compenser un certain niveau de corruption.
+ Paquets parasites : Dst peut recevoir des paquets parasites (c'est-à-dire, des paquets qui ne sont pas envoyés par Src au titre de la métrique). De nombreuses applications peuvent être perturbées par les paquets parasites.

Selon, par exemple, le niveau de protocole observé, certaines des questions énumérées ci-dessus peuvent n'être pas distinguées des autres par l'application ; il peut être important de préserver la distinction pour les opérateurs de Src, Dst, et/ou le ou les réseaux intermédiaires.

5.1 Applications de mesures

La méthode d'échantillonnage donne un moyen d'effectuer des mesures sans considération des mécanismes éventuels de qualité de service (QS) utilisés dans le réseau IP. À titre d'exemple, pour un mécanisme de QS sans grandes garanties, des mesures peuvent être utilisées pour s'assurer que la "meilleure" classe obtient le service qui a été promis pour la classe de trafic en question. De plus, un opérateur pourrait étudier la qualité d'un service bon marché, à faibles garanties, mis en œuvre en utilisant l'éventuelle bande passante résiduelle dans les autres classes. De telles mesures pourraient être faites soit en étudiant la faisabilité d'un nouveau service, soit sur une base régulière.

Les mesures de service de livraison IP ont été discutées au sein de l'Union Internationale des Télécommunications (UIT). Un cadre de mesures de niveau de service IP (qui fait référence au cadre pour les performances IP de la [RFC2330]) qui est destiné à convenir pour la programmation des services a été approuvé comme Recommandation UIT-T Y.1540 [7]. La Recommandation UIT-T Y.1540 couvre les définitions abstraites des métriques de performances. Le présent mémoire décrit une méthode utile à la fois pour la planification de service et pour les besoins d'essais d'utilisateur final, dans les mesures actives aussi bien que passives.

Les mesures de délai peuvent être unidirectionnelles [3], [4], par paires unidirectionnelles, ou aller-retour [RFC2681]. En conséquence, les mesures peuvent être effectuées avec des horloges d'hôte synchronisées ou non synchronisées. Les différentes possibilités sont énumérées ci-dessous.

Le réglage de mesure de référence pour tous les types de mesures est montré à la Figure 2.

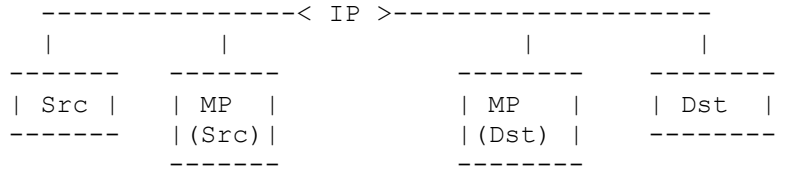

Figure 2 : Exemple de réglage de mesure

Un exemple de l'utilisation de la méthode est un réglage avec un hôte de source (Src), un hôte de destination (Dst), et les points de mesure correspondants (MP(Src) et MP(Dst)) comme le montre la Figure 2. Des équipements séparés pour les points de mesure peuvent être utilisés si la conduite des mesures par Src et/ou Dst peut affecter de façon significative les performances de délai à mesurer. Le MP(Src) devrait être placé/mesuré près du point de sortie des paquets de Src. Le MP(Dst) devrait être placé/mesuré près du point d'entrée des paquets pour Dst. "Près" est défini comme une distance suffisamment petite pour qu'on puisse s'attendre à ce que les caractéristiques de niveau application mesurées (comme le

délai) suivent les caractéristiques de performances correspondantes entre Src et Dst à une précision adéquate. Le principe de base est ici que les résultats de mesure entre MP(Src) et MP(Dst) soient les mêmes que pour une mesure entre Src et Dst, dans la cible de marge d'erreur générale de la mesure (par exemple, < 1 ms ; le nombre de paquets perdus est le même). Si ce n'est pas possible, la différence entre la mesure de MP-MP et la mesure de Src-Dst devrait de préférence être systématique.

Le réglage d'essai qui vient d'être décrit satisfait à deux importants critères :
1) L'essai est fait avec des métriques de flux réalistes, simulant, par exemple, un appel bidirectionnel de voix sur IP (VoIP).
2) On peut obtenir des caractéristiques unidirectionnelles ou d'aller-retour.

Il est aussi possible d'avoir des points de mesure intermédiaires entre MP(Src) et MP(Dst), mais cela sort du domaine d'application du présent document.

5.1.1 Mesure unidirectionnelle

Dans l'intérêt de la spécification de métriques qui soient aussi généralement applicables que possible, des mesures de niveau application fondées sur les délais unidirectionnels sont utilisées dans les exemples de métriques. Les implications des mesures de niveau application pour des applications bidirectionnelles, telles que de conférences interactives multimédia, sont exposées ci-dessous.

Effectuer une seule mesure unidirectionnelle ne donne d'informations sur le comportement du réseau que dans une direction. De plus, le flux au niveau du transport réseau ne simule pas avec précision une connexion multimédia bidirectionnelle.

5.1.2 Paire de mesures unidirectionnelles

Paire de délai unidirectionnel se réfère à deux flux multimédia : de Src à Dst et de Dst à Src pour les mêmes Src et Dst. À titre d'exemple, pour certaines applications, les performances de délai de chaque chemin unidirectionnel sont plus importantes que le délai d'aller-retour. C'est le cas pour les signaux à délai limité tels que ceux de VoIP. Des raisons possibles de la différence entre les délais unidirectionnels sont l'acheminement différent des flux de Src à Dst et de ceux de Dst à Src.

Par exemple, une paire de mesures unidirectionnelles peut montrer que de Src à Dst on a un délai moyen de 30 ms, alors que de Dst à Src on a un délai moyen de 120 ms. Sur une mesure de délai d'aller-retour, cet exemple paraîtrait une moyenne de délai de 150 ms. Sans la connaissance de l'asymétrie, on peut manquer un problème que l'application à l'une ou l'autre extrémité peut avoir avec des délais de plus de 100 ms en moyenne.

De plus, les paires de mesures de délai simulent un appel VoIP bidirectionnel plus précisément qu'une seule mesure unidirectionnelle.

5.1.3 Mesure du délai d'aller-retour

Du point de vue des flux multimédia périodiques, les mesures d'aller-retour présentent deux avantages : elles évitent le besoin de synchronisation de l'horloge des hôtes et elles permettent une simulation de communication bidirectionnelle. Le premier aspect signifie qu'une mesure est facilement effectuée, car aucun équipement particulier ou réglage de NTP n'est nécessaire. La dernière propriété signifie que les flux de mesure sont transmis dans les deux directions. Donc, la mesure donne des informations sur la qualité de service telle que rencontrée par les applications bidirectionnelles.

L'inconvénient des mesures d'aller-retour est le besoin de plus de bande passante qu'un essai unidirectionnel et une comptabilité plus complexe des pertes de paquet. De plus, le flux qui est retourné vers l'envoyeur d'origine peut être plus sporadique que celui de la première "jambe" du voyage aller-retour. Le dernier problème, signifie cependant qu'en pratique le flux de retour peut subir une plus mauvaise QS que le flux sortant, et les estimations de performances ainsi obtenues sont pessimistes. La possibilité d'un acheminement et de mises en file d'attente asymétriques doit être prise en compte durant l'analyse des résultats.

Noter qu'avec des arrangements convenables, les mesures d'aller-retour peuvent être effectuées en utilisant une paire de mesures unidirectionnelles.

5.2 Statistiques calculées à partir d'un seul échantillon

Certaines statistiques peuvent être particulièrement pertinentes pour des applications simulées par des flux périodiques, tels que la gamme de valeurs de délai enregistrées durant l'échantillonnage.

Par exemple, une métrique d'échantillon génère 100 paquets à MP(Src) avec les mesures suivantes à MP(Dst) :
+ 80 paquets reçus avec un délai [i] ≤ 20 ms
+ 8 paquets reçus avec un délai [i] > 20 ms
+ 5 paquets reçus avec des en-têtes de paquet corrompus
+ 4 paquets provenant de MP(Src) sans paquet correspondant enregistré à MP(Dst) (effectivement perdu)
+ 3 paquets reçus avec la charge utile de paquet corrompue et un délai [i] ≤ 20 ms
+ 2 paquets qui dupliquent un des 80 paquets reçus correctement comme indiqué à a première ligne

Par cet exemple, les paquets sont considérés acceptables si ils sont reçus avec des délais inférieure ou égaux à 20 ms et sans en-tête ou charge utile de paquet corrompus. Dans ce cas, le pourcentage de paquets acceptables est de 80/100 = 80 %.

Pour une application différente qui va accepter les paquets avec une charge utile corrompue et pas de limite de délai (pour autant que le paquet soit reçu) le pourcentage de paquets acceptables est de (80 + 8 + 3)/100 = 91 %.

5.3 Statistiques calculées à partir de plusieurs échantillons

Il peut être intéressant de faire plusieurs essais en utilisant cette méthode pour collecter un "échantillon d'échantillons". Par exemple, il peut être plus approprié de simuler 1 000 appels VoIP de deux minutes qu'un seul appel de 2 000 minutes. Quand on considère une collection de plusieurs échantillons, des problèmes comme l'intervalle entre les échantillons (par exemple, des minutes, des heures) la composition des échantillons (par exemple, une durées Tf-T0 égale, des tailles de paquet différentes) et les considérations de réseau (par exemple, faire des échantillons différents sur des combinaisons de liaison à hôte différentes) devraient être pris en compte. Pour des éléments comme l'intervalle entre les échantillons, le schéma d'usage pour les applications intéressantes devrait être examiné.

Lors du calcul des statistiques pour plusieurs échantillons, des statistiques plus générales (par exemple, la médiane, les percentiles, etc.) peuvent être pertinentes avec un plus grand nombre de paquets.

5.4 Conditions fondamentales

Dans de nombreux cas, les résultats peuvent être influencés par les conditions existant à Src, Dst, et/ou tout réseau intervenant. Les facteurs qui peuvent affecter les résultats incluent : les niveaux de trafic et/ou les salves durant l'échantillonnage, les défaillances de liaison et/ou d'hôte, etc. Des informations sur les conditions d'arrière plan peuvent n'être disponibles que par des moyens externes (par exemple, des appels téléphoniques, la télévision) et peuvent ne devenir disponibles que des jours après la prise des échantillons.

5.5 Considérations relatives au délai

Pour les sessions multimédia interactives, le délai de bout en bout est un facteur important. Un délai trop long réduit la qualité de la session multimédia perçue par les participants. Une approche pour gérer les délais de bout en bout sur un chemin Internet impliquant des technologies de couche liaison hétérogènes est d'utiliser des quotas de délai par domaine (par exemple,. 50 ms pour un certain domaine IP). Cependant, ce schéma a de claires insuffisances, et peut trop restreindre le problème de réaliser un objectif de délai de bout en bout. Une mise en œuvre plus souple devrait s'intéresser à des problèmes comme la possibilité de délais asymétriques sur les chemins, et à la sensibilité d'une application aux variations de délai dans un certain domaine. Il y a plusieurs solutions de remplacement quant à la façon dont une statistique de délai devrait être utilisée pour gérer la QS de bout en bout. Cette question, bien que très intéressante sort du domaine d'application de ce mémoire et ne sera pas discutées plus avant ici.

6. Considérations pour la sécurité

6.1 Attaques de déni de service

Cette méthode génère un flux périodique de paquets d'un hôte (Src) à un autre hôte (Dst) à travers des réseaux intervenants. Cette méthode pourrait être détournée pour des attaques de déni de service dirigées contre Dst et/ou le ou les réseaux intervenants.

Les administrateurs de Src, Dst, et des réseaux intervenants devraient établir des accords bilatéraux ou multilatéraux

concernant les horaires, la taille, et la fréquence des collectes de métriques d'échantillons. L'utilisation de cette méthode en dehors des termes des accords entre les participants pourrait causer un rejet immédiat, l'élimination des paquets, ou d'autres procédures de rétorsion définies entre les parties affectées.

6.2 Confidentialité des données d'utilisateur

L'utilisation active de cette méthode génère des paquets pour un échantillon plutôt que de prendre des échantillons sur les données d'usager, et ne menace pas la confidentialité des données d'usager. Les mesures passives doivent restreindre leur attention aux en-têtes intéressants. Comme les charges utiles d'usager peuvent être temporairement mémorisées pour l'analyse de longueur, les précautions convenables DOIVENT être prises pour garder ces informations sûres et confidentielles.

6.3 Interférence avec la métrique

Il est possible d'identifier qu'un certain paquet ou flux de paquets fait partie d'un échantillon. Avec cette connaissance chez Dst et/ou dans les réseaux intervenants, il est possible de changer le traitement des paquets (par exemple, d'augmenter ou diminuer le délai) et d'introduire une distorsion des performances mesurées. Il est aussi possible de générer des paquets supplémentaires qui paraîtraient faire partie de la métrique d'échantillon. Ces paquet supplémentaires perturberaient vraisemblablement les résultat de la mesure de l'échantillon.

Pour décourager le genre d'interférence mentionnées ci-dessus, une vérification des interférences sur les paquets, comme un hachage cryptographique, PEUT être utilisé.

7. Considérations relatives à l'IANA

Comme cette méthode et cette métrique ne définissent pas de protocole ou de valeurs bien connues, il n'y a pas de considérations relatives à l'IANA dans le présent mémoire.

8. Références normatives

[1] [RFC2026] S. Bradner, "Le processus de normalisation de l'Internet -- Révision 3", (BCP0009) octobre 1996. (*MàJ par* RFC3667, RFC3668, RFC3932, RFC3979, RFC3978, RFC5378, RFC6410)

[2] [RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[3] [RFC2330] V. Paxson, G. Almes, J. Mahdavi, M. Mathis, "Cadre pour la mesure des performances d'IP", mai 1998. *(Information)*

[4] [RFC2679] G. Almes, S. Kalidindi, M. Zekauskas, "Métrique de délai unidirectionnel pour IPPM", septembre 1999. *(P.S.)*

[5] [RFC3393] C. Demichelis, P. Chimento, "Métrique de variation de délai de paquet IP pour la mesure des performances IP (IPPM)", novembre 2002. *(P.S.)*

9. Références pour information

[6] ETSI TS 101 329-5 V1.1.2, "End-to-end Quality of Service in TIPHON systems; Part 5: Quality of Service (QoS) measurement methodologies", janvier 2002.

[7] Recommandation UIT-T Y.1540, "Service de communications de données au protocole Internet – Transfert de paquet IP et paramètres de performances de disponibilité", février 1999.

[8] [RFC2681] G. Almes, S. Kalidindi, M. Zekauskas, "Métrique de délai d'aller-retour pour IPPM", septembre 1999. *(P.S.)*

10. Remerciements

Les auteurs souhaitent remercier les présidents du groupe de travail IPPM (Matt Zekauskas et Merike Kaeo) pour leurs commentaires qui ont rendu le présent document plus clair et plus précis. Howard Stanislevic et Will Leland ont aussi présenté des commentaires et questions utiles. Nous saluons avec gratitude les défis continuels de Henk Uijterwaal pour développer les raisons d'utiliser cette méthode. Les auteurs ont construit sur les substantielles fondations édifiées par les auteurs du cadre pour les performances IP [3].

11. Adresse des auteurs

Vilho Raisanen
Nokia Networks
P.O. Box 300
FIN-00045 Nokia Group
Finland
téléphone : +358 7180 8000
mél : Vilho.Raisanen@nokia.com

Glenn Grotefeld
Motorola, Inc.
1501 W. Shure Drive, MS 2F1
Arlington Heights, IL 60004 USA
téléphone : +1 847 435-0730
mél : g.grotefeld@motorola.com

Al Morton
AT&T Labs
Room D3 - 3C06
200 Laurel Ave. South
Middletown, NJ 07748 USA
téléphone : +1 732 420 1571

12. Déclaration complète de droits de reproduction

Copyright (C) The Internet Society (2002). Tous droits réservés.

Le présent document et ses traductions peuvent être copiés et fournis aux tiers, et les travaux dérivés qui les commentent ou les expliquent ou aident à leur mise en œuvre peuvent être préparés, copiés, publiés et distribués, en tout ou partie, sans restriction d'aucune sorte, pourvu que la déclaration de droits de reproduction ci-dessus et le présent paragraphe soient inclus dans toutes telles copies et travaux dérivés. Cependant, le présent document lui-même ne peut être modifié d'aucune façon, en particulier en retirant la notice de droits de reproduction ou les références à la Internet Society ou aux autres organisations Internet, excepté autant qu'il est nécessaire pour le besoin du développement des normes Internet, auquel cas les procédures de droits de reproduction définies dans les procédures des normes Internet doivent être suivies, ou pour les besoins de la traduction dans d'autres langues que l'anglais.

Les permissions limitées accordées ci-dessus sont perpétuelles et ne seront pas révoquées par la Internet Society ou ses successeurs ou ayant droits.

Le présent document et les informations y contenues sont fournies sur une base "EN L'ÉTAT" et le contributeur, l'organisation qu'il ou elle représente ou qui le/la finance (s'il en est), la INTERNET SOCIETY et la INTERNET ENGINEERING TASK FORCE déclinent toutes garanties, exprimées ou implicites, y compris mais non limitées à toute garantie que l'utilisation des informations ci encloses ne violent aucun droit ou aucune garantie implicite de commercialisation ou d'aptitude à un objet particulier.

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.