Groupe de travail Réseau
Request for Comments : 3724
Catégorie : Information
Traduction Claude Brière de L'Isle

J. Kempf, éditeur
R. Austein, éditeur
IAB

mars 2004

La montée du milieu et l'avenir du bout en bout : Réflexions sur l'évolution de l'architecture de l'Internet

Statut de ce mémoire
Le présent mémoire apporte des informations à la communauté de l'Internet. Il ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le principe de bout en bout est la ligne directrice architecturale centrale de l'Internet. Dans ce document, on examine brièvement le développement du principe de bout en bout tel qu'il a été appliqué à l'architecture de l'Internet au fil des ans. On expose les tendances actuelles dans l'évolution de l'architecture de l'Internet en relation avec le principe de bout en bout, et on essaye de tirer des conclusions sur l'évolution du principe de bout en bout, et donc de l'architecture de l'Internet qu'il soutient, à la lumière de ces tendances actuelles.

Table des matières

1. Introduction

Une des lignes directrices clé de l'architecture de l'Internet est le principe de bout en bout dans les articles de Saltzer, Reed, et Clark [1], [2]. Le principe de bout en bout était à l'origine articulé sur la question de savoir où il était le mieux de placer les fonctions dans un système de communication. Puis, dans les années suivantes, il a évolué pour traiter la question de maintenir l'ouverture, une fiabilité et une robustesse croissantes, et de préserver les propriétés de choix de l'utilisateur et de facilité de développement de nouveaux services comme exposé par Blumenthal et Clark dans [3] ; ces questions ne faisaient pas partie de l'articulation originelle du principe de bout en bout.

Dans le présent document, on examine comment l'interprétation du principe de bout en bout a évolué au fil des ans, et où il en est actuellement. On examine les tendances du développement de l'Internet qui ont conduit à une pression pour définir des services dans le réseau, un sujet qui a déjà reçu une certaine attention de la part de l'IAB dans la RFC3238 [5]. On décrit certaines considérations sur la façon dont le principe de bout en bout pourrait évoluer à la lumière de ces tendances.

2. Brève histoire du principe de bout en bout

2.1 Au début...

Le principe de bout en bout était à l'origine articulé comme la question de savoir quel était le meilleur endroit où mettre des fonctions dans un système de communication.

La fonction en question ne peut être complètement et correctement mise en œuvre qu'avec la connaissance et l'aide de l'application qui réside aux points d'extrémité du système de communication. Donc, la fourniture de la fonction en question au titre du système de communication lui-même n'est pas possible. (Parfois, une version incomplète de la fonction fournie par le système de communication peut être utile comme amélioration des performances [1].)

Un exemple spécifique d'une telle fonction est la garantie de livraison [1]. L'ARPANET original retournait un message "Demande du prochain message" chaque fois qu'il livrait un paquet. Bien que ce message soit trouvé utile au sein du réseau comme forme de contrôle d'encombrement, comme l'ARPANET refusait d'accepter un autre message pour la même destination jusqu'à ce que soit retourné l'accusé de réception du précédent, il n'était jamais particulièrement utile comme indication de garantie de livraison. Le problème était que la pile d'hôte chez l'hôte envoyeur ne voulait normalement pas savoir simplement que le réseau avait livré un paquet, mais plutôt, la couche de pile de l'hôte d'envoi veut savoir que la couche de pile de l'hôte receveur a bien traité le paquet. En termes de structure moderne de pile IP, une couche transport fiable exige une indication que le traitement du transport s'est achevé avec succès, comme donné par un message ACK de TCP [4], et pas simplement une indication de la couche IP que le paquet est arrivé. De façon similaire, un protocole de couche application peut exiger un accusé de réception spécifique d'application qui contienne, entre autres choses, un code d'état qui indique ce qu'on a fait de la demande.

Les exemples spécifiques donnés dans [1] et les autres références de l'époque [2] impliquent principalement la transmission de paquets de données : intégrité des données, garanties de livraison, suppression de message dupliqué, chiffrement par paquet, et gestion de transaction. Du point de vue de l'architecture Internet d'aujourd'hui, on verrait la plupart d'entre eux comme des fonctions de couche transport (intégrité des données, garanties de livraison, suppression de message dupliqué, et peut-être gestion de transaction) et les autres comme des fonctions de couche réseau avec soutien à d'autres couches lorsque nécessaire (par exemple, chiffrement de paquet) et non des fonctions de couche application.

2.2 ...Ensuite...

Avec le développement de l'Internet, le principe de bout en bout s'est graduellement élargi à la question de savoir où il serait meilleur de mettre l'état associé aux applications dans l'Internet : dans le réseau ou aux nœuds d'extrémité. Le meilleur exemple est la description de la RFC1958 [6]:

Ce principe a d'importantes conséquences si on exige des applications qu'elles survivent à des défaillances partielles du réseau. Une conception de protocole de bout en bout ne devrait pas s'appuyer sur la conservation de l'état (c'est-à-dire, des informations sur l'état de la communication de bout en bout) à l'intérieur du réseau. Un tel état ne devrait être conservé que dans les points d'extrémité, d'une façon telle que l'état ne puisse être détruit que lorsque le point d'extrémité lui-même coupe la communication (c'est ce qu'on appelle le sort partagé). Une conséquence immédiate de cela est que les datagrammes sont mieux que des circuits virtuels classiques. Le travail du réseau est de transmettre les datagrammes aussi efficacement et souplement que possible. Tout le reste devrait être fait aux extrémités.

L'articulation originelle du principe de bout en bout – que la connaissance et l'assistance du point d'extrémité est essentielle et qu'omettre une telle connaissance et mettre en œuvre une fonction dans le réseau sans une telle connaissance et assistance n'est pas possible – a pris un certain temps pour percoler à travers la communauté de l'ingénierie, et avait évolué à partir de ce point à une position architecturale générale sur ce qui appartient au réseau et ce qui ne lui appartient pas. La RFC1958 utilise le terme de "application" pour signifier la pile réseau toute entière sur le nœud d'extrémité, incluant les couches réseau, transport, et application, à l'opposé de l'articulation antérieure du principe de bout en bout comme étant sur le système de communication lui-même. Le "sort partagé" décrit assez clairement cela : le sort d'une conversation entre deux applications est seulement partagé entre les deux applications ; le sort ne dépend en rien du réseau, excepté pour ce qui est de la capacité du réseau à passer les paquets d'une application à l'autre.

Le principe de bout en bout dans cette formulation est précisément sur quelle sorte d'état est conservé et où.

Pour effectuer son service, le réseau entretient des informations d'état : chemins, garanties de QS qu'il fait, informations de

session lorsque c'est utilisé dans la compression d'en-tête, historique de compression pour la compression de données, et ce qui s'y apparente. Cet état doit être autonome ; des procédures ou protocoles adaptatifs doivent exister pour déduire et conserver cet état, et le changer lorsque la topologie ou l'activité du réseau change. Le volume de cet état doit être minimisé, et la perte de l'état ne doit pas résulter en plus qu'un déni de service temporaire tant qu'existe la connexité. L'état configuré manuellement doit être gardé à un minimum absolu [6].

Dans cette formulation du principe de bout en bout, l'état impliqué dans l'obtention des paquets d'une extrémité du réseau à l'autre est conservé dans le réseau. L'état est un "état mou", dans ce sens qu'il peut être rapidement abandonné et reconstruit (ou même obligé d'être périodiquement renouvelé) lorsque change la topologie du réseau à cause de la mise en service et du retrait de service des routeurs et commutateurs. L'"état dur", l'état duquel dépend le bon fonctionnement de l'application, est seulement conservé dans les nœuds d'extrémité. Cette formulation du principe est un changement radical par rapport à la formulation d'origine du principe, la participation du nœud d'extrémité étant exigée pour la bonne mise en œuvre de la plupart des fonctions.

En résumé, la connaissance générale à la fois du principe lui-même et de ses implications sur la façon de traiter l'état inévitable s'est accrue au fil du temps pour devenir un (sinon le) principe fondateur de l'architecture de l'Internet.

2.3 ..Et maintenant

Un exemple intéressant de la façon dont le principe de bout en bout continue d'influencer le débat technique qui a lieu dans la communauté de l'Internet est la mobilité IP. L'architecture existante d'acheminement Internet fait peser de sévères contraintes sur la façon dont la mobilité IP peut correspondre étroitement au principe de bout en bout sans subir de changements fondamentaux . IPv6 mobile, décrit dans la spécification IPv6 mobile par Johnson, Perkins, et Arkko [7], exige un mandataire d'acheminement dans le réseau de rattachement du nœud mobile (l'agent de rattachement) pour maintenir la transposition entre le localisateur d'acheminement du nœud mobile, l'adresse d'entretien, et l'identifiant de nœud du nœud mobile, l'adresse de rattachement. Mais le mandataire d'acheminement du sous réseau local (l'agent étranger) qui était une caractéristique de l'ancienne conception de l'ancien IPv4 mobile [8] qui compromettait l'acheminement de bout en bout, a été éliminé. Le nœud d'extrémité traite maintenant sa propre adresse d'entretien. De plus, IPv6 mobile inclut des mécanismes sûrs pour optimiser l'acheminement de façon à permettre l'acheminement de bout en bout entre le nœud d'extrémité mobile et le nœud correspondant, supprimant le besoin d'acheminer à travers le mandataire d'acheminement global chez l'agent de rattachement. Ces caractéristiques se fondent toutes sur des considérations de bout en bout. Cependant, le besoin d'un mandataire d'acheminement global chez l'agent de rattachement dans IPv6 mobile est déterminé par l'affectation d'un nom d'emprunt à l'identifiant de nœud global au moyen de l'identifiant d'acheminement dans l'architecture d'acheminement Internet, sujet qui a été discuté dans un atelier de l'IAB et dont le rapport figure dans la RFC2956 [9], et cela n'a pas changé dans IPv6.

En dépit de cette contrainte, la vision qui émerge du groupe de travail de l'IETF qui développe les normes pour le réseautage mobile est celle d'un nœud mobile largement autonome avec plusieurs options de liaisons sans fil, parmi lesquelles le nœud mobile fait son choix. Le nœud d'extrémité est donc responsable de la maintenance de l'intégrité de la communication, comme l'implique le principe de bout en bout. Cette sorte d'application innovante du principe de bout en bout dérive des mêmes considérations de base de fiabilité et de robustesse (intégrité de la liaison sans fil, changements de la connexité et de la disponibilité de service avec le mouvement, etc.) qui ont motivé le développement original du principe de bout en bout. Alors que la fiabilité de base des liaisons filaires, de l'acheminement, et des équipements de commutation s'est considérablement améliorée depuis la formalisation du principe de bout en bout voici 15 ans, la fiabilité ou la non fiabilité des liaisons sans fils est gouvernée plus directement par la physique de base du support et les conditions instantanées de propagation radioélectriques.

3. Tendances opposées au principe de bout en bout

Alors que le principe de bout en bout continue de fournir des fondations solides à beaucoup des travaux de conception de l'IETF, l'application spécifique du principe de bout en bout décrit dans la RFC1958 a été de plus en plus remise en question de diverses directions. L'IAB a été concerné pendant quelques temps par les tendances qui s'opposent au principe de bout en bout, par exemple les RFC2956 [9] et RFC2775 [12]. Ces documents se sont principalement concentrés sur la réduction de la transparence due à l'introduction des NAT et autres mécanismes de traduction d'adresse dans l'Internet, et les conséquences pour le principe de bout en bout de divers scénarios qui impliquent le déploiement complet, partiel, ou le non déploiement de IPv6. Plus récemment, le sujet de l'inquiétude à glissé vers les conséquences du déploiement de services dans le réseau. L'opinion de l'IAB sur les services marginaux à connexion libre (OPES, *Open Pluggable Edge Services*) dans la RFC3238 [5] est destiné affirmer l'intérêt architectural de définir des services dans le réseau et de poser les questions sur la façon dont de tels services peuvent résulter à compromettre la confidentialité, la sécurité et l'intégrité des données de bout en bout. Clark, et al. dans [10] et Carpenter dans la RFC3234 [11] traitent aussi ce sujet de la définition de service dans le réseau.

Peut être que la meilleure récapitulation des forces qui militent contre le principe de bout en bout est l'article de Blumenthal et Clark dans [3]. Les auteurs font le point sur les développements à l'origine de l'Internet parmi une communauté de professionnels de même culture technique qui avaient confiance les uns dans les autres, et était administré par des institutions universitaires et gouvernementales qui mettaient en application une politique excluant toute utilisation commerciale. Les détenteurs de parts majeurs dans l'Internet sont aujourd'hui assez différents. Par conséquent, de nouvelles exigences sont apparues ces dix dernières années. Des exemples de ces exigences sont exposées dans les paragraphes qui suivent. On trouvera d'autres discussions sur les pressions qui s'exercent sur le principe de bout en bout dans l'Internet d'aujourd'hui dans l'exposé de Reed [13] et dans l'article de Moors à la conférence de 2002 sur les communications internationales de l'IEEE [14].

3.1 Le besoin d'authentification

Peut-être que le seul changement le plus important par rapport à l'Internet d'il y a 15 ans est le manque de confiance entre les utilisateurs. Comme les utilisateurs finaux de l'Internet d'il y a 15 ans étaient peu nombreux, et étaient largement enclins à utiliser l'Internet comme un outil de recherches académiques et de communication des résultats de la recherche (l'utilisation explicitement commerciale de l'Internet était interdite quand il était dirigé par le gouvernement des USA) la confiance entre les utilisateurs finaux (et donc l'authentification des nœuds d'extrémité qu'ils utilisent) et entre les opérateurs des réseaux et leurs usagers n'était tout simplement pas un problème en général. Aujourd'hui, les motivations de certains individus qui utilisent l'Internet ne sont pas toujours entièrement conformes à l'éthique, et, même si elles le sont, l'hypothèse que les nœuds d'extrémité vont toujours coopérer pour réaliser une action mutuellement bénéfique, comme l'implique le principe de bout en bout, n'est pas toujours adéquate. De plus, la croissance du nombre d'usagers qui ne sont pas assez sophistiqués en matière de technologie ou simplement pas intéressés par la préservation de leur propre sécurité, a obligé les opérateurs de réseau à devenir plus proactifs pour déployer des mesures pour empêcher les utilisateurs naïfs ou non intéressés de générer par inadvertance ou intentionnellement des problèmes de sécurité.

Alors que le principe de bout en bout n'exige pas des utilisateurs une confiance mutuelle implicite, le manque de confiance dans l'Internet d'aujourd'hui exige des concepteurs d'applications et de systèmes qu'ils fassent des choix sur la façon de traiter l'authentification, tandis que ce choix n'était que rarement apparent 15 ans plus tôt. Un des plus courants exemples des éléments de réseau qui s'interposent entre les hôtes d'extrémité et ceux qui sont dédiés à la sécurité : les pare-feu, les points d'extrémité de tunnel de VPN, les serveurs de certificats, etc. Ces intermédiaires sont conçus pour protéger le réseau contre une attaque sans gène ou pour permettre à des nœuds d'extrémité dont les utilisateurs peuvent n'avoir pas de raison inhérente de se faire confiance de réaliser un certain niveau d'authentification.

En même temps, ces mesures agissent comme des entraves aux communications de bout en bout. Les tiers de confiance intermédiaires ne sont pas une exigence pour la sécurité, car des mécanismes de sécurité de bout en bout, comme S/MIME [15], peuvent être utilisés à la place, et lorsque des mesures d'introduction de tierce partie comme l'infrastructure PKI, ou que des clés sont utilisées dans le DNS pour échanger du matériel de clés, elles n'empiètent pas nécessairement sur le trafic de bout en bout après que l'authentification a été réalisée. Même si des tierces parties sont impliquées, il appartient en fin de compte aux points d'extrémité et en particulier à leurs utilisateurs, de déterminer à quels tiers ils font confiance.

3.2 Nouveaux modèles de service

Les nouveaux modèles de service inspirés par les nouvelles applications exigent de réaliser le niveau de performances approprié comme partie fondamentale du service délivré. Ces modèles de service sont un changement significatif par rapport au modèle original de service au mieux. La messagerie électronique, le transfert de fichiers, et même l'accès à la Toile ne sont pas perçus comme défaillants si les performances se dégradent, bien que l'usager puisse être frustré au moment où il voudrait achever la transaction. Cependant, pour l'audio et la vidéo en direct, pour ne rien dire de la voix et de la vidéo bidirectionnelles en temps réel, réaliser le niveau de performances appropriées, quoique cela puisse signifier pour une expérience acceptable du service par l'usager, fait partie de la livraison du service, et un consommateur qui s'abonne au service est en droit d'attendre le niveau de performances pour lequel il a souscrit. Par exemple, les distributeurs de contenu délivrent parfois les contenus via des serveurs de distribution de contenu qui sont dispersés dans l'Internet en diverses localisations pour éviter des retards de livraison si le serveur est topologiquement assez loin du client. Les services de revente de bande passante et de multimédia sont un nouveau modèle de service pour de nombreux fournisseurs de services.

3.3 La montée des tiers

Il y a 15 ans, les institutions universitaires et gouvernementales géraient l'Internet. Ces institutions ne s'attendaient pas à faire des profits de leurs investissements dans la technologie du réseautage. À l'opposé, l'opérateur de réseau avec lequel traitent aujourd'hui la plupart des utilisateurs de l'Internet est le fournisseur d'accès commercial. Les FAI commerciaux font tourner leur réseau comme une entreprise, et leurs investisseurs s'attendent à juste titre à ce que l'entreprise dégage un profit. Ce changement du modèle d'affaire a conduit à un certain nombre de pressions sur les FAI pour augmenter les perspectives d'affaires en déployant de nouveaux services.

En particulier, la vente standard d'un compte avec tuyau binaire à numérotage avec messagerie électronique et accès protégé est devenu un service de base, résultant en un profil à faible profit. Alors que de nombreux FAI sont heureux avec ce modèle d'affaires et sont capables de survivre avec cela, d'autres aimeraient déployer des modèles de service différents qui aient un potentiel de profit supérieur et fournissent à l'abonné plus de services ou des services différents. Un exemple est la revente d'accès binaire à haut débit via le câble ou le DSL couplé avec du multimédia en direct. Certains FAI qui offrent un accès haut débit déploient aussi des réseaux de distribution de contenu pour augmenter les performances de supports de direct. Ces services sont normalement déployés de telle sorte qu'ils ne soient accessibles qu'au sein du réseau du FAI, et il en résulte qu'ils ne contribuent pas à ouvrir de service de bout en bout. Du point de vue d'un FAI, cependant, l'offre de tels services est une incitation pour le consommateur à acheter le service du FAI.

Les FAI ne sont pas le seul tiers intermédiaire qui soit apparu dans les dix dernières années. À la différence des implications précédentes des organisations et gouvernements dans la gestion de l'Internet, les administrateurs de réseaux d'entreprise et les personnalités gouvernementales sont devenus de plus en plus demandeurs d'opportunités de s'interposer entre les deux parties d'une conversation de bout en bout. Une motivation bénigne de cette implication est d'atténuer le manque de confiance, afin que le tiers agisse comme ancre de confiance ou comme promoteur de bon comportement entre les deux extrémités. Une motivation moins bénigne est pour le tiers d'insérer sa politique pour ses raisons propres, peut-être de taxation ou même de censure. Les exigences des tiers n'ont souvent que peu ou rien du tout à voir avec les aspects techniques, mais découlent plutôt de considérations particulières sociales et légales.

4. Où va le principe de bout en bout ?

Étant données les pressions exercées sur le principe de bout en bout discutées dans la section précédente, une question se pose sur l'avenir du principe de bout en bout. Le principe de bout en bout a t-il ou non un avenir dans l'architecture de l'Internet ? Si il a bien un avenir, comment devrait il s'appliquer ? Une approche clairement improductive pour répondre à cette question est d'insister sur le principe de bout en bout comme principe fondamental ne souffrant aucun compromis. Les pressions décrites ci-dessus sont réelles et puissantes, et si la communauté technique actuelle de l'Internet choisissait d'ignorer ces pressions, le résultat probable est qu'une opportunité du marché sera créée pour une nouvelle communauté technique qui n'ignorera pas ces pressions mais qui pourrait ne pas comprendre les implications de ses choix de conception. Une approche plus productive est de revenir sur les premiers principes et de réexaminer ce que le principe de bout en bout essaye d'accomplir, et de mettre à jour notre définition et l'exposition du principe de bout en bout compte tenu de la complexité de l'Internet d'aujourd'hui.

4.1 Conséquences du principe de bout en bout

Dans cette section, on considère les deux principales conséquences souhaitables du principe de bout en bout : la protection de l'innovation et la fourniture de la fiabilité et de la robustesse.

4.1.1 Protection de l'innovation

Une conséquence désirable du principe de bout en bout est la protection de l'innovation. Exiger des modifications du réseau afin de déployer de nouveaux services est toujours normalement plus difficile que de modifier les nœuds d'extrémité. Le contre argument – que de nombreux nœuds d'extrémité sont maintenant essentiellement des boîtes closes qu'on ne peut pas mettre à jour et que de toutes façons la plupart des usagers ne veulent pas les mettre à jour – ne s'applique pas à tous les nœuds et à tous les usagers. Beaucoup de nœuds d'extrémité sont toujours configurables par l'usager et un pourcentage notable d'usagers sont des "adopteurs précoces" qui veulent rester au contact d'une certaine culture technologique afin d'essayer de trouver de nouvelles idées. Et, même pour les boîtes closes et les usagers non impliqués, le code téléchargeable qui respecte le principe de bout en bout peut fournir une rapide innovation de service. Exiger de quelqu'un qui a une nouvelle idée de service de convaincre un cartel de FAI ou d'administrateurs de réseau d'entreprise de modifier leurs réseaux est beaucoup plus difficile que de simplement créer une page sur la Toile avec un logiciel téléchargeable pour mettre le service en œuvre.

4.1.2 Fiabilité et confiance

Cependant, un souci croissant aujourd'hui est la diminution de la fiabilité et de la robustesse qui résulte d'attaques actives délibérées contre l'infrastructure du réseau et les nœuds d'extrémité. Alors que les développeurs à l'origine de l'Internet se souciaient de défaillances de systèmes à grande échelle, les attaques de la subtilité et de la variété que subit l'Internet d'aujourd'hui n'étaient pas un problème durant le développement de l'Internet d'origine. En aucun cas le principe de bout en bout n'était destiné couvrit la diminution de fiabilité résultant des attaques délibérément orchestrées pour tirer parti de fautes subtiles dans les logiciels. Ces attaques font partie du problème plus large de la rupture de la confiance discutée au paragraphe 3.1. Donc, la question de la rupture de la confiance peut être considérée comme une autre fonction de biais sur l'architecture de l'Internet.

La réaction immédiate à cette rupture de la confiance a été d'essayer de restaurer la sécurité dans les protocoles existants. Bien que cet effort soit nécessaire, il n'est pas suffisant. La question de la confiance doit devenir un principe architectural aussi ferme dans la conception des protocoles à l'avenir que le principe de bout en bout l'est aujourd'hui. La confiance n'est pas seulement l'affaire d'ajouter quelques protections cryptographiques à un protocole après qu'il a été conçu. C'est plutôt avant de concevoir le protocole que les relations de confiance entre les éléments de réseau impliqués dans le protocole doivent être définies, et des frontières doivent être tracées entre les éléments de réseau qui partagent une relation de confiance. Les frontières de la confiance devraient être utilisées pour déterminer quel type de communication survient entre les éléments de réseau impliqués dans le protocole et quels éléments de réseau se signalent les uns aux autres. Lorsque la communication survient à travers une frontière de confiance, une protection cryptographique ou une autre protection de sécurité de quelque sorte peut être nécessaire. Des mesures supplémentaires peuvent être nécessaires pour sécuriser le protocole lorsque les éléments de réseau communicants ne partagent pas une relation de confiance. Par exemple, un protocole peut avoir besoin de minimiser l'état chez le receveur avant d'établir la validité des accréditifs de l'envoyeur afin d'éviter une attaque de déni de service par épuisement de mémoire.

4.2 Le principe de bout en bout dans la conception des applications

La préoccupation exprimée par le principe de bout en bout est applicable aussi à la conception des applications. Deux points clés dans la conception des protocoles d'application sont de s'assurer qu'ils ne dépendent de rien qui pourrait casser le principe de bout en bout et de s'assurer qu'ils peuvent identifier les points d'extrémité de façon cohérente. Un exemple du premier est celui des violations de couche – créer des sujétions qui rendraient impossible à la couche transport, par exemple, de faire son travail correctement. Une autre question est le désir d'insérer plus d'infrastructure d'applications dans le réseau. Les considérations architecturales autour de cette question sont discutées dans la RFC3238 [5]. Ce désir ne résulte pas nécessairement en une violation du principe de bout en bout si le partage des fonctions est fait de telle sorte que les services fournis dans le réseau opèrent avec la connaissance explicite et l'implication des points d'extrémité, lorsque de telles connaissances et implications sont nécessaires pour le bon fonctionnement du service. Le résultat devient une application répartie, dans laquelle le principe de bout en bout s'applique à chaque connexion impliquée dans la mise en œuvre de l'application.

5. La normalisation de l'Internet devient l'arène du conflit

Les normes de l'Internet sont de plus en plus devenues le théâtre d'affrontements [10]. Les FAI ont certaines préoccupations, les milieux d'affaires et les gouvernement en ont d'autres, et les fabricants de matériels et logiciels de réseautage encore d'autres. Souvent, ces préoccupations sont en conflit, et parfois elles sont en conflit avec les préoccupations des utilisateurs finaux. Par exemple, les FAI sont réticents à déployer des services de QS inter domaines parce que, entre autres raisons, chaque instance connue crée une faiblesse significative et facilement exploitable aux attaques de DoS/DDoS. Cependant, certains utilisateurs aimeraient avoir disponible de bout en bout Diffserv ou la QS de style Intserv pour améliorer la prise en charge des applications multimédia vocales et vidéo entre les nœuds d'extrémité de domaines différents, comme exposé par Huston dans la RFC2990 [16]. Dans ce cas, les préoccupations de sécurité, de robustesse, et de fiabilité du FAI sont en conflit avec le désir des utilisateurs d'un type de service différent.

Ces conflits vont inévitablement être reflétés dans l'architecture de l'Internet qui vient. Certains de ces conflits sont impossibles à résoudre au niveau technique, et ne seraient même pas souhaitables, parce qu'ils impliquent des choix sociaux et législatifs qu'il n'est pas au pouvoir de l'IETF de faire (pour un contre argument dans le domaine de la vie privée, voir Goldberg, et al. [17]). Mais pour les conflits qui n'impliquent pas de choix techniques, les importantes propriétés de choix de l'usager et de pouvoir, de fiabilité et d'intégrité de service de bout en bout, de prise en charge de la confiance et du "bon comportement de citoyen du réseau," et de stimulation de l'innovation dans les services devraient être la base sur laquelle se fait la résolution. Le conflit se jouera alors sur le terrain de l'architecture résultante.

6. Conclusions

Le principe de bout en bout continue de guider les développements techniques de la normalisation de l'Internet, et reste aussi important aujourd'hui que par le passé pour l'architecture de l'Internet. Dans de nombreux cas, le démembrement du principe de bout en bout entre ses diverses conséquences conduit à une approche répartie dans laquelle le principe de bout en bout s'applique aux interactions entre les parties individuelles de l'application, alors que les conséquences éclatées, protection de l'innovation, fiabilité, et robustesse, s'appliquent à l'application entière. Alors que le principe de bout en bout avait été généré comme un argument ciblé sur le besoin de connaissance et d'assistance des nœuds d'extrémité pour mettre correctement en œuvre les fonctions dans un système de communication, des propriétés particulières de second ordre développées par l'Internet par suite du principe de bout en bout se sont vues reconnaître comme aussi importantes, sinon plus, que le principe lui-même. Le choix de l'utilisateur final et sa montée en puissance, l'intégrité du service, la prise en charge de la confiance, et le "bon comportement citoyen sur le réseau" sont toutes des propriétés qui se sont développées comme conséquences du principe de bout en bout. Reconnaître ces propriétés dans une proposition particulière de modification de l'Internet est devenu plus important qu'avant lorsque augmentent les pressions pour incorporer des services dans le réseau. Toute proposition d'incorporation de services dans le réseau devrait être mise en balance avec ces propriétés avant de passer aux actes.

7. Remerciements

Beaucoup des idées présentées ici apparaissaient à l'origine dans les travaux de Dave Clark, John Wroclawski, Bob Braden, Karen Sollins, Marjory Blumenthal, et Dave Reed sur les forces qui influencent actuellement l'évolution de l'Internet. Les auteurs tiennent particulièrement à saluer le travail de Dave Clark, qui a été le promoteur original du principe de bout en bout, et qui continue d'inspirer et guider l'évolution de l'architecture de l'Internet, et John Wroclawski, avec qui les conversations durant le développement de cet article ont aidé à préciser les questions qui sont en débat sur l'Internet.

8. Considérations pour la sécurité

Le présent document ne propose aucun nouveau protocole, et n'implique donc aucune considération de sécurité à cet égard. Cependant, tout au long de document, il y a des discussions sur les questions de confidentialité et d'intégrité et sur les exigences architecturales créées par ces questions.

9. Références pour information

[1] Saltzer, J.H., Reed, D.P., et Clark, D.D., "End-to-End Arguments in System Design," ACM TOCS, Vol 2, n°4, novembre 1984, pp 277-288.

[2] Clark, D., "The Design Philosophy of the DARPA Internet Protocols," Proc SIGCOMM 88, ACM CCR Vol 18, n° 4, août 1988, pp. 106-114.

[3] Blumenthal, M., Clark, D.D., "Rethinking the design of the Internet: The end-to-end arguments vs. the brave new world", ACM Transactions on Internet Technology, Vol. 1, n° 1, août 2001, pp 70-109.

[4] J. Postel (éd.), "Protocole de commande de transmission – Spécification du protocole du programme Internet DARPA", RFC0793, STD 7, septembre 1981.

[5] S. Floyd, L. Daigle, "Considérations architecturales et de politique de l'IAB pour des services marginaux à connexion libre (OPES)", RFC3238, janvier 2002. *(Information)*

[6] B. Carpenter, éd., "Principes de l'architecture de l'Internet", RFC1958, juin 1996. (*MàJ par* RFC3439) *(Information)*

[7] D. Johnson, C. Perkins, J. Arkko, "Prise en charge de la mobilité dans IPv6", RFC3775, juin 2004. *(P.S.) (Obs., voir* RFC6275)

[8] C. Perkins, éd., "Prise en charge de la mobilité IP pour IPv4", RFC3344, août 2002. (*MàJ par* RFC4721) *(P.S.)*

[9] M. Kaat, "Compte rendu de l'atelier 1999 de l'IAB sur la couche réseau", RFC2956, octobre 2000. *(Information)*

[10] Clark, D.D., Wroclawski, J., Sollins, K., et Braden, B., "Tussle in Cyberspace: Defining Tomorrow's Internet", Proceedings of Sigcomm 2002.

[11] B. Carpenter, S. Brim, "Boîtiers de médiation : taxonomie et problèmes", RFC3234, février 2002. *(Information)*

[12]B. Carpenter, "Transparence de l'Internet", RFC2775, février 2000. *(Information)*

[13] Reed, D., "The End of the End-to-End Argument?", avril 2000, http://www.reed.com/dprframeweb/dprframe.asp?section=paper&fn=endofendtoend.html .

[14] Moors, T., "A Critical Review of End-to-end Arguments in System Design," Proc. 2000 IEEE International Conference on Communications, pp. 1214-1219, avril 2002.

[15] B. Rmasdell, "Spécification de message S/MIME version 3", RFC2633, juin 1999. (*Obsolète, voir* RFC3851) *(P.S.)*

[16] G. Huston, "Prochaines étapes de l'architecture de qualité de service pour IP", RFC2990, novembre 2000. *(Infor.)*

[17] Goldberg, I., Wagner, D., et Brewer, E., "Privacy-enhancing technologies for the Internet," Proceedings of IEEE COMPCON 97, pp. 103-109, 1997.

10. Informations sur les auteurs

Internet Architecture Board
mél : iab@iab.org

Membres de l'IAB au moment de l'achèvement du présent document :

Bernard Aboba
Harald Alvestrand
Rob Austein
Leslie Daigle
Patrik Faltstrom
Sally Floyd
Jun-ichiro Itojun Hagino
Mark Handley
Geoff Huston
Charlie Kaufman
James Kempf
Eric Rescorla
Mike St. Johns

11. Déclaration complète de droits de reproduction

des droits dans les documents de l'ISOC figurent dans les BCP 78 et BCP 79.

Des copies des dépôts d'IPR faites au secrétariat de l'IETF et toutes assurances de disponibilité de licences, ou le résultat de tentatives faites pour obtenir une licence ou permission générale d'utilisation de tels droits de propriété par ceux qui mettent en œuvre ou utilisent la présente spécification peuvent être obtenues sur répertoire en ligne des IPR de l'IETF à http://www.ietf.org/ipr.

L'IETF invite toute partie intéressée à porter son attention sur tous copyrights, licences ou applications de licence, ou autres droits de propriété qui pourraient couvrir les technologies qui peuvent être nécessaires pour mettre en œuvre la présente norme. Prière d'adresser les informations à l'IETF à ietf- ipr@ietf.org.

Remerciement

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