Groupe de travail Réseau
Request for Comments : 1546
Catégorie : Information
Traduction Claude Brière de L'Isle

C. Partridge, BBN
T. Mendez, BBN
W. Milliken, BBN
november 1993

Service d'envoi à la cantonade pour les hôtes

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

Résumé
La présente RFC décrit un service internet d'envoi à la cantonade pour IP. Le principal objet de ce mémoire est d'établir la sémantique du service d'envoi à la cantonade dans un internet IP. Dans la mesure du possible, ce mémoire essaye de faire abstraction du service réellement fourni par l'inter réseau. Ce mémoire décrit un service expérimental et ne propose pas un protocole. Le présent mémoire est produit par l'équipe de recherche de l'Internet (IRTF, *Internet Research Task Force*).

Motivation
Il y a un certain nombre de situations dans le réseautage où un hôte, une application, ou un utilisateur souhaite localiser un hôte qui prend en charge un service particulier mais, si plusieurs serveurs prennent en charge le service, il ne se soucie pas particulièrement de quel serveur est utilisé. L'envoi à la cantonade est un service d'inter réseautage qui répond à ce besoin. Un hôte transmet un datagramme à une adresse d'envoi à la cantonade et l'inter réseau est chargé de faire au mieux pour livrer le datagramme à au moins, et de préférence un seul, des serveurs qui acceptent les datagrammes pour l'adresse d'envoi à la cantonade

La motivation de l'envoi à la cantonade est qu'il simplifie considérablement la tâche de trouver un serveur approprié. Par exemple, les utilisateurs, au lieu de consulter une liste des serveurs archie et de choisir le plus proche, pourrait simplement taper : telnet archie.net et être connectés au plus proche serveur archie. Les résolveurs du DNS n'auraient plus besoin d'être configurés avec les adresses IP de leurs serveurs, mais pourraient plutôt envoyer une interrogation à une adresse d'envoi à la cantonade bien connue du DNS. Les sites FTP reflétés pourraient de même partager une seule adresse d'envoi à la cantonade, et les utilisateurs pourraient simplement envoyer par FTP à l'adresse d'envoi à la cantonade pour atteindre le plus proche serveur.

Questions d'architecture
Ajouter l'envoi à la cantonade au répertoire des services IP nécessite de prendre des décisions sur la façon d'arbitrer entre les exigences architecturales de IP et celles de l'envoi à la cantonade. Cette section discute ces questions d'architecture.

La première question d'architecture et la plus critique est comment faire cohabiter les service sans état de IP avec le désir d'avoir une adresse d'envoi à la cantonade qui représente un seul hôte virtuel. La meilleure façon d'illustrer ce problème est d'en donner quelques exemples. Dans ces deux exemples, deux hôtes (X et Y) desservent une adresse d'envoi à la cantonade et un autre hôte (Z) utilise l'adresse d'envoi à la cantonade pour contacter un service.

Dans le premier exemple, supposons que Z envoie un datagramme UDP adressé à l'adresse d'envoi à la cantonade. Étant donné qu'une adresse d'envoi à la cantonade est logiquement considérée comme l'adresse d'un seul hôte virtuel, serait il possible que le datagramme soit livré à X et Y ? La réponse à cette question doit clairement être oui, la livraison à X et Y est permise. Il est permis à IP de dupliquer et dérouter des datagrammes, de sorte qu'il y a clairement des scénarios dans lesquels un seul datagramme pourrait être livré aux deux points X et Y. L'implication de cette conclusion est que la définition de l'envoi à la cantonade dans un environnement IP fournit une livraison au mieux du datagramme en envoi à la cantonade à un, mais éventuellement plus d'un, des hôtes qui desservent l'adresse d'envoi à la cantonade de destination.

Dans le second exemple, supposons que Z envoie deux datagrammes adressés à l'adresse d'envoi à la cantonade. Le premier datagramme est livré à X. À quel hôte (X ou Y) le second datagramme est-il livré ? Il serait pratique pour les protocoles à états pleins comme TCP que tous les datagrammes d'une connexion soient livrés à la même adresse d'envoi à la cantonade. Cependant, parce que IP est sans état (et donc ne peut pas garder trace de où les datagrammes antérieurs ont été livrés) et parce que un des buts de l'envoi à la cantonade est de prendre en charge les services de réplication, il semble clair que le second datagramme peut être livré à X ou à Y. Les protocoles à états pleins devront utiliser des mécanismes

supplémentaires pour assurer que les derniers datagrammes sont envoyés au même hôte. On discute ci-dessous les suggestions sur la façon de faire cela avec TCP.

Ayant examiné ces deux exemples, il semble clair que la définition correcte de l'envoi à la cantonade IP est un service qui fournit une livraison sans état au mieux d'un datagramme à la cantonade à au moins un hôte, et de préférence à seulement un hôte, qui dessert l'adresse d'envoi à la cantonade. Cette définition rend clair que les datagrammes envoyés à la cantonade reçoivent le même type de service de base que les datagrammes IP. Et bien que la définition permette la livraison à plusieurs hôtes, il est clair que le but est la livraison à juste un hôte.

Adresses d'envoi à la cantonade
Il apparaît qu'il y a un certain nombre de façons pour prendre en charge les adresses d'envoi à la cantonade, certaines utilisent de petites parties de l'espace d'adresses existant, d'autres exigent qu'une classe spéciale d'adresses IP soit allouée.

L'avantage majeur de l'utilisation de l'espace d'adresses existant est qu'il peut rendre l'acheminement plus facile. Par exemple, considérons une situation où une portion de chaque numéro de réseau IP peut être utilisée pour l'envoi à la cantonade. C'est-à-dire qu'un site, si il le désire, pourrait allouer un ensemble de ses adresses de sous réseau à être des adresses d'envoi à la cantonade. Si, comme le prévoient certains experts, les chemins d'envoi à la cantonade sont traités tout comme les chemins d'hôte par les protocoles d'acheminement, les adresses d'envoi à la cantonade ne vont pas exiger d'annonce particulière en dehors du site – les chemins d'hôte pourraient être classés avec le chemin de réseau. (Si les adresses d'envoi à la cantonade sont prises en charge par des hôtes en-dehors du réseau, alors ces hôtes vont quand même devoir être annoncés en utilisant des chemins d'hôte). Les inconvénients majeurs de cette approche sont (1) qu'il n'y a pas de moyen facile pour les protocoles à états pleins comme TCP de découvrir qu'une adresse est d'envoi à la cantonade, et (2) il est plus difficile de prendre en charge une adresse d'envoi à la cantonade bien connue à l'échelle de l'Internet. La raison pour laquelle TCP a besoin de savoir qu'une adresse est d'envoi à la cantonade est exposée plus en détails ci-dessous. Le souci sur les adresses bien connues d'envoi à la cantonade exige quelques explications. L'idée est que l'Internet pourrait établir qu'une adresse d'envoi à la cantonade particulière est l'adresse logique du serveur DNS. Le logiciel d'hôte pourrait être configuré chez le fabricant à toujours envoyer des interrogations DNS à l'adresse d'envoi à la cantonade du DNS. En d'autres termes, l'envoi à la cantonade pourrait être utilisé pour prendre en charge l'auto configuration des résolveurs du DNS.

Les avantages majeurs de l'utilisation d'une classe séparée d'adresses sont qu'il est facile de déterminer si une adresse est une adresse d'envoi à la cantonade et que les adresses bien connues d'envoi à la cantonade sont plus faciles à prendre en charge. L'inconvénient clé est que l'acheminement peut être plus douloureux, parce que les protocoles d'acheminement vont devoir garder trace de plus de chemins d'envoi à la cantonade

Une approche intermédiaire est de prendre une partie de l'espace d'adresses actuel (disons les adresses de classe C 256) et de faire les adresses réseau dans les adresses d'envoi à la cantonade (et d'ignorer la partie hôte de l'adresse de classe C). L'avantage de cette approche est qu'elle fait ressembler les chemins d'envoi à la cantonade à des chemins du réseau (qui sont plus faciles à traiter pour certains protocoles d'acheminement). Les inconvénients sont qu'elle utilise de façon inefficace l'espace d'adresses et limite très sévèrement le nombre d'adresses d'envoi à la cantonade qui peuvent être prises en charge.

Face à ce choix, il semble plus sage d'utiliser une classe d'adresses distincte. Prendre les adresses d'envoi à la cantonade dans l'espace d'adresses existant semble devoir plus probablement causer des problèmes dans les situations dans lesquelles des applications échouent à tort à reconnaître des adresses d'envoi à la cantonade (si les envois à la cantonade font partie de l'espace d'adresse de chaque site) ou utilisent l'espace d'adresses de façon inefficace (si des adresses réseau sont utilisées comme adresses d'envoi à la cantonade). Et les avantages de l'utilisation des adresses d'envoi à la cantonade pour l'auto configuration semble irrésistible. Donc le présent mémoire suppose que les adresses d'envoi à la cantonade vont être une classe distincte d'adresses IP (non encore allouées). Comme chaque adresse d'envoi à la cantonade est une adresse d'hôte virtuel et que le nombre d'hôtes d'envoi à la cantonade semble ne devoir pas être plus grand que le nombre de services offerts par des protocoles comme TCP et UDP, l'espace d'adresses pourrait être assez petit, prenant peut-être en charge pas plus de 2**16 adresses différentes.

Transmission et réception de datagrammes à la cantonade
Historiquement, les services IP ont été conçus pour fonctionner même si des routeurs ne sont pas présents (par exemple, sur des LAN sans routeur). De plus, nombreux sont ceux qui dans la communauté Internet ont historiquement pensé que les hôtes ne devraient pas avoir à participer aux protocoles d'acheminement pour fonctionner. (Voir, par exemple, la page 7 du STD 3, RFC 1122). Pour fournir un service d'envoi à la cantonade cohérent avec ces traditions, le traitement des adresses d'envoi à la cantonade varie légèrement selon le type de réseau sur lequel sont envoyés les datagrammes qui ont des adresses d'envoi à la cantonade.

Sur un réseau à supports partagés, comme un Ethernet et ou anneau à jetons, il doit être possible de transmettre un datagramme en envoi à la cantonade à un serveur aussi sur le même réseau sans consulter un routeur (qui pourrait ne pas exister). Il y a au moins deux façons dont cela peut être fait.

Une approche est de faire une recherche ARP pour l'adresse d'envoi à la cantonade Les serveurs qui prennent en charge l'adresse d'envoi à la cantonade peuvent répondre à une demande d'ARP, et l'hôte envoyeur peut transmettre au premier serveur qui répond. Cette approche est une réminiscence du mandataire ARP (RFC 1027) et comme le mandataire ARP, elle exige des temporisations d'antémémoire ARP pour que les adresses d'envoi à la cantonade restent petites (environ une minute) afin que si un serveur d'envoi à la cantonade a une défaillance, les hôtes purgent rapidement l'entrée d'ARP et interrogent d'autres serveurs qui prennent en charge l'adresse d'envoi à la cantonade

Une autre approche est que les hôtes transmettent les datagrammes en envoi à la cantonade sur une adresse de diffusion groupée de niveau liaison. Les hôtes qui desservent une adresse d'envoi à la cantonade sont supposés être à l'écoute de l'adresse de diffusion groupée de niveau liaison pour les datagrammes destinés à leur adresse d'envoi à la cantonade. Par la diffusion groupée sur le réseau local, il n'y a pas besoin qu'un routeur achemine les datagrammes en envoi à la cantonade. Un mérite de cette approche est que si il y a plusieurs serveurs et qu'un d'eux a une défaillance, les autres vont quand même recevoir les demandes. Un autre avantage possible est que, comme les entrées d'envoi à la cantonade de ARP doivent être périmées rapidement, l'approche de la diffusion groupée peut être moins consommatrice de trafic que l'approche ARP parce que dans celle-ci, les transmissions à une adresse d'envoi à la cantonade vont probablement causer une diffusion d'ARP, tandis que dans l'approche de la diffusion groupée, les transmissions sont seulement pour un groupe de diffusion groupée choisi. Un inconvénient évident est que si il y a plusieurs serveurs sur un réseau, ils vont tous recevoir le message en envoi à la cantonade, alors que la livraison à un seul serveur est désirée.

Sur les liaisons en point à point, la prise en charge de l'envoi à la cantonade est plus simple. Une seule copie du datagramme d'envoi à la cantonade est transmise le long de la liaison appropriée vers la destination d'envoi à la cantonade

Quand un routeur reçoit un datagramme en envoi à la cantonade, le routeur doit décider si il devrait transmettre le datagramme, et si il le doit, transmettre une copie du datagramme au prochain bond sur le chemin. Noter que bien qu'on puisse espérer qu'un routeur va toujours connaître le prochain bond correct pour un datagramme en envoi à la cantonade et ne va pas avoir à envoyer en diffusion groupée les datagrammes en envoi à la cantonade sur un réseau local, il y a probablement des situations dans lesquelles il y a plusieurs serveurs sur un réseau local, et pour éviter d'envoyer à un qui a eu récemment une défaillance, les routeurs peuvent souhaiter envoyer les datagrammes en envoi à la cantonade sur une adresse de diffusion groupée de niveau liaison. Parce que les hôtes peuvent envoyer en diffusion groupée tous les datagrammes, les routeurs devraient veiller à ne pas transmettre un datagramme si ils pensent qu'un autre routeur va aussi le transmettre.

Les hôtes qui souhaitent recevoir des datagrammes pour une adresse d'envoi à la cantonade particulière vont devoir annoncer aux routeurs qu'ils se sont joints à l'adresse d'envoi à la cantonade Sur des réseaux à supports partagés, le meilleur mécanisme est probablement qu'un hôte envoie périodiquement en diffusion groupée des informations sur les adresses d'envoi à la cantonade qu'il prend en charge (éventuellement en utilisant une version améliorée de IGMP). Les messages en en diffusion groupée assurent que tous les routeurs sur le réseau entendent que l'adresse d'envoi à la cantonade est prise en charge sur le sous réseau local et peuvent annoncer ce fait (si c'est approprié) aux routeurs du voisinage. Noter que si il n'y a pas de routeurs sur le sous réseau, les messages en diffusion groupée vont simplement être ignorés. (L'approche de la diffusion groupée est suggérée parce qu'il semble qu'elle est probablement plus simple et plus fiable que de développer un protocole d'enregistrement, dans lequel un serveur d'envoi à la cantonade devrait s'enregistrer auprès de chaque routeur sur son réseau local).

Sur des liaisons en point à point, un hôte peut simplement annoncer ses adresses d'envoi à la cantonade au routeur à l'autre extrémité de la liaison.

On observe que les protocoles d'annonces sont une forme de protocole d'acheminement et qu'il peut y avoir du sens à simplement exiger que les serveurs d'envoi à la cantonade participent (au moins en partie) aux échanges de messages d'acheminement réguliers.

Quand un hôte reçoit un datagramme IP destiné à une adresse d'envoi à la cantonade qu'il prend en charge, l'hôte devrait traiter le datagramme IP juste comme si il était destiné à une des adresses IP non d'envoi à la cantonade de l'hôte. Si l'hôte ne prend pas en charge l'adresse d'envoi à la cantonade, il devrait éliminer en silence le datagramme.

Les hôtes devraient accepter les datagrammes avec une adresse de source d'envoi à la cantonade, bien que certains protocoles de transport (voir ci-dessous) puissent refuser de les accepter.

Comment UDP et TCP utilisent l'envoi à la cantonade
Il est important de se souvenir que l'envoi à la cantonade est un service sans état. Un inter réseau n'a pas d'obligation de livrer deux paquets successifs envoyés à la même adresse d'envoi à la cantonade pour le même hôte.

Parce que UDP est sans état et que l'envoi à la cantonade est un service sans état, UDP peut traiter les adresses d'envoi à la cantonade comme des adresses IP régulières. Un datagramme UDP envoyé à une adresse d'envoi à la cantonade est juste comme un datagramme UDP en envoi individuel du point de vue de UDP et de son application. Un datagramme UDP provenant d'une adresse d'envoi à la cantonade est comme un datagramme provenant d'une adresse d'envoi individuel. De plus, un datagramme provenant d'une adresse d'envoi à la cantonade pour une adresse d'envoi à la cantonade peut être traité par UDP tout comme un datagramme en envoi à la cantonade (bien que la sémantique d'application d'un tel datagramme ne soit pas tout à fait claire).

L'utilisation par TCP de l'envoi à la cantonade est moins directe parce que TCP est à états pleins. Il est difficile d'envisager comment on va maintenir l'état TCP avec un homologue d'envoi à la cantonade quand deux segments TCP successifs envoyés à l'homologue d'envoi à la cantonade pourraient être livrés à des hôtes complètement différents.

La solution à ce problème est de ne permettre des adresses d'envoi à la cantonade que comme adresse distante d'un segment TCP SYN (sans le bit ACK établi). TCP peut alors initier une connexion à une adresse d'envoi à la cantonade. Quand le SYN-ACK est renvoyé par l'hôte qui a reçu le segment d'envoi à la cantonade, le TCP initiateur devrait remplacer l'adresse d'envoi à la cantonade de son homologue par l'adresse de l'hôte qui retourne le SYN-ACK. (Le TCP initiateur peut reconnaître la connexion pour laquelle le SYN-ACK est destiné en traitant l'adresse d'envoi à la cantonade comme une adresse à caractère générique, qui correspond à tout segment SYN-ACK entrant avec l'accès et adresse de destination corrects, pourvu que l'adresse complète du SYN-ACK, incluant l'adresse de source, ne corresponde pas à une autre connexion et que les numéros de séquence dans le SYN-ACK soient corrects.) Cette approche assure qu'un TCP, après avoir reçu le SYN-ACK, est toujours en communication avec un seul hôte.

Applications et envoi à la cantonade
En général, les applications utilisent les adresses d'envoi à la cantonade comme toute autre adresse IP. La seule utilisation d'applications de l'envoi à la cantonade qui pose problème est celle d'applications qui essayent de conserver des connexions à états pleins sur UDP et des applications qui essayent de conserver l'état à travers plusieurs connexions TCP. Parce que l'envoi à la cantonade est sans état et ne garantit pas la livraison de plusieurs datagrammes en envoi à la cantonade au même système, une application ne peut pas être sûre qu'elle est en communication avec le même homologue dans deux transmissions UDP successives ou dans deux connexions TCP successives à la même adresse d'envoi à la cantonade.

Les solutions évidentes à ces problèmes sont d'exiger des applications qui souhaitent conserver l'état qu'elles apprennent l'adresse d'envoi individuel de leur homologue sur le premier échange de datagrammes UDP ou durant le première connexion TCP et qu'elles utilisent l'adresse d'envoi individuel dans les futures conversations.

Envoi à la cantonade et diffusion groupée
Il a souvent été suggéré que la diffusion groupée IP peut être utilisée pour la localisation de ressource, de sorte qu'il est utile de comparer les services offerts par la diffusion groupée IP et l'envoi à la cantonade IP.

Sémantiquement, la différence entre les deux services est qu'une adresse d'envoi à la cantonade est l'adresse d'un seul hôte (virtuel) et que l'inter réseau va faire un effort pour livrer les datagrammes d'envoi à la cantonade à un seul hôte. Il y a deux implications à cette différence. D'abord, les applications qui envoient aux adresses d'envoi à la cantonade n'ont pas besoin de se soucier de gérer les TTL de leurs datagrammes IP. Les applications qui utilisent la diffusion groupée pour trouver un service doivent équilibrer leurs TTL pour maximiser les chances de trouver un serveur tout en minimisant les chances d'envoyer des datagrammes à un grand nombre de serveurs dont elles ne se soucient pas. Ensuite, faire une connexion TCP pour une adresse d'envoi à la cantonade a un sens, tandis que la signification de l'établissement d'une connexion TCP à une adresse de diffusion groupée n'est pas claire. (une connexion TCP à une adresse de diffusion groupée va probablement essayer d'établir une connexion avec plusieurs homologues simultanément, ce que TCP n'est pas destiné à prendre en charge).

D'un point de vue pratique, la différence majeure entre l'envoi à la cantonade et la diffusion groupée est que l'envoi à la cantonade est une utilisation spéciale de l'adressage en envoi individuel tandis que la diffusion groupée exige un support d'acheminement plus sophistiqué. L'observation importante est que plusieurs chemins pour une adresse d'envoi à la cantonade apparaissent à un routeur comme plusieurs chemins à une destination d'envoi individuel, et le routeur peut utiliser des algorithmes standard pour choisir le meilleur chemin.

Une autre différence entre les deux approches est que la localisation de ressource en utilisant la diffusion groupée cause normalement l'envoi de plus de datagrammes. Pour trouver un serveur en utilisant la diffusion groupée, une application est

supposée transmettre et retransmettre un datagramme en diffusion groupée avec des TTL IP successivement plus grands. Le TTL est initialement gardé petit pour essayer de limiter le nombre de serveurs contactés. Cependant, si aucun serveur ne répond, le TTL doit être augmenté avec l'hypothèse que les serveurs disponibles (si il en est) sont plus loin que ce qui était accessible avec le TTL initial. Par suite, la localisation de ressource en utilisant la diffusion groupée cause l'envoi d'un ou plusieurs datagrammes en diffusion groupée vers plusieurs serveurs, avec le TTL de certains datagrammes qui expire avant d'atteindre un serveur. Avec l'envoi à la cantonade, la gestion du TTL n'est pas requise et donc (en ignorant le cas de perte) un seul datagramme a besoin d'être envoyé pour localiser un serveur. De plus, ce datagramme va suivre un seul chemin.

Une différence mineure entre les deux approches est que l'envoi à la cantonade peut être moins tolérant aux fautes que la diffusion groupée. Quand un serveur d'envoi à la cantonade a une défaillance, certains datagrammes peuvent continuer d'être mal acheminés au serveur, tandis que si le datagramme avait été en diffusion groupée, d'autres serveurs l'auraient reçu.

Travaux connexes

Le protocole d'accès aux hôtes ARPANET AHIP-E décrit dans la RFC 878 prend en charge l'adressage logique qui permet à plusieurs hôtes de partager une seule adresse logique. Ce schéma pourrait être utilisé pour prendre en charge l'envoi à la cantonade au sein d'un sous réseau PSN.

Considérations sur la sécurité

Il y a au moins deux problèmes de sécurité dans l'envoi à la cantonade, qui sont simplement mentionnés ici sans suggérer de solutions.

D’abord, il est clair que des hôtes malveillants pourraient se porter volontaires pour desservir une adresse d'envoi à la cantonade et détourner des serveurs légitimes sur eux-mêmes les datagrammes en envoi à la cantonade.

Ensuite, des hôtes espions pourraient répondre aux interrogations en envoi à la cantonade avec des informations inappropriées. Comme il n'y a pas de moyen de vérifier les membres dans une adresse d'envoi à la cantonade, il n'y a pas de moyen de détecter que l'hôte espion ne dessert pas l'adresse d'envoi à la cantonade pour laquelle l'interrogation originale a été envoyée.

Remerciements

Le présent mémoire a bénéficié des commentaires de Steve Deering, Paul Francis, Christian Huitema, Greg Minshall, Jon Postel, Ram Ramanathan, et Bill Simpson. Cependant, les auteurs sont seuls responsables de toutes les idées de ce travail.

Adresses des auteurs

Craig Partridge
Bolt Beranek et Newman
10 Moulton St
Cambridge MA 02138
mél : craig@bbn.com

Trevor Mendez
Bolt Beranek et Newman
10 Moulton St
Cambridge MA 02138
mél : tmendez@bbn.com

Walter Milliken
Bolt Beranek et Newman
10 Moulton St
Cambridge MA 02138
mél : milliken@bbn.com