RFC 7971 : Application-Layer Traffic Optimization (ALTO) Deployment Considerations

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 novembre 2016

Date de publication du RFC : Octobre 2016

https://www.bortzmeyer.org/7971.html

Il est fréquent aujourd'hui sur l'Internet qu'une application cherche à accéder à un contenu (mettons un film, ou bien la mise à jour d'un gros logiciel) qui est disponible à plusieurs endroits. Dans ce cas (qui est notamment fréquent pour le téléchargement en pair-à-pair), quelle source utiliser ? La « meilleure », bien sûr, mais comment la connaître ? Le but du protocole ALTO est de permettre de distribuer de l'information sur la topologie du réseau, afin que les applications puissent choisir la source la plus proche d'elles. ALTO est déjà normalisé (RFC 7285 [1]), ce nouveau RFC sert juste à décrire les scénarios d'usage et à donner des conseils pratiques de déploiement (déploiement qui semble très limité pour l'instant).

Outre le RFC décrivant le protocole (RFC 7285), il peut être utile de lire la description du problème qu'ALTO veut résoudre, le RFC 5693, et le cahier des charges, dans le RFC 6708.

La section 2 de notre RFC résume le fonctionnement d'ALTO. C'est un protocole client-serveur, le serveur ALTO connait l'information (la topologie du réseau, qui est connecté à qui, par quel genre de liens), le client est l'application qui veut accéder au contenu, il connait un ensemble potentiel de sources, et il veut savoir quelle est la « meilleure ». Par exemple, dans le cas de BitTorrent, le client a les adresses IP de l'essaim, il veut savoir à laquelle ou lesquelles demander les bouts de fichier ("*chunks*") qui forment le contenu. Le client ALTO peut être un processus séparé, tournant en permanence, ou bien une bibliothèque liée à l'application. Il doit évidemment parler le protocole ALTO, donc connaitre HTTP et JSON.

Pour déployer ALTO, il y a donc quatre entités logiques à considérer :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7285.txt

— L'origine de l'information (celle qui a compilé les informations de topologie, par exemple en commençant par lister les préfixes IP connus),
— Le serveur ALTO, qui va distribuer cette information,
— Le client ALTO, qui va la récupérer,
— L'application ("*resource consumer*", dans le RFC), qui va en faire quelque chose d'utile.

Ces entités sont typiquement gérées par des organisations différentes. Un exemple typique (mais ce n'est pas la seule possibilité) est que le FAI soit à l'origine de l'information (il connait son réseau), et la mette dans un serveur ALTO qu'il gère, ses abonnés ayant installé une application de partage de fichiers qui inclut un client ALTO. Dans ce cas, il y aurait deux organisations, le FAI gérant les deux premières entités et l'abonné les deux dernières. Mais d'autres répartitions peuvent exister.

Les organisations qui peuvent être impliquées sont en effet multiples : FAI et opérateurs réseau, bien sûr, utilisateurs, évidemment (agissant, soit seuls, soit en groupes se répartissant le travail), mais aussi des tiers, spécialisés dans la collecte et la distribution de cette information (par exemple des CDN). On pourrait même voir apparaitre des sociétés qui ne font que de l'ALTO.

Tout ceci a des conséquences sur le déploiement. Par exemple, un utilisateur peut faire confiance à un FAI mais pas à des tiers. Un FAI peut souhaiter distribuer de l'information à ses abonnés mais pas à tout l'Internet. ALTO définit un protocole, pas une politique : ce protocole permet différents modèles, y compris celui de serveurs ALTO spécialisés et payants. Autre conséquence de l'utilisation de telle ou telle répartition du travail, on pourrait avoir des serveurs ALTO partiels, qui ne contiennent de l'information que sur certains réseaux.

Dans tous les cas, le RFC rappelle qu'ALTO est juste une optimisation : une application doit fonctionner même si elle ne trouve aucun serveur ALTO, ou bien s'ils sont en panne.

Un petit rappel utile sur ALTO : il existe deux modes de fonctionnement différents, qui ont tous les deux des conséquences importantes, notamment sur la confidentialité. Dans le premier mode, le serveur ALTO fournit l'information qu'il a (sous forme de "*maps*", des ensembles de données sur le réseaux, les liens, leur coût, etc) et le client cherche dedans ce qui l'intéresse. Ce mode préserve la vie privée du client (qui ne dit pas au serveur ce qui l'intéresse) mais pas celle du serveur (qui doit tout envoyer). Il n'est pas évident que beaucoup de FAI acceptent cela. Dans le second mode, le serveur permet des interrogations sur un point particulier (« qui est le plus proche de moi ? `192.0.2.87`, `203.0.113.122` ou bien `198.51.100.20` ? »). Ce mode évite au serveur de tout divulguer mais oblige en revanche le client à révéler ses intentions (ici, les adresses IP des pairs potentiels, ce qui peut intéresser des organisations répressives comme la HADOPI). Notez que la fuite d'informations du serveur existe aussi dans le second mode : plusieurs clients ALTO peuvent coopérer pour poser beaucoup de questions et extraire ainsi une partie substantive de la base.

La partie 3 de notre RFC en vient aux conseils concrets pour les FAI. On considère que l'objectif du FAI est de minimiser ses coûts, donc a priori de garder le maximum de trafic en local (il y a des exceptions, que liste le RFC). Le serveur ALTO que gère le FAI va donc annoncer des coûts plus faibles pour les liens locaux.

Mais, d'abord, le FAI doit « remplir » le serveur ALTO avec de l'information. Cette étape d'avitaillement commence par la récolte d'informations sur le réseau. A priori, le FAI connait son propre réseau, et n'a donc pas de mal à récolter ces informations. Outre sa propre documentation interne, le FAI peut aussi utiliser de l'information issue d'autres sources, par exemple les protocoles de routage comme BGP (cf., entre autres, le RFC 7752) ou bien des mesures actives ou passives (cf. entre autres, le RFC 7491). Rappelez-vous qu'ALTO est uniquement un protocole permettant d'accéder à de l'information sur la topologie. Comment cette information a été récoltée et agrégée n'est pas de la responsabilité d'ALTO, de même que le protocole HTTP ne se soucie pas de comment est fabriquée la page HTML qu'il sert.

Le FAI doit ensuite appliquer ses critères (coût, performance, etc) à la topologie. Ces critères sont forcément imparfaits. Le client ALTO ne doit pas s'attendre à ce que l'information qui lui est donnée soit idéale dans tous les cas. Par exemple, le serveur ALTO peut indiquer un lien rapide et pas cher mais qui, au moment où le téléchargement commencera, sera saturé par un trafic intense (ALTO ne prétend pas être temps-réel). Et il y a bien d'autres choses qui ne seront pas connues de ceux qui ont compilé l'information, ou bien qui n'auront pas été incluses dans la base de données du serveur ALTO (« la carte n'est pas le territoire »). Les données distribuées par ALTO, les "*maps*", sont supposées être relativement statiques. Mais, dans le monde réel, les choses changent et le client recevra donc peut-être une information légèrement dépassée.

Si vous trouvez le concept de "*map*" un peu abstrait, la section 3.5 du RFC donne plusieurs exemples. Par exemple, dans le cas le plus simple, celui d'un petit FAI ayant un seul opérateur de transit, les adresses dudit FAI seront dans le PID ("*Provider-defined IDentifier*", cf. RFC 7285, section 5.1) 1, tout le reste de l'Internet étant le PID 2. Cela donnera une "*map*" (syntaxe décrite dans le RFC 7285, section 9.2) :

```
{
...
 "network-map" : {
   "PID1" : {
     "ipv4" : [
       "192.0.2.0/24",
       "198.51.100.0/25"
     ],
     "ipv6" : [
       "2001:db8:100::/48"
     ]
   },
   "PID2" : {
     "ipv4" : [
       "0.0.0.0/0"
     ],
     "ipv6" : [
       "::/0"
     ]
   }
 }
}
```

Un FAI plus gros, et à la topologie plus complexe, a plein de possibilités. Par exemple, ses propres réseaux peuvent être dans des PID différents, s'il veut pouvoir garder le trafic local à un de ses réseaux. Un exemple est celui où le même FAI a des abonnés fixes et mobiles, et où on souhaite limiter les transferts des abonnés fixes vers les mobiles, pour réduire l'utilisation des liens hertziens.

Reste ensuite à effectuer le déploiement des serveurs ALTO. Il existe plusieurs mises en œuvre logicielles d'ALTO et des compte-rendus d'expérience figurent dans les "*Internet-Drafts*" `draft-seidel-alto-map-calcula` et `draft-lee-alto-chinatelecom-trial` et dans le RFC 6875 (ainsi que, pour un protocole antérieur à ALTO, dans le RFC 5632). Cette expérience montre que certaines façons de collecter l'information peuvent être coûteuses : si un FAI a plusieurs liens avec l'Internet, et reçoit un flux BGP complet, et veut mettre chaque préfixe de la DFZ dans ses "*maps*", il doit prévoir des machines assez costaud pour traiter cette information importante et assez changeante. Et le résultat serait une "*map*" qu'il serait difficile d'envoyer à tous les clients, vu sa taille. Il faut donc prévoir, dans ce cas extrême, de l'agrégation vigoureuse des préfixes IP.

La section 4 de notre RFC couvre ensuite l'utilisation d'ALTO, une fois qu'il est déployé. Normalement, tout le monde a intérêt à ce que ALTO soit utilisé : le FAI veut que les utilisateurs épargnent les

liens réseaux les plus lents et les plus coûteux et les utilisateurs veulent les meilleures perfomances. En théorie, tout le monde trouvera son intérêt à utiliser ALTO.

Un exemple est celui de BitTorrent. Si les pairs BitTorrent incluent un client ALTO, chaque pair, quand il reçoit une liste d'adresses IP de l'essaim, peut alors interroger le serveur ALTO et trouver les « meilleurs » pairs. Ils peuvent même échanger cette information entre eux (PEX, "*Peer EXchange*", dans le monde BitTorrent). Mais une autre possibilité est que ce ne soient pas les pairs qui interrogent le serveur ALTO mais le "*tracker*" (pour les essaims fonctionnant avec une machine qui sert de "*tracker*", ce qui n'est pas toujours le cas). Ainsi, il n'est pas nécessaire de mettre un client BitTorrent dans chaque pair, c'est le "*tracker*" qui, grâce à l'information ALTO, choisit les meilleurs pairs pour chacun, et ne leur envoie que cela.

Le RFC se conclut pas une section 7 sur la sécurité. Parmi les problèmes à considérer, il y a le fait qu'un serveur ALTO malveillant, ou bien un serveur se faisant passer pour un serveur ALTO légitime, peut empoisonner le client avec de fausses données.