

RFC 6646 : DECoupled Application Data Enroute (DECADE) Problem Statement

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 10 juillet 2012. Dernière mise à jour le 20 septembre 2012

Date de publication du RFC : Juillet 2012

<https://www.bortzmeyer.org/6646.html>

Le groupe de travail DECADE <<http://tools.ietf.org/wg/decade>> de l'IETF travaillait à optimiser les applications pair-à-pair notamment en leur permettant de stocker facilement des données dans le réseau (on devrait dire le "cloud", pour que ce RFC se vende mieux). Ce RFC décrit précisément les problèmes que DECADE essayait de résoudre, les solutions étant prévues pour de futurs documents. Le principal problème identifié est de doter les applications P2P d'accès à des caches dans le réseau, évitant d'utiliser de manière répétée des liens coûteux et/ou lents. DECADE ayant été fermé en septembre 2012 <<http://www.ietf.org/mail-archive/web/decade/current/msg00805.html>>, le projet ne se conclura sans doute pas.

Ce n'est pas que ces caches n'existent pas déjà : des tas d'applications en ont. Mais ils souffrent de limites : étant souvent spécifiques à une application (BitTorrent, FlashGet, Thunder, etc), ils ne peuvent pas être réutilisés via un protocole standard, et ils n'ont pas de mécanismes de contrôle d'accès permettant, par exemple, de mettre des données dans le cache mais de limiter leur accès à certains.

Le pair-à-pair sert à beaucoup de choses (deux cas connus sont le partage de fichiers, et le "streaming" vidéo) et ces usages sont souvent très consommateurs de ressources réseau. Cette consommation <http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009> justifie qu'on travaille activement à limiter le gaspillage. C'est particulièrement gênant pour « le dernier kilomètre », la ligne, relativement lente, qui connecte M. Toutlemonde à son FAI. Les accès actuellement commercialisés sont presque toujours asymétriques (bien plus de capacité dans le sens TF1- ζ temps-de-cerveau que dans le sens citoyen-producteur- ζ réseau). Si M. Toutlemonde a un gros fichier sur le disque dur de son PC à la maison, et que dix personnes le téléchargent, le gros fichier encombrera dix fois l'accès « montant » de M. Toutlemonde, à son grand dam. Il est ainsi courant que la grande majorité de la capacité montante soit prise par le pair-à-pair. M. Toutlemonde pourrait « téléverser » le fichier une fois pour toutes chez un hébergeur situé « dans le nuage » mais attention : pour qu'il conserve les avantages du pair-à-pair, cela devrait être intégré dans les applications, sans qu'il y ait besoin d'un

compte Dropbox (avec acceptation de conditions d'usage qui disent que le gérant du nuage fait ce qu'il veut des données), d'un téléversement explicite, etc. Bref, que cela se fasse tout seul.

Un problème analogue à celui de M. Toutlemonde est celui de l'hébergeur dont un client a un fichier qui intéresse dix personnes à l'extérieur de l'hébergeur. Faire passer le fichier dix fois sur les coûteux liens de transit n'est pas une utilisation géniale de la capacité réseau... À noter qu'une autre voie d'optimisation, complémentaire de celle de DECADE, est celle du groupe de travail ALTO <<http://tools.ietf.org/wg/alto>>, qui consiste à faciliter la découverte de ressources proches (« télécharger localement »), comme décrit dans le RFC 5693¹. ALTO ne fonctionne que si le contenu est déjà disponible localement. Sinon, DECADE prend le relais. Deux autres efforts IETF qui ont un rapport avec DECADE, et lui sont complémentaires, sont PPSP <<http://tools.ietf.org/wg/ppsp/>>, sur la conception d'un protocole de "streaming" en pair-à-pair (RFC 7574), et LEDBAT <<http://tools.ietf.org/wg/ledbat/>>, sur des mécanismes permettant à des applications non critiques de céder automatiquement les ressources réseau aux autres (RFC 6297 et RFC 6817).

On l'a vu, il existe déjà des applications pair-à-pair qui ont des formes de cachage des données. Mais chacune nécessite d'être adaptée à un protocole pair-à-pair particulier, alors que le travail de DECADE est plutôt de chercher des solutions génériques, qui pourraient convenir à tout nouveau protocole. Une telle solution générique n'existe pas actuellement. Mais des projets ont déjà été définis comme les "Data Lockers" <<http://cs-www.cs.yale.edu/homes/yry/projects/p4p/open-data-lockers-nov-2010-co.pdf>>. Avec un tel système, le PC de M. Toutlemonde pourrait téléverser le fichier dans le nuage, là où la capacité réseau est meilleure, et les pairs de M. Toutlemonde aller le chercher là-bas, sans que M. Toutlemonde ait d'action explicite à faire, et sans qu'il gaspille les ressources du dernier kilomètre.

L'exercice de DECADE sera donc de définir un protocole d'accès standard à ces ressources de stockage dans le nuage. Ce protocole comportera deux parts : la **signalisation** (permettant de découvrir les caractéristiques de ces ressources) et le **transfert** permettant de lire et d'écrire le contenu. La difficulté sera d'identifier ce qui est suffisamment commun chez tous les protocoles, pour faire l'objet d'une normalisation. Et le protocole devra être assez souple pour s'adapter à des applications pair-à-pair qui ont des caractéristiques très différentes.

Une étude a déjà été faite par le groupe de travail DECADE sur les systèmes de stockage des données en ligne. Documentée dans le RFC 6392, elle liste les systèmes existants sur lesquels aurait pu être basé le futur protocole DECADE.

Si cela vous semble encore un peu flou, vous pouvez sauter à la section 4 qui présente des études de cas pour certaines applications. Par exemple, pour BitTorrent, ce qui est envisagé est de modifier les pairs pour qu'ils envoient les blocs de données (l'unité de transfert de base de BitTorrent) non pas à chaque autre pair mais à un cache dans le réseau, en indiquant au pair où le bloc a été mis.

Un autre cas étudié est celui des distributeurs de contenu (par exemple une vidéo) et qui voudraient le mettre le plus proche possible des « globes oculaires » (les consommateurs de contenu). Garder la vidéo sur son petit site Web mal connecté ne permettra pas une distribution efficace. Faire appel à un CDN imposera l'utilisation de l'interface spécifique de ce CDN, et tout sera à recommencer en cas de changement de fournisseur. Le protocole standard mentionné plus haut résoudrait ce problème. Pour ce cas, encore plus que pour celui du pair-à-pair, il est important que celui qui met des données dans le réseau puisse indiquer les règles d'accès (par exemple, ne distribuer qu'à des utilisateurs identifiés).

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc5693.txt>

Tout cela, vous vous en doutez, soulève plein de problèmes de sécurité. La section 5 les passe en revue. D'abord, il y a un risque évident de déni de service, par exemple avec un méchant stockant tellement de données qu'il remplit tout le nuage et ne laisse rien pour les autres. Il est donc crucial d'avoir des mécanismes d'authentification et d'autorisation.

Ensuite, lorsqu'on dit « distribution de contenu multimédia », « partage en pair-à-pair », on peut être sûr que des hordes de juristes vont accourir et réclamer que les règles définies par l'industrie du divertissement soient automatiquement mises en œuvre par les systèmes techniques, ici par le stockage dans le nuage. (Par exemple, distribution du contenu à certains pays seulement, pour permettre de faire payer plus un sous-ensemble des pays.) Le RFC dit sagement que ce genre de demandes est hors-sujet pour le projet DECADE.

Le fournisseur du système de stockage va en apprendre beaucoup sur les utilisateurs, ce qui peut menacer leur vie privée. Même si le contenu est chiffré, le fait que N personnes demandent le même fichier est déjà une indication utile (qu'elles ont les mêmes centres d'intérêt). Un autre risque avec un fournisseur de stockage méchant est qu'il modifie le contenu des fichiers qu'on lui a confié. Le RFC ne fournit pas de solutions pour ces deux derniers problèmes (une signature cryptographique permettrait de traiter le second).

Bref, ce n'est pas le travail qui manquait pour le groupe DECADE. Il travaillait sur les trois futurs RFC de cahier des charges pour le protocole d'accès au stockage, de description de l'architecture du système, et de l'intégration avec les protocoles existants, comme BitTorrent. Mais les difficultés colossales de ce travail ont eu raison du groupe, qui a été dissous en septembre 2012. (Après coup, le travail déjà fait a été publié dans le RFC 7069.)