RFC 7336 : Framework for Content Distribution Network Interconnection (CDNI)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 22 août 2014

Date de publication du RFC : Août 2014

https://www.bortzmeyer.org/7336.html

Ce RFC est le nouveau cadre technique pour les solutions standard d'interconnexion de CDN. Après le document de description du problème (RFC 6707 [1]), une liste de scénarios d'usage (RFC 6770) et un cahier des charges formel (RFC 7337), voici une nouvelle étape du travail du groupe CDNI de l'IETF. Il remplace un ancien travail équivalent, qui n'avait pas débouché, dans le RFC 3466.

Personnellement, je trouve qu'il ne va pas très loin par rapport aux RFC 6707 et RFC 7337. Mais, bon, c'est la description officielle de l'architecture des futurs protocoles d'interconnexion de CDN donc, allons-y.

N'attendez pas de ce RFC des protocoles précis : les spécifications viendront plus tard, ce qui est décrit ici est une architecture de haut niveau, très proche de ce qui avait été écrit dans le RFC 6707. (Par contre, terminologie et architecture du vieil RFC 3466 sont abandonnés.) Le principal ajout est que l'interface de routage des requêtes ("*Request routing interface*") est désormais découpée en deux, une interface de redirection ("*Request routing indirection Interface*") et une interface d'échange d'informations ("*Footprint & Capabilities Interface*"). Autrement, je vous renvoie à mon article sur le RFC 6707. Outre la terminologie des RFC 6707 et RFC 7337, quelques concepts nouveaux apparaissent :

Rappel « CDN amont » : celui sollicité par le client qui veut du contenu, mais qui n'a pas le contenu (ou bien, pour une raison ou pour une autre, qui ne peut pas / ne veut pas servir la requête) et doit donc utiliser les mécanismes CDNI pour déléguer ; le RFC écrit aussi "*uCDN*" pour "*upstream CDN*",

Rappel « CDN aval » : celui qui a le contenu et va donc servir le client ; le RFC écrit aussi "*dCDN*" pour "*downstream CDN*",,

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc6707.txt

— « Domaine CDN » : le nom de domaine dans l'URL qui identifie le CDN. Par exemple, pour le site Web de l'Élysée, qui utilise le CDN de Level 3, c'est actuellement `cdn.cdn-tech.com.c.footprint.net`.
— « Redirection Itérative » : lorsque le CDN amont renvoie simplement au CDN aval, sans essayer de traiter la requête lui-même,
— « Redirection Récursive » : lorsque le CDN amont fait le travail de redirection lui-même, sans que le client qui accédait au contenu en soit même conscient.

La section 3 du RFC est un survol général du fonctionnement de CDN interconnectés. L'opérateur A gère le CDN amont, celui qui a un lien avec le fournisseur de contenu, qui a choisi A pour servir ses ressources. L'opérateur A a un accord avec l'opérateur B, qui gère un possible CDN aval, qui pourra servir des clients intéressés, par exemple sur une base de proximité géographique (mettons que A est en Europe et B aux États-Unis). Avant que le client n'arrive, A et B auront donc échangé des messages (via les interfaces MI et FCI, cf. RFC 7337) pour que B sache quoi servir (interface MI, envoi de métadonnées) et pour que A sache les capacités de B (interface FCI). Lorsque le client final envoie sa requête, elle est d'abord dirigée (par les techniques habituelles des CDN existants) vers A. Via l'interface RI, le client est redirigé vers B (voir plus loin les techniques de redirection). Le client envoie alors ses requêtes à B. Celui-ci doit contacter A pour obtenir le contenu lui-même (cette opération n'utilise pas les protocoles CDNI) et il sert ce contenu au client. Ensuite, il contactera A pour remplir les statistiques de ce dernier (interface LI).

La section 3 détaille ensuite les mécanismes de redirection récursifs et itératifs. La section 2 du RFC avait déjà résumé ces techniques de base utilisées par les CDN pour la redirection des requêtes. Dans le cas le plus simple, un client (par exemple un navigateur Web) va interroger un CDN qui, soit lui répondra, soit le renverra vers le CDN aval. Pour cette redirection, on peut utiliser le DNS ou bien des mécanismes de redirection du protocole applicatif (par exemple, en RTSP, un code de retour 302). D'abord, le DNS. Le principe est d'envoyer des réponses différentes selon le client. Ce dernier est situé en Europe et interroge un CDN amont qui ne sert de contenu qu'en Amérique ? Pas de problème, aux requêtes sur le domaine CDN, on renvoie l'adresse IP d'un CDN aval qui est présent en Europe. Il y a quelques précautions à prendre (se souvenir que les réponses DNS seront gardées en cache et qu'il faut donc choisir intelligemment le TTL, sans compter le fait que certains résolveurs trichent en gardant en cache plus longtemps, prêter attention à DNSSEC si on génère les redirections au vol, cf. section 3.4.1) mais cette méthode est simple et est déjà utilisée par les CDN actuels, non connectés entre eux. L'avantage de la technique DNS est qu'elle est complètement invisible à l'application, qui ne se rend même pas compte qu'elle a été servie par un autre CDN que celui demandé. L'un de ces inconvénients est que le serveur DNS qui fait autorité ne connait pas le client mais son résolveur DNS. Si le client utilise un résolveur DNS public (comme OpenDNS), le client du contenu et le résolveur peuvent être sur des continents différents et la redirection ne se fera pas vers le CDN optimal. Autre inconvénient, on ne pourra tenir compte, dans l'URL original, que du nom de domaine, le reste de l'URL n'étant pas connu du serveur DNS.

À noter qu'il existe une variante, où on ne renvoie pas directement l'adresse IP mais un nom (technique CNAME ou, mieux, DNAME). C'est le cas de l'Élysée citée plus haut :

```
% dig A www.elysee.fr
...
;; ANSWER SECTION:
www.elysee.fr. 3600 IN CNAME cdn.cdn-tech.com.c.footprint.net.
```

Autre possibilité de redirection, la redirection HTTP : cette fois, on se sert des codes de retour 301 ou 302 qui indiquent au client HTTP qu'il doit aller chercher ailleurs ce qu'il voulait. La nouvelle URL est donnée dans la réponse (en-tête `Location:`). Cette fois, le serveur peut changer tout l'URL, pas juste le nom de domaine, on connait l'adresse IP du client original (le RFC oublie de mentionner qu'il peut être un relais), ce qui peut permettre de mieux choisir le serveur, et enfin on a plein d'autres informations qui peuvent être utiles pour une redirection intelligente, comme la marque du logiciel client utilisé.

Il y a par contre des inconvénients, le changement de domaine fait que les "*cookies*" ne suivront pas, et les caches ne gardent pas en mémoire les redirections (le RFC 7234 le permet mais ce n'est pas fréquemment mis en œuvre).

La section 4 du RFC donne quelques détails sur les différentes interfaces du système, interfaces qui avaient été présentées dans les RFC 6707 et RFC 7337. Dans certains cas, l'interconnexion des CDN se fait à l'intérieur du protocole de communication déjà utilisé ("*in-band*"). C'est le cas des redirections HTTP. Dans d'autres cas, on utilise un protocole externe ("*out-of-band*"). Il faut également noter, pour comprendre la complexe combinaison d'interfaces de CDNI que, bien que les interfaces soient largement indépendantes, elles reposent sur des conventions communes, par exemple pour le nommage des ressources.

Parmi les détails creusés dans ce RFC 7336 sur les interfaces :

— Une liste des éléments d'information qui peuvent être intéressants pour l'interface de journalisation, LI ("*Logging Interface*"). Conceptuellement, cette interface peut être vue simplement comme une copie des fichiers `apache/access.log` du CDN aval vers l'amont... Attention, le champ indiquant le nom de domaine demandé (`VirtualHost` dans Apache) peut être différent de l'original, s'il y a eu redirection HTTP.
— Certains services de l'interface de communication de métadonnées (MI pour "*Metadata Interface*") peuvent être assurés par le mécanisme de redirection. Par exemple, si le fournisseur de contenu veut limiter l'accès aux utilisateurs européens, il suffit que le CDN amont ne redirige pas vers le CDN américain, pour les requêtes de ce contenu à accès limité. (Le RFC note toutefois que cela manque de souplesse : par exemple, il y a peu de chances que le CDN aval ait une couverture géographique qui coïncide parfaitement avec les exigences de géo-limitation du fournisseur de contenu.)

La section 5 du RFC décrit plusieurs scénarios d'usage de CDNI quand il sera terminé. Par exemple, bien que le modèle de référence (et les exemples que j'ai cités) soient unidirectionnels (le CDN A délègue au CDN B et jamais le contraire), on pourra se servir de CDNI pour les CDN maillés, avec des graphes arbitraires entre les différents CDN.

Déléguer ses fonctions soulève évidemment tout un tas de questions, comme toute sous-traitance. Le CDN amont peut-il faire confiance au CDN aval pour servir le contenu correctement ? Les statistiques de trafic qu'il remonte sont-elles correctes ou bien modifiées dans l'intérêt exclusif du CDN aval ? La section 6 explore le problème de la confiance dans un monde de CDN connectés. Notons que le fournisseur de contenu a déjà aujourd'hui le même problème avec son opérateur CDN : dès qu'on sous-traite, la question de la confiance surgit. Mais CDNI rend les choses un peu plus compliquées : un fournisseur de contenu qui a signé avec l'opérateur de CDN amont peut ne pas être conscient que celui-ci a un accord avec l'opérateur CDN aval. Et si un opérateur CDN modifiait les fichiers avant de les envoyer ? Il existe évidemment des solutions techniques, comme la signature cryptographique des fichiers. Mais, fondamentalement, il faut une combinaison de confiance et de quelques vérifications (par exemple des sondages aléatoires faits par divers clients pour vérifier que le contenu est bien là, et bien conforme à ce qui est demandé).

En parlant de confiance et de sécurité, la section 7 se demande quelles sont les conséquences de l'interconnexion de CDN pour la vie privée (l'existence d'une section nommée "*Privacy considerations*" est récente dans les RFC et vient du RFC 6973). Un CDN est bien placé pour observer beaucoup de choses dans le comportement de l'utilisateur, par exemple à quels fichiers il accède, de `mécanique_quantique_pour_les_nuls.epub` à `how_to_make_bombs.avi`. L'utilisateur qui accède à un site Web ne sait typiquement pas si celui-ci utilise un CDN (cela se trouve relativement facilement mais tout le monde n'a pas les compétences ou le temps nécessaire). Il fait confiance au site Web, mais ne se rend pas compte qu'il fait également confiance à l'opérateur CDN (qui peut avoir une autre éthique, ou être soumis à d'autres lois : lorsqu'on visite `<http://www.elysee.fr/>`, on croit faire confiance à un organisme public français, alors qu'il est en fait servi par un CDN états-unien, soumis au "*Patriot Act*").

Certaines fonctions de CDNI sont justement conçues pour faire circuler de l'information sur l'activité des utilisateurs, notamment l'interface de journalisation (LI). Il faudra donc s'assurer qu'elles disposent de protections appropriées.

Et, toujours sur la sécurité, la section 8 note également d'autres points délicats, qui s'ajoute aux questions de sécurité déjà existantes pour les CDN actuels :

— Certaines exigences des fournisseurs de contenu (distribution limitée géorgraphiquement, ou bien limitée dans le temps) sont plus difficiles à satisfaire lorsqu'il y a interconnexion des CDN,
— Par contre, les menottes numériques ne sont pas affectées par CDNI puisqu'elles reposent typiquement sur des mécanismes présents dans le contenu lui-même,
— Les interfaces entre CDN doivent être protégées, contre l'écoute (cas des journaux d'activité dans la section précédente) mais aussi contre les modifications non autorisées (imaginez qu'un méchant modifie les contenus servis lorsqu'ils passent d'un CDN amont au CDN aval), même si l'interconnexion se fait en utilisant l'Internet public, non sécurisé.

Deux fournisseurs de solutions techniques, Cisco et Alcatel-Lucent, ont annoncé qu'ils travaillaient sur des prototypes d'interconnexion de CDN, utilisant le futur protocole qui sera la concrétisation de ce cadre.