RFC 7443 : Application Layer Protocol Negotiation (ALPN) Labels for Session Traversal Utilities for NAT (STUN) Usages

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 29 janvier 2015

Date de publication du RFC : Janvier 2015

https://www.bortzmeyer.org/7443.html

ALPN, normalisé dans le RFC 7301 [1], est une option du protocole de sécurité TLS pour permettre à un client TLS d'indiquer au serveur TLS quelle application il veut utiliser (car il n'y a pas que HTTPS qui utilise TLS...) Cela permet, notamment, d'utiliser un seul port (le seul qui passera depuis tous les réseaux, 443) pour plusieurs applications. Ce nouveau RFC 7443 utilise ALPN pour permettre à un client STUN de signaler au serveur TLS qu'il veut faire du STUN, et lui permet également de spécifier quel usage de STUN (par exemple le relayage des sessions TCP nommé TURN).

STUN sert normalement aux clients tristement coincés derrière un stupide boitier, genre routeur NAT, pour communiquer avec d'autres malheureux dans le même cas (et qui ne peuvent donc pas être appelés directement). Il est surtout utilisé pour le pair-à-pair et pour la communication multimédia (téléphonie sur IP par exemple). STUN peut fonctionner sur TLS, pour plus de sécurité (RFC 8489, section 6.2.2, et RFC 7350 si on utilise UDP). Notre nouveau RFC permet à STUN-sur-TLS d'utiliser l'extension TLS ALPN en indiquant comme application un de ces deux choix :

- `stun.turn` : utilisation de STUN et de TURN (RFC 8656),
- `stun.nat-discovery` : utilisation de STUN pour découvrir les caractéristiques d'un routage NAT.
- Après une sérieuse discussion à l'IETF, il a été décidé qu'il n'y aurait **pas** d'application « STUN générique » (par exemple pour des usages futurs encore inconnus).

Ces deux noms sont désormais enregistrés dans la liste des protocoles applicatifs ALPN <https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml#alpn-protocol-ids>.

À l'heure actuelle, il ne semble pas qu'il y ait encore de mise en œuvre de ce système mais les clients WebRTC devraient logiquement être dans les premiers à s'y mettre.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7301.txt