

RFC 4925 : Softwire Problem Statement

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 11 juin 2008

Date de publication du RFC : Juillet 2007

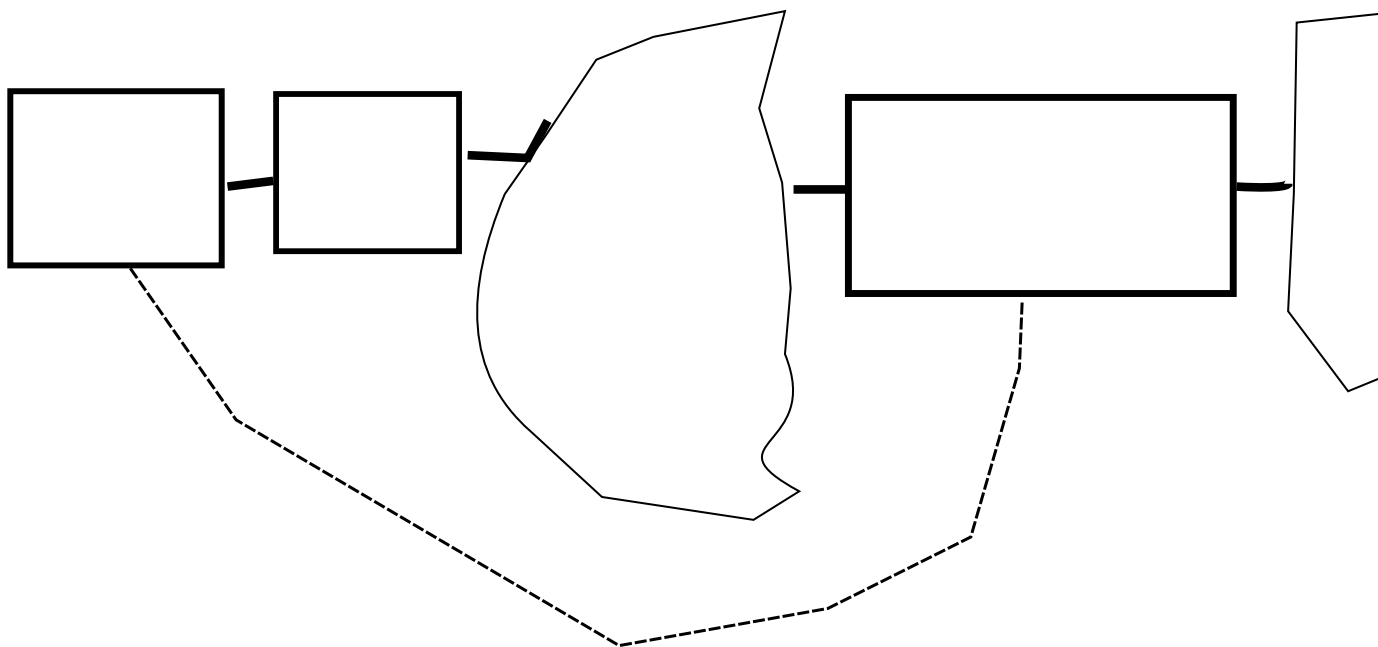
<https://www.bortzmeyer.org/4925.html>

Les réseaux informatiques typiques d'il y a vingt ans étaient multi-protocoles et ces protocoles co-existaient plus ou moins harmonieusement. Pour connecter deux réseaux via un troisième, parlant un protocole différent, on utilisait souvent des tunnels. C'est ainsi que, par exemple, IP a servi à connecter beaucoup de réseaux AppleTalk. Puis IP a tout remplacé et les réseaux sont devenus mono-protocole. Maintenant, avec l'épuisement des adresses IPv4 qui se rapproche, avec le déploiement d'îlots IPv6 qu'il faut relier entre eux, les tunnels reviennent, et avec eux beaucoup de complexité. Un groupe de travail de l'IETF, "*softwire*" <<http://tools.ietf.org/wg/softwire>> (« câbles virtuels ») travaille donc à une meilleure spécification de ces tunnels. Ce RFC est la première étape publiée de leur travail.

Les idées derrière le système des « câbles virtuels » ("*soft wires*") sont très anciennes. Par exemple, le système de « courtier en tunnels » ("*tunnel broker*") du RFC 3053¹, en janvier 2001, était déjà un câble virtuel, même si le mot n'existait pas encore. Mais pourquoi avoir remplacé les tunnels par des « câbles virtuels » ? La raison principale est cosmétique : les tunnels souffrent d'une mauvaise réputation, lents, compliqués, peu fiables, posant des problèmes de MTU. Comme les balayeurs sont devenus techniciens de surface, comme le surveillant général est devenu conseiller d'éducation, les tunnels sont devenus des "*soft wires*" (la section 1.1 détaille le vocabulaire et définit le câble virtuel comme un tunnel, créé sous le contrôle d'un protocole, ce qui exclut donc les tunnels manuels).

Ce premier RFC ne fait que définir le problème. D'autres documents, en cours d'élaboration à l'IETF, s'occuperont des protocoles effectifs. La section 1 introduit le problème, spécifier des câbles virtuels qui pourront être établis rapidement, mais durer longtemps, afin de connecter des réseaux IP entre eux (typiquement, des réseaux IPv6 via un réseau IPv4). Cette section introduit également la grande distinction entre les topologies « Centraliser et redistribuer » ("*Hubs and Spokes*") et « Maillage » ("*Mesh*"). Dans le premier cas, le réseau est organisé autour de points proéminents (les "*hubs*") qui concentrent le trafic et le redistribuent. Dans le second, tout le monde est au même niveau.

La section 2 est consacrée au « Centraliser et redistribuer ». Les tunnels du RFC 4213 sont un exemple typique de cette approche. Voici, extrait de cette section, un cas où une machine double pile



(v4 et v6) se trouve sur un réseau local où le CPE est purement v4 (la section 2.2 décrit plus finement ce cas), et qui est connecté à un FAI purement v4. Elle va donc établir un câble virtuel avec un concentrateur de câbles virtuel (le « *hub* ») qui va ensuite la connecter aux réseaux v6. Seul IPv6 circulera sur ce câble virtuel. Comme précisé dans la section 2.4, le protocole du câble virtuel doit permettre la délégation d'un préfixe IPv6 fixe, même si l'adresse IPv4 du CPE change. On peut utiliser pour cela le RFC 3633. Cette exigence fait que 6to4 ne permet pas de créer de véritables câbles virtuels, puisque l'adresse IPv6 change en même temps que la v4.

Dans le mode « Centraliser et redistribuer », c'est toujours la machine double pile qui crée le câble virtuel, en se connectant au concentrateur. Elle est nommée l'initiateur (section 2.5). Le concentrateur est typiquement un routeur double pile (section 2.6). Le RFC impose que le protocole permette « des millions » d'initiateurs. Le protocole de découverte du concentrateur n'est pas spécifié. Enfin, la section 2.11 détaille les exigences de sécurité, comme la possibilité d'authentifier les initiateurs.

La section 3, elle, parle de l'architecture maillée. Dans cette architecture, un réseau uniquement IPv4 connecte des clients IPv6 entre eux en fournissant des AFBR (*Address Family Border Routers*) qui parlent les deux protocoles et peuvent créer des câbles virtuels entre eux. Cela ressemble donc beaucoup aux VPN, par exemple dans le RFC 4364, mais sans l'exigence de gérer plusieurs espaces d'adressage distincts.

Les câbles virtuels, en pratique, vont nécessiter d'encapsuler les paquets d'un protocole (en général IPv6) dans un autre (en général IPv4). Les sections 2.13 et 3.5 discutent de l'encapsulation en notant que toutes les techniques existantes doivent pouvoir être utilisées. Cela implique GRE (RFC 2784), MPLS (RFC 3031) ou L2TP (RFC 3931).

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc3053.txt>