RFC 7575 : Autonomic Networking - Definitions and Design Goals

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 juin 2015

Date de publication du RFC : Juin 2015

https://www.bortzmeyer.org/7575.html

Ce nouveau RFC, issu de l'IRTF et donc assez futuriste, se penche sur les « réseaux autonomes » ("*autonomic networking*"), c'est-à-dire sur les réseaux qui se débrouillent tout seuls, sans administrateur réseaux, sans DSI, sans ICANN, etc. Un réseau autonome doit se configurer, s'optimiser, guérir des pannes et se protéger des attaques sans intervention humaine. Ce RFC n'explique pas comment les réaliser (c'est le début d'un programme de recherche) mais définit la terminologie et les buts à atteindre. Il a été publié en même temps que le RFC 7576 [1], qui analysait les techniques existantes et leurs limites. (Le groupe de travail IETF ANIMA <https://tools.ietf.org/wg/anima> travaille sur les aspects plus concrets de ce sujet.)

La première description de tels réseaux autonomes date de 2001 (l'article de Kephart et Chess <http://users.soe.ucsc.edu/~griss/agent-papers/ieee-autonomic.pdf>). L'idée est que toutes les boucles de régulation du système doivent être fermées, sans interaction avec l'extérieur (d'où l'adjectif « autonome »). IP lui-même a éte partiellement conçu pour fonctionner ainsi (la fameuse demi-légende de l'Internet prévu pour résister à une attaque nucléaire). Un protocole comme OSPF est autonome dans la mesure où il s'adapte tout seul aux changements de topologie. Toutefois, IP n'a jamais été complètement autonome et les évolutions qu'il a subi allaient plutôt dans le sens de mettre plus d'intelligence dans la configuration externe que dans le réseau lui-même. Est-ce grave ? Pour un grand réseau d'un Tier 1, on peut penser que son propriétaire préfère que le réseau n'ait pas trop d'autonomie (Skynet ?) et suive plutôt la politique configurée. Mais les réseaux autonomes sont tentants pour l'Internet des objets, quand on a un grand nombre de petites machines très simples, ensemble qui serait très difficile ou impossible à configurer avec les outils existants. Notre RFC estime que les deux approches (configuration extérieure centralisée, et fonctionnement réparti autonome) ont leurs avantages et inconvénients,

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc7576.txt

et que pas mal de réseaux utiliseront une de ces deux approches pour certaines fonctions et la seconde pour les autres fonctions. Ne cherchez donc pas de réseau complètement autonome tout de suite.

De toute façon, l'approche autonome ne peut pas tout faire. Elle nécessite de découvrir tout seul un certain nombre de choses et la politique de gestion du réseau (qui peut s'en servir, pour quoi...) est un bon exemple de quelque chose qui ne peut pas être découvert, qui doit être configuré explicitement.

Les réseaux autonomes ont fait l'objet d'un très grand nombre d'études scientifiques et de publications (la section 7 du RFC contient des lectures, pour les gourmands, notamment trois synthèses de l'existant). Attention, on dit « autonome » et pas « automatique ». Il faut se gérer seul, pas juste dérouler automatiquement un script pré-établi par un humain (voir la section 2 sur les définitions). Par exemple, un système automatique doit être reprogrammé lorsque l'environnement change alors qu'on attend d'un réseau autonome qu'il s'adapte seul.

Donc, que veut-on d'un réseau autonome ? La section 3 décrit les buts. Le réseau doit être auto-géré ce qui se décline en :

— Se configure tout seul. Les machines démarrent, se découvrent, trouvent les liens qui les relient et se mettent à les utiliser. Pas d'admin' pour avoir tapé des `default_router=fe80::1`.
— Se guérit tout seul. Une pelleteuse arrache un câble ? Le réseau contourne le problème automatiquement (ceci marche dans l'Internet actuel : rappelez-vous qu'on a déjà certaines fonctions qui peuvent marcher de manière autonome).
— S'optimise tout seul en trouvant la meilleure façon d'accomplir les tâches définies.
— Se protège tout seul car le monde est hostile et cruel et des hackers chinois islamistes à cagoule vont attaquer le réseau.

Évidemment, en trichant, on peut définir tout réseau comme « autonome » si on élargit la définition pour inclure, par exemple, un contrôleur central (comme avec le SDN). Le RFC est donc plus spécifique : « tout seul » veut dire « en n'utilisant que des fonctions qui sont sur les machines terminales ». Comme dit l'Internationale, le réseau autonome n'a « ni Dieu, ni César, ni tribun[, ni contrôleur SDN] ».

Comme on ne peut pas envisager un Internet complètement autonome, ces réseaux autonomes vont devoir coexister avec les méthodes de gestion traditionnelles (comme Netconf). Cela peut nécessiter un mécanisme d'arbitrage si les deux méthodes sont en désaccord. Le RFC utilise un exemple tiré de l'aviation : un avion où le pilote automatique se coupe automatiquement si le vol sort d'une certaine plage de paramètres (par exemple si l'angle d'incidence est trop élevé). Toutefois, on peut aussi se dire qu'une crise n'est pas le meilleur moment pour passer brutalement le contrôle au pilote stressé et le RFC demande donc que les mécanismes autonomes ne se coupent pas tout seuls, même dans des situations non prévues.

Autre but de nos réseaux autonomes : qu'ils soient sûrs. On doit pouvoir, par exemple, empêcher un intrus de rejoindre le réseau, ce qui implique un certain mécanisme d'authentification, qui ne sera pas forcément totalement autonome (par exemple un certificat émis par une AC, une base d'utilisateurs centralisée, etc). Bref, il faudra sans doute de la cryptographie.

« Autonome » ne veut pas dire « isolé et sourd-muet » (sinon, ce ne serait pas un réseau). La machine doit communiquer avec des pairs mais aussi avec des autorités, comme cela qui lui communique le travail à faire, à qui la machine terminale transmet des rapports, des statistiques, etc. C'est ce qu'on nomme l'interface Nord (car placée en haut sur les schémas et tant pis pour l'Australie `<http://www.flourish.org/upsidedownmap/>`).

On a vu que le réseau n'est pas créé pour satisfaire les machines mais pour accomplir un certain travail. Il faudra donc un mécanisme pour informer les machines de ce travail, et des changements dans

les définitions de ce travail. Ce mécanisme doit être de haut niveau, sinon, ce ne sera plus un réseau autonome, on retournerait à la configuration centralisée traditionnelle. Par exemple, le RFC demande que ce mécanisme n'expose pas la version d'IP utilisée (IPv4 ou IPv6) : cela doit rester un détail technique interne au réseau.

J'ai parlé plus haut de transmettre des rapports à l'autorité centrale. Il est évidemment nécessaire de prévenir les humains qui ont acheté et déployé ces machines de l'efficacité de celles-ci : le travail a-t-il été fait ? Mais, pour respecter le principe d'un réseau autonome, les rapports ne doivent pas porter sur des détails d'implémentation que le réseau doit résoudre lui-même (comme « le lien entre la machine X et la machine Y ne marche plus »). Il faut au contraire un mécanisme de communication abstraite, synthétisant l'information, pour ne pas écrouler l'autorité centrale sous les détails. Imaginons que l'autorité ait envoyé le but de haut niveau « économise l'énergie », le rapport devrait être du genre « 30 % de réduction de la consommation, obtenu en éteignant 40 % des ports réseau ». Pour résumer : les rapports devraient décrire le réseau globalement, pas machine par machine ou lien par lien.

Le RFC 7576 montre qu'il existe déjà un certain nombre de protocoles et de fonctions autonomes dans la famille IP. Mais le but du projet « réseaux autonomes » n'est pas uniquement d'empiler des solutions mais de les intégrer dans un cadre commun, qui reste à développer.

Enfin, « autonome » est un adjectif qu'on peut appliquer à toutes les couches. Par exemple, les commutateurs typiques aujourd'hui sont autonomes au niveau 2 (on les branche n'importe comment et ils font une topologie qui marche). Les routeurs peuvent en faire autant au niveau 3, comme vu avec l'exemple OSPF.

Un bon cahier des charges doit aussi avoir des non-buts : ce qu'on ne cherche pas à atteindre. C'est le rôle de la section 4 du RFC. Les non-buts sont :

— Supprimer complètement tout opérateur humain (Skynet, encore). Les humains vont rester, mais en se concentrant sur des fonctions de haut niveau, comme la définition et la vérification des politiques.
— Résoudre tous les problèmes. De temps en temps, il se produira un évènement dont le réseau ne saura pas se dépêtrer seul. Là encore, des humains devront intervenir. Ce sera au moins le cas pour les pannes matérielles, tant que les ordinateurs n'auront pas de périphériques leur permettant d'aller à la casse eux-même...
— Supprimer tout contrôle central. Comme le note le RFC, la Direction Générale ne serait sans doute pas d'accord.

Enfin, notre RFC se termine par une description, en section 5, d'un modèle de référence des réseaux autonomes, reprenant les points vus précédemment.