RFC 5810 : ForCES Protocol Specification

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 19 mars 2010

Date de publication du RFC : Mars 2010

https://www.bortzmeyer.org/5810.html

Ce RFC conclut, après un très long travail, les efforts du groupe de travail Forces <http://tools.ietf.org/wg/forces> de l'IETF. Ce groupe était chargé de produire un protocole permettant la communication entre les différents éléments d'un routeur, afin de permettre d'acheter ces éléments chez des vendeurs différents. Un tel protocole pourrait permettre d'ouvrir le monde actuellement très fermé des routeurs de haut de gamme, mais il n'est pas sûr du tout qu'il soit un jour effectivement mis en œuvre.

Le travail de Forces avait commencé il y a de nombreuses années et le premier RFC, le RFC 3654 [1] avait été publié en 2003. Maintenant, grâce à ce RFC 5810 (et quelques compagnons comme le RFC 5811 sur le protocole de transport), le travail est quasiment terminé et la partie Normalisation de Forces avec lui. Il reste à l'implémenter et à faire en sorte qu'il soit disponible dans les routeurs...

Conformément au cahier des charges du RFC 3654, et au cadre général de Forces exposé par le RFC 3746, ce nouveau protocole permet la communication entre deux catégories d'élements qui composent un routeur, les CE ("*Control Element*") et les FE ("*Forwarding Element*"). (La section 3 rappelle le vocabulaire de Forces.) Les premiers, les CE, font tourner des algorithmes compliqués comme OSPF ou BGP, ils prennent des décisions « de haut niveau » et les seconds, les FE, font le travail « bête » mais ultra-rapide, de commutation de chaque paquet. Aujourd'hui, dans un routeur (Forces dit NE, pour "*Network Element*", et pas routeur) haut de gamme, le CE est typiquement un processeur standard, avec un système d'exploitation (parfois un Unix),le FE est un ASIC aux capacités bien plus limitées mais aux performances fantastiques. Comme le protocole de communication entre le CE et le FE est privé, pas question de faire tourner du logiciel libre sur le CE, pas question d'acheter le processeur à un vendeur et les ASIC à un autre. C'est ce problème que Forces veut résoudre.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc3654.txt

Dans Forces, la relation entre les CE et les FE est simple : le CE est le maître et le FE l'esclave. Les informations nécessaires au FE sont regroupées dans des LFB ("*Logical Function Block*") dont la description est faite en XML (cf. RFC 5812 et un exemple dans le RFC 6956). Le protocole lui-même n'utilise pas XML. Le protocole ne spécifie que la communication entre FE et CE, pas celles qui pourraient exister entre FE ou bien entre CE, ni celle qui relie les CE à leur gérant (l'interface d'administration du routeur). (La section 4 rappelle le cadre général de Forces, exposé dans le RFC 3746.) Le protocole Forces est également responsable de l'établissement et de la terminaison des associations entre un routeur (NE) et des CE ou FE (section 4.4). Une fois l'association faite, le CE envoie des ordres au FE, ordres exprimés avec le protocole Forces, et encapsulés dans un protocole de transport, le TLM ("*Transport Layer Mapping*") qui fait l'objet d'un RFC séparé (RFC 5811).

La section 4.3.1 du RFC détaille la question de l'atomicité des requêtes Forces. Le protocole permet des requêtes atomiques (toutes sont exécutées, ou bien aucune ne l'est, section 4.3.1.1.1) mais aussi des requêtes exécutées séquentiellement jusqu'au premier échec (section 4.3.1.1.3) ou encore des requêtes exécutées même si la précédente était un échec (section 4.3.1.1.2). Mieux, Forces permet des transactions ACID (section 4.3.1.2).

L'encodage des paquets sur le câble fait l'objet de la section 6. Tous les paquets ont un en-tête commun, suivi d'un ou plusieurs TLV. Parmi les champs de l'en-tête commun, un numéro de version sur 4 bits (actuellement 1), le type du message, sur 8 bits (les différents types sont décrits en section 7 et le tableau complet est dans l'annexe A.1) et les adresses (nommées ID) de l'expéditeur et du destinataire. Ces ID, ces adresses, sont codés sur 32 bits et doivent être uniques à l'intérieur du routeur (mais pas forcément pour tout l'Internet). Rappelez-vous qu'un des buts de Forces est de pouvoir gérer des équipements très complexes, où CE et FE ne sont pas forcément dans la même boîte. À noter que les adresses des CE et des FE sont séparées (les premières commencent toujours par 00 et les secondes par 01).

Une fois passé l'en-tête commun, viennent les TLV, décrits dans la section 6.2. Le choix de TLV permet de simplifier l'analyse des messages, certains FE n'apprécieraient en effet pas forcément de devoir analyser du XML. À noter que le champ Valeur d'un TLV peut contenir d'autres TLV.

Le contenu légal d'un message (quels TLV, en fonction de son type) est le sujet de la section 7. Par exemple (section 7.1.6), si le type est `Config` (créer ou bien mettre à jour un attribut du FE) ou `Query` (récupérer la valeur d'un attribut du FE), il ne peut pas y avoir de TLV de réponse dans le message (mais il y a un TLV `PATH-DATA` qui contient l'identificateur de l'attribut qu'on vise). Si le type est `QueryResponse` (réponse à une question posée), en revanche, le TLV de réponse (section 7.1.7) est obligatoire. Comme le protocole Forces est très asymétrique (les CE commandent et les FE obéissent), la plupart des messages ne peuvent être émis que dans une seule direction (par exemple, un `GET` ne peut être que d'un CE vers un FE, le FE, en bon subordonné, ne doit pas poser des questions à son supérieur). Les questions et réponses sont détaillées en section 7.7 et un registre IANA `<https://www.iana.org/assignments/forces-parameters/forces-parameters.xhtml>` stocke les valeurs possibles. L'annexe C donne plusieurs exemples d'encodage.

La traditionnelle section sur la sécurité est la 9. Les menaces contre Forces ont été décrites dans le RFC 3746. Forces peut être configuré avec zéro sécurité (section 9.1), notamment si tous les composants, CE et FE, sont dans une seule boîte fermée (ce qui est le cas de la plupart des routeurs aujourd'hui). Autrement, la sécurité dépend essentiellement des services du TML (section 5).

Notre RFC 5810 ne normalise que les bits qui seront transportés entre CE et FE, pas la manière dont ils seront encapsulés dans un protocole de transport. La section 5 ne spécifie pas de telles règles mais expose le cahier des charges que devront respecter celles-ci (appelé le TML pour "*Transport Mapping*

Layer"). Au moins une encapsulation est obligatoire pour Forces, celle du RFC 5811 mais d'autres sont possibles.

Parmi les exigences de cette section, la fiabilité de la délivrance des paquets (au moins pour certains d'entre eux), la sécurité (au minimum la possibilité d'authentifier CE et FE, de préférence avec des mécanismes existants comme TLS ou IPsec), le contrôle de congestion (cf. RFC 2914), la possibilité de haute disponibilité (section 8), etc.

Je ne connais pas encore d'implémentation de niveau « production ». Ce n'est pas un travail évident, Forces est riche et complexe, peut-être trop.