

RFC 6041 : ForCES Applicability Statement

Stéphane Bortzmeyer

<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 octobre 2010

Date de publication du RFC : Octobre 2010

<https://www.bortzmeyer.org/6041.html>

Le protocole ForCES ("*Forwarding and Control Element Separation*"), décrit dans le RFC 5810¹, normalise la communication entre les différents éléments d'un routeur, de façon à permettre la création d'un routeur par l'assemblage de composants venus de constructeurs différents. Ce RFC 6041 se focalise sur l'**applicabilité** de ForCES, à savoir dans quels cas ce protocole est applicable et ce qu'on peut exactement lui demander. Ce RFC peut donc servir d'introduction de haut niveau à ForCES.

ForCES considère un routeur comme composé d'un élément de contrôle, qui parle les protocoles de routage comme OSPF, c'est le CE ("*Control Engine*"), et d'un ou plusieurs éléments qui transmettent effectivement les paquets, les FE ("*Forwarding Engine*"). ForCES est le mécanisme par lequel le CE communique avec ses FE. Outre le protocole lui-même, dans le RFC 5810, ForCES a aussi un modèle de données (RFC 5812) et un protocole de transport (RFC 5811). Dans quels cas peut-on les employer et, inversement, quand sont-ils inapplicables? La section 4 forme le cœur du RFC et c'est surtout elle qui est résumée ici.

D'abord, ForCES est prévu pour des routeurs assez gros pour que les fonctions de contrôle et de transmission soient séparées. Sur un engin bas de gamme, où tout tient dans le même circuit, ForCES n'est sans doute pas utile. Par contre, les routeurs du milieu et du haut de gamme ont déjà une séparation physique entre le mécanisme de contrôle et les mécanismes de traitement des interfaces réseaux. Comme ce CE et ces FE doivent communiquer (par exemple, si le CE apprend par OSPF qu'une route pour 192.0.2.192/26 passe par l'interface ge-0-1, il doit communiquer cette information au FE qui gère cette interface, mais aussi à tous les autres pour qu'ils lui transmettent ce trafic). Les routeurs ont donc tous un protocole de communication entre CE et FE mais il est toujours privé (un des rares qui soit documenté est le Netlink de Linux, dans le RFC 3549). Avec ForCES, se profile la possibilité d'un protocole standard pour les remplacer.

1. Pour voir le RFC de numéro NNN, <https://www.ietf.org/rfc/rfcNNN.txt>, par exemple <https://www.ietf.org/rfc/rfc5810.txt>

Quels services, dans cette communication entre FE et CE, peuvent être assurés par ForCES? Notons bien (section 4.1) que ForCES ne traite pas de la découverte par le CE de ses FE, découverte qui doit être assurée autrement. En revanche, une fois celle-ci effectuée, ForCES pilote l'association entre CE et FE, et la transmission des informations comme, par exemple, le nombre de ports réseaux que gère le FE. Le CE peut ensuite configurer le FE (par exemple en lui indiquant les adresses IP locales, qui doivent être transmises au CE), comme indiqué en section 4.1.3.

Mais le principal service assuré par ForCES est évidemment l'envoi d'informations de routage (section 4.1.4). Un CE transmet à ses FE les adresses IP à router, de façon à ce que les paquets soient transmis à la bonne interface réseau.

La section 4.1 note de nombreux autres services. Citons-en juste un : l'envoi par le CE de règles de filtrage (quels paquets abandonner, et sur quels critères), en section 4.1.7.

De quoi a besoin ForCES pour rendre ces services, et qui n'est pas forcément présent sur tous les routeurs? De capacité réseau (section 4.2). Entre le CE et le FE, la capacité n'est pas infinie et des opérations comme l'envoi d'une table de routage complète peuvent être non-triviales sur un réseau d'interconnexion lent, d'autant plus que ForCES se veut utilisable pour des futures tables de routage, plus grandes que celle d'aujourd'hui (fin octobre 2010, il y a 340 000 entrées dans la table de routage BGP globale).

Cette question de la capacité en amène une autre, celle de la localité. ForCES sépare logiquement le CE et le FE. Peuvent-ils aussi être séparés physiquement, et mis dans des boîtes différentes? La section 4.3 examine la question. Le principe est que la disponibilité du routeur ne devrait pas être affectée par la séparation du contrôle et de la transmission. La connexion entre le FE et le CE est donc un bus très fiable, ou en tout cas aussi fiable que le CE, de façon à partager son sort. En pratique, cela veut dire que ForCES est utilisable sans problème pour les NE ("*Network Element*", typiquement un routeur) où tout tient dans une seule boîte, avec des lames différentes pour le CE et les FE, mais un seul châssis et une interconnexion en Ethernet, PCI, etc (le cas de la majorité des routeurs actuels). Une telle configuration simplifiera notamment les problèmes de sécurité (cf. section 5). Mais ForCES peut aussi marcher dans des cas où CE et FE sont situés dans des boîtiers séparés.

Pas de protocole réaliste sans possibilité de **gestion**. La section 6 détaille le comportement de ForCES face aux exigences de la gestion du réseau. Le point important est que, quel que soit le degré de séparation entre CE et FE, ForCES permet de voir le routeur comme un élément unique. Cela se réalise en faisant passer l'essentiel des fonctions de gestion à travers le CE. Notre RFC recommande ainsi que tous les messages SNMP soient transmis au CE (par exemple en utilisant les mécanismes du RFC 2741). Ceux qui vont quand même directement traités par les FE doivent, ou bien être en lecture seule, ou bien permettre une notification du CE, afin que celui-ci reste seul maître. ForCES dispose d'une MIB, décrite dans le RFC 5813, qui permet d'accéder à des informations comme les associations entre le CE et les FE.