RFC 5706 : Guidelines for Considering Operations and Management of New Protocols and Protocol Extensions

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 décembre 2009

Date de publication du RFC : Novembre 2009

https://www.bortzmeyer.org/5706.html

Ce n'est pas tout de normaliser des protocoles. Pour qu'ils ne rendent pas la vie impossible aux administrateurs réseaux, il faut encore qu'ils soient faciles à administrer. Cela peut être plus facile si ces questions opérationnelles ont été prises en compte dès le début. Ce RFC 5706 [1] demande donc que tout nouveau protocole fait à l'IETF reçoive, dès le début, une sérieuse attention pour ses problèmes de gestion. Le faire a posteriori est en effet souvent moins efficace.

Ce RFC est essentiellement composé d'une liste de recommandations (très détaillées) aux auteurs de nouveaux protocoles, expliquant les étapes qu'ils doivent suivre pour que leur protocole soit « gérable ». Cette liste est résumé dans l'annexe A, qu'il suffit normalement de suivre pas-à-pas pour que le protocole soit complet.

La section 1.1 resitue la question : cela fait longtemps que l'IETF demande aux auteurs de protocole de prévoir les mécanismes de gestion pratique dès le début. Un cadre existe pour cela, autour du SMI (modèle décrivant les variables du protocole) du RFC 2578 (et du protocole qui lui est le plus souvent associé, SNMP ; voir le RFC 3410). Mais ce modèle est trop étroit et ne couvre pas l'intégralité de ce qu'il faut savoir pour le déploiement et l'administration d'un protocole. Sans aller jusqu'à formellement imposer une section "*Management Considerations*" dans les RFC (comme il existe une "*Security Considerations*" obligatoire), notre RFC 5706 demande une attention sérieuse portée, dès le début, aux questions de gestion et d'opération des réseaux.

La différence entre « gestion » ("*management*") et « opération » ("*operation*") est décrite en section 1.2. Les opérations, c'est faire fonctionner le réseau, même sans mécanisme de gestion. La gestion, c'est utiliser des mécanismes qui ont été créés dans le but d'améliorer les opérations.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5706.txt

Contrairement à l'idée dominante à l'IETF depuis quinze ans, et depuis les grandes luttes entre SNMP et CMIP, il n'est plus envisagé (section 1.3) d'atteindre le Graal du mécanisme unique. Toutes les solutions sont désormais acceptables, pourvu qu'elles marchent. (Parmi les échecs du SMI, on peut noter celui décrit par le RFC 3197. Aujourd'hui encore, les serveurs DNS sont gérés par des mécanismes non-standard comme la commande `rndc` de BIND.)

Le RFC 5706 va donc donner des lignes directrices et des conseils, plutôt que des obligations. C'est donc un assouplissement par rapport à l'ancienne politique de l'IESG qui exigeait une MIB (description des variables en suivant le SMI) pour tout protocole, au grand désespoir de certains auteurs.

Les sections 1.4 et 1.5 rappellent l'histoire tourmentée des mécanismes de gestion des réseaux TCP/IP. Par exemple, une date importante avait été le RFC 1052 en 1988, qui séparait le langage de modélisation (celui qui sert à écrire la MIB) du protocole d'accès aux données (aujourd'hui SNMP). Une autre avait été le RFC 3139 en 2001, qui listait les obligations d'un mécanisme de gestion. Le RFC 3535 en 2003, faisait le bilan des mécanismes utilisés et critiquait notamment la dépendance vis-à-vis d'un format binaire, celui de SNMP.

La première grande section de notre RFC 5706 est donc la section 2, consacrée aux **opérations** : comment le nouveau protocole va t-il fonctionner ? Il ne suffit pas pour cela que le protocole soit lui-même bien conçu. Il doit aussi s'insérer dans l'environnement humain et technique existant. Ses concepteurs doivent donc réflechir au débogage, à la configuration, à la mise à jour depuis une précédente version...

Comme exemple de mauvaise interaction avec l'existant, le RFC cite l'exemple du "*damping*" de BGP (RFC 2439). Lorsqu'une route annoncée en BGP change trop souvent, les routeurs BGP commencent à ignorer cette route. Mais cette technique n'avait pas pris en compte l'interaction avec d'autres techniques comme la "*path exploration*" et avait donc créé autant de problèmes qu'elle en avait résolu, menant certains administrateurs à couper le "*damping*".

Avant même que le protocole ne fonctionne, il faut le configurer. C'est le but de la section 2.2 qui commence en rappelant un sage principe du RFC 1958 : « tout ce qui peut être configuré peut être mal configuré ». Ce RFC (et son lointain successeur, le RFC 5505) recommandait de préférer les configurations automatiques. Pour les cas où une valeur par défaut a un sens, il faut éviter toute configuration (mais permettre de connaitre les valeurs effectivement configurées).

Parfois, il y avait déjà une version plus ancienne du protocole qui tournait (ou bien un ancien protocole jouant le même rôle). La norme doit alors prévoir un mécanisme de migration, dit la section 2.3. D'autres principes de ce genre forment le reste de la section 2.

La section 3, elle, s'occupe de la gestion de réseaux. Il ne s'agit plus uniquement de faire marcher le réseau, il faut encore le faire marcher bien. Cela passe par l'identification des entités à gérer, puis de la méthode à utiliser. L'ancienne approche qui répondait à toutes ses questions par « il faut écrire une MIB » a montré ses limites. Un ensemble de variables n'est pas un protocole, d'autant plus qu'elle ne concerne en général qu'une des deux extrémités de la communication. Comme le dit le RFC 3535, « une MIB est souvent une liste d'ingrédients sans une recette ». L'introduction de la section 3 donne des pistes pour améliorer les choses.

Un des credos principaux de l'IETF est l'interopérabilité, couverte dans la section 3.1. Appliquée à la gestion du réseau, l'interopérabilité veut dire qu'on devrait pouvoir choisir librement le programme utilisé pour gérer un équipement, et l'utiliser quel que soit l'équipement réseau qu'on gère. Cela implique un protocole standard de gestion.

Beaucoup d'équipements réseau peuvent être gérés via une page Web (elle-même souvent très peu standard, avec abus de fonctions qui ne marchent que sur certains navigateurs, même si le RFC ne mentionne pas ce point), ou parfois via la ligne de commande. Mais cela ne suffit pas. Si on gère des dizaines d'équipements différents, ce qui est courant dans un réseau de taille moyenne, la complexité devient vite unsupportable. Pour que la gestion du réseau soit simplifiée et soit automatisable, une normalisation de ces interfaces est nécessaire.

Historiquement, tout le monde était d'accord sur le papier avec une telle approche. Mais, en pratique, ces interfaces, même celles en ligne de commande, plus faciles à spécifier, n'ont jamais été standardisées. L'IETF n'a pas aidé, en se focalisant sur un seul schéma de données (le SMIv2 du RFC 2578) et un seul protocole (SNMP, du RFC 3410). Ces mécanismes ne convenaient pas à tous et les « autres » interfaces, ignorées de l'IETF, étaient développées mais sans norme unificatrice. Désormais, l'IETF a une vision plus ouverte, et considère d'autres langages de schéma (comme les W3C Schema) ou d'autres protocoles (comme Netconf, dans le RFC 6241, ou syslog, dans le RFC 5424).

La normalisation est plus facile à dire qu'à faire. Normaliser au niveau de la syntaxe est déjà délicat mais, idéalement, il faudrait aussi normaliser la sémantique, pour qu'un même nom décrive bien le même concept partout. Cela impose de développer des modèles, aussi bien des modèles d'information que des modèles de données. (La différence est expliquée dans le RFC 3444 et la section 3.2 couvre les modèles d'information.)

Un protocole ne fonctionne jamais sans pannes. La très riche section 3.3 se penche sur la gestion des pannes. Bien sûr, les mécanismes de gestion du réseau ne vont pas réparer la panne tout seuls. Mais ils peuvent aider à la diagnostiquer. Par exemple, tout protocole devrait avoir un mécanisme de détection de la vie d'un élément du réseau, pour pouvoir répondre à la question simple « Est-il encore en marche ? ». C'est le but de protocoles aussi variés que l'ICMP "*echo*" du RFC 792, du protocole echo de TCP ou UDP (RFC 862, mis en œuvre dans des programmes comme echoping `<http://echoping.sourceforge.net/>` et malheureusement presque abandonné aujourd'hui), les appels `NULL` dans Sun-RPC (section 11.1 du RFC 1831), etc.

Dans un ordre surprenant, la section 3 passe ensuite à la gestion de la configuration (sous-section 3.4). Quels paramètres de configuration, lesquels survivent au redémarrage, que dit le RFC 3139, etc. Cette section, comme le reste du RFC, est trés détaillée, abordant même le problème de l'internationalisation (et, oui, il faut permettre l'UTF-8 dans les fichiers de configuration). D'autre part, le RFC demande également qu'on puisse vérifier la configuration avant de la charger dans l'équipement réseau, pour éviter de laisser celui-ci dans un état invalide, voire de gêner le bon fonctionnement du réseau.

Pour beaucoup d'opérateurs, notamment dans les réseaux traditionnels de téléphonie, il n'y a pas de gestion de réseau sans comptabilisation du trafic. C'est le sujet de la section 3.5, qui renvoie au RFC 2975, et qui dit bien que la comptabilisation n'est nullement obligatoire, qu'elle doit faire l'objet d'un choix réfléchi.

Plus importante est la gestion des performances : tout le monde veut que le réseau aille vite. Pour cela, le point de départ (section 3.6) est de mesurer les performances, pour déterminer, par exemple, si un changement les améliore ou bien les dégrade. Deux groupes de travail de l'IETF se consacrent à ce sujet, BMWG `<http://tools.ietf.org/wg/bmwg>` pour les mesures en laboratoire et IPPM `<http://tools.ietf.org/wg/ippm>` pour celles dans la nature.

La sécurité est un gros sujet en soi, lors de la configuration d'un système, et est traitée dans la section 3.7. Par exemple, un nouveau protocole devrait comporter une analyse des menaces et des solutions possibles. Certains protocoles prévus pour la gestion de réseau ont une utilisation directe en sécurité.

Par exemple, les "*traps*" SNMP et syslog sont couramment utilisés pour alerter les administrateurs sur des phénomènes qui peuvent être une attaque.

Une fois les problèmes des opérations (section 2) et de la gestion (section 3) ainsi décrits, qu'en faire, lorsqu'on définit un nouveau protocole ? Documenter, dit la section 4. Il devrait idéalement y avoir une section "*Manageability Considerations*" dans les RFC, juste avant les "*Security Considerations*", et contenant les informations essentielles pour ceux qui auront à opérer et à gérer le nouveau protocole. Si le ou les concepteur(s) du protocole estiment que cette section n'a pas lieu d'être pour leur création, alors ils devraient l'indiquer explicitement (ce qui garantit que l'absence d'une "*Manageability Considerations*" n'est pas un oubli). Le premier RFC à avoir suivi cette règle (avant même qu'elle soit formalisée) est apparemment le RFC 5440 (dans sa section 8).