RFC 6632 : An Overview of the IETF Network Management Standards

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 juin 2012

Date de publication du RFC : Juin 2012

https://www.bortzmeyer.org/6632.html

Selon une vieille blague de l'informatique, « ce qu'il y a de bien avec les standards, c'est qu'il y en a beaucoup parmi lesquels choisir. » Cette blague a été reprise dans un célèbre dessin de xkcd <http://xkcd.com/927/>. Le but de ce RFC est-il de prendre le relais en montrant la variété des normes IETF relatives à la gestion des réseaux TCP/IP ?

En fait, non. Le but est de s'arrêter deux secondes de développer des nouveaux protocoles et de regarder ce qui existe (il y a donc une imposante bibliographie, reflet des très nombreux RFC cités). À une époque, il y avait un rêve, celui d'un protocole unique pour la gestion des réseaux (cela devait être SNMP). L'évolution des choses fait qu'aujourd'hui, l'architecte réseaux a à sa disposition plusieurs protocoles, dont les rôles se recouvrent en bonne partie. Même chose pour le membre de l'IETF qui développe un nouveau protocole et cherche des mécanismes de gestion de ce protocole. Ce RFC est donc juste un moyen de les aider à y voir plus clair. Il peut ausssi servir aux autres SDO qui veulent se renseigner sur le travail déjà existant, pour éviter de le dupliquer. Le lecteur pressé peut sauter tout de suite à l'annexe A du RFC (résumée à la fin de cet article), qui classe rapidement les protocoles avec des tableaux synthétiques.

D'abord, c'est quoi, la gestion des réseaux ? Ce sont l'ensemble des méthodes et techniques mises en œuvre par l'administrateur réseaux pour s'assurer que le réseau va bien, prévoir ses évolutions, et réparer ses pannes. Cela va du bon vieux ping aux mécanismes les plus complexes. (Si vous suivez les débats sur la neutralité de l'Internet <https://www.bortzmeyer.org/neutralite.html>, vous êtes peut-être déjà tombé sur des termes comme « services gérés » ou « gestion de trafic ». Il faut savoir que ces termes relèvent de la propagande des opérateurs réseaux, qui cherchent à justifier des services privilégiés - et plus chers - en prétendant qu'ils seraient « gérés », comme si le reste de l'Internet marchait tout seul. Les termes corrects sont « services privilégiés » et « discrimination de trafic ».)

Il y a déjà eu des RFC analogues à celui-ci (section 1.2). Par exemple, le RFC 6272 [1] faisait le tour de tous les protocoles TCP/IP (y compris ceux sur la gestion de réseaux) dans le contexte de la "*Smart grid*". Le RFC 3535 rendait compte d'un atelier de l'IAB consacré à la gestion de réseaux, qui avait examiné la situation en 2002. Le RFC 5706 posait les règles relatives à la gestion pour tous les nouveaux protocoles IETF, imposant qu'ils prennent en compte cette gestion dès le premier RFC. Enfin, les RFC 4221 et RFC 6371 décrivent le cas spécifique de la gestion des réseaux MPLS et sont à l'origine d'un conflit de compétences avec l'UIT qui dure encore aujourd'hui (cf. RFC 5704). Plusieurs "*Internet-Drafts*" sont également en cours de rédaction sur ce sujet de l'**OAM** ("*Operations, Administration and Maintenance*", ce sigle est souvent utilisé dans le monde MPLS pour parler de la gestion des réseaux).

La section 2 de notre RFC couvre les protocoles de gestion généralistes, qui peuvent servir à tout. Le premier est évidemment SNMP (section 2.1). Il s'agit en fait d'une structure modulaire, avec un modèle de données (les fameuses MIB), un mécanisme d'encodage de ces données sur le réseau et un protocole, SNMP. Le RFC de description général est le RFC 3410, pour SNMPv3. Un réseau est vu par SNMP comme un ensemble de machines gérées (les **agents**), une ou plusieurs machines de gestion (le ou les **managers**) et le protocole utilisé entre les deux (SNMP). Les variables exportées par l'agent sont décrites dans une MIB, et il en existe des dizaines de normalisées et encore plus de privées.

SNMP v1 (RFC 1157) et v2 avaient de sérieuses limites en matière de sécurité, la version officielle aujourd'hui est donc la v3, normalisée dans le RFC 3411 (mais la v1 reste très utilisée). SNMP est présent partout, pour lire les valeurs des variables des équipements réseaux, faire des statistiques, aider à déboguer les pannes, etc. C'est un des grands succès de l'IETF.

Pour décrire les données récupérées en SNMP, un cadre standard existe nommé SMI ("*Structure of Managed Information*"), actuellement en version 2, normalisée dans les RFC 2578 et RFC 2579. Ces RFC définissent entre autre le langage dans lequel sont écrits les MIB.

SNMP est, on l'a vu, très répandu, et le RFC lui consacre à juste titre de nombreuses pages, parlant de sa sécurité, du mécanisme de transport, etc. Un autre protocole très populaire pour la gestion de réseaux est syslog (section 2.2). Il est concurrent de SNMP pour le signalement de problèmes (les "*traps*" de SNMP) mais, autrement, il ne remplit pas le même rôle. syslog sert à une machine à transmettre de l'information (pas forcément une panne) en temps réel, à des fins d'alarme ou de journalisation. Décrit d'abord dans le RFC 3164, il est désormais normalisé (sous une forme bien plus riche) dans le RFC 5424. Le syslog traditionnel des débuts ne prévoyait pas de structure pour le message envoyé : c'était juste du texte libre. Le RFC 5424 a introduit la notion de messages syslog structurés, analysables par un programme.

Si syslog est très répandu (on trouve des récepteurs syslog en logiciel libre sur tous les Unix, tous les routeurs savent émettre du syslog, etc), je ne suis pas sûr que les extensions modernes, encore peu implémentées, soient souvent utilisées.

Autre protocole très répandu dans la boîte à outils de l'administrateur réseaux, IPFIX (souvent désigné par son ancien nom, NetFlow). La section 2.3 décrit son rôle : IPFIX permet de récolter de l'information statistiques sur les flots de données qui sont passés par un routeur (« `[2001:db8:1::42]:35612` a parlé à `[2001:db8:cafe::1337]:80` et il a reçu 935 ko ») et de la transmettre à une machine de gestion. Avoir des compteurs par flot (un flot étant typiquement une connexion TCP complète) permet d'avoir une information plus légère que si on transmettait des données sur chaque paquet.

1. Pour voir le RFC de numéro NNN, `https://www.ietf.org/rfc/rfcNNN.txt`, par exemple `https://www.ietf.org/rfc/rfc6272.txt`

L'architecture d'IPFIX est décrite dans le RFC 5470 et le protocole est dans le RFC 7011. L'ancien Netflow, lui, était décrit dans le RFC 3954. IPFIX/Netflow est très répandu et la plupart des opérateurs l'utilisent pour suivre l'activité de leurs réseaux. (Le logiciel libre ntop <http://www.ntop.org/nprobe/nprobe-complies-with-ipfix-specification/> le parle, entre autres.)

Si on veut suivre les paquets individuels, il y a le protocole PSAMP ("*Packet SAMPling*") du RFC 5474. Il permet d'utiliser le protocole d'IPFIX pour transmettre des données sur les paquets (qu'on a pu, pour limiter le trafic, échantilloner, comme bien expliqué dans le RFC 5475).

IPFIX, syslog et SNMP (tel que réellement utilisé dans la plupart des cas, sans ses fonctions d'écriture) ne font que lire les informations. Si on veut les modifier, si on veut changer la configuration d'un routeur, par exemple, que fait-on ? SNMP avait théoriquement un mécanisme pour cela mais, en pratique, il n'est que très rarement utilisé. L'atelier de l'IAB raconté dans le RFC 3535 identifiait ce manque (section 2.4) et l'un des résultats a été le protocole NETCONF normalisé dans le RFC 6241. NETCONF permet d'envoyer des commandes de configuration (encodées en XML) à un équipement réseau. Relativement récent, NETCONF n'est pas encore d'usage universel.

Pour décrire les données manipulées par NETCONF, l'IETF a un langage, YANG (RFC 6020). Celui-ci dispose d'un certain nombre de types de données pré-existants, normalisés dans le RFC 6991. Ces types sont évidemment proches de ceux que le SMI v2 avait déjà, pour SNMP. Idéalement, il faudrait encore ajouter une traduction standard de SMI vers YANG, afin de pouvoir récupérer toutes les MIB existantes. Pour l'utilisation de NETCONF et de YANG dans une solution globale, voir le RFC 6244. YANG est encore plus récent que NETCONF et encore peu déployé.

Tous ces protocoles, SNMP, syslog, NETCONF, etc, sont génériques et peuvent servir à gérer des tas de protocoles différents. La section 3 couvre au contraire les protocoles de gestion spécifiques, liés à une tâche donnée. Elle commence avec les protocoles de gestion de l'allocation d'adresses IP (section 3.1). D'abord, DHCP (RFC 2131 et RFC 8415). Il permet de transmettre à une machine son adresse IP mais aussi plein d'autres informations de configuration comme le résolveur DNS à utiliser (RFC 3646). DHCP n'offre aucun mécanisme de sécurité et le RFC rappelle donc qu'il vaut mieux ne l'utiliser que sur des réseaux dont l'accès physique est contrôlé.

Les adresses IP peuvent aussi être configurées automatiquement, sans serveur, dans le cadre décrit par le RFC 5889.

Depuis de nombreuses années, l'Internet est en cours de transition (très lente) d'IPv4 vers IPv6. Cette transition a donné naissance à tout un ensemble de techniques spécifiques <https://www.bortzmeyer.org/transition-ipv6-guilde.html>, à commencer par le RFC 4213.

Une part importante de la gestion des réseaux est la mesure des performances (section 3.4). Ce n'est pas tout d'aller bien, il faut encore aller vite. Un groupe de travail IETF spécialisé, IPPM <http://tools.ietf.org/wg/ippm> existe depuis longtemps pour développer des métriques (des grandeurs mesurables et rigoureusement définies) pour les réseaux TCP/IP. Il a produit un document de cadrage (RFC 2330), un document sur le développement de nouvelles métriques (RFC 6390), et de nombreuses métriques comme le délai de transmission (RFC 7679), le taux de pertes (RFC 7680), la mesure de la duplication de paquets (RFC 5560), etc. Pour pouvoir mesurer effectivement ces métriques, plusieurs protocoles ont été créés comme OWAMP ("*One-way Active Measurement Protocol*", RFC 4656).

Toujours dans cette section de protocoles divers, une part importante est dédiée à RADIUS (RFC 2865), protocole permettant l'authentification d'un client, connecté à un NAS ("*Network Access Server*"), et utilisant un serveur d'authentification partagé entre plusieurs NAS. RADIUS permet par exemple à un

FAI de centraliser l'authentification afin d'éviter que chaque NAS ait une base d'utilisateurs différente. Il est très largement utilisé aujourd'hui. De nombreux RFC sont venus lui ajouter telle ou telle fonction, ou guider les programmeurs (RFC 5080).

Officiellement, RADIUS a un concurrent, Diameter (RFC 6733). Conçu après, incompatible avec la base déployée, censé résoudre des problèmes réels ou supposés de RADIUS, Diameter n'a guère eu de succès. Le RFC oublie complètement de mentionner cet échec ; RADIUS est simple et facilement implémentable, Diameter, grosse usine à gaz, ne l'a jamais réellement concurrencé.

La section 3 décrit encore plusieurs autres protocoles peu connus, mais j'arrête ici. Il y a un autre gros morceau à avaler, les modèles de données pour la gestion de réseaux (section 4). Ils sont très nombreux et couvrent beaucoup d'aspects de la gestion de réseaux. Un de mes préférés est le peu connu RMON (RFC 2819), qui modélise des sondes réseaux. Il permet de déclencher à distance, avec SNMP, des mesures du réseau.

L'annexe A, présentée au début, est une sorte de résumé pour lecteurs pressés. Elle classe les différents protocoles de gestion de réseaux (rappelez-vous que la liste est longue) selon divers critères (fonctionnement en "*push*" ou en "*pull*", passif ou actif, extensibilité de leur modèle de données, etc)

Le premier tableau, en A.1, classe les protocoles selon leur place dans le chemin des normes (cf. RFC 2026, notre RFC ne tient pas encore compte de la réduction de ce chemin à deux entrées, dans le RFC 6410). Ainsi, SNMP est "*Internet standard*" (norme au sens propre) alors qu'IPFIX n'est que "*Proposed standard*" (projet de norme) et que DHCP n'a jamais décollé de la première étape, "*Draft standard*" (proposition de norme), en dépit de son très vaste déploiement.

Autre façon de classer, en A.2, selon les tâches à accomplir. Syslog et SNMP permettent la surveillance du réseau mais SNMP permet en outre d'agir sur la configuration de celui-ci (en pratique, il n'est guère utilisé pour cette tâche). NETCONF peut faire de la configuration, mais, si on veut mesurer les performances, ce sont SNMP et IPFIX.

Comment ces protocoles font-ils leur travail (A.3) ? SNMP et NETCONF sont "*pull*" (la machine de gestion décide quand agir), Syslog, RADIUS ou IPFIX sont purement "*push*" (ils réagissent aux événements extérieurs). Notez que SNMP a aussi une fonction "*Push*", les notifications (auutrefois nommées "*traps*").

Autre façon de les regarder travailler (A.4), certains protocoles sont actifs posant des questions au réseau (ping et traceroute - RFC 1470, BFD - RFC 5880, OWAMP, etc). D'autres sont passifs, observant simplement le réseau (IPFIX, PSAMP, etc).

Le travail de gestion des réseaux ne s'arrêtera jamais. Il y aura toujours de nouveaux problèmes et de nouvelles solutions. L'annexe B décrit un travail récent à l'IETF, la gestion de l'énergie, préoccupation désormais très forte, en raison de l'augmentation des coûts de l'électricité et des soucis écologiques plus présents (menant par exemple à des lois plus strictes). Actuellement, dans la gestion de réseaux, il est rare que la consommation électrique soit prise en compte. Les serveurs ne distribuent pas cette information et les logiciels de gestion ne la demandent pas. On surveille le taux de pertes de paquets, le débit, mais pas la consommation électrique au niveau de chaque machine.

Une des difficultés pour effectuer cette mesure est que la consommation électrique est souvent mieux mesurée en dehors de la machine, par exemple par une source PoE, ou bien par un bandeau électrique « intelligent ». Il faut donc travailler, entre autres, sur la liaison entre une machine et sa consommation. C'est la tâche du groupe de travail IETF EMAN <http://tools.ietf.org/wg/eman> (cf. RFC 6988 et RFC 7326, publiés depuis).