
SNMPv2

Christophe MEESEN

En 1988 l'Internet Activities Board (IAB) approuva le développement de SNMP (Simple Network Management Protocol) et de CMOT (Common Management Information Protocol over TCP/IP). A ce moment là, SNMP devait être une solution à court terme et CMOT a long terme.

CMOT est dérivé de CMIP (Common Management Information Protocol) qui devait lui être utilisé sur OSI. En attendant que OSI émerge et remplace TCP/IP... il fut convenu de développer CMOT dans une phase purement transitoire.

L'IAB imposa que CMOT et SNMP utilisent la même base de données d'objets gérables. Donc une SMI (structure of managed information) et une MIB (managed information base) communes devaient être définies et utilisées.

Cette décision avait pour objectif de faciliter la transition future de SNMP vers CMOT.

Il est rapidement apparu que cette contrainte était non réaliste car en SNMP on manipule essentiellement des variables et en CMIP on manipule des objets dans le sens de la technologie orientée objet.

En 1989 la séparation des deux protocoles fut acceptée par l'IAB et les deux protocoles suivirent alors une évolution parallèle et indépendante.

Une fois libéré de la contrainte de compatibilité avec OSI, les progrès ont été rapides. SNMP a été adopté par de nombreux constructeurs et est devenu à ce jour un standard populaire de gestion réseau.

L'amélioration du protocole SNMP a été poursuivie dans de nombreuses directions. La plus importante fut la définition de la MIB RMON (remote monitoring). RMON permet au gestionnaire réseau d'avoir une vue d'ensemble de son réseau et des appareils qui y sont connectés.

Beaucoup d'autres extensions ont vu le jour, certaines sont dépendantes des vendeurs et d'autres sont communes telle que la MIB de gestion d'interface FDDI, token ring,...

Si RMON est allé le plus loin dans ce que l'on peut faire avec SNMP, il y a toute fois une limite. Lorsque SNMP est utilisé pour des réseaux plus grands et plus sophistiqués, les déficiences deviennent apparentes. Elles sont essentiellement dans le domaine de la sécurité et de la fonctionnalité.

Beaucoup a été fait pour remédier à ces déficiences. Un premier pas fut un ensemble de documents publiés en 1992 proposant une amélioration de la sécurité de SNMP en tant que nouveau standard. Cette amélioration n'était pas compatible avec la version SNMP courante. Elle impliquait une modification importante du protocole.

Dans le même mois une proposition pour une nouvelle version du protocole SNMP fut proposée: SMP (Simple Management Protocol). Les changements apportés par SMP étaient aussi importants que secureSNMP.

SMP a été accepté comme base pour définir la nouvelle génération du protocole SNMP: SNMPv2. Il fut également convenu qu'il n'y aurait qu'une seule transition de SNMP vers SNMPv2. Donc les deux propositions secureSNMP et SMP furent suspendues bien qu'elles contribuèrent largement à la définition du nouveau protocole SNMPv2.

Deux groupes de travail furent créés. Un groupe étudia tous les aspects sécurité et l'autre le reste des améliorations proposées. Le résultat fut la publication au début 1993 de 12 documents proposant et décrivant SNMPv2 comme le nouveau standard.

SNMPv2 ne changera que très peu avant de devenir un standard à part entière. Actuellement il a le statut de "standard brouillon" (draft standard). C'est l'état intermédiaire entre le "standard proposé" (proposed Standard) et un "standard définitif".

SNMPv2 est le produit de 4 personnes qui ont chacune joué un rôle important dans l'histoire de SNMP:

Jeffrey Case, SNMP Research, Inc., and University of Tennessee
Keith McCloghrie, Huges LAN Systems
Marshal Rose, Dover Beach Consulting, Inc.
Steven Waldbusser, Carnegie-Mellon University

Les améliorations apportées par SNMPv2 se répartissent en 4 catégories:

1. domaine d'application:

SNMPv2 est conçu pour faciliter la gestion de n'importe quelle ressource, pas seulement de ressource réseau. SNMPv2 peut donc être utilisé pour gérer des applications, des systèmes et pour communiquer entre gestionnaires.

Grâce à l'ajout des fonctions de communication de gestionnaire à gestionnaire, SNMPv2 peut être aussi utilisé en gestion distribuée.

SNMPv2 propose un cadre concis et flexible pour décrire les informations en promouvant l'extensibilité dans la définition de MIBs.

De même SNMPv2 propose un moyen pour décrire les conditions de "conformance" à la définition de MIB standard ou bien, pour la MIB d'un agent donné, les capacités effectivement implémentées ou non implémentées.

2. taille, vitesse et efficacité:

SNMPv2 reste "simple", pour permettre le développement de petites et rapides implémentations. Le format des messages de type Trap n'est plus différent des autres messages afin de simplifier les routines d'interprétation des messages.

Le changement majeur dans cette catégorie est l'ajout de la commande *get bulk* pour l'échange de grandes quantités d'informations. La commande *get bulk* est une requête de plusieurs *get next* successifs. Auparavant, on était obligé de faire une succession de *get next* pour lire une table, avec SNMPv2 une seule commande et réponse peuvent maintenant suffire pour cela.

3. sécurité et privautés:

SNMPv2 permet de garantir l'authentification des messages et/ou l'encryptage des messages. Ce système est très riche et permet de définir l'accès à chaque variable, le type de sécurité et de protocole utilisé pour chaque transaction. Il est ainsi possible de spécifier qui

peut faire quelle opération sur quelle variable et avec quel degré de sécurité: non sécurisé, authentifié ou encrypté.

4. déploiement et compatibilité:

SNMPv2 a été conçu pour être utilisé sur TCP/IP, OSI et d'autres architectures de communication. SNMPv2 permet aussi de communiquer avec des plates-formes supportant le protocole SNMPv1.

SNMPv2 va certainement compliquer l'image de la gestion réseau pour la plus part des utilisateurs. Certaines personnes attendent que SNMPv2 devienne un standard, d'autres veulent profiter immédiatement des avantages de SNMPv2 et enfin, comme toujours, d'autres refusent radicalement tout changement ... en attendant OSI...

Ceci conduira tôt ou tard à des problèmes d'interopérabilité.

Aujourd'hui, SNMPv2 se met lentement en place quelque fois de façon partielle où c'est souvent la partie sécurité qui est délaissée. C'est à dire que le contrôle d'accès se réduit à un accès non sécurisé pour toutes les variables.

L'évolution de SNMPv1 vers SNMPv2 est une étape importante dans l'évolution de SNMP. Le champ d'application couvert maintenant par SNMP s'est largement étendu.

Toutefois il faut bien se rappeler que SNMP est un standard d'échange d'information de gestion. Ceci n'est qu'une partie du problème de la gestion réseau. Pour ce qui concerne l'interface utilisateur, il reste encore beaucoup à faire. Il y a bien sur la présentation des informations mais aussi leur interprétation.

Il serait bien de disposer, par exemple, d'un langage permettant à l'utilisateur ou aux vendeurs de définir un traitement à effectuer avec les informations obtenue par SNMP. Par exemple les dispositions à prendre ou les actions à effectuer face aux conclusions que le système peut tirer de ces informations.

Si SNMPv2 poursuit son évolution vers un protocole de gestion simple et performant, il reste encore du chemin à parcourir avant de disposer de vrais outils de gestion réseau.