TP SNMP

Olivier AUBERT

2002

1 Utilisation des outils CMU

À l'aide des commandes `snmpget` et `snmpgetnext`, et en vous référant au fichier `/usr/share/snmp/mibs/RFC1213-MIB.txt`, répondez aux questions suivantes.

Pour les équipements `134.214.88.9`, `134.214.90.32` et `134.214.90.7` :
- Quel est le type (PC, switch, routeur, etc) de ces équipements ?
- Quel est l'OID des sociétés qui ont construit ces équipements (variable MIB `sysObjectID`) ?
- Depuis combien de temps sont-ils en marche ?
- Combien ont-ils d'interfaces ?
- Quelles sont les adresses MAC de leurs interfaces (s'il est possible de le dire) ? Rappel : l'OID correspondant à cette variable pour chaque interface est formée par l'OID normal de cette variable dans la MIB suffixé par le numéro (index) de l'interface dans la table.
- Quel est le débit de chacune des interfaces et leur MTU ?
- Combien de paquets IP ont été émis par la première interface active de ces équipements ?

Les questions précédentes sont seulement quelques exemples des données auxquelles un administrateur peut être amené à s'intéresser. Le choix des données pertinentes est fonction du problème à traiter, du matériel utilisé et du réseau étudié.

2 Accès direct aux informations

Il est possible d'accéder aux informations de gestion en utilisant les fonctionnalités intégrées aux équipements réseau, comme `telnet` ou `http`. Les login/mots de passe de consultation sont usuellement `user/user` ou `monitor/monitor`.

3 Utilisation d'un outil graphique

Nous allons utiliser tkined pour visualiser les mêmes informations, d'une manière plus pratique. Pour cela, lancer l'exécutable `tkined` et cliquer sur l'icône représentant un point d'interrogation. Elle permet de créer de nouveaux éléments dans notre système. Après avoir créé un nouvel élément, revenir en mode sélection (icône flèche) et le sélectionner. Le bouton droit de la souris permet alors de modifier ses attributs. Fixez son nom à un parmi `sw710he` à `sw710ho`.

Dans le menu `Tools`, vous pouvez sélectionner un des modules de Tkined. Nous en verrons un certain nombre. Le principe pour tous ces modules est de faire apparaître un nouvel item dans la barre de menu, proposant de nouvelles fonctionnalités.

Sélectionnez le menu *SNMP Browser* et retrouvez à partir de là les mêmes informations que celles demandées précédemment.

Sélectionnez ensuite *SNMP Trouble*, qui permet d'accéder plus rapidement aux différentes informations importantes d'un équipement. Visualisez quelques-unes des valeurs.

4 Découverte de réseau

On ne construit habituellement pas la carte de notre réseau à la main. Les outils graphiques proposent des modules de découverte automatique plus ou moins évolués. Tkined fournit le module *IP Discover*. Sélectionnez l'item *Discover IP Network* et précisez un des quatres numéros de réseau suivants : 134.214.88.0, 134.214.89.0, 134.214.90.0 ou 134.214.91.0. Après un certain temps, tkined affiche une carte des équipements réseau identifiés.

Il vous reste alors à organiser le graphe afin de faire correspondre les éléments à la topologie (logique ou physique) la plus appropriée pour votre cas. Le module *IP Layout* fournit quelques aides pour ce faire. Identifiez différents types d'équipement représentés.

5 Monitoring de machine

Nous allons mettre en place un système de monitoring sur une des machines. Il est possible de le faire sur un certain nombre de variables, comme par exemple un simple test de fonctionnement de l'équipement ou bien sur la quantité d'octets transférés.

Pour activer la vérification de la connexion de l'équipement, choisissez le module *IP-Monitor* puis *Check reachability*. Ceci va créer un *job* de surveillance, donc les paramètres sont modifiables via *Modify Monitor Job*. Passez l'intervalle de vérification à une valeur plus faible et essayez de déconnecter l'équipement pour voir ce qui se passe.

Pour surveiller une variable SNMP, il faut utiliser le module *SNMP-Monitor*. Trouvez une valeur à surveiller en utilisant, dans le module *SNMP-Trouble*, le menu *Show MIB Scalars* qui va vous indiquer pour chaque type de MIB les valeurs scalaires qu'il est possible d'observer. Les MIB `IF-MIB`, `IP-MIB` et `TCP-MIB` sont les plus susceptibles de contenir des objets intéressants.

6 Installation d'un agent

Installez le paquetage `snmpd` depuis le serveur 134.214.90.7. Effectuez les modifications adéquates dans le fichier de configuration `/etc/snmp/snmpd.conf`. Relancez le démon snmpd par la commande `/etc/init.d/snmpd restart`. Vérifiez depuis tkined que de nouvelles informations sont accessibles.

Consultez la documentation se trouvant dans le répertoire `usr/share/doc/snmpd/` pour enrichir les informations disponibles (espace disque disponible, mémoire disponible, etc). Vous pouvez utiliser les informations issues de la MIB `UCD-SNMP-MIB.txt`.

7 Utilisation de MRTG

MRTG est un outil permettant de surveiller des variables SNMP sur des serveurs, et de produire des graphes à partir des observations. On le trouve notamment mis en œuvre sur des routeurs, afin de déterminer le trafic passant par chacune de ses interfaces par exemple. Les graphes sont produits sous la formes de fichier PNG dans des documents HTML, afin de pouvoir être accessibles depuis n'importe quel navigateur web.

Vous pouvez installer le paquetage `mrtg` sur votre machine, et vous référer à la page de manuel `mrtg-reference` pour configurer MRTG. Vous pouvez par exemple le configurer afin d'afficher des statistiques sur le trafic réseau d'un des switchs.