IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

# TP - Supervision réseau - SNMP

FIP IR312

Automne 2018

## 1 Généralités sur SNMP

Les équipements réseaux se paramètrent généralement au travers d'interfaces de type `telnet` ou navigateur web. Ces interfaces conviennent bien si elles sont manipulées par un humain. En revanche, si les équipements doivent être manipulés et surveillés par des logiciel de maintenance, il faut un protocole plus structuré. C'est là qu'intervient SNMP.

SNMP (*Simple Network Management Protocol*) est un protocole applicatif (par-dessus UDP) pour gérer/-diagnostiquer des équipements réseau (serveur, switch, routeur, etc.) Selon la terminologie SNMP on trouve un **manager** (client) et un **agent** (serveur).

Deux types de fonctionnement :

**poll :** le manager interroge/configure l'agent ;

**trap :** l'agent alerte le manager d'un imprévu.

Primitives du protocole v1 :

**get-request :** le manager demande une information à un agent ;

**get-next-request :** le manager demande l'information suivante à l'agent ;

**set-request :** le manager met à jour une information sur un agent ;

**get-reponse :** l'agent répond à un get-request ou a un set-request ;

**trap :** l'agent envoie une alarme au manager.

En terme de sécurité, le manager s'authentifie auprès de l'agent en indiquant le nom de la *communauté* à laquelle il appartient. Typiquement, la communauté `public` a le droit de faire des requêtes `get` mais pas des requêtes `set`. De plus, certains agents peuvent également filtrer sur l'adresse IP du manager.

De multiples versions : v1 v2c v2 v3 (plus toutes les extensions propriétaires de constructeurs), sont décrits par une petite quarantaine de RFC (qui définissent, abrogent, redéfinissent, annulent, remplacent,..., digne d'un texte de loi français !). Finalement, seule la version 1 est supportée par tous.

Concrètement, l'agent (serveur) écoute sur le port UDP 161 les requêtes d'un manager et lui répond. Un manager (client) peut également comporter un daemon qui reste à l'écoute sur le port UDP 162 des éventuelles alertes (trap) qu'un agent peut lui envoyer.

Les objets échangés par SNMP (chaînes, scalaires, tableaux de scalaires) sont organisés et standardisés dans une MIB (*Management Information Base*), selon une organisation arborescente, notation pointée :

— partie commune à tous les agents en général
— partie commune à tous les agents d'un même type de matériel
— partie spécifique à chaque constructeur

Chaque objet est repéré dans la MIB par un OID [1] (*Object Identifier* norme ASN.1, voir le `man 5 variables`), par des numéros ou par des noms (dont le "début" peut être implicite). Par exemple les trois OID suivants désignent le même objet :

— `.1.3.6.1.2.1.1.1.0`
— `.iso.org.dod.internet.mgmt.mib-2.system.sysDescr.0`
— `system.sysDescr.0`

La commande `snmptranslate` peut faire cette traduction pour vous (lire le `man`). Pour afficher la MIB : `snmptranslate -Tp -IR iso | less`

1. `http://www.alvestrand.no/objectid/`

# 2 Utilisation des outils CMU / UCD

Le protocole SNMP n'est pas franchement prévu pour être utilisé directement par un humain. Vous vous en rendrez compte par la suite, les requêtes sont un peu fastidieuses à écrire à la main, mais cela est tout de même possible grâce à quelques outils en ligne de commande. C'est de plus très pédagogique...

Les universités américaines de Carnegie Mellon d'abord et de Davis (California) ont développé un ensemble d'outils pour SNMP, des commandes et des agents. Les paquetages sont connus sous les noms `cmu-snmp` [2] et `ucd-snmp` [3]. Une nouvelle mouture de ces outils est maintenant disponible sous le nom `net-snmp` [4].

Nous allons utiliser ces commandes en les appliquant à divers équipements.

Ces commandes implémentent les primitives SNMP. On a ainsi `snmpget` et `snmpgetnext`. Une autre est commode et se sert de `getnext` itérativement, il s'agit de `snmpwalk`.

La syntaxe générale de ces commandes est la suivante :
`snmp`***`xxx`*** `-v1` *`nom_machine_ou_IP`* `-c` *`community OID`*
Exemple :
```
snmpget -v1 router -c public system.sysDescr.0
```

La syntaxe générale de ces commandes est accessible via `man snmpcmd`.

## 2.1 Utilisation des commandes `snmpget` et `snmpgetnext`

À l'aide de ces deux commandes et en vous référant [5] au fichier `RFC1213-MIB` [6] vous répondrez aux questions suivantes :

1. Quelle est la description (textuelle) de la machine `galaxie-eth0.enst-bretagne.fr` ?
2. Quel est l'OID attribué à la société qui a construit cette machine (variable MIB `sysObjectID`) ?
   Notez que cet OID nous renvoie vers une extension privée (par entreprise) pour laquelle il faudrait ajouter la MIB [7] à notre manager SNMP pour utiliser ces extensions...
3. Combien a t'elle d'interfaces ?
4. Quelle est l'adresse MAC de ces interfaces (s'il est possible de le dire) ? (rappel : l'OID correspondant à cette variable pour chaque interface est formé par l'OID normal de cette variable dans la MIB suffixé par le numéro, l'index de l'interface dans la table).
5. Quel est le débit de chacune de ces interfaces et leur MTU ? (Qu'est-ce que le MTU d'une interface ?)
6. Combien de paquets ont été émis par la première interface active des ces machines ?

Il existe aussi une commande appelée `snmpwalk`, ne correspondant pas à une primitive SNMP mais qui utilise la primitive `GetNext` de manière automatique. Cette commande permet de parcourir des tables par exemple. Testez `snmpwalk` sur l'objet `interfaces`.

**Remarque :** il est facile de poser de telles questions pour un exercice "scolaire". Dans la réalité il est bien plus délicat de définir la pertinence des informations examinées. On ne peut pas tout examiner, il faut choisir et il n'y a pas de "vérité" en la matière. Ce qui est judicieux pour un équipement le sera moins pour un autre.

## 2.2 Une MIB pour imprimante

Nous allons utiliser une MIB optionnelle. Le fichier de description est déjà présent sur le PC (`Printer-MIB`), mais ce module n'est pas chargé par défaut avec la MIB principale. Il faut donc le faire explicitement lorsque l'on veut utiliser une commande SNMP.

Voici un exemple de requête :
`snmp`***`xxx`*** `-v1 -c public -m SNMPv2-TC:Printer-MIB` *machine oid*

L'option `-m` est suivie par la liste des modules à prendre en compte, c-à-d. la MIB standard et la nouvelle MIB que vous voulez raccrocher à la MIB standard. Lorsque vous interrogez une imprimante, cela doit être précisé pour chaque commande `snmp`***`xxx`*** (remplacer ***`xxx`*** par `get getnext walk`, etc.) (Voir `man snmpcmd`).

2. `ftp://ftp.andrew.cmu.edu/pub/net`
3. `http://www.ece.ucdavis.edu/ucd-snmp/`
4. `http://www.net-snmp.org/`
5. Utilisez les commandes `less` ou `more`, et évitez les *éditeurs* comme `vi gedit` ou autre : si vous modifiez ces fichiers par mégarde, cela risque de poser des soucis pour la suite !
6. Vous le retrouverez à l'aide de la commande `locate`, ou en cherchant dans les répertoires des MIB indiqués par `net-snmp-config --default-mibdirs`
7. en l'occurrence téléchargeable sur `ftp://ftp.cisco.com/`

Quelle information récupère la commande suivante ?

```
snmpget -v1 -c public -m SNMPv2-TC:Printer-MIB imp-df-400.priv.enst-bretagne.fr
printmib.prtMarker.prtMarkerTable.prtMarkerEntry.prtMarkerPowerOnCount.1.1
```

Interrogez maintenant des imprimantes de l'école sur des objets du groupe *printmib.prtAlert*. (Par exemple l'imprimante `imp-df-400.priv.enst-bretagne.fr`). Pour retrouver la désignation exacte des OID qui nous intéressent, n'hésitez pas à lire le contenu du fichier `Printer-MIB` (sans le modifier s'il vous plaît) et à jouer avec la commande `snmptranslate` vu plus haut.

**Remarque :** HP propose un outil Unix (essentiellement pour HP-UX, SunOS et Solaris...) pour administer ses imprimantes : l'outil `hpnpadmin`. Cet outil est en fait un manager SNMP avec une MIB pour les imprimantes HP.

# 3 Utilisation d'un outil graphique de parcours de MIB

En complément de ces outils classiques en ligne de commande, il existe un certain nombre d'outil professionnels offrant un environnement graphique et permettant à un administrateur réseau de gérer ses équipements par SNMP [8]. L'un des plus connu est l'outil `openview` (HP). On trouve également quelques outils libres comme `qtmib` [9], `tkmib` ou `mbrowse` [10].

Nous allons maintenant utiliser cet outil `mbrowse` qui offre une interface graphique supposée proche de celle des outils professionnels.

## 3.1 Questions

Vous interrogerez l'agent `galaxie-eth0` (il s'agit d'un routeur).

Vous pouvez refaire les questions précédemment testées avec les outils `net-snmp`.

Visualisation de la table de routage :

Repérez la table de routage dans le groupe `ip` de la MIB. Sélectionnez l'élément `ipRouteEntry`, et dépliez ses branches. En vous promenant dans cet arborescence et à l'aide de l'action `Walk`, répondez aux questions suivantes :

1. Quelles sont les caractéristiques principales de la direction par défaut (adresse 0.0.0.0) : interface de sortie et adresse du prochain routeur ?
2. Repérez les interfaces correspondant à des réseaux *subnettés*, donnez le netmask et indiquez sur combien de bits sont réalisés les masques (questions de rappel général sur IP).

# 4 D'autres outils classiques

**MRTG** *Multi Router Traffic Grapher* [11] est un outil qui permet de monitorer la charge du réseau. Il se comporte comme un manager SNMP qui interroge régulièrement les équipements et réalise des mesures statistiques. Il produit des jolis graphiques à insérer dans des pages web. Par contre, il ne fait pas de corrélation d'événements (pour cela on utilise un outil comme nagios ou snort, voir le cours sur la sécurité et les IDS *Intrusion Detection System*).

**cacti** [12] Il peut-être considéré comme le successeur de MRTG. Il fait la même chose mais en mieux ;-) Son fonctionnement est basé sur RRDTool (un outil de gestion de base de données circulaires) pour stocker les mesures relevées périodiquement.

**scotty** L'université de Twente aux Pays Bas [13], qui a participé à la définition du protocole, a réalisé des outils et des librairies permettant d'implémenter son propre agent et son manager (dans le langage Tcl). Les outils `scotty` et `tkined` ont cependant une vocation "universitaire", et les derniers développements datent de juin 2001.

8. Pour une (petite) liste d'outils SNMP : `http://www.snmpworld.com`
9. `http://sourceforge.net/projects/qtmib/`
10. `http://sourceforge.net/projects/mbrowse/`
11. `http://people.ee.ethz.ch/~oetiker/webtools/mrtg/`
12. `http://www.cacti.net/`
13. `http://wwwhome.cs.utwente.nl/~schoenw/scotty/`

**snmpd** La plupart des équipements réseau embarquent un agent SNMP. Cependant, un simple ordinateur en réseau peut également fournir des services de type "agent SNMP" dès lors qu'il a un daemon comme le programme `snmpd` (lire le `man`) qui publie des informations comme l'état des interfaces réseau, l'utilisation des disques durs, etc.