# Exercices SNMP, partie I

Remarque : Bon nombre de commandes utilisées dans cet exercice n'ont pas besoin d'être exécutées en tant que root, mais il est prudent de les exécuter toutes en tant que root. Il est donc plus simple de lancer un shell en tant que root et d'entrer toutes les commandes à ce niveau. Vous pouvez lancer un shell de root ainsi :

```
$ sudo -s
```

ou

```
$ sudo -s
```

## 0. Installation des outils de client (manager)

```
# apt-get install snmp
# apt-get install snmp-mibs-downloader
```

La deuxième des deux commandes ci-dessus téléchargent les MIB standards de l'IETF et IANA, qui ne sont pas incluses par défaut.

Note: afin que ceci fonctionne, vous devez activer la source Ubuntu "multiverse" dans votre configuration APT. Ceci a déja été fait pour vous ici.

Maintenant, éditez le fichier /etc/snmp/snmp.conf

Remplacez cette ligne:

```
mibs :
```

... afin qu'elle devienne:

```
# mibs :
```

Note: En ajoutant '#' devant le mot 'mibs "', vous *commentez" la déclaration, qui dans son état précédent, disait aux outils SNMP de ne* pas* charger automatiquement les MIBs dans le répertoire /usr/share/mibs/

## 1. Configuration de SNMP sur votre routeur Cisco

Pour cet exercise, nous allons travailler en groupe. Une personne dans chaque groupe sera désignée pour entrer les commandes au clavier.

Rappel: Groupe 1: pc1-4, Groupe2: pc5-8, etc.

Si vous n'êtes pas certain du groupe auquel vous appartenez, référez vous au Diagramme Réseau sur http://noc.ws.nsrc.org/

Connectez-vous à votre routeur:

```
$ ssh cisco@rtrN.ws.nsrc.org    (ou "ssh cisco@10.10.N.254")

où N est le numéro de votre groupe

username: cisco
password: <MOT DE PASSE DONNÉ EN CLASSE>

rtrN> enable
Password: <MOT DE PASSE DONNÉ EN CLASSE>
rtr1# configure terminal        (conf t)
```

On va ajouter une Access List (liste d'accès) pour l'accès à SNMP, puis activer SNMP, donner une communauté et indiquer au routeur de garder les même index SNMP même après un redémarrage.

```
rtrN(config)# access-list 99 permit 10.10.0.0 0.0.255.255
rtrN(config)# snmp-server community NetManage ro 99
rtrN(config)# snmp-server ifindex persist
```

On sort du mode config et on sauve la configuration en mémoire permanente.

```
rtrN(config)# exit
rtrN# write memory                  (wr mem)
rtrN# exit                        (until you return to your pc)
```

Nous allons voir maintenant si ces changements ont eu un effet.

## 2. Essai de SNMP

Pour vérifier que l'installation SNMP est opérationnelle, exécutez la commande snmpstatus sur chacun des dispositifs suivants

```
$ snmpstatus -c 'NetManage' -v2c <IP_ADDRESS>
```

Où IP_ADDRESS correspond à la liste suivante :

```
* Le routeur de backbone :      10.10.0.254
* Le serveur NOC :              10.10.0.250
* Le routeur de votre groupe :  10.10.N.254
* Le commutateur du backbone :  10.10.0.253
* Les points d'accès :          10.10.0.251
```

## 3. SNMP Walk et OID

Vous allez maintenant utiliser la commande 'snmpwalk', qui fait partie de la boîte à outils SNMP, sur chacun des équipements testés plus haut afin de lister les tables associées aux OID ci-dessous :

```
.1.3.6.1.2.1.2.2.1.2
.1.3.6.1.2.1.31.1.1.1.18
.1.3.6.1.4.1.9.9.13.1
.1.3.6.1.2.1.25.2.3.1
.1.3.6.1.2.1.25.4.2.1
```

Vous essaierez avec deux variantes de la commande 'snmpwalk' :

```
$ snmpwalk     -c 'NetManage' -v2c <IP_ADDRESS> <OID>
```

et

```
$ snmpwalk -On -c 'NetManage' -v2c <IP_ADDRESS> <OID>
```

... où OID est l'un des trois OID listés ci-dessus : .1.3.6...

Remarque : l'option "-On" active l'affichage numérique, à savoir : aucune conversion OID <-> MIB de l'objet n'aura lieu.

Pour ces OID :

a) Tous les équipements répondent-ils ?

b) Avez-vous remarqué quelque chose d'important à propos de l'OID sur la sortie ?

## 4. Configuration de snmpd sur votre PC

Pour cet exercice, votre groupe doit vérifier que le service snmpd fonctionne et répond aux requêtes provenant des autres machines.

On comment par activer snmpd sur votre machine, puis on teste si votre machine répond, et enfin on vérifie chacune des machines des autres groupes.

- Installation de l'agent SNMP (démon):

## apt-get install snmpd

- Configuration:

  On va créer une sauvegarde de la configuration livrée en standard, puis on créera la notre.

## cd /etc/snmp

## mv snmpd.conf snmpd.conf.dist

## editor snmpd.conf

Ensuite, copiez/collez la section suivante (SAUF les lignes "– couper ici –")

```
-- couper ici -------------------------

#  Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161

# Configure Read-Only community and restrict who can connect
rocommunity NetManage  10.10.0.0/16
rocommunity NetManage  127.0.0.1

# Information about this host
sysLocation    NSRC Network Management Workshop
sysContact     sysadm@pcX.ws.nsrc.org

# Which OSI layers are active in this host
# (Application + End-to-End layers)
sysServices    72

# Include proprietary dskTable MIB (in addition to hrStorageTable)
includeAllDisks  10%

-- couper ici -------------------------
```

Sauver le fichier et quitter l'éditeur.

- Redémarrez snmpd

**service snmpd restart**

## 5. Vérifiez que snmpd fonctionne:

```
$ snmpstatus -c NetManage -v2c localhost
```

Qu'observez-vous ?

## 6. Testez vos voisins

Vérifiez maintenant que vous pouvez exécuter snmpstatus avec le serveur de votre voisin :

```
$ snmpstatus -c NetManage -v2c pcN.ws.nsrc.org
```

Par exemple, dans le groupe 5, vous pouvez tester avec:

- pc17.ws.nsrc.org
- pc18.ws.nsrc.org
- pc19.ws.nsrc.org
- pc20.ws.nsrc.org

## 8. Ajoutez des MIB

Lorsque vous aviez exécuté :

```
$ snmpwalk -c NetManage -v2c 10.10.0.1  .1.3.6.1.4.1.9.9.13.1
```

vous aviez peut-être remarqué que le client SNMP (snmpwalk) ne parvenait pas à interpréter tous les OID issus de l'agent :

```
SNMPv2-SMI::enterprises.9.9.13.1.3.1.2.1 = STRING: "chassis"
SNMPv2-SMI::enterprises.9.9.13.1.3.1.6.1 = INTEGER: 1
```

Qu'est-ce que "9.9.13.1.3.1" ?

Pour pouvoir interpréter cette information, nous devons télécharger des MIB supplémentaires :

Nous allons utiliser les MIBs suivantes (ATTENDEZ avant de les récupérer!)

```
MIB CISCO : ftp://ftp.cisco.com/pub/mibs/v2/CISCO-SMI.my
            ftp://ftp.cisco.com/pub/mibs/v2/CISCO-ENVMON-MIB.my
```

Pour faciliter les choses, nous avons un miroir local sur http://noc.ws.nsrc.org/mibs/

```
# apt-get install wget
# cd /usr/share/mibs
# mkdir cisco
# cd cisco

# wget http://noc.ws.nsrc.org/mibs/CISCO-SMI.my
# wget http://noc.ws.nsrc.org/mibs/CISCO-ENVMON-MIB.my

Il faut maintenant indiquer aux commandes snmp* qu'elles doivent
charger les MIBs Cisco. Donc, nous allons éditer le fichier
/etc/snmp/snmp.conf, et ajouter les deux lignes suivantes:

mibdirs +/usr/share/mibs/cisco
mibs +CISCO-ENVMON-MIB:CISCO-SMI
```

Enregistrez le fichier et quittez.

Faites maintenant un nouvel essai :

```
$ snmpwalk -c 'NetManage' -v2c 10.10.X.254  .1.3.6.1.4.1.9.9.13.1
```

Que remarquez-vous ?

## 8. SNMPwalk - le reste de la MIB-II

Essayez d'exécuter snmpwalk sur des hôtes (routeurs, commutateurs, machines) que vous n'avez pas encore testés, dans le réseau 10.10.0.X

Notez le type d'informations que vous pouvez obtenir.

```
$ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifDescr
$ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifAlias
$ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifTable | less
$ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifXTable | less
$ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifOperStatus
$ snmpwalk -c 'NetManage' -v2c 10.10.0.X ifAdminStatus
$ snmpwalk -c 'NetManage' -v2c 10.10.0.X if
```

(Avec la commande 'less', utilisez la touche espace pour la page suivante, 'b' pour la page précédente, et 'q' pour quitter).

Voyez vous une différence entre 'ifTable' et 'ifXTble' ?

Pouvez-vous expliquer la différence entre ifOperStatus et ifAdminStatus ? Pouvez-vous imaginer un scénario où cela pourrait être utile ?

## 9. Autres choses intéressantes dans les MIB-OID

- Utilisez SNMP pour examiner:

  ```
  a) les processus qui s'exécutent sur le serveur de votre voisin
     (hrSWRun)
  b) l'espace disque disponible sur le serveur de votre voisin
     (hrStorage)
  c) les interfaces sur le serveur de votre voisin (ifIndex, IfDescr)
  ```

  Pouvez-vous utiliser des noms abrégés pour parcourir ces tables OID ?

- Faites un essai avec la commande "snmptranslate", par exemple :

  ```
  $ snmptranslate .1.3.6.1.4.1.9.9.13.1
  ```

- Essayez avec différents OID