Université de Marne la Vallée
UFR Ingénieurs 2000

Kim Tuan DOAN
Ngoné DIOP

Filière Informatique et Réseaux
Deuxième année

[RAPPORT TP SNMP]

Année : 2006/2007

Introduction

L'étude de ce TP porte sur le protocole SNMP (Simple Network Management Protocol). C'est un protocole de supervision de réseau utilisé dans notre étude pour de la configuration et du contrôle d'éléments de réseau.

Dans ce TP nous allons étudier les outils mettant en œuvre le protocole du coté client et du coté serveur. Par la suite nous étudierons les outils de supervision de réseau ainsi que les alarmes.

I. Présentation de SNMP

SNMP est un protocole de supervision de réseaux. Il permet d'automatiser des mécanismes réseaux, de détecter des erreurs et apporte de la vérification par un SAL (Service Agreement Level). Il existe 3 types d'entités au niveau SNMP :

Les équipements managés

Les agents

Les stations de management

Les équipements managés sont des composants réseaux dont la couche applicative est sur SNMP. Ils agissent en tant que serveurs et s'occupent de répondre aux requêtes SNMP.

Les agents sont des éléments réseaux comportant une application chargée de fournir des informations et des fonctionnalités de gestion définies par une MIB d'un sous système donné.

Les stations de management sont des systèmes de management de réseau (Network Management Systems). Ce sont des clients SNMP fournissant des opérations d'administration.

Le protocole est basé sur un modèle réseau client - serveur. Il est basé sur de l'UDP où un agent est sur le port 161 et un manager sur le port 162. Chaque requête utilise un formatage SNMP v1 ou v2. La version 3 du protocole apporte de la sécurité.

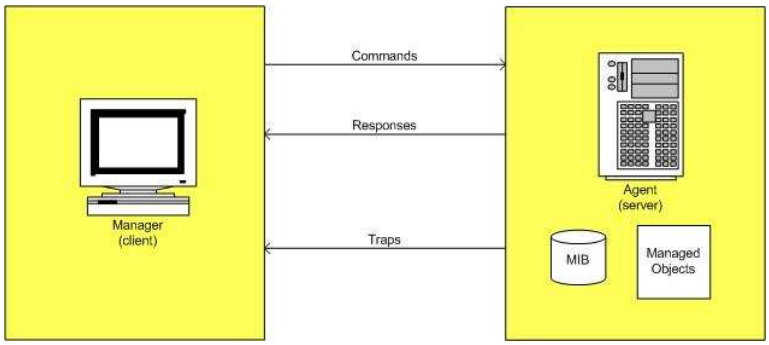


Figure 1 : Schéma de communication entre agent et superviseur

Une requête de client se fait par un envoi d'une commande (*GetRequest, GetNextRequest, SetRequest, GetBulk)* au serveur. La réponse de l'agent est toujours un *GetResponse*.

Les objets réseaux managés sont des données stockés dans une base d'informations de gestion MIB (Management Information Base). La MIB a une hiérarchie sous forme d'arbre, les branches correspondent aux catégories logiques et les feuilles correspondent aux informations sur les objets. Cette hiérarchie est similaire à l'arborescence des domaines Internet. MIB est décrite en ASN1 (Abstract Syntax Notation One) et est structurée en SMI (Structure of Management Information).

SNMP inclut une commande serveur -> client sans réponse nommée trap (alerte). Une alerte est produite lors d'un évènement non synchronisé, un dépassement de seuil par exemple.

II. Préliminaires

SNMP est un protocole basé sur la couche applicative. L'étude se fera à l'aide des logiciels Net-SNMP. Les machines d'étude utilisent une distribution Debian Linux. L'installation des outils se fait par la commande :

apt-get install snmp snmpd mbrowse

Le paquetage snmp comprend des outils client tels que snmpget, snmpset, snmpwalk, aussi un outil serveur snmpd (un serveur lançable en démon).

mbrowse est une interface graphique permettant d'explorer une MIB.

III. Configuration client (superviseur)

Un client SNMP se configure par un fichier de configuration nommé snmp.conf. Le paquetage snmp fournit un utilitaire de génération de fichier de configuration snmpconf.

Voici la procédure complète de configuration de notre client :

```
# snmpconf
The following installed configuration files were found:
   1:  ./snmp.conf
   2:  /etc/snmp/snmpd.conf
   3:  /etc/snmp/snmptrapd.conf
   4:  /usr/share/snmp/snmp.conf
   5:  /usr/share/snmp/snmptrapd.conf
Would you like me to read them in?   Their content will be
merged with the
output files created by this session.
Valid answer examples: "all", "none","3","1,2,5"
Read in which (default = all):
I can create the following types of configuration files for
you.
Select the file type you wish to create:
(you can create more than one as you run this program)
   1:  snmpd.conf
   2:  snmptrapd.conf
   3:  snmp.conf
Other options: quit
Select File: 3
```

L'utilitaire permet de générer une configuration pour serveur ou client. snmp.conf est le fichier utilisé par notre client.

```
The configuration information which can be put into snmp.conf
is divided
into sections.  Select a configuration section for snmp.conf
that you wish to create:
   1:  Debugging output options
   2:  Default Authentication Options
   3:  Output style options
   4:  Textual mib parsing
Other options: finished
Select section: 2
Section: Default Authentication Options
Description:
  This section defines the default authentication
  information.  Setting these up properly in your
  ~/.snmp/snmp.conf file will greatly reduce the amount of
  command line arguments you need to type (especially for
snmpv3).
Select from:
   1:  The default port number to use
   2:  The default snmp version number to use.
   3:   The default snmpv1 and snmpv2c community name to use
when needed.
   4:   The default snmpv3 security name to use when using
snmpv3
   5:  The default snmpv3 context name to use
   6:  The default snmpv3 security level to use
   7:  The default snmpv3 authentication type name to use
   8:  The default snmpv3 authentication pass phrase to use
   9:  The default snmpv3 privacy (encryption) type name to use
  10:  The default snmpv3 privacy pass phrase to use
Other options: finished, list
Select section:
Configuring: defversion
Description:
  The default snmp version number to use.
    override: with -v on the command line.
    arguments: 1|2c|3
Enter the default snmp version number to use (1|2c|3): 1
Finished Output: defversion  1
```

Nous définissons une version de protocole SNMP v1.

```
Configuring: defcommunity
Description:
  The default snmpv1 and snmpv2c community name to use when
needed.
    If this is specified, you don't need to include the
community
    name as an argument to the snmp applications.
    override: with -c on the command line.
    arguments: communityname
Enter the default community name to use: ig2k
Finished Output: defcommunity  ig2k
```

Nous définissons un nom de communauté utilisé pour l'authentification de client. Un défaut majeur de la version 1 de SNMP est que le nom de communauté est transmit en clair.

```
Select section: 4
Section: Textual mib parsing
Description:
  This section controls the textual mib parser.  Textual
  mibs are parsed in order to convert OIDs, enumerated
  lists, and ... to and from textual representations
  and numerical representations.
Select from:
   1:  Specifies directories to be searched for mibs.
   2:  Specifies a list of mibs to be searched for and loaded.
   3:  Loads a particular mib file from a particualar path
   4:   Should errors in mibs be displayed when the mibs are
loaded
   5:   Should warnings about mibs be displayed when the mibs
are loaded
   6:  Be strict about about mib comment termination.
   7:  Should underlines be allowed in mib symbols (illegal)
   8:  Force replacement of older mibs with known updated ones
Other options: finished, list
Select section: 1
Configuring: mibdirs
Description:
  Specifies directories to be searched for mibs.
    Adding a '+' sign to the front of the argument appends the
new
    directory to the list of directories already being
searched.
    arguments: [+]directory[:directory...]
Enter the list of directories to search through for mibs:
/usr/share/snmp/mibs:/tmp/mibs/
Finished Output: mibdirs  /usr/share/snmp/mibs:/tmp/mibs/
```

Nous personalisons les répertoires des fichiers de description MIB et SMI.

```
Select section: 2
Configuring: mibs
Description:
  Specifies a list of mibs to be searched for and loaded.
    Adding a '+' sign to the front of the argument appends the
new
    mib name to the list of mibs already being searched for.
    arguments: [+]mibname[:mibname...]
Enter the list of mibs to read: +ALL
Finished Output: mibs  +ALL
```

Les répertoires précédemment sont chargés par défaut par l'option +ALL.

IV. Installation de l'agent SNMP sur un routeur

Pour mettre en place un réseau supervisé afin d'y réaliser des tests et donc comprendre le fonctionnement du protocole SNMP, la configuration d'un agent va être effectuée sur un routeur Cisco 2500. Ce dernier est déjà équipé d'un agent SNMP. Chaque équipement que l'on voudrait manager à distance devrait disposer d'un agent SNMP. Cet agent est un serveur, c'est à dire qu'il reste à l'écoute du port UDP 161 pour répondre aux requêtes (*get*) ou aux demandes de modifications de l'administrateur (*set*).

La configuration de cet agent sera détaillée en 2/. Mais cette dernière sera précédée d'une configuration du routeur visant à le rendre fonctionnel sur notre réseau local. Cette opération ne nécessitant pas de routage, il ne sera ainsi pas nécessaire d'activer des protocoles de routage mais pour l'utilisation de SNMP, une sécurisation sera nécessaire.

1. Configuration du routeur

La configuration du routeur se fait par son interface console, laquelle sera connectée à un ordinateur par son port série. Cet ordinateur va accéder à l'interface de configuration du routeur à l'aide du logiciel « **minicom** ». Il s'agit d'un programme de communication qui émule un hyper terminal et permettant d'administrer un équipement connecté sur le port série d'un ordinateur sous Unix par l'intermédiaire de terminal. Pour le lancer, il faut taper la commande « **minicom –o** » :

Figure 2 : Lancement de l'interface de configuration du routeur

Nous voyons qu'il est possible de connecter notre router avec les données figurant dans la partie basse de l'écran : 9600 bauds de débit, 8 bits sans parité, 1 bit de stop et sans contrôle de flux (NOR). « **Router>** » nous montre que nous accédons à l'interface de configuration du routeur.

Maintenant que le routeur est démarré, nous allons le réinitialiser pour obtenir un routeur vierge qui nous permettra de réaliser nos tests sans contrainte. Il faut pour cela taper la commande « **erase startup-config** » puis « **reload** ».

Un mot de passe pour sécuriser l'accès au routeur est nécessaire. Il faut pour cela entrer dans le mode super utilisateur avec « **enable** » puis « **configure terminal** » pour entrer dans le panneau de configuration général du routeur. Dans ce "menu", il faut taper « **enable secret "cisco" », "cisco"** étant le mot de passe que l'on souhaite attribuer.

Le routeur doit apparaître sur le réseau. Pour cela, nous configurons son interface ethernet avec l'adresse IP 192.168.1.1 avec le masque par défaut. Depuis le menu "configure terminal", il faut accéder à un sous menu qui permet de configurer une interface donnée. Pour l'interface ethernet, il faut taper « **interface ethernet 0** ». Pour lui assigner une adresse IP, il faut taper « **ip address 192.168.1.1 255.255.255.0** ». Il faut ensuite le lancer en tapant « **no shutdown »**.

Nous allons procéder à une dernière configuration qui aura pour but de permettre la connexion du routeur en **telnet**. Cette configuration consiste à mettre un mot de passe spécifique pour **telnet**.

Il faut d'abord quitter la configuration de l'interface ethernet avec la séquence de touches « Ctrl + Z » ou taper « **end »** pour revenir dans le menu configuration terminal. De puis ce menu, il suffit de taper la commande « **line vty 0 4** » pour configurer un maximum de cinq sessions telnet simultanées, puis la commande « **password "cisco" »** pour spécifier un mot de passe (ici cisco) et enfin « **login »** pour activer l'accès.

Une fois toute la configuration du routeur effectué, il sauvegarder la configuration en tapant « **write »** dans le menu principal (taper deux fois Ctrl+Z pour arriver au menu principal). Il faut à présent configurer l'agent SNMP.

2. Configuration d'un agent sur le routeur

Comme spécifié ci-dessus, l'agent va écouter les demandes du client, l'administrateur et réaliser les actions demandées. Les commandes de configuration de l'agent commencent toutes par « **snm-server** » et les commandes de visu de statistiques par « **show snmp ».** Pour l'activation et la configuration de l'agent sur notre routeur nous allons suivre les étapes suivantes :

2.1 Configuration générale

Cette configuration concerne les parties générales du matériel. On peut noter

- La dénomination du matériel
- Sa localisation qu'on peut spécifier avec la commande « **snmp-server location IG2K – Salle de TP Réseau 2059 »**
- Les informations qui vont permettre de contacter l'administrateur du matériel « **snmp-server contact root@ig2k.fr »**

2.2 Positionnement des droits d'accès au MIB du matériel

Nous avons la possibilité de spécifier des droits de lecture et/ d'écriture. La communauté « ig2k » aura le droit de lire toutes les informations alors que la communauté "secret" aura en plus le droit d'écriture dans la base de données.

- Pour la lecture il suffit de taper « **snmp-server community ig2k RO »** RO est l'attribut de cette directive qui spécifie la lecture seule.
- L'écriture étant sensible nous décidons de le limiter à un seul ordinateur, la console de supervision qui a pour adresse « 192.168.1.2 ». On aura alors deux actions à effectuer
    - Restriction au PC console : « **access-list 1 permit 192.168.1.2 »**

- Attribution du droit d'écriture à la communauté « secret » : « **snmp-server community secret RW 1 »**. RW 1 spécifie la lecture et l'écriture à la liste 1 spécifié ci-dessus.

2.3 La gestion des alarmes

Le superviseur dispose d'un serveur qui reste à l'écoute, sur le port UDP 162, des éventuels signaux d'alarme. Ces alarmes sont des alertes à l'initiative de l'agent. Par exemple, il pourra émettre une alerte si le débit sur une interface réseau atteint une valeur considérée par l'administrateur comme critique. Il peut y avoir une multitude d'alertes possibles, suivant la complexité de l'agent. La température du processeur, le taux d'occupation des disques durs, le taux d'occupation CPU...

Pour notre routeur on souhaiterait diriger les alarmes vers la communauté « ig2k » sur la machine « 192.168.1.2 ». Cela se fait avec la commande « **snmp-server host 192.168.1.2 ig2k »**. Il faudra également choisir l'interface par laquelle les traps (alarmes) devront être envoyés, en l'occurrence l'interface « ethernet 0 » est celle qui est choisie : « **snmp-server trap-source ethernet 0** ».

Depuis l'interface « ethernet 0 » et à destination de l'adresse IP « 192.168.1.2 », toutes les alarmes vont être activées par la commande « **snmp-server enable traps** ».

IV. Utilisation des outils sur le Superviseur (manager)

Maintenant que le routeur configurer on peut faire des tests de requêtes et des demandes de modifications depuis le superviseur. Pour fournir ces services, le protocole SNMP propose les directives suivantes :

- get-request Le Manager SNMP demande une information à un agent SNMP
- get-next-request Le Manager SNMP demande l'information suivante à l'agent SNMP
- set-request Le Manager SNMP met à jour une information sur un agent SNMP
- get-reponse L'agent SNMP répond à un *get-request* ou a un *set-request*

Sous Linux des outils de requêtes et des outils de modification des données sont disponibles. Ces outils sont tous sous la bannière de la commande générique snmpcmd qui est une sorte d'interface qui définit les commandes spécifiques pour interroger un agent SNMP.

1. Les commandes de requêtes

Il s'agit essentiellement des commandes sui vont permettre de récupérer des informations sur la MIB de la machine managée à laquelle on s'adresse. Deux catégories de commandes peuvent être distingués : les commandes qui permettent de lire des informations (**get*), et les commandes qui permettent d'afficher l'arborescence d'un nœud de la MIB.

- *snmptranslate* permet de traduire les objets contenus dans MIB en information lisible, c'est-à-dire en texte et en valeurs numérique. L'exemple suivant permet de déterminer le nom complet de l'objet sysUpTime et son numéro mais également le fichier de MIB ou la définition de cet objet se trouve.

```
# snmptranslate -IR -On -Td sysUpTime
.1.3.6.1.2.1.1.3
sysUpTime OBJECT-TYPE
  -- FROM       SNMPv2-MIB, RFC1213-MIB
  SYNTAX        TimeTicks
  MAX-ACCESS    read-only
  STATUS        current
  DESCRIPTION   "The time (in hundredths of a second) since the
                network management portion of the system was last
                re-initialized."
::=  {  iso(1)  org(3)  dod(6)  internet(1)  mgmt(2)  mib-2(1)
system(1) 3 }
```

- *snmpwalk* permet de lister les tous les éléments contenus dans un nœud. Nous l'utilisons ici pour parcourir l'arbre partant du nœud system. Nous notons ainsi la présence de sysUpTime dans ce noeud.

```
# snmpwalk 192.168.1.1 system
SNMPv2-MIB::sysDescr.0 = STRING: Cisco Internetwork Operating
System Software
IOS (tm) 3000 Software (IGS-I-L), Version 11.1(24a), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Fri 09-Mar-01 19:43 by pnicosia
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.30
SNMPv2-MIB::sysUpTime.0 = Timeticks: (211874) 0:35:18.74
SNMPv2-MIB::sysContact.0 = STRING: root@ig2k.fr
SNMPv2-MIB::sysName.0 = STRING: Router
SNMPv2-MIB::sysLocation.0 = STRING: IG2K - Salle Reseau 2059
SNMPv2-MIB::sysServices.0 = INTEGER: 6
```

- *snmpget* et *snmpgetnext* : *snmpget* permet de récupérer un objet SNMP en précisant une instance si l'objet existe en plusieurs exemplaires alors que *snmpgetnext* permet de récupérer le premier objet d'un nœud sans préciser l'instance. Dans l'exemple ci-dessous, on récupère la même information (l'adresse physique correspondant à l'interface ayant l'adresse logique **192.168.1.1)** en utilisant ces deux commandes.

```
# snmpget -c ig2k 192.168.1.1
interfaces.ifTable.ifEntry.ifPhysAddress.1
IF-MIB::ifPhysAddress.1 = STRING: 0:10:7b:81:bf:34

# snmpgetnext -c ig2k 192.168.1.1
interfaces.ifTable.ifEntry.ifPhysAddress
IF-MIB::ifPhysAddress.1 = STRING: 0:10:7b:81:bf:34
```

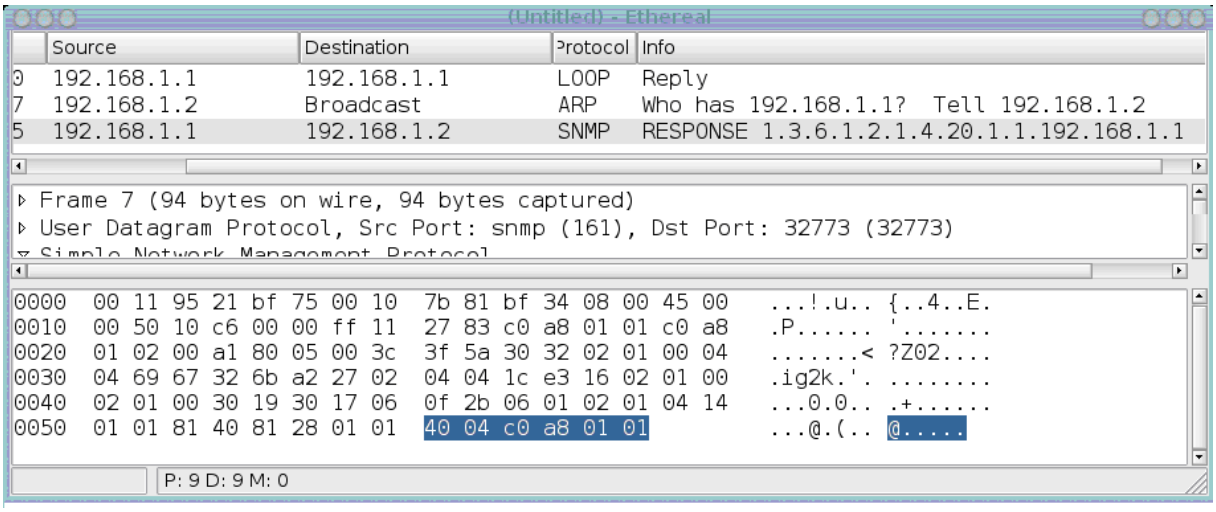
2. Modifications

- *snmpset* permet de faire des modifications en configurant un objet SNMP. Nous avons configuré l'agent sur le routeur pour qu'il n'accepte les requêtes de modifications provenant uniquement de la communauté "secret". Dans l'exemple ci-dessous, nous changeons la valeur de l'objet location.

```
# snmpset -c secret 192.168.1.1 system.sysLocation.0 s test
SNMPv2-MIB::sysLocation.0 = STRING: test
```

3. Format des réponses

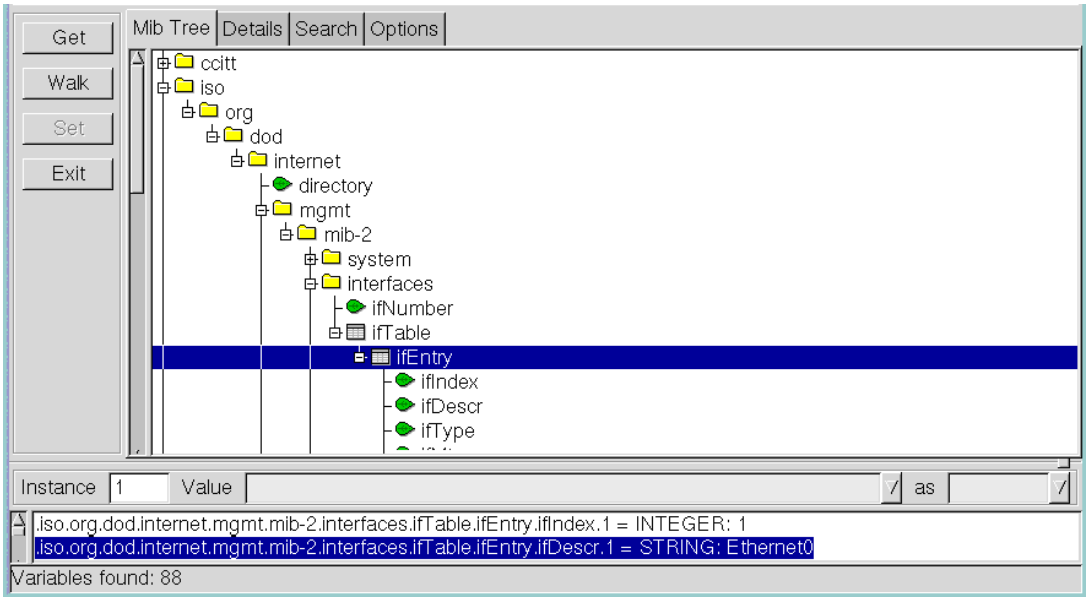
Les réponses envoyées par les agents sont codées au format ASN-1. Il s'agit d'une notation formelle qui permet de spécifier les données transmises par les protocoles de télécommunications indépendamment des langages informatiques et de la représentation physique de ces données, pour toutes sortes d'applications communicantes et de données aussi complexes (ou aussi simples) soient-elles.



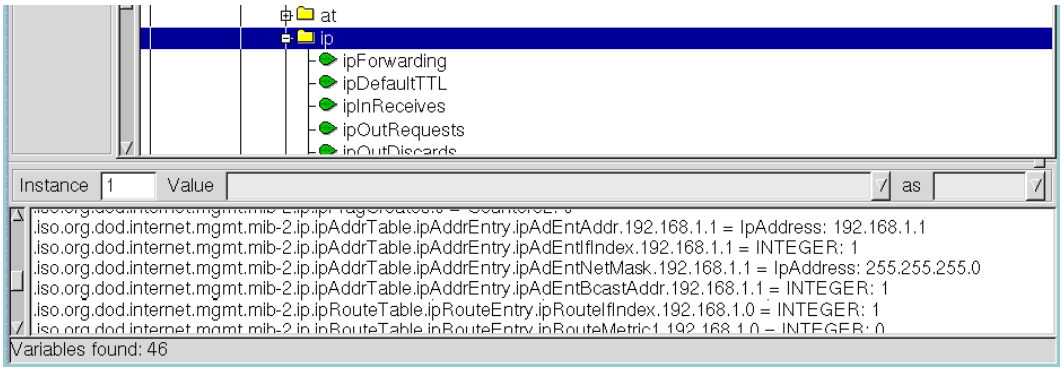
4. L'outil graphique « mbrowse »

Les commandes citées ci-dessus sont fournies dans l'outil graphique « mbrowse ».

L'exemple ci-dessous permet de faire l'équivalent de la commande « snmpwal » sur l'objet ifEntry.



L'exemple ci-dessous permet de faire l'équivalent de la commande « snmget » sur le nœud ip.



L'exemple ci-dessous permet de désactiver 'interface Ethernet 0.