Emilie MATHIEU
Sabrina VALETTE
Benoit BENEZECH

Luc ESCHBACH
Thierry VOURIOT
Camille DARNET

PoucanKi

CAS 0 - Sujet 4

SNMP : SIMPLE NETWORK MANAGEMENT PROTOCOLE

DESS Informatique

Février 2004

SOMMAIRE

Sujet

Récupération des traps SNMP sur station Windows ou Linux.
Vous devez installer sur votre station NT le service SNMP. Vous devez ensuite spécifier et réaliser une petite application récupérant des traps publiques et privées pouvant être générées.

Introduction

Dans l'histoire des réseaux, la gestion a toujours été une discipline en retard sur les autres tâches à effectuer. Logiquement, un réseau est d'abord mis sur pied pour la transmission et la commutation d'informations.

Dans un premier temps, la gestion est simple, et peut se faire avec les moyens du bord (gestion individuelle des composants). Lorsque le réseau devient complexe, le nombre de composantes s'accroît souvent exponentiellement, et l'opérateur tend à perdre la vue d'ensemble de son réseau. Il n'est dès lors plus possible d'exploiter rationnellement le réseau sans disposer d'un ensemble d'outils qui permettent de générer une vue synthétique de certains aspects du réseau, et de mettre en évidence d'éventuelles difficultés.

Les cinq domaines fonctionnels de l'administration tels que définis dans l'OSI:

- **La gestion des pannes :** permet la détection, la localisation, la réparation de pannes et le retour à une situation normale dans l'environnement.
- **La comptabilité** : permet de connaître les charges des objets gérés, les coûts de communication, ... Cette évaluation est établie en fonction du volume et de la durée de la transmission. Ces relevés s'effectuent à deux niveaux : Réseau et Application.
- **La gestion des configurations** : permet d'identifier, de paramétrer les différents objets. Les procédures requises pour gérer une configuration sont la collecte d'information, le contrôle de l'état du système, la sauvegarde de l'état dans un historique.
- **L'audit des performances** : permet d'évaluer les performances des ressources du système et leur efficacité. Les performances d'un réseau sont évaluées à partir de quatre paramètres : le temps de réponse, le débit, le taux d'erreur par bit et la disponibilité.
- **La gestion de la sécurité :** une des fonctions de gestion concerne le contrôle et la distribution des informations utilisées pour la sécurité. Un sous-ensemble de la MIB concerne les informations de sécurité (SMIB). Il renferme le cryptage et la liste des droits d'accès.

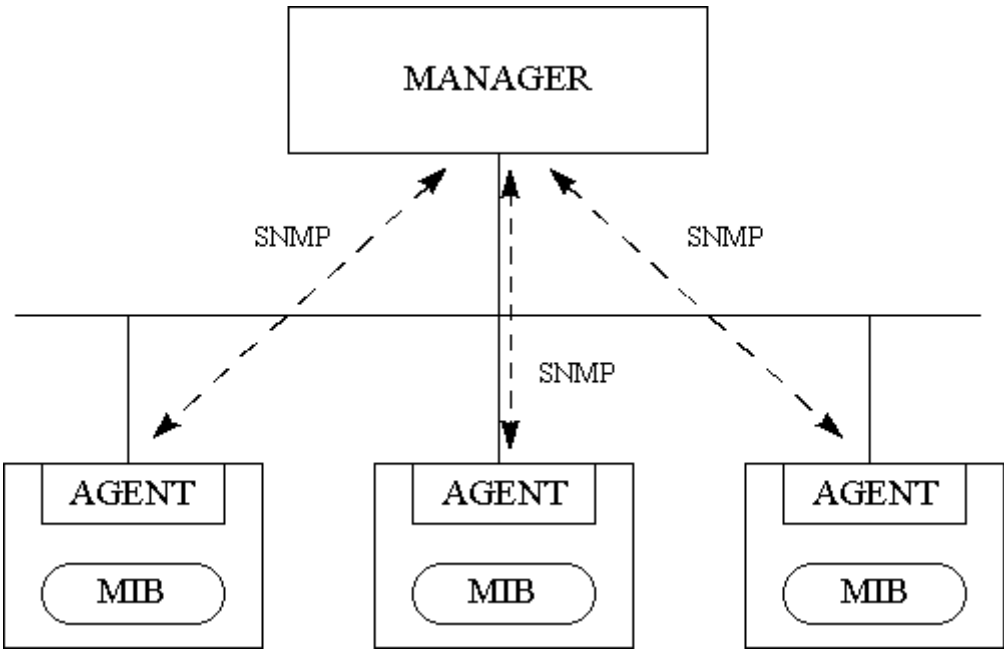
Description de SNMP

SNMP est un protocole, comme son nom l'indique, pour effectuer de la gestion de réseau. Il permet de contrôler un réseau à distance en interrogeant les stations qui en font partie sur leur état et en modifiant leur configuration, de faire des tests de sécurité et d'observer différentes informations liées à l'émission de données. Il peut même être utilisé pour gérer des logiciels et bases de données à distance. Depuis qu'il est devenu un standard TCP/IP, son utilisation a beaucoup augmenté. D'ailleurs, il est le protocole le plus utilisé pour gérer des équipements de réseau (routeurs, ponts, etc.) et beaucoup de logiciels de gestion de réseau sont basés sur ce protocole.

Principe :

SNMP fonctionne à partir de quatre éléments :

- les **MIBs (Management Information Base)**;
- les **agents**;
- le **manager**;
- le protocole **SNMP**.



Chaque noeud administrable du réseau (équipements et stations) possède une base de données contenant des informations locales au noeud, appelée **Management Information Base**. Un **agent** sur le noeud se charge de collecter les informations en réponse aux interrogations d'un **manager**. L'agent peut prendre l'initiative de la communication avec un manager en lui envoyant des Traps pour signaler des évènements anormaux (alarmes).

Le transport des informations entre les agents et le manager se fait à l'aide du protocole SNMP (Simple Network Management Protocol).

Management Information Base (MIB) :

Une MIB définit les informations spécifiques d'administration réseaux et leur signification. Elle est composée d'un ensemble de valeurs et paramètres manipulables par le système d'administration. Les informations disponibles sont de type :

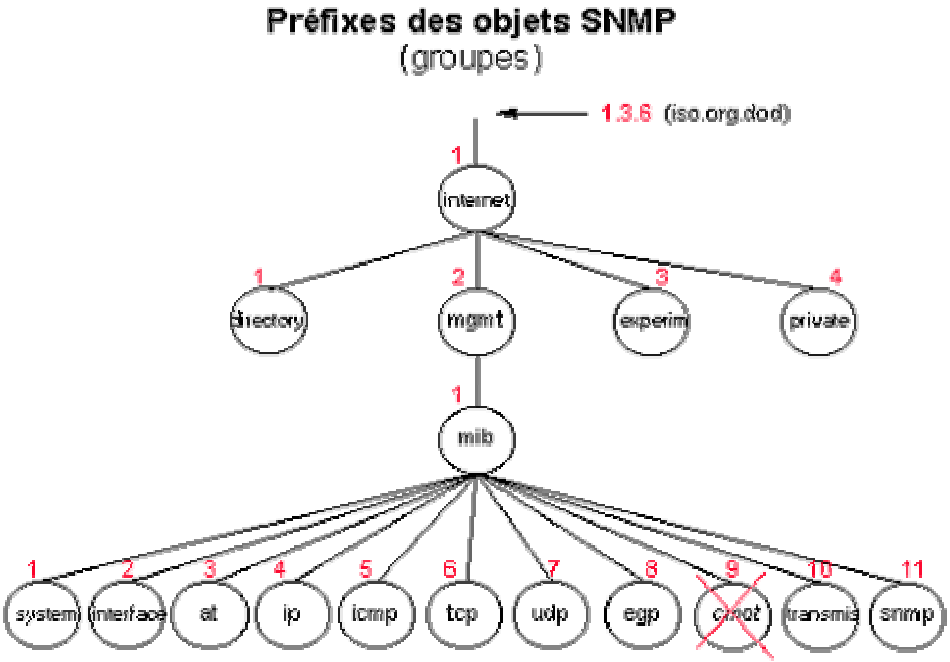
- statiques : nom, constructeur, version d'un équipement;
- dynamiques : état à un instant donné;
- statistiques : compteurs, trafic depuis la mise en route de l'équipement.

Chaque noeud (ponts, routeurs, ...) est représenté par un ensemble de variables. La définition et l'identification de ces variables sont précisées par la norme **SMI** (Structure of Management Information).

Le standard est défini dans la RFC1213.

L'arborescence MIB-2 :

Les informations stockées dans la MIB sont rangées dans une arborescence. L'arborescence MIB-2 est une évolution de la MIB disposant d'objets supplémentaires. Elle constitue une branche du groupe **iso.org.dod.internet.mgmt**.



Groupe	Commentaires
system	Informations générales sur le système.
interfaces	Informations sur les interfaces entre le système et les sous-réseaux.
at	Table de traduction des adresses entre internet et les sous-réseaux.
ip	Informations relatives à l'implantation et à l'exécution d'IP (Internet Protocol).
icmp	Informations relatives à l'implantation et à l'exécution de ICMP (Internet Control Message Protocol).
tcp	Informations relatives à l'implantation et à l'exécution de TCP (Transmission Control Protocol).
udp	Informations relatives à l'implantation et à l'exécution de UDP (User Datagram Protocol).
egp	Informations relatives à l'implantation et à l'exécution de EGP (Exterior Gateway Protocol).
transmission	Informations sur la transmission et sur les protocoles utilisés par chaque interface.
snmp	Informations relatives à l'implantation et à l'exécution de SNMP.

Object identifier :

Les variables de la MIB-2 sont identifiées par le chemin dans l'arborescence, noté de deux façons :

- à l'aide des noms de groupes : **iso.org.dod**
- à l'aide des numéros des groupes : **1.3.6**.

Les MIBs propriétaires :

La description de l'arborescence MIB est normalisée par l'ISO mais certains constructeurs d'équipements réseaux ont défini des branches supplémentaires afin d'y inclure des informations spécifiques à leur matériel. Ces branches sont appelées **MIBs propriétaires**.

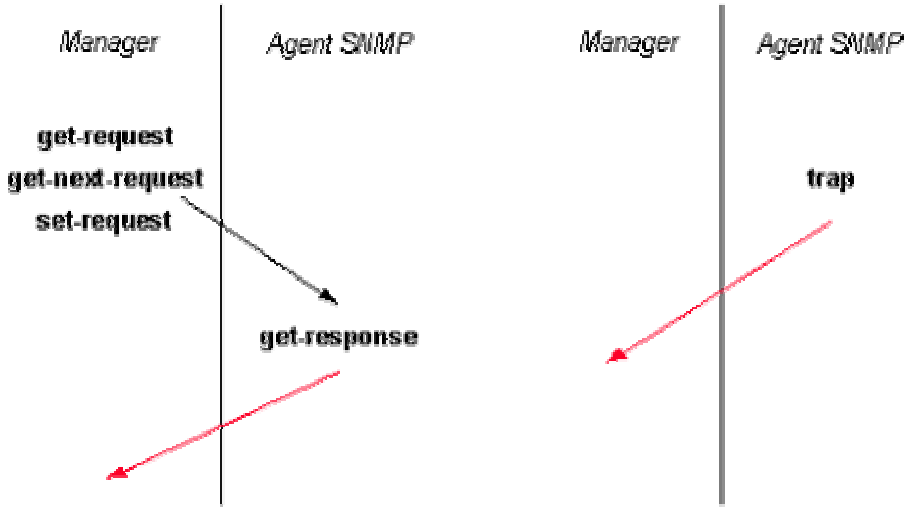
Les MIBs propriétaires sont consultables par des managers spécifiques qui peuvent fonctionner de façon autonome (SPECTRUM de Cabletron) ou être intégrés aux plates-formes du marché.

Protocole SNMP :

Le protocole SNMP est chargé d'assurer le transport d'informations entre le manager et les agents. Il doit prendre en compte :

- la scrutation des agents : le manager (station administration) questionne les différents agents.
- la remontée des alarmes en provenance des agents.

Ces fonctions sont assurées par cinq primitives de service :

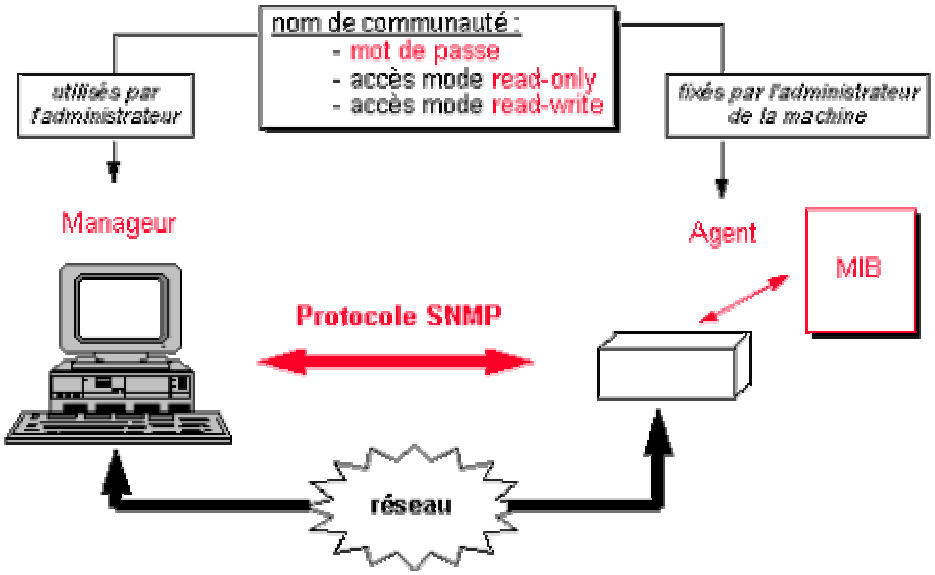


Primitives	Descriptions
GetRequest	le manager demande une information à l'agent
GetNextRequest	le manager demande l'information suivante à l'agent
SetRequest	le manager initialise une variable de l'agent
GetResponse	l'agent retourne l'information au client
Trap	interruption - l'agent envoie une information à un client

Les noms de communautés :

L'accès aux informations des MIBs est contrôlé par un mécanisme simple utilisant des noms de communautés. Un nom de communauté peut être assimilé à un mot de passe connu par l'agent et utilisé par le manager pour se faire reconnaître. Les noms de communautés sont configurés sur l'agent et autorisent trois types d'accès sur les variables de la MIB gérées par l'agent :

- Pas d'accès
- Read-Only
- Read-Write.



Le nom de communauté circule en clair sur le réseau. Beaucoup d'administrateurs préfèrent ainsi limiter l'accès sur les MIBs en lecture seule et se déplacent sur les équipements pour modifier certaines valeurs.

Les agents SNMP :

L'agent SNMP collecte les informations de la MIB de l'équipement et répond aux requêtes du manager. On trouve maintenant des agents SNMP sur tout équipement dit administrable. Les constructeurs fournissent également des agents pour les stations du réseau.

Toutefois, certains anciens équipements administrables ne sont pas conformes à SNMP. Dans ce cas, il peut être possible d'utiliser un proxy-agent sur un équipement SNMP, qui va servir d'intermédiaire avec l'équipement non SNMP.

Les managers SNMP :

Les managers sont chargés de questionner les agents et de fournir à l'administrateur les informations récupérées. Ils doivent également gérer les Traps et prévenir l'administrateur.

Les outils SNMP vont du simple "browser" de MIB qui permet juste de lire les variables, jusqu'à la plate-forme d'administration qui peut les afficher de façon pertinente sur des cartes du réseau.

Le marché des plates-formes d'administration est réparti entre deux grandes familles :

- les constructeurs de systèmes distribués (HP, BULL, IBM) :
  - HP Openview (pour Unix ou Windows NT)
  - ISM
  - Tivoli
- Les constructeurs de solutions pour réseaux locaux
  - Novell Network Management System

SNMP versions 1, 2 et 3 :

Il existe 3 versions du protocole SNMP : SNMPv1, SNMPv2 et SNMPv3.

SNMP v1 en 1987 :
Volonté de simplicité :
- protocole non-connecté, fonctionne avec un réseau déficient sans l'encombrer
- asynchrone
- le nom de la communauté circule en clair

→ Problème de sécurité

SNMP v2 en 1993 :
Meilleure sécurité :
- transport avec authentification
- chiffrement des données possible

→ version peu répandue, n'a jamais percé sur le marché

SNMP v3 en 1998 :
Modèle se voulant plus général, incluant les autres versions :
- d'avantage d'informations pour identifier les différentes entités
- sécurité accrue, avec des droits d'utilisateurs

→ Version en pleine expansion

Installation et configuration du service SNMP

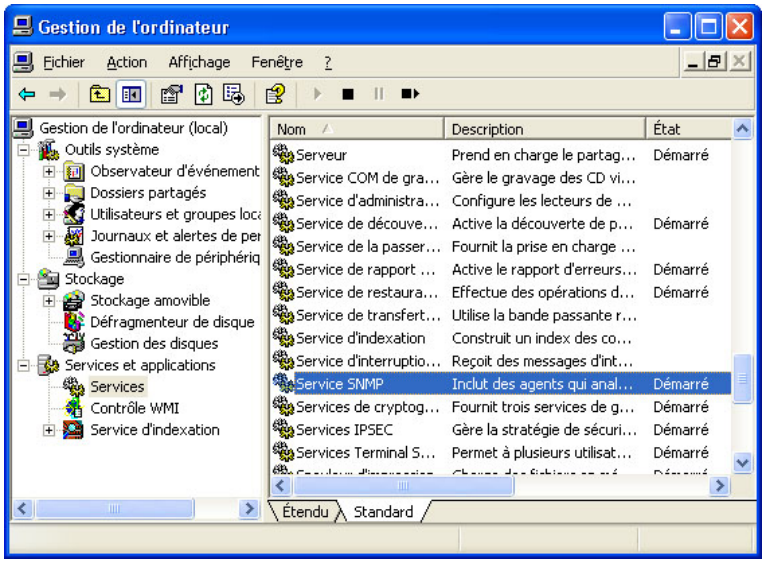
Sous Windows XP :

Installation :

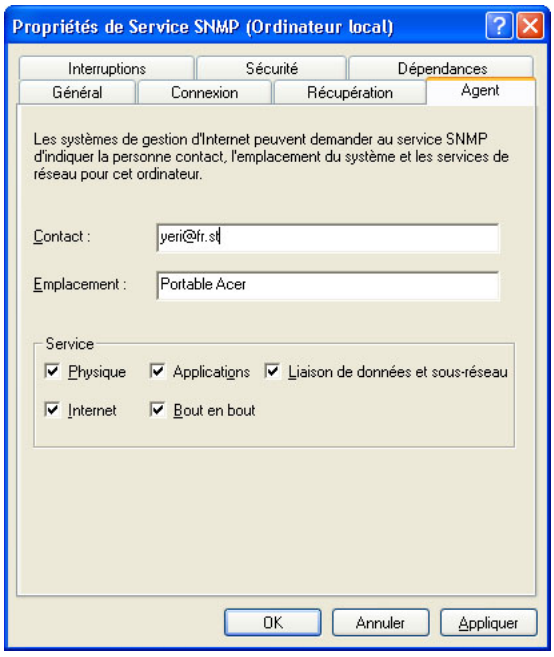
Allez dans le panneau de configuration :

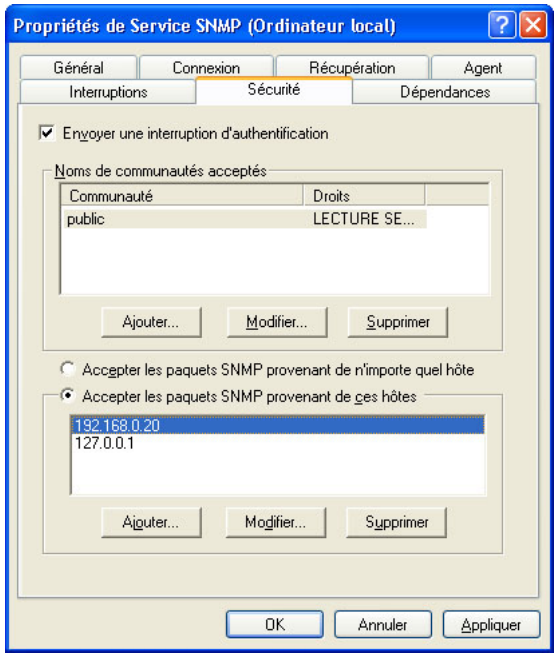
- Ajout/suppression de logiciels,
- ajouter ou supprimer des composants Windows,
- sélectionnez "Outils de gestion et d'analyse",
- cliquez sur "Détails",
- cochez "SNMP (Protocole simplifié de gestion de réseaux)"

Configuration :



Ouvrir le service SNMP dans la liste des services de Windows. Ensuite il suffit de remplir les champs *Contact* et *Emplacement* dans l'onglet *Agent*. Puis dans l'onglet Sécurité, on ajoute une nouvelle communauté publique avec les droits en lecture seule. On peut également ajouter une autre communauté avec des droits en écriture. Enfin on spécifie les adresses IP des machines qui communiqueront avec l'agent SNMP.





Sous Linux :

Installation :

Il suffit d'installer les paquets NET-SNMP et NET-SNMP UTILS.
Site web: http://net-snmp.sourceforge.net

Configuration:

La configuration est faite pour que :

- Toute machine du LAN puisse lire la totalité de la MIB, à travers la communauté "public"
- Seule la machine locale puisse écrire, à travers la communauté "private".

Commencez par sauvegarder le fichier `/etc/snmp/snmpd.conf` qui a été créé avec l'installation.

Créez ensuite un nouveau fichier `/etc/snmp/snmpd.conf` comme suit :

```
# 1° créer des relations entre les communautés et des noms de sécurité
#           nom.secu    source            communaute
com2sec     Local       localhost         private
com2sec     LocalNet    192.168.0.0/24    public

# 2° créer des relations entre des noms de groupes et les noms de sécurité
#           nom.groupe  version           nom.secu
group       RWGroup     v1                Local
group       ROGroup     v1                LocalNet

# 3° Créer les diverses vues qui seront autorisées aux groupes
#
view        tout        included          .1

# 4° Indiquer les accès aux vues suivant les groupes
#    nom.groupe contexte modele.secu niveau.secu prefixe lecture ecriture
notification
access ROGroup "" v1 noauth exact tout none none
access RWGroup "" v1 noauth exact tout tout none
```

Relancez le démon SNMP par la commande : `/etc/init.d/snmps restart`

Application SNMPManager

Développement :

Le choix du langage de programmation fût très rapidement effectué. En effet, le langage Java a été choisi pour de nombreuses raisons :

- nous avions déjà une bonne connaissance de ce langage
- portabilité des applications sur toutes les plates-formes (Windows, Unix, Linux, Macintosh, ….).
- programmation orientée objet qui permet un meilleur découpage de l'application.
- API Swing permettant la création d'interfaces graphiques très rapidement.
- réutilisation de packages déjà développés dans d'autres applications

Pour la communication avec les agents SNMP on utilise un package Java open source développé par Jonathan Sevy. Ce package contient notamment les différents types de données utilisés par SNMP, ainsi que des classes permettant l'envoi de requêtes GET et SET. De plus une interface nous permet de capturer les traps SNMP.

Ce package utilise la version 1 de SNMP qui est compatible avec les autres versions de SNMP puisque celle-ci est une sous-couche versions 2 et 3.

Les classes du package SNMP : (extrait de la javadoc)

Class Summary	
SNMPBERCodec	SNMPBERCodec defines methods for converting from ASN.1 BER encoding to SNMPObject subclasses.
SNMPBitString	Class representing a general string of bits.
SNMPCounter32	Defines a 32-bit counter, whose value wraps if initialized with a larger value.
SNMPCounter64	Defines a 64-bit counter, whose value wraps if initialized with a larger value.
SNMPGauge32	Defines a 32-bit gauge, whose value "pegs" at the maximum if initialized with a larger value.
SNMPInteger	Defines an arbitrarily-sized integer value; there is no limit on size due to the use of Java.lang.BigInteger to store the value internally.
SNMPIPAddress	Class to hold IP addresses; special case of SNMP Octet String.
SNMPMessage	Defines the SNMPMessage class as a special case of SNMPSequence.
SNMPNSAPAddress	Defines class for holding physical 6-byte addresses.
SNMPNull	Object representing the SNMP Null data type.
SNMPObject	Abstract base class of all SNMP data type classes.

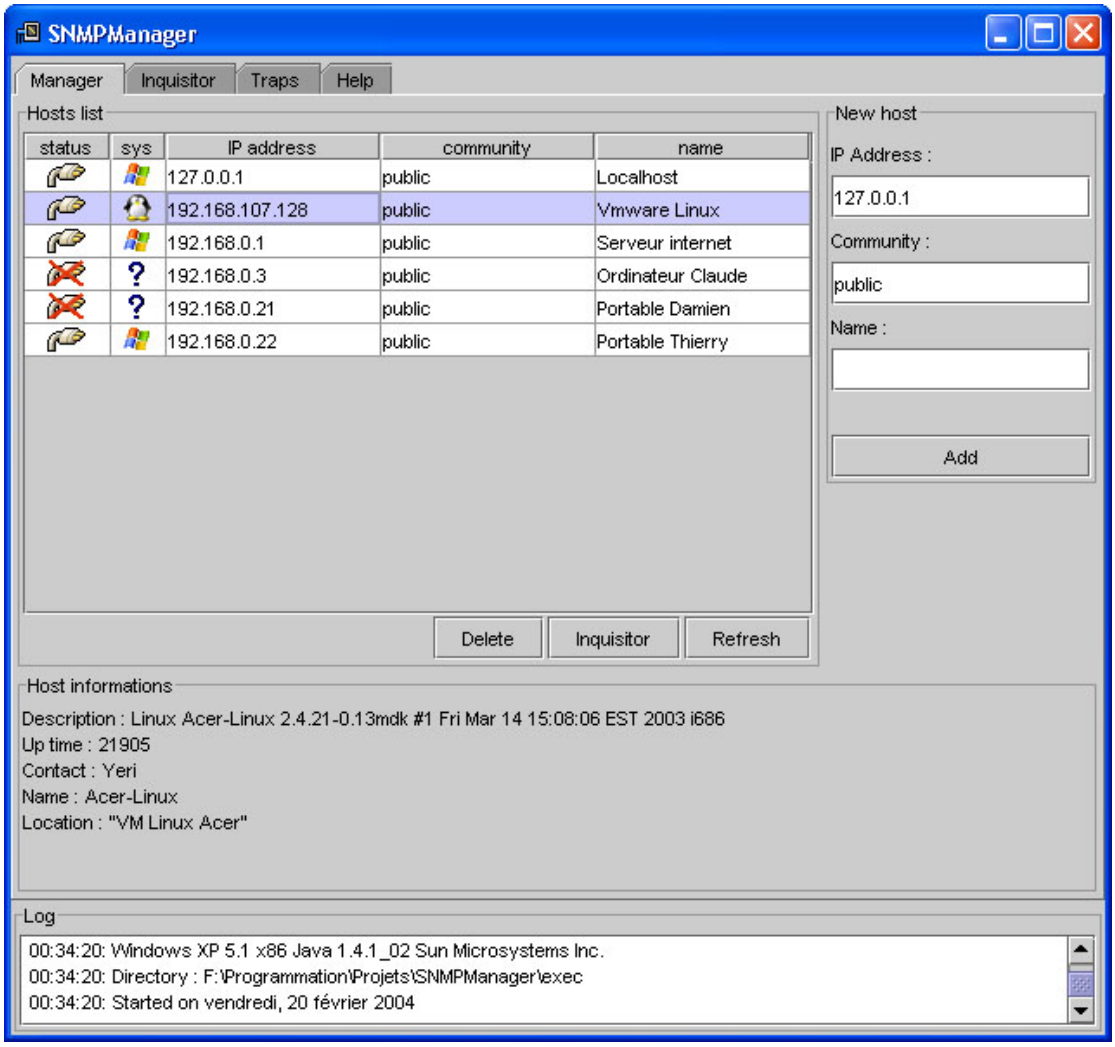
SNMPObjectIdentifier	Class representing ASN.1 object identifiers.
SNMPOctetString	Class representing a general string of octets.
SNMPPDU	The SNMPPDU class represents an SNMP PDU from RFC 1157, as indicated below.
SNMPSequence	One of the most important SNMP classes.
SNMPTimeTicks	SNMP datatype used to represent time value.
SNMPTrapPDU	The SNMPTrapPDU class represents an SNMP Trap PDU from RFC 1157, as indicated below.
SNMPUInteger32	Defines a 32-bit unsigned integer value; wraps if initialized with a larger value.
SNMPUnknownObject	Used when an unknown SNMP object type is encountered.
SNMPv1AgentInterface	The class SNMPv1AgentInterface implements an interface for responding to requests sent from a remote SNMP manager.
SNMPv1CommunicationInterface	The class SNMPv1CommunicationInterface defines methods for communicating with SNMP entities.
SNMPv1TrapListenerInterface	The class SNMPv1TrapListenerInterface implements a server which listens for trap messages sent from remote SNMP entities.
SNMPv1TrapSenderInterface	The class SNMPv1TrapSenderInterface implements an interface for sending trap messages to a remote SNMP manager.
SNMPVarBindList	The SNMPVarBindList class is a specialization of SNMPSequence that contains a list of SNMPVariablePair objects.
SNMPVariablePair	The SNMPVariablePair class implements the VarBind specification detailed below from RFC 1157.

Manuel utilisateur :

L'interface de SNMPManager utilise une représentation sous la forme de trois onglets ; Manager, Inquisitor, Traps.
Un log, en bas de l'interface, tient au courant l'utilisateur sur les traitements en cours ainsi que sur les éventuelles erreurs et les traps reçues.

Onglet « Manager » :

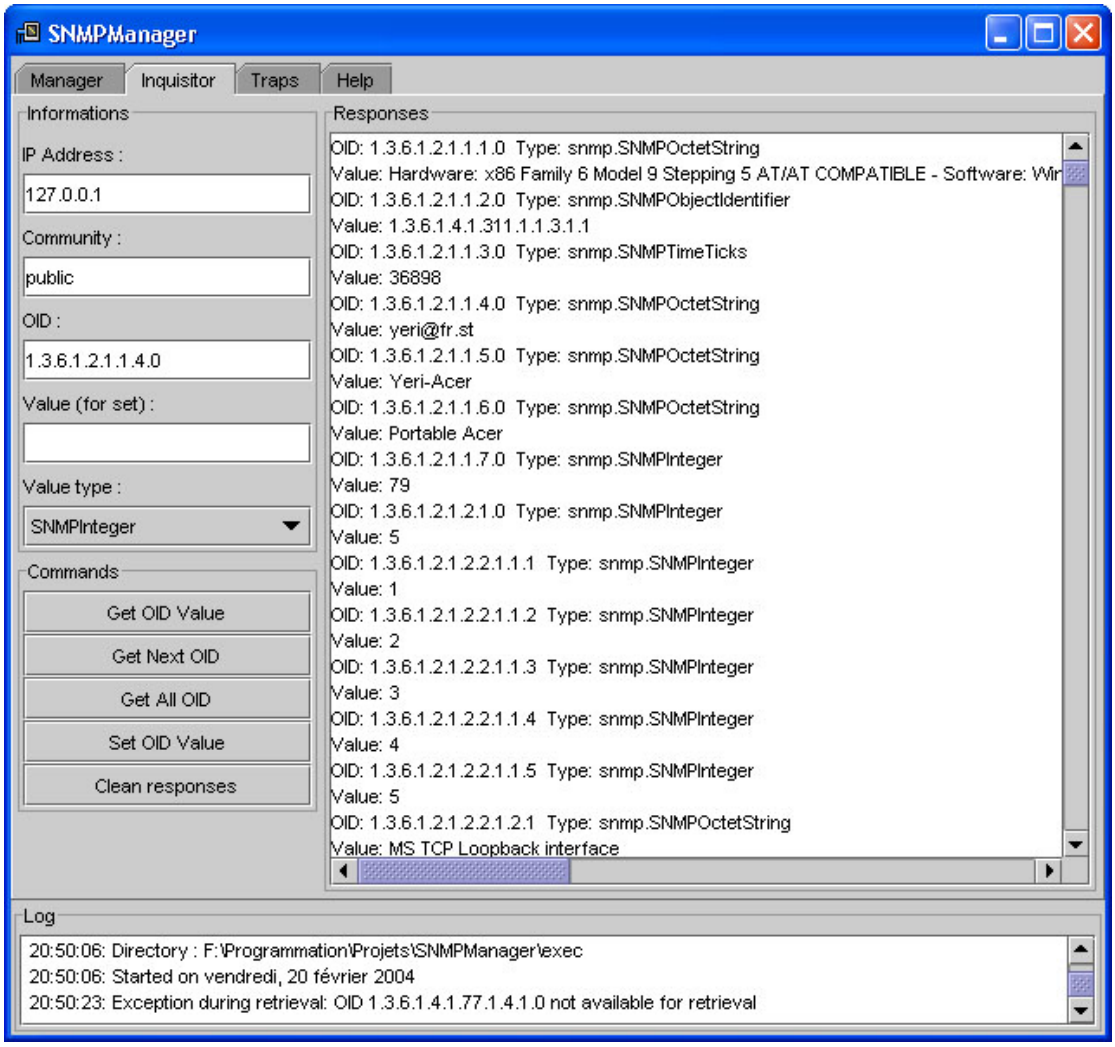
Cette partie de l'application permet de surveiller et d'interroger rapidement plusieurs agents SNMP du réseau.



La zone *New host* permet d'ajouter de nouvelles machines à surveiller.
La zone *Hosts list* montre un tableau contenant toutes les machines que le manager surveille. La colonne *status* montre si l'agent SNMP répond aux requêtes et la colonne *sys* affiche le système d'exploitation présent sur la machine. Ce tableau est rafraîchit toutes les soixante secondes. Enfin, la sélection d'une ligne permet d'afficher dans la zone *Host informations* quelques informations fournies par l'agent SNMP.

Onglet « Inquisitor » :

Cette page permet d'interroger ou de changer certaines variables d'un agent SNMP.



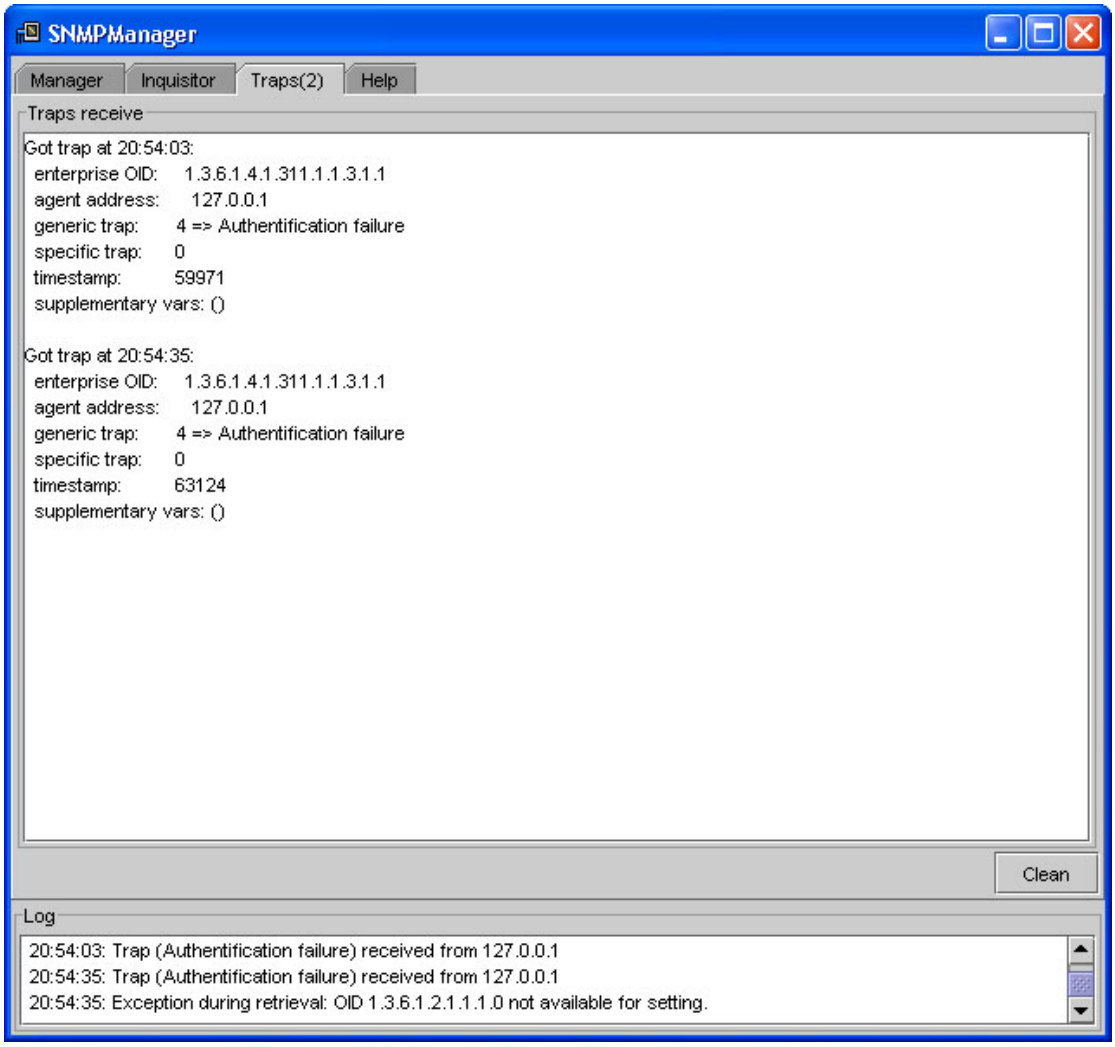
La zone *Informations* permet de spécifier l'adresse IP et la communauté de l'agent SNMP qu'on veut interroger. Ensuite, on choisit un numéro OID (qui correspond aux numéros de groupes dans la MIB) pour recevoir ou changer une valeur particulière. Le champs *Value* permet de donner une nouvelle valeur et le champ *Value type* définit le type de cette nouvelle valeur.

Les commandes suivantes sont disponibles :

- *Get OID Value* : retourne la valeur correspondant à l'OID spécifié.
- *Get Next OID* : retourne la valeur correspondant à l'OID suivant.
- *Get All OID* : retourne toutes les valeurs de la MIB.
- *Set OID Value* : change la valeur correspondant à l'OID spécifié.

Onglet « Traps » :

Affiche les différentes traps reçues par l'application.



Lorsqu'une trap a été envoyée au manager par un agent, on affiche les données de cette trap dans la zone de texte. Un message dans le log ainsi qu'un signal sonore permet d'avertir également l'utilisateur lorsqu'une trap est reçue.

Pour générer une trap, on peut utiliser la commande `snmptrap` disponible dans le package SNMP-NET.

Conclusion

SNMP est un des protocoles les plus utilisés dans la gestion de réseaux, la raison de son succès est principalement sa simplicité qui lui permet notamment d'être implanté dans de nombreux périphériques (routeurs, switch, …).

Par contre dans la version 1 du protocole, un gros problème de sécurité se pose du fait de la circulation du nom de communauté en clair. La version 2 a corrigé ce problème mais n'a pas vraiment réussi à s'implanter chez les utilisateurs. Heureusement la version 3 qui corrige également ces problèmes est actuellement en pleine expansion.

Les applications liées à ce protocole sont très nombreuses et permettent notamment d'évaluer les performances d'un réseau, de configurer des périphériques à distance ou encore de détecter d'éventuelles pannes matérielles.