Institut de la Francophonie pour l'Informatique

Rapport

Travail d'Intérêt Personnel Encadré

Les protocoles pour la gestion des réseaux Informatiques

Professeur : Victor MORARU
Étudiant : NGUYEN Manh Tuong
Promotion 10

Hanoi, Juillet 2005

Table des matières

Avant-propos

De nos jours, les réseaux informatiques sont de plus en plus grands, plus complexes et ils sont indispensables à gérer. Il existe plusieurs outils pour faire ce la, donc les connaissances sur le méthodes qui travaille, les protocoles qui utilise est très important.

Dans la carde du TIPE, j'ai fait la recherche sur les protocoles existant qui permettent de comprendre les méthodes, les mechanism de la gestion de réseau informatique.

Ce rapport se compose de 4 chapitres :

Chapitre 1 : Introduction à la gestion des réseaux informatiques

Chapitre 2 : Protocole pour la gestion des réseaux dans le modèle OSI : CMIS/CMIP

Chapitre 3 : Protocole pour la gestion des réseaux dans le modèle TCP/IP : SNMP scène

Chapitre 4 : Partie pratique, utilisation de SNMP dans l'environnent Linux et sous Windows. Je me termine ce rapport par quelques conclusions sur le sujet.

Je tiens à sincèrement remercier mon professeur Victor MORARU pour son encadrement, son aide et ses conseils pendant mon travail du TIPE.

Liste des acronymes

ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
CMIP	Common Management Information Protocol
CMIS	Common Management Information Services
CMOT	CMIP over TCP/IP
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
MIB	Management Information Base
NMA	Network Management Application
NMS	Network Management Station
NME	Network Management Entity
OSI	Open System Interconnection
PDU	Protocol Data Unit
RFC	Request For Comment
SMAFE	System Management Application Entity
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Data Protocol

Chapitre I. Introduction à la gestion des réseaux informatiques

1.1. Introduction

De nos jours, le réseau est en train de devenir obligatoire pour tout le domaine de la vie. La gestion des réseaux donc est indispensable. Il faut souvent avoir recours à des techniques d'administration pour pouvoir contrôler son fonctionnement mais aussi afin d'exploiter au mieux les ressources disponibles, et de rentabiliser au maximum les investissements réalisés .

1.2. Généralités

La gestion des réseaux informatiques constitue un problème dont l'enjeu est de garantir au meilleur coût non seulement la qualité du service global rendu aux utilisateurs mais aussi la réactivité face aux besoins de changement et d'évolution.

La gestion des réseaux informatiques se définit comme étant l'ensemble des moyens mis en œuvre (connaissances, techniques, méthodes, outils) pour superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes de coût et de qualité. La qualité de service se décline sur plusieurs critères, du point de vue de l'utilisateur final, notamment la disponibilité, la performance (temps de réponse), la fiabilité, la sécurité…

Les activités d'administration sont communément classées en activités de :

Supervision qui consiste à surveiller les systèmes et à récupérer les informations sur leur état et leur comportement, ce qui peut être fait par interrogation périodique ou par remontée non sollicitée d'informations de la part des équipements de réseaux eux-mêmes.

- Administration qui désigne plus spécifiquement les opérations de contrôle « à froid » du réseau avec la gestion des configurations et de la sécurité,

- Exploitation qui désigne l'ensemble des activités permettant de traiter les problèmes opérationnels sur le réseau : maintenance, assistance technique…

1.3. Principe général

Sur le point de l'administration, un système de réseau informatique se compose d'un ensemble d'objets qu'un système d'administration surveille et contrôle. Chaque objet est géré localement par un processus appelé agent qui transmet régulièrement ou sur sollicitation les informations de gestion relatives à son état et aux événements qui le concernent au système d'administration.

Le système d'administration comprend un processus (manager ou gérant) qui peut accéder aux informations de gestion de la MIB locale via un protocole d'administration comme SNMP ou CMIP de qui le met en relation avec les divers agents.

Le principe se repose donc sur les échanges :

- D'une part, entre une base d'informations appelée MIB(Management Information Base) et l'ensemble des éléments administrés (objets) ;
- D'autre part, entre les éléments administrés et le système d'administration.

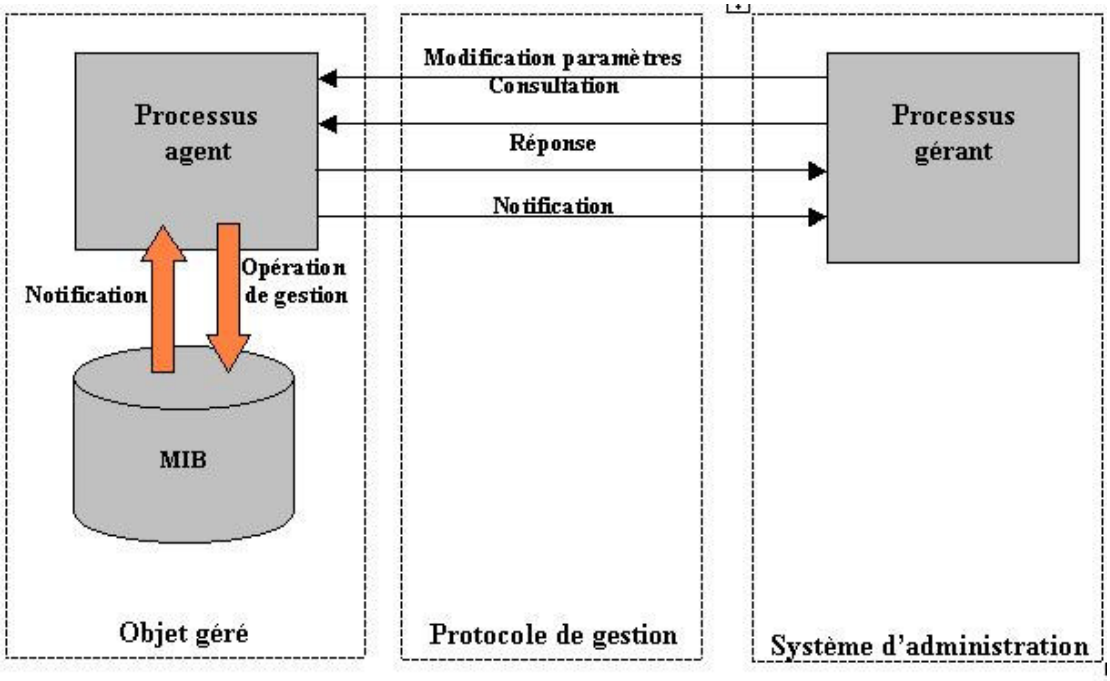


Fig.1 - Structure fonctionnelle d'une d'administration réseau

1.4. Architecture d'administration

Le figure ci-dessous donne une architecture classique d'administration appelé le modèle Gérant/ Agent (Manager/Agent). Le système est composant d'une entité d'administration et des entités de gestion (NME) qui sont géré par cette entité et un protocole pour la gestion comme CMIP ou SNMP.

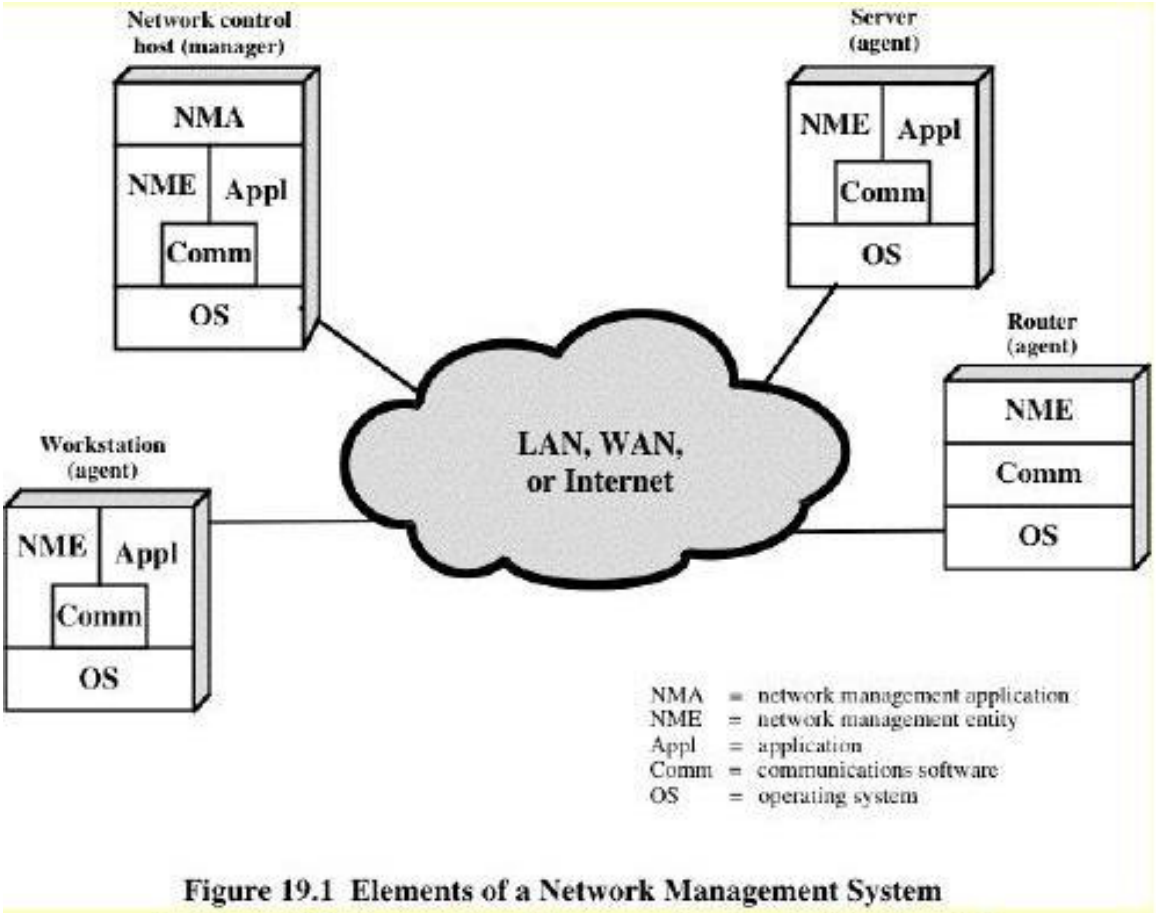


Figure 19.1 Elements of a Network Management System

Stallings, "Business Data Communications", 4/e, Fig 19.1

Chaque entité dans le réseau a un Agent pour l'opération de gestion, une base de données stockées dans MIB et assume les travaux ci-dessous :

- Collecter des informations statistiques concernant à la communication, les

opérations de réseau.

- Stocker les informations localement dans les MIBs.

- Répondre les commands de l'entité de contrôle de réseau, inclus : Transmet des informations statistiques à l'entité d'administration de réseau, modifie les paramètres, donne des informations d'état…

L'entité d'administration a une entité de gestion (NME) et aussi un logiciel pour gérer le réseau appelé NMA (Network Management Application). NMA contient une interface permettant l'administrateur fait des opérations de gestion.

Chapitre II. Protocole pour la gestion des réseaux dans le modèle OSI : CMIS/CMIP

Protocole de l'information de gestion commune (CMIP) est un protocole d'OSI utilisé avec les services d'information de gestion commune (CMIS), supporte l'échange de l'information entre les applications de gestion de réseau et les agents de gestion. CMIS définit un système des services d'information de gestion de réseau. CMIP supporte une interface qui fournit les fonctions qui peut-être utilisé à supporter pour le modèle OSI. Les spécifications de CMIP pour des réseaux de TCP/IP s'appellent CMOT (CMIP au-dessus de TCP) et la version pour IEEE 802 LAN s'appelle CMOL (CMIP au-dessus de LLC). On propose CMIP/CMIS en tant que protocole de concurrence à SNMP dans la suite de TCP/IP.

CMIP n'indique pas la fonctionnalité de l'application de gestion de réseau, il définit seulement le mécanisme d'échange de l'information des objets contrôlés et n'indique pas comment l'information doit être employée ou interprétée.

Le protocole CMIP pour le modèle OSI se base sur trois modèles suivants:

- Modèle d'architecture MSA (Managed System and Agents) qui définit l'architecture de la gestion du protocole CMIP et la notion de systèmes gérés et gérants.
- Modèle d'information qui définit le modèle de représentation des l informations de gestion,
- Modèle fonctionnel SMFA (Specific Management Function Area) qui définit des domaines fonctionnels d'administration et leurs relations.

2.1. Modèle d'Architecture

Ce modèle définit une structure en couches comprenant trois activités de gestion :

+ **La gestion système** (**Systems-Management**),
+ **La gestion de couches** (**Layer Management**),
+ **La gestion d'opérations de couche** (**Layer Operation**).

Le modèle repose essentiellement sur les échanges des informations de gestion concernant les ressources (objets gérés) du réseau entre système au niveau de la couche application (**gestion système**) via un protocole de gestion système **SMP** (**System Management Protocol**).

La couche application du modèle OSI est constituée d'un ensemble de **processus applicatifs AP** (**System Management Application Process,** regroupe un ensemble d'éléments nécessaires à son bon déroulement), notamment le processus **SMAP** (**System Management Application Process**) qui prend en charge la gestions système. On distingue deux types de processus applicatifs : **Le gérant** (**manager**) sur les systèmes d'administration et **l'agent** sur les systèmes administrés. L'entité d'application **SMAE (Application Entity**) est l'éléments qui prend en charge la gestion de la communication pour le processus applicatifs SMAP en faisant quatre éléments de services d'application (**ASE, Application Service Elements**) en particulier **CMIS**(**Common Management Information Service**).

Il s'agit de faire remonter toutes les informations de gestion concernant une ressource (routeur, pont, commutateur, protocole,…) gérée par un **processus agent** dans le **SMAP** (**System Management Application Process**). Et ce, par l'intermédiaire du **SMAE** (**System Management Application Entity**). Le transfert d'information vers le processus gérant est assuré par un ensemble de primitives d'accès aux informations défini par **CMIS** via le protocole **CMIP** (**Common Management Information Protocol**).

Le modèle repose aussi sur les échanges horizontaux entre couches d'éléments administrés différents (**gestion de couches**) soit via le protocole de gestion de réseau CMIP en utilisant un protocole OSI classique pour le transfert d'information spécifique à

la couche.

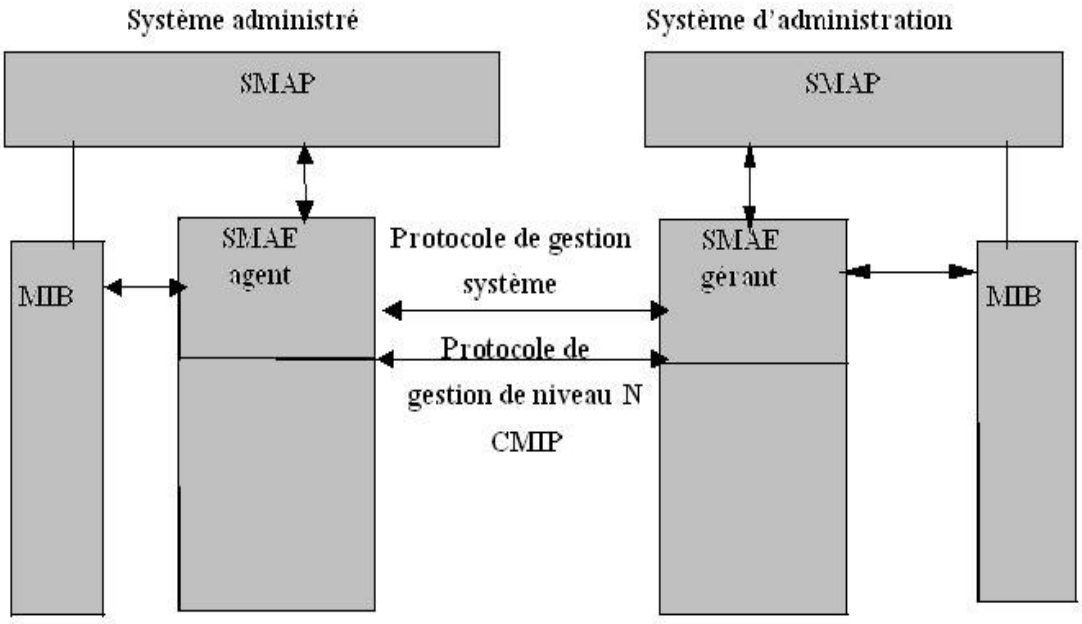


Fig. : Modèle d'architecture de la gestion ISO

2.2. Modèle d'information

2.2.1. Concept d'objet

Dans le protocole CMIP, touts les informations gérées sont organisées comme des objets. Au niveau le plus fondamental, chaque objet administré peut inclure :

- Attribues que contiennent les valeurs décrivant l'état de l'objet, ou les objets contenus cette par référence.
- Des comportements - représentez les types de comportement que l'objet contrôlé montrera. Ceci est actuellement exprimé en directives pour la définition des objets contrôlés comme texte. Le dispositif contrôlé mettra en application typiquement ceci de la façon appropriée à son rôle dans le système.
- Actions - les services ont fourni par l'objet contrôlé qui peut être activé sur la demande du système de gestion.

- Avis - messages qui peuvent être lancés par l'objet contrôlé sur l'occurrence des événements critiques de système.
- Paquets - collections d'attributs, de comportements, d'actions, et d'avis qui peuvent être groupés dans une ou plusieurs caractéristiques contrôlées de classe d'objet.

2.2.2. Concept d'organisation des Objets

Comme dans n'importe quel système intensif de données, l'information doit être maintenue dans un certain schéma avec lequel les utilisateurs (typiquement systèmes de gestion) peuvent accéder à l'information. Dans le schéma de gestion d'OSI, il y a trois types de rapports entre les objets contrôlés, incluant:

- Arbre d'héritage: définit la classe contrôlée d'objet superbe et des sous-classes, comme C++, les classes dérivées sont reliées. Quand une classe est héritée d'une classe superbe, elle possède toutes les caractéristiques de la superbe-classe, avec les attributs, les comportements et les actions additionnels.
- L'arbre de contenance: définit les objets qui sont contenu dans d'autres objets contrôlés. Par exemple, un sous-réseau peut contenir plusieurs éléments administrés.
- Nommant l'arbre: définit la manière dans laquelle différents objets sont mis en référence dans les contraintes de l'architecture de gestion.

Comme dans le cas d'autres systèmes orientés, l'héritage fournit une capacité de définir l'information générale et commune dans les classes basses, et définissent des comportements et des attributs plus spécifiques dans les classes dérivées. Suivant les indications du schéma ci-dessous, le cas du SMI d'OSI, toutes les classes sont dérivées de plus haut niveau de la classe d'objet désignée sous le nom du **top**. Après cette hiérarchie d'héritage, vous pouvez voir que le système est dérivé de X.721 : Complétez avec les types spécifiques de systèmes étant dérivés de la classe contrôlée « système d'objet. » Pendant que chaque type plus spécifique de classe est ajouté à l'arbre de transmission, la classe dérivée ajoute l'information plus spécifique au type d'objet représenté. Par

exemple, une connexion multipoints peut ajouter l'information décrivant les points spécifiques de connexion étant incluse dans la connexion.

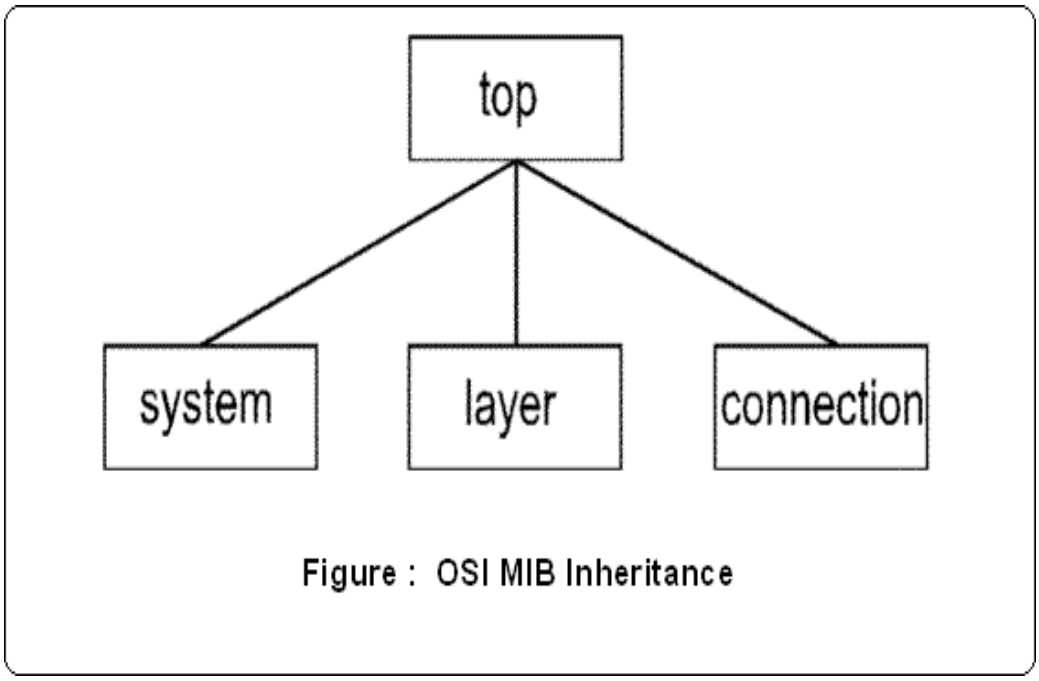


Figure : OSI MIB Inheritance

Contenance

La contenance est un dispositif qui permet les objets contrôlés "contiennent" d'autres objets contrôlés dans le système. Par exemple, un commutateur de paquets peut contenir plusieurs étagères d'équipement, dont chacune contient alternativement qu'un ou plusieurs le circuit emballe. Le rapport de contenance est un mécanisme commode pour segmenter l'organisation d'information contrôlée de systèmes. Le mécanisme de contenance est réalisé par l'inclusion de la marque de l'objet de l'objet (contenu) subalterne dans la classe (contenant) supérieure. Les marques d'objet sont stockées en tant qu'attributs dans la classe supérieure. Seulement un objet supérieur peut contenir n'importe quel objet contrôlé par subalterne simple, imposant que la contenance de MIB soit réalisée par une structure de l'arbre (MIT - Managed Information Tree).

2.2.3. Structure des informations d'administration de réseaux (SMI)

En complément du standard MIB qui définit les informations spécifiques d'administration réseaux et leur signification, un standard séparé spécifie l'ensemble des règles utilisées pour définir et identifier les variables MIB. Ce sont les règles de gestion des informations d'administration, SMI (Structure of Management Information). Pour que le protocole d'administration de réseaux reste simple, SMI pose des restrictions sur les types de variables autorisées dans la MIB, spécifie les règles de nommage de ces variables et crée les règles de définition des types de variables.

Par exemple: SMI comprend des définitions de termes comme *IpAddress* (défini comme une chaîne de 4 octets) et *Counter* (entier appartenant à l'intervalle [0,2^32-1] et indique que ce sont les termes utilisés pour définir les variables MIB. De plus, SMI décrit la façon dont la MIB référence les tables de valeurs (les tables de routage IP, par exemple).

Définitions formelles utilisant ASN.1

Le standard SMI indique que toutes les variables MIB doivent être définies et référencées à l'aide de la notation ISO de syntaxe abstraite ASN.1 (Abstract Syntax Notation 1). ASN.1 est un langage formel qui présente 2 caractéristiques principales: une notation utilisée dans les documents manipulés par les humains et une représentation codée et concise de la même information, utilisée dans les protocoles de communication. Dans les 2 cas, la notation formelle élimine toutes les ambiguïtés possibles, tant du point de vue de la représentation que de la signification. Au lieu de dire par exemple, qu'une variable contient une valeur entière, un concepteur qui utilise ASN.1 doit définir la forme exacte et le domaine des valeurs prises par cet entier.

Les messages

Le format et la longueur des messages CMIP sont variables et relativement complexes. On utilise ASN.1 pour décrire la structure des messages CMIP. Voici un exemple d'utilisation d'ASN.1 décrivant la structure d'une trame Ethernet:

```
Ethernet-Frame::= SEQUENCE {
        destAddr OCTET STRING (SIZE(6)),
        srcAddr OCTET STRING (SIZE(6)),
        etherType INTEGER (1501..65535),
        data ANY (SIZE(46-1500)),
        crc OCTET STRING (SIZE(4))
}
```

Dans ce cas, il sert à attribuer à la variable de gauche la définition du membre de droite. SEQUENCE représente une liste ordonnée d'éléments. Cette liste ordonnée contient les champs d'une trame Ethernet, notamment l'adresse de destination, l'adresse source, le type d'Ethernet, les données et le CRC.

Le type d'un champ est spécifié à la suite du nom. Par exemple, destAddr et srcAddr sont déclarés comme étant de type OCTET STRING, définissant une variable de 0 ou plusieurs octets.La valeur de chaque octet est comprise entre 0 et 255. La taille de la chaîne obtenue est placée après la déclaration de la chaîne OCTET STRING. Ethertype est défini en tant que INTEGER, à savoir une valeur entière de taille et de précision arbitraire. Le (1501..65535) situé juste après permet de définir sa plage de valeur. Le champ de donnée est de type ANY et sa taille varie de 46 à 1500 octets.En utilisant la notation ASN.1, les messages SNMP prennent le format suivant:

```
SNMP-message::= SEQUENCE {
        version INTEGER {version-1(1)},
        community OCTET STRING,
        data ANY }
```

2.3. Modèle fonctionnel

L'OSI a regroupé les activités d'administration en cinq groupes fonctionnels :

- **La gestion des anomalies**(**Fault Management**) dont l'objectif est le diagnostic rapide de toute défaillance interne ou externe du système, tout dysfonctionnement (panne d'un routeur) ; ces pannes pouvant être d'origine interne résultant d'un élément en panne ou d'origine externe résultant dépendant de l'environnement du système(coupure d'un lien publique).

Cette gestion implique :

+ La surveillance des alarmes(filtre, report, …) ; il s'agit de surveiller le système et de détecter les défauts. On établit un taux d'erreurs et un seuil à ne pas dépasser. On distingue cinq types d'alarmes

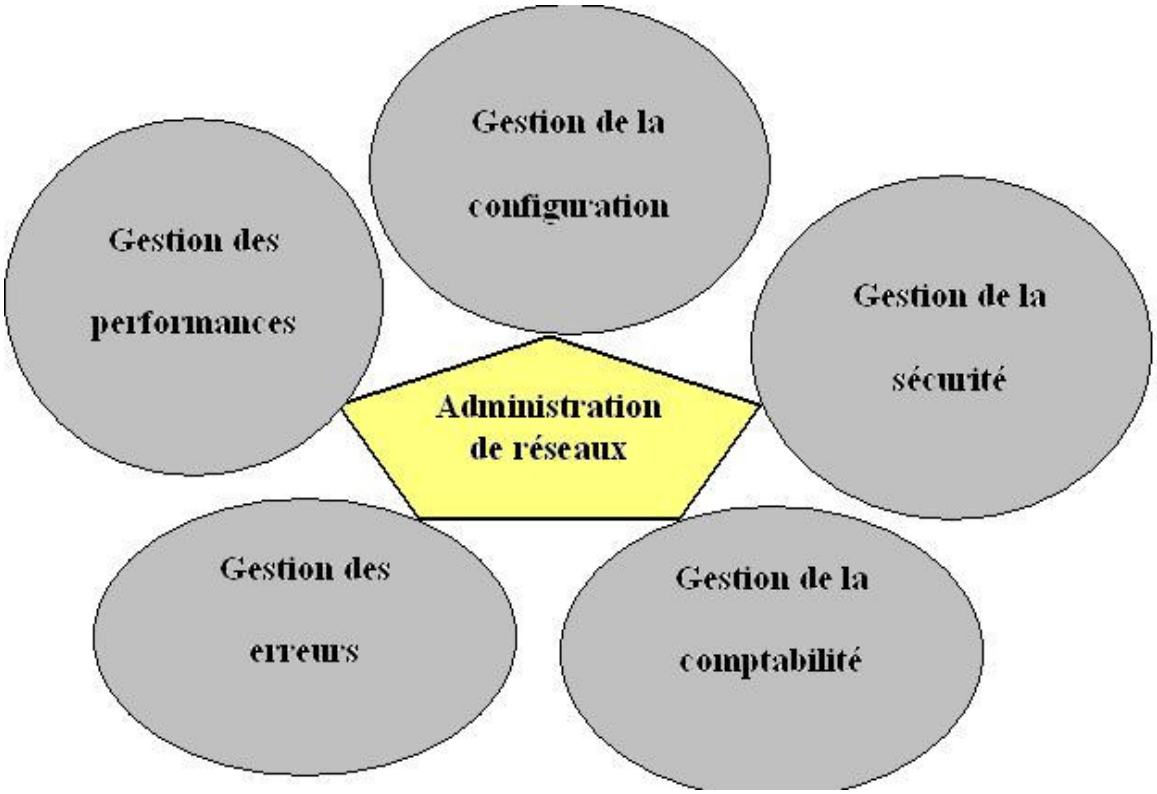
+ Le traitement des anomalies

+ La localisation et le diagnostic des incidents(séquences de tests) la journalistique des problèmes, etc.

- **La gestion de la configuration** (**Configuration Management**), consiste à identifier de manière unique chaque objet administré par un nom ou un identificateur d'objet(**OID, Object Identifier**). Il s'agit également de gérer la configuration matérielle et logicielle et de préciser la localisation géographique.

- **La gestion des performances** (**Performance Management**) consiste à contrôler, à évaluer la performance et l'efficacité des ressources, à savoir le temps de réponse, le débit, le taux d'erreur par bit, la disponibilité (aptitude à écouler du trafic et à répondre aux besoins de communication pour lequel la ressource a été mise en service). Elle comprend la collecte d'informations statistiques(mesure du trafic, temps de réponse, taux d'erreurs, etc.), le stockage et l'interprétation des mesures (archivage des informations statistiques dans la MIB, calculs de charge du système, tenue et examen des journaux chronologiques de l'état du système). Elle est réalisée à l'aide d'outil de modélisation et simulation permettant d'évaluer l'impact d'une modification de l'un des paramètres du système.

- **La gestion de la sécurité** (**Security Management)** concerne le contrôle d'accès au réseau, la confidentialité des données qui y transitent, leur intégrité et leur authentification (l'entité participant à la communication est bien celle qui a été éclairée).
- **La gestion de la comptabilité** (**Accounting Management**) consiste à gérer la consommation réseau par abonné, de relever les informations permettant d'évaluer les coûts de communication. La comptabilité est établie en fonction du volume et de la durée des transmissions.



2.4. CMIS, CMIP

CMIS/CMIP est au cœur du modèle d'administration OSI en mettant en œuvre les demandes d'informations nécessaires à l'administration d'un réseau.

CMIS définit un système de services de communication d'informations de gestion fournissant les moyens d'échanger des informations entre un processus gérant et un processus agent, et entre entités d'application SMAE (System Management Application

Entity) de processus agents différents via le protocole CMIP. CMIP définit le mécanisme permettant d'effectuer les échanges des informations de gestion.

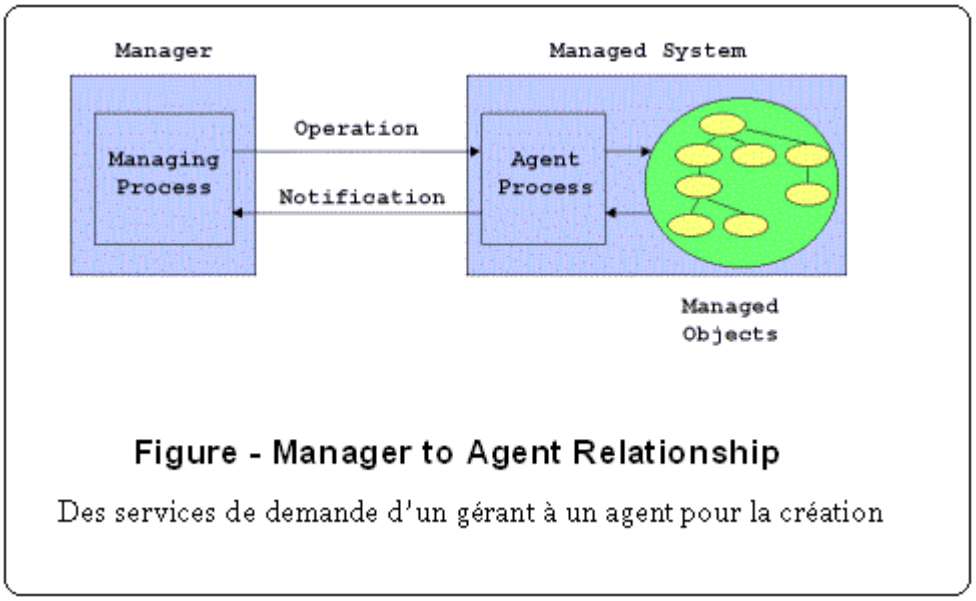


Figure - Manager to Agent Relationship

Des services de demande d'un gérant à un agent pour la création

CMIS définit plusieurs services dont :

- Des services de demande d'un gérant à un agent pour la création (**M-CREATE**) ou la destruction (**M-DELETE**) d'informations concernant des objets de gestion, signalisation faite par un agent à un gérant par rapport aux changements d'état d'un objet (**M-EVENT-REPORT**), mettre à jour une information (**M-SET**), obtenir une valeur (**M-GET**).
- Des services concernant les mises en relation entre SMAE pour l'échange d'informations notamment l'initialisation (**M-INITIALIZE**), la fermeture (**M-TERMINATE**).
- Des services d'annulation (**M-ABORT**)…

Chapitre III. Protocole pour la gestion des réseaux dans le modèle TCP/IP : SNMP

SNMP est l'un des protocoles les plus répandus permettant d'administrer le réseau informatique est l'utilisation du protocole SNMP (Simple Network Management Protocol)**.**

Il est développé a partir d'année 80s, et il est devenu le standard actuel d'administration de réseaux TCP/IP . Actuellement c'est la version 3 de ce protocole qui est en cours de diffusion. Cette version se compose des fonctionnalités nouvelles, en particulier sur le plan de la sécurité.

3.1. Quelques concepts fondamentaux

3.1.1. Station d'administration (NMS)

Ce terme désigne le périphérique utilisé par l'administrateur pour gérer son réseau. Celui-ci doit obligatoirement posséder :

- Des applications spécifiques à l'administration.
- Une interface avec l'administrateur.
- La capacité à pouvoir récupérer des informations des éléments administrés.
- Une base de données obtenue à partir des MIBs des éléments administrés.

La station NMS peut envoyer des requêtes à un périphérique afin d'obtenir des informations sur son paramètre. L'agent du périphérique reçoit la requête et renvoie les informations demandées. Lorsqu'elle reçoit cette réponse, la station NMS peut utiliser les informations de configuration du périphérique afin de déterminer les opérations à entreprendre en fonction de son état.

3.1.2. Agent de gestion

Ce terme désigne des agents de SNMP. Ils sont installés dans des périphériques qui supporte le protocole SNMP par exemple: dans des ordinateurs que des hubs, des routeurs, ou encore tout autre type de périphériques. Ces agents connaissent les paramètres du périphérique sur lequel il s'exécute et ont pour devoir de répondre aux requêtes de la station d'administration

3.1.3. Les MIBs

Ces bases de données sont assimilées à des bibliothèques d'objets nous renseignant sur tous les types de données en rapport avec l'activité du réseau. Nous la détaillerons lors de notre partie suivant.

3.1.4. Les alarmes

Il est évident qu'une machine de gestion ne peut constamment demander aux stations surveillées quel est leur état parce que dans un réseau, normalement, il y a beaucoup de périphériques. C'est la raison pourquoi il est possible de demander aux stations d'émettre de temps en temps (une fois par heure par exemple) un rapport sur son état et pourquoi pas quelques statistiques. Cela permet de soulager le travail de la station d'administration qui n'a plus qu'à écouter ses protégés si elle n'a pas d'autres actions de gestion à faire.

3.1.6. Les PROXIES (Les Délégations)

L'utilisation de SNMP nécessite que tous les agents supportent un protocole commun, tel que UDP et IP, ce qui va limiter l'utilisation à certaines machines en excluant les PC et les stations de travail, ces dernières pouvant implémenter TCP/IP mais pour lesquelles il serait indésirable d'ajouter SNMP.

Afin de résoudre ce problème, le concept de **proxy** a été développé. Ces **proxies** suppléent les machines inadaptées car ils connaissent les objets de la MIB nécessaires pour la gestion du système mandaté. La communication entre le **proxy** et la machine

suppléée ne peuvent pas utiliser SNMP pour dialoguer et il faut donc, pour le proxy, s'adapter aux protocoles connus par la seconde machine, c'est ce qui est illustré par la figure ci-dessous

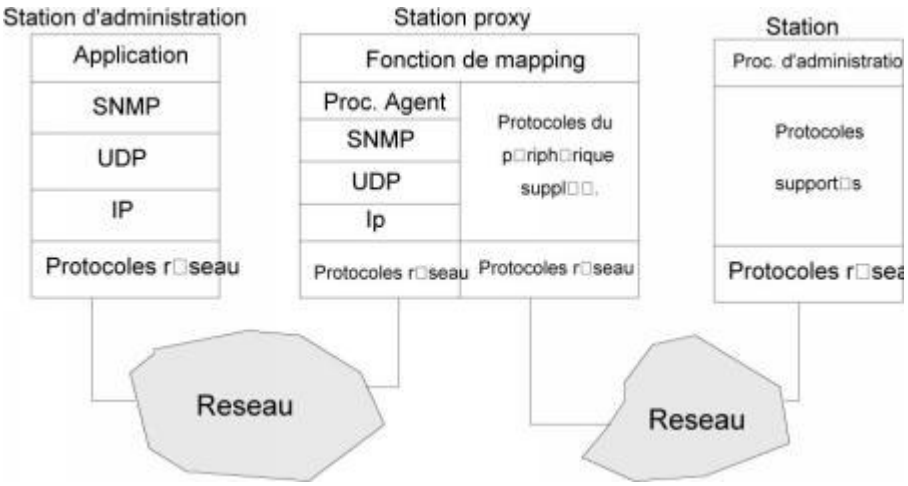


Figure : Gestion des machines ne supportant pas SNMP.

3.3. Architecture de SNMP

L'architecture de gestion du réseau proposée par le protocole SNMP est basée sur trois éléments principaux :

3.3.1. Les équipements gérés (managed devices):

Ce sont des éléments du réseau (**ponts, hubs, routeurs ou serveurs**), contenant des "objets de gestion" (managed objects) pouvant être des informations sur le matériel, des éléments de configuration ou des informations statistiques

3.3.2. Les agents de gestion

C'est-à-dire une application de gestion de réseau résidant dans un périphérique et chargé de transmettre les données locales de gestion du périphérique au format SNMP

3.3.3 Les systèmes de gestion de réseau (network management systems notés NMS):

C'est-à-dire une console au travers de laquelle les administrateurs peuvent réaliser des tâches d'administration

SNMP a été crée pour être une couche utilisant TCP/IP à un niveau supérieur. Le protocole d'administration opère en accord avec UDP (User Datagram Protocol) et IP. A chaque action de la station d'administration, le processus de contrôle accède à la MIB et avertit l'utilisateur par l'intermédiaire d'une interface graphique.

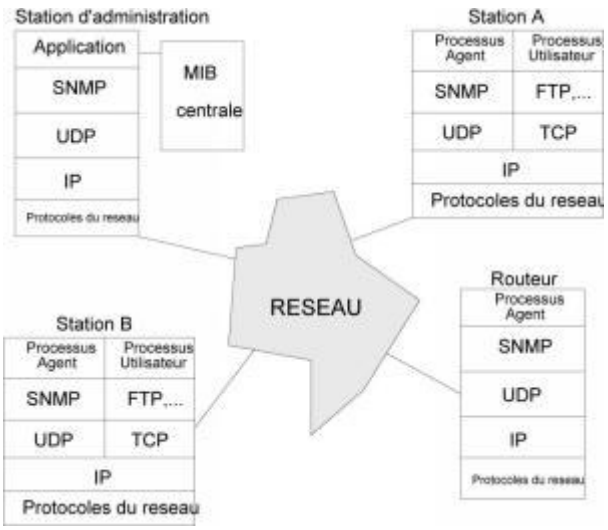


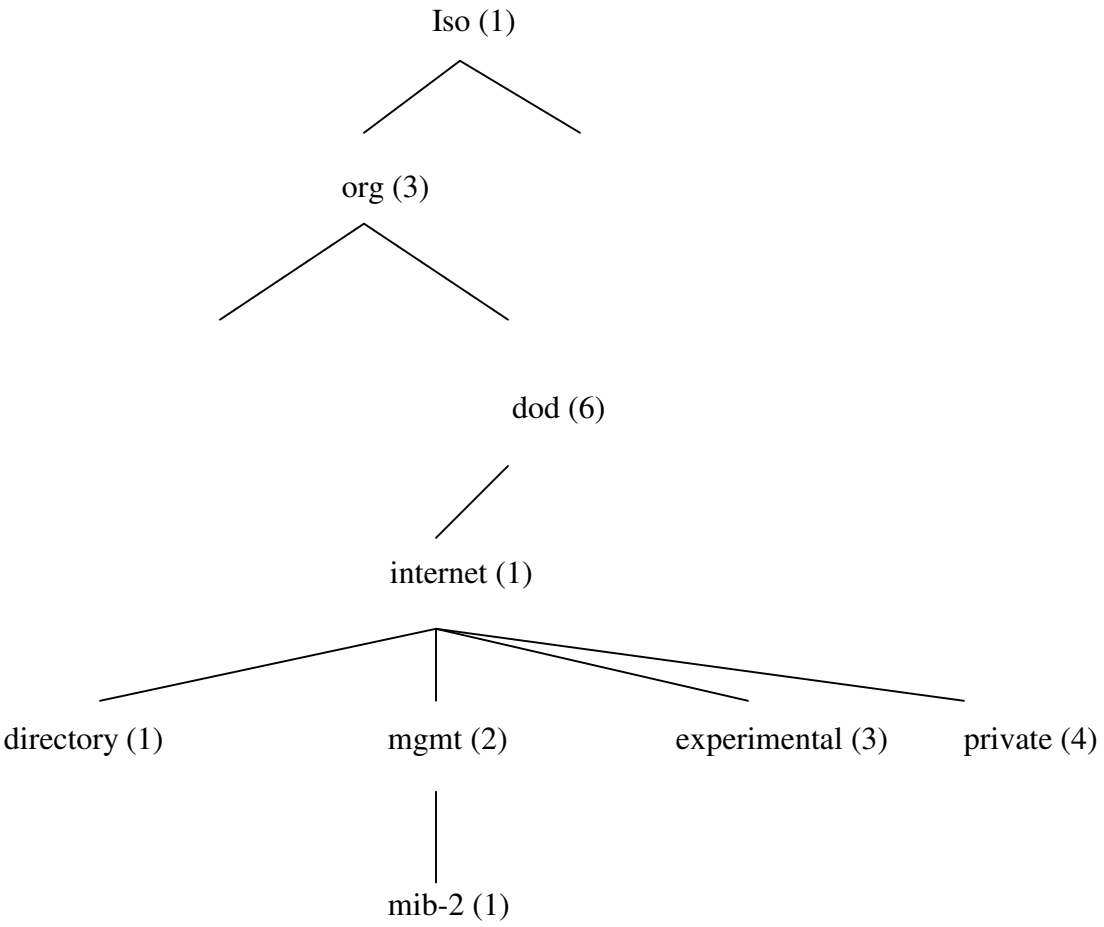
Figure : Mise en oeuvre de SNMP dans un réseau.

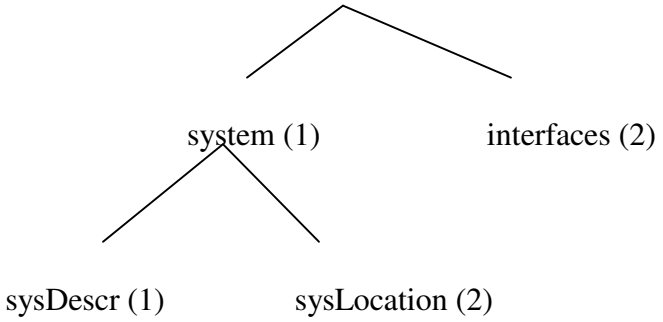
Chaque agent administratif doit lui aussi implémenter SNMP et UDP/IP afin de pouvoir interpréter les requêtes qui permettent à la machine d'administration d'accéder sa MIB. SNMP étant relié à UDP qui est un protocole sans connexion, il est lui aussi sans connexion, c'est pourquoi les connexions entre station d'administration et agents administratifs ne sont jamais maintenus.

3.3. Modèle d'information

3.3.1 Structure et représentation des noms d'objets

Dans SNMP, touts les objets mangeables peuvent être des informations matérielles, des paramètres de configuration, des statistiques de performance et autres objets qui sont directement liés au comportement en cours de l'équipement . Les objets sont classés dans une sorte de base de donnée appelée MIB. Les objets de MIB reçoivent un identifiant unique composé de séquences de chiffres séparés par des points. Cette séquence se lit de gauche à droite et correspond à des nœuds dans l'arborescence des noms



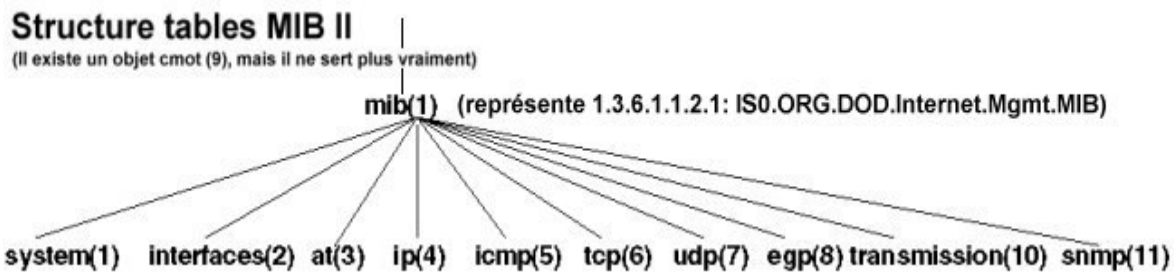


- La gestion de réseau est définie par la branche iso(1). Dans cette branche on trouve un certain nombre de définitions d'organisations subordonnées. La gestion de réseau entre dans le nœud org(3).
- Sous le nœud dod(6) se trouvent un certain nombre de réseaux subordonnés. La gestion de réseau entre dans le nœud internet(1).
- Sous le nœud internet(1) se trouvent un certain nombre de nœuds subordonnés représentant différents services et tentatives de normalisation. La gestion de réseau standardisée se trouve dans le réseau mgnt(2).
- Sous le nœud mgnt(2) se trouvent un certain nombre de nœuds subordonnés représentant différents services et tentatives de normalisation. La gestion de réseau standardisée se trouve dans le nœud MIB-2(1).
- Sous le nœud mib-2(1) se trouvent un certain nombre de nœud subordonnés représentant différents groupement de variables MIB.
- Sous le nœud system(1), on trouve 2 variables MIB sysDescr(1) et sysLocation(2). Les identifiants d'objets de ces variables s'obtiennent en ecrivant de gauche à droite les différents nœuds, séparés par des points :

  + sysDescr : 1.3.6.1.2.1.1.1
  + sysLocation : 1.3.6.1.2.1.1.2

3.3.2 Les tables MIB

Ce sont des tables contenant les informations de l'élément du réseau. Ces informations sont hiérarchisées sous forme d'arbre :



system : Description de toutes les entités gérés

interfaces : Interface de données dynamiques ou statiques

at (adress translation) : Table d'adresses IP pour les correspondances d'adresses MAC

ip : Statistiques du protocole IP, adresse cache et table de routage

icmp : Statistiques du protocoles ICMP

tcp : Paramètres TCP, statistiques et table de connexion

udp : Statistiques UDP

egp : Statistiques EGP, table d'accessibilité

snmp : Statistiques du protocole SNMP

En plus du standard MIB de TCP/IP, qui s'appelle maintenant MIB-II, un nombre important de RFC détaillent des variables MIB pour divers type de périphériques. Examinons quelques éléments de données de la MIB pour en clarifier le contenu.

Variables MIB	Catégorie	Signification
sysUpTime	système	Durée écoulé depuis dernier démarrage
ifNumber	interfaces	Nombre d'interfaces réseau
ifMtu	interfaces	MTU d'une interface particulière
ipDefaultTTL	ip	Valeur utilisée dans le champ TTL

ipInReceives	ip	Nbre de datagrammes reçus
ipForwDatagrams	ip	Nbre de datagrammes acheminés
ipOutNoRoutes	ip	Nbre d'erreurs de routage
ipReasmOKs	ip	Nbre de datagrammes réassemblés
ipFragOKs	ip	Nbre de datagrammes fragmentés
ipRoutingTable	ip	Table de routage IP
icmpInEchos	icmp	Nbre de demandes d'echo ICMP reçues
tcpMaxConn	tcp	Nbre maxi de connexions TCP autorisées
tcpInSegs	tcp	Nbre de segments reçus par TCP
udpInDatagrams	udp	Nbre de datagrammes UDP reçus

Les valeurs des éléments de chacune des variables ci-dessus peuvent être enregistrées au moyen d'un seul entier. Toutefois, la MIB permet également de définir des valeurs plus complexes, comme par exemple la variable ipRoutingTable qui fait référence à la table de routage d'un routeur. Des variables MIB supplémentaires sont définies pour le contenu de la table et pour permettre aux protocoles d'administration de réseaux de référencer les données correspondant à chaque entrée.

3.2. Protocole SNMP

SNMP est un protocole utilisé dans des programmes de gestion de réseaux informatiques dans le monde TCP/IP. Leur fonctionnement est asymétrique, il est constitué d'un ensemble de requêtes, de réponses et d'un nombre limité d'alertes. La « Station de Gestion » envoie des requêtes à l'agent, lequel retourne des réponses. SNMP utilise le protocole UDP [RFC 768].

Le port **161** est utilisé par l'agent pour **recevoir les requêtes** de la station de gestion. Le port **162** est réservé pour la station de gestion pour **recevoir les alertes des agents**. Le schéma ci-dessus résume bien le fonctionnement du protocole SNMP.

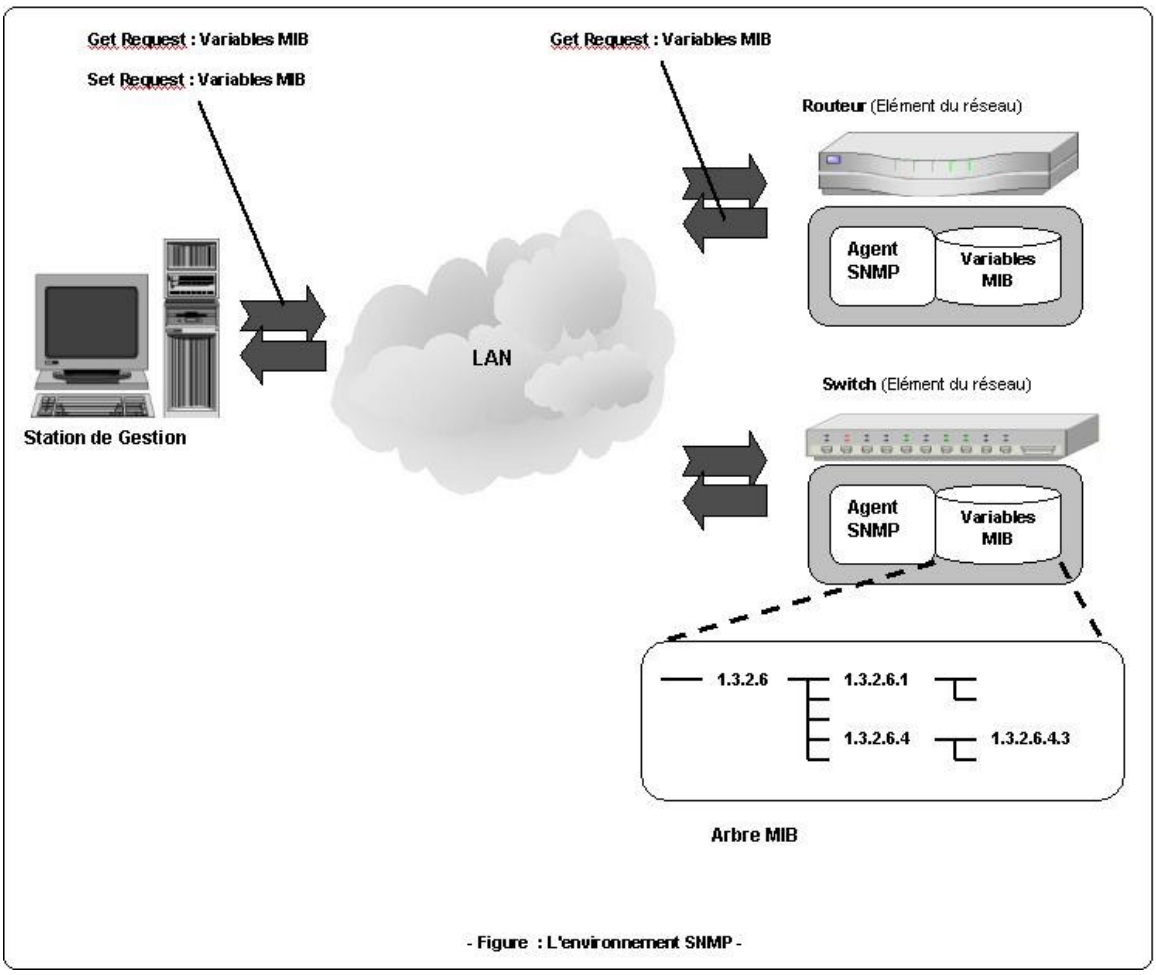
Le gestionnaire SNMP doit être à même de lire et de modifier les valeurs des variables MIB des périphériques qu'il gère.

Lorsqu'un événement inattendu se produit sur un des périphériques gérés, par exemple un échec de transmission et une modification d'état, le périphérique envoie un

message de *trap SNMP* au gestionnaire SNMP. Ce message contient une indication de l'événement ayant provoqué la génération du message. Le gestionnaire SNMP doit alors prendre des mesures qui s'imposent. Il peut se contenter d'enregistrer le message dans un fichier de suivi, ou prendre des mesures plus immédiates, par exemple demander des informations complémentaires au périphérique lui ayant envoyé le message. Ces informations supplémentaires sont obtenues grâce à des requêtes de lecture des variables MIB. Si le gestionnaire SNMP est programmé pour contrôler le périphérique, il peut lui demander de modifier la valeur de ses variables MIB.

Lorsque le gestionnaire décide de modifier l'état du périphérique, il le fait en modifiant les variables MIB du périphérique. Par exemple, le gestionnaire modifiera la variable MIB *ipPowerOff* d'un périphérique afin de l'éteindre à distance.

Comme les variables MIB sont ordonnées selon leur identificateur d'objet, le gestionnaire SNMP peut parcourir toutes les variables du périphérique en utilisant la commande SNMP *GetNext*.



- Figure : L'environnement SNMP -

3.1.1. Les opérations

Le protocole SNMP supporte trois types de requêtes : GET, SET et TRAP. Il utilise alors les opérations suivantes pour la gestion du réseau :

3.1.1.1. Type de lire les informations GET

- **GetRequest** : Cette requête permet aux stations de gestion (manager) d'interroger les objets gérés et les variables de la MIB des agents. La valeur de l'entrée de la MIB (nom) est passée en paramètre. Elle permet d'accéder à une variable précise.
- **GetNextRequest** : Cette requête permet aux stations de gestion de recevoir le contenu de l'instance qui suit l'objet nommé (passé en paramètre) dans la MIB. Cette commande permet en particulier aux stations de gestion de balayer les tables des MIB. Elle permet d'accéder à plusieurs variables simultanément.

- **GetResponse**: À des requêtes, l'agent répond toujours par *GetResponse*. Toutefois si la variable demandée n'est pas disponible, le *GetResponse* sera accompagné d'une erreur *noSuchObject*.

***Par Exemple*: GetRequest(1.3.6.1.2.1.6.4)** provoque le retour de **GetResponse (tcpMaxConn = x)** où x est le résultat de la requête).

- **GetBulkRequest** : (version 2 et version 3) Cette requête est une amélioration du SNMP, elle permet aux stations de gestion (manager) d'interroger les objets gérés et les variables de la MIB des agents**.** Il permet à la station de gestion de récupérer efficacement des grandes données .

3.1.1.2. Type de modification des informations SET

- **SetRequest** : Cette requête permet aux stations de gestion de modifier une valeur de la MIB ou d'une variable et de lancer des périphériques. Elle permet par exemple à un manager de mettre à jour une table de routage. SetRequest provoque aussi le retour de GetResponse

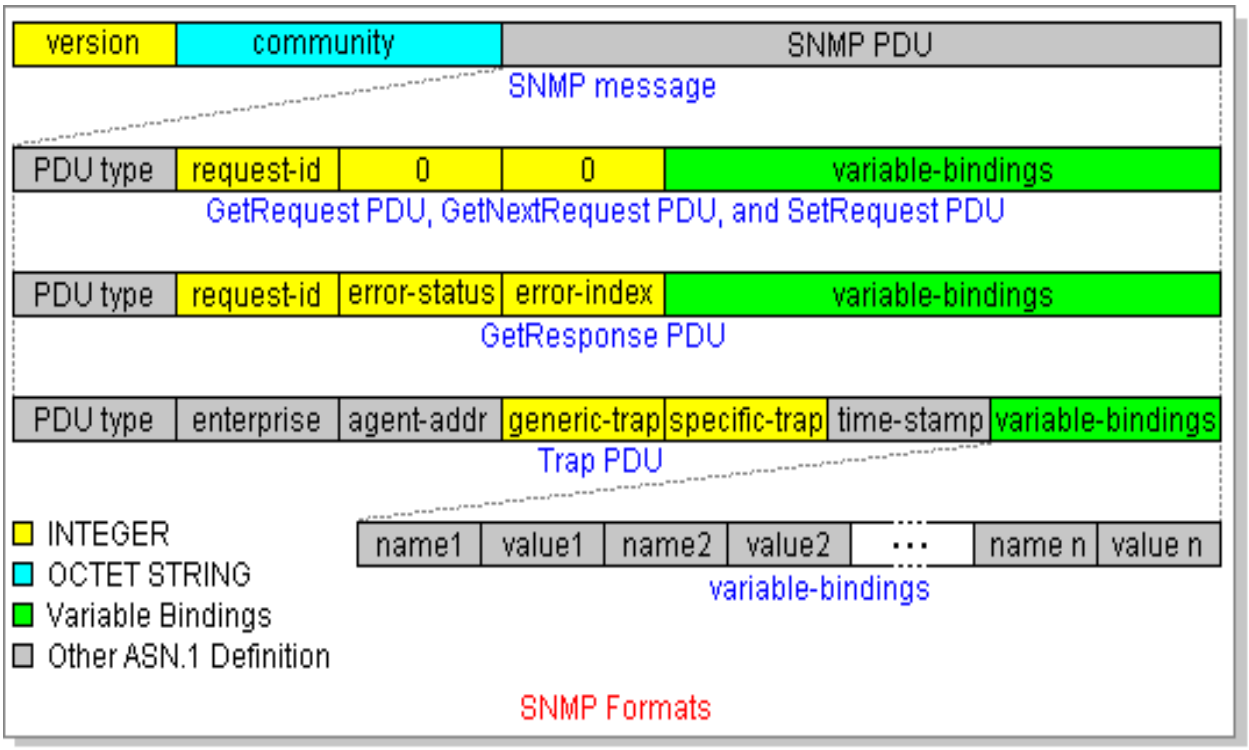
Par Exemple: **SetRequest(1.3.6.1.2.1.6.13.1.1 = 12)** provoque le retour de **GetResponse(tcpConnState = 12)**.

3.1.1.3. Type de non sollicités

- **Les alarmes TRAP** : Lorsqu'un périphérique entre dans un état anormal, l'agent SNMP prévient le gestionnaire SNMP par le biais d'un Trap SNMP. Le message **Trap** peuvent être **cold start** (démarrage à froid), **warm start** (démarrage à chaud**), réinitialisation de l'agent SNMP**, **authentication failure** (échec d'authentification, lorsqu'un nom de communauté incorrect est spécifié dans une requête), **loss of EGP neighbour** (perte de voisin EGP)…
- **InformRequest *:*** (version 2 et version 3) Le but de l'InformRequest-PDU est réellement de faciliter la communication d'information entre les stations de gestion de réseau. L'agent SNMP sur un NMS peut choisir d'informer des autres d'une certaine information en envoyant une InformRequest-PDU à ce autre l'agent de SNMP.

3.1.2. Description du protocole

3.1.2.1. Format des PDUs



Description des champs :

- **version** : Version de SNMP.
- **community** : Nom de la communauté (agit comme un mot de passe).
- **request-id** : Utilisé pour différencier les messages.
- **error-status** : Utilisé pour signaler une erreur (0 si pas d'erreur).
- **error-index** : Indique la sous-catégorie d'erreur.
- **variablebindings** : Nom des variables avec leurs valeurs.
- **enterprise** : Type de l'objet générant l'alarme.
- **agent-addr** : Adresse de l'émetteur de l'alarme.
- **generic-trap** : Identificateur de l'alarme.
- **specific-trap** : Identificateur d'alarme spécifique.
- **time-stamp** : Temps écoulé depuis la dernière réinitialisation de l'entité.

Le champ **communauté**(**community**) est une chaîne de caractère qu'il faut voir comme un mot de passe de validation d'une requête SNMP par l'agent ou par le manager. Si la communauté est incorrecte, la requête est rejetée. La communauté passe en clair sur le réseau.

3.1.2.2. Envoie d'un message

Pour envoyer un message, l'agent de SNMP doit exécuter des procédures suivante :

1. Utilise ASN.1 pour créer un PDU.
2. Ce PDU est émis à un service d'authentification , avec des adresses de destination, et de la source et du nom de la communauté, le service d'authentification va alors exécuter leurs opérations et les opérations de cryptage.
3. Le message est construit à partir du PDU avec l'ajout du nom de la communauté et la version de SNMP.
4. Ce nouvel objet ASN.1, est enfin codé en utilisant BER et envoyé au service de transport.

3.1.2.3. Réception d'un message

Pour envoyer un message, l'agent de SNMP doit exécuter des procédures suivante :

1. Le message est reçu et se voit opérer une vérification syntaxique. Si le message est défectueux, il est ignoré.
2. Le numéro de version est vérifié, s'il n'est pas conforme, le message est ignoré.
3. Le nom d'utilisateur, le PDU, l'adresse de source et de destination au niveau transport, sont émis à un service d'authentification.
    - Si l'authentification échoue, le service prévient l'entité transport de SNMP, laquelle envoie une alarme et ignore le message.
    - Si l'authentification réussit, le service renvoie un PDU de la forme d'un objet ASN.1 qui se conforme à la norme RFC 1157.
4. L'entité du protocole va vérifier la syntaxe de message (sous la forme ASN.1). Si le message est échoue, le message est ignoré. En revanche, le politique d'accéder

SNMP est choisi et PDU est traité continûment.

3.1.2.4. Interaction avec la couche transport UDP

- **Quelques rappels sur UDP**
  - Les trames UDP sont véhiculées dans les paquets IP comme étant des données.
  - Chaque trame possède une adresse de source et une adresse de destination qui permettent aux protocoles de niveau supérieurs comme SNMP de pouvoir adresser leurs requêtes.
  - Le protocole UDP peut utiliser un checksum optionnel qui couvre l'en-tête et le données de la trame. En cas d'erreur, la trame UDP reçue est ignorée.

  Il y a deux ports désignés pour l'utilisation de SNMP : le numéro 161pour les requêtes standard et le numéro 162 pour l'écoute des alarmes destinées à la station d'administration.

- **Cas de perte PDU**

  UDP est un protocole qui n'est pas fiable à 100% et la perte de trames est donc possible. Or rien n'empêche UDP de perdre un trame contenant un message SNMP. Dans ce cas, plusieurs cas s'offrent à nous :
  - Le paquet perdu est du type **Get** ou une réponse d'un agent administré. Cela provoque un manque d'information au niveau de la station d'administration qui n'est pas important : Voyant la réponse ne pas arriver, la station d'administration peut décider d'elle même de renvoyer sa requête. L'identificateur de requête étant identique, il n'y a pas de risque de recevoir plusieurs réponses dues à des questions dupliquées. En cas de non-réponse permanent, cette station peut déclarer ce périphérique muet comme défaillant.

- Le paquet perdu est du type **Set**. Il est alors plus judicieux de faire un **Get** sur cette entrée afin de savoir si c'est la requête qui a été perdue ou alors sa réponse.
- C'est une alarme qui a été perdue. Comme aucun acquittement n'est nécessaire suite à une alarme, la station d'administration ne sera jamais avertie par le signal. Il est donc nécessaire que la station d'administration scrute régulièrement l'état de ses agents pour se mettre au courant des éventuels changements pour lesquels il n'aurait pas reçu d'alarme.

3.6. Sécurité dans des versions de SNMP

SNMP Version 1

Le SNMP Version 1 n'est pas un protocole sécurisé. Cependant, il a un système minimal de sécurité appelé les communautés de SNMP. Lés communautés (community) de SNMP ont le rôle comme des mots de passe pareils pour l'information de SNMP. Il y a trois genres de communauté de SNMP: Fixe, lecture/écriture, et piège (trap).

- Fixe (read-only): Permet de publier le SNMP des demandes obtiennent et de **GetNext** à l'agent et obtiennent une réponse. La corde est envoyée avec le SNMP obtiennent ou des demandes et si l'agent de SNMP emploie la même corde fixe, alors lui de **GetNext** traite la demande.
- Lecture/écriture : Le genre lecture/écriture nous permet également de publier le SNMP des demandes obtiennent et de GetNext et s'attendent à une réponse. En plus, le genre lecture/écriture nous permet aussi d'exécuter des demandes **SetRequest** *de* SNMP. Si un objet de MIB a une valeur d'ACCÈS de « lecture/écriture », alors vous pouvez changer la valeur de cet objet de MIB avec un SNMP **SET** et le genre lecture/écriture correcte de la Communauté de SNMP. Si l'objet de MIB a une valeur d'ACCÈS de « read-only », alors nous ne pouvons pas changer la valeur - même avec du genre lecture/écriture correcte.
- Piège (trap) : En général, la valeur de la communauté (community) de piège n'est pas utilisé. Elle a été conçue pour permettre à des administrateurs de réseau de grouper des entités en masse compacte de réseau ensemble dans des groupes, ou à

des communautés. Puis, les stations de gestion peuvent être configurés pour traiter seulement des pièges reçus d'une ou plusieurs communautés uniques - identifiant la communauté d'une entité par la valeur de la communauté de piège envoyée avec le piège. Puisque la plupart des applications de gestion de réseau ont d'autres manières de limiter quelles entités sont contrôlées, cette capacité est habituellement superflue.

Si nous essayons d'accéder à un agent de SNMP avec une valeur fausse de la Communauté de SNMP, l'agent ne nous fournira pas l'information. Dans la plupart des cas, les valeurs du champ communauté de SNMP pour un objet de réseau ne peuvent pas être obtenues ou changées par l'intermédiaire du SNMP. Souvent, les valeurs du champ communauté de l'agent de SNMP devront être définies dans un dossier de configuration qui est téléchargé à l'agent.

SNMP Version 2

Le cadre de sécurité de SNMP V2 traite le problème de l'authentification de l'expéditeur de message, de son contenu et des problèmes d'oreille indiscrète. SNMPv2 soutient l'utilisation du protocole d'authentification d'identifier la fiabilité de sources et d'empêcher la modification de message.

SNMPv2 soutient l'utilisation du chiffrage de garder l'intimité de messages. Le procédure recommandé d'authentification est le protocole ''Digest Authentication''. Ce protocole est basé sur **message-digest** pour authentifier la source de message et pour empêcher le message trifouillant.

Message -digest:

C'est un message traité comme une séquence des nombres de 32 bits. Il est juste un calcul mathématique exécuté sur ces nombres et inclus avec le message. Le protocole coupe des messages dans bits, les mélange vers le haut à un ingrédient secret et choisit quelques bits ici et se réunir là dans son résultat. Le résultat est envoyé à l'émetteur avec le message original. L'authentification montre seulement que le message est véritable, il

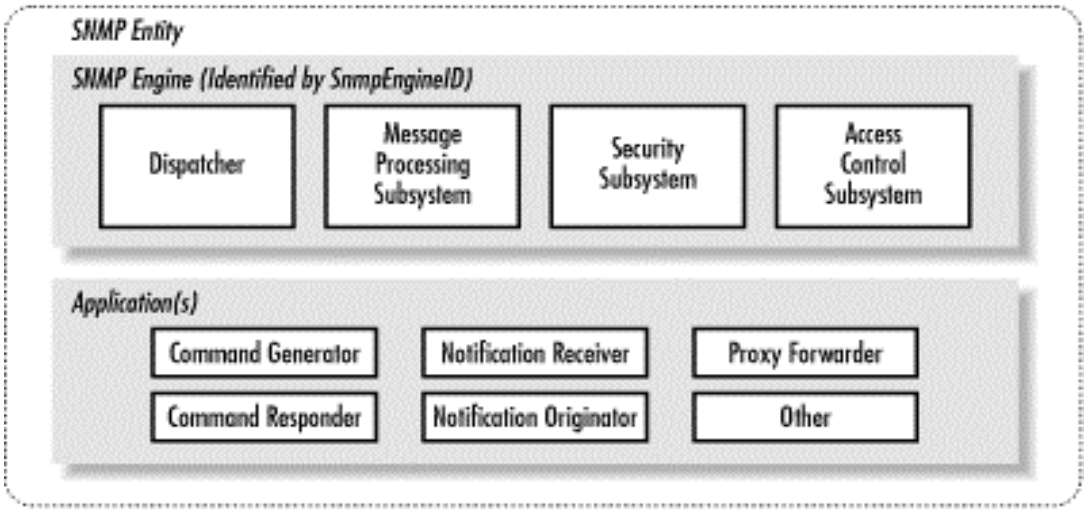
n'empêche pas une oreille indiscrète de lire le message.

SNMP Version 3

SNMP V3 peut résoudre les problèmes de sécurité qui ont infesté SNMPv1 et SNMPv2. Il n'y a aucun autre changement au protocole. Il n'y a aucune nouvelle opération. SNMPv3 soutient toutes opérations définies par Versions 1 et 2.

Le changement le plus important est que la version 3 abandonne la notion des gérants (manager) et des agents. Des gérants et les agents s'appellent maintenant les *entités de* SNMP. Chaque entité se compose d'un moteur de SNMP et d'une ou plusieurs applications de SNMP.

Le moteur de SNMP V3 :



- Il se compose de quatre morceaux : l'expéditeur, le sous-ensemble de traitement de message, le sous-ensemble de sécurité, et le sous-ensemble de contrôle d'accès. Le travail de l'expéditeur est d'envoyer et recevoir des messages. Il essaye de déterminer la version de chaque message reçu (c.-à-d., v1, v2, ou v3) et, si la version est soutenue, remet le message au loin au sous-ensemble de traitement de message. L'expéditeur envoie également des messages de SNMP à d'autres entités .

- Le sous-ensemble de traitement de message prépare des messages pour être envoyé et extrait des données à partir des messages reçus. Un système de traitement de message

peut contenir des modules de traitement de message multiple. Par exemple, un sous-ensemble peut avoir des modules pour traiter les demandes SNMPv1, SNMPv2, et SNMPv3. Il peut également contenir un module pour d'autres modèles de traitement qui doivent être définis encore

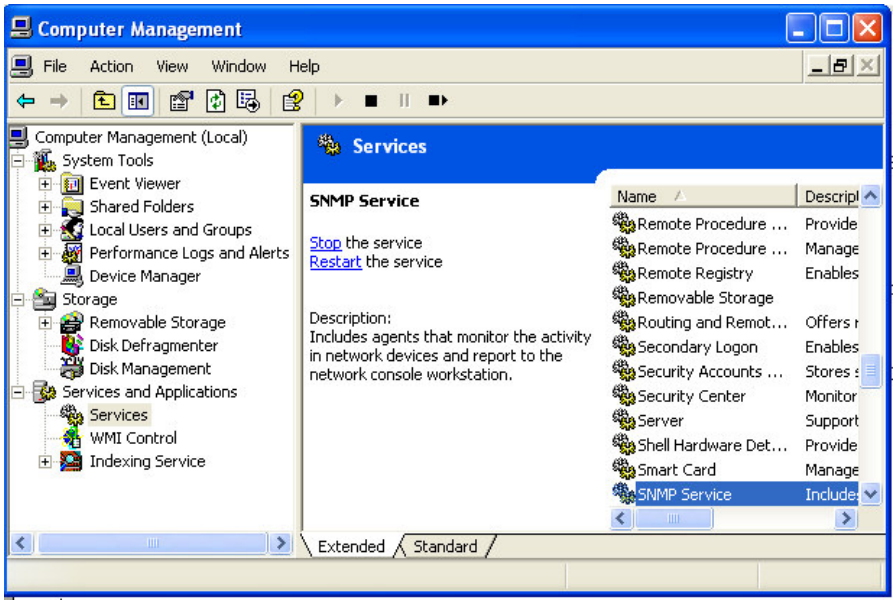
- Le sous-ensemble de sécurité fournit des services d'authentification et d'intimité. L'authentification emploie des valeurs de la communauté (versions 1 et 2 de SNMP) ou l'authentification utilisateur-basée par SNMPv3. l'authentification Utilisateur-basée emploie les algorithmes de **MD5** ou de **SHA** pour authentifier des utilisateurs sans envoyer un mot de passe dans l'espace libre. Le service d'intimité emploie l'algorithme de **DES** pour chiffrer et déchiffrer des messages de SNMP. Actuellement, le **DES** est le seul algorithme utilisé, bien que d'autres puissent être ajoutés à l'avenir .

Chapitre IV. Partie pratique

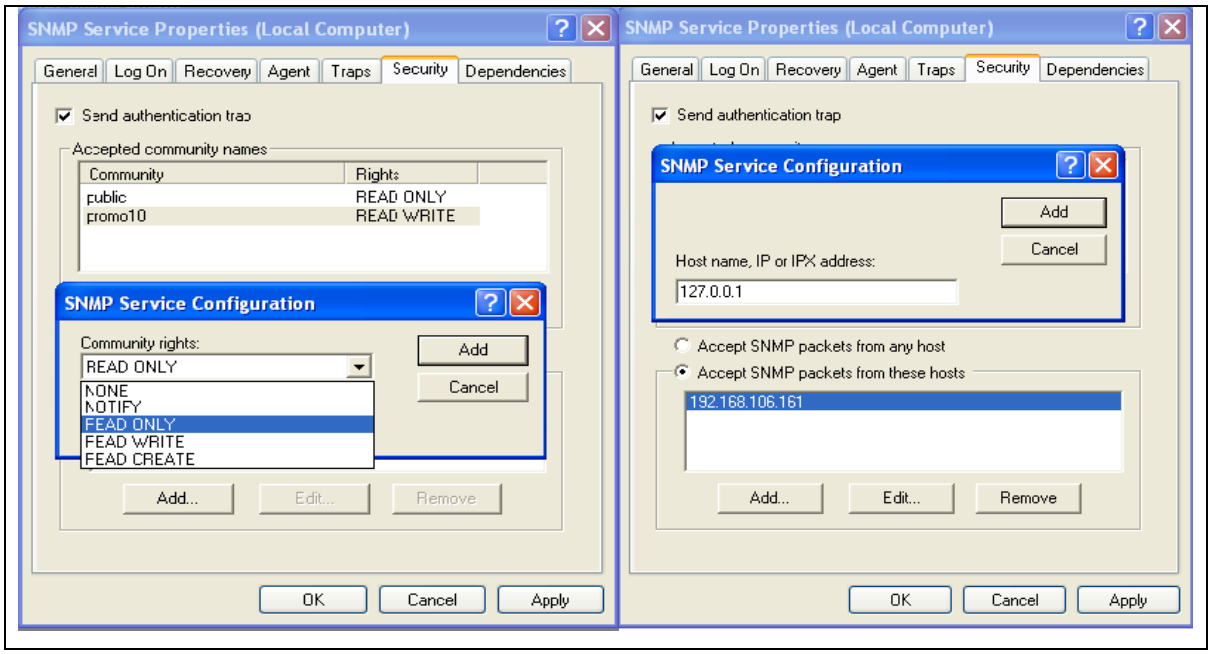
4.1. Manipulation de SNMP sous Windows

L'installation de SNMP sous Windows ne pose guère de problèmes. Il faudra juste faire un peu attention à ne pas laisser l'accès à n'importe qui sur n'importe quoi.

Gérez le poste de travail, par exemple en cliquant du bouton droit sur "Poste de travail" dans le menu



Configurer le champ communauté (community) pour la sécurité et spécifie les stations qui peut accéder à cet agent là.



4.2. Manipulation SNMP et manipuler sous Linux

La mise en pratique de SNMP est présentée au travers la mise en oeuvre du package NETSNMP.NET-SNMP supporte toutes les trois versions SNMPv1, SNMPv2 et SNMPv3 que ce soit côté agent SNMP comme du côté manager SNMP via les commandes en ligne NET-SNMP.

4.2.1. Installation de NET-SNMP

L'installation de NET-SNMP est des plus traditionnels sous Linux :

Décompression :

```
# cd
# tar xvzf net-snmp-5.0.2.tar.gz
# ln -s net-snmp-5.0.2 net-snmp
```

Configuration. On choisira d'utiliser par défaut SNMPv1 :

```
# cd ~/net-snmp
# ./configure
```

Compilation :

```
# make
```

Installation :

```
# make install
```

Les commandes Linux NET-SNMP sont recopiées dans le répertoire /usr/local/bin et /usr/local/sbin qu'il faudra rajouter à sa variable d'environnement PATH.

Les fichiers correspondants aux MIBs exploités côté manager SNMP par les commandes en ligne NET-SNMP sont sous /usr/local/share/snmp/mibs.

4.2.2. Configuration et lancement de l'agent SNMP NET-SNMP

L'agent SNMP NET-SNMP est l'exécutable snmpd sous /usr/local/sbin. Il possède un fichier de configuration général s'appelant snmpd.conf à copier sous /usr/local/share/snmp.

Le point le plus important est qu'on doit configurer les valeurs du champ communauté pour controller la validation.

```
syscontact nmtuong@ifi.edu.vn
syslocation Le placard de l'entree

# 1° créer des relations entre les communautés et des noms de sécurité
#       nom.secu          source                  communaute (comme un mot de passe)
com2sec Local           localhost                 promotion10
com2sec IFILocal       192.168.106.0/24         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             IFILocal
#3° Créer les diverses vues qui seront autorisées aux groupes
#
view    tout        included      .1

#4° Indiquee 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
……..
```

La valeur de communauté "public" pourra lire la totalité de la MIB depuis n'importe quelle machine du LAN (192.168.106.0/24), la communauté "promotion10" pourra lire et écrire partout où ce sera possible dans la MIB, uniquement depuis le poste local (localhost).

4.2.3. Tests de l'agent SNMP NET-SNMP

Le test de l'agent SNMP NET-SNMP se fait en utilisant un manager SNMP. Dans le cas du package NET-SNMP, on a accès à des commandes en ligne sous /usr/local/bin

permettant d'émettre des requêtes SNMP.

Il convient d'abord de configurer son environnement Linux. Pour accéder aux objets de la MIB d'un agent sous forme symbolique et non sous forme décimale OID, il faut aller lire l'ensemble des fichiers MIB sous /usr/local/share/snmp/mibs :

```
#
# PATH
#
PATH=$PATH:/usr/local/bin:/usr/local/sbin
#
# MIBS : forces to read all MIB files under /usr/local/share/snmp/mibs
#
MIBS=ALL
#
# exporting all variables
#
export PATH MIBS
```

- Récupération par SNMPv1 de la valeur courante de l'objet sysUpTime géré par l'agent SNMP de la machine localhost :

```
# snmpget -v 1 -c promotion10 localhost system.sysUpTime.0
SNMPv2-MIB::sysUpTime.0 = Timeticks: (12908) 0:02:09.08
```

- Récupération de la valeur courante de l'objet sysUpTime avec SNMPv2c :

```
# snmpget -v 2c -c promotion10 localhost system.sysUpTime.0
SNMPv2-MIB::sysUpTime.0 = Timeticks: (13966) 0:02:19.66
```

4.3. Utilisation de PRTG pour surveiller le trafic du réseau

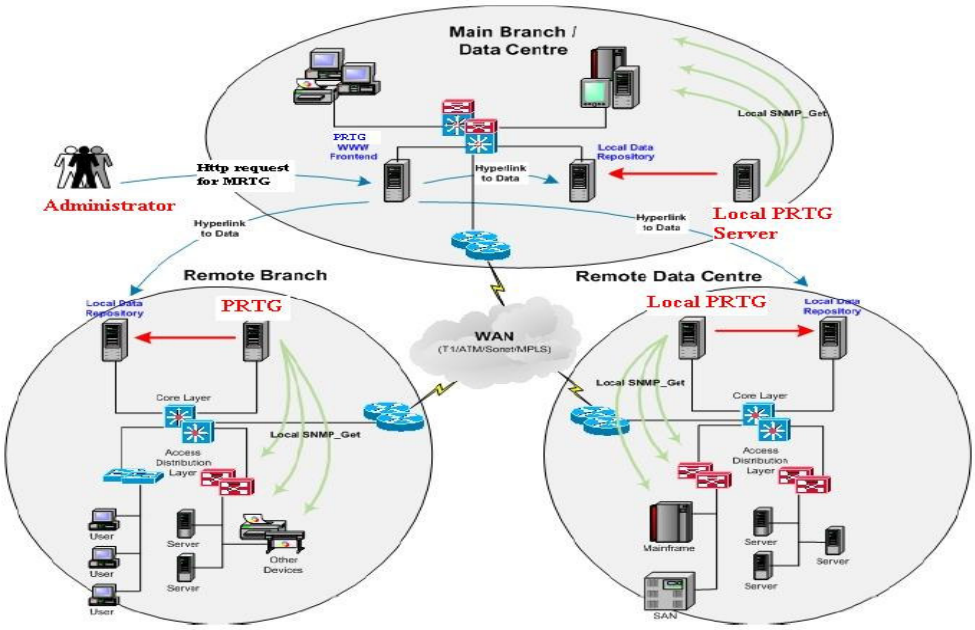
PRTG est une application d'administration réseaux qui peut surveiller n'importe quelle machine qui exécute le protocole SNMP. Il est une applications qui exécute des requêtes SNMP pour interro ger un agent (serveur/routeur) de façon intermittente. Il obtient ses données SNMP de la façon suivante:

- Interroge l'agent et obtient les valeurs spécifiques d'un OID SNMP.
- Met à jour la graphique variable avec les nouvelles valeurs et supprime l'ancien graphique. La nouvelle version du graphique est sauvegardée à un emplacement qui peut être local ou distant.
- Marque les nouvelles valeurs dans un fichier de carnet de bord (log). Ce fichier

peut être en local ou sur une machine distante.

La version classique de PRTG construit les graphiques immédiatement après avoir obtenu une nouvelle valeur SNMP, il ne conserve pas l'historique des données pour une futur référence.

Voilà l'architecture de PRTG



….

Conclusion

Dans le modèle OSI, Il existe un protocole connu pour la gestion de réseaux CMIP, CMOT (Version de CMIP dans le monde TCP/IP). Il est un protocole orienté connexion, c'est à dire que chaque message est acquitté. CMIP est basé sur un principe de notification et d'événement. L'avantage principal du CMIP est la sécurisé, il peut fonctionner sur des réseaux hétérogènes mais leur inconvénient est la complexité. À cause du problème, il n'est pas utilisé largement dans la réalité.

En effet, dans le monde TCP/IP, Le protocole SNMP est un protocole simple, il garde largement l'avantage et donc est une bonne solution pour la gestion des réseaux informatiques. Cependant, les faiblesses dans ce protocole est la sécurité. Dans des ses dernières versions, les faiblesses sont plus améliorées. Mais avec leurs avantages connus, SNMP est la meilleure solution pour gérer un réseau informatique. C'est la raison pour laquelle la plupart réseaux informatiques, aujourd'hui, l'utilisent.

Références

[1] . Network Management:

- M. Sloman, *Network and Distributed Systems Management*, Addison Wesley, 1994.
- W. Stallings: *SNMP, SNMPv2 and CMIP: The Practical Guide to Network Management Standards*, Addison-Wesley, 1993.

[2]. Sécurité : Protocole SNMP
http://www.securinfo.umontreal.ca/general/texte_snmp.html

[3]. Admnistration des réseaux. http://duda.imag.fr/PS/3-eme-annee/SDTR-1998/Administration.ppt

[4]. Les RFC disponibles à http://www.rfc-editor.org/

SNMPv1 : RFC 1155 1156 1157

SNMPv2 : RFC 1902 1903 1904 1905 1906 1907

SNMPv3 : RFC 3411 3412 3413 3414 3415 3416 3417 3418

CMIP : RFC 1189

[5]. SNMP V3. http://www.hn.edu.cn/book/NetWork/NetworkingBookshelf_2ndEd/snmp/appf_01.htm#enettdg-APP-F-FIG-1.html

[6]. Des faiblesses dans le protocole réseau SNMP. http://www.laboratoire-microsoft.org/n/securite/

[7]. CMIP(Common Management Protocol) http://www.linktionary.com/c/cmip.html

[8]. CMIP/CMIS - Object Oriented Network Management.
http://www.cellsoft.de/telecom/cmip.htm

[9]. Common Management Information Protocol.
http://www.sei.cmu.edu/str/descriptions/cmip_body.html

[10]. Administration SNMP. http://www.jalix.org/ressources/reseaux/tcp-ip/_guide-internet/guide/snmp.htm

[11]. MRTG and SNMP Concepts. http://vegan.net/MRTG/concepts.php

[12]. Installation des services SNMP sous Linux
http://www.xenux.net/?article=50&skin=skin1

[13].PRTG Traffic Grapher
http://www.pcactual.com/Laboratorio/Productos/Comunicaciones/Internet/20040607017