

## **Table des matières :**

Remerciements.....	3
INTRODUCTION : .....	4
NOKIA SIEMENS NETWORKS.....	5
NSN MAROC .....	5
CHAPITRE I : INTRODUCTION AUX CONCEPTS DE BASE DE LA GESTION DE RESEAU .....	8
I.1 LA GESTION RESEAU .....	8
I.2 RESSOURCE A GERER .....	8
I.3 ORGANISATION D'UNE ADMINISTRATION .....	8
I.4 LES SYSTEMES DE GESTION DE RESEAU .....	9
I.5 MODELE DE GESTION .....	9
I.6 PRINCIPE GENERAL D'ADMINISTRATION .....	10
I.7 ARCHITECTURE D'ADMINISTRATION .....	10
I.8 CONCLUSION .....	11
CHAPITRE II : LE PROTOCOLE SNMP.....	12
II.1 HISTORIQUE .....	12
II.2 PRESENTATION DU PROTOCOLE SNMP .....	12
II.3 LES COMPOSANTS DE BASE DE SNMP .....	13
II.4 PRINCIPE DE FONCTIONNEMENT .....	14
II.5 STRUCTURE SMI (STRUCTURE OF MANAGEMENT INFORMATION) .....	17
II.6 MIB (MANAGEMENT INFORMATION BASE) .....	18
II.6.1 LA STRUCTURE DE DONNEES MIB .....	18
II.6.2 LES TABLES MIB .....	20
II.6.3 EXEMPLE ILLUSTRATIF .....	22
II.7 LES DIFFERENTES VERSIONS DE SNMP .....	23
II.8 LA SECURITE .....	23
II.9 AVANTAGES ET INCONVENIENTS .....	24
CONCLUSION .....	24
CHAPITRE III IMPLEMENTATION JAVA DE L'APPLICATION DE GESTION .....	25
MON TRAVAIL CONSISTE D'IMPLEMENTER UNE APPLICATION JAVA POUR LA SUPERVISION ET LA GESTION DU RESEAU .....	25
III.1 PRESENTATION DU LANGAGE JAVA .....	26
III.1.1 LES CARACTERISTIQUES .....	26
III.2 OUTILS DE DEVELOPPEMENT .....	27
III.3 PRESENTATION DE L'APPLICATION .....	27
III.3.1 ENVIRONNEMENT DE DEVELOPPEMENT .....	27
III.3.2 EXPLICATION DU PROGRAMME .....	27
III.4 LORIOTPRO .....	27
III.4.1 INTRODUCTION .....	27
III.4.2 PERIMETRE D'UTILISATION .....	28
III.4.3 VISUEL ET ERGONOMIQUE.....	28
III.4.4 PERFORMANCE ET COMPATIBILITE AUX STANDARDS. ....	29
III.4.5 INTRODUCTION A LA SIMULATION D'INTERRUPTION SNMP ET NOTIFICATION SNMP .....	29

III.4.6 ENVOI DES TRAPPES SIMULEES ET LA NOTIFICATION .....	31
III.5 MYSQL ODBC .....	33
III.5.1 INTRODUCTION .....	34
III.5.2 ONGLET SOURCES DE DONNEES UTILISATEUR .....	35
III.5.3 AJOUT DU SUPPORT DE PHP POUR LORITPRO WEB SERVER .....	37
III.6 CREATION DE BASE DE DONNEES AVEC PHPMYADMIN .....	38
III.6 CONFIGURATION DE TRAP SOUS WINDOWS .....	41
CONCLUSION GENERAL .....	43

## REMERCIEMENTS

Au début, je tiens à remercier le corps administratif et professoral de la Faculté des sciences et techniques de Fès, pour l'enseignement de qualité qu'ils m'ont prodigué tout au long de mon cursus universitaire.

Je remercie mon encadrant le professeur ECHATOUI Nor-Said et le professeur ABARKAN Houssine pour la précieuse assistance et le suivi qu'ils ont apportés à l'évolution de mon projet, pour leur qualité d'encadrement et leur grand soutien. Je voudrais également remercier Mr. BOURAGBA Hamza et Mr. LAAZRI Abdellahet chef de département Network planning Mme RAHMANI Ikram Directeur entreprise pour leurs conseils, leur aide et leur bonne humeur. Cette entité a été pour moi un bon exemple de collaboration, ce qui a permis à mon stage de se dérouler dans d'excellentes conditions.

Enfin, j'adresse mes remerciements aux membres du jury qui ont accepté d'évaluer mon travail, et aussi à toute personne ayant contribué de près ou de loin, à l'élaboration de mon projet.

## INTRODUCTION :

Les réseaux informatiques ont aujourd'hui autant d'importance que les ordinateurs eux mêmes, au point que la plupart de nos activités ne pourraient plus être envisagées sans la mise en place de ces réseaux.

L'évolution des réseaux en multiplication du nombre des machines, et la complexité géographiquement augmentante pose un problème majeur sur la manière dont ceux-ci sont pratiquement gérée.

Pour la résolution de ce problème on peut utiliser l'oriotPro qui permet d'analyser le réseau et de détecter des panes et les stocker dans une base de données à l'aide du protocole SNMP.

Comme son nom l'indique le protocole SNMP, simple network management protocole (protocole de gestion de réseau simplifié) qui est actuellement à sa version 3, standardisée par l'IETF de puis Mars 2002, version qui constitue le fruit de plusieurs études et recherches au domaine de sécurité et de communication depuis 1988.

Ce protocole que nous allons étudier plus en détails au cours de ce travail a pour rôle exclusif la gestion de réseau, il à été développé pour apporter des moyens simple d'administration en distance aux administrateurs.

Cette étude comporte 3 chapitres brièvement décrits comme suivent :

- Le chapitre 1 est une introduction aux concepts de base de la gestion de réseau ; il permet de comprendre les enjeux stratégiques de la gestion et de se familiariser avec ses activités. Il présente une méthode qui permet à l'administrateur réseau de concevoir une architecture de gestion.
- Le chapitre 2 décrit le protocole SNMP. Il explique le fonctionnement, les différentes composantes d'une architecture de gestion basée sur SNMP et montre les échanges entre la station de gestion et les agents SNMP à des fins de surveillance.
- Le chapitre 3 traite l'implémentation de l'application en java. Il montre pas à pas comment ont peut mettre au point une application de supervision en se base sur le protocole SNMP en java.

## Nokia Siemens Networks

Dans ce qui suit, nous donnons un bref historique sur Nokia, puis nous allons présenter Nokia Siemens Networks (NSN), la nouvelle entreprise née de la fusion de Nokia Networks et Siemens COM, et en particulier la division NSN du Maroc.

### 1. Divisions de Nokia

Nokia est un leader mondial des télécommunications mobiles, et joue un rôle primordial dans la croissance et l'épanouissement de l'industrie de la mobilité. Nokia enrichit la vie quotidienne des utilisateurs et accroît la productivité des entreprises en fournissant des produits sécurisés et simples à utiliser.

Depuis le début de l'année 2004, Nokia est organisée en quatre Business Groups :

- **Mobile Phones** : développe et produit des téléphones mobiles, basés principalement sur les technologies GSM, CDMA et TDMA.
- **Multimédia** : développe des terminaux mobiles avancés qui intègrent des fonctionnalités aux télécommunications telles que l'imagerie, les jeux, la musique, les médias et les technologies informatiques.
- **Networks** : est un des principaux fournisseurs d'équipements d'infrastructure réseau, de plates-formes de fourniture de services et de services associés en direction des opérateurs mobiles et des fournisseurs de services.
- **Enterprise solution** : propose des terminaux d'entreprise, des solutions de sécurité de réseau IP, des solutions «firewalls» et réseaux privés virtuels (VPN), et des solutions de connectivité mobile.

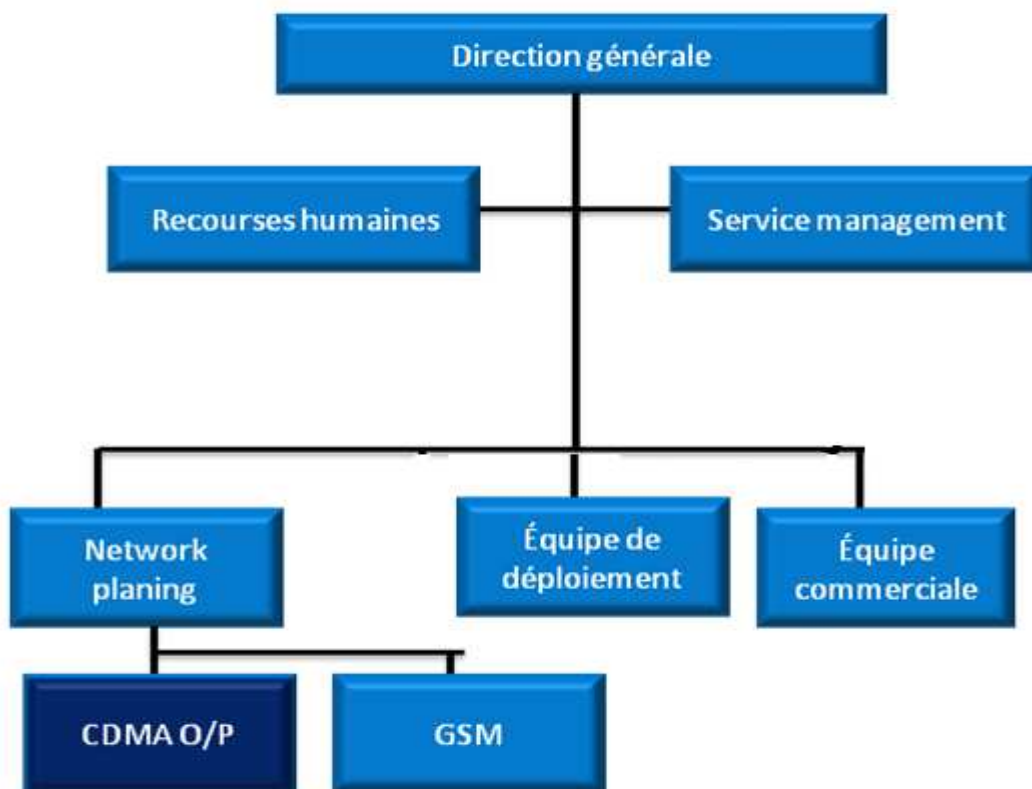
Le 18 juin 2006, Nokia et Siemens annoncent la fusion de leurs activités de télécommunications, donnant ainsi naissance à un géant multinational : Nokia Siemens Networks (NSN)

### NSN Maroc

Nokia Siemens Networks Maroc fait partie de *Nokia Siemens Networks Business Group*, et collabore étroitement avec *Maroc Telecom*, premier opérateur mobile au Maroc.

NSN Maroc fournit, principalement, à son client *Maroc Telecom*, les équipements du réseau radio GSM ainsi que les prestations de services associés.

L'architecture organisationnelle de NSN Maroc, où s'est déroulé mon stage, est concentrée autour de trois pôles principaux :



### **Le Network Planning**

Il représente le cœur du travail de NSN Maroc. Il s'occupe de la partie technique (planification du réseau, dimensionnement, optimisation et maintenance du réseau BSS de Maroc Telecom). Le groupe de Network Planning est divisé par zones géographiques ; une équipe s'occupe du projet de Casablanca, une autre de celui de Rabat et une troisième pour la zone Nord Est. Ces différentes équipes sont supervisées par un manager.

### **Une équipe commerciale**

Cette équipe se charge de toutes les procédures financières, l'établissement des comptes de NSN Maroc et la planification du budget pour chaque six mois.

## **Une équipe de déploiement**

Elle se charge de négocier l'installation des nouveaux sites avec les propriétaires dans le cas des contrats Télécom, de la supervision de la construction des sites et de la fourniture du matériel.

# **CHAPITRE I : INTRODUCTION AUX CONCEPTS DE BASE DE LA GESTION DE RESEAU**

## **I.1 La gestion reseau**

La gestion de réseau est la tâche quotidienne de tout administrateur réseau. Il s'agit entre autre d'assurer le suivi du réseau, de définir des procédures et de les faire connaître aux utilisateurs, de gérer les mots de passe, de prendre en charge le suivi des sauvegardes et résoudre les éventuels incidents qui peuvent survenir. Au-delà, anticipé les évolutions technologiques et intégrer de nouveaux outils de gestions. Vérifier le fonctionnement optimal de chaque matériel, paramétrer celui-ci, ou de le mettre à jour régulièrement. Ainsi, dans les réseaux informatiques d'aujourd'hui, la gestion est un problème de tous les jours. Le recours à des techniques d'administration efficace est important pour une bonne gestion économique des moyens de communication dont on dispose, mais aussi pour avoir une vue d'ensemble des équipements et des systèmes de communication utilisés par l'entreprise. C'est à niveau qu'intervient l'administration réseau.

L'administration réseau met en œuvre des moyens humains, techniques, et financières de contrôle, de coordination et de surveillance des diverses ressources mise en œuvre en respectant les contraintes de coûts et de qualité. Avec objectif, de maintenir le service et de permettre l'évolution du système.

## **I.2 Ressource à gérer**

Plusieurs niveaux de gestion doivent être distingués, dont il est nécessaire de comprendre l'utilité. Un bon critère de différenciation peut être appliqué à partir des éléments constitutifs du réseau, soit des équipements réseau, des ordinateurs, des logiciels, ou des utilisateurs. À titre d'exemple :

- ✚ La gestion de l'infrastructure réseau : elle concerne la gestion de tous les éléments du réseau et des logiciels embarqués qui constituent les différents réseaux de l'entreprise. On désigne par élément du réseau chacun des équipements qui sont branchés au réseau, ainsi que les logiciels y résidant. Les routeurs, les concentrateurs, les répéteurs, les passerelles, les modems, la connectivité, sont les éléments qui constituent l'infrastructure du réseau.
- ✚ La gestion des ordinateurs : elle concerne tous les aspects relatifs à la gestion des points d'accès au réseau. Elle englobe la gestion des stations terminales, ainsi que de tous les logiciels supportés par ces stations : système d'exploitation réseau, les applications et les services de communication mis à la disposition des usagers

## **I.3 Organisation d'une administration**

Il existe différents types de décision d'administration :

- ❖ Décisions opérationnelles : décision à court terme, concernant l'administration au jour le jour et opérations temps réel sur le système.
- ❖ Décisions tactiques : décision à moyen terme concernant, l'évolution du réseau et l'application des politiques de long terme.
- ❖ Décisions stratégiques : décision de long terme concernant les stratégies pour le futur en exprimant les nouveaux besoins et désirs des utilisateurs.
- ❖ Ces types déterminent différents niveaux d'administration:
  - Le contrôle opérationnel réseau pour les décisions Opérationnelles
  - La gestion réseau pour les décisions tactiques
  - L'analyse de réseau pour les décisions tactiques et stratégiques
  - La planification pour les décisions stratégiques

## I.4 Les systèmes de gestion de réseau

Un système de gestion réseau est une collection d'outils pour contrôler et gérer le réseau qui comprend :

- ❖ Une interface pour opérateur avec un ensemble de commandes pour exécuter la plupart des tâches d'administration de réseaux.
- ❖ Un minimum d'équipements supplémentaire intégré au système existant

## I.5 Modèle de gestion

La mise en œuvre de la gestion se fait à travers le modèle d'administration suivante :

- ❖ Le modèle informationnel.
- ❖ Le modèle organisationnel.
- ❖ Le modèle Fonctionnel.
- ❖ Le modèle de communication.
- ❖ L'administration dans le réseau IP utilise seulement deux modèles à savoir :
  - Le modèle informationnel.
  - Le modèle de communication.

### Le modèle Informationnel

Il permet de définir les objets administrés (nom, fonction, relations et attributs divers). La base de données ainsi constituée est appelée MIB. Cette base est organisée de manière hiérarchique sous forme d'arbre. La description des objets dans la MIB est faite en utilisant la syntaxe ASN1 (Abstract Syntax Notation one).

### Le modèle de communication

Ce modèle sous entend, un protocole dédié aux échanges de gestion, des messages de commandes/réponse et des messages de notification.



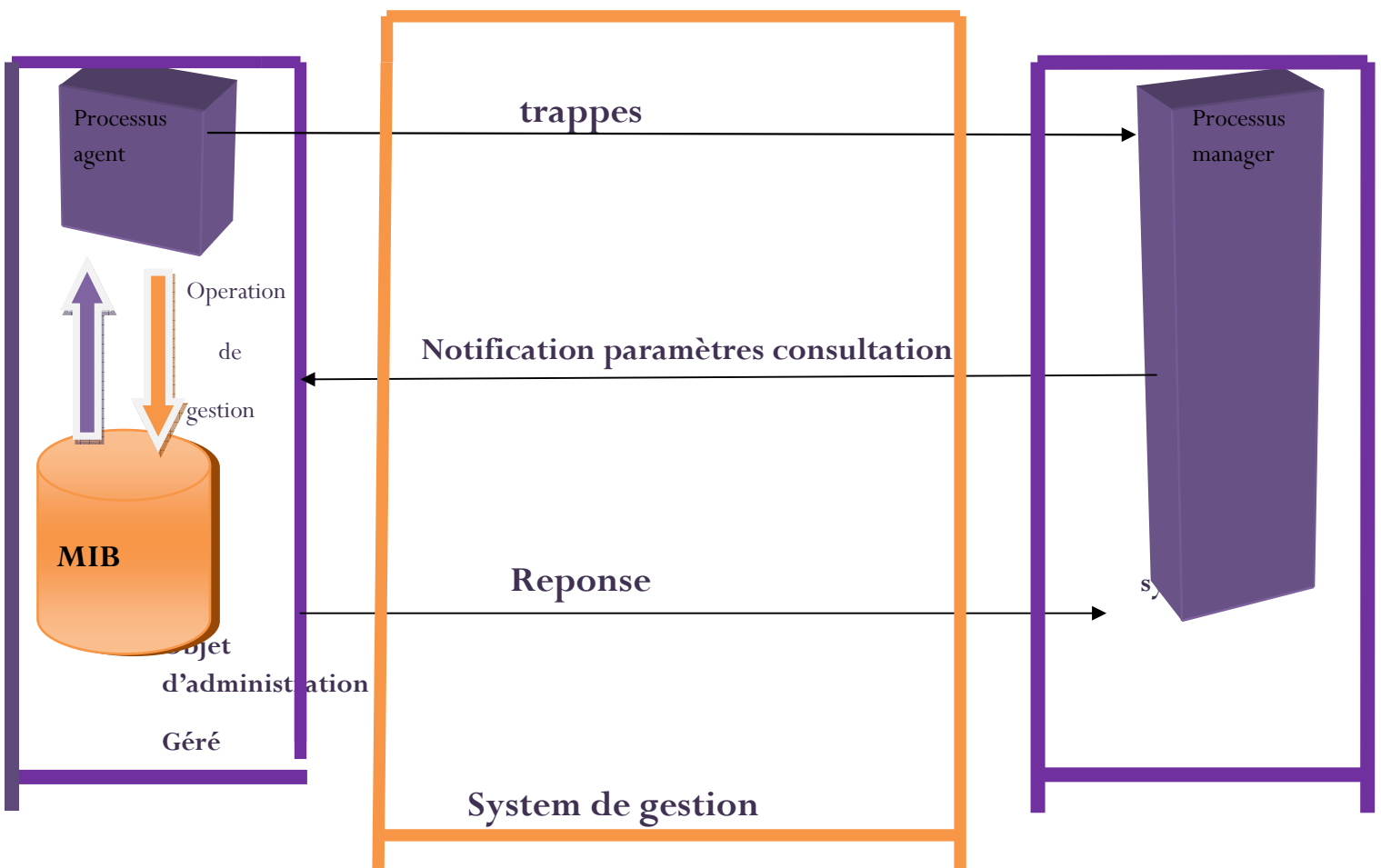
## I.6 Principe général d'administration

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 qui le met en relation avec les divers agents.

Le principe se repose donc sur les échanges :

- ❖ Entre une base d'informations appelée MIB (Management Information Base) et l'ensemble des éléments administrés (objets).
- ❖ Entre les éléments administrés et le système d'administration.



## I.7 Architecture d'administration

L'architecture classique d'administration la plus utilisée est le modèle Gérant/ Agent (Manager/Agent), comme nous l'avons montré dans les principes d'administration. Le système est

composé d'une entité d'administration et des entités de gestion (NME) qui sont géré par cette entité et un protocole pour la gestion

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 commandes 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.

## 1.8 Conclusion

Ce chapitre nous a permis de présenter les concepts de base de la gestion de réseau pour aider l'administrateur dans sa tâche de conception d'un système de gestion optimal en fonction des objectifs de l'entreprise. Le chapitre suivant sera consacré à l'étude du protocole SNMP qui est une solution de gestion envisagé dans cette étude.

## Chapitre II : LE PROTOCOLE SNMP

### II.1 Historique

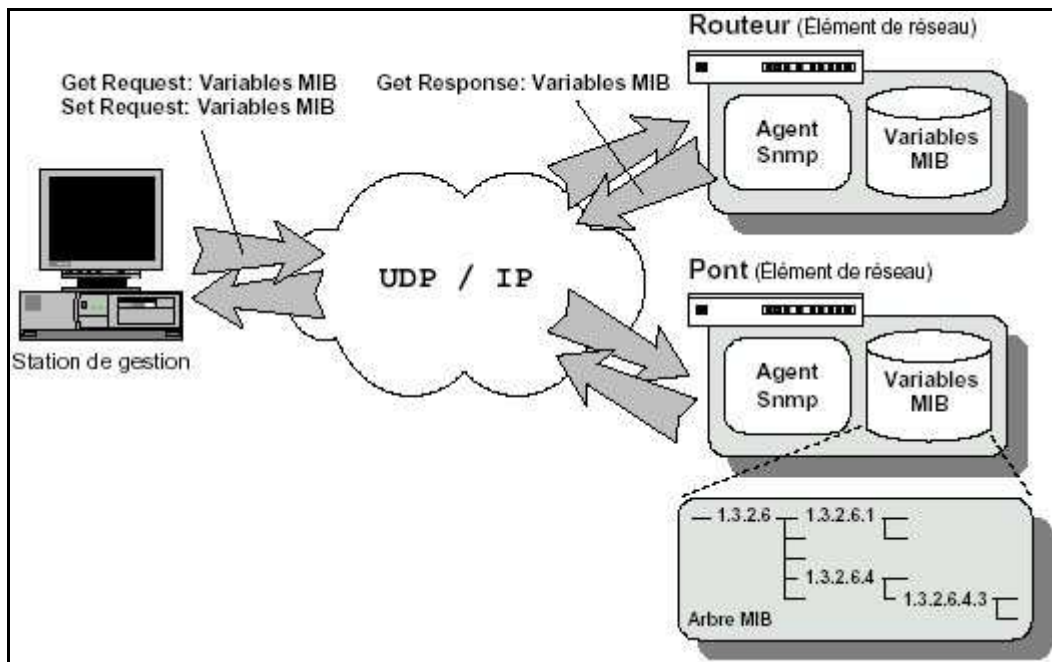
SNMP (Simple Network Management Protocol) a été défini par l'IETF (Internet Engineering Task Force) en 1989. Depuis, il est devenu un standard pour la gestion de réseaux. Il permet de faciliter l'échange d'information d'administration entre différentes entités d'un réseau pour disposer d'une cartographie du réseau, fournir un inventaire précis de chaque entité, gérer les Performances, détecter et résoudre des problèmes.

### II.2 Présentation du protocole SNMP

**SNMP** acronyme de « Simple Network Management Protocol » est le protocole de gestion de réseaux proposé par l'IETF. Il est actuellement le protocole le plus utilisé qui permet aux administrateurs réseau de gérer les équipements du réseau et de diagnostiquer les problèmes de réseau.

L'environnement de gestion SNMP est constitué de plusieurs composantes : une station de gestion de réseau (NMS- Network Management Stations), des éléments de réseaux (NE, Network Elements), des variables MIB et un protocole. Les différentes composantes du protocole SNMP sont les suivantes:

- **Les éléments réseaux** sont les équipements ou les logiciels que l'on cherche à gérer (concentrateur, routeur, pont, etc.). Chaque élément réseau dispose d'une entité dite **agent** de réseaux qui répond aux requêtes de la plate-forme de gestion.
- **Les agents** sont des modules qui résident dans les éléments réseau. Ils vont chercher l'information de gestion.
- **La plate-forme de gestion du réseaux (appelé aussi manager)** exécute les applications de gestion qui contrôlent les éléments réseaux.
- **Une MIB** (*Management Information Base*) est une collection d'objets résidant dans une base d'information virtuelle.



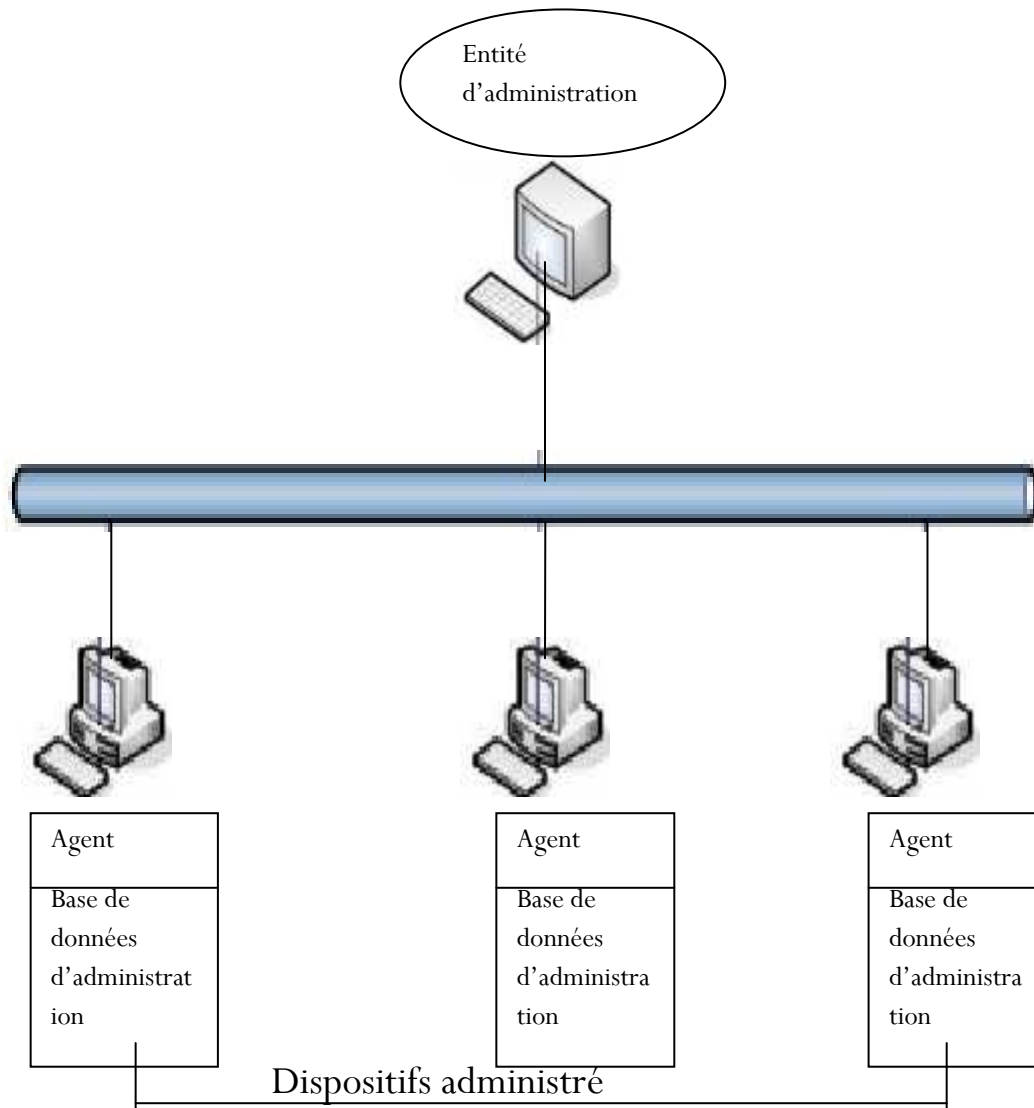
Environnement SNMP

## II.3 Les composants de base de SNMP

Un réseau administré par SNMP dispose de trois composants clé : les dispositifs administrés, les agents et les systèmes d'administration réseau (NMS, Network Management System).

- ✚ Un dispositif administré est un nœud réseau qui contient un agent SNMP et qui réside sur un réseau administré. Les dispositifs administrés collectent et conservent des informations d'administration, et rendent ces informations disponibles aux NMS à l'aide de SNMP. Les dispositifs administrés, parfois appelés « éléments réseau », peuvent être des routeurs, des serveurs d'accès, des commutateurs, des ponts, des hubs, des hôtes ordinateurs ou des imprimantes.
- ✚ Un agent est un module logiciel d'administration réseau qui réside sur un dispositif administré. Un agent possède une connaissance locale des informations d'administration et traduit celle-ci en un format compatible avec SNMP.
- ✚ Un NMS Les systèmes de gestion de réseau (network management system notés NMS): C'est-à-dire une console au travers de laquelle les administrateurs peuvent réaliser des tâches d'administration, exécutent des applications qui surveillent et contrôlent des dispositifs administrés. Un NMS fournit l'essentiel des ressources de traitement et mémoires nécessaires à l'administration réseau. Il doit y avoir un ou plusieurs NMS sur un réseau administré.

SNMP est un protocole d'administration distribuée. Un système peut opérer soit comme un NMS, soit comme un agent, ou les deux à la fois. Lorsqu'un système fonctionne comme NMS et agent, un autre NMS est susceptible d'exiger que le système interroge des dispositifs administrés qui fournissent un résumé des informations apprises ou rapportent les informations d'administration conservées en local.

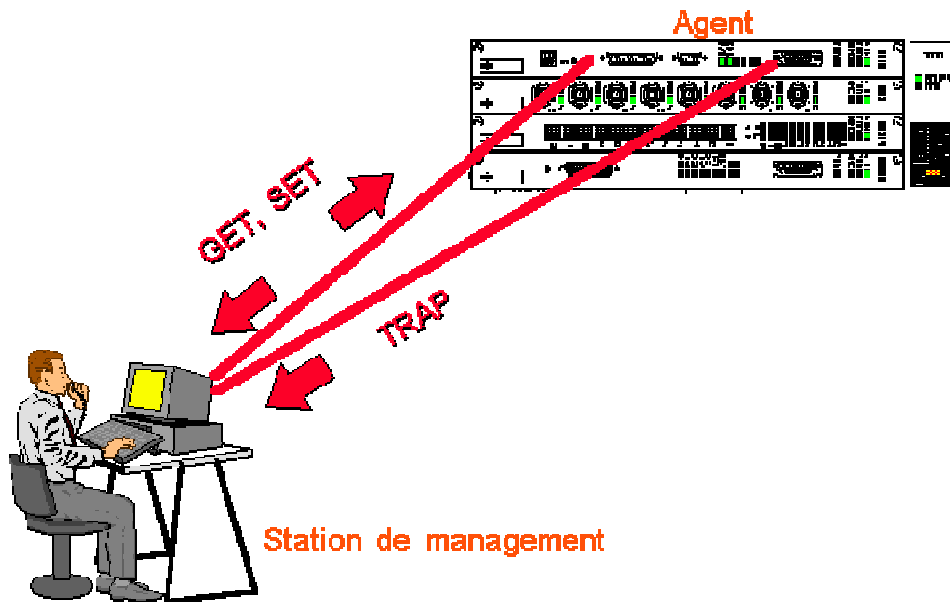


## II.4 Principe de fonctionnement

Le système de gestion de réseau est basé sur deux éléments principaux: un superviseur et des agents. Le superviseur est la console qui permet à l'administrateur réseau d'exécuter des requêtes de management. Les agents sont des entités qui se trouvent au niveau de chaque interface connectant l'équipement managé au réseau et permettant de récupérer des informations sur différents objets.

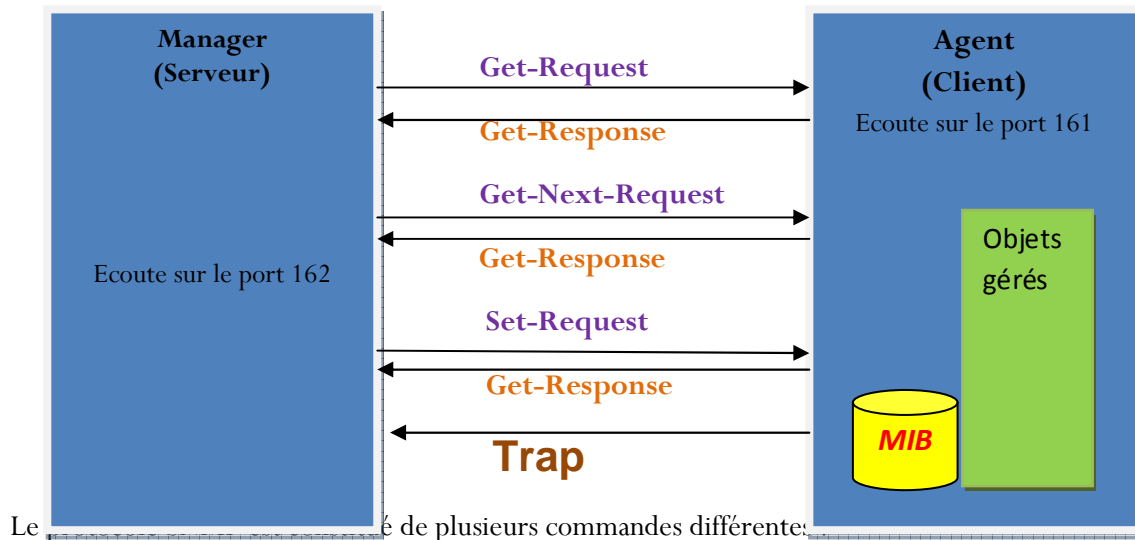
Switchs, hubs, routeurs et serveurs sont des exemples d'équipements contenant des objets manageables. Ces objets manageables peuvent être des informations matérielles, des paramètres de configuration, des statistiques de performance et autres objets qui sont

directement liés au comportement en cours de l'équipement en question. Ces objets sont classés dans une sorte de base de donnée appelée MIB ("Management Information Base"). SNMP permet le dialogue entre le superviseur et les agents afin de recueillir les objets souhaités dans la MIB.



SNMP utilise le protocole UDP. Deux ports sont désignés pour l'utilisation de SNMP :

- Port 161 pour les requêtes à un agent SNMP.
- Port 162 pour l'écoute des alarmes destinées à la station d'administration.



Le **Trap** est une commande de plusieurs commandes différentes:

<b>GetRequest</b>	envoyée par le manager à l'agent, a pour objectif de demander une information à l'agent.
<b>GetNextRequest</b>	Obtenir directement le contenu de la variable suivante.

<b>get-reponse</b>	L'agent SNMP répond à un get-request ou a un set-request
<b>SetRequest</b>	définir la valeur d'une variable de l'agent administré. Cela permet d'effectuer des modifications sur le matériel.
<b>Trap</b>	Un message d'information est envoyé à la station d'administration lorsqu'un événement particulier ou anormal survient.

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

Type PDU (Protocol Data Unit)	Nom
0	GetRequest
1	GetNextRequest
2	SetRequest
3	GetResponse
4	Trap

### 🌀 Format des messages SNMP

En-tête commune SNMP			En-tête à lire et à positionner			Variables à lire et à positionner				
Version(0)	Communauté	TypePDU (0-3)	Id.requête	Status d'erreur	Index d'erreur	Nom var.	Valeur var.	Nom var.	Val var.	..

			En-tête de trap				Variables		
Version(0)	Communauté	TypePDU (0-3)	entrepris e	Adresse agent	Type de trap (0-7)	Code spécifique	Nom var.	Val var.	..

### 🌀 **Champ commun :**

- Version du protocole : Ce champ correspond à la version de SNMP. On place la valeur zéro dans le champ version pour SNMPv1, et la valeur 3 pour SNMPv3.
- Nom de communauté: il permet de s'assurer de l'identité de l'expéditeur du message (Mot de passe).
- Type: Il contient le type du PDU SNMP.

### ⌘ Champ PDU des messages « requête » :

- id. requête: Le champ identificateur de la requête est défini par le manager lors de l'envoi d'une requête et utilisé par l'agent dans sa réponse. Cela permet d'associer la réponse à la requête vu que le protocole transport utilisé est UDP.
- Statut erreur : est l'indicateur du type d'erreur. Il est positionné par l'agent. Si aucune erreur ne s'est produite, ce champ est mis à zéro. Les réponses négatives possibles sont :

Statut D'erreur	Nom	Description
0	<i>noError</i>	Pas d'erreurs.
1	<i>tooBig</i>	Réponse de taille trop grande.
2	<i>NoSuchName</i>	Variable inexistante.
3	<i>badValue</i>	Ecriture d'une valeur invalide.
4	<i>readOnly</i>	Variable en lecture seule.
5	<i>genErr</i>	Autre erreur.

- Index erreur : Il indique la variable qui a provoqué l'erreur (uniquement dans les cas *noSuchName*, *badValue* et *readOnly*).
- Une liste des noms de variables et de leurs valeurs termine le message.
- 

## II.5 Structure SMI (Structure Of Management Information)

La structure SMI décrit les règles de description de l'information et permet d'identifier d'une façon unique un objet de la MIB géré par un agent SNMP. Chaque objet possède donc un identificateur unique ou OID (Object ID).

SMI s'intéresse aussi à la représentation des données (et leur type) pour chaque objet de la MIB. Un objet de la MIB est déclaré et défini en langage ASN.1 (Abstract Syntax Notation 1 : langage de représentation de donnée).

SNMP n'utilise qu'une petite partie du langage ASN.1. Au niveau des types, seuls quelques uns sont utilisés comme :

- INTEGER : valeur entière sur 32 bits en complément à 2.
- OCTET STRING : chaîne de caractères.
- IpAddress : adresse IP.
- PhysAddress : adresse MAC (6 octets pour un réseau de type Ethernet).
- Counter : entier de 32 bits non signé qui s'accroît de 0 à (2exp32 -1) puis revient à 0.
- TimeTicks : compteur de temps sur 32 bits non signé en 1/100 de s



## II.6 MIB (management information base)

Une MIB (Management Information Base, base d'information pour la gestion du réseau) est un ensemble d'informations structuré sur une entité réseau, par exemple un routeur, un commutateur ou un serveur. Ces informations peuvent être récupérées, ou parfois modifiées, par un protocole comme SNMP.

La structure de la MIB est hiérarchique : les informations sont regroupées en arbre. Chaque information a un ( objet identifié), une suite de chiffres séparés par des points, qui l'identifie de façon unique et un nom, indiqué dans le document qui décrit la MIB.

La MIB se présente comme une base de données normalisée, qui permettra de lire et d'écrire sur les équipements distants, de façon également normalisée. Ce sera à l'agent lui-même de faire la traduction entre les informations transmises par SNMP et la plate-forme.

définit un modèle hiérarchique des variables.

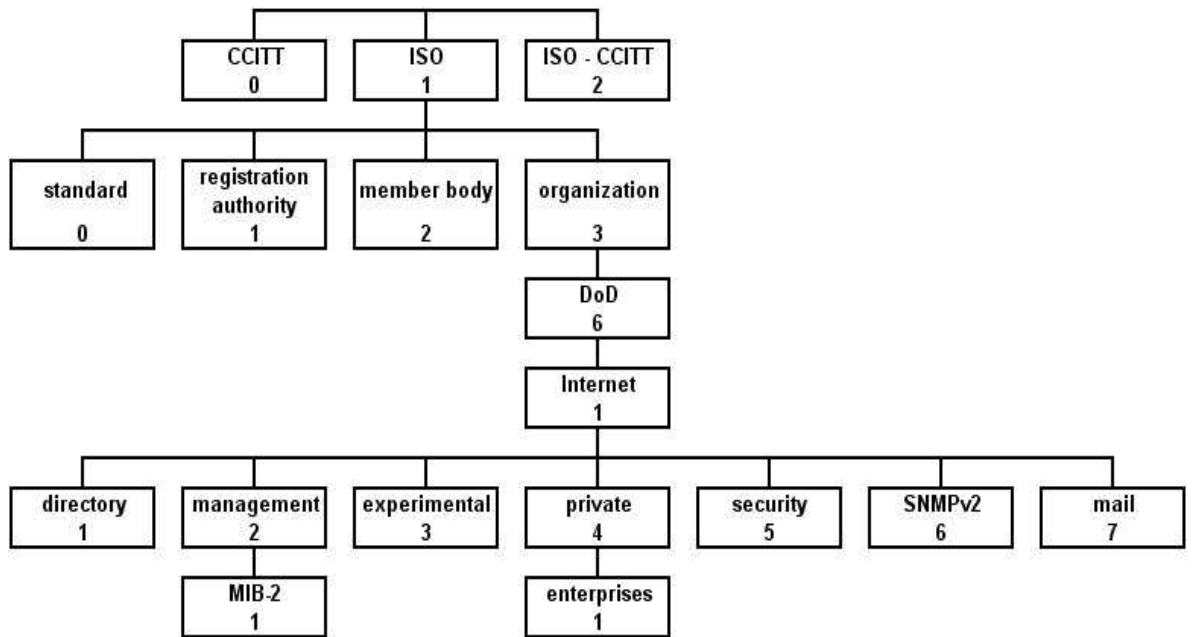
Dans ce dernier, les variables sont répertoriées dans une hiérarchie d'objets. Chaque objet est identifié par ce que l'on appelle un OID (Object Identifier). La hiérarchie de ces objets se représente sous la forme d'un arbre. Les branches constituent les différents OIDs et les feuilles les variables. Une variable peut donc être référencée par la liste ordonnée des différents OIDs parcourus à partir de la racine de l'arbre.

### II.6.1 La structure de données MIB

Elle est organisée hiérarchiquement. Elle contient une partie commune à tous les agents SNMP, en général, d'un même type de matériel et une partie spécifique à chaque constructeur. Elle peut contenir des scalaires (valeurs uniques) ou des tableaux de scalaires.

Les appellations des diverses rubriques sont aussi normalisées. Ces appellations servent à rendre les choses plus lisibles, mais ce sont les index qui sont significatifs en SNMP. En réalité, chaque niveau de la hiérarchie est repéré par un index numérique (écrit entre parenthèses juste à côté de l'appellation). Chaque objet pourra être identifié de façon symbolique ou en utilisant son OID.

La figure ci-dessous représente la structure hiérarchique d'une MIB :



- 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 organization(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 les différents services et tentatives de normalisation. La gestion de réseau standardisée se trouve dans le réseau management(2).
- Sous le nœud management(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 nœuds subordonnés représentant différents groupements de variables MIB.
- Sous le nœud system(1), on trouve 2 variables MIB sysDescr(1) et sysLocation(2).

Un paramètre sera accessible lorsque l'on connaîtra son chemin complet, depuis la racine de l'arbre, en haut sur le dessin.

Il s'agit ici de l'arbre représentant les divers paramètres. La valeur du paramètre, sera atteinte en y ajoutant un dernier index, qui commencera à 0 et y restera pour les scalaires et ira jusqu'à n pour les tableaux.

Pour accéder aux variables souhaitées, on utilisera l'OID (Object Identification) qui désigne l'emplacement de la variable à consulter dans la MIB. Lorsqu'une entreprise veut définir son propre ensemble de variables de gestion, elle va enregistrer son numéro d'objet sous le nœud :

*iso.org.dod.internet.private.entreprises*

Ces MIB seront dites privés. Elles correspondent à la racine 1.3.6.1.4.1.

### **Les fichiers MIB**

Les fichiers MIB décrivent précisément chaque chiffre (OID) de la liste identifiant une variable (la clé), et sa signification.

Prenons l'exemple simple de la variable contenant le nom du matériel interrogé. Il s'agit d'une propriété de l'objet standard « system » qui est « sysName ». Le chemin absolu est : « *iso.org.dod.internet.mnmt.mib-2.system.sysName* ».

Le fichier MIB décrivant l'objet « system » :

```
sysName OBJECT-TYPE  
SYNTAX DisplayString (SIZE (0..255))  
ACCESS read-write  
STATUS mandatory  
DESCRIPTION  
"An administratively-assigned name for this  
managed node. By convention, this is the node's  
fully-qualified domain name."  
 ::= { system 5 }
```

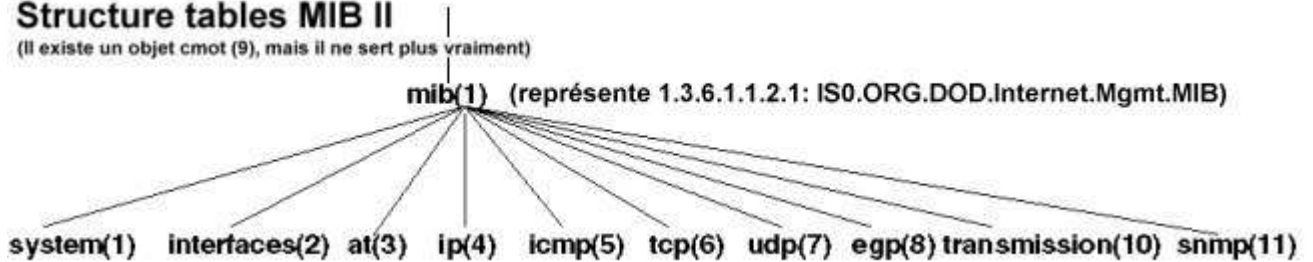
Le fichier fournit toutes les informations relatives à la propriété « sysName » :

- Syntaxe : il s'agit d'une chaîne de caractères de taille variant entre 0 et 255.
- Accès : l'accès à cette variable se fait en lecture ou en écriture
- Etat : cette variable existe et est toujours utilisable.
- Description : il s'agit du nom complet du nœud.
- Sa place dans l'arborescence : 5<sup>e</sup> propriété de l'objet « system » : On en déduit que cette variable a pour clé la valeur 1.3.6.1.2.1.1.5.

## **II.6.2 Les tables MIB**

## Structure tables MIB II

(Il existe un objet cmot (9), mais il ne sert plus vraiment)



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 gérées
- **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 protocole 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
ipOutNoRoutesip		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

## II.6.3 Exemple illustratif

Pour obtenir la valeur de la variable «uptime» (le temps depuis lequel le système est en service) de la machine locale, il suffit d'envoyer dans le champ « Object identifier » du message SNMP la valeur suivante : 1.3.6.1.2.1.1.3.0 qui signifie la valeur du chemin .iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.

La valeur 0 ajouté à la fin du chemin permet d'obtenir la valeur de la feuille cherchée **uptime**

Les messages échangés, dans ce cas, entre le manager et l'agent seront sous la forme suivante :

- Message « **Get-request** » :

Version : 1
Community : public
PDU type : GET
Request Id : 0x34339329
Error Status : NO ERROR
Error Index: 0
Object identifier 1: <b>1.3.6.1.2.1.1.3.0</b> (SNMPv2-MIB::sysUpTime.0)
Value : NULL

- Message « **Get-response** » :

Version: 1
Community : public
PDU type : RESPONSE
Request Id : 0x34339329
Error Status : NO ERROR
Error Index : 0

Object identifier 1 : **1.3.6.1.2.1.1.3.0** (SNMPv2-MIB ::sysUpTime.0)

Value : Timeticks : (24049155) 2 days, 18 :48 :11.55

## II.7 Les différentes versions de SNMP

**SNMP v1** : SNMP version 1 (SNMPv1) est la première implémentation du protocole SNMP a été conçue à la fin des années 80 et standardisée dans le courant de l'année 1990. Elle est écrite dans le RFC (Request For Comments) 1157 et fonctionne dans le cadre des spécifications de SMI (Structure of Management information). SNMPv1 opère sur des protocoles, tels qu'UDP (User Datagram Procol), IP (Internet Protocol), OSI CLNS (ConnectionLess Network Service), AppleTalk DDP (Datagram-Delivery Protocol) et Novell IPX (Internetwork Packet Exchange). SNMPv1 est largement utilisé et fait office de protocole de facto pour l'administration réseau dans la communauté internet. Certaines lacunes telles que le manque de hiérarchie, des codes d'erreurs, etc. a entraîné le développement d'une nouvelle version de SNMP, nommée SNMPv2, et dont la conception a commencé en 1993.

**SNMP v2** : SNMP version 2 (SNMPv2) est une évolution de la version initiale, SNMPv1. A l'origine, en 1993, SNMPv2 a été publié sous la forme d'un ensemble de propositions de standards internet, il s'agit d'un avant projet de standard. A l'instar de SNMPv1, SNMPv2 fonctionne dans le cadre des spécifications de SMI. En théorie, SNMPv2 offre plusieurs améliorations par rapport à SNMPv1 et notamment des opérations de protocole supplémentaires.

**SNMP v3** : La nouvelle version du protocole SNMP vise essentiellement à inclure la sécurité des transactions. La sécurité comprend l'identification des parties qui communiquent et assurent que la conversation soit privée, même si elle passe par un réseau public.

## II.8 La sécurité

Sous SNMPv1 et SNMPv2c, la sécurité est assurée par deux choses :

- Dans sa requête, il faut envoyer une chaîne de communauté, qui correspond en quelque sorte à un mot de passe, et dont les droits varient suivant cette chaîne : il est ainsi possible d'autoriser certaines personnes un accès en lecture seule, et à d'autres personnes un accès complet suivant la communauté qu'ils utilisent.

- L'agent peut vérifier et contrôler l'origine des données, afin de vérifier que la personne en question a accès aux informations. Il s'agit généralement d'une vérification basée sur l'adresse IP source.

Nous constatons toutefois la sécurité est particulièrement lacunaire pour deux raisons : le contenu de la transaction n'est pas crypté, et il suffit que la communauté soit connue de n'importe qui pour que cette personne puisse lire les informations.

Ces différents problèmes ont été résolus dans SNMPv3. En effet, celui-ci propose plusieurs modèles de sécurités différents :

- Le premier modèle est dépourvu de sécurités et est comparable à SNMPv1/v2c.

- Le second modèle offre des capacités d'authentification par utilisateur, c'est-à-dire que chaque utilisateur dispose d'un mot de passe d'accès, ainsi que d'une clé publique de cryptage permettant de sécuriser le contenu de la transaction.
- Le troisième modèle ajoute au précédent un niveau de cryptage supplémentaire en utilisant le principe d'échange des clés privées : le contenu des paquets est ainsi totalement crypté mais ce modèle n'est applicable qu'en fonction des lois sur la cryptographie en vigueur

## II.9 Avantages et inconvénients

### *Avantages*

L'avantage majeur dans le fait d'utiliser SNMP est qu'il est de conception simple. Le résultat flagrant de cette simplicité est une administration de réseau simple à implémenter et rapide.

Un autre avantage de SNMP est qu'il est de nos jours, vraiment très répandu.

L'expansion est un autre avantage de SNMP. De par sa simplicité de conception, il est facile de mettre à jour le protocole pour qu'il réponde aux besoins des utilisateurs futurs.

SNMP est basé sur le protocole de transport UDP ce qui nécessite moins de ressources et de connexions simultanées qu'avec TCP.

Et enfin, c'est une solution peu chère.

### *Inconvénients*

Le premier défaut de SNMP est qu'il contient quelques gros trous de sécurité à travers lesquels des intrus peuvent accéder aux informations transitant sur le réseau.

Puisque SNMP se trouve au dessus de UDP, il n'y a pas de reprise sur erreur, ni de contrôle de flux. La requête ou la réponse peut être égarée.

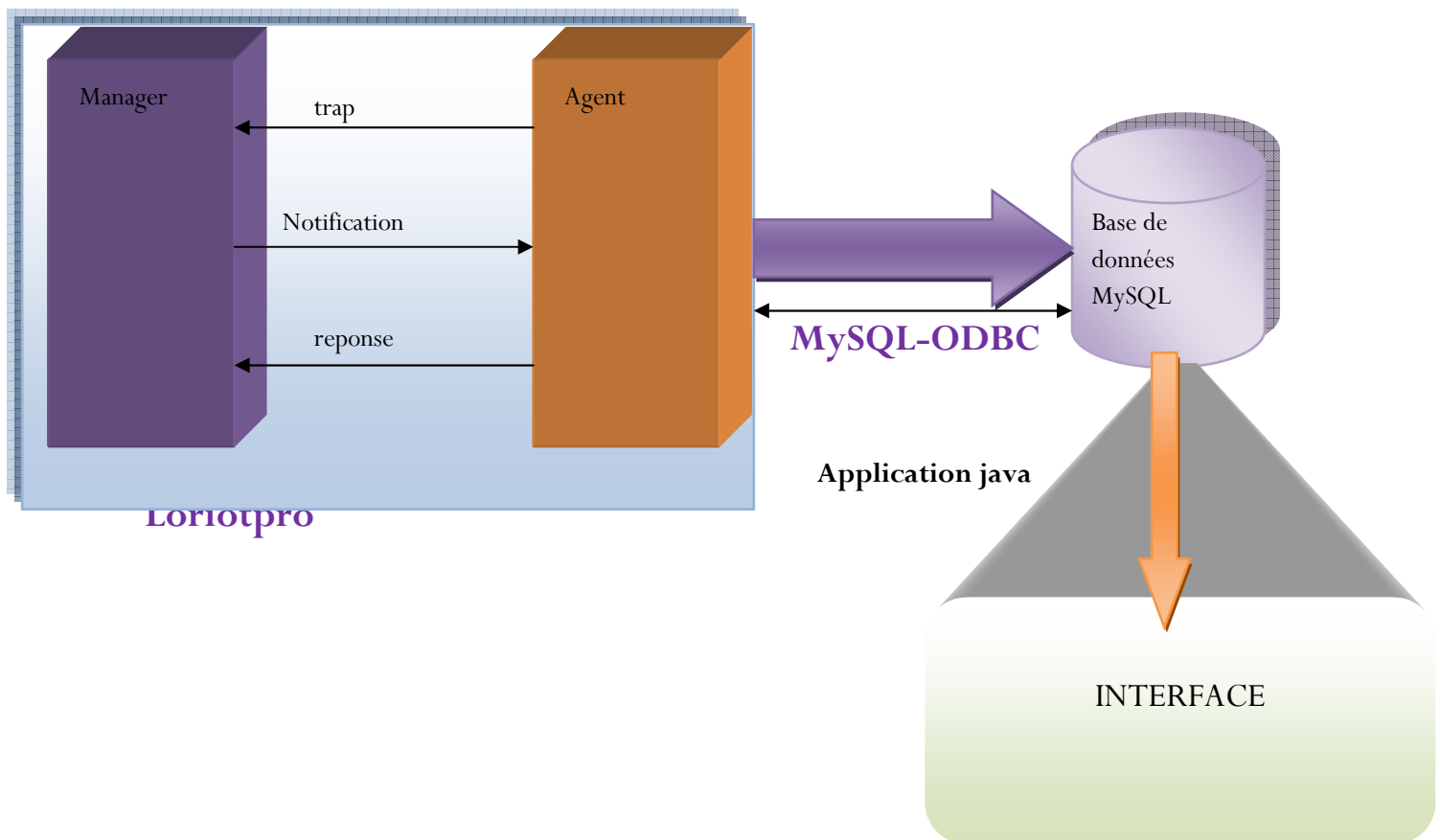
## Conclusion

Ce chapitre nous a permis de comprendre le fonctionnement du protocole SNMP. Grâce à ces requêtes d'administration et sa simplicité de mise au point l'administrateur peut maintenir son réseau malgré la complexité.

Dans le chapitre qui suit il sera question de concrétiser les informations que nous venons de voir dans ce chapitre en mettant au point un module logiciel de gestion

## Chapitre III IMPLEMENTATION JAVA DE L'APPLICATION DE GESTION

Mon travail consiste d'implémenter une application java pour la supervision et la gestion du réseau.



### **Le principe de travail se base sur :**

- Loriotpro qui permet de détecter l'échange d'information entre l'agent et le manager.
- Une base de données MySQL pour stocker toutes les informations.
- MySQL-ODBC pour connecter Loriotpro avec la base de données.
- Une interface développé avec le langage java où sur la quelle les informations stockés dans la base de données sont affichées.



## III.1 Présentation du langage java

### III.1.1 Les caractéristiques.

Java possède un certain nombre de caractéristiques qui ont largement contribué à son énorme succès :

- ✚ Java est interprété : le code source est compilé en pseudo code ou byte code puis exécuté par un interpréteur Java : la Java Virtual Machine (JVM).
  
- ✚ Java est indépendante de toute plate-forme : il n'y a pas de compilation spécifique pour chaque plate forme. Le code reste indépendant de la machine sur laquelle il s'exécute.
  
- ✚ Java assure la gestion de la mémoire : l'allocation de la mémoire pour un objet est automatique à sa création et Java récupère automatiquement la mémoire inutilisée grâce au garbage collector qui restitue les zones de mémoire laissées libres suite à la destruction des objets.
  
- ✚ Java est sûr : la sécurité fait partie intégrante du système d'exécution et du compilateur:
  - ✓ Aucun programme ne peut ouvrir, lire, écrire ou effacer un fichier sur le système de l'utilisateur.
  - ✓ Aucun programme ne peut lancer un autre programme sur le système de l'utilisateur.
  - ✓ Les programmes ne peuvent pas se connecter à d'autres sites Web que celui dont ils proviennent.
  
- ✚ Java est multitâche : il permet l'utilisation de threads qui sont des unités d'exécution isolées. La JVM, elle même, utilise plusieurs threads.

Ainsi a ce basant sur ces caractéristiques, nous avons porté notre choix sur ce langage pour le développement de notre application, dans le but de pouvoir déployé notre application largement dans n'importe quelle plate forme.

## III.2 Outils de développement

La communauté Java est très productive car elle regroupe :

- ✚ Sun, le fondateur de Java à travers le JCP (Java Community Process) qui est le processus de traitement des évolutions de Java dirigé par Sun. Chaque évolution est traitée dans une JSR (Java Specification Request) par un groupe de travail constitué de différents acteurs du monde Java.
- ✚ des acteurs commerciaux dont tous les plus grands acteurs du monde informatique excepté Microsoft.
- ✚ la communauté libre qui produit un très grand nombre d'api et d'outils pour Java.

L'ensemble des API et des outils utilisables est énorme et évolue très rapidement. Hormis les API intégrés dans jdk, pour le développement notre application nous avons utilisé aussi **loriotpro** qui est un API commercialisé conçu pour les applications SNMP.

## III.3 Présentation de l'application

### III.3.1 Environnement de développement

Nous avons développé cette application dans la plate forme Windows xp, à l'aide de l'Environnement de développement intégré NETBEANS. Ce qui rend le déploiement de l'application facile dans la plate forme Windows, mais aussi sous d'autres plate formes par la portabilité de java pour toute machine possédant Jvm (java virtuelle machine).

### III.3.2 Explication du programme

Ce programme comporte une plusieurs classes dont chaque une est composée de plusieurs méthodes, responsable de la supervision de message de gestion circulant entre la station de gestion et les agents snmp présent dans le réseau.

Avant de pouvoir utiliser le programme, il faut d'abord configurer l'agent snmp du nœud que nous souhaitons manager.

## III.4 LORIOTPRO

### III.4.1 Introduction

Le processus de découverte est devenu un système expert dédié à la découverte des réseaux. Il fait une analyse autonome de tous les réseaux disponibles, découvre l'IP de l'hôte, puis analyse ces hôtes afin de déterminer leurs fonctions (routeur, serveur, stations, imprimante). Les hôtes découverts sont ajoutés à l'annuaire de LorientPro avec une configuration de contrôle automatique. LorientPro est un système de véritable expert en utilisant des stratégies de découverte. Ceci peut être appliqué

individuellement pour l'analyse avancée des ressources systèmes. Par exemple, par défaut un système d'exploitation Windows sera analysé à la recherche de ses caractéristiques, CPU, disques, mémoire, et par la suite suivi fonctions seront automatiquement ajoutés à l'objet répertoire d'accueil. Les stratégies de découverte sont basées sur des scripts LUA et peuvent être facilement étendues par les opérateurs à répondre à leurs besoins et adaptées au type de matériel à découvrir.

LoriotPro Extended Edition V5 comprend un générateur de Windows frontal graphique de tendance basée sur le célèbre programme de RRD Tool. Deux modules plug-in sont disponibles, le module RRD Collector pour la collecte des données, le stockage dans des bases RRD et leur affichage graphiques, le module RRD Manager pour la gestion avancée des bases RRD exploitation et la maintenance. Les graphiques sont entièrement configurables à partir d'une interface graphique de Windows pour suivre l'évolution d'un ou plusieurs des données recueillies. Les données collectées peuvent être des objets SNMP, temps de réponse IP d'un ou de plusieurs valeurs de retour à distance et de l'exécution du script LUA.

LoriotPro Extended Edition V5 peut résoudre des problèmes très complexes des réseaux et l'administration système avec le puissant et évolutif langage de script incorporé LUA. Grâce à cette solution unique, votre architecture réseau et l'environnement graphique de LoriotPro peuvent être surveillés et contrôlés par des programmes très convenables.

L'environnement de développement intégré à LoriotPro vous permet d'écrire rapidement des applications puissantes dédiées à la surveillance et l'audit des ressources de votre système d'information. Des dizaines d'exemples prêts à l'emploi sont fournis et il ya une possibilité d'automatiser les tâches récurrentes et fastidieuses administration.

LoriotPro utilise les bases de la langue source ouverte LUA et prévoit des ajouts des dizaines de fonctions dédiées à la surveillance et le suivi par SNMP, la cartographie et la représentation symbolique de la vue active et la corrélation des événements et des alarmes.

### **III.4.2 Périmètre d'utilisation.**

Le logiciel LoriotPro a un périmètre d'utilisation extrêmement large et sait s'adapter aux besoins les plus divers. Il est déjà utilisé par nombre de clients opérateurs de télécommunication à travers le monde pour la surveillance d'infrastructure réseaux complexes. Ce choix a été principalement basé sur les performances techniques de LoriotPro pour la supervision et le filtrage d'alarmes en provenance de centaines d'équipements critiques ou sensibles. Il est aussi beaucoup utilisé par des sociétés de services et les banques pour la surveillance d'applications verticales ou de leur système d'information mais aussi dans l'industrie et les transports (supervision de systèmes et d'application dans la messagerie aérienne). Les ISP et les diffuseurs (broadcast) apprécient la souplesse du produit LoriotPro pour la télésurveillance de leurs équipements réseau et de diffusion avec des contraintes particulières.

### **III.4.3 Visuel et ergonomique.**

LoriotPro se distingue par son interface utilisateur qui permet rapidement d'identifier un défaut dans une infrastructure de centaines, voire de milliers de machines. Son interface graphique exploite

l'environnement multi fenêtre de Windows et permet ainsi de créer des visuels dynamiques de votre système d'information appelé Active View. Ces tableaux de bord entièrement modulaires affichent en permanence les statuts de fonctionnement et de disponibilité et les valeurs de charge de vos ressources informatiques (liens Ethernet, mémoires, disques, services réseaux, serveurs, application etc).

### III.4.4 Performance et compatibilité aux standards.

C'est la caractéristique la plus importante mais aussi la moins visible de LorientPro. La capacité de LorientPro à contrôler la disponibilité de milliers d'éléments est énorme et ceci grâce à une architecture interne exploitant le multi tâche de Windows. La maîtrise totale des processus de collecte et de traitement des événements et des alarmes qui peuvent affluer par centaines en quelques secondes est aussi un facteur clé pour assurer un réel contrôle de votre environnement. La compatibilité de LorientPro aux standards d'Internet et le support du standard SNMP, la référence en matière de protocole de gestion réseau, est une vraie garantie de pérennité du produit et de compatibilité avec les milliers d'équipements et de logiciels déjà présents sur le marché.

### III.4.5 Introduction à la simulation d'interruption SNMP et notification SNMP

Une partie de mon travail consiste à utiliser le simulateur d'interruption comme outil de simulation des trap

Le simulateur d'interruption SNMP est un outil idéal fourni avec LorientPro pour la simulation d'interruption SNMP et les tests de filtre trap LorientPro ou d'un serveur piège. Trap Simulator permet de forger des faux SNMPv1 trap ou notifications SNMPv2c et de les envoyer à n'importe quel récepteur trap SNMP.

SNMP Trap simulation est très utile pour tester les filtres trap dans LorientPro et vérifier que les actions associées soient bien exécutées.

#### snmp V1 trap versus snmp v2c notification

Les traps SNMPv1 ont été définis dans la RFC 1157, avec les champs suivants:

Enterprise	Identifie le type d'objet géré générer la trap de SNMP V1. domaine de l'entreprise contient la valeur de sysObjectID de l'appareil émetteur SNMP v1 vendeur trap. For spécifiques pièges, SNMP v1 domaine générique type de piège est fixé à enterpriseSpecific (6).
Agent address	Fournit l'adresse de l'objet pour géré et générer les traps de SNMP .

Generic trap type	Indique l'un des types d'un certain nombre de SNMP génériques les trappes.
Specific trap code	Indique l'un des nombreux trappes de codes spécifiques.
Time stamp	Fournit la quantité de temps qui s'est écoulé entre la réinitialisation le dernier réseau et la génération de trappes SNMP
Variable bindings	Le champ de données de piège contenant PDU. Chaque variable associés contraignant une instance d'objet particulier MIB avec sa valeur actuelle

Le standard SNMP v1 trappes génériques sont les suivants:

0	coldStart	Le dispositif de SNMP effectue un pouvoir sur les
1	warmStart	Le dispositif de SNMP effectue un rechargement software ou IPL
2	linkDown	Un de l'interface de l'appareil snmp descendant
3	linkUp	Un de l'interface de l'appareil snmp montant
4	authenticationFailure	Un gestionnaire SNMP tente d'accéder à un agent SNMP avec une communauté mal ou les droits d'utilisation erronée
5	egpNeighborLoss	perte Extérieur protocole de passerelle d'un routeur voisin
	enterprise specific	Entreprise trappes de propriété

En SNMPv2c trappe est définie comme une notification et formaté différemment comparant à SNMPv1. Il a les paramètres suivants

sysUpTime	Même que horodatage SNMPv1 piège
snmpTrapOID	champ d'identification du trap. Pour les trap génériques, les valeurs sont définies dans la RFC 1907, pour les trap spécifiques au fournisseur snmpTrapOID est essentiellement une concaténation du paramètre Enterprise SNMPv1 et deux autres sous-identificateurs, '0', et le paramètre spécifique SNMPv1 code piège.
VarBindList	Une liste de liaisons de variables

## A partir du simulateur trapSNMP

IP Source Used in V1 Trap: [ ] IP Destination: 127.0.0.1 Trap Community: public Refresh Trap List

V1 Standard Trap: [ ]

V1 Enterprise Trap and V2 Notification (Double click to select an item)

Name	Trap V1 Name or Father	Ver...	V1 enterpris...	MIB
linkUp	snmpTraps	2		IF-MIB
linkDown	snmpTraps	2		IF-MIB
authenticationFailure	snmpTraps	2		snmpv2-mib
warmStart	snmpTraps	2		snmpv2-mib
coldStart	snmpTraps	2		snmpv2-mib
a3Com	unitDeparture_v1	1	89	A3COM0017-ST.stackUnitDesc/(OS)string.stackUnitSerialNumber/(OS)s
a3Com	remPollFailureTrap_v1	1	75	A3COM0019-RM.remPollAddress.remPollProtocol.remPollInformation,
a3Com	remPollSuccessTrap_v1	1	74	A3COM0019-RM.remPollAddress.remPollProtocol.remPollInformation,
a3Com	secureViolation4_v1	1	88	A3COM0021-PO.secureAddrRowStatus/(IN)145.ifAdminStatus/(IN)145,
a3Com	secureViolation3_v1	1	86	A3COM0021-PO.secureAddrRowStatus/(IN)145.ifAdminStatus/(IN)145,a
a3Com	secureViolation2_v1	1	78	A3COM0021-PO.secureAddrRowStatus/(IN)145.rptrPortAdminStatus/(IN)
a3Com	secureAddrRowStatus_v1	1	95	A3COM0021-PO.secureAddrRowStatus/(IN)145.rptrPortAdminStatus/(IN)

linkUp

Object Name : [ linkUp ]  
Children of Object : [ snmpTraps ]  
From MIB Description : [ IF-MIB ]  
Registered in File : [ IF-MIB-2000061400002-rfc2863.mib ] The File is loaded

SYNTAX : [0]  
V2 Notification :  
[ IfIndex ]  
[ ifAdminStatus ]  
[ ifOperStatus ]

ACCESS : No defined [0]  
STATUS : CURRENT

OID LEN (10) : 1.3.6.1.6.3.1.1.5.4.  
iso(1).org(3).dod(6).internet(1).snmpv2(6).snmpModules(3).snmpMIB(1).snmpMIBObjects(1).snmpTraps(5).linkUp(4)

V2 Notification Options:

Send a simulated V1 trap when sending V2 Notification  
 Send a simulated V2 Notification with SNMP V2C  
 Send a simulated V2 Notification with SNMP V3

IF-MIB:linkUp  
 V2/V3 Trap are INFORM format

IfIndex/(IN)145.ifAdminStatus/(IN)145.ifOperStatus/(IN)145.

Send

### III.4.6 Envoi des trappes simulées et la notification

Pour envoyer un SNMP v1 forgé traps, il est possible de sélectionner l'adresse de la source de la trap. Ensuite, entrer l'adresse et la communauté. Si on envoie cette trap à partir de LorientPro celui-ci utilise l'adresse de loopback 127.0.0.1. Vérifier que la communauté est bonne si vous voulez vérifier un filtre fixé sur la communauté trap dans le filtre trap LorientPro. Dans la liste déroulante une trape V1 standard ou dans l'entreprise V1 et la liste de notification. La trap est le nom affiché dans la zone de texte du bas et le champ de la variable fixation est terminé.

Name	La trap ou la notification de nom définit dans la MIB
Trap V1 name or father	le nom complet du trap dans SNMP v1 ou le nom de l'objet père pour SNMP v2c
Version	la version SNMP, SNMP v1 ou SNMP v2
V1 Enterprise specific	Un numéro unique qui identifie cette trape entre tous les trappes de ce fournisseur
MIB	Le fichier MIB compilées sur le gestionnaire de LorientPro où est définit cette trape
Objects	La liste des objets des liaisons de variables et leur valeur arbitraire sont affectées pour la simulation

La liste contient tous les trappes SNMP V1 (Enterprise) et SNMP v2c notification).

énumérés ou SNMP Trap. Vous pouvez utiliser l'outil SNMP Walker pour trouver que les fichiers MIB ainsi les trap ou les notifications sont pris en charge par un dispositif.

**Dans l'exemple ci-dessous nous sélectionnons un SNMP v2 notification. Une trap SNMP V1 en même temps.**

LoriotPro - TrapSimulator

IP Source Used in V1 Trap: 127.0.0.1 IP Destination: 127.0.0.1 Trap Community: public

V1 Standard Trap: [ ] Refresh Trap List

V1 Enterprise Trap and V2 Notification (Double click to select an item)

Name	Trap V1 Name or Father	Ver...	V1 enterpris...	MIB	
linkUp	snmpTraps	2		IF-MIB	IfIndex/(IN)145,ifAdminStatus/(IN)145,ifOperStatus/(IN)
linkDown	snmpTraps	2		IF-MIB	IfIndex/(IN)145,ifAdminStatus/(IN)145,ifOperStatus/(IN)
authenticationFailure	snmpTraps	2		SNMPv2-MIB	
warmStart	snmpTraps	2		SNMPv2-MIB	
coldStart	snmpTraps	2		SNMPv2-MIB	
a3Com	unitDeparture_v1	1	89	A3COM0017-ST	stackUnitDesc/(OS)string,stackUnitSerialNumber/(OS)s
a3Com	remPollFailureTrap_v1	1	75	A3COM0019-RM	remPollAddress,remPollProtocol,remPollInformation,
a3Com	remPollSuccessTrap_v1	1	74	A3COM0019-RM	remPollAddress,remPollProtocol,remPollInformation,
a3Com	secureViolation4_v1	1	88	A3COM0021-PO	secureAddrRowStatus/(IN)145,ifAdminStatus/(IN)145,
a3Com	secureViolation3_v1	1	86	A3COM0021-PO	secureAddrRowStatus/(IN)145,ifAdminStatus/(IN)145,a
a3Com	secureViolation2_v1	1	78	A3COM0021-PO	secureAddrRowStatus/(IN)145,rprtPortAdminStatus/(IN)
a3Com	secureAddrRowStatus_v1	1	95	A3COM0021-PO	secureAddrRowStatus/(IN)145,a3Com/(IN)145,ifAdminSt

Object Name : [ linkUp ]  
 Children of Object : [ snmpTraps ]  
 From MIB Description : [ IF-MIB ]  
 Registered in File : [ IF-MIB-200006140000Z-rfc2863.mib ] The File is loaded

SYNTAX : [0]  
 V2 Notification :  
 [ IfIndex ]  
 [ ifAdminStatus ]  
 [ ifOperStatus ]

ACCESS : No defined (0)  
 STATUS : CURRENT

OID LEN (10) : 1.3.6.1.6.3.1.1.5.4.  
 iso(1).org(3).dod(6).internet(1).snmpV2(6).snmpModules(3).snmpMIB(1).snmpMIBObjects(1).snmpTraps(5).linkUp(4)  
 LoriotPro Extensions :  
 Dup name found: 0 IOD Marked Deleted: 0

V2 Notification Options

Send a simulated V1 trap when sending V2 Notification  
 Send a simulated V2 Notification with SNMP V2C  
 Send a simulated V2 Notification with SNMP V3

IF-MIB:linkUp  
 V2/V3 Trap are INFORM format

Help

IfIndex/(IN)145,ifAdminStatus/(IN)145,ifOperStatus/(IN)145.  
 Send

On peut modifier la valeur des liaisons de variables dans le champ inférieur de l'écran. Dans notre exemple, les objets de la variable de liaison sont définies et à l'importation à partir du fichier MIB. Les valeurs ont été fixées arbitrairement à 145 par LoriotPro, mais on peut les modifier. Et après le choix de nom il faut l'envoyé (send) , et il va êtres enregistrer dans la base de données.

### III.5 MySQL ODBC

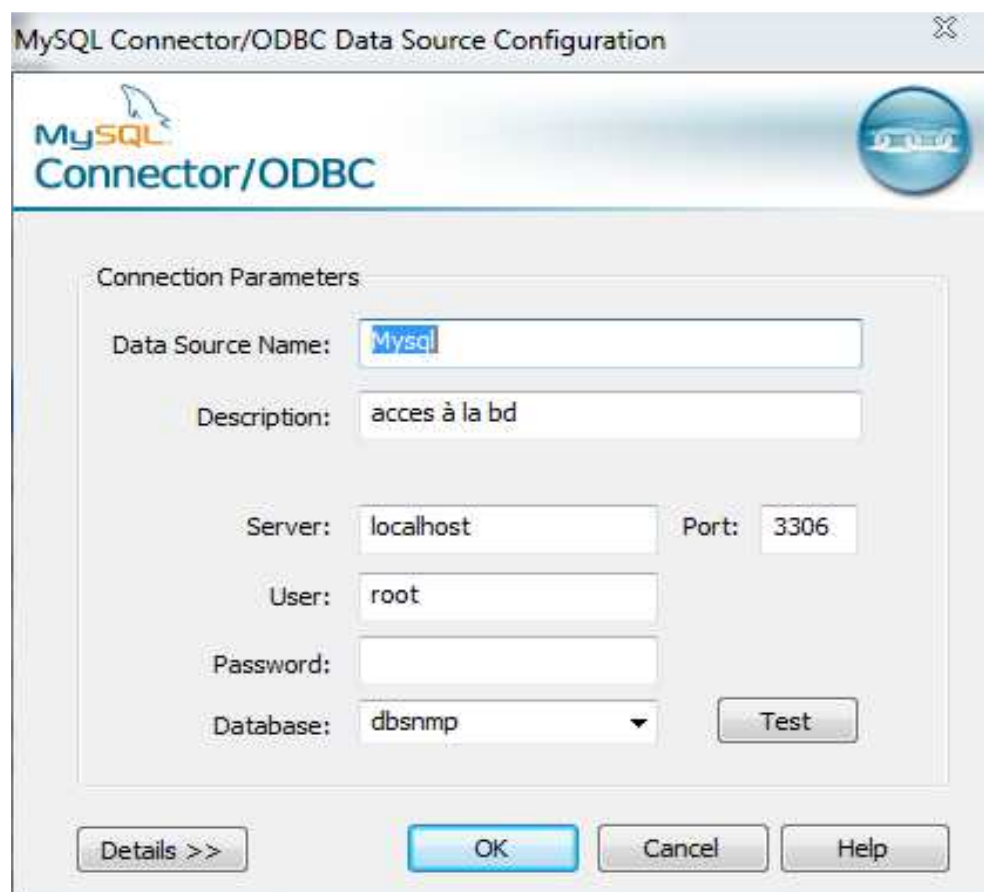


### III.5.1 Introduction

Open Database Connectivity (ODBC) est une interface de programmation d'applications largement acceptée (API) d'accès base de données. Il est basé sur l'interface de niveau d'appel (CLI) des spécifications de X / Open et l'ISO / CEI pour les API de base de données et utilise Structured Query Language (SQL) comme langue d'accès à la base de données.

La configuration du pilote peut être faite directement à partir de LorientPro ou à partir de Microsoft Windows de données ODBC outil Administrateur de source.

L'image ci-dessous montre la configuration de MySQL-ODBC-connector



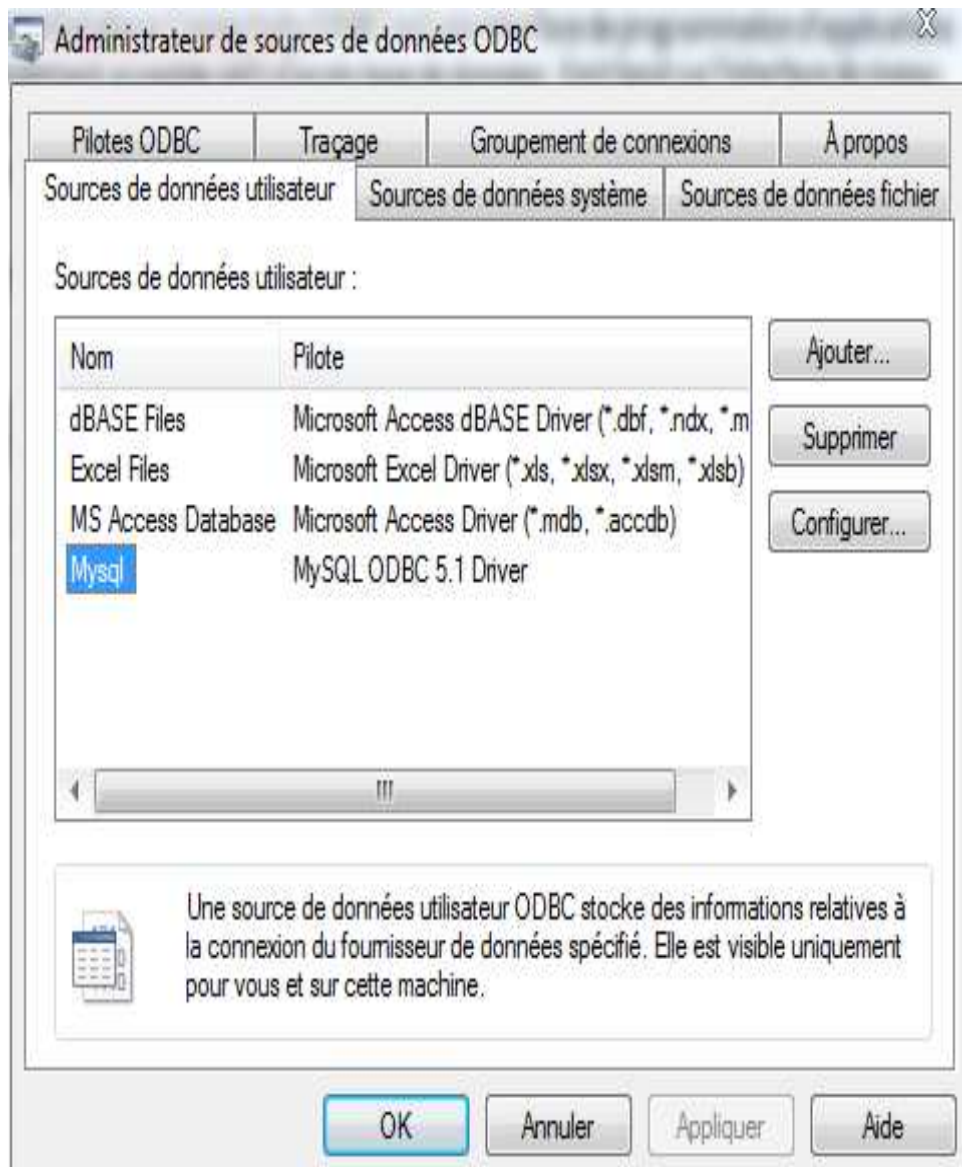
Data Source Name	Un nom utilisé pour identifier cette source de données
Description	Description du nom pour la source de données

Server	le nom ou l'adresse IP du serveur sur lequel le serveur de base de données est installé
User	Le nom d'utilisateur utilisé pour accéder à la base de données
Password	Le mot de passe de cet utilisateur
Database	Le nom de la base (Doit être «LoriotPro»)

Lorsque le champ est défini, on peut vérifier la connexion à la base de données (Test).  
**L'image ci-dessous montre que la connexion est réussite.**



### III.5.2 Onglet Sources de données utilisateur



Ajoute, supprime ou configure des sources de données ayant des noms de source de données utilisateur. Ces sources de données existent localement sur un ordinateur et seule la personne qui est en train d'utiliser l'ordinateur peut y accéder.

Il est nécessaire pour créer la base de données pour LorientPro manuellement d'installer le serveur MySQL et celle-ci doit être en marche.

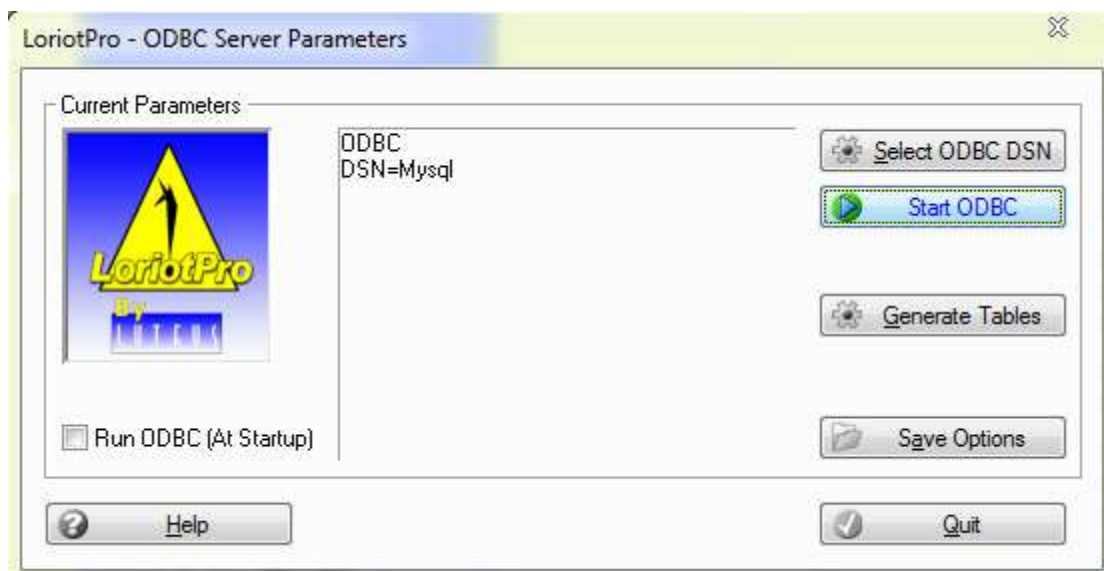
- ❖ Ce chapitre explique comment utiliser la construction dans le magicien de configuration du serveur ODBC.
- ❖
- ❖ Cet assistant vous aide à:
- ❖

- ❖ Créer un nom de DataSource (si pas encore créé avec la source de données ODBC outil Administrateur).

Sélectionner une source de données ODBC Nom.

Créer les tables nécessaires pour SQL LorientPro.

Start Stop l'accès au pilote ODBC et à la base de données LorientPro.



Configurer l'option de démarrage et enregistrer les paramètres.

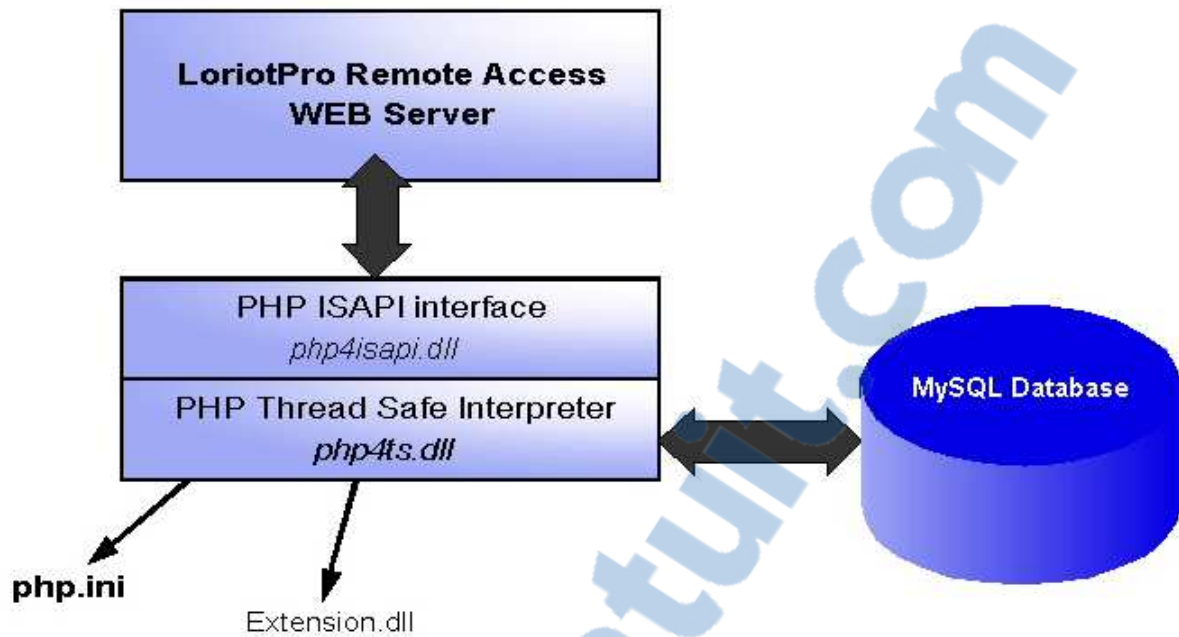
### III.5.3 Ajout du support de PHP pour Lorientpro web Server

LorientPro serveur WEB utilise une interface ISAPI de PHP pour accéder aux bases de données MySQL. PHP est un langage de script largement utilisé à des fins générales qui est particulièrement adapté au développement Web et peut être intégré facilement au HTML. PHP fournit également un ensemble complet et natif de la fonction qui nous permet d'accéder à MySQL.

Utilisation des appels de fonction ISAPI, pages Web peuvent appeler des programmes qui sont écrits sous forme de DLL sur le serveur, en général d'accéder aux données dans une base de données.

Quand une page Web est affichée par le serveur WEB LorientPro et si le script PHP est inclus dans cette page, ils sont forwarded à l'interpréteur PHP que d'exécuter le script. La plupart des scripts que nous fournissons effectue l'accès à une base de données MySQL.

**L'affichage diagramme la suite de la composante de l'infrastructure.**



## Le lancement d'EasyPHP

On ne peut pas à proprement parler du lancement d'EasyPHP, il s'agit en fait de la mise en route du serveur Apache et de MySQL. Il permet de créer des bases de données qu'on peut les connecter avec LorientPro à l'aide de Mysql-connector-ODBC.

## III.6 Création de base de données avec phpMyAdmin

Pour créer une base de données en entrant le nom de la base de données et en cliquant sur créer

The screenshot shows the phpMyAdmin 2.6.1 interface. The main content area displays the 'MySQL' section with a 'Créer une base de données' form. The form includes a text input field for the database name, a dropdown menu for 'Interclassement', and a 'Créer' button. A red arrow points to the 'Créer' button. The left sidebar shows navigation options like 'Afficher l'état du serveur', 'Afficher les variables du serveur', 'Afficher les processus', 'Jeux de caractères et interclassement', 'Privilèges', 'Bases de données', and 'Exporter'. The right sidebar shows settings for 'phpMyAdmin' such as 'Language: French (fr-utf-8)', 'Jeu de caractères pour MySQL: UTF-8 Unicode (utf8)', 'Interclassement pour la connection MySQL: utf8\_general\_ci', 'Thème / Style: Original', 'Documentation de phpMyAdmin', 'Afficher les informations relatives à PHP', and 'Site officiel de phpMyAdmin'.

Seveur: localhost Base de données: loriotpro

Structure SQL Exporter Rechercher Requête Opérations Supprimer

Table	Action	Enregistrements	Type	Interclassement	Taille	Perte
loriot_events		20	MyISAM	latin1_swedish_ci	9,0 Ko	-
loriot_hosts		0	MyISAM	latin1_swedish_ci	1,0 Ko	-
loriot_managers		0	MyISAM	latin1_swedish_ci	1,0 Ko	-
loriot_netflow		0	MyISAM	latin1_swedish_ci	1,0 Ko	-
loriot_networks		0	MyISAM	latin1_swedish_ci	1,0 Ko	-
5 table(s)	Somme	20	--	latin1_swedish_ci	13,0 Ko	0 Octets

Tout cocher / Tout décocher Pour la sélection :

Version imprimable Dictionnaire de données

Créer une nouvelle table sur la base loriotpro:

Nom:

















































Champs:  Exécuter

On choisit la base de données qu'on vient de créer dans la liste à gauche de l'écran, par exemple : si on crée une base de données (loriotpro).

Dans cet exemple la base contient cinq tables :

- ❖ **Loriot\_managers** : Cette table contient la différenciation des systèmes LorientPro installés qui permettent d'accéder à la base de données.
- ❖ **Loriot\_host** : Cette table contient toutes les hôtes exportés de LorientPro à la base de données.
- ❖ **loriot\_networks** : Cette table contient tous les hôtes exportés de LorientPro à la base de données.
- ❖ **loriot\_event** : Cette table contient tous les hôtes exportés de LorientPro à la base de données.
- ❖ **Loriot\_netflow** : Cette table est utilisée par le Service LorientNetFlowCollectorService.sp Plugin.
- ❖ Ce plugin est un exemple fourni avec le SDK qui démontre l'utilisation des fonctions ODBC et leur mise en œuvre.
- ❖ Ce plugin fonctionne en tant que collectionneur et recueille de l'information à partir de périphériques Cisco Netflow.

On remarque dans la figure ci-dessous que les traps sont stockés dans la table loiriot\_event sous forme de champs.

Champ	Type	Interclassement	Attributs	Null	Défaut	Extra	Action
<input type="checkbox"/> l_timestamp	int(4)			Oui	NULL		     
<input type="checkbox"/> l_manager_id	int(4)		UNSIGNED	Oui	0		     
<input type="checkbox"/> l_reference	int(4)		UNSIGNED	Oui	0		     
<input type="checkbox"/> l_level	int(4)		UNSIGNED	Oui	0		     
<input type="checkbox"/> l_string	char(255)	latin1_swedish_ci		Oui	0		     
<input type="checkbox"/> l_ip_agent_add	char(15)	latin1_swedish_ci		Non			     
<input type="checkbox"/> l_ip_source_add	char(15)	latin1_swedish_ci		Non			     
<input type="checkbox"/> l_number	int(4)		UNSIGNED	Non		auto_increment	     

Pour voir le contenu en cliquant sur afficher

	l_timestamp	l_manager_id	l_reference	l_level	l_string	l_ip_agent_add	l_ip_source_add	l_number
 	1275150702	100000	10	1	<1> DSN=[Mysql] for database [] open with success	127.0.0.1	127.0.0.1	1
 	1275150703	100000	9	4	<4> Database Closed : (62) (null) La table loirio...	127.0.0.1	127.0.0.1	2
 	1275150709	100000	9	4	<4> Database watchdog : Poll to reinit Closed dat...	127.0.0.1	127.0.0.1	3
 	1275150709	100000	10	1	<1> DSN=[Mysql] for database [] reopen with succes...	127.0.0.1	127.0.0.1	4
 	1275150720	100000	9	4	<4> Database Closed : (62) (null) La table loirio...	127.0.0.1	127.0.0.1	5
 	1275150730	100000	9	4	<4> Database watchdog : Poll to reinit Closed dat...	127.0.0.1	127.0.0.1	6
 	1275150730	100000	10	1	<1> DSN=[Mysql] for database [] reopen with succes...	127.0.0.1	127.0.0.1	7
 	1275150741	100000	9	4	<4> Database Closed : (62) (null) La table loirio...	127.0.0.1	127.0.0.1	8
 	1275150751	100000	9	4	<4> Database watchdog : Poll to reinit Closed dat...	127.0.0.1	127.0.0.1	9
 	1275150751	100000	10	1	<1> DSN=[Mysql] for database [] reopen with succes...	127.0.0.1	127.0.0.1	10
 	1275150762	100000	9	4	<4> Database Closed : (62) (null) La table loirio...	127.0.0.1	127.0.0.1	11
 	1275150772	100000	9	4	<4> Database watchdog : Poll to reinit Closed dat...	127.0.0.1	127.0.0.1	12
 	1275150772	100000	10	1	<1> DSN=[Mysql] for database [] reopen with succes...	127.0.0.1	127.0.0.1	13
 	1275150784	100000	9	4	<4> Database Closed : (62) (null) La table loirio...	127.0.0.1	127.0.0.1	14
 	1275150793	100000	9	4	<4> Database watchdog : Poll to reinit Closed dat...	127.0.0.1	127.0.0.1	15
 	1275150793	100000	10	1	<1> DSN=[Mysql] for database [] reopen with succes...	127.0.0.1	127.0.0.1	16
 	1275150805	100000	9	4	<4> Database Closed : (62) (null) La table loirio...	127.0.0.1	127.0.0.1	17
 	1275150814	100000	9	4	<4> Database watchdog : Poll to reinit Closed dat...	127.0.0.1	127.0.0.1	18
 	1275150814	100000	10	1	<1> DSN=[Mysql] for database [] reopen with succes...	127.0.0.1	127.0.0.1	19
 	1275151134	100000	216	1	<1> Load new Service plugin : TrapSimulator V5.02...	192.168.1.15	127.0.0.1	20

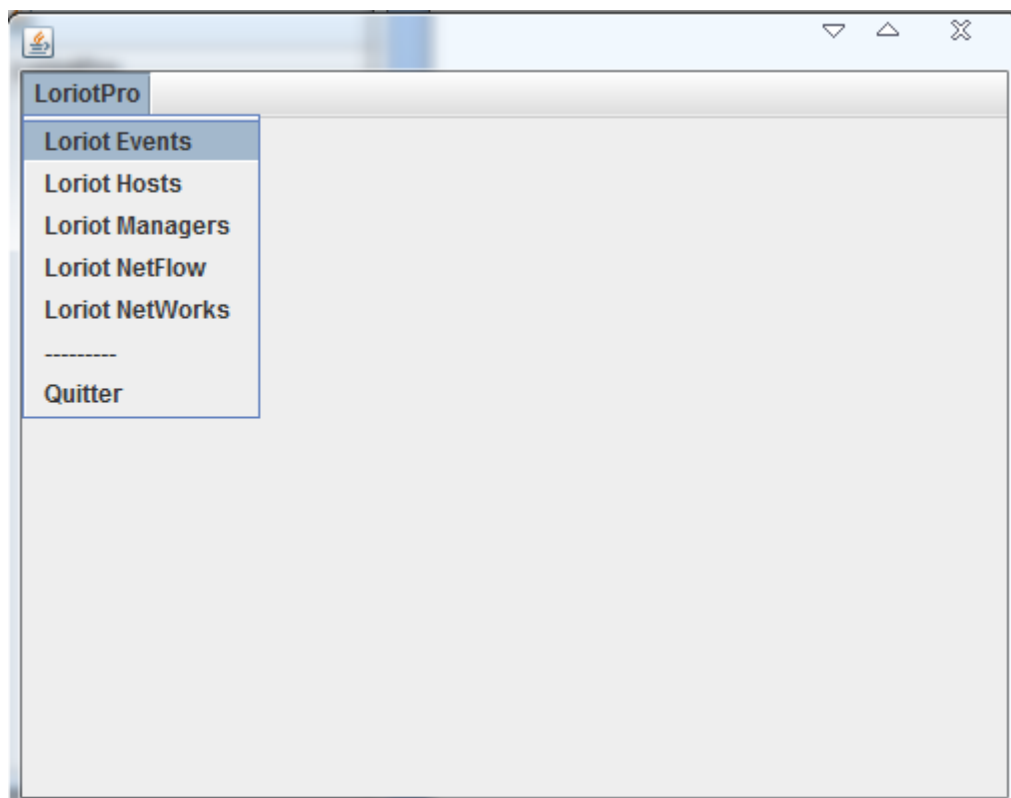
**Timestamp** : C'est une séquence de caractères, indiquant la date et / ou l'heure à laquelle un certain événement s'est produit, c'est l'heure ou laquelle un événement est enregistré par un ordinateur.

Ces données sont généralement présentées dans un format cohérent, permettant de comparer facilement les deux enregistrements différents.

**Manager\_id** : La gestion des identités ou IDM est un terme lié à la façon dont les humains sont identifiés et autorisés à travers des réseaux informatiques. Il couvre des questions telles que la façon dont les utilisateurs ont une identité, la protection de l'identité et les technologies de soutien que la protection comme les protocoles réseau, les certificats numériques, des mots de passe et ainsi de suite.

### III.6 Configuration de trap sous windows

Après configuration du nœud que nous souhaitons manager, on lance l'application. Après exécution, une fenêtre s'ouvre et nous montrent les tables qui se trouvent au niveau de la base de données.



En choisissant par exemple la table lorient\_event où les informations qu'on a besoin de les superviser sont stockées. On voit dans l'image ci dessous toutes les informations : le temps, le serveur, les références, la base de données, l'adresse de l'agent, l'adresse de la source, le numéraux de champ



LoriotPro

I_timestamp	I_manager_id	I_reference	I_level	I_string	I_ip_agent a...	I_ip_source ...	I_number
1275150702	100000	10	1	<1> DSN=[My...	127.0.0.1	127.0.0.1	1
1275150709	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	3
1275150709	100000	10	1	<1> DSN=[My...	127.0.0.1	127.0.0.1	4
1275150720	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	5
1275150730	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	6
1275150730	100000	10	1	<1> DSN=[My...	127.0.0.1	127.0.0.1	7
1275150741	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	8
1275150751	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	9
1275150751	100000	10	5	<1> DSN=[My...	127.0.0.1	127.0.0.1	10
1275150762	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	11
1275150772	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	12
1275150772	100000	10	1	<1> DSN=[My...	127.0.0.1	127.0.0.1	13
1275150784	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	14
1275150793	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	15
1275150793	100000	10	1	<1> DSN=[My...	127.0.0.1	127.0.0.1	16
1275150805	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	17
1275150814	100000	9	4	<4> Databas...	127.0.0.1	127.0.0.1	18
1275150814	100000	10	1	<1> DSN=[My...	127.0.0.1	127.0.0.1	19
1275151134	100000	216	1	<1> Load ne...	192.168.1.15	127.0.0.1	20
1275178338	100000	219	6	<6> Session ...	127.0.0.1	127.0.0.1	24
1275178353	100000	218	6	<6> Session ...	127.0.0.1	127.0.0.1	25
1275178368	100000	218	6	<6> Session ...	127.0.0.1	127.0.0.1	26
1275178402	100000	218	6	<6> Session ...	127.0.0.1	127.0.0.1	27
1275178433	100000	218	6	<6> Session ...	127.0.0.1	127.0.0.1	28

Supprimer Enregistrer Actualiser Quitter

- Le bouton enregistrer sert à enregistrer une modification dans la base de données à partir de cette interface.
- Le bouton actualiser permet de savoir s'il y a une nouvelle information a été ajouter.
- Le bouton supprimer permet de supprimer un des champs existant.
- Le bouton quitter permet de quitter l'application

D'après cette interface on peut superviser toutes les trap entre l'agent et le manager, ce qui permet de superviser et de réparer les pannes avant qu'elles se propagent.

## CONCLUSION GENERAL

Cet exercice nous a été profitable parce qu'il nous a permis d'élargir notre connaissance sur le protocole SNMP. Grâce à lui, nous avons pu dégager l'étendue du travail d'administration comme définie par l'ISO, cette charge que nous avons qualifiée de lourde vu les efforts que doivent conjuguer les administrateurs réseau pour garder en état de marche leurs réseaux et intervenir au plus vite possible en cas de panne.

Nous avons aussi vu que le protocole SNMP a été développé pour faciliter cette administration et qu'à l'aide des requêtes SNMP simple (get, set ....) et la remontée d'informations par trap SNMP, on pouvait maintenir son réseau.

C'est ainsi que nous nous sommes efforcés d'implémenter une application de supervision de réseau exploitant le protocole SNMP pour concrétiser ses informations. L'application tourne malgré le bug qui est encore attaché, mais nous comptons améliorer dans les jours avenir.

## **Bibliographie :**

<http://www.frameip.com/snmp/>

<http://www-igm.univ-mlv.fr/~dr/XPOSE2002/vollerein/>

<http://leroy-dubois.name/index.php/articles-informatique/43-introduction-au-service-snmp.html>

[http://fr.wikipedia.org/wiki/Simple\\_network\\_management\\_protocol](http://fr.wikipedia.org/wiki/Simple_network_management_protocol)