République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira de Bejaia
Faculté des sciences exactes
Département d'Informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme en Master option : ASR

Thème :

Conception et réalisation d'une application de gestion de réseaux basé sur le protocole SNMP

Cas d'etude SONATRACH

Réalisé par :

M^elle SMAOUN Lyna

Membres de jurys :

Président : Mr Amroun Kamel

Examinatrice : Mr Mir Faudil

Promoteur : M^r Mehaoud Kamel

Année universitaire : 2015/2016

Remerciements

Je remercie énormément le bon Dieu de m'avoir donné la force et la Patience d'élaborer ce modeste mémoire qui j'espérons qu'il sera à la hauteur.

Je tiens aussi à remercier et à exprimer ma profonde gratitude à Mr Mehaoud Kamel, mon promoteur pour la confiance qu'il m'a accordé durant la réalisation de ce projet, je tien, à lui exprimer ma profonde reconnaissance pour le temps précieux qu'il m'a consacrée.

J'adresse aussi mes remerciements aux membres de jury qui me font honneur en acceptant de juger notre travail.

Je remercie Mr Arkoub Malek pour son entière disponibilité au sein l'entreprise Sonatrach
Je remercie la personne la plus cher à mon cœur qui m'a soutenu malgré tous et jusqu'au bout MAdJID
En fin Je remercie tous ceux qui ont contribué de près ou de loin à ce que modeste travail puisse voir le jour.

Dédicaces

Je dédie ce modeste travail à mes parents pour leurs soutiens tous aux longs de mes études,mon frère et mes sœurs, mes amis proches spécialement madjid ,mes copine de chambre et a toute la famille Smaoun et Graba.

lyna

Table des matières

Chapitre III : Etude de l'organisme d'accueille

Chapitre IV : analyse des besoin et conception

Chapitre V : réalisation d'une application de gestion de réseaux baser sur SNMP

Listes des figures

Liste des tableaux

Introduction générale

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. On assiste à leur déploiement à tous les niveaux de la société, dans les entreprises, au niveau national et international, y compris dans les domiciles des usagers. Quant aux entreprises, ces réseaux leur apportent un moyen efficace pour mettre en œuvre un travail coopératif, pour faire communiquer des ordinateurs distants, pour partager des données, mais aussi pour imprimer à distance, envoyer des messages, et accéder à des bases de données délocalisées.

L'évolution des réseaux informatique pose un problème majeur : la manière dont ceux-ci sont pratiquement géré. En effet, avec la multiplication des machines qui ne cessent d'être fabrique des jours aux jours, la complexification des architectures qui s'en suivent, il devient évidement difficile de gérer un réseau.

Une autre contrainte de la gestion est la dépendance de service : Les activités des entreprises deviennent aussi dépendantes du fonctionnement de ce moyen de communication. Aussi est-il donc crucial que les services de communications du réseau soient disponibles en permanence. Les éventuels dysfonctionnements ou pannes doivent être détectés le plus rapidement possible et traités dans un délai compatible avec les activités de l'entreprise. C'est en cette activité de surveillance du réseau et des services qu'il offre que consiste, précisément, la gestion de réseau. Cette dernière couvre différentes tâches qui doivent être réalisées dans des échelles de temps plus ou moins importantes. Les cinq activités principalement reconnues en sont la gestion de la configuration, la gestion des fautes, la gestion des performances, la gestion de la sécurité et enfin la gestion des comptabilités. Ces activités peuvent être plus ou moins importantes selon l'activité de l'entité qui met en place le réseau.

Le protocole SNMP (Simple Network Management Protocole) que nous allons étudier plus en détails au cour de ce travail a pour rôle exclusif la gestion de réseau, il a été développé pour apporter des moyens simple d'administration en distance aux administrateurs.

Le but de cette étude consistera dans un premier temps de comprendre le principe de ce protocole, son fonctionnement, et son apport dans la tâche de l'administration et dans le second temps exploiter le langage de programmation java pour implémenter une application de gestion de réseau basé sur ce protocole.

Pour l'élaboration de ce présent travail, nous avons procédé d'abord par une lecture approfondie des ouvrages de référence à la matière en vue de bien assimiler le concept théorique de base qui régit l'administration réseau, le protocole SNMP et la programmation en java. Mais aussi par des entretiens réguliers avec les professionnels qualifier à la matière et nos différents encadreurs.

Ce travail comporte 5 chapitres brièvement décrits comme suivent :

Ø 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.

Ø 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.

Ø Le chapitre 3 présente l'organisme d'accueil qui nous a permis d'étudier sont réseau afin d'implémenter notre application.

Ø Le chapitre 4 traite l'analyse des besoins et la conception de l'application.

Ø Le chapitre 5 traite l'implémentation de l'application en java. Il montre pas à pas comment on peut mettre au point une application de gestion en se base sur le protocole SNMP en java.

Chapitre I : administration et gestion de réseaux

I.1. Introduction

De nos jours, le réseau est en train de devenir obligatoire dans tous les domaines 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.

Dans ce chapitre nous présentons les principes de la gestion de réseaux et les différents protocoles qui existent.

I.2. Définition d'un réseau informatique [1]

Ensemble de machines interconnectées qui servent à échanger des flux d'information. Un réseau répond à un besoin d'échanger des informations**.**

I.3. Qu'est-ce que la gestion de réseaux ? [3]

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…

I.4. Fonction de base de la gestion de réseaux

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 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.

I.4. Type de gestion [4]

a. Gestion configuration

La gestion de la configuration permet de désigner et de paramétrer différents objets.
Les procédures requises pour gérer une configuration sont la collecte d'informations, le Contrôle de l'état du système et enfin la sauvegarde de l'état dans un historique.
Elle couvre l'ensemble des fonctionnalités suivantes :

- Démarrage, initialisation des équipements ;
- Positionnement des paramètres ;
- Cueillette des informations d'état et intervention dans les paramètres ;
- Modification de la configuration du système ;
- Association des noms aux objets gérés ;
- Changement de l'adresse IP d'une machine ;
- Changement de l'adresse IP d'un routeur ;
- Changement de la table de routage

b. Gestion de fautes

La gestion des fautes permet la détection, la localisation, la réparation des pannes et le Rétablissement du service. Elle couvre l'ensemble des fonctionnalités suivantes :

- La détection des fautes : elle comprend la préparation de rapports d'incidents de la gestion de compteurs ou des seuils d'alarme, le filtrage d'événements par filtrage en amont des informations, l'affichage des dysfonctionnements.
- La localisation : on y procède au moyen de rapports d'alarme, de mesures et de tests.
- La réparation : elle consiste à prendre les mesures correctives (réaffectation de ressources, « routage », limitation du trafic par filtrage, maintenance), ou encore à rétablir du service (tests de fonctionnement, gestion de systèmes de secours, etc.).
- L'enregistrement des historiques d'incidents et statistiques : la gestion des fautes ne peut se limiter à ces actions ponctuelles, nécessaires mais insuffisantes pour donner le service attendu. C'est la raison pour laquelle elle comporte aussi, d'une part, l'enregistrement d'historiques d'incidents et la compilation de statistiques qui peuvent porter sur la probabilité des pannes, leur durée, les délais de réparation et, d'autre part, un rôle d'interface avec les usagers qui consiste à les informer des problèmes réseau et à leur donner la possibilité de signaler eux-mêmes des incidents :
  – la déconnexion d'un câble ;
  – une mauvaise configuration d'un équipement ;
  – une interface défectueuse d'un routeur ;
  – la réinitialisation accidentelle.

Elle fournit des fonctions qui permettent à des fins de planification des ressources du réseau :

- De recueillir des données statistiques (taux d'erreurs, temps de transit, débit, etc.) ;
- De maintenir et analyser des journaux sur l'historique de l'état du système (événements).

Les informations obtenues serviront à l'analyse et à la planification du réseau. On peut diviser cette partie en deux : l'une traitant de la gestion de la performance en temps réel et l'autre en temps différé. Pour gérer la performance d'un réseau en temps réel, il faut mettre en place les fonctionnalités suivantes :

- Enregistrements des mesures de performance : cela passe par l'établissement et la mise à jour des critères et des conditions de mesure, la gestion de la collecte d'informations, le filtrage, la compilation de statistiques, l'adoption de mesures à la demande ou encore la gestion des fichiers de collecte.
- Surveillance de l'activité du réseau par visualisation de l'utilisation des ressources, le signalement des dépassements de seuils et l'analyse de la performance : cela implique une visualisation du fonctionnement du réseau (avec comme variables pertinentes par exemple la répartition de la charge, les différents débits, les temps de réponse ou encore la disponibilité) et une analyse des causes possibles de dépassement de seuil par corrélation avec les pannes d'équipements, au moyen de divers indicateurs.
- Changement de configuration proactive et réactive : le fait de gérer la performance en temps réel suppose que l'on soit capable de prendre des mesures correctives (ou réactives) et préventives (ou proactives). La gestion réactive vise à établir lors de la détection d'un problème de performance des mesures de réaffectation des ressources par modification des paramètres de configuration ou par redistribution du trafic. Ces mesures, de par leurs natures, sont prises afin de répondre à un problème déjà existant. La gestion proactive consiste à prendre des mesures initiales permettant d'éviter d'arriver à une situation critique. Cette tâche est effectuée en temps différé et comporte quant à elle un ensemble de sous-tâches :
  – l'analyse des informations par la compilation de statistiques, d'historiques où encore d'indicateurs de qualité du service ;

– l'édition de tableaux de bord et de rapports, qu'ils soient périodiques ou qu'ils soient effectués à la demande ;

– une certaine forme d'analyse prévisionnelle par la constitution de matrices de trafic, par la détection de risques de saturation ou d'engorgement, par des simulations de scénarios, par le suivi de la gestion corrective, et enfin par la planification et le dimensionnement du réseau.

c. Gestion de performances

La gestion de la performance comprend les procédures de collecte de données et d'analyse statistique devant aboutir à la production de tableaux de bord.
Elle fournit des fonctions qui permettent à des fins de planification des ressources du réseau :

- De recueillir des données statistiques (taux d'erreurs, temps de transit, débit, etc.)
- De maintenir et analyser des journaux sur l'historique de l'état du système (événements). Les informations obtenues serviront à l'analyse et à la planification du réseau. On peut diviser cette partie en deux : l'une traitant de la gestion de la performance en temps réel et l'autre en temps différé. Pour gérer la performance d'un réseau en temps réel, il faut mettre en place les fonctionnalités suivantes :
- Enregistrements des mesures de performance : cela passe par l'établissement et la mise à jour des critères et des conditions de mesure, la gestion de la collecte d'informations, le filtrage, la compilation de statistiques, l'adoption de mesures à la demande ou encore la gestion des fichiers de collecte.
- Surveillance de l'activité du réseau par visualisation de l'utilisation des ressources, le signalement des dépassements de seuils et l'analyse de la performance : cela implique une visualisation du fonctionnement du réseau (avec comme variables pertinentes par exemple la répartition de la charge, les différents débits, les temps de réponse ou encore la disponibilité) et une analyse des causes possibles de dépassement de seuil par corrélation avec les pannes d'équipements, au moyen de divers indicateurs.
- Changement de configuration proactive et réactive : le fait de gérer la performance en temps réel suppose que l'on soit capable de prendre des mesures correctives (ou réactives) et préventives (ou proactives). La gestion réactive vise à établir lors de la détection d'un problème de performance des mesures de réaffectation des ressources par modification des paramètres de configuration ou par redistribution du trafic. Ces mesures, de par leurs natures, sont prises afin de répondre à un problème déjà existant. La gestion proactive consiste à prendre des mesures initiales permettant d'éviter d'arriver à une situation critique. Cette tâche est effectuée en temps différé et comporte quant à elle un ensemble de sous-tâches :
  – l'analyse des informations par la compilation de statistiques, d'historiques ou encore d'indicateurs de qualité du service ;
  – l'édition de tableaux de bord et de rapports, qu'ils soient périodiques ou qu'ils soient effectués à la demande ;
  – une certaine forme d'analyse prévisionnelle par la constitution de matrices de trafic, par la détection de risques de saturation ou d'engorgement, par des simulations de scénarios, par le suivi de la gestion corrective, et enfin par la planification et le dimensionnement du réseau.
  .

d. Gestion de sécurités

La gestion de la sécurité est une fonction de gestion qui concerne le contrôle et la distribution des informations utilisées pour la sécurité. Elle englobe le cryptage et la liste des droits d'accès.

À l'appui des politiques de réseau, la gestion de réseau consiste à collecter les informations de gestion et à les interpréter. Voici les fonctionnalités qui doivent être mises en œuvre :

- Dans ce contexte, il faut dans un premier temps assurer la sécurité relative à l'administration du réseau elle-même, c'est-à-dire gérer les droits d'accès aux postes de travail, gérer les droits liés aux attentes des opérateurs, et enfin les autorisations d'accès aux informations de gestion.

- Ensuite, il faut garantir la sécurité des accès au réseau géré ; pour cela, il faut mettre en place des mécanismes qui impliquent des fonctions telles que la définition des conditions d'utilisation, l'activation ou la désactivations des mécanismes, la modification de certains paramètres ou encore la gestion des listes d'autorisation (aux machines, à différents services ou à divers éléments de réseau) ; il faut évidemment en outre effectue un contrôle des accès (identités, horaires, temps de connexion, destination) et une détection des tentatives d'accès frauduleuses (enregistrement, compilation de statistiques et déclenchement d'alarmes si nécessaire).

- Enfin, il faut garantir la sécurité de l'information par la gestion de mécanismes de protection, de cryptage et de décryptage, et par la détection d'incidents et de tentatives de fraude.

Voici les fonctions de gestion de sécurité qui doivent être mises en œuvre pour supporter cette activité :

• Soutien à l'authentification.
• Contrôle et maintenance des autorisations.
• Contrôle et maintenance des commandes d'accès.
• Gestion des clés.
• Maintenance et examen des fichiers de sécurité.

Nous ne traiterons pas vraiment de la gestion de sécurité mais seulement des besoins sécurisés pour les opérations de gestion.

e. Gestion de compatibilités

La gestion de la comptabilité permet de connaître les charges des objets gérés, les coûts de communication, etc. Cette évaluation est établie en fonction du volume et de la durée de la transmission. Elle couvre l'ensemble des fonctionnalités suivantes :

- Les mesures sur l'utilisation des ressources, et leur enregistrement en vue d'obtenir des historiques ;

- Le contrôle des quotas par utilisateur en faisant des mises à jour des consommations courantes et en vérifiant les autorisations de consommation ;

- Le suivi et le contrôle des dépenses par stockage et mise à jour des tarifs des opérateurs, par gestion des tickets de taxation, par évaluation en temps réel de la consommation courante, par vérification des factures, et enfin par suivi des coûts d'exploitation et de matériels (investissement, amortissement et maintenance) ;

- La gestion financière : bien évidemment, on retrouve dans la gestion comptable une partie financière qui consiste à ventiler les coûts (par service, par utilisateur ou encore par application), à analyser et prévoir les dépenses et enfin à étudier les possibilités de réduction des coûts ;
- La facturation : finalement, l'activité de gestion comptable aboutit à une facturation interne, ce qui implique la gestion des clients et des trafics, la production de tickets de taxation et de factures, le contrôle de la facturation et enfin le stockage des historiques.

I.5. Architecture d'administration [2]

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

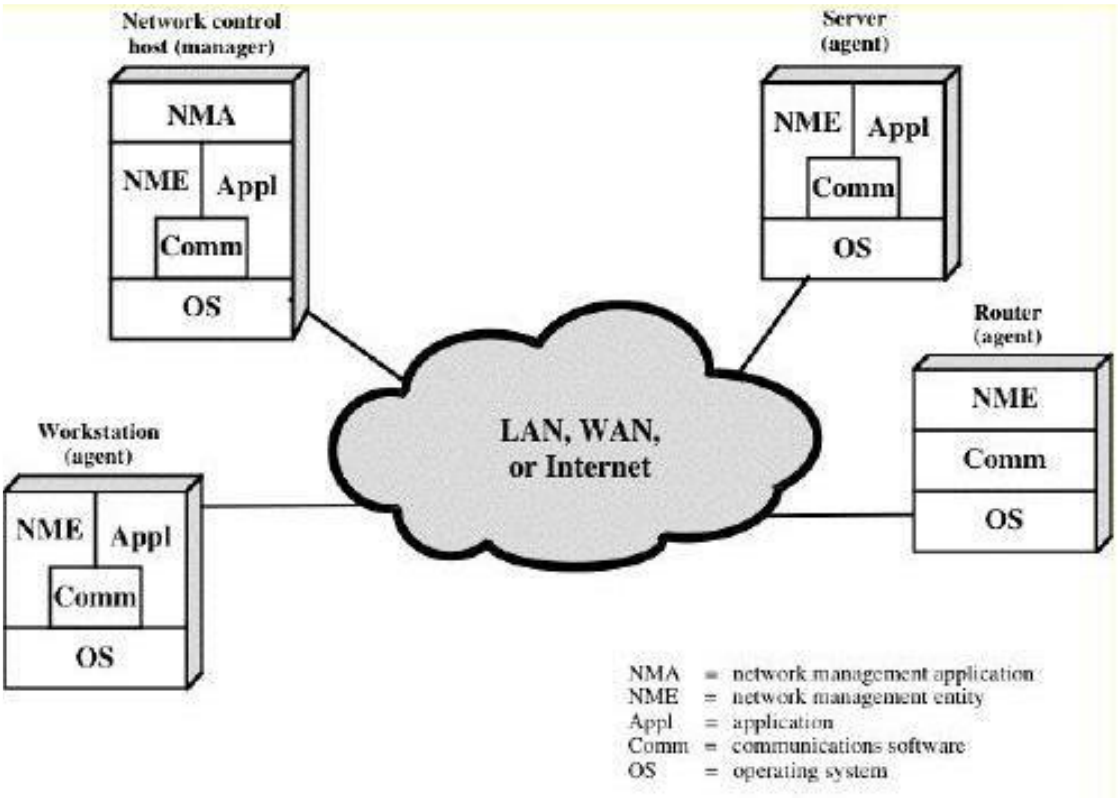

Figure 1 : l'architecture Gérant/Agent

I.6. Les protocoles de gestion de réseaux [2]

Les organismes de normalisation et les consortiums internationaux ont proposé plus d'une dizaine de solutions dont les plus populaires sont :

- **SNMP** : proposé par l'IETF en 1988 pour la gestion des environnements TCP/IP.

SNMP (Simple network management protocol) est devenu le protocole de gestion de référence en raison du succès des protocoles de l'IETF (tels que IP, TCP). Cet environnement est actuellement le plus déployé et utilisé.

- **TMN/CMIP** : proposés respectivement par l'UIT-T et l'ISO. L'architecture TMN (Telecommunication management network) et le protocole CMIP (Common management information protocol) constituent la norme dans le domaine de la gestion de réseau de télécommunication. CMIP présente une version améliorée de SNMP tandis que TMN introduit un cadre de travail pour planifier, installer, maintenir, utiliser et administrer un réseau de télécommunication et les services associés. La complexité de ces deux entités a été un frein à leur expansion dans les petits réseaux et ils sont quasi exclusivement utilisés dans les réseaux opérateurs.

- **WEBM/DMI/CIM** : proposés par les fabricants des postes de travail et les serveurs regroupés dans le consortium DMTF (Desktop management task force, dénommé aujourd'hui Distributed management task force). Leur objectif est de pousser les aspects gestion jusqu'aux postes de travail et les serveurs incluant ainsi tous les éléments du système d'information de l'entreprise. Différents environnements ont été proposés : DMI (Desktop management interface), CIM (Common information model), WBEM (Web based management) et DEN (Directorie enabled network), qui représentent différentes approches d'intégration mais qui sont en train d'être intégrés dans la même architecture.

- **DME** : proposée par les fabricants de logiciels regroupés dans l'OSF (Open software fundation), cette architecture dite DME (Distributed management environnement) est orientée vers la gestion exclusive des postes Unix. Nous ne traiterons pas de ce modèle car il est très orienté poste Unix mais ne prend pas en compte la gestion des équipements réseaux.

- **OMA** : proposée par le consortium OMG (Object management group), cette architecture de gestion orientée objets distribués, dite OMA (Object management architecture) est basée sur Corba (Common objet request broker architecture) et se propose d'apporter une solution de gestion distribuée intégrant les différentes approches suscitées.
- **JMX** : proposée par le consortium Java, JMX (JavaTM management extensions) est un ensemble de spécifications et API pour la gestion de réseau, faisant partie de la solution J2EETM. Elle se propose également de fournir une solution unifiée par rapport aux solutions SNMP/TMN/WEBM.

I.7.Conclusion

Dans ce chapitre nous avons vu les principes de gestion de réseaux et les différents protocoles qui facilite cette tâche. Le chapitre suivant sera consacré à l'étude du protocole SNMP.

Chapitre II : Le protocole SNMP

II.1. Introduction

Parmi les différents protocoles de gestion de réseaux à distance, on trouve le protocole SNMP (Simple Network Management Protocole). Dans ce chapitre nous allons étudier en détail son fonctionnement.

II.2. Présentation [4]

SNMP (Simple Network Management Protocol) est le protocole de gestion de réseaux proposé par l'IETF. Il est actuellement le protocole le plus utilisé pour la gestion des équipements de réseaux. C'est un protocole relativement simple. Pourtant l'ensemble de ses fonctionnalités est suffisamment puissant pour permettre la gestion des réseaux hétérogènes complexes. Il est aussi utilisé pour la gestion à distance des applications : les bases de données, les serveurs, les logiciels, etc.

II.3. Historique [5]

Vers la fin des années 70, les petits réseaux isolés évoluèrent vers des grands réseaux interconnectés. Ils devinrent de plus en plus difficiles à gérer et le développement d'un protocole spécifique s'avéra alors nécessaire. En 1988, l'Internet Activities Board (IAB) approuva le développement de SNMP (Simple Network Management Protocol) et de CMOT (Common Management Information Protocol Over TCP/IP). A ce moment-là, SNMP devait être une solution à court terme et CMOT à long terme. CMOT est dérivé de CMIP (Common Management Information Protocol) qui devait, lui, être utilisé sur OSI. En attendant que OSI émerge et remplace TCP/IP (!) ... il fut convenu de développer CMOT dans une phase purement transitoire. L'IAB imposa que CMOT et SNMP utilisent la même base de données d'objets gérables. Donc une SMI (Structure of Managed Information) et une MIB (Management Information Protocol) communes devaient être définies et utilisées. Cette décision avait pour but de faciliter la transition future de SNMP vers CMOT. Il est rapidement apparu que cette contrainte était non réaliste car en SNMP, on manipule essentiellement des variables et en CMIP, on manipule des objets au sens de la technologie orientée objet. En 1989, la séparation des deux protocoles fut acceptée par l'IAB et les deux protocoles suivirent alors une évolution parallèle et indépendante. Une fois libéré de la contrainte de compatibilité avec OSI, les progrès ont été rapides. SNMP a été adopté par de nombreux constructeurs et est devenu à ce jour un standard très répandu de gestion réseau.

II.4. Les composants de SNMP [4]

L'environnement de gestion SNMP est constitué de plusieurs composants : la station de supervision, les éléments actifs du réseau, les variables MIB et un protocole.

Les éléments actifs du réseau sont les équipements ou les logiciels que l'on cherche à gérer. Cela va d'une station de travail à un concentrateur, un routeur, un pont, etc. Chaque élément du réseau dispose d'une entité dite agent qui répond aux requêtes de la station de supervision. Les agents sont des modules qui résident dans les éléments réseau. Ils vont chercher l'information de gestion comme par exemple le nombre de paquets reçus ou transmis.

- **La station de supervision** (appelée aussi manager) exécute les applications de gestion qui contrôlent les éléments réseaux. Physiquement, la station est un poste de travail.

- **La MIB :** (Management Information Base) est une collection d'objets résidant dans une base d'information virtuelle. Ces collections d'objets sont définies dans des modules MIB spécifiques.

- **Le protocole** : qui permet à la station de supervision d'aller chercher les informations sur les éléments de réseaux et de recevoir des alertes provenant de ces mêmes éléments.

II.5. Fonctionnement [6]

Le protocole SNMP est basé sur un fonctionnement asymétrique. Il est constitué d'un ensemble de requêtes, de réponses et d'un nombre limité d'alertes. Le manager envoie des requêtes à l'agent, lequel retourne des réponses. Lorsqu'un événement anormal surgit sur l'élément réseau, l'agent envoie une alerte (trap) au manager.
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.

II.5.2.1. Emission d'un message [6]

Pour envoyer un message, l'agent suit la procédure suivante :

- Le PDU est construit.
  - Est soumis à un service d'authentification où, après étude des adresses de destination, de la source et du nom de la communauté, on choisira ou non la nécessité de crypter le PDU.
  - Le message est construit à partir du PDU avec l'ajout du nom de la communauté et la version de SNMP.
  - Ce nouvel objet ASN.1, est enfin codé et envoyé au service transport.

II.5.2.2. Réception d'un message [6]

- Le message est reçu et se voit opérer une vérification syntaxique. Si le message est défectueux, il est ignoré.
- Le numéro de version est vérifié, s'il n'est pas conforme, le message est ignoré.
- Le nom d'utilisateur, le PDU, l'adresse source et destination au niveau transport, sont soumis à un service qui se charge de l'authentification.
- Si l'authentification échoue, le service prévient l'entité transport de SNMP, la quelle 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.

II.6. Les commandes SNMP

II.6.1. Les requêtes SNMP

Il existe quatre types de requêtes : GetRequest, GetNextRequest, GetBulk, SetRequest.

- **GetRequest :** permet la recherche d'une variable sur un agent.
- **GetNextRequest :** permet la recherche de la variable suivante.
- **GetBulk :** permet la recherche d'un ensemble de variables regroupées.
- **SetRequest :** permet de changer la valeur d'une variable sur un agent.

II.6.2. Les réponses SNMP

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

- **Get Response :** est générée par une entité du protocole uniquement sur réception de la GetRequest-PDU, GetNextRequest-PDU, ou Striqués-PDU.

Dès la réception de la GetResponse-PDU, l'entité du protocole de réception présente son contenu à son entité d'application SNMP.

II.6.3. Les alertes (Traps, Notifications)

Les alertes sont envoyées quand un événement non attendu se produit sur l'agent. Celui-ci en informe la station de supervision via une trap. Les alertes possibles sont : Cold Start, Warm Start, Link Down, Link Up, AuthentificationFailure.

- **Cold Start :** piège signifie que l'entité du protocole d'envoie se réinitialise tels que la configuration de l'Agent ou de l'entité mise en œuvre peut être modifiée.

- **Warm Start :** piège signifie que l'entité du protocole d'envoie se réinitialise de telle sorte que ni la configuration de l'Agent ni l'entité mise en œuvre est modifiée.

- **Link Down :** piège signifie que l'entité de protocole d'envoi reconnaît une défaillance dans l'un des liens de communication représentés dans la configuration de l'agent. Le piège-PDU de type Link Down contient, comme le premier élément de son variable-bindings, le nom et la valeur de l'instance ifIndex pour l'Interface affectée.

- **Link Up :** piège signifie que l'entité du protocole d'envoi reconnaît que l'un des liens de communication représentés dans la configuration de l'agent est venu.
  Le piège-PDU de type Link Up contient, comme le premier élément de sa variable-bindings, le nom et la valeur de l'instance ifIndex pour l'Interface affectée.

- **Authentification Failure** : piège signifie que le protocole d'envoi d'entité est le destinataire d'un message du protocole qui ne sont pas correctement authentifié. Alors que les mises en œuvre du protocole SNMP doivent être capables de générer ce piège, ils doivent aussi être capables de supprimer l'émission de ces pièges par un mécanisme spécifique de mise en œuvre.

II.7. Format du PDU de SNMP [6]

SNMP Message

Version	Community	SNMP PDU

GetRequest, GetNextRequest PDU and SetRequest PDU

PDU type	Request id	0	0	Variablebindings

GetResponse PDU

PDU type	Request id	error-status	error-index	Variablebindings

Trap PDU

PDU type	Enterprise	Agent-addr	Generic-Trap	Specific-trap	Time-stamp	Variablebindings

Variablebindings

name1	value1	name2	value2	...	name n	value n

Figure 2 : Format du PDU de SNMP

Description des champs :

- **Version** : Version de SNMP.
- **Community** : sert à faire de l'authentification. En fait on peut définir plusieurs groupes qui auront des droits différents sur les objets de la MIB (lecture seule, lecture/écriture)
- **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. Rq : Lors d'une opération **Get**, les valeurs sont NULL.
- **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.

II.8. Les différentes versions de SNMP [4]

II.8.1 SNMPv1 : Ceci est la première version du protocole, tel que définie dans le RFC 1157. La sécurité de cette version est triviale, car la seule vérification qui est faite est basée sur la chaîne de caractères " community ". SNMPsec Cette version ajoute de la sécurité au protocole SNMPv1. La sécurité est basée sur des groupes. Très peu ou aucun manufacturier n'a utilisé cette version qui est maintenant largement oubliée.

II.8.2. SNMPv2p (historique) : Beaucoup de travaux ont été exécutés pour faire une mise à jour de SNMPv1. Ces travaux ne portaient pas seulement sur la sécurité. Le résultat est une mise à jour des opérations du protocole, des nouvelles opérations, des nouveaux types de données. La sécurité est basée sur les groupes de SNMPsec.

II.8.3. SNMPv2c (expérimental) : Cette version du protocole est appelée " community stringbased SNMPv2 ". Ceci est une amélioration des opérations de protocole et des types d'opérations de SNMPv2p et utilise la sécurité par chaîne de caractères " community " de SNMPv1.

II.8.4. SNMPv2u (expérimental) : Cette version du protocole utilise les opérations, les types de données de SNMPv2c et la sécurité basée sur les usagers.

II.8.5. SNMPv2* (expérimental) : Cette version combine les meilleures parties de SNMPv2p et SNMPv2u. Les documents qui décrivent cette version n'ont jamais été publiés dans les 12 RFC. Des copies de ces documents peuvent être trouvées sur le site web et SNMP Research (un des premiers à défendre de cette version).

II.8.6. SNMPv3 (standard actuel) : Cette version comprend une combinaison de la sécurité basée sur les usagers et les types et les opérations de SNMPv2p, avec en plus la capacité pour les " proxies ". La sécurité est basée sur ce qui se trouve dans SNMPv2u et SNMPv2*.

II.9. Structure SMI (Structure of Management Information) [10]

La structure des informations de gestion (SMI), une norme SNMP décrit dans le RFC GTN 1155, définit la structure des informations MIB et les types de données admissibles. Le SMI identifie la manière dont les ressources au sein du MIB sont représentés et nommés. La philosophie derrière SMI est d'encourager la simplicité et l'extensibilité dans le MIB.

La spécification SNMP comprend un modèle, connu sous le nom de syntaxe abstraite numéro un (ASN.1) macro type d'objet

II.9.1. ASN.1[9]

ASN.1 est l'acronyme de syntaxe abstraite numéro un, un langage de description des informations structurées ; En général, l'information destinée à être transmise à travers un certain milieu d'interface ou de communication. ASN.1 a été normalisé à l'échelle internationale. Il est largement utilisé dans la spécification des protocoles de communication.

II.10. Le MIB [7]

Est une collection d'objets décrits formellement, dont chacun représente un type particulier d'information. Objets MIB accessibles et peuvent être gérés avec le Simple Network Management Protocol (SNMP) grâce à un système de gestion de réseau. Cette collection d'objets contient des informations requises par un système de gestion et l'information est stockée sous la forme d'un ensemble de variables MIB.

MIB extensions d'objet sont définis pour chaque ensemble d'entités apparentées qui peuvent être gérés. Ils définissent les actes d'état des informations telles que les statistiques de trafic, le nombre d'erreurs, et le contenu actuel des structures de données internes tels que la table de routage IP de l'ordinateur.

Tous les objets MIB sont basés sur une définition commune de l'information de gestion. Ceci est appelé la structure de gestion de l'information (SMI) et comprend le modèle d'information de gestion, les types de données autorisés et les règles pour préciser les catégories d'information de gestion.

II.10.1. Structure du MIB [4]

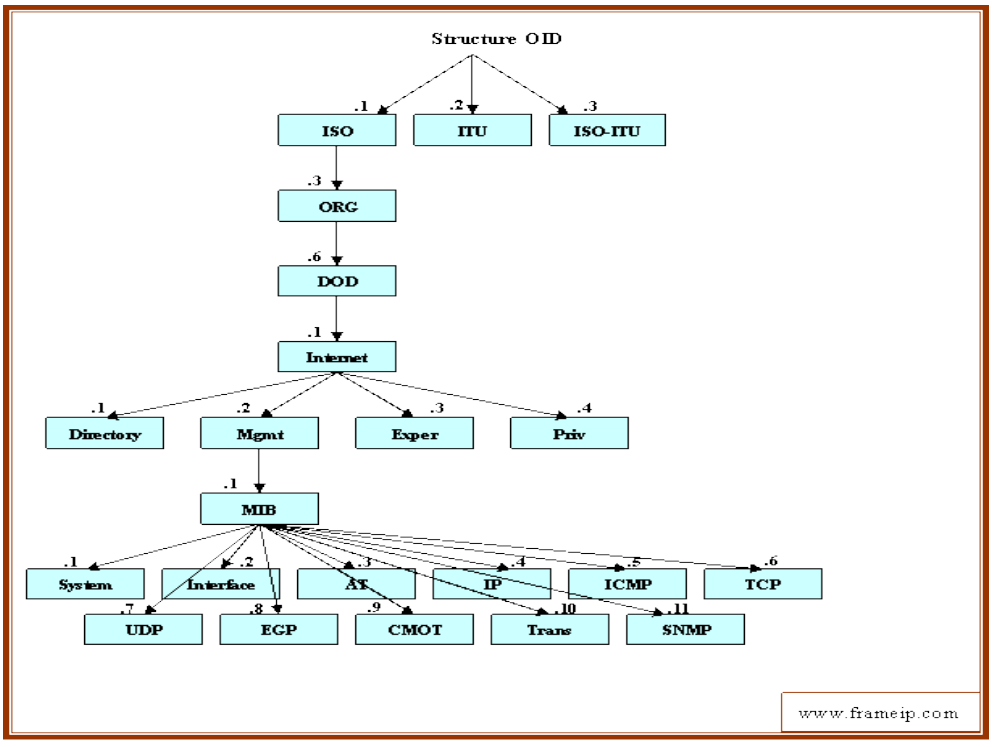

Figure 3 : Structure de la MIB

II.10.2. Description des champs de la MIB

Objet	Nombre de Sous objets	Description
Système	7	Informations générales concernant l'agent à travers le système
Interface	23	Informations concernant chaque interface IP de l'agent
Adrresse translation	3	La table de translation d'adresses qui réalise la correspondance entre l'adresse MAC et l'adresse IP
IP	38	Compteurs IP
ICMP	26	Compteurs ICMP
TCP	19	Compteurs TCP
UDP	7	Compteurs UDP
EGP	18	Compteurs EGP
CMOT	0	Compteurs pour CMOT (protocole OSI équivalent à SNMP)
Transmission	0	Modes de transmission et protocoles d'accès de chaque interface. Remplacera *at*
SNMP	30	Statistiques du trafic SNMP

Tableau 1 description des champs de la MIB

II.10.3. MIB objet [10]

SNMP définit deux types d'objets :

- **Scalaire :** ce sont des types simple (integer, counter, etc.). Le standard SNMP définit un nombre restreint de types de données scalaires.

- **Tableaux bidimensionnels :** SNMP offre une deuxième structure de donnée sous forme de tableau bidimensionnels. Une table SNMP contient des objet ligne contient le même ensemble de types de scalaires.

II.10.4. MIB Objet Identifiers [10]

Chaque objet dans le MIB a un *identificateur d'objet* (OID), que la station de gestion utilise pour demander la valeur de l'objet à partir de l'agent. Un OID est une séquence d'entiers qui identifie de manière unique un objet géré en définissant un chemin d'accès à cet objet par le biais d'une structure arborescente appelée l'*arbre OID* ou arbre d'enregistrement. Quand un agent SNMP doit accéder à un objet géré spécifique, il traverse l'arbre OID pour trouver l'objet. La hiérarchie et le format d'identificateur d'objet MIB est représenté dans la figure suivante :

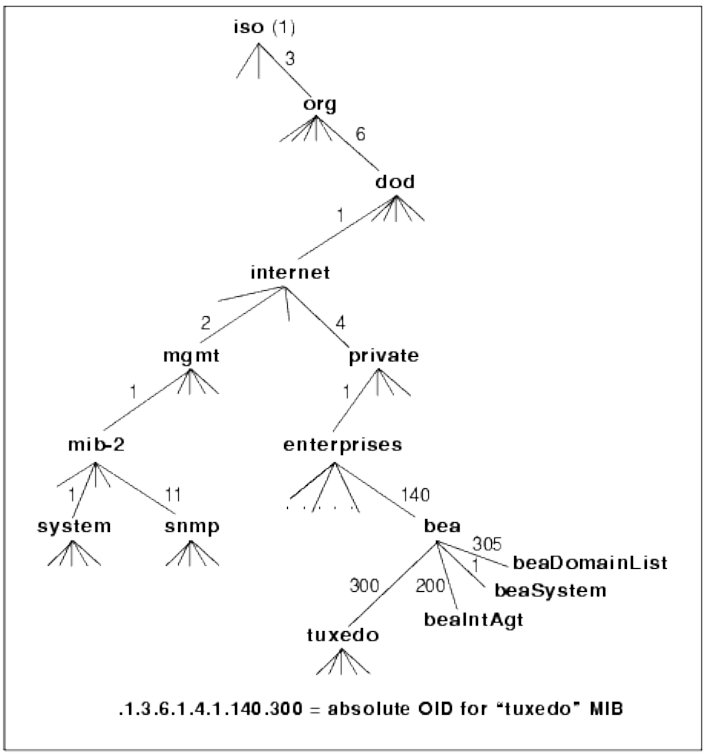

Figure 4 : hiérarchie et format d'un OID

II.10.5. Object Identifiers absolues et relatives [10]

OID absolus spécifient un chemin d'accès à un attribut de la racine de l'arbre OID. Les noms de OID absolus commencent toujours par un point et doivent spécifier chaque nœud de l'arbre OID à partir du nœud de plus haut à l'objet géré spécifique. Par exemple : .1.3.6.1.2.1.1.1

OID relative spécifient un chemin d'accès à l'attribut par rapport à un nœud dans l'arbre OID. Par exemple, 2.1.1.1 spécifie l'objet sysDescr dans le système groupe, par rapport au noeud Internet dans l'arborescence des OID.

II.10.6. Spécification Object Identifiers [10]

En plus d'utiliser la notation "dot-dot", une série de nombres entiers séparés par des points pour décrire OID, vous pouvez OID également exprimer en utilisant des symboles textuels au lieu de chiffres pour représenter les nœuds dans le chemin d'accès à l'objet, ou en utilisant une combinaison des deux entiers et des symboles textuels. Une *symbolique* OID utilise des mots clés mnémotechniques pour spécifier l'objet géré.

II.11. SNMP object description [8]

Un fichier de MIB contient des définitions de la structure de l'arbre global et des définitions d'objets de types feuilles qui vont permettre la collecte d'informations.

La définition d'un objet SNMP avec la norme SMI V1 est réalisée au moyen de 5 champs et sont résume dans le tableau suivant :

Champ	Description
OBJECT-TYPE	Ce champ fournit le nom de l'objet, ce nom est unique et permettra de collecter des information en utilisant la notation nominale. Ce champ est défini dans la RFC 1212
SYNTAX	Ce champ définit le type de valeurs gérées par l'objet : Les principales valeurs sont : **INTEGER** **GAUGE** **CONTER** **TIMESTAMP** **OCTET STRING** **OBJET IDENTIFIER** **NULL** **DISPLAYSTRING** **Avec la version 2 du SMI, il peut définir de nouvelles syntaxes à partir des syntaxes de base. Une nouvelle syntaxe utilise le mot clef TEXTUAL CONVENTION.**
ACCESS	Ce champ indique comment cet objet peut être adressé. Les valeurs possibles pour ce champ sont : **Read-only** : lecture seule. **Read-write** : lecture écriture. **Write-only** : en écriture seulement. Not-accessible : ne peut pas être adressé.
STATUS	Ce champ indique le statut de l'objet par rapport à la norme définie par le fichier de MIB. Un fichier de MIB standard va définir un ensemble d'objets dont certains devront être impérativement implémentés au niveau de l'gent pour répondre à la norme. Certains objets ne sont pas obligatoirement implémentés au niveau de l'agent en fonction du statut de l'objet définit dans la MIB.

	Les valeurs possibles pour ce champ sont : **Mandatory** : cet objet doit impérativement être implémenté au niveau de l'agent pour que l'agent puisse être compatible avec la norme. **Optional :** cet objet n'pas obligation d'être implémenté au niveau de l'agent. **Obselete :** cet objet n'est plus obligatoirement implémenté sur les agents de nouvelles générations.
DESCRIPTION	Ce champ contient une information dans un format texte décrivant l'usage ou l'utilisation de la valeur associée à l'objet. Le texte est encadré par des guillemets

Tableau 2: Tableau des champs de définition d'un objet SNMP en SMI V1

II.12. Conclusion

Dans ce chapitre, nous avons décrit le protocole SNMP, son fonctionnement, et ses différentes commandes. Ainsi que la structure de la MIB et ses différents composant.

Chapitre III : étude de l'organisme d'accueil

III.1. Introduction

Ce chapitre est consacré à la présentation de l'organisme d'accueil et l'étude de son réseau et sa gestion.

III.2. Présentation de SONATRACH

Sonatrach " Société Nationale pour la Recherche, la Production, le Transport, la Transformation et la Commercialisation des Hydrocarbures s.p.a " est une entreprise publique algérienne et un acteur majeur de l'industrie pétrolière.

Sonatrach est une compagnie nationale d'envergure internationale, c'est la clé de voûte de l'économie algérienne.

Le groupe pétrolier et gazier Sonatrach intervient dans l'exploration, la production, le transport par canalisation, la transformation et commercialisation des hydrocarbures et de leurs dérivés.

III.3. Les différentes branches de SONATRACH

Pour atteindre ces objectifs et optimisé son fonctionnement la Sonatrach a dégagé des 1992 cinq secteurs d'activité de base résumer dans l'organigramme suivant :

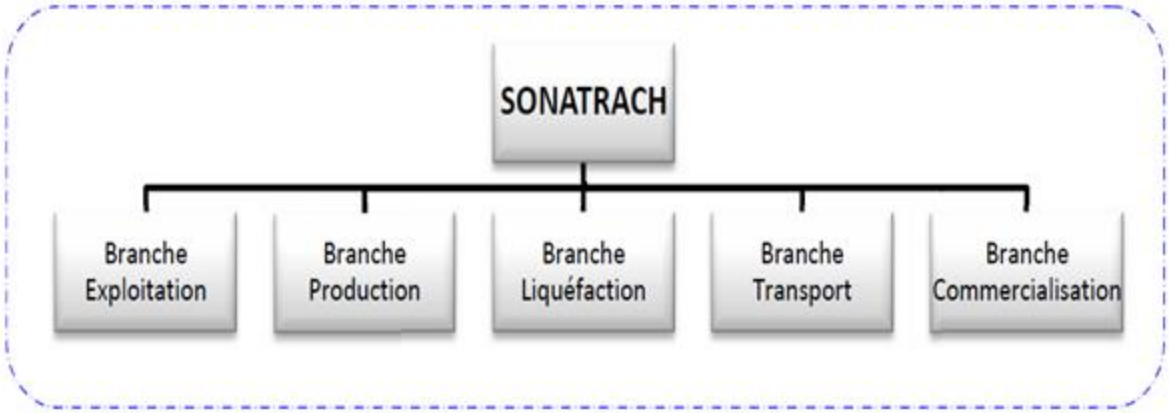

Figure 5 : les différentes branches de sonatrch

III.4. Présentation de la RTC

L'activité de transport par canalisation (TRC) est en charge de l'acheminement des hydrocarbures pétroles brut, gaz et condensât vers les ports pétroliers, les zones de stockages et les pays d'exploitation.

La SONATRACH possède six directions régionales de transport des hydrocarbures :

- La direction régionale Est (Skikda)
- La direction régionale Centre (Béjaia)
- La direction régionale Ouest (Arzew)
- La direction régionale de Haoud-EL-Hamra
- La direction régionale d'Ain Amenas
- La direction régionale Tebssa.

III.5. Structure de la RTC Bejaia

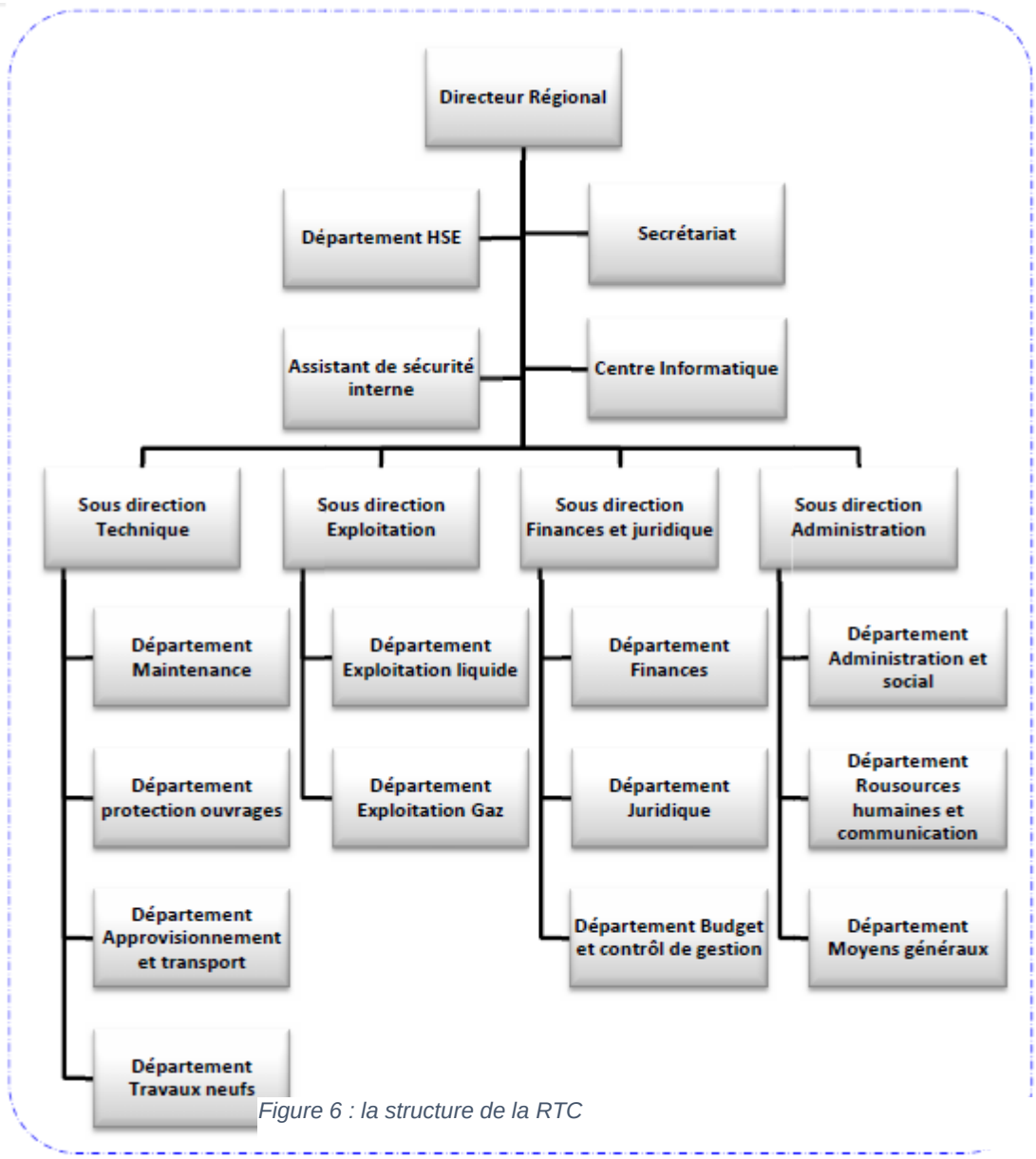

Figure 6 : la structure de la RTC

III.6. Etude du réseau de la RTC

III.6.1. Partie réseau

III.6.1.1. Présentation globale du réseau

Le réseau informatique de la RTC de Bejaia est constitué de deux bâtiment, l'ancien bâtiment sa topologie physique est en étoile étendue (voir figure 4.1), et le nouveau bâtiment sa topologie hybride (en étoile et en annaux).

III.6.1.2. Architecture de l'ancien bâtiment

Pour mettre en place le réseau de l'ancien bâtiment, la RTC à utiliser du matériel de type Cisco catalyst (routeur 6509, switch 2950, switch 3550). Le matériel est relié soit par fibre optique, soit par câble de cuivre.

Le Protocol HSRP est utilisé entre les deux routeurs de la salle informatique et la salle maintenance dans le cas d'une éventuelle panne d'un des routeurs, c'est-à-dire si l'un des routeurs tombe en panne l'autre prend automatiquement le relais, et cela en créant un routeur virtuel entre eux

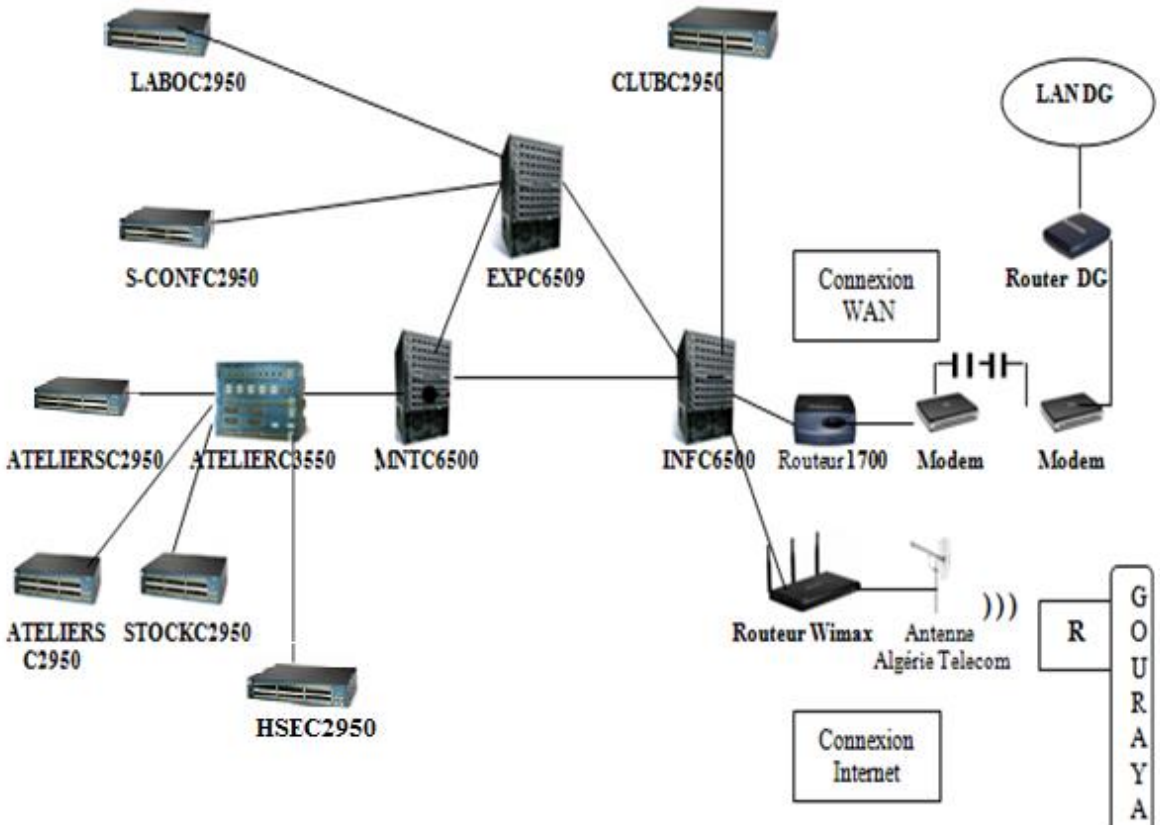

Figure 7 : architecture de l'ancien bâtiment

III.6.1.3. Architecture du nouveau bâtiment

Le réseau du nouveau bâtiment est constitué à partir de matériels Cisco catatyst (2 routeur 6509, 13 switch3750). Le réseau suit une architecture de trois couches spécifiques au matériel de type Cisco :

- Couche cœur
- Couche distribution
- Couche accès

Le materiels est relier par la fibre optique. Les deux routeurs sont liés par un câble cuivre croiser et s'envoie mutuellement des paquets Hello toute les 30seconde pour vérifier l'état des routeurs. Si l'un ne répond pas c'est qu'il y a un problème donc l'autre routeur va prendre automatiquement le relais.

III.6.1.4. La liaison entre ancien et nouveau bâtiment

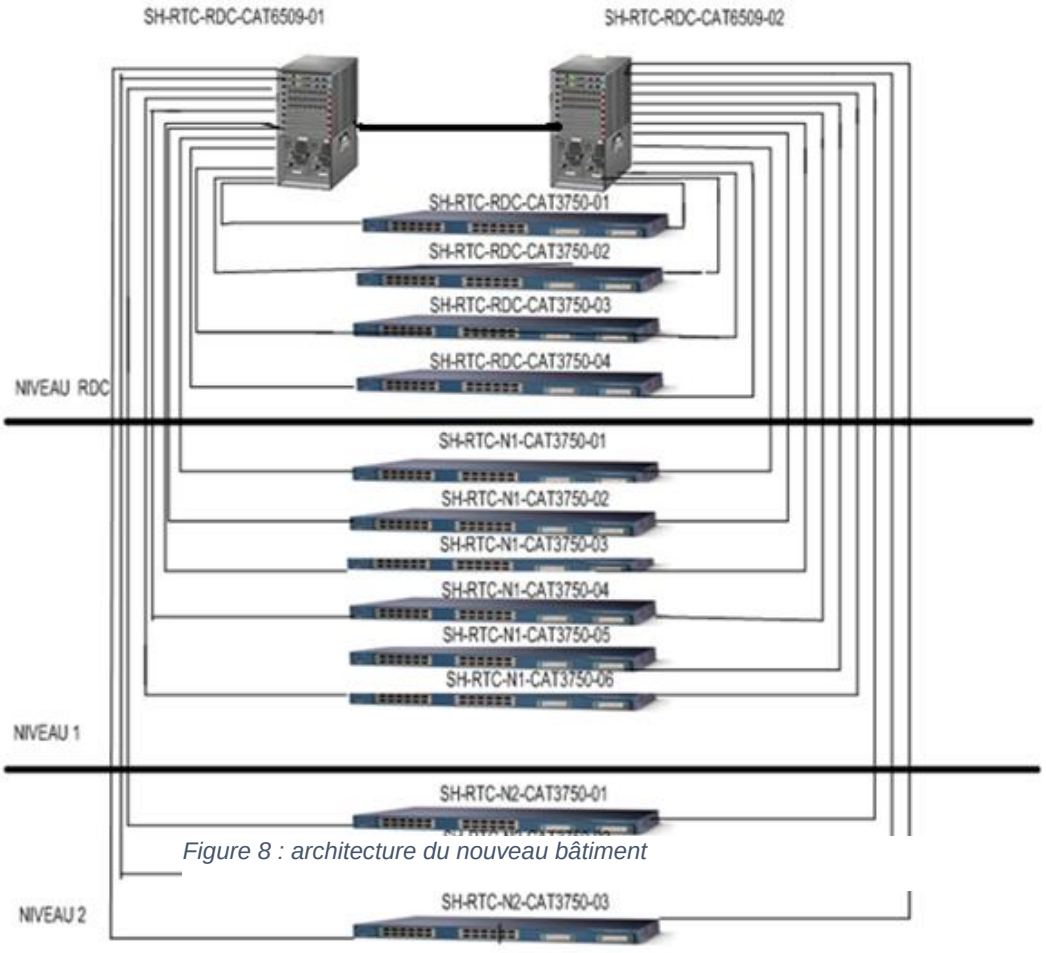

Figure 8 : architecture du nouveau bâtiment

La liaison entre l'ancien bâtiment et le nouveau se fait par la fibre optique. Tous les routeurs sont reliés entre eux pour que le réseau fonctionne toujours dans le cas d'une éventuelle panne de l'un des routeurs.

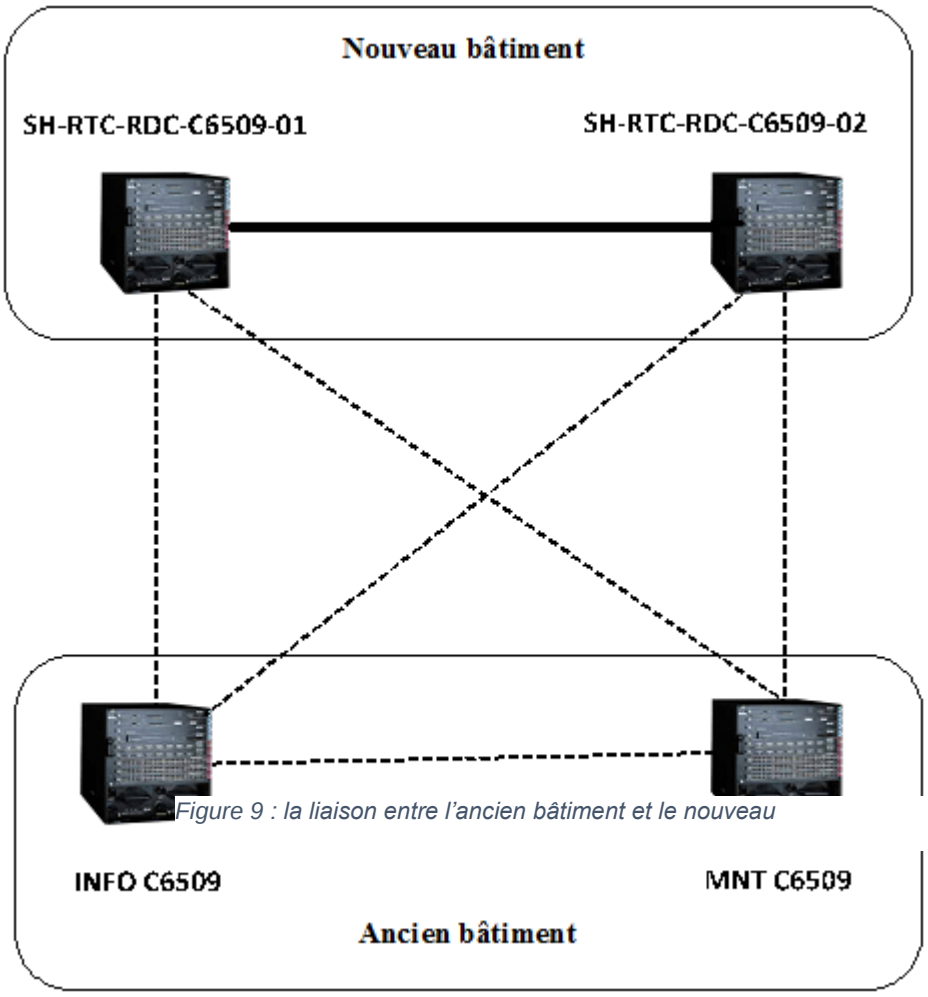

Figure 9 : la liaison entre l'ancien bâtiment et le nouveau

III.6.2. Partie système

La partie système de la RTC est constituer de :

- D'un contrôleur de domaine
- Serveur Dell power Edge 2800
- Active Directory
- Protocol DNS
- Protocol DHCP
- Serveur d'applications
- Ex change serveur 2004
- Anti-virus « F-secure »

- Serveur de fichier
- Serveur de bases de données
- Serveur LMS

III.6.3. Partie sécurité

La sécurité du réseau de la RTC est composée de quatre partie :

- **Partie equipement**
  - Websence Entreprise
  - Websence filtrage
- **Partie firewall**
  - Firewall juniper ssg550.
- **Partie Proxy**
  - Proxy Blue Coat SG 510
- **Real secure site protector ISS**
  - ISS Proventia GX 4002
  - ISS Proventia GX 5008

III.7. Présentations des problèmes existants

Sonatrach possède un grand réseau diviser en deux réseaux local nouveaux et ancien bâtiment et sa gestion est très difficile et complique.

III.8. Proposition d'une solution

La solution proposer est d'implémenter une application de gestion de réseaux baser sur le protocole SNMP, afin de rendre la gestion de réseaux de cette entreprise plus facile.

III.9. Conclusion

Ce chapitre présente l'organisme d'accueil ainsi que la structure de son réseau, les difficultés de le géré et propose une solution afin de remédier à ces difficultés.

Chapitre IV : Analyse des besoins et conception

IV.1. Introduction

La conception de logiciel est un art qui nécessite de l'expérience. Elle consiste à traduire les besoins en spécifiant comment l'application pourra les satisfaire avant de procéder à sa réalisation.

Ce chapitre sera consacré à la présentation du projet et du processus de modélisation (UML2.5) d'une part.

Et d'autre part détailler la phase analyse des besoins et la conception du projet.

IV.2. Présentation langage de modélisation

IV.2.1. Définition du processus unifié (UP)

Un processus unifié est un processus de développement logiciel construit sur UML ; il est itératif et incrémental, centré sur l'architecture, conduit par les cas utilisations et piloté par les risques.

IV.2.1. Définition du langage UML 2.5

UML (Unified Modeling Language) se définit comme un langage de modélisation graphique et textuel destiné à comprendre et décrire des besoins, spécifier et documenter des systèmes, esquisser des architectures logicielles, concevoir des solutions et communiquer des points de vue. UML unifie à la fois les notations et les concepts orientés objet.

IV.2.3 Les diagrammes de UML

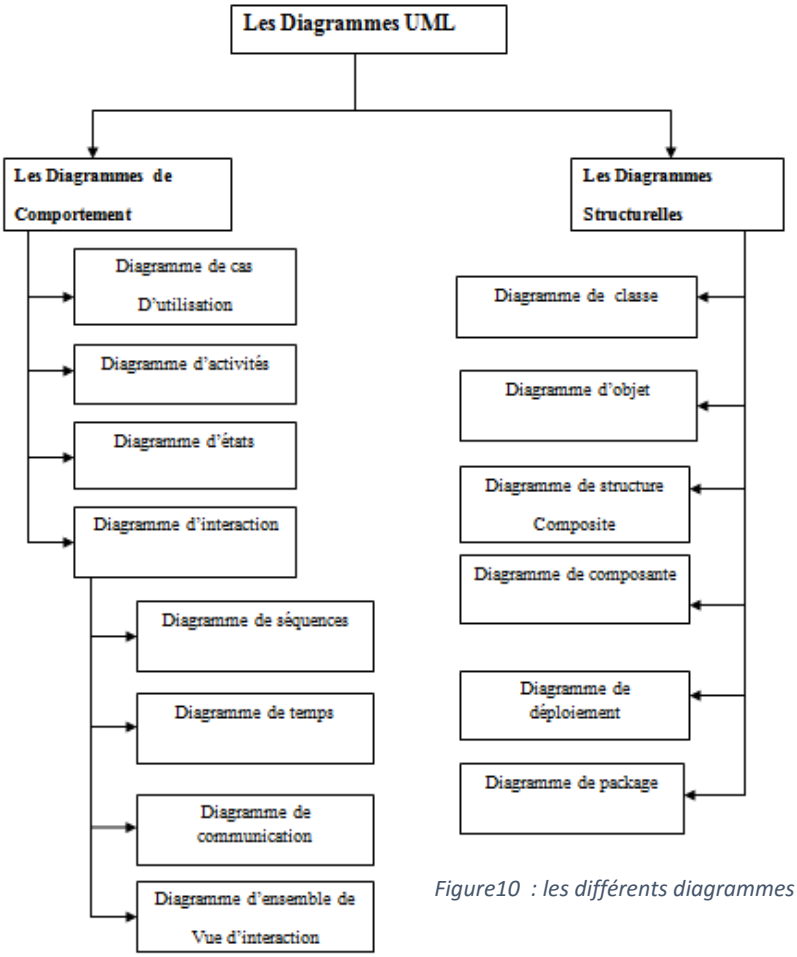

Figure10 : les différents diagrammes de l'uml

IV.3. Analyse des besoins

Afin de garantir la réussite et l'efficacité du projet, il faut définir avec précision les bordures de la solution à développer.

Les besoins d'utilisation de l'application sont repartis en besoin fonctionnels et non fonctionnels.

IV.3.1. Les besoins fonctionnels

Les besoins fonctionnels incluent les modules de gestion de l'application à réaliser tels que :

- **Gestion des utilisateurs** : permet d'ajouter, modifier, supprimer un autre administrateur.
- **Supervision des équipements** : permet de contrôler l'état de configuration des équipements
- **Gestion des fautes :** permet la récupération des alarmes (traps)
- **Gestion des performances :** l'application doit permettre de gérer des rapports de chaque équipement qui décrit ses informations et aussi d'enregistrer trace d'administrateur dans son historique.

IV.3.2. Les besoins non fonctionnels

Les besoins non fonctionnels sont les exigences qui ne concernent pas spécifiquement le comportement du système, mais plutôt d'identifier les contraintes internes et externes du système tels que :

- Le code doit être claire pour permettre des futures évolutions ou amélioration.
- L'ergonomie : l'application offre une interface conviviale et facile à utiliser.
- La sécurité : l'application doit respecter la confidentialité des données

IV.3.3. Identification des acteurs

- **Client :** sa tâche est de superviser le réseau et d'envoyer les requête SNMP.
- **Agent :** sa tâche est de répondre aux requêtes émises par l'administrateur et généré des alarmes en cas d'erreur.

IV.3.4. Identification des messages

- Message Get
- Message GetNext
- Mesage Set
- Messge traps

IV.3.5. Liste des cas d'utilisation

Cas d'utilisation	Acteur	Action
Gestion des compte	Administrateur	Modifier le mot de passe
Gestion des traps	Administrateur	Ecouter les traps
Gestion de la MIB	Administrateur	Chargement de la MIB
Gestion des requête SNMP	Administrateur	Exécution des requête SNMP
Répondre aux requête	Agent	Répondre aux requêtes émises par l'administrateur
Génération des traps	Agent	Génère les alarmes en cas de d'erreur
Maintenir la MIB	Agent	Mise à jour des valeur objet de la MIB

Tableau 3 : liste des cas d'utilisation

IV.3.6. Diagramme des cas d'utilisations

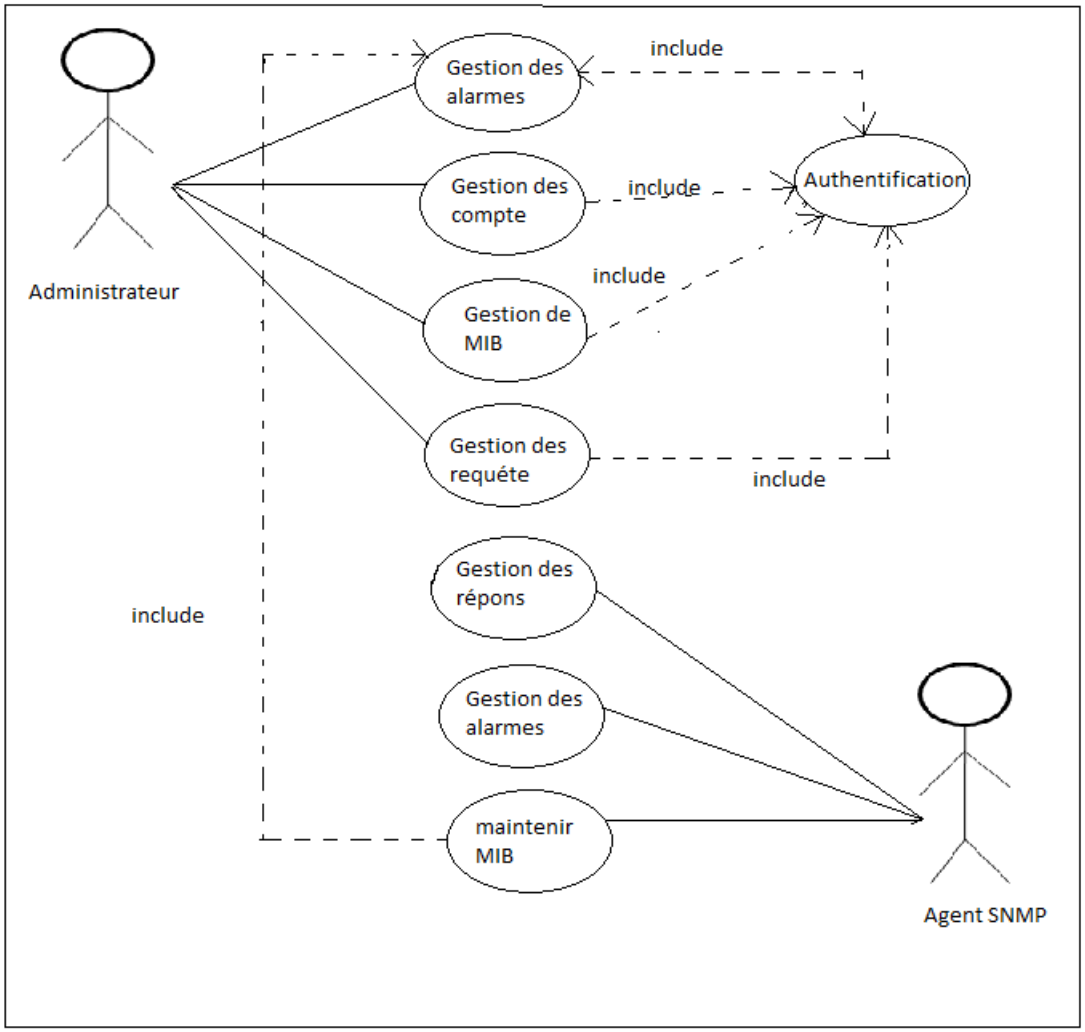

Figure 11 : Diagramme des cas d'utilisation

IV.3.7. Description des cas d'utilisation

- **Cas d'utilisation gestion de compte :**
  Acteur : administrateur :
  Objectif : modifier le mot de passe et le nom d'utilisateur.
  Pré- condition : exécuter l'application.
  Post- condition : ouverture de session.
- **Cas d'utilisation gestion des traps :**
  Acteur : administrateur.
  Objectif : Ecouter les traps genre par l'agent SNMP.
  Pré- condition : authentification.
  Post-condition : ouverture de session.
  Scenario nominal : l'administrateur lance l'écouter de traps sur le port 162
- **Cas d'utilisation la gestion de MIB :**

Acteur : administrateur.
Objectif : charger/décharger la MIB.
Pré- condition : authentification.
Post-condition : l'administrateur doit sélectionner la MIB à charger /décharger.
Scenario nominal : l'administrateur demande de charger/décharger le système exécute sa demande.

- **Cas d'utilisation gestion de requête :**
  Acteur : Administrateur.
  Objectif : consultation et mise à jour des objets de la MIB.
  Pré- condition : authentification.
  Post-condition : sélectionner un objet de la MIB et introduire l'OID et la communauté.
  Scenario nominal : l'administrateur interroge l'agent sur la valeur d'un objet en choisissant le type de requête (get, set ……).
- **Cas d'utilisation répons aux requêtes :**
  Acteur : agent.
  Objectif : exécuter les requêtes émises par l'administrateur.
  Pré- condition : demande une valeur d'un objet par l'administrateur.
  Post-condition : réception des requêtes émises par l'administrateur.
  Scenario nominal : exécuter les requêtes et envoyer les résultats à la station admin.

- **Cas d'utilisation gestion des alarmes :**
  Acteur : agent.
  Objectif : envoyer les notifications à l'administrateur.
  Pré- condition : l'administrateur doit lancer l'écouteur de traps.
  Post-condition : envoyer les traps sur le port 162.
  Scenario nominal : l'agent génère les traps ensuite il répond a l'écouteur qui a été lancer par l'admin.

- **Cas d'utilisation maintenir la MIB :**
  Acteur : agent.
  Objectif : consultation des objets de la MIB et mise à jour des variables de la MIB.
  Pré- condition : réception d'une requête émise par l'administrateur.
  Post-condition : introduire la nouvelle valeur à mettre à jour.
  Scenario nominal : exécuter les requête et mètre a jour la MIB.

IV.4. Diagrammes de séquence des cas d'utilisation de l'application

IV.4.1. Diagramme de séquence de cas utilisation gestion des requêtes

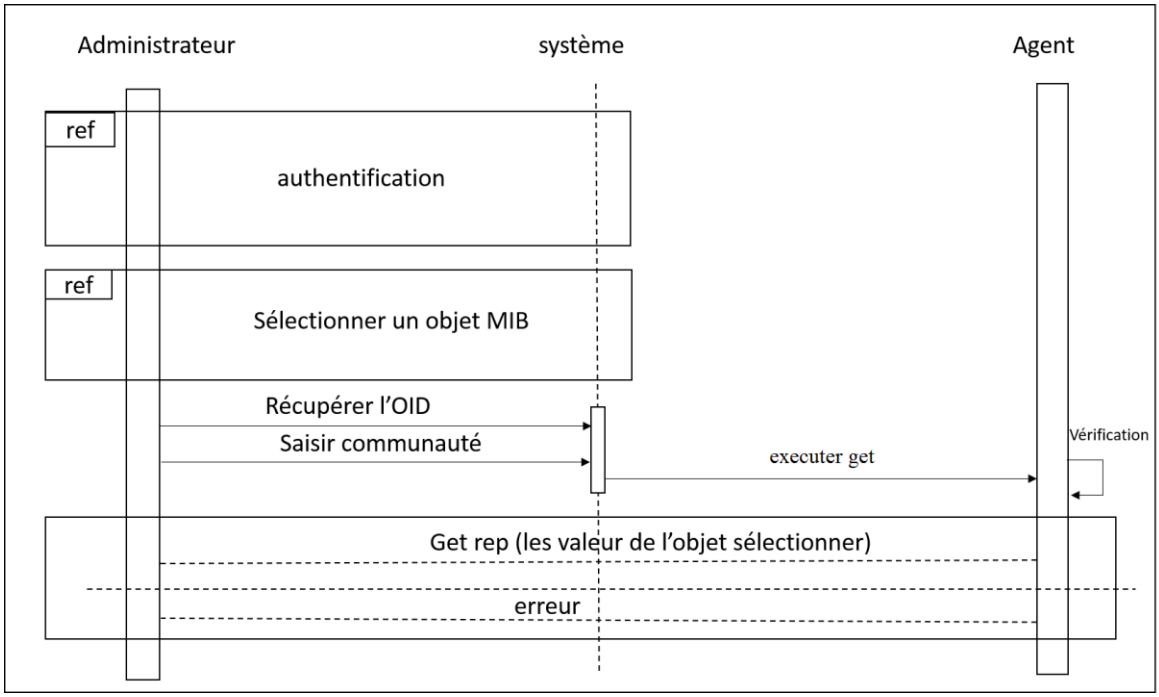

Figure 12 : diagramme de séquence de cas d'utilisation gestion de requête get /getnext

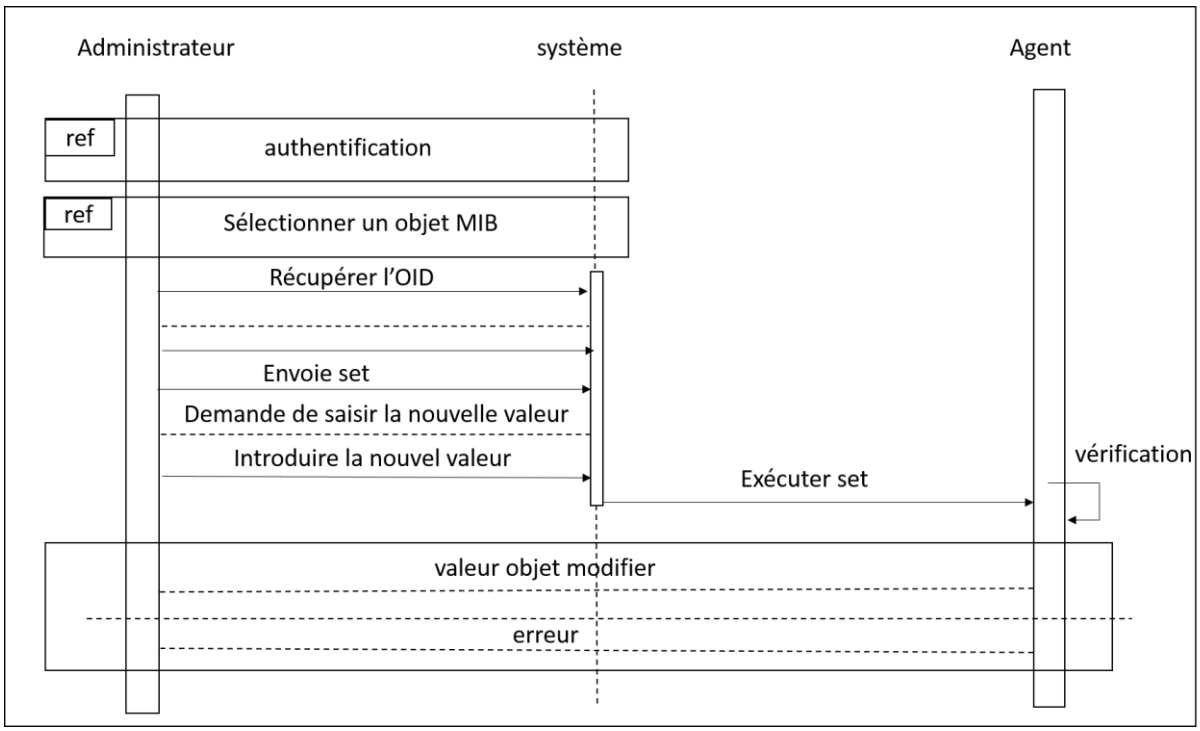

Figure 13 : diagramme de séquence de cas d'utilisation gestion de requête set

IV.4.2. Diagramme de séquence cas d'utilisation gestion de la MIB

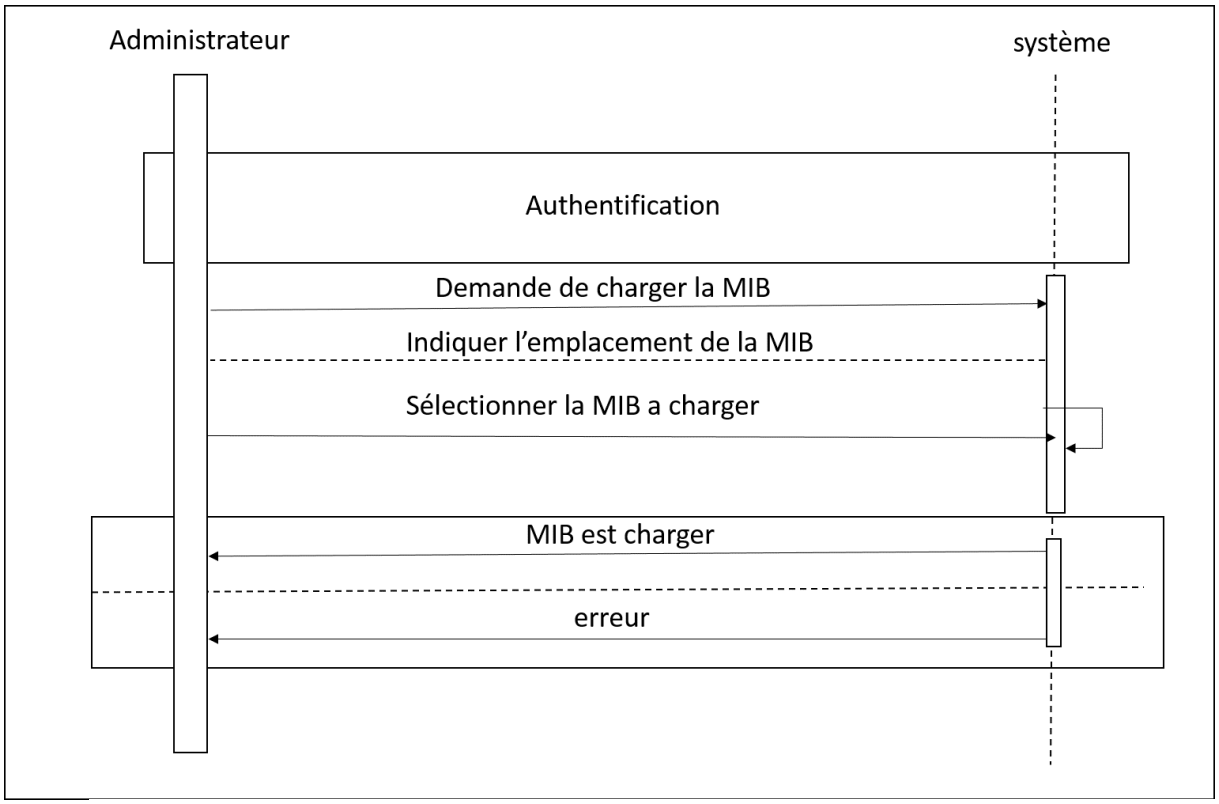

Figure14: diagramme séquence cas d'utilisation gestion de la MIB

IV.5. Diagramme de classe de l'application

IV.5.1. Dictionnaire de donnée

Classe	atribut	Methode
Fenetre		Main()
Client		Requet()
Mib		Initialize()
Snmpget		Requestget()
Snmpgetnext		Requestgetnext()
Snmpset		Reuestset()
Snmptrapreceiv		Trapreceiv()
Snmptrapsender		Trapsend()

Tableau 4 : dictionnaire de données

IV.5.2. Diagramme de classe

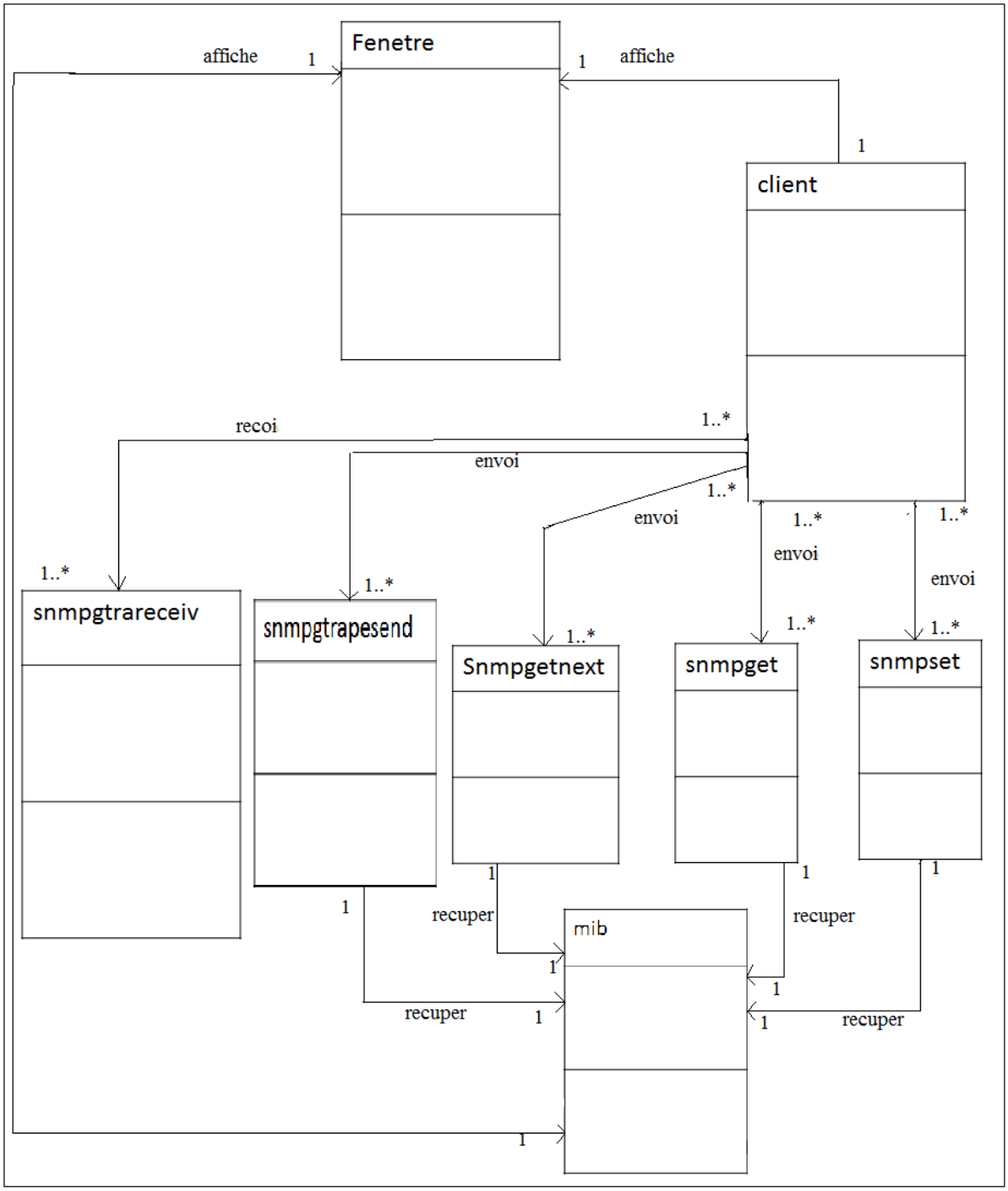

Figure 15 : diagramme de classe de l'application

IV.6. Maquette de l'application

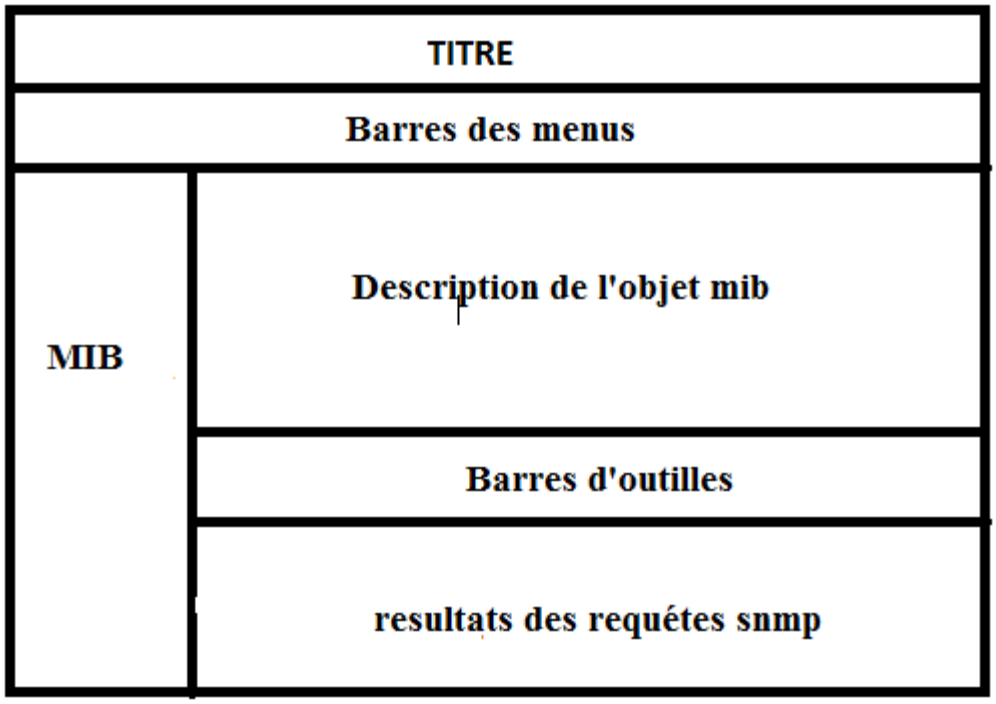

Figure 16 : maquette de l'application

IV.7. Conclusion

Ce chapitre, présente les différentes étapes suivies pour la conception de l'application et la description des fonctionnalités de cette dernière.

Chapitre V : Réalisation d'une application de gestion de réseaux sur SNMP

V.1. Introduction

Le développement d'une application de gestion de réseaux, nécessite l'installation de certains éléments de base comme d'un IDE, une API et la maitrise d'un langage de programmation. C'est ce que présente ce chapitre.

V.2. Présentation des éléments utiliser pour développer l'application

V.2.1. Java

Le langage **Java** est un langage de programmation informatique orienté objet créé par James Gosling et Patrick Naughton, employés de Sun Microsystems, avec le soutien de Bill Joy (cofondateur de Sun Microsystems en 1982), présenté officiellement le 23 mai 1995 au *SunWorld*.

V.2.2. Eclipse

Eclipse est un projet, décliné et organisé en un ensemble de sous-projets de développements logiciels, de la fondation Eclipse visant à développer un environnement de production de logiciels libre qui soit extensible, universel et polyvalent, en s'appuyant principalement sur Java.
Son objectif est de produire et fournir des outils pour la réalisation de logiciels, englobant les activités de programmation (notamment environnement de développement intégré et frameworks) mais aussi d'AGL recouvrant modélisation, conception, test, gestion de configuration, reporting… Son EDI, partie intégrante du projet, vise notamment à supporter tout langage de programmation

V.2.3. L'api snmp4j

SNMP4J est une classe d'entreprise open source libre pour la mise en œuvre de SNMP sous Java ™ SE 1.4 ou version ultérieure. SNMP4J prend en charge la génération de commande (gestionnaires), ainsi que la commande de répondre (agents). Sa conception orientée objet propre est inspirée par SNMP ++, qui est une API SNMPv1 / v2c / v3 bien

V.3. Installation de l'agent SNMP sur Windows

L'agent SNMP permet aux logiciels de supervision de collecter à distance sur vos serveurs Windows et vos postes de travail Windows, une multitude d'informations sur leur état de fonctionnement et sur leur usage mais aussi d'inventorier les composants matériels ou logiciels de vos systèmes.
Grâce à cet agent vous pouvez à tout moment connaitre, l'état de vos disques, des processeurs, l'utilisation de la mémoire ou des interfaces réseaux mais aussi la température interne, la liste des processus ou des services, des applications installés etc.

V.3.1. Etape D'installation de l'agent

Voici l'exemple sur un Windows 7, le nom des options peut changer sensiblement d'une version à l'autre de Windows. Pour installer l'agent Microsoft SNMP sur un Windows 7, vous devez ouvrir le **panneau de contrôle** et cliquez sur **Programmes** puis dans le menu sélectionnez **Activer ou désactiver des fonctionnalités Windows**

Figure17: fenêtre de panneau de configuration

Dans la liste des fonctionnalités, cochez la case *Protocole SNMP*

Figure 18 : fonctionnalité de Windows

Cochez le protocole SNMP Simple Network Management Protocol. Ceci est nécessaire pour installer l'agent SNMP et d'autres services SNMP.
Il est normalement inutile d'avoir le fournisseur SNMP WMI. Le composant fournisseur de SNMP WMI permet aux applications WMI d'accéder aux informations SNMP (Simple Network Management) à travers WMI (Windows Management Instrumentation).

V.3.2. Configuration de l'agent

La configuration du service SNMP est effectuée par le biais de l'option de propriétés de service. Pour y accéder, ouvrez le panneau de configuration et sélectionnez *Outil d'administration*

Figure 19: outils d'administration

Finalement sélectionner l'icône des Services puis la liste des services rechercher le service SNMP et double cliquez.

Figure 20 : fenêtre Service

Avertissement : Le service de Trap SNMP n'est pas utilisé pour envoyer des Traps SNMP mais seulement pour recevoir les Traps SNMP. S'il n'y a aucune application de réception du Traps sur ce système ne pas le démarrer.

La fenêtre de propriétés de service SNMP est affiché

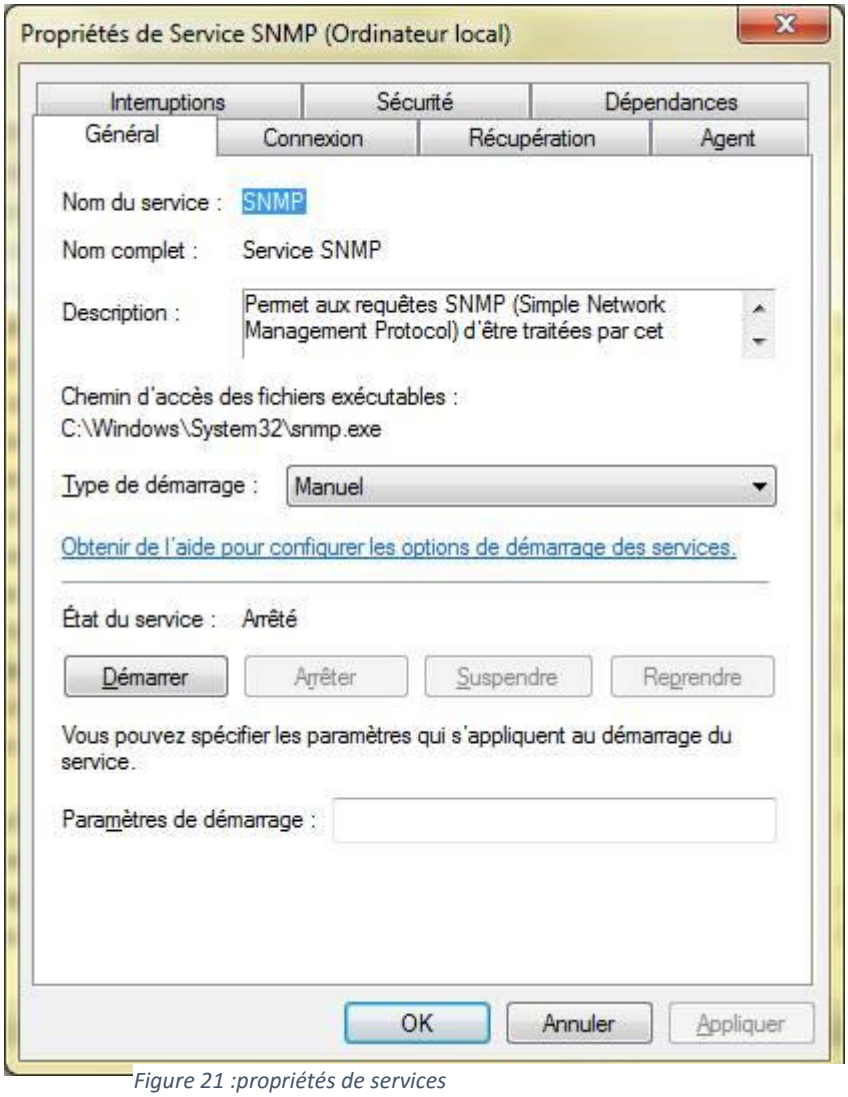

Figure 21 :propriétés de services

Vous pouvez aussi modifier le type de démarrage dans l'onglet **Récupération**.
Le processus SNMP s'exécute sous le compte système local ou un compte peut être spécifié, onglet **Connexion**.

Dans l'onglet Agent, les variables SNMP de la Mib2 system peuvent être définies

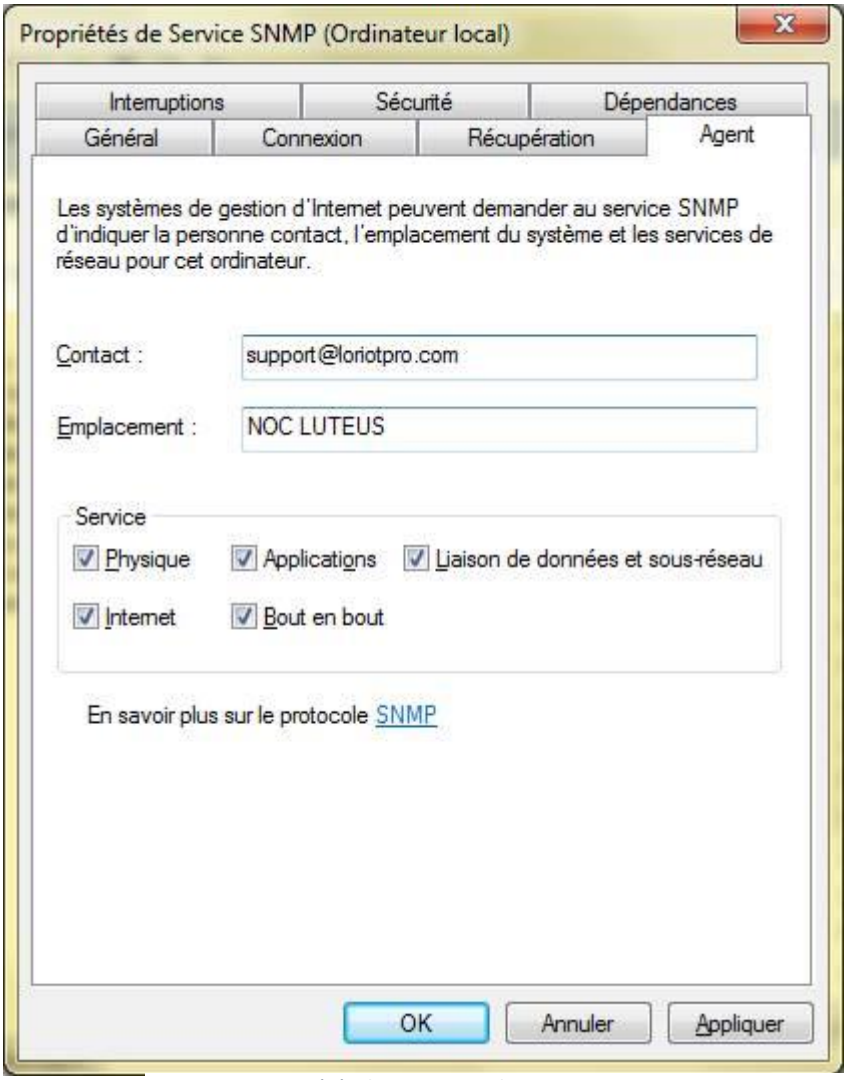

Figure 22 : propriétés de service onglet agent

Spécification des propriétés de l'équipement. Vous pouvez définir ici la valeur standard mib2 ***syscontact*** et ***syslocation***. Le *sysname* est le nom de l'hôte et ne peut pas être modifiée ici (c'est le nom de la machine Windows).
Contact : Nom et les coordonnées de l'administrateur (objet *syscontact de la mib2)*
Emplacement : Emplacement du dispositif. Ici vous pouvez entrer l'adresse, le numéro de bâtiment, étage, salle, numéro de rack. (Objet *syslocation de la mib2)*
Services : les propriétés avancées de l'agent indiquant les fonctions fournies par cet équipement : (objet sysservices de la mib2)
Physique : Cet équipement propose des services physiques au réseau, hub, répéteur Ethernet
Liaison de données et de sous-réseaux : Cet équipement propose des services de liaison, par exemple, pont, (Couche 2 du modèle OSI).

Internet : Cet équipement propose des services de transport IP (Couche 3 du modèle OSI)
End-to-end : Cet équipement propose des services de bout en bout (Protocole TCP). (Couche 4 du modèle OSI)

Applications : Cet équipement propose des services d'application, servur d'application (couche 7 du modèle OSI)
Les modifications apportées ici modifient la veleur de l'objet SNMP **sysservices**
iso(1).org (3). dod (6). internet (1). mgmt. (2). mib-2(1). system (1). sysServices(7)

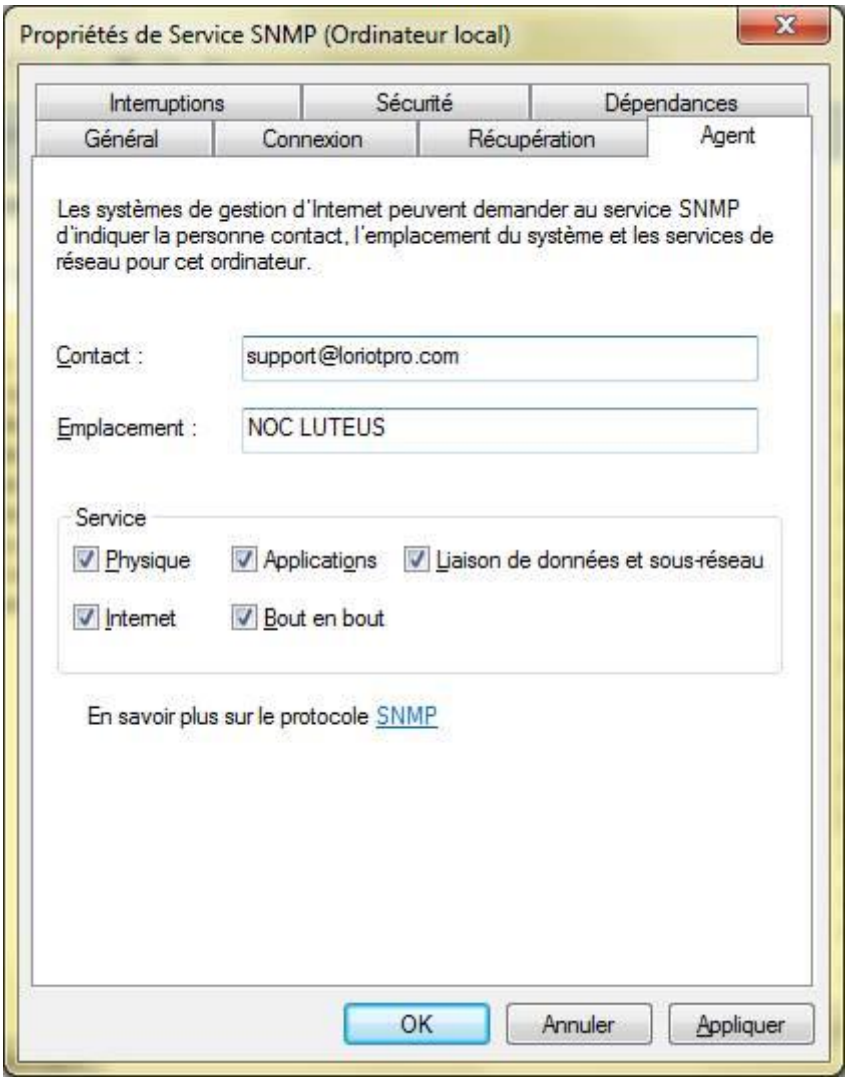

Figure 23 : propriété de services

Les options suivantes doivent être configurées pour activer la sécurité SNMP :

Nom de la communauté a accepté. Le service SNMP nécessite la configuration d'au moins un nom de communauté par défaut. Le nom **public** est généralement utilisé comme nom de la communauté parce que c'est le nom commun qui est universellement reconnu dans toutes les implémentations de SNMP. Vous pouvez supprimer ou modifier le nom de la communauté par défaut ou ajouter plusieurs noms de communauté. Si l'agent SNMP reçoit une demande d'une communauté qui n'est pas sur cette liste, il peut générer un Trap d'authentification (option ci-après). Si aucun nom de la communauté n'est défini, l'agent SNMP refuse toutes les requêtes entrantes SNMP en provenance des manager SNMP.

Autorisations. Vous pouvez sélectionner les niveaux d'autorisation qui déterminent la façon dont un agent traite les demandes SNMP de diverses communautés. Par exemple, vous pouvez configurer le niveau d'autorisation pour bloquer l'agent SNMP de traiter toute demande d'une communauté spécifique.

Accepter des paquets SNMP de n'importe quel hôte. Dans ce contexte, l'hôte de la source et la liste des hôtes acceptables consulter le système de gestion SNMP source et la liste des autres systèmes de gestion acceptable. Lorsque cette option est activée, aucuns les paquets SNMP ne sont rejetés, fondée sur le nom ou l'adresse de l'hôte source ou sur la base de la liste des hôtes acceptables. Cette option est activée par défaut.

Accepter uniquement les paquets SNMP provenant de ces hôtes. Cette option offre une sécurité limitée. Lorsque l'option est activée, seuls les paquets SNMP a reçu des hôtes sur une liste d'hôtes acceptables sont acceptés. L'agent SNMP rejette les messages des autres hôtes et envoie un piège d'authentification.

Envoyer des interruptions d'authentification. Lorsqu'un agent SNMP reçoit une demande qui ne contient pas un nom valide de communauté ou l'hôte qui envoie le message n'est pas sur la liste des hôtes accepter, l'agent peut envoyer un message Trap d’erreur d’authentification à un ou plusieurs destinations du Trap manager SNMP.

V.4. Présentation de l'interface de l'application

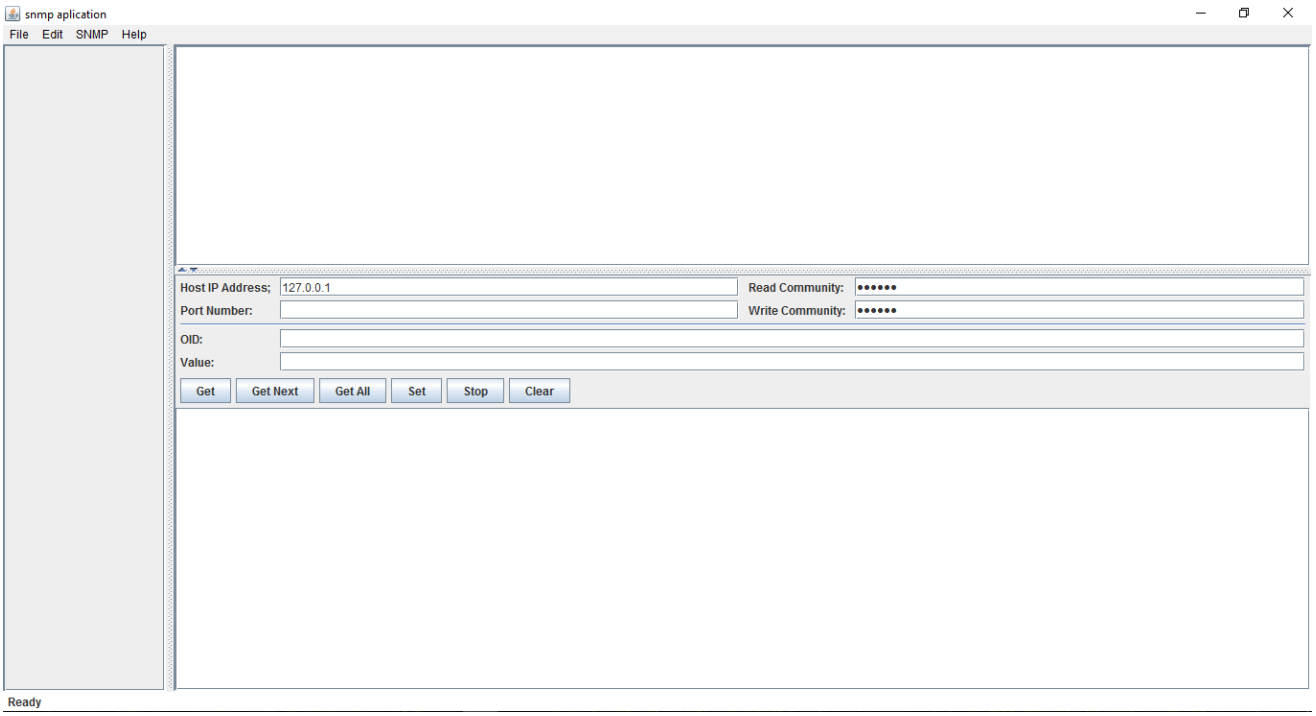

Figure 24 : interface de l'application

V.5. Conclusion

Dans ce chapitre, nous avons présenté les différents éléments d'utiliser pour le développement de l'application, ainsi que les étapes a suive pour installer un agent SNMP sur Windows, et pour finir un petit aperçu sur l'application développer.

Conclusion générale

Ainsi Vient de s'achever un travail qui a été bénéfique, du fait qu'il constitue mon premier contact avec le monde pratique.

Cette étude effectuée au sein de Sonatrach plus précisément au centre Informatique, m'a permis d'évaluer mes connaissances théoriques acquises durant notre formation et grâce à la contribution du personnel de l'organisme d'accueil j'ai pu réaliser une application de gestion de réseaux baser sur le protocole SNMP.

Développer une application de gestion de réseaux demande beaucoup de connaissance concernant la méthode de conception à suivre. Dans ce cas j'ai opté pour la méthode UP en présentons les fonctionnalités de l'application modélisés avec le langage UML.

Durant la réalisation de ce projet j'ai essayé de couvrir le maximum des besoins, ainsi qu'augmenter l'efficacité des fonctionnalités de l'application, tout cela pour faciliter la tâche aux l'administrateur réseaux.

Il n'est pas de ma présentation de dire que mon travail répond exhaustivement à tous les problèmes posés. En effet, ce travail étant une œuvre humaine, n'est pas un modèle unique et parfait, c'est pourquoi je reste ouverte à toutes les critiques et je suis prêts à recevoir toutes les suggestions et remarques tendant à améliorer d'avantage cette étude. Etant donné que tout travail informatique a été toujours l'œuvre d'une équipe.

Enfin, j'espérons que ce travail sera bénéfique pour les étudiants qui feront référence à ce mémoire.

[1] : http://www.sti.ac-versailles.fr/IMG/pdf/reseau.pdf

[2] : NGUYEN Manh Tuong, Rapport Travail d'Intérêt Personnel Encadré : Les protocoles pour la gestion des réseaux Informatiques, Hanoi, Juillet 2005.

[3] : Nazim Agoulmine et Omar Cherkaoui ,Pratique de le gestion de réseau, Groupe Eyrolles, 2003.

[4] : http://www.frameip.com/snmp/

[5] : http://christophe.cassar.free.fr/SNMP/introduction.html

[6] : http://www.linux-france.org/article/gvallee/snmp/snmp.html#ref1

[7] : https://technet.microsoft.com/en-us/library/cc977629.aspx

[8] : http://www.loriotpro.com/Products/On-line_Documentation_V5/LoriotProDoc_FR/C3-

[9] : http://www.bgbm.org/TDWG/acc/Documents/asn1gloss.htm

[10] : http://docs.oracle.com/cd/E13203_01/tuxedo/tux90/snmpmref/1tmib.htm#1030143s

Résumé :

De nos jours, les entreprises essaient de bénéficier des avantages qu'offre les réseaux informatiques en domaine de communication et échange de donnée.

Le travail réalisé dans ce mémoire consiste à la conception et réalisation d'une application de gestion de réseaux baser sur le protocole SNMP, Dans la phase de conception nous avons utilisé le processus UP qui utilise les diagrammes du langage de modélisation UML dans chaque une de ces étapes.

Nous avons terminé avec une réalisation, ou nous avons utilisé un ensemble d'outils : le langage java et l'api snmp4j tout ça sous environnement éclipse.