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

Université Saad Dahlab, Blida
USDB.

Faculté des sciences.
Département informatique .

Mémoire pour l'obtention
d'un diplôme d'ingénieur d'état en informatique.
Option : IA

Sujet :

Evolution d'une plate-forme d'administration par SNMP

Présenté par : ZATOUT Mhamed
ARRACHE Abderezak

Promotrice : M^elle^ SOUAMI Feryel
Encadreur : AKKA Abdelhakim

Organisme d'accueil : LA CNAS.

- promotion 2006-

Dédicaces

Je dédie ce modeste travail à :

Mes très chers parents qui veillent sans cesse sur moi avec leurs prières et leurs recommandations

Mes très chers frères et sœurs

Toute ma famille

Mon binôme Abderezak et toute sa famille

Mes amis : Mourad, Adel, Raouf, Yahia, Ridha.

A tous ceux qui sont proches de mon cœur et que je n'ai pas cité les noms

Mohamed

Dédicaces

Je dédie ce modeste travail à :

Mes très chers parents qui veillent sans cesse sur moi avec leurs prières et leurs recommandations Mes très chers frères et sœurs

Toute ma famille

Mon binôme Med et toute sa famille

Mes amis : Yoness,Omar,Mohamed, Hamza, Brahim .

A tous ceux qui sont proches de mon cœur et que je n'ai pas cité les noms

Abderezak

Remerciements

Tout d'abord, nous remercions le bon DIEU de nous avoir donner le courage et la volonté de mener à bien notre projet de fin d'étude.

Nos remerciements s'adressent à notre promotrice M^elle Souami Feryel de nous avoir conseillé et dirigé durant notre travail.

Nous remercions vivement M^er Akka Abdelhakime, notre encadreur de nous avoir proposé ce sujet et pour son aide précieuse, sa patience et sa disponibilité.

Enfin, l'expression de nos profondes reconnaissances pour tous ceux qui nous ont aidé à réaliser ce projet.

Sommaire

INTRODUCTION GENERALE:

L'importance croissante des réseaux (LAN & WAN) pour les entreprises, ainsi que la diversité des équipements utilisés entraînent une augmentation de la complexité de leurs gestions. En effet, le nombre important et croissant des machines et d'utilisateurs nécessite une administration de plus en plus difficile à mettre en place.

La gestion des réseaux peut être comparée à la gestion d'une entreprise. Si un service d'une entreprise, qu'il soit de petite ou de grande importance, ne fonctionne pas à sa pleine capacité ou ne fonctionne plus, il peut désorganiser l'ensemble de l'entreprise et créer de lourdes pertes. Il en est de même pour un réseau composé d'éléments divers et complexes. L'informatique ayant une importance de plus en plus grande pour le traitement des données, les entreprises ne peuvent plus se permettre d'ignorer la gestion de leurs réseaux.

La gestion des réseaux est un facteur déterminant du bon fonctionnement du parc informatique d'une entreprise. Le nombre d'éléments qui composent le réseau et leurs éloignements potentiels peuvent rendre l'administration très difficile à assurer. En effet, pour gérer un réseau, il faut tenir compte de plusieurs paramètres, comme la gestion des performances, des pannes, etc.... Pour réaliser ces différentes tâches, plusieurs protocoles ont été implémentés. On peut distinguer les protocoles SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) et CMIP/CMIS (**C**ommon **M**anagement **I**nformation **P**rotocol/**S**ervices).

Dans ce présent mémoire nous allons présenter notre travail, qui consiste à faire la conception et la réalisation d'un superviseur réseau qui assure une des fonctions de la gestion des réseaux, la surveillance de l'état du réseau et la gestion des anomalies.

Un superviseur est un outil de gestion très utilisé dans les entreprises. Il permet aux administrateurs de contrôler l'état de leurs réseaux et de détecter et localiser rapidement les anomalies, il offre aux administrateurs une présentation de leurs réseaux sous forme d'une cartographie, il permet également de déterminer les éléments responsables des problèmes.

Il existe différents outils proposés par des sociétés commerciales, comme Tivoli de IBM, Open view de HP, Unicentre TNG Computer Associates, open Master de Bull,

Et ciscoWorks de cisco.

Dans notre travail, nous sommes limités à travailler sur des réseaux locaux Ethernet TCP/IP, qui sont aujourd'hui les réseaux les plus répandus dans les entreprises. Le protocole de gestion que nous allons présenter dans ce mémoire et l'utiliser dans la réalisation du superviseur, est le protocole **SNMP** (**S**imple **N**etwork **M**anagement **P**rotocol).

Ce mémoire se subdivise en deux parties; La première est consacrée à la présentation théorique. On commence par une description des différents aspects de la gestion des réseaux en général, puis on spécifie la gestion des réseaux via le protocole SNMP. Dans cette dernière phase, nous présentons un briefe historique sur le protocole, l'architecture de gestion utilisée, les différents éléments manipulés par le protocole de gestion et spécialement la base d'information de gestion MIB (**M**anagement **I**nformation **B**ase). A la fin de cette phase nous détaillons le protocole SNMP proprement dit avec ses différentes versions et nous terminons par une conclusion.

La deuxième partie de ce mémoire comprend trois chapitres. Le premier concerne la conception du superviseur, dans laquelle on présente l'architecture logicielle et matérielle du superviseur, puis la conception en utilisant le langage UML (**U**nified **M**odeling **L**anguage). Le second chapitre traite la réalisation du superviseur, dans lequel on aborde l'environnement matériel et logiciel de développement et les différents algorithmes utilisés. Quant à la présentation de l'interface du superviseur, ainsi que les résultats obtenus lors des tests du superviseur sur le réseau de la CNAS sont illustrés dans le dernier chapitre.

– D'entreprendre des actions de prévention, d'éducation et d'informations sanitaires.

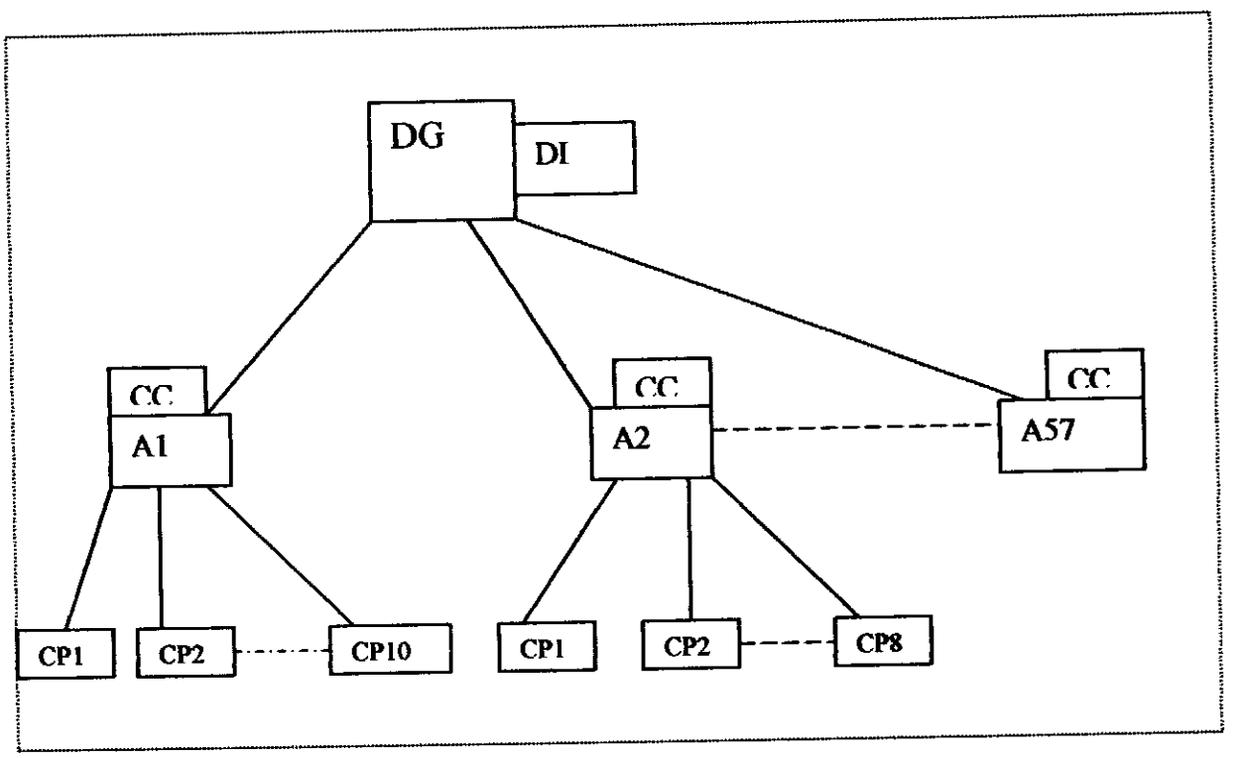
– De faire procéder à l'immatriculation des assurés sociaux, et aux employeurs.

– D'assurer en ce qui concerne l'information des bénéficiaires et des employeurs.

– De rembourser les dépenses occasionnées par le fonctionnement de diverses commissions et juridictions.

4- Les structures de la CNAS :

La C NA S est définie comme suit :



DG : direction générale
DI : direction informatique
CC : centre de calcul
A : agence
CP: centre payeur

4.1. Direction générale :

Elle se suite ben aknoun , son rôle est de gérer toutes les informations provenant des directions centrales a travers les wilaya d'Alger.

La direction générale est représentée par des agences locales au qu'elles sont rattachées plusieurs structures (centre payeur et antenne).

4.2. Direction informatique :

Il se trouve une seul direction informatique qui est rattachée a la direction générale comme il a montré **l'organigramme 1** son rôle est d'établir les différents programmes utilise dans les structures de la CNAS ainsi que la maintenance.

4.3. Centre paveur :

C'est la o u les assure se dirige pour le remboursement voir **organigramme1**

4.4. Agence :

4.4.1. Définition :

Son rôle est de coordonner et de contrôler les activités des centres payeurs et des antennes d'entreprise cl le cas échéant antennes d'administration, on trouve dans chaque wilaya une agence en exception la wilaya d'Alger.Les agences sont subdivisées en plusieurs comme le montre **l'organigramme 2** sous direction dont les plus important sont :

- **SOUS DIRECTION DE PRESTATION :**

Elle contient 3 services :

- ✓ service de rentes.
- ✓ service des allocations familiales.
- ✓ Service des assu'ées.

- **SOUS DIRECTION DE RECOUVREMENT :**

File contient 3 services :

- ✓ service immatriculation employeur.
- ✓ service immatriculation assurée.
- ✓ service cotisation.

4.4.2. Les types d'agence :

Les agences de wilaya sont classées en trois catégories:

1ère catégorie:

Agences gérant au moins **200.000 assurés sociaux,** elle comprend cinq sous structures chargées, respectivement:

- Des prestations, dont les tâches sont réparties entre deux à quatre responsables de gestion.

- De recouvrement et du contentieux, dont les tâches sont réparties entre trois responsables de gestion.
- Des opérations financières, dont les tâches sont réparties entre deux responsables de gestion.
- De l'administration des moyens et des réalisations"à caractère sanitaire et social, dont les tâches sont réparties entre deux ou trois responsables de gestion.
- Du contrôle médical dirigé par un médecin.

2ème catégorie:

Agences gérant **moins de 200.000 et au moins 100.000 assurés sociaux,** elle comprend quatre sous structures chargées, respectivement:

- des prestations dont les lâches sont réparties entre deux ou trois responsables de gestion.
- des opérations financières du recouvrement et du contentieux dont les tâches dont réparties entre trois ou quatre responsables de gestion.
- de l'administration des moyens et des réalisations à caractère sanitaire et social, dont les tâches sont réparties entre deux responsables de gestion'.
- du contrôle médical dirigé par un médecin

3ème catégorie:

Agence gérant **moins de** 100.000 **assurés sociaux,** elle comprend quatre sous structures chargées, respectivement:

- des prestations.
- des opérations financières, du recouvrement et du contentieux.
- de l'administration des moyens et des réalisations à caractère sanitaire et social.
- du contrôle médical dirigé par un médecin.

4.5. Centre de calcul :

Il est chargé de l'exploitation et la saisie des données ainsi l'édition de:

- L'immatriculation
- Allocation familiale.
- Comptabilité ...etc.

Le centre de calcul fait partie de l'agence et chaque agence à un centre de calcul sauf les wilayas dont le taux de population est très petite, leur travail se fait par d'autres centres de calcul.

EXEMPLE :

– Agence de ANNABA : centre de calcul de ANNABA.

– Agence de TAREF : centre de calcul de ANNABA.

5-Intrannet de la CNAS ; L'intranet de la CNAS est composé de:

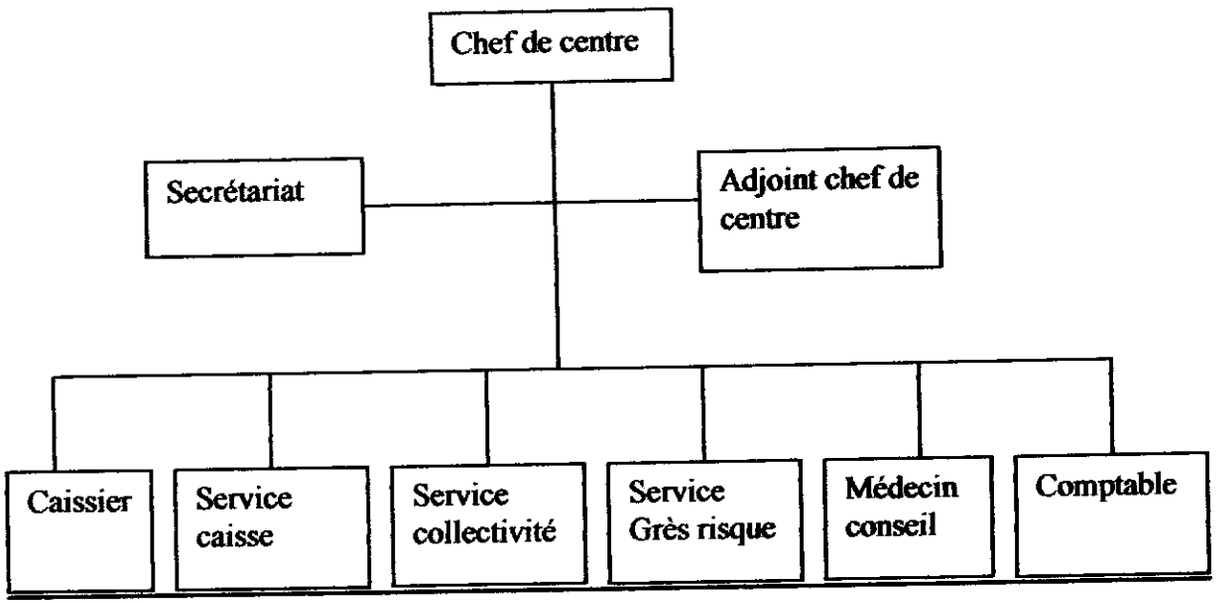
- Deux serveurs Web.
- Un serveur FTP.
- Un serveur de messagerie (Mail) /DNS.
- Un serveur de routage et accès distant /DHCP.
- Deux serveurs Proxy pour la navigation Internet.

Le tableau sut vaut détail les spécifications technique de chaque serveur :

Serveur :	*Spécification Matérielle :*	*Spécification logicielle :*
WWW	Serveur P3	• Windows NT 4.0 scrver. • Serveur web RESIN 2.0 +java 2.0+MySql
Web CNAS	IBM p3	• Windows 2000 serveur • Serveur web Apache+MySql
Routage +HDCP Acc2s distant	Siemens P3	• Windows NT 4.0 serveur
Mail +DNS	Siemens P3	• Linux Mandrak Coporate Edition 1.0 • Send Mail
FTP	Siemens P3	• Linux Mandrak Coporate Edition 1.0 • WU-FTP
Serveur Proxy	Unisys AQUANTA Siemens P3	• Windows NT 4.0 serveur • Proxy 2.0

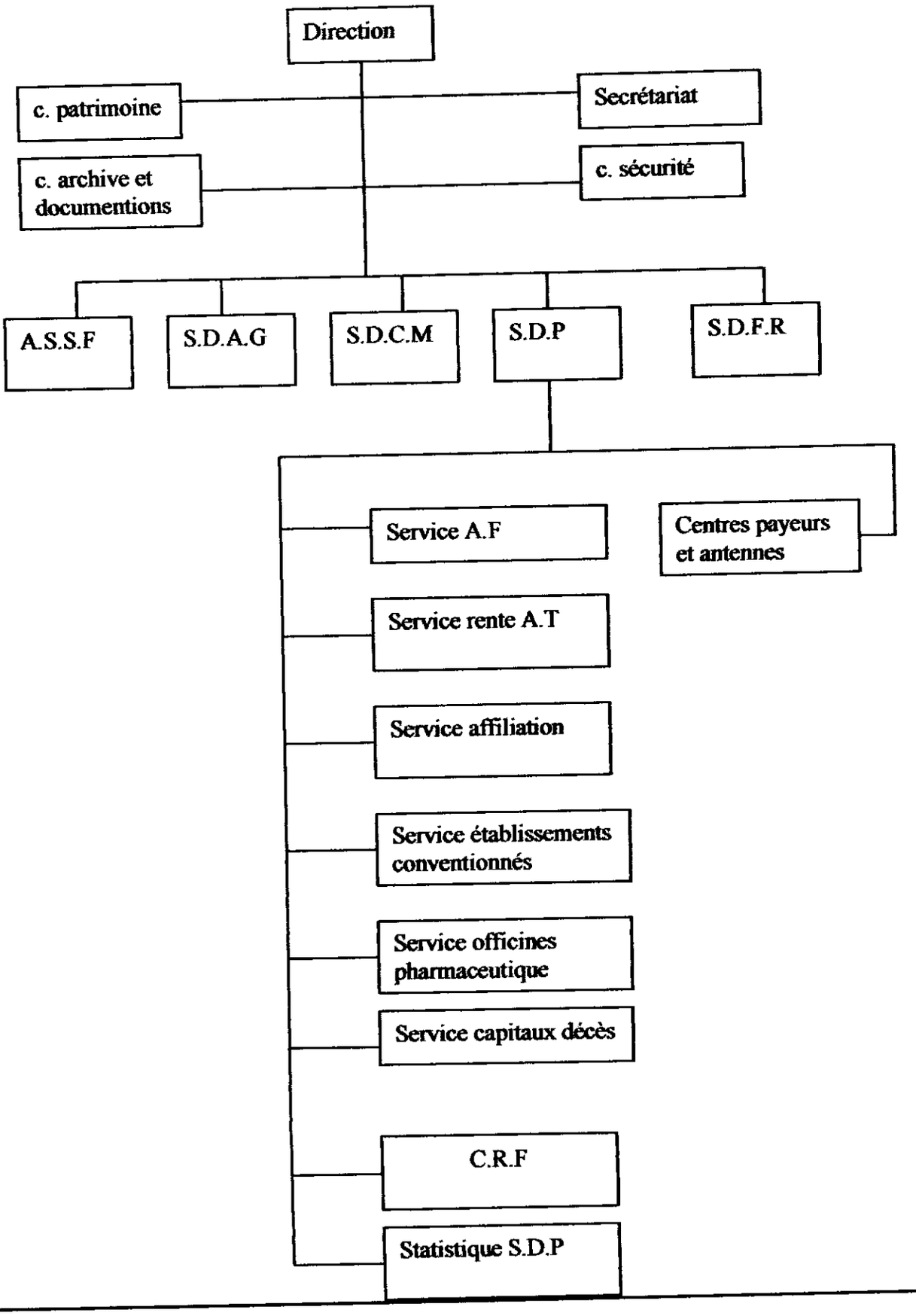
L'intranet de la CNAS est relié à Internet par une ligne spécialisée (128ko).

Organigramme1 au niveau centre payeur et antenne :



Organigramme 2 de l'agence 1er catégorie:

ABREVIATION	Désignation
C	Cellule
A.S.S.F	Actions sanitaires Sociales et Familiales
S.D.A.G	Sous Direction d'Administration Générale
S.D.C.M	Sous Direction de Contrôle Médicale
S.D.P	Sous Direction des Prestations
S.D.F.R	Sous Direction des Finances et de Recouvrement
A.F	Allocation Familiales
A.T	Accidente de Travail
C.R.P	Commission de Recours préalables


Direction
c. patrimoine
Secrétariat
c. archive et documentions
c. sécurité
A.S.S.F
S.D.A.G
S.D.C.M
S.D.P
S.D.F.R
Service A.F
Centres payeurs et antennes
Service rente A.T
Service affiliation
Service établissements conventionnés
Service officines pharmaceutique
Service capitaux décès
C.R.F
Statistique S.D.P

6-Adressage CNAS:

6-1-Introduction:

La CNAS a décidé d'utiliser un format d'adressage significatif assurant sa sécurité. Ainsi à partir de l'adresse, on peut retrouver plusieurs informations, comme le code Wilaya ainsi que d'autre informations détaillées dans les paragraphes suivants.

6-2-structure (format) :

00001010.000 **WWWWW.*WSSSSSSS. PPPPPPPP***

6-3-sinification de chaque champ :

6-3-1-Le champ"000":

Cet trois bits sont réservés pour désigner es différents organismes de la Sécurité sociale.

Et pour que notre formule reste utile dans le cas où les diffirents réseaux privés des organismes seront fusionnée, réservé ce champ.

La codification des organismes est la suivant :

Code	Valeur en décimale	**Organisme**
001	1	CNAS
010	2	CNAC
011		CASNOS
100	4	CNR
101	5	CACOBATBH
110	6	MTSS
111 000	7 0	Réservée pour utilisation ultérieure

6-3-2-Le champ "WWWWWW":

Il est réservé pour le code Wilaya dont les valeurs varient de 1 à 62. utilisé la codification actuelle comme 1 pour la wilaya **Adrar et 16 pour la** wilaya d'Alger.

Cependant pour la wilaya d'Alger qui constitue une exception, on a rajouté des Wilaya pour désigner les grandes structures de la CNAS.

Code	Nom
56	Direction informatique
57	Gens de mer
58	Capas
59	Direction Générale
60	Mohamed V
61	Touileb

6-3-3-Le champ "SSSSSS":

Il est sur 7 bits ces valeurs varient de, 0 à 127 **et on les a réservés pour** désigner les différentes structures de chaque wilaya comme le montre le tableau suivent

Code	Désignation
1	Agence
2	Centre de calcul
3 à 70	CP 1 au CP67
71 à 90	Antenne1 à antenne2O
91 à 127	Autres structures

6-3-4-Le champ " P P P P P P P P " :

Il désigne les postes du réseau ; les valeurs varieront de 1 à 254. On a éliminé la valeur (adresse réseau) et la valeur 255(adresse de diffusion).

6-3-4-Le champ *"00001010"* :

C'est un champ réservé aux réseaux privés de classe A par l'internic

6-4-le masque associé :

Représentation binaire:

11111111.11111111. 11111111. 00000000

Représentation décimale:

255.255.255.0

7-CONCLUSION:

Dans ce chapitre nous avons présenté l'organisme d'accueil et ses missions ainsi que les poste de travail qui nous concernent afin de faciliter la recherche de l'information.

CHAPITRE I
LA GESTION DES RESEAUX

I-1-Introduction:

La gestion des réseaux se définit comme l'ensemble des activités liées au contrôle, à la coordination et à la surveillance des ressources qui participent à l'établissement de communications. Gérer un réseau revient à observer son activité tel que la collecte des statistiques sur le débit réel ou le calcul des taux d'erreurs, à contrôler les opérations en cours (Contrôle des accès, statut des connexions) et à agir sur l'ensemble de ses ressources de communication (Activer, initialiser une station ou un routeur). [Cha 99]

Différents protocoles permettent la remontée d'information des équipements vers le manager. Cela permet d'identifier les éléments raccordés au réseau et de connaître leur état. Une bonne gestion doit réaliser les objectifs suivants :

- Offrir aux utilisateurs un service de qualité.
- Permettre l'évolution du système en incluant de nouvelles fonctionnalités.
- Optimiser les performances des services pour les utilisateurs.
- Permettre une utilisation maximale des ressources pour un coût minimal.

Pour répondre au mieux à ces besoins, l'administrateur du réseau doit disposer de trois types d'actions pour suivre l'état du réseau et pouvoir réagir :

- Des actions en temps réel pour connaître l'état de fonctionnement de son réseau (surveillance et diagnostic des incidents, mesure de la charge réelle, maintenance, contrôle, informations aux utilisateurs... etc.) et agir sur celui-ci (réparation, ajout/retrait de nouveaux abonnés) ainsi que d'en assurer la sécurité (contrôler les accès, donner/retirer des droits d'accès... etc.).
- Des actions différées pour planifier, optimiser, quantifier et gérer les évolutions du réseau (statistiques, comptabilité, facturation, prévention, évaluation de charges... etc.)
- Des actions prévisionnelles qui lui permettent d'avoir une vision à moyen et long terme, d'évaluer des solutions alternatives, de choisir les nouvelles générations de produit, de vérifier la pertinence de la solution réseau pour un problème donné. [Cha 99]

I-2.Les deux facettes de l'administration :

L'administration des réseaux et des systèmes est bâtie à partir de briques du marché : les administrateurs techniques, les agents inclus dans les équipements, les produits de gestion administrative. L'ensemble de ces éléments compose deux domaines complémentaires :

- La gestion administrative : liée à l'organisation de l'entreprise.
- La gestion technique : relative au fonctionnement du réseau.

I-3.Les besoins fonctionnels de la gestion des réseaux :

Les besoins fonctionnels sont regroupés autour de 5 grandes fonctionnalités : la gestion de la configuration, des performances, des anomalies, des informations comptables et de la sécurité.

I-3-1-La gestion de la configuration :

Rendre un réseau opérationnel, c'est tout d'abord le configurer. Il s'agit de donner une description formelle et non ambiguë de tous les éléments constitutifs, de son architecture et de son mode de fonctionnement (notion de paramétrage du réseau). On obtient une image du réseau, en considérant chacun de ses composants physiques (éléments du réseau) et logiques (protocoles de communication), comme un objet élémentaire. Un objet peut être caractérisé par un type, des attributs, un état, des relations entre objets. La description successive de toutes les ressources du réseau autorise une vue des nœuds, des voies logiques et physiques de celui-ci, c'est à dire de sa topologie. Cette carte du réseau est en réalité obtenue en utilisant des langages de configuration propres à chaque architecture de réseau.

Le réseau prend alors connaissance de son architecture, de l'implantation de chaque entité, de leur localisation et des moyens d'y accéder. La cohérence de la configuration du réseau est vérifiée, lors de la phase de génération. Les phases de configuration et de génération constituent l'initialisation du réseau après lesquelles il devient opérationnel et capable de répondre à une demande de service réseau. Un réseau peut voir son architecture évoluer au cours de son utilisation (ajout, suppression, modification logique et/ou matérielle), nécessitant une reconfiguration. Cette phase doit pouvoir se faire en dynamique, sans entraîner un arrêt, même partiel, du service du réseau. [Cha 99]

I-3-2-La gestion des performances :

Les réseaux de communication sont généralement soumis à un trafic aléatoire résultant de l'utilisation imprévisible des ressources mises à la disposition des utilisateurs. Ceci a pour conséquence de rendre variable la qualité de service qu'ils ressentent. L'évaluation des performances des réseaux a pour objectifs :

- De prévoir et de quantifier la qualité de service.
- D'identifier et de paramétrer les outils du réseau nécessaires pour satisfaire la qualité de service.

Les évaluations de performances s'effectuent lors des différentes phases de La vie du réseau : à sa conception (dimensionnement du réseau), lors de Changements d'équipement (prise en compte des expériences passées), durant Le suivi du réseau (vérification et analyse fine des temps de réponse, de traversée, évaluation du débit efficace et maximum, test et contrôle du comportement du réseau, réglage des paramètres du système).

On dispose d'indicateurs de qualité de service définis pour ces réseaux portant sur leur temps de traversée, leur débit efficace, le taux de perte d'informations, le taux de refus d'établissement de communication, le temps de réponse (délai de transmission), le taux d'utilisation, le taux de pannes. En effet, lorsqu'un paquet arrive à un équipement, il est utilisé immédiatement si l'équipement est libre, sinon il est mis en file d'attente. Ainsi, les ressources du réseau ne sont pas réservées pour la durée d'une communication mais partagées entre les différents flux traversant un équipement. Le temps de traversée d'un paquet dépend alors du trafic qu'il rencontre le long de son chemin dans le réseau. Le débit efficace est le flux maximum d'informations des utilisateurs que le réseau peut effectivement acheminer. Afin d'obtenir un meilleur rendement, il faut assurer le partage des ressources, la régulation des flux du trafic et l'intégrité des informations transférées. [Cha 99]

I-3-3-La gestion des anomalies :

La détection des pannes (localisation et signalisation) est indispensable pour que les mécanismes de réparation et de reconfiguration puissent se réaliser et laisser un système dans un état opérationnel. Les pannes peuvent provenir aussi bien des logiciels que du matériel. La détection des pannes peut se réaliser à partir de périphériques spécialisés ou par logiciel. L'origine d'une défaillance peut se détecter par logiciel, soit par des mécanismes de " senseur " ou de " chiens de gardes " internes ou encore par la surveillance d'une unité par une autre. Cela est réalisé par les fonctions de :

- Surveillance et de prise en compte des événements non sollicités (alarmes).
- Localisation des pannes par des tests.
- Détermination et identification des pannes par analyse ou via des systèmes experts de correction.

Des tests périodiques et systématiques autorisent la signalisation de défaillances des équipements. De plus, la plupart des équipements intègrent des mécanismes de contrôle et de surveillance divers (détection d'erreur de parité en mémoire ou sur bus). Toutes ces détections donnent lieu à des transferts d'informations à des fins de gestion aux points de contrôle du réseau dont dépendent les équipements. Les points de contrôle peuvent agir à distance sur des systèmes en déclenchant des procédures de tests; par exemple ils autorisent des actions de télémaintenance et de télésurveillance en temps réel ou en différé.

[Cha 99]

I-3-4-La gestion des informations comptables :

La gestion des informations comptables consiste à assurer toutes les fonctions relatives à la comptabilisation de l'utilisation des ressources du réseau par les utilisateurs. Elle vise en générale la facturation en fonction de la tarification ainsi que la gestion et la surveillance des quotas d'utilisation des ressources.

I-3-5-La gestion de la sécurité :

La sécurité des réseaux revient à mettre à disposition des systèmes des procédures et des outils qui assurent :

- A l'émetteur d'un message : que ce dernier parvient bien au bon destinataire et qu'il ne pourra être compromis que par celui-ci, que le destinataire ne pourra nier avoir reçu le message et prétendre avoir reçu un message non expédié.
- Au destinataire de message : l'authentification de l'émetteur, l'intégrité du message, que l'émetteur ne peut nier avoir envoyé le message et que seuls les émetteurs autorisés pourront lui envoient des messages.

La gestion des services de sécurité doit permettre le contrôle d'accès, l'authentification des correspondants, la confidentialité et l'intégrité des données. Le service d'authentification peut être rendu en mettant en œuvre des services d'annuaire électronique. Ces derniers gèrent des références d'usagers comme des attributs et délivrent des jetons d'authentification. Il s'agit d'une procédure asynchrone. L'authentification peut être simple (identification et mot de passe) ou forte en utilisant un mot de passe protégé par crypto–système à clé publique **D**ata **E**ncryption **S**tandard (DES), **D**ata **E**ncryption **A**lgorithm **1** (DEA 1). [Cha 99]

I-4. Architecture des protocoles TCP/IP :

Le modèle TCP/IP est structuré en quatre couches principales qui s'appuient sur une couche matériélle. (Voir figure I.1)

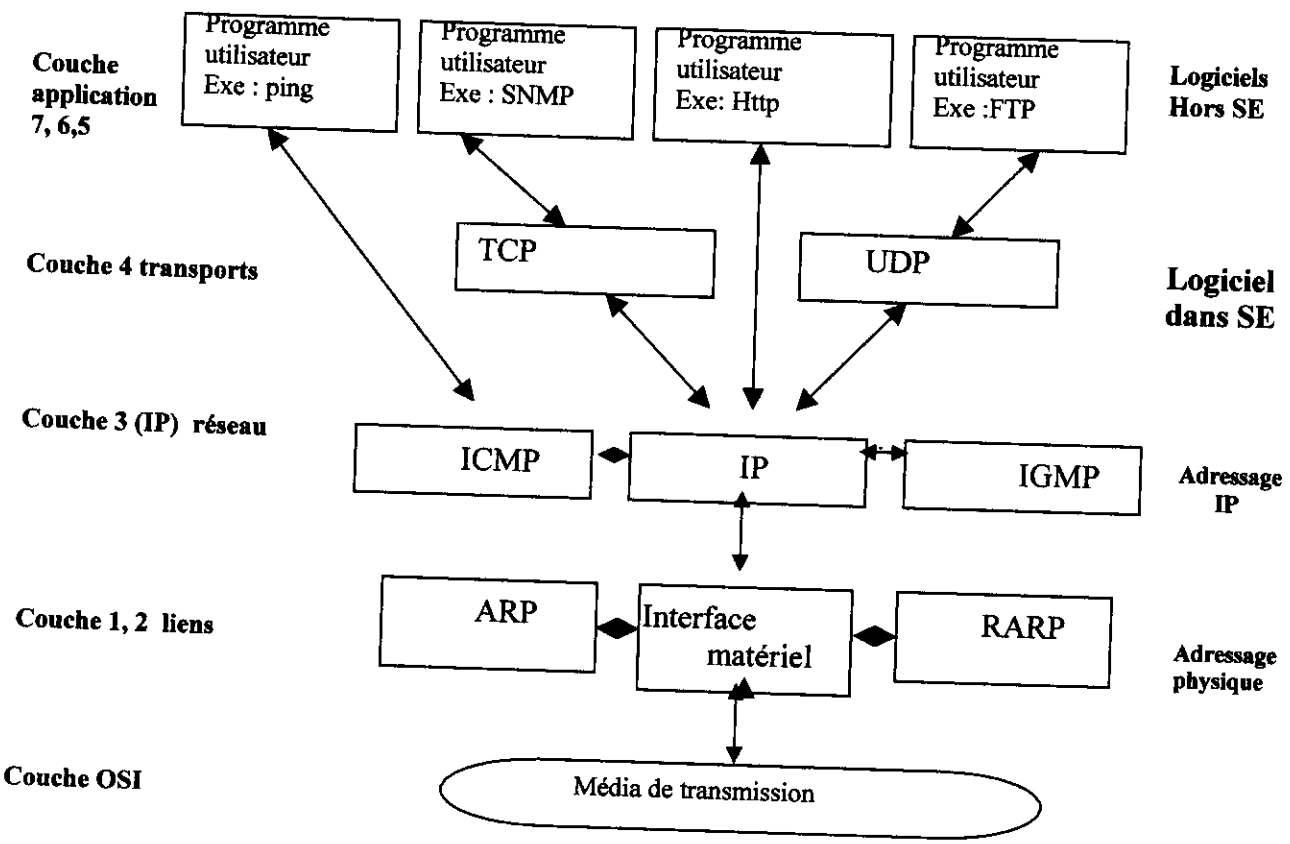
Les quatre couches sont :

- La couche liens (c o u c h e d'acces) : c'est l'interface physique avec le média de transmission. Elle est constituée d'une carte d'interface et son pilote du système d'exploitation.
- La couche réseau ou couche IP (**I**nternet **P**rotocol) : elle gére la circulation des paquets à travers le réseau en assurant leur routage, elle comprend également les protocles ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol) et IGMP (**I**nternet **G**roup **M**anagement **P**rotocol).

-la couche transport : elle assure en premier lieu la communication de bout en bout en faisant abstraction des machine intermédiaires entre l'émetteur et le

Destinataire .en second lieu, elle régule le flux de données et assure un transport fiable (données transmise sans erreurs et reçues dans l'ordre de leurs émission) dans le cas de TCP (Transmission control Protocol) ou non fiable dans le cas UDP (User Datagram Protocol). Dans le cas du protocole UDP, il n'est pas garanti qu'un datagramme arrive à bon port, c'est la couche supérieure de s'en assurer.

La figure I-1 illustre l'interaction entre les différents protocoles du modèle TCP/IP.



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

Université Saad Dahlab, Blida
USDB.

Faculté des sciences.
Département informatique .

Mémoire pour l'obtention
d'un diplôme d'ingénieur d'état en informatique.
Option : IA

Sujet :

Evolution d'une plate-forme d'administration par SNMP

Présenté par : ZATOUT Mhamed
ARRACHE Abderezak

Promotrice : M^elle^ SOUAMI Feryel
Encadreur : AKKA Abdelhakim

Organisme d'accueil : LA CNAS.

- promotion 2006-

Dédicaces

Je dédie ce modeste travail à :

Mes très chers parents qui veillent sans cesse sur moi avec leurs prières et leurs recommandations

Mes très chers frères et sœurs

Toute ma famille

Mon binôme Abderezak et toute sa famille

Mes amis : Mourad, Adel, Raouf, Yahia, Ridha.

A tous ceux qui sont proches de mon cœur et que je n'ai pas cité les noms

Mohamed

Dédicaces

Je dédie ce modeste travail à :

Mes très chers parents qui veillent sans cesse sur moi avec leurs prières et leurs recommandations Mes très chers frères et sœurs

Toute ma famille

Mon binôme Med et toute sa famille

Mes amis : Yoness, Omar, Mohamed, Hamza, Brahim .

A tous ceux qui sont proches de mon cœur et que je n'ai pas cité les noms

Abderezak

Remerciements

Tout d'abord, nous remercions le bon DIEU de nous avoir donner le courage et la volonté de mener à bien notre projet de fin d'étude.

Nos remerciements s'adressent à notre promotrice M^elle Souami Feryel de nous avoir conseillé et dirigé durant notre travail.

Nous remercions vivement M^er Akka Abdelhakime, notre encadreur de nous avoir proposé ce sujet et pour son aide précieuse, sa patience et sa disponibilité.

Enfin, l'expression de nos profondes reconnaissances pour tous ceux qui nous ont aidé à réaliser ce projet.

Sommaire

INTRODUCTION GENERALE:

L'importance croissante des réseaux (LAN & WAN) pour les entreprises, ainsi que la diversité des équipements utilisés entraînent une augmentation de la complexité de leurs gestions. En effet, le nombre important et croissant des machines et d'utilisateurs nécessite une administration de plus en plus difficile à mettre en place.

La gestion des réseaux peut être comparée à la gestion d'une entreprise. Si un service d'une entreprise, qu'il soit de petite ou de grande importance, ne fonctionne pas à sa pleine capacité ou ne fonctionne plus, il peut désorganiser l'ensemble de l'entreprise et créer de lourdes pertes. Il en est de même pour un réseau composé d'éléments divers et complexes. L'informatique ayant une importance de plus en plus grande pour le traitement des données, les entreprises ne peuvent plus se permettre d'ignorer la gestion de leurs réseaux.

La gestion des réseaux est un facteur déterminant du bon fonctionnement du parc informatique d'une entreprise. Le nombre d'éléments qui composent le réseau et leurs éloignements potentiels peuvent rendre l'administration très difficile à assurer. En effet, pour gérer un réseau, il faut tenir compte de plusieurs paramètres, comme la gestion des performances, des pannes, etc.... Pour réaliser ces différentes tâches, plusieurs protocoles ont été implémentés. On peut distinguer les protocoles SNMP (Simple Network Management Protocol) et CMIP/CMIS (Common Management Information Protocol/Services).

Dans ce présent mémoire nous allons présenter notre travail, qui consiste à faire la conception et la réalisation d'un superviseur réseau qui assure une des fonctions de la gestion des réseaux, la surveillance de l'état du réseau et la gestion des anomalies.

Un superviseur est un outil de gestion très utilisé dans les entreprises. Il permet aux administrateurs de contrôler l'état de leurs réseaux et de détecter et localiser rapidement les anomalies, il offre aux administrateurs une présentation de leurs réseaux sous forme d'une cartographie, il permet également de déterminer les éléments responsables des problèmes.

Il existe différents outils proposés par des sociétés commerciales, comme Tivoli de IBM, Open view de HP, Unicentre TNG Computer Associates, open Master de Bull,

Et ciscoWorks de cisco.

Dans notre travail, nous sommes limités à travailler sur des réseaux locaux Ethernet TCP/IP, qui sont aujourd'hui les réseaux les plus répandus dans les entreprises. Le protocole de gestion que nous allons présenter dans ce mémoire et l'utiliser dans la réalisation du superviseur, est le protocole **SNMP** (**S**imple **N**etwork **M**anagement **P**rotocol).

Ce mémoire se subdivise en deux parties; La première est consacrée à la présentation théorique. On commence par une description des différents aspects de la gestion des réseaux en général, puis on spécifie la gestion des réseaux via le protocole SNMP. Dans cette dernière phase, nous présentons un briefe historique sur le protocole, l'architecture de gestion utilisée, les différents éléments manipulés par le protocole de gestion et spécialement la base d'information de gestion MIB (**M**anagement **I**nformation **B**ase). A la fin de cette phase nous détaillons le protocole SNMP proprement dit avec ses différentes versions et nous terminons par une conclusion.

La deuxième partie de ce mémoire comprend trois chapitres. Le premier concerne la conception du superviseur, dans laquelle on présente l'architecture logicielle et matérielle du superviseur, puis la conception en utilisant le langage UML (**U**nified **M**odeling **L**anguage). Le second chapitre traite la réalisation du superviseur, dans lequel on aborde l'environnement matériel et logiciel de développement et les différents algorithmes utilisés. Quant à la présentation de l'interface du superviseur, ainsi que les résultats obtenus lors des tests du superviseur sur le réseau de la CNAS sont illustrés dans le dernier chapitre.

PRESENTATION DE L'ORGANISME D'ACCUEI

1-Introduction:

Nous présentons dans ce chapitre notre organisme d'accueil on définissant ses missions et ces différents structures avec une brève étude sur l'intranet existant.

2-Présentation de la CNAS :

La Caisse Nationale des Assurances Sociales des Travailleurs Salariés, par abréviation « C.N.A.S » est un établissement public à caractère administratif, doté de la personnalité morale et de l'autonomie financière, régis par les lois et les règlements en vigueur.

La C N A S . est placée sous la tutelle du Ministre chargé de la Sécurité Sociale, le Siège de la Caisse est fixé à Alger.

Dans chaque wilaya, la C.N.A.S dispose d'une .structure dénommée "agence de wilaya" fonctionnant comme annexe de la caisse nationale concernée.

D'autres annexes peuvent être créées, par arrêté conjoint du ministre de tutelle et du ministre chargé des finances, sous la dénomination de centre de commue, *ou* d'antenne d'entreprise ou d'administration.

3-Mission de la CNAS :

- De gérer les prestations en nature et en espèce des assurances sociales, des accidents de travail et des maladies professionnelles.

– De gérer les prestations familiales.

– D'assurer le recouvrement, le contrôle et le contentieux des recouvrements des cotisations au financement des prestations.

- De contribuer à promouvoir la politique de prévention des accidents de travail et des maladies professionnelles.

– De gérer les prestations dues aux personnes bénéficiaires des conventions et accords internationaux de sécurité sociale.

- D'entreprendre (les actions sous forme de réalisations à caractère sanitaire et social.

– D'exercer le contrôle médical des bénéficiaires.

- D'entreprendre des actions de prévention, d'éducation et d'informations sanitaires.

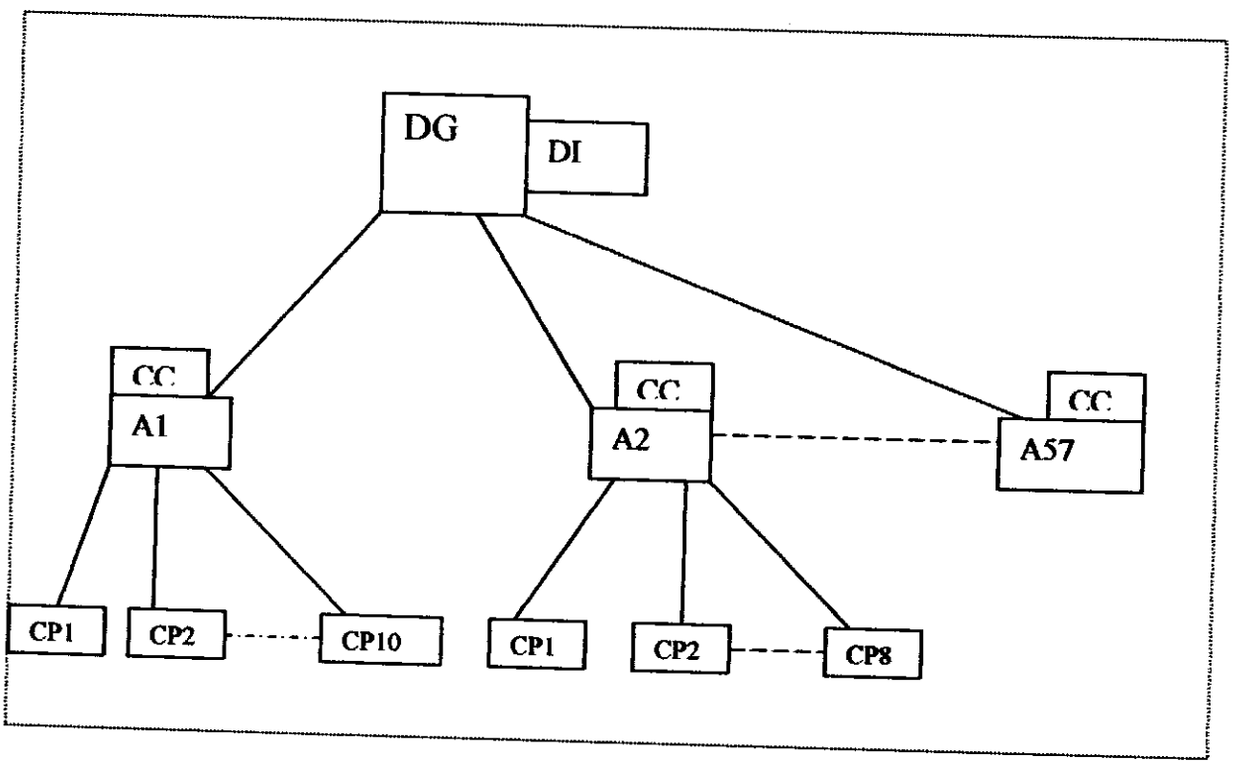
- De faire procéder à l'immatriculation des assurés sociaux, et aux employeurs.

- D'assurer en ce qui concerne l'information des bénéficiaires et des employeurs.

- De rembourser les dépenses occasionnées par le fonctionnement de diverses commissions et juridictions.

4- Les structures de la CNAS :

La C NA S est définie comme suit :



DG : direction générale
DI : direction informatique
CC : centre de calcul
A : agence
CP: centre payeur

4.1. Direction générale :

Elle se suite ben aknoun , son rôle est de gérer toutes les informations provenant des directions centrales a travers les wilaya d'Alger.

La direction générale est représentée par des agences locales au qu'elles sont rattachées plusieurs structures (centre payeur et antenne).

4.2. Direction informatique :

Il se trouve une seul direction informatique qui est rattachée a la direction générale comme il a montré **l'organigramme 1** son rôle est d'établir les différents programmes utilise dans les structures de la CNAS ainsi que la maintenance.

4.3. Centre paveur :

C'est la o u les assure se dirige pour le remboursement voir **organigramme1**

4.4. Agence :

4.4.1. Définition :

Son rôle est de coordonner et de contrôler les activités des centres payeurs et des antennes d'entreprise cl le cas échéant antennes d'administration, on trouve dans chaque wilaya une agence en exception la wilaya d'Alger.Les agences sont subdivisées en plusieurs comme le montre **l'organigramme 2** sous direction dont les plus important sont :

- **SOUS DIRECTION DE PRESTATION :**

Elle contient 3 services :

- ✓ service de rentes.
- ✓ service des allocations familiales.
- ✓ Service des assu'ées.

- **SOUS DIRECTION DE RECOUVREMENT :**

File contient 3 services :

- ✓ service immatriculation employeur.
- ✓ service immatriculation assurée.
- ✓ service cotisation.

4.4.2. Les types d'agence :

Les agences de wilaya sont classées en trois catégories:

1ère catégorie:

Agences gérant au moins **200.000 assurés sociaux,** elle comprend cinq sous structures chargées, respectivement:

- Des prestations, dont les tâches sont réparties entre deux à quatre responsables de gestion.

- De recouvrement et du contentieux, dont les tâches sont réparties entre trois responsables de gestion.
- Des opérations financières, dont les tâches sont réparties entre deux responsables de gestion.
- De l'administration des moyens et des réalisations"à caractère sanitaire et social, dont les tâches sont réparties entre deux ou trois responsables de gestion.
- Du contrôle médical dirigé par un médecin.

2ème catégorie:

Agences gérant **moins de 200.000 et au moins 100.000 assurés sociaux,** elle comprend quatre sous structures chargées, respectivement:

- des prestations dont les lâches sont réparties entre deux ou trois responsables de gestion.
- des opérations financières du recouvrement et du contentieux dont les tâches dont réparties entre trois ou quatre responsables de gestion.
- de l'administration des moyens et des réalisations à caractère sanitaire et social, dont les tâches sont réparties entre deux responsables de gestion'.
- du contrôle médical dirigé par un médecin

3ème catégorie:

Agence gérant **moins de** 100.000 **assurés sociaux,** elle comprend quatre sous structures chargées, respectivement:

- des prestations.
- des opérations financières, du recouvrement et du contentieux.
- de l'administration des moyens et des réalisations à caractère sanitaire et social.
- du contrôle médical dirigé par un médecin.

4.5. Centre de calcul :

Il est chargé de l'exploitation et la saisie des données ainsi l'édition de:

- L'immatriculation
- Allocation familiale.
- Comptabilité ...etc.

Le centre de calcul fait partie de l'agence et chaque agence à un centre de calcul sauf les wilayas dont le taux de population est très petite, leur travail se fait par d'autres centres de calcul.

EXEMPLE :

- Agence de ANNABA : centre de calcul de ANNABA.
- Agence de TAREF : centre de calcul de ANNABA.

5-Intrannet de la CNAS ; L'intranet de la CNAS est composé de:

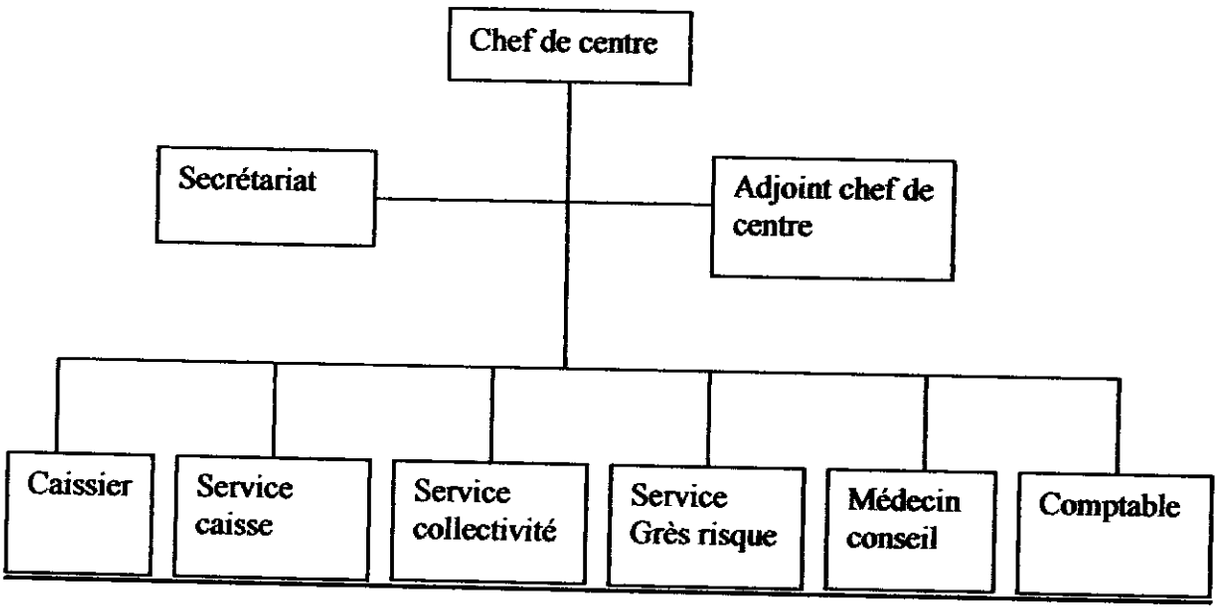
- Deux serveurs Web.
- Un serveur FTP.
- Un serveur de messagerie (Mail) /DNS.
- Un serveur de routage et accès distant /DHCP.
- Deux serveurs Proxy pour la navigation Internet.

Le tableau sut vaut détail les spécifications technique de chaque serveur :

Serveur :	*Spécification Matérielle :*	*Spécification logicielle :*
WWW	Serveur P3	• Windows NT 4.0 scrver. • Serveur web RESIN 2.0 +java 2.0+MySql
Web CNAS	IBM p3	• Windows 2000 serveur • Serveur web Apache+MySql
Routage +HDCP Acc2s distant	Siemens P3	• Windows NT 4.0 serveur
Mail +DNS	Siemens P3	• Linux Mandrak Coporate Edition 1.0 • Send Mail
FTP	Siemens P3	• Linux Mandrak Coporate Edition 1.0 • WU-FTP
Serveur Proxy	Unisys AQUANTA Siemens P3	• Windows NT 4.0 serveur • Proxy 2.0

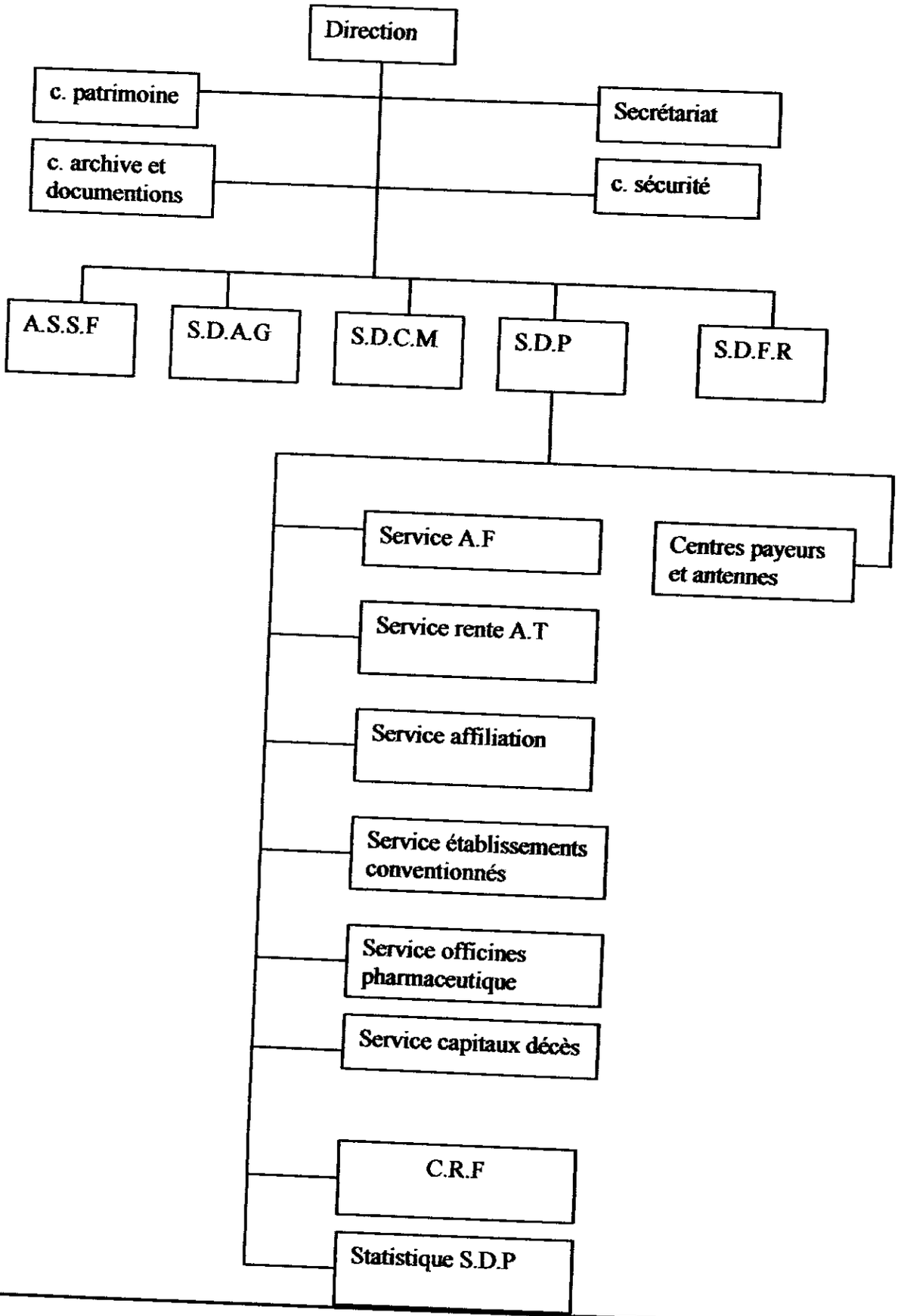
L'intranet de la CNAS est relié à Internet par une ligne spécialisée (128ko).

Organigramme1 au niveau centre payeur et antenne :



Organigramme 2 de l'agence 1er catégorie:

ABREVIATION	Désignation
C	Cellule
A.S.S.F	Actions sanitaires Sociales et Familiales
S.D.A.G	Sous Direction d'Administration Générale
S.D.C.M	Sous Direction de Contrôle Médicale
S.D.P	Sous Direction des Prestations
S.D.F.R	Sous Direction des Finances et de Recouvrement
A.F	Allocation Familiales
A.T	Accidente de Travail
C.R.P	Commission de Recours préalables


Direction
c. patrimoine
Secrétariat
c. archive et documentions
c. sécurité
A.S.S.F
S.D.A.G
S.D.C.M
S.D.P
S.D.F.R
Service A.F
Centres payeurs et antennes
Service rente A.T
Service affiliation
Service établissements conventionnés
Service officines pharmaceutique
Service capitaux décès
C.R.F
Statistique S.D.P

6-Adressage CNAS:

6-1-Introduction:

La CNAS a décidé d'utiliser un format d'adressage significatif assurant sa sécurité. Ainsi à partir de l'adresse, on peut retrouver plusieurs informations, comme le code Wilaya ainsi que d'autre informations détaillées dans les paragraphes suivants.

6-2-structure (format) :

00001010.000 **WWWWW.*WSSSSSSS.* *PPPPPPP***

6-3-sinification de chaque champ :

6-3-1-Le champ"000":

Cet trois bits sont réservés pour désigner es différents organismes de la Sécurité sociale.

Et pour que notre formule reste utile dans le cas où les diffirents réseaux privés des organismes seront fusionnée, réservé ce champ.

La codification des organismes est la suivant :

Code	Valeur en décimale	**Organisme**
001	1	CNAS
010	2	CNAC
011		CASNOS
100	4	CNR
101	5	CACOBATBH
110	6	MTSS
111 000	7 0	Réservée pour utilisation ultérieure

6-3-2-Le champ "WWWWWW":

Il est réservé pour le code Wilaya dont les valeurs varient de 1 à 62. utilisé la codification actuelle comme 1 pour la wilaya **Adrar et 16 pour la** wilaya d'Alger.

Cependant pour la wilaya d'Alger qui constitue une exception, on a rajouté des Wilaya pour désigner les grandes structures de la CNAS.

Code	Nom
56	Direction informatique
57	Gens de mer
58	Capas
59	Direction Générale
60	Mohamed V
61	Touileb

6-3-3-Le champ "SSSSSS":

Il est sur 7 bits ces valeurs varient de, 0 à 127 **et on les a réservés pour** désigner les différentes structures de chaque wilaya comme le montre le tableau suivent

Code	Désignation
1	Agence
2	Centre de calcul
3 à 70	CP 1 au CP67
71 à 90	Antennel à antenne2O
91 à 127	Autres structures

6-3-4-Le champ "PPPPPPPP" :

Il désigne les postes du réseau ; les valeurs varieront de 1 à 254. On a éliminé la valeur (adresse réseau) et la valeur 255(adresse de diffusion).

6-3-4-Le champ *"00001010"* :

C'est un champ réservé aux réseaux privés de classe A par l'internic

6-4-le masque associé :

Représentation binaire:

11111111.11111111. 11111111. 00000000

Représentation décimale:

255.255.255.0

7-CONCLUSION:

Dans ce chapitre nous avons présenté l'organisme d'accueil et ses missions ainsi que les poste de travail qui nous concernent afin de faciliter la recherche de l'information.

CHAPITRE I
LA GESTION DES RESEAUX

I-1-Introduction:

La gestion des réseaux se définit comme l'ensemble des activités liées au contrôle, à la coordination et à la surveillance des ressources qui participent à l'établissement de communications. Gérer un réseau revient à observer son activité tel que la collecte des statistiques sur le débit réel ou le calcul des taux d'erreurs, à contrôler les opérations en cours (Contrôle des accès, statut des connexions) et à agir sur l'ensemble de ses ressources de communication (Activer, initialiser une station ou un routeur). [Cha 99]

Différents protocoles permettent la remontée d'information des équipements vers le manager. Cela permet d'identifier les éléments raccordés au réseau et de connaître leur état. Une bonne gestion doit réaliser les objectifs suivants :

- Offrir aux utilisateurs un service de qualité.
- Permettre l'évolution du système en incluant de nouvelles fonctionnalités.
- Optimiser les performances des services pour les utilisateurs.
- Permettre une utilisation maximale des ressources pour un coût minimal.

Pour répondre au mieux à ces besoins, l'administrateur du réseau doit disposer de trois types d'actions pour suivre l'état du réseau et pouvoir réagir :

- Des actions en temps réel pour connaître l'état de fonctionnement de son

réseau (surveillance et diagnostic des incidents, mesure de la charge réelle, maintenance, contrôle, informations aux utilisateurs... etc.) et agir sur celui-ci (réparation, ajout/retrait de nouveaux abonnés) ainsi que d'en assurer la sécurité (contrôler les accès, donner/retirer des droits d'accès... etc.).

- Des actions différées pour planifier, optimiser, quantifier et gérer les évolutions du réseau (statistiques, comptabilité, facturation, prévention, évaluation de charges... etc.)
- Des actions prévisionnelles qui lui permettent d'avoir une vision à moyen et long terme, d'évaluer des solutions alternatives, de choisir les nouvelles générations de produit, de vérifier la pertinence de la solution réseau pour un problème donné. [Cha 99]

I-2.Les deux facettes de l'administration :

L'administration des réseaux et des systèmes est bâtie à partir de briques du marché : les administrateurs techniques, les agents inclus dans les équipements, les produits de gestion administrative. L'ensemble de ces éléments compose deux domaines complémentaires :

- La gestion administrative : liée à l'organisation de l'entreprise.
- La gestion technique : relative au fonctionnement du réseau.

I-3.Les besoins fonctionnels de la gestion des réseaux :

Les besoins fonctionnels sont regroupés autour de 5 grandes fonctionnalités : la gestion de la configuration, des performances, des anomalies, des informations comptables et de la sécurité.

I-3-1-La gestion de la configuration :

Rendre un réseau opérationnel, c'est tout d'abord le configurer. Il s'agit de donner une description formelle et non ambiguë de tous les éléments constitutifs, de son architecture et de son mode de fonctionnement (notion de paramétrage du réseau). On obtient une image du réseau, en considérant chacun de ses composants physiques (éléments du réseau) et logiques (protocoles de communication), comme un objet élémentaire. Un objet peut être caractérisé par un type, des attributs, un état, des relations entre objets. La description successive de toutes les ressources du réseau autorise une vue des nœuds, des voies logiques et physiques de celui-ci, c'est à dire de sa topologie. Cette carte du réseau est en réalité obtenue en utilisant des langages de configuration propres à chaque architecture de réseau.

Le réseau prend alors connaissance de son architecture, de l'implantation de chaque entité, de leur localisation et des moyens d'y accéder. La cohérence de la configuration du réseau est vérifiée, lors de la phase de génération. Les phases de configuration et de génération constituent l'initialisation du réseau après lesquelles il devient opérationnel et capable de répondre à une demande de service réseau. Un réseau peut voir son architecture évoluer au cours de son utilisation (ajout, suppression, modification logique et/ou matérielle), nécessitant une reconfiguration. Cette phase doit pouvoir se faire en dynamique, sans entraîner un arrêt, même partiel, du service du réseau. [Cha 99]

I-3-2-La gestion des performances :

Les réseaux de communication sont généralement soumis à un trafic aléatoire résultant de l'utilisation imprévisible des ressources mises à la disposition des utilisateurs. Ceci a pour conséquence de rendre variable la qualité de service qu'ils ressentent. L'évaluation des performances des réseaux a pour objectifs :

- De prévoir et de quantifier la qualité de service.
- D'identifier et de paramétrer les outils du réseau nécessaires pour satisfaire la qualité de service.

Les évaluations de performances s'effectuent lors des différentes phases de La vie du réseau : à sa conception (dimensionnement du réseau), lors de Changements d'équipement (prise en compte des expériences passées), durant Le suivi du réseau (vérification et analyse fine des temps de réponse, de traversée, évaluation du débit efficace et maximum, test et contrôle du comportement du réseau, réglage des paramètres du système).

On dispose d'indicateurs de qualité de service définis pour ces réseaux portant sur leur temps de traversée, leur débit efficace, le taux de perte d'informations, le taux de refus d'établissement de communication, le temps de réponse (délai de transmission), le taux d'utilisation, le taux de pannes. En effet, lorsqu'un paquet arrive à un équipement, il est utilisé immédiatement si l'équipement est libre, sinon il est mis en file d'attente. Ainsi, les ressources du réseau ne sont pas réservées pour la durée d'une communication mais partagées entre les différents flux traversant un équipement. Le temps de traversée d'un paquet dépend alors du trafic qu'il rencontre le long de son chemin dans le réseau. Le débit efficace est le flux maximum d'informations des utilisateurs que le réseau peut effectivement acheminer. Afin d'obtenir un meilleur rendement, il faut assurer le partage des ressources, la régulation des flux du trafic et l'intégrité des informations transférées. [Cha 99]

I-3-3-La gestion des anomalies :

La détection des pannes (localisation et signalisation) est indispensable pour que les mécanismes de réparation et de reconfiguration puissent se réaliser et laisser un système dans un état opérationnel. Les pannes peuvent provenir aussi bien des logiciels que du matériel. La détection des pannes peut se réaliser à partir de périphériques spécialisés ou par logiciel. L'origine d'une défaillance peut se détecter par logiciel, soit par des mécanismes de " senseur " ou de " chiens de gardes " internes ou encore par la surveillance d'une unité par une autre. Cela est réalisé par les fonctions de :

- Surveillance et de prise en compte des événements non sollicités (alarmes).
- Localisation des pannes par des tests.
- Détermination et identification des pannes par analyse ou via des systèmes experts de correction.

Des tests périodiques et systématiques autorisent la signalisation de défaillances des équipements. De plus, la plupart des équipements intègrent des mécanismes de contrôle et de surveillance divers (détection d'erreur de parité en mémoire ou sur bus). Toutes ces détections donnent lieu à des transferts d'informations à des fins de gestion aux points de contrôle du réseau dont dépendent les équipements. Les points de contrôle peuvent agir à distance sur des systèmes en déclenchant des procédures de tests; par exemple ils autorisent des actions de télémaintenance et de télésurveillance en temps réel ou en différé.

[Cha 99]

I-3-4-La gestion des informations comptables :

La gestion des informations comptables consiste à assurer toutes les fonctions relatives à la comptabilisation de l'utilisation des ressources du réseau par les utilisateurs. Elle vise en générale la facturation en fonction de la tarification ainsi que la gestion et la surveillance des quotas d'utilisation des ressources.

I-3-5-La gestion de la sécurité :

La sécurité des réseaux revient à mettre à disposition des systèmes des procédures et des outils qui assurent :

- A l'émetteur d'un message : que ce dernier parvient bien au bon destinataire et qu'il ne pourra être compromis que par celui-ci, que le destinataire ne pourra nier avoir reçu le message et prétendre avoir reçu un message non expédié.
- Au destinataire de message : l'authentification de l'émetteur, l'intégrité du message, que l'émetteur ne peut nier avoir envoyé le message et que seuls les émetteurs autorisés pourront lui envoient des messages.

La gestion des services de sécurité doit permettre le contrôle d'accès, l'authentification des correspondants, la confidentialité et l'intégrité des données. Le service d'authentification peut être rendu en mettant en œuvre des services d'annuaire électronique. Ces derniers gèrent des références d'usagers comme des attributs et délivrent des jetons d'authentification. Il s'agit d'une procédure asynchrone. L'authentification peut être simple (identification et mot de passe) ou forte en utilisant un mot de passe protégé par crypto–système à clé publique **D**ata **E**ncryption **S**tandard (DES), **D**ata **E**ncryption **A**lgorithm **1** (DEA 1). [Cha 99]

I-4. Architecture des protocoles TCP/IP :

Le modèle TCP/IP est structuré en quatre couches principales qui s'appuient sur une couche matériélle. (Voir figure I.1)

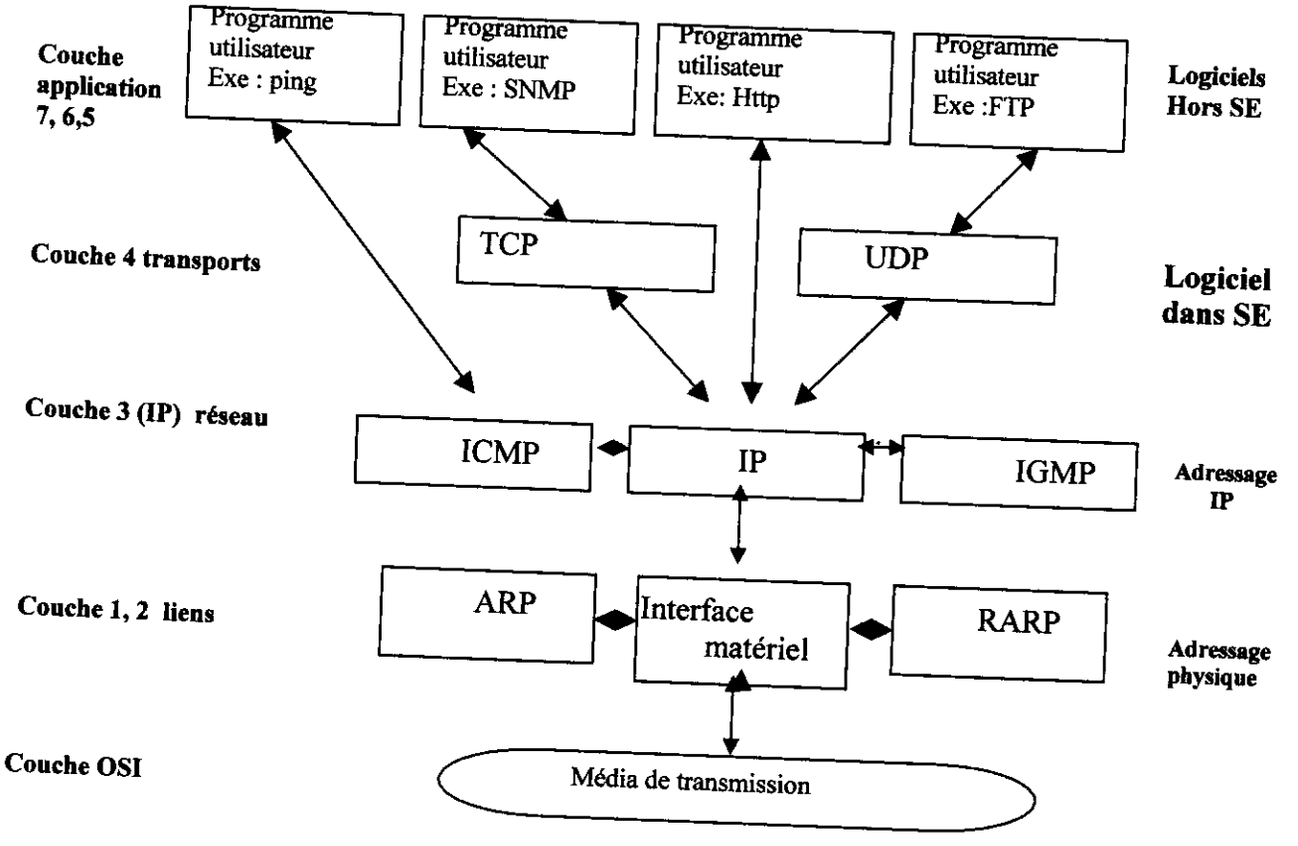
Les quatre couches sont :

- La couche liens (c o u c h e d'acces) : c'est l'interface physique avec le média de transmission. Elle est constituée d'une carte d'interface et son pilote du système d'exploitation.
- La couche réseau ou couche IP (**I**nternet **P**rotocol) : elle gére la circulation des paquets à travers le réseau en assurant leur routage, elle comprend également les protocles ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol) et IGMP (**I**nternet **G**roup **M**anagement **P**rotocol).

-la couche transport : elle assure en premier lieu la communication de bout en bout en faisant abstraction des machine intermédiaires entre l'émetteur et le

Destinataire .en second lieu, elle régule le flux de données et assure un transport fiable (données transmise sans erreurs et reçues dans l'ordre de leurs émission) dans le cas de TCP (Transmission control Protocol) ou non fiable dans le cas UDP (User Datagram Protocol). Dans le cas du protocole UDP, il n'est pas garanti qu'un datagramme arrive à bon port, c'est la couche supérieure de s'en assurer.

La figure I-1 illustre l'interaction entre les différents protocoles du modèle TCP/IP.



- La couche application : c'est les programmes utilisateurs comme par exemple SNMP (**S**imple **N**etwork **M**anagement **P**rotocol) , SMTP (**S**imple **M**ail **T**ransfert **P**rotocol),HTTP(**H**yper **T**ext **T**ransport **P**rotocol),FTP(**F**ile **T**ransport **P**rotocol) ...etc. [Doug2000]

I-5.Les Protocoles de gestion:

Avant 1988, chaque fournisseur employait son propre protocole. Le responsable du réseau se trouvait donc confronté à des centaines d'équipements et applications difficilement administrables en raison de leurs protocoles propriétaires. Dans l'attente de la mise en place généralisée d'un protocole standard (SNMP par exemple), des outils traducteurs s'imposaient Pour convertir le protocole propriétaires en protocole connus du gestionnaire de réseau. Ces outils se répandent aujourd'hui sur le marché. [Biz 97]

Plusieurs protocoles ont été implémentés pour réaliser les différentes tâches précédemment décrites. On peut distinguer les protocoles SNMP et CMIP/CMIS.

L'administration des réseaux se subdivise en plusieurs fonctionnalités. La gestion des configurations qui regroupe les fonctions d'installation, de contrôle, de surveillance et de gestion des identifiants. Lors de pannes, il faut déterminer, le plus rapidement possible, l'emplacement et le type du problème à résoudre. Les besoins en ressource des applications sont de plus en plus importants et nécessitent une gestion des performances du réseau afin d'y répondre. La comptabilisation des périodes et des ressources machines utilisées permet de répartir les coûts liés au réseau. L'interconnexion de l'ensemble des stations accroît la possibilité d'intrusions illicites sur le réseau. Il est donc nécessaire de définir une politique de sécurisation. [Rich2001]

Le protocole SNMP est un standard car il est actuellement devenu le plus utilisé pour la gestion des réseaux. Son principe de fonctionnement repose sur le principe du polling, c'est à dire que la station de gestion interroge régulièrement tous les éléments gérés. Chaque point du réseau dispose d'une base d'information regroupant les données liées, par exemple : nombre de trames reçues par point du réseau.

Le protocole CMIP/CMIS (**C**ommon **M**anagement Information **P**rotocol/**S**ervices) est beaucoup moins utilisé que le SNMP du fait de la complexité de son implémentation. C'est un protocole normalisé OSI s'appuyant sur trois types d'activités qui sont la gestion système, la gestion de couches et la gestion d'opérations de couche. Cette dernière s'appuie sur les différentes couches de transport en mode IP ainsi elle permet une gestion très détaillée et plus sécurisée du réseau.

Nous avons utilisé dans notre travail le protocole SNMP qui se décline en plusieurs versions incluant des fonctionnalités sécuritaires, d'authentification, que nous allons décrire dans le chapitre suivant.

I-6.Le modèle de gestion par SNMP :

L'architecture SNMP a été initialement développée pour être supportée par le système d'exploitation UNIX dans un environnement TCP/IP, et pour fonctionner en mode datagramme (non connecté) avec l'utilisation d'UDP. L'architecture SNMP est composée d'un ensemble de noeuds gérés (MN: **M**anaged **N**odes), une station de gestion centralisée **NMS** (**N**etwork **M**anagement **S**tation) et d'une base d'information MIB (**M**anagement **I**nformation **B**ase) qui contient tous les objets gérés et un protocole de gestion qui permet

l'échange d'information entre la station de gestion et les différentes machines

gérées .SNMP est donc conforme à la normalisation de l'ISO en matière

d'administration des réseau (OSI Management Framework 1990) puisque SNMP

définit : [Del 97]

- Des stations d'administration appelées « Managers ».
- Des stations administrées appelées « Agents ».
- Un protocole d'échange entre entité gérante et entité gérée.
- Une base d'information « MIB » .

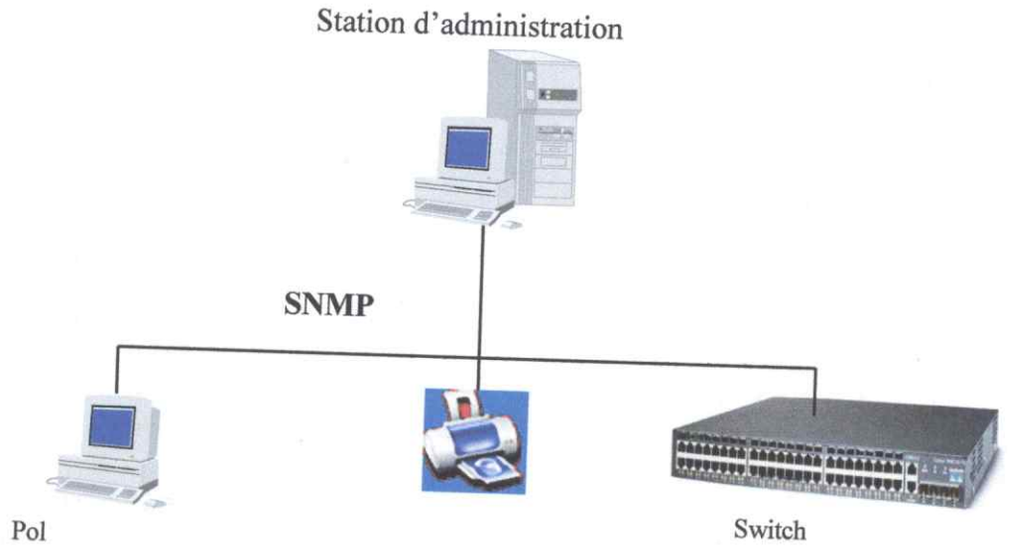


Fig I-2 :Le modèle centralisé de la gestion par SNMP

De l'administration est organisée de manière à ce que la complexité du système soit centralisée sur la station d'administration et que l'installation des agents sur les élément s du réseau reste simple et d'un faible coût .peu de ressource sont nécessaire pour faire fonction ces agents qui peuvent être implémentés dans les équipements sans modification de structure, tel qu'il est illustré par la figure I-2. [Del197]

Dans cette section, nous allons vois la NMS et les différente types d'agent existant dans le modèle de gestion par SNMP ,la base d'information et le protocole SNMP seront détaillés dans le chapitre suivent.

I-6-1)la station d'administration :(NMS network management station).

Une station d'administration est définie comme la station qui surveille l'état du réseau, c'est la composante centrale de l'architecture : elle demande périodiquement des information et centralise les alertes provenant de chacun des nœuds gérés a fin de permettre à l'administrateur de surveiller individuellement chacun de ces nœuds. Elle maintient sa propre base d'information de gestion à laquelle d'autres station d'administration du réseau peuvent accéder.

Une station d'administration peut gérer plusieurs noeuds et plusieurs stations d'administration peuvent gérer des noeuds identiques.

Les commandes pour l'interrogation des agents sont lancées à partir de la station d'administration, soit par l'opérateur, soit par des scripts automatiques. Il existe deux grands types d'administrateurs SNMP : les systèmes propriétaires, développés par la plupart des constructeurs équipements, et les plates-formes ouvertes accueillant des applications élaborées par ces mêmes constructeurs et développeurs extérieurs. Le manager comporte un noyau SNMP dont le rôle est d'interpréter la MIB et d'associer des icônes aux objets gérés.

I-6-2) Les noeuds gérés :

Les nœuds à gérer peuvent être soient des agents simples ou spéciaux :

a) Les agents :

Les agents SNMP sont implémentés dans les équipements compatibles SNMP et fournissent des informations à la MIB. Chaque agent possède une vue partielle sur la MIB, cette vue concerne la partie de la MIB où ses objets représentent l'équipement à administrer par l'agent. La nature des informations peut être, par exemple, la consultation des capteurs et de variables d'état dans la mémoire d'un routeur.

Un noeud géré peut être n'importe quel élément du réseau, tels qu'une station de travail, un serveur ou une imprimante. Ça peut être également des éléments réseaux logiques ou physiques, une passerelle, un pont, un modem, un multiplexeur... etc. Chaque noeud supporte un agent « serveur » qui s'exécute sur la machine gérée.

On doit dans certains cas faire appel à des agents spéciaux pour pouvoir gérer des équipements distants à travers un WAN (**W**ide **A**ria **N**etwork) ou des équipements qui possèdent des protocoles propriétaires. [Del96]

b) Les agents spéciaux :

b-1) Les agents RMON :

L'agent RMON (**R**emote network **MON**intoring) est situé dans une sonde, il surveille les paramètres de fonctionnement d'un réseau local (taux d'erreur, collisions... etc.). Il peut déclencher des alertes de performances et se comporter comme un analyseur de protocole local. Il remonte les informations soit vers un gestionnaire SNMP supportant la RMON MIB, soit vers un outil de gestion propriétaire tel qu'illustré dans la figure I-3. [Del 96]

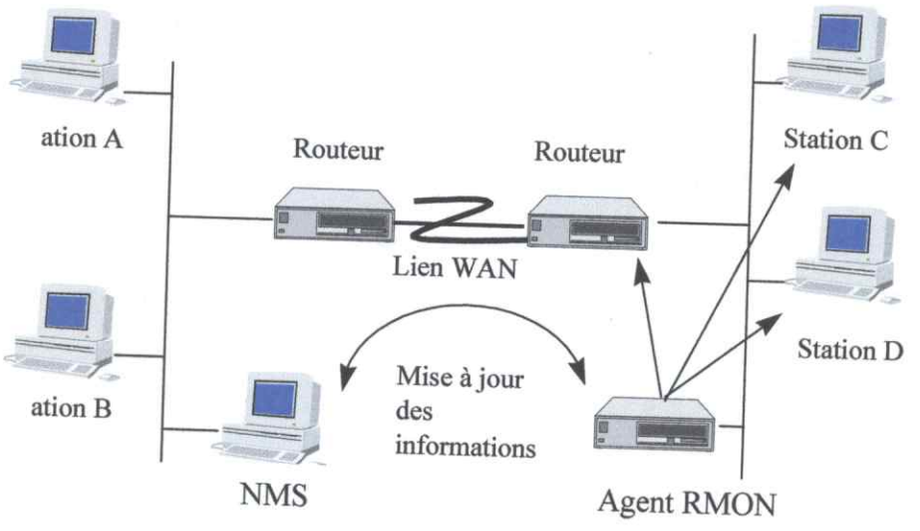


Fig I-3 : L'agent intelligent RMON

b-2) Les agents Proxy :

Certaines machines peuvent avoir des protocoles propriétaires qui n'utilisent pas le protocole UDP. Dans ce cas, on peut utiliser des agents par procuration appelés PROXY AGENT. Ces agents utilisent des mécanismes de translation de protocoles. La traduction peut se faire au niveau de la couche transport ou de la couche application (adaptation du protocole SNMP). Cet agent Proxy gère un ensemble de noeuds propriétaires par scrutation de ces composants. L'agent Proxy se comporte comme le représentant d'un ensemble de noeuds gérés pouvant dialoguer avec la station d'administration. La figurel-4 montre le fonctionnement d'un agent proxy. [Del 96]

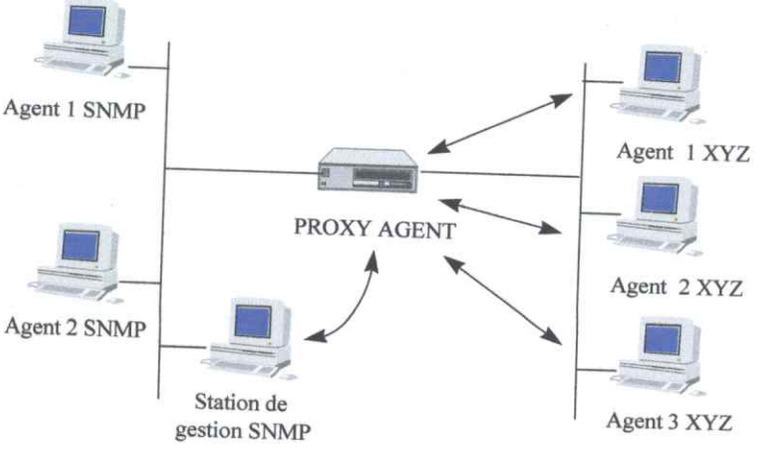


Fig I-4 :L'agent proxy

I-7. CONCLUSION:

La gestion des réseaux est devenue aujourd'hui une nécessité pour assurer une utilisation rationnelle des ressources du réseau ; elle se compose en plusieurs fonctionnalités. La première est la gestion des configurations qui permet de rendre le réseau opérationnel avec une configuration optimale. La deuxième est la gestion de contrôle et de sécurité, elle est obligatoire car l'interconnexion de l'ensemble des stations accroît la possibilité d'intrusions illicites sur le réseau.

La gestion des pannes permet de déterminer le plus rapidement possible l'endroit et le type des anomalies. La gestion des performances assure de répondre aux besoins en ressource des applications aux utilisateurs du réseau. La gestion de comptabilité permet de répartir les coûts liés au réseau.

Il est donc nécessaire de définir une politique de gestion du réseau complète.

Il y a deux protocoles de gestion, CMIP pour les réseaux OSI et SNMP pour les réseaux TCP/IP, ce dernier est devenu aujourd'hui un standard.

De la même façon qu'il n'existe pas deux architectures des réseaux identiques, il n'existe pas deux gestions des réseaux similaires. Il est de la responsabilité du gestionnaire des réseaux de trouver un compromis judicieux entre la nature des services offerts aux utilisateurs, la qualité de ces services et les moyens à mettre en œuvre pour assurer le succès de cette politique.

Dans notre travail, nous allons réaliser un outil de gestion des réseaux dont lequel nous allons utiliser le protocole SNMP. Il vise la gestion des performances, la gestion de et des anomalies en réalisant un superviseur du réseau avec une cartographie de la topologie.

CHAPITRE II
LA GESTION PAR SNMP

II-1.GENERALITE SUR SNMP :

II-1-1.Historique :

La conscience d'un manque dans le domaine de la gestion des réseaux Apparaît en mars 1987, avec Bob Braden qui était responsable de la NSF (National Science Foundation) et exprime à ses collaborateurs la nécessité de disposer d'outils d'administration pour le réseau national de la recherche, NSFnet.[Del 96]

Grâce au professeur Jeffrey Case de l'université du Tennesse, un nouveau protocole SGMP (Simple Gateway Monitoring Protocol) est mis au point moins d'un an plus tard. SGMP est un protocole pour la gestion des routeurs. Les fonctions de SGMP étaient limitées à celle d'une interface pour visualiser l'état des routeurs. Il était clair par conséquent que SGMP était une solution de courte durée.

L'Internet Team qui était responsable de l'implémentation du protocole SGMP, fut choisie par la communauté Internet pour développer un successeur à SGMP offrant des fonctions de gestion plus étendues. En 1988, L'architecture de SNMP fut définie par l'IETF (Internet Engineering Task Force) dans le RFC 1067(Request For Comment) et ratifiée comme standard Internet dans le RFC 1098. Aujourd'hui la dernière spécification de SNMP est le RFC 1157.[Del 96]

Les chercheurs pensaient, à l'époque, que le développement de SNMP serait très rapidement surpassé par un phénomène de migration vers les standards OSI, mais le phénomène inverse se produisit grâce à sa simplicité, à sa souplesse d'utilisation et à sa rapide disponibilité comme un standard accepté par la plupart des intervenants du marché des communications. SNMP était prévu pour un environnement TCP/IP, mais il est rapidement sorti de ce cadre afin de gérer d'autres types de réseaux, et des équipements régis par d'autre modèle.

Bien que SNMP soit intégré par la plupart des fabricants, amenant une large distribution, quelques problèmes rencontrés dans le domaine de la sécurité ont restreint L'utilisation de SNMP dans les réseaux WAN. Les mécanismes de sécurité définis dans la spécification d'origine de SNMP furent les principales réclamations demandées dans le changement de version.

En effet dans la première spécification de 1988 [Del 96], il n'était pas possible d'inclure des considérations de sécurité pour les raisons suivantes :

- Les groupes individuels de standardisation ne pouvaient pas être d'accord sur une stratégie commune.
- A l'époque, il n'y avait pas assez d'expériences pratiques dans ce domaine.
- Les utilisateurs sont restés silencieux sur le sujet et aucune pression ne fût exercée sur les groupes de standardisation.

Une proposition « Secure SNMP », publiée dans le RFC 1352 en juillet 1992[Del 96], présenta un nouveau mécanisme d'authentification et de codage indépendant pour améliorer la sécurité. Il fut fortement critiqué car ce mécanisme manquait de compatibilité avec la version 1. En effet tous les produits installés devaient être remplacés ou mis à jour.

Le groupe de travail sur la sécurité SNMP et le groupe de travail du SNMP, réussirent à publier la spécification du protocole SNMP v2 dans le RFC 1446 en utilisant ou en incluant les travaux précédemment réalisés notamment « Secure SNMP » et les travaux sur RMON. La MIB utilisée par la version 2 de SNMP fut publié dans la RFC 1447. En 1993 le travail sur le standard SNMP v2 fut terminé par les groupes de travail Internet (Internet Working Groups) et ratifié par IETF (Internet Engineering Task Force). Ces standards furent publiés dans les RFC 1441 à 1452.[Del 96]

1-2.Définition de SNMP :

Le protocole **SNMP** (**S**imple **N**etwork **M**anagement **P**rotocol) est un protocole d'administration de réseau issu du monde TCP/IP. C'est un protocole de couche applicative, il utilise l'UDP qui est un protocole de transport en mode non connecté. Le choix de UDP contre TCP est justifié par la simplicité et la faible taille du code. Il existe par ailleurs des solutions SNMP non routables, c'est à dire sans les couches intermédiaires 3 et 4. Ces solutions permettent de réduire l'encombrement des agents SNMP dans les équipements. Elles sont adoptées par certains constructeurs pour la gestion des cartes adaptateurs.[Rich2001]

1-3.Les avantages de SNMP :

Le protocole SNMP est le plus répandu à ce jour. Presque tous les nouveaux équipements télécoms sont munis d'un agent SNMP. Près de 20% des équipements en service supportent le protocole SNMP et certains désormais ne sont plus administrables qu'à travers ce protocole. De plus, l'offre SNMP en matière de gestionnaire de réseau est excessive. De nombreux systèmes sont aujourd'hui opérationnels. Dans la pratique, seuls quelques équipements télécoms haut de gamme, et destinés à priori aux opérateurs, sont munis d'agents CMIP. Toutefois, si les besoins des opérateurs de télécommunication ne peuvent pas être satisfaits par le protocole SNMP, très peu de systèmes d'administration basés sur CMIP sont opérationnels dans le monde. [Rich2001]

SNMP occupe cette position grâce aux avantages suivants :

- Protocole très simple et facile à utiliser.
- Permet une télé-administration des différentes machines.
- Le modèle fonctionnel de surveillance et de gestion est extensible.
- Indépendant de l'architecture des machines administrées.

1-4. Les fonctionnalités de SNMP :

D'un point de vue fonctionnel SNMP offre aux managers des réseaux un point de contrôle central à partir duquel ils peuvent essentiellement effectuer trois types de tâches :

- Superviser les performances d'un réseau est un point essentiel. Quand un problème se produit, avant de tenter n'importe quelle action, le manager a besoin d'informations sur l'état du réseau et la façon dont il fonctionne. Ces différentes informations sont encore plus probantes lorsqu'il s'agit de statistiques effectuées en temps réel sur le réseau.

- Contrôler/commander le réseau signifie la possibilité de changer des variables de n'importe quel équipement. Généralement ces changements interviennent, soit au moment de la mise en configuration des équipements, soit à partir des données collectées lors de la phase de supervision.

- Administrer le réseau signifie collecter des informations qui seront placées dans l'historique du réseau.

C'est la combinaison de ces trois aspects qui permet de gérer les réseaux de façon relativement efficace.

1-5. Les versions du SNMP :

Actuellement il y a trois versions du protocole SNMP qui sont :

SNMP Version 1 (SNMPv1): Défini dans la RFC 1157 avec un mécanisme de sécurité basé sur la notion de communauté (mot de passe en clair dans les requêtes et réponses)

SNMP Version 2 (SNMPv2): Défini dans les RFC 1905, 1906 et 1907.Il introduit deux nouveaux types de paquets get-bulk-request et inform-request (communication entre plate- formes).

SNMP Version 3 (SNMPv3): Défini dans les RFC 2570, 2571, 2572, 2573, 2574 et 2575. Il introduit de nouveaux mécanismes de sécurité (forte authentification et confidentialité). [Oli2001]

1-6.L'ASN-1 :

ASN-1 (**A**bstract **S**yntax **N**otation **O**ne) est un langage formel qui présente deux caractéristiques principales : Une notation utilisée dans les documents manipulés par script et une représentation codée de la même information, utilisée dans les protocoles de communication. Dans les deux cas la notation formelle précise, élimine toutes les ambiguïtés possibles, tant du point de vue de la représentation que de la signification. Au lieu de dire, par exemple, qu'une variable contient une valeur entière, un concepteur qui utilise ASN-1 doit définir la forme exacte et le domaine des valeurs prises par cet entier. Une telle précision est nécessaire dans le cas de mises en oeuvre qui impliquent des machines hétérogènes n'utilisant pas toutes la même représentation des éléments de données.[Cha 99]

Parallèlement au fait de rendre les documents non ambigus, ASN-1 contribue également à simplifier la conception des protocoles d'administration des réseaux et à garantir leur interopérabilité. Il définit avec précision comment coder le nom et la valeur d'un élément de donnés dans un message. Donc, une fois que la description d'une MIB a été exprimée en ASN-1, la forme lisible par l'homme peut être directement et automatiquement traduite dans la forme codée utilisée dans les messages.

Les protocoles d'administration des réseaux utilisent la notation formelle ASN-1 pour définir le nom et le type des variables de la base de données d'informations d'administration des réseaux. La précision de la notation élimine toute ambiguïté de forme ou de contenu au niveau des variables. [Cha 99]

On distingue deux types d'utilisations principales pour SNMP :

- Description des messages de communication.
- Description des objets SNMP.

Ce langage définit différents types de données gérées sous SNMP d'après trois Catégories :

- Données simples :
  - integer
  - octet string
  - object identifier

- Données dites simplement construites :
  - Sequence
  - Sequence of
- Données applicatives:
  - IpAddress
  - NetworkAddress
  - Counter
  - Gauge
  - TimeTicks

Les définitions de ces types de données en annexe [B]

I-7.Comparaison OSI – SNMP :

Le protocole SNMP est composé de plusieurs parties dont chacune d'elle correspond à une couche du modèle OSI, comme il est illustré dans la figure II-1. Il utilise le protocole IP pour la couche réseau et le protocole UDP pour le transport des informations entre les différentes entités du modèle de gestion par SNMP. L'ouverture d'une session SNMP est réalisée par la partie authentification de ce dernier; les informations gérées par SNMP sont présentées via la notation ASN-1 et structure via la structure SMI (Structure Management Information) qui sera détaillée à la suite de ce chapitre.

Dans la couche application, on trouve les applications qui utilisent le protocole de gestion qu'elles soient un système de gestion de réseau complexe à base du protocole SNMP ou une simple application d'interrogation des agents.

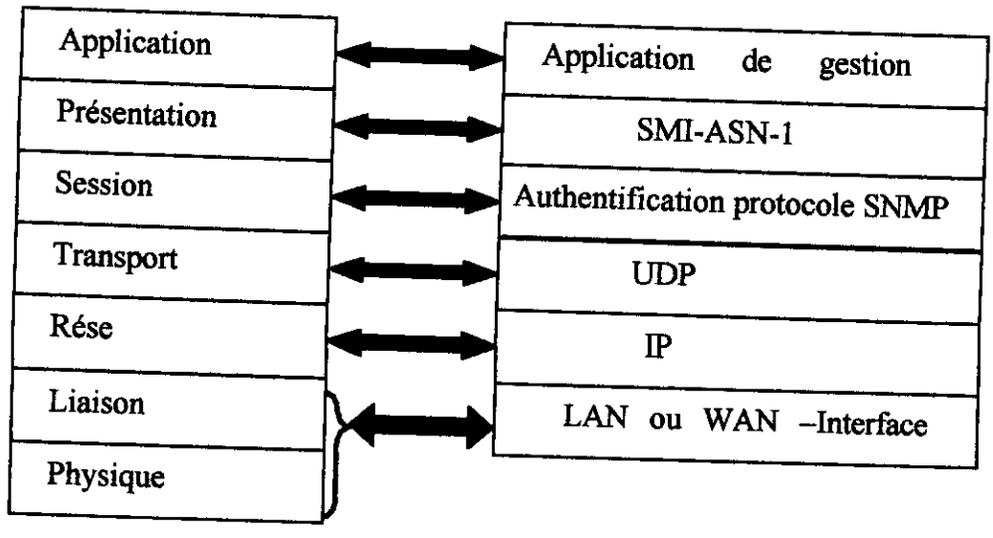


Fig II-1 : comparaison entre SNMP et le modèle OSI

II-2. LA BASE D'INFORMATION DE GESTION (MIB)

2-1 Définition de la MIB :

La Base d'Information de Gestion (MIB) est une base de données faisant référence à des objets clairement définis, mais ne se trouvant pas stockés dans une base de données réelle gérée par SNMP. La MIB peut être considéré comme une base de données virtuelle. La valeur des objets est stockée quelque part et c'est au programme serveur (daemon SNMP) de les retrouver lorsqu'ils sont réclamés par le gestionnaire. Une MIB est une collection de tous les objets que maintient un agent donné.[Biz 97]

La MIB est une base de donnée d'information maintenue par un agent interrogeable ou paramétrable par un manager. Elle spécifie en détails les données associées aux différents éléments qui composent un réseau géré avec le protocole SNMP. Par exemple, la MIB spécifie d'une part qu'un logiciel IP doit disposer d'un compteur d'octets comptabilisant tous les octets qui arrivent sur une interface réseau et d'autre part que le logiciel d'administration peut uniquement lire ces compteurs. La structure de cette base de données fait référence à l'arbre MIT (**M**anagement **I**nformation **T**ree). Cet arbre est composé à la fois des objets que l'on peut retrouver dans un réseau mais également des propriétés liées à chaque objet (ex : un routeur Cisco et le nombre de paquets IP transmis).

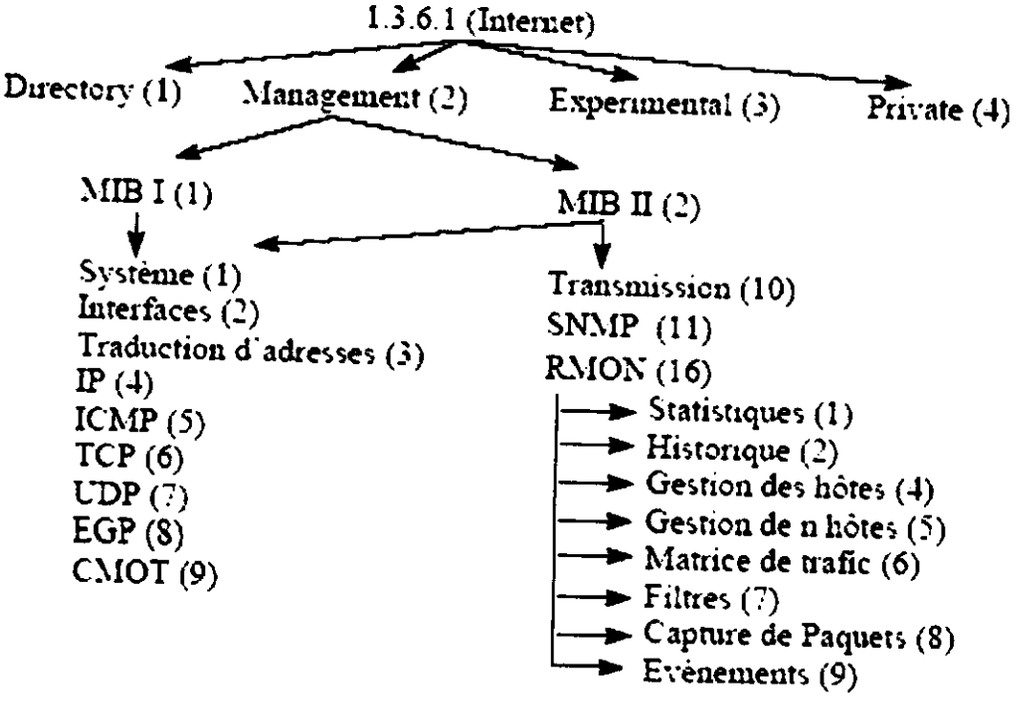


Fig II-2 : l'arbre de définition de la MIB-I et la MIB-II

Actuellement, la base la plus utilisée est la MIB-II car elle est plus riche que la première version et contient des éléments propres à la gestion SNMP. Une MIB est composée des informations élémentaires à laquelle les constructeurs peuvent ajouter à la MIB leurs propres définitions. En fonction de ses besoins

et des fonctionnalités offertes par une MIB propriétaire, cela peut déterminer le choix d'un équipement.[Rich 2001]

Nous allons décrire la MIB-II, dont les spécifications sont dans la RFC 1213. Elle décompose les informations d'administration des réseaux en 11 catégories standard illustrés dans le Tableau II-1. Elle ajoute des nouveaux groupes par rapport à la MIB-I (Le groupe SNMP et CMOT). [Biz 97]

Catégorie MIB	Permet d'avoir les informations sur :	Nb objets
System	Le système d'exploitation de la machine ou du routeur	7
interfaces	Chaque interface réseau	23
AT(translation	La traduction d'adresse (ex. correspondance ARP)	3
Ip	Statistique sur le logiciel IP	38
Icmp	Statistique sur le logiciel ICMP	26
Tcp	Statistique sur le logiciel TCP	19
Udp	Statistique sur le logiciel UDP	7
Egp	Statistique sur le logiciel EGP	18
Transmission	Ce groupe est prévu pour « raccrocher » d'autres modules de MIB qui concernent des médias de transmission plus spécifiques qui viennent compléter les informations contenues dans le groupe interface.	0
Cmot	Compteurs pour CMOT (protocole OSI équivalent à SNMP)	0
SNMP	Statistique sur le logiciel SNMP	30

Tab II-1 :Catégories d'information MIB-II

L'indépendance de la définition de la MIB par rapport au protocole d'administration a deux avantages. D'abord, cela permet à un constructeur de mettre dans les équipements, comme un routeur, un logiciel agent SNMP avec la certitude qu'il fonctionnera correctement lorsque les éléments de la MIB auront été définis. Le deuxième avantage, est qu'un utilisateur peut se servir du même client d'administration (le manager) pour gérer des équipements identiques (routeurs) mais ayant des MIB différentes.

2.2 Structure des informations d'administration (SMI) :

a)Définition :

En plus du standard MIB, qui définit les informations spécifiques d'administration et leur signification, Il faut aussi un autre standard qui spécifie l'ensemble des règles utilisées pour définir et identifier les variables MIB. Ce sont les règles de gestion des informations d'administration, SMI (Structure of Management Information).

Une SMI est un ensemble de règles établies afin de définir et d'identifier des variables. On peut la considérer comme une couche au-dessus de ASN-1 dans la représentation des données. Cette structure correspond à une syntaxe utilisée pour la description d'un objet pour lequel elle détermine 3 attributs :[Cha 99]

- Identifiant
- Syntaxe du type
- Codage

b)Descriptions des éléments SMI :

b.1)Syntaxe du type :

Cette syntaxe comporte 3 éléments :

• L'utilisation des différents types spécifiés par ASN-1.

• Une mise en place d'informations administratives : c'est à dire la définition de mode d'accès (read only, read/write, write only, not accessible) et le statut (obsolète, optionnel, obligatoire).

• Un modèle de macro " Object Type " qui instaure une délimitation par les Termes 'begin' et 'end', et une liste de valeurs particulières pour symboliser les différents accès et statuts.

b.2)Identifiant de l'objet :

Un identificateur d'objet est un type de donnée spécifiant un objet désigné "d'autorité", c'est- à-dire que ces identificateurs ne sont pas assignés au hasard, mais alloués par une organisation qui a la responsabilité d'un groupe d'identificateurs. Il consiste en une séquence d'entiers séparés par des points décimaux. Ces entiers recouvrent une structure d'arbre. Il y a une racine non nommée au sommet de l'arbre, à partir de laquelle commencent les identificateurs d'objets.

Toutes les variables de la MIB débutent avec l'identificateur d'objet 1.3.6.1.2.1. Chaque nœud de l'arbre reçoit un nom en clair. Le nom correspondant à l'identificateur d'objet « 1.3.6.1.2.1 » est « iso.org.dod.internet.mgmt.mib ».Ces libellés sont bien sûr plus compréhensibles pour nous. Les noms des variables MIB contenues dans les paquets échangés entre le manager et l'agent sont des identificateur d'objet numériques qui commencent tous par 1.3.6.1.2.1,comme illustré dans la figure II-3.[Rich 2001]

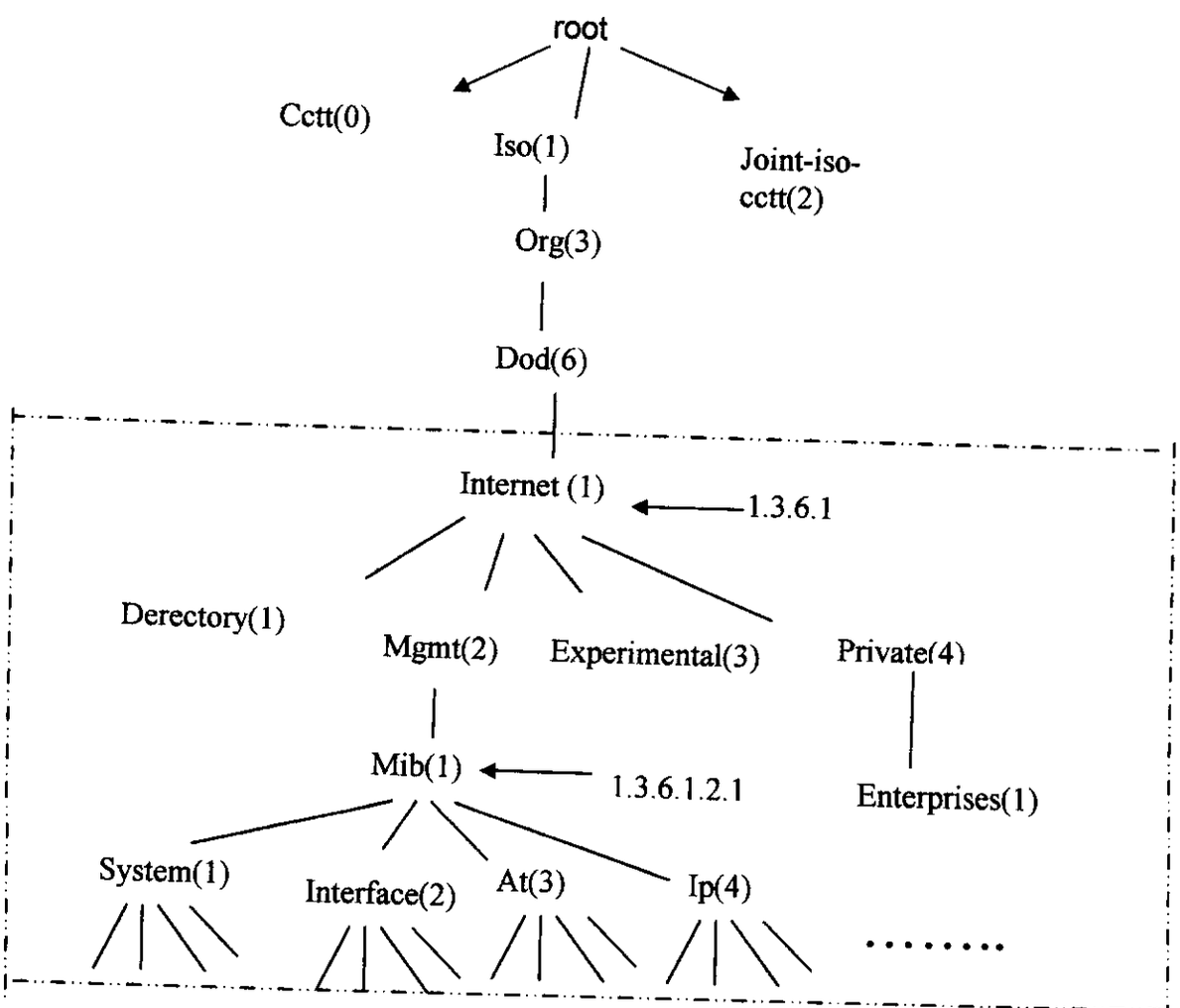


Fig II-3 Identificateurs d'objets contenus dans la MIB

2-3.Type de variable de la MIB :

Les variables de la MIB sont soit de type simple soit de type Table. Par exemple le groupe UDP contient quatre variables simples et une table à deux entrées comme qu'illustré dans la figure II-4

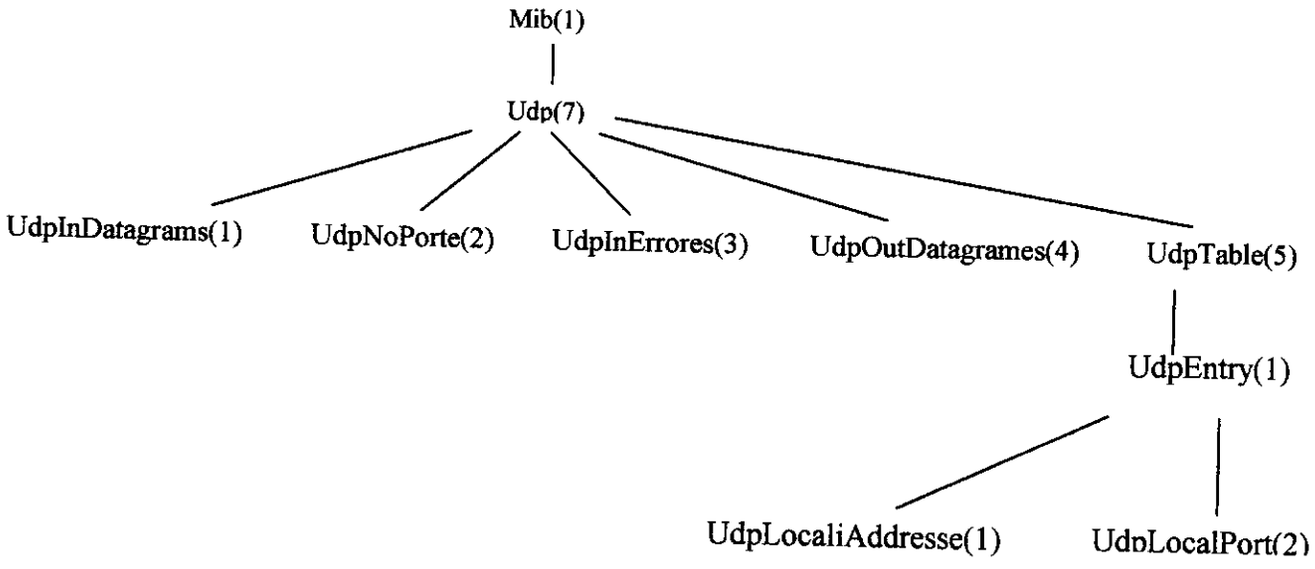


Fig II-4 : Le groupe UDP de la MIB-II

a) Variables simples :

Les variables simples sont référencées en ajoutant " .0 " à l'identificateur d'objet de la variable. Par exemple le compteur udpInDatagrams qu'illustré dans la figure II-3, dont l'identificateur d'objet est 1.3.6.1.2.1.7.1 est référencé 1.3.6.1.2.1.7.1.0. Le label de cette référence est iso.org.dod.internet.mgmt.mib.udp.udpInDatagrams.0.

Bien que les références à cette variable soient normalement abrégées en udpIn Datagrams.0, le nom de la variable qui apparaît dans le message SNMP est l'identificateur d'objet 1.3.6.1.2.1.7.1.0.

b)Tables

Un ou plusieurs index sont spécifiés dans MIB pour chacune des tables. Pour la table de scrutations UDP montrée dans la figure II-4, la MIB définit les index comme une combinaison des deux variables locales udpLocalAddress, qui est une adresse IP, et udpLocalPort qui est un entier.

Prenons par exemple une table de scrutation UDP de trois lignes : la première ligne est pour l'adresse IP 0.0.0.0 et le port 67, la seconde pour 0.0.0.0 et le port 161, et la troisième pour 0.0.0.0 et le port 520 comme le montre la Figure II-5.

udpLocalAddress	UdpLocalPort
0.0.0.0	67
0.0.0.0	161
0.0.0.0	520

2-4.Ordonnancement lexicographique :

L'ordre dans la MIB est basé sur les identificateurs d'objet. Toutes les entrées des tables MIB sont ordonnées de façon lexicographique par leur identificateur d'objet. Deux points clés résultent de cet ordonnancement lexicographique [Rich2001]. Pour illustrer l'ordonnancement lexicographique de la MIB nous avons la table de scrutation UDP (figure II-5) comme exemple :

1. Puisque les instances d'une variable donnée (udpLocalAddress) apparaissent avant toutes les instances de la variable suivante dans la table (udpLocalPort), ceci implique que les tables sont accédées selon l'ordre colonne ligne. Ceci repose bien sur l'ordonnancement lexicographique des identificateurs d'objet, non sur celui des noms en clair.

2. L'ordre des lignes d'une table dépend des valeurs dans l'index de la table. Dans la Figure II.5, « 67 » est inférieur à «161», qui est inférieur à «520» (au niveau Lexicographique). Par exemple les six variables de la Figure II-6 sont ordonnées

Ligne	Identificateur d'objet	Nom abrégé	Valeur
1	1.3.6.1.2.1.7.5.1.1.0.0.0.0.67 1.3.6.1.2.1.7.5.1.2.0.0.0.0.67	UdpLocalAdress.0.0.0.0.67 UdpLocalPort.0.0.0.0.67	0.0.0.0 67
2	1.3.6.1.2.1.7.5.1.1.0.0.0.0.161 1.3.6.1.2.1.7.5.1.2.0.0.0.0.161	UdpLocalAdress.0.0.0.0.161 UdpLocalPort.0.0.0.0.161	0.0.0.0 161
3	1.3.6.1.2.1.7.5.1.1.0.0.0.0.520 1.3.6.1.2.1.7.5.1.2.0.0.0.0.520	UdpLocalAdress.0.0.0.0.520 UdpLocalPort.0.0.0.0.520	0.0.0.0 520

Fig. II-6 : Identification d'instance pour les lignes de la table de scrutation UDP.

Ligne	Identificateur 'objetOrdonné de façon lexicographique	Nom abrégé	Valeur
1	1.3.6.1.2.1.7.5.1.1.0.0.0.0.67 1.3.6.1.2.1.7.5.1.1.0.0.0.0.161 1.3.6.1.2.1.7.5.1.1.0.0.0.0.520	UdpLocalAdress.0.0.0.0.67 UdpLocalAdress.0.0.0.0.161 UdpLocalAdress.0.0.0.0.520	0.0.0.0 0.0.0.0 0.0.0.0
2	1.3.6.1.2.1.7.5.1.2.0.0.0.0.67 1.3.6.1.2.1.7.5.1.2.0.0.0.0.161 1.3. 6.1.2.1.7.5.1.2.0.0.0.0.520	UdpLocalPort.0.0.0.0.67 UdpLocalPort.0.0.0.0.161 UdpLocalPort.0.0.0.0.520	67 161 520

Fig. II-7 : L'ordonnancement lexicographique de la table de scrutation UDP

2-5. Description des groupes de la MIB :

La MIB-II. Définit dans la RFC 1213 contient 12 groupes : le groupe System,le groupe Interface, le groupe Traduction d'adresse,le groupe IP,ICMP, TCP, UDP, EGP, CMOT, Transmission,SNMP et le groupe RMON:[Rich 2001]

2-5-1.Groupe system : (1.3.6.1.2.1.1)

Le groupe system est simple; il consiste en sept variables simples (c'est-à-dire sans tables). [voir figure 1 de l'annexe A]

2-5-2.Groupe interface : (1.3.6.1.2.1.2)

Une seule variable simple est définie pour ce groupe : le nombre d'interfaces sur le système.[voir figure 2 de l'annexe A]

Ce groupe définit aussi une table de 22 lignes. Chaque ligne définit les caractéristiques de chaque interface. [Voir figure 3 de l'annexe A]

2-5-3.Groupe AT : (1.3.6.1.2.1.3)

Le groupe de conversion d'adresse est indispensable pour tous les systèmes, mais son rôle a été diminué dans MIB-I. A partir de MIB-II, chaque groupe de protocole réseau (par exemple IP) contient ses propres tables de translation d'adresse. Pour IP, il s'agit de ipNetToMediaTable.

Une seule table de 3 colonnes est définie dans le groupe AT. [voir figure 4 l'annexe A]

2-5-4.Groupe IP : (1.3.6.1.2.1.4) :

Le groupe IP définit de nombreuses variables et trois tables[voir figure 5 de l'annexe A] La première table du groupe IP est la table d'adresse IP, elle contient une rangée pour chaque adresse IP sur le système. Chaque ligne contient 5 variables [voir figure 6 de l'annexe A], la deuxième table du groupe IP est la table de routage (iprouteDesc)[voir figure 7 de l'annexe A] et la table finale dans le groupe IP est la table de conversion d'adresse [fig 8 de l'annexe A]

2-5-5.Groupe icmp : (1.3.6.1.2.1.5)

Le groupe icmp consiste en quatre compteurs généraux (nombre total de Messages ICMP en entrée et en sortie, et le nombre de messages ICMP avec Erreurs en entrée et sortie) ainsi que 22 compteurs pour les différents types de Messages ICMP : 11 compteurs d'entrée et 11 compteurs de sortie.

[Voir figure 9 de l'annexe A]

2-5-6.Groupe tcp: (1.3.6.1.2.1.6)

Le group tcp définit des variables simples et une table unique, la table de connexion TCP (tcpConnTable). La figure 10 de l'annexe A décrit les variables simples dont beaucoup d'entre elles font référence aux états du protocole TCP.
Le groupe tcp a une table unique, la table de connexion TCP, montrée en Figure 11 de l'annexe A, elle contient une ligne par connexion. Chaque ligne contient 5 variables : l'état de la connexion, l'adresse locale IP, le numéro de port local, l'adresse IP distante et le numéro de port distant .

2-5-7.Groupe udp : (1.3.6.1.2.1.7)

Le groupe udp définit 4 variables simples décrites dans la Figure 12 de l'annexe A et une table de scrutation udp qui contient deux lignes updLocalAdress et udpLocalPort. Le groupe UDP décrit aussi une table appelée udpTable qui a deux variables simples, la figure 13 de l'annexe A donne la description de cette table.

2-5-8.Groupe egp : (1.3.6.1.2.1.8)

Il gère le protocole EGP (External Gateway Protocol) ou (routage des paquets entre routeurs).Ce groupe contient 5 variables simples (egpInMsgs, egpInErrors, egpOutMsgs, egpOutErrours, egpAs) et une table egpNeighTable. L'implémentation de ce groupe est obligatoire pour tous les systèmes qui implémentent le protocole EGP. [Voir figure 14 de l'annexe A]

2-5-9. Groupe transmission (1.3.6.1.2.1.10)

Ce groupe ne contient que le type Objet Identifier (transmission number) qui permet d'identifier le type de media utilisé pour la transmission.

2-5-10.Groupe snmp : (1.3.6.1.2.1.11)

Ce groupe est requis pour chaque entité mettant en oeuvre le protocole SNMP. Il contient le nombre de message SNMP entrants et sortants, le nombre de mauvaises versions reçues ou de nom de communauté invalide et la répartition du type de requêtes reçues et envoyées (get, get_next, set et trap).Ce groupe ne contient que des variables simples (30 variables), ils sont regroupés en quatre catégories : variables d'information générale sur le protocole, variable concerne les codes de retour, les objets statiques en entrée et objets statiques en sortie. [Voir figure 15, 16,17 et 18 de l'annexe A]

2-6.La MIB RMON :

C'est une MIB spéciale qui contient les objets nécessaires à la télé administration via SNMP d'un équipement de mesure. Cette MIB est tout d'abord un standard qui émerge dans le monde SNMP. Elle doit fournir l'interopérabilité entre les équipements de mesure et les stations d'administration (les managers), permettant ainsi aux utilisateurs la coopération de différents constructeurs. Elle gère pour l'instant le niveau 2 (liaison) de l'OSI. La RMON MIB est constituée de neuf groupes :[Del 96]

- STATISTICS : statistiques du trafique (octets, paquets, erreurs...)
- HISTORY : accumulation des statistiques en fonction du temps.
- HOST : statistiques par station découverte par l'agent.
- HOSTTOPN : permet le filtrage des ordinateurs qui contiennent une source de statistiques.
- MATRIX : matrice de statistique sur le trafic entre couple de stations.
- ALARM : positionnement d'alarmes selon les seuils.
- EVENT : génération d'événements selon les alarmes reçues.
- FILTER : positionnement des filtres de données.
- CAPTURE : capture de paquets des filtres de données.

II-3. LE PROTOCOLE SNMP :

3-1 Les fonctionnalités SNMP :

SNMP a choisi une approche originale de l'administration des réseaux car au lieu de définir un grand nombre de commande, il conçoit toutes ses opérations conformément au principe « *aller cherche et enregistre* ».[Rich 2001]

SNMP ne définit que 5 types de messages entre manager et agent. Les trois premiers messages sont expédiés du manager vers l'agent et les deux derniers de l'agent vers le manager, comme le montre la figure II-8.

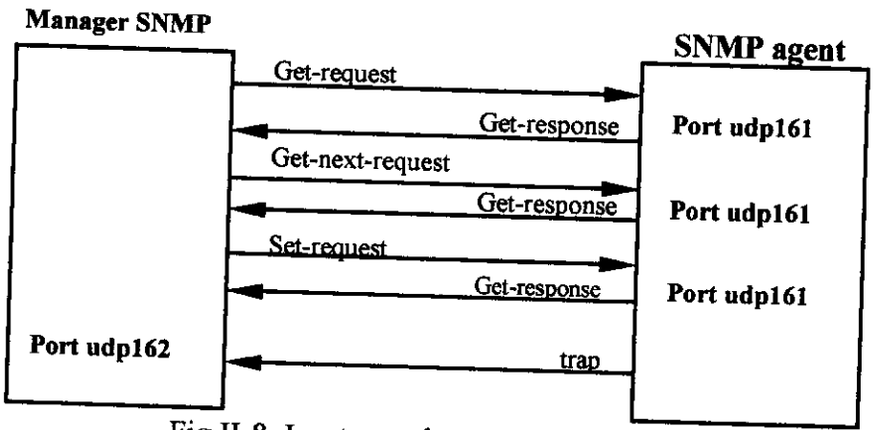


Fig II-8 :Les types de messages SNMP

get-request : permet à la station d'administration d'interroger un agent afin d'obtenir la valeur d'une ou plusieurs variables,

get_next-request : permet la lecture d'une valeur suivant une ou plusieurs autres variables d'un agent sans en connaître le nom. Elle est utilisée pour récupérer des valeurs d'instances dont on ne connaît pas l'index à priori. C'est par exemple le cas des valeurs d'objets contenus dans les tableaux. Une commande GetNext sur un objet de la MIB permet d'obtenir la valeur de l'instance suivante qui le suit dans l'ordre lexicographique des OID : Cela permet de faire un parcours récursif des objets instances dans la MIB (opération appelée« walk »).

set-request : permet de modifier la valeur d'une ou plusieurs variables d'un agent.

get-response : Renvoyer la valeur d'une ou plusieurs variables ; il s'agit d'un message retourné par l'agent au manager en réponse aux opérateurs get-request, get-next-request et set- request.

Trap : il est aussi possible pour l'agent d'envoyer un trap au manager, pour lui indiquer que quelque chose vient de se produire sur l'agent, qui doit être porté à sa connaissance. Les traps sont envoyés au port UDP 162 sur le manager.

3-2. Transport :

Puisque quatre des cinq messages SNMP sont de type demande/réponse (le manager envoie une demande, l'agent renvoie une réponse), SNMP se contente d'utiliser UDP, ceci implique qu'une requête du manager peut ne pas aboutir à l'agent, et qu'une réponse de l'agent peut ne pas revenir au manager. Le manager est chargé d'implémenter un time out et la retransmission en cas d'absence de réponse. Le manager envoie ses demandes aux agents sur le port 161 et l'agent envoie les alertes (trap) sur le port 162. Grâce à l'utilisation de ports distincts, un même système peut facilement être simultanément agent et manager.

Le choix d'un protocole non connecté est dû au fait qu'en cas de problèmes réseau (ce qui est un des cas d'utilisation d'un outil d'administration réseau), une connexion TCP a de bonnes chances d'être interrompue, alors que des datagrammes UDP parviendront à remonter des informations, même partielles.

3-3 La spécification d'un message SNMP v1 et v2 :

Le message SNMP se compose de deux parties distinctes comme le montre la figure suivante : « Les messages SNMPv1 et v2 ont le même format »

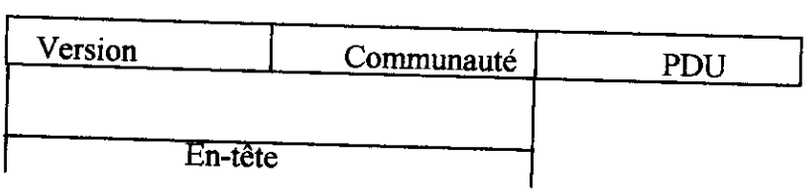


Fig II-9: format du message snmp v1 et v2

3-3-a) En-tête commune SNMP :

Elle est composée de :

• **Version :** Le champ version correspond au numéro de version SNMP, il vaut « 0 » pour SNMP-v1 et « 1 » pour SNMP-v2. Le manager et les agents doivent utiliser la même version.

• **Communauté :** SNMP définit une communauté comme étant une relation entre un agent SNMP et une ou plusieurs stations d'administration SNMP. Une communauté SNMP est caractérisée par son nom qui est une simple chaîne de caractères. Cette chaîne de caractères est appelée le « *nom de la communauté SNMP* », il désigne le mot de passe (en clair sous forme de chaîne de caractères) entre le manager et l'agent. La valeur standard est la chaîne de 6 caractères « public ».

3-3-b)PDU (protocol Data Unit):

Il y a cinq types de PDUs résumés dans le tableau suivant :

Type PDU	Nom
0	get-request
1	get-next-request
2	set-request
3	get-response
4	trap

Tab II-2 Type de PDU pour les messages SNMP

b-1) Format de PDU des requêtes de type GET et SET :

Un premier format est utilisé pour les PDU du genre GET, ou SET :

Type de PDU	ID de requête	Statut d'erreur	Index d'erreur	Obj 1, val 1

Fig II-10: La forme de PDU de genre GET ou SET

• *L'identificateur de requête(ID)* :Il est défini par le manager et retourné par l'agent dans le message get-response. Ceci permet au client (le manager) de faire le rapprochement entre la réponse du serveur (l'agent) et sa propre requête. Ceci permet en outre au manager d'émettre plusieurs requêtes vers un ou plusieurs agents, puis de trier les réponses.

• *Statut d'erreur* : Le code de statut d'erreur est retourné par l'agent qui Identifie l'erreur. Le tableau suivant résume les différentes valeurs possibles de ce champ et sa description

statut d'erreur	Nom	Description
0	NoError	tout est OK
1	TooBig	l'agent ne peut pas récupérer la réponse en un seul message
2	NosuchName	l'opération spécifie une variable non existante
3	Badvalue	une opération d'écriture spécifie une valeur ou une syntaxe invalide
4	Readonly	le manager a essayé de modifier une variable en lecture seule
5	GenErr	une autre erreur

Tab II-3 : Valeurs de statut d'erreur de SNMP

• *Index erreur* : Si une erreur se produit, l'index d'erreur et l'offset entier Spécifient quelle variable est en erreur. Il est défini par l'agent uniquement dans le cas des erreurs noSuchName, badvalue et readonly.

• *Obj/Val* :Une liste des noms de variables et leur valeur suit les requêtes get et set.

b-2)Format de PDU des requêtes TRAP :

Un second format est utilisé pour le cinquième type PDU TRAP illustre dans la figure suivante:

Type de PDU	Entreprise	Adresse Agent	Type Générique	Type Spécifique	Timestamp	Obj 1, val 1

Fig II-11 : Format de PDU Trap

• *Type de PDU* : dans ce cas toujours égale à 4.

• *Entreprise* : identifie l'entreprise de management qui a défini la Trap.

• *Adresse Agent* : adresse IP de l'agent.

• *Type Générique* : décrit quel type de problème est survenu. (7 valeurs sont possibles). Six traps spécifiques sont définis, et la septième permet à un constructeur d'implémenter un trap spécifique de l'entreprise. Le tableau II-4 décrit ces valeurs :

• *Type Spécifique* : est utilisé afin d'identifier une trap spécifique à une entreprise.

• *Timestamp* : contient la valeur de l'objet sysUptime représentant le temps écoulé depuis la dernière initialisation. Il donne le temps qui s'est écoulé depuis le démarrage de l'agent (en nombre de TimeTicks - 1/100 de secondes)

• *Obj/Val* : association du nom de la variable à transmettre avec sa valeur.

Six traps spécifiques sont définis, avec un septième permettant à un constructeur d'implémenter un trap spécifique de l'entreprise. Le tableau suivant décrit les valeurs pour le champ type de traps. Ces six traps sont illustrées dans le tableau suivant. [Rich 2001]

Type	Nom	Description
0	ColdStart	L'agent est lui-même initialisé
1	WarmStart	L'agent est lui-même réinitialisé
2	linkDown	Une interface est passé de l'état haut à l'état bas. La première variable de message identifier l'interface
3	LinkUp	Une interface est passée de l'état bas à l'état haut. La première variable de message identifier l'interface
4	authentificationFailure	Le manager SNMP a émis un message de communauté invalide
5	egpNeighborLoss	Un homologue EGP est passé à l'état bas. La première variable des messages contient l'adresse IP de l'homologue
6	entrepriseSpecific	Avoir une information sur le trap

Tab II-4 Types de traps

3-4.L'encapsulation du message SNMP :

Dans ce schéma ci-dessous, on décrie la forme d'un message SNMP avec un en-tête UDP et IP. On ne précise pas la taille en octets que pour les en-têtes IP et UDP, car le codage utilisé pour les messages SNMP (ASN-I) varie en fonction du type de la variable et de sa valeur.

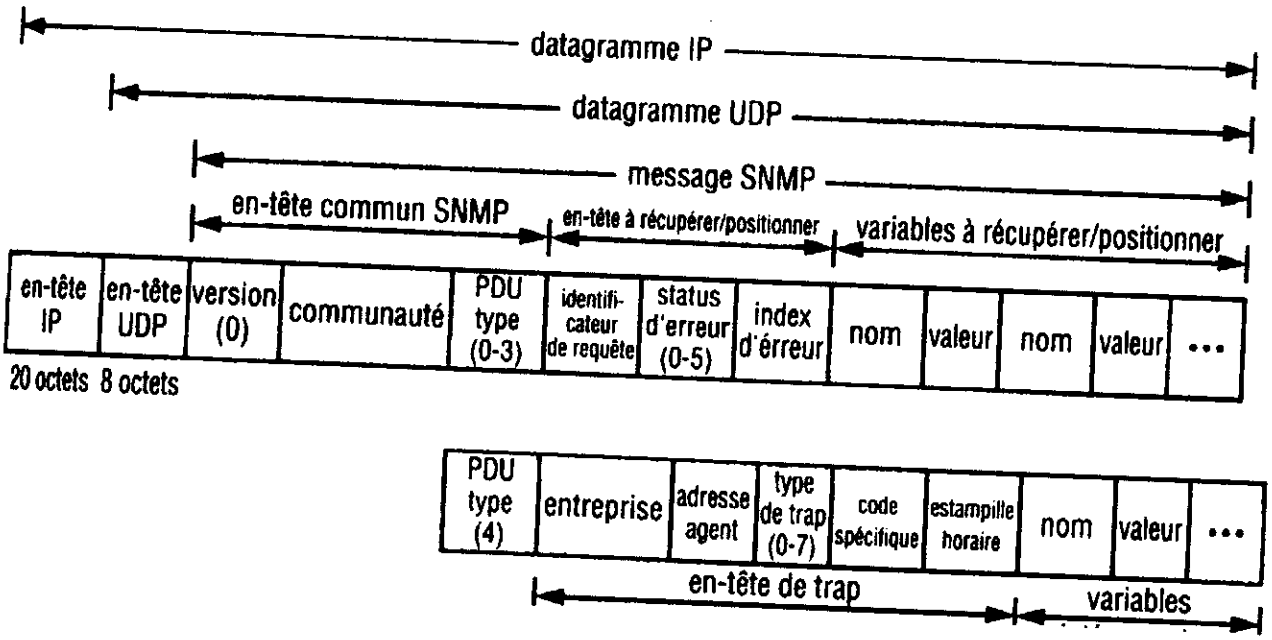


Fig II-12 : La forme des messages snmp

Les primitives sont codées en ASN-I avec le code BER (Basic Encoding Rules). Le format des PDUs (Protocol Data Unit) SNMP suit globalement un même schéma, sauf pour les Traps SNMP. Le format des messages SNMP en ASN-I est donné dans l'annexe B.

3-5.La sécurité dans SNMP v1 :

La sécurité dans le protocole SNMPv1 est basé sur deux mécanismes, l'authentification et les autorisations en utilisant le nom de communauté :[Biz 97]

3-5-a)Authentification :

L'authentification se fait de façon très simple. Le nom de la communauté est placé en clair dans le message SNMP. Si le nom de la communauté correspond à une communauté définie au niveau de l'agent, l'entité SNMP émise est considérée comme étant authentifiée comme un membre de la communauté.

3-5-b) Autorisation :

Une fois que l'entité SNMP émise est authentifiée comme un membre de la communauté, le client (noeud sur lequel se trouve l'agent) doit déterminer à quel niveau d'accès peut se placer la requête SNMP.

	Accès de l'objet selon la MIB			
Mode d'accès	**lecture seule**	**lecture/écriture**	**écriture seule**	**non accessible**
lecture seule	3	3	1	1
Lecture/écriture	3	2	4	1

Classe	**opérations autorisées**
1	aucune
2	get-request, get-next-request, set-request, trap
3	get-request, get-next-request, trap
4	get-request, get-next-request, set-request, trap

Tab II-5 : Les modes d'accès sur les objets MIB

Pour chaque objet, la communauté définit un mode d'accès qui peut être l'un des suivants:

- Lecture seulement,
- Lecture/écriture.

En faisant des intersections entre la vue des différentes communautés vis à vis des modes d'accès, on définit pour chaque objet le profil de communauté *(comunity profile)*. Ainsi, pour chaque objet, le profil de communauté définit les opérations qui sont autorisées sur cet objet.

3-6.SNMP version 2(v2) :

3-6-1. Les limitations de SNMP v1 :

Il y a quatre grandes faiblesses dans le protocole SNMP v1 : tout d'abord, c'est un protocole trop gourmand, il utilise uniquement le protocole UDP/IP, il a une sécurité faible et il ne permet pas la communication de gestionnaire à gestionnaire.

a)Protocole gourmand :

SNMP est basé sur le principe de pooling pour obtenir des informations sur le fonctionnement du réseau, ce qui fait de SNMP est un protocole " bavard ", grand consommateur de bande passante. Pour diminuer la charge, il a était rajouté à SNMP V2 de nouveaux verbes GetBulk et de nouveaux critères d'erreurs dans les messages afin d'éviter une surcharge du réseau dû à la communication trop importante entre agents et gestionnaire.[Biz 97]

b)Protocole unique (TCP/IP) :

La gestion de réseau s'adresse à des organisations qui utilisent plus d'un protocole, de ce fait, SNMP est trop restreint dans son mode de fonctionnement d'un protocole unique TCP/IP. C'est pourquoi les RFCs prenant en compte d'autre mode de transport que IP tel que RFC1418 (OSI), RFC1419 (AppleTalk Datagramm Delivery Protocol DDP) et RFC1420 (Novell's Internetwork Packet eXchange) ont été intégré dans la logique de SNMPv2.[Biz 97]

c) sécurité :

la sécurité au moment de la description de SNMP n'avait pas été prise en considération car la gestion des éléments de fonctionnement d'un réseau ne semblait pas être un élément crucial de sécurité .donc SNMP a été bâti sur logique de mot de passe (commutity name)inséré dans chaque message (malheureusement en clair).SNMP V2 remédie a cette logique et crée un concept de partie pouvant être utilisé à d'autres fins qu'uniquement sécuritaire.[Biz 97]

d) Absence de communication de type Manager à Manager : Le protocole SNMP doit son succès à sa simplicité, et celle-ci vient en partie du dialogue qui s'établit entre un manager et son agent avec un petit nombre de verbes. SNMP v2 doit dépasser cette simplicité et montrer sa possibilité d'établir des liaisons de manager e à manager, afin de montrer qu'il peut gérer des réseaux importants ne se réduisant pas à un seul et unique manager. [Biz 97]

3-6-2.Les nouveautés apportées par SNMPv2

La 2eme version de SNMP est apparue en 1993, elle apporte surtout une amélioration pour la sécurité des messages par rapport à SNMPv1. Les différences majeures entre les deux versions sont : [Del 96]

- De nouveaux types de PDUs sont ajoutés pour rendre la communication entre le manager et les agents plus efficaces et permettre la communication entre managers.
- Deux nouvelles MIB sont définies: la MIB SNMPv2 et la MIB SNMPv2-M2M (Manager To Manager).
- Avec SNMPv2 le domaine de transport ne se limite pas au modèle TCP/IP mais sur d'autres modèles comme OSI et IPX/SPX de Novell (Internet work Paquet eXchange).

• SNMPv2 fournit des améliorations pour la sécurité par rapport à SNMPv1.Avec SNMPv1, le nom de communauté passé du manager à l'agent est un mot de passe en clair. SNMPv2 gère l'authentification et la confidentialité.

• SNMPv2 a définit un nouveau mode d'administration autre que la communauté.

3-6-2-1.Les types de PDUs de SNMPv2 :

SNMPv2 garde les PDUs définit dans SNMPv1 sauf le PDU trap de SNMPv1 qui est remplacé par un nouveau PDU SNMPv2-TRAP. Donc en tous, il y a sept types de PDU dans le protocole SNMPv2,*GETRequest* ,*GETNEXT-Request,Response* ,*SetRequest* et les trois nouveaux PDUs suivants :

1. Un nouveau type de paquet **Get-Bulk-Request** permet au manager de lire un arbre complet de la MIB en une seule requête (on est limité par la taille du message), c'est à dire que cette commande remplace plusieurs GetRequest et GetNextRequest, ce qui a pour effet de supprimer de nombreux messages et donc de diminuer considérablement le volume de données transmises sur le réseau.
2. Un autre type de paquet **inform-request** permet au manager d'envoyer de l'information à un autre manager. Avec ce nouveau type de paquet SNMPv2 efface l'une des limitations de SNMPv1 en intégrant à l'intérieur de SNMPv2 une communication manager à manager avec la MIB manager to manager.
3. Un nouveau type d'alerte est définit dans SNMPv2 « **SNMPv2-Trap** ». Ce type d'alerte remplace la requête Trap de l'ancienne version, mais il garde le même format des autres PDUs ce qui simplifie l'interprétation des messages.

3-6-2-2.Les nouvelles branches ajoutées à l'arbre « Internet OID » :

Il y a eu un rajout de deux grandes branches dans l'arbre "OID" consistant en une branche spécifique à la sécurité 1.3.6.1.5 et en une autre SNMPv2 1.3.6.1.6. Sous cette dernière il y a trois sous-groupes qui s'occupent du mode de transports (Transport Domain) snmpDomain, de la gestion des proxies snmpProxys et des modules de la MIB de SNMPv2 eux-mêmes snmpModules. Il y a aussi une branche pour SNMPv2 et une autre pour la gestion de Manager à Manager (M2M) et celle des parties (partyMib).

3-6-2-3.Multi domaines de transports :

L'évolution du SNMP supportant des modèles différents (OSI, IPX/SPX) que celui du TCP/IP. SNMPv2 définit formellement l'implémentation du protocole sur ces couches de transports. Ainsi SNMPv2 a différents domaines de transports :

a)Sur UDP dans TCP/IP : Il utilise snmpUDPdomain, c'est le transport le plus classique, il permet une certaine forme de compatibilité avec SNMPv1. La deuxième version continuera à écouter sur le port UDP 161 (Get, GetNext, Response) et à annoncer sur le port UDP 162 (SNMPv2 Trap). [Biz 96]

b) Sur OSI : Les requêtes SNMPv2 utilisent un TSDU (Transport Service Data Unit) pour les Connexion Less mode Transport Service (CLTS). Mais les modes avec ou sans connexions sont possibles sur une logique OSI (CLNS Connexion Less mode Network Service) ou CONS (Connexion Oriented Network Service). [Biz 96]

c) Sur Apple Talk : Il utilise SnmpDDP domain, les messages sont envoyés à travers un Datagram Delivery Protocol (DDP) qui est utilisé avec le type 8, et l'entité SNMPv2 agit dans son rôle d'agent avec le numéro 8 de socket DDP, alors que c'est le numéro 9 qui est utilisé pour exécuter les notifications (traps). [Biz 96]

d) Sur IPX/SPX de Novell : Il utilise SnmpIPXDomain : le SNMPv2 est sérialisé dans des IPX Datagrammes, il utilise les paquets de type 4. Son rôle d'agent est à l'écoute sur les sockets IPX de numéro36869 (900FH) et envoie les notifications sur le numéro de socket IPX36880 (9010H). [Biz 96]

3-6-2-4.Sécurité :

La seule sécurité implémentée en SNMPv1 est la « community name », c'est un mot de passe en clair dans chaque message, par contre SNMPv2 a apporté plusieurs solutions contre les menaces qui sont :

Mascarade : Une entité prend l'identité d'une entité autorisée, la solution est : l'algorithme d'authentification (MD5 :Digest Authentification Protocol) qui permet d'identifier l'émetteur et d'assurer l'intégrité des messages et leur origine.

Modifications Des Informations : Une entité modifie un message en cours de route (y compris la falsification d'une valeur d'un objet) la solution est : l'algorithme d'authentification.

Modification De L'ordre Des Messages : Ça concerne le rendement, le retard ou la retransmission des messages, la solution est la synchronisation des horloges.

Divulgation Des Informations : Une entité peut observer un dialogue entre un superviseur et un agent (exemple : découverte des mots de passe suite à SetRequest sur user Password), la solution est de faire un cryptage (DES : Data *Encryption Standard* : il s'occupe du chiffrage du message pour le protéger contre la divulgation).

3-6-2-5 Le Modèle d'administration de SNMPv2:

Le modèle administratif de SNMPv2 remplace les communautés, ce qui permet d'établir les relations entre les différentes entités SNMPv2. Le coeur du modèle est le "SNMPv2 Party". C'est un concept d'environnement d'exécution restreint à un certain nombre d'actions (pour des raisons de sécurité). Chaque « SNMPv2 Party » comprend une simple et unique identité (qui sera définie par un OBJECT-IDENTIFIER), un emplacement logique dans le réseau et son type de transport. Les messages SNMPv2 sont transférés entre deux Parties, mais un agent SNMPv2 pourra définir plusieurs Party chacune ayant ses propres paramètres. [Biz 97]

Les propriétés les plus importantes d'une party sont présentées dans le tableau suivant :

propriétés	Description
PartyIdentity	une identification unique
PartyTDomain	Protocole de transport *exemple : snmpUDPDomain*
PartyAddress	L'adresse à utiliser pour envoyer un message *exemple : port UDP 161*
partyMaxMessageSize	la longueur maximum d'un message
PartyAuthProtocol	Le protocole d'authentification : noAuth
PartyAuthClock	temps local (utilisé pour la synchroniser deux parties)
PartyAuthPrivate	clé privée d'authentification
PartyAuthPublic	clé publique
PartyPrivProtocol	le protocole de confidentialité
PartyPrivPrivate	clé privée
partyPrivPublic	clé publique

Tab II.6 : Les propriétés d'une parité d'administration de SNMPv2

3-6-3.Cohabitation SNMP et SNMPv2 :

L'une des fonctions les plus importantes est la coexistence entre l'ancien SNMP et SNMPv2. Les différents éléments du réseau qui répondent aujourd'hui à SNMP, ne sont pas obligés de migrer d'un seul coup vers le nouveau protocole SNMPv2. Alors que dans les équipements qui ont SNMPv2 implémenté par le constructeur, le fonctionnement en parallèle des deux protocoles a été prévu et une technique de Proxy Agent a été élaborée pour cette cohabitation.

La fonction de PROXY au niveau du gestionnaire permet de passer d'un protocole (SNMP) à un autre (SNMPv2). Le Proxy fait la traduction d'un monde vers l'autre et le gestionnaire peut ainsi réagir en gestionnaire SNMP ou SNMPv2. De plus, la MIB-II continue à être utilisé par l'ancien protocole SNMP. Elle est aussi prise en compte par SNMPv2 qui l'a enrichie de toute une nouvelle partie de l'arbre de l'Internet OID. (1.3.6.1.6).

3-7. SNMP version 3(v3) :

La troisième version de SNMP (définie dans les RFC2570 et 2574) est apparue juste pour améliorer la deuxième version de SNMP de façon à sécuriser de bout en bout le système. Pour cela,il fallait redéfinir l'authentification et le cryptage, les autorisations et les contrôles d'accès et y adjoindre la possibilité d'administrer ces fonctions à distance.[Del 96]

La troisième version de SNMP se révèle complète et sécurisée, elle recourt à un système de chiffrement à clé privée USM (User-based Security Model) pour sécuriser la transmission des messages sur le réseau. Le sous système de sécurité met plusieurs modèles à disposition. Les requêtes sont reparties vers les générateurs et receveurs de notification et d'applications et le générateur de commandes. En plus elle interagit avec les anciennes versions du protocole.

Le standard SNMPv3 donne un cadre précis d'administration et suffisamment d'ouvertures pour permettre d'intégrer les extensions nécessaires, comme par exemple de nouveaux modèles de sécurité.

3-7-1.Format des messages SNMPv3 :

msg Version	msgID	msgMax Size	msg Flags	msg Security-Model	Paramètres de sécurité (opt)	context EngineID	context Name	PDU

Fig.II-13 spécification d'un message SNMPv3

les différents paramètres du message sont les suivants :

- *Le numéro de version* : Comme en SNMPv1 et v2, permet au dispatcher de savoir à quel sous-système du message processing envoyer le message.
- *MsgID* : C'est l'identifiant du message SNMP qui permet de corréler commandes et réponses.

• *MsgMaxSize* : Il indique la taille maximale des messages supportée par l'entité SNMP.

• *MsgFlags* : Il définit la manière dont sont supportés les messages Reports et l'authentification.

• *msgSecurityModel* : Il définit le modèle de sécurité utilisé, ce qui déterminera la signification du bloc suivant (paramètres de sécurité) et déterminera aussi si la suite du message sera cryptée.

• *contextEngineID et contextName :* Ils permettent de déterminer le contexte de la requête : En SNMPv3, à l'OID de la MIB qui identifie un objet se rajoute la notion de contexte qui permet d'avoir plusieurs instances de MIB sur une entité SNMP et qui seront identifiées par un « contexte ». Par exemple, pour un équipement implémentant deux ponts.

• *ContextName* : Il permet d'identifier la MIB du pont d'où on désire interroger.

3-7-2. Architecture du SNMPv3

3-7-2-1.SNMP entité :

Dans SNMPv3, la différenciation agent/manager s'efface au profit de la notion plus générale d'entité SNMP « snmp entity ». Cette dernière peut jouer le rôle de manager, d'agent ou les deux à la fois, en employant la terminologie SNMPv1. Ce modèle est un modèle de type peer to peer. Une entité SNMP est constituée d'un moteur (engine) et d'applications (figure II-14). [Oli 2001]

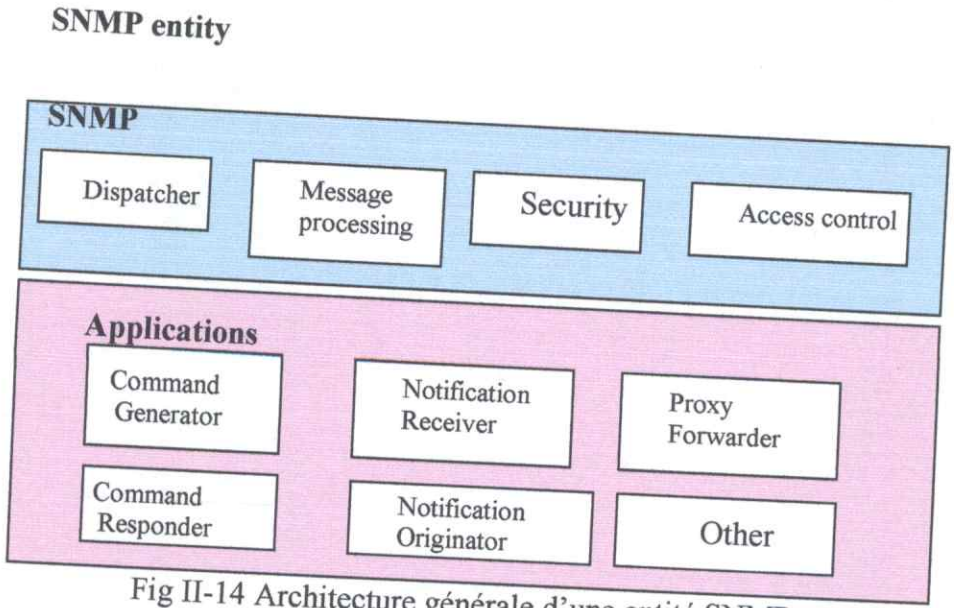


Fig II-14 Architecture générale d'une entité SNMP

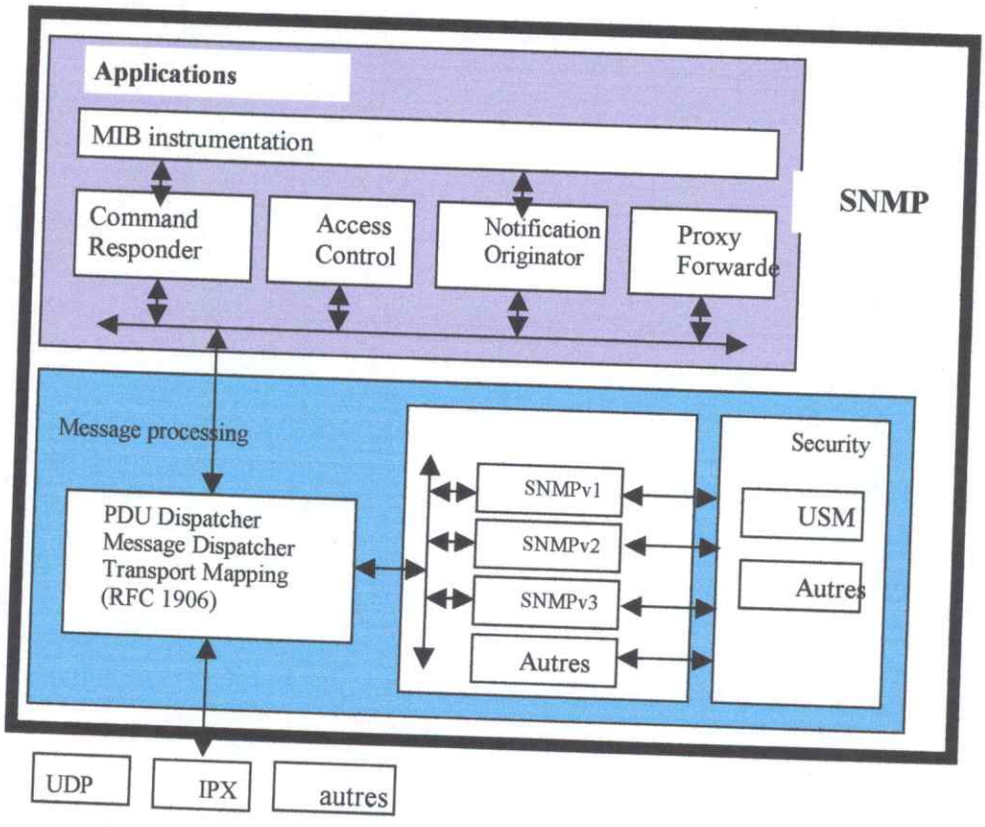


Fig II-15 : L'agent SNMP de la version 3

3-7-2-2.SNMP Engine (moteur SNMP) :

Le moteur assure la technique du travail .il est composé de plusieurs Modules :

a)Le dispatcher (Transporteur) :

Il pointe les messages qui arrivent du réseau vers le bloc de traitement des messages qui sera capable de les traiter (par exemple le sous-système SNMPv1 ou SNMPv3 du module message processing). Inversement, il redirige les messages en provenance de ce module vers le réseau, encapsulé dans le protocole adéquat (par exemple, UDP/IP ou IPX).

Le message « processing » s'occupe du décodage et de l'assemblage des Messages. Des sous-systèmes gèrent les différents types de messages utilisables par l'entité (SNMPV1, SNMPV2, SNMPV3,)

b)Le module « security » :

Il traite de la sécurité des échanges, si elle est nécessaire : c'est lui qui est chargé de traiter la confidentialité des communications et l'authentification du correspondant. Plusieurs protocoles sont définis et utilisables et l'architecture SNMPv3 est extensible de manière à permettre l'utilisation d'autres modèles de sécurité que ceux prévus à l'origine USM (User- based Security Model) est le modèle de sécurité de SNMPv3 qui répond de manière complète aux problèmes, alors que le Community-based Security Model utilisé par SNMPv1 et v2 est plus qu'élémentaire).

c)Le module contrôle d'accès « Access control» :

Il traite le contrôle d'accès aux ressources par l'entité SNMP en fonction des prérogatives accordées. Un modèle est défini dans SNMPv3 : VACM (View-based Access Control Model) qui permet de définir des vues sur la MIB, vues sur lesquelles les opérations SNMP pourront être limitées. Par exemple, il sera possible d'accéder à des tables de configuration en lecture mais pas en écriture, ou encore il ne sera pas possible du tout d'accéder, même en lecture, à certaines parties de la MIB. Le module de MIB VACM permet de configurer ce contrôle de manière fine mais complexe.

3-7-3. Sécurité dans SNMP v3 :

C'est le principale progrès de SNMPv3 : SNMPv1 et SNMPv2 offrent un modèle de sécurité réseau à base des noms de communauté, qui n'assure que l'authentification. Par ailleurs, il est très facile de le détourner puisque les noms de communauté circulent en clair sur le réseau. Ce modèle reste une option dans SNMPv3.

Un modèle complet est proposé avec USM (User-based Security Model). Ce dernier s'appuie sur les protocoles HMAC-MD5-96 (basé sur MD5) et HMAC-SHA-96 (basé sur SHA) pour l'authentification et CBC-DBS (cryptage symétrique) pour la privauté, sachant que d'autres protocoles peuvent être utilisés. Ces protocoles sont basés sur un système de clés et sont configurés à l'aide d'un module de MIB. [Oli 2001]

II-4- CONCLUSION:

SNMP est le standard incontournable dans le domaine de l'administration des réseaux d'entreprise, son utilisation s'est étendue au-delà du réseau, dans le monde du système et des applications.

La version 2 de SNMP apporte de très nettes améliorations par rapport à la première version tout en essayant de rester « simple ». Cette version permet une plus grande sécurisation des données et augmente la facilité et la rapidité d'accès à la MIB. La version 2 étant compatible avec SNMP v1, l'essor de SNMP risque de s'accroître de façon plus importante. Les limitations des versions 1 et 2 sont comblées avec la version 3. Ce dernier standard demande toutefois plus de travail d'implémentation et de mise en œuvre.

Dans tous les cas, La mise en œuvre d'une administration de réseau efficace demande un travail non négligeable en terme de choix de mise en place d'outils, d'organisation, de formation et d'implication du personnel.

CHAPITRE III
LA CONCEPTION

III-1.Introduction :

Aujourd'hui, avoir un système de gestion des réseaux est devenu une obligation pour assurer le bon fonctionnement du réseau dans une entreprise, surtout avec leur taille qui ne cesse d'augmenter. Pour cela nous avons réalisé un superviseur de réseau appliqué sur le réseau de la CNAS. Ce dernier est un réseau commuté de taille assez importante.

Le réseau est très souple car les brassages des branchements sont assez fréquents afin d'accroître les performances du réseau ou à cause du besoin de déplacement ou d'ajout de machine. Il devient alors très difficile de connaître l'organisation des machines. C'est pour cela que l'administrateur réseau est amené à déterminer ponctuellement sur quel nœud du réseau est branché un ordinateur, ce qui lui permettra de :

- Vérifier qu'une machine est effectivement attachée au bon VLAN. (Virtual Local Area Network).
- Localiser rapidement l'intrus lorsqu'un utilisateur connecte au réseau une machine non autorisée détectable par son adresse MAC (Media Access Control).
- Détecter rapidement si un utilisateur change l'endroit de branchement d'une machine et alerter l'administrateur.
- Avertir l'administrateur du réseau si un équipement a un comportement Défectueux.
- Déterminer les machines responsables du trafic excessif quand certaines branches du réseau sont saturées.

Le besoin fonctionnel essentiel est donc l'établissement de la topologie qui constitue la base du logiciel. Elle doit être mise à jours régulièrement selon un intervalle de temps spécifié et mettre en évidence les correspondances entre les équipements du réseau et les ports du branchement.

On complète la topologie par des informations caractéristiques du réseau :

- La récupération du mode de fonctionnement des différentes interfaces réseau car ces renseignements permettront aux administrateurs d'identifier les causes des performances bien inférieures à celles attendues.
- La récupération des statistiques sur le trafic d'une interface donnée; le débit, le nombre de paquets reçus ou envoyés, ...etc.
- L'administrateur peut explorer la MIB d'un équipement.

Dans notre travail nous avons choisi de faire une conception et une implémentation objet vue que la programmation orientée objet permet une bonne représentation du monde réel et surtout qu'elle facilite la réutilisation des codes. Nous avons utilisé le langage de modélisation UML (Unified modeling language) qui permet la modélisation objet.

III-2.Architecture :

2-1-Architecture logicielle :

Notre système de supervision est composé de trois paquages comme le montre la figure ci-dessous:

- Un manager qui interroge les agents du superviseur.
- Les agents SNMP.
- Une persistance qui permet la sauvegarde sur disque l'état du superviseur et du réseau.

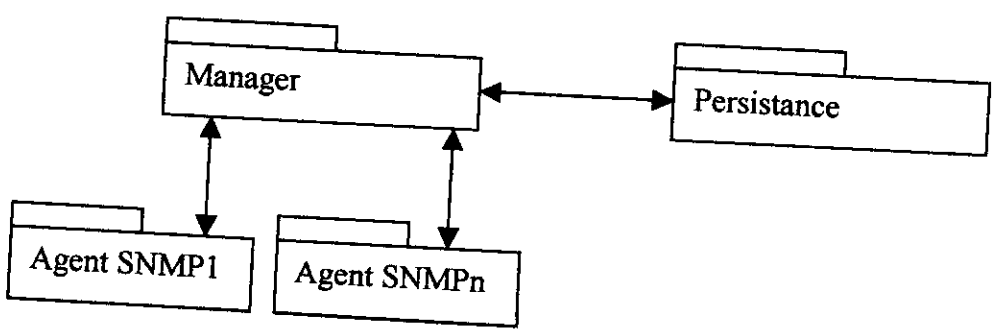
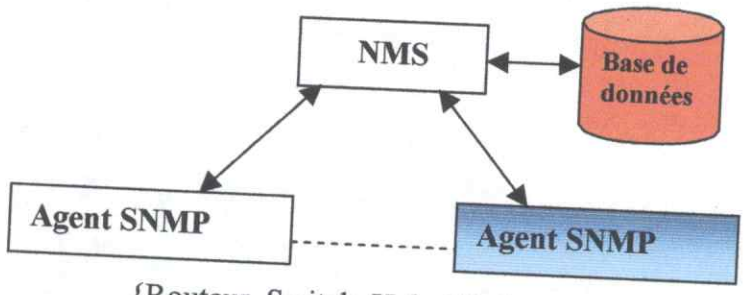


Fig III-1 Architecture logicielle du superviseur

2-2-Architecture matérielle :

Le système de supervision doit être déployé comme suit :

1. La station NMS (Network Management Station) contient le manager, elle est connectée au réseau local à un port qui appartient à tous les VLANs.
2. Agent SNMP : L'agent SNMP est installé sur chaque équipement du réseau par les constructeurs sinon c'est à l'administrateur de l'activer et le configurer.



{Routeur, Switch, Hub, PC, Imprimante…}

Fig III-2 Déploiement de superviseur réseau

III-3.Quelques notions sur UML:

3-1.Définition du UML :

U.M.L est un langage unifié de la modélisation objet. Il est le résultat d'un long processus initialisé par trois grands méthodistes Grady Booch, Ivar Jacobson et Jim Rumbaugh. Sa notation est un formalisme issu de la fusion de la notation de Booch, d'OMT (Object Modeling Technique) et OOSE (Object Oriented Software Enginneering) et les concepteurs de l'UML l'ont conçue pour être lisible sur des supports très variés et simples.

UML s'est très rapidement imposée à la fois auprès des utilisateurs et sur le terrain de normalisation. [Pie97]

Le langage UML se concentre sur la description du développement de logiciel plutôt que sur la formation du processus de développement lui-même. Il peut ainsi être utilisé pour décrire les éléments du logiciel obtenu par l'application de différents processus de développement. UML n'est pas une notation fermée, il est générique, extensible et configurable par l'utilisateur. UML ne recherche pas la spécification à outrance; il n'y a pas une représentation graphique pour tous les concepts imaginables ; en cas de besoin particuliers des précisions peuvent être apportés au moyen de mécanismes d'extension et de commentaires textuels.

Une grande liberté est donnée aux outils pour le filtrage et la visualisation d'information. L'usage de couleurs, de dessins et d'attributs graphiques particuliers sont laissés à la discrétion de l'utilisateur. [Pie97]

3-2.Les diagrammes d'UML :

Un diagramme donne à l'utilisateur un moyen de visualiser et de manipuler des éléments de modélisation. UML définit neuf sortes de diagrammes pour représenter les points de vues de modélisation. L'ordre de présentation de ces différents diagrammes ne reflète pas un ordre de mise en oeuvre dans un projet mais simplement une démarche pédagogique.

Les diagrammes peuvent montrer tous ou une partie des caractéristiques des éléments de modélisation, selon le niveau de détail utile dans le contexte d'un diagramme donné. [Pie97] Voici les différents diagrammes d'UML :

1. **Les diagrammes d'activités** qui représentent le comportement d'une opération en termes d'actions.
2. **Les diagrammes de cas d'utilisation** qui représentent les fonctions du système du point de vue de l'utilisateur.
3. **Les diagrammes de classes** qui représentent la structure statique en termes de classes et de relations.
4. **Les diagrammes de collaboration** qui sont une représentation spatiale des objets, des liens et des interactions.
5. **Les diagrammes de composants** qui représentent les composants physiques d'une application.
6. **Les diagrammes de déploiement** qui représentent le déploiement des composants sur les dispositifs matériels.
7. **Les diagrammes d'états transitions** qui représentent le comportement d'une classe en termes d'états.
8. **Les diagrammes d'objets** qui représentent les objets et leurs relations et qui correspondent à des diagrammes de collaboration simplifiés, sans représentation des envois de messages.
9. **Les diagrammes de séquence** qui sont une représentation temporelle des objets et de leurs interactions. [pie97]

Dans notre conception, nous n'avons utilisé que le diagramme de cas d'utilisation, le diagramme de collaboration et le diagramme des classes. Nous pensons que ces trois diagrammes sont suffisants pour établir une description et une conception détaillée du superviseur réseau.

III-4 Le diagramme des cas d'utilisation:

4-1.Détermination des cas d'utilisation :

Avant de déterminer les cas d'utilisation, il faut tout d'abord déterminer les acteurs qui interviennent dans le système.

Un acteur représente un rôle joué par une personne ou une chose qui interagit avec le système. [pie97]

Dans le système de supervision de réseau il y a deux acteurs :

- Administrateur : c'est un acteur manipulant le superviseur en effectuant des opérations sur les agents existant dans le réseau.
- Agent : tout équipement existant dans le réseau local (LAN) supportant la pile TCP/IP et intègre l'agent SNMP. Il peut être soit un serveur, une station de travail, une imprimante, un switch, hub ou un routeur.

Après la définition des différents acteurs de superviseur, on détermine leurs cas d'utilisation.

Un cas d'utilisation est un comportement du système en réponse à une interaction d'un acteur, on peut associer à chaque acteur un ou plusieurs cas d'utilisations.

Dans notre étude, Nous avons repéré les cas d'utilisations cités dans le tableau Suivant :

Acteur	Cas d'utilisation
Administrateur	o Configuration du superviseur. • Configuration du protocole SNMP. • Configuration de la plage d'adresses. o Détection des machines du réseau. o Détecter la topologie. o Explorer une MIB d'un équipement. o Modifier les propriétés d'un agent. o Enregistrer les nouveaux agents. o Supprimer un agent. o Compléter la topologie manuellement. o Lancer un PING sur une plage adresse IP. o Faire des statistiques.
Agent	o Répondre aux requêtes envoyées par le manager

Tab III-1 Les cas d'utilisations

La figure III-3 montre le diagramme des cas d'utilisation du superviseur réseau.

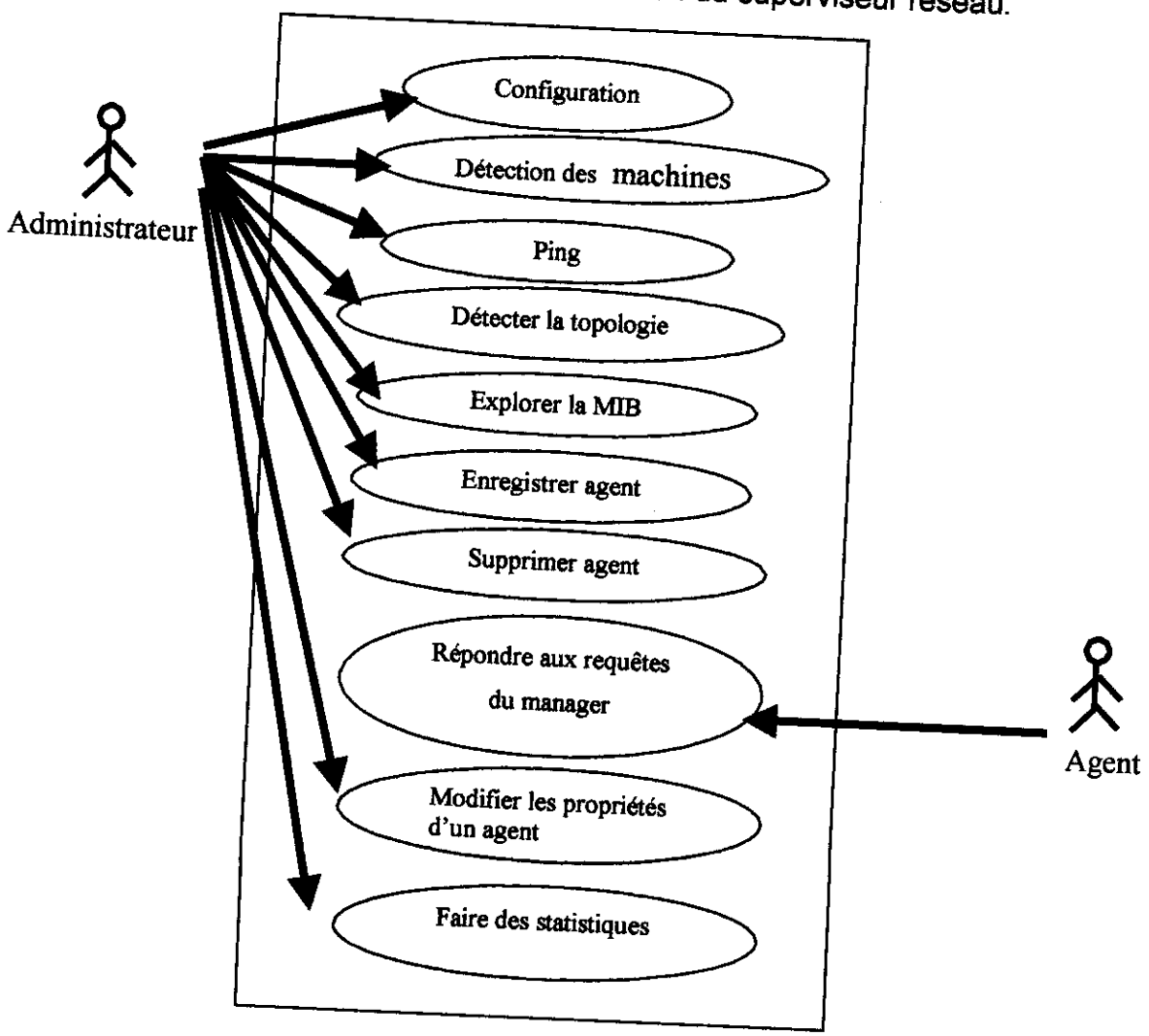


Fig III-3 Diagramme des cas d'utilisation du superviseur

4-2.Descriptions des cas d'utilisation :

4-2-1.configuration du superviseur :

a)configuration du protocole SNMP :

Dans ce cas d'utilisation s'executent les actions suivantes :

- L'administrateur lance l'operation de configuration de SNMP.
- Le systeme lit le fichier de configuration du superviseur.
- Le système lui repond par une interface de saisie avec les paramètres par defaut de la configuration.
- L'administrateur valide les paramétres par défaut ou les modifis
- Le sytéme enregistre les paramétres validés par l'administrateur.

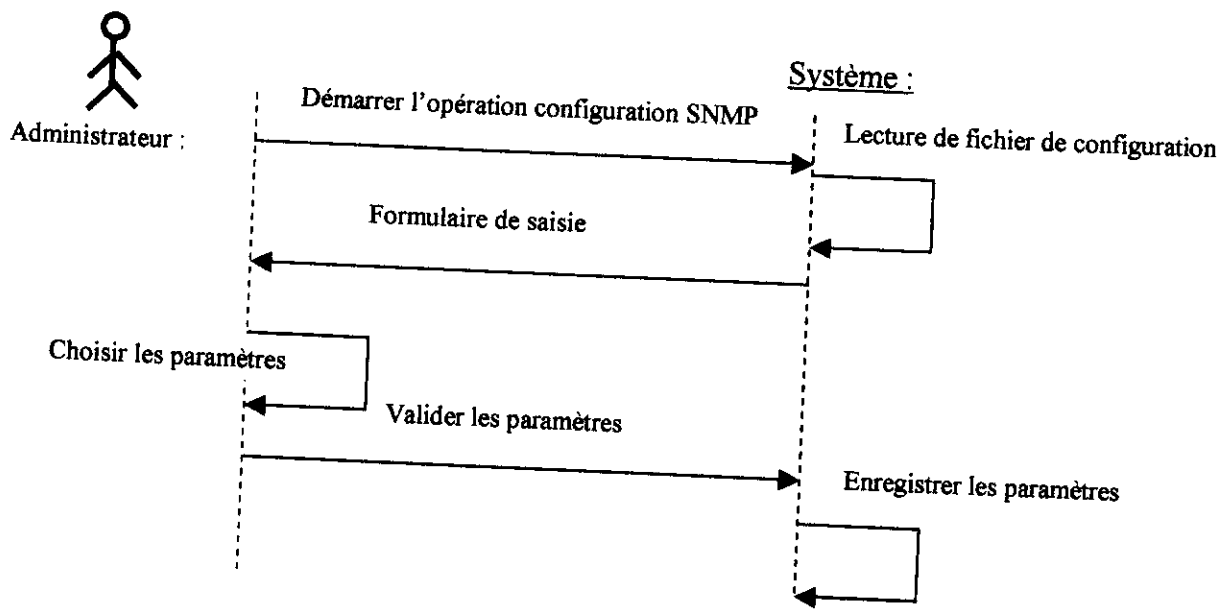


Fig III-4 Cas d'utilisation « configuration SNMP »

b) configuration de la plage d'adresses:

Ce cas d'utilisation comporte les actions suivantes :

- L'administrateur lance l'opération de modification de la plage d'adresses.
- Le système lit le fichier de configuration du superviseur.
- Le système lui répond par un formulaire de saisie dans lequel il y a la plage d'adresses utilisée.
- L'administrateur saisis la plage d'adresses.
- Le système contrôle les adresses saisies et enregistre la nouvelle plage d'adresses.

Le déroulement de ce cas d'utilisation est représenté dans la figure suivante :

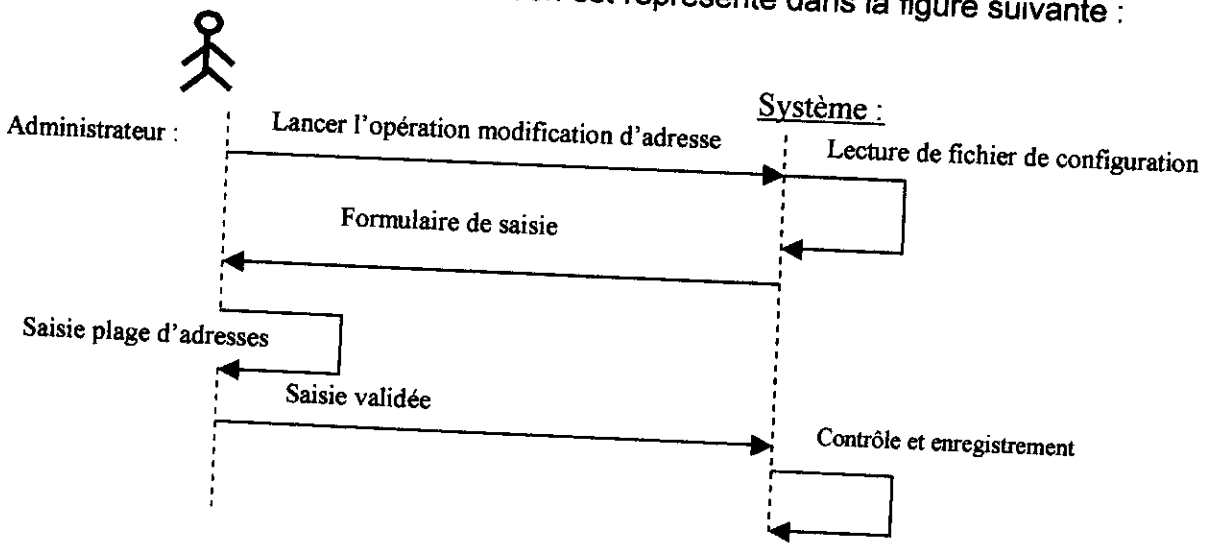


Fig III-5 Cas d'utilisation « configuration plage »

4-2-2) Détection des machines du réseau :

Ce cas d'utilisation comporte les actions suivantes :

- L'administrateur lance la détection des machines du réseau.
- Le système répond par une interface qui indique l'état d'avancement de l'opération.
- L'administrateur peut à n'importe quel moment interrompre cette opération.
- Le système envoie des requêtes Ping (ICMP)à chaque adresse de la plage d'adresses IP et il attend la réponse. S'il y a une réponse alors il sauvegarde l'adresse IP et quelques informations sur l'agent.
- Le système affiche une interface qui représente le résultat de la détection. La figure ci-dessous illustre le déroulement de ce cas d'utilisation.

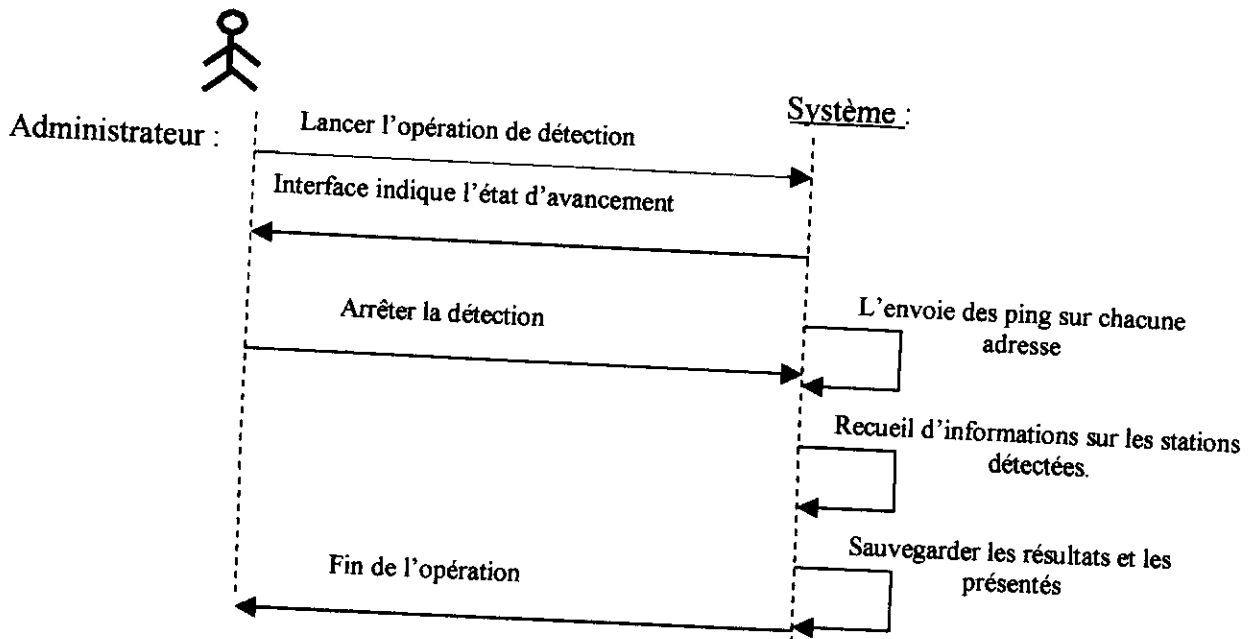


Fig III-6 Cas d'utilisation « Détection des machines »

4-2-3) Exploration de la MIB d'un agent :

Dans ce cas d'utilisation, il se déroule les actions suivantes :

- L'administrateur lance l'explorateur de la MIB.
- Le système lui répond par une interface de saisie.
- L'administrateur sélectionne l'adresse IP ou le nom de l'agent qu'il veut interroger.
- Le système lui répond en activant les zones de saisie pour sélectionner le groupe et la table qu'il veut l'interroger.
- L'administrateur envoie sa requête.
- Le système analyse la requête et l'envoyer à l'agent.
- L'agent reçoit la requête s'il n'y a pas d'erreur.
- L'agent traite et vérifie la requête.
- L'agent renvoie la réponse au système.
- Le système reçoit la réponse et l'affiche.

La figure ci-dessous illustre le déroulement de ce cas d'utilisation.

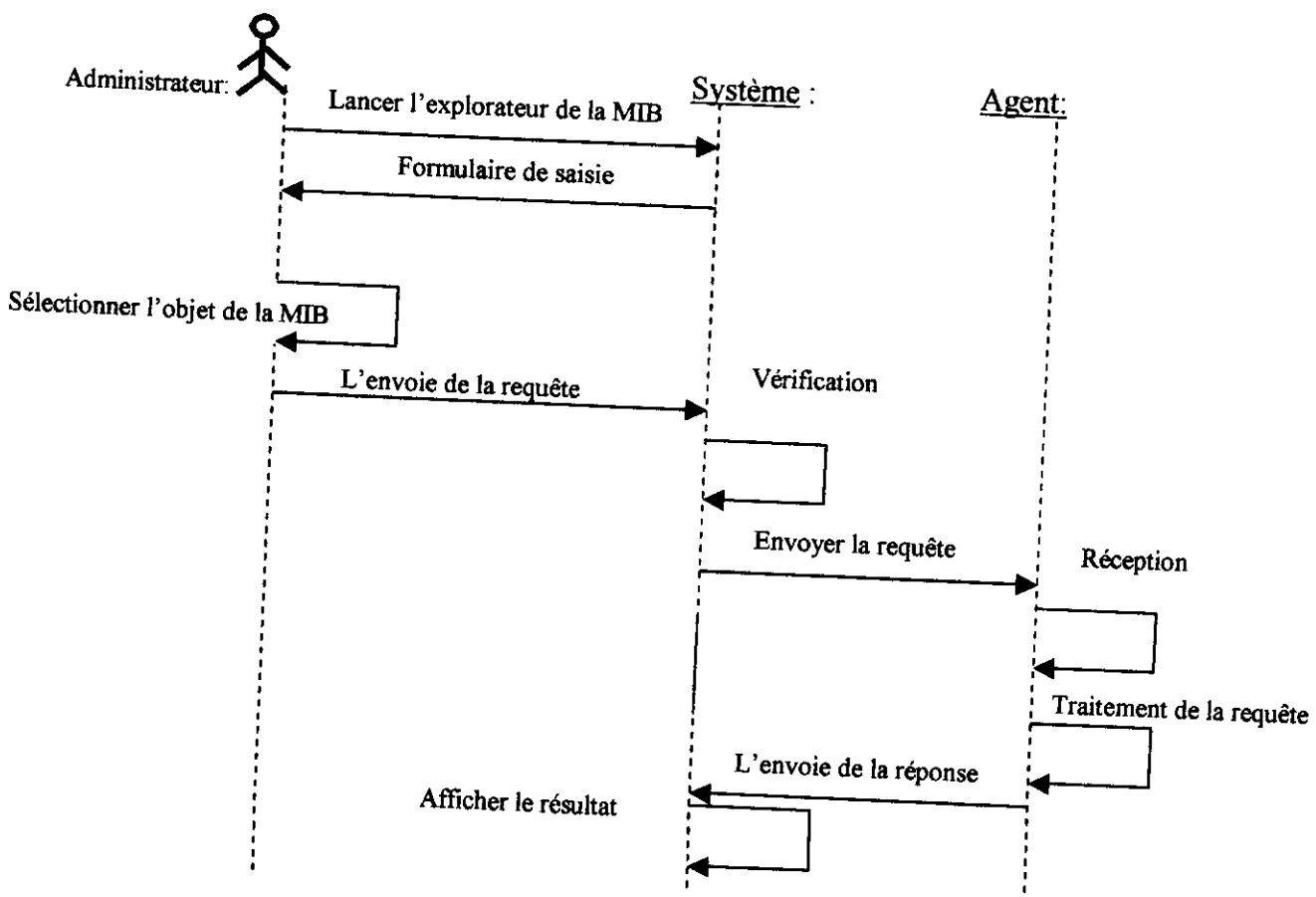


Fig III-7 Cas d'utilisation « Exploration de la MIB »

4-2-4) l'enregistrement des nouveaux agents :

Ce cas d'utilisation comporte les actions suivantes :

- L'administrateur lance l'opération de sauvegarde des nouveaux agents.
- Le système vérifie s'il y a des nouveaux agents, si oui alors le système met à jour ces données en sauvegardant les nouveaux agents, sinon il envoie un message d'information à l'administrateur.

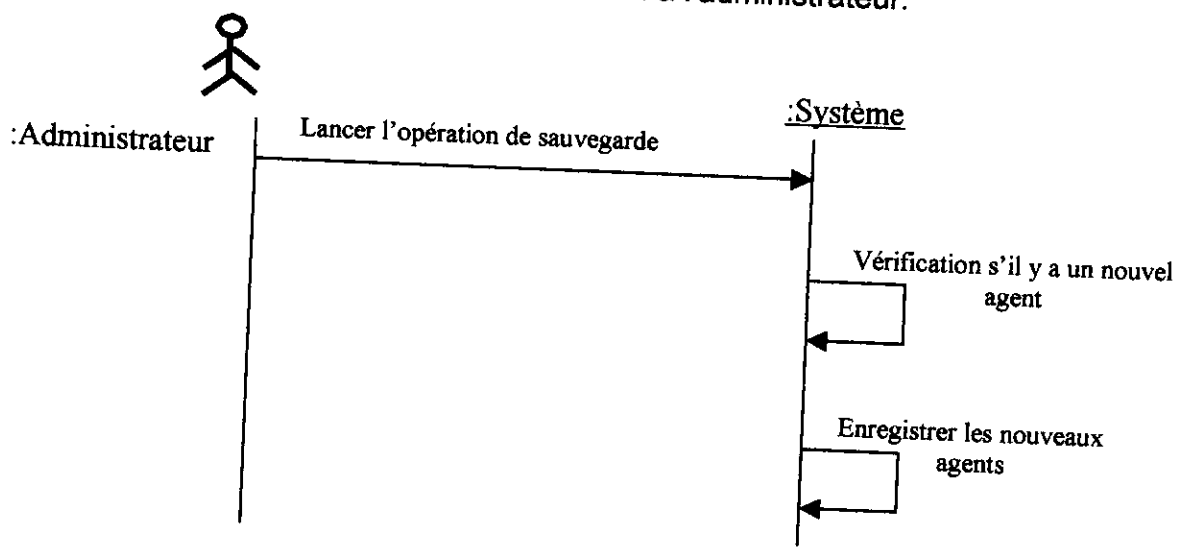


Fig III-8 Cas d'utilisation «enregistrement de l'agent avec succès

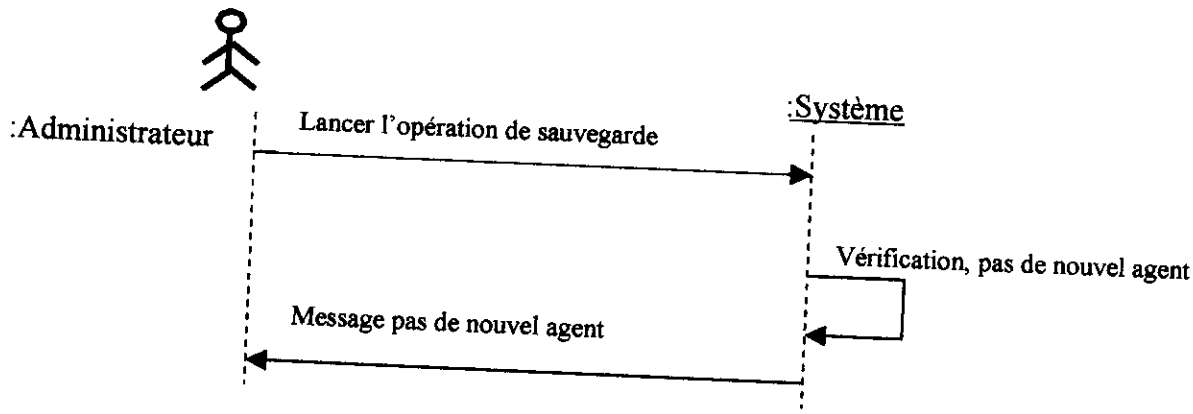


Fig III-9 Cas d'utilisation « enregistrement de l'agent non réalisé

4-2-5) Suppression d'agent :

Dans ce cas d'utilisation, il s'exécute les actions suivantes :

- L'administrateur sélectionne l'agent à supprimer.
- L'administrateur lance l'opération de la suppression de l'agent sélectionné.
- Le système lui répond par un message de confirmation.
- L'administrateur confirme ou annule la suppression.

- Si l'administrateur confirme l'opération, le système supprime l'agent de
- la base et met à jour la cartographie.

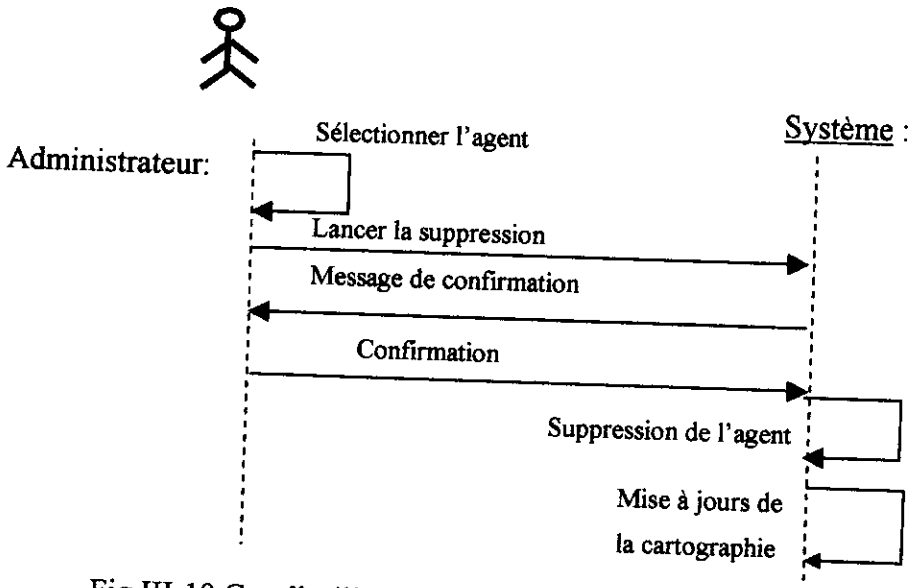


Fig III-10 Cas d'utilisation « suppression d'un agent avec succès»

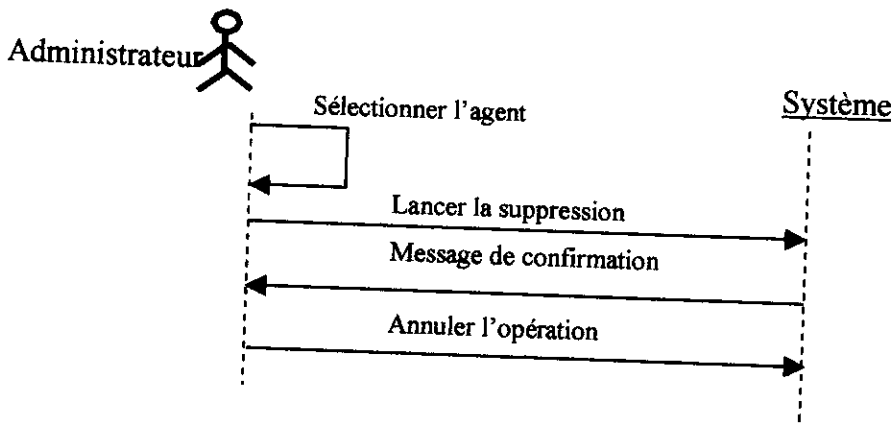


Fig III-11 Cas d'utilisation « suppression annulée »

4-2-6) Détection de la topologie du réseau :

Il s'agit de la découverte du réseau :
Dans ce cas d'utilisation, il se déroule les actions suivantes :

- L'administrateur lance la détection de la topologie.
- Le système lui repond par une interface de l'état d'avancement.
- Le système recherche les Switchs dans la liste des agents et il va les sauvegarder dans une liste de Switch.
- Le système lance des requêtes à chaque Switch pour obtenir la liste des hosts connectés à ce Switch .

- Le Switch traite la requête et envoie la réponse au système .
- Le système reçoit la réponse du switch, traite les informations et il les sauvegarde.
- Le système envoie une fenêtre dont laquelle il demande à l'administrateur de choisir un switch comme étant une racine de la topologie.
- L'administrateur choisi la racine de la topologie.
- Le système sauvegarde le choix de l'administrateur.
- Le système envoie une fenêtre dans laquelle il dessine la topologie détectée. La figure suivante décrit ce cas d'utilisation :

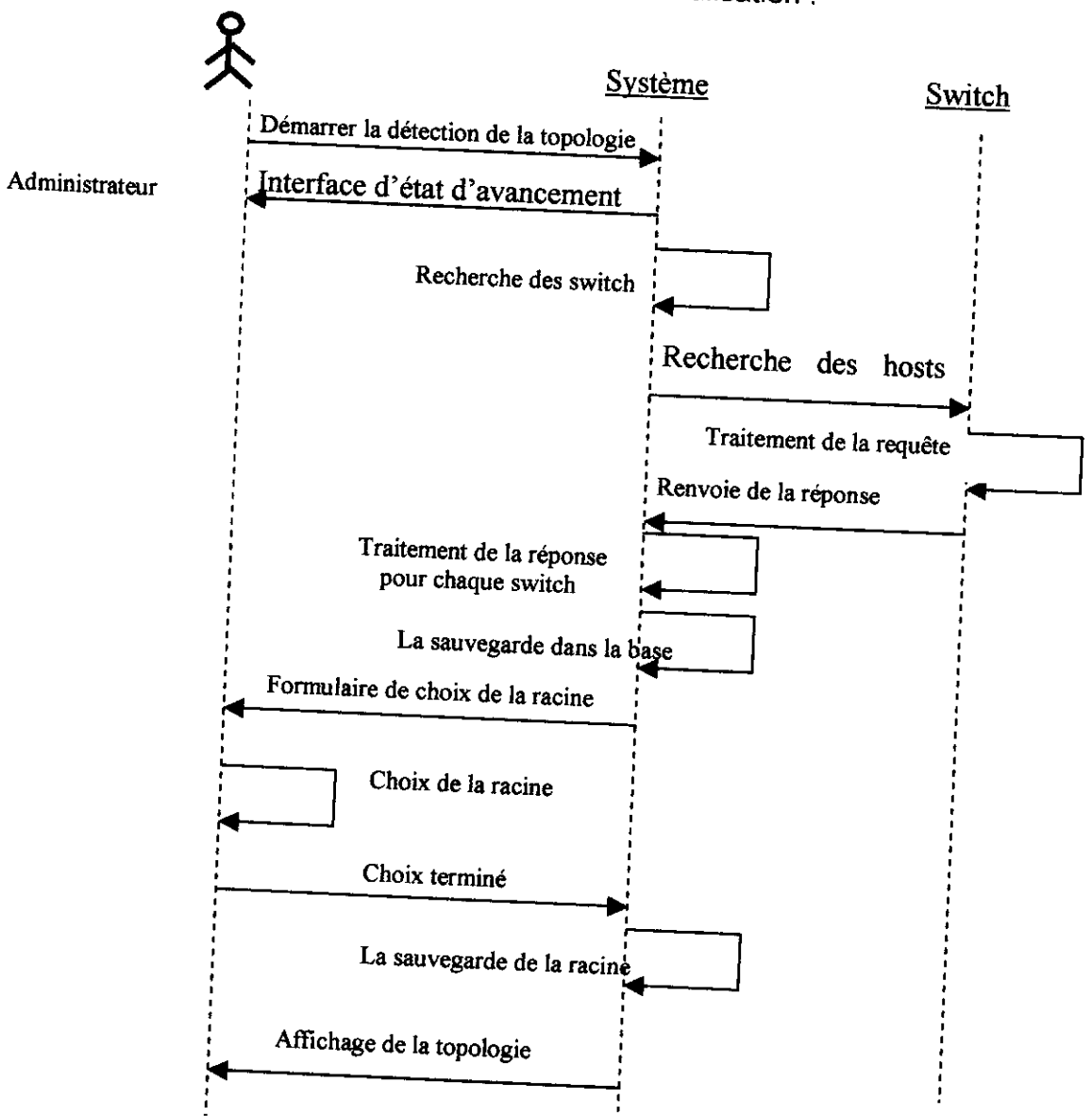


Fig III-12 Cas d'utilisation « détection de topologie »

4-2-7) modification de la topologie manuellement :

Ce cas d'utilisation se déroule lorsque l'administrateur veut ajouter un élément dans la topologie manuellement sans faire une détection automatique ou lorsqu'elle n'est pas complète. Dans ce cas d'utilisation il s'exécute les opérations suivantes :

1. L'administrateur lance l'ajout manuel de l'élément dans la topologie.
2. Le système recherche la liste des agents non connectés et des nœuds qui ont des ports libres.
3. Le système répond par un formulaire de saisie qui concerne l'élément ajouté au nœud et à quel numéro de port.
4. L'administrateur choisi le nœud, l'agent à connecter au nœud sélectionné et le numéro de port.
5. Le système vérifie les informations saisies.
6. Le système met à jour la topologie du réseau. La figure suivante illustre ce cas d'utilisation :

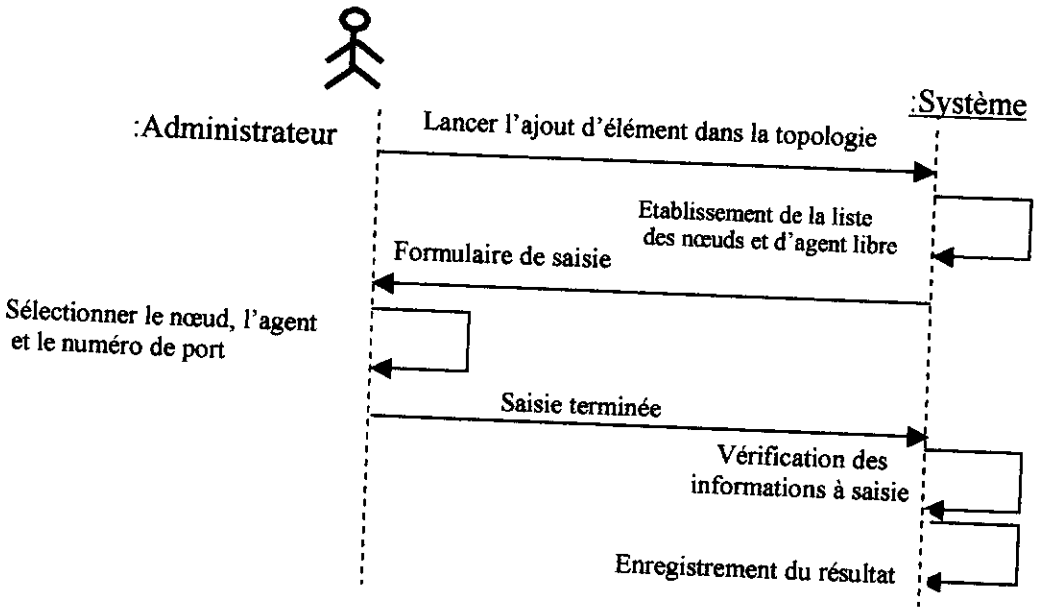


Fig III-13 Cas d'utilisation « ajout manuel dans la topologie »

4-2-8) Ping du réseau :

Dans ce cas, il se déroule les opérations suivantes :

- L'administrateur lance le ping.
- Le système lui répond par une interface de saisie.

- L'administrateur saisi les adresses IP sur lesquelles il va lancer les requêtes Ping.
- Le système vérifie les informations saisies.
- Le système envoie des requêtes PING (ICMP) pour chaque adresse.
- Le système affiche le résultat.

La figure suivante illustre ce cas d'utilisation :

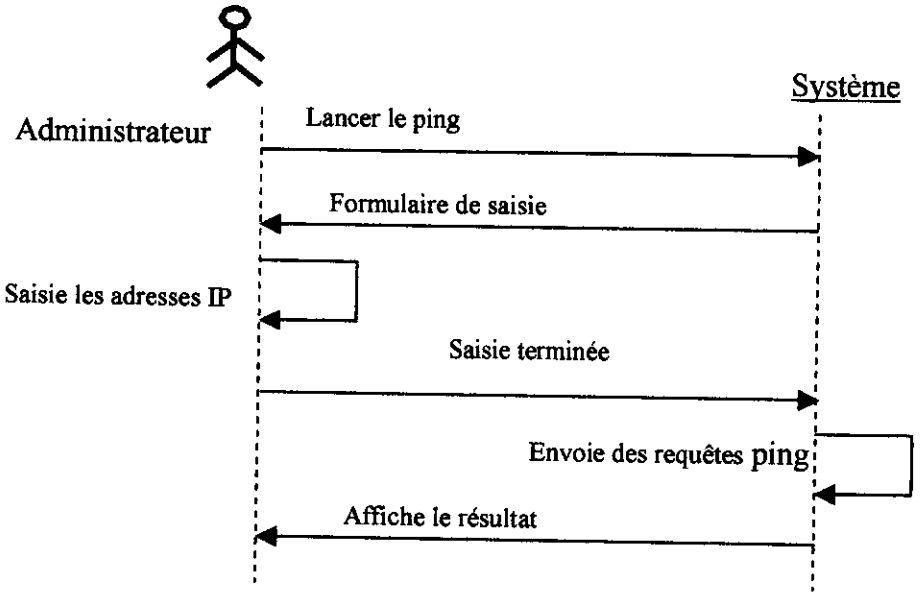


Fig.III-14 Cas d'utilisation « le Ping »

4-2-9) Répondre aux requêtes envoyées par le manager :

Ce cas d'utilisation est réalisé par l'agent SNMP lorsqu'il reçoit une requête du manager. Il contient les opérations suivantes :

- Le système ouvre une session SNMP.
- Le système construit l'entête de la requête en mettant la version du protocole, le nom de communauté et adresse de destination.
- Le système crée le PDU (Protocol Data Unit) et l'envoyé à l'agent.
- L'agent reçoit la requête.
- L'agent vérifie la version et le nom de communauté de la requête.
- L'agent vérifie le nom ou l'adresse IP source s'il est autorisé à accepter des requêtes de cette adresse.
- L'agent traite la requête reçue et crée un PDU de réponse.
  - L'agent envoie la réponse au manager.

La figure III-15 - illustre ce cas d'utilisation :

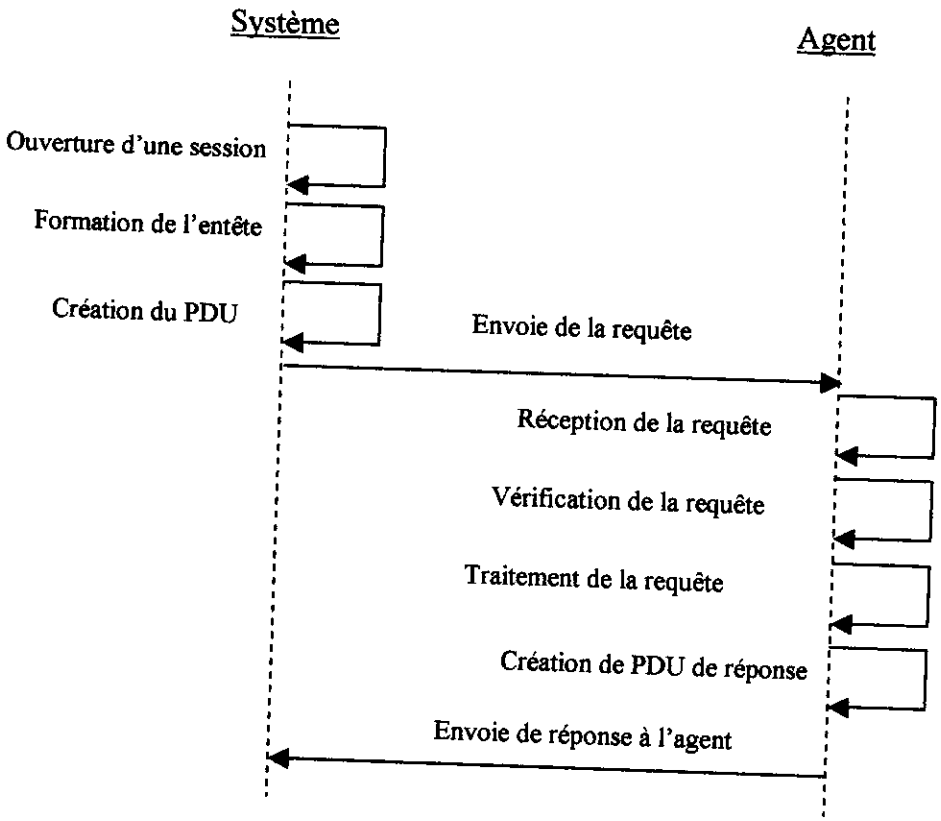


Fig.III-15 Cas d'utilisation «répondre à une requête du manager»

4-2-10) Visualisation des propriétés d'un agent :

Ce cas d'utilisation s'exécute lorsque l'utilisateur veut voir les propriétés d'un agent, il comporte les actions suivantes :

- L'administrateur sélectionne un agent.
- L'administrateur demande les propriétés de l'agent sélectionné.
- Le système recherche l'agent sélectionné dans la liste des agents.
- Le système répond par une fenêtre de représentation des propriétés de l'agent.

La figure III-16 illustre ce cas d'utilisation :

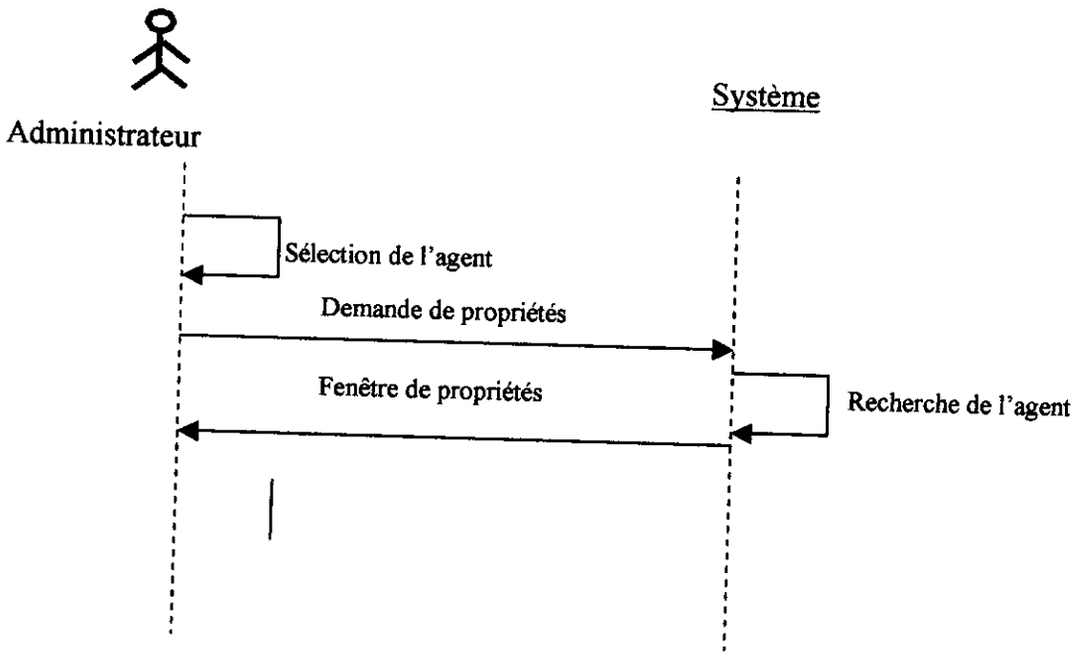


Fig.III-16 Cas d'utilisation « Visualisation des propriétés d'un agent »

4-2-11) Faire des statistiques :

Ce cas d'utilisation se déroule lorsque l'administrateur veut avoir les statistiques sur l'état du réseau. Il contient les opérations suivantes :

1. L'administrateur demande des statistiques.
2. Le système lui répond par une interface de sélection pour sélectionner la machine sur laquelle il veut faire des statistiques.
3. L'administrateur sélectionne la machine et lance la capture des données.
4. Le système fait la capture des données et les affiche sous forme de graphe.

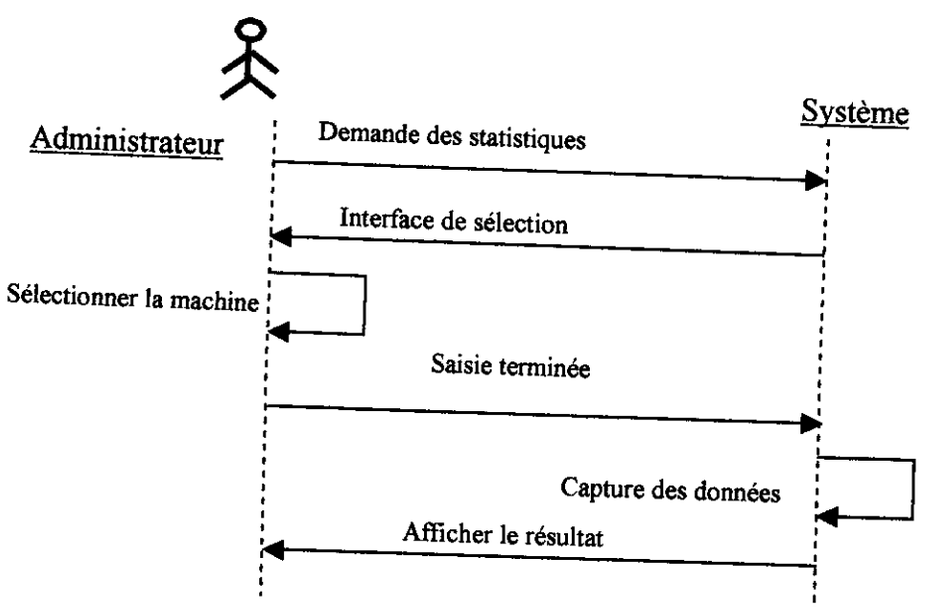


Fig.III-17 Cas d'utilisation « Faire des statistiques »

III-5. Description des collaborations:

Les différents cas d'utilisation sont réalisés par la collaboration des objets du domaine, la réalisation des cas d'utilisation fait intervenir aussi des objets supplémentaires qui n'appartiennent pas au domaine d'application mais qu'ils sont nécessaires à son fonctionnement. Ces objets ajoutés assurent en générale l'interface entre le système et ses acteurs. [Pie97]

Les interfaces utilisateur peuvent être décrites au moyen des classes qui représentent les différentes fenêtres.

5-1. Modification de configuration de SNMP :

Ce cas d'utilisation est déclanché lorsque l'administrateur veut modifier la configuration du protocole SNMP, il se réalise par la collaboration des objets instance des classes suivants : Document-configuration, Modifie-configuration. Ce cas d'utilisation commence par la lecture de fichier de configuration et se termine par la mise à jours de ce fichier.

La figure III-18 montre la collaboration des objets pour la réalisation de ce cas d'utilisation.

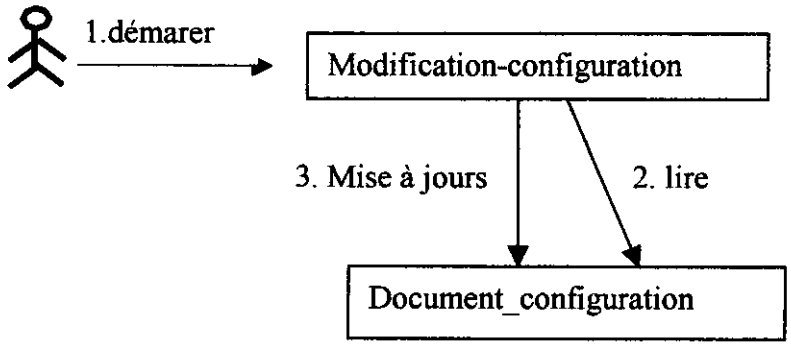


Fig III-18 Collaboration des objets « modification de la configuration SNMP »

5-2. Modification de la plage d'adresses :

Ce cas d'utilisation se réalise via la collaboration des objets instances des deux classes, Modification-d'adresse et Document_configuration. Le résultat de ce cas d'utilisation se termine par la mise à jours du fichier de configuration.

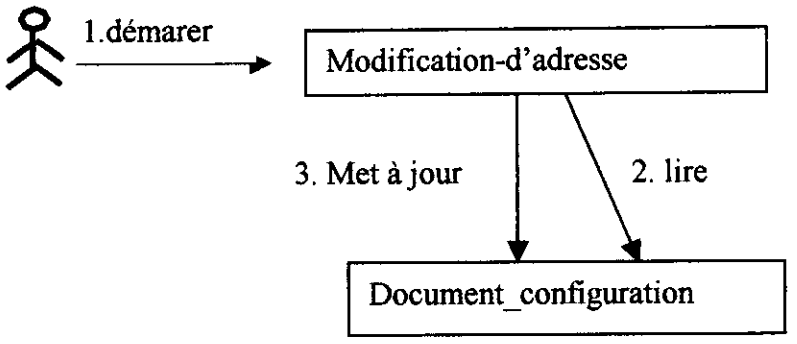


Fig III-19 Collaboration des objets « modification de la plage d'adresse »

La figure III-20 représente un diagramme de classe préliminaire selon les deux collaborations des objets précédentes.

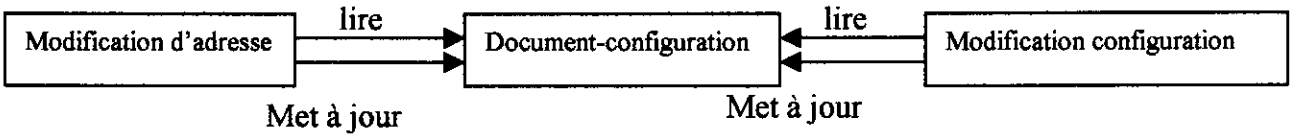


Fig III-20 : diagramme de classe : Modification plage d'adresse et configuration SNMP

5-3. Détection des machines du réseau :

Ce cas d'utilisation permet à l'administrateur de détecter les machines qui existent dans le réseau et d'extraire les informations nécessaires. Il commence par la création des threads de ping pour chaque adresse et il se termine par une création de la liste des agents. Ce cas d'utilisation se réalise par la collaboration des objets instances des classes suivantes : Thread- scan, Lancer_Détection, Agent, Liste-agent, Fenêtre-liste-agent et Requete_SNMP.

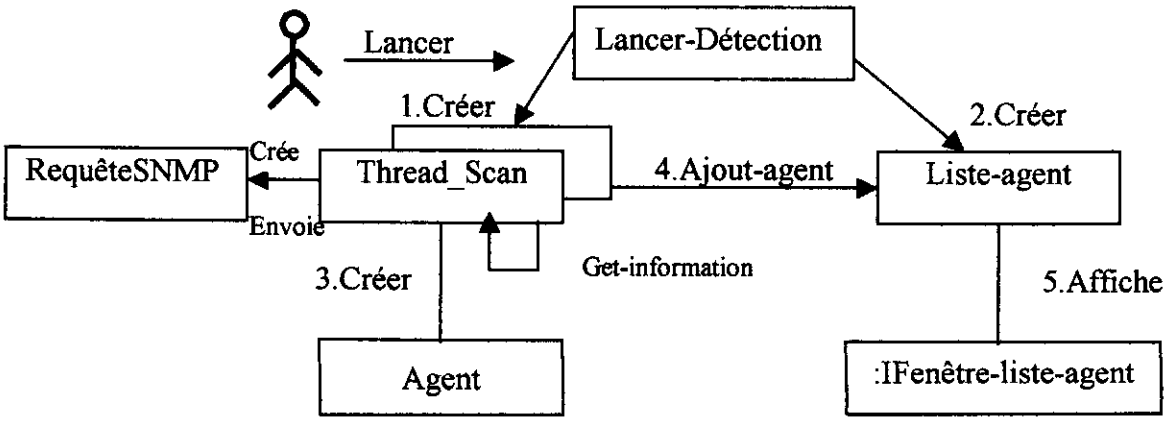


Fig III-21 Collaboration des objets « Détection des machines du réseau »

Le comportement de la procedure Get-Information est expliqué dans la figure III-22 :

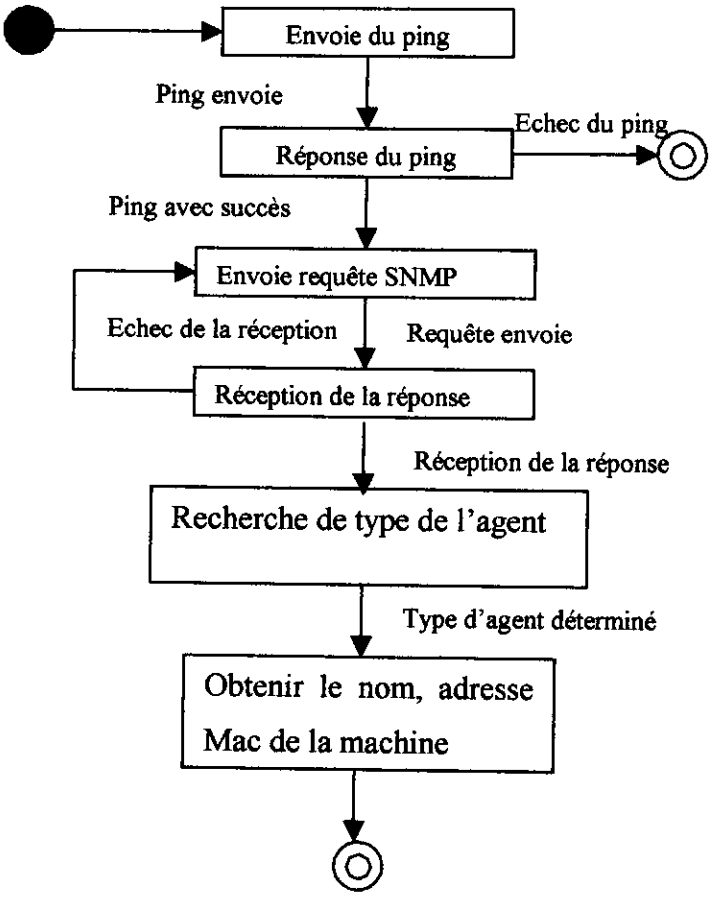


Fig III-22 comportement de la procédure get-information

La figure III-23 illustre le diagramme de classe issu de la collaboration d'objets précédente .

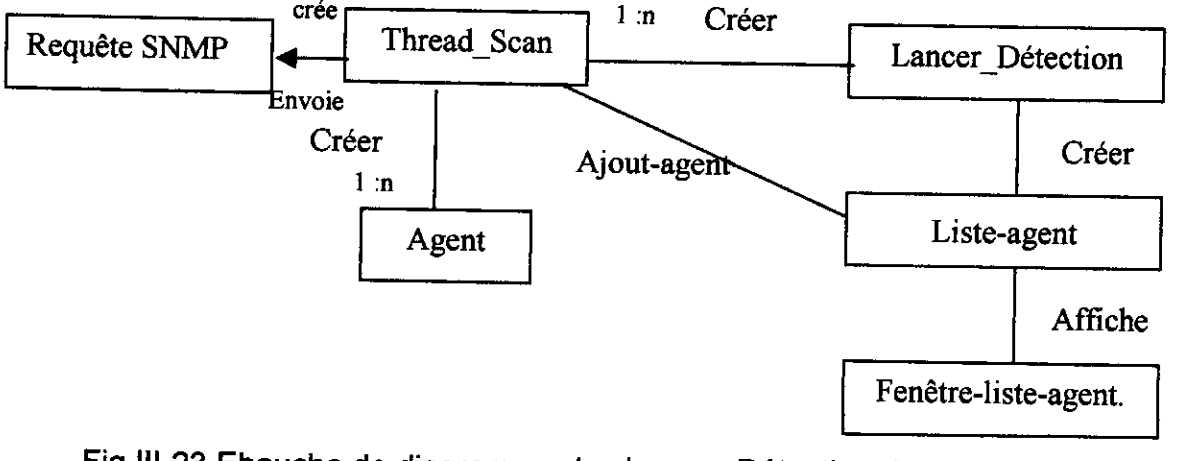
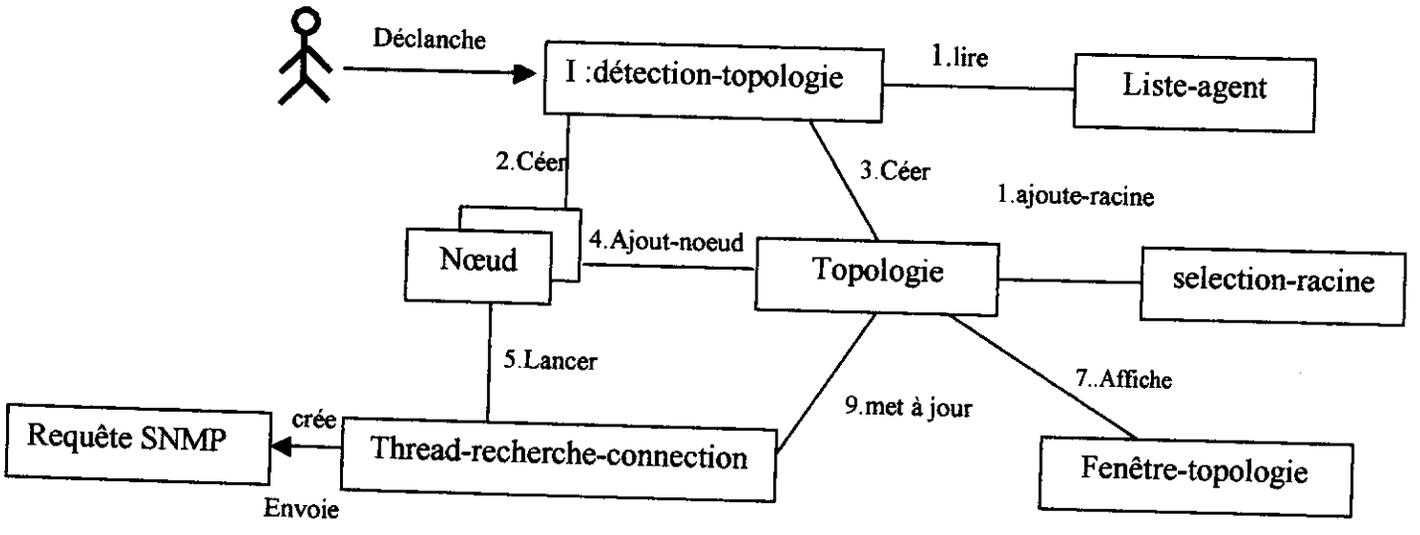


Fig III-23 Ebauche de diagramme de classe « Détection des machines »

5-4.La détection de la topologie :

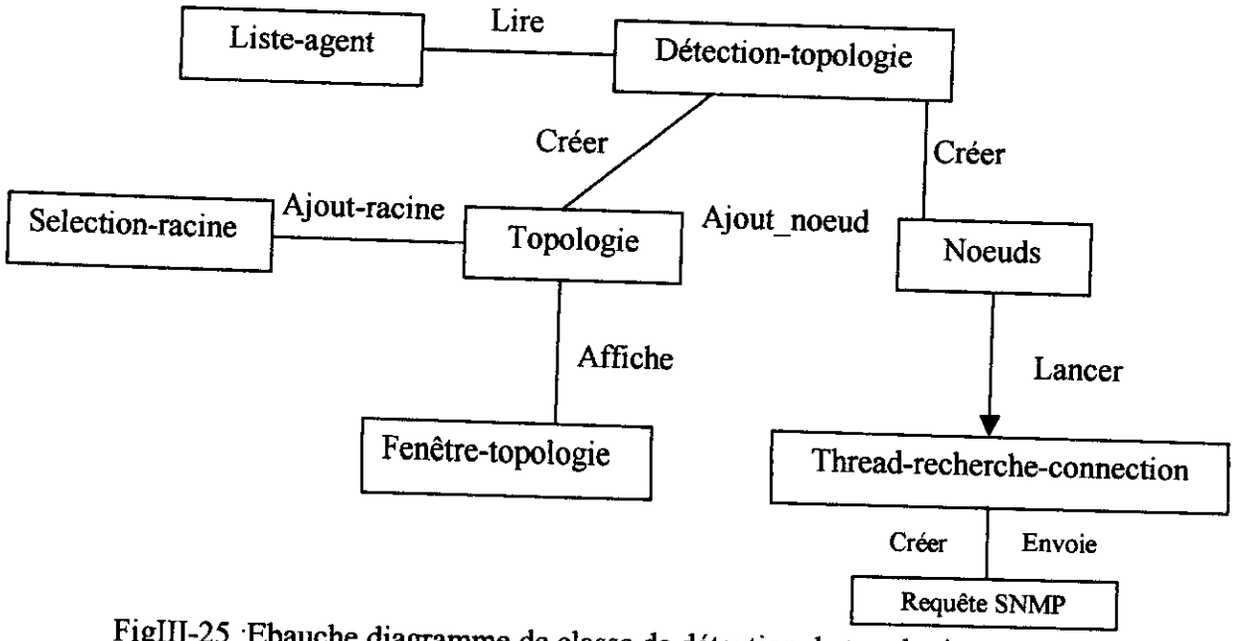
Ce cas d'utilisation permet la detection de la topologie du réseau, ce cas est realisé par la collaboration des objets instances des classes Liste-agent, Topologie, Thread-Recherche- connection, Selection-racine , Fenêtre-topologie et Requête_SNMP.Il commance par la recherche des nœuds dans la liste des agents et se termine par l'affichage de la topologie dans une fenêtre .

La figure III-24 illustre la collaboration des objets :



FigIII-24 Collaboration d'objets « détection topologie »

Cette collaboration d'objets nous donne le diagramme de classe qu'illusté dans la figureIII-5:



FigIII-25 :Ebauche diagramme de classe de détection de topologie

5-5. Exploration de la MIB d'un équipement :

Ce cas d'utilisation s'exécute lorsque l'administrateur veut explorer la MIB d'un agent en sélectionnant son adresse IP. La réalisation de ce cas s'effectue par la collaboration des objets instances des classes :I Exploration MIB, Thread, Requête SNMP et Liste-agent.

La figure III-26 illustre cette collaboration des objets :

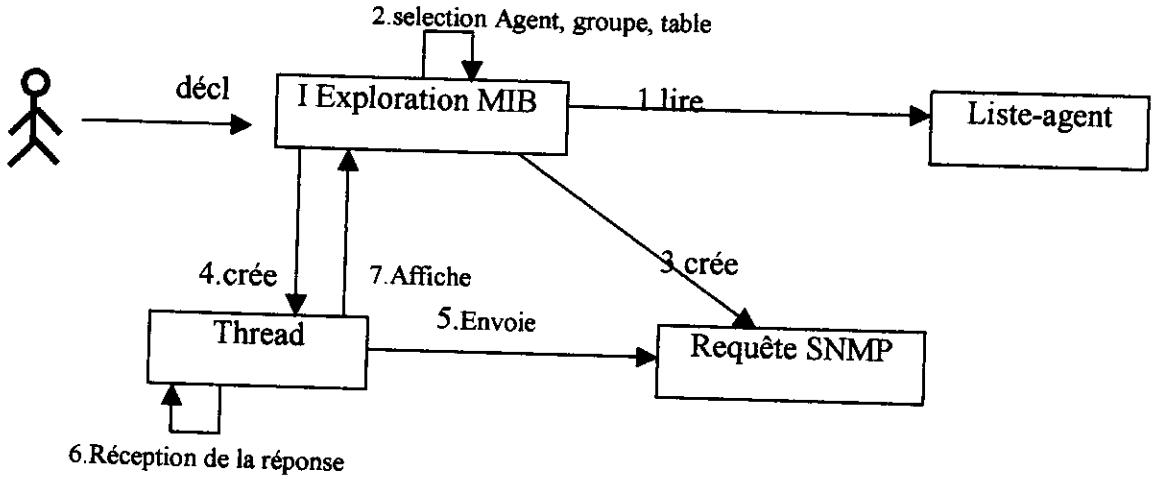


Fig III-26 : Collaboration des objets « exploration de la MIB »

La figure FigIII-27 montre le diagramme de classe préliminaire issue de cette collaboration d'objets.

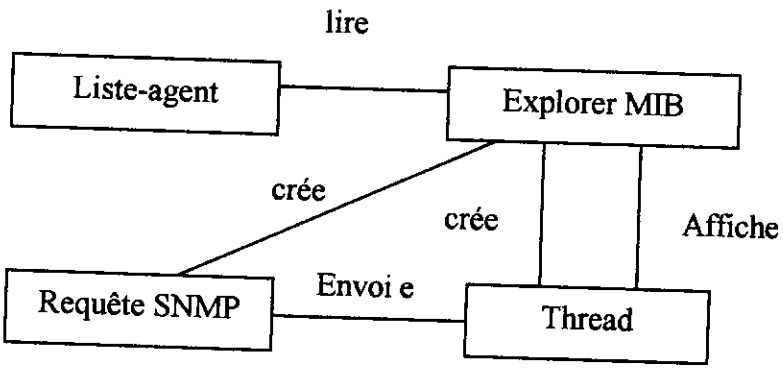


Fig III-27 Ebauche diagramme de classe : Exploration de la MIB

5-6. Enregistrer un nouvel agent :

Ce cas d'utilisation se declanche lorsque l'administrateur veut enregistrer un nouvel agent detecté; ce cas d'utilisation se réalise par la collaboration des objets instances des classes :liste-agent ; base-agent qu'illustré dans la figure III-28.

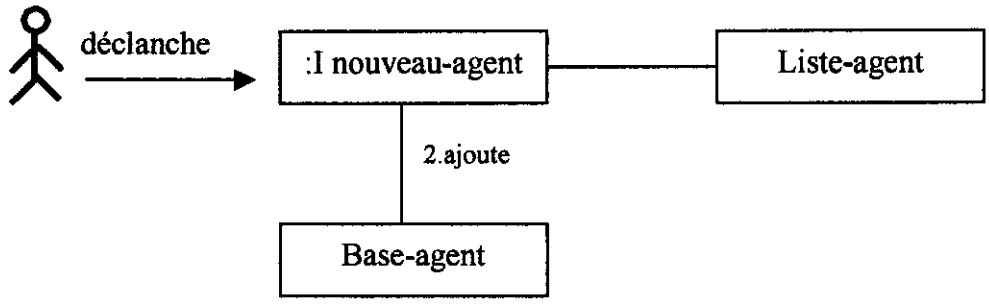


Fig III-28 collaboration des objets « Enregistré un nouvel agent »

5-7.Suppression d'un agent :

Ce cas d'utilisation se réalise lorsque l'administrateur selectionne un agent et qui veut le supprimer. Il se réalise par la collaboration des objets instances des classes list-agent ; Isuppression ; base-agent.

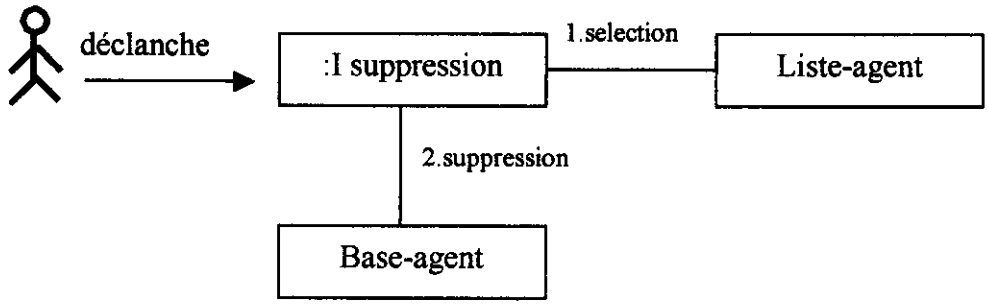
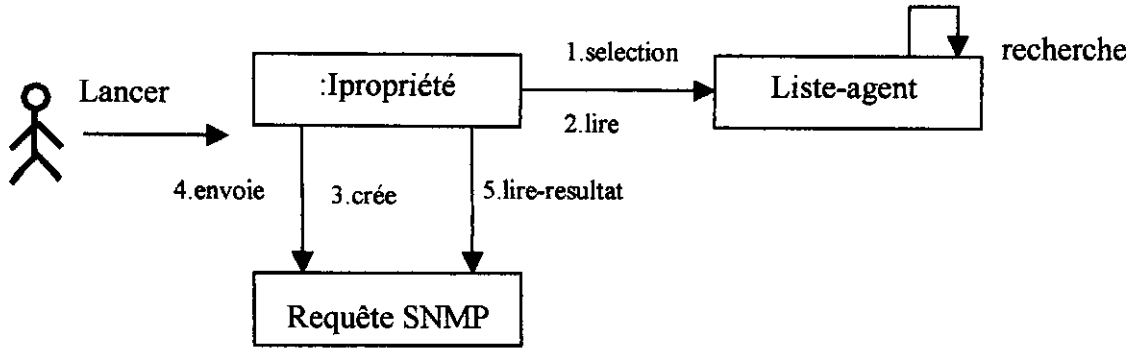


Fig III-29 : Collaboration des objets « suppression d'un agent »

5-8.Visualiser les propriétés :

Ce cas d'utilisation se réalise lorsque l'utilisateur sélectionne un agent pour visualiser sur les propriétés, il est exécuté par la collaboration des objets instances des classes : Ipropriété; Liste-agent ; Requête SNMP.

La figure suivante illustre cette collaboration d'objet.



FigIII-30 :Collaboration des objets «Visualiser les propriétés d'un agent »

La figure III-31 illustre le diagramme de classe issue de cette collaboration d'objet

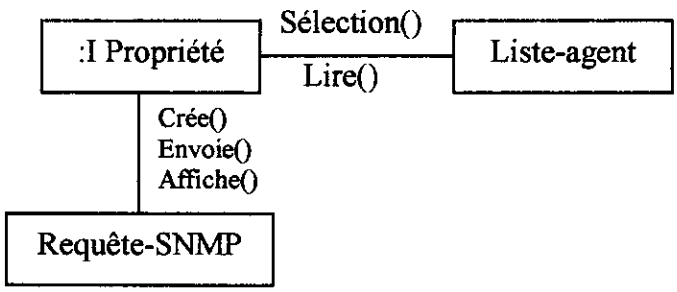


Fig III-31 Ebauche diagramme de classe « propriété d'un agent »

5-9.Lancer un ping :

Ce cas d'utilisation se réalise lorsque l'administrateur veut lancer les requêtes ping sur chaque adresse IP de la plage d'adresses, ce cas est réalisé par la collaboration des objets instances des classes : I Fenêtre-ping ; Thread.

La figure III-32 illustre cette collaboration :

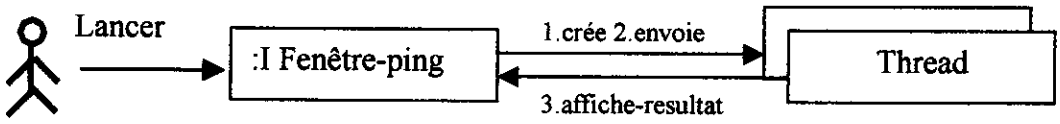


Fig III-32 : Collaboration d'objets « Lancer-ping »

5-10.Faire des statistiques :

Ce cas d'utilisation permet à l'utilisateur d'avoir des statistiques sur l'état du réseau ou l'état d'une machine spécifique. Il est réalisé par la collaboration des objets instances des classes : Thread-satistique, Liste-agent, Fenêtre-statistique et requête-SNMP La figure III-33 représente la collaboration d'objets :

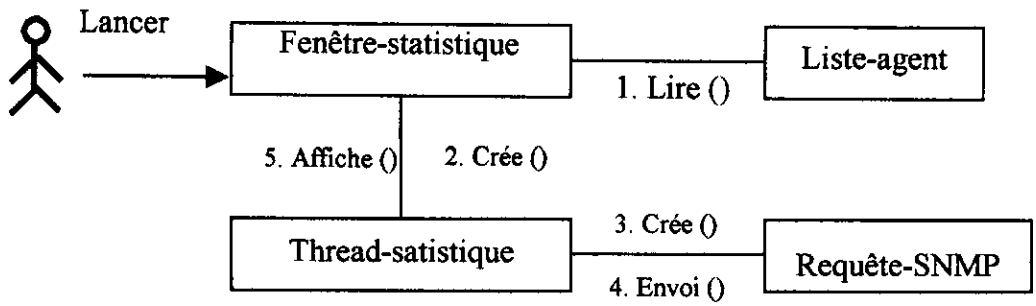


Fig III-33 : Collaboration d'objets : faire des statistiques

Le diagramme de classe préliminaire issu de cette collaboration d'objet est illustré dans la figure ci-dessous.

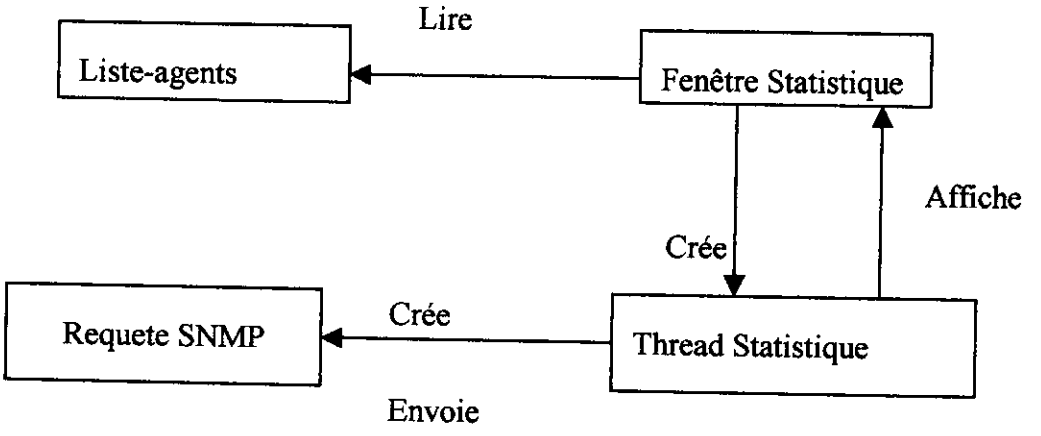


Fig III.34 : Ebauche de diagramme de classe « faire des statistiques »

5-11. Ajout manuel dans la cartographie :

Ce cas d'utilisation se déroule lorsque l'administrateur veut ajouter ou modifier des hubs ou des équipements branchés sur des hubs à la topologie du réseau. Afin d'enrichir sa cartographie par des équipements que l'application n'a pas pu trouver sur quelle machine sont connectés. Il est réalise par la collaboration d'objet instance des classes suivante : Toplogie , Nœud , Ajout_topologie, Liste_agent

La figure suivante montre cette collaboration d'objet :

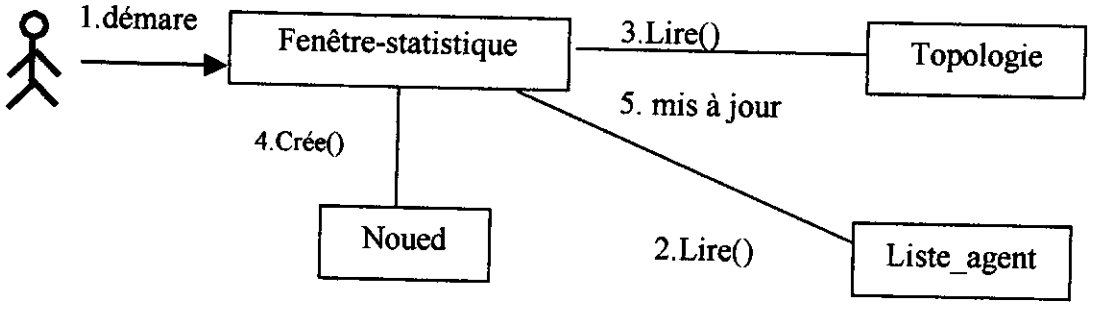


Fig III-35 : Collaboration d'objets : Ajout manuel dans la topologie

Le diagramme de classe ébauche de cette collaboration d'objet est illustré dans la figure ci-dessous

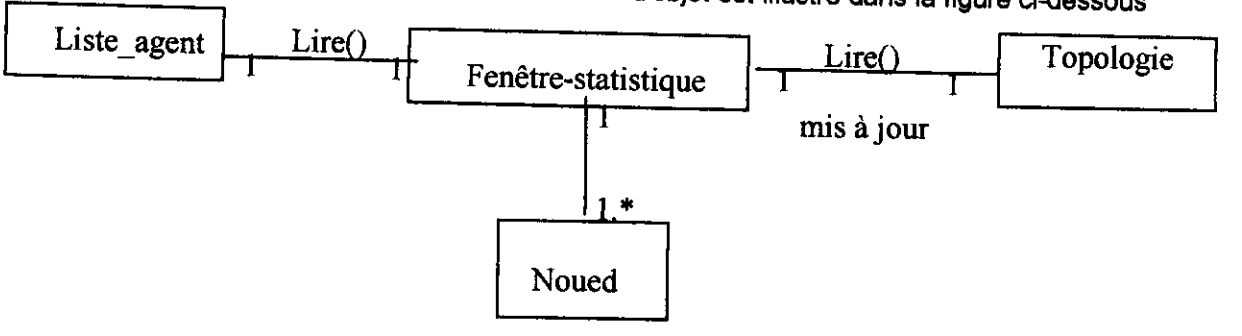


Fig III-36 : Ebauche de diagramme de classe : Ajout manuel dans la topologie

III-6. Diagramme final des classes:

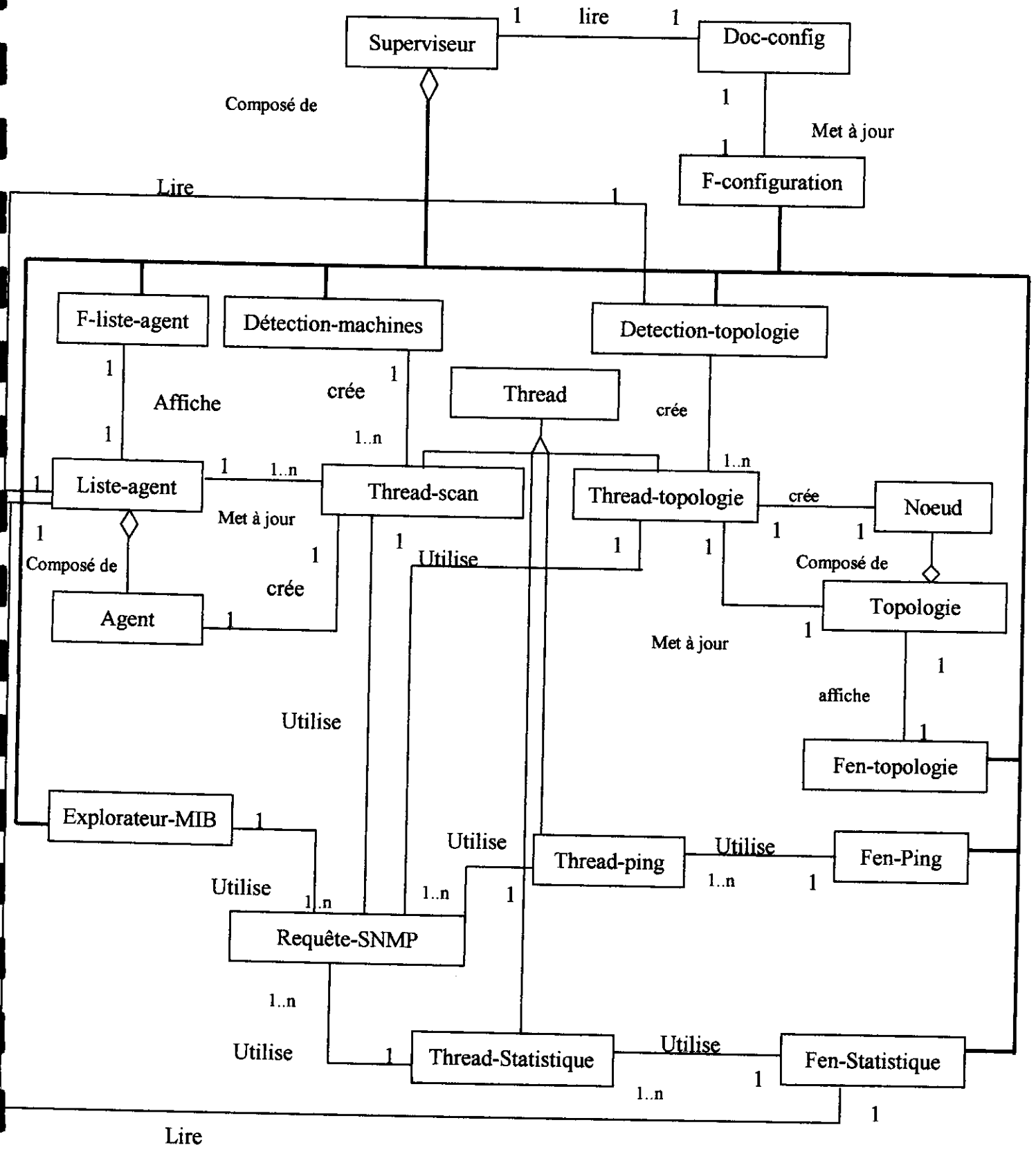


Fig III.37 : Diagramme de classe finale

III-7. La Persistence:

7-1-Introduction :

Afin d'assurer la persistance des données du superviseur, nous avons opté pour l'utilisation d'une base de données, cette dernière doit contenir toutes les informations obtenues par le superviseur sur l'état du réseau et elle doit être mise à jours régulièrement par l'administrateur.

La base doit respecter les règles suivantes :

- Un équipement du réseau est défini par son adresse Mac, adresse IP, le nom de la machine et la localisation, la date la première détection et sa description.
- Chaque équipement à un seul type qui peut être soit un PC, serveur, imprimante, switch, Hub ou un routeur.
- Un nœud de la topologie doit être soit un switch, un Hub ou un routeur.
- Chaque équipement du réseau est connecté au moins à un nœud.
- Chaque équipement du réseau a un seul père sauf la racine.

7-2-L'intérêt de l'utilisation de la base :

Avoir une base de données nous permet de :

1- Détecter les nouveaux équipements connectés au réseau lorsqu'un équipement est détecté par le superviseur et qui n'existe pas dans la base, cela permet aussi de le localiser rapidement.

2- Connaître l'état d'un équipement existant c'est à dire actif ou éteint.

3-Détecter les changements des branchements dans le réseau lorsqu'une machine change de nœud de connexion (switch) ou même change le port dans le même switch.

7-3-Le modèle logique de données de la base utilisée :

La base de données que nous avons utilisée contient les tables suivantes :

- La table Agent : Elle contient les informations sur les équipements du réseau (adresse Mac, Adresse IP, nom de la machine, localisation, date de la première détection, description de la machine).

  La clé primaire de cette table est l'adresse Mac puisqu'elle est unique au monde pour tous les constructeurs.

- La table Type : contient les différents types d'équipement qui peuvent exister dans le réseau.

- La table Topologie : cette table représente la topologie détectée du réseau, elle contient trois colonnes : l'adresse Mac du père, l'adresse Mac du fils, le numéro de port du fils et numéro de port du père.

La clé primaire de cette table est la concaténation de l'adresse Mac du père avec l'adresse Mac du fils.

La figure suivante représente le modèle logique de données de cette base.

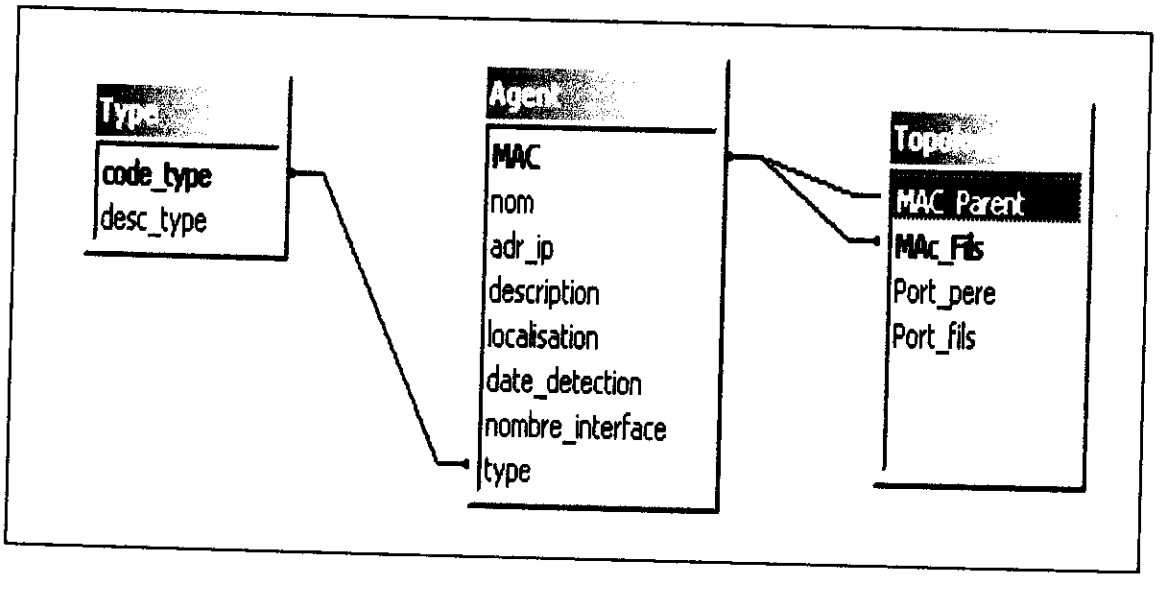


Fig III. 38 : Le modèle logique de données de la base de données

CHAPITRE IV
LA RÉALISATION

IV-1. Introduction

Notre travail consiste à réaliser un système de supervision réseau local TCP/IP via le protocole de gestion SNMP, la fonctionnalité la plus importante du superviseur est l'établissement d'une cartographie d'un réseau Ethernet TCP/IP avec un rafraîchissement régulier des informations présentées. Pour réaliser cet objectif nous avons décomposé le problème en quatre phases principales :

•La première phase est la détection des équipements existants dans le réseau en envoyant des requêtes ping (ICMP) sur la plage d'adresses utilisée dans le réseau.

•La deuxième phase consiste à récupérer les informations nécessaires de chaque machine du réseau et déterminer le type de chacune d'elles.

•La troisième phase consiste à découvrir la topologie du réseau en récupérant les listes des adresses Mac des machines connectées sur un nœud (Switch), cette liste est appelée « Forwarding list ».

•La quatrième phase est la représentation de la topologie sous forme d'une cartographie.

La figure suivante illustre la fonction générale du superviseur.

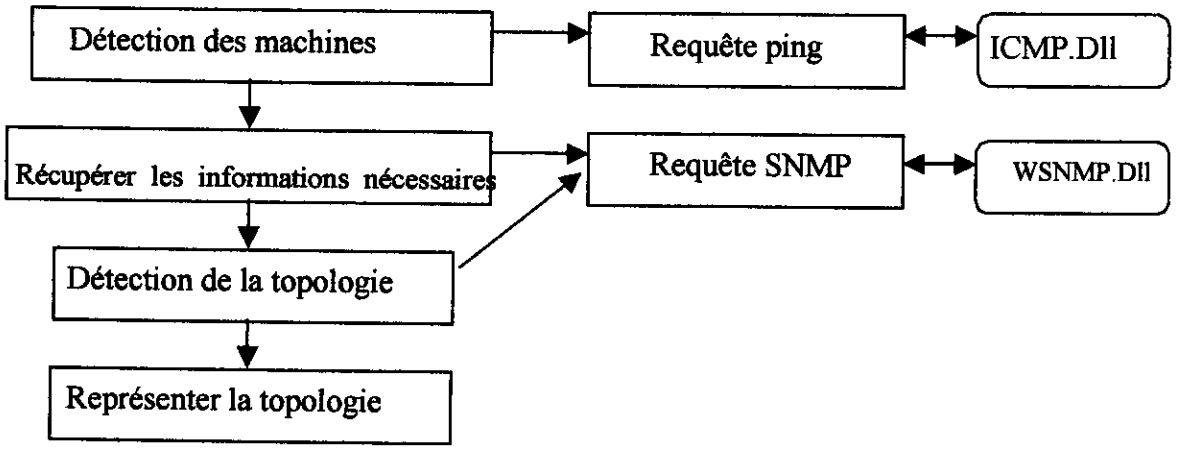


Fig IV-1 : Fonctionnement général du superviseur

Les deux bibliothèques utilisées ICMP.Dll et WSNMP.Dll seront décrites à la suite de ce chapitre.

Nous complètons le superviseur par d'autres fonctionnalités qui sont :

• Un MIB explorateur :Afin de permettre l'exploration de la MIB d'un équipement.

• Une interface de ping : Pour faire des pings sur une plage d'adresses définie par l'administrateur.

• Faire des Statistiques : Afin de donner à l'administrateur une idée générale sur le fonctionnement de son réseau.

IV-2. Environnement matériel de développement:

Au cours du développement de notre système de supervision, nous avons utilisé un poste de travail connecté à un réseau local. Le réseau doit contenir des équipements informatiques comme des Switch (possède une adresse IP) , Hub, routeur, imprimantes réseaux...etc. Tout équipement de notre réseau local doit avoir un agent SNMP implémenté par le constructeur sinon l'administrateur doit l'installer et le configurer correctement.

Si la politique de gestion d'un réseau local utilise les VLANs (Virtual Local Area Network) pour sécuriser le réseau, il faut que le PC de développement appartienne au VLAN qui contient les SWITCHs du réseau.

IV-3.Environnement logiciel de développement:

3-a) Langage de programmation :

Nous avons utilisé le Builder C++ 6.0 comme langage de programmation orienté objet. Nous avons choisi l'orienté objet pour la facilité de développement, de maintient et de la réutilisation des différents modules de l'application.

Nous avons utilisé l'Interbase pour créer une base de données pour la persistance des données (sauvegarder l'état du réseau), c'est le système de gestion des bases de données (SGBDR) intégré dans le Builder.

3-b) Les bibliothèques utilisées :

Nous avons utilisé deux bibliothèques qui sont :

- **ICMP.dll** : Cette bibliothèque contient des fonctions du protocole ICMP, elle est utilisée pour la réalisation des requêtes PING afin de détecter toutes les machines qui existent dans le réseau. Cette bibliothèque est chargée en mode dynamique,c'est à dire que les fonctions sollicitées de cette bibliothèque sont chargées dans la mémoire seulement à la demande de l'application et à la fin de leurs utilisation l'application les décharge de la mémoire .

- **WSNMP32.dll** : Cette bibliothèque regroupe toutes les fonctions nécessaires pour l'utilisation du protocole SNMP (création des PDUs, envoie des requêtes, réception des réponses). Elle est utilisée en mode statique, c'est à dire que l'application charge toutes les fonctions de Cette bibliothèque en mémoire au démarrage et elles restent résidantes dans la mémoire. Cette bibliothèque constitue le noyau de notre application, donc il faut qu'elle soit présente tout le temps dans la mémoire.

3-c) L'installation de l'agent SNMP :

Pour installer le service **Microsoft SNMP** sur toutes les versions de Windows 2000. il faut suivre les étapes suivantes :

1-Aller au panneau de configuration et choisir « ajout/suppression des programmes ».

2-Selectionner « ajout/suppression des composant Windows ».

3-Choisir « outils de gestion et d'analyse » puis cliquer sur « détail ».

4-Choisir le service SNMP.

Après l'installation du service, il est cependant possible de configurer cet Agent SNMP. Il est même très fortement conseillé d'effectuer ce paramétrage pour des raisons de sécurité. A partir de l'outil gestion de l'ordinateur qui se trouve dans (panneau de configuration\outils d'administration\..).

1-Dans « service d'application » sélectionner « service ».

2-Dans la liste des services sélection « service SNMP » et ouvrir sa fenêtre des

Propriétés. (pour plus de détails voir l'annexe C)

Remarque : les postes de travail qui ont le système d'exploitation WindowsNT (Win2000, Windows XP,...), l'activation et configuration de l'agent SNMP est possible, donc ces équipements peuvent être manager par notre superviseur. Par contre, pour les postes de travail qui ont des anciens systèmes d'exploitation comme WIN98, Milinieum. Ces machines sont seulement détectées par le superviseur et décrites comme des machines qui n'ont pas l'agent SNMP installé.

IV-4.Les principales fonctionnalités du superviseur:

4-1. La détection des machines dans le réseau :

C'est la phase initiale de l'utilisation du superviseur, elle prend la plage d'adresses utilisée dans le réseau et envoie les requêtes ping (ICMP) sur chacune d'elle afin de déterminer les machines existantes dans le réseau. Le résultat est sauvegardé dans une liste. L'envoie et la réception des réponses des requêtes ICMP sont réalisés par des threads et à chaque adresse on associe un Thread qui envoie un ping et attend la réponse.

Les fonctions utilisées pour envoyer des requêtes Ping de la bibliothèque ICMP.Dll qu'est disponible dans tous les systèmes d'exploitation sont :

(WINAPI*pfnHV) plcmpCreateFile : Ouverture de service.

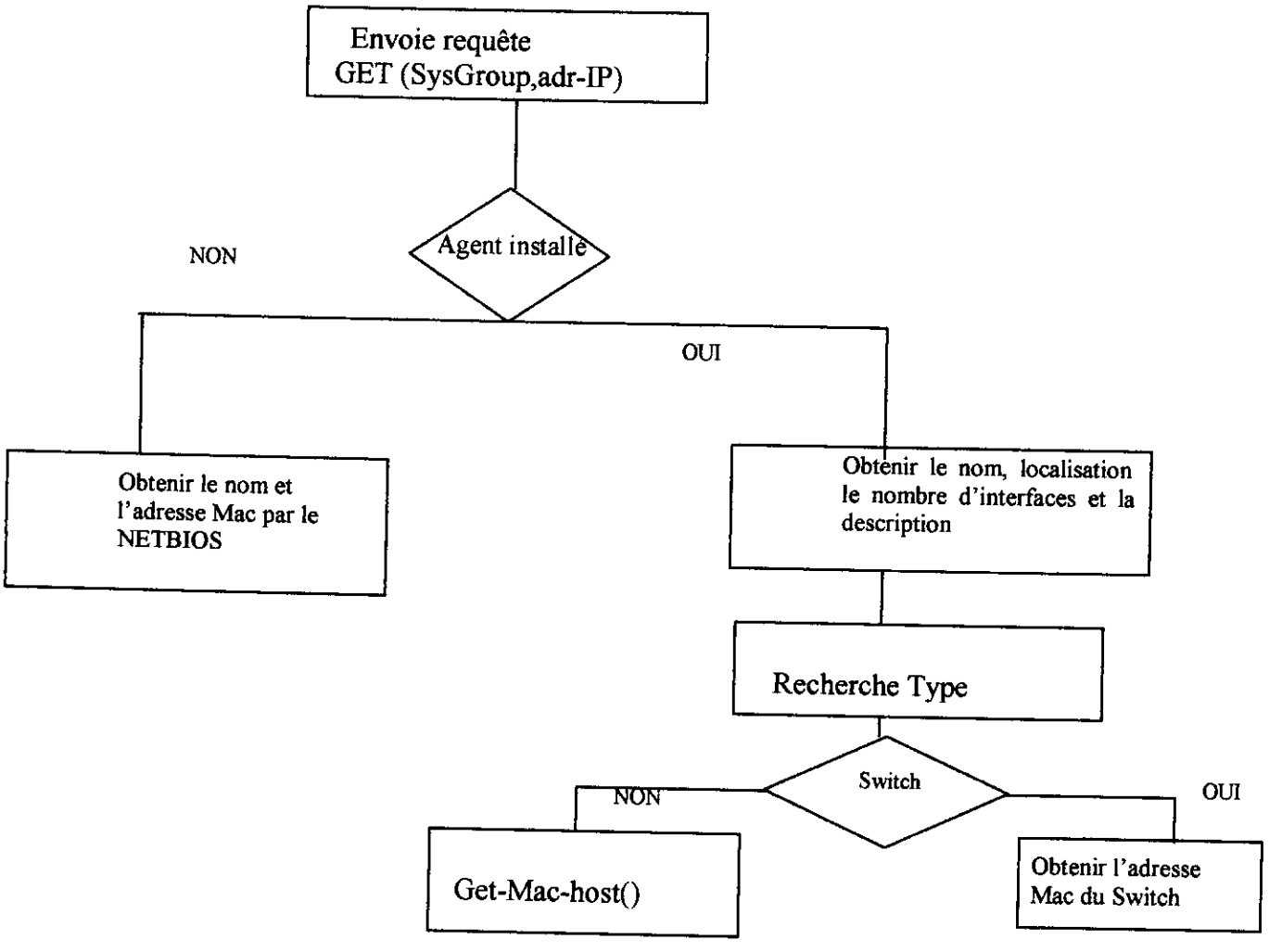
(WINAPI*pfnDHDPWPipPDD) plcmpSendEcho : Envoie des requêtes.

(WINAPI*pfnBH) plcmpCloseHandle : Fermeture de service.

4-2.Le recueil d'information sur les machines détectées:

Le recueil d'information (nom de la machines, adresse MAC, localisation, description, nombre d'interface réseau) sur les machines du réseau détectées s'effectue par l'envoie d'une requête GET et GET-NEXT de SNMP sur le groupe système de la MIB, on obtient la description, le nom et la localisation, si l'agent SNMP est installé sur la machine. Si l'agent n'est pas installé sur la machine, alors on utilise le NETBIOS pour avoir l'adresse Mac et le nom de la machine.

L'organigramme suivant illustre le déroulement de cette phase :



FigIV-2 : Organigramme de recueil d'information

•Get (Sys Group,adr-IP) est une requête SNMP de type GET avec l'identificateur d'objet (1.3.6.1.2.1.1.1.0Æ 1.3.6.1.2.1.1.6.0). Cette requête permet d'avoir les variables de groupe système de la MIB.

•Le nombre d'interfaces est obtenu en utilisant la requête Get 1.3.6.1.2.2.1.0

•L'adresse Mac du Switch est obtenue par l'envoie de la requête SNMP Get 1.3.6.1.2.1/.1.1.1

•L'adresse Mac des hosts est obtenue par la requête SNMP Get1.3.6.1.2.1.2.2.6.1

•La détermination du type de la machine détectée se base sur sa description obtenue par SNMP, si l'agent SNMP n'est pas installé alors on utilise le nom de la machine.

Le recueil d'information sur les machines en utilisant le protocole SNMP suit trois étapes :

4-2-1 : L'envoie de requête SNMP :

Le système de gestion SNMP envoie une demande à un agent en utilisant le nom de l'agent (ou son adresse IP). La demande est routée par l'application au port 161 (port UDP). Le nom d'hôte est résolu en adresse IP à l'aide d'une des méthodes de résolution.

L'envoi d'une requête SNMP suit les étapes suivents:

1) Initialisation du service SNMP et création d'une session : SnmpStartup();

hSession =SnmpCreateSession ();

2) L'ajout d'un nom de communauté, adresse source, adresse destination, numéro de version,

SnmpStrToEntity (hSession, "172.167.0.1");

SnmpStrToContext (hSession, &dCtx);

3) La construction de la PDU via ASN-1

,SnmpCreateVbl (hSession, NULL, NULL);

SnmpCreatePdu (hSession, SNMP_PDU_GET, 100, 0, 0, hVbl);

4) L'envoi de datagramme contenant l'objet ASN.1 spécifié

SnmpSendMsg (hSession, 0, hDst, hCtx, hPdu);

5) La fermeture de service :SnmpCleanup();

Les requêtes SNMP sont envoyées par le protocole UDP sur le port 161 des agents.

4-2-2. Le traitement de la requête de manager par l'agent SNMP :

Il suit l'algorithme suivant :

1) réception du message dans la mémoire tampon

2) analyse du message

- message ASN-1 correct ?=> non => fin

- version OK ? => non => fin

-Examen de la communauté et des données contenues dans le message

-l'agent vérifie le nom d'hôte ou l'adresse IP de la source. Il doit être autorisé à accepter des paquets du système de gestion, sinon le paquet sera supprimé

- examen de la PDU reçue (analyse syntaxique)

Si message correct

- construction d'une nouvelle PDU correspondant à la requête reçue.
- construction du message et envoi

si non :Signale l'erreur : envoie la réponse avec le numéro d'erreur et l'index : Archive l'erreur et trap éventuel

fsi

4-2-3. La réception de la réponse de l'agent SNMP :

La réception des réponses de l'agent par le manager suit l'algorithme suivant : Réception du message : SnmpRecvMsg (hSession, NULL, NULL, NULL, &hPdu); Analyse du message : SnmpGetPduData (hPdu, &lType, &lReqId, &lErr, &lIdx, &hVbl); Si Err <> 0 alors < erreur dans la requête envoie de manager vers l'agent >

Sinon:

lire les valeurs retournées par l'agent dans la liste varbindlist (Vbl)

<SnmpGetVb (hVbl, i+1, &dName, &dValue);>

finsi

4-3. La découverte de la topologie :

La complexité de la découverte de la topologie d'un réseau Ethernet Vient de la transparence intrinsèque aux commutateurs: les différentes machines branchées au réseau ignorent que celui-ci comporte des commutateurs (*hubs* ou *switchs*).

Le comportement des hub et des switchs est différent. Un hub n'est qu'un boîtier comportant un certain nombre de ports; tout ce qui est reçu sur un port est retransmis sur tous les autres. Comme cette méthode n'est pas très efficace, la plupart du temps on utilise des switchs; ceux-ci diffèrents des hubs parce qu'ils tentent d'envoyer les paquets que sur le bon port. Pour cela, ils tiennent à jour une table du type {adresse physique, port}. Lorsqu'il doit transmettre un paquet dont l'adresse est dans sa table, il l'envoie uniquement sur le port associé; sinon il se comporte comme un hub, c'est-à-dire qu'il l'envoie sur tous les ports.

La table est mise à jour à chaque paquet transitant par l'équipement qui en extrait les adresse. Cette table est un cache: toutes les informations sont datées et supprimées au bout d'un certain temps. La liste des adresses physiques correspondant à un port dans cette table est appelée *forwarding list*.

Grâce au protocole SNMP, nous pouvons récupérer ces *forwarding lists* d'une manière standard dans la *BRIDGE-MIB*. A partir de là, on sait sur quel port chaque équipement réseau "voit" une machine. Mais étant donné que cette liste n'existe pas dans les hubs et si le réseau contient des hubs alors le résultat obtenu concerne que les switchs et les machines directement branchées sur des switchs sans passer par des hub.

La détection de la topologie est réalisée en trois étapes, elle commence par la récupération des « forwading list » de chaque Switch du réseau, puis elle traite ces listes afin de déterminer les liaisons entre les équipements de type (Nœud i, fils j, N°port_père, N°port_fils). Et à la fin le système insert les résultats dans la table topologie de la base de données. Cette découverte ne concerne pas les hubs et les machines connectées aux hubs à cause de l'absence de la table de correspondance de l'adresse Mac et Numéro de port dans les hubs.

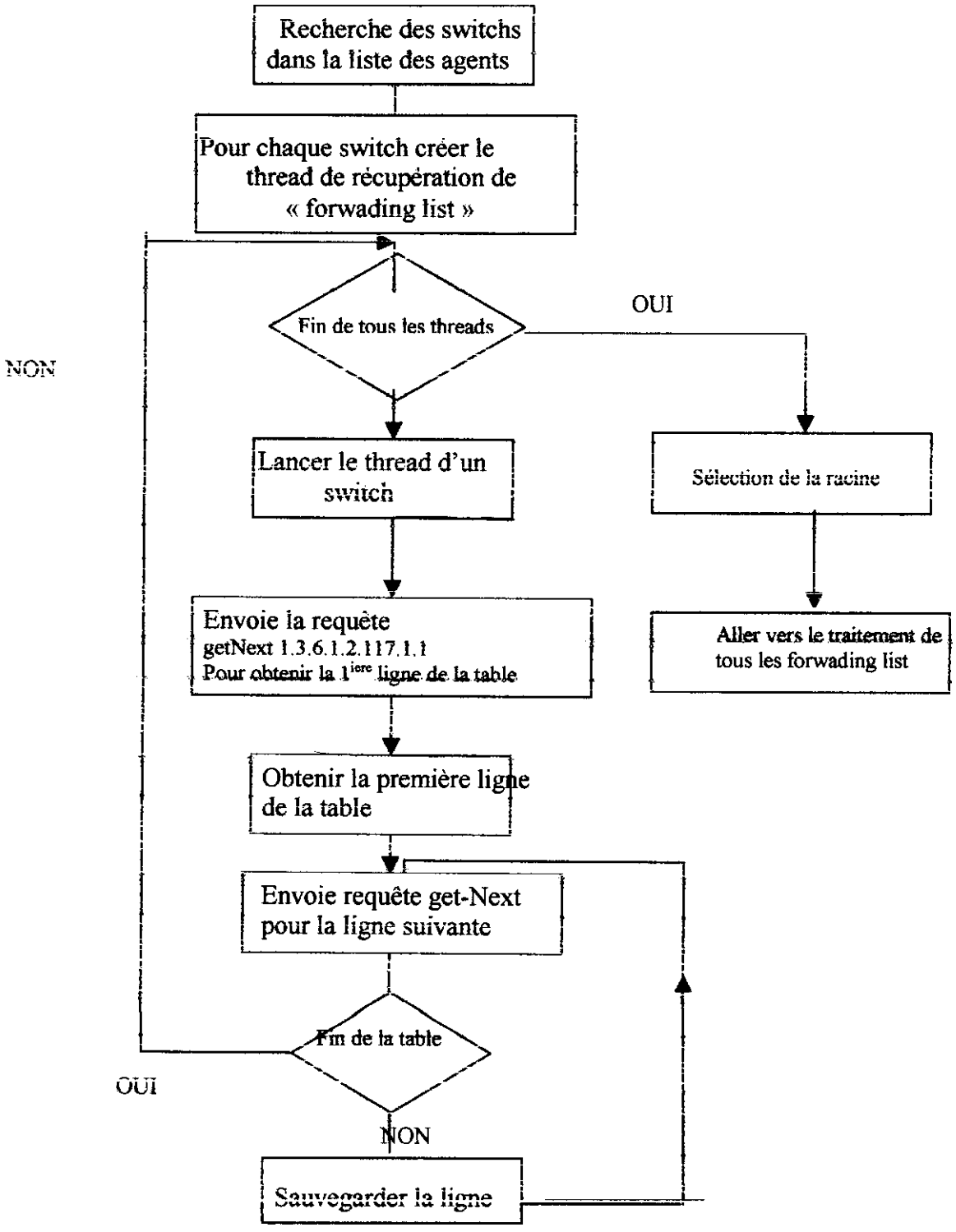
On note ici que lorsqu'un port P1 du Swtich (S1) est connecté au port P2 du Switch (S2) alors la liste obtenue du port P1 du Switch (S1) contient le Switch (S2) et toutes les machines connectées directement et indirectement au Switch (S2) et

inversement pour la liste obtenue du port P2 du Switch (S2).

4-3-1. La récupération des « forwading list » des swtichs :

Le déroulement de cette étape est illustré dans l'organigramme suivant :

Fig IV-3 : Récupération de « Forwading list »



4-3-2.le traitement de « Forwading list » :

L'organigramme suivant illustre comment en tire les liens entre les machines à partir des « forwading list » obtenues dans l'étape précédente.

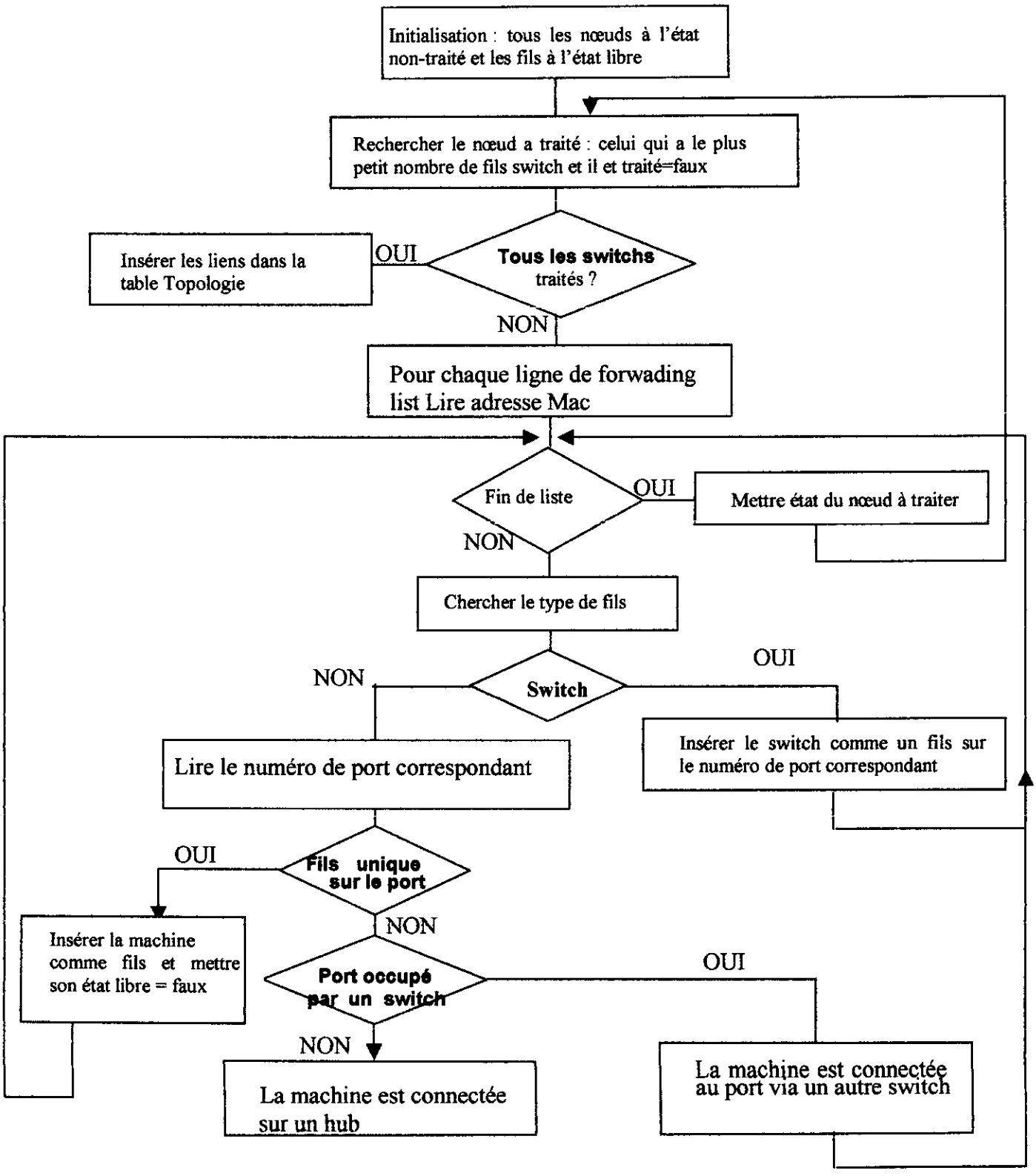


Fig IV-4 : Organigramme de traitement de « Forwading list »

4-3-3. La sauvegarde de la topologie :

La dernière étape de la découverte de topologie est la sauvegarde des résultats trouvés dans la table topologie. Les Hubs et les machines connectées aux Hubs sont considérés comme des machines libres et c'est à l'administrateur de les ajoutés dans la topologie manuellement car les Hubs ne permettent pas d'avoir les liens entre l'adresse Mac et numéro de port.

4-4. La présentation de la topologie :

Notre algorithme de construction de cartographie suppose que le réseau dont on veut déterminer sa topologie ne comporte pas de boucle, c'est pour cela que la topologie va être présentée sous forme d'arbre. Dont la racine est le switch qui a le plus grand nombre de switchs fils. La construction de l'arbre qui représente le réseau se fait en deux parties, la première est la construction des nœuds internes de l'arbre (c'est-à-dire le placement des switchs et des hubs) puis vient le placement des autres équipements qui sont les feuilles de l'arbre.

Le placement des feuilles est plus facile et nettement moins critique que le placement des nœuds internes de l'arbre, en effet une erreur dans le placement d'une feuille n'affecte que cette dernière, mais une erreur dans le placement d'un nœud interne affecte tout l'arbre.

4-4-1. Le placement des nœuds internes dans l'arbre :

Tous les équipements manipulés ici sont des noeuds internes de l'arbre (Switch ou hub).On va employer le terme « nœud »pour les désigner.

L'algorithme de construction de l'arbre commence par la lecture de la table topologie, puis il commence à appeler la procédure construction_arbre() avec comme argument la racine. Cette dernière est choisie par l'administrateur parmi une liste de nœuds proposés par l'application. La procédure construction_arbre(Neoud *N , int coord_x ,int coord_y) est une procédure récursive, elle dessine le nœud N et calcule les coordonnées des noeuds fils , puis la procédure s'appelle elle-même mais avec argument le fils le plus à gauche du nœud N puis ses fils droits. Ainsi La construction de l'arbre est réalisée par un parcours préfixe (père, fils gauche, fils droit) de la topologie.

IV-5.Conclusion :

Dans notre réalisation nous pensons avoir concrétisé tous les cas d'utilisation décrits dans la conception et que nous avons réalisé l'essentiel des besoins fonctionnels demandés notamment l'élaboration de la cartographie du réseau.

Nous allons passer maintenant au test du superviseur sur le réseau de la CNAS.

CHAPITRE V
TEST DU SUPERVISEUR SUR LE RÉSEAU DE LA CNAS

V-1. Introduction:

Le superviseur réseau que nous avons conçu est un outil de surveillance des équipements réseau connectés à un réseau local TCP/IP. Notre superviseur utilise le protocole de gestion SNMP, donc il est nécessaire que n'importe quelle machine appartenant au réseau local doit avoir un agent SNMP intégré en elle.

On a testé notre superviseur sur le réseau local de la CNAS qui contient environ 100 machines (serveurs, imprimantes réseau, switch, Hub et des postes de travail).

Notre système est implémenté sur une station de gestion (NMS) qui est connectée à un port spécifique qui appartient à tous les VLANs du réseau.

Notre application est de type MDI (Multi Dynamique Interface) c'est à dire qu'elle est composée d'une fenêtre mère et des fenêtrer filles « MDI Child » :

1- La fenêtre principale : c'est la fenêtre de démarrage toujours visible, elle permet d'accéder aux différentes fonctionnalités du superviseur et de gérer les fenêtres filles.

2- Les fenêtres de type « MDI Child » : Elles permettent de présenter les différents résultats trouvés par le superviseur.

V-2. Présentation du Superviseur :

Nous allons présenter le déroulement de l'utilisation des fonctionnalités du superviseur qui sont :

- Le démarrage du superviseur.
- La configuration du superviseur.
- La détection des machines du réseau.
- La détection de la topologie.
- La présentation de la topologie
- L'ajout d'une machine dans la cartographie.
- La visualisation des propriétés d'un agent.
- L'exploration de la MIB d'un agent.
- L'utilisation de Ping.
- L'acquisition des statistiques sur l'état du réseau.

2-I. Fenêtre principale :

C'est la fenêtre principale de l'application qui permet d'accéder aux autres fenêtres. Elle est composée d'un menu principal, d'une barre d'outil et d'une zone d'affichage des fenêtres MDI Child : (FigV-1)

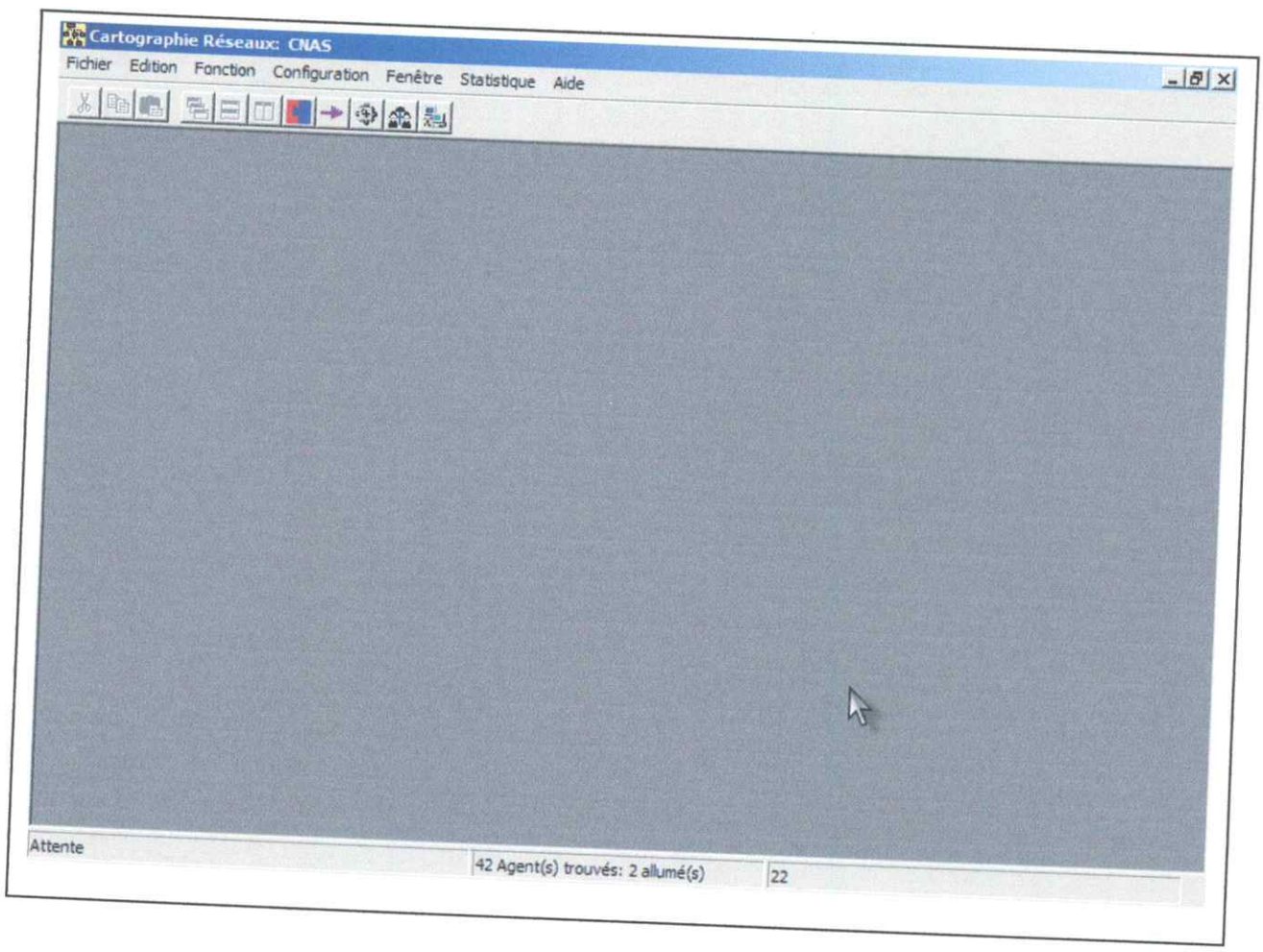


Fig V-1 : La fenêtre principale du superviseur

1-Le Menu Principal : Il permet l'accès aux différentes fenêtres du superviseur.

2-La barre d'outils : Permet d'effectuer les fonctionnalités importantes du superviseur.

3-La zone d'affichage des fenêtres MDI Child : Dans cette zone nous allons afficher les différentes fenêtres de l'application (Listes des agents, L'arborescence, Topologie).

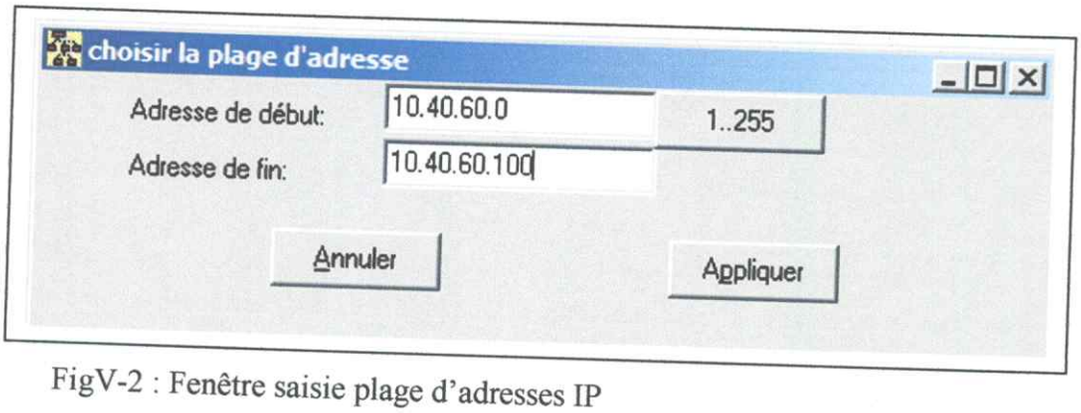
2. Configuration du superviseur :

L'administrateur a deux fenêtres pour configurer son superviseur et qui sont :

2-a) Fenêtre « saisie plage d'adresses IP » :

Tout d'abord l'administrateur doit définir au superviseur la plage d'adresses IP utilisée dans son réseau local, puis il peut valider la plage saisie ou l'annuler. (FigV-2)

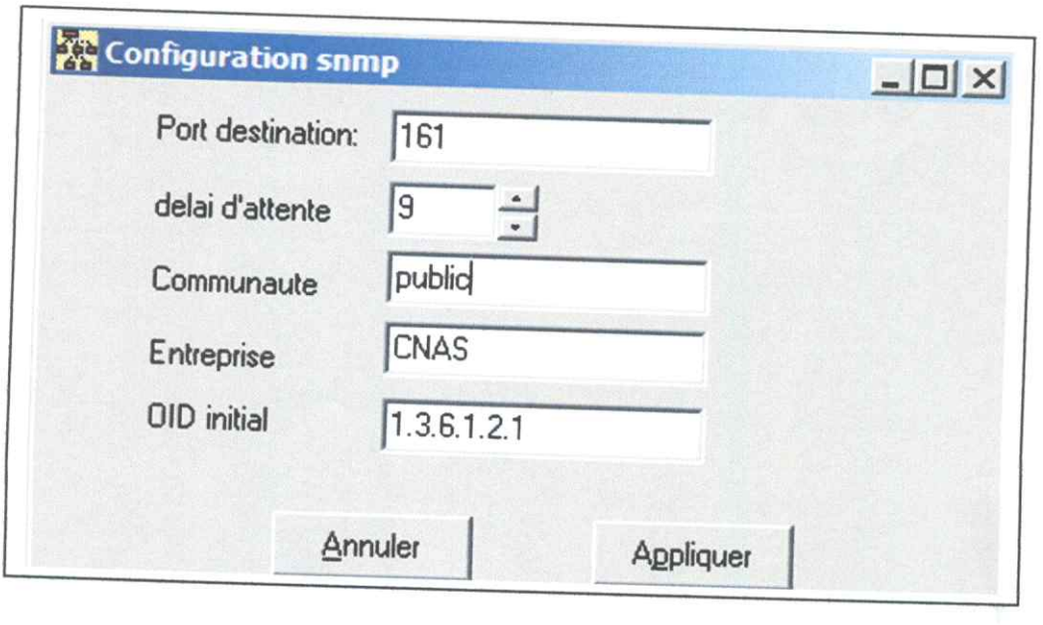
Pour accéder à cette fenêtre, il faut aller au menu principal, cliquer sur configuration puis sélectionner plage d'adresses.



FigV-2 : Fenêtre saisie plage d'adresses IP

2-b) Fenêtre « Configuration SNMP » :

Cette fenêtre permet une modification de la configuration par défaut du SNMP. Pour afficher cette fenêtre, il faut aller au menu principal, cliquer sur « configuration » puis sélectionner « configuration SNMP».(FigV-3)



FigV-3 : Fenêtre « configuration SNMP »

2-3. La détection des machines du réseau:

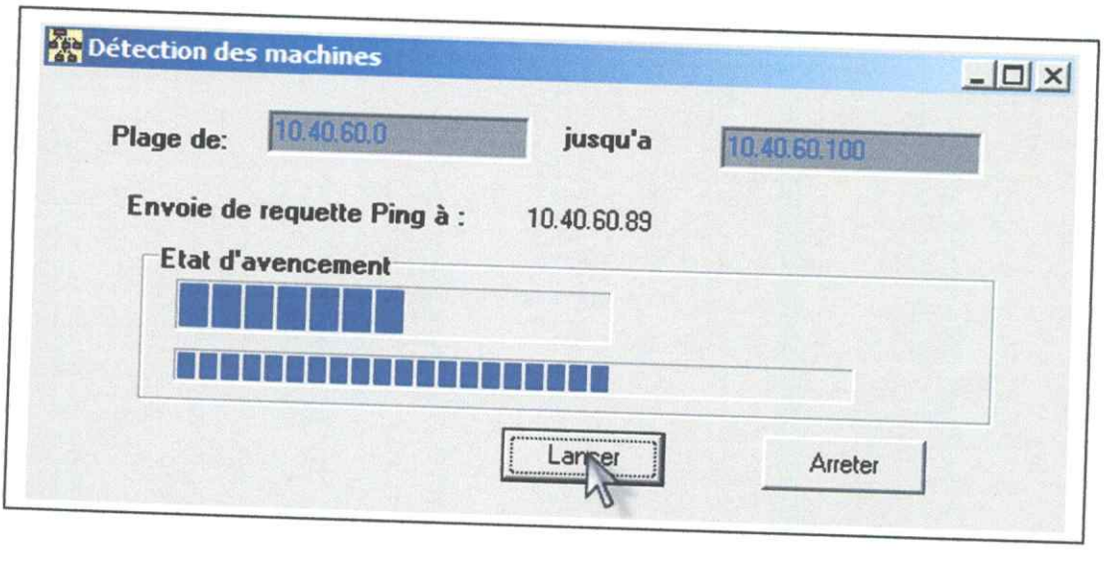
Cette opération permet de détecter les machines existantes dans le réseau, elle commence par le lancement du scan via la fenêtre « Détection des machines » et se termine par l'affichage du résultat dans la fenêtre « liste des agents » de la figure V-5.

a) Fenêtre « Détection des machines » :

L'administrateur peut lancer la détection des machines en cliquant sur le bouton « lancer le scan » ou aller au menu principal, cliquer sur fonction puis sélectionner

« Lancer scanne », la fenêtre de la figure ci-dessous s'affiche. Pour lancer l'opération on utilise le bouton « Lancer », pendant le déroulement on peut également l'arrêter en cliquant sur le bouton « Arrêter ». (FigV-4)

Dans cette fenêtre en affiche l'état d'avancement de la détection des machines sur la une plage d'adresses, l'adresse IP en cours et la plage d'adresses sur laquelle la détection des machines s'effectue.



FigV-4 : Fenêtre « Détection des machines»

b) Fenêtre « Afficher la liste des agents détectés » :

Cette fenêtre permet d'afficher le résultat de la détection des machines, elle présente la liste des agents sous forme d'icônes. Chaque type d'agent est

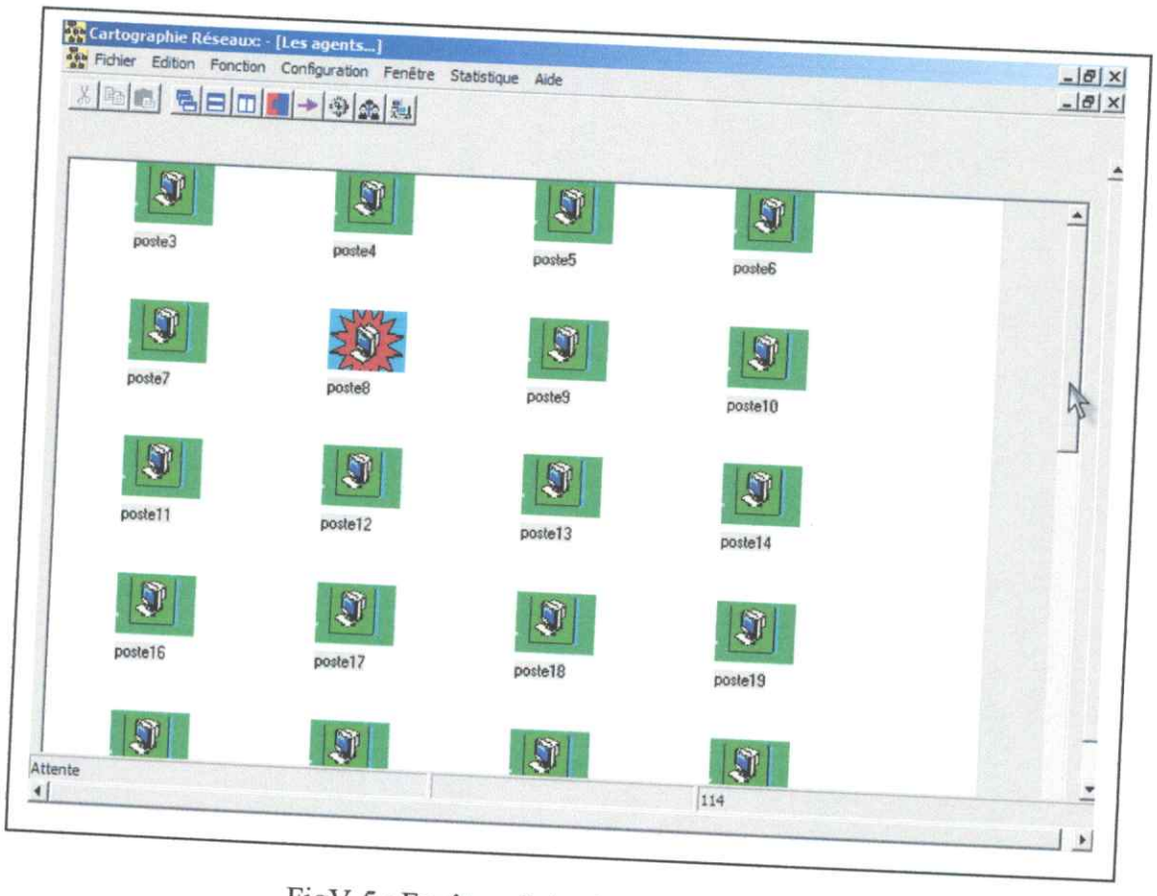
présenté par une icône selon son état (actif, éteint ou nouveau).Ou dessous de l'icône on affiche le nom de la machine pour les switchs, hubs et imprimantes. Les machines de type serveur ou station de travail on affiche le nom d'utilisateur, s'il n'y a pas d'utilisateur on affiche le nom de la machine comme le montre la figure V-5.

Pour afficher cette fenêtre, il faut cliquer sur le bouton « afficher les agents » ou aller au menu principal cliquer sur « fenêtre » puis sélectionner « liste des agents ». L'administrateur peut supprimer un agent, enregistrer les nouveaux agents, voir les propriétés d'un agent ou explorer la MIB d'un équipement en utilisant le «pop-menu».

Le tableau suivant donne les différentes icônes utilisées et leurs significations.

Icône	Signification	Icône	Signification
	Station de travail éteinte		Hub allumé
	Switch éteint		Hub éteint
	Switch allumé		Nouvelle Station de travail
	Serveur éteint		Station de travail allumée
	Serveur allumé		Imprimante

TabV-1:Lesicônesutilisésdanslesupervise



FigV-5 : Fenêtre «liste des agents»

2-4. Lancement de détection de la topologie :

Cette opération est lancée via la fenêtre de la figure V-6. Elle permet de détecter la topologie utilisée dans le réseau. Elle se termine par la fenêtre du choix de la racine de l'arbre de topologie de la figure V-7.

4-a)Etat d'avancement de la détection :

Via cette fenêtre, l'utilisateur peut lancer l'opération de détection de topologie en cliquant sur le bouton « Lancer ».

Pour accéder à cette fenêtre, aller au menu principal, cliquer sur « Fonction » ensuite sélectionner « Détecter la topologie ». (Fig V-6)

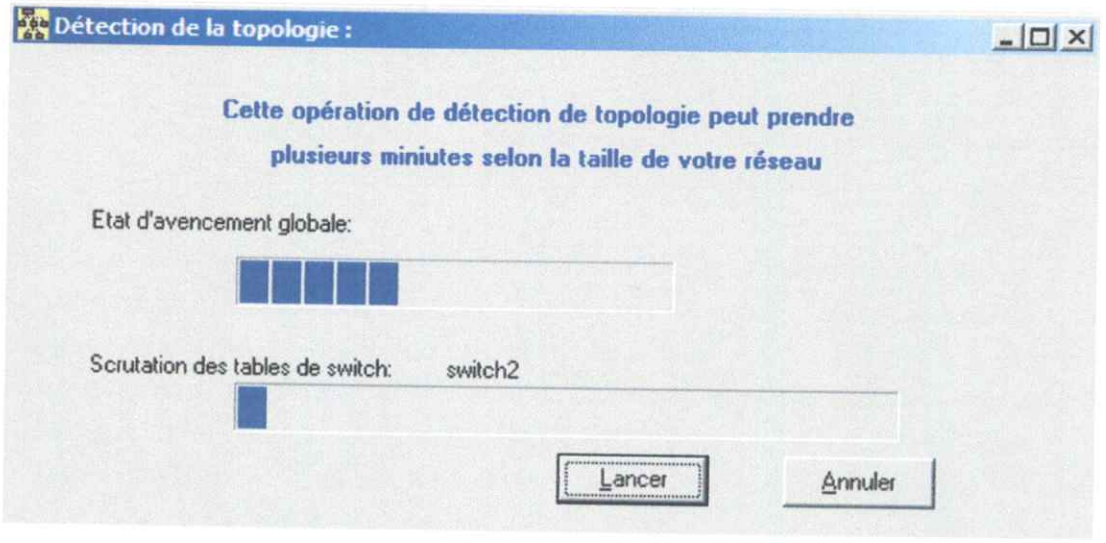
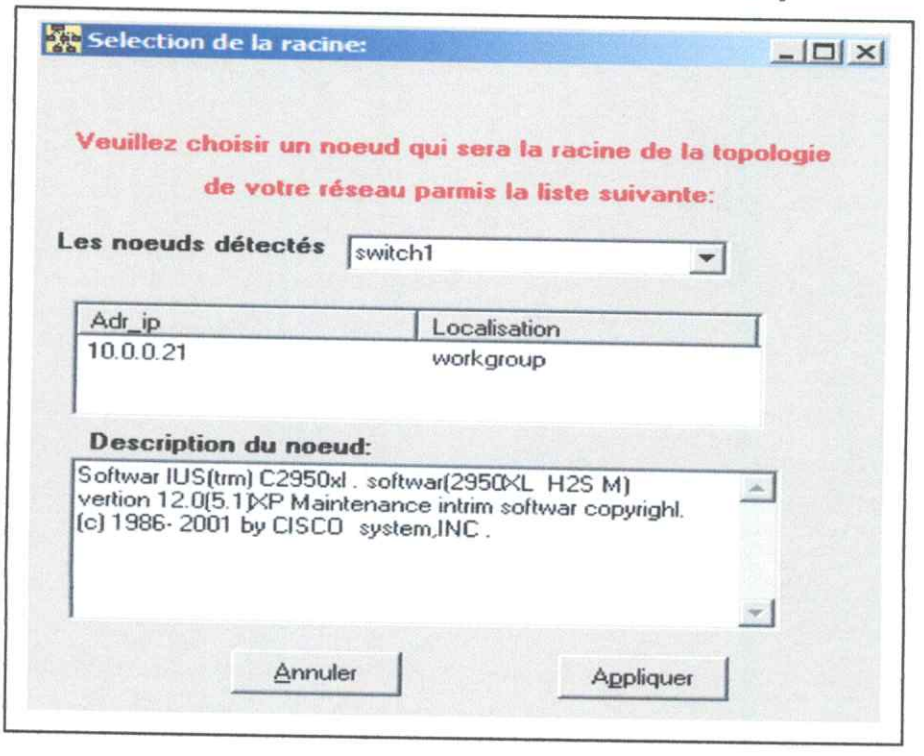


Fig V-6 : Etat d'avancement de détection de topologie

4-b) Fenêtre « Sélection de la racine» :

Cette fenêtre permet à l'administrateur de choisir la racine de l'arborescence parmi une liste des switchs, après la phase de détection de la topologie. Cette fenêtre (FigV-7) se déclanche automatiquement après la fin de détection de topologie. Les switchs proposés par cette fenêtre sont ceux qui ont le plus grand nombre de switchs fils direct.

Dans cette fenêtre on affiche l'adresse IP, la localisation et la description du switch sélectionné pour aider l'administrateur à faire un choix juste.



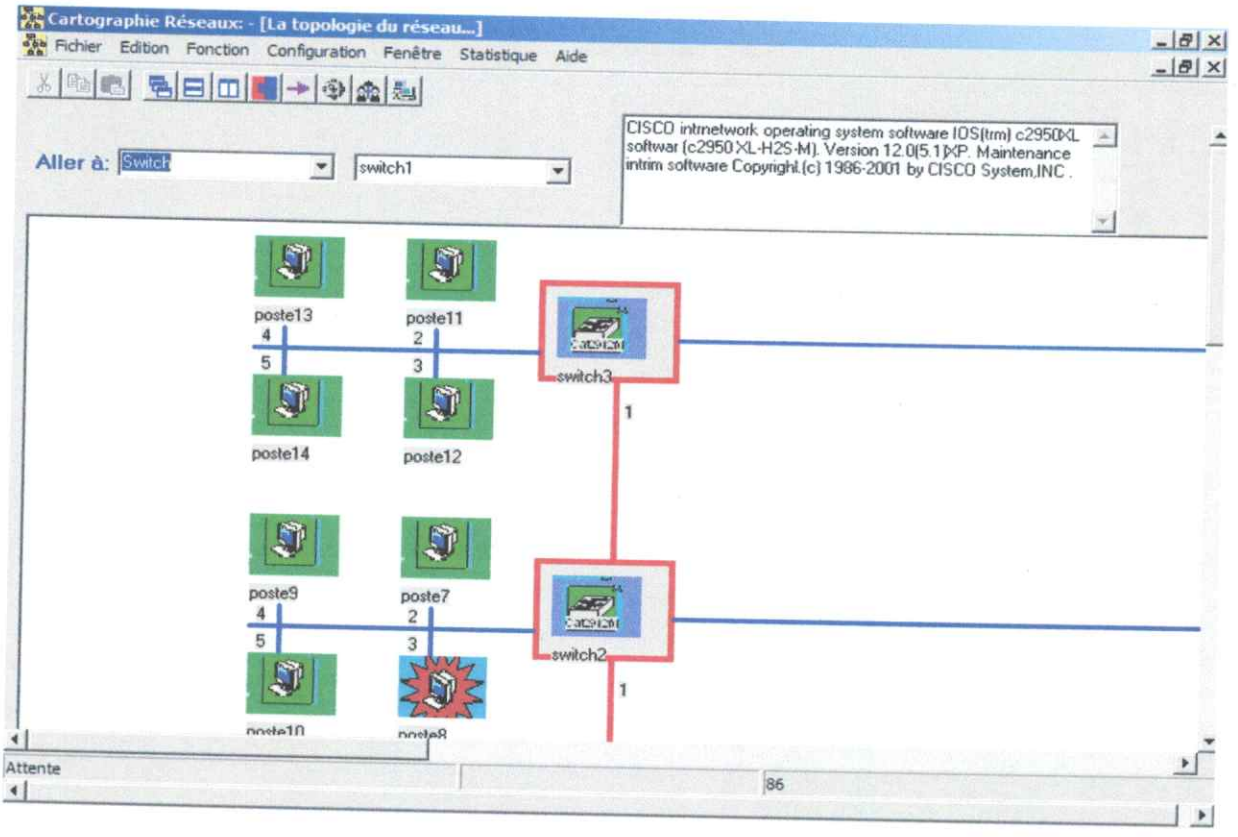
FigV-7 : Fenêtre « Sélection de la racine»

2-5. Présentation de la topologie :

Il y a deux fenêtres qui présentent la topologie du réseau ; la permière donne la cartographie détaillée du réseau et la deuxième présente la topologie sous forme d'arborescence.

a) Fenêtre « Cartographie du réseau » :

Cette fenêtre donne une vue détaillée de l'arborescence du réseau, car elle affiche notamment les Switchs et Hubs ainsi que tous les autres équipements connectés aux noeuds, elle donne la connectivité entre les hôtes (poste de travail, serveur, imprimante) et les équipements d'interconnexion (Switch,Hub) avec le numéro du port auquel une machine est connectée .Pour accéder à cette fenêtre, il faut cliquer sur le bouton « Présenter l'arborescence ». (FigV-8)



FigV-8 : Fenêtre «Cartographie du réseau»

L'administrateur peut parcourir la cartographie en utilisant la fonction « Aller à ». Lorsqu'il sélectionne un équipement parmi la liste des machines les deux barres de défilement changent afin de visualiser l'équipement sélectionné et afficher sa description.

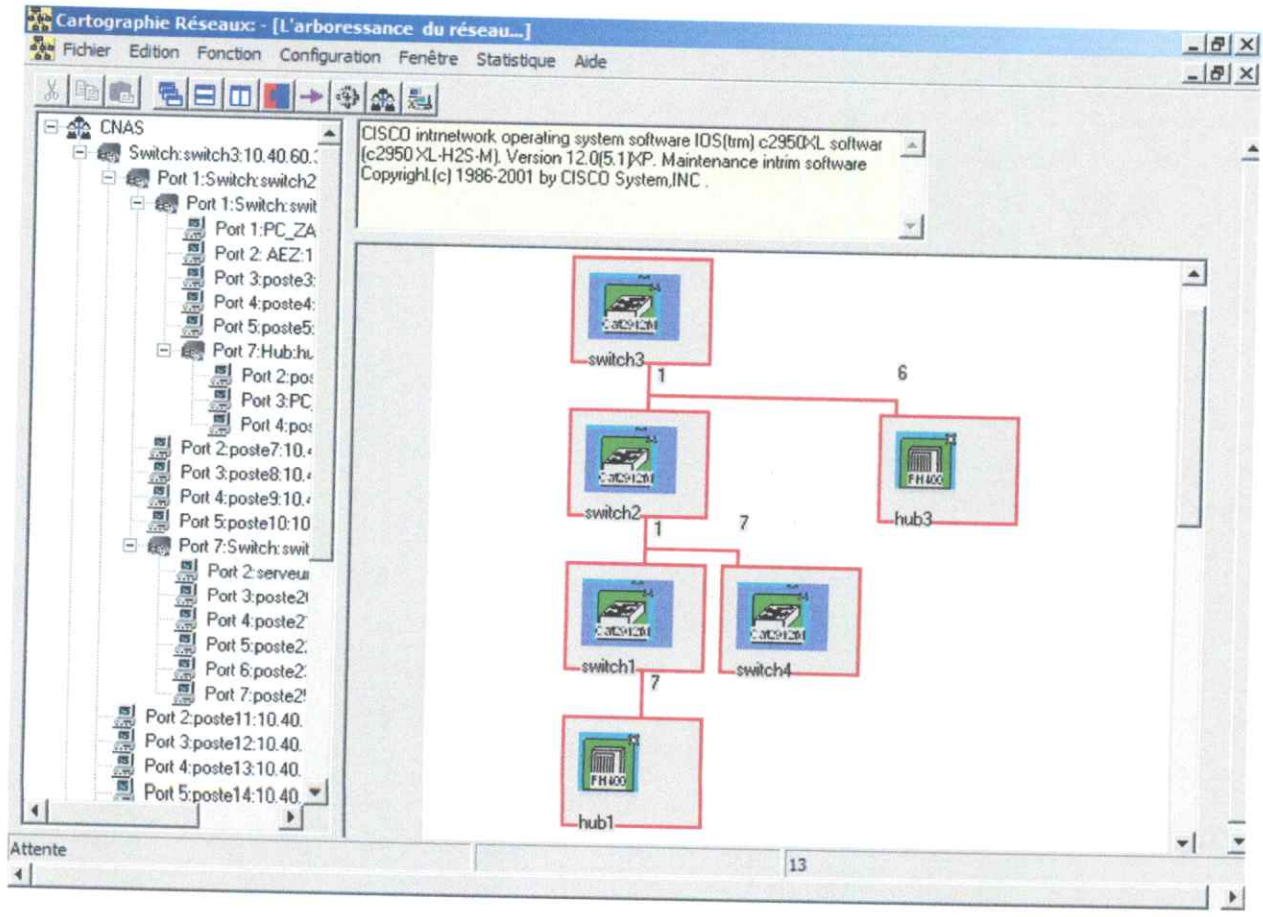
b) Fenêtre « Arborescence du réseau » :

Cette fenêtre affiche la topologie générale du réseau, c'est à dire seulement les noueds (switchs et hubs). Pour afficher cette fenêtre, il faut aller au menu principal, cliquer sur « Fenêtre » puis sélectionner « arborescence du réseau ». Elle est composée de deux parties comme le montre la figure V-9:

• La partie (1) de la figure V-9 : Dans cette partie on affiche l'arboréssance du réseau avec les numéros des ports. Dans la racine de l'arboréssance on mit les machines qui ne sont pas encore ajoutées à la cartographie pour permettre à l'administrateur de les ajoutées manuellement.

• La partie (2) de la figure V-9: Dans cette zone on affiche la cartographie du réseau, mais on ne présente que les nœuds, c'est à dire les switchs et les hubs avec les numéro du ports.

• Dans La zone (3) de la figure V-9 : On affiche la déscription du noeud sélectionné. Cette zone est invisible lorsqu'il n'y a pas un noeud sélectionné.



FigV-9 : Fenêtre « Arborescence du réseau »

6- L'ajout des éléments dans la topologie :

L'administrateur peut ajouter des éléments à la cartographie manuellement soit :

• Parce que l'opération de détection de topologie n'a pas introduit toutes les machines du réseau dans la cartographie, cela est dû à la présence des hubs qui n'ont pas la table de correspondance (adresse MAC, numéro de port).

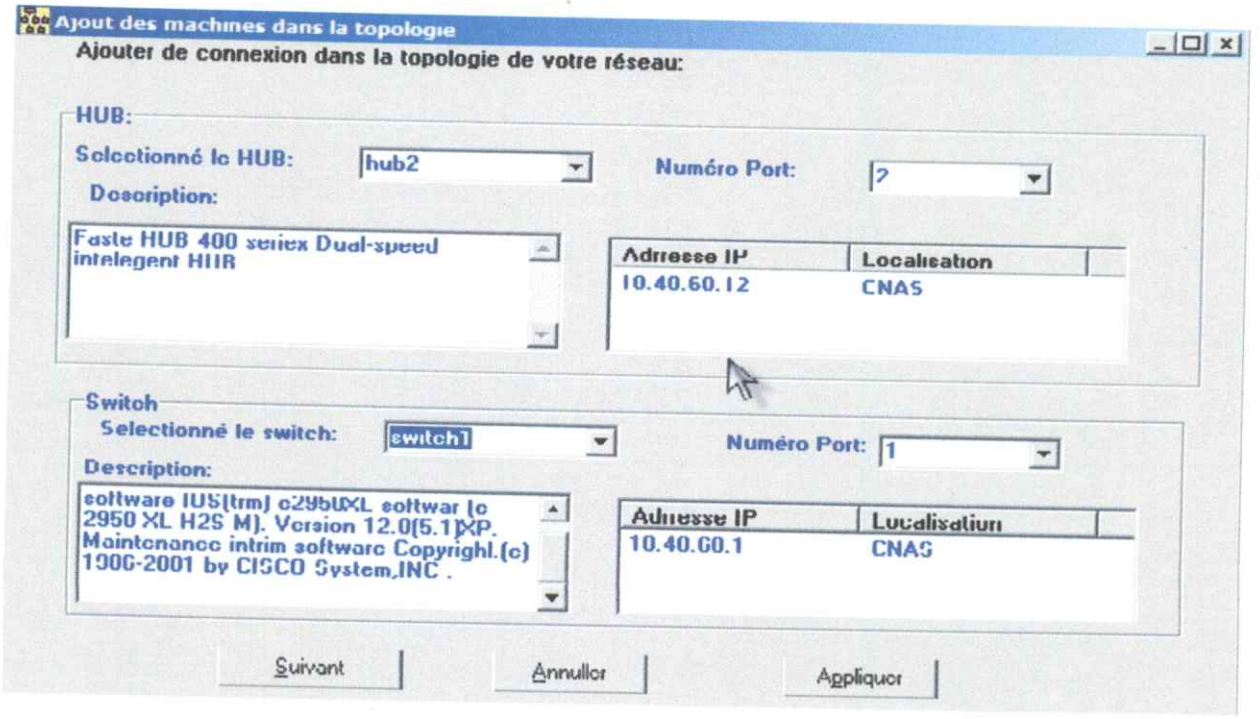
• Parce qu'il y a un nouvel équipement dans le réseau et l'administrateur ne veut pas lancer l'opération de détection de topologie à nouveau.

• L'administrateur a fait une erreur lors de l'ajout d'une machine dans la cartographie et veut la corriger.

6-a) Fenêtre « ajouter un Hub à la cartographie » :

Cette fenêtre permet d'ajouter un Hub à la cartographie en donnant à l'administrateur les noms des Hubs libres (non associer à un noeud dans la cartographie) et la liste des nœuds de la cartographie qui n'ont pas des ports vides. L'administrateur sélectionne le Hub, et le numéro du port puis il sélectionne le père du Hub et à quel numéro de port le connecter.

Pour accéder à cette fenêtre, il faut utiliser le pop menu de la fenêtre cartographie (figure V-8) ou la fenêtre d'arborescence (figure V-9), puis cliquer sur « Ajouter un Hub».



FigV-10 : Fenêtre « L'ajout d'un Hub »

Pour valider ses choix l'administrateur clique sur le bouton « Appliquer », alors la fenêtre (Fig V-11) s'affiche pour inviter l'administrateur à donner les machines qui sont branchées sur ce hub.

6-b) Fenêtre « associer les machines au Hub ajouté » :

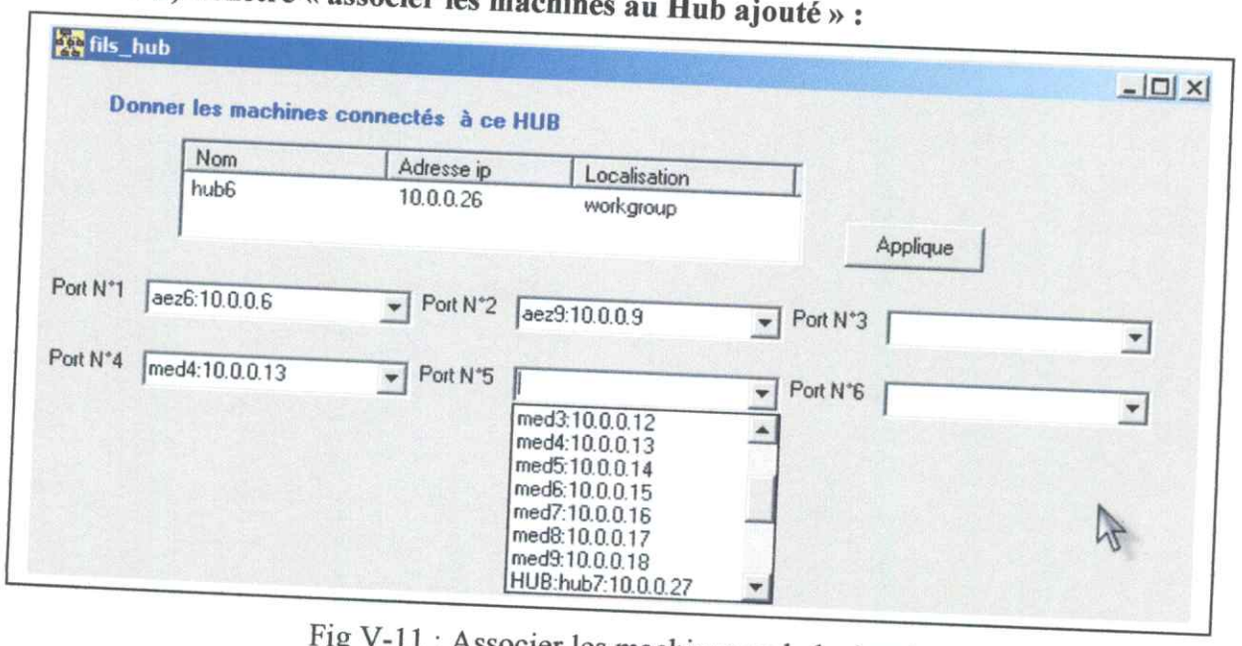


Fig V-11 : Associer les machines au hub ajouté

Cette fenêtre est composée de plusieurs listes déroulantes ou chacune d'elle correspond à un port du hub. Ces listes contiennent les machines non associes à aucun nœud dans la cartographie. La liste qui correspond au port sur le quelle le hub est branche avec un nœud est désactivée comme le montre le numéro (1) de

La figure V-11.

6-c) Fenêtre « ajouter une machine libre à un noeud » :

Cette fenêtre permet à l'administrateur d'ajouter une machine dans son réseau, en sélectionnant la machine parmi la liste des équipements libres, puis il sélectionne à quel switch ou Hub veut associer cette machine. (Fig V-12)

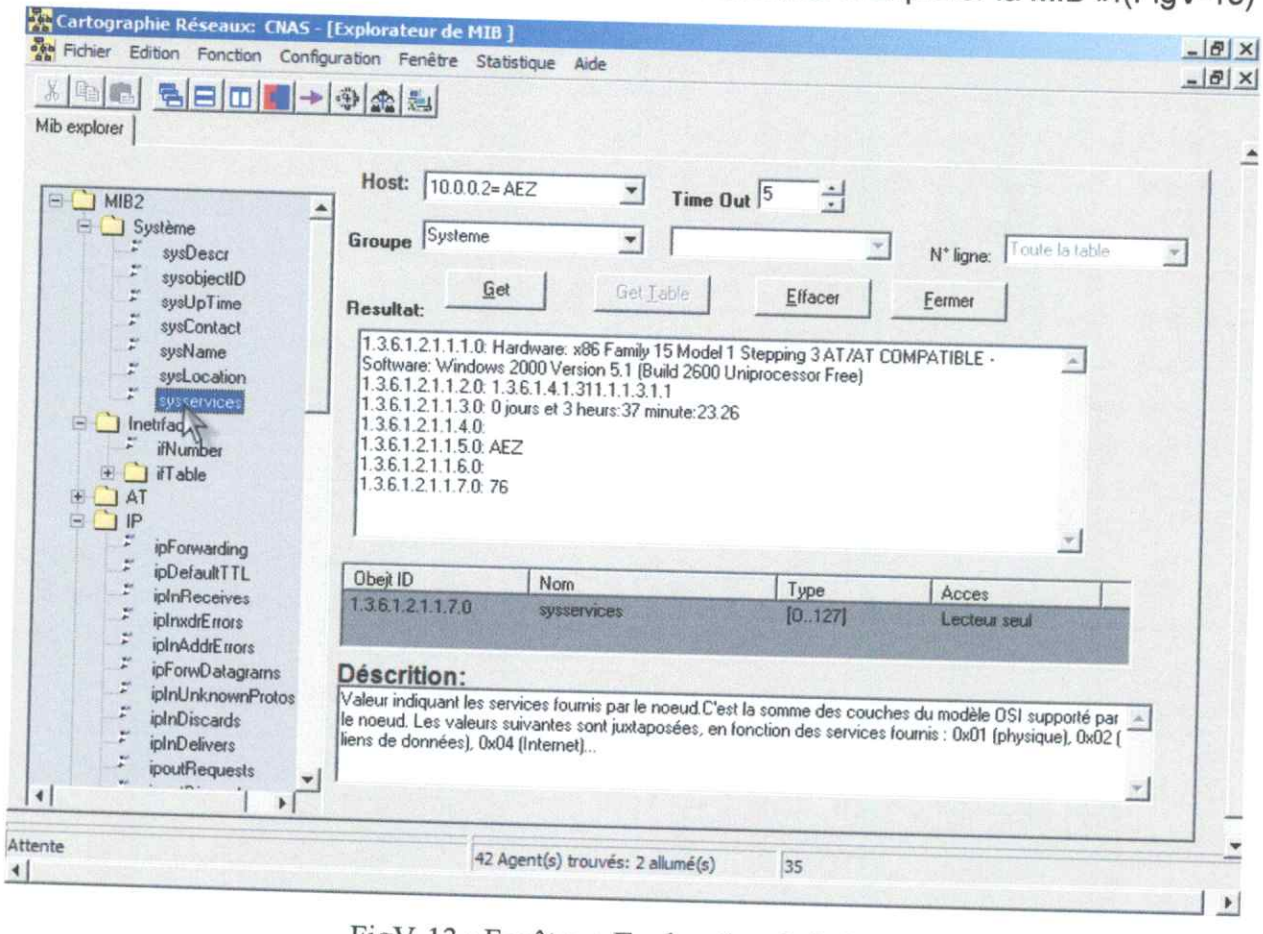
Fig V-12 : Fenêtre « L'ajout d'une machine »

Pour accéder à la fenêtre V-12, il faut utiliser le pop menu de la fenêtre cartographie(figure V-8) ou la fenêtre d'arborescence (figure V-9), puis cliquer sur «Ajouter une machine».

2-7. L'exploration de la MIB d'un agent :

Cette fenêtre permet à l'administrateur d'interroger les MIB des différents équipements qui existent dans le réseau, sachant que l'agent SNMP doit être intégré dans n'importe quel équipement.

Pour accéder à l'explorateur de la MIB, on clique sur l'agent concerné par le bouton droit de la sourie, ensuite cliquer sur « Explorer la MIB », ou aller au menu principal, on clique sur « Fonction » ensuite sélectionner « Explorer la MIB ».(FigV-13)

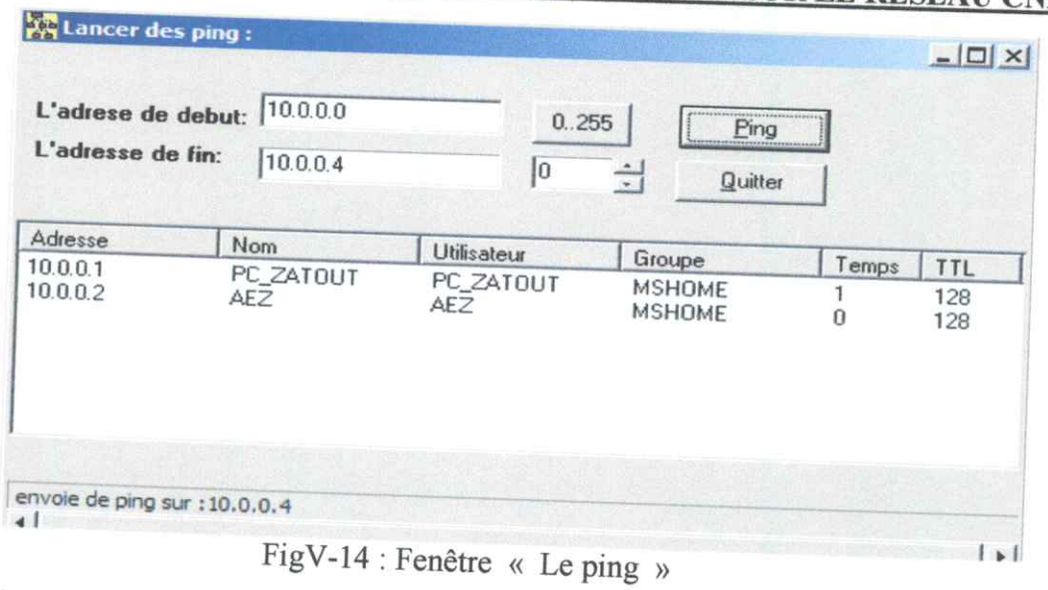


FigV-13 : Fenêtre « Exploration de la MIB»

2-8-L'utilisation du Ping :

Cette fenêtre permet d'envoyer des requêtes ping sur une plage d'adresses IP et d'afficher la liste des machines actives sur cette plage, en donnant le nom de la machine active, le nom de la session ouverte sur la machine et le nom du groupe, , le temps de réponse et le TTL (Time To live).

Pour accéder à cette fenêtre il faut aller au menu principal, cliquer sur « fonction » , ensuite sélectionner « Ping ». (FigV-14)



FigV-14 : Fenêtre « Le ping »

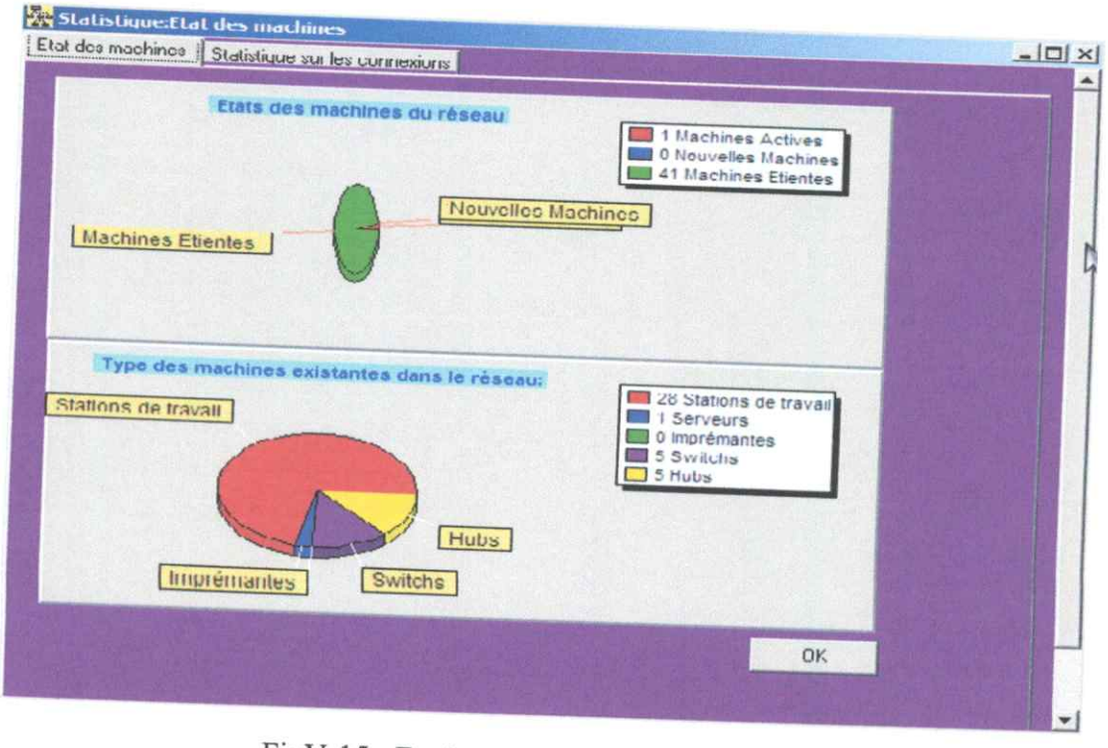
2-9. Statistiques :

Ce volet comporte deux fenêtres qui sont :

a) Fenêtre « Etats des machines » :

Cette fenêtre permet de donner une idée générale sur l'état du réseau. Elle donne le pourcentage des machines actives ou éteintes ainsi que les nouvelles machines connectées. Cette fenêtre permet aussi de donner le nombre des différents types de machines existantes dans le réseau. (FigV-15)

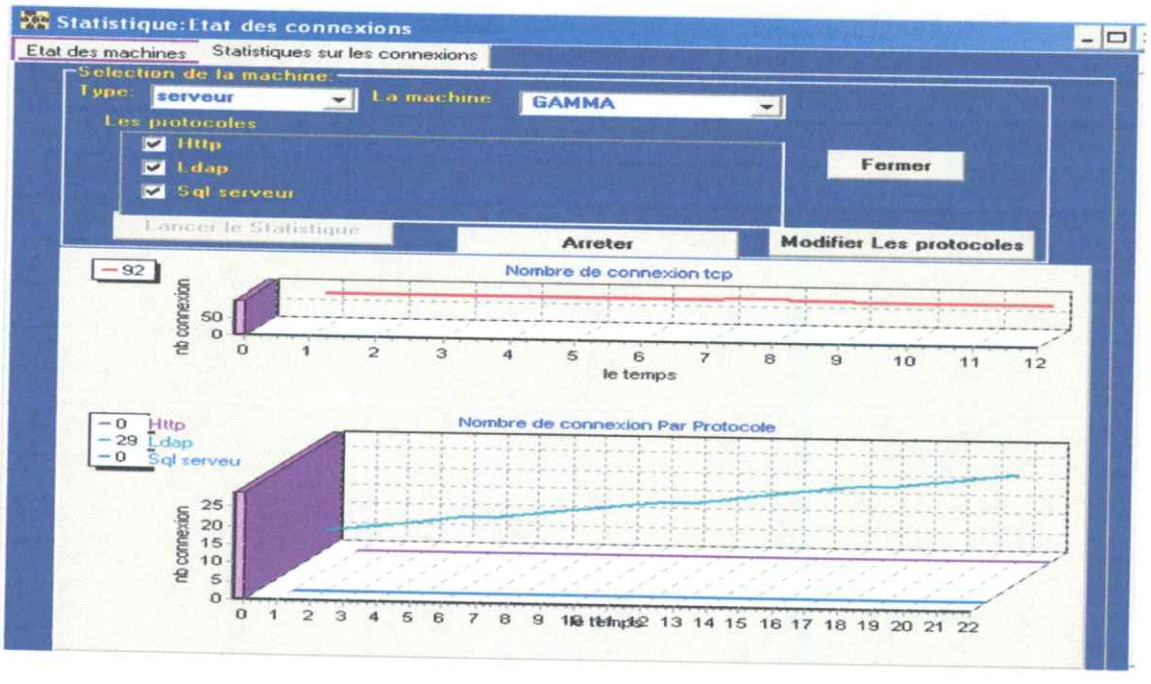
Pour accéder à cette fenêtre, il faut aller au menu principal, cliquer sur « Statistique », ensuite sélectionner « Etats des machines ».



FigV-15 : Fenêtre « Etats des machines »

b) Fenêtre « statistique sur les connexions » :

Cette fenêtre permet de donner le nombre des connexions TCP des différents ports d'une machine. Pour accéder à cette fenêtre, il faut aller au menu principal, cliquer sur « Statistique », ensuite sélectionner « Statistique sur les machines ». (FigV-16) L'administrateur sélectionne la machine concernée et les protocoles sur lesquelles il veut avoir des statistiques. Cette fenêtre comprend deux graphes.



FigV-16 : Fenêtre « statistique sur les connexions »

• Le graphe (1) de la figure V.16 : Ce graphe donne la variation de nombre de connexion TCP en fonction du temps de la machine sélectionnée.

• Le graphe (2) de la figure V.16 : Ce graphe est composé de plusieurs courbes de couleurs différentes. Chaque courbe correspond à la variation de nombre de connexion TCP sur un des protocoles sélectionnés.

• Le bouton (3) de la figure V-16 : Il permet d'afficher la fenêtre V-17 pour ajouter un protocole, modifier ou de suppression des protocoles sur lesquels l'administrateur veut effectuer des captures.

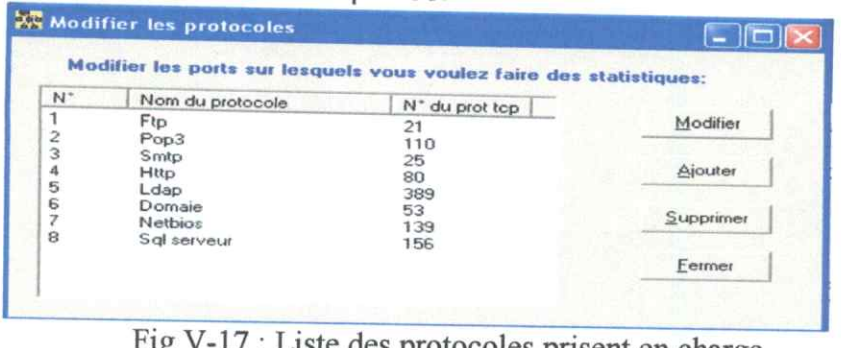


Fig V-17 : Liste des protocoles prisent en charge

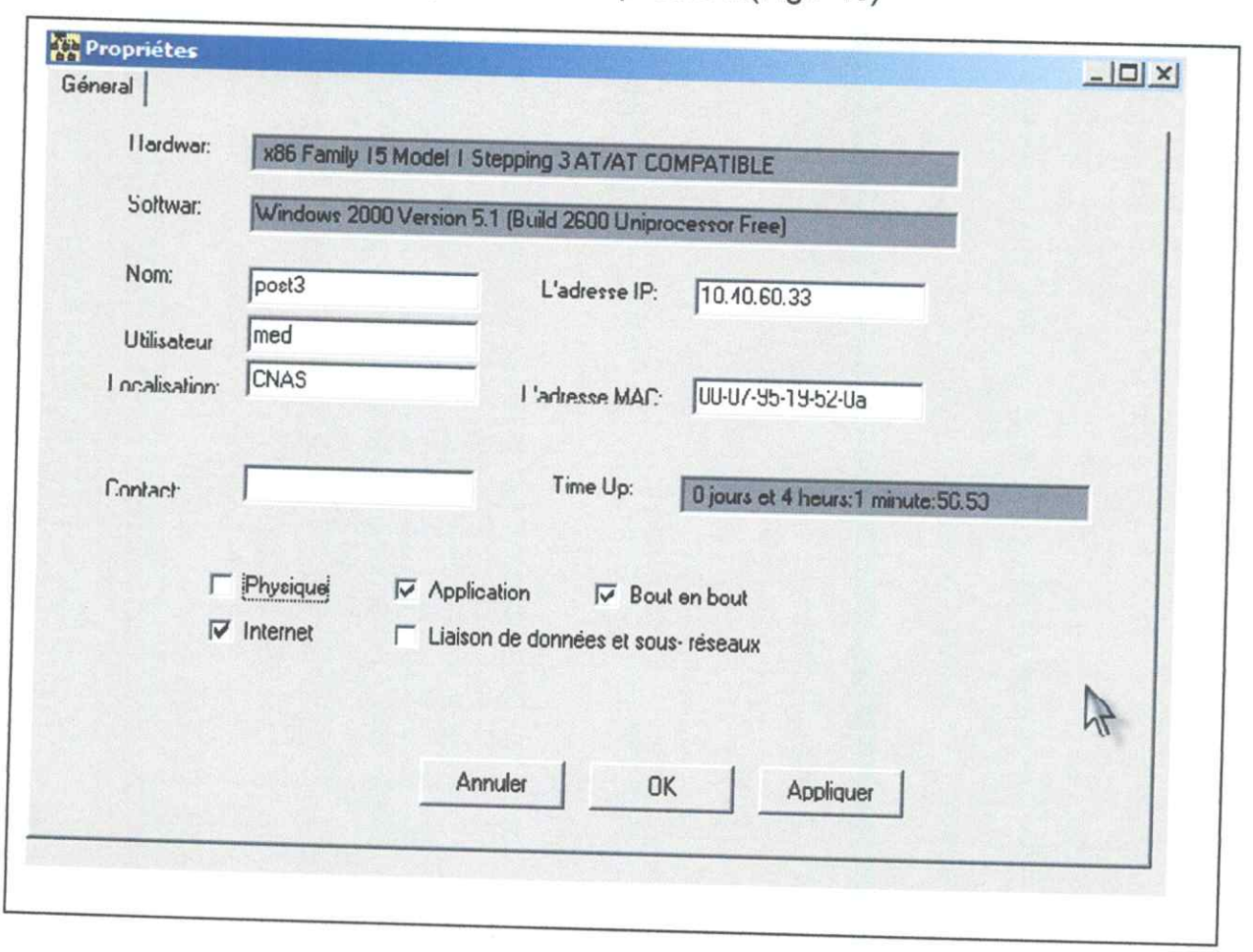
• Le bouton « Modifier » permet de modifier le nom, le numéro ou la couleur de présentation d'un protocole sélectionné parmi la liste des protocoles.

• Le bouton « Ajouter » permet d'ajouter un protocole dans la liste ; l'administrateur donne le nom, le numéro de port et la couleur de présentation du graphe de variation de nombre de connexion sur ce port en fonction de temps.

2-10. Visualisation des propriétés d'un agent :

Cette fenêtre permet de visualiser les propriétés d'un agent sélectionné, elle donne des propriétés spécifiques à chaque équipement intégrant l'agent SNMP.

Pour accéder à cette fenêtre, il faut cliquer sur l'agent concerné par le bouton droit de la souris, ensuite cliquer sur « Propriétés ».(FigV-18)



FigV-18 : Fenêtre «Propriétés d'un agent»

V-3. Conclusion:

L'utilisation du superviseur doit être sur une station de travail liée au réseau via un port qui appartient à tous les VLANs.

Nous avons testé notre superviseur sur les systèmes d'exploitation Windows 2000 et XP, Il marche aussi sur Millinieum et Windows 98 mais il faut ajouter dans le même répertoire du superviseur ou dans le répertoire « system32 » la bibliothèque WSNMP32.DLL. Lors du test de notre superviseur dans la station de travail de l'administrateur réseau de la CNAS, nous avons obtenu dans la cartographie que les switchs et les machines connectées directement aux switchs. Les hubs et les machines connectées aux hubs ont été ajoutées manuellement dans la cartographie. Pour cela, il se peut qu'il y ait des erreurs dans les liens entre les hubs et les stations de travails car nous n'avons pas toute la topologie du réseau de la CNAS.

RESUME :

Avoir une bonne gestion des réseaux est devenue aujourd'hui une nécessité pour assurer une bonne exploitation des ressources. La gestion concerne le domaine de la configuration, de performances, d'anomalies, de comptabilité et de sécurité. Le protocole SNMP est devenu un standard dans ce domaine.

Ce que nous avons présenté rentre dans le cadre d'offrir à l'administrateur un outil de gestion de performances et d'anomalies d'un réseau Ethernet TCP/IP en utilisant le protocole SNMP. Cet outil présente la topologie du réseau sous forme d'une cartographie.

Mots clés :

Gestion des réseaux, SNMP, Découverte de la topologie, Cartographie, MIB, Agent SNMP.

ABSTRACT:

To acquire a good management of networks today became a necessity to assure a good exploitation of resources. The management regards the domain of the profile, of performances, of anomalies, accounting and security, the SNMP protocol became a switchboard in this field.

This Work includes in the setting to offer to the administrator a management tool of performances and anomalies of a network Ethernet TCP/IP with the use the SNMP protocol. This tool presents the topology of the network under shape of cartography.

Key words:

Network management, SNMP, Discovery Topology, Cartography, MIB, Agent SNMP.

ملخص:

أصبح تسييرةـكبش المعلوماتية فى يومنا هذا شيء حتمي للاستغلال الجيد و العقلاني للموارد . تسيير الشبكات يتضمن عدة مجالات: مجال تسير القدرات . مجال تسير الخلل, مجال المحاسبة و الأمن .لقد أصبح البروتوكول SNMP الرائد في هذا المجال .

ان هذا العمل يندرج في اطار اعطاءريـــسـه الشبكة آداة للتسيير الجيد للقدرات و الخلل في شبكة المعلوماتية المحلية من نوع (Ethernet TCP/IP) وذلك باستعمال البروتوكول SNMP. هذه الأداة تقوم برسم خريطة الشبكة.

المفاتيح :

تسيير شبكة المعلوماتية، اكتشاف الشبكة، خريطة الشبكة، البروتوكول SNMP .

BIBLIOGRAPHIE

Livres :

[Rich2001] W.Richard Stevens «TCP/IP illustre protocoles» volume 1 Vuibert édition 2001.

[Doug2000] Douglas Comer «TCP/IP Architecture Protocoles Applications », DUNOD, 3ieme edition 2000 .

[Gil1998] Gilbert Held «Ethernet network » second edition 1998 .

[And1997] Andrew Tanenbaum « Réseaux », PRENTICE HALL 3emeédition 1997 .

[Puj2000]. Pujolle « Les réseaux » Eyrolles 3 ieme édition 2000.

[Mc2002] Steve McQuery « INCD Interconnexion des Systèmes réseaux Cisco » édition 2002.

[Pie97] Pierre Alain Muller « Modélisation objet avec UML » édition 1997.

[Ham 2003] Hamlati Anis, Zentor Hanane Kheira « Gestion des Réseaux » mémoire de fin d'étude d'ingénieur année 2003 université de BLIDA.

Internet :

[Biz97] Bizien Vincent et Fontaine Jean-Guilllaume « La gestion de réseaux SNMP et CMIS/CMIP » année 97 EPITA.

[Cha99] Charlemagne Gomez, Florent Ledru et Franck Tegnet « gestion de réseaux et protocoles » année 99 EPITA.

[Del96] Delobelle Alexis et Demaison Ludovic« La gestion des réseaux informatiques » année 96 EPITA

[Oli 2001] Olivier Willm « Administration des réseaux informatique » Technique d'ingénieur 2001 article (IP3000) année 2001.

ANNEXE A : DESCRIPTION DE LA MIB-II :

1.Groupe system :

Nom	Type de données	R/W	Description
sysDescr	Displaystring		Description textuelle de l'entité.
sysobjectID	ObjectID		Identificateur du vendeur dans le sous-arbre 1.3.6.1.4.1
sysUpTime	TimeTicks		Temps en centièmes de seconde depuis le redémarrage du management de réseau.
sysContact	DisplayString	•	Nom de la personne et comment la contacter.
sysName	Displaystring	.	Nœud du nom de domaine (FQDN).
sysLocation	DisplayString	•	Localisation physique du nœud.
sysservices	[O..127]		Valeur indiquant les services fournis par le noeud. C'est la somme des couches du modèle OSI supporté par le noeud. Les valeurs suivantes sont juxtaposées, en fonction des services fournis : 0x01 (physique), 0x02 (liens de données), 0x04 (Internet), 0x08 (application).

Figure 1 :Variables simples dans le groupe system

2.Groupe interface :

Nom	Type de données	R/W	Description
ifNumber	INTEGER		Nombre d'interfaces réseau sur le système

Figure 2 Variable simple groupe *ifInterface*

Table d'interface, index = <*IfIndex*>			
No	Type de	R/W	Description
iflrndex	INTEGER		Index de l'interface, entre 0 et if Number.
ifDescr	Displaystring		Description textuelle de l'interface.
ifType	INTEGER		Type, par exemple : 6=Ethernet, 7=802.3 Ethernet, 9=802.5 token ring, 23=PPP, 28=SLIP, et beaucoup d'autres valeurs.
ifmtu	INTEGER		MTU de l'interface.
ifspeed	Gauge		Vitesse en bits/sec.
ifPhysAddress	PnysAddress		Adresse physique, 0 pour les interfaces sans adresse physique (ex : liaisons séries.
ifAdminstatus	[1-3]	•	Etat désiré de l'interface : 1=up, 2=clown, 3=testing.
ifoperstatus	[1-3]		Etat courant de l'interface : 1=up, 2=clown,
ifLastchange	TimeTicks		Valeur de sysUpTime quand l'interface est entrée dans l'état actuel.
iflnoctets	counter		Nombre total d'octets reçus, y compris les caractères de trame.

ifInUcastPkts	counter		Nombre de paquets unicasts délivrés aux couches supérieures,
ifInNUcastPkts	counter		Nombre de paquets non unicasts (ex : broadcast ou multicast) délivrés aux couches supérieures.
ifInDiscards	counter		Nombre de paquets reçus rejetés même s'il n'y avait pas d'erreurs dans le paquet (ex : out of buffers.
ifInErrors	counter		Nombre de paquets reçus rejetés à cause d'erreurs.
ifInUnknownProtos	counter		Nombre de paquets reçus rejetés à cause d'un protocole inconnu.
ifoutoctets	counter		Nombre total d'octets transmis, y compris les caractères de trame.
ifoutUcastPkts	counter		Nombre de paquets unicasts reçus des couches Supérieures.
ifoutNUcastPkts	counter		Nombre de paquets non unicasts (ex : broadcast ou multicast) reçus des couches supérieures.
ifoutDiscards	counter		Nombre de paquets sortants rejetés même s'il n'y avait pas d'erreurs dans le paquet (ex : out of buffers.
ifoutErrors	counter		Nombre de paquets sortants rejetés à cause d'erreurs.
ifoutQLen	Gauge		Nombre de paquets dans la file d'attente de sortie.
ifSpecific	GbjectiD		Une référence à la définition de la MIB spécifique à ce type de média.

Figure 3 Table d'interface

3.Groupe AT :

Table de translation d'adresse, index = *<atIfIndex>.1.<atNetAddress>*			
Nom	**Type de données**	**R/W**	**Description**
atIfIndex	INTEGER		Numéro d'interface:ifIndex
atPhysAddress	PhysAddress	•	Adresse physique. (entrée est invalidée
atNetAddress	Network Address	•	si la longueur de la chaîne est 0.Adresse IR

Figure 4 Table de translation d'adresses : atTable

4.Groupe ip :

Nom	**Type de données**	**R/W**	**Description**
ipForwarding	[1_2]	•	1 signifie que le système retransmet les datagrammes IP, et 2 qu'il ne le fait pas.
ipDefaultTTL	INTEGER	•	Valeur de TTL par défaut quand la couche de transport n'en fournit pas.
ipInReceives	counter		Nombre total de datagrammes IP reçus de toutes les interfaces.

ipInxdrErrors	counter		Nombre de datagrammes IP rejetés à cause d'erreurs d'en-tête (ex : erreur de somme de contrôle, mauvais numéro de version, TTL dépassé, etc..
IpInAddrErrors	counter		Nombre de datagrammes IP rejetés à cause d'une erreur d'adresse.
ipForwDatagrams	counter		Nombre de datagrammes IP avec essai de transmission
ipInUnknownProtos	counter		Nombre de datagrammes IP adressés localement avec un champ protocole invalide.
IpInDiscards	counter		Nombre de datagrammes IP reçus rejetés à cause d'un manque d'espace buffer.
IpInDelivers	counter		Nombre de datagrammes IP délivrés à un module de protocole approprié.
IpoutRequests	counter		Nombre total de datagrammes IP passés à IP pour transmission. N'inclue pas ceux qui sont comptés par ipForwDatagram.
IpoutDiscards	counter		Nombre de datagrammes IP sortants rejetés à cause d'un manque d'espace buffer.
IpoutNoRoutes	counter		Nombre de datagrammes IP rejetés parce qu'aucune route n'a été trouvée.
ipReasmTimeout	INTEGER		Nombre de secondes maxi pendant lesquelles les fragments reçus sont maintenus avant ré assemblage.
IpReasmRegdq	counter		Nombre de fragments IP reçus qui ont besoin d'être rassemblés.
IpReasmoxs	counter		Nombre de datagrammes IP rassemblés avec succès.
IpReasmFails	counter		Nombre d'échec de l'algorithme de ré assemblage IP
IpFragsORs	counter		Nombre de datagrammes IP qui ont été fragmentés avec succès.
IpFragFails	counter		Nombre de datagrammes IP qui avaient besoin d'être fragmentés, mais qui n'ont pas pu l'être à cause du flag «dont fragment».
IpFragcreates	counter		Nombre de datagrammes IP générés par fragmentation.
ipRoutingDiscards	counter		Nombre d'entrées de routage rejetées même si elles étaient valides.

Figure 5 Variables simples dans le groupe ip

Table			**index** = *<ipAdEntAddr>*
Nom	**Type de**	**R/w**	**Description**
ipAdEntAddr	IpAddress		Adresse IP pour cette ligne.
ipAdEntIfIndex	INTEGER		Numéro d'interface correspondante : ifIndex.
ipAdEntNetMask	IpAddress		Masque de sous-réseau pour cette adresse IP
ipAdEntBcastAddr	[0..1]		Valeur du bit le moins significatif de l'adresse de broadcast.Normalement 1.
ipAdEntReasmMax Size	[0..65535]		Taille du datagramme IP le plus grand qui peut être rassemblé sur cette interface

Figure 6 Table d'adresses IP : ipAddrTable

Table de routage IP, index = *<ipRouteDest>*			
Nom	**Type de données**	**R/W**	**Description**
ipRouteDest	ipAddress	•	Adresse IP de destination. Une valeur de 0.0.0.0 indique une entrée par défaut.
ipRouteIfIndex	INTEGER	•	Numéro d'interface : ifIndex.
ipRouteMetricl	INTEGER	•	Métrique de routage primaire. La signification de cette métrique dépend du protocole de routage (ipRouteProto). Une valeur de -1 signifie qu'il n'est pas utilisé.
ipRouteMetric2	INTEGER	•	Métrique de routage alternatif.
ipRouteMetric3	INTEGER	•	Métrique de routage alternatif.
ipRouteMetric4	INTEGER	•	Métrique de routage alternatif.
ipRouteNextHop	ipAddress	•	Adresse IP du routeur de saut suivant.
ipRouteType	INTEGER	•	Type de route : 1 = autre, 2 = route invalide, 3 = directe, 4 = indirecte.
ipRouteProto	INTEGER		Protocole de routage : 1 = autre, 4 = redirection ICMP, 8 = RIP, 13 = OSPF, 14 = BGP, et autres.
ipRouteAge	INTEGER	•	Nombre de secondes depuis que la route a été mise à jour ou déterminée correcte.
ipRouteMask	ipAddress	•	Le ET logique de ce masque et de l'adresse IP de destination est comparée à ipRouteDest.
ipRouteMetric5	INTEGER	•	Métrique de routage alternatif.
ipRouteInfo	objectID	•	Référence aux définitions de la MIB spécifique à ce protocole de routage.

Figure 7 Table de routage IP :ipRouteTable

Table de translation d'adresse IP, index = *<ipNetToMediaifIndex><ipNetToMediaNetAddress>*			
Nom	**Type de données**	**R/W**	**Description**
ipNetToMediaIfIndex	INTEGER	•	Interface correspondante : ifIndex.
ipNetToMediaPhysAddress	PhysAddress	•	Adresse physique.
ipNetToMediaNetAddress	IpAddress	•	Adresse IP.
ipNetToMediaType	[1_4]	•	Type de translation : 1 = autre, 2 = invalidée,3 = dynamique, 4 = statique.

Figure 8 Table de translation d'adresses IP : ipNetToMediaTable.

5. Groupe icmp

Nom	Type de données	R/W	Description
icmpInMsgs	counter		Nombre total de messages ICMP reçus.
icmpInErrors	Counter		Nombre de messages ICMP reçus avec des erreurs (ex : somme de contrôle ICMP invalide).
icmpInDestUnreachs	counter		Nbre de messages reçus ICMP destination non accessible
icmpInTimeExcds	counter		Nombre de messages reçus ICMP temps dépassé.
icmpInParmProbs	counter		Nombre de messages reçus ICMP problème de paramètre.
icmpInsrcQuenchs	counter		Nombre de messages reçus ICMP extinction de source.
icmpInRedirects	Counter		Nombre de messages reçus ICMP redirection.
icmpInEchos	counter		Nombre de messages reçus ICMP requête echo.
icmpInEchosReps	counter		Nombre de messages reçus ICMP réponse echo.
icmpInTimestamps	Counter		Nombre de messages reçus ICMP requête d'estampille
icmpInTimestampReps	Counter		Nombre de messages reçus ICMP réponse d'estampille
icmpInAddrMasks	counter		Nombre de messages reçus ICMP requête de masque
icmpInAddrMaskReps	counter		Nombre de messages reçus ICMP réponse de masque
icmpoutmsgs	Counter		Nombre total de messages ICMP envoyés.
icmpoutErrors	counter		Nombre de messages ICMP non émis à cause d'un problème d'ICMP (ex : manque de buffers).
icmpoutDestunreachs	counter		Nombre de messages émis ICMP destination non
icmpoutTimeExcds	counter		Nombre de messages émis ICMP temps dépassé.
icmpoutParmProbs	counter		Nombre de messages émis ICMP problème de paramètre.
icmpoutsrcQuenchs	counter		Nombre de messages émis ICMP extinction de source.
icmpoutRedirects	counter		Nombre de messages émis ICMP redirection.
icmpoutEchos	counter		Nombre de messages émis ICMP requête echo.
icmpoutEchosReps	counter		Nombre de messages émis ICMP réponse echo.
icinpoutTimestamps	counter		Nombre de messages émis ICMP requête d'estampille
icmpoutTimestampReps	counter		Nombre de messages émis ICMP réponse d'estampille horaire.
icmpoutAddrMasks	counter		Nombre de messages émis ICMP requête de masque d'adresse

Figure 9. Variables simples du groupe icmp.

6.Groupe tcp :

Nom	Type de données	R/W	Description
tcpConnstate	Integer [1..12]		Etat de la connexion : 1 = CLOSED, 2 = LISTEN, 3 = SYN SENT, 4 = SYN RCVD, 5 = ESTABLISHED, 6 = FIN WAIT 1, 7 = FIN _WAIT 2, 8 =CLOSE WAIT, 9 = LAST ACK, 10 = CLOSING, 11 = TIME_WAIT, 12 = efface TCB. La seule valeur à laquelle le manager peut positionner cette variable est 12 (c'est-à-dire la terminaison immédiate de la connexion).
tcpConnLocalAddress	IpAddress		Adresse IP locale. 0.0.0.0 indique que le scrutateur est d'accord pour accepter les connexions sur toutes les interfaces.
tcpConnLocalPOrt	[0..65535]		Numéro de port local.
tcpConnRemAddres	IpAddress		Adresse IP distante.
tcpConnRemPort	[0..65535]		Numéro de port distant.

Figure 10 Table de connexion TCP : tcpConnTable.

Nom	Type de données	R/W	Description
tcpRtOAlgorithm	INTEGER		Algorithme utilisé pour calculer la valeur du time out de retransmission : 1 = aucun des suivants, 2 = un RTO constant, 3 = MIL-STD-1778 Appendice B, 4 = algorithme de Van Jacob son.
tcpRtoMin	INTEGER		Valeur mini du timeout de retransmission, en millisecondes.
tcpRtoMax	INTEGER		Valeur maxi du timeout de retransmission, en millisecondes.
TcpMaxConn	INTEGER		Nombre maxi de connexions TCP.
tcpActiveopens	Counter		Valeur -1 si dynamique Nombre de transitions des états CLOSED à SYN SENT.
tcpPassiveopens	Counter		Nombre de transitions des états LISTEN à SYN RCVD.
tcpAttemptFails	Counter		Nombre de transitions des états SYN SENT ou SYN RCVD à CLOSED, plus le nombre de transitions de SYN RCVD à LISTEN.
tcpEstabResets	Counter		Nombre de transitions des états ESTABLISHED ou CLOSE WATT à CLOSED.
tcpCurrEstab	Gauge		Nombre de connexions en cours dans les états ESTABLISHED ou CLOSE WAIT.
tcpInsegs	Counter		Nombre maxi de segments reçus.
tcpoutsegs	Counter		Nombre maxi de segments émis, en excluant ceux qui contiennent seulement des octets retransmis.
tcpRetranssegs	Counter		Nombre total de segments retransmis.
tcpInErrs	Counter		Nombre total de segments reçus avec une erreur (comme une somme de contrôle invalide).
tcpoutRsts	Counter		Nombre total de segments émis avec le flag RST à 1.

Figure 11. *Variables simples dans le groupe tcp*

7.Groupe udp :

Nom	Type de données	R/W	Description
UdpInDatagrams	compteur		Nombre de datagrammes UDP délivrés aux processus utilisateur.
udpNoPorts	compteur		Nombre de datagrammes UDP reçus pour lesquels aucun processus applicable ne correspond au port de destination.
udpInErrors	compteur		Nombre de datagrammes UDP non livrables pour une raison autre que pas d'application sur le port de destination (par exemple erreur checksum UDP).
udpoutDatagrams	compteur		Nombre de datagrammes UDP émis.

Figure 12 : les variables simples de groupe udp

Nom	Type de données	R/W	Description
udpLocalAddress	IpAddress		Adresse Ip locale de scrutateur. .0.0.0.0 indique que le scrutateur voudrait recevoir des datagrammes sur n'importe quelle interface.
udpLocalPort	[0..65535]		Numéro de port local de ce scrutateur.

Figure 13 : udpTable

8-Le groupe EGP 1.3.6.1.2.1.8

Il contient les informations propres aux protocoles EGP

NOM	Type de	R/W	Description
EgpIn	counter		Le nombre total des messages EGP reçus sans erreur.
EgpErrors	counter		Le nombre total des messages EGP reçus prouvés en erreur.
EgpOutMsgs	counter		Le total de messages EGP localement produits.
EgpErrors	counter		Le nombre de messages EGP générés localement non envoyés à cause des limitations de ressources à l'intérieur d'une entité EGP.

Figure14 groupe EGP

9-groupe SNMP : 1.3.6.1.2.1.11

NOM	Type de	R/W	Description
SnmpInPkts	counter		Nombre total de PDU reçues de la couche inférieure.
SnmpOutPkts	counter		Nombre total de PDU envoyées à la couche inférieure.
SnmpBadVersions	counter		Nombre total de PDU reçues ayant un numéro de version différent du numéro local.
SnmpBadCommunityNames	counter		Nombre total de PDU ayant un nom de communauté inconnu.
SnmpBadCommunityUses	counter		Nombre total de PDU ne pouvant être traités dans le cadre de cette communauté.
SnmpInASNParseErrs			Nombre total d'erreurs au moment de l'interprétation d'un objet ASN.1
SnmpInBadTypes	counter		Nombre total de PDU avec un type inconnu

Figure15 le groupe SNMP

Code de retour

NOM	Type de	R/W	Description
SnmpInBigs	counter		Nombre de PDU reçues avec comme ErrorStatus'too bigs'(la réponse ne tient pas dans un message UDP).
SnmpInNoSuchNames	counter		Nombre de PDU reçues avec comme ErrorStatus'noSuchNames'(nom inconnu).
SnmpInBadValues	counter		Nombre de PDU reçues avec comme ErrorStatus'badValue'.
SnmpInReadOnlys	counter		Nombre de PDU reçues avec comme ErrorStatus'readOnly'.
SnmpInGenErrs	counter		Nombre de PDU reçues avec comme ErrorStatus'genErr'.

Figure16 le variable de code de retour SNMP

Objets Statiques en Entrée :

NOM	Type de	R/W	Description
SnmpInTotalReqVars			Nombre d'objets de la MIB qui ont fait l'objet d'une requête Get-Request ou get-Next .
SnmpInTotalSetVars			Nombre d'objets de la MIB qui ont fait l'objet d'une requête set-Request .
SnmpInGetRequests	counter		Nombre total de PDU Get-request traitées par le protocole SNMP.
SnmpInGetNexts	counter		Nombre total de PDU Get-Next traitées par le protocole SNMP.
SnmpInSetRequests	counter		Nombre total de PDU Set-request traitées par le protocole SNMP.
SnmpInGetRsponses	counter		Nombre total de PDU Get-Rsponse traitées par le protocole SNMP.
SnmpInTraps	counter		Nombre total de PDU Trap traitées par le protocole SNMP.
SnmpOutTooBigs	counter		Nombre total de PDU SNMP qui ont été générés par l'entité de protocole et pour lesquelles la valeur du champ 'ErrorStatus' est 'tooBig'
SnmpOutNoSuchNames	counter		Nombre total de PDU SNMP qui ont été générés par l'entité de protocole SNMP et pour lesquelles la valeur du champ 'ErrorStatus' est 'noSuchName'
SnmpOutBadValues	counter		Nombre total de PDU SNMP qui ont été générés par l'entité de protocole SNMP et pour lesquelles la valeur du champ 'ErrorStatus' est 'BadValue'
SnmpOutGenErrs	counter		Nombre total de PDU SNMP qui ont été générés par l'entité de protocole SNMP et pour lesquelles la valeur du champ 'ErrorStatus' est 'genErr'

Figure17 les objets statiques en entrée du groupe SNMP

Objets Statique En Sortie :

NOM	Type de	R/W	Description
SnmpOutGetRequests.	counter		Nombre total de PDU de type Get-Request qui ont été générés par l'entité de protocole SNMP
SnmpOutGetNexts.	counter		Nombre total de PDU de type Get-Next qui ont été générés par l'entité de protocole SNMP
SnmpOutSetRequests.	counter		Nombre total de PDU de type Set-Request qui ont été générés par l'entité de protocole SNMP
SnmpOutGetResponses.	counter		Nombre total de PDU de type Get-Response qui ont été générés par l'entité de protocole SNMP
SnmpOutTraps.	counter		Nombre total de PDU de type Trap qui ont été générés par l'entité de protocole SNMP
SnmpEnableAuthTraps	Integer		Indication sur la configuration de l'agent SNMP concernant la génération du Trap d'Authentification

Figure18 les objets statiques en sortiée du groupe SNMP

ANNEXE B : La notation abstraite de syntaxe (ASN-I)

I)Type des variables de la MIB :figure 14

Nom	type	Octets	Signification
Integer	Numérique	4	Entier (32 bits en général)
Counter32	Numérique	4	Compteur 32 bits entiers non signé
Gauge32	Numérique	4	Valeur non signé
Integer32	Numérique	4	32 bits mémé sur une UC de 64 bits
Uinteger32	Numérique	4	Comme Integer32 mais non signé
Counter64	Numérique	8	Compteur de 64 bits
TimeTicks	Numérique	4	En centième de secondes depuis un instant donné
Bit String	Chaîne	4	Suite de 1 à 32 bits
OctetString	Chaîne	>= 0	Chaîne de caractères de longueur variable
DisplayString			Une chaîne de mots de 8 bits
Objet Identifier	Chaîne	> 0	Liste d'entier
IpAddress	Chaîne	4	C'est une chaîne de 4 octets reprenant l'adresse IP
PhysAddress	Chaîne	6	C'est une chaîne d'octets spécifiant une adresse physique (par exemple une adresse Ethernet sur 6 octets).
SÉQUENCE			comparable à une structure en langage C Liste ordonnée d'autres types ASN.1
SÉQUENCE OF			vecteur, dont tous les éléments ont le même type de donnée
udpLocalAddress	IpAddress		contient l'adresse IP locale
udpLocalPort	Integer		Comprise entre 0 et 65535, qui précise le numéro de port local.

II. La notation abstraite de syntaxe (ASN.1) :

A.S.N.1 est un langage formel qui permet de définire le nom et le type des variables de la base de données d'informations d'administration MIB. La précision de cette notation élimine toute ambiguïté de forme ou de contenu au niveau des variables. Elle présente deux caractéristiques principales : Une notation utilisée dans les documents manipulés par les humains et une représentation codée de la même information, utilisée dans les protocoles de communication. Les notions suivantes concernant ASN.1 sont nécessaires à connaître pour comprendre la MIB.

a)Module

Un module ASN.1 décrit une collection d'objets. La syntaxe de déclaration d'un module A.S.N.1 est la suivante :

NomModule Definition ::=
BEGIN
Relation avec les autres modules (clauses IMPORT et EXPORTE)
Définition des objets
END

b)Objets

Les objets définis avec ASN.1 peuvent être :

- Des types, avec des types simples comme INTEGER ou BOOLEAN,et des types construits permettant de définir des listes (SEQUENCE) et des tableaux (SEQUENCE OF) ;
- Des valeurs, c'est-à-dire des objets ayant un type précédemment défini ;
- Des macros, qui permettent d'étendre les définitions et définir de nouveaux types.

Par convention, les types commencent par une majuscule, les valeurs par une minuscule et les macros sont tout entières en majuscules. Les commentaires sont précédés de deux tirets. Les types de base des objets A.S.N.1 sont données dans le tableau suivant : (tananboum)

Type	Description	Code
INTEGER	Entier 32 bits	2
OCTET STRING	Chaîne d'octets	4
BIT STRING	Chaîne de bits	3
OBJECT IDENTIFIER	Séquence d'entiers identifiant un objet à l'aide de son positionnement à partir de la racine de la MIB	5
ENUMERATION OF INTEGER	Permet de représenter une énumération de valeurs par des entiers non nuls (ex. : on(1),off :2))	5

Les types de base des données ASN.1 autorisé dans SNMP

b)Objets tabulaires :

Ils sont décrits au moyen des types construits ASN.1. Le tableau suivant donne les types des objets tabulaires supportés par SNMP est utilisée dans les MIB.

Type	Description
SEQUENCE	Liste ordonnée d'autres types ASN.1
SEQUENCE OF TYPE	Liste ordonnée d'éléments du même type

Les types tabulaires de données ASN.1 autorise dans SNMP

III.Format des messages SNMP en notation ASN.1 :

Contrairement à la plupart des protocoles TCP/IP, les messages SNMP n'ont pas une structure fixe mais utilisent la notation ASN.1.Un message SNMP contient, comme nous l'avant vu, trois parties principales : une version de protocole, un identificateur de communauté et une zone de données.

RFC1157-SNMP DEFINITIONS ::= BEGIN

IMPORTS
ObjectName, ObjectSyntax, NetworkAddress, IpAddress, TimeTicks
FROM RFC1155-SMI;
Message ::= SEQUENCE {
version INTEGER {version-1 (0)},-- Version 1 for this RFC
community OCTET STRING, -- Community name

```
data ANY -- e.g. PDUs
}
```

La zone de données se décompose en unités de données de protocole (PDU).Chaque PDU est constituée d'une demande émise par le client (le manager) ou d'une réponse émise par le serveur (l'agent).

```
-- Protocol data units
PDUs ::= CHOICE { get-request       GetRequest-PDU,
                  get-next-request  GetNextRequest-PDU,
        get-response      GetResponse-PDU,
        set-request       SetRequest-PDU,
      trap                Trap-PDU
}
GetRequest-PDU ::= [0] IMPLICIT PDU
GetNextRequest-PDU::=[1] IMPLICIT PDU
GetResponse-PDU ::= [2] IMPLICIT PDU
SetRequest-PDU ::= [3] IMPLICIT PDU

PDU ::= SEQUENCE {
      request-id INTEGER,                    -- Request identifier
      error-status INTEGER {                 -- Sometimes ignored
            noError (0),toobig (1),noSuchName (2),badValue (3),readOnly (4),genError (5)},
error-index INTEGER,                         -- Sometimes ignored
variable-binding VarBindList }               -- Values are sometimes ignored

Trap-PDU ::= [4] IMPLICIT SEQUENCE {
      enterprise OBJECT IDENTIFIER,          ,--Type of object generating trap
      agent-addr NetworkAddress               s-- Only one type of network adresses
                                             -- IP adress of object generating trap
      generic-trap INTEGER {                 -- Generic trap type
                coldStart (0),warmStart ( 1),linkDown ( 2),linkUp (3),authenticationFailure
                (4)
                egpNeighborLoss ( 5),enterpriseSpecific (6)
      } ,
specific-trap INTEGER,                       -- Specific code
time-stamp TimeTicks,                -- Elapse time since the last reinitialization of the entity
variable-binding VarBindList          -- "Interesting" information
}

-- Variable binding
VarBind ::= SEQUENCE
{name ObjectName,
value ObjectSyntax}

VarBindList ::= SEQUENCE OF VarBind
END
```

Pour compléter la définition d'un message SNMP, il est nécessaire de préciser la syntaxe de chacun des cinq types de PDU, nous avons indiqué à titre d'exemple la structure de PDU *GetRequest* et *trap*.

ANNEXE C : Installation et configuration de SNMP sous Windows 2000 :

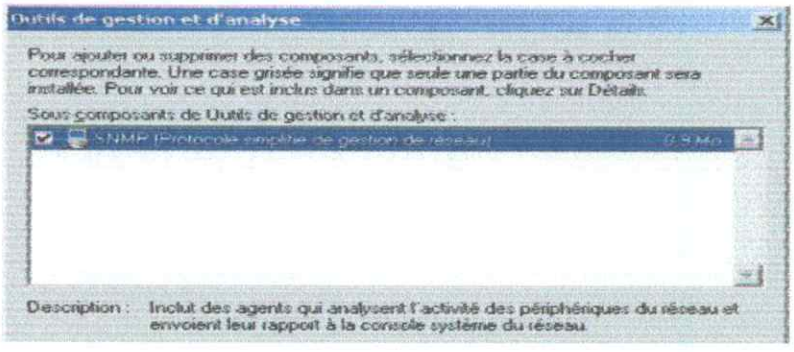
Le protocole **SNMP** (*Simple Network Management Protocol*) est implémenté en standard dans toutes les moutures de *Windows 2000*. Sa mise en place est très aisée : il suffit de suivre les étapes décrites ci-dessous.

- Dans le **Panneau de Configuration**, double-cliquez sur **Ajout/Suppression de Programmes** .

- Cliquer ensuite sur **ajout/suppression des composants Windows**

L'**Assistant Composants de Windows** s'ouvre alors. Celui-ci vous permet d'installer ou de désinstaller des composants additionnels pour *Windows* (tels que les services DHCP, DNS ou WINS sous *Windows 2000 Server*).

- Pointez sur **Outils de gestion et d'analyse**, puis cliquez sur le bouton **Détails,**



La boîte d'**Outils de gestion et d'analyse** s'ouvre alors, vous permettant de choisir quels composants vous désirez installer. Dans le cas d'une station *Windows 2000 Professionnel*, seul le protocole **SNMP (Protocole simplifié de gestion de réseau)** est disponible ; d'autres options sont cependant disponibles sous *Windows 2000 Server*.

- Sélectionnez le protocole **SNMP** puis cliquez sur **OK**. Cliquez ensuite sur **Suivant** : *Windows* enregistre les nouveaux composants installés (le CD-Rom d'installation de *Windows 2000* vous sera éventuellement demandé). Cliquez sur **Terminer** : Le protocole SNMP est maintenant installé sur votre ordinateur.

Windows 2000 ne propose en standard qu'un **Agent SNMP** : celui-ci ne fait qu'envoyer des informations vers un **Système de Gestion SNMP**, c'est-à-dire un logiciel externe au système d'exploitation.

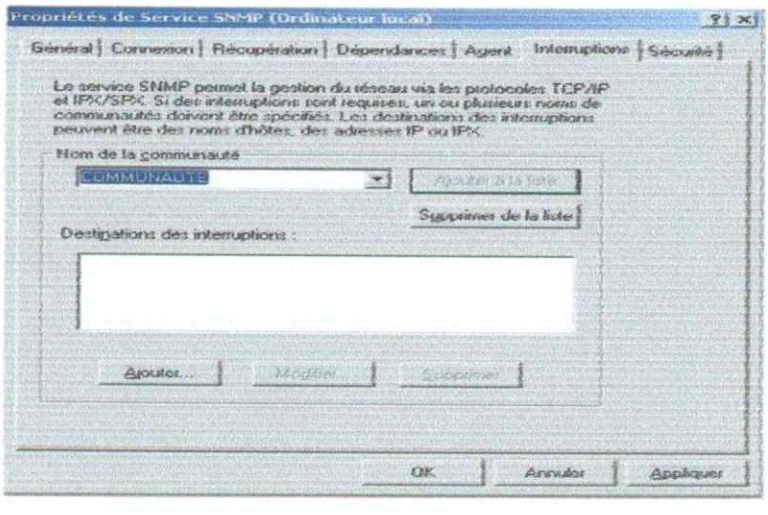
Il est cependant possible de configurer cet **Agent SNMP** : il est même très fortement conseillé d'effectuer ce paramétrage pour des raisons de sécurité.

- Pour accéder à la configuration de **SNMP**, cliquez avec le bouton droit sur l'icône du *Poste de Travail* puis cliquez sur **Gérer**.

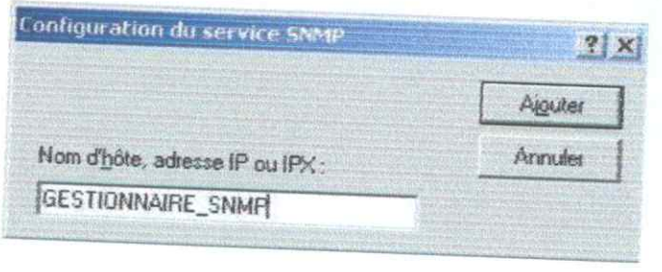
La console de Gestion de l'ordinateur s'ouvre alors. Ouvrez **Services et applications** puis pointez sur **Services**. La liste de tous les services présents sur votre système apparaît.

Deux nouveaux services ont fait leur apparition : **Service SNMP** et **Service de piège SNMP**. Ce dernier ne disposant pas d'option de configuration directe, nous nous intéresserons donc uniquement au **Service SNMP**.

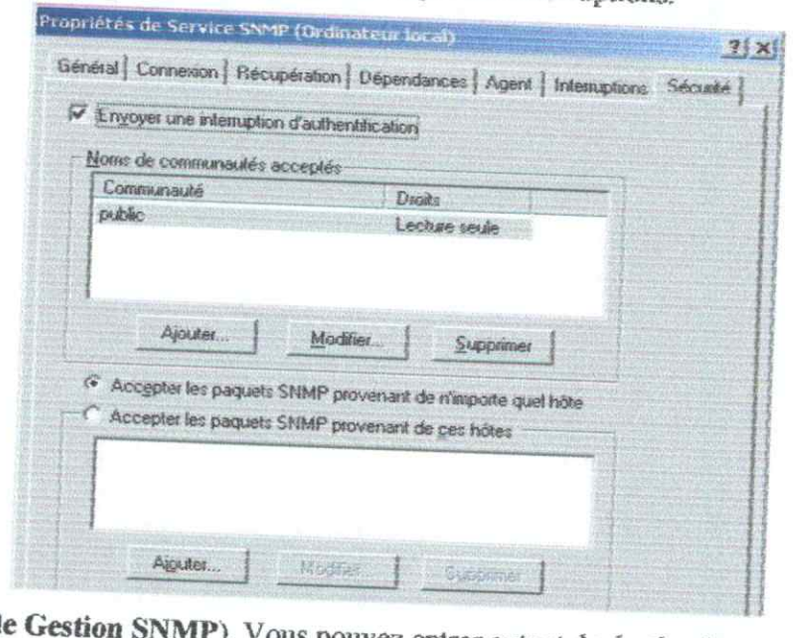
- Double-cliquez sur **Service SNMP**. Ses propriétés apparaissent. Les quatre premiers onglets (*Général*, *Connexion*, *Récupération* et *Dépendances*) servent à configurer les options classiques de tout service (le type de démarrage, la réponse de l'ordinateur en cas de défaillance du service).
- Cochez la case *Physique* si votre ordinateur gère les périphériques physiques, tels qu'une partition de disque dur.
- Cochez la case *Applications* si votre ordinateur utilise des applications qui envoient des données avec le protocole TCP/IP.
- Cochez la case *Liaison de données et sous-réseau* si votre ordinateur gère un pont.
- Cochez la case *Internet* si votre ordinateur est un routeur (passerelle IP).
- Cochez la case *Bout en Bout* si votre ordinateur est un hôte IP.



L'onglet **Interruptions** sert à gérer les interruptions SNMP que votre ordinateur va envoyer. En effet, lorsqu'un événement particulier survient sur la machine **Agent SNMP**, celle-ci va envoyer une interruption SNMP au **Système de Gestion SNMP** pour lui indiquer la nature de l'événement. Ces interruptions se gèrent au travers de communautés, c'est-à-dire un ensemble de machines auxquelles l'Agent va envoyer ses interruptions.



Dans le champ **Nom de la communauté**, entrez (en respectant la casse) le nom de la communauté vers laquelle l'Agent va envoyer ses interruptions.



Système de Gestion SNMP). Vous pouvez entrer autant de destinations que nécessaire.

L'onglet **Sécurité** permet de sécuriser le service SNMP. En effet, par défaut, tous les **Systèmes de Gestion SNMP** peuvent effectuer des requêtes sur l'**Agent SNMP** de votre ordinateur. Il convient donc de limiter cet accès, en définissant par exemple les noms de communautés acceptés. Par défaut, le nom de communauté est *Public*, c'est-à-dire tout le monde. Pour sécuriser votre Agent, supprimez la communauté *Public*, et ajoutez-en une nouvelle, en cliquant sur le bouton **Ajouter** Vous pouvez définir le nom de la nouvelle communauté, mais également les droits de cette communauté parmi *Aucun*, *Notifier*, *Lecture Seule*, *Lecture/Ecriture* et *Lire/Créer*. Choisissez les paramètres appropriés et cliquez sur **Ajouter.**

Il est également possible de sécuriser votre Agent SNMP en définissant un à un les hôtes dont votre ordinateur va accepter les requêtes. Pour ce faire, cochez la case **Accepter les paquets SNMP provenant de ces hôtes**, cliquez sur **Ajouter** et entrez le nom ou l'adresse de la machine acceptée. Vous pouvez également entrer autant de machines que nécessaire.