UNIVERSITE SAAD DAHLAB DE BLIDA
FACULTE DES SCIENCES
DEPARTEMENT D'INFORMATIQUE

Mémoire en vue d'obtention du diplôme de Master
Spécialité : ingénierie du logiciel

Conception et réalisation d'un système de supervision des ressources matérielles et applicatives d'un réseau d'entreprise avec gestion des alertes

Présentée par :

MADACI Hamza

HACHI Youcef

omoteur :
ne REZOUG Nachida

Encadreur :
Mr BOUKABOU Abdelhamid

2012/2013

Remerciements

C'est avec l'aide de dieu qu'a vu le jour ce présent travail.

En premier lieu, Nous remercions tout particulièrement le chef du service informatique, ***Mr BENHAMMADI farid*** *pour avoir placé sa confiance en nous et pour avoir mis personnellement à notre disposition les moyens humains et matériels nécessaires au bon déroulement de notre stage.*

Nous adressons également des remerciements spéciaux à ***Mr*** **BOUKABOU Abdelhamid** *qui a su nous apporter un suivi et un soutien sans faille lors de notre stage*

On exprime toute notre gratitude à notre promotrice, ***Mme*** **REZOUG Nachida**, *pour l'effort fourni, les conseils prodigués, sa patience et sa persévérance dans le suivi.*

A tout le personnel du service Informatique, nous disons un grand merci pour leur disponibilité et leur accueil.

Nous voudrions également remercier nos parents pour: leur soutien moral tout au long de notre cycle.

On n'oublie pas nos plus nos enseignants, qui tout au long du cycle d'études à ***USDB****, nous ont transmis leur savoir.*

On remercie tout particulièrement les membres de jury d'avoir bien voulu accepter de faire partie de la commission d'examinateur, a toute personne qui a participé de près ou de loin pour l'accomplissement de ce modeste travail.

RESUME :

Le travail effectué dans ce projet représente notre contribution à la conception et a la réalisation d'un outil de surveillance et supervision dans un réseau informatique, il intègre le domaine de la sécurité des systèmes d'information.

Cet outil permet a l'administrateur d'inventorier son parc informatique et détecter l'introduction d'une machine étrangère a son réseau tout en surveillant des éventuels changements qui pourraient affecter la configuration matérielle ou logicielles des équipements dont il est responsable.

Mots Clés :

SNMP, MIB, OID, WMI

ABSTRACT :

This work represents our contribution, conception, realization of Network monitoring tool, it allows to network administrator to inventory his omputer park, disable any foreign connection by supervising the hardware configuration of the equipements, this became possible by using SNMP protocole to collecte information and launch the supervision.

Key words :

SNMP, MIB, OID, WMI

ملخص:

هذا العمل هو مساهمتنا في تصميم وإنجاز أداة لرصد والإشراف على شبكة الحاسوب , و يسمح لمدير الشبكة لجرد الشبكة ورصد جميع المكونات والمعدات, من جهة أخرى تساعد المشرف على رصد أي جهاز دخيل على الشبكة وبالتالي توفر مراقبة كلية للأجهزة وهذا باستعمال بروتوكول عدة تقنيات

المفاتيح:

SNMP, MIB, OID, WMI

Introduction générale

1. Contexte

L'informatique est de plus en plus présente dans notre vie de tous les jours. On compte désormais sur les services offerts par les réseaux pour le fonctionnement de l'outil informatique, que ce soit en entreprise, lors de transactions bancaires, lors de téléconférences, etc. Les services offerts sont devenus quasi-indispensables. Pour assurer que ces services soient convenables, il est nécessaire de surveiller le réseau et d'agir quand une erreur se produit.

Les systèmes informatiques étant de plus en plus complexes, leur surveillance et la localisation des problèmes deviennent de plus en plus ardus pour l'administrateur réseaux et systèmes. La pression est d'autant plus forte que les entreprises ou organismes s'appuient sur le système d'information pour leur activité, demandant ainsi une très grande réactivité de la part de l'administrateur.

Sur les réseaux de nombreuses composantes sont donc à surveiller: l'utilisation de la largeur de bande, l'état de fonctionnement des liens, les éventuels goulets d'étranglement, les problèmes de câblage, le bon cheminement de l'information entre les machines, l'ensemble des applications circulant dans le réseau etc. Pour ce faire différents points stratégiques sont à observer comme les routeurs, les concentrateurs, les liens, les postes, les imprimantes, le système.

Ainsi, en cas de panne ou de mauvais fonctionnement sur le réseau, l'administrateur doit pouvoir interpréter l'information reçue pour identifier la source du problème.

De ce fait, les administrateurs réseau font appel à des logiciels de surveillance et de supervision de réseaux afin de vérifier l'état du réseau en temps réel de l'ensemble du parc informatique sous leur responsabilité. Et être aussi informés automatiquement (par email, par SMS) en cas de problèmes. Grâce à un tel système, les délais d'interventions sont fortement réduits et les anomalies peuvent être aussitôt prises en main avant même qu'un utilisateur peut s'en apercevoir.

Ainsi, la supervision des réseaux s'avère nécessaire et indispensable. Elle permet entre autre d'avoir une vue globale du fonctionnement et des problèmes pouvant survenir sur un réseau mais aussi d'avoir des indicateurs sur la performance de son architecture.

2. Problématique

Ayant un très grand nombre de machines à gérer, l'administrateur est incapable de vérifier leurs disponibilité (en ligne ou pas), de déterminer la qualité des services qu'ils offrent, ni détecter la défaillance des équipements (charge CPU, Etat mémoire, surcharge du disque….) et les applications, ni les surcharges et pénurie temporaire des ressources. Le seul moyen de détecter ces anomalies ne peut se faire que par la réception des différentes plaintes et réclamations des employés.

Pour mieux comprendre la situation on propose les schémas suivants :

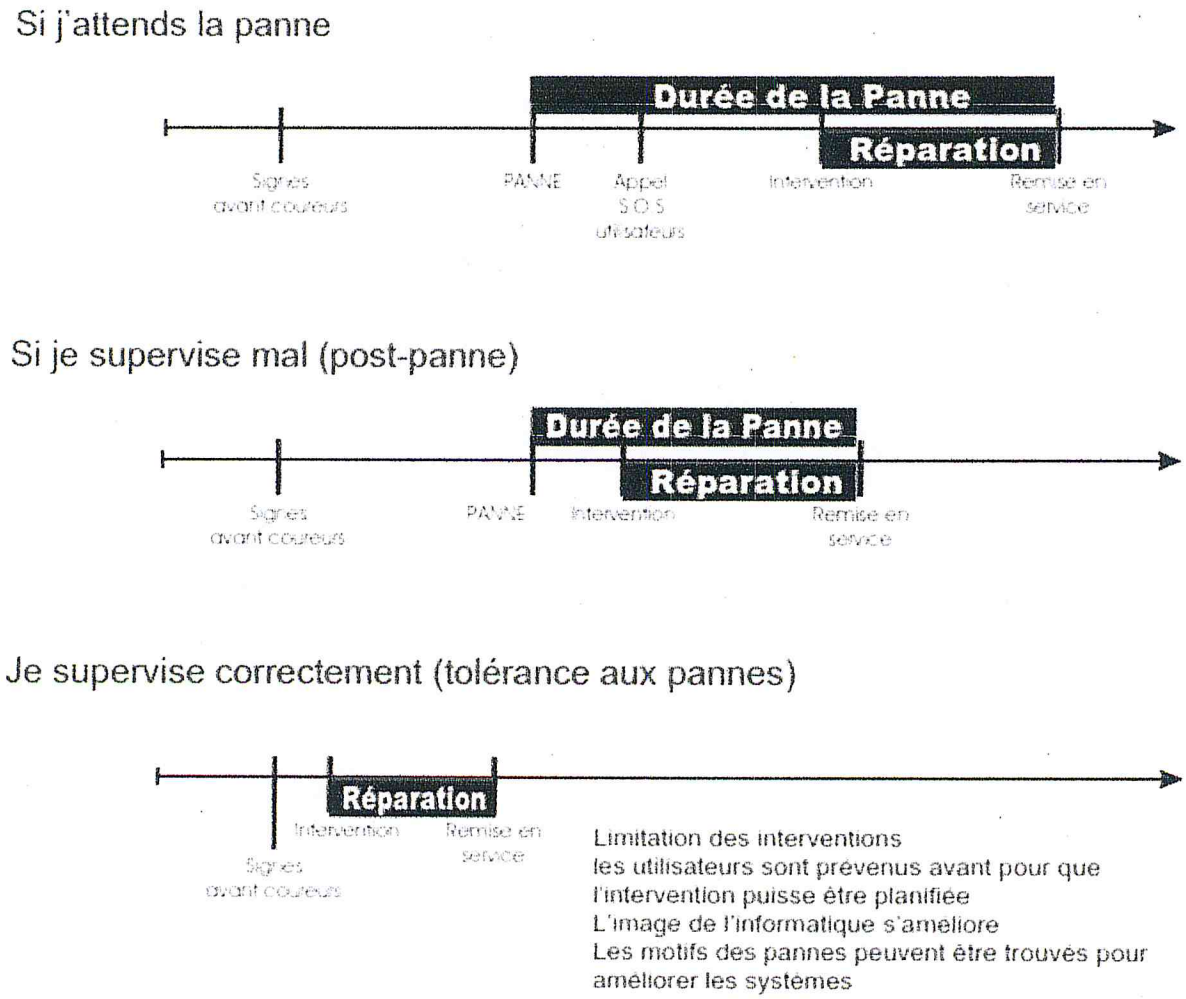

Figure 1:Principe du supervision

3. Description de thème

Le but de ce projet est donc de trouver une solution optimale pour la gestion des serveurs et le monitoring de ses équipements et applications en premier lieu, offrir la possibilité de devenir

« Pro actif » face aux problèmes rencontrés en un second lieu, et finalement et le plus important, de pouvoir détecter et interpréter en un simple coup d'œil les causes et origines des problèmes rencontrés afin de les fixer le plus rapidement possible.

Il faut pouvoir surveiller de manière continu l'état de réseau afin d'éviter un arrêt de production de trop longue durée. C'est là ou la supervision intervient. Elle doit permettre d'anticiper les problèmes et de faire remonter des informations sur l'état des équipements.

Plus le système est important et complexe, plus la supervision devient compliquée sans les outils indispensables.

Le thème consiste à réaliser un outil de surveillance et de supervision qui permet aux administrateur réseaux de vérifier en temps réel l'état du réseau sous leur responsabilité ainsi que l'état des équipements composant le parc informatique de leur entreprise ,et permet aussi de les informer de l'ensemble des applications utilisées par les employés sur ses équipements et d'alertes automatiquement (par email, par message ,etc..) en cas d'anomalie ou de problème.

Chapitre1 : Etat de L'art

Partie 1 : Généralités sur les réseaux

1. Introduction

Un réseau informatique permet à plusieurs machines (ordinateurs au sens large) de communiquer entre elles afin d'assurer des échanges d'informations: du transfert de fichiers, du partage de ressources (imprimantes et données), de la messagerie ou de l'exécution de programmes à distance.

2. Définition d'un réseau

Un réseau est un ensemble de choses connectées entre elles qui échangent des informations. Pour les ordinateurs, il y a au moins deux ordinateurs reliés entre eux qui s'échangent des données.

Un réseau permet :

- La communication de plusieurs ordinateurs entre eux (ou de plusieurs personnes entre elles)
- Le partage de fichiers, d'imprimantes.
- Le jeu à plusieurs.
- L'unicité de l'information (pour des fichiers souvent mis à jour, le réseau permet de mettre à jour tous les PC le constituant).
- Une organisation plus efficace et donc une meilleure productivité.

Il existe différents réseaux :

- Les réseaux Peer to Peer (deux ordinateurs reliés seulement donc ils ont une "fonction" égale sur le réseau)
- Les réseaux Client/serveur. Ils sont organisés avec des postes serveurs qui fournissent l'information au client (comme internet par exemple).

3. L'organisation d'un réseau (ou éventuellement topologie)

Il existe plusieurs organisations de réseaux, qui ont chacune des capacités et des contraintes différentes. On choisira donc une topologie plus qu'une autre en fonction du réseau à mettre en place.

3.1 Topologie en bus

Dans une topologie en bus, tous les ordinateurs sont connectés à un seul câble continu ou segment.

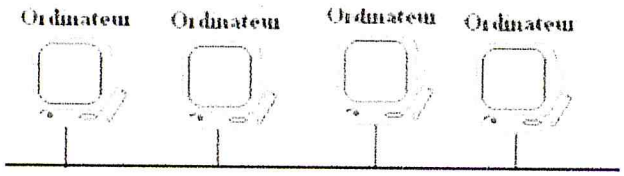

Figure 2:Topologie en bus [1]

Les avantages de ce réseau : coût faible, faciliter de mise en place, distance maximale de 500m pour les câbles 10 base 5 et 200m pour les câbles 10 base 2. La panne d'une machine ne cause pas une panne du réseau.

Les inconvénients : s'il y a une rupture d'un bus sur le réseau, la totalité du réseau tombe en panne. Le signal n'est jamais régénéré, ce qui limite la longueur des câbles, il faut mettre un répéteur au-delà de 185 m.

La technologie utilisé est Ethernet 10 base 2. [1]

3.2 Topologie en étoile

La topologie en étoile est la plus utilisée. Dans la topologie en étoile, tous les ordinateurs sont reliés à un seul équipement central : le concentrateur réseau. Ici le concentrateur réseau peut être un concentrateur, un commutateur, un routeur…

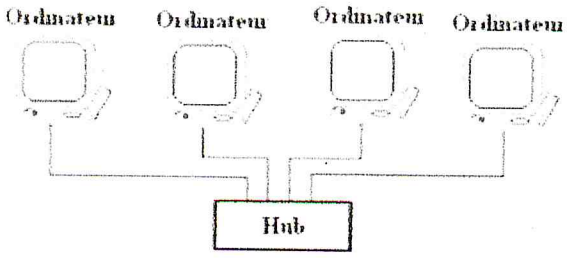

Figure 3:Topologie en étoile

Les avantages de ce réseau ce que la panne d'une station ne cause pas la panne du réseau et qu'on peut retirer ou ajouter facilement une station sans perturber le réseau. Il est aussi très facile à mettre en place.

Les inconvénients sont que le coût est un peu élevé, la panne du concentrateur centrale entraine le disfonctionnement du réseau.

La technologie utilisé est Ethernet 10 base T, 100 base T. [1]

3.3 Topologie en anneau

Dans un réseau possédant une topologie en anneau, les stations sont reliées en boucle et communiquent entre elles avec la méthode « chacun à son tour de communiquer ». Elle est utilisée pour le réseau token ring ou FDDI. [1]

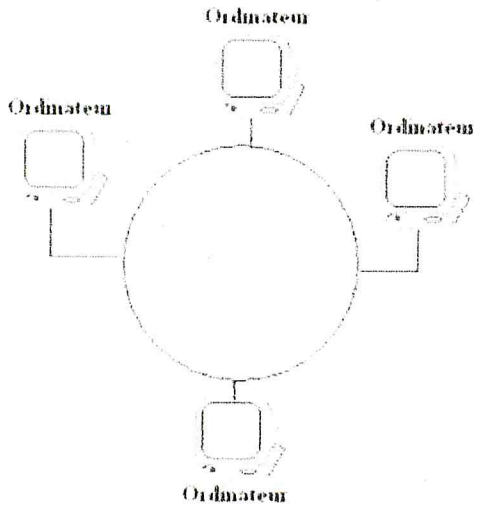

Figure 4:Topologie en anneau [1]

4. Matériel

Le matériel informatique est l'ensemble des composants formant la partie matérielle (physique) d'un ordinateur.

4.1 Modem

Le modem est le périphérique utilisé pour transférer des informations entre plusieurs ordinateurs via un support de transmission filaire et non filaire (ligne téléphonique par exemple). Les ordinateurs fonctionnent de façon numérique, ils utilisent le codage binaire (une série de 0 et de 1), mais les lignes téléphoniques sont analogiques. Les signaux numériques passent d'une valeur à une autre, il n'y a pas de milieu, de moitié, c'est du (tout ou rien) « un ou zéro ».

Les signaux analogiques par contre n'évoluent pas «par pas ». Ils évoluent de façon continue. Ainsi, le modem module les informations numériques en ondes analogiques. En sens inverse, il démodule les données analogiques pour les convertir en numérique. Le mot « modem » est ainsi un acronyme pour « MODULATEUR/DÉMODULATEUR ». [2]

Figure 5: modem [2]

4.2 Carte réseau

La carte réseau est certainement l'autre matériel le plus connu dans le domaine : c'est un adaptateur qui sait décoder le signal électrique (ou électromagnétique dans certains cas) émis par une autre carte du même standard en un signal utilisable par votre ordinateur.
De manière général, chez un particulier on trouve des cartes FastEthernet (les fameuses cartes RJ45, 10/100 TX, 100 base TX...). Ces cartes sont prévues pour recevoir un certain type de signal électrique, porté par un câble d'un certain type (RJ45, Ethernet). Inutile de bidouiller la prise téléphone pour économiser un modem, ça ne marchera pas.
Elles sont de 3 types : PCI, USB (à fuir) et PCMCIA.
Une carte Ethernet est à brancher sur un périphérique Ethernet. [3]

4.3 HUB et SWITCH

Le hub, souvent confondu avec le Switch, en français le premier s'appelle un concentrateur, c'est juste une multiprise pour le réseau, ce qui entre par une prise est envoyé sur toutes les autres prises. Le second est appelé commutateur, c'est une multiprise, mais « intelligente », ce qui entre sur une prise n'est envoyé qu'à la prise de destination (on verra plus tard comment ça marche).
Il faut juste retenir ceci pour l'instant, entre un hub et un Switch, choisissez le Switch. [3]

4.4 Les routeurs

Un routeur réunit des réseaux au niveau de la couche réseau (couche 3), il permet de relier 2 réseaux avec une « barrière » entre les deux. En effet, il filtre les informations pour n'envoyer que ce qui est effectivement destiné au suivant. L'utilisation la plus courante est la connexion de multiples stations vers INTERNET. Les données transitant sur réseau local (non destinées à Internet) ne sont pas transmises à l'extérieur. [2]

Figure 6: routeur [2]

5. Les différents types de réseau

On distingue différents types de réseaux selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue.

On fait généralement trois catégories de réseaux :

- ✓ LAN (local area network)
- ✓ MAN (metropolitan area network)
- ✓ WAN (wide area network)

5.1 Les LAN

LAN signifie Local Area Network (en français Réseau Local). Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet). [5]

5.2 Les MAN

Les MAN (Metropolitan Area Network) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même réseau local.

Un MAN est formée de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique). [5]

5.3 Les WAN

Un WAN (Wide Area Network ou réseau étendu) interconnecte plusieurs LANs à travers de grandes distances géographiques.

Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles.

Les WAN fonctionnent grâce à des routeurs qui permettent de "choisir" le trajet le plus approprié pour atteindre un nœud du réseau.

Le plus connu des WAN est Internet. [5]

6. Le modèle OSI

Le modèle OSI (Open System Interconnection Model) défini en 1977 régit la communication entre 2 systèmes informatiques selon 7 niveaux. A chaque niveau, les deux systèmes doivent communiquer "compatibles". En matériel réseau, nous n'utilisons que les couches inférieures, jusqu'au niveau 3, Ces niveaux sont également appelés couches.

L'OSI est un modèle de base normalisé par l'International Standard Organisation (ISO).

Application		**Couche** Application		**Couche** Application	⇑	
		Couche Présentation		**Couche** Présentation	⇑	
		Couche Session		**Couche** Session	⇑	
Transport des données		**Couche** Transport		**Couche** Transport	⇑	
		Couche Réseau **(Network)**		**Couche** Réseau **(Network)**	⇑	Paquet
		Couche liaison de données (Data Link)		**Couche** liaison de données **(Data Link)**	⇑	Trames
		Physique **(Physical)**		**Couche** Physique **(Physical)**	=	BIT
		Support de communication				

Figure 7 : Modèle OSI

- **Niveau 7 (application):** gère le format des données entre logiciels.
- **Niveau 6 (présentation):** met les données en forme, éventuellement de l'encryptage et de la compression, par exemple mise en forme des textes, images et vidéo.

- **Niveau 5 (session):** gère l'établissement, la gestion et coordination des communications
- **Niveau 4 (transport):** s'occupe de la gestion des erreurs, notamment avec les protocoles UDP et TCP/IP
- **Niveau 3 (réseau):** sélectionne les routes de transport (routage) et s'occupe du traitement et du transfert des messages: gère par exemple les protocoles IP (adresse et le masque de sous-réseau) et ICMP. Utilisé par les routeurs et les switchs manageables.
- **Niveau 2 (liaison de données):** utilise les adresses MAC. Le message Ethernet à ce stade est la trame, il est constitué d'un en-tête et des informations. L'en-tête reprend l'adresse MAC de départ, celle d'arrivée + une indication du protocole supérieur.
- **Niveau 1 (physique):** gère les connections matérielles et la transmission, définit la façon dont les données sont converties en signaux numériques: ça peut-être un câble coaxial, paires sur RJ45, onde radio, fibre optique, ...

A chacun de ces niveaux du modèle OSI, on encapsule un en-tête et une fin de trame (message) qui comporte les informations nécessaires en suivant les règles définies par le protocole réseau employé. Le protocole est le langage de communication (la mise en forme) utilisé pour le transfert des données (actuellement TCP/IP mais d'autres ont été utilisés comme NetBeui (antérieur à Windows 98), Novell IPX, ...). Sur le graphique ci-dessous, la partie qui est rajoutée à chaque couche est sur fond blanc. La partie en grisée est celle obtenue après encapsulation (intégration) du niveau précédent. La dernière trame, celle qu'on obtient après avoir encapsulé la couche physique, est celle qui sera envoyée sur le réseau. [6]

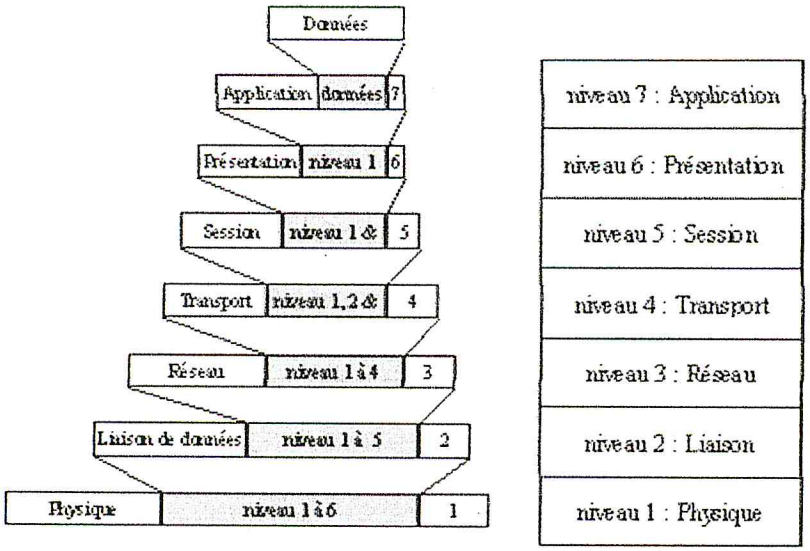

Figure 8:les niveaux du modèle OSI [6]

7. Adresse IP

Une adresse IP est un numéro unique. Ce numéro est unique car il permet à un ordinateur connecté à un réseau utilisant le protocole TCP/IP (comme internet par exemple) de l'identifier.

Une adresse IP est un nombre de 32 bits composé de 4 numéros allant de 0 à 255 (4 numéros de 8 bit, sauf le dernier numéro qui ne peut excéder 254) séparés par des points.

Exemple d'une adresse IP : 127.0.0.1

Une adresse IP est composée de deux parties distinctes.

- Une partie appelée **net-ID** située à gauche, elle désigne le réseau contenant les ordinateurs.
- Une autre partie appelée **host-ID** désignant les ordinateurs de ce réseau.

Prenons pour exemple un réseau ayant une adresse IP de ce type : 192.168.0.0 comprenant une dizaine d'ordinateurs. Les adresses IP de ces 10 ordinateurs varient de 192.168.0.1 à 192.168.0.10.

Plus l'adresse réseau est courte (occupe le moins de chiffres), plus le réseau pourra contenir d'ordinateurs. Il existe donc 3 classes de réseau notées **A, B et C** qui se différencient par le nombre d'octets désignant le réseau.

- **Classe A :**

Dans une adresse IP de classe A, l'adresse réseau est désignée par le premier octet qui doit être d'une valeur inférieure à 128. Le réseau composé de 0 uniquement n'existe pas, et le réseau 127 désigne votre ordinateur. La plage utilisable est comprise entre **1.0.0.0 et 126.0.0.0**

Ce réseau peut contenir 16646144 ordinateurs.

- **Classe B :**

Dans une adresse IP de classe B, l'adresse réseau est désignée par les deux premiers octets. La plage utilisable est comprise entre **128.0.0.0 et 191.255.0.0**

Ce réseau peut contenir 65024 ordinateurs.

- **Classe C :**

Dans une adresse IP de classe C, l'adresse réseau est désignée par les trois premiers octets. La plage utilisable est comprise entre **192.0.0.0 et 233.255.255.0**

Ce réseau peut contenir 254 ordinateurs. [4]

De plus en plus d'internautes disposent d'une adresse IP fixe. Pour disposer d'une adresse IP fixe, il faut faire une demande auprès de l'INTERNIC (c'est votre FAI qui s'en charge).

Voici les plages d'adresses IP réservées :

- 10.0.0.1 à 10.255.255.254
- 172.16.0.1 à 172.31.255.254
- 192.168.0.1 à 192.168.255.254

8. Le masque de sous réseau

Lorsqu'on *configure un réseau, on parle souvent de masque de sous réseau*. Celui ci sert à capacité d'un ordinateur à communiquer avec un autre d'un même réseau ou pas. En fonction du masque, des restrictions d'accès sont appliqués, et les ordinateurs ne pourront pas communiquer, donc ne se verront pas dans les favoris réseaux.

Le masque de sous réseau le plus courant, celui que l'on utilise généralement à la maison est **255.255.255.0**

A quoi cela correspond t-il ? Eh bien c'est simple. Ce masque de sous réseau va permettre aux ordinateurs ayant une adresse IP ayant 3 premiers octets identiques de communiquer ensemble. Ex : l'ordinateur ayant l'IP 192.168.0.1 pourra communiquer avec l'autre ayant une IP telle que 192.168.0.2, mais pas 192.169.0.2

Voici un tableau qui sera sûrement plus clair (le but est de faire communiquer l'ordinateur 1 et l'ordinateur 2) :

Adresse IP de l'ordinateur 1	Adresse IP de l'ordinateur 2	Masque de sous réseau
192.168.0.1	192.168.0.2	255.255.255.0
192.168.10.1	192.168.0.3	255.255.0.0
192.56.78.98	81.63.75.17	0.0.0.0

Tableau 1 : Adresse et masque réseau

En clair lorsque les bits du masque de sous réseau sont à 1 alors les bits des adresses IP des ordinateurs pouvant communiquer entres eux doivent être identiques.

Exemple pour le masque de sous réseau 255.255.255.0

Valeur normale	Valeur binaire
255.255.255.0	11111111 11111111 11111111 00000000
192.168.0.1	11000000 10101000 00000000 00000001

192.168.0.2	11000000 10101000 00000000 00000010

Tableau 2: Transformation en binaire du masque

Partout où le masque de sous réseau prend pour valeur 1, la valeur correspondante entre les deux ordinateurs doit être identique.

Il existe cependant d'autres sous réseaux comme par exemple 255.255.255.128. Examinons ce cas de figure :

Valeur normale	Valeur binaire
255.255.255.128	11111111 11111111 11111111 10000000
192.168.0.200	11000000 10101000 00000000 11001000
192.168.0.100	11000000 10101000 00000000 01100110
192.168.0.128	11000000 10101000 00000000 10000000

Tableau 3 : Transformation en binaire du masque

On le voit maintenant, seuls les ordinateurs ayant respectivement l'adresse 192.168.0.200 et 192.168.0.128 peuvent communiquer. On peut ainsi diviser un réseau en plein de petits sous réseaux. [4]

9. Les protocoles

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines), c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe

plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers, d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs. [12]

• **TCP/IP** : Transmission Control Protocol / Internet Protocol

Défini la norme de communication, (en fait un ensemble de protocoles) des ordinateurs reliés à Internet. Va contenir les protocoles HTTP, FTP, SMTP, …

• **DNS :** permet de retrouver une adresse IP en fonction d'un nom d'ordinateur (un peu comme un annuaire).

• **FTP :** sert à transporter des fichiers d'un ordinateur à l'autre.

• **DHCP : (Dynamic Host Configuration Protocol)** (DHCP) est un terme anglais désignant un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres TCP/IP d'une station, notamment en lui assignant automatiquement une adresse IP et un masque de sous réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS et des serveurs de noms NBNS (connus sous le nom de serveurs WINS sur les réseaux de la société Microsoft).[13]

• **IRC :** permet de créer des «salons» de discussion en direct.

• **ICQ :** permet de savoir si quelqu'un est en ligne et de dialoguer avec lui.

• **NTP :** permet de mettre les ordinateurs à l'heure par internet à 500 millisecondes.

• **P2P :** permettent de partager des fichiers à grande échelle.

• **NNTP :** permet d'accéder à des forums de discussion sur des milliers de sujets différents.

• **SSH :** permet d'avoir un accès sécurisé à des ordinateurs distants.

• **SMTP :** permet d'envoyer des emails, et le protocole POP3 de les recevoir.

• **DNS :** Domain Name Server : système de nom de domaine ou système d'affectation de nom.

• **FTP:** protocole définissant les règles de transfert des fichiers par Internet. Lorsqu'un utilisateur télécharge un fichier par ftp, il le recopie de l'ordinateur distant sur le sien (ou l'inverse).

• **SNMP :** Le protocole *SNMP* (Simple Network Management Protocol) est un protocole qui facilite l'échange d'information de gestion entre les équipements du réseau. Il permet aux administrateurs réseau de gérer les performances du réseau, de diagnostiquer et de résoudre les problèmes.[14]

Composants SNMP :

- *Le système d'administration de réseaux (NMS, Network Management System):* le composant NMS fournit la quantité de ressources mémoire et de traitements requises pour la gestion du réseau.

• *Les unités gérées*: ces unités sont des nœuds du réseau contenant un agent SNMP. Ces unités peuvent être des routeurs, des serveurs d'accès, des commutateurs, des ponts, des concentrateurs, des ordinateurs hôtes ou des imprimantes.

• *Les agents*: les agents sont des modules logiciels de gestion du réseau résidant sur les unités gérées. Ils contiennent les données locales des informations de gestion et les convertissent en un format compatible avec SNMP.

• **TELNET :** protocole standard permettant l'interfaçage de terminaux et d'applications à travers Internet.

Ce protocole fournit les règles de bases pour permettre de relier un client (système composé d'un affichage et d'un clavier) à un ordinateur distant (coté serveur). [11]

10. Notion de port

Lors d'une communication en réseau, les différents ordinateurs s'échangent des informations qui sont généralement destinées à plusieurs applications (le client mail et le navigateur internet par exemple).

Seulement ces informations transitent par la même passerelle. Il faut donc savoir pour quelle application telle information est destinée. On attribue donc des ports pour chaque application.

10.1 Définition

Un port est comme une porte en schématisant. Les informations sont multiplexées (comme dans les voitures récentes) et passent par la passerelle. A leur arrivée (vers le serveur) ou à leur réception (vers votre machine) elles sont démultiplexées et chaque information distincte passe par le port qui lui est associé. Les informations sont ensuite traitées par l'application correspondante.

Un port est codé sur 16 bits, il y a donc 65536 ports.

L'adresse IP plus le port (exemple : **127.0.0.1:80**) est appelée socket.

Les ports ce sont vus attribuer une assignation par défaut pour aider à la configuration des réseaux. Voici les principaux ports et le protocole les utilisant :

Port	Service ou Application
21	FTP
23	Telnet
25	SMTP
53	DNS
80	HTTP
110	POP3
119	NNTP

Tableau 4: ports et Protocoles

Les ports 0 à 1023 sont les ports reconnus ou réservés et sont assignés par l'IANA (Internet Assigned Numbers Authority).

Les ports 1024 à 49151 sont appelés ports enregistrés et les ports 49152 à 65535 sont les ports dynamiques (ou privés). [4]

10.2 Principe des ports

Ils mettent en relation deux applications distantes (ex. client et serveur Web) ils permettent de partager une connexion entre plusieurs applications. [8]

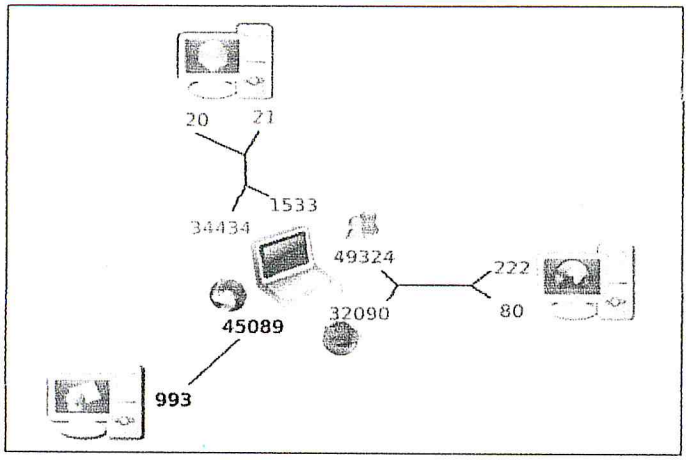

Figure 9 : les ports [8]

11. Architecture client/serveur

L'architecture client serveur s'appuie sur un poste central, le serveur, qui envoi des données aux machines clientes.

Des programmes qui accèdent au serveur sont appelés programmes clients (client FTP, client mail).

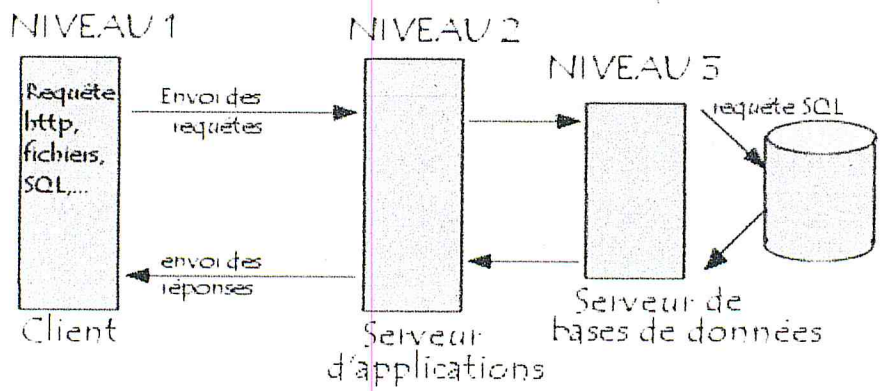

Figure 10 : Architecture client/serveur [7]

Qu'est-ce qu'un serveur ?

On appelle logiciel serveur un programme qui offre un service sur le réseau. Le serveur accepte des requêtes, les traite et renvoie le résultat au demandeur. Le terme serveur s'applique à la machine sur lequel s'exécute le logiciel serveur.

Pour pouvoir offrir ces services en permanence, le serveur doit être sur un site avec accès permanent et s'exécuter en permanence (daemon - suffixe d pour le nom du logiciel ex. ftpd). [7]

Qu'est-ce qu'un client ?

On appelle logiciel client un programme qui utilise le service offert par un serveur. Le client envoie une requête et reçoit la réponse. Le client peut-être raccordé par une liaison temporaire.

Qu'appelle-t-on architecture client/serveur ?

C'est la description du fonctionnement coopératif entre le serveur et le client. Les services internet sont conçus selon cette architecture. Ainsi, chaque application est composée de logiciel serveur et logiciel client. A un logiciel serveur, peut correspondre plusieurs logiciels clients développés dans différents environnements: Unix, Mac, PC...; la seule obligation est le respect du protocole entre les deux processus communicants. Ce protocole étant décrit dans un RFC (Request For Comment). [7]

11.1 Avantages

- **Unicité de l'information :** pour un site web dynamique par exemple (comme vulgarisation-informatique.com), certains articles du site sont stockés dans une base de données sur le serveur. De cette manière, les informations restent identiques. Chaque utilisateur accède aux mêmes informations.
- **Meilleure sécurité :** Lors de la connexion un PC client ne voit que le serveur, et non les autres PC clients. De même, les serveurs sont en général très sécurisés contre les attaques de pirates.
- **Meilleure fiabilité :** En cas de panne, seul le serveur fait l'objet d'une réparation, et non le PC client.
- **Facilité d'évolution :** Une architecture client/serveur est évolutive car il est très facile de rajouter ou d'enlever des clients, et même des serveurs. [4]

11.2 Inconvénients

- Absence méthodologie éprouvée.

"sensible", mettre un VPN hardware n'est pas suffisant. Une sécurité logicielle complémentaire incluant des contrôles d'accès au niveau administration serveur (serveur, dossier, droits d'accès) et logiciels de sécurités vérifiant le trafic sur le réseau interne n'est pas superflu.

- Les routeurs peuvent être remplacés par une solution basée sur un serveur 2003 ou 2008, par un logiciel proxy comme WinGate ou par un ordinateur configuré spécifiquement en Linux
- Un **serveur proxy** est parfois intégré dans les routeurs (mais généralement sous Windows ou Linux)
- Les **firewalls** sont intégrés dans certains routeurs mais des logiciels assurent (presque) des fonctions équivalentes, souvent intégrés dans l'anti-virus (ex.:Symantec, ZoneAlarm, Mcafee au niveau des stations)
- Les **réseaux privés intégrés (VPN)** sont intégrés dans certains systèmes d'exploitation serveurs mais peuvent également être des équipements spécifiques.
- Les **anti-virus** sont le plus souvent des logiciels, mais peuvent être implantés dans des routeurs qui vérifient tout le trafic extérieur.

Selon l'application, le niveau de sécurité souhaité, le nombre d'utilisateurs, ... et les budgets, la conception du réseau utilisera une solution logicielle ou hardware ou une combinaison de ces solutions. D'autres programmes de gestion réseaux (logiciels) permettent de gérer les trafics, les utilisateurs, ... En clair, par hardware, vous pouvez bloquer l'accès complet à un serveur, par software, autoriser seulement une partie des ressources d'un serveur. Les solutions des droits d'accès intègrent le plus souvent les deux. [6]

13. Conclusion

Dans le présent chapitre nous avons défini les différentes notions relatives à notre domaine d'étude « le réseau informatique » de façon claire et complète.

Ces notions sont considéré comme un guide qui va nous aidé à comprendre les différentes fonctionnalités des réseaux.

Partie 2 : Etude d'existant

1. Introduction

La fiabilité des SI est absolument nécessaire pour l'entreprise et son fonctionnement afin de garantir cette caractéristique et autres telles que la continuité et la qualité de service.

La sécurité et la disponibilité, les administrateurs réseau et système emploient des outils de supervision adaptés à la gestion des différents composants matériels ou logiciels du réseau,

Qui proviennent en général des divers constructeurs et qui ont des modes de fonctionnement hétérogènes. Ainsi, ces outils doivent fournir une vue globale ou détaillée et cohérent des réseaux qu'ils gèrent, et les informations récupérées doivent être sauvegardées pour les utiliser dans cette activité de supervision.

Dans ce chapitre nous allons traiter la notion de « surveillance et supervision informatique » au tant que secteur d'aide à l'administration réseau. Commençant par la définition de différentes notions relatives à l'administration réseau, par la suite nous allons présenter le domaine de la surveillance et supervision informatique tout en mettant l'accent sur la différence entre la surveillance et la supervision ainsi les différents outils et logiciels utilisés dans ce domaine.

2. Définition de l'administration réseaux

L'administration réseau, ou administration système, consiste à contrôler, coordonner et surveiller les différentes ressources mises en place dans le but de fournir des services opérationnels aux utilisateurs du système. Les ressources sont les équipements et les données du réseau alors que les services sont ceux offerts par les différents serveurs, les applications, Internet, etc.

En d'autre terme, administrer un réseau c'est vouloir tirer le meilleur profit de la structure gérée. De façon globale, l'administration réseau a pour objectif de regrouper un ensemble de techniques de gestion cohérentes pour :

- Maintenir l'état opérationnel du système.
- offrir aux utilisateurs une certaine qualité de service.
- permettre l'évolution du système en incluant de nouvelles fonctionnalités.

3. Domaines de l'administration réseau

L'administration réseau est étroitement liée à l'environnement dans lequel elle s'exerce. En effet, il est possible de scinder chaque environnement informatique en trois parties qui sont : les utilisateurs ou consommateurs de services, les serveurs d'applications ou fournisseurs de services et le mécanisme de transport reliant les utilisateurs aux fournisseurs.

Une administration efficace doit être en mesure de prendre en charge ces trois composants de l'environnement.

3.1 Administration des utilisateurs

Elle fournit l'ensemble des mécanismes pour :

- Garantir l'*accessibilité et la connexion aux applications. En effet la disponibilité* des applications est une condition primordiale pour le bon fonctionnement du réseau. Les utilisateurs doivent pouvoir se connecter aux différentes applications à tout moment, par conséquent, ils doivent disposer d'un ensemble d'outils qui leurs assurant la transparence des méthodes d'accès et de connexion aux différentes applications.
- Simplifier l'accès aux serveurs de noms afin de localiser les ressources mises à disposition des utilisateurs.
- Assurer la confidentialité et la sécurité. Le système doit fournir l'ensemble des mécanisme qui permettent d'assurer la confidentialité des informations de l'utilisateur, de sécuriser son environnement et de prévenir dans le cas de perte ou altération des échanges effectués.
- Garantir une certaine qualité de service, qui n'est, suivant l'ITU (International Télécommunication Union), que l'effet global produit par la performance d'un service qui détermine le degré de satisfaction de l'usager du service. [23]

3.2 Administration des serveurs

Elle présente l'ensemble des dispositifs mis en place pour :

- Assurer la connexion et la distribution des applications.
- Assurer la gestion et la distribution des données.
- Contrôler et protéger l'accès aux applications et aux ressources qu'elles utilisent. [23]

3.3 Administration des mécanismes de transport

Permet de :

- Gérer des opérations qui se déroulent au sein du réseau, ce qui donne la possibilité d'intervenir sur le fonctionnement globale du système.
- Mettre en place des dispositifs de détection d'incidents et de correction de fautes.ces dispositifs peut être utilisés comme des outils d'évaluation des performances du système.
- Déterminer la meilleure configuration qui améliore les performances du système.
- Fournir un certain nombre d'informations permettant de déterminer les nouveaux besoins à prendre en compte et les parties du système concernées. [23]

4. Fonctions administratives

L'ISO (*Industrial Standard of Organization*) *avait imaginé dés 1990* des fonctions administratives liées au Management des réseaux, regroupées en cinq familles :

La configuration : Configuration Management

Les pannes et incidents : fautes Management

Les performances : performances Management

La sécurité : Security Management

La compatibilité : Accounting Management

Ces cinq domaines fonctionnels ont été nommés SMFA (Spécifique Management Functional Area) par l'ISO.

L'ISO a défini deux protocoles essentiels que l'on rencontre dans son architecture de supervision.

ISO 9595 : CIMS Services communs

ISO 9596 : CMIP protocole commun

- Les défauts externes indépendants des appareils eux mêmes, mais liées à l'environnement propre du réseau (alimentation électrique défaillante, lien inter-réseau coupé).

Alors que les défauts internes sont permanents et dans les plupart des cas aisément décelables, les défauts externes sont intermittents par nature, voire totalement aléatoire, et leur résolution est sensiblement plus compliquée.

Le traitement d'une panne est composé de trois étapes :

- La signalisation du fonctionnement anormal d'un élément actif ou d'un lien, inter-réseau.
- La localisation du défaut sur l'infrastructure.
- La confirmation du retour à un comportement normale du réseau.

Trois outils permettent de détecter les défauts : les messages d'erreur, les tests et les seuils. Le message d'erreur est généré spontanément par un composant en défaut et enregistré dans un journal (Error log). Le message horodaté comporte des informations essentielles comme l'identifiant du composant et le type d'incident.

Les tests représentant le deuxième outil permettant de détecter les problèmes dans le réseau. On distingue deux type de tests : les tests de sécurité et les tests de diagnostic .alors que tous les composants du réseau sont simultanément concernés par les tests de sécurité, le diagnostic ne s'appliquera qu'à un appareil en particulier (ou plusieurs appareils) mais de façon séparée, avec la logique la plus fine possible.

Les seuils s'appliquent d'avantage à un mode dégradé du réseau, lorsque le niveau de performance maximum est atteint, ou lorsque la bande passante d'un lien inter-réseau est saturée. La gestion des seuils peut être vue comme un mécanisme d'anticipation d'une panne bloquante ou d'un fonctionnement en mode dégradé. Il convient généralement de positionner un seuil à 70% ou à 80%.

L'historisation des incidents peut aider le technicien ou l'ingénieur dans la compréhension des dysfonctionnements du réseau. [25]

L'ISO, bien avant la situation actuelle ou nous sommes confrontés à de multiples menaces, et ou le cout de la sécurité (abordée de façon globale) du système d'information atteint un niveau alarmant, avait classifié assez précisément les risques encourus :

- Mascarade : une entité (ou une machine physique sur le réseau) se fait passer pour une autre afin d'obtenir ses pouvoirs.
- Duplication du message : même risque.
- Perturbation du service : dégradation d'une machine ou d'un service « fonctionnement désordonné du réseau en raison d'une modification des règles de routage.
- Modification des services d'une entité : suppression ou modification des comptes sur un serveur par exemple.
- Ajout des services à une entité du réseau : activation d'une fonction de mirroring de port sur un commutateur Ethernet pour une écoute illicite du trafic.

Il existe heureusement quelques mécanismes de protection, qui peuvent se répartir selon deux familles distinctes : au niveau réseau et au niveau applicatif. [25]

4.5 Gestion de la compatibilité

Cette gestion a pour mission de relever les informations permettant d'évaluer le cout d'usage d'une ressource (service de fichier, impression..). Cette mesure tient compte de deux paramètres essentiels :

- Du temps d'utilisation de la ressource (utilisation d'un logiciel de bureautique par exemple).
- Du volume d'information échangé (cas typique de connexion sur un réseau public à commutation de paquets dont la facturation est fonction du nombre d'octets transmis). [25]

5. La surveillance

Les moyens de surveillance sont habituellement orientés vers la surveillance régulière du bon fonctionnement des applications importantes et des services essentiels au bon fonctionnement du système informatique (DNS par exemple) et l'émission d'alertes en cas de dysfonctionnements. Ces systèmes peuvent également être destinataires des alertes générées

par les équipements eux-mêmes quand ils en sont capables (par exemple via l'utilisation de traps SNMP pour les équipements supportant ce type de protocole de gestion). Ces outils visent à améliorer le fonctionnement du système, en détectant rapidement des défaillances pour y pallier efficacement. [23]

5.1 Définition

La surveillance est une procédure de récupération des informations et comparaison afin d'observé tous changement ou défaillance survient le réseau.

5.2 Domaines de surveillance

On peut surveiller :

- L'état physique d'une machine : température, disques.
- La charge d'une machine : nombre d'utilisateur, de requêtes, la CPU, débit réseau ...
- Disponibilité applicative : présence de processus et leur réponse par exemple.
- Les messages inscrits en logs systèmes (Event-Viewer) concernant une application ou un composant système.
- Les performances du réseau : débit, latence, taux d'erreur, QoS ...
- La nature des protocoles d'un réseau et leur taux relatif : UDP, TCP, ICMP, idem pour la couche 4...
- Les attaques connues sur un Pare-feu par exemple. [23]

6. Supervision réseau

La notion de 'supervision' a, souvent, été confondue avec celle de 'surveillance', la différence entre les deux notions est très mince, elle réside dans la portées de chacune. On dénote par supervision une opération de surveillance qui porte sur plusieurs organes ou entités, ça veut dire que la notion de supervision englobe celle de la surveillance.

6.1 Définition

Le monitoring (supervision) est d'un point de vue théorique assez simple à expliquer. Il s'agit en fait de répéter de manière régulière un processus de test ou de surveillance d'une personne ou d'un bien. Le but étant d'obtenir très rapidement et simplement une vision

précise des événements ou anomalies sur la période analysée.
Appliqué à l'informatique, on obtient un système capable de surveiller des serveurs ou tout autre équipement (Firewalls, routeurs…) permettant de remonter différents niveaux d'informations dans divers buts. [24]

La supervision désigne un ensemble de concepts recouvrant la surveillance du bon fonctionnement d'un système informatique (matériel, services, applicatifs) en production.

On distingue trois types :

6.1.1 Supervision système

La supervision système porte principalement sur les trois types principaux de ressources système : processeur, mémoire et stockage.

6.1.2 Supervision réseau

La supervision réseau porte sur la surveillance de manière continue de la disponibilité des services en ligne - du fonctionnement, des débits, de la sécurité mais également du contrôle des flux.

6.1.3 Supervision des applications

La supervision des applications (ou supervision applicative) permet de connaître la disponibilité des machines en terme de services rendus en testant les applications hébergées par les serveurs.

À titre d'exemple, un serveur Web peut avoir une supervision système et réseau avec des signaux au vert, et la machine ne sera pourtant pas disponible au sens du service Web si apache n'est pas présent ou n'est pas en mesure de servir des pages Web. [23]

6.2 Intérêt et rôle

Le concept de supervision réseau est né au début des années 1980, lors de la croissance importante de mises en place de réseaux informatiques dans les entreprises. La taille grandissante de ceux-ci ainsi que leur hétérogénéité posaient un réel problème de gestion et d'administration, multipliant les besoins en main d'œuvre d'experts administrateurs. C'est donc à cette époque qu'ont été menées les premières réflexions sur un nouveau concept, celui de la supervision.

La supervision doit permettre de gérer les anomalies (détection et résolution des problèmes), les configurations (inventaire, configuration matérielle et logicielle), les performances (évaluer les comportements et optimiser le fonctionnement), la sécurité (filtrage des accès, redondance des équipements, sauvegarde) et la comptabilité (déterminer l'utilisation et le coût de ressources réseau). La supervision doit correspondre à un système réactif et proactif.

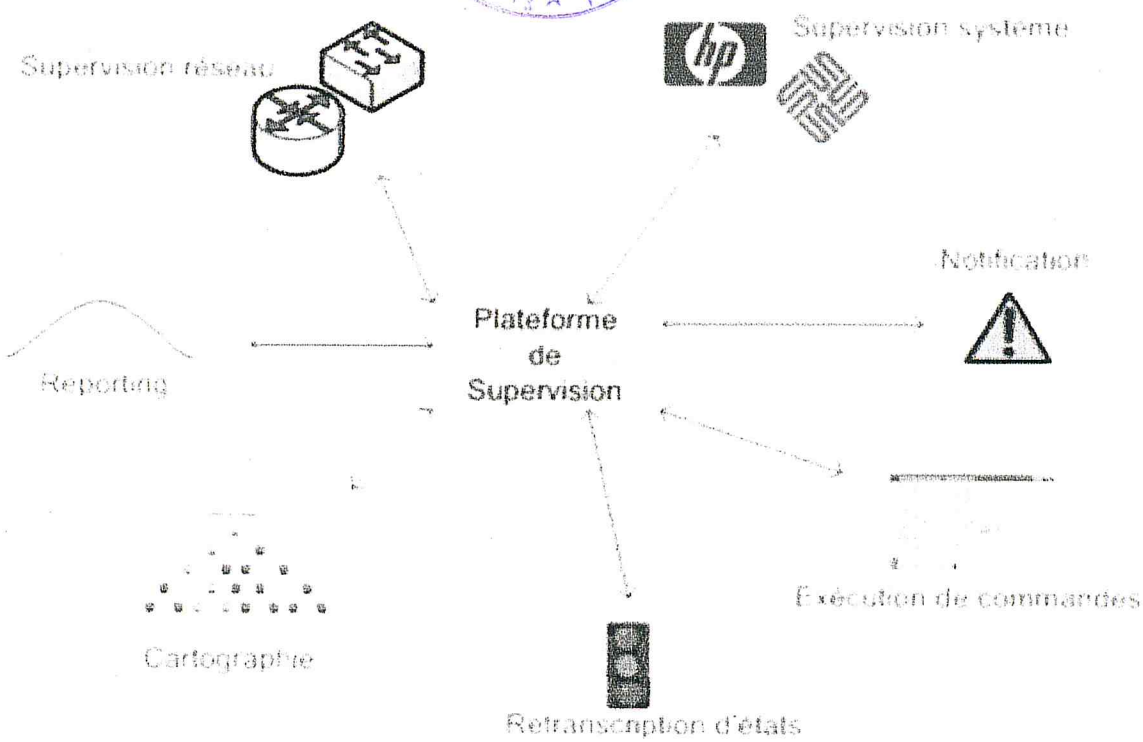

Figure 12:Rôles principaux d'une plateforme de supervision [23]

Supervision réseau : elle consiste à la surveillance continue de la disponibilité des services, du fonctionnement global du réseau, de la bande passante consommée, la sécurité, etc.

Supervision système : elle consiste à la vérification des ressources matérielles et logicielles (mémoire, CPU, disque dur, mise à jour, etc..).

Exécution de commandes : ce module consiste au lancement automatique d'un certain nombre d'action ou programmes.

Envoi d'alertes : c'est une forme de notification (par SMS, par e-mail, etc..) dans le cas d'un fonctionnement anormal.

Cartographie : consiste à schématiser l'architecture surveillée.

Rapports d'activités : ils représentent les tableaux de bord et les histogrammes.

7. Approches de la supervision

Définissons maintenant ce que nous pouvons en faire avec les approches ou types d'informations pouvant être fournies par le monitoring.

La Fiabilité : Il s'agit de loin de l'utilisation la plus courante du monitoring informatique. Le but ici est de surveiller en permanence la disponibilité de l'équipement afin de détecter la moindre anomalie et si nécessaire de remonter une alerte.

La Performance : Le monitoring de performance a pour but de retourner des informations sur la disponibilité d'un équipement comme par exemple le temps de résolution DNS, le temps de connexion, le temps de récupération du premier octet et dans le cas d'une page Web le temps de récupération de la page et de l'ensemble des éléments de celle-ci (image, .css, scripts…). Grâce à cette analyse, vous allez pouvoir diagnostiquer une montée en charge difficile ou même un surdimensionnement de votre bande passante.

Le Contenu : Dans ce cas, les informations retournées par les éléments surveillés sont analysés, pour par exemple, détecter la suppression d'un fichier sur un serveur ftp, la modification d'une page Web ou la disparition d'un mot clef. [24]

8. Outils de supervision

8.1 Les scripts

Cette technique consiste, à récupérer des résultats de commandes ou scripts exécutés sur des postes distants, ces derniers fournissent des données de supervision au poste de contrôle centrale pour qu'il les traite et affiche les données pertinentes sur la console d'administration, afin de donner à l'administrateur une vision claire sur l'état des machines.

8.2 Fichier log

Les journaux d'événements (ou fichier log) sont des fichiers textes enregistrant de manière chronologique les événements exécutés par un serveur ou une application informatique.

Toutes les actions des utilisateurs (ouverture d'une session, connexion à un site, exécution d'une application, etc.) génèrent des traces enregistrées dans des fichiers log. L'analyse des fichiers Log peut se faire manuellement, dans le cas des fichiers simples à lire. Mais dans la plupart des cas, les fichiers Log ne sont pas aisés à déchiffrer, ce qui oblige les administrateurs à utiliser des outils d'analyse qui permettent d'extraire des informations pertinentes et compréhensibles. L'accès aux fichiers de journalisation est, souvent, limité car ils contiennent des informations confidentielles (adresse IP, configuration du système, liste des processus, etc.)

Il existe plusieurs types de journalisations, ces types différents suivant les données à enregistrer (journalisation applicative, journalisation du système, etc.). Dans la majorité des cas les événements enregistrées sont classée par degré de gravité (erreur, débogage, alertes, etc.), ceci permet à l'administrateur de prendre les mesures de correction nécessaires suivants les catégories des notifications. [19]

8.3 Le protocole SNMP

8.3.1 Présentation

SNMP signifie Simple Network Management Protocol (protocole simple de gestion de réseau en Français). C'est un protocole qui permet comme son nom l'indique, de gérer les équipements réseaux ainsi que les machines informatiques. Ce protocole est donc utilisé par les administrateurs réseaux pour détecter à distance les problèmes qui surviennent sur leur réseau.

Chaque machine, que ce soit sous Windows ou sous Linux possède de nombreuses informations capitales pour l'administrateur réseaux.

On retrouve des informations comme la quantité de RAM utilisé, l'utilisation du CPU, l'espace disque et encore bien d'autres indicateurs.

SNMP va permettre de remonter ces informations à l'administrateur de façon centralisé pour pouvoir réagir au plus vite aux pannes éventuelles. [15]

8.3.2 Choix du protocole UDP

L'IETF (Internet Engeneering Task Force) retenu UDP (User Datagram Protocol) dans son architecture SNMP.

Par opposition à TCP, lourd et complexe à implémenter en raison de ses services en mode connecté, UDP est un protocole simple, dont le traitement ne grève pas les performances de l'élément actif du réseau. En effet, les appareils mis en œuvre dans un réseau ont pour priorité d'effectuer les opérations pour lesquelles ils sont prévus : un routeur est conçu pour router les datagrammes et les acheminer dans un réseau maillé, la gestion des événements étant importante mais secondaire quant au fonctionnement global du réseau. UDP est simple à implémenter et performant à exécuter.

Malgré tout il reste un protocole en mode non connecté. Cela entraine les faiblesses suivantes :

- Fonctionnement non contextuel : UDP ne gère pas le séquencement des messages qui peuvent, dans un réseau IP, arriver au destinataire dans un ordre différent de celui d'émission.
- UDP ne gère pas la fragmentation et limite la taille des messages SNMP à 484 octets (taille maximale de 512 octets dont 8 octets d'en-tête et 20 octets de pseudo en-tête).
- Comme IP, UDP ne prend en charge ni la gestion d'erreur (détection et reprise), ni la garantie de remise des informations.

Le protocole SNMP utilise deux ports UDP, définis par la RFC 3232 (Assigned Numbers) :

- Le port 161, ouvert dans l'élément actif (que l'on appellera Agent), pour la réception d'un message d'interrogation ou de modification d'une variable de configuration, envoyé par la station de supervision (que l'on appellera Manager).
- Le port 162, ouvert dans le Manager à l'écoute d'un message d'alarme émis par l'Agent.

Avant tout, les ressources d'un élément actif à superviser sont quasiment identiques quelle que soit l'origine de l'appareil. En effet tous les routeurs intègrent des interfaces, des buffers, des tables de routage, tous les commutateurs Ethernet sont constitués d'interface ayant des attributs spécifiques (vitesse, mode de transmission, appartenance à un VLAN, éventuels paramètres de QoS et de filtrage).

Il convient donc, pour une bonne intégration de ces appareils dans un plate-forme de supervision, de modéliser leurs ressources de manière exhaustive, pour pouvoir les manipuler (mise à jour d'une table de routage, modification de la configuration d'un port de commutateur) d'une part, et recueillir des informations quant à leur fonctionnement (statistiques, incidents éventuels) d'autre part. de plus, ces opérations doivent pouvoir être effectuées en faisant abstraction de leur système d'exploitation spécifique.

Toutes ces informations constituent une base de données appelée MIB (Management Information Base). Ainsi, tous les éléments actifs du réseau seront vus comme autant de MIB's. Bien entendu le schéma de cette base de données est défini par L'IETF et fait l'objet de la RFC 1156 (mai 1990). Pour une parfaite interopérabilité, la MIB doit être connue de l'appareil lui-même et de la plate-forme de supervision.

Cette base de données est organisée de façon arborescente, codé en ASN.1.

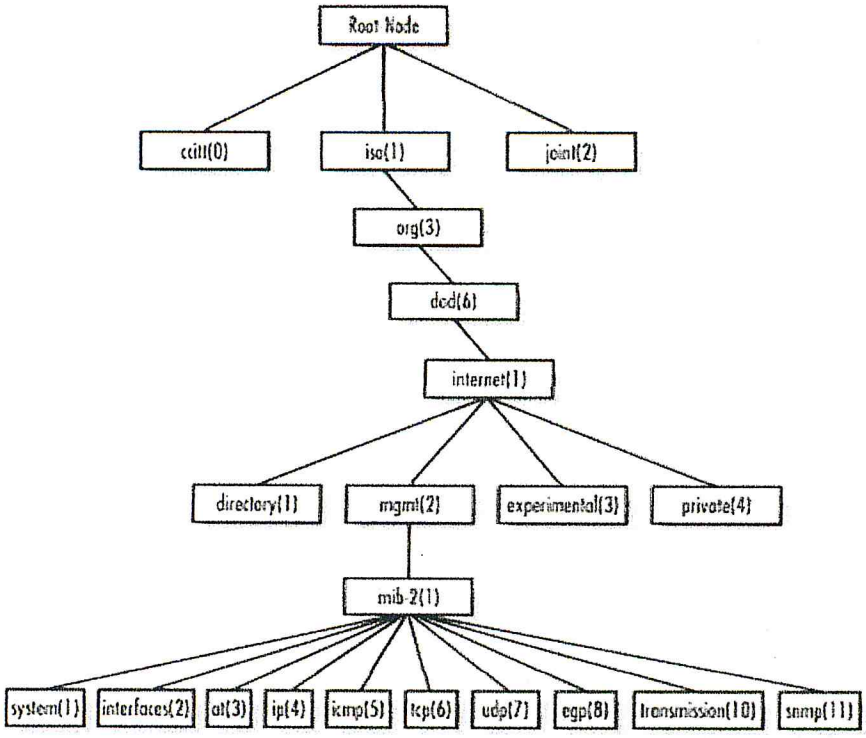

Figure 13 : Arborescence de la MIB [15]

Le logiciel traitant la MIB implémenté dans l'élément actif est appelé Agent et le logiciel implémenté dans la plate-forme de supervision est appelé Manager.

Manager et Agent échangent les données à l'aide d'un protocole de communication spécifique SNMP. [15]

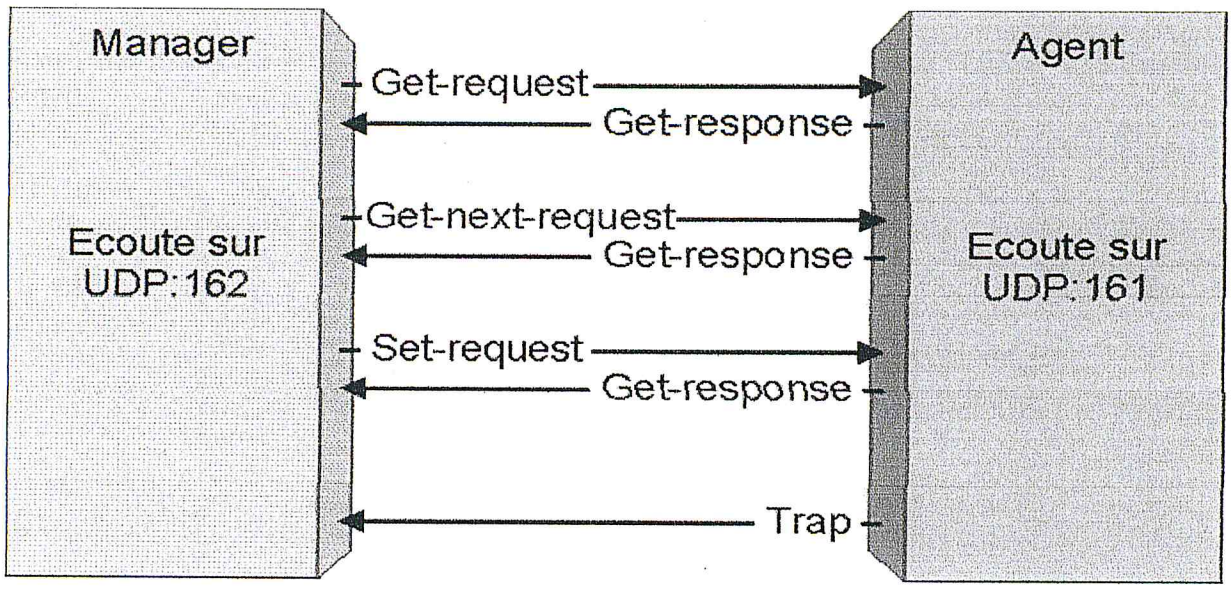

Figure 14: Types des messages SNMP [15]

8.3.3 Manger SNMP

La station de gestion du réseau (Manager) contient le protocole de communication et les applications de gestion. Composée d'un poste de travail (console), de bases de données (MIB's) identiques à celles déployées dans les éléments actifs du réseau et, de fait, toutes les variables connues des systèmes.

Le Manager permet de collecter les données relatives aux équipements connectés au réseau et de les gérer. Ces données peuvent etre utilisées pour élaborer des tableaux de bord ou des rapports d'incidents. Le Manager (élément de l'architecture SNMP) peur être nommé NMS (Network Manager Système) par certains éditeurs de suites logicielles.

Les informations gérées par le Manager SNMP se limitent bien souvent aux trois premières couches du modèle OSI (ou au deux premières couches du modèle TCP/IP). L'architecture SNMP (organisation des MIB's, structure des messages échangés) a été définie dans ce sens. Ceci étant, des applications complémentaires peuvent y être adjointes pour constituer une plate-forme de supervision plus générale, ayant la visibilité des ressources systèmes (charge des processeurs des serveurs, gestion mémoire, capacité des disques durs..) voire des applications informatiques. Des interfaces (MIB's spécifiques) peuvent également contrôler les éléments d'environnement (mesure de la température et de l'hygrométrie dans les salles informatiques, contrôle de l'accès aux locaux techniques, gestion des onduleurs

électriques notamment). La finalité est de mettre à disposition des équipes d'exploitation (et des spécialistes) une vue globale de l'état du système informatique. [15]

8.3.4 Agent SNMP

C'est un logiciel implémenté dans les éléments actifs du réseau (et composants connexes) que doit superviser le Manager.

Comme tout logiciel, l'Agent SNMP nécessite des ressources en processeur et en mémoire. Ainsi, un hub Ethernet géré par un Manager, dont la fonction initiale est d'être un simple répéteur électrique (niveau OSI 1) sera doté de composants électroniques et logiciels (Agent et MIB) dédies à la supervision. La plupart des routeurs et commutateurs Ethernet du marché (s'ils sont dits mangeables) intègrent nativement les éléments nécessaires à leurs supervisions. L'implémentation des MIB's définies par l'IETF est obligatoire.

Les paramètres de l'agent SNMP seront :

- Son adresse IP et le masque de sous réseau associé.
- L'adresse éventuelle du routeur par défaut.
- L'adresse IP de son Manager.
- Le nom de communauté SNMP en lecture seule (read only).
- Le nom de communauté SNMP en lecture écriture (read-write).

Notez qu'un Agent peut connaitre plusieurs Managers et que les communautés SNMP peuvent être multiples, en lecture comme en écriture.

Cela veut dire qu'en complément de la connectivité IP, les éléments actifs doivent être dotés d'un port console asynchrone pour la connexion d'un terminal écran-clavier nécessaire au paramétrage initial de l'appareil. Dans la plupart des cas, l'implémentation IP de ces équipements intègre les protocoles TELNET pour la console distante, TFTP pour la sauvegarde des configurations et ICMP pour les tests ECHO (Ping). Le protocole ARP est indispensable à la corrélation adresse MAC/adresse IP. [15]

8.3.5 Avantages

- Accès centralisé : la gestion réseau s'effectue depuis une machine centrale sans soucis, et c'est même préférable.

- Fiabilité : le protocole utilisé permet de s'assurer que les requêtes sont bien arrivées à destination et qu'elles ont été correctement interprétées.
- Gestion de la diversité : l'utilisation d'une interface standard à tous les matériels permet de contrôler de la même manière tous l'équipement réseaux, ce qui a des avantages indéniables lorsque l'on dispose d'un parc informatique très diversifié.

8.3.6 Inconvénients

- Le premier défaut de SNMP est qu'il contient quelques gros trous de sécurité à travers lesquels des intrus peuvent accéder aux informations transitant sur le réseau. Ces intrus pourraient aussi bien provoquer un shut-down sur certains terminaux. La solution à ce problème est apportée dans SNMPv2 qui implémente des mécanismes de sécurité en ce qui concerne le caractère privé des données, l'authentification et le contrôle d'accès.
- Puisque SNMP se trouve au dessus de UDP, il n'y a pas de reprise sur erreur, ni de contrôle de flux. La requête ou la réponse peut être égarée, ce qui peut être gênant dans le cas du trap. Le Manager surveille donc son environnement en procédant à des interrogations régulières de ses agents, c'est ce que l'on appelle le Polling. SNMP est donc un protocole bavard. Cette surcharge de trafic n'est pas trop gênante sur un réseau local mais devient embarrassante via le réseau public. (Ce qui rend CMIP plus adapté aux grands réseaux)

8.4 Protocole CMIP/CMIS

CMIP (Common Management Information Protocol/Services) est un protocole définit par OSI et IETF dans le RFC 1189, ce protocole définit le format des messages et les procédures utilisées pour échanger des informations de gestion et d'administration de façon a gérer, exploiter, maintenir et approvisionner un réseau. Il repose sur l'utilisation des MIBs contenant les informations utiles a l'administration de réseau. Techniquement, ce protocole est adapté a la gestion des équipements plus complexes que SNMP, ainsi si des ressources sont disponibles, les services offerts par CMIP dépassent ceux de SNMP. [16]

8.4.1 Fonctionnement de CMIP

Le CMIP est un protocole de gestion développé par ISO pouvant fonctionner sur des réseaux hétérogènes. Nous pouvons le comparer avec SNMP sur le fait que les deux

protocoles se servent de tables MIB pour effectuer leur travail. D'ailleurs, le CMIP a été construit a partir du SNMP. Par contre, leur fonctionnement est plutôt différent puisque dans le protocole CMIP, la station s'occupant de la gestion ne va pas chercher elle-même les informations, elle attend que les stations rapportent leur état. Le CMIP est un protocole très évolué comparativement au SNMP, les stations doivent pouvoir exécuter les tests elles-mêmes, par exemple, une station, qui a eu plusieurs problèmes consécutifs à accéder a un serveur de fichier doit avertir l'ordinateur de gestion. [16]

8.4.2 Avantage

- Sécurité développée : l'avantage le plus connu du protocole CMIP /CMIS est la sécurité des informations échangées.
- Modèle d'information basé sur l'approche orientée objet. [16]

8.4.3 Inconvénients

- La plupart des applications de supervision de réseau supportant le protocole CMIP sont des systèmes complexes, difficiles à mettre en œuvre notamment sur un système de traitement de l'information (un ordinateur) de taille modeste.
- De surcroit, ces systèmes demandent un long apprentissage pour parvenir à leur maitrise et n'offrent pas toujours de fonctions d'animation de données évoluées.
- Non supporté par tous les équipements. [16]

A cause de ces inconvénients il n'est pas utilisé largement dans la réalité.

9. Outils complémentaire pour la supervision

La plupart des logiciels de supervision utilisent des outils élémentaires pour récupérer des informations ou des statistiques sur les éléments composant le réseau, parmi ces outils on cite le WMI et CPUID de la compagnie Microsoft Windows.

9.1 WMI et la supervision

WMI (Windows Management Instrumentation) est l'implémentation de Microsoft du Web-Based Enterprise Management (WBEM), le standard du Distributed Management Task Force (DMTF). Il prend en charge le modèle de données CIM (Common Information Model), qui décrit les objets d'un environnement de gestion.

WMI permet de surveiller et contrôler les ressources systèmes de windows. Grâce à lui, vous pouvez récupérer énormément d'informations de votre machine en local mais aussi des machines distantes.

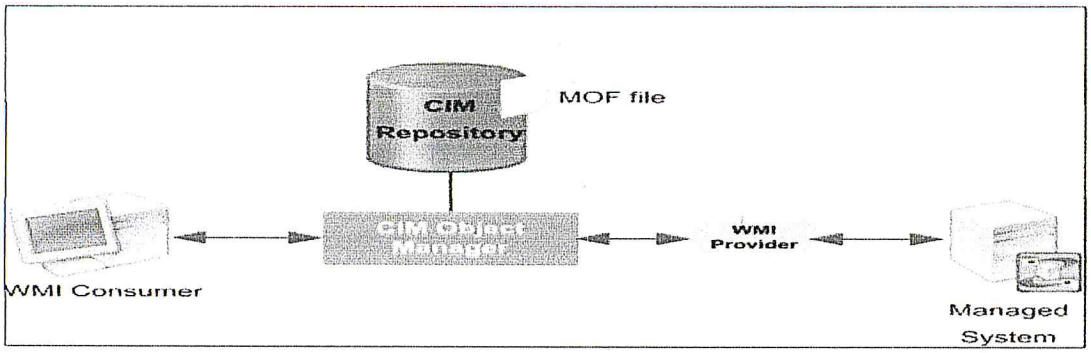

Figure 15: Fonctionnement de WMI

9.1.1 Obtenir les données

Tout simplement en effectuant des requêtes proches de SQL, j'ai nommé WQL.(si vous maîtrisez la norme SQL, vous n'aurez pas de difficultés à vous y retrouver).

Exemple de requête:

*[" SELECT *FROM Win32_LogicalDisk WHERE FreeSpace<2000000 "]*

En plus de récupérer des informations de supervision, vous pouvez aussi agir sur vos machines, par exemple pour installer ou désinstaller des programmes:

Exemple de script :

```
[Set objWMIService = GetObject("wingmgmts :"_
& "{impersonationLevel=impersonate} !\\"_
&strComputer & " \root\cimv2")
Set colSoftware = objWMIService.ExecQuery_
("Select * from Win32_Product "_
& "Where Name = 'Personnel database'")
```

For Each objSoftware in colSoftware

objSoftware Unistall()

Next]

Enfin, WMI contient une infrastructure évènementielle qui vous alertera en fonction de votre politique de supervision.

Exemple de script: (Lorsqu'un évènement Windows apparait, une action est déclenchée. Dans ce cas, un popup)

[Sub SINK_OnObjectReady(objObject, objAsynContext)

WScript Echo (objObject. TargetInstance.Message)

End Sub

Set objWLIServices = GetObject(_

"WinMgmts :{impresonationLevel=impersonate, (security)}")

'Create the event sink object that receives the events

Set sink = WScript.CreateObject("WbemScripting.SWbemSink","SINK_")

'Set up the event selection. SINK_onObjectReady is called when

'a Win32_NTLogEvent event occurs

objWMIServices.ExecNotificationQueryAsync sink, _

*" SELECT * FROM__InstanceCreationEvent " & _*

"WHERE TargetInstance ISA Win32_NTLogEvent' "

WScript.Echo "Waiting for events"]

9.1.2 Avantage

- Une base de données importante (vous trouverez forcément votre bonheur).
- Un accès ouvert et simple (WQL) aux données.

- Accès aux informations à distance (nécessite droits administrateur sur la machine distante et ouverture firewall).

9.1.3 Inconvénients

- Uniquement pour les plateformes Windows.
- Peu d'informations réseaux par rapport à SNMP.
- Natif à partir de Windows 2000 SP4. [18]

9.2 CPUID (Central processor unit identify)

Le CPUID est un produit Intel destiné pour les processeurs de type pentium. Il donne la possibilité d'extraire différentes caractéristiques de ces processeurs telles que la vitesse, le constructeur, le numéro de série etc. Actuellement le CPUID est devenu un standard utilisé par des constructeurs des processeurs comme AMD, UMC et CYRIX. Ce produit utilise des instructions, pour extraire ces informations, écrites en assembleur ce qui facilite leurs exploitations. [17]

10. Logiciels de supervision

Un logiciel de supervision est composé d'un ensemble de pages (d'écrans), dont l'interface opérateur est présentée très souvent sous la forme d'un synoptique.

10.1 HP OpenView

HP OpenView Est une plate forme de supervision réseau, proposent un ensemble d'outil d'administration, développée par la compagnie HP (Hewlett-Packard) . il est composé de plusieurs produit indépendants tels qu'ITO (information technology opération), gestionnaire des nœuds, gestionnaire de performance……, l'utilisation de ces produits peut nous ramener à des graphiques qui permet un affichage d'état courant des équipements et un système d'alarme permet de gère tout les équipements. Il est basé sur le protocole SNMP pour dialoguer avec les différentes machines, ainsi il peut être atteint depuis la station de supervision, une console distante ou un navigateur, garantissant une grands accessibilité aux fonctionnalités fournie par le gestionnaire des nœuds telles que :

- La cartographie du l'ensemble du réseau.

- La collecte des informations critiques du réseau.
- La génération automatique des statistiques et les analyses graphique.

Ainsi, les principales fonctionnalités de cet outil sont classées en six familles :

Optimisation de l'infrastructure, gestion de réseau, les opérations, le système, gestion de performance et système d'alarme.

10.1.1 Avantages

- Centralisation de la gestion du réseau (les administrateurs peuvent superviser toutes les serveurs et à n'importe quels endroits).
- Une représentation graphique simple de touts les équipements du réseau facilite l'interaction administrateur/événement.
- Supervision des équipements variés (pc, switch.....) et des divers systèmes d'exploitation (unix, windows, solaris..).
- La capacité de collecte les informations concernant le réseau et de les représenter graphiquement.

10.1.2 Inconvénients

- Logiciel lourd.
- Le cout de cet outil est très élevé.
- Nécessite d'autres modules (gestion de performance, gestion d'historique...). [16]

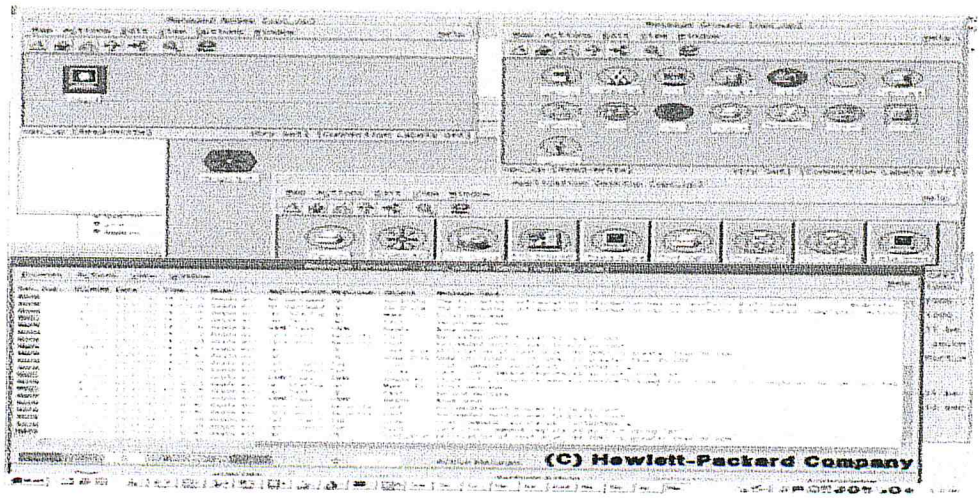

Figure 16: Interface HPOpenView

10.2 CiscoWorks

10.2.1 Présentation

CiscoWorks est un superviseur réseau propriétaire conçu par la fabriquant Cisco. Il est dirigé spécialement pour la supervision des équipements Cisco sur des petits réseaux tels que les réseaux de campus.

Grace à une interface de navigateur web fournit par CiscoWorks l'operateur peut administrer le réseau d'une façon plus efficace. De plus, il peut réduire la probabilité des erreurs humaines avec les outils qu'ils facilitent la configuration et le dépannage des routeurs, commutateur et d'autres équipements.

10.2.2 Fonctionnalités

Les fonctionnalités de CiscoWorks sont distinguées en deux catégories :

- **Gestion du cycle de vie des unités :**

CiscoWorks fournit les outils pour suivre les changements sur la configuration des unités (matériel et logiciel) et faire des mises à jour selon ces modifications (mot passe, identifiant…) dans le but d'assurer la sécurité du réseau.

- **Gestion d'infrastructure de réseau :**

CiscoWorks peut représenter l'ensemble du réseau c-à-d tous les équipements informatiques existants sur le réseau et même ceux qui différent de la technologie Cisco (PC, serveur, application).

10.2.3 Avantages

Parmi les avantages connus de ce produit on trouve :

- Simple à utiliser et à manipuler car il dispose d'une interface web.
- Dispose d'une topologie graphique du réseau.
- Collecte les différentes informations matérielles et logiciels, nécessaires à la supervision, concernant les équipent Cisco. [16]

10.2.4 Inconvénients

- CiscoWorks assure la supervision seulement des équipements Cisco, donc pour un réseau hétérogène la cartographie sera faussée.
- Il est destiné pour la supervision d'un nombre d'équipement très réduit, alors il n'est pas efficace pour les réseaux de grand envergure.
- C'est un produit propriétaire et non modulaire, donc on ne peut pas lui ajouter des modules supplémentaires.
- Le cout d'acquisition de produit est chère comparativement aux autre produits. [16]

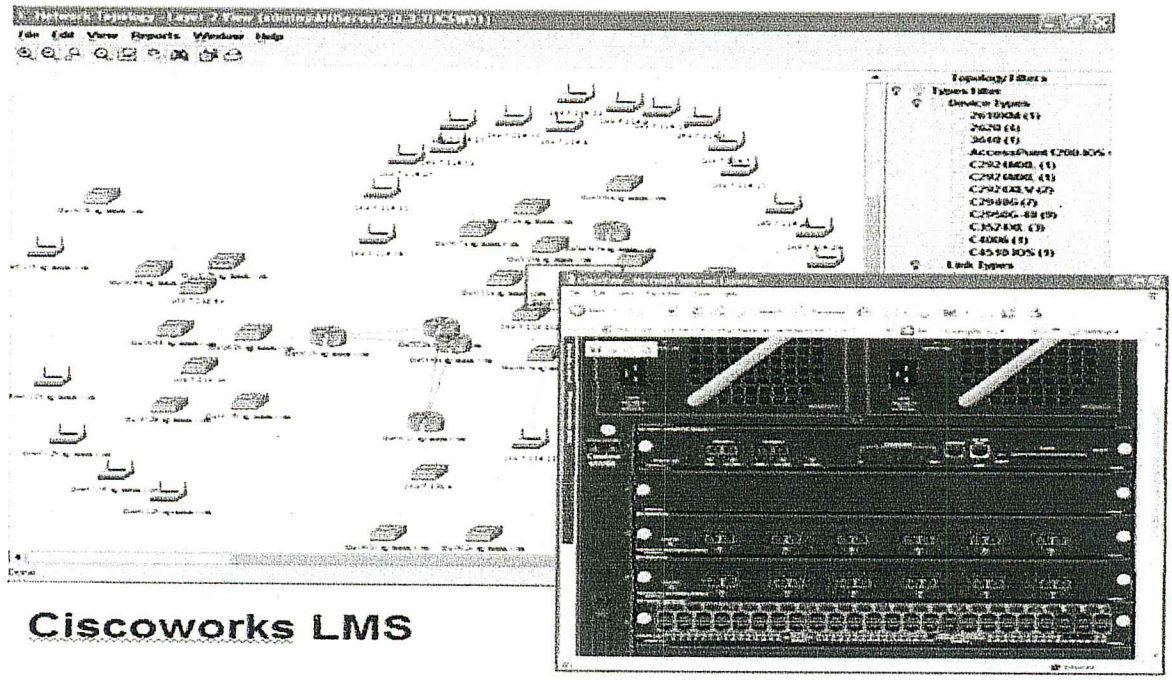

Figure 17: Interface Ciscoworks

10.3 Nagios

10.3.1 Présentation

Cet outil est un moniteur de supervision des services open source. Il permet la supervision des différents services réseau comme SMTP, http, Mail, Messagerie..... Et des ressources système telles que CPU, espace disque,... ce logiciel a été développé pour fonctionner sur une plateforme linux.

Les service de surveillance lancent et retournent l'information à Nagios. a tout moment, si un problèmes est rencontré, les services dérangés peuvent envoyer des

avertissements aux administrateurs de réseau de différentes manières par exemple e-mail, SMS.... Nagios

A une interface web permet de consulter très facilement de nombreuses informations telles que l'état courant du réseau, l'historique des évènements ainsi que des comptes-rendus d'activité. [22]

10.3.2 Avantages

- C'est un logiciel gratuit et appartient au monde open source.
- Une conception simple de plug-ins permettant aux administrateurs de développer facilement leurs propres fonctionnalités de surveillance, il permet l'évolution suivant les besoins de l'administrateur réseau et système.
- Utilise une interface web ce qui le rend accessible depuis n'import quel navigateur.

10.3.3 Inconvénients

- Nagios ne repose sur aucune norme de supervision de réseaux, plus particulièrement, dans le contexte ou Nagios
- Répond à la supervision de services dans le monde IP, que celle-ci ne repose pas sur SNMP.
- Nagios, fonctionne seulement sur une plateforme Unix donc il n'est pas multiplateforme.
- Nagios ne garde pas l'historique de changement d'état (l'utilisation des logs).
- Pour la découverte réseau, Nagios ne dispose pas d'un plugin qui lui donne une vue globale sur le réseau ce qui oblige l'administrateur à ajouter les machines un par un sur la configuration. [20]

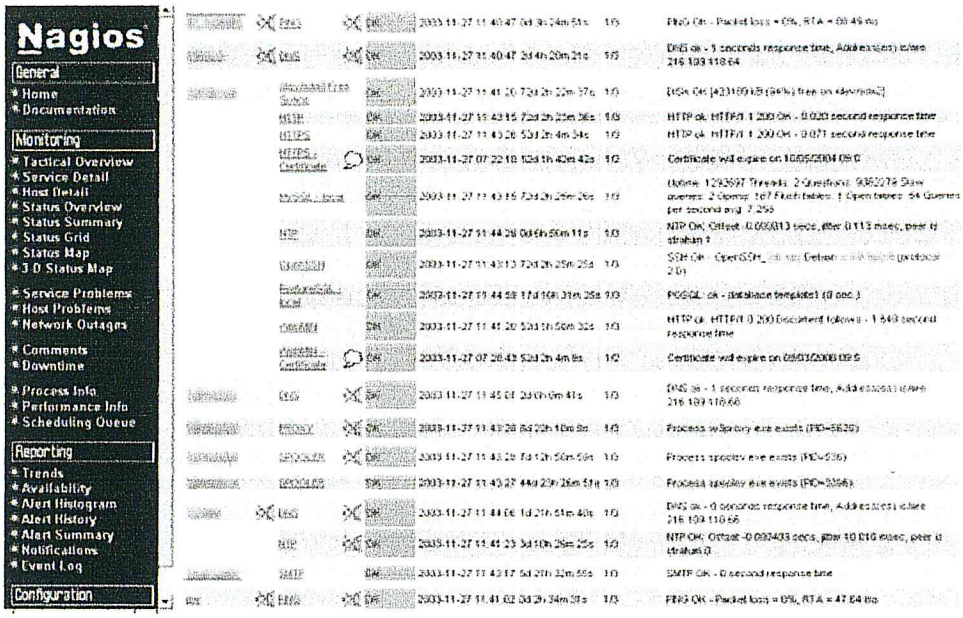

Figure 18: Interface Nagios

10.4 Zabbix

10.4.1 Présentation

Créé en 2001, puis donnant naissance à une entreprise nommée Zabbix SIA en 2005, Zabbix est une solution de supervision open-source de plus en plus prisée. L'entreprise vise à faire de Zabbix un logiciel reconnu dans le milieu de la supervision et créer une communauté autour de lui pour permettre une évolution plus rapide. A côté de cela, cette société propose un service de maintenance commercial.
Zabbix permet plusieurs moyens d'acquérir les données :

- Via SNMP : comme tous ses concurrents
- Via test de service : Il n'y a rien a installer sur l'équipement surveillé, mais les tests sont limités à des Ping ou test de protocoles (SMTP, HTTP,...)
- Via l'agent Zabbix local : C'est une originalité, installer un agent permet d'obtenir toute information sur l'équipement sans utiliser le protocole SNMP

L'architecture logicielle est découpée en composants dans le but de faciliter le monitoring distribué :

- Serveur : Le serveur est le cœur de l'application Zabbix. Il centralise les données et permet de les attendre (trapping) ou d'aller les chercher (polling). Il centralise aussi

toutes les informations de configuration et permet d'alerter les administrateurs en cas de problème.

- Le proxy : Élément optionnel de l'architecture, il permet de bufferiser les données reçus des différents sites dans le but d'alléger les traitements pour le serveur.
- L'agent : Une fois installé sur un système, l'agent va collecter les données locales et les envoyer au serveur.
- L'interface Web : Celle-ci est une partie du serveur bien qu'il n'est pas obligatoire qu'elle se trouve sur la même machine que le serveur. L'interface permet de configurer entièrement Zabbix, d'accéder aux statistiques ainsi qu'à d'autres informations

Tous ces composants sont écrits en C afin de garder de hautes performances, ormis bien évidemment l'interface Web développée en PHP.
L'interface est divisée en cinq parties :

- Monitoring : La partie affichage des statistiques, graphiques, alertes, cartographie, etc...
- Inventory : l'inventaire des machines et équipements
- Report : Statistiques sur le serveur Zabbix et rapport de disponibilité des services sur les machines supervisées
- Configuration : Comme son nom l'indique, permet de configurer entièrement Zabbix
- Administration : Permet de gérer les moyens d'alertes (SMS, Jabber, Email, ...) et les utilisateurs.

10.4.2 Avantage

- Une solution très complète : cartographie de réseaux, gestion poussée d'alarmes via SMS, Jabber ou Email, gestion des utilisateurs, gestion de pannes, statistiques et reporting.
- Une entreprise qui pousse le développement, et une communauté croissante
- Une interface vaste mais claire.
- Une gestion des templèates poussée, avec import/export xml, modifications via l'interface.
- Des performances au rendez-vous : l'application a été testée avec succès avec 10000 équipements supervisés
- Compatible avec MySQL, PostgreSQL, Oracle, SQLite.

10.4.3 Inconvénients

- Interface est un peu vaste, la mise en place des templates n'est pas évidente au début : petit temps de formation nécessaire.
- L'agent zabbix communique par défaut en clair les informations, nécessité de sécuriser ces données (via VPN par exemple).
- Commence à être connu, mais pas encore auprès des entreprises : Peu d'interfaçage avec d'autres solutions commerciales. [6]

Figure 19: Interface ZABBIX

10.5 NetMRG

10.5.1 Présentation

Créé en 2001, NetMRG veut se distinguer des autres en proposant des petites améliorations : Visualisation des graphiques avec historiques et "auto-scroll", utilisation de modèles (templates) pour plus facilement ajouter de nouveaux graphiques, mise à jour du logiciel simplifiée, Gestion des jours de travail.
L'architecture logicielle est découpée en composants :

- **Un moteur C++** chargé de récolter les données (Via scripts, Données SNMP ou MySQL). Conçu dans le but de supporter une charge conséquente (Application

multithread grâce à threads). Ce moteur est au cœur de l'application, il ordonnance les tâches et gère les interactions en plus de son rôle de "récolteur".

- **RRDTOOL** composant vu précédemment qui apporte sa puissante gestion des données ainsi que ses atouts indéniables en matière de génération de graphique.
- **Une base de données MySQL** permettant de sauvegarder la configuration.
- **Une interface réalisée grâce à PHP**, qui permet de modifier la configuration et d'afficher les graphiques au format PNG générés par RRDTOOL. Pour retrouver les graphiques on doit tout d'abord passer par un arbre qui organise les différentes machines et statistiques associées. Ce "Device Tree" affiche tout d'abord des groupes (Group) lesquels contiennent des machines (Device), puis on accède aux différents services ou valeurs monitorées (Sub device) avant de trouver à l'intérieur les graphiques (Monitors). Des "events" sont également visibles en cas de problème.

10.5.2 Avantage

- Performances : L'application semble pouvoir tenir la charge avec énormément de machines surveillées grâce au moteur multithread.
- Alarmes : Il est possible de configurer des évènements qui avertissent l'administrateur d'un fonctionnement anormal.
- Interface : L'interface permet de gérer un grand nombre de machines, classées dans des groupes.
- Gestion des utilisateurs

10.5.3 Inconvénients

- Interface : L'interface n'est pas très accueillante et est déroutante au début.
- Configuration : Il n'est pas très aisé d'ajouter de nouveaux équipements à surveiller si l'on sort du cadre du Template prédéfinie.
- Un développement lent, peu de versions et très espacées dans le temps (environ une année).
- Aucune gestion de carte de réseau, et aspect rudimentaire des alarmes. Aucune gestion de panne. [20]

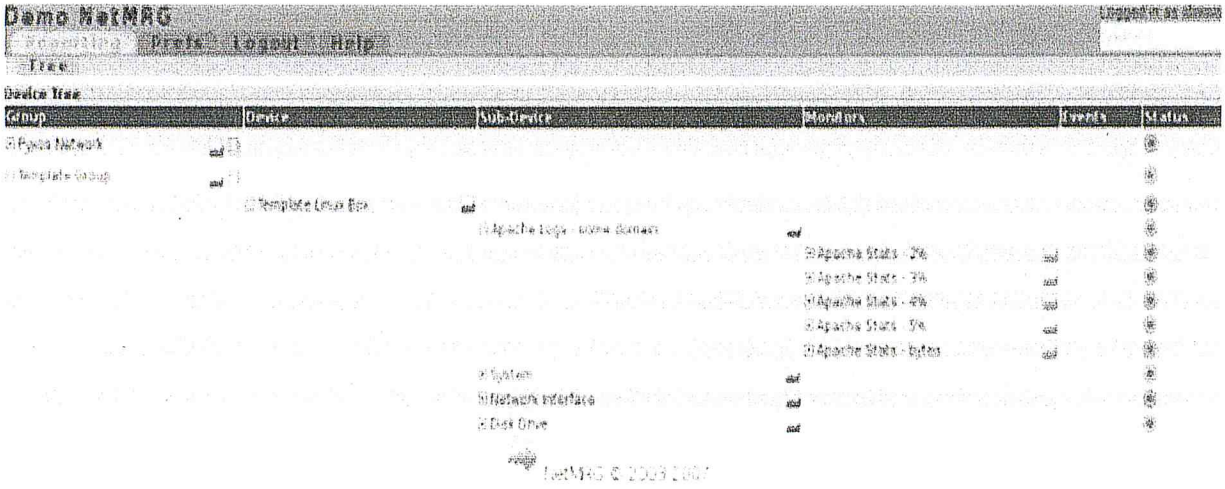

Figure 20: Interface NetMRG

11. Etude comparative des solutions de supervision

Les solutions de supervision existent avec une dense variété, certaines sont spécialisée dans la supervision de certains composant du SI, d'autre sont plus globale. La différenciation s'effectue généralement sur le nombre de paramètres exploitables et leur finesse d'analyse.

11.1 Référence de comparaison et d'évaluation

11.1.1 La spécialisation et complexité

- Des solutions de visualisation de l'état du réseau.
- Des solutions de gestion de performances.
- Des solutions de gestion des pannes.
- Des solutions dites complètes.

11.1.2 Type de la licence

- Les logiciels Open Source : sont caractérisé par une licence gratuite, et sont hautement personnalisable
- Les solutions de surveillance d'entrée de gamme : commencer par des solutions d'entrée de gamme bon marché. Elles reposent sur les bases élémentaires :
- Surveillance SNMP de la bande passante ou contrôle de disponibilité via Ping.

- Les solutions de surveillance dites « spécialisé » : concernent les solutions ciblant des portions spécifiques de réseau.
- Les logiciels de gestion de réseaux d'entreprise (propriétaire).

11.1.3 L'architecture de la supervision

- Centralisé
- Hiérarchique
- Distribuée

11.1.4 Capacité de supervision

- L'utilisation des outils standards : agent, SNMP, Syslog.
- Méthode de stockage de données.
- Présentation des informations : Maps, rapports, groupement hiérarchique, possibilité d'intégration des modules greffons (plugins).
- Diversité des alertes : un bip sonore, un simple message, un message graphique, un email jusqu'à un SMS.
- Une interface web.
- Gestion de contrôle d'accès. [21]

11.2 Tableau comparative

Le tableau suivant représente les principaux points forts et faibles des solutions de supervision et surveillance :

11.2.1 Outils de supervision

Outils base sur le protocole :	Point fort	Point faible
SNMP	• Simple a utilisé • Gestion de la diversité • Accès centralisé	• La sécurité • Pas de reprise sur les erreurs • Pas de contrôle de flux

	• surveillance des ressources des hôtes • gestion d'alertes • gestionnaire d'événement • Accès centralisé	• Graphes pas assez clairs • Administration compliquée
Zabix	• Découverte automatique des services (LDAP, SMTP…) • Surveillance temps réel : performance/disponibilité • Cartographie de réseau • Gestion d'alertes (SMS, Jabber ou Email) • Surveillance site web : « scenario » • Gestion de pannes	• Interface vaste et compliquée • Pas très connu
NetMRG	• Gestion d'alertes • Gestion d'un nombre important de machines • Performant en matière de graphs • Performant pour l'analyse des routeurs	• Aucune gestion de panne • Interface compliquée

Tableau 6: Tableau comparative (Logiciels de supervision)

12. Travaux réalisés

12.1 Conception et réalisation d'un système de supervision réseau a base d'agents

Consiste à réaliser un système de supervision informatique à base de traces numériques qui permet de surveiller les activités des utilisateurs et suivre l'état du matériel.

Le système suivre une approche basée sur les agents mobiles qui est une architecture récente dédiée à la réalisation des systèmes distribués, cette approche modélise les applications à travers un ensemble d'agents mobiles.

Un agent mobile est un système informatique, situé dans un environnement, qui agit d'une façon autonome et flexible pour atteindre les objectifs pour lesquels il a été conçu. [24]

12.1.1 Les objectifs

Assurer la collecte des informations de comportement des machines, que ce soit en local (applications lancées, ou sur le WEB (sites visités à partir de la machine).

Assure la collecte des informations concernant les composants des machines du réseau (information sur le matériel).

N'extraire que les informations utiles pour le processus de supervision. [24]

12.1.2 Les imperfections

- Pas de gestion des alertes.
- Pas de surveillance de services.
- Pas de gestion des utilisateurs.
- L'approche utilisée est difficile à mettre en œuvre par rapport au protocole SNMP.

12.2 Conception et implémentation d'une plate forme de supervision réseau et système basée sur une politique de sécurité

Consiste a la réalisation d'une plate forme de supervision réseau et système basant sur une politique de sécurité qui supervise le réseau en donnant son cartographié générale et le système en comparant les applications installées, les composants des équipements et les services fournis dans le réseau a une politique de sécurité définit par les administrateurs de réseau et système de l'entreprise. [16]

Une PSSI (Politique de Sécurité des systèmes d'informations) est une déclaration formelle des règles auxquelles doivent se conformer les personnes recevant un droit d'accès au capital technologique et informatif d'une entreprise.

Elle doit prévoir un schéma organisationnel de sécurité, s'appuyer sur des normes, des processus, des personnes et combiner plusieurs outils. Parmi les moyens employés on peut citer :

- La protection par des règles (classification des informations…).
- La protection par des outils (chiffrement..).
- La protection par des contrats (clauses, obligations..).
- La protection par l'identification (tatouage, marquage, copyright..).
- La protection par le dépôt (marques, brevets, droit d'auteur..).
- La protection par l'assurance (polices, exclusions..). [16]

12.2.1 Les fonctionnalités

- Un audit des différents composants matériels ou logiciels constituants le réseau.
- Une vue globale du réseau et la configuration de chaque constituant.
- Avertir l'administrateur lorsqu'une anomalie est détecté ou toute violation aux règles de la politique de sécurité tel que le changement d'un composant, ou la connexion d'une machine inconnue… [16]

12.2.2 Les imperfections

- Pas de gestion des alertes.
- Pas de gestion des utilisateurs.
- Aucune surveillance de services.

13. Conclusion

Tous ces logiciels que nous avons décris ci-dessus sont considérés comme un aboutissement et une réussite dans leur branche selon des statistique concerne les outils de supervision, cependant, on voit qu'ils ont tous leurs propres inconvénients qui doivent être résolus.

Un bon moniteur de supervision doit englober tous les avantages de ces derniers (l'accès centralisé, facile a utilisé, gestion des alertes, la sécurité, etc.…) et aussi remédier à leurs lacunes et inconvénients (la complexité, le cout, le nombre d'équipements supervisé,

etc. …) afin de converger vers la perfection et atteindre un niveau de supervision et de fiabilité optimum.

D'où la nécessité d'avoir un superviseur générique qui se base sur une interface simple pour suivre les besoins de l'entreprise basé sur le protocole SNMP qui est le plus utilisé et facile a implémenté dans les réseaux locaux.

Chapitre2 : Conception

1. Introduction

Nous allons présenter dans ce chapitre un cadre conceptuel permettant de schématiser l'architecture du système de supervision que nous proposons.

Nous rappelons tout d'abord que notre travail a pour visée l'observation régulière de l'état des équipements constituent le réseau, afin d'assurer leur disponibilité en terme de ressource matériels et logiciels, et détecté toutes anomalies et alerter l'administrateur.

Tout d'abord nous allons commencer le chapitre par l'introduction de l'organisme d'accueil, la maquette de réseau, par la suite nous allons présenter notre solution et définir toutes les taches nécessaires de notre système.

2. Organisme d'accueille

2.1 Introduction

L'École Militaire Polytechnique 'EMP' est un établissement de formation supérieur pluridisciplinaire, relèvent du ministère de la défense nationale et placé sous la tutelle pédagogique du ministère de l'enseignement supérieur et de la recherche scientifique.

Elle bénéficie d'un cadre agréable où s'intègrent harmonieusement, espaces verts et infrastructures modernes, de formation, de recherche, d'hébergement, de sport et de loisirs.

La proximité des principaux établissements de formation supérieure de la région centre, ainsi que de nombreux pôles industriels, favorise une dynamique de coopération et d'échanges, orientant le développement continu des activités de l'école vers les centres d'intérêt et les préoccupations de son environnement.

2.2 Maquette de réseau

La topologie de réseau utilisé est la topologie étoile, Dans une topologie de réseau en étoile, les équipements du réseau sont reliés à un système matériel central (le noyau). Celui-ci a pour rôle d'assurer la communication entre les différents équipements du réseau.

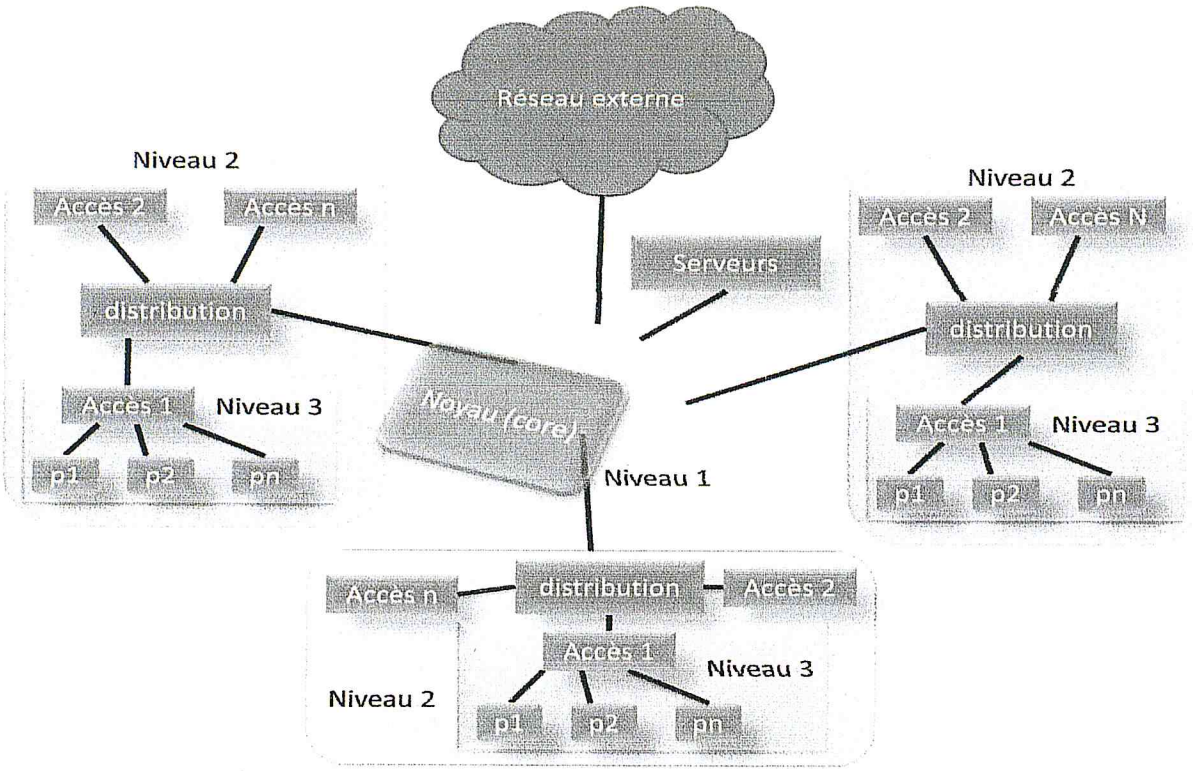

Figure 21:Maquette réseau

Les avantages :

- Ajout facile de postes.
- Localisation facile des pannes.
- Le débranchement d'une connexion ne paralyse pas le reste du réseau.
- Simplicité éventuelle des équipements au niveau des nœuds : c'est le concentrateur qui est intelligent.

Les inconvénients :

- Plus onéreux qu'un réseau à topologie en bus (achat du concentrateur et d'autant de câbles que de nœuds).
- Si le concentrateur est défectueux, tout le réseau est en panne.

3. Contexte de travail

Nous allons récapituler dans cette partie les éléments basique de notre système ainsi que toutes les exigences auxquelles il doit obéir. En résumé notre système a pour objectifs :

- D'assurer la collecte des informations des équipements constituent le réseau.
- Assurer la surveillance des ressource matérielles et logiciels.
- Capter les anomalies et trouver les causes de ces anomalies.
- Alerter l'administrateur.
- Donner la main a l'administrateur pour accéder à un équipement.

3.1 Architecture fonctionnelle

Dans l'objectif de concevoir notre application de supervision, nous avons opté a adopter l'architecture client serveur ou :

Le client représente un agent qui est installé sur chaque composant du réseau qui peut être une station de travail, un serveur, un routeur, un Switch…

L'application de supervision doit être connectée à un port qui appartient à tous les réseaux.

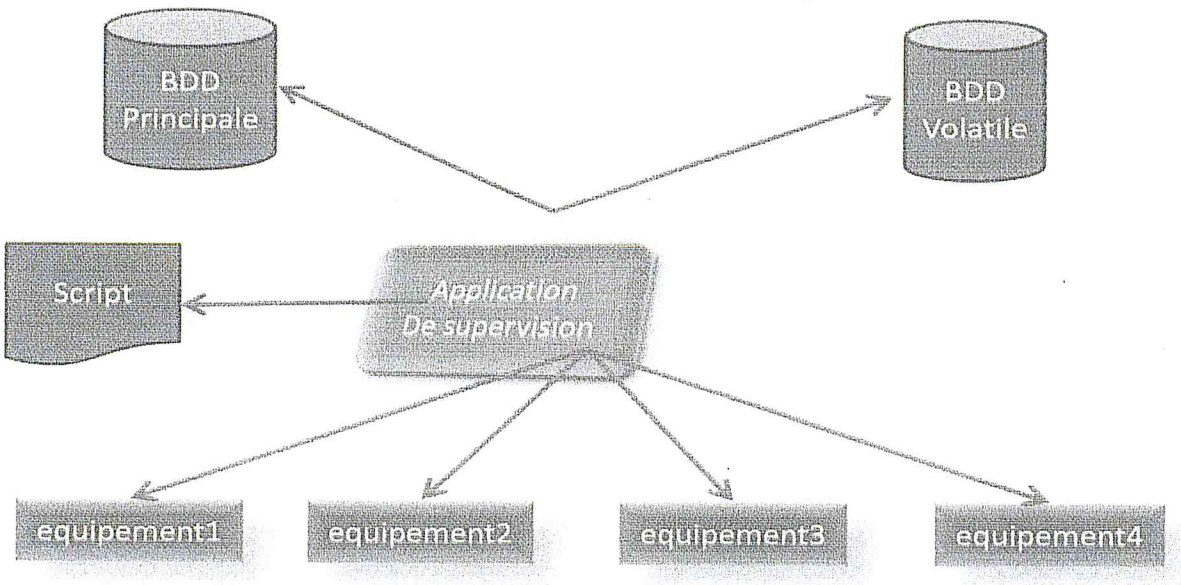

Figure 22:Architecture fonctionnelle

3.2 Architecture matérielle

Cette architecture Permet la représentation des déférents outils et taches majors de notre solution afin d'assurer l'activité de surveillance et de supervision.

La surveillance est une procédure de récupération des informations et comparaison afin d'observé tous changement ou défaillance survient le réseau.

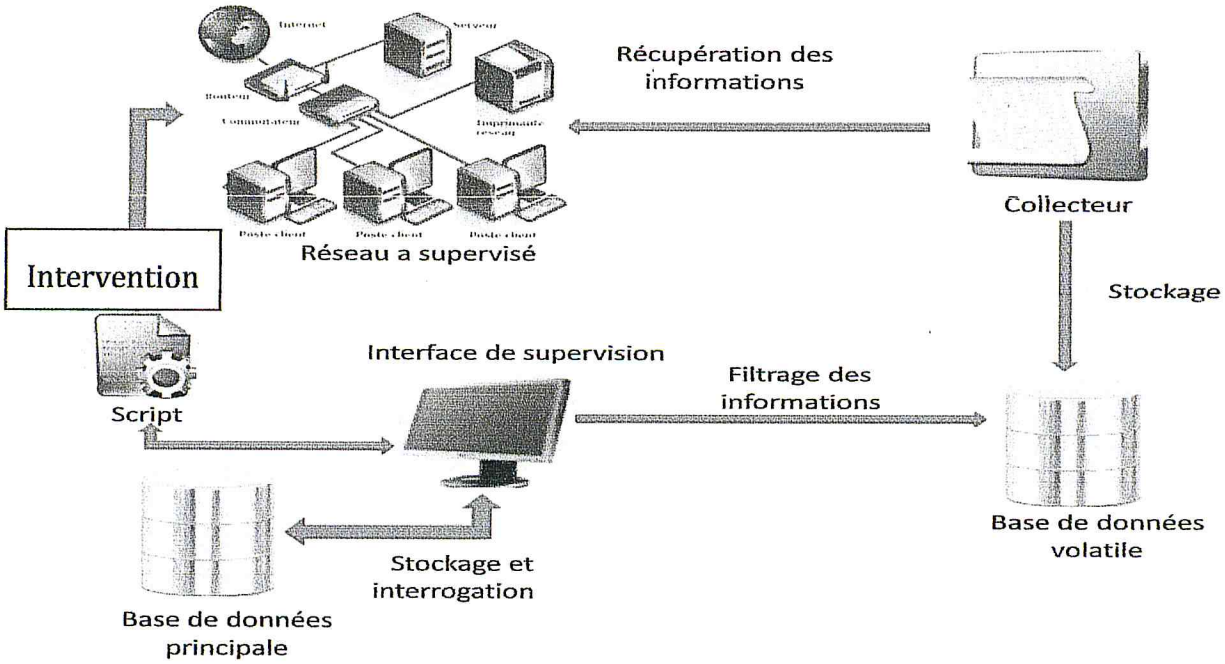

Figure 23: Architecture matérielle

L'architecture est composé de :

Réseau : le *réseau comporte les différents équipements tels que* (routeurs, commutateurs, serveurs, imprimantes, ordinateurs).

Collecteur : c'est un ensemble d'outils utilisé qui assurent l'extraction des informations comme le protocole SNMP, WMI, CPUID.

Base de données volatile (temporaire) : est une base de données secondaire pour stocker les informations récupérées par le collecteur

Interface de supervision : c'est l'interface graphique utilisé par l'administrateur afin d'assuré la procédure de la surveillance

Base de données principale : c'est la base de données essentielle dans notre système elle contient toutes les informations jugé nécessaire par l'administrateur, utilisé pour comparé les nouvelles données avec les précédents.

Afin de réaliser la tache de supervision il est nécessaire d'ajouté des éléments dans notre architecture, des scripts installées dans tous les équipements.

A l'aide des scripts l'administrateur aura la possibilité de faire plusieurs taches comme la configuration des serveurs, activer ou désactiver les protocoles, interagir a distance…

3.3 Définition des taches

Cette partie consiste à expliqué toutes les taches composant l'architecture.

3.3.1 Récupération des informations

C'est la première étape, le rôle de cette tache est de :

- Scanner le réseau et récupéré toutes les adresses IP.
- Collecter le plus grande nombre d'informations possibles (matérielles et logiciels).

3.3.2 Stockages

Apres la collection des informations il est nécessaire de l'organisées et pour cela on a utilisé une base de donnée volatile pour mieux représenté les informations.

3.3.3 Filtrage des informations

Pour simplifier la tache de surveillance l'administrateur peut choisir que les informations jugé nécessaire, pour avoir une vue générale sur l'état de réseau, il peut choisir un nombre des ressources à superviser.

3.3.4 Stockage et interrogation

Permet de sauvegarder dans la base de données principale toutes les informations sélectionnées par l'administrateur afin de comparé régulièrement les informations stockées avec la base de données volatiles et alerter l'administrateur en cas de panne.

3.3.5 Intervention

En cas ou il faut que l'administrateur interagir pour résoudre des problèmes, on a installé des scripts qui lui permettent d'accéder a distance et résoudre ces problèmes, il peut aussi faire des configurations au niveau des serveurs comme (DHCP, DNS…).

4. Démarche de travail

D'après l'objectif de notre travail qui consiste à réaliser un outil permettant a un administrateur d'assurer un ensemble d'information concernant les équipements (matériels, logiciel) existant dans le réseau et reste active à citer les déférent problèmes et anomalie ainsi donné la capacité de faire contrôler le réseau dans le but de régler les problèmes ou d'appliqué des configurations.

Information, anomalie et configuration sont les éléments de base de notre travail chaque élément réaliser a cause des techniques et des méthodes qu'ont peut dire que la conception dépendant a la présentation de ces techniques en séquence et de manière simple pour cela on va utiliser la modélisation libre grâce à plusieurs facteurs :

- Facilité de réalisation et de suivi.
- Explication simple et claire.

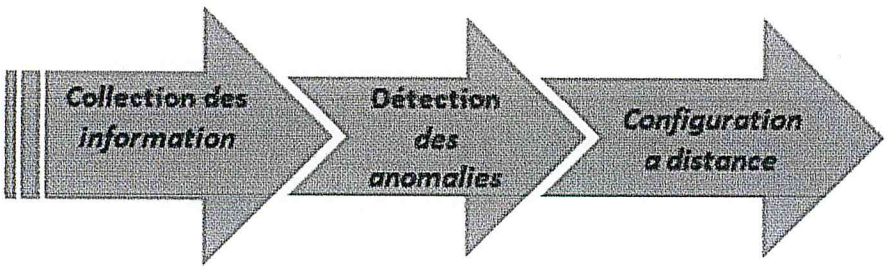

Figure 24:Les phases de la supervision

4.1 Phase Collection des informations

C'est la première partie du fonctionnement de supervision. En considère comme la phase principale car elle est responsable de la collecte les informations nécessaire a consulter et au même temps l'utilisation dans les phases qui suivent.

Cette phase est divisée en deux taches qui sont :

- Le Scan de réseau.
- La récupération des informations matériels et logiciels.

4.1.1 Le Scan de réseau

C'est une méthode très utilisé qui consiste a détecté la présence des équipements (ordinateur, router, Switch,.....)Dans un réseau informatique.

Leur principe est l'envoie des lignes de commande réseau permettant d'obtenir des informations et en particulier le temps de réponse de la machine à travers le réseau et aussi l'état de connexion avec cette machine (renvoi code d'erreur correspondant).

4.1.2 Procédure pour Scanner le réseau

- L'administrateur lance le scan du réseau.
- Le système lui répond par une fenêtre indiquant l'adresse de réseau.
- L'administrateur saisit l'adresse IP de réseau.
- Le système envoie des paquets PING à chaque adresse IP de la plage d'adresse.
- Il enregistre le résultat de scan dans la base de donné temporaire
- Le système résultat de scan avec précision l'état de connexion de chaque adresse IP.

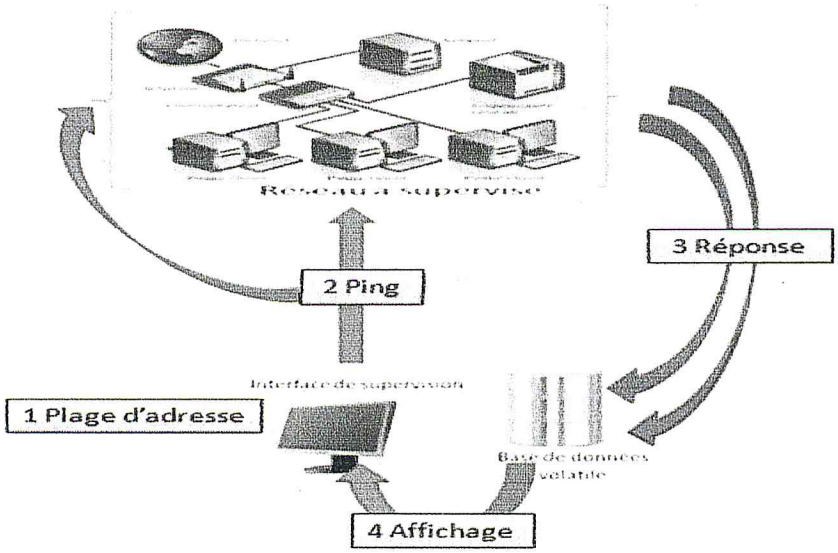

Figure 25:Scan d'un réseau

4.1.3 Collecte des informations

Cette tache consiste à collecter et récupère les informations nécessaires concerner les déférents machines du réseau et ça a l'aide des deux outils SNMP et WMI.

4.1.4 Collecte d'information (SNMP):

Le protocole SNMP se base sur le fait qu'il existe une station de gestion réseau, le manageur, dont le rôle est de contrôler le réseau et de communiquer via ce protocole avec un agent. L'agent est de manière générale une interface SNMP embarquée sur le matériel destiné à être administré à distance.

Manager, agent, communauté, Oid et Mib sont les éléments propriétaires pour la fonction de protocole SNMP dont la relation entre ces éléments se fait de la manière suivant :

- Le manager SNMP interrogé l'agent SNMP du machine à superviser par des commande (Get, Getnext,……) est ça nécessite trois paramètres important l'adresse IP du machine qui possède l'agent et aussi la communauté (on concéder comme un mot de passe pour accéder a l'agent) et un Oid.
- Le manager envoyé l'Oid qui est le mot clé de l'information à récupéré.
- L'agent recevez l'Oid est sélectionné l'information après la traduction d'Oid a l'aide de Mib.
- L'agent envoie l'information ou un message d'erreur au Manager.
- Le manager recevez les informations à fin de consulte par l'administrateur.

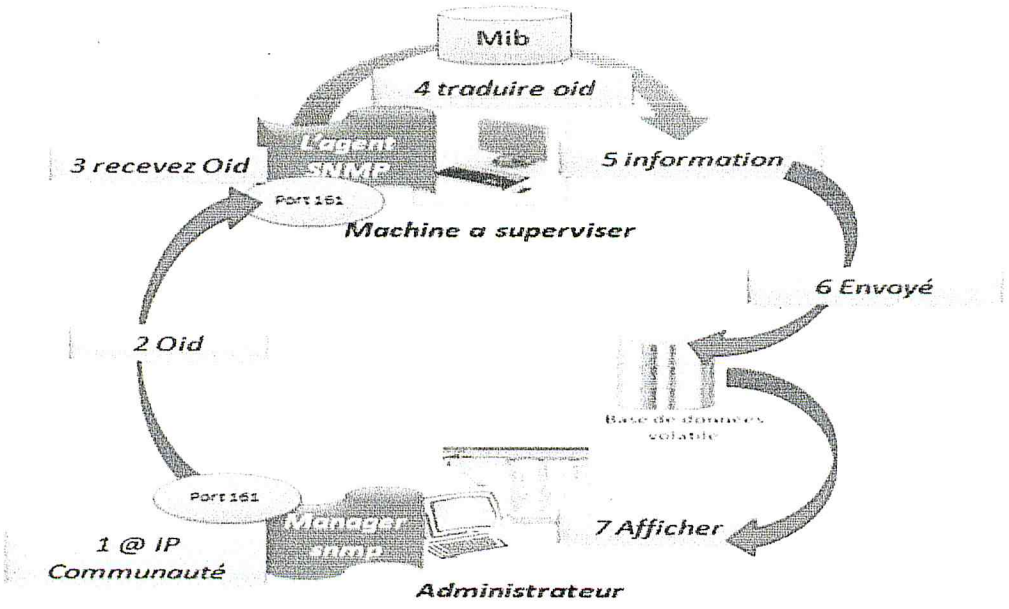

Figure 30: Information a l'aide de SNMP

Pour réaliser les étapes précédents SNMP doit exploite les capacités du protocole de transport UDP :

Le protocole UDP fonctionne en mode non connecté, c'est-à-dire qu'il n'existe pas de lien persistant entre la station d'administration et l'agent administré. Cela oblige les deux parties à s'assurer que leurs messages sont bien arrivés à destination, ce qui apporte également un important gage de fiabilité pour la gestion réseau.

- Deux ports sont désignés pour l'utilisation de SNMP :
  - ✓ Port 161 pour les requêtes à un agent SNMP.
  - ✓ Port 162 pour l'écoute des alarmes destinées à la station d'administration.

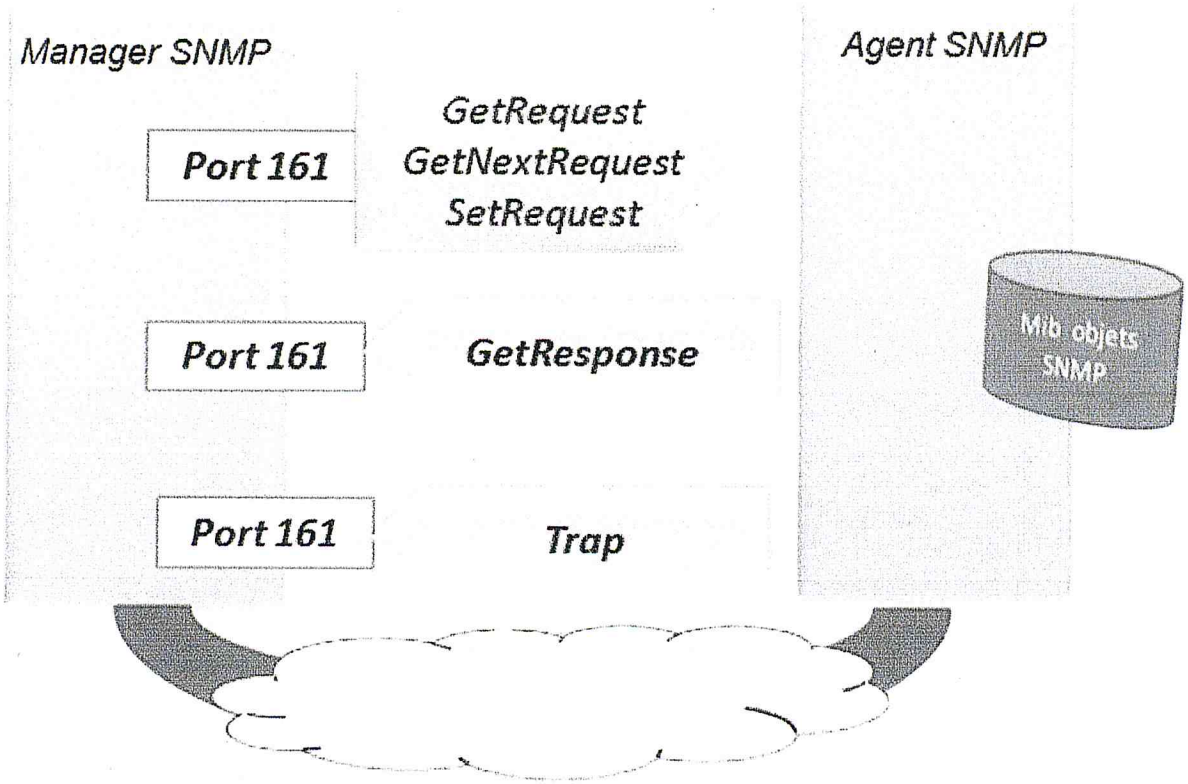

Figure 31 : SNMP et le protocole de transport UDP

4.1.5 Collecte d'information (WMI):

WMI permet de surveiller et contrôler les ressources systèmes de Windows. Grâce à lui, vous pouvez récupérer énormément d'informations de votre machine en local mais aussi des machines distantes.

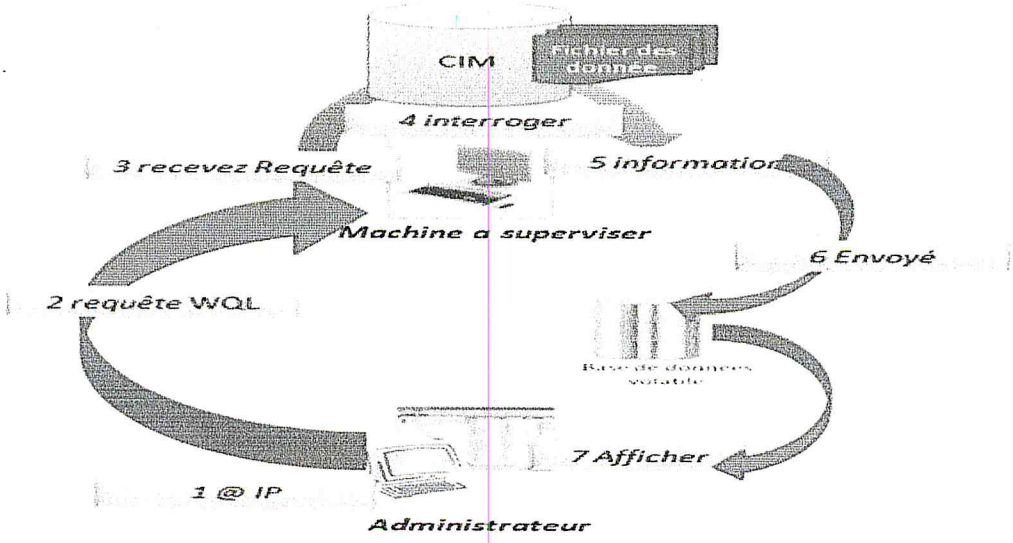

Figure 32: Information a l'aide de WMI

4.2 Phase de détection des anomalies

La détection des anomalies dans un réseau est classée parmi les choses importantes pour assurer le suivi d'un réseau, gère et éviter les problèmes qui peuvent diminue la performance.

A ce niveau en utilise SNMP car il dispose d'une méthode très pratique qui donne à l'administrateur la possibilité de recevoir les Trap SNMP envoyés par les agents SNMP installés au niveau des machines de réseau en cas de problème.

D'autre part on va utiliser la méthode qui informe l'administrateur des problèmes et des changements qu'il peut avoir dans le réseau et ça a l'aide de base de données temporaire.

4.2.1 Procédure de Détection des anomalies (trap SNMP)

- Le système reste en attente pour n'importe quelle trap peut être envoyé par les agents SNMP.
- L'administrateur lance la commande de détection des anomalies.
- En cas de trap le système affiche à L'administrateur dans le but de prendre la décision nécessaire.
- Le système garde des traces pour tous les trap.

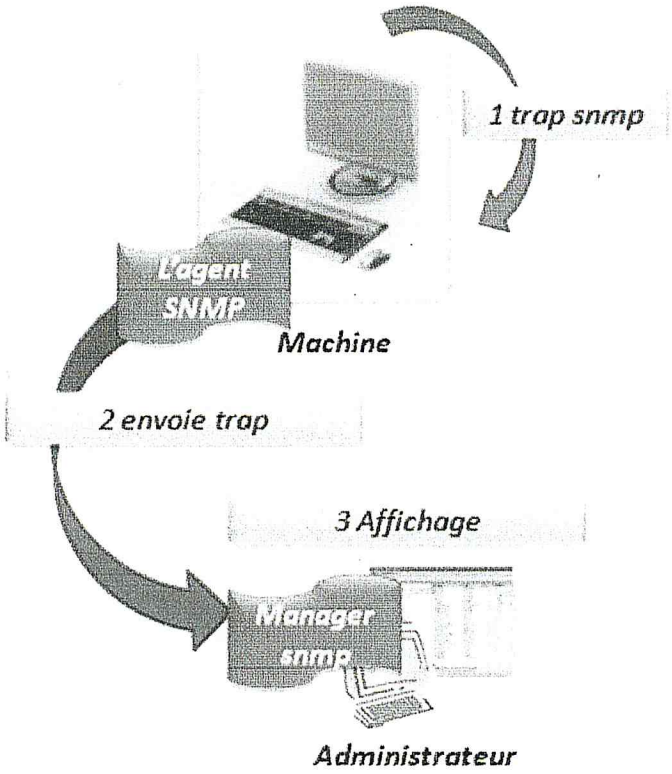

Figure 26:Réception des Trap SNMP

4.2.2 Procédure de Détection des anomalies (comparaison)

- L'administrateur lance la détection des problèmes.
- Le système effectue une comparaison entre la base temporaire et la base de données principale.
- En cas d'anomalies Le système alerte l'administrateur avec des informations précises de problème.
- Le système envoie un mail a l'administrateur indique le problème.
- Le système garde l'historique pour chaque problème.

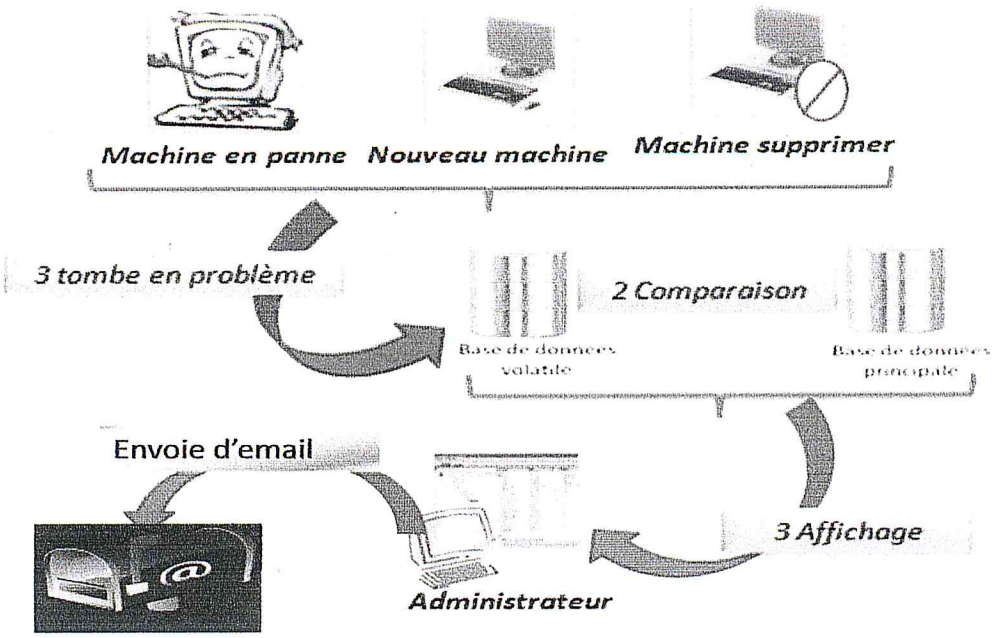

Figure 27:Détection des anomalies

4.3 Phase de Contrôle de réseau

Une surveillance de réseau est insuffisante pour une bonne administration de réseau c'est pour ça qu'une méthode de contrôle des machines doivent être nécessaire.

4.3.1 Technique utilisé

Parmi les meilleures technique de Piloter une machine à distance nous trouvons que la méthode qui consiste à placer un script dans une machine ce script permet de recevoir des lignes de commande envoyé par l'administrateur ensuite exécuter ces commande dans le cadre de la maintenance et aussi pour dépanner un utilisateur à distance ensuite envoyé le résultat a l'administrateur.

4.3.2 Procédure de configuration à distance

- Un script est lancé dans une machine.
- L'administration lance la configuration à distance.
- Le système affiche une liste des machines.
- L'administrateur sélection l'une des machine afficher et saisir un mot de passe afin d'établir une relation au machine.

- Le système ouvre à l'administrateur la possibilité de saisir et d'envoie des lignes de commande.
- Après chaque ligne de commande exécutée à la destination le système affiche le résultat envoyé par l'agent.

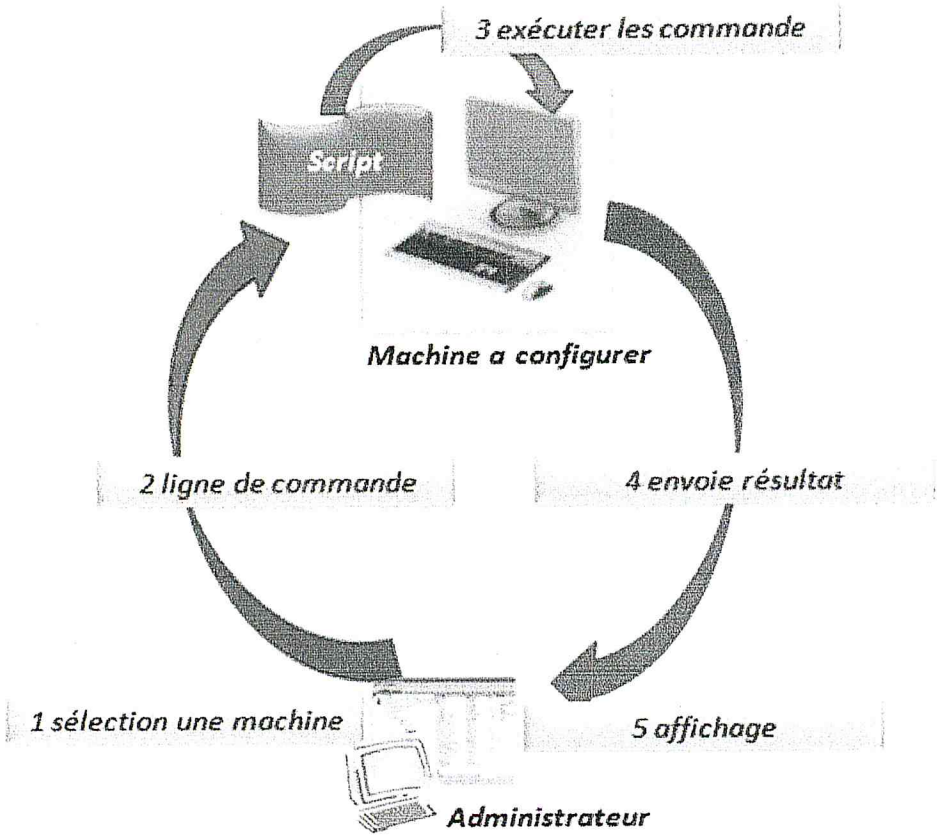

Figure 28:Contrôle a distance

5. Persistance

Pour pouvoir maintenir et représenter les différentes informations obtenues par notre outil de supervision, nous avons utilisé deux bases de données.

manières , une lorsque l'administrateur a besoin de faire la supervision (détection des anomalies) dans ce cas l'opération de remplissage sera lancée par l'administrateur, l'autre manière de remplissage est lorsque le système le fait automatiquement dans des périodes régulières définies par l'administrateur et a partir des informations collectées et sauvegardées sur la base de données volatile des alertes peuvent être affichés par le système si un changement d'états est détecté.

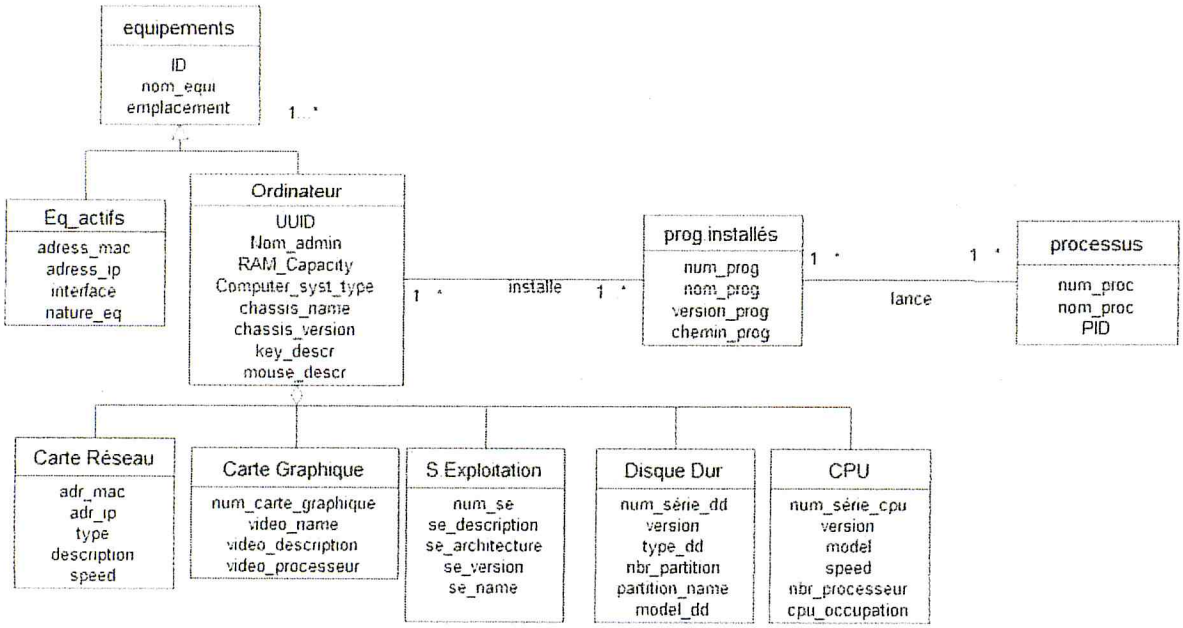

Figure 34 : Diagramme de classe de la BDD temporaire

L'utilisation de la base de données temporaire permet de :

- Récupérer et sauvegarder les informations matérielles et logiciels sur les composant du réseau a n'importe quel moment
- Détecter les équipements de réseau
- Détecter la présence de nouveaux équipements étrangers au réseau
- Détecter les différents changements d'états qui arrivent aux équipements (équipement déconnecté, absence d'un composant sur un ordinateur, nouveaux composant sur les machines du réseau..).

Chapitre3 : Réalisation

1 Environnement de travail

Nous décrivons dans ce chapitre l'environnement de travail requis qui est le développement d'une application réseau utilisant le protocole SNMP.

Pour qu'une application réseau puisse être mise en œuvre, il est nécessaire que les composants réseaux qui interagissent avec l'application soient bien installes et bien configures.

En particulier le protocole SNMP qui doit être installe sur tous les postes clients. Les composants de l'environnement du travail sont :

- système d'exploitation : Windows.

- Protocoles : SNMP et UDP.

- Langage de programmation : JAVA.

1.1 Choix du protocole SNMP

Le protocole SNMP (Simple Network Mangement Protocol) est un protocole, comme son nom l'indique, qui permet d'assurer la gestion du réseau. Il permet également de contrôler un réseau à distance en interrogeant les stations qui en font partie sur leur état et configurer leur configuration, de faire des tests de sécurité et observer les différentes informations liées a l'émissions de données. Il peut même être utilise pour gérer les logiciels et bases de données liées a distance.

Le protocole SNMP est le protocole le plus adéquat à notre application, et le plus simple utiliser.

1.2 Choix de langage de programmation java

Java est un langage de programmation informatique orienté objet créé par James Gosling et Patrick Naughton de Sun Microsystems. Mais c'est également un environnement d'exécution.

Java peut être séparée en deux parties. D'une part, votre programme écrit en langage Java et d'autre part, une machine virtuelle (JVM) qui va se charger de l'exécution de votre programme Java.

C'est cette plateforme qui garantit la portabilité de Java. Il suffit qu'un système ait une machine virtuelle Java pour que tout programme écrit en Java puisse fonctionner.

Avec le langage Java, vous pouvez développer, des applications Desktop, développer des applets pour vos sites web, développer des sites en JSP, des applications pour téléphone mobile. La première chose à faire est bien évidemment d'apprendre à faire des applications standalones simples.

1.3 Installation et configuration de l'agent SNMP

L'agent SNMP est nécessaire si vous souhaitez surveiller un système d'exploitation de Windows à partir du logiciel de supervision **LoriotPro** ou de tout autre logiciel ayant une fonction de Manager SNMP.

L'agent SNMP de Windows est nécessaire pour répondre aux requêtes SNMP et pour envoyer des Traps SNMP ou notifications du et vers le manager SNMP.
Les Traps sont envoyés par l'agent SNMP et selon les objets de MIB pris en charge.

1.4 Installation de l'agent

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

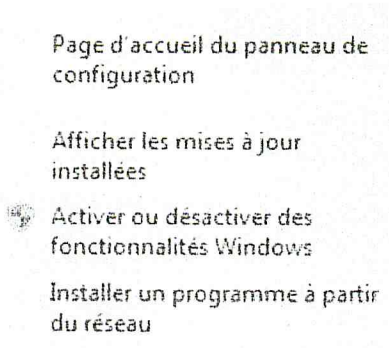

Figure 35: Activer ou désactiver des fonctionnalités Windows

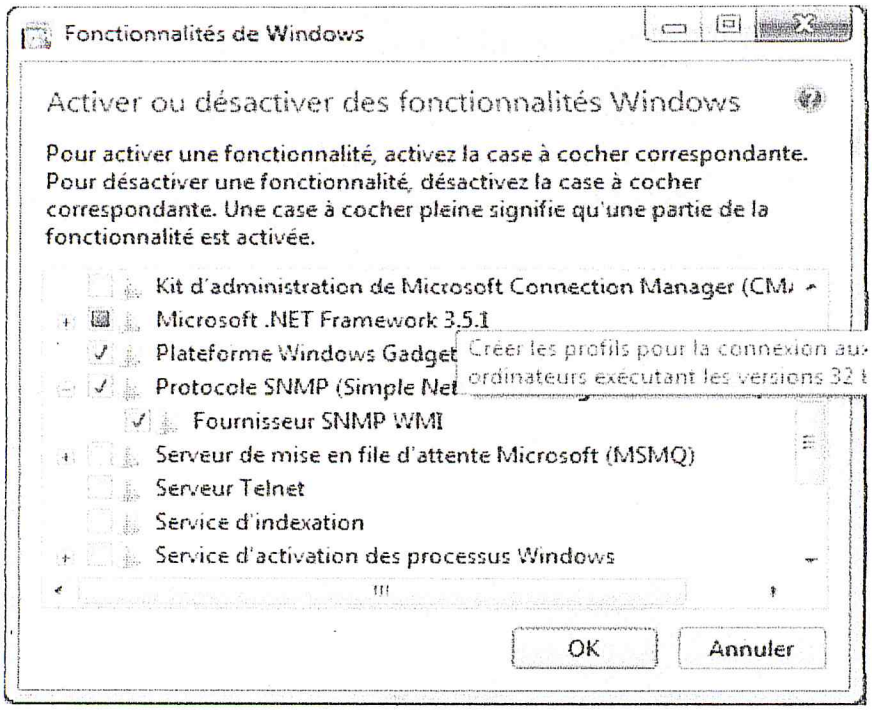

Figure 36 : Fonctionnalités de Windows

Cochez le protocole SNMP Simple Network Management Protocol. Ceci est nécessaire pour installer l'agent SNMP et d'autres services SNMP.

Configuration de l'agent

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

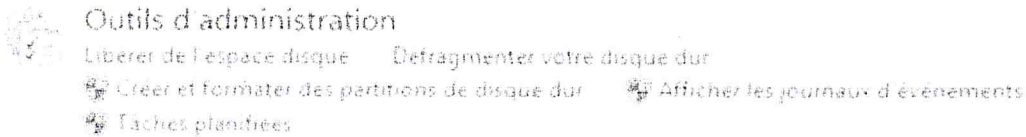

Figure 37 : Outils d'administration

Finalement sélectionner l'icône des Services

Figure 38 : Icône Services

Puis la liste des services rechercher le service SNMP et double cliquez.

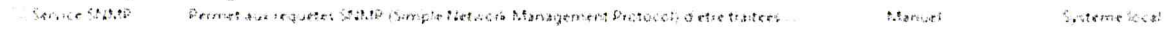

Figure 39 : Service SNMP

La fenêtre de propriétés de service SNMP est affichée

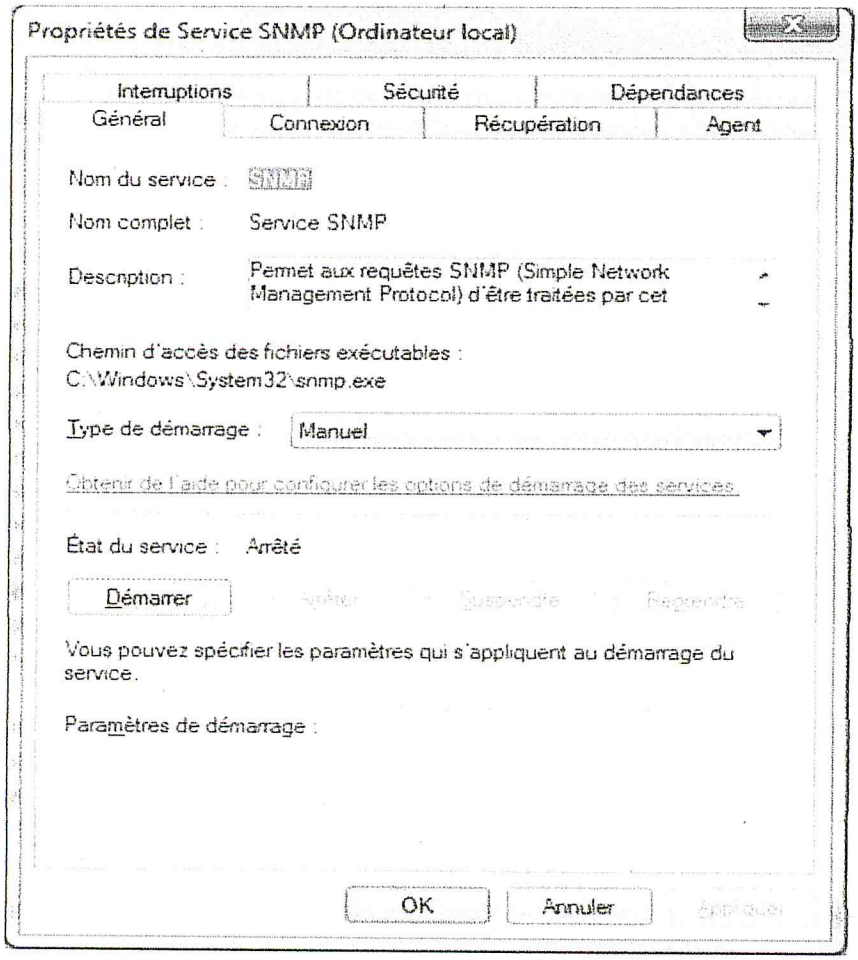

Figure 40 : Propriétés de services SNMP

Vous pouvez aussi modifier le type de démarrage dans l'onglet Récupération.

Le processus SNMP s'exécute sous le compte système local ou un compte peut être spécifié, onglet Connexion.

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

2 Présentation des interfaces

Pour la création des interfaces nous avons eu recours aux bibliothèques de java qui sont java.awt et java.swing.

*java.awt et javax.swing : sont deux paquetages consacrés a la création et a la gestion de l'interface graphique utilisateur (GUI : Graphique User Interface=IHM : Interface Homme Machine). De nombreuses classes que définit l'AWT (Abstract Window Toolkit) ont cédé place a celles développées dans le paquetage javax.swing de java2. La plupart des classes du paquetage javax.swing définissent des éléments GUI, les classes Swing font partie d'un ensemble plus général des fonctionnalités de programmation GUI qu'on appelle la Java fondation Classes ou tout simplement JFC.

2.1 Authentification

Lorsque l'administrateur lance l'application, une demande d'authentification apparait, l'administrateur doit introduire son nom et le mot de passe puis il valide.

Figure 41 : Authentification

2.2 Interface principale

L'interface principale de notre application constituée d'une barre d'outils, zone d'affichage et le menu principale

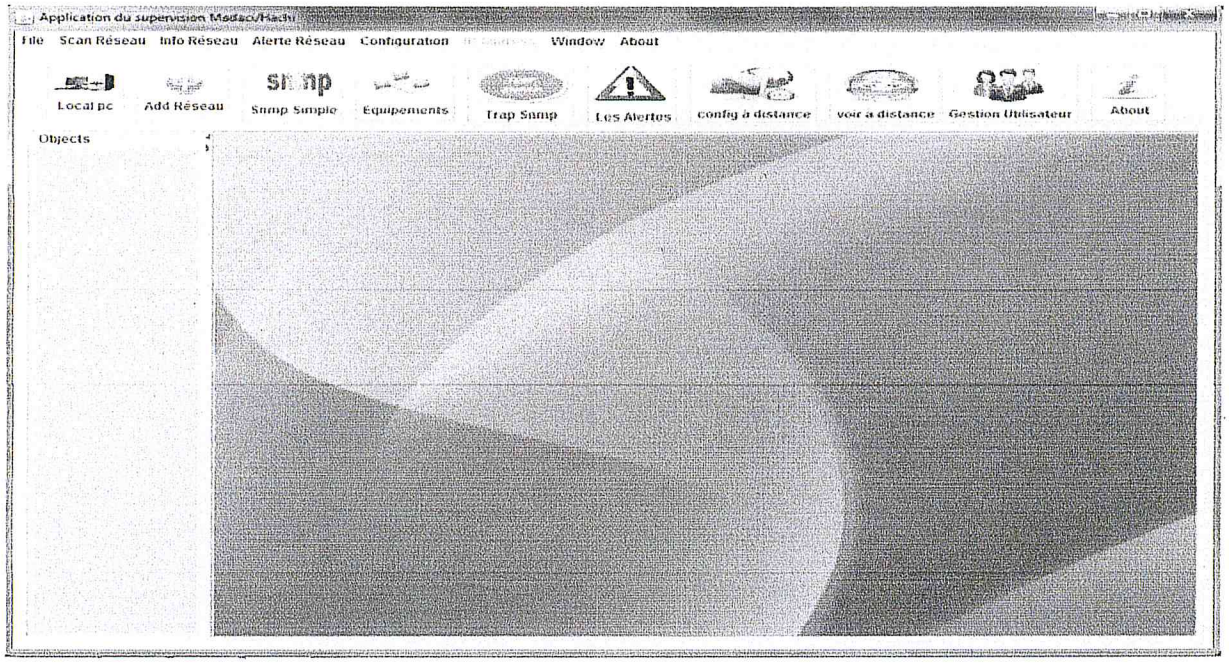

Figure 42 : Fenêtre principale

2.3 Adresse du réseau à scanner

La figure suivante permet à l'administrateur de spécifier l'adresse du réseau.

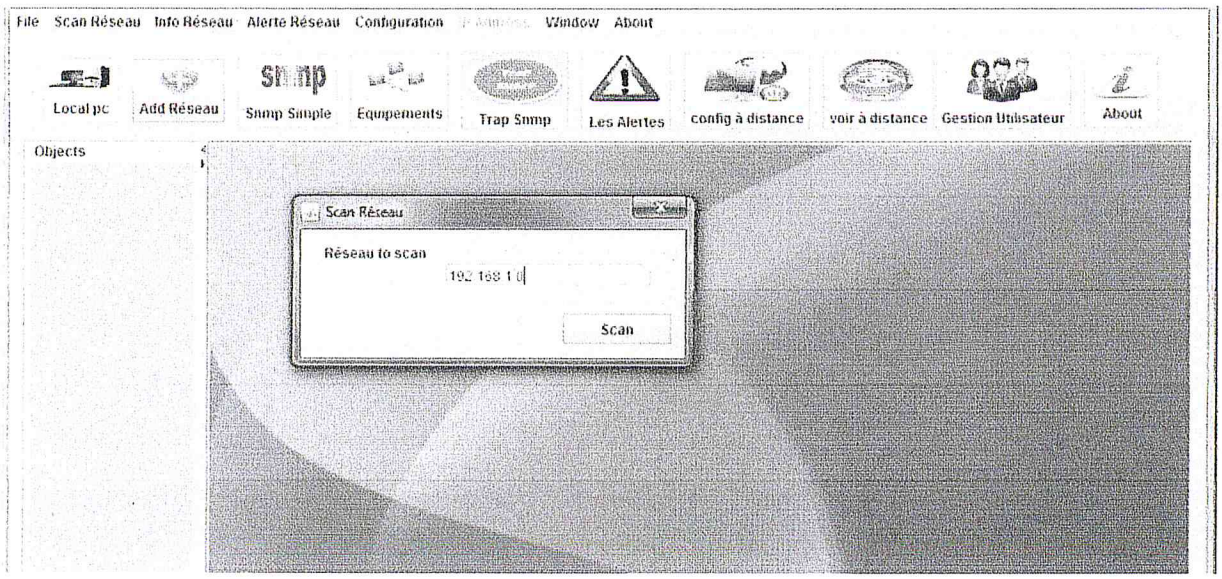

Figure 43 : Adresse du Réseau

2.4 Scan du réseau

Cette figure montre l'opération du scan

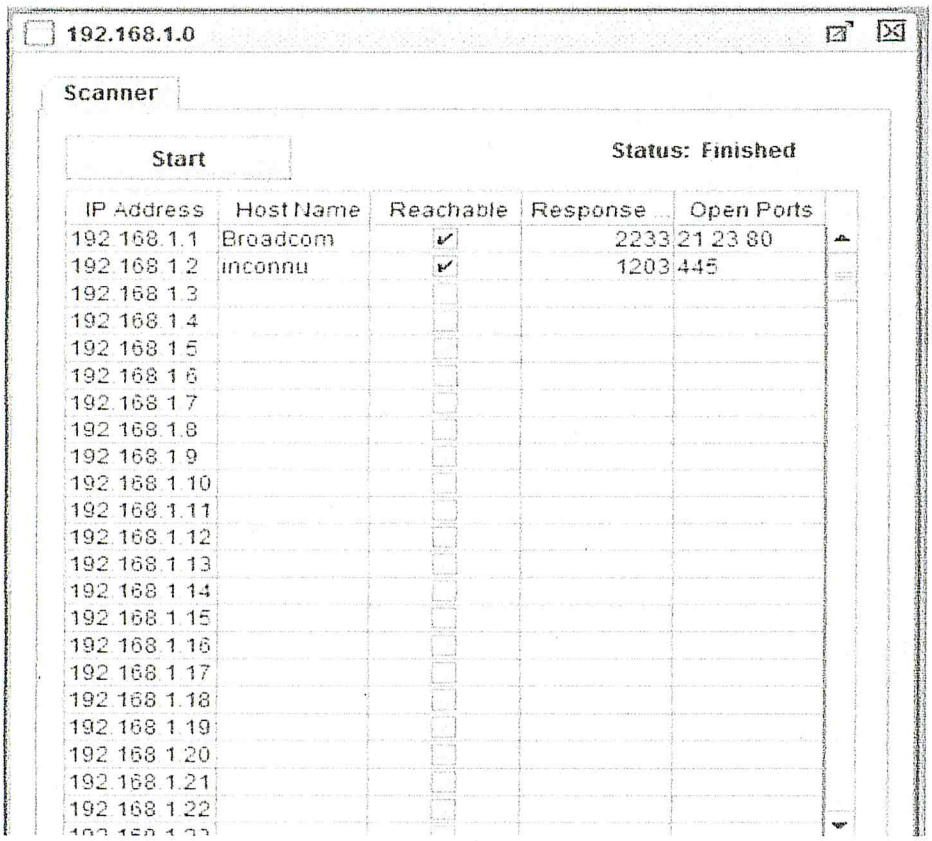

Figure 44 : Scan

2.5 Liste d'équipements

Apres le scan du réseau l'administrateur peut consulter la liste des machiné trouvée, cette fenêtre contient un ensemble de buttons afin de consulter les caractéristique de chaque machine, avant de consulter les caractéristique l'administrateur doit charger les informations de chaque machine comme la figure montre.

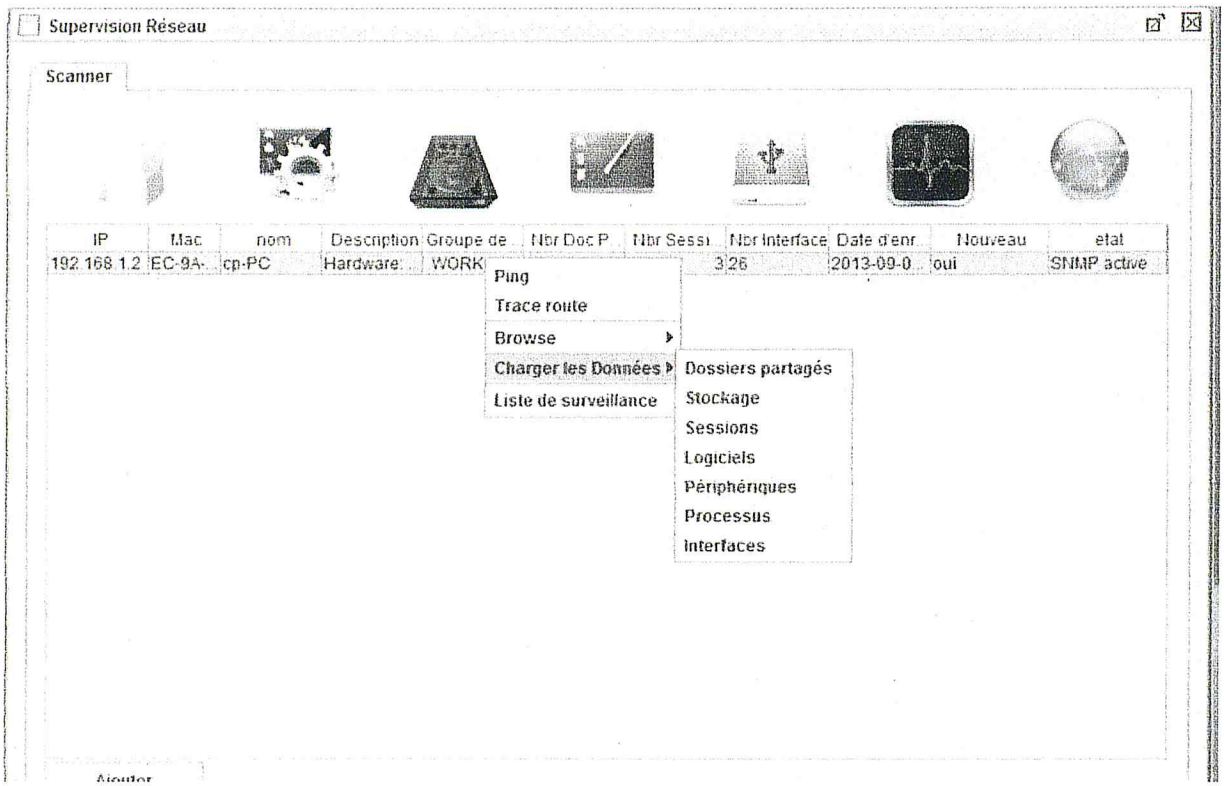

Figure 45 : Liste d'équipements

2.6 Trap SNMP

Cette fenêtre permet de capturé les traps envoyés par les machines.

Figure 46 : TRAP SNMP

2.7 Configuration a distance

Offrir à l'administrateur un accès à distance a toutes les machines de son réseau afin de faire des configurations.

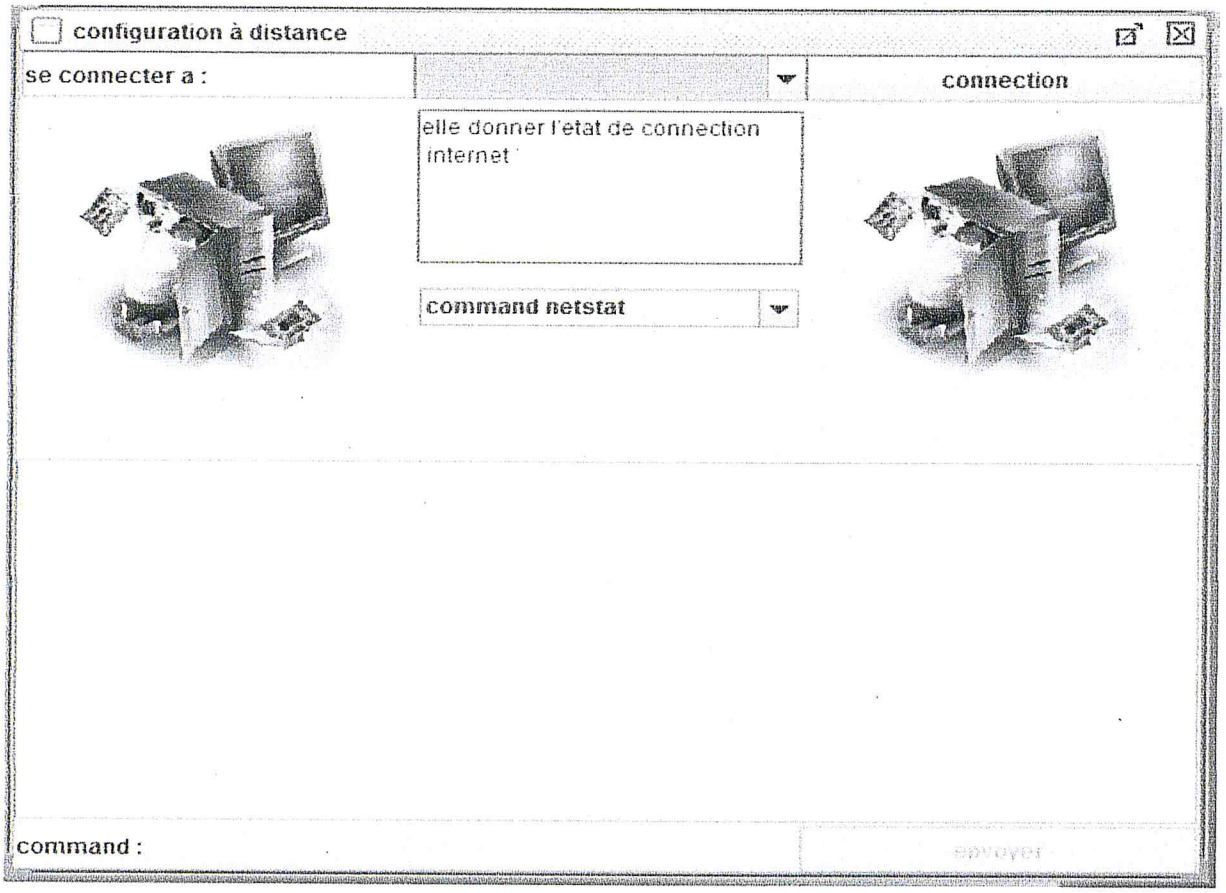

Figure 47 : Configuration

Conclusion Générale

Conclusion et perspectives

Le travail effectué dans ce projet fait partie du domaine de la sécurité des réseaux informatique. Il est un complément a d'autres outils de sécurité et de surveillance des réseaux. Actuellement, plusieurs moyens de sécurité sont combinés pour répondre aux nouvelles exigences. Ce projet nous a permis d'approfondir, essentiellement, nos connaissances sur la sécurité informatique, l'architecture et le fonctionnement des réseaux.

La surveillance des réseaux informatiques est devenue une nécessité au sein des entreprises surtout avec l'augmentation de la taille des réseaux d'aujourd'hui et la diversité des équipements utilisés. Le protocole SNMP s'est imposé comme un standard dans le domaine de la gestion des réseaux. Il est introduit dans les équipements réseaux par la plupart des constructeurs.

Dans cette optique nous avons présenté, dans ce mémoire, la conception et la réalisation d'un outil de surveillance à base du protocole SNMP. Cet outil, de base pour l'administrateur des réseaux locaux Ethernet a base de TCP/IP, lui permet (a l'administrateur)

De surveiller les connexions des machines a son réseau toute en ayant une description détaillée de leurs configurations matérielles et logiciels. Il peut être utilisé :

- Pour faire l'inventaire du parc informatique.
- Pour faire des configurations.

Le terme parfait n'existe pas dans tous les domaines d'informatique,

Selon cette phrase on est obligées de donner des perspectives afin d'améliore la supervision dans notre projet parmi les perspectives on a :

- Créer une gestion des règles de sécurité pour but de rendre les alertes en mode dynamique.
- Changer la manière de fonctionnement des procédures d'application à fin d'exécuter périodiquement avec un délai spécifié.

Sommaire

BIBLIOGRAPHIE

[2] : Yannick MUKOLE MPALUNGUNU, « Etude sur le déploiement d'un réseau informatique administre par Windows 2008 Serveur avec une optimisation du QOS dans une entreprise publique » (2010)

[13]: Billy KAMANGO OSEMBE, « Réalisation d'un utilitaire d'analyse de trafic d'une interface réseau » (2010)

[14]: Willy OLENGA SEKE DJAMBA, « Implémentation d'une application de gestion de réseau base sur le protocole SNMP » (2007)

[15] : François PIGNET, « Réseaux informatique supervision et administration »,eni, (2007)

[16] : HACHOU, Younes KHETTOU, « Conception et implémentation d'une plate forme de supervision réseau et système basée sur une politique sécurité. », Mémoire de fin d'étude Master2, (2009).

[21] : Mr BENREZZAK Ali, « élaboration d'un cahier des charges pour la réalisation d'un logiciel de supervision du réseau informatique de l'HCA/1°RM ».Mémoire de fin d'étude Ingénieur (2012).

[22] : Mr ALLAL Messouad , « mise en place d'une plateforme de supervision des réseaux informatiques des Forces Navales. » Mémoire de fin d'étude Ingénieur (2012).

[24] : khadija BELMESSOUS ,Badr Eddine BOUZEBRA , « Conception et réalisation d'un système de supervision réseau à base d'agents » Mémoire de fin d'étude Ingénieur.(2012)

WEBOGRAPHIE

[1]: Les topologies des réseaux http://www.samomoi.com/reseauxinformatiques/les_topologies_des_reseaux.php consulté le 18/03/2013

[3]: Les réseaux informatique, www.infos-du-net.com. consulté 21/03/2013.

[4]:Anthony, Types de réseaux (2007) ,http://www.vulgarisation-informatique.com/. Consulté le 21/03/2013

[5]: Zbakh Abdel ALI, Notion de réseau informatique http://lycee.voila.net/mod4_chap1.pdf Consulté le 21/03/2013

[6]: Le magasin informatique ,http://www.ybet.be consulté le 20/03/2013

[7]: André Aoun, Jacques Chabert, Michel Jacob (2001), Architecture client/serveur, http://www.httr.upstlse.fr/pedagogie/cours/internet/services/servclie.htm, consulté le 23/03/2013

[8]: Formation réseaux : Notions de base, http://www.via.ecp.fr/ consulté le 25/04/2013

[9]: Client / Serveur, http://personnel.univreunion.fr/courdier/cours/archics/1_Pourquoi_le_CS/1_Pourquoi_le_CS.pdf consulté 01/04/2013

[10]: Présentation de l'architecture d'un système client/serveur,

http://www.commentcamarche.net/contents/222-environnement-client-serveur , consulté le 01/07/2013

[11]: Université nice,les réseaux informatiques 2012 http://bioinfo.unice.fr/enseignements/GBM/cours/reseau.pdf consulté le 05\04\2013

[12] : Eric BAHATI – SHABANI, Mise en place d'un réseau VPN au sein d'une entreprise. Cas de la BRALIMA Sarl en RDC 2011,

http://www.memoireonline.com/01/13/6733/m_Mise-en-place-dun-reseau-VPN-au-sein-dune-entreprise-Cas-de-la-BRALIMA-Sarl-en-RDC0.html consulté le 25/04/2013

[18]:A new network vision, http://www.netforge.fr consulté le 24/04/2013.

[19]: journal de net, les fichiers log, des indicateurs utiles(2009), http://www.journaldunet.com/developpeur/algo-methodes/tutoriel-pratique/les fichiers-log-des-indicateurs-utiles.shtml, consulté le 23/04/2013.

[20] : étude des outils de surveillance (monitoring) réseau (2009) http://www.o00o.org/monitoring/index.html, consulté le 22/04/2013.

[23]: http://fr.wikibooks.org/wiki/Utilisateur:Rortalo/Sécurité_informatique /Observation,_surveillance,_supervision. consulté le 22/04/2013.