REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE
LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU
FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire

de fin d'études

En vue de l'obtention d'un Master 2 en informatique

Option : Système informatique.

Thème :

Conception et réalisation d'une application de gestion de réseaux multiplateformes

Proposé et dirigé par :
Mr M.RAMDANE

Réalisé par :
Mr Djadel Mourad

Jury composé de :

Président : .....
Examinateurs : .....
.....
.....

Promotion : 2011/2012

À ma famille et à mes amis.

REMERCIEMENTS

Je tiens à remercier vivement mon promoteur Mr M.RAMDANE pour m'avoir proposé ce sujet, pour la qualité de son encadrement, et son suivi durant toute la durée du projet.

Je remercie chaleureusement les membres du jury pour l'honneur qu'ils me font en acceptant de juger ce mémoire de fin d'études.

Je tiens remercier toute l'équipe air moins, et mes camarade de jeu à Counter, ainsi que tous mes amis de la promotion Master 2011-2012.

Enfin, je remercie toutes les personnes ayant contribué de prés ou de loin au bon accomplissement de ce travail.

Sommaire

Sommaire

Chapitre 3 : Administration réseau.

Chapitre 4 : Conception.

Chapitre 5 : Réalisation et implémentation.

Introduction générale

Les réseaux informatiques ont aujourd'hui autant d'importance que les ordinateurs eux mêmes, au point que la plupart de nos activités ne pourraient plus être envisagées sans la mise en place de ces réseaux. On assiste à leur déploiement à tous les niveaux de la société, dans les entreprises, au niveau national et international, y compris dans les domiciles. Quant aux entreprises, ces réseaux leur apportent un moyen efficace pour mettre en œuvre un travail coopératif, pour faire communiquer des ordinateurs distants, pour partager des données, mais aussi pour imprimer à distance, envoyer des messages, et accéder à des bases de données délocalisées.

Le réseau n'est pas une entité statique. Il subit des évolutions. Son évolution a mis en jeu bien des aspects technologiques. On peut même parler de mutation au vu des progrès fulgurants qu'il a enregistrés depuis ces débuts.

L'évolution de réseau pose un problème majeur : la manière dont ceux-ci sont pratiquement gérée. En effet, avec la multiplication des machines qui ne cessent d'évoluer de jours en jours, des nouvelles architectures logicielles et matérielles toujours plus complexe, il devient évidement difficile de gérer un réseau.

A cette difficulté s'ajoute aussi le problème d'hétérogénéité des technologies et celle d'offrir une vu unifiée du réseau à l'administrateur et, d'autre part, la distribution et la grande quantité d'informations à collecter et à traiter.

Le matériel d'infrastructure réseau est donc de plus en plus sophistiqué et permet d'être contrôlé en distance : c'est là un des points fondamentaux de la gestion réseau, il est aujourd'hui nécessaire, étant donné l'étendue et la complexité des réseaux, de pouvoir le gérer à distance depuis son poste de travail et n'avoir qu'à se déplacer qu'en derniers recours, lors qu'une opération physique est nécessaire.

Comme son nom l'indique le protocole SNMP, simple network management protocole (protocole de gestion de réseau simplifié) que nous allons étudier plus en détails au cour de ce travail à pour rôle la gestion de réseau. Il à été développé pour apporter des moyens simple d'administration à distance aux administrateurs.

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

Ce travail comporte 5 chapitres brièvement décrits comme suivent :

- Le chapitre I s'intitule « Généralités sur les réseaux informatique », présente quelques notions de base concernant les réseaux, l'architecture OSI, et le monde de l'internet de façon générale.
- Le chapitre 2 s'intitule « Les Réseaux multiplateformes », consacré aux principales notions d'hétérogénéité d'un réseau informatique, il comprendra aussi une description des plateformes existantes, avec leurs services réseau.
- Le chapitre 3 s'intitule « Administration Réseau » est une introduction aux concepts de base de la gestion de réseau et notation une large étude du protocole SNMP. Il explique le fonctionnement, les différentes composantes d'une architecture de gestion basée sur SNMP et montre les échanges entre la station de gestion et les agents SNMP à des fins de surveillance.
- Le chapitre 4 s'intitule « Conception », la méthode d'analyse et la de conception de notre application y est largement expliquer.

- Le chapitre 5 s'intitule « Réalisation », comporte quant a lui la présentation de l'environnement dans lequel notre application a été réalisée, les outils utilisés et quelques interfaces de celle-ci.

Chapitre I

Généralités sur les Réseaux

Introduction :

Vu l'évolution rapide de l'information et l'intérêt croissant, de vouloir gagner en temps, de conserver les données, de limiter le nombre d'employés, et pas mal d'autres raisons ont poussé les entreprises à chercher des solutions informatiques capables de répondre à leurs besoins.

Aujourd'hui les réseaux informatiques sont devenus très vaste, ils sont employés dans toutes les entreprises. Les réseaux couvrent complètement la planète grâce à divers équipements et l'apparition de l'Internet et le Web offrent des services énormes.

Ce premier chapitre aura pour objectif de présenter quelques notions sur les réseaux informatiques en premier lieu puis donnera un aperçu sur l'Internet et le Web.

1. Les Réseaux informatiques :

1.1. Définition d'un réseau :

Un réseau informatique est un ensemble interconnecté d'ordinateurs autonomes permettant d'échanger des informations, la communication peut avoir lieu dans les deux sens : émission et réception. La communication est réalisée grâce à des protocoles de communication. Un réseau comporte généralement des serveurs qui fournissent des services aux autres machines (clients).

Une connexion réseau ne nécessite pas forcément un câble en cuivre (une ligne physique), mais elle peut être réalisée par laser (infrarouge), par ondes courtes ou par satellite.

1.2. L’intérêt d’un réseau :

Un réseau informatique peut servir plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels, connexion à internet, etc.)
- La communication entre personnes (courrier électronique, discussion en direct)
- La communication entre processus (entre des ordinateurs industriels par exemple)
- La garantie de l'unicité et de l'universalité de l'accès à l'information (bases de données en réseau, cohérence des données)

Les réseaux permettent aussi de standardiser les applications, on parle généralement de « Groupware », des outils permettant à plusieurs personnes de travailler en réseau.

Par exemple la messagerie électronique et les agendas de groupe permettent de communiquer plus efficacement et plus rapidement.

Voici un aperçu des avantages qu'offrent de tels systèmes :

- Diminution des coûts grâce aux partages des données et des périphériques,
- Standardisation des applications,
- Accès aux données en temps utile,
- Communication et organisation plus efficace.

1.3. Type de Réseaux :

On différencie les types de réseaux (privé) selon, leur taille (nombre de machines), leur vitesse de transfert des données, ainsi que leur étendue. Les réseaux privés sont des réseaux appartenant à une même organisation. On distingue généralement quatre catégories de réseaux :

1.3.1. Réseau PAN « Personal Area Network » :

Désigne un réseau restreint d’équipements informatiques habituellement utilisés dans le cadre d’une utilisation personnelle. Les bus utilisés les plus courants son l’USB, les technologies sans fil telles que Bluetooth ou IR (infra rouge).

1.3.2. Réseau LAN « Local Area Network » :

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. Par exemple une salle informatique, une habitation particulière, un bâtiment ou un site d’entreprise. Souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbps (pour un réseau Ethernet) et 1Gbps (en FDDI ou Gigabit Ethernet). La taille d'un réseau local peut atteindre jusqu'à 100 utilisateurs voir plus.
Dans le cas d’un réseau d’entreprise, on utilise souvent le terme RLE pour réseau local d’entreprise.

1.3.3. Réseau MAN « Metropolitan Area Network » :

Les MAN 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 formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

Par exemple, une université peut avoir un MAN qui lie ensemble plusieurs réseaux locaux situé dans un espace d'1 dm.

1.3.4. Réseau WAN « Wide Area Network » :

Un WAN (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.

1.4. La Topologie des réseaux :

Un réseau informatique est constitué d'ordinateurs reliés entre eux grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données).

1.4.1. Topologie Physique :

L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé topologie physique. On distingue généralement les topologies suivantes :

- **Topologie en bus :**

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot « bus » désigne la ligne physique qui relie les machines du réseau.

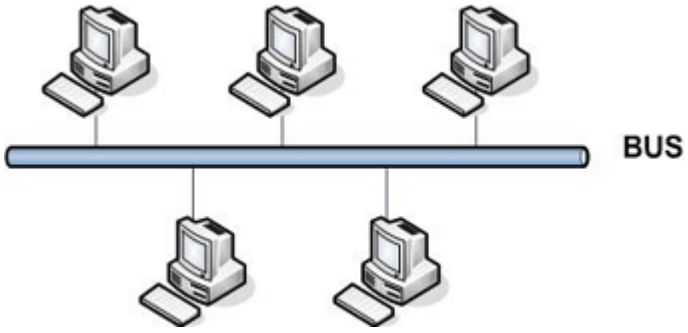


Fig1.1. Topologie en bus.

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.

- **Topologie en étoile :**

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais hub, littéralement moyen de roue). Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles il est possible de raccorder les câbles réseau en provenance des ordinateurs, et il a pour rôle d'assurer la communication entre les différentes jonctions.

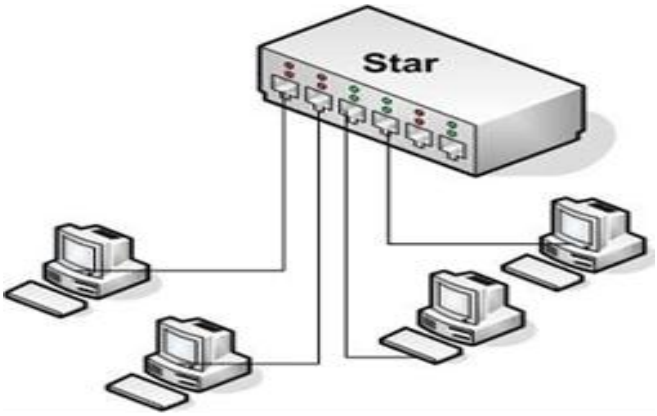


Fig.1.2. Topologie en étoile.

Contrairement aux réseaux construits sur une topologie en bus, les réseaux suivant une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau. Le point névralgique de ce réseau est le concentrateur, car sans lui plus aucune communication entre les ordinateurs du réseau n'est possible.

- **Topologie en anneau :**

Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour.

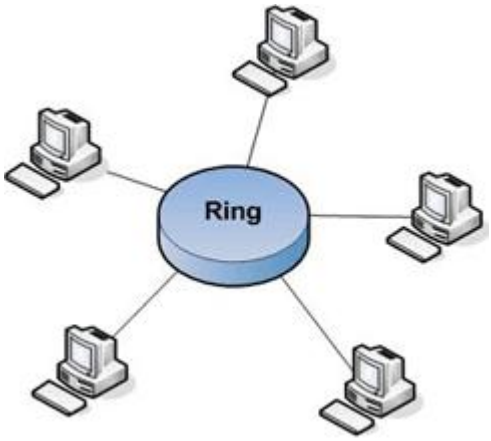


Fig.1.3. Topologie en anneau.

En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va gérer la communication entre les ordinateurs qui lui sont reliés en accordant à chacun d'entre-eux un temps de parole.

- **Topologie en arbre :**

Aussi connu sous le nom de topologie hiérarchique, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.

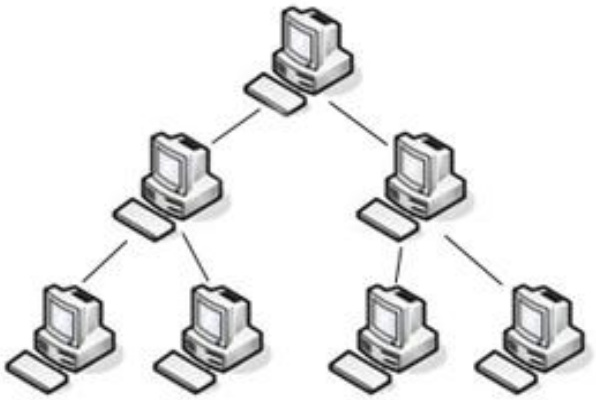


Fig.1.4. Topologie en arbre.

- **Topologie maillée :**

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons point à point. Une unité réseau peut avoir (1, N) connexions point à point vers plusieurs autres unités. Chaque terminal est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé.

Cette topologie se rencontre dans les grands réseaux de distribution (Exemple : Internet). L'information peut parcourir le réseau suivant des itinéraires divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties.

Cette topologie est très efficace car en cas de rupture d'un lien, l'information peut quand même être acheminée.

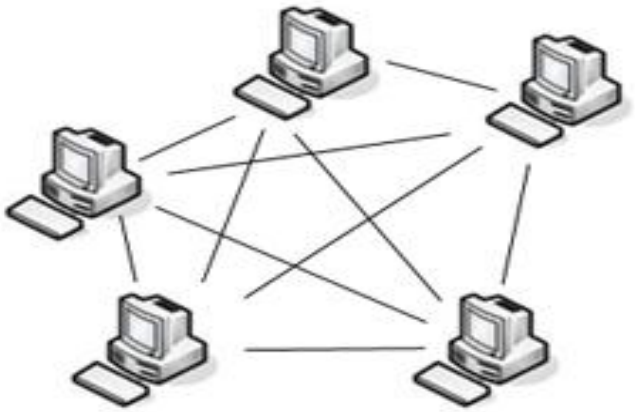


Fig.1.5. Topologie maillée.

❖ **Topologie Hybride :**

La structure hybride de réseau emploie un mélange de différents genres de structures de réseau.

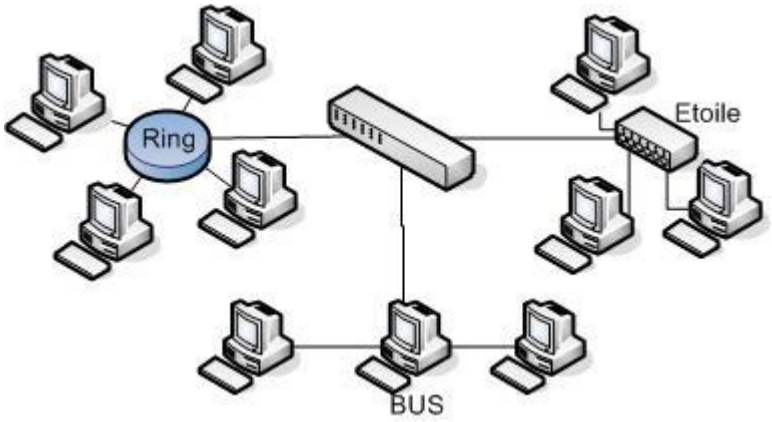


Fig.1.6. Topologie hybride.

1.4.2. Topologie logique :

La topologie logique, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

❖ **Ethernet :**

Tous les ordinateurs d'un réseau Ethernet sont reliés à une même ligne de transmission, et la communication se fait à l'aide d'un protocole appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detect).
Avec ce protocole toute machine est autorisée à émettre sur la ligne à n'importe quel moment et sans notion de priorité entre les machines. Cette communication se fait de façon simple :

- Chaque machine vérifie qu'il n'y a aucune communication sur la ligne avant d'émettre.
- Si deux machines émettent simultanément, alors il y a collision (plusieurs trames de données se trouvent sur la ligne au même moment)
- Les deux machines interrompent leur communication et attendent un délai aléatoire, puis la première ayant passé ce délai peut alors réémettre

La vitesse de ce réseau est de 10 MBPS.

- **Token ring :**

L'anneau à jeton (Token ring) est une technologie d'accès au réseau basé sur le principe de la communication au tour à tour. Chaque ordinateur du réseau a la possibilité de parler à son tour. C'est un jeton (un paquet de données), circulant en boucle d'un ordinateur à un autre, qui détermine quel ordinateur a le droit d'émettre des informations.

Lorsqu'un ordinateur est en possession du jeton il peut émettre pendant un temps déterminé, après lequel il remet le jeton à l'ordinateur suivant.

En réalité les ordinateurs d'un réseau de type "anneau à jeton" ne sont pas disposés en boucle, mais sont reliés à un répartiteur (appelé MAU, Multistation Access Unit) qui va donner successivement la parole à chacun d'entre-eux.

- **FDDI :**

La technologie LAN FDDI (Fiber Distributed Data Interface) est une technologie d'accès au réseau sur des lignes de type fibre optique. Il s'agit en fait d'une paire d'anneaux (l'un est dit primaire, l'autre, permettant de rattraper les erreurs du premier, est dit secondaire). Le FDDI est un anneau à jeton à détection et correction d'erreurs (c'est là que l'anneau secondaire prend son importance).

La topologie FDDI ressemble de près à celle de Token ring à la différence près qu'un ordinateur faisant partie d'un réseau FDDI peut aussi être relié à un concentrateur MAU d'un second réseau. On parle alors de système biconnecté.

2. Architecture des réseaux :

Le transport des données d'une extrémité à l'autre d'un réseau nécessite un support physique de communication. Cependant, pour que ces données arrivent correctement au destinataire, avec la qualité de service exigée, il faut une architecture logicielle.

L'ensemble des protocoles nécessaires constitue une architecture.

- **Définition d'un protocole :**

Un protocole est un ensemble de règles qui définissent les modalités de fonctionnement d'une communication entre deux ordinateurs, c'est-à-dire qu'un protocole permet de définir de façon standardisée la manière dont les informations sont échangées entre les équipements du réseau : il s'agit de procédures qui contrôlent le flux d'information entre deux équipements.

Des logiciels spécifiques qui gèrent ces protocoles sont installés sur les équipements d'interconnexion comme les commutateurs réseau, les routeurs, les commutateurs téléphoniques, les antennes GSM, etc.

2.1. L'architecture « OSI Open System Interconnexion »:

Au départ, les entreprises de fabrication d'appareils informatiques avaient des architectures réseaux propres à leurs équipements. Ce qui fait que la communication entre des machines de différents constructeurs était alors difficile (voir même impossible) sauf en cas d'un accord des fabricants.

Pour remédier à ce problème, l'ISO (International Standard Organisation) a créé un model de référence appelé modèle OSI (Open Systems Interconnection), un model qui prend en charge l'hétérogénéité des équipements.

Le model OSI comporte 7 couches. Ces 7 couches sont représentées ainsi :

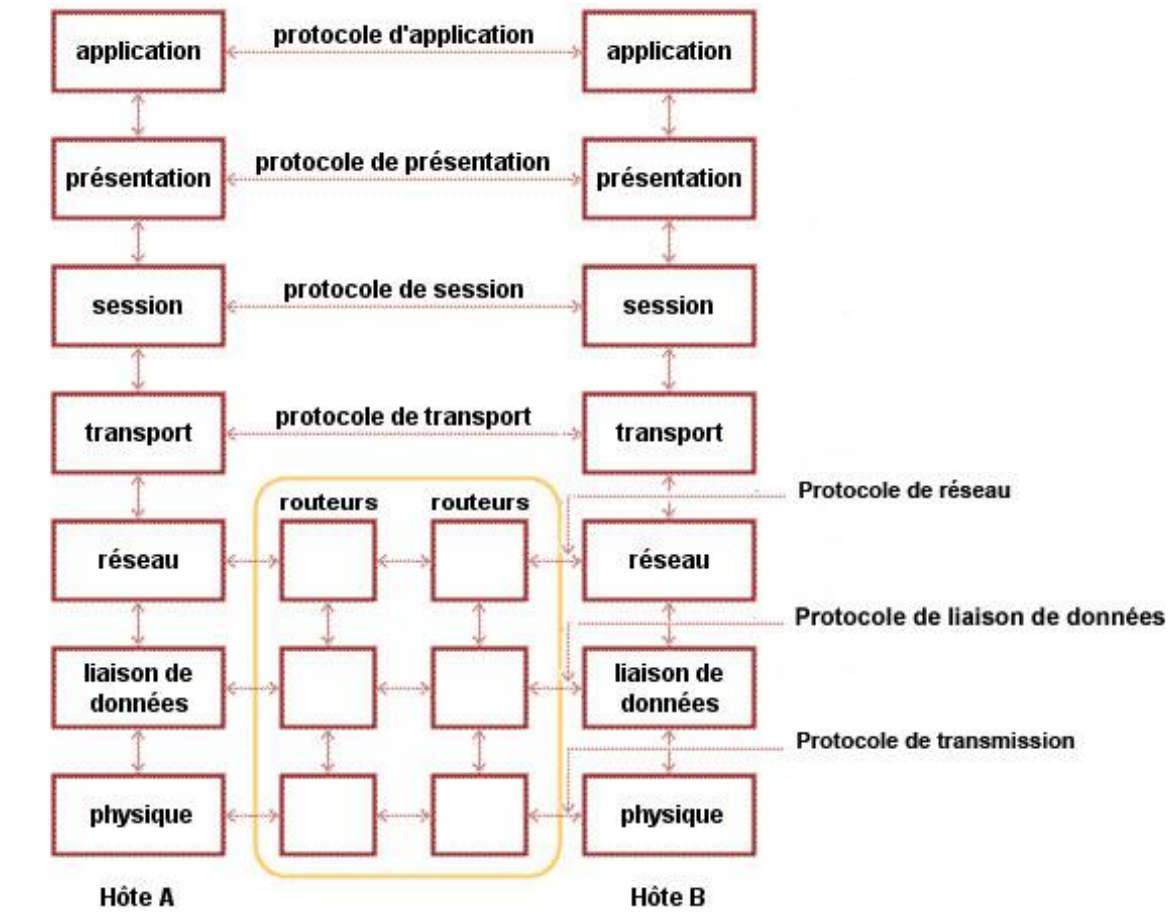


Fig.1.7. Couche de modèle OSI.

Les principes qui ont conduit à ces 7 couches sont les suivants :

- Une couche doit être créée lorsqu'un nouveau niveau d'abstraction est nécessaire
- Chaque couche a des fonctions bien définies
- Les fonctions de chaque couche doivent être choisies dans l'objectif de la normalisation internationale des protocoles

- Les frontières entre couches doivent être choisies de manière à minimiser le flux d'information aux interfaces,
- Le nombre de couches doit être tel qu'il n'y ait pas cohabitation de fonctions très différentes au sein d'une même couche et que l'architecture ne soit pas trop difficile à maîtriser.

Les couches basses (1, 2, 3 et 4) sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les couches hautes (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. Par ailleurs, les couches 1 à 3 interviennent entre machines voisines, et non entre les machines d'extrémité qui peuvent être séparées par plusieurs routeurs. Les couches 4 à 7 sont au contraire des couches qui n'interviennent qu'entre hôtes distants.

2.1.1. La couche physique :

La couche physique s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données (un bit 1 envoyé doit bien être reçu comme bit valant 1).

Concrètement, cette couche doit normaliser les caractéristiques électriques (un bit 1 doit être représenté par une tension de 5 V, par exemple), les caractéristiques mécaniques (forme des connecteurs, de la topologie...), les caractéristiques fonctionnelles des circuits de données et les procédures d'établissement, de maintien et de libération du circuit de données.

2.1.2. La couche liaison de données :

Cette couche a pour rôle de « lien », elle va transformer la couche physique en une liaison a priori sans erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur.

Rappelons que pour la couche physique, les données n'ont aucune signification particulière. La couche liaison de données doit donc être capable de reconnaître les frontières des trames. Cela peut poser quelques problèmes, puisque les séquences de bits utilisées pour cette reconnaissance peuvent apparaître dans les données.

La couche liaison de données doit être capable de renvoyer une trame lorsqu'il y a eu un problème sur la ligne de transmission. De manière générale, un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Cette couche intègre également une fonction de contrôle de flux pour éviter l'engorgement du récepteur.

2.1.3. La couche réseau :

C'est la couche qui permet de gérer le sous-réseau; le routage des paquets sur ce sous-réseau et l'interconnexion des différents sous-réseaux entre eux.
Cette couche doit permettre d'acheminer les blocs de données (les paquets) jusqu'à l'utilisateur final, blocs provenant d'une fragmentation des messages du niveau supérieur (Couche Transport). En effet, pour aller

de l’émetteur au récepteur, il faut passer par des nœuds de transfert intermédiaires ou par des passerelles, qui interconnectent le réseau.
La couche réseau contrôle également l'engorgement du sous-réseau.

2.1.4. La couche transport :

Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.
Cette couche est également responsable de l'optimisation des ressources du réseau, elle est capable de créer plusieurs connexions réseau par processus de la couche session pour répartir les données, par exemple pour améliorer le débit. Ou bien utiliser une seule connexion réseau pour transporter plusieurs messages à la fois grâce au multiplexage. Dans tous les cas, tout ceci doit être transparent pour la couche session.

Elle est également responsable du type de service à fournir à la couche session, et finalement aux utilisateurs du réseau : service en mode connecté ou non, avec ou sans garantie d'ordre de délivrance, diffusion du message à plusieurs destinataires à la fois... Cette couche est donc également responsable de l'établissement et du relâchement des connexions sur le réseau.

2.1.5. La couche session :

Le rôle de la couche session est de fournir aux entités de présentation les moyens nécessaires à l’organisation et à la synchronisation de leur dialogue. A cet effet, cette couche doit fournir les services nécessaires à l’établissement d’une connexion, de son maintien et de sa libération.

Comme son nom l’indique cette couche à pour fonction d’ouvrir et de fermer des sessions entre les utilisateurs. En effet, il est inutile d’émettre de l’information s’il n’y a personne à l’autre extrémité pour récupérer ce qui a été envoyé. Il faut donc s’assurer que l’utilisateur que l’on veut atteindre, ou du moins son représentant, qui peut être une boite aux lettres électronique, par exemple est bien présent.

Cette couche possède les fonctionnalités nécessaires à l’ouverture, à la fermeture et au maintien de la connexion.

2.1.6. La couche présentation :

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises, c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information.

Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.

2.1.7. La couche application :

La couche application joue le rôle d'une interface d'accès des applications au réseau. C'est la couche la plus proche de l'utilisateur. Elle fournit des services réseaux aux applications de l'utilisateur. Principalement des services de transfert de fichier (FTP), de messagerie (SMTP)…

2.2. L'architecture TCP/IP :

2.2.1. Présentation :

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport, TCP (Transmission Control Protocol) qui est utilisé par-dessus un protocole réseau, IP (Internet Protocol). C'est en fait une architecture réseau en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches (Le modèle OSI a été mis à côté pour faciliter la comparaison entre les deux modèles.):

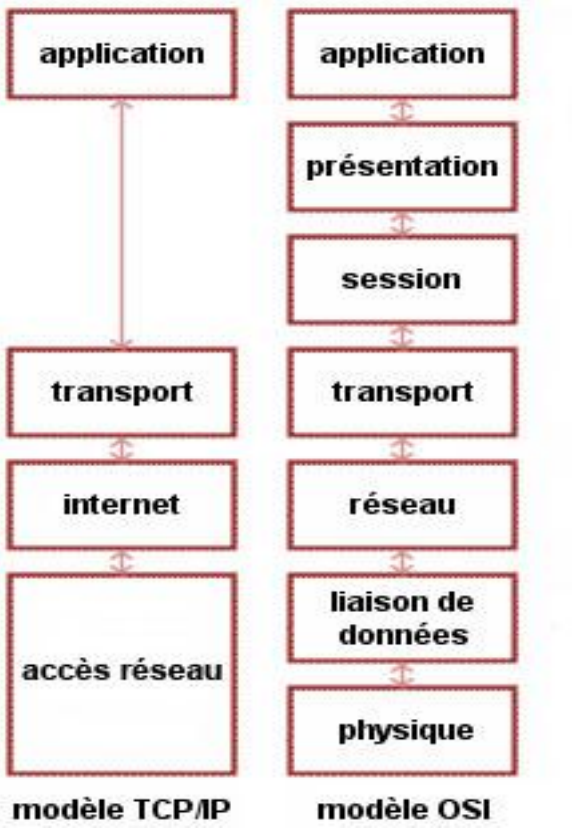


Fig.1.8. Couche du modèle TCP/IP

2.2.2. La couche accès réseau :

La couche accès réseau aussi appelée « couche de liaison de données », est réellement une interface au réseau physique. Cette interface peut ou ne peut pas assurer la livraison fiable des informations, et peut manipuler des paquets ou un flot de données.

L'implémentation de cette couche est laissée libre. De manière plus concrète, cette implémentation est typique de la technologie utilisée sur le réseau local. Par exemple, beaucoup de réseaux locaux utilisent Ethernet ; Ethernet est une implémentation de la couche accès réseau.

2.2.3. La couche internet :

Cette couche réalise l'interconnexion des réseaux (hétérogènes) distants sans connexion. Son rôle est de permettre l'injection de paquets dans n'importe quel réseau et l'acheminement des ces paquets indépendamment les uns des autres jusqu'à destination. Comme aucune connexion n'est établie au préalable, les paquets peuvent arriver dans le désordre ; le contrôle de l'ordre de remise est éventuellement la tâche des couches supérieures.

Du fait du rôle imminent de cette couche dans l'acheminement des paquets, le point critique de cette couche est le routage.

2.2.4. La couche transport :

Son rôle est le même que celui de la couche transport du modèle OSI : permettre à des entités paires de soutenir une conversation. Cette couche assure le transfert de bout en bout des données.

Deux protocoles sont utilisés :

- **TCP :** Est un protocole orienté connexion, qui assure une communication fiable en utilisant des messages d'acquittements pour pouvoir retransmettre toutes informations non reçus.
- **UDP :** Est un protocole, orienté non connexion et non fiable, utilisé pour des applications qui nécessitent un mécanisme de transport rapide étant donné qu'il n'intègre aucun mécanisme de contrôle de fiabilité de la communication.

2.2.5. La couche application :

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport, tout simplement parce que les couches présentation et session sont apparues inutiles. On s'est en effet aperçu avec l'usage, que les logiciels réseau n'utilisent que très rarement ces 2 couches.

Cette couche contient tous les protocoles de haut niveau, comme par exemple Telnet, TFTP (trivial File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (HyperText Transfer Protocol).

Le point important pour cette couche est le choix du protocole de transport à utiliser. Par exemple, TFTP (surtout utilisé sur réseaux locaux) utilisera UDP, car on part du principe que les liaisons physiques sont suffisamment fiables et les temps de transmission suffisamment courts pour qu'il n'y ait pas d'inversion de paquets à l'arrivée.

3. Internet et Web :

Internet est un gigantesque réseau mondial d'ordinateurs qui englobe plusieurs autres réseaux ordinateurs de moindre taille, offrant à l'échelle planétaire des informations et des services très variés. L'arrivée du web a apporté convivialité et interactivité à Internet, il permet l'accès à des bases de données par le biais de différentes méthodes.

3.1. Internet :

Le mot Internet vient d'un terme d'origine anglais, a été dérivé du concept "Internetting" qui se traduit en français « Interconnecter des réseaux ». Internet un réseau international d'ordinateurs, plus précisément un réseau de réseaux d'ordinateurs, qui communiquent entre eux grâce à un protocole d'échange de données standard (TCP/IP). Les différents ordinateurs branchés au réseau Internet communiquent entre eux, et la démarche est transparente pour l'utilisateur.

3.2. Extranet et Intranet :

3.2.1. Extranet :

Un réseau extranet est un réseau du type Internet (donc essentiellement basé sur le protocole IP), c'est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau.

L'accès à l'extranet se fait via Internet, par une connexion sécurisée avec mot de passe dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise. L'extranet est donc en général un site à accès sécurisé qui permet à l'entreprise de n'autoriser la consultation d'informations confidentielles qu'à certains intervenants externes comme à ses fournisseurs, ses clients, aux cadres situés à l'extérieur de l'entreprise, aux commerciaux, etc.

L'extranet est système supplémentaire offrant par exemple aux clients d'une entreprise un accès privilégié à certaines ressources informatiques de l'entreprise.

3.2.1. Intranet :

Un intranet est un ensemble de services internet internes à un réseau local, c'est-à-dire accessibles uniquement à partir des postes d'un réseau local, ou bien d'un ensemble de réseaux bien définis, et invisibles (ou inaccessibles) de l'extérieur.

Il consiste à utiliser les standards de communication de l'internet (en utilisant les protocoles TCP/IP), comme par exemple l'utilisation de navigateurs internet (client basé sur le protocole HTTP) et des serveurs web (protocole HTTP), pour réaliser un système d'information interne à une organisation ou une entreprise.

3.3. Le web « World Wide Web »:

Le World Wide Web, littéralement "toile d'araignée mondiale", ou Web est le service le plus connu et le plus utilisé offert par le réseau Internet. Il repose essentiellement sur le protocole HTTP qui offre une certaine facilité de navigation sur le réseau.

3.4. Type de ressources :

Les divers types de ressources du web ont des usages assez distincts :

- Les ressources constituant les pages web : document HTML, image (JPG, GIF, PNG…), script JavaScript, feuilles de styles CSS, sons, animations…
- Les ressources accessible depuis une page web mais consultables avec une interface particulière : flux audio, flux vidéo…
- Les ressources conçus pour être consulté séparément : document (PDF, Word), vidéo, musique, document de travail (autre fichier)…

3.5. Terminologie du Web :

3.5.1. HTML :

Hypertext Markup Language, généralement abrégé HTML, est le format de données conçu pour représenter les pages web. C'est un langage de balisage qui permet d'écrire de l'hypertexte, d'où son nom. HTML permet également de structurer sémantiquement et de mettre en forme le contenu des pages web, d'inclure des ressources multimédias dont des images, des formulaires de saisie, et des éléments programmables tels que des applets.

3.5.2. Site Web :

Un site web est composé d'un ensemble de documents structurés en utilisant le langage HTML, nommés pages web, stockés (hébergés) sur un ordinateur (serveur) connecté au réseau mondial (internet). Une page web contient essentiellement du texte, et est souvent enrichie d'images, de sons, de vidéos et de liens vers d'autres pages web.

3.5.3. Serveur Web :

On appelle serveur Web aussi bien le matériel informatique que le logiciel, qui joue le rôle de serveur informatique dans le World Wide Web.

- En tant que matériel, un serveur Web est un ordinateur comme un autre. Comme tout serveur, il relié à un réseau informatique et fait fonctionné un logiciel serveur.
- En tant que logiciel, un serveur Web est plus précisément un serveur HTTP, HTTP étant le principal protocole de communication employé par le World Wide Web.

3.5.4. Navigateur Web :

Un navigateur web est un logiciel conçu pour consulter le World Wide Web. Techniquement, c'est au minimum un client HTTP.

Il existe de nombreux navigateurs web, pour toute sorte de matériels (ordinateur personnel, tablette tactile, téléphones mobiles, etc.) et pour différents systèmes d'exploitation (Linux, Windows, Mac OS, Android). Les plus utilisés sont Mozilla Firefox, Internet Explorer, Google Chrome, Safari et Opera.

4. Le modèle Client Serveur :

4.1. Définition :

L'architecture client-serveur est un modèle de fonctionnement logiciel qui peut se réaliser sur tout type d'architecture matérielle, à partir du moment où ces architectures peuvent être interconnectées.

Cette architecture est basée sur l'utilisation de deux types de logiciels, à savoir un logiciel serveur et un logiciel client s'exécutant normalement sur 2 machines différentes, mais peut s'exécuter sur la même machine. L'élément important dans cette architecture est l'utilisation de mécanismes de communication entre les 2 applications.

Le dialogue entre les applications peut se résumer par :

- Le client demande un service au serveur
- Le serveur réalise ce service et renvoie le résultat au client

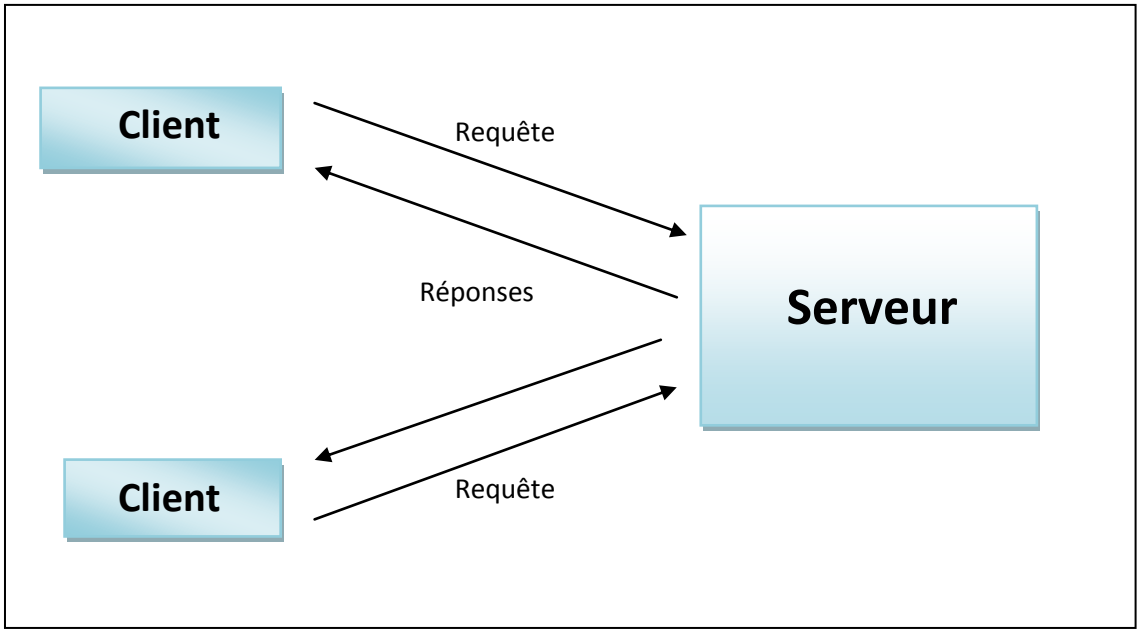


Fig.1.9. Modèle Client/Serveur.

Un des principes fondamental est que le serveur réalise un traitement pour le client.

4.2. Les principes généraux :

Il n'y a pas véritablement de définition exhaustive de la notion de client-serveur, néanmoins des principes régissent ce que l'on entend par client-serveur :

- **Service :** Le serveur est fournisseur de services. Le client est consommateur de services.
- **Protocole :** C'est toujours le client qui déclenche la demande de service. Le serveur attend passivement les requêtes des clients.
- **Partage des ressources :** Un serveur traite plusieurs clients en même temps et contrôle leurs accès aux ressources.
- **Localisation :** Le modèle client-serveur masque aux clients la localisation du serveur.

- **Hétérogénéité :** Le modèle client-serveur est indépendant des plates-formes matérielles et logicielles.
- **Redimensionnement :** Il est possible d'ajouter et de retirer des stations clientes. Il est possible de faire évoluer les serveurs.
- **Intégrité :** Les données du serveur sont gérées sur le serveur de façon centralisée. Les clients restent individuels et indépendants.
- **Souplesse et adaptabilité :** On peut modifier le module serveur sans toucher au module client. La réciproque est vraie. Si une station est remplacée par un modèle plus récent, on modifie le client (en améliorant l'interface, par exemple) sans modifier le serveur.

4.3. La répartition des tâches :

Dans l'architecture client-serveur, une application est constituée de trois parties :

- L'interface utilisateur
- La logique des traitements
- La gestion des données.

Le client n'exécute que l'interface utilisateur (souvent une interface graphique) ainsi que la logique des traitements (formuler la requête), laissant au serveur de bases de données la gestion complète des manipulations de données.

La liaison entre le client et le serveur correspond à tout un ensemble complexe de logiciels appelé middleware qui se charge de toutes les communications.

- **Middleware :**

Un des composants clé de l'architecture Client-Serveur est le middleware qui est simplement un logiciel assurant la médiatisation entre clients et serveurs dans le cadre d'architecture de systèmes hétérogènes. En d'autres termes c'est un ensemble de services logiciels construit au dessus d'un protocole de transport afin de permettre l'échange des requêtes et des réponses associées entre clients et serveurs de manière transparente, permettant de cacher l'hétérogénéité des composants mis en jeux(réseaux, SGBD…).

4.4. Les différents modèles de Client-Serveur :

En fait, les différences sont essentiellement liées aux services qui sont assurés par le serveur. On distingue couramment :

4.4.1. Le Client-serveur de données :

Dans ce cas, le serveur assure des tâches de gestion, stockage et de traitement de données. C'est le cas le plus connu de Client-Serveur est qui est utilisé par tous les grands SGBD. La base de données avec tous ses outils (maintenance, sauvegarde …) est installée sur le serveur. Sur les clients, un logiciel d'accès est installé permettant d'accéder à la base de données du serveur. Tous les traitements sur les données sont effectués sur le serveur qui renvoie les informations demandées (souvent à travers une requête SQL) par le client, qui s'occupe ensuite de la présentation.

4.4.2. Le Client-serveur de présentation :

Dans ce cas la présentation des pages affichées par le client est intégralement prise en charge par le serveur. Cette organisation présente l'inconvénient de générer un fort trafic réseau.

4.4.3. Le client-serveur de traitement :

Dans ce cas, le serveur effectue des traitements à la demande du client. Il peut s'agir de traitement particulier sur des données, de vérification de formulaires de saisie… Ces traitements peuvent être réalisés par des programmes installé sur des serveurs mais également intégrés dans des bases de données, dans ce cas, la partie donnée et traitement sont intégrés.

4.5. Les différentes architectures :

4.5.1. L'architecture 2 tiers :

Dans une architecture deux tiers, encore appelée client-serveur de première génération ou client-serveur de données, le poste client se contente de déléguer la gestion des données à un service spécialisé. Le cas typique de cette architecture est une application de gestion exploitant un SGBD centralisé.

Ce type d'application permet de tirer partie de la puissance des ordinateurs déployés en réseau pour fournir à l'utilisateur une interface riche, tout en garantissant la cohérence des données, qui restent gérées de façon centralisée.

La gestion des données est prise en charge par un SGBD centralisé, s'exécutant le plus souvent sur un serveur dédié. Ce dernier est interrogé en utilisant un langage de requête qui, plus souvent, est SQL. Le dialogue entre client et serveur se résume donc à l'envoi de requêtes et au retour des données correspondant aux requêtes.

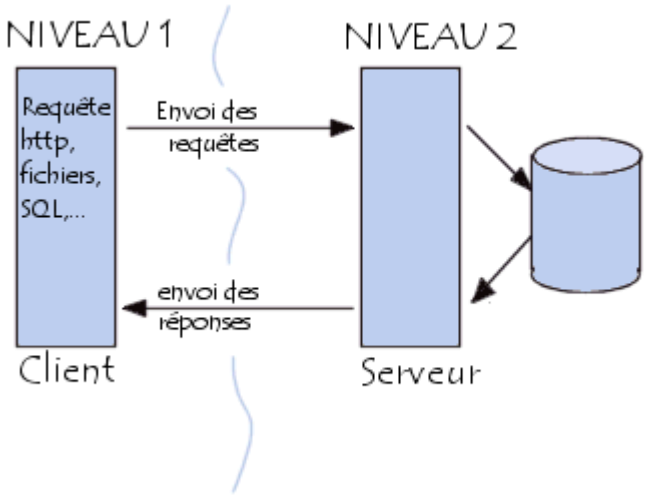


Fig.1.10. Architecture 2 tiers.

Cet échange de messages transite à travers le réseau reliant les deux machines. Il met en œuvre des mécanismes relativement complexes qui sont, en général, pris en charge par un middleware.

Il est très coûteux et très contraignant de vouloir faire porter l'ensemble des traitements applicatifs par le client, du coup le client devient un client lourd, avec un certain nombre d'inconvénients :

- On ne peut pas soulager la charge du client, qui supporte la grande majorité des traitements applicatifs.
- Le client est fortement sollicité, il devient plus complexe et doit être mis à jour régulièrement pour répondre aux besoins des utilisateurs.
- Les applications se prêtent assez mal aux fortes montées en charge car il est difficile de modifier l'architecture initiale.
- La relation étroite qui existe entre le client et le serveur complique les évolutions de ce dernier.

Malgré tout, l'architecture deux tiers présente de nombreux avantages qui lui permettent de présenter un bilan globalement positif :

- Elle permet l'utilisation d'une interface utilisateur riche.
- Elle a permis l'appropriation des applications par l'utilisateur.
- Elle a introduit la notion d'interopérabilité.

4.5.2. L'architecture 3 tiers :

Cette architecture trois tiers, également appelée client-serveur de deuxième génération ou client-serveur distribué sépare l'application en 3 niveaux de services distincts :

- **Premier niveau :** L'affichage et les traitements locaux (contrôles de saisie, mise en forme de données...) sont pris en charge par le poste client.
- **Deuxième niveau :** Les traitements applicatifs globaux sont pris en charge par le service applicatif.
- **Troisième niveau :** Les services de base de données sont pris en charge par un SGBD.

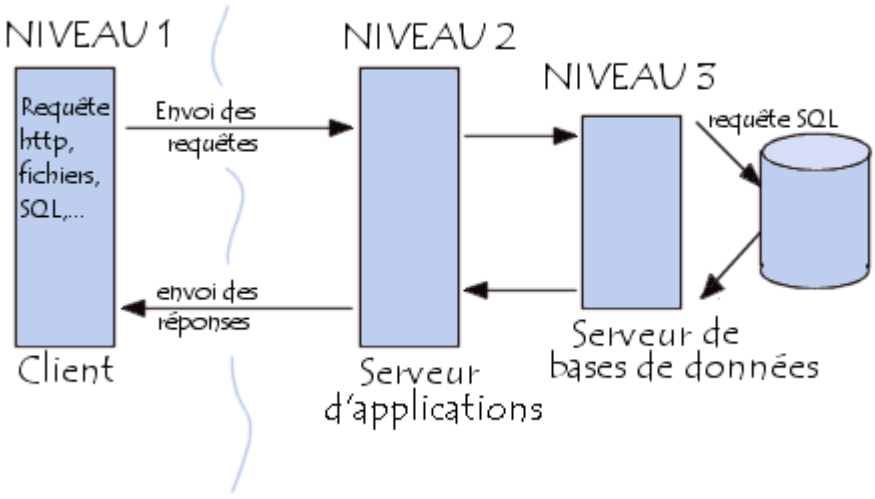


Fig.1.11. Architecture 3 tiers.

Tous ces niveaux étant indépendants, ils peuvent être implantés sur des machines différentes, de ce fait :

- Le poste client ne supporte plus l'ensemble des traitements, il est moins sollicité et peut être moins évolué, donc moins coûteux.
- Les ressources présentes sur le réseau sont mieux exploitées, puisque les traitements applicatifs peuvent être partagés ou regroupés (le serveur d'application peut s'exécuter sur la même machine que le SGBD).
- La fiabilité et les performances de certains traitements se trouvent améliorées par leur centralisation.
- Il est relativement simple de faire face à une forte montée en charge, en renforçant le service applicatif.

Dans l'architecture trois tiers, le client est communément appelé client léger, par opposition au client lourd des architectures deux tiers. Il ne prend en charge que la présentation de l'application avec, éventuellement, une partie de logique applicative permettant une vérification immédiate de la saisie et la mise en forme des données.

Le serveur de traitement constitue l'élément central de l'architecture et se trouve fortement sollicité. Dans ce type d'architecture, il est difficile de répartir la charge entre client et serveur. On se retrouve confronté aux problèmes de dimensionnement du serveur et de gestion de la montée en charge.

4.5.3. L'architecture n tiers :

L'architecture n-tiers a été pensée pour pallier aux limitations des architectures trois tiers et concevoir des applications puissantes et simples à maintenir. Ce type d'architecture permet de distribuer plus librement la logique applicative, ce qui facilite la répartition de la charge entre tous les niveaux.

Cette évolution des architectures trois tiers met en œuvre une approche objet pour offrir une plus grande souplesse d'implémentation et faciliter la réutilisation des développements.

Théoriquement, ce type d'architecture supprime tous les inconvénients des architectures précédentes :

- Elle permet l'utilisation d'interfaces utilisateurs riches,
- Elle sépare nettement tous les niveaux de l'application,
- Elle offre de grandes capacités d'extension,

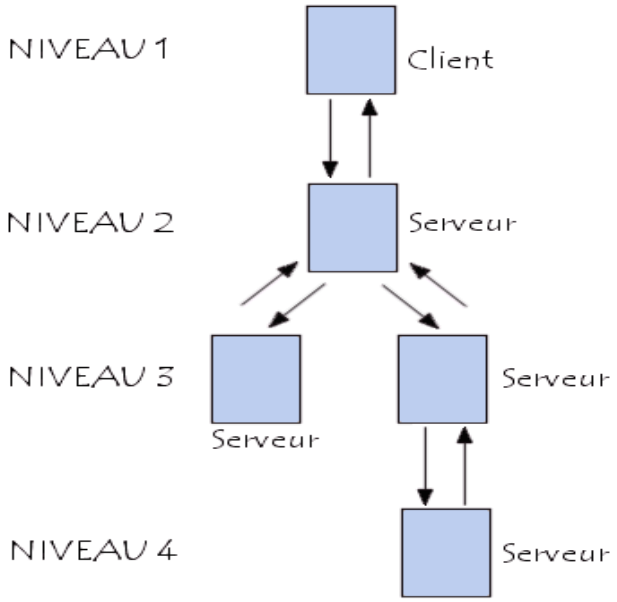


Fig.1.12. Architecture n tiers.

L'appellation « n-tiers »pourrait faire penser que cette architecture met en œuvre un nombre indéterminé de niveaux de service, alors que ces derniers sont au maximum trois. En fait, l'architecture n-tiers qualifie la distribution d'application entre de multiples services et non la multiplication des niveaux de service.

Cette distribution est facilitée par l'utilisation de composants « métier », spécialisés et indépendants, introduits par les concepts orientés. Elle permet de tirer pleinement partie de la notion de composants métiers réutilisables.

Ces nouveaux concepts sont basés sur la programmation objet ainsi que sur des communications standards entre application.

5. Le Peer to Peer :

5.1. Définition :

Peer-to-Peer signifie littéralement pair à pair. Ce concept introduit ainsi une relation d'égal à égal entre deux ordinateurs. Le modèle pair à pair se définit comme le partage des ressources et des services par échange direct entre systèmes. Ces échanges peuvent porter sur les informations, les cycles de traitement, la mémoire cache ou encore le stockage sur disque des fichiers.
Contrairement au modèle client / serveur, chaque système est une entité réseau complète qui remplit à la fois le rôle de serveur et celui de client.

5.2. Principe général :

Les systèmes pair-à-pair permettent à plusieurs ordinateurs de communiquer via un réseau, de partager simplement des objets, des fichiers le plus souvent, mais également des flux multimédia continus (streaming), le calcul réparti, un service (comme la téléphonie avec Skype) sur Internet.

Le pair-à-pair a permis une décentralisation des systèmes, auparavant basés sur quelques serveurs exposés à la censure et à l'enregistrement en masse de données privées : il permet à tous les ordinateurs de jouer directement le rôle de client et serveur (voir client-serveur)

En particulier, les systèmes de partage de fichiers permettent de rendre les objets d'autant plus disponibles qu'ils sont populaires, et donc répliqués sur un grand nombre de nœuds. Cela permet alors de diminuer la charge (en nombre de requêtes) imposée aux nœuds partageant les fichiers populaires, ce qui facilite l'augmentation du nombre de nœuds et donc de fichiers dans le réseau.

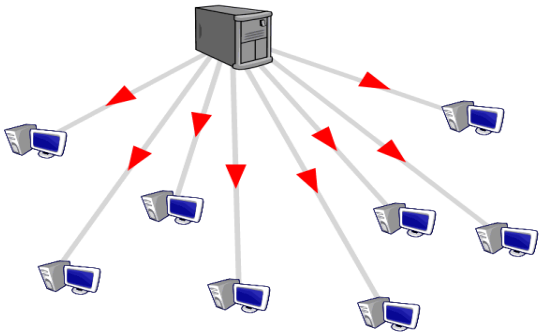


Fig.1.13. Model Client/Server

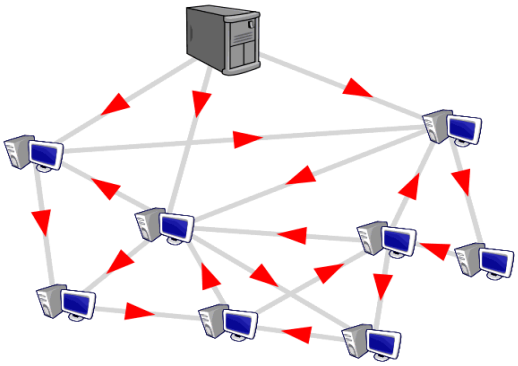


Fig.1.14. Model Peer to Peer

5.3. Avantages du model Peer to Peer:

L'architecture d'égal à égal a tout de même quelques avantages parmi lesquels :

- Un coût réduit (les coûts engendrés par un tel réseau sont le matériel, les câbles et la maintenance).
- Une simplicité à toute épreuve!
- La fiabilité du réseau.
- La décentralisation des ressources.

5.4. Inconvénients du Peer to Peer :

Les réseaux d'égal à égal ont énormément d'inconvénients :

- Ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer
- La sécurité est très peu présente
- C’est un model qui incite au piratage.

Ainsi, les réseaux d'égal à égal ne sont valables que pour un petit nombre d'ordinateurs (généralement une dizaine), et pour des applications ne nécessitant pas une grande sécurité (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

5.5. Administration d’un réseau Peer to Peer :

Le réseau poste à poste répond aux besoins d’une petite entreprise mais peut s’avérer inadéquat dans certains environnements, car l’un de ses plus grands défaut est la difficulté dans son administration, difficulté rencontré surtout dans :

- Gestion des utilisateurs et de la sécurité
- Mise à disposition des ressources
- Maintenance des applications et des données

- Installation et mise à niveau des logiciels utilisateurs

Dans un réseau poste à poste typique, il n'y a pas d'administrateur. Chaque utilisateur administre son propre poste. D'autre part tous les utilisateurs peuvent partager leurs ressources comme ils le souhaitent (données dans des répertoires partagés, imprimantes, cartes fax etc.)

Conclusion :

Les progrès réalisés dans les technologies de l'information nous ont fait entrer dans une nouvelle ère, celle de l'informatique ouverte au grand public.

Au cours de se chapitre, nous avons présenté certains concepts des nouvelles technologies de l'information et de la communication. Des éléments essentielle qui nous aiderons à mieux comprendre les notions de réseaux et pour mener à bien la suite du projet.

Chapitre II

Les Réseaux Multiplateformes

Introduction :

Aujourd'hui, les réseaux sont de plus en plus hétérogène, composé de différents types de matériels et logiciels et de multiples systèmes d'exploitation qui doivent tous être capables de communiquer les uns avec l'autre.

Il ya de moins en moins de Windows pur ou de Unix (Linux) pur, dans la plupart des réseaux, les machines utilisent des systèmes Windows côte à côte avec les serveurs Web UNIX, accessible par les ordinateurs Windows, Linux et Mac.

Ajouter au mélange une variété de téléphones intelligents (Windows Mobile, iPhone, Android, Symbian et autres) qui ont besoin de télécharger le courrier et, éventuellement, accéder aux autres ressources réseau, et vous avez la un réel défi.

1. Les réseaux multiplateformes :

1.1. Définition du terme « Multiplateforme » :

Le terme Multiplateformes se rapporte aux possibilités du logiciel ou du matériel pour fonctionner de façon identique sur différentes plates-formes (Windows, Unix, Mac, etc.). Par exemple beaucoup d'applications Windows et Macintosh produisent maintenant des fichiers binaires compatibles, ce qui signifie que les utilisateurs peuvent allez d'une plateforme a une autre sans ce soucier de convertir leurs données.

1.2. Définition :

Un réseau multiplateforme est un réseau composé de différentes machines, que se soit au niveau matériel (architecture de la machine) ou au niveau logiciel (Système d'exploitation). Chaque machine

client (Windows, Linux, Mac) peut se connecter au réseau et utiliser ses fonctionnalités sans se préoccuper du type de serveur (Windows, Linux, Mac) qui fournis le service.

Souvent il est difficile de partager des fichiers entre plates-formes en raison de différents protocoles réseau, mais dans un réseau multiplateforme ce problème est éliminé.

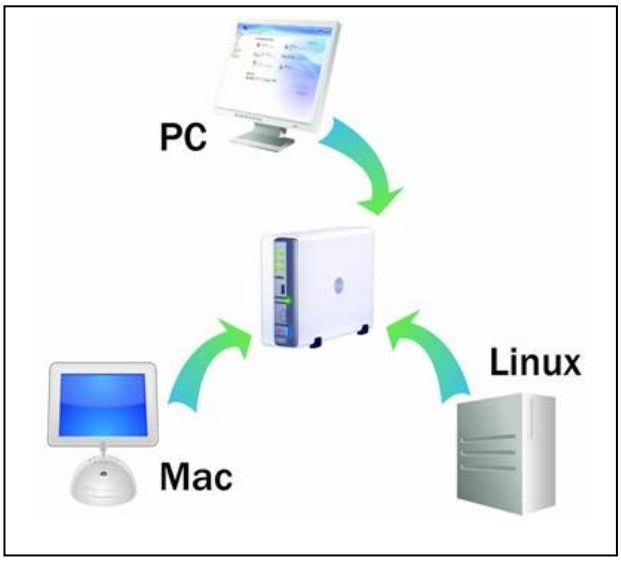


Fig2.1. Communication entre plateformes.

1.3. Définition 2 :

Les réseaux hétérogènes sont des réseaux multi fournisseurs, c'est à dire que les composants matériels ou logiciels proviennent de fournisseurs différents. Le défi des environnements réseaux hétérogènes est l'interopérabilité.

De nos jours, la majorité des réseaux sont des réseaux hétérogènes parce que :

- La technologie a évolué.
- Les fournisseurs recherchent la plus grande compatibilité de leurs produits
- Les administrateurs réseaux sont devenus « multi compétents » pour mettre en œuvre une telle complexité
- Les réseaux se construisent petit à petit, par petits bouts
- Les utilisateurs ont leurs préférences (le MAC pour les graphistes, UNIX pour les adeptes de la ligne de commande, les PC pour la part de marché, ...).

❖ **Avantages d'interconnecter des réseaux :**

L'évolution et le développement des architectures client-serveur fait qu'aujourd'hui le réseau local s'étend au réseau d'entreprise. L'utilisateur depuis son poste de travail a besoin d'accéder de manière transparente à l'information de l'entreprise, voire de la planète.

Les besoins d'interconnexion naissent essentiellement des situations suivantes :

- Interconnecter deux réseaux locaux.
- Étendre les possibilités en distance d'un réseau local au delà de ses contraintes de base.
- Interconnecter plusieurs réseaux locaux distants en donnant l'impression aux utilisateurs de travailler sur un seul réseau local.
- Insérer un réseau local dans un réseau d'ordinateurs hôtes pour permettre à une station de travail d'avoir accès aux données du réseau distant.
- Interconnecter deux réseaux d'ordinateurs hôtes d'architectures différentes.

❖ **Autres significations « interconnecter des réseaux » :**

- C'est permettre le partage des services offerts par un ensemble de réseaux.
- C'est permettre à des réseaux distincts d'échanger des informations sans pour autant apparaître globalement comme un réseau unique (ou le contraire).
- C'est aussi pouvoir utiliser un même terminal pour accéder à des applications diverses sur des ordinateurs hôtes.
- C'est pouvoir effectuer des échanges entre applications à travers plusieurs réseaux.

2. Etude des plateformes existantes :

2.1. Plateforme Linux :

2.1.1. Historique de Linux :

Linus B.Torvalds est à l'origine de ce système d'exploitation entièrement libre. Au début des années 90, il voulait mettre au point son propre système d'exploitation pour son projet de fin d'étude. Linus Torvalds avait pour intention de développer une version d'UNIX pouvant être utilisé sur une architecture de type 80x86.

Fig2.2. Interface de Linux.

Le premier clone d'UNIX fonctionnant sur PC a été Minix, écrit par Andrew Tanenbaum, un système d'exploitation minimal pouvant être utilisé sur PC. Linus Torvalds décida donc d'étendre les possibilités de Minix, en créant ce qui allait devenir Linux. Amusées par cette initiative, de nombreuses personnes ont contribué à aider Linus Torvalds à réaliser ce système, si bien qu'en 1991 une première version du système a vu le jour. C'est en mars 1992 qu'a été diffusée la première version ne comportant quasiment aucun bug.

Avec le nombre croissant de développeurs travaillant sur ce système, celui-ci a rapidement pu intégrer des redéveloppements libres des outils présents sous les systèmes UNIX commerciaux. De nouveaux outils pour Linux apparaissent désormais à une vitesse vertigineuse.

L'originalité de ce système réside dans le fait que Linux n'a pas été développé dans un but commercial. En effet aucune ligne de code n'a été copiée des systèmes UNIX originaux (en effet Linux s'inspire de nombreuses versions d'UNIX commerciales: BSD UNIX, System V.). Ainsi, tout le monde, depuis sa création, est libre de l'utiliser mais aussi de l'améliorer.

Bien que Linux ait été initialement conçu pour fonctionner sur plateforme PC, il a désormais été porté vers de nombreuses autres plateformes, telles que Macintosh, et même des plateformes telles que des assistants personnels (PDA), voire des consoles de jeu vidéo.

2.1.2. Notions de noyau et de distribution :

Linux est architecturé autour d'un noyau (kernel en anglais) chargé de prendre en charge le matériel. On appelle distribution l'assemblage d'un ensemble de logiciels autour d'un noyau Linux afin de fournir un système clé en main.

La plupart des distributions proposent également une installation graphique qui leur est propre ainsi qu'un système de gestion de paquetages permettant d'installer automatiquement des logiciels en gérant les dépendances (les logiciels sous Linux sont parfois liés à des librairies externes ou s'appuient sur d'autres logiciels).

Chaque distribution possède ses avantages et ses inconvénients. En effet si certaines sont plus adaptées à des débutants et proposent des interfaces graphiques évoluées, d'autres privilégient la sécurité ou l'évolutivité. Les distributions les plus connues sont :

- La distribution RedHat ;
- La distribution Debian ;
- La distribution SuSe ;
- La distribution Knoppix ;
- La distribution Slackware ;
- La distribution Mandriva.

2.1.3. La licence GPL de GNU :

Le code source du noyau de Linux est accessible gratuitement, ce qui fait que ce système peut être compilé sur d'autres plates-formes que le PC. Afin de permettre la distribution de programmes libres de droits, la fondation FSF (Free Software Foundation, traduisez Fondation pour les logiciels libres) a développé un projet nommé GNU (pour la petite histoire, GNU est un acronyme récursif signifiant «GNU is Not Unix»).

Les utilitaires GNU sont soumis aux termes de la licence d'utilisation GPL (General Public License) décrivant les conditions légales de l'utilisation, de la distribution ou la modification du code source.

Voici à titre indicatif quelques aspects de cette licence :

- La licence GPL permet la modification du programme original, et sa diffusion (sous licence GPL).
- La licence GPL autorise la vente du logiciel libre sous sa forme originelle ou modifiée, à condition que le vendeur autorise la diffusion (même gratuite) du logiciel ainsi modifié.
- La licence GPL autorise l'utilisation du logiciel à des fins lucratives (permettant des bénéfices).
- Les logiciels sous licence GPL restent la propriété de leurs auteurs, personne ne peut donc s'approprier tout ou partie des droits d'auteur.
- La licence n'implique aucune forme de rémunération des auteurs.

2.1.4. Les caractéristiques du système :

Linux est un système d'exploitation proche des systèmes UNIX pouvant être exécuté sur différentes plates-formes matérielles : x86 (plates-formes à base de processeurs Intel, AMD, etc.), Sparc, PowerPC, Alpha, ARM, etc. Ainsi le système Linux peut fonctionner aussi bien sur des ordinateurs personnels que des consoles de jeu ou des assistants personnels.

Linux est ainsi un système multi plate-forme. Il est également multi-utilisateurs, mais aussi multi-tâches et multi-processeurs.

Linux est considéré comme un système fiable, robuste et puissant. Il est d'ailleurs capable de fonctionner avec très peu de ressources sur des ordinateurs bas de gamme très peu puissants.

2.1.5. Le système X :

X est une interface graphique, qui a été développée au MIT, permettant de créer des applications graphiques fonctionnant sur diverses plateformes.

X-Window est l'interface graphique des stations UNIX. X-Window est en quelque sorte aux systèmes Unix ce que l'interface Windows est au DOS. L'avantage majeur de ce système est l'utilisation d'une interface graphique en complément à certaines commandes.

Sous Linux il existe une implémentation libre du système X-Window appelée XFree86. XFree86 supporte un nombre très important de cartes vidéo, mais certaines ne sont pas supportées. Toutefois avec la communauté du libre, le portage des pilotes des nouvelles cartes graphiques est de plus en plus rapide.

2.1.6. Réseau Linux :

Linux supporte les deux protocoles de base des systèmes UNIX: TCP/IP et UUCP. La plupart des réseaux TCP/IP utilisent l'Ethernet pour le transport physique des données. Linux supporte la plupart des cartes Ethernet populaires pour le PC.

Linux supporte également SLIP (Serial Line Internet Protocol) et PPP (Point do Point Protocol), qui permettent de se connecter à l'Internet (ou tout autre réseau TCP/IP) par modem. Vous aurez besoin d'un accès à une machine serveur SLIP ou PPP, connectée au réseau. Un grand nombre d'entreprises ou d'universités proposent de tels services. En fait, si votre système Linux possède à la fois une connexion Ethernet et un modem, vous pouvez le configurer en tant que serveur de ce type pour d'autres machines.

UUCP (UNIX-to-UNIX Copy) est un mécanisme plus ancien entre machines UNIX. Traditionnellement, les machines UUCP se connectent entre elles par téléphone à l'aide d'un modem, mais UUCP est aussi capable de transporter des données sur une liaison TCP/IP. Si vous ne pouvez avoir accès à un réseau TCP/IP, vous pouvez configurer votre système de façon qu'il reçoive et envoie des fichiers et le courrier électronique par UUCP.

2.1.7. La documentation sur Linux :

Linux étant un système distribué librement, la documentation à son propos est très abondante. En effet, lorsque Linux a été développé, de nombreuses personnes ont rédigé des petits guides d'utilisation. Toutefois ceux-ci étaient généralement trop compliqués pour être accessibles à l'ensemble de la communauté Linux et étaient pour la plupart écrits en anglais, c'est pourquoi des personnes ont décidé d'écrire des documentations en français. On peut notamment citer :

- The Linux Documentation Project
- Google Linux pour des recherches spécifiques sur Linux
- Le guide du ROOTard d'Eric Dumas
- Le système d'exploitation Linux, de Rémy Card, René Cougnenc et Julien Simon

De nombreux documents ont aussi été mis au point par des personnes diverses, il s'agit des Mini « HowTo ». Ces documents expliquent des points précis de Linux de façon simple.

2.1.8. Avantages de Linux :

- Open source (libre), le code source du noyau système et des programmes sont accessibles à tous (sous licence GPL).
- Gratuit (aucune license à payer).
- Compatibilité multi-architecturales Linux s'installe sur toute sorte de machines : Intel (x86), powerpc, sparc, amd64 (ia64), mips, alpha, arm,....
- Aucun virus et spyware (fichiers espions) n'affectent les fichiers ou programmes systèmes de manières critiques ou dangereuses.
- Pas besoin de pare-feu, Sur un *ordinateur local seulement* (sauf pour un serveur), même s'il est recommandé d'en installer un, il n'est pas urgent ou obligatoire d'installer un logiciel pare-feu (firewall) car les services réseaux activés (web, ftp, ping, ...) protègent les ports utilisés.
- Existe plusieurs sortes de distributions (plus de 200). Alors, là, il y en a pour tous les goûts.

- Une distribution Linux récente peut fonctionner sur des anciennes machines (à partir des architectures Intel 386) incluant des programmes récents et ce, sans ralentir le système.
- Evolution rapide des distributions les plus connus (en moyenne, une nouvelle version majeure tout les six à sept mois pour les distributions les plus populaire).
- Compatible avec toutes les normes des technologies du web et informatique ouvert comme W3C pour le net, OpenDocument pour la bureautique…
- Il y'a énormément de support techniques et de documentation gratuit.
- Plus de choix de logiciels libre et gratuits.
- Est beaucoup moins gourmand en ressources systèmes (RAM, CPU, Espace disque,...) que les autres systèmes d'exploitation (Windows et Mac OS).
- Une sécurité plus sévère et efficace sur l'accessibilité des programmes (droits d'accès).
- A une plus grande tolérance aux pannes que les autres systèmes.

2.1.9. Inconvénients de Linux :

- Linux est complexe, En effet Linux possédant une structure complexe qui demande de la part de l'utilisateur une grande recherche.
- Le nombre impressionnant de distributions, et ce n'est pas évident de choisir pour un utilisateur débutant.
- Un manque de pilotes ou de drivers propriétaires pour Linux. La plupart des constructeurs de matériels informatiques ne produisent pour la plateforme linux.
- La configuration est souvent moins simple que dans les logiciels commerciaux. Il vaut mieux avoir un esprit un peu technicien.
- Certains types de logiciels tels que les jeux sont beaucoup plus fournis sous MS-Windows que sous Linux.

2.2. Plateforme Mac OS X :

2.2.1. Présentation :

Mac OS X est une ligne de systèmes d'exploitation propriétaires développés et commercialisés par Apple, dont la version la plus récente (Mac OS X 10.7, dit Lion) est installée sur tous les Macintosh vendus actuellement.

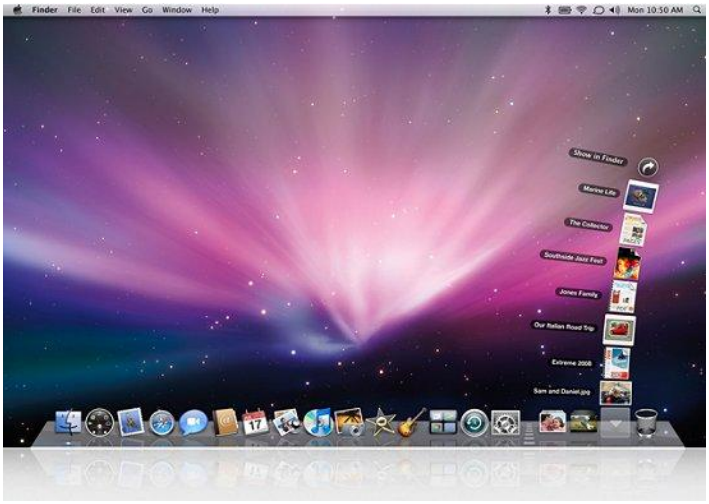


Fig2.3. Interface Mac OS X.

Mac OS X est le successeur du système Mac OS, qui avait été le principal système d'exploitation d'Apple depuis 1984. Contrairement à ses prédécesseurs, Mac OS X fait partie de la famille des systèmes d'exploitation UNIX, basé sur les technologies développées par NeXT(Une tres grande entreprise de devellopement de software) depuis le milieu des années 1980 jusqu'au rachat de la société par Apple en 1997.

Il est surtout connu pour être un des premiers systèmes grand public ayant une interface graphique, inspiré de Xerox Alto, et basée sur les fenêtres, icones, menus et utilisation de la souris.

La première version du système fut Mac OS X Server 1.0, commercialisée en 1999, suivie par une version orientée pour le grand public en mai 2001.

La version serveur de Mac OS X est architecturalement identique à la version grand public, mais incorpore des logiciels facilitant la mise en place et l'administration de réseau, de serveur de messagerie électronique et de serveur Samba, entre autres.

2.2.2. XNU, « X is Not Unix » :

Le Kernel de MacOs X utilise le micro-kernel Mach (version 3) comme noyau de base pour la gestion des opérations, il est en forte relations avec le matériel (Threads, mémoire...) et inclus en plus des services issus du système FreeBSD pour les opérations de plus haut niveau telles que la gestion réseau, de la sécurité Unix ou encore les processus Unix.

Ce Kernel est de type hybride. L'ensemble est connu par le système comme formant une unique tâche et chacune de ses composantes s'exécute dans un groupe de Thread. L'intérêt d'intégrer certains services BSD directement au niveau de Kernel est un choix technique de la part d'Apple qui permet d'optimiser les temps d'accès à ces services. En effet, les opérations effectuées en espace Kernel sont prioritaires et nécessites moins de transactions que les opérations effectuées en espace utilisateur.

Le Kernel XNU inclus aussi « Platform expert » celui-ci permet d'isolé le code du système de la plupart des spécificités relatives aux différentes architectures matérielles. Cela permet au système d'être fortement

portable. Par ailleurs signalons que MacOS X fonctionne actuellement sous PowerPC, Intel, et ARM (MacOS X mobile).

XNU dispose d'une architecture de gestion de drivers systèmes avancée. Celle-ci porte le nom de IOKit. Le développement des drivers est orienté objet. Ceux-ci, appelés Kext (Kernel Extention) sont chargeables à chaud quelque soit leur type ce qui permet d'éviter des redémarrages dans de nombreux cas de figure.

2.2.3. Le système de fichier HFS :

Mac OS X travaille avec VFS (Virtual File System) ce qui lui permet de pourvoir éventuellement utiliser n'importe quel système de fichier au sein du système. Cependant le système de fichier par défaut est HFS+ depuis 1998. Bien que vieillissant, celui-ci dispose néanmoins de toutes les fonctionnalités modernes (il est par ailleurs comparable à NTFS).
HFS se présente sous plusieurs versions :

- HFS : la version originale de système de fichiers de Mac OS (parfois utilisé encore dans certains CD-ROM)
- HFS+ : une version modifiée du HFS (introduit avec Mac OS 8.1) qui permet la gestion de plus gros disques (le plus répandu actuellement).
- HFSX : une nouvelle déclinaison du HFS (introduit avec Mac OS X v10.3).

2.2.4. L'aspect Multi-Architectures :

Mac OS X a été conçu pour être portable, il dispose d'une couche d'abstraction pour le matériel (Platform expert) permettant de diminuer les différences qui existent entre les architectures des processeurs. Le système peut par conséquent être porté vers de multiples architectures avec un minimum d'effort.

Cependant, Mac OS X va plus loin, en effet, lors de la transition du PowerPc vers l'architecture Intel en 2005, Apple a utilisée une technologie de la société Transitive pour permettre l'exécution des binaires PowerPc sous Mac OS X Intel. Cette Technologie appelée « Rosetta » permet de traduire à la volée les instructions d'une architecture à une autre. Ce procédé réduit les performances originales d'environs 50% mais permet d'effectuer des transitions d'architecture d'une manière transparente pour les utilisateurs.

Enfin, l'héritage de NextStep permet à Mac OS X d'exploiter des Fat-binaries ou Universal-binaries. Celles-ci permettent de créer un unique fichier exécutable contenant plusieurs architectures. Les binaires des différentes architectures sont simplement concaténées et un header est renseigné avec le nombre d'architectures contenues, leurs tailles et leurs adresses de début dans le fichier, cela est possible grâce au compilateur GCC modifié par Apple. L'environnement d'exécution natif (Mach-O) sait lire cette entête et charge simplement la bonne architecture en mémoire puis l'exécute comme un exécutable standard. Ce principe simple permet à Mac OS X de pouvoir évoluer sans se soucié des évolutions matériels puisse qu'il existe une stratégie de transition bien rodé.

2.2.5. Avantages de Mac OS :

- Mac OS X dispose d'une interface utilisateur qui prend moins de ressources système.
- Une meilleure sécurité, vous avez beaucoup moins de chances d'être infecter par un virus sur votre Mac que sur votre PC.
- Mac OS X dispose d'une interface simple, facile à utiliser, parfaite aussi bien pour débutants et les professionnels. C'est assez facile pour l'utilisateur à domicile, et assez puissant pour les programmeurs.
- Mac OS X dispose d'une grande contité de programme qui sont fournit avec le système d'exploitation.
- Si vous avez besoin d'exécuter un programme Windows, vous pouvez exécuter Boot Camp sur tous les Macs Intel Leopard et installer Windows sur votre Mac.

2.2.6. Inconvénients de Mac OS :

- Mac OSX est indissociable de la plateforme Mac : il faut donc acheter un Mac pour en bénéficier.
- Le prix d'un Mac et relativement cher, bien plus cher qu'un PC.
- Un catalogue de logiciel pas très riche
- L'évolution des composants matériel et logiciel est plus lente

2.3. La plateforme Windows :

2.3.1. Présentation :

Windows (littéralement « Fenêtres » en anglais) est une gamme de systèmes d'exploitation produite par Microsoft, principalement destinés aux ordinateurs compatibles PC.

Fig2.4. Interface Windows XP.

C'est le successeur de MS-DOS. Depuis les années 1990, et notamment la sortie de Windows 95, il rencontre un succès indéniable, dû en partie au fait que son éditeur passa de très nombreux accords d'exclusivité avec les constructeurs d'ordinateur leur interdisant d'installer un autre système. Vendu préinstallé sur la quasi-totalité des ordinateurs personnels qui ne proposent par ailleurs aucun autre système au choix, il possède un statut de quasi-monopole (ce qui n'est pas le cas sur les serveurs).

La gamme Windows est composée de plusieurs branches :

- La première branche, dite branche 16 bits, couvre Windows 1 à 3.11 (3.2 en chinois). Elle est apparue en 1985 et fonctionnait uniquement sur compatibles PC, en mode 16 bits.
- La deuxième branche, dite branche Windows NT (Windows NT 3.1, NT 4.0, puis Windows 2000), est apparue en 1993. C'est un développement repartant de zéro, destiné aux ordinateurs personnels, aux serveurs et à des ordinateurs non compatibles PC. Elle a d'abord été utilisée dans les entreprises. Avec Windows XP, sorti en 2001, qui continue la branche Windows NT cette branche est désormais aussi grand public, et se poursuit avec Windows Vista et Windows 7.
- La troisième branche, parfois appelée branche Windows 9x, est apparue en 1995 et a existé parallèlement avec la branche NT. Cette branche a débuté avec Windows 95, suivi de Windows 98 et Windows Me. Elle était plus connue du grand public et avait pour vocation de remplacer la première branche. C'est la première branche grand public 32 bits.
- La quatrième branche, dite branche Windows CE, apparue en 1996 avec Windows CE 1.0. Elle est destinée aux systèmes embarqués et matériels légers et portables (assistant personnel, téléphone portable). C'est la base de Windows Mobile et Pocket PC.

3. Les services réseaux :

3.1. Définition :

Un service réseau est une fonctionnalité assurée par un ordinateur (généralement un serveur), consistant en l'aptitude à la fourniture d'informations à d'autres ordinateurs via une connexion réseau normalisée. Autrement dit un service réseau est un logiciel ayant pour but de répondre à une demande provenant du réseau. Ils se basent sur des protocoles.

Il ya une multitude de services réseaux, quelqu'un sont unique a Windows ou a linux, mais les principaux services sont disponible quelque soit l'architecture.

3.2. DNS « Domain Name System » :

3.2.1. Définition :

Chaque ordinateur directement connecté à internet possède au moins une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre 192.153.5.26 mais avec un nom de domaine ou des adresses plus explicites (appelées adresses FQDN) du type www.google.com. Ainsi, il est possible d'associer des noms en langage courant aux adresses numériques grâce à un système appelé DNS (Domain Name System).

On appelle résolution de noms de domaines (ou résolution d'adresses) la corrélation entre les adresses IP et le nom de domaine associé.

3.2.2. Noms d'hôtes :

Aux origines de TCP/IP, étant donné que les réseaux étaient très peu étendus ou autrement dit que le nombre d'ordinateurs connectés à un même réseau était faible, les administrateurs réseau créaient des

fichiers appelés tables de conversion manuelle. Ces tables de conversion manuelle étaient des fichiers séquentiels, associant sur chaque ligne l'adresse IP de la machine et le nom littéral associé, appelé nom d'hôte.

3.2.3. Introduction au Domain Name System :

Le système précédent de tables de conversion nécessitait néanmoins la mise à jour manuelle des tables de tous les ordinateurs en cas d'ajout ou de modification d'un nom de machine. Ainsi, avec l'explosion de la taille des réseaux, et de leur interconnexion, il a fallu mettre en place un système de gestion des noms hiérarchisé et plus facilement administrable. Le DNS propose :

- Un espace de noms hiérarchique permettant de garantir l'unicité d'un nom dans une structure arborescente, à la manière des systèmes de fichiers d'Unix.
- Un système de serveurs distribués permettant de rendre disponible l'espace de noms.
- Un système de clients permettant de « résoudre » les noms de domaines, c'est-à-dire interroger les serveurs afin de connaître l'adresse IP correspondant à un nom.

3.2.4. L'espace de noms :

La structuration du système DNS s'appuie sur une structure arborescente dans laquelle sont définis des domaines de niveau supérieurs (appelés TLD, pour Top Level Domains), rattachés à un nœud racine représenté par un point.

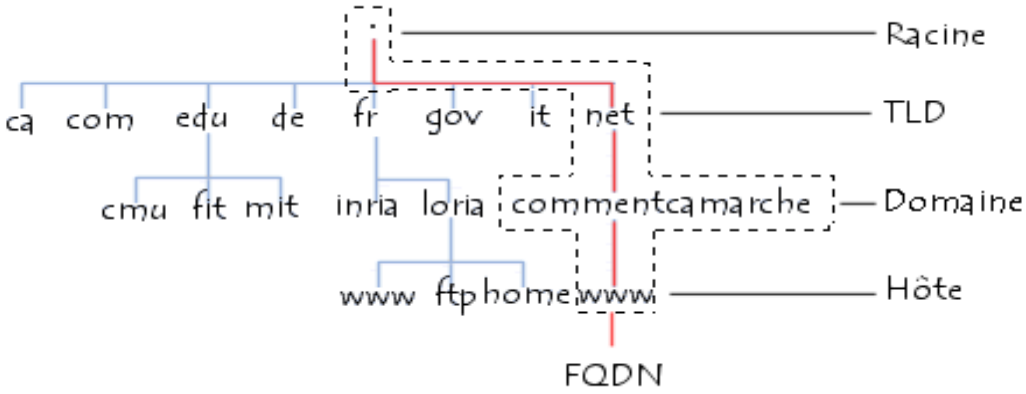


Fig.2.5. Espace de noms.

On appelle « nom de domaine » chaque nœud de l'arbre. Chaque nœud possède une étiquette d'une longueur maximale de 63 caractères. L'ensemble des noms de domaine constitue ainsi un arbre inversé où chaque nœud est séparé du suivant par un point.

L'extrémité d'une branche est appelée hôte, et correspond à une machine ou une entité du réseau. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré, ou le cas échéant dans le sous-domaine. A titre d'exemple le serveur web d'un domaine porte ainsi généralement le nom www.

Le mot « domaine » correspond formellement au suffixe d'un nom de domaine, c'est-à-dire l'ensemble des étiquettes de nœuds d'une arborescence, à l'exception de l'hôte.

Le nom absolu correspondant à l'ensemble des étiquettes des nœuds d'une arborescence, séparées par des points, et terminé par un point final, est appelé adresse FQDN (Fully Qualified Domain Name, soit Nom de Domaine Totalement Qualifié). La profondeur maximale de l'arborescence est de 127 niveaux et la longueur maximale d'un nom FQDN est de 255 caractères. L'adresse FQDN permet de repérer de façon unique une machine sur le réseau des réseaux. Ainsi www.google.com représente une adresse FQDN.

3.2.5. Résolution de noms de domaine :

Le mécanisme consistant à trouver l'adresse IP correspondant au nom d'un hôte est appelé « résolution de nom de domaine ». L'application permettant de réaliser cette opération (généralement intégrée au système d'exploitation) est appelée « résolveur ».

Lorsqu'une application souhaite se connecter à un hôte connu par son nom de domaine (par exemple www.google.com), celle-ci va interroger un serveur de noms défini dans sa configuration réseau. Chaque machine connectée au réseau possède en effet dans sa configuration, les adresses IP de deux serveurs de noms de son fournisseur d'accès.

Une requête est ainsi envoyée au premier serveur de noms (appelé « serveur de nom primaire »). Si celui-ci possède l'enregistrement dans son cache, il l'envoie à l'application, dans le cas contraire il interroge un serveur racine. Le serveur de nom racine renvoie une liste de serveurs de noms faisant autorité sur le domaine (dans le cas présent les adresses IP des serveurs de noms primaire et secondaire de google.com).

Le serveur de noms primaire faisant autorité sur le domaine va alors être interrogé et retourner l'enregistrement correspondant à l'hôte sur le domaine (dans notre cas www).

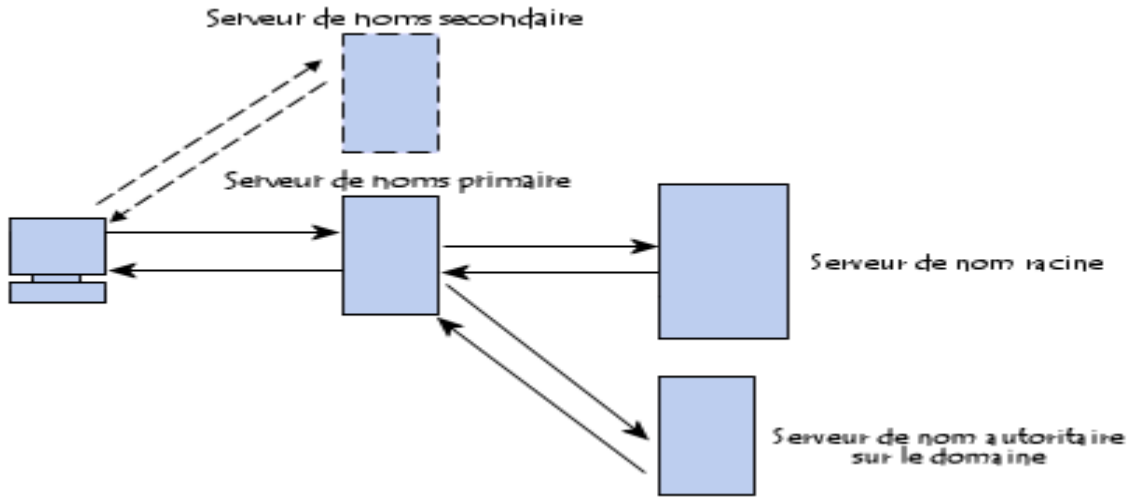


Fig.2.6. Résolution de noms de domaine.

3.2.6. Types d'enregistrements :

Un DNS est une base de données répartie contenant des enregistrements, appelés RR (Resource Records), concernant les noms de domaines.

En raison du système de cache permettant au système DNS d'être réparti, les enregistrements de chaque domaine possèdent une durée de vie, appelée TTL (Time To Live, ou espérance de vie), permettant aux serveurs intermédiaires de connaître la date de péremption des informations et ainsi savoir s'il est nécessaire ou non de la revérifier.

D'une manière générale, un enregistrement DNS comporte les informations suivantes :

Nom de domaine (FQDN)	TTL	Type	Classe	RData

- **Nom de domaine :** Le nom de domaine doit être un nom FQDN, c'est-à-dire être terminé par un point. Si le point est omis, le nom de domaine est relatif, c'est-à-dire que le nom de domaine principal suffixera le domaine saisi.
- **Type:** Une valeur sur 16bits spécifiant le type de ressource décrit par l'enregistrement.
- **Classe :** La classe peut être soit IN (correspondant aux protocoles d'internet, soit CH (pour le système chaotique)
- **RDATA :** il s'agit des données correspondant à l'enregistrement.

3.3. DHCP « Dynamic Host Configuration Protocol » :

3.3.1. Définition :

Le DHCP est un service réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, et également des serveurs de noms DNS.

La conception initiale d'IP supposait la pré-configuration de chaque ordinateur connecté au réseau avec les paramètres TCP/IP adéquats : c'est l'adressage statique (nommée IP fixe). Sur des réseaux de grandes dimensions ou étendues, où des modifications interviennent souvent, l'adressage statique engendre une lourde charge de maintenance et des risques d'erreurs. En outre les adresses assignées ne peuvent être utilisées même si l'ordinateur qui la détient n'est pas en service : un cas typique où ceci pose problème est celui des fournisseurs d'accès à internet, qui ont en général plus de clients que d'adresses IP à leur disposition, mais dont les clients ne sont jamais tous connectés en même temps.

DHCP apporte une solution à ces deux inconvénients :

- Seuls les ordinateurs en service utilisent une adresse de l'espace d'adressage.
- Toute modification des paramètres (adresse de la passerelle, des serveurs de noms) est répercutée sur les stations lors du redémarrage.
- La modification de ces paramètres est centralisée sur les serveurs DHCP.

3.3.2. Fonctionnement :

L'ordinateur équipé de TCP/IP, mais dépourvu d'adresse IP, envoie par diffusion un datagramme (DHCP DISCOVER) qui s'adresse au port 67 de n'importe quel serveur à l'écoute sur ce port. Ce datagramme comporte entre autres l'adresse physique (MAC) du client.

Tout serveur DHCP ayant reçu ce datagramme, s'il est en mesure de proposer une adresse sur le réseau auquel appartient le client, diffuse (broadcast sur le domaine de diffusion) une offre DHCP (DHCP OFFER) à l'attention du client (sur son port 68), identifié par son adresse physique. Cette offre comporte l'adresse IP du serveur, ainsi que l'adresse IP et le masque de sous-réseau qu'il propose au client. Il se peut que plusieurs offres soient adressées au client.

Le client retient une des offres reçues (la première qui lui parvient), et diffuse sur le réseau un datagramme de requête DHCP (DHCP REQUEST). Ce datagramme comporte l'adresse IP du serveur et celle qui vient d'être proposée au client. Elle a pour effet de demander au serveur choisi l'assignation de cette adresse, l'envoi éventuel des valeurs des paramètres, et d'informer les autres serveurs qui ont fait une offre qu'elle n'a pas été retenue.

Le serveur DHCP choisi élabore un datagramme d'accusé de réception (DHCP ACK pour acknowledgement) qui assigne au client l'adresse IP et son masque de sous-réseau, la durée du bail de cette adresse (dont découlent deux valeurs T1 et T2 qui déterminent le comportement du client en fin de bail), et éventuellement d'autres paramètres :

- Adresse IP de la passerelle par défaut,
- Adresses IP des serveurs DNS,
- Adresses IP des serveurs NBNS (WINS).

Les serveurs DHCP doivent être pourvus d'une adresse IP statique.

3.4. FTP « File Transfer Protocol » :

3.4.1. Définition :

File Transfer Protocol (protocole de transfert de fichiers), ou FTP, est un protocole de communication destiné à l'échange de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.

FTP obéit à un modèle client-serveur, c'est-à-dire qu'une des deux parties, le client, envoie des requêtes auxquelles réagit l'autre, appelé serveur. En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé serveur FTP, qui rend public une arborescence de fichiers similaire à un système de fichiers UNIX. Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande).

Deux ports sont standardisés (well known ports) pour les connexions FTP : le port 21 pour les commandes et le port 20 pour les données. Ce protocole peut fonctionner avec IPv4 et IPv6.

FTP a pour objectifs de :

- permettre un partage de fichiers entre machines distantes
- permettre une indépendance aux systèmes de fichiers des machines clientes et serveur
- permettre de transférer des données de manière efficace

3.4.2. Modes de fonctionnement :

FTP peut s'utiliser de deux façons différentes :

- **Mode actif :**

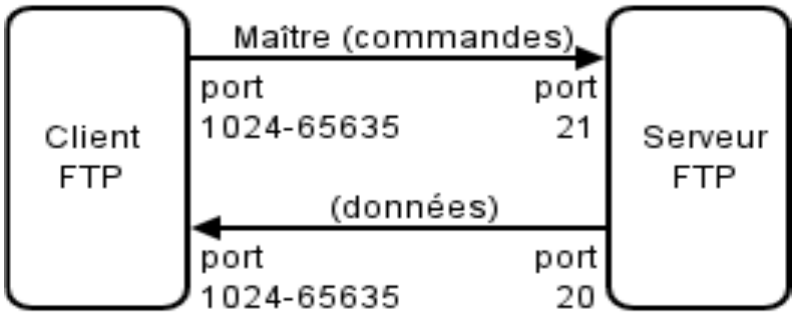


Fig.2.7. Mode actif.

En mode actif, c'est le client FTP qui détermine le port de connexion à utiliser pour permettre le transfert des données. Ainsi, pour que l'échange des données puisse se faire, le serveur FTP initialisera la connexion de son port de données (port 20) vers le port spécifié par le client. Le client devra alors configurer son pare-feu pour autoriser les nouvelles connexions entrantes afin que l'échange des données se fasse. De plus, il peut s'avérer problématique pour les utilisateurs essayant d'accéder à des serveurs FTP lorsque ces utilisateurs sont derrière une passerelle NAT. Étant donnée la façon dont fonctionne le NAT, le serveur FTP lance la connexion de données en se connectant à l'adresse externe de la passerelle NAT sur le port choisi. Certaines passerelles NAT n'ayant pas de correspondance pour le paquet reçu dans la table d'état, le paquet sera ignoré et ne sera pas délivré au client.

- **Mode passif :**

Fig.2.8. Mode passif.

En mode passif, le serveur FTP détermine lui-même le port de connexion à utiliser pour permettre le transfert des données (data connexion) et le communique au client. En cas de présence d'un pare-feu

devant le serveur, celui-ci devra être configuré pour autoriser la connexion de données. L'avantage de ce mode est que le serveur FTP n'initialise aucune connexion. Ce mode fonctionne sans problèmes avec des clients derrière une passerelle NAT. Dans les nouvelles implémentations, le client initialise et communique directement par le port 21 du serveur ; cela permet de simplifier les configurations des pare-feu serveurs.

3.5. NFS « Network File System » :

NFS permet très simplement de partager des données entre plusieurs machines. Par exemple, un utilisateur qui se connecte sur un réseau n'aura plus à se logger sur une machine précise : via NFS, son home directory lui sera livré sur la machine où il se connecte.

NFS n'est toutefois pas un protocole très performant et n'est pas utilisable de manière confortable au travers une connexion par modem (internet). En revanche, sur un réseau local, son utilisation offre une grande souplesse tant aux utilisateurs qu'aux administrateurs.

Il faut néanmoins prendre quelques précautions par rapport à ce service. En effet, permettre à n'importe qui d'écrire des données sur son réseau n'est pas conseillé, certaines mesures indispensables, limitent les risques.

Donc une machine joue le rôle de serveur de fichiers. Elle est appelée serveur NFS, et

- on dit qu'elle exporte tout (arborescence racine /) ou partie de son système de fichiers,
- en le partageant par une liste de stations accessibles par réseau,
- en installant toutefois des restrictions d'accès.

3.6. NIS « Network Information Service » :

Ce service repris par tous les systèmes a été développé par SUN, il est aussi connu sous le nom "Yellow Pages" (YP ou pages jaunes). Ce service NIS, permet de centraliser (à la manière du DNS) les fichiers d'administration importants, fichier de mot de passe, fichiers des tables des machines, fichier des groupes ... Lorsqu'on souhaite activer ce service, on crée un domaine de NIS du nom voulu qui sera utilisé par les clients.

Le principe des NIS est de transformer les fichiers d'administration importants et utilisés sur l'ensemble des serveurs en autant de base de données interrogeables via le réseau. On les appelle les maps ou cartes. Ceci permet une centralisation des informations et ainsi une administration plus simple.

Les contreparties de ce système sont des problèmes de fiabilité et de sécurité malgré la mise en place des NIS+ (service NIS sécurisé).

3.7. Le service de messagerie électronique :

3.7.1. Définition :

Ce service est l'un des principaux utilisés dans les réseaux, internet et intranet. L'envoi d'un courrier électronique doit être possible et ne doit pas bloquer l'émetteur si le destinataire n'est pas accessible (réseau défaillant, matériel en panne ou arrêté ...).

C'est pourquoi il a été mis en place un système de spool, qui permet de stocker pendant un certain temps le courrier avant de pouvoir l'émettre ou l'émettre à nouveau. Le courrier utilise le protocole de transport TCP. Si le destinataire peut recevoir le message, le client envoie une copie et attend la réponse du serveur indiquant si le message est bien arrivé. Si tout s'est bien déroulé, la copie dans le spool est détruite. Le destinataire stocke à son tour le message dans une zone de spool. Si l'envoi n'est pas possible, le message est conservé dans le premier spool. Le système le scrute à intervalles réguliers pour déterminer s'il y a des messages à expédier.

Le service de courrier électronique se base sur plusieurs protocoles dont les principaux sont SMTP (Simple Mail Transport Protocol), POP (Post Office Protocol), IMAP (Interactive Mail Access Protocol) ... Des extensions à ces protocoles permettent d'obtenir un meilleur service, comme l'important MIME.

3.7.2. SMTP « Simple Mail Transport Protocol » :

SMTP est le protocole de transport du courrier électronique et utilise TCP/IP. Le port correspondant à SMTP est le port 25. Lorsque vous envoyez un courrier, vous le faites via ce protocole en utilisant des commandes texte sans vous en rendre compte grâce à des interfaces comme Outlook express, ou Netscape.

Mais il est tout à fait possible d'envoyer du courrier sans utiliser les interfaces habituelles mais en se connectant tout simplement sur le port 25 du serveur de courrier. Des mots clés permettent ensuite d'ouvrir la connexion TCP, d'identifier le client (HELO), d'entrer l'adresse de l'expéditeur (MAIL FROM:), du destinataire (RCPT TO:), le texte de votre message (DATA), d'envoyer le tout et de fermer la connexion TCP (QUIT).

3.7.3. POP « Post Office Protocol » :

Ce protocole ne remplace pas SMTP, il offre un autre service. Il utilise un autre port de communication. Ce port est, pour la version 3, POP3, le port 110. On le retrouve dans le fichier des services /etc/services. La version 2 de POP utilise le port 109. Le protocole de communication pour ce service est uniquement TCP.

Ce service permet à un poste client, de récupérer le courrier d'un utilisateur en le transférant localement (sur le disque dur de la machine cliente). Chaque consultation de sa boîte aux lettres détruit les messages, une fois transférés localement du serveur distant. Le fait de détruire les messages sur le serveur de messagerie et de le rapatrier localement pose des problèmes lorsque l'utilisateur travaille sur plus d'un poste client. C'est pourquoi, POP est très utilisé mais a tendance à être remplacé par le service IMAP plus souple.

3.7.4. MIME « Multi-purpose Internet Mail Extensions » :

Cette spécification de format n'est pas un service mais un additif au courrier électronique indépendant des protocoles de transport. Il y a donc homogénéisation des courriers. Ce phénomène permet une compréhension dans tous les cas, indépendamment des plates-formes de travail. MIME encode le message en fonction de son contenu. Avant l'arrivée de MIME, les courriers étaient codés au format ASCII US c'est à dire sur 7 bits. Il ne pouvait y avoir d'accents, MIME introduit deux autres types de codage QP

(Quoted-Printable pour les caractères nécessitant plus de 7 bits) et Base64 (pour tout ce qui est binaire fichier attaché).

Il existe donc des entêtes en fonction du format de message envoyé. Content-Type indique si il y a une image, de la vidéo, de l'audio, etc. Content-Transfer-Encoding indique le type d'encodage utilisé, 7 bits, 8 bits, binary.

3.8. UPnP « Universal Plug and Play » :

Plug and Play (PnP), ou littéralement « on branche et ça marche », caractérise la facilité d'installation d'un nouvel équipement dans un système informatique. Techniquement, le système d'exploitation reconnaît le périphérique que l'on vient d'adjoindre à l'ordinateur, trouve le pilote nécessaire pour le faire fonctionner ou demande de charger ce pilote et lance le travail après avoir réadapté ses paramètres pour tenir compte du nouveau dispositif. L'installation du matériel est ainsi grandement simplifiée par la configuration automatique des paramètres du pilote, tels que l'interruption utilisée, la plage des ports d'entrées/sorties employés, etc.

« Universal Plug and Play » (UPnP) reprend les concepts de PnP pour les étendre à tout le réseau, facilitant la découverte et le contrôle de dispositifs, tels qu'une imprimante réseau, un routeur ADSL ou tout autre équipement périphérique maintenant connecté au réseau local.

L'architecture UPnP permet une mise en réseau poste à poste d'ordinateurs personnels, d'appareils réseaux et de périphériques sans fil. C'est une architecture ouverte, distribuée, basée sur les protocoles TCP/IP, UDP et HTTP.

UPnP permet la communication entre deux dispositifs quelconques sur le réseau local. Parmi ses possibilités :

- Indépendance vis-à-vis des médias et des périphériques : UPnP peut être utilisé sur plusieurs supports (cable, Wi-Fi, Bluetooth).
- Aucun pilote spécifique n'est utilisé, des protocoles communs leurs sont préférés.
- Contrôle par interface utilisateur (UI Control). L'architecture d'UPnP permet le contrôle des dispositifs par une interface utilisateur visible depuis un navigateur web.
- Indépendance vis-à-vis du système d'exploitation et du langage de programmation. Tout système d'exploitation et tout langage de programmation peut être utilisé pour créer des produits UPnP. UPnP ne spécifie ni ne contraint d'API pour les applications exécutées sur des points de contrôle ; les fournisseurs de systèmes d'exploitations peuvent créer les API dont les clients ont besoin.
- Basé sur les technologies internet : entre autres IP, TCP, UDP, HTTP et XML.
- Contrôle applicatif. L'architecture d'UPnP permet également un contrôle par des applications conventionnelles, des programmes.
- Extensibilité. Chaque produit UPnP peut implémenter des services spécifiques à ses périphériques au-dessus de l'architecture de base.

L'architecture UPnP supporte la zéro configuration, le « réseau invisible » et la découverte automatique pour plusieurs catégories de périphériques. Chaque périphérique peut joindre dynamiquement un réseau,

obtenir une adresse IP, annoncer son nom, préciser ses possibilités sur simple demande et interroger les autres périphériques sur leur présence et leurs capacités. Les serveurs DHCP et DNS sont facultatifs et ne sont utilisés que s'ils sont présents sur le réseau. Les périphériques peuvent se déconnecter du réseau automatiquement sans laisser d'informations erronées.

La base du réseau UPnP est l'adressage IP. Chaque périphérique doit avoir un client DHCP et rechercher un serveur DHCP quand il est connecté pour la première fois au réseau. Si aucun serveur DHCP n'est disponible, c'est-à-dire que le réseau n'est pas géré, le périphérique s'assigne lui-même une adresse. Si durant les transactions DHCP, le périphérique obtient un nom de domaine, par exemple, par un serveur DNS, le périphérique devrait utiliser ce nom pour chaque opération réseau sinon il doit utiliser son adresse IP.

4. La sécurité dans un réseau multiplateforme :

Obtenir un système capable d'exécuter différents systèmes d'exploitation pour interopérer peut être une tache ardus, du coup l'accent dans un réseau multiplateforme s'éloigne de l'aspect sécurité, pour se concentré d'abord sur la manière de faire fonctionner le réseau, et sa stabilité. La capacité de partager des plates-formes devient l'objectif.

La plupart des administrateurs réseaux sont formés sur un type particulier de système (Windows, Unix, Mac…), et même dans le cas ou l'administrateur a connaissance générale de la façon d'administrer des plateformes différentes, cela ne signifie pas que cette personne comprend tous les aspects de sécurité. La sécurité est un domaine spécialisé.

Donc pour la sécurité d'un réseau multiplateforme, l'administrateur doit être capable de configurer et de gérer les différents types de systèmes du réseau, et aussi avoir une formation sur la sécurité de ces différents systèmes. Cela inclut à la fois une bonne base dans les concepts généraux de sécurité informatique et spécifiques à chaque système d'exploitation. Cela permet d'utiliser les mécanismes de sécurité intégrée du système d'exploitation particulier à votre avantage, et de savoir quand il est nécessaire de se tourner vers des solutions tierces.

La compétence est basée en partie sur les comportements habituels. Si une personne doit se rappeler les différentes étapes et procédures pour chaque type d'appareils ou systèmes, il y'a un grand risque de confusion et d'erreurs, ce qui rendrai le réseau vulnérable.

C'est pourquoi est il meilleur, avec un réseau hétérogène, d'avoir toute une équipe pour la sécurité, différents membre spécialisé chaque un dans un type de systèmes.

- **Inventaire du réseau**

La première étape pour la sécurisation du réseau est de savoir exactement ce que compose votre réseau, que ce soit le matériels et le logiciel (Systèmes d'exploitations).

Il existe une diversité d'outils qui peuvent être utilisés pour découvrir et documenter les éléments qui composent votre réseau. La clé est d'utiliser un outil qui supporte tous les systèmes d'exploitation qui existent sur votre réseau.

Les plates-formes le plus souvent négligé (et donc laissé non sécurisé ou faiblement sécurisé) sont les utilisateurs ordinateurs portables des téléphones qui ne sont pas connectés en permanence au réseau, ainsi que ceux qui fonctionnent dans des machines virtuelles.

L'ordinateur est peut être équipé de Windows comme OS principal, mais si cet ordinateur est également l'hôte d'une machine virtuelle fonctionnant sous Linux, vous avez à traiter l'OS virtuel comme une autre machine sur le réseau et le sécuriser en conséquence. De même, il ne faut pas oubliez que beaucoup d'utilisateurs de Linux et Mac également exécuter Windows dans un environnement virtualisé parce qu'ils ont besoin de certaines applications de Windows qu'ils ne peuvent pas exécuter toute autre manière.

Il peut y'avoir également des machines, en particulier dans les situations de développement ou d'essais, qui multi-boot des systèmes d'exploitation différents.

Un inventaire complet doit inclure tous le matériel et tout le logiciel qui fonctionne sur votre réseau, même si ce n'est pas sur le réseau à temps plein.

- **Les bases**

Les mêmes concepts de sécurité de base s'appliquent à la fois des réseaux hétérogènes et homogènes, donc il va sans dire que, indépendamment de la plate-forme (s), il faut:

- Installer un bon pare-feu (firewall).
- Utilisez des anti-virus (y compris sur les systèmes non-Windows) et les garder à jour.
- Mettre en œuvre l'audit de sécurité / surveillance pour détecter les infractions tenté
- Désactivant les services inutiles.
- Fermer les ports inutilisés.
- Restreindre l'accès physique aux systèmes.
- Restreindre l'accès administratif pour ceux qui en ont vraiment besoin; sur les systèmes UNIX, restreindre l'accès root pour les terminaux sécurisés
- Mettre en œuvre des autorisations de niveau dossier, sur les systèmes UNIX, la partition du système de fichiers et l'utilisation en lecture seule des partitions pour le stockage des fichiers qui ne changent pas souvent.
- Appliquer des politiques de mot de passe forts.
- Dans les environnements de haute sécurité, il faut exiger une authentification.
- Sur les systèmes UNIX, utilisez SSH (Secure Shell) pour un accès en ligne de commande à distance
- Utilisez le cryptage: pour protéger les fichiers sur le disque, pour protéger les données traversant le réseau, pour protéger le système d'exploitation de l'accès non autorisé.
- Mettre en œuvre une infrastructure à clé publique pour délivrer des certificats numériques.

- **Faire appel a une équipe de l'extérieur**

Une vérification par une tierce personne peut être utile afin d'évaluer et de conseiller sur la mise en œuvre de la sécurité dans un réseau complexe.

Une entreprise qui effectue des vérifications de sécurité extérieure régulière aura un personnel expérimenté dans l'examen des différents types de systèmes et sera former sur les vulnérabilités actuelles et de nouvelles solutions. Ils peuvent effectuer des tests de pénétration pour une évaluation dans le monde réel, et découvrir où se trouvent les vulnérabilités, et ils peuvent vous conseiller sur les moyens les plus efficaces et plus rentables pour combler les lacunes.

Les réseaux multiplateformes présentent des défis de sécurité spéciale, mais les administrateurs doivent apprendre à relever ces défis, car ces réseaux sont de plus en plus adopter. Les mêmes concepts de base s'appliquent indépendamment de la plateforme, mais elles seront réalisées différemment sur différents systèmes d'exploitation.

Conclusion :

Dans ce chapitre nous nous somme familiariser avec le terme multiplateforme dans le domaine des réseaux informatiques. Une étude sur les principales plateformes existantes a été faite, avec les services réseaux qu'elles offrent.

Ce chapitre est une étape important dans notre travail, affin de s'adapter et comprendre le fonctionnement de ces plateformes. Car le résultat final de notre application est de gérer un réseau sur n'importe la quelque de ces plateformes.

Chapitre III

Administration Réseau

Introduction :

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

Ce troisième chapitre a pour but d'introduire les notions d'administration réseau en premier lieu, puis de présenter le protocole SNMP, qui est un protocole majeur dans la gestion réseau.

6. Administration Réseau :

6.1. Définition :

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

L'administration des réseaux informatiques se définit comme étant l'ensemble des moyens mis en œuvre (connaissances, techniques, méthodes, outils) pour superviser, exploiter des réseaux informatiques et planifier leur évolution en respectant les contraintes de coût et de qualité.

La qualité de service se décline sur plusieurs critères, du point de vue de l'utilisateur final, notamment la disponibilité, la performance (temps de réponse), la fiabilité, la sécurité.

Les objectifs de l'administration des réseaux pour l'administrateur sont :

- Optimisation des ressources pour l'utilisation.
- Détection et prévision des erreurs.
- Signalisation des pannes.

- Calculs des statistiques.
- Calculs de facturations à l'utilisation des ressources.
- Le support technique pour les utilisateurs.

6.2. Ressource à gérer :

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

- **La gestion de l'infrastructure réseau :** elle concerne la gestion de tous les éléments du réseau et des logiciels embarqués qui constituent les différents réseaux de l'entreprise. On désigne par élément du réseau chacun des équipements qui sont branchés au réseau, ainsi que les logiciels qui y résidant. Les routeurs, les concentrateurs, les passerelles, les modems, la connectivité, sont les éléments qui constituent l'infrastructure du réseau.

- **La gestion des ordinateurs :** elle concerne tous les aspects relatifs à la gestion des points d'accès au réseau. Elle englobe la gestion des stations terminales, ainsi que de tous les logiciels supportés par ces stations : système d'exploitation réseau, les applications et les services de communication mis à la disposition des usagers.

6.3. Aspects de l'administration :

La supervision peut porter sur plusieurs aspects. Pour simplifier on peut les classer dans trois catégories principales qui sont les suivantes :

- **La Fiabilité :** Il s'agit de l'utilisation la plus courante de la gestion du réseau. Une surveillance permanente de la disponibilité de l'équipement est effectuée, et ce pour détecter la moindre anomalie et de la signaler à l'administrateur.

- **La Performance :** L'administration de performance a pour but de retourner des informations sur le rendement d'un équipement ou d'un service 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, scripts...). Grâce à cette analyse, on va pouvoir diagnostiquer une montée en charge difficile ou même un surdimensionnement de votre bande passante.

- **Le Contenu :** Dans ce dernier cas, on analyse les informations retournées par les éléments surveillés pour détecter, par exemple, la suppression d'un fichier sur un serveur FTP, la modification d'une page Web ou encore la disparition d'un mot clef.

6.4. Principe général :

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

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

Le principe repose donc sur les échanges :

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

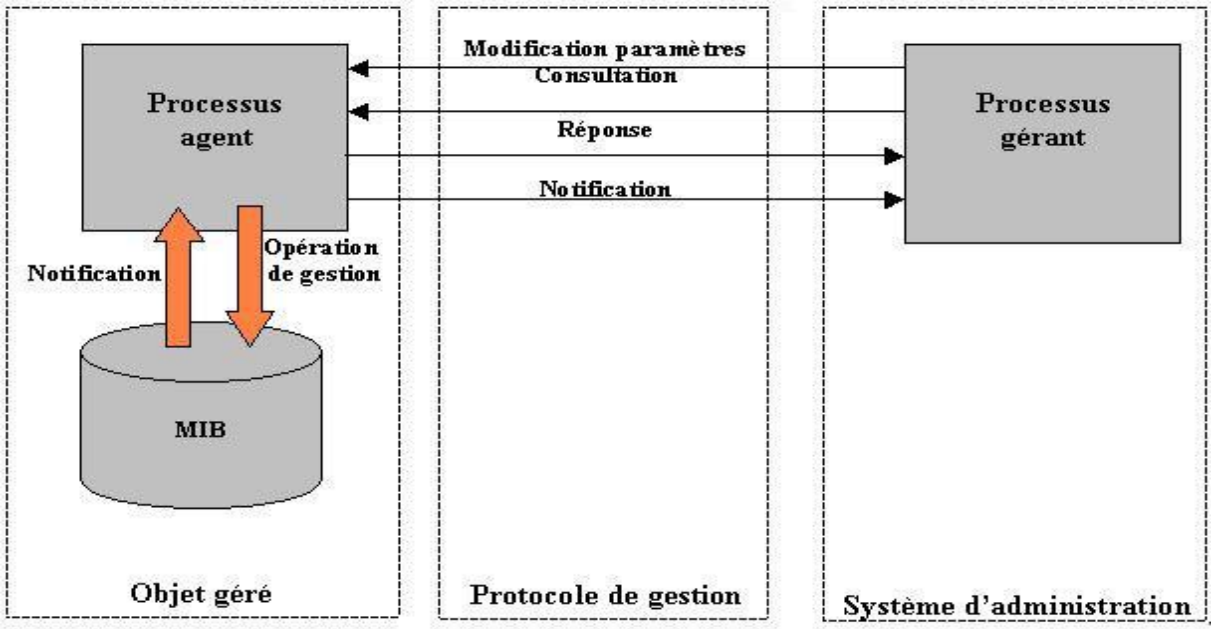


Fig.3.1. Structure fonctionnel d'une administration réseau.

6.5. Architecture d'administration :

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

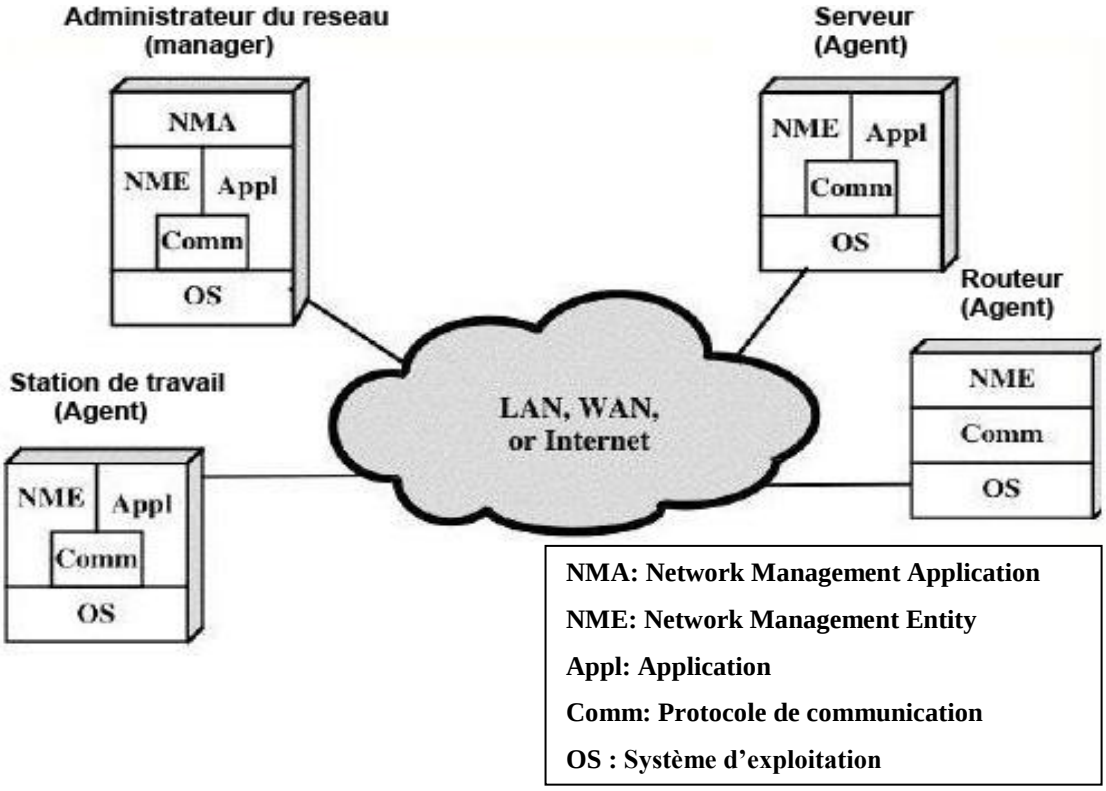


Fig.3.2. Eléments d'un système d'administration de réseau.

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

- Collecter des informations statistiques concernant la communication, les opérations de réseau.
- Stocker les informations localement dans les MIBs.
- Répondre aux commandes de l'entité de contrôle de réseau, inclus : Transmission des informations statistiques à l'entité d'administration du réseau, modification de paramètres, transmission d'informations sur l'état du nœud.

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

7. Protocoles de gestion de réseau SNMP:

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

Il est le protocole le plus utilisé pour gérer des équipements réseau (routeurs, ponts, etc.) et beaucoup de logiciels de gestion de réseau sont basés sur ce protocole.

Actuellement c'est la version 3 de ce protocole qui est en cours de diffusion. Cette version se compose des fonctionnalités nouvelles, en particulier sur le plan de la sécurité.

7.1. Présentation du protocole :

SNMP est un protocole de la famille TCP/IP (Transport control prototcol, Internet protocol), Etant un protocole Internet, il est compatible à toutes plateformes hétérogènes et est installé sur la plupart des matériels réseaux tels que routeurs et commutateurs et peut donc être utilisé sur tous les réseaux de type Internet. Il exploite les capacités du protocole de transport.

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.

Cette technologie se situe entre la couche 4 (Transport) et la couche 7 (application)

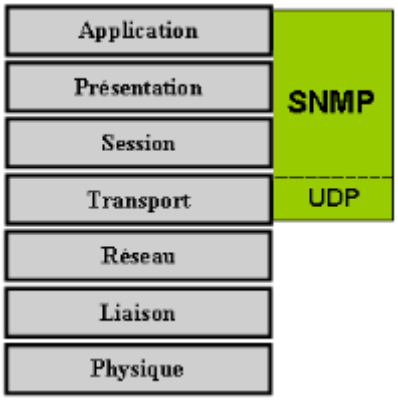


Fig.3.3. SNMP dans la hiérarchie des couches ISO.

7.2. Les composants de base de SNMP :

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

- **Un dispositif administré :** est un nœud réseau qui contient un agent SNMP et qui réside sur un réseau administré. Les dispositifs administrés collectent et conservent des informations d'administration, et rendent ces informations disponibles aux NMS à l'aide de SNMP. Les dispositifs administrés, parfois appelés « éléments réseau », peuvent être des routeurs, des serveurs d'accès, des commutateurs, des ponts, des hubs, des hôtes ordinateurs ou des imprimantes.
- **Un agent :** est un module logiciel d'administration réseau qui réside sur un dispositif administré. Un agent possède une connaissance locale des informations d'administration et traduit celle-ci en un format compatible avec SNMP.

- **Les MIBs :** Ce sont des bases de données similaires à des bibliothèques d'objets se trouvant dans chaque dispositif administré, nous renseignant sur tous les types de données en rapport avec l'activité du réseau. Nous la détaillerons un tard dans ce chapitre.
- **Un NMS :** ou systèmes de gestion de réseau (network management system notés NMS): C'est une console au travers de laquelle les administrateurs peuvent réaliser des tâches d'administration, exécutent des applications qui surveillent et contrôlent des dispositifs administrés. Un NMS fournit l'essentiel des ressources de traitement et mémoires nécessaires à l'administration réseau. Il peut y avoir un ou plusieurs NMS sur un réseau administré.

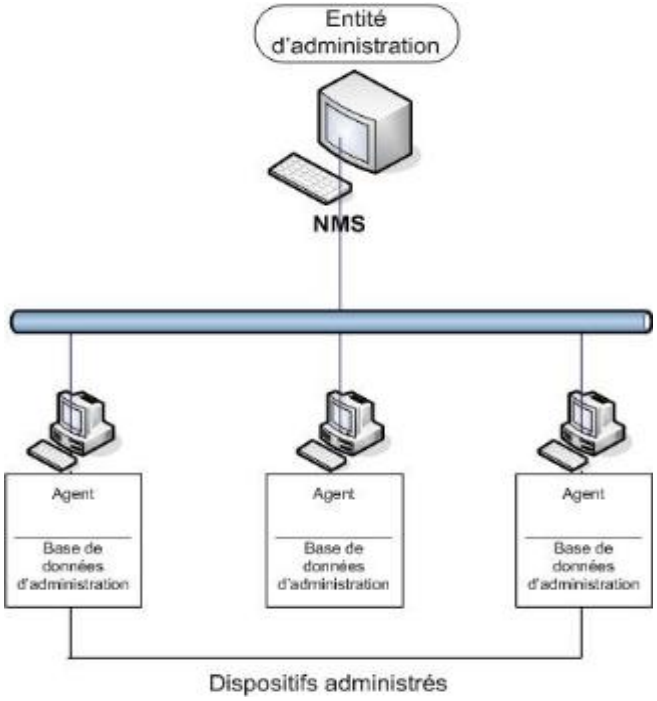


Fig.3.4. Schémas de gestion de réseau avec SNMP

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

7.3. Les opérations :

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

7.3.1. GetRequest :

Cette requête permet aux stations de gestion (manager) d'interroger les objets gérés et les variables de la MIB des agents. La valeur de l'entrée de la MIB (nom) est passée en paramètre. Elle permet d'accéder à une variable précise.

7.3.2. GetNextRequest :

Cette requête permet aux stations de gestion de recevoir le contenu de l'instance qui suit l'objet nommé (passé en paramètre) dans la MIB. Cette commande permet en particulier aux stations de gestion de balayer les tables des MIB. Elle permet d'accéder à plusieurs variables simultanément.

7.3.3. GetResponse:

A chaque envoie d'un message à l'exception de TRAP, un message de réponse est retourné. Ils ont chacun une signification bien distincte :

- GET-response : tout s'est bien passé, l'information est transmise.
- NoSuchObject' : aucune variable n'a été trouvée.
- NoAccess : vous ne disposez pas des bons droits d'accès.

7.3.4. SetRequest :

Cette requête permet aux stations de gestion de modifier une valeur de la MIB. Elle permet par exemple à un manager de mettre à jour une table de routage. SetRequest provoque aussi le retour de GetResponse.

7.3.5. Les Alarmes TRAP :

Lorsqu'un périphérique entre dans un état anormal, l'agent SNMP prévient le gestionnaire SNMP par le biais d'un Trap SNMP.

7.3.6. InformRequest : (version 2 et version 3 de SNMP)

Le but de l'InformRequest est réellement de faciliter la communication d'information entre les stations de gestion de réseau. L'agent SNMP sur un NMS peut choisir d'informer d'autres NMS d'une certaine information en envoyant une InformRequest.

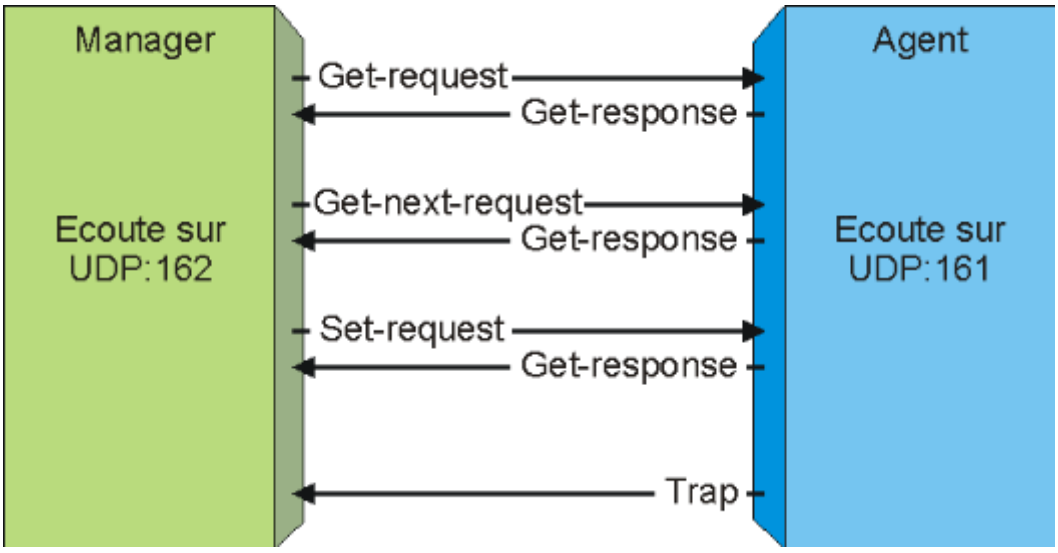


Fig.3.5. Operations SNMP.

❖ **Format de message SNMP :**

Une requête SNMP est construite de la façon suivante :

Fig.3.6. Format de message SNMP.

- **V: version SNMP (v1, v2, v3)**
- **C : type de communauté (public ou private)**
- **D : donnée (requête: GET, GET_NEXT, TRAP ...)**

➢ **Communauté :**

Un agent SNMP est plus ou moins finement paramétrable, suivant le système. Il est possible, par exemple de créer des groupes de sécurité qui auront accès en lecture seule, d'autres en lecture/écriture, d'autres encore en lecture seule, mais sur certaines branches seulement.

Chaque groupe devra disposer d'une sorte de mot de passe, appelé "community". En général, la communauté "public" est celle qui a le droit de lecture sur les informations non sensibles.

7.4. Structure SMI (Structure Of Management Information) :

La structure SMI définit les règles de description des informations de la MIB, et permet d'identifier de façon unique un objet de la MIB géré par un agent SNMP. Chaque objet possède un identificateur unique ou OID (Object ID).

La SMI définit le cadre dans lequel une MIB peut être définie ou construite. En d'autres termes, elle définit les composants d'un module de MIB et le langage formel pour décrire les objets gérés.

La SMI spécifie que tous les objets gérés doit avoir un nom, une syntaxe, et un codage. Le nom est caractérisé par l'OID. La syntaxe définit le type de données de l'objet géré (par exemple, entier ou une chaîne). Un sous-ensemble des définitions de ASN.1 sont utilisées pour la syntaxe SMI. Le codage décrit comment l'information associée à l'objet géré est formaté comme une série d'éléments de données pour la transmission sur le réseau.

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

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

❖ **ASN.1 :**

ASN.1 est un langage formel présentant un double intérêt : Une notation rigoureuse facilement compréhensible par l'homme et aussi bien par la machine. Son haut degré de précision écarte tout risque d'erreur et contribue à harmoniser la mise en œuvre des protocoles de communication. En effet, une standardisation est nécessaire car il est tout à fait possible qu'une même information puisse apparaitre de façon incompatible d'un environnement à un autre.

ASN.1 est utilisée pour décrire le format des messages SNMP lors des communications entre les stations gérées et les stations gérantes. Ce langage intervient donc dans la transmission et la réception des données mais, plus encore, il intervient aussi dans la syntaxe des objets SNMP (ObjectSyntax), en définissant le nom et le type des variables de la MIB,

La syntaxe d'un objet SNMP, sous ASN.1 peut entrer dans une des catégories suivantes :

- Les types de données dits simple : Integer, Octet String…
- Les types de données dit « simplement-construits » : Les listes, les tableaux
- Les types de données applicatifs : IpAdress, PhysAddress, Counter, Gauge, TimeTicks.

7.5. La structure de données MIB :

7.5.1. Définition :

La MIB est une base de données gérée par un agent SNMP regroupant les objets gérés en respectant les règles SMI. Elle possède une structure d'arbre similaire à celle employé dans le DNS (Domain Name System). On retrouve une racine à partir de laquelle on référencie de façon absolue un objet par son OID (nœud de l'arbre).

Un objet administré (parfois appelé un objet MIB, un objet ou une MIB) est l'une des nombreuses caractéristiques possibles d'un dispositif administré. Des objets administrés sont composés d'une ou plusieurs instances d'objets, lesquelles sont essentiellement des variables.

Un identificateur d'objet (ou ID d'objet) identifie de manière unique un objet administré dans la hiérarchie de la MIB.

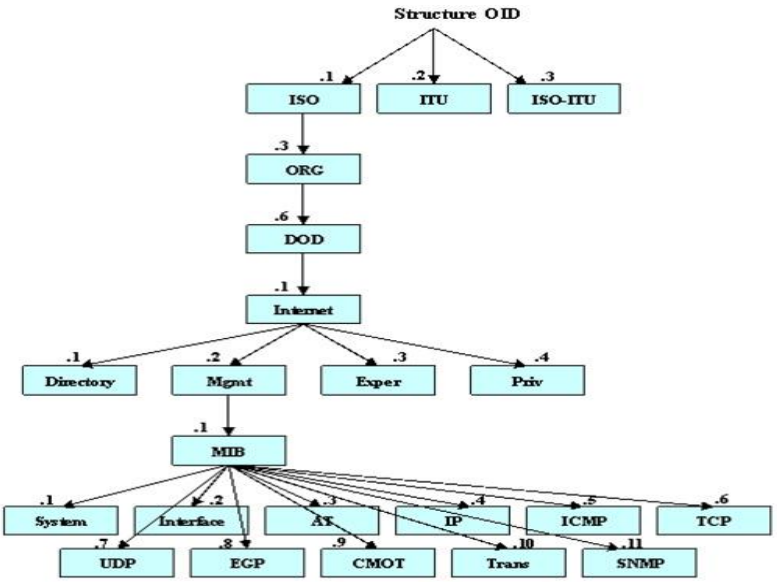


Fig.3.7. Structure de la MIB.

- **System :** Description de toutes les entités gérées
- **Interfaces :** Interface de données dynamiques ou statiques
- **at. (adresse translation) :** Table d'adresses IP pour les correspondances d'adresses MAC
- **Ip :** Statistiques du protocole IP, adresse cache et table de routage
- **Icmp :** Statistiques du protocole ICMP
- **Tcp :** Paramètres TCP, statistiques et table de connexion
- **Udp :** Statistiques UDP
- **Egp :** Statistiques EGP, table d'accessibilité
- **Snmp :** Statistiques du protocole SNMP

Examinons quelques éléments de données de la MIB pour en clarifier le contenu.

Variable MIB	**Catégorie**	**Signification**
sysUpTime	Système	Durée écoulé depuis dernier démarrage
ifNumber	Interfaces	Nombre d'interfaces réseau
ifMtu	Interfaces	MTU d'une interface particulière
ipDefaultTTL	Ip	Valeur utilisée dans le champ TTL
ipInReceives	Ip	Nbre de datagrammes reçus
ipForwDatagrams	Ip	Nbre de datagrammes acheminés
ipOutNoRoutes	Ip	Nbre d'erreurs de routage
ipReasmOKs	Ip	Nbre de datagrammes réassemblés
ipFragOKs	Ip	Nbre de datagrammes fragmentés
ipRoutingTable	Ip	Table de routage IP
icmpInEchos	Icmp	Nbre de demandes d'echo ICMP reçues
tcpMaxConn	Tcp	Nbre maxi de connexions TCP autorisées
tcpInSegs	Tcp	Nbre de segments reçus par TCP
udpInDatagrams	Udp	Nbre de datagrammes UDP reçus

Fig.3.8. Exemple de variable MIB.

7.5.2. Description d'un objet de la MIB :

Un fichier de MIB contient des définitions de la structure de l'arbre global et des définitions d'objets de type feuille qui vont permettre la collecte d'informations. La définition d'un objet de la MIB avec la norme SMI V1 est réalisée au moyen de 5 champs :

Champ	Description
OBJECT-TYPE	Ce champ fournit le nom de l'objet, ce nom est unique et permettra de collecter des informations en utilisant la notation nominale.
SYNTAX	Ce champ définit le type de valeurs gérées par l'objet : Les principales valeurs sont :Integer, octect String, ipAddress, PhysAddress, counter, et TimeTicks. Avec la version 2 du SMI, il est possible de définir de nouvelles syntaxes à partir des syntaxes de base. Une nouvelle syntaxe utilise le mot clef TEXTUAL CONVENTION.
ACCESS	Ce champ indique comment cet objet peut être adressé. Les valeurs possibles pour ce champ sont : ➢ Read-only : lecture seule. ➢ Read-write : lecture écriture. ➢ Write-only : en écriture seulement. ➢ Not-accessible : ne peut pas être adressé.
STATUS	Ce champ indique le statut de l'objet par rapport à la norme définie par la MIB. La MIB va définir un ensemble d'objets dont certains devront être impérativement implémentés au niveau de l'agent pour répondre à la norme tant dit que certains objets ne sont pas obligatoirement implémentés au niveau de l'agent en fonction du statut de l'objet défini dans la MIB. Les valeurs possibles pour ce champ sont : ➢ Mandatory : Cet objet doit impérativement être implémenté au niveau de l'agent pour que l'agent puisse être compatible avec la norme. ➢ Optional : Cet objet n'a pas l'obligation d'être implémenté au niveau de l'agent. ➢ Obselete : cet objet n'est plus obligatoirement implémenté sur les agents de nouvelles générations.
DESCRIPTION	Ce champ contient une information dans un format texte décrivant l'usage ou l'utilisation de la valeur associée à l'objet. Le texte est encadré par des guillemets.

Fig.3.9. Tableau des champs de définition d'un objet MIB en SMI V1

➢ **Exemple :** Définition de l'objet SysName avec SMI V1

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

7.5.3. Extension de la MIB :

Au bout d'un moment, les variables choisies pour la Mib (puis la mib-2) se sont avérées insuffisantes pour plusieurs applications. On va donc trouver deux autres types de Mib que sont les private Mib et les Mib R-MON (Remote network Monitoring).

Les privates Mib, permettent aux entreprises de rajouter des variables pour une implémentation particulière des agents SNMP. Cela leur permet d'ajouter de nouvelles variables en fonctions des applications qu'elles veulent.

Les Mib R-MON permettent par exemple de placer des agents SNMP sur des supports physiques. Sur un câble, on peut connecter une sonde R-MON qui va enregistrer tout ce qui se passe et que l'administrateur pourra interroger pour avoir des informations sur les collisions, les débits à un endroit précis.

7.6. Techniques de supervision avec SNMP :

SNMP peut être utilisé de deux manières distinctes : le polling et les traps.

7.6.1. Le Polling :

Le polling consiste simplement à envoyer une requête à intervalles réguliers pour obtenir une valeur particulière. Cette technique est appelée « vérification active ». Vous pouvez, par programme ou script, vérifier si les valeurs sont correctes. Si la requête échoue, il est possible qu'il y ait un problème avec le périphérique. Cependant, vu que le SNMP s'appuie sur UDP, il est conseillé de réitérer la requête pour confirmer le problème (surtout dans le cas d'une vérification au travers d'Internet).

7.6.2. Les traps :

Les traps consistent à faire de la vérification passive ; en gros, on configure l'agent SNMP pour qu'il contacte un autre agent SNMP en cas de problème. C'est-à-dire que l'on peut configurer un périphérique réseau (comme un routeur) pour qu'il envoie un trap SNMP lors de certains événements. Par exemple, le routeur peut envoyer un trap lorsqu'il détecte que la ligne est coupée (down). Quand un événement trap apparait, l'agent sur le périphérique va envoyer le trap vers une destination pré-configurée communément

appelé trap host. Le trap host possède son propre agent SNMP qui va accepter et traiter les traps lorsqu'ils arrivent. Le traitement des traps est effectué par des trap handlers. Le handler peut faire ce qui est approprié pour répondre au trap, comme envoyer un courriel d'alerte par exemple.

7.7. Evolution des versions de SNMP :

Plusieurs version du protocole on vue le jour à savoir :

- SNMPv1 : Ceci est la première version du protocole. La sécurité de cette version est triviale, car la seule vérification qui est faite est basée sur la chaîne de caractères "community ".
- SNMPsec : Cette version ajoute de la sécurité au protocole SNMPv1. La sécurité est basée sur des groupes. Très peu ou aucune entreprise n'a utilisé cette version qui est maintenant largement oubliée.
- SNMPv2p : Beaucoup de travaux on été exécutés pour faire une mise à jour de SNMPv1. Ces travaux ne portaient pas seulement sur la sécurité. Le résultat est une mise à jour des opérations du protocole, des nouvelles opérations, des nouveaux types de données. La sécurité est basée sur les groupes de SNMPsec.
- SNMPv2c (expérimental): Cette version du protocole est appelé "community stringbased SNMPv2". Ceci est une amélioration des opérations de protocole et des types d'opérations de SNMPv2p et utilise la sécurité par "community " de SNMPv1.
- SNMPv2u (expérimental): Cette version du protocole utilise les opérations, les types de données de SNMPv2c et la sécurité basée sur « USM » (qu'on l'enverra par la suite).
- SNMPv3 (standard actuel): Cette version comprend une combinaison de la sécurité basée sur « USM » et les types et les opérations de SNMPv2p, avec en plus la capacité d'utiliser les " proxies ". La sécurité est basée sur ce qui se trouve dans SNMPv2u et SNMPv2c.

7.7.1. SNMPv1 :

SNMP version 1 (SNMPv1) est la première implémentation du protocole SNMP. Elle fonctionne dans le cadre des spécifications de SMI (Structure of Management information). SNMPv1 opère sur des protocoles, tels que UDP, IP, OSI CLNS (ConnectionLess Network Service), AppleTalk DDP (Datagram-Delivery Protocol) et Novell IPX (Internetwork Packet Exchange). SNMPv1 est largement utilisé et fait office de protocole de référence pour l'administration réseau dans la communauté internet.

Elle encore la version la plus utilisée. Malgré les autres versions, aucune d'entre elles n'a jamais été adoptée comme standard. La version 3 est actuellement en voie d'être adoptée. On place la valeur zéro dans le champ version pour SNMPv1, et la valeur 3 pour SNMPv3.

- **Faiblesse de SNMPv1 :**

Une des plus grandes faiblesses du protocole SNMPv1 est l'absence d'un mécanisme adéquat pour assurer la confidentialité et la sécurité des fonctions de gestion. Les faiblesses comprennent aussi l'authentification et le cryptage, en plus de l'absence d'un cadre administratif pour l'autorisation et le contrôle d'accès.

7.7.2. Les améliorations de SNMPv2c :

SNMPv2c a introduit quelques nouveaux types, mais sa nouveauté majeure est l'opération GETBULK, qui permet à une plate forme de gestion, de demander en bloc de plusieurs variables consécutives dans la MIB de l'agent. Généralement, on demande autant de variables que l'on peut mettre dans un paquet SNMP. Ceci règle un problème majeur de performance dans SNMPv1. Avec la version 1, la plate forme est obligée de faire un GETNEXT et d'attendre la réponse pour chaque variable de gestion.

7.7.3. SNMPv3 :

Cette nouvelle version du protocole SNMP vise essentiellement à inclure la sécurité des transactions. La sécurité comprend l'identification des parties qui communiquent et l'assurance que la conversation soit privée, même si elle passe par un réseau public.
Cette sécurité est basée sur 2 concepts :

7.7.3.1. **User Security Module (USM) :**

Trois mécanismes sont utilisés. Chacun de ces mécanismes a pour but d'empêcher un type d'attaque.

- **L'authentification :** Empêche quelqu'un de changer le paquet SNMPv3 en cours de route et de valider le mot de passe de la personne qui transmet la requête.
- **Le cryptage :** Empêche quiconque de lire les informations de gestions contenues dans un paquet SNMPv3.
- **L'estampillage du temps :** Empêche la réutilisation d'un paquet SNMPv3 validé à la réception d'être retransmis par quelqu'un.

7.7.3.2. VACM (View Access Control Model):

Permet le contrôle d'accès à la MIB. Ainsi on a la possibilité de restreindre l'accès en lecture et/ou écriture pour un groupe ou par utilisateur.

7.8. D'autres protocoles de gestion réseau :

- **Le WMI :**

WMI ou Windows Management Instrumentation, contrairement aux autres protocoles n'est compatible qu'avec le système d'exploitation Windows. Il permet à tout administrateur de contrôler, gérer, d'installer, collecter des informations localement comme à distance.

De manière générale, il étend les possibilités de base d'administration de Windows. Cependant, bien qu'il puisse faire office d'outil de monitoring il n'est pas recommandé pour cet usage. Ce protocole peut se montrer assez gourmand.

- **Le CMIP :**

CMIP ou Common Management Information Protocol, un standard OSI qui est utilisé avec le protocole CMIS, Common Management Information Services pour le monitoring et les contrôles de réseaux hétérogènes.

CMIP a été proposé comme remplacement au protocole beaucoup moins sophistiqué qu'était SNMP mais n'a pas rencontré un franc succès. CMIP a la particularité d'offrir une meilleure sécurité et est capable de reporter des conditions inhabituelles d'un réseau.

3. Quelques Systèmes de gestion réseau existant :

Le marché de la supervision informatique déborde de logiciels de monitoring, il en existe une diversité, quelqu'un sont payants et d'autres font parti du monde libre et on peut même on trouver des Open Sources.

3.1. Les logiciels payants :

Les gros éditeurs logiciels ont rapidement compris que la supervision était une ressource clé pour les entreprises qui, de plus en plus, utilisent des systèmes informatiques et ont donc besoin d'une disponibilité toujours plus grande de leur infrastructure informatique.

Par conséquent, la supervision est un domaine dans lequel les sociétés n'hésitent pas à investir depuis quelques années. Ayant rapidement compris cela, les gros éditeurs logiciels sont donc très vite entrés dans la course aux logiciels de supervision.

Aujourd'hui, la majorité des gros éditeurs logiciels propose des outils de supervision. On retrouve, parmi les plus connus : HP : la gamme Openview (NNM, OVO, ...); IBM : Tivoli ; BMC : Patrol ; Computer ; Associates : Unicenter TNG.

Ces outils possèdent tous leurs avantages et inconvénients face à la concurrence. Et bien entendu, tous ont également le même défaut, à savoir: leurs prix coûteux.

Cette constatation faite, il est alors logique de voir de plus en plus de sociétés aujourd'hui regarder du côté du logiciel libre, où les projets commencent depuis quelques années à devenir de plus en plus professionnels et suivis.

Dans ce qui va suivre, nous présenterons deux leaders des logiciels payants de supervision: HP OpenView et IBM Tivoli.

3.1.1. HP OpenView :

HP OPEN VIEW est un outil de supervision reconnu sur le marché. Son principal avantage est la centralisation des informations sur un seul poste. Il a pour rôle de gérer et de surveiller entre autre les infrastructures et services réseaux. Ce logiciel est donc destiné aux moyennes et grandes entreprises qui souhaitent avoir une vue globale de leur réseau et de son état.

- **Principe de fonctionnement :**

HPOV est un produit qui propose, aux personnes chargées de l'exploitation des systèmes d'information, les fonctionnalités suivantes :

- Une vue globale du système informatique.

- Un contrôle homogène des différents composants du système informatique.
- Une vision des incidents et leur impact (gestion des alertes).

La plate-forme HP OpenView est composée principalement de « OVOW » (OpenView Opération for Windows) qui regroupe entre autre d'une base SQL SERVER. Le logiciel est assorti d'un serveur HTTP Apache pour l'accès aux interfaces Web des outils.

- **La console OVOW :**

La console OVOW permet à l'opérateur d'avoir une vision globale de son réseau informatique. L'opérateur peut visualiser d'un seul coup d'œil la disponibilité globale d'un service, la gravité d'une erreur, la raison principale de cette erreur.

- **Les nœuds :** Pour OVOW, chaque client est un « nœud ». Un nœud correspond donc à un élément surveillé (un nœud peut être un serveur, un photocopieur ...).
- **Les agents OVOW :** OVOW a besoin d'un agent pour pouvoir surveiller un élément. Un agent OVOW est un programme que l'on déploie à partir du serveur HPOV sur un nœud. On doit spécifier à cet agent un domaine cible (Que doit-on surveiller ?).

3.1.2. IBM Tivoli Monitoring :

Les solutions IBM Tivoli Monitoring sont conçues pour une meilleure gestion des applications en ligne essentielles à l'entreprise en :

- Surveillant de manière proactive les ressources système vitales.
- En détectant efficacement les goulets d'étranglement et les problèmes potentiels.
- En répondant automatiquement aux événements.

En s'appuyant sur les meilleures pratiques pour identifier et résoudre les problèmes d'infrastructure, IBM Tivoli Monitoring a été conçu pour aider les opérateurs à surveiller et gérer les matériels et logiciels, comprenant les systèmes d'exploitation, les bases de données et les applications sur des environnements répartis.

Ce moniteur de supervision se classe parmi les leaders du domaine, puisque il offre de nombreux avantages. En effet, il :

- Surveille de manière proactive les composants de votre infrastructure à la demande, en vous aidant à isoler et prévenir rapidement les problèmes de performance.
- Visualise les mesures de performances historiques et en temps réel sous forme de tableaux et graphiques, avec en plus des conseils spécialisés et des actions automatiques au sein d'IBM Tivoli Enterprise Portal.
- Consolide la surveillance à l'aide d'une seule console de travail personnalisable.

- Fournit des outils de surveillance puissants et personnalisables à davantage d'opérateurs nécessitant beaucoup moins de compétences et formation en programmation pour déployer le produit.
- Aide à réduire les coûts opérationnels informatiques globaux en simplifiant l'installation et la configuration, et en déployant des règles allégées avec des fonctionnalités de surveillance automatique.
- Effectue automatiquement le suivi de l'état des principaux composants de votre environnement informatique complexe et reçoit des alertes uniquement en cas d'incident.
- Aide à optimiser l'offre de services informatiques en intégrant des produits de gestion et des processus informatiques pour stimuler les performances.
- Aide à optimiser le temps de réalisation en simplifiant l'installation et la surveillance.

3.2. Les offres du monde libre :

Depuis une dizaine d'années déjà, plusieurs projets de supervision ont vu le jour au sein de la communauté du logiciel libre. Il suffit pour cela d'aller faire une simple recherche sur le Net pour se rendre compte de la multitude de projets émergeants autour de la supervision système et réseau.

Nous présenterons ainsi, les systèmes de monitoring plus populaires.

3.2.1. NAGIOS :

Nagios, le successeur de Netsaint, est un logiciel de monitoring et de supervision libre sous licence GPL. Il offre une solution de surveillance efficace dans un système informatique complexe. Il permet de surveiller le bon fonctionnement des services d'une ou plusieurs machines dans un réseau hétérogène. Il est écrit en C et fonctionne grâce à un ensemble de plugins (qui eux peuvent être écrits dans n'importe quel langage).

Prévu à l'origine pour fonctionner sous Linux, Nagios a été modifier pour fonctionner également sous les autres systèmes Unix, et Windows

Plusieurs améliorations ont été apportées à Nagios pour qu'il devienne un partenaire simple à utiliser et remarquablement fiable et efficace.

❖ **Fonctionnalités de Nagios :**

Nagios offre à l'utilisateur plusieurs fonctionnalités, à savoir **:**

- Surveillance des services réseaux (SMTP, POP3, HTTP, DHCP, etc.).
- Surveillance des ressources des hôtes (charge processeur, utilisation des disques, etc.).
- Permettre aux utilisateurs de développer facilement leurs propres vérifications de services grâce à son système de plugins.
- Paralléliser la vérification des services.
- Possibilité de définir la hiérarchie du réseau en utilisant des hôtes "parents", ce qui permet la détection et la distinction entre les hôtes qui sont à l'arrêt et ceux qui sont injoignables.

- Possibilité de définir des gestionnaires d'évènements qui s'exécutent pour des évènements sur des hôtes ou des services, pour une résolution proactive des problèmes.
- Interface web optionnelle, pour voir l'état actuel du réseau, notification et historique des problèmes, fichiers log, etc.
- Une interface permettant l'intégration simple de plugins.
- De prévenir par email ou par toute autre méthode personnalisée en cas de problème.
- Déclencher des procédures personnalisées pour résoudre les problèmes.
- La consultation des différents événements et données collectés via une interface web.
- Archivage automatique des données collectées.

Dans la figure suivante, les fonctionnalités de Nagios se résument **:**

Fig.3.10. Fonctionnalités de Nagios.

Cependant, pour pallier aux éventuelles lacunes du Nagios, des plugins peuvent être ajoutés qui sont personnalisés selon les besoins d'utilisation, pour accomplir ou améliorer d'autres services et tâches.

❖ **Architecture de Nagios :**

Nagios est un programme modulaire de telle sorte que son évolution puisse être facile, il se compose principalement de trois parties :

- **L'ordonnanceur :** C'est le moteur de l'application qui s'occupe de l'ordonnancement des tâches de supervision.
- **L'interface Web :** qui permet d'avoir une vue d'ensemble du système informatique et des possibles anomalies, Nagios s'appuie sur simple serveur Web tel apache.
- **Les sondes :** Les sondes de Nagios (Plugins) sont de petits scripts ou programmes. Ces minis programmes que l'on peut compléter selon nos besoins pour superviser chaque tache.

La figure suivante montre cette architecture:

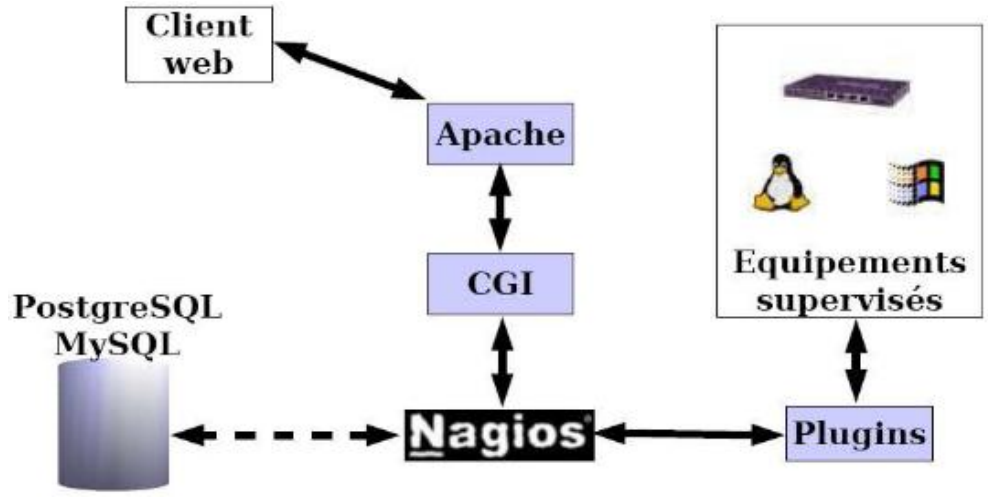


Fig.3.11. Architecture de Nagios.

3.2.2. Autres logiciels libres :

❖ **MRTG :**

MRTG (Multi Router Traffic Grapher) est un outil de supervision du trafic réseau. Il génère des pages HTML de représentation en temps réel du trafic réseau. Le logiciel prend toute sa dimension comme produit fini, mais également comme brique spécialisée d'une solution intégrée plus large. Il s'intègre notamment parfaitement dans la solution de supervision de Nagios. Son architecture logicielle permet l'intégration sur des plates-formes et composants hétérogènes.

❖ **CACTI :**

CACTI est un logiciel de supervision réseau les plus recent. Il peut-être considéré comme un successeur à MRTG. Cacti permet de représenter graphiquement divers statuts de périphériques réseau utilisant SNMP ou encore grâce à des scripts (Bash, PHP, Perl, VBs...) pour avoir par exemple l'espace disque restant ou bien la mémoire utilisée, la charge processeur ou le ping d'un élément actif. Les données sont récoltées auprès des différents agents SNMP (ou auprès des scripts locaux) grâce à un script php. Pour de meilleures performances un exécutable, nommé cactid, peut également effectuer les interrogations.

❖ **ZENOOS :**

ZENOOS représente une alternative à des plates-formes de supervisions comme Tivoli ou OpenView, notamment pour les entreprises de taille moyenne. Il assure des fonctions de découverte, d'inventaire, de supervision de la disponibilité, de gestion de performance, de gestion des évènements et des alertes qui peuvent être envoyées par email.

Le produit s'interface avec de nombreux utilitaires de supervision et d'administration open source. Zenoss est disponible en version GPL ou commerciale (avec support).

Conclusion :

Dans tous ce qui vient d'être exposé à travers ce chapitre on a constaté les potentialités immenses offertes par le protocole SNMP grâce a sa simplicité de mise en œuvre, sa stabilité, sa souplesse. Grace à ce protocole la gestion des réseaux es devenue plus simple et plus performantes qu'auparavant.

Chapitre IV

Conception

Introduction :

Notre travail consiste à concevoir et à réaliser une plate forme d'administration réseau basé sur le protocole SNMP. Après avoir pris connaissances des concepts d'administration réseau et du protocole SNMP, dans cette partie nous détaillerons le coté conception de la plate forme.

Nous rappelons que notre application doit assurée une gestion des équipements du réseau a partir de n'importe quel point de connexion possédant les droit d'accès nécessaires.

2. Le cahier des charges :

- **Définition :**

Le cahier des charges trace les objectifs à atteindre et définit les différentes fonctions et taches qui seront prêtes à être exécuter lors de la fin de la réalisation de l'application.

Pour notre projet, l'application sera représentée sous forme d'une fenêtre contenant plus onglets, et derrière chaque onglet se cache une, ou un ensemble de fonctionnalités.

En résumé, la plate forme à réaliser doit permettre les fonctions suivantes :

- Scanner le réseau et fournir une liste des machines qui le compose.
- Pouvoir récupérer un nombre informations sur chaque machine avec le protocole SNMP, et éventuellement les modifier si la donnée est modifiable.
- Implémentation des requêtes du protocole SNMP.
- Un service d'alarme qui indique un disfonctionnement sur une machine du réseau.
- Un service de statistique qui va fournir des statistiques sur les flux entrant et sortant.

3. Architecture générale :

La figure suivante donne un aperçu global de l'ossature de l'application à développer.

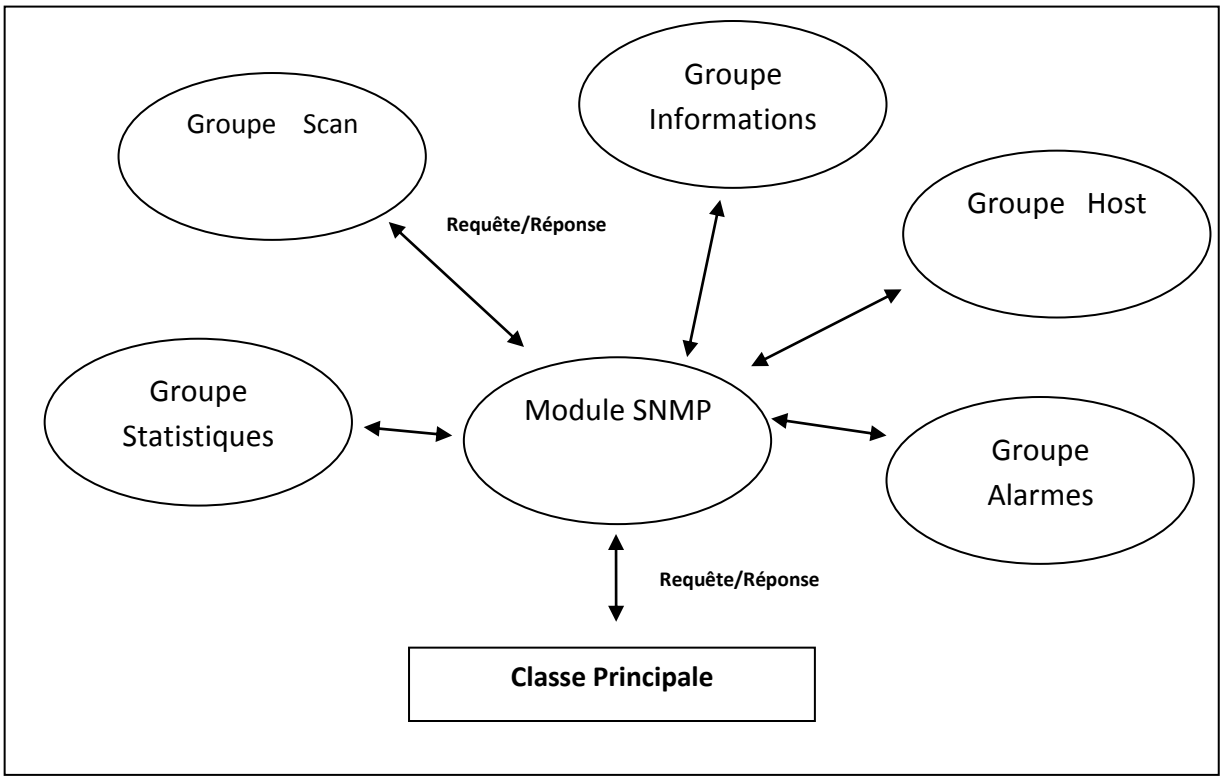


Fig.4.1. Architecture de la plate forme.

4. Etude de l'environnement de travail :

L'application est fondée sut trois axes principaux qui sont :

- Une interface graphique, qui est la classe principale.
- Un module d'interrogation SNMP.
- Plusieurs groupes, dont chaque un a une fonction bien précise.

4.1. La classe principale :

La classe principale représente l'interface graphique de l'application, elle permet de consulter les différents groupes, et de récupérer leurs résultats, et cela grâce au module d'interrogation SNMP qui sert d'intermédiaire.

Elle permet notamment d'avoir une vision globale du réseau et de chacun de ses éléments qui le compose graphiquement.

4.2. Module d'interrogation SNMP :

Cette partie de l'application a pour rôle d'interroger une machine, et de récupérer les données de gestion nécessaire à notre application et les transmettre a la classe principale, de scanner le réseau et de récupérer les données de base de chaque éléments de ce dernier.

Pour notre application le protocole SNMP, n'est pas exploitée à 100%, on a choisit d'implémenter les groupes suivants :

4.2.1. Le groupe Scan :

Cette fonctionnalité a pour objectif de lister les machines actives dans un intervalle d'adresses IP paramétrable et de donner des informations sur les éléments découverts, afin de savoir si une machine est bien active, nous avons choisi d'utilisé un Ping java a temps de réponse paramétrable, ceci après avoir testé d'autres méthodes telle que la connexion TCP.

En effet le choix du Ping java offert à partir de la version 5 de java (dénommée tigre) est du à la faiblesse de temps de réponse nécessaire pour avoir la disponibilité d'une machine. On peut dire que c'est comme un Ping système mais seulement avec 2 paquets envoyés. Le résultat de la disponibilité de la machine est presque en temps réel a quelque seconde prés.

Le résultat du scan est afficher dans une table, avec une colonne qui affiche si le service SNMP et bien activer, en sélectionnant une machine découvert on peut accéder a ces détails si évidement le service SNMP est active pour cet élément.

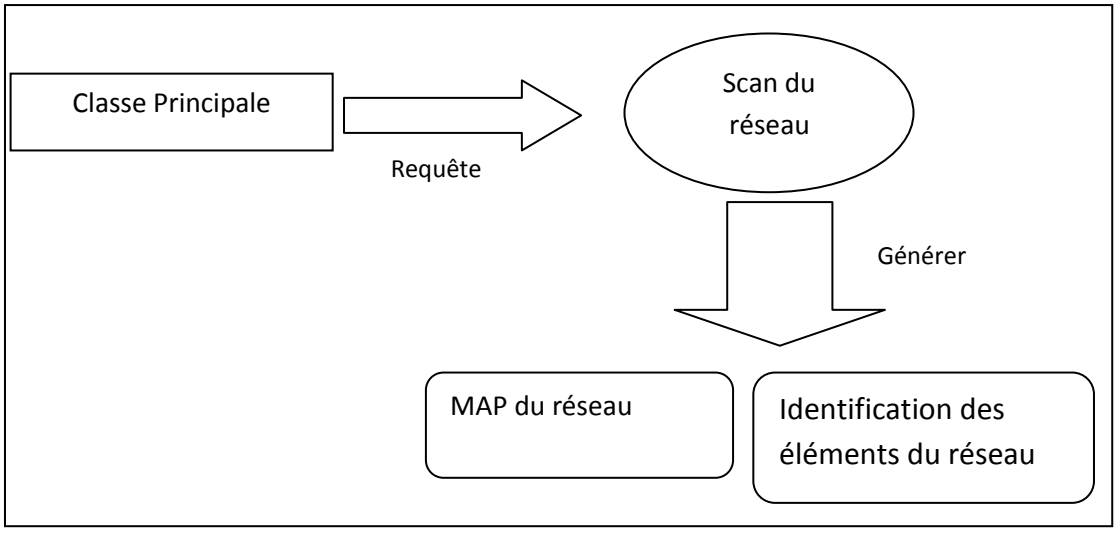


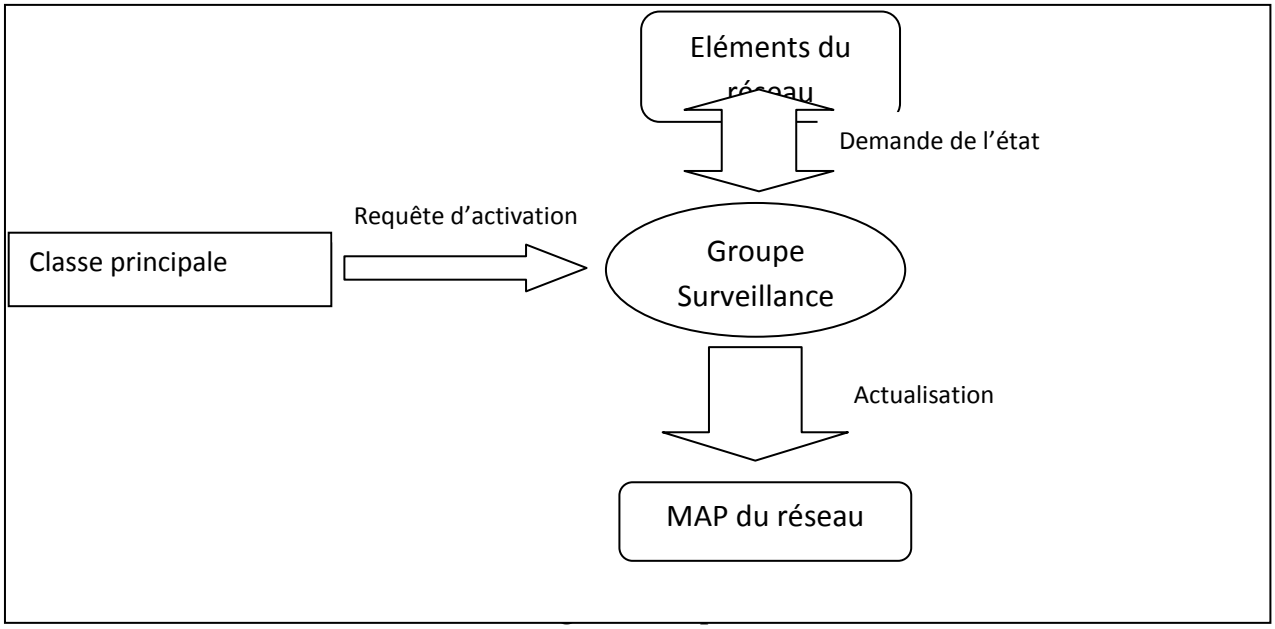
Fig.4.2. Groupe Scan.

❖ **Le groupe surveillance :**

Après qu'un scan du réseau a été effectuer sur un intervalle d'adresse IP, et qu'une table contenant tous les machines a été générer, l'application aura créé en parallèle une carte du réseau (Une MAP) en même temps que le scan lui-même.

Lors du scan réseau, des qu'une machine a été trouver, la MAP réseau est mise a jour en ajoutant cet élément avec son adresse IP.

Des la fin du scan réseau le service surveillance peut être activé, ce service permet de savoir en temps real si les éléments trouver lors du scan sont toujours active. En cas de déconnection de la machine, ou de problème de connexion entre l'application et cette machine, une alarme est émise, et un indicateur va clignoter sur la MAP réseau avec entre autre un signal sonore.



4.2.2. Le groupe informations :

Ce service permet de récolter un ensemble d'information sur les éléments du réseau. Pour les besoins de l'application, les informations récoltées se résume à :

- L'adresse IP de la machine.
- Le nom de la machine.
- Informations sur le propriétaire de la machine (Contact système).
- Informations sur l'emplacement de la machine (Location système).
- Le type de hardware et software de la machine.
- La liste des processus exécutés par la machine.
- La liste des services exécutés par la machine.

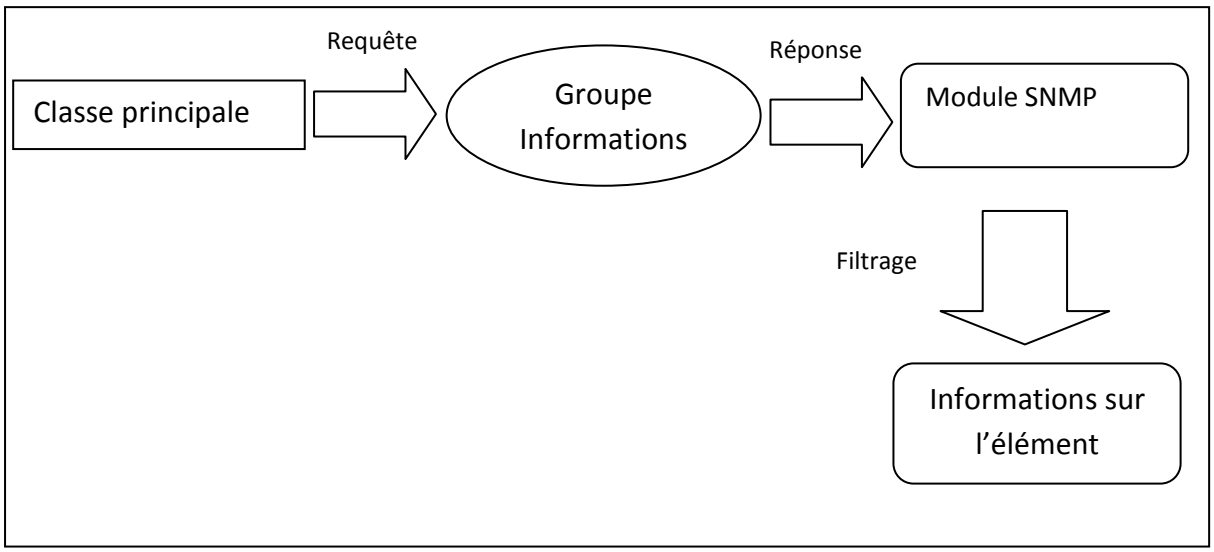


Fig.4.4. Groupe Informations.

4.2.3. Le groupe statistique :

Ce groupe contient des objets mesurés concernant chaque interface de chaque machine du réseau, les statistiques de chaque interface sont prises séparément par rapport aux autres, se qui permet a notre application d'acquérir des données sur plusieurs éléments du réseau simultanément. Ces statistique ont pour usage la gestion es performances, et la gestion des fautes.

- **La gestion de performance :**

Elle est assurée par une collecte de données qui permet d'avoir le taux de l'utilisation de la bande passante, assurée par un calcul effectué sur le nombre d'octets circulant sur l'élément du réseau.

Afin de les interpréter nous avons opté pour une représentation graphique qui s'étale sur une période paramétrable.

Les objets de la MIB utilisés :

- ifIndex
- ifDescr
- ifInOctets
- ifOutOctets

- **La gestion des erreurs :**

Elle est assurée par une collecte de données d'objets relatifs aux erreurs survenues sur une interface d'une machine bien précise du réseau. Un aperçu des erreurs de trafics de cette interface survenues sur le réseau est représenté graphiquement dans un histogramme.

Les objets de la MIB utilisés :

- ifIndex
- ifDescr
- ifInErrors
- ifOutErrors

4.2.4. Le groupe Host :

Ce service permet de connaitre les données spécifiques à une station. A cet effet nous avons choisi de représenter un cumule des données suivantes :

- La machine émettrice.
- L'heur de la mise sous tension de l'interface de la machine (depuis de la prise des statistiques)
- Le nombre total d'octets émis et reçu.
- Le nombre total d'erreurs émis et reçu.

❖ **Le groupe TopHost :**

Ce service permet de mettre en évidence les éléments les plus actifs du réseau selon les critères suivants :

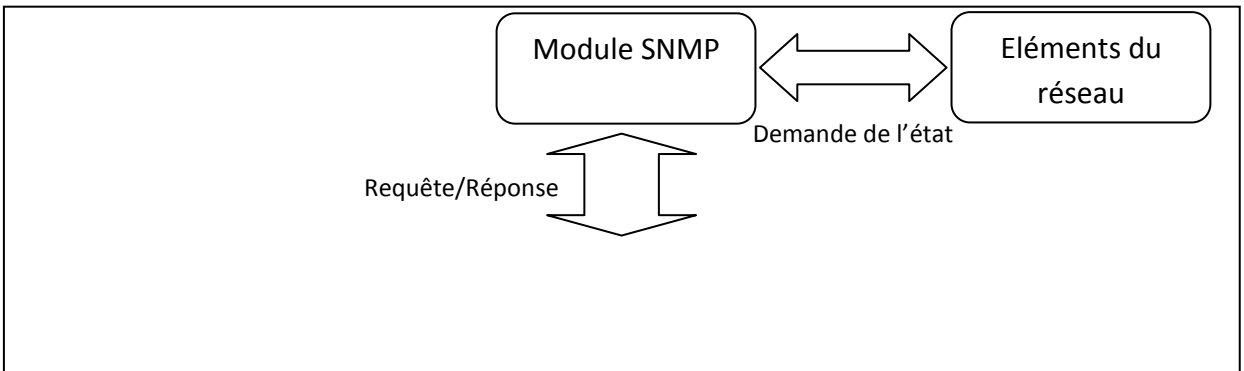
- Les éléments qui émettent le plus ou reçoivent le plus
- Les éléments générant le plus d'erreurs

Les statistiques récoltées peuvent êtres illustrées par tables et graphes qui représentent les données récoltées. Ce groupe n'est pas implémenté dans l'application vu que nous avons une vision sur les données citées dans le groupe host, en ajoutant une fonction de tri nous obtenons un classement des machines actives.

4.2.5. Le groupe alarmes :

Ce groupe a pour rôle de paramétrer la gestion des alarmes et de fixer les valeurs des seuils supérieurs pour un objet voulu à valeur numérique, ainsi que de générer les alarmes vers la station d'administration (La classe principale), en cas ou il ya une violation des limites fixées lors de la configuration des alarmes.

Ce groupe est géré par une classe qui permet d'affecter les données nécessaires à la configuration d'une alarme à partir d'une interface graphique. Par exemple si on fixe une valeur d'alarme pour la gestion des erreurs de trafic, dés que cette valeur sera dépassée, l'utilisateur de l'application sera averti d'une telle alarme, ce que peut s'interprété par un problème sur la machine d'où est émise l'alarme.



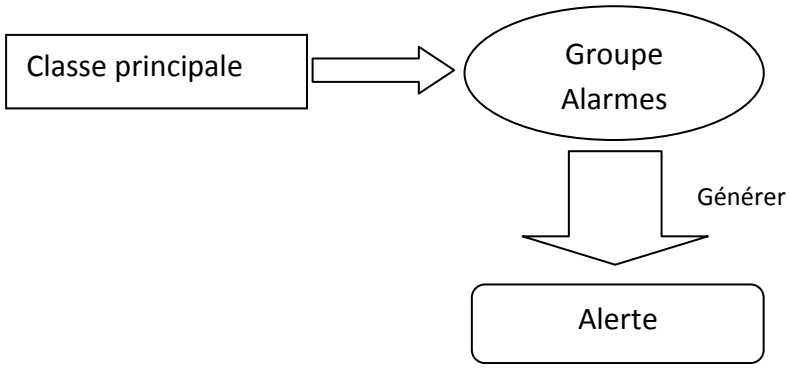


Fig.4.5. Groupe Alarmes.

4.2.6. Le groupe SNMP :

Ce groupe implémente les méthodes de base du protocole SNMP.

❖ **La méthode GetOID :**

Elle permet de récupérer la valeur d'une variable de la MIB, quelque soi la machine du réseau. Il suffit d'entrer l'adresse IP de la machine, de vérifier la valeur du « Community », ainsi que de donner la valeur de l'identifiant de la variable (OID) dont on veut récupérer la valeur.

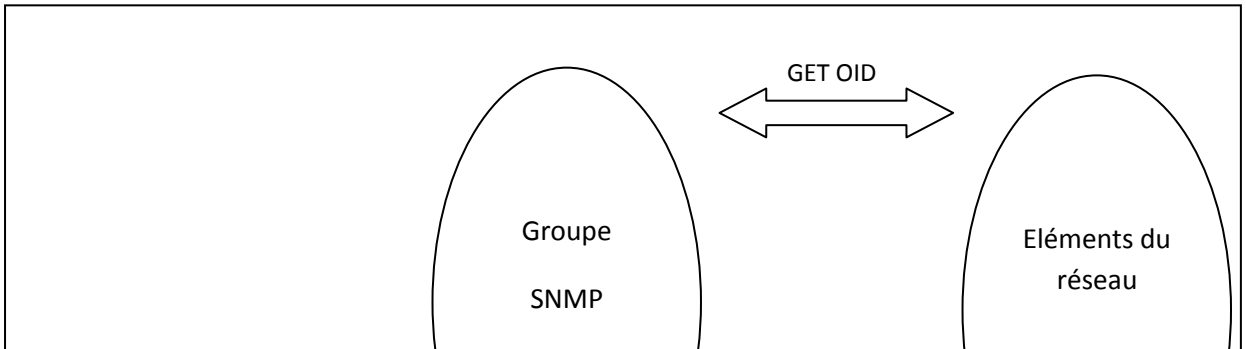
❖ **La méthode SetOID :**

Elle permet de modifier la valeur d'une variable de la MIB. Comme pour GetOID, il suffit de donner l'adresse IP, le « Community » et l'OID pour utiliser cette méthode. Mais contrairement à la lecture, l'écriture n'est pas toujours permise, certaines variable de la MID sont en Lecture-Seul, donc impossible à modifier. Par exemple l'OID « 1.3.6.1.2.1.1.1.0 » qui représente le type de hardware et software de la machine, qui est en Lecture-Seul.

Le groupe SNMP dispose également de la fonction Walk. Cette fonctionnalité a pour but de donner toutes les valeurs de tous les objets de la MIB d'une machine. Elle est développée en utilisant la fonctionnalité GetNext (avoir la prochaine), en commençant par avoir la première valeur du premier objet de la MIB, en suite on avance pas à pas jusqu'à atteindre la fin des objets. Pour ce qui est de la valeur de début si l'utilisateur ne donne pas de valeur, l'application va automatiquement chercher la première valeur de la MIB.

4.2.7. Le récepteur de Traps :

Le récepteur de traps, permet de récupérer les traps envoyé par les machines du réseau. Lorsqu'un élément du réseau entre dans un état anormal, l'agent SNMP de cet élément prévient notre application par le biais d'une Trap SNMP.



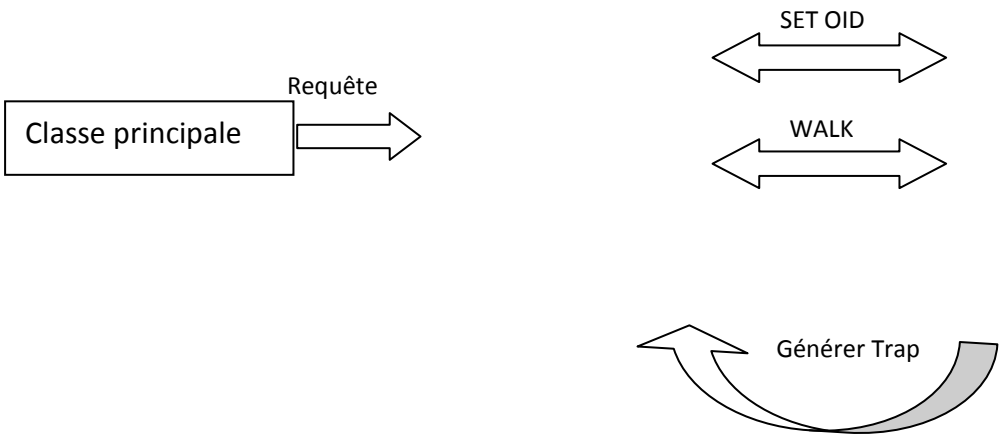


Fig.4.6. Groupe SNMP et récepteur de traps.

Il faut noter que l'agent SNMP se trouvant sur la machine qui envoi les traps, a besoin d'une petite configuration, entre autre l'adresse IP ou sera envoyer les traps générés.

Remarque :

- La gestion de la sécurité est laissée aux spécificités de protocole SNMP.
- La version SNMP implémentées est SNMP v1, cela est du au faite que c'est la version la plus stable et la plus simple d'utilisation.

Conclusion :

Dans ce chapitre nous avons vu modèle conceptuel de notre application, modèle nécessaire pour entamer la réalisation.

Dans ce qui suit, nous aborderons le chapitre qui concerne la réalisation de l'application dans lequel on présentera les choix effectué afin de réaliser ce qui a été dans ce chapitre.

Chapitre V

Réalisation et Implémentation

Introduction :

Afin de mettre en œuvre les fonctionnalités de notre application, nous allons présenter dans ce chapitre son implémentation. Notre travail consiste à réaliser est une application de gestion réseau TCP/IP en exploitant les objets de la MIB, il interprète sous forme de graphes et de tables les données relatives au réseau administré.

Dans ce chapitre nous allons présenter notre environnement de développement et les outils utilisés pour mener à terme la réalisation de notre application

2. L'environnement de développement :

2.1. L'environnement d'exécution :

Notre application s'exécute sur tous les systèmes qui intègrent une JVM. L'une des principales raisons d'avoir choisie java comme langage de programmation est le faite que l'application final, serai utilisable par tous, il suffit d'installer la JVM.

2.2. L'environnement de programmation :

Tous développement de logiciel passe traditionnellement par une étape très délicate ; le choix du langage adéquat. Effectivement, afin de développer ce logiciel, qui est une application purement réseau, il nous a fallu choisir un langage qui offre les outils nécessaires à l'exploitation des réseaux.

Notre application nécessite beaucoup de manipulation des modules du protocole TCP/IP tels que les requêtes SNMP, Paquets ICMP…etc. Pour cela, notre choix s'est porté sur l'outil de développement NetBeans IDE 6.8 de sun Microsystem comme environnement de programmation, qui offre une convivialité de travail, et également la possibilité d'intégrer de beaucoup de plugins et une souplesse de programmation. La JDK utilisée est la version 6.

Le choix du langage s'est porté sur JAVA pour diverses raisons :

- Il dispose d'une bibliothèque riche.
- Il permet la portabilité et la réutilisabilité.
- Java supporte le modèle Client/Serveur
- Java autorise le multithreading.

❖ **Les API externes à la JDK utilisée :**

Afin d'exploiter le protocole SNMP et pouvoir afficher des graphismes on a fait appel à des APIs java externes qui sont respectivement SNMPCommunicationInterface et JFreeChart.

SNMPCommunicationInterface :

SNMPCommunicationInterface est une API gratuit, qui gère le protocole SNMP. C'est une API très populaire dans le monde du SNMP vu que c'est une API libre. Elle peut être employée pour développer des applications de gestion de réseau ; pour construire des applets, des composants, et des applications réparties d'EJB, de CORBA, et de RMI. La bibliothèque fournit les fonctions et les composants le plus généralement utilisés pour rendre le développement plus simple.

JFreeChart :

JFreeChart est une bibliothèque open source qui permet d'afficher des données statistiques sous la forme de graphique. Elle possède plusieurs formats dont le camembert, les barres ou les lignes et propose de nombreuses options de configuration pour personnaliser le rendu des graphiques. Elle peut s'utiliser dans des applications JAVA ou des applications web et permet également d'exporter le graphique sous la forme d'une image. Pour la télécharger : http://www.jfree.org/jfreechart/.

MIB browser :

Le logiciel libre ServersCheck MIB Browser vous permet d'interroger n'importe quel périphérique compatible SNMP en utilisant le SNMPv1, SNMPv2 et même le protocole SNMPv3 sécurisé. Comme une application Java peut fonctionner sur tout système ayant le Run Time Java installé. Il peut effectuer des GET, GETNEXT, WALK et commandes SET SNMP.

MIB Browser vous permet de regarder la hiérarchie des variables de la MIB de SNMP sous forme d'arbre et vous fournit des informations additionnelles sur chaque nœud.

3. Installation du service SNMP sous Windows :

Avant de pouvoir utiliser notre application, il faut d'abords configuré l'agent SNMP de la machine que vous souhaitez gérer. Voici les étapes à suivre pour configurer l'agent sous Windows :

3.1. Installation du service SNMP :

- **Ouvrez l'Assistant Composants de Windows :** Cliquez sur Démarrer, puis cliquez sur Panneau de configuration, double-cliquez sur Ajout/Suppression de programmes, puis cliquez sur Ajouter/supprimer des composants Windows.
- Dans Composants, cliquez sur Outils de gestion et d'analyse (sans activer ni désactiver la case à cocher correspondante), puis cliquez sur Détails.
- Activez la case à cocher SNMP (Protocole simplifié de gestion de réseau), puis cliquez sur OK.
- Cliquez sur Suivant. (SNMP démarre automatiquement à la fin de l'installation)

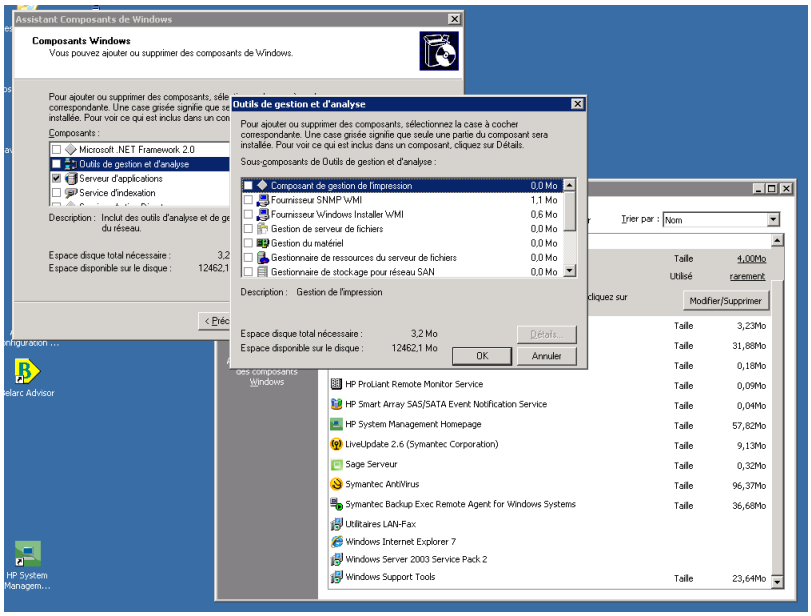


Fig.5.1. Installation SNMP sous Windows 1.

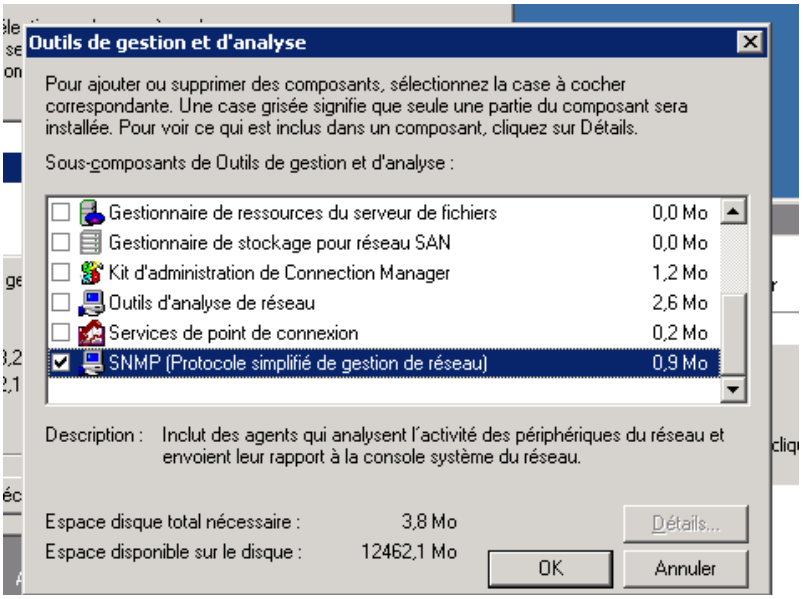


Fig.5.2. Installation SNMP sous Windows 2.

3.2. Configuration des propriétés de l'agent SNMP :

- Ouvrez le Gestionnaire des Services, et rechercher le service SNMP.
- En cliquant avec le botton droit sur le service, un menu apparait et cliquez sur Propriétés.
- **Sous l'onglet Agent** : Dans Contact, tapez le nom de l'utilisateur ou de l'administrateur de cet ordinateur.
- Dans Emplacement, tapez l'emplacement physique de l'ordinateur et du contact.
- Sous Service, activez les cases à cocher appropriées pour cet ordinateur, puis cliquez sur OK.

Gestion de la sécurité : Toujours dans les propriétés du service SNMP :

- **Sous l'onglet Sécurité** : Activez Envoyer une interruption d'authentification, si vous souhaitez qu'un message d'interruption soit envoyé à chaque échec d'authentification.
- Sous Noms de communautés acceptés, cliquez sur Ajouter.
- Sous Droits de communauté, sélectionnez un niveau d'autorisation pour permettre à l'hôte de traiter les requêtes SNMP en provenance de la communauté choisie.
- Dans Nom de communauté, tapez un nom de communauté en respectant la casse, puis cliquez sur Ajouter.
- Dans Propriétés de service SNMP, indiquez si les paquets SNMP en provenance d'un hôte sont acceptés ou non : Pour accepter les requêtes SNMP provenant d'un hôte du réseau, quelle que soit son identité, cliquez sur Accepter les paquets SNMP provenant de n'importe quel hôte. Pour limiter l'acceptation de paquets SNMP, cliquez sur Accepter les paquets SNMP provenant de ces hôtes, sur Ajouter, tapez le nom d'hôte, l'adresse IP ou IPX appropriés, puis cliquez à nouveau sur Ajouter.

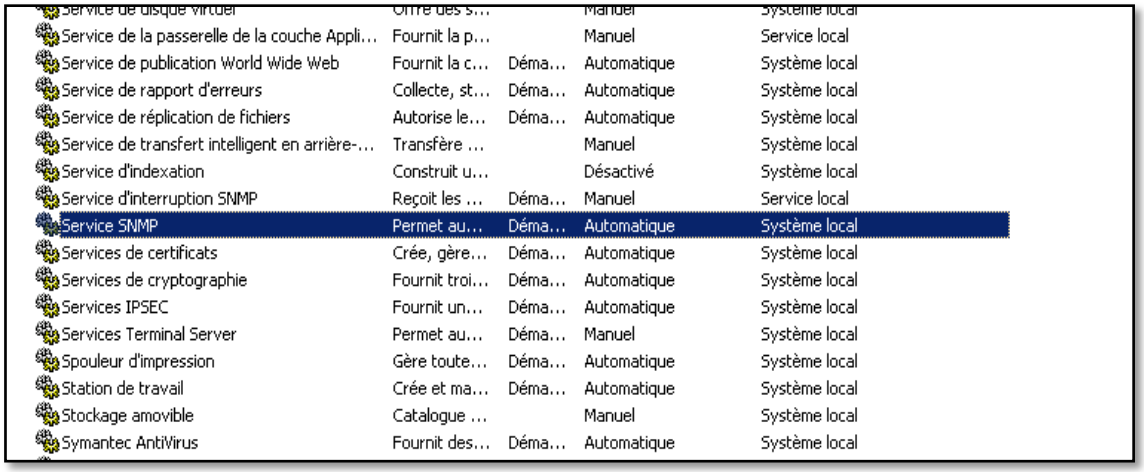


Fig.5.3. Configuration de SNMP sous Windows 1.

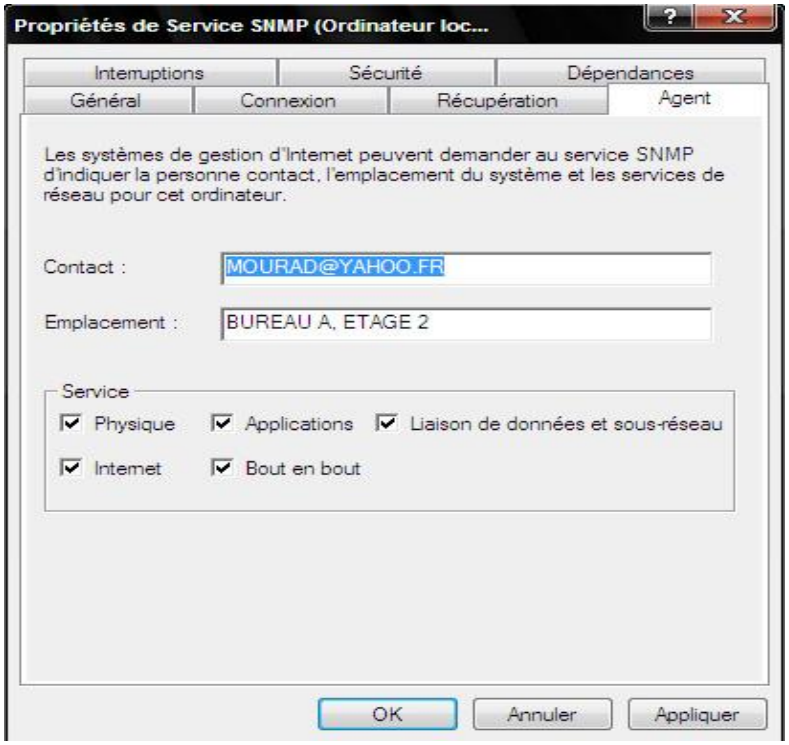


Fig.5.4. Configuration de SNMP sous Windows 2.

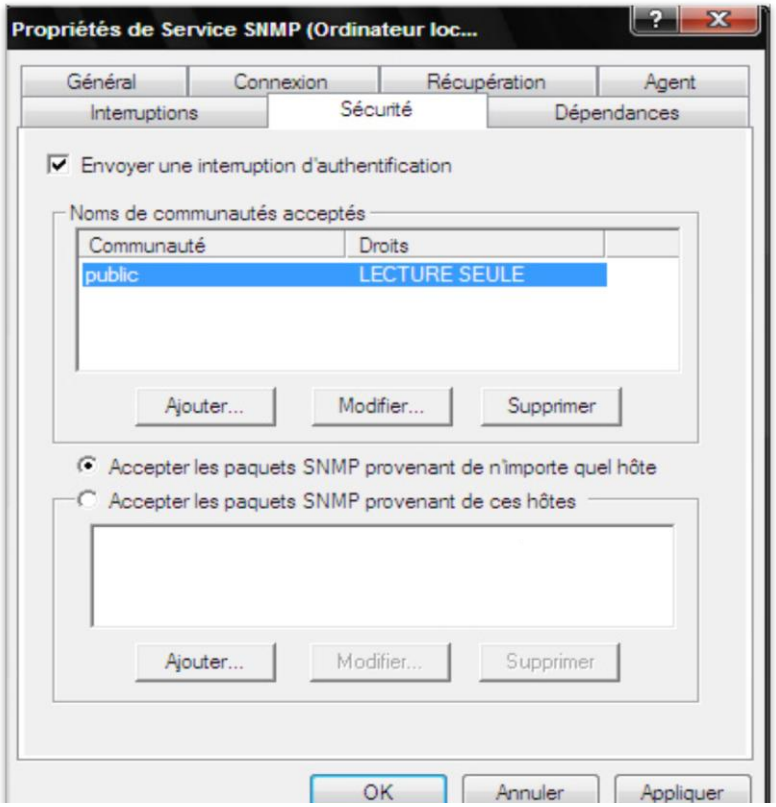


Fig.5.5. Configuration de SNMP sous Windows 3.

4. Installation du service SNMP sous Linux :

Les étapes suivantes nous montrent comment installer le service SNMP sous Linux étant donné que celui-ci est un système d'exploitation que nous utilisons pour l'administration de réseau dans notre travail. Sachant que la mise en œuvre de SNMP sous Linux se fera en utilisant le package NET-SNMP qui est un standard libre.

4.1. Le package NET-SNMP :

Le projet NET-SNMP appelé anciennement UCD-SNMP a été développé par l'université américaine Carnegie Mellon University (CMU) puis amélioré et maintenant maintenu par l'université américaine University of California Davis (UCD).

NET-SNMP est un ensemble d'applications utilisées pour implémenter le protocole SNMP (v1, v2c & v3) utilisant ã la fois l'IPv4 & IPv6. Il possède notamment les outilles et les fonctionnalités suivantes :

- Une API d'accès à SNMP.
- Un agent SNMP extensible.
- Des commandes en ligne pour interroger des agents SNMP.
- Des commandes en ligne pour gérer et générer des TRAPs SNMP.
- Une version de la commande UNIX netstat utilisant SNMP.

- Un browser de MIB SNMP (TKMIB).

NET-SNMP est porté sur différents systèmes et en particulier sur :

- Linux (noyaux 2.4 à 1.3).
- Solaris (2.8 à 2.3) et SunOS (4.1.4 à 4.1.2).
- NetBSD (1.5alpha à 1.0).
- FreeBSD (4.1 à 2.2).
- Windows.
- ….

NET-SNMP supporte SNMPv1, SNMPv2 et SNMPv3 que ce soit côté agent SNMP comme du côté manager SNMP via les commandes en ligne NET-SNMP.

4.2. Installation de NET-SNMP :

Ouvrir une fenêtre Terminal et exécuter la commande suivante :

```
#apt-get install snmpd
```

Il faut s'assurer de posséder les droit « root » afin de pouvoir installer le package.

4.3. Configuration de NET-SNMP :

Pour configurer NET-SNMP, il suffit d'éditer le fichier « /etc/snmp/snmpd.conf » comme suit :

```
syscontact Contact_de_la_machine
syslocation Localisation_de_la_machine
# sec.nom    source          community
com2sec readonly  default         public
com2sec readwrite default         private
# Creation des vues
view all    included  .1
view system included  .1.3.6.1.2.1.1
```

A ce stade il faut redémarrer le service :

```
/etc/init.d/snmpd restart
```

Et la configuration SNMP sur la machine Linux maintenant est active.

5. Présentation de l'application :

Dans ce qui suit on présente les interfaces graphiques de notre application.

5.1. Scan Réseau :

Après le lancement de l'application le service « scan réseau » s'affiche en premier, il suffit de donner un intervalle d'adresse IP, et l'application affichera la liste des machines active de cet intervalle.

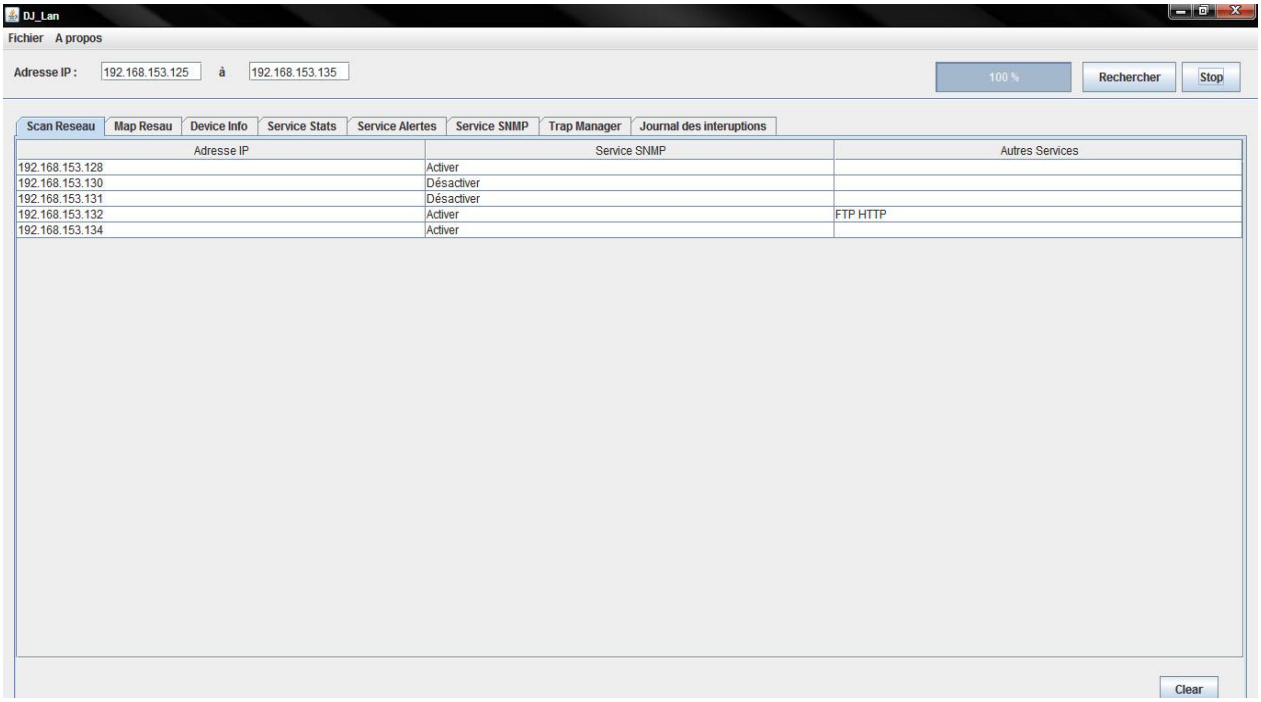


Fig.5.6. Service Scan réseau.

5.2. MAP réseau :

Au cour du scan réseau, une carte du réseau, et automatiquement généré en fonction des machines trouver dans l'intervalle d'adresse IP donné a scanner.

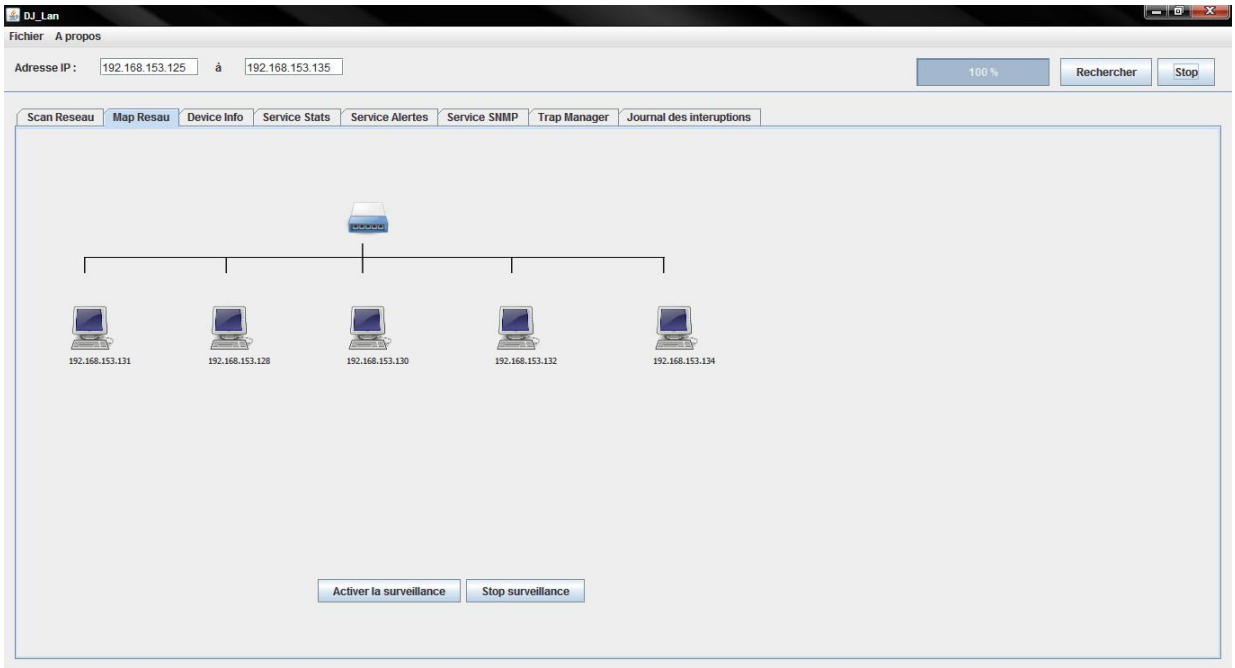


Fig.5.7. Map réseau.

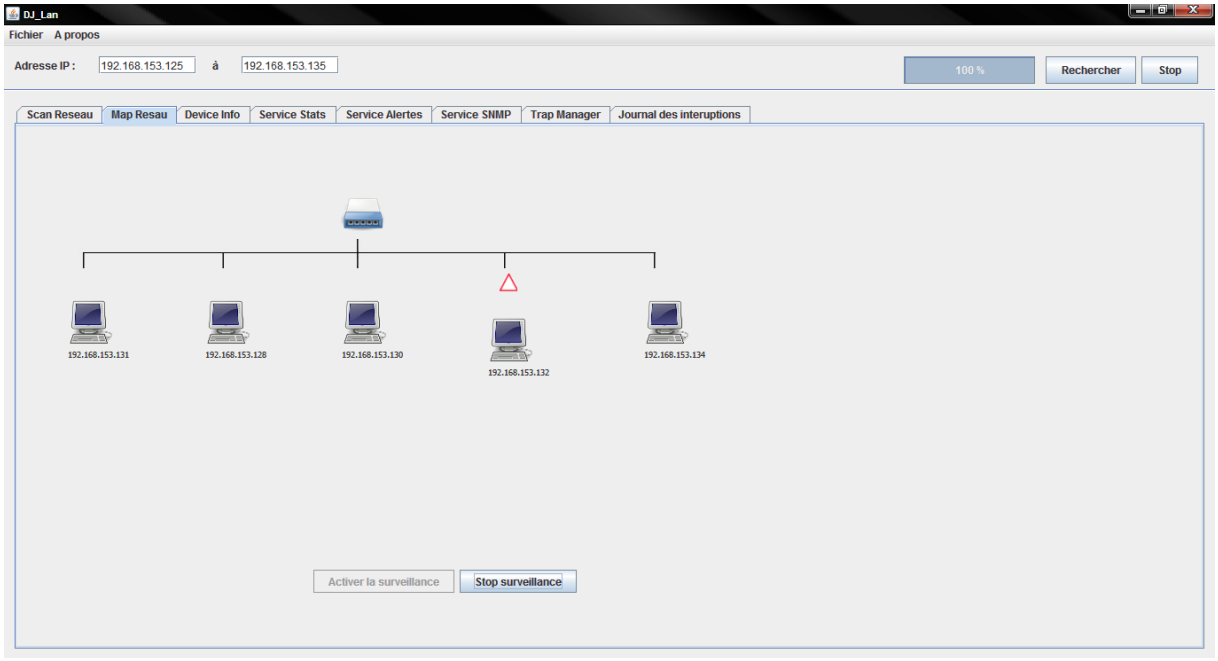


Fig.5.8. Surveillance du réseau.

Le service surveillance permet d'alerter l'administrateur, en cas de problème.

5.3. Service Informations :

En sélectionnant une machine dans la listes des machines trouvé lors du scan, on pourra afficher un certain nombre d'information sur cet élément, notamment le type de hardware et software, ainsi que la liste des processus exécuter sur cette machine, et bien d'autres informations.

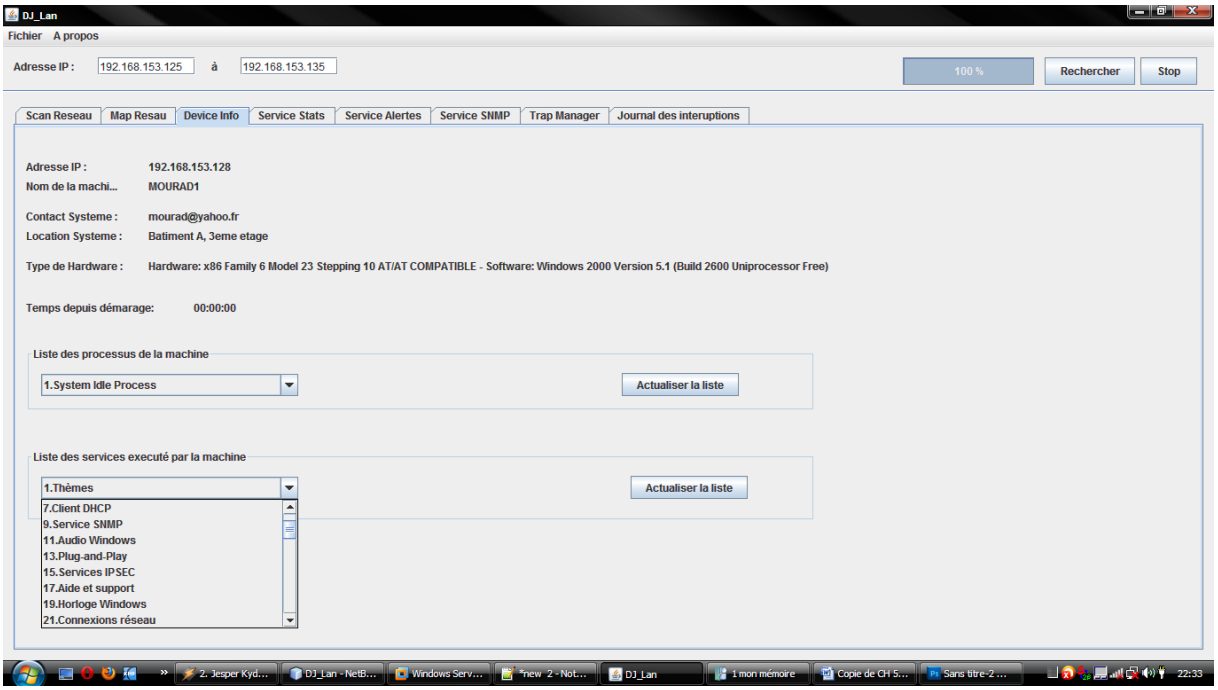


Fig.5.9. Service informations sur la machine.

5.4. Service Statistiques :

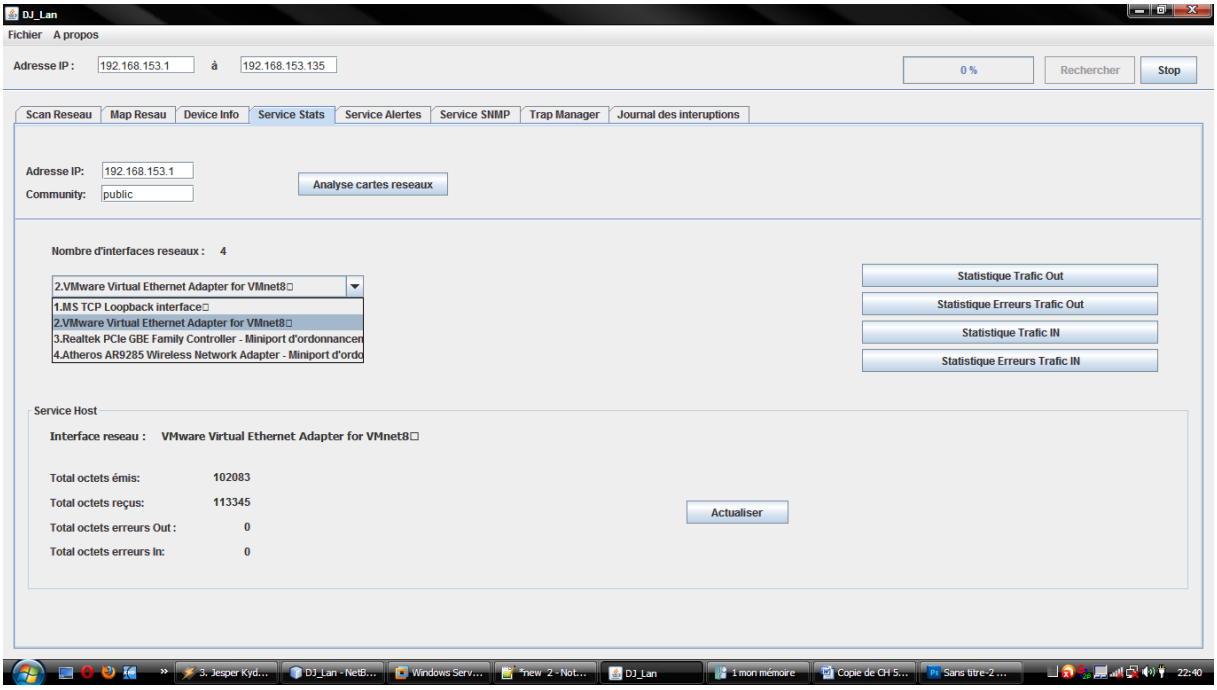


Fig.5.10. Service statistiques.

Ce service permet d'avoir un certain nombre de statistique sur une machines, on cliquant sur les bottons de droite, on pourra afficher des graphique relative au trafic réseau entant, sortant, les paquets contenant des erreurs lors des communications réseau.

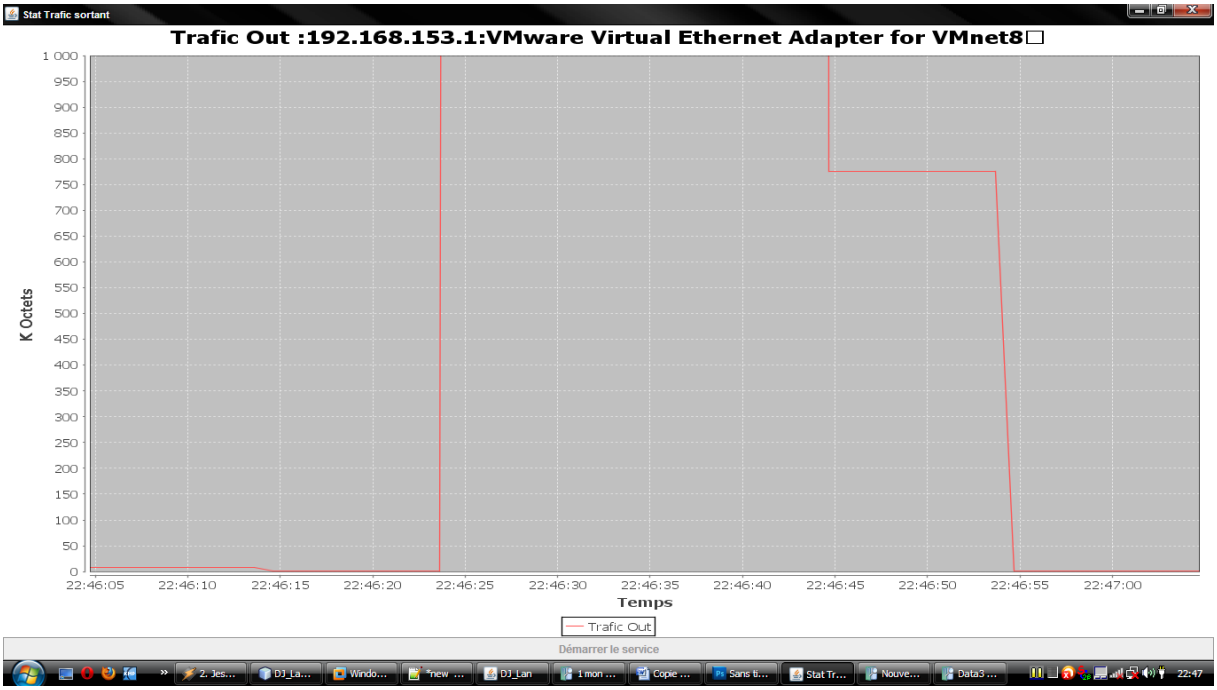


Fig.5.11. Histogramme du trafic réseau sortant.

Par exemple lors dune copie d'un fichier par réseau, on voit que le graphe du trafic sortant monter, et lors de la fin du transfert le graphe redescend.

5.5. Service Alertes :

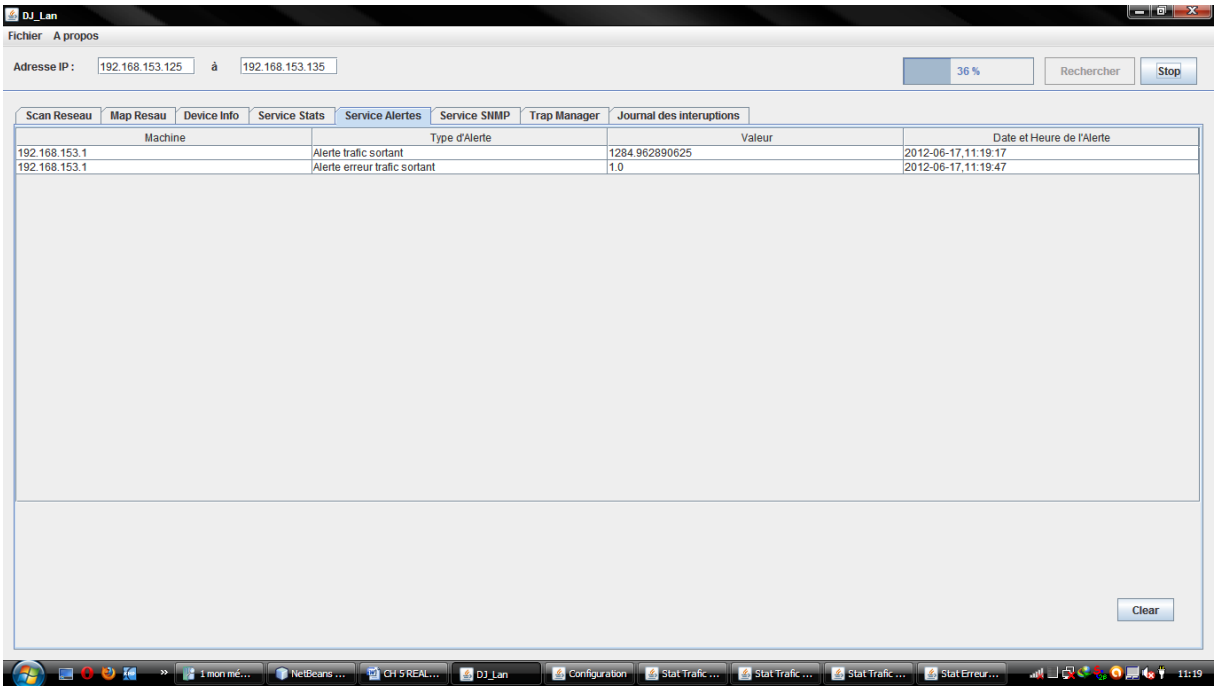


Fig.5.12. Service Alertes

Des alarmes vont se déclencher selon la configuration qui a été faite sur l'application. Par exemple si le taux d'erreurs dépasse celui autorisé par l'application, alors l'utilisateur sera prévenu.

5.6. Service SNMP :

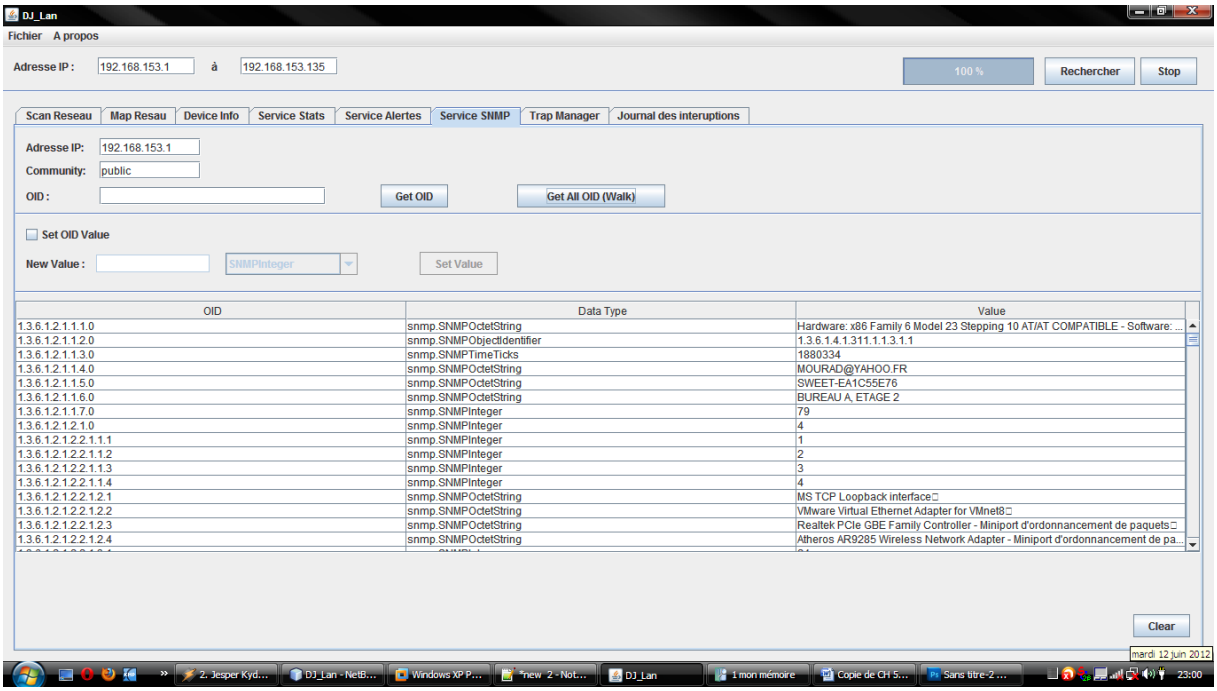


Fig.5.13. Service SNMP.

Ce service permet de récupérer, les OID de la MIB dune machine, et éventuellement modifier certaine variable si c'est possible.

5.7. Trap manager :

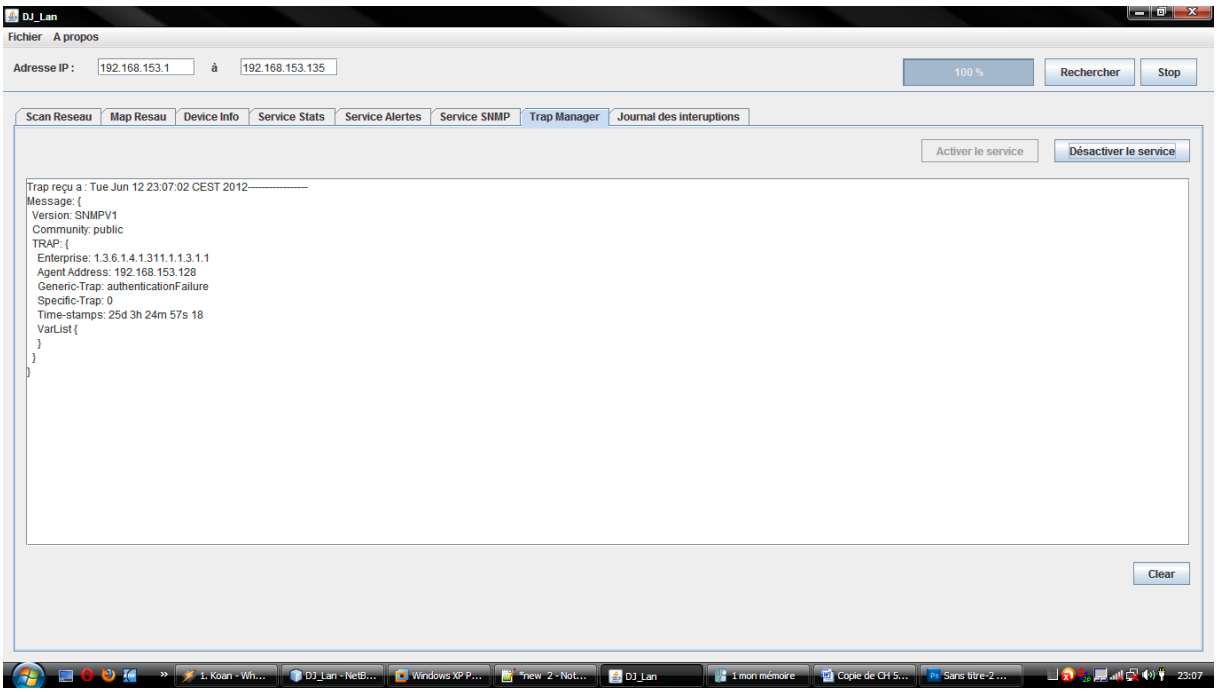


Fig.5.14. Trap Manager

Lorsqu'un agent dune machine du réseau envoi une trap, alors celle-ci sera affichée dans cet anglet. Par exemple si quelqu'un essai d'accéder a une variable de la MIB avec un mauvais « community » alors une trap sera généré.

5.8. Configuration de l'application :

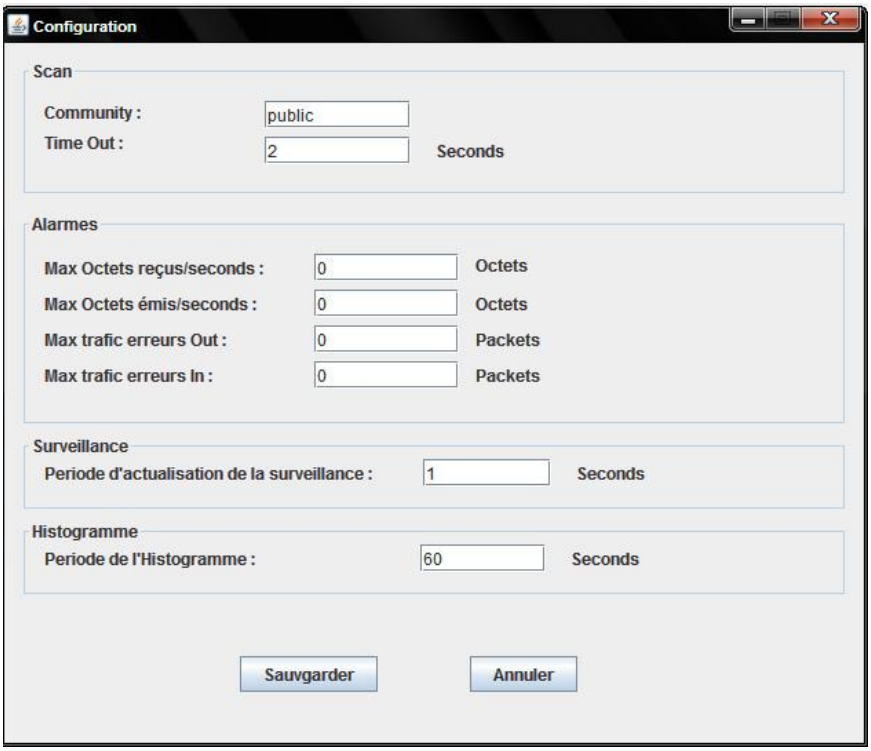


Fig.5.15. Configuration de l'application.

Dance cette fenêtre l'utilisateur pourra paramétrer l'application, selon ces envies.

5.9. Journal des interruptions :

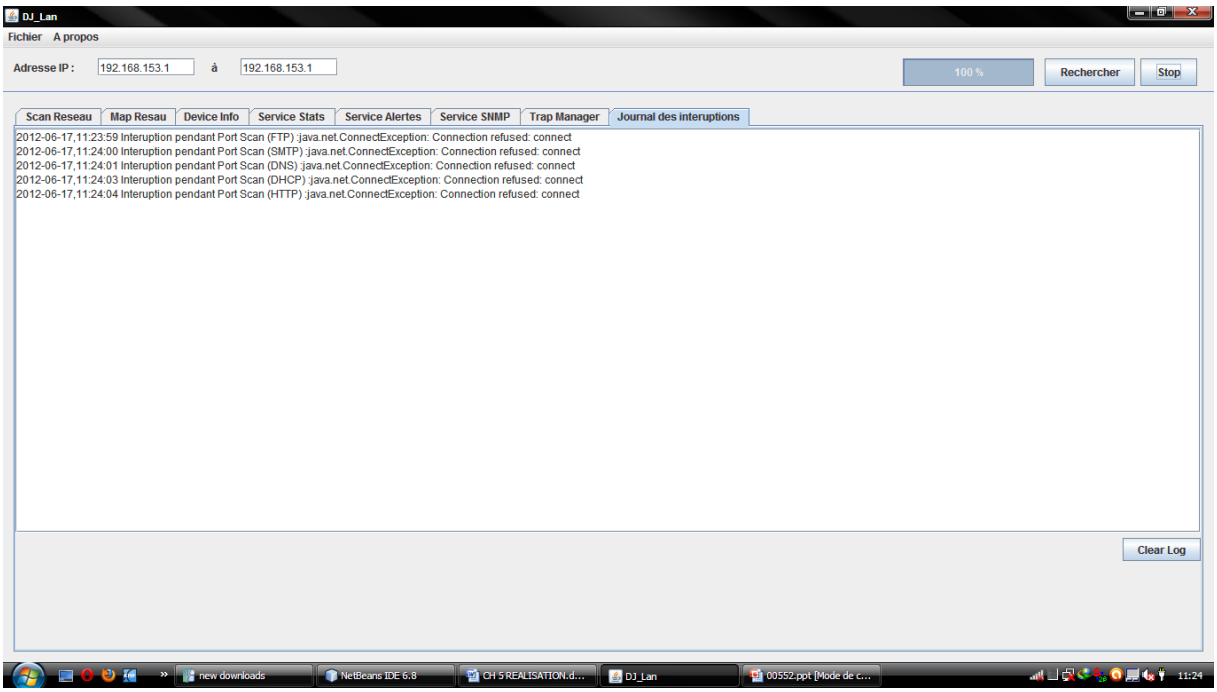


Fig.5.16. Journal des interruptions.

Vu que notre application, est une application réseau, donc elle utilise beaucoup les sockets et les threads, on a préféré créer un journal d'interruption, qui affiche les interruptions rencontrées lors de l'utilisation de la plateforme.

Conclusion :

Dans ce chapitre, nous avons présenté l'environnement d'implémentation et de développement de notre application, précédemment schématisé dans le chapitre précédent.

La description de notre application s'est faite en présentant les interfaces essentielles de notre application.

Conclusion générale

De nos jours pour une entreprise, il est pratiquement impossible de se passer de l'outil informatique quelque soit le domaine d'application. Et qui dit outil informatique, implique automatiquement réseaux informatique.

Ainsi, l'Administration de Réseau Informatique apparaît comme l'une des plus importantes préoccupations pour tout entreprise digne de se nom.

Dans le travail que nous avons effectué « Conception et réalisation d'une application de gestion de réseau multiplateforme », nous avons constaté la richesse du travail de l'administration réseaux et sa complexité, du aux taches qui doivent être assuré avec pertinence.

Cet exercice nous a été énormément profitable, car il nous a permis d'élargir notre connaissance sur le protocole SNMP. Grâce à elle, nous avons pu dégager l'étendu du travail d'administration réseau, cette charge que nous avions qualifié de lourde vu les efforts que doivent conjuguais les administrateurs réseau pour garder en état de marche leurs réseaux et d'intervenir au plus vite possible en cas de panne.

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

C'est ainsi que nous nous sommes efforcé d'implémenter une application de gestion de réseau exploitant le protocole SNMP pour concrétiser ses informations récoltées lors de nos recherches.

En guise de perspectives, notre application peut être améliorée en lui intégrant les fonctionnalités suivantes :

- Pouvoir récupérer plus d'informations sur les éléments du réseau, tel que le taux d'utilisation de la CPU, la mémoire utilisée par la machine, ainsi que la taille de l'espace disque.
- Enrichir l'application avec plus de graphes.
- Intégration d'une base de données afin de pouvoir sauvegarder les statistique d'une machine, afin d'avoir un historique complet de la machine en question.

Bibliographie

[1] : Technologie réseaux avancées, édition JRES 2001.

[2] : Service SNMP de détection de faute pour des systèmes répartis, André SCHIPER, 2002.

[3] : Mémoire : Utilisation du protocole SNMP pour la gestion a distance d'une interface, Haithem Hmida, 1998

[4] : Mémoire : Conception et réalisation d'une application de gestion de réseau à base de Composants répartis, Mohamed Arezki, 2000

[5] : Pujolle « Les réseaux ». Edition EYROLLES 2008.

[6] : Vers une conceptualisation de la sécurité des réseaux hétérogènes, Michel Riguidel, 2009

[7] : Le protocole SNMP et les tables MIB, Marc-André Lamontagne, 1999

[8] : Cours réseaux, Frédéric Jacquenod, 2007

[9] : Pascal Nicolas « Architecture de réseau », 1999

Sites Web :

www.ipframe.com
www.snmp.com
http://irp.nain-t.net
http://www.commentçamarche.com
http://www.developpez.net
http://formsys.net