R 閒 ublique Alg 閞 ienne D 閒 ocratique et Populaire
Ministre de l'enseignement Sup 閞 ieur et de la Recherche Scientifique

Université Amar Telidji Laghouat

Département de Génie Informatique

Projet de fin d'étude
Pour l'obtention de diplôme d'ingénieur d'état en informatique

Option : Système d'information avancée

Thème :

Réalisation d'une application d'aide à l'administration réseau

Encadr? par :

- Dr.Ouinten Youcef

R 閱 lis? par :

- Boukhalkhal Ahmed
- Sahel Naima

Session 2004

Remerciements

Louange à notre Seigneur "ALLAH " qui nous à doté de la merveilleuse faculté de raisonnement.

Louange à notre créateur qui nous a incité à acquérir le savoir, c'est à lui que nous adressons toutes notre gratitude en premier lieu.

En second lieu, nous tenons à remercier notre encadreur Dr.Ouinten Youcef, qui à été toujours disponible malgré ses nombreuses occupations, et pour sa confiance, sa patience, et dont les encouragements et les conseils judicieux nous furent d'une très grande utilité.

Nous voudrons aussi exprimer nos profondes gratitudes à nos parents pour l'amour et l'encouragements durant la rédaction de ce mémoire et tout au long de nos études en informatique.

Enfin, nous remercions tous les enseignants du département de l'informatique et tous nos collègues et nos amis pour leurs supports durant tout ce travail et pour tous les bons moments passés ensembles.

Résumé

Les gestionnaires de réseaux avec serveurs sont les plus nombreux par rapport aux réseaux poste à poste. Ils représentent l'offre stratégique des constructeurs jusque là cantonnés à gérer des réseaux locaux.
En marge de l'extension de ces derniers dans un monde hétérogène, la tâche de l'administrateur devient de plus en plus complexe, il est important de disposer d'outils d'administration performants permettant de contrôler et d'optimiser le réseau.
Le but de ce projet de fin d'étude pour l'obtention d'un diplôme d'ingénieur d'état en informatique, est de créer une application qui comporte plusieurs outils permettant de :

- surveiller les postes de travail
- contrôler les sessions
- gérer les ressources partagées
- gérer les comptes utilisateurs
- faire des statistiques et diagnostics sur le réseau

Pour développer cette application nous avons fait appel à la technique de programmation des APIs windows. Microsoft Windows offre des fonctions contenues dans des librairies appelables depuis les langages de programmation tels que Delphi, Visuel Basic, C++, etc. Dans ce travail nous avons porté notre choix sur le langage de programmation Pascal sous l'environnement Delphi.

Tables des matières

No table of contents entries found.

Introduction

Dans les dernières années, les réseaux informatiques sont devenus une ressource indispensable au bon fonctionnement d'une organisation, ils touchent de plus en plus notre vie courante. On compte sur les services offerts par les réseaux pour les transactions bancaires, les recherches Web, la téléconférence, etc.

Cela s'est traduit par une augmentation de la complexité de l'opération des réseaux, cette complexité peut être analysée selon deux directions : l'évolution de la taille des réseaux et la complexité des équipements et protocoles mis en œuvre. Parallèlement au développement des réseaux, on verra de plus en plus d'applications se servir de ces réseaux pour échanger des informations.

Ce travail est réalisé dans le cadre d'un projet de fin d'étude pour l'obtention d'un diplôme d'ingénieur d'état en informatique.

Après avoir observé de plus près ce phénomène, nous consacrons le premier chapitre à une introduction aux réseaux informatiques où l'on donnera les concepts de base et les notions élémentaires nécessaires à la compréhension des réseaux, ainsi que les différentes architectures protocolaires.

Les technologies de soutien du développement de ces réseaux de communication, ainsi que les normes qui définissent les interconnexions entre ces réseaux peuvent accroître dans de grandes proportions l'efficacité de beaucoup d'activités reparties dans toute l'industrie. Mais il y'a aussi des problèmes à régler, qui risquent sans cela d'inhiber tous ces réseaux de communication et de les empêcher de répondre à nos besoins. Une préoccupation majeure est de savoir si l'on peut arriver à mettre sur pied une gestion efficace des réseaux.

Pour cela, dans le second chapitre, nous allons détailler cet aspect et nous donnerons une définition et les disciplines de la gestion de réseau ainsi que les principales fonctions de base effectuées régulièrement par un administrateur réseau. Ce qui nous emmène à la déduction des besoins d'un outil d'administration. Par la suite nous exposerons l'organisation globale d'une administration.

Le troisième chapitre, est consacré à l'étude la plate-forme Windows NT où seront exposées, ses caractéristique, son organisation et les concepts de base en matière de gestion des comptes, de groupes et de ressources partagées, suivie d'un bref aperçu sur les API Windows.

Finalement, le dernier chapitre traite les divers types d'outils d'administration, suivis de la description d'un modèle qui donne une vision globale de l'application qui nous avons développé. Nous présentons, aussi dans cette partie une description des routines nécessaires à la construction d'une telle application suivie d'un exemple d'exécution pour les différentes parties de l'application. Nous terminerons par une conclusion qui résumera nos impressions sur ce qui a été réalisé et ce qui pourrait être amélioré ou ajouté dans des développements futurs.

Chapitre 1

Introduction sur les réseaux

On découvre qu'il devient de plus en plus facile de construire de puissants réseaux transparents, capable de lier entre elles les différentes parties des entreprises, et celle-ci avec le monde entier.
Cette première partie vise à poser les fondements des réseaux et présenter les matériels nécessaires à la construction d'un réseau, ainsi que les principales architectures protocolaires.

1. Définition d'un réseau :

Un réseau en générale est le résultat de la connexion de plusieurs machines entre elles, afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations de manière simple et rapide.
Un réseau informatique est un ensemble de composants matériels et logiciels permettant d'assurer un service dans la gestion courante des entreprise et des administrations (banque, commerce, recherche,…) ainsi que dans la vie courante des particuliers (messagerie, loisir,…).
Les objectifs principaux d'un réseau sont :

- Partage des ressources : On peut partager des données pour quelles soient accessibles localement ou à distance et aussi partager des périphériques coûteux (imprimante, disque durs, etc…).
- Fiabilité des données : On s'arrange pour que les fichiers soient dupliqués sur plusieurs machines.
- Communication entre les utilisateurs : les utilisateurs peuvent échanger des messages au sein d'un même groupe de travail ou à travers le monde entier à l'aide de la messagerie sur Internet.
- Partage des applications : tous les utilisateurs du réseau ont accès au mêmes logiciels d'applications.
- Réduction des coûts : les grandes installations sont 10 fois plus rapides que des micro mais 1000 fois plus chère. D'où des systèmes à base de micros puissants avec des données partagées localisées sur un ou plusieurs serveurs de fichiers.

2. Classification des réseaux :

On peut faire une première classification des réseaux suivant la distance qui sépare les ordinateurs, on distingue 3 catégories de réseau :

- Les réseaux locaux, également appelé *LAN (Local Area Network)* : ce sont des réseaux interne aux entreprises. Ils servent au transport de toutes les informations de l'entreprise. En règle générale, les bâtiments à câbler s'étendent sur plusieurs centaines de mètres. Le débit des ces réseaux va de quelques mégabits à plusieurs centaines de mégabits par seconde.

- Les réseaux métropolitains, ou *MAN (Metropolitan Area Network)* : Ce sont des réseaux qui permettent l'interconnexion des entreprises sur des réseaux spécialisés a haut débit qui est géré à l'échelle d'une métropole, c'est en fait un réseau de réseaux.
- Les réseaux étendus, ou *WAN (Wide Area Network)* : Ce sont des réseaux nationaux ou internationaux destinés à transporter des données numériques sur des distances à l'échelle d'un pays.

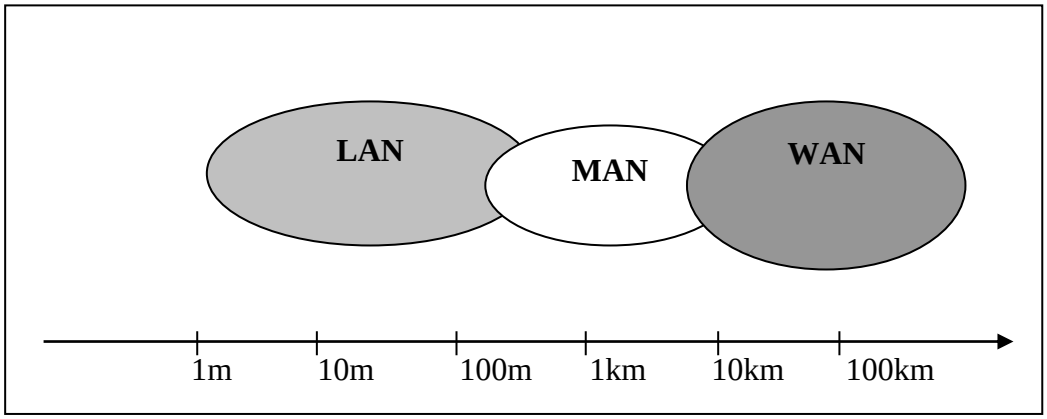

Fig.1.1 Les différentes catégories de réseaux informatiques.

3. Composants d'un réseau :

Tous les réseaux, même les plus compliqués, présentent les trois même composants de base :

- Les serveurs qui fournissent les services sur le réseau
- Les clients qui utilisent les services du réseau
- Le média qui permet aux différents éléments du réseau de communiquer.

Les serveurs :

Le serveur est chargé de la gestion du réseau. Il pilote l'ensemble du réseau et ses applications. Sur ce serveur se trouve, également, connecté des périphériques comme des imprimantes et des unités de stockage. L'ensemble de ces périphériques sont partagés est deviennent ainsi des ressources du réseaux.

Il existe plusieurs type de serveur de communication :

- Serveurs de fichier : ils partagent l'accès aux fichiers et à des imprimantes connectées au réseau
- Serveurs d'application : ils contiennent des applications que les utilisateurs du réseau peuvent utiliser
- Serveurs de messagerie : ils permettent aux usagers d'échanger des messages électroniques avec d'autres usagers
- Serveurs de télécopie : ils permettent aux utilisateurs de recevoir et d'envoyer des télécopies à travers le réseau.

Les clients :

Tout ce qui utilise les services fournis par un serveur est un client. Les postes de travail des utilisateurs sont des clients et tous les PC peuvent être considérés comme des clients, le client est, généralement, un ordinateur qui permet aux utilisateurs d'utiliser beaucoup d'espace disque, des périphériques évolués, de communiquer et de partager des données avec d'autres utilisateurs.

Le média :

Pour leur permettre de communiquer avec le serveur, les utilisateurs sont reliés à celui-ci par le média qui constitue le support physique de communication entre le serveur et les stations, et permet d'y faire transiter des données à haute vitesse. C'est le support à travers lequel, tous les éléments d'un réseau communiquent entre eux.

Il existe différent média pour connecter des réseaux :

- Câble coaxial: est composé d'un câble entouré d'un isolant, lui-même recouvert d'une tresse métallique, elle-même recouverte d'un isolant. Il permet des vitesses de transmission bien plus élevées avec un débit maximum 10 Mbit/s et des connexions à plus grande distance. Le gros désavantage du câble coaxial est la grande difficulté de localiser l'emplacement d'une panne.
- Câble à paires torsadées : ce type de câble est utilisé pour du câblage dit universel :
    - Câble UTP (Unshielded Twisted Pair : Paires torsadées non blindées), le moins cher, fin et flexible car il n'y a pas de blindage. Les risques de radio interférences sont élevés. Ce câble est cependant tout à fait suffisant pour un réseau domestique dans lequel les distances se limitent en général à quelques mètres.
    - Câble STP (Shielded Twisted Pair : Paires torsadées blindées) avec un seul blindage entourant l'ensemble des fils. Ce câble est très courant. Il est encore assez flexible et n'est pas trop cher. Les risques de radio interférences sont réduits.
    - Câble STP avec un blindage séparé autour de chaque paire de fils. Il est cher et n'est pas à recommander pour un réseau domestique.

Les différents types de câble à paires torsadées sont standardisés en catégories selon l'affaiblissement du signal relatif à la longueur de câble.

- Câble de catégorie 3 : largeur de bande maximum 16 MHz
- Câble de catégorie 5 : largeur de bande maximum 100 MHz.

- Fibre optique : est le support presque parfait pour les transmissions de données. Il permet de dépasser les 1 000 Go par seconde, le câble en fibre optique consiste en un cœur de verre ou de plastique qui transporte le signal sous la forme de pulsation de lumière. Cependant, le coût du câble fibre optique a diminué et de nombreuses entreprises qui avaient évité la fibre s'orientent progressivement vers ce support en raison de ses capacités quasiment illimitées.

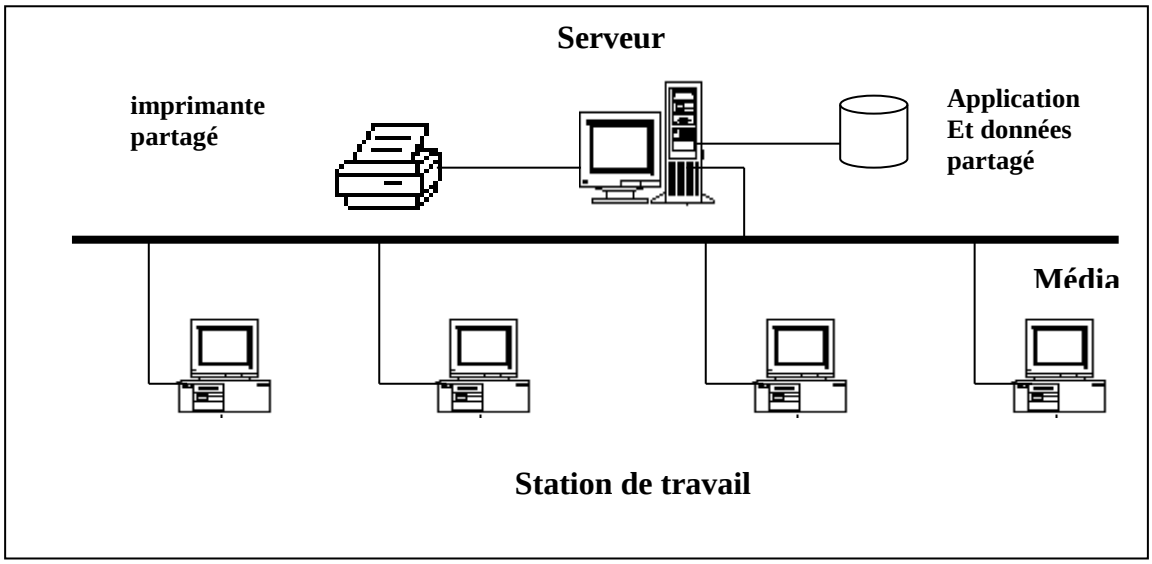

Fig.1.2 Les composants d'un réseau informatique.

4. Topologie des réseaux :

Par topologie, nous entendons la façon dont on connecte les machines au serveur. Il en existe, principalement, trois :

- **Bus :** tous les équipements sont branchés, en série, au serveur. On utilise un câble coaxial pour ce type de topologie. L'avantage du bus est sa simplicité de mise en œuvre et sa bonne immunité au perturbation électromagnétique. Par contre si le câble est interrompu toute communication sur le réseaux est impossible.
- **Etoile :** dans cette topologie, toutes les liaisons sont issues d'un point central, on utilise les câbles en paire torsadée ou en fibre optique. Pour ce type de topologie l'avantage est que les connexions sont centralisées et facilement modifiables, si un câble est interrompu le reste du réseau n'est pas perturbé. L'inconvénient, qui est de taille, de cette topologie réside dans le fait qu'elle nécessite une importante quantité de câble.
- **Anneau :** les équipements sont reliés entre eux en formant une boucle. La liaison est point à point et l'information est gérée comme dans la topologie bus. Pour le câblage on utilise des paires torsadées ou de la fibre optique. L'avantage de cette topologie est qu'elle offre deux chemins alternatifs pour aller d'un point à l'autre.

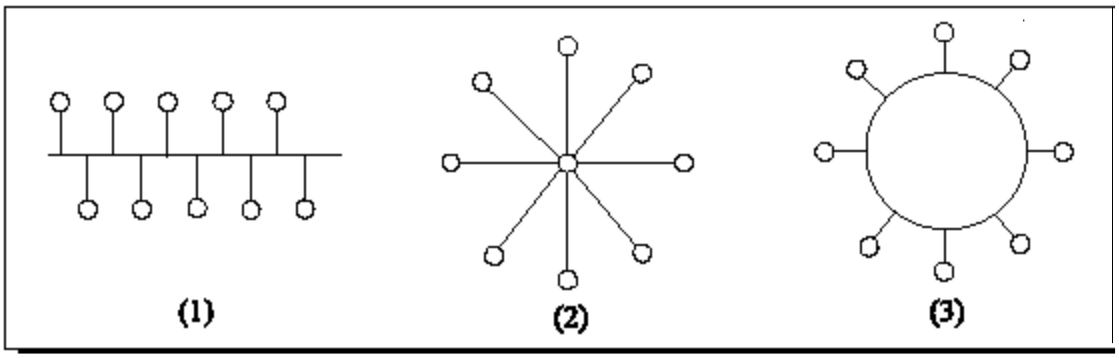

Fig.1.3 Topologie des réseaux : 1) Bus 2)Etoile 3)Anneau

5. Le modèle de référence OSI de ISO :

Au début des années 70, chaque constructeur a développer sa propre solution réseau autour d'une architecture et d'un protocole privé (SNA d'IBM, DECnet,TCP/IP du DoD,…). Il est vite apparu qu'il serait difficile, sinon impossible, d'interconnecter ces différents réseaux, si une norme internationale n'était pas établie. Cette norme établie par ISO *(Inernationnal Standarisation Organisation)* est la norme OSI (Open System Interconnection).

"Un système ouvert est un ordinateur, terminal, un réseau, n'importe quelle équipement apte à échanger des informations avec d'autre équipements hétérogènes et issu de constructeurs différents. " [1].

Cette norme de communication repose sur l'empilement de 7 couches pouvant communiquer verticalement entre elles telle qu'illustré dans tableau 1.

Tableau 1 : Le modèle de référence OSI

7. Couche Application **Application utilisant le réseau**
6. Couche Présentation **Formate les données en fonction de l'application**
5. Couche Session **Réparti les données suivant les application**
4. Couche Transport **Détection et correction des erreurs**
3. Couche Réseau **S'occupe de la connexion sur le réseau**
2. Couche Liaison **Transfert de données fiable sur le lien physique**
1. Couche Physique **Définie les caractéristiques physiques du média**

6. L'architecture TCP/IP:

En comparaison avec le modèle OSI on peut citer l'architecture de communication de donnée qui utilise le protocole TCP/IP qui a émergé comme un standard pour plus de 90% des réseaux actuels. Cette architecture repose sur 4 couches superposées telle définies dans Tableau 2.

Tableau 2 : Architecture utilisant le protocole TCP/IP

7. Couche Application **Application utilisant le réseau**
4. Couche Transport **Assure le transfert d'un site à un autre**
3. Couche Internet **Définie les datagrammes et leur routage**
1. Couche Physique **Ensemble de routine d'accès au média**

Les données sont transférées verticalement d'une couche à une autre en y insérant un entête qui permet de rajouter des informations identifiant le type de données, le service demandé, le destinataire et l'adresse source..

Tableau 3 : Encapsulation des données

Couche Application				Données
Couche Transport			Entête	Données
Couche IP		Entête	Entête	Données
Couche Physique	Entête	Entête	Entête	Données

La notion de protocole se trouve à tous les niveaux des modèles en couches, on appelle protocole l'ensemble des règles et de format prédéfinis déterminant les caractéristiques de communication de processus de la couche.

6.1 La couche physique :

Cette couche a pour fonction l'encapsulation des datagrammes de couche IP et la traduction des adresses IP en adresses physiques utilisées sur le réseau. Elle concerne la manière dont sont transportés les signaux sur le support physique du réseau. A ce niveau, le réseau transporte et reçoit des bits individuels.

6.2 La couche Internet :

La couche au-dessus de la couche physique de la hiérarchie des protocoles est la *couche Internet.* Le Protocole Internet (IP), *RFC 791*, constitue le cœur même de TCP/IP et il s'agit du protocole le plus important de la couche Internet. IP fournit le service de base en matière d'expédition de datagrammes sur lequel les réseaux TCP/IP sont bâtis.
Tous les protocoles situés dans les couches au-dessus ou au-dessous de la couche IP utilise ce protocole pour transmettre les données. Toutes les données TCP/IP passent par IP, que cela soit en entrée ou en sortie, en fonction de leur destination finale.

6.2.1 Le protocole Internet (IP) :

Ce protocole constitue la brique de base de l'Internet. Ses fonctions consistent à :

- Définir le datagramme, unité élémentaire de transmission sur l'Internet
- Définir le système d'adressage Internet
- Faire transiter les données entre la couche d'accès réseau et la couche de transport.
- Router les datagrammes vers les sites distants
- Fragmenter et ré-assembler les datagrammes.

Tableau 4 : Datagramme IP

BITS

0	4	8	12	16	20	24	28 31
Version	I.H.L.	Type de service		Longueur totale			
Identification				flags	Offset de fragmentation		
Durée de vie		Protocole		Checksum de l'entête			
Adresse source							
Adresse destinataire							
Options						Padding	
DONNEES							

* I.H.L : ***I****nternet* ***H****eader* ***L****ength.*

6.2.2 le protocole ICMP (Internet Control Message Protocol):

Une partie intégrante d'IP, définit dans le *RFC 792*, assure un dialogue IP/IP pour transmettre ses messages et pour permettre, notamment le contrôle de flux, la synchronisation des horloges l'estimation des temps de transit et la mise à jour des tables de routage. Ces opérations jouent un rôle informatif pour TCP/IP. Il est à noter que les premiers outils de surveillance et de gestion de réseaux s'appuient sur le protocole ICMP (Ping, Traceroute, etc.).

6.2.3 Le routage IP :

C'est l'une des fonctionnalités principales de la couche IP. Elle consiste à choisir la manière de transmettre un datagramme IP à travers les divers réseaux. D'une manière générale, le routage des datagramme dans un réseau consiste à fixer par quelle ligne de sortie chaque commutateur réexpédie les datagrammes qu'il reçoit. Ceci se fait en fonction de la destination finale du datagramme et selon une table de routage qui indique, pour chaque destination finale, quelles sont les voies de sortie possibles.

6.3 Couche Transport :

Cette couche doit assurer, en mode connecté ou non connecté, un transfert transparent de données.
Les deux protocoles les plus importants de cette couche sont :

-TCP (Transmission Control Protocol)

-UDP (User Datagram Protocol)

Ces deux protocoles permettent la transmission de données entre la couche application et la couche Internet.

6.3.1 Le protocole UDP :

UDP fournit un service de transmission de datagrammes beaucoup moins coûteux en ressource, un peut comme le service de transmission fournit par IP. Ceci permet donc aux application d'échanger des messages à travers le réseau avec un minimum de surcharge due au protocole.
UDP est un protocole datagramme non fiable et en mode non connecté. Le terme non fiable signifie simplement qu'il n'existe aucune technique propre au protocole pour vérifier que les données ont atteint leur destination correctement. Si la quantité de données est réduite, la surcharge générée par la création des connexions et par la vérification de la bonne réception des données peut être supérieure au coût d'une retransmission totale des données. Dans ce cas, UDP est le choix le plus efficace pour un protocole de la couche transport.

Tableau 5 : Entête UDP

0	16 31
Source Port	Destination Port
Longueur	Checksum
Données	

6.3.2 Le protocole TCP :

Les applications, qui ont besoin que le protocole de transport fournisse un système de transmission sûr, utilisent TCP car il vérifie que les données sont correctement transmises à travers le réseau et dans l'ordre d'émission, TCP est un protocole fiable, orienté connexion et utilisant un flot d'octets.
En principe, TCP doit pouvoir supporter la transmission de données sur une large gamme d'implémentation des réseaux.

Tableau 6 : Entête TCP

<table>
<tr><td colspan="4">0 4 8 12</td><td colspan="4">16 20 24 28 31</td></tr>
<tr><td colspan="4">Source Port</td><td colspan="4">Destination Port</td></tr>
<tr><td colspan="8">Numéro de séquence</td></tr>
<tr><td colspan="8">Numéro d'acquittement</td></tr>
<tr><td>Offset</td><td colspan="2">Réservé</td><td>Flags</td><td colspan="4">Fenêtre</td></tr>
<tr><td colspan="4">Checksum</td><td colspan="4">Urgent Pointer</td></tr>
<tr><td colspan="6">Options</td><td colspan="2">Padding</td></tr>
<tr><td colspan="8">Données</td></tr>
</table>

6.4 Couche application :

Cette couche inclut tous les processus qui utilisent les protocoles de la couche transport pour transmettre de l'information, il existe un grand nombre de protocoles applicatifs de ce genre. La plus part fournit des services utilisateurs.
Les protocoles applicatifs les plus connus et les plus fréquemment implantés sont :

FTP (*File Transfert Protocol*) : Utilisé pour transférer des fichiers d'une manière interactive ;

Telnet (*Network Terminal Protocol*) : Permet d'effectuer des login distants à travers le réseau ;

SMTP (*Simple Mail Transfert Protocol*) : Protocole de transport de courrier électronique ;

DNS (*Domain Name Service*) : Cet applicatifs fait correspondre adresse IP et noms de machine et de réseaux ;

NFS (*Network File System*) : Ce protocole permet aux fichiers d'être partagés par plusieurs machines connectées à un réseau.

En résumé :

Nous avons décrit brièvement tout au long de ce chapitre divers éléments clé dont l'assemblage constitue le réseau. La solution TCP/IP est aujourd'hui la plus répandue. C'est une hiérarchie à quatre couches : Application, Transport, Internet et physique. Nous avons examiné la fonction de chacune de ces couches.

L'expérience que nous avons acquise sur les réseaux nous à naturellement conduit à recenser quelques domaines clé auxquels se rapportent l'ensemble des éléments constituant le réseau. Ces différents domaines sont :

- L'administration réseau
- Le système d'exploitation du réseau
- Les services réseaux.

Nous nous proposons dans les chapitres qui vont suivre de décrire quelque domaine clé, ceci permettra d'avoir une vision globale des différentes technique mise en œuvre sur les réseaux.

Chapitre 2

L'administration de réseau

Les réseaux informatiques évoluent actuellement très vite, par leurs technologies et leurs méthodes, et l'administration se trouve toujours confrontée à une multitude d'outils souvent locaux, hétérogènes et en partie manuelle. Or, l'efficacité et l'adéquation de l'administration à la puissance des réseaux gérés, est un enjeu décisif pour la mise en place des réseaux du futur. Ceci passe par une bonne compréhension des rôles et des responsabilités de l'administration ainsi que les limites de son application.

L'administration du réseau se concentre à l'origine sur ce qui se passe après que le réseau soit installé. Bien qu'il soit vrai que l'administration réseau doit inclure la mise en œuvre d'une installation du réseau, à l'origine elle n'était concernée que par l'exploitation du réseau.

Dans ce chapitre, nous allons nous concentrer sur les tâches d'administration réseau de base. La mise en œuvre d'outils administratifs varie d'un système d'exploitation réseaux (NOS) à un autre et chaque NOS fournit un moyen d'accomplir ces fonctions administratives de base. Dans ce qui suit, Nous avons choisi de traiter les taches d'administration réseau, dans l'ordre qu'un administrateur qui installe un nouveau système d'exploitation réseau aurait besoin typiquement de les adresser.

1. Définition :

Une définition précise de l'administration des réseaux est ambitieux, par contre on peut se pose la question de savoir pourquoi on a besoin d'une administration de réseau.

La définition d'une administration de réseau ne peut pas être universelle. Actuellement, il en existe plusieurs qui dépendent essentiellement des critères choisis. Mais on peut dire que l'administration d'un réseau consiste en un ensemble d'éléments matériels, logiciels, et humains nécessaires à la maîtrise et au contrôle du fonctionnement, de l'évolution et des coûts de l'architecture du système. [2]

D'une façon générale, une gestion réseau a pour objectif d'englober un ensemble de techniques de gestion mise en œuvre.

Le premier objectif important à atteindre est la disponibilité du réseau, on imagine bien qu'il est important pour les clients utilisateurs d'avoir un réseau opérationnel, car une indisponibilité du réseau aussi courte soit-elles peut avoir une incidence directe sur les transactions qui s'effectuent à travers le réseau.

Un autre objectif important est de pouvoir tirer le meilleur parti du réseau, d'optimiser son utilisation et donc d'augmenter le rendement global du système.

Le troisième objectif est de donner à l'administrateur du réseau la possibilité d'améliorer l'utilisation des éléments d'interconnexion et des lignes de communication c'est a dire de permettre l'évolution du système en incluant de nouvelles fonctionnalités.

2. Les disciplines :

Les disciplines de l'administration de réseau sont actuellement regroupées autour de trois grands axes :

- L'administration des utilisateurs.
- L'administration des serveurs ou fournisseurs des services.
- L'administration de la machine de transport liant les utilisateurs aux fournisseurs.

a. L'administration des utilisateurs :

l'administrateur doit permettre a l'utilisateur de se connecter aux différentes applications. Pour ce la, le système d'administration réseau doit disposer d'un ensemble d'outils qui permettent d'assurer la transparence des méthodes d'accès et de connexion aux différentes applications, la localisation des ressources, leur fonctionnement et leur utilisation.

Le système d'administration réseau doit, aussi, fournir l'ensemble des mécanismes qui permettent de garantir la confidentialité des informations de l'utilisateur, de sécuriser son environnement, et de prévenir toute perte ou altération des échanges effectués par l'utilisateur.

b. L'administration des serveurs :

recouvre l'ensembles des mécanismes a mettre en place pour bien garantir la fiabilité de transmission des informations sur le réseau et offre un certain nombre d'outils de transfert de ces informations. Il permet aussi de contrôler et de protéger l'accès à ces applications par une distribution de droits.

c. L'administration de la machine de transport :

permet de fournir des mécanismes de détection et de correction. Si une alerte est déclenchée, des actions doivent être prises pour résoudre rapidement le problème et réduire son influence sur la qualité de service. On doit, dans ce cas tenir à jour en permanence la liste des éléments (logiciel et matériels) qui constituent un système réseau.

3. Architecture d'un système de gestion des réseaux :

un système de gestion des réseaux est bâti sur une collection d'outils (contrôles, surveillance) pour assurer le bon fonctionnement et la meilleur productivité du réseau.

Il n'existe pas de règle précise à appliquer pour définir l'architecture d'un système de gestion de réseau, par contre les points suivants doivent être considérés lors du développement d'un tel système :

- Le système doit posséder une interface graphique pour mieux visualiser la hiérarchie du réseau et d'établir le lien logique entre ses niveaux hiérarchiques.
- Le système doit être capable de retirer des informations a partir de tous les dispositifs connectés au réseau.
- Le système doit être facile a étendre et a personnaliser : puisque il n'existe pas un système universel pour tous les types de réseaux, le système doit permettre l'ajout de nouvelles applications.

- Le système doit posséder une base de données relationnelle dans laquelle on peut sauvegarder toute sort d'information requise par les applications de gestion.
- Le système doit être capable a détecter les problèmes qui peuvent survenir dans le réseau.

Selon ces aspects, trois architectures de système de gestion des réseaux ont été établies :

a. **Architecture centralisée :** chaque application dans cette architecture doit enregistrer ses données sur un support de stockage commun de la machine centrale.

b. **Architecture distribuées :** cette architecture regroupe plusieurs systèmes de gestion où chaque application gère uniquement une partie du réseau et enregistre ses données dans son propre support.

c. **Architecture hiérarchique :** c'est un mixage des deux architectures précédentes, le système central correspond à la racine hiérarchique, les systèmes distribués correspondent aux autres branches de la hiérarchie et c'est l'architecture la plus flexible.

4. Les principales fonctions de ISO :

les fonctions d'administration du réseau doivent permettre de récolter un grand nombre d'information sur les différents éléments du réseau puis réduire leurs volume en sélectionnant, seulement, les informations significatives. Les informations retenues sont stockées dans une base de données d'administration. Pour extraire ces informations il faut mettre à la disposition de l'administrateur et de l'opérateur du réseau une interface utilisateur qui leur permettra de traiter ces informations.
Selon l'organisation internationale de standardisation (ISO) l'administration du réseau peut être cernée par les axes ou grands domaines fonctionnels de base suivants :

- la gestion des pannes.
- la gestion des performances.
- la gestion de la configuration.
- la gestion de la compatibilité.
- la gestion de la sécurité.

4.1 La gestion des pannes :

C'est le processus de localisation et de correction des problèmes du réseau. Une panne est définie comme toute anomalie qui affecte le bon fonctionnement des opérations du réseau. Le processus de la gestion de panne commence quand une faute suspecte est rapportée. Juste après, une analyse des symptômes rapportés est effectuée pour identifier le problème. Après que le problème soit identifié et bien défini, la source de la faute doit être isolée pour que l'action corrective adéquate puisse être prise.

Quelques problèmes sont identifiables facilement, mais d'autres peuvent être causés par l'interaction de plusieurs facteurs. Parfois, le processus du dépannage des problèmes causés par un seul facteur, peut s'avérer difficile si le problème est intermittent.
La gestion des pannes est la tâche, de l'administrateur du réseau, la plus importante. Sans procédures adéquates pour la gestion des pannes, les administrateurs du réseau peuvent se retrouver à passer tout de leur temps à garder le réseau opérationnel. de manière globale la gestion des pannes est composé de deux phases : la prise en compte d'un problème et sa résolution.

4.2 La gestion des configurations :

C'est le processus qui consiste à rassembler des informations sur le réseau, et de les utiliser pour optimiser l'utilisation des différents éléments du réseau. Elle permet un contrôle de la configuration du point de vue fonctionnel et opérationnel, le suivi et la réalisation des modifications apportées dans le cadre de la maintenance. Elle permet, aussi, de localiser sans ambiguïtés tout élément dans le réseau.
Les tâches de gestion de la configuration communes incluent la tache de maintenir un inventaire à jour de tout le matériel installé dans le réseau. La gestion de la configuration est une fonction préalable à la gestion de la performance.

4.3 La gestion des performances :

C'est le processus qui permet d'évaluer la performance des composants matériels et logiciels du réseau.
La performance d'un réseau peut être mesurée par deux paramètres : le temps de réponse et la disponibilité du réseau. Le temps de réponse du réseau est le temps de réponse nécessaire à un système pour réagir à une sollicitation d'un utilisateur. La disponibilité se traduit généralement par le mesure du temps pendant lequel un réseau ou un élément du réseau est disponible ou n'est pas disponible pour les utilisateurs, entre d'autre termes, par le temps moyenne entre deux pannes successives.
De manière générale, toute activité associée à la maintenance, à l'amélioration la vitesse du réseau, à l'amélioration de la sensibilité, et à l'amélioration de la faculté d'adaptation d'un réseau, est liée à la gestion de la performance.

4.4 La gestion de la compatibilité :

comporte quatre grandes fonctionnalités concernant :

- la charge des ressources, dont le rôle est de déterminer et de surveiller la charge admissible des ressources,
- le coût des ressources, dont l'objet est de déterminer le prix d'utilisation des ressources,
- la facturation, dont le rôle est de récupérer l'ensemble des informations de coût imputable à un utilisateur,
- la gestion des limites utilisateur, qui consiste à déterminer et à surveiller les quotas d'utilisation des ressources par les utilisateurs.

4.5 La gestion de sécurité :

Une des fonctions principales de l'administration réseau, comprend essentiellement la sécurisation de l'accès au réseau lui-même. Il s'agit d'utiliser des mécanismes de sécurité tel que le contrôle d'accès (par authentification), pour protéger les informations et les ressources partagées.
L'essentiel de la fonction sécurité d'un système d'administration de réseau consiste a organiser des listes de contrôles d'accès d'une manière cohérente en fonction des différents types d'utilisation, et a planifier leur évolution en fonction de l'évolution de l'organisation de l'entreprise.

5. Le besoin d'un outil d'administration :

La complexité des réseaux peut être analysée selon deux directions : l'évolution de la taille des réseaux et la complexité des équipements utilisés. Bien que les serveurs existent toujours, les terminaux sont devenus plus intelligents. Ces deux aspects sont a l'origine du besoin d'outils qui permettent leurs exploitations. Les efforts de homme, seuls, ne sont pas suffisants pour gérer un grand réseau composé de diffèrent moyens de communication. L'utilisation d'outils d'administration est plus que nécessaire.
Les considérations énoncées ci-dessus permettent d'identifier les besoins de l'administration de réseaux :

- S'adapter à toutes les tailles de réseaux.
- Gérer des équipements hétérogènes et plus ou moins complexes.
- Permettre les opérations de gestion à distance.
- Assister l'utilisateur en :
  - automatisant certaines tâches.
  - aidant l'utilisation dans les tâches qui ne sont pas automatisées.
- Fournir une vue adaptée du réseau selon les opérations à réaliser.

6. L'organisation d'une administration :

Administrer un réseau, c'est tirer le meilleur partie de la structure que l'on utilise. Il s'agit d'un système dual car la conception d'une administration dépend étroitement de la structure à gérer, mais le comportement futur de cette structure dépendra de son administration.
Il existe différents types de décision d'administration :

- **décisions opérationnelles :** décisions à court terme, concernant l'administration au jour le jour et opérations temps réel sur le système.
- **décisions tactiques :** décisions à moyen terme concernant l'évolution du système et l'application des politiques à long terme.
- **décisions stratégiques :** décision à long terme concernant les stratégies pour le futur en exprimant les nouveaux besoins des utilisateurs.

Selon ces types de décision l'organisation a quatre niveaux hiérarchiques d'administration :

- **le service de gestion du réseau réel :**qui permet de représenter l'interface directe avec les informations provenant du système géré, dans ce cas le système fait le contrôle opérationnel (décisions opérationnelles) son rôle consiste essentiellement à :
  - collecter des données,
  - prendre en compte des alertes et notifier des événements,
  - déterminer les problèmes,
  - faire le recouvrement du réseau,
  - contrôler la configuration,
  - activer, désactiver ou redémarrer des éléments,
  - effectuer la maintenance technique.

- **le service de gestion du réseau logique :** représente le lien entre les décisions opérationnelles et les décisions tactiques, elle s'appuie sur une source d'information stockée dans une base de données de gestion. Son rôle consiste à :
  - comprimer les informations de gestion,
  - maintenir l'inventaire,
  - gérer et interpréter les tickets de trouble,
  - évaluer le trafic,
  - contrôler la sécurité,
  - gérer les modifications.

- **le service de gestion de performance :** Il s'appuie également sur une base de données de gestion, il représente le lien entre les décisions tactiques et stratégiques son rôle consiste à :
  - établir et maintenir une base de données des performances,
  - analyser et régler le système,
  - définir les indicateurs de performance.

- **le service de gestion de la planification :** Il s'appuie sur une base de données de gestion, et répond aux décisions stratégiques. Son rôle consiste à :
  - établir les besoins,
  - étudier et déterminer une solution,
  - planifier l'implémentation de cette solution.

Cependant, quelle que soit l'organisation mise en place, elle doit répondre aux critères qui la gouvernent.

Comme le montre la figure 2.1, l'accent à été mis sur les aspects informationnels, temporels et la nécessité des différents services de gestion.

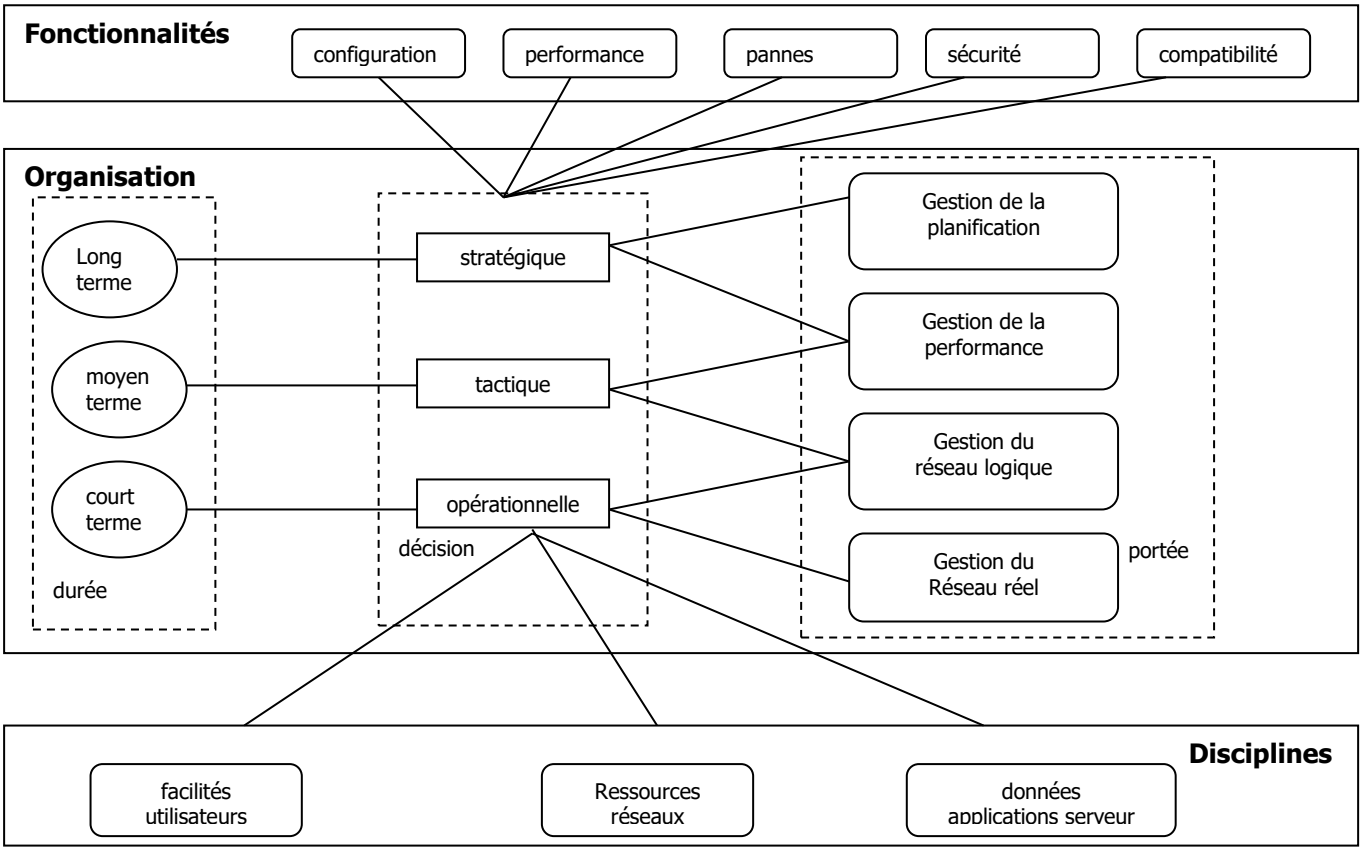

Fig.2.1 Organisation globale

En résumé :

Le système de gestion nécessite une définition de sa structure, de son fonctionnement et de son organisation. Certaines opérations devant pouvoir être réalisées en dépit d'une quelconque panne. De plus, des contraintes de temps réel sont souvent à prendre en compte. Ce chapitre a présenté les fondements théoriques en terme de l'administration réseau, les disciplines et les fonctions de base qui doivent être prise en charge par l'administrateur ainsi que les différentes architectures des systèmes de gestion de réseau et l'organisation d'une administration.

Chapitre 3

La plate-forme Windows NT

Windows NT ayant beaucoup évolué ces dernières années, il est mieux accepté par le marché. Il est considéré comme le système d'exploitation le mieux adapté pour les ordinateurs de bureau haut de gamme. Il met en œuvre un ensemble d'idées qui proviennent de différents produits et travail en grande partie comme UNIX. Sa conception satisfera la plupart des administrateurs critiques, en plus il est moins cher qu'UNIX dans de nombreux cas. En comparaisons avec Linux, Linux est un système gratuit,il est plus populaire et le plus facile à obtenir.L'inconvénient de Linux est peut être le fait qu'aucun société n'est en charge de son développement, il n'existe pas de service après vente et il ne fait aucun doute que l'absence d'aide technique peut s'avérer un problème avec l'utilisateur.
La persévérance de Microsoft a été couronnée de succès, puisque Windows NT est devenu un produit complet, fiable, et fonctionnant bien.
Comme Windows NT peut être une plate-forme de bureau, serveur réseau, beaucoup d'entreprise le considère comme une opportunité de consolider leur réseau à partir d'un système d'exploitation unique, convivial et puissant.

Dans ce chapitre, nous allons présenter une description rapide des dispositifs de Windows NT. La compréhension de son architecture nous conduira à la compréhension de ses possibilités.

1. Caractéristiques de Windows NT :

Windows NT présente de nombreux dispositifs qui le placent parmi les systèmes d'exploitation pour micro ordinateurs et station de travail au plus haut niveau. La plupart de ces dispositifs sont tout à fait souhaitables sur les stations de travail et essentiels pour un serveur de réseau.
Quand le projet de Windows NT a été commencé, Microsoft voulait assurer que le Windows NT serait un système d'exploitation du réseau avancé avec la modernité inhérente et flexibilité pour survivre bien dans le futur. Ils ont, ainsi, défini plusieurs caractéristique importantes qui sont : Robustesse, portabilité, compatibilité, performance et sécurité.

- **Robustesse :**

  La robustesse de Windows NT provient d'une somme d'expériences acquises dans la conception de systèmes d'exploitation.
  Windows NT inclut quelques-uns des dispositifs les plus fiables tel que le dispositif de restauration des registres utilisé pour enregistrer la configuration des données sur le serveur.
  Parmi ces dispositifs on trouve la capacité à dupliquer automatiquement les répertoires sur les serveurs et la capacité de configurer RAID (Redundant Arrays of Inexpensives Disks) qui améliore les performances et la tolérance de panne de disque durs.
  Windows NT fournit une plate-forme extrêmement stable pour les services du réseau de l'entreprise.

- **Portabilité :**

La majorité des systèmes d'exploitation sont écrits pour un matériel spécifique. Windows NT est probablement le système le plus portable parmi les systèmes d'exploitation sur le réseau et ce, pour deux raisons de conception. Tout d'abord, le programme est écrit en C, un langage qui lui permet d'être porté aisément sur tous les matériels. Ensuite, toutes les parties de Windows NT qui doivent être écrites pour un matériel particulier doivent être isolées dans une zone appelée Hardware Abstraction Layer (HAL).

Windows NT est déjà disponible pour de très nombreuses plates-formes :

- Intel x86,
- ordinateurs d'architecture MIPS RISC,
- calculateurs Digital Alpha AXP RISC,
- ordinateurs PowerPC RISC.

- **Compatibilité :**

Windows NT supporte une grande variété de programmes, y compris les programmes écrits pour les systèmes d'exploitation standards suivants :

- MS-DOS,
- Application 16-bits Windows,
- Application 32-bits Windows,
- OS/2 (en partie),
- POSIX, une interface de type UNIX.

Et aussi, Windows NT intégre des protocoles permettant de fournir des services réseaux avec d'autres systèmes d'exploitation tel que Netware, UNIX, OS/2 et Windows 9x.

- **Performance :**

Windows NT a été conçu pour fournir un haut niveau de performance système et dispose de quelques caractéristiques qui lui permettent d'être un environnement concurrentiel. Parmi ces caractéristiques on peut citer :

- *Grande capacité de mémoire* : Windows NT peut gérer jusqu' à 4 Go de mémoire,
- *Multitâche et multiflot* : le fonctionnement multitâche donne l'illusion de faire plusieurs choses à la fois, tandis que le multiflot le fait réellement. Ce type de fonctionnement tire parti de la capacité de certains processeurs d'exécuter deux ou plusieurs tâches appelées flot dans des zones distinctes de la mémoire.

  Windows NT autorise les applications à démarrer leur propre flot. Une tâche complexe peut se diviser en plusieurs sous-tâches qui pourront être exécutées simultanément et concourir ensemble à produire un résultat. Des applications multiflots peuvent produire plus de résultats dans un délai donné qu'une application multitâche.
- *Support des multiprocesseurs :* Windows NT peut exploiter jusqu'à 255 processeurs, cela permet d'ajouter des processeurs pour augmenter la performance du système.

- **Sécurité :**

Windows NT peut être configuré pour obtenir un très haut niveau de sécurité.
La sécurité sur Windows NT est beaucoup plus fine, l'administrateur détermine qui a le droit d'accéder au réseau et quels sont les fichiers auxquels chacun peut accéder, le contrôle est effectué au niveau du fichier. Windows NT a, aussi, introduit le nouveau système de gestion de fichier NTFS (New Technology File System) qui améliore les performances du réseau, la sécurité de fonctionnement et l'accès.
NTFS compense les défaillances des disques en utilisant un dispositif qui automatiquement redirige les données d'un mouvais secteur du disque vers un secteur de substitution et introduit la sécurité dans le système de gestion des fichiers. Pour accéder aux fichiers, un utilisateur doit avoir un compte et un mot de passe.

2. Organisation d'un réseau NT :

Si les réseaux étaient toujours simples, s'ils ne comprenaient jamais plus d'un seul serveur ou quelques utilisateurs, il serait facile de les administrer et de les utiliser. Toutes les ressources seraient groupées en un seul endroit, et tous les utilisateurs en un même lieu géographique. Il n'y aurait pas de confusion quand à la localisation d'une ressource, ni à la manière de l'atteindre.
De nombreux réseaux ne sont, cependant, pas simples. Ils comportent de multiples serveurs et s'étendent souvent sur plusieurs lieux, les serveurs stockant très souvent plusieurs giga-octets de fichiers, les utilisateurs ne savent pas où chercher ce qu'ils veulent. Les concepteurs de réseaux ont, néanmoins, cherché les meilleurs façon de simplifier la localisation des ressources de réseau.
Les réseaux locaux offrent des services à travers le partage des ressources de poste à poste ou à travers les serveurs centraux. Quelle que soit la méthode utilisée, elle doit permettre aux utilisateurs de localiser les ressources disponibles.
Cette section examine quelques-unes des techniques utilisées par le concepteur de Windows NT pour organiser les ressources de réseaux :

- Services d'annuaires,
- Groupes de travail,
- Domaines.

Ces éléments de base permettant de bâtir des réseaux d'entreprise facile à gérer et à utiliser.

2.1 Services d'annuaires :

Un annuaire réseau fonctionne à l'instar des pages jaunes de l'annuaire téléphonique. Les ressources peuvent être groupées logiquement pour rendre leur localisation plus facile. Les utilisateurs peuvent consulter l'annuaire pour rechercher l'information qu'ils désirent obtenir ou naviguer dans l'annuaire de façon intelligente.
Le concept d'un service d'annuaire est attrayant. Au lieu d'ouvrir une session sur plusieurs serveurs, un utilisateur en ouvre une seule sur le réseau pour accéder à toutes les ressources réseaux offertes par le service d'annuaire, quel que soit le serveur qui le fournit. L'utilisateur ne voit que l'annuaire réseau. Un service d'annuaire est une manière très formelle d'organiser les ressource réseau.

2.2 Groupes de travail :

Les groupes de travail sont à l'opposé des services d'annuaires. Alors que ces derniers sont formels et se prêtent à l'administration centralisée, les groupes de travail sont informels est sont contrôlés par les utilisateurs qui mettent en commun leurs ressources informatiques.
Un groupe de travail est un ensemble d'ordinateurs et d'utilisateurs connectés ensemble de façon à partager des ressources communes. Chaque utilisateur a sa propre base d'annuaire pour gérer ses ressources et ses utilisateurs.

La mise en œuvre est simplifiée, mais il faut administrer séparément chaque utilisateur, cette solution convient à un petit nombre de machine pour des utilisateur travaillant en commun et n'ayant pas besoin d'une sécurité centralisée. Des utilisateurs individuels gèrent le partage des ressources sur leur PC, en déterminant ce qui sera partagé et qui aura l'autorisation d'accès.

2.3 Domaines :

Les domaines empruntent les concepts de groupes de travail et de services d'annuaire. Comme les groupes de travail, les domaines peuvent être assez informels et administrés en utilisant un contrôle à la fois centralisé et local et comme l'annuaire, le domaine organise les ressources de plusieurs serveurs en une structure administrative. Les utilisateurs reçoivent les privilèges d'ouvrir une session sur un domaine plutôt que sur chacun des serveurs individuels. Chaque domaine doit avoir :

- Un contrôleur principal de domaine (CPD) sur lequel est administrée la base de données d'annuaire. Un CPD est un serveurs Windows NT qui stocke la copie maître de la base de données des utilisateurs et de groupes du domaine.
- Un ou plusieurs contrôleurs secondaires de domaine (CDS) et aussi un serveur Windows NT. Ils peuvent stocker les copies de base de données d'annuaire et ils se repartissent, avec le CPD, la tâche d'authentification des utilisateurs au moment de l'ouverture d'une session.

Les domaines sont essentiellement des groupes de travail améliorés, l'accès aux ressources du domaine est contrôlé par le contrôleur de domaine. L'utilisateur se voit assigné un seul compte de domaine ainsi qu'un mot de passe contrôlant l'accès à toutes les ressources du domaine.
Les domaines de Windows NT supportent aussi l'utilisation de groupes permettant aux administrateurs d'assigner et de changer les permissions pour un grand nombre d'utilisateurs de façon plus efficace.

2.4 Relation d'approbation :

De nombreuses organisations possèdent plusieurs serveurs de réseaux locaux, ce qui ne pose pas de problème puisque les domaines permettent d'administrer facilement les serveurs multiples. Mais ceci pourrait conduire une organisation à avoir besoin d'établir deux domaines ou plus. Par exemple :

- Si de nombreux serveurs sont placés dans un domaine, la performance peut en souffrir.
- Pour de meilleures performances, la base de données du domaine ne doit pas excéder 40 Mo, limitant ainsi le nombre de stations de travail, d'utilisateurs et de groupe.
- Certains départements préfèrent gérer leurs propres ressources.

Chaque domaine a ses propres utilisateurs. Mais les utilisateurs souhaitent travailler non seulement dans leur domaine, mais aussi dans un autre domaine. Pour pouvoir communiquer d'un domaine à l'autre, il faut établir des relations d'approbation entre ces domaines.

Heureusement, Windows NT permet d'établir des relations d'approbation entre domaines. La figure 3.1 illustre une simple relation d'approbation entre deux domaines. Le domaine B est configuré pour approuver le domaine A. L'approbation peut jouer dans les deux sens. Figure 3.2, les domaines C et D sont configurés pour s'approuver mutuellement.

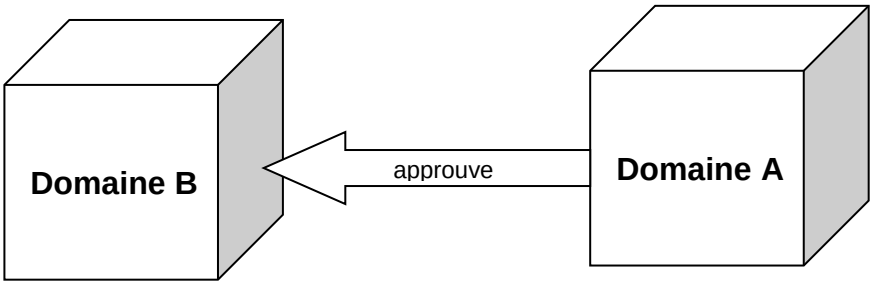

Fig.3.1 Une relation d'approbation simple

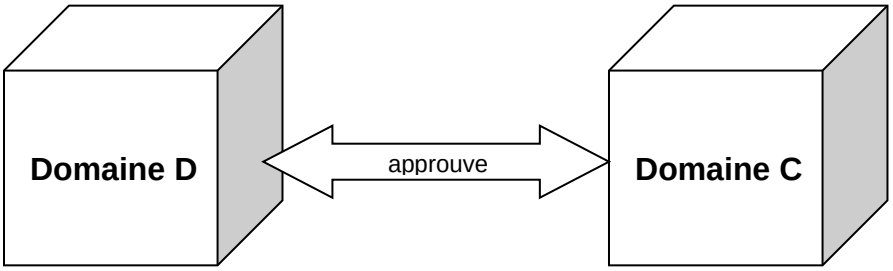

Fig.3.2 Domaines configurés pour s'approuver mutuellement

3. Utilisateurs et groupes :

Les comptes d'utilisateurs permettent aux utilisateurs un accès au serveur et ses ressources, les droits et les permissions accordées à ces comptes permettent de faire des actions appropriées et définissent les restrictions adéquates qui sont nécessaires aux différentes ressources.

Un compte contient des informations sur l'utilisateur notamment son nom, son mot passe et diverses entrées facultatives qui indiquent quand et comment l'utilisateur ouvre une session.

Un groupe rassemble plusieurs utilisateurs, y compris d'autre groupes, il y est définit les droits et les permissions de ses membres. Tout utilisateur appartenant à un groupe bénéficie des même droits accordés au groupe.

L'information des comptes utilisateurs et groupes est enregistrée dans la base de données du domaine, entretenu par le CPD. Chaque compte utilisateur et groupe est identifié par une identité de sécurité (SID).

Le SID est un nombre généré par Windows NT lorsque le compte est créé.

La sécurité de Windows NT est basée sur les quatre types d'entités suivantes :

- Comptes utilisateurs locaux,
- Comptes utilisateurs globaux,
- Groupes locaux,
- Groupes globaux.

3.1.1 Comptes utilisateurs locaux :

Les entités locales ne peuvent pas être utilisées hors du domaine où elles ont été créées. Ces comptes peuvent cependant être placés à la fois dans les groupes globaux et locaux.

- ce compte est mémorisé dans l'annuaire local de la machine,
- son nom doit être unique sur cette machine.

Cependant, ces comptes sont un peut plus difficiles à administrer que les comptes globaux.

3.1.2 Comptes utilisateurs globaux :

Dans la terminologie de Windows NT, une entité globale peut être utilisée par des domaines autres que celui où elle a été créée. Ils constituent le type de compte le plus utilisé sur les réseaux Windows NT.

Les comptes utilisateurs globaux peuvent obtenir des privilèges réseau sur la base individuelle, il est, néanmoins, plus fréquent d'inclure ces comptes dans des groupe et de leur accorder des privilèges de groupe. Cette méthode s'avère plus pratique pour modifier les privilèges d'un grand nombre d'utilisateurs.

- ce compte est mémorisé dans le CDP et recopie dans le CDS,
- son nom doit être unique sur tout le domaine.

3.1.3 Comptes utilisateurs prédéfinis :

Windows NT possède deux comptes utilisateur par défaut :

Le *compte utilisateur de l'administrateur* permet de gérer le serveur quand il est créé lors de la première fois installation pour permettre l'accès au serveur. C'est le compte du responsable de réseau, le gestionnaire du domaine. Ce compte ne peut être détruit ni désactivé, bien qu'il puisse être renommé.

Le *compte utilisateur invité* ne peut être supprimé, mais il peut être fermé et renommé. Ce compte est fermé par défaut, mais il peut être ouvert si vous désirez autoriser l'accès à votre domaine ou serveur à des utilisateurs invités.

3.2.1 Groupes locaux :

Ce sont les groupes locaux qui donnent aux utilisateurs les accès aux ressources (dossiers, fichiers, imprimantes,…etc.) et permettent aussi de lancer des tâches système sur une machine (gestion de dossier, copies des fichiers, sauvegardes,…etc.).
Les groupes locaux peuvent contenir à la fois des utilisateurs et des groupes globaux. Cette fonctionnalité permet d'utiliser un groupe local pour rassembler des entités issues de plusieurs domaines et de les gérer comme un groupe dans le domaine local. Tous les utilisateurs et les groupes globaux dans le groupe local héritent des mêmes privilèges du groupe local.

3.2.2 Groupes locaux prédéfinis :

Les groupes prédéfinis sont des groupes qui ont des droits d'utilisateur déterminés. Ces groupes ne peuvent pas être supprimés ou renommés.
Les serveurs Windows NT possèdent les groupes locaux suivants :

- *Administrateur :* les membres du groupe local d'administrateurs ont pratiquement toute autorité sur le domaine, la station de travail ou le serveur où le groupe est localisé.
- *Utilisateur :* la plupart des utilisateurs seront membres du groupe local des utilisateurs. Les membres de ce groupe ne peuvent entrer en session sur le contrôleur de domaine principale ou de sauvegarde. Cependant, ils peuvent ouvrir des sessions sur les domaines, stations de travail et serveurs.
- *Utilisateur avec pouvoir :* les membres du groupe utilisateurs avec pouvoir peuvent travailler sur les stations de travail et les serveurs en tant qu'utilisateurs. Ils peuvent créer des comptes utilisateurs et modifier les comptes qu'ils ont créés. Les utilisateurs avec pouvoir peuvent ajouter des comptes utilisateurs aux groupes prédéfinis utilisateurs, invités et utilisateurs avec pouvoir. Ils peuvent également démarrer et arrêter le partage des imprimantes et des fichiers sur les stations de travail et les serveurs.
- *Opérateur de sauvegarde :* ce groupe résout un vieux problème dans l'administration des réseaux locaux. Souvent, les sauvegardes sur bandes magnétiques sont effectuées par des opérateurs qui n'ont pas besoin de privilèges d'administrateur. Les membres du groupe des opérateurs de sauvegarde peuvent sauvegarder et restaurer des fichiers, ouvrir une session locale et arrêter le système, mais ils ne sont pas autorisés à manipuler la sécurité ou remplir d'autres fonctions administratives.
- *Duplicateur :* les membres de ce groupe peuvent effectuer la duplication de fichiers dans le domaine, sur la station de travail ou le serveur.
- *Invités :* ils peuvent utiliser les ressources du domaine, mais ne peuvent le faire qu'en ouvrant une session à travers le réseau, l'ouverture de sessions locales sur le serveur est interdite. Les membres du groupe des invités sur les stations de travail et serveur on des droits limités. Ils ne peuvent pas gérer des groupes locaux, ni verrouiller la station de travail.

Les contrôleurs de domaine comportent les groupes locaux suivants :

- *Opérateurs de serveur :* les utilisateurs de ce groupe peuvent effectuer beaucoup de tâches administratives, à l'exception de la sécurité. Ils peuvent rendre les ressources partageables ou non, formater les disques sur serveur, sauvegarder et restaurer les fichiers, ouvrir des sessions locales sur les serveurs et arrêter ces derniers.
- *Opérateurs de comptes :* les opérateurs de comptes peuvent gérer les comptes utilisateurs et les groupes dans le domaine. Ils peuvent créer, supprimer et modifier la plupart des utilisateurs des groupes locaux et globaux, mais ne peuvent pas donner de droit d'accès aux utilisateurs. Ils ne peuvent pas gérer les comptes des administrateurs ou modifier les administrateurs de groupes locaux, les opérateurs de serveur, les opérateurs de comptes, les opérateurs de sauvegarde ou d'impression.
- *Opérateurs d'impression :* les membres du ce groupe peuvent partager, arrêter de partager et gérer les imprimantes fonctionnant sur un domaine Windows NT. Ils peuvent ouvrir des sessions locales sur le serveurs et arrêter ces dernières.

3.2.3 Groupes globaux :

Les groupes globaux sont des listes de comptes utilisateurs. Ils permettent d'organiser ses comptes dans un seul domaine selon leur fonction et leur localisation. Un groupe global peut comporter des comptes utilisateurs provenant uniquement du domaine où le groupe global a été ajouté aux groupes locaux pour transmettre les droits à ces membres, il doit toujours être créé sur le CDP.

- Les groupes globaux ne peuvent pas contenir les utilisateurs appartenant à d'autre domaine.
- Les groupes globaux ne peuvent pas contenir d'autres groupes.

3.2.4 Groupes globaux prédéfinis :

Les contrôleurs du domaine comportent les groupes globaux suivants :

- *Administrateurs de domaine* : chaque domaine inclut un groupe global prédéfinis nommé "admins". Ce groupe est ajouté automatiquement au groupe local des administrateurs, ce qui fait que tous les membres du groupe admins sont des administrateurs du domaine.
- *Utilisateurs de domaine* : tous les comptes utilisateurs dans un domaine sont automatiquement inclus dans le groupe global des utilisateurs du domaine. Ce dernier est à son tour inclus dans le groupe local des utilisateurs. Dans les réseaux multi-domaines, on peut inclure le groupe des utilisateurs du domaine dans les groupes d'utilisateurs locaux des autres domaines qui approuvent le domaine entré en session. C'est une façon simple d'accorder des privilèges d'utilisateur sur des domaines multiples.
- *Invités du domaine* : l'utilisateur invité est normalement inclus dans le groupe global des invités du domaine, lui même inclus dans le groupe local des invités.Les membres de ce groupe ou ceux du groupe des invités ont des privilèges d'invités dans le domaine.

4. Services sous Windows NT :

Certains serveurs réseau fournissent des services essentiels à des machines clientes. Au contraire des services applicatifs, ces services ne sont pas directement accessibles aux utilisateurs, ils sont utilisés par les machines reliées au réseau pour simplifier leur installation, leur configuration ainsi que leurs opérations sur le réseau.
TCP/IP fournit certains services réseaux qui permettent d'accomplir les tâches précédentes.

Les fonctions réalisées par ces serveurs et décrites dans cette section sont particulièrement variées :

- Service de nom pour convertir les adresses IP en noms de machines, comme le DNS a été développé pour servir de dépôt central de noms sur Internet, il s'agit d'un système de base de données distribuée et hiérarchique qui fournit les noms de machines et leur adresses pour toutes les machines reliées à l'Internet.
- Serveurs de configuration simplifiant l'installation de machines réseau qui gèrent une partie (ou toute) la configuration TCP/IP. DHCP offre l'ensemble complet des paramètres de configuration TCP/IP pour un administrateur réseau permettant de le contrôler à partir d'une machine centrale. Il fournit également un système d'allocation dynamique d'adresses permettant une utilisation maximale d'un réseau avec un nombre restreint d'adresses.
- Serveurs de courrier électronique permettent de faire transiter les messages à travers le réseau. SMTP est un simple protocole de question/réponse qui fournit un système de transmission de courrier entre la machine émettrice et la machine destinataire. Parfois, une telle transmission n'est pas possible et le courrier doit être routé vers un serveur de courrier.
- Serveurs de fichier et d'impression rendent le réseau beaucoup plus pratique pour les utilisateurs. Avec le partage de fichiers, les utilisateurs et les programmes accèdent aux fichiers situés sur des machines distantes comme s'il s'agissait de fichiers locaux. Un serveur d'impression permet aux imprimantes d'être partagées par tous les utilisateurs du réseau.

Tous les services présentés peuvent être installés sur Windows NT.
Windows NT est devenu une plate-forme populaire pour la fourniture de services réseau et permet aux clients une utilisation maximale et optimale de ces services ainsi que des ressources du réseau.

5. Partage des ressources :

Les utilisateurs peuvent bénéficier des services réseau par la mise en place de partage des ressources.

Partager est la technique de base utilisée par tous les produits réseau de Microsoft afin de rendre les répertoires et les fichiers sur les serveurs accessibles aux clients.
Windows NT offre la possibilité de partager des fichiers dans un environnement centralisé et robuste. Un très haut niveau de sécurité peut être ainsi obtenu, et les fichiers sont stockés sur des serveurs centraux où ils peuvent être atteints par de nombreux utilisateurs.

La sécurité de Windows NT est basée sur quatre séries de possibilités offertes aux utilisateurs :

- **Aptitude :** les utilisateurs les obtiennent lorsqu'ils sont assignés à des groupes prédéfinis.
- **Droits :** initialement assignés aux groupes prédéfinis, mais peuvent être assignés aux groupes ou utilisateurs par l'administrateur.
- **Partage :** ensemble de fichiers partagés sur le réseau et auxquels peut être assigné une sécurité au niveau du partage.
- **Permissions :** caractéristique du système de fichiers qui peuvent être assignées aux groupes ou directement aux utilisateurs.

Les administrateurs se préoccupent rarement des droits et n'ont pas de contrôle direct sur les aptitudes, le grand travail consiste à mettre en place des fichiers partageables et à en déterminer les permissions.
Les permissions de partage de dossier permettent de contrôler qui peut y accéder et qu'est ce qu'il peut faire. Tout utilisateur autorisé a alors accès aux fichiers et au sous dossiers contenus dans le dossier partagé.
Chaque partage doit avoir un nom unique. Si on en crée deux ou plus pour le même répertoire, il faut s'assurer que le nom de partage et le commentaire expliquent bien à quoi sert chaque partage, et qui peut l'utiliser.

5.1 Permissions des partages :

Les permissions de partage établissent un ensemble maximum de permissions disponibles à l'intérieur d'une arborescence de répertoires partagés. D'autres attributions de permissions peuvent en restreindre l'accès, mais ne peuvent pas s'ajouter aux permissions établies par les permissions de partage.
Trois types de permissions peuvent être assignés aux répertoires partagés :

- **Lire :** les utilisateurs ont les possibilités suivantes :
  - Lister les dossiers et fichiers
  - Ouvrir des sous-répertoire
  - Lire les données des fichiers et leurs attributs
  - Exécuter les fichiers de programme.
- **Modifier :** les utilisateurs ont les possibilités suivantes en plus de Lire :
  - Créer des sous-répertoires et fichiers
  - Modifier le contenu des fichiers de données
  - Modifier les attributs de sous-répertoires et fichiers
  - Supprimer des sous-répertoires et fichiers.
- **Contrôle total :** les utilisateurs ont les permissions Modifier ainsi que les possibilités suivantes (effectives seulement sur les fichiers NTFS) :
  - Changer les permissions
  - Prendre le statut de propriétaire.

Ces permissions de partage peuvent être assignées aux utilisateurs et groupes.

5.2 Partages administratifs :

Windows NT crée plusieurs partages administratifs pour assister les administrateurs ayant besoin d'accéder aux lecteurs à travers le réseau :

- **ADMIN$:** un partage Admins$ est associé au répertoire qui stocke les fichiers du système d'exploitation de Windows NT.
- **Lettre-lecteur$:** un partage administratif est crée pour chaque disque dur sur le serveur. C$, par exemple, est un partage administratif associé à la racine du lecteur C.
- **IPC$:** cette ressource est utilisée par le mécanisme des tubes nommés, qui permet la communication entre les programmes.
- **Print$:** ce partage supporte le partage des imprimantes.
- **REPL$:** lorsqu'un serveur de duplication est configuré, ce partage est crée. Il est nécessaire de réaliser une duplication d'exportation.

Les nom des partages administratifs se terminent par un $. Tous les partages finissant par un $ ne seront pas affichés dans les listes explorables sur le réseau.

6. Le système LanManager :

Le modèle réseau de Windows NT provient de deux lignes de produits :
LanManager et Windows pour Workgroup. La possibilité d'administrer plusieurs serveurs indépendamment dans un même domaine provient de LanManager, l'approche intuitive du partage des ressources du réseau a pour origine Windows pour Workgroup.
Le produit LanManager est le gestionnaire de réseau développé par Microsoft. Il est une évolution du logiciel MS-Net qui représentait la première génération des gestionnaires de réseau et a été la base de nombreux gestionnaires de réseaux.
Actuellement, LanManager évolué, dans sa version 2 et 2.2, est sur disponible sur le marché. Le système LanManager est construit sur deux composantes :
Une partie serveur qui fournit les services réseau et l'administration de station de travail, et une partie redirecteur qui permet aux stations DOS, Windows et OS/2 d'accéder aux services de la partie serveur.
LanManager s'appuie sur le système d'exploitation OS/2, et utilise ses fonctionnalités comme le multitâche, la gestion de fichiers avancée (espace disques de grande capacité et d'accès rapide, etc.). Il tire partie des processeurs Intel, bien qu'il conserve des performances parfaitement acceptables sur des serveurs à base de 80286.
Un serveur LanManager supporte un grand nombre de protocoles de communication : TCP/IP, NetBeui (version 2.0), ISO, AppleTalk. Tous ces protocoles permettent à une station d'accéder aux ressources d'un serveur (disques, imprimantes, application, etc.).
Un grand nombre de constructeurs informatiques ont adopté les gestionnaires de réseau LanManager ou Netware dans leurs architectures qu'ils représentent à eux deux plus de 70% du marché global des gestionnaires de réseaux, il existe aujourd'hui des versions disponibles de LanManager et du Netware sur un grand nombre de plates-formes.

Cette évolution constitue un des axes majeurs de développement des solutions de gestionnaires de réseaux locaux d'entreprise et permet d'assurer de manière transparente une intégration complète des réseaux locaux dans le système d'information de l'entreprise. [3]

7. Les API Windows:

API est l'abréviation de *"Application Programming Interface"*. En fait ce sont des procédures stockées dans des bibliothèques (DLL : *"Dynamic-Link Library"*, en français "Bibliothèques de liaisons dynamiques"). Ces librairies contiennent des procédures que l'ont peut appeler depuis plusieurs programmes.

L'interface de programmation Win32 (Win32 API) est commune aux systèmes d'exploitation Windows 9x et Windows NT. Les API Windows offrent aux programmeurs la possibilité d'interagir avec le système d'exploitation. Elles offrent des possibilités presque infinies, et dépassent de très loin les possibilités apportées par les environnement de développement (Delphi, Visual Basic, etc.). Par exemple, elles permettent de contrôler une application, d'accéder à la base de registres, de jouer des sons, etc.

Les API ne sont en fait que des fonctions semblables à celle que l'on peut créer dans un environnement de développement. En règle générale, on leur fournit un certain nombre de paramètres, et elles renvoient quelque chose, ou réalisent une action précise. Ces fonctions sont contenues dans des fichiers DLL, tels que "user32.dll", "Netapi32.dll", ou bien d'autres encore. Les fonctions les plus couramment utilisées sont celles qui constituent Microsoft Windows lui-même. Ces procédures sont toutefois écrites en langage C, et doivent donc être déclarées avant de pouvoir les utilisées avec d'autres langages.

Les API Windows sont plutôt faciles à utiliser, une fois que l'on connaît leur déclaration et leurs paramètres. Leurs difficultés sont autres : les problèmes se posent généralement lorsqu'on cherche l'API qui nous rendrait service, puisqu'on se trouve alors confronté à des milliers de fonctions aux noms pas toujours très explicites. Lorsque enfin on a trouvé celle qui convient, on découvre qu'on est incapable de l'utiliser, car on ne connaît ni sa déclaration, ni ses paramètres, ni son utilisation. Pour résoudre ce problème, il y a deux solutions : la première est de chercher des exemples utilisant cette API, la deuxième est d'acquérir un livre spécialisé sur les API (il n'en existe que quelques uns en français) [10]. Cela dit, elle peut souvent se montrer utile, ne serait-ce que pour savoir quel API peut nous servir.

Pour ceux qui programme en C++, il existe d'autres autres sources très intéressantes qui sont la documentation de Visual C++, qui propose une liste de toutes les API, le MSDN Online sur le site de Microsoft (qui contient entre autres cette documentation), et le fichier d'aide **win32.hlp** (Win32 programmer's Reference). Ce fichier d'aide contient une description très complète des APIs de Windows, des structures à utiliser, mais là encore, en C++.

Voici quelques applications des API :

- Utilisation des fonctions multimédia.
- Utiliser des fonctions du noyaux Windows (mémoire, processus, etc.).
- Travailler dans la base de registres.
- Gérer et manipuler les routines de réseaux.

Table3.1 : Les bibliothèques d'API les plus courantes

Fichier	Description
Advapi32.dll	Bibliothèque de services API avancés gérant de nombreuses API, y compris de nombreux appels de sécurité et de registre
Comdlg32.dll	Bibliothèque d'API de boîte de dialogue commune
Gdi32.dll	Bibliothèque d'API pour périphérique à interface graphique
Kernel32.dll	Support d'API de base pour les noyaux Windows 32 bits
Iphlpapi.dll	Manipulation des protocoles TCP/IP
Lz32.dll	Routines de compression 32 bits
Mpr.dll	Bibliothèque de routeurs fournisseurs multiples
Netapi32.dll	Bibliothèque d'API réseau 32 bits
Shell32.dll	Bibliothèque d'API Shell 32 bits
User32.dll	Bibliothèque pour routines d'interfaces utilisateur
Version.dll	Bibliothèque de versions
Winmm.dll	Bibliothèque multimédia Windows
Winspool.drv	Interface de spouleur d'impression contenant des appels API de spouleur d'impression

Dans notre application, nous avons utilisé et manipulé les trois types d'APIs suivant :

- APIs LanManger.
- APIs IP Helper.
- WNet fonctions.

7.1 APIs LanManager :

Toutes les fonctions d'accès à un serveur peuvent être réalisées à l'intérieur d'une application, par l'intermédiaire d'interface de programmation API. C'est un point fondamental qui permet à LanManager de s'intégrer facilement dans une architecture informatique donnée, afin de pouvoir s'adapter aux contraintes spécifiques d'une entreprise ou pour faciliter l'intégration des développements logiciels dans un environnement réseaux.
Une offre LanManager alliée au système d'exploitation Windows NT permet un environnement très concurrentiel. Microsoft à importé plusieurs APIs de LanManager et les intégré dans Windows NT. Ces APIs fournissent l'accès à toutes les ressources du réseau et offrent également plusieurs

fonctions permettant de gérer les comptes utilisateur, les groupes, le partage des ressources et le contrôle des sessions ainsi que les services réseaux. Ces APIs sont déclarées dans la bibliothèque Netapi32.dll.

7.2 APIs IP Helper (Internet Protocol Helper) :

Tous les ordinateurs sont capables de se connecter à d'autres ordinateurs via l'Internet utilisant les protocoles TCP/IP. Le système d'exploitation Windows NT garde toutes les informations dans une base de données appelées MIB (Management Information Base) et plus précisément dans une table d'état concernant les connections et les trafics sur l'ordinateur local. L'administrateur à besoin de savoir les statistiques et les trafics sur le serveur pour prendre certaines décisions.
Les APIs, IP Helper, sont intégrées dans Windows 9x et Windows NT et elles permettent de récupérer la configuration réseau TCP/IP du poste local, on peut ainsi obtenir le nom de l'ordinateur, les adresse IP, la configuration des interfaces, la table ARP (Adress Resolution Protocol), et des statistique sur les différents protocoles tel que TCP, UDP, IP et ICMP. On va pouvoir par exemples développer l'équivalent des commandes MS DOS Netstat, route, Arp. Ces APIs sont contenues dans la bibliothèque Iphlpapi.dll.[4]

7.3 Fonctions Wnet (Windows Networking Functions) :

Les applications écrites pour Windows peuvent utiliser les fonctions WNet dans les API Win32 pour implémenter et développer des logiciels réseaux sans faire des ajustements pour un fournisseur particulier ou configuration du réseau physique, car les fonctions WNet sont indépendamment du réseau.
Ces APIs peuvent être utilisées pour visualiser ou détecter toutes les ressources connectées aux réseaux, et ajouter et annuler les connections sur ces ressources en commençant à la racine du réseau.
Les ressources de tous les fournisseurs du réseau peuvent être inscrites pour la documentation ou manipulation. Ces APIs sont contenues dans la bibliothèque Mpr.dll.

En résumé :

Dans ce chapitre, nous avons énuméré certaines caractéristiques de Windows NT qui permettent de découvrir les possibilités de ce produit. Windows NT est réellement un grand produit, puissant avec beaucoup d'avantage et une grande possibilité de développements futurs.
Ensuite, nous avons abordé les différentes techniques d'organisation du réseau NT qui est extrêmement importantes et peut avoir de sérieuses implications sur la sécurité et la performance du réseau.
Ce chapitre permet de comprendre les concepts de base sur la gestion de comptes utilisateurs, groupes et le partage des ressources.
On a aussi exposé les API que le programmeur peut utiliser pour permettre à leur application d'accéder aux services fournis par le système d'exploitation Windows NT.

Chapitre 4:

Conception et réalisation

Les éditeurs de système d'exploitation et les administrateurs de réseau entretiennent une vieille querelle depuis l'invention de l'ordinateur. L'éditeur semble souvent préférer ajouter des gadgets à ses systèmes plutôt que les outils nécessaires aux administrateurs. Tandis que ces derniers attendent toujours des outils pour répondre à des besoins précis. On trouvera toujours un administrateur à qui il manquera l'outil nécessaire pour réaliser une tâche particulière sur le réseau dans un temps raisonnable.

Ce chapitre est consacré à ce problème, il peut arriver que personne ne dispose de l'outil dont a besoin un administrateur. Dans ce cas un outil personnalisé représente le seul moyen d'atteindre l'objectif recherché. Ce chapitre examinera la tâche des administrateurs qui consiste à créer des outils spécialisés leur permettant de travailler plus rapidement et plus simplement qu'avec des outils intégrés au système d'exploitation.

Actuellement, la grande majorité des outils d'administration personnalisés font probablement partie de la catégorie des utilitaires. Un outil utilitaire est petit et rapide et effectue généralement très bien une ou deux tâches.

Les deux premières sections de ce chapitre concerneront les divers types d'outils et leur fonctionnalité par rapport à une situation donnée. Les trois sections suivantes présentent une modélisation de l'application et sa description ainsi que les routines utilisées pour réaliser cette application.

1. Présentation des types d'outils :

Les outils couramment utilisés par les administrateurs peuvent être classés de plusieurs façons. Le choix de l'outil à utiliser pour accomplir une tâche donnée est un élément important de la spécification de l'outil. Ce que l'outil doit faire a des incidences sur son apparence et ses capacités.

1.1 Classification selon le type d'utilisation :

Une méthode évidente de classification des outils consiste à déterminer ce qu'on en fera d'une façon générale. La liste suivante présente plusieurs façons de définir le type d'outil selon son utilisation [5] :

- **Surveillance :** il s'agit du type de logiciel utilisé quotidiennement par les administrateurs leur permettant de les assister pour déterminer l'état courant du réseau. Un logiciel de surveillance peut, par exemple, indiquer à un administrateur la quantité de mémoire restante sur un serveur ou l'état courante des disques durs.
- **Analyse :** la simple connaissance des statistiques du réseau est parfois insuffisante, les logiciels d'analyse prennent les données brutes des logiciels de surveillance les étudient puis retournent un résultat.
- **Evènement :** certains type d'outils permette à l'administrateur de consulter les événements par la conservation des audits, Ils affichent tous les événements survenus sur l'ordinateur

depuis une certaine date. Ces applications permettent à l'administrateur de chercher la cause d'un problème et de détecter certains type de pannes.

- **Maintenance automatisée :** certains types de maintenance sont effectués quotidiennement et ne nécessitent pas l'intervention de l'administrateur. Il suffit à l'administrateur de définir les paramètres une fois pour toutes et le logiciel pourra effectuer la maintenance de façon automatique. Toute automatisation d'une tâche de maintenance augmente l'efficacité de l'administrateur réseau et diminue les risques d'erreurs.
- **Configuration :** les logiciels d'aujourd'hui disposent de plus d'option de configuration. Un éditeur de système d'exploitation peut parfois cacher certaines des options de configuration les plus puissantes. Par crainte que l'utilisateur ne les utilise de façon incorrecte.
- **Utilisateur :** l'administrateur a, toujours, besoin de gérer les clients sur le réseau. Il est nécessaire de mettre à sa disposition un outil qui permettra de créer, supprimer ou modifier les comptes utilisateurs. Grâce à ces comptes des utilisateurs peuvent accéder aux ressources dont ils ont besoin sur le réseau.
- **Suivi :** l'automatisation du suivi de la maintenance et des événements d'erreurs sur un serveur permet à un administrateur de retracer plus facilement les problèmes. En utilisant l'historique du système.

1.2 Classification par emplacement, utilisateur et sensibilité des données :

On peut également classer les outils selon le lieu où ils sont utilises et la personne qui les emploie. La liste suivante montre comment classer les types d'outils par emplacement et niveau d'utilisateur.[5]

- **Distance :** la distance entre la station et le serveur a une grande influence sur le type d'outil, un outil utilisé sur un réseau local n'a pas besoin d'être aussi petit ou d'utiliser aussi peu de bande passante du réseau qu'un outil destiné à une utilisation sur l'Internet.
- **Niveau d'expertise :** un outil conçu pour un nouvel administrateur doit disposer de plus de fonctionnalités d'assistance. Un outil peut inclure des dialogues destinés à prévenir l'administrateur des risques potentiels et des écrans d'aide décrivant complètement les fonctionnalités de l'outil. Mais ceci peut conduire à une augmentation de la taille de l'outil ce qui rendra la gestion du réseau moins efficace.
- **Moyen de communication :** les réseaux locaux sont en général des connexions à grande vitesse et la création d'un outil qui communique beaucoup avec le serveur n'est pas problématique. Une connexion par réseau commuté est ridiculement lente. Il faut donc optimiser les communications pour les administrateurs distants utilisant le réseau téléphonique commuté. Ce qui peut parfois conduire à supprimer certaines fonctionnalités.
- **Sensibilité des données :** certains des outils créent géreront des données extrêmement sensibles, comme les mots de passe des utilisateurs. Et d'autres traiteront des données moins sensibles comme la vitesse de traitement d'un serveur. Le fait que les données manipulées par l'outil soient sensibles ou non peut donc déterminer si elles doivent être cryptées (et a quel niveau). Ce qui aura une influence sur la vitesse de traitement de l'outil.

- **Besoins de gestion :** un outil qui ne fait que surveiller un réseau est moins complexe à construire que celui qui utilise les informations recueillies pour prédire des disfonctionnement du réseau. La complexité des tâches de gestion traitées par l'outil en détermine les caractéristiques.

Certains types d'outils peuvent ne pas figurer dans cette liste. Il faut donc prévoir précisément la façon dont un outil sera utilisé avant de commencer à le concevoir.

2. Choix du type d'outil à utiliser :

L'administration peut avoir besoin d'un outil qui indique le niveau actuel d'utilisation du processeur ou si une panne matérielle s'est effectivement produite. Certains choix ne sont cependant pas aussi simples à déterminer, car on ne connaît pas les besoins futurs des administrateurs.
Il peut être intéressant d'examiner les besoins actuels et futurs, à moins que tout soit déjà parfaitement déterminé, cela comprend notamment la définition de la façon dont l'administrateur utilisera l'outil aujourd'hui et demain.
Il faut également déterminer le type et la quantité d'informations nécessaires à l'administrateur. On peut, par exemple, construire un outil de surveillance qui utilise les données existantes du serveur et découvrir que l'administrateur doit en fait calculer les valeurs dont il a besoin. Un outil d'analyse qui effectue les calculs peut alors être préférable au simple outil de surveillance.
Il faut aussi déterminer à quel point un outil doit être automatisé. L'automatisation doit soulager l'administrateur des tâches ennuyeuses. Mais ne doit pas lui enlever la responsabilité des prises de décision basée sur des faits tangibles.
Il peut aussi être délicat de déterminer le niveau d'expertise, Même un administrateur expert peut manquer de connaissances ou d'expérience et ne pas parvenir à exploiter pleinement un outil personnalisé.
Il est donc important de déterminer le type exact d'outil à crées et aussi de spécifier ce qu'il fera précisément. Les outils personnalisés débutent souvent sous la forme d'un gadget pratique sur le bureau du programmeur et finissent dans les mains d'un utilisateur qui n'aura aucune idée de ce qu'il fait. Il faut donc choisir le type d'outil selon le profil de l'utilisateur et non pas selon le profil de celui qui l'a initialement conçu.

Un outil conçu pour une utilisation sur un réseau local peut parfois combiner plus de fonctions dans un seul grand outil plutôt que d'avoir plusieurs petits outils à usage unique.
Pour cela nous essayerons de combiner quelque type d'outil. Notre application est destinée aux réseaux locaux elle contiendra quelques outils de surveillance et d'analyse qui permettront à un administrateur de gérer l'environnement utilisateur d'une manière simple et rapide.

3. l'architecture d'un logiciel d'administration de réseau :

l'architecture de l'application va varier en fonction des fonctionnalités de la plate-forme.
Une vue générique d'une plate-forme divisée en trois grandes catégories :

- Le logiciel utilisateur
- Le logiciel de gestion réseau
- Le logiciel de communication et de support des données.

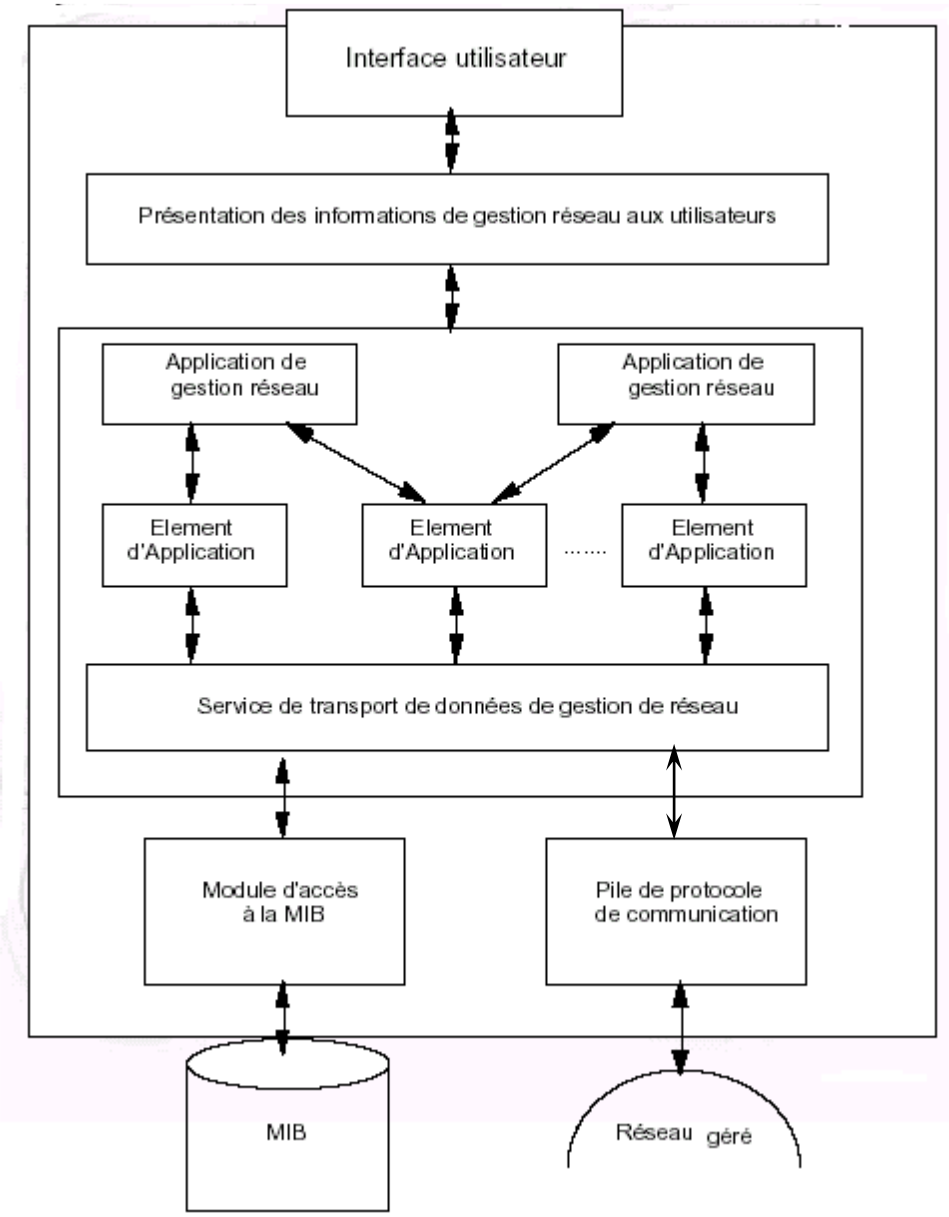

Fig.4.1 l'architecture d'un logiciel d'administration de réseau

4. Modélisation de l'application :

Pour modéliser notre application, nous avons utilisé le diagramme des cas d'utilisation qu'est l'un des diagrammes de l'UML le plus important. Les cas d'utilisation sont une technique de description des systèmes étudié privilégiant le point du vue de l'utilisateur. Il est composé d'un ensemble d'actions déclenchées par un acteur externe (notre cas l'acteur est l'administrateur) et qui produit un résultat identifiable.

Un cas utilisation représente la relation entre un acteur et une fonctionnalité du système, il peut faire appel aux services d'un autre cas, un diagramme peut regrouper différents cas selon un critère choisi par l'analyste.

La figure 4.1 représente l'interaction entre l'administrateur et les différentes foncions de notre application.

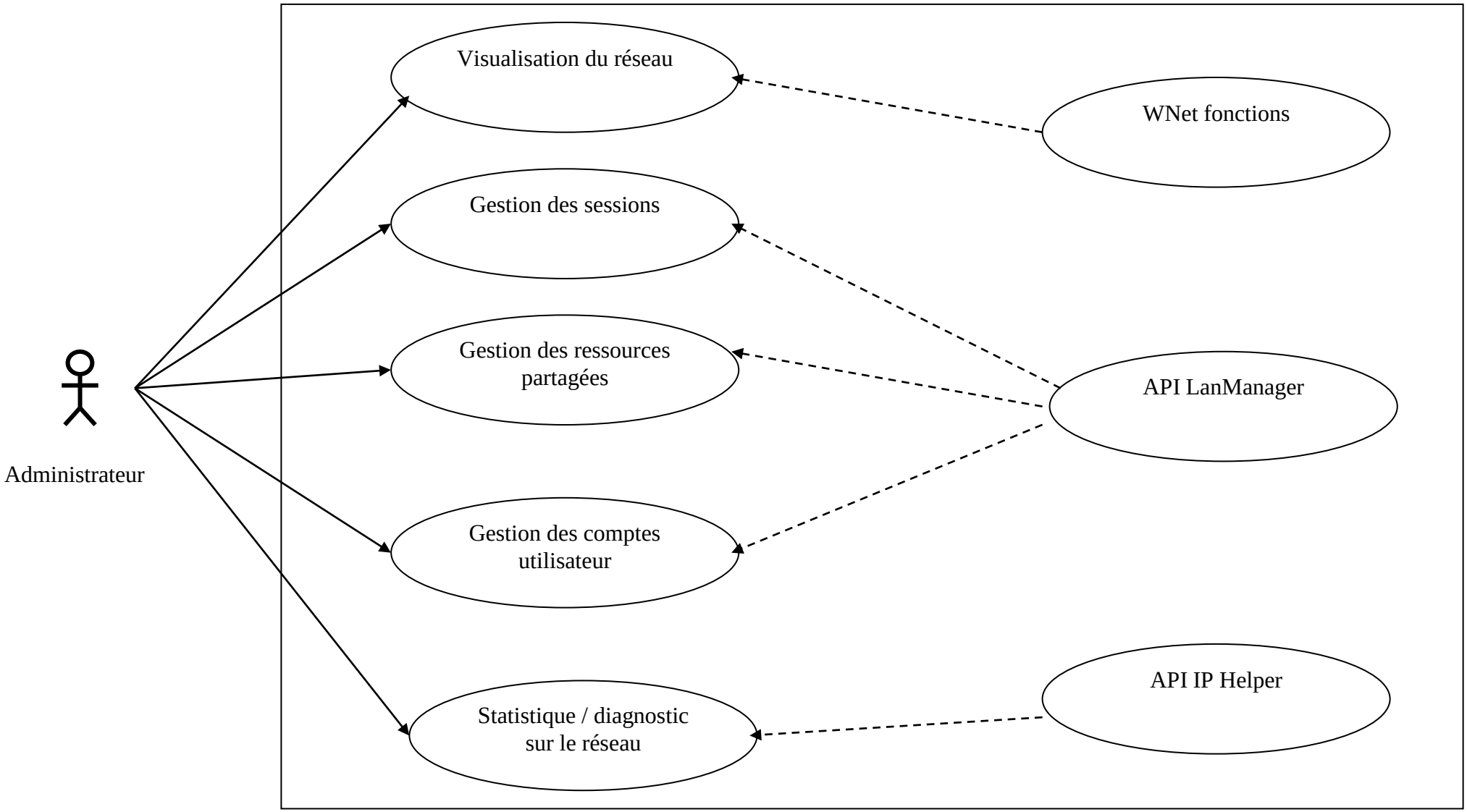

Fig.4.2 Modélisation de l'application

5. Présentation des routines de l'application :

L'application que nous avons développée est basée essentiellement sur la programmation réseau, ce qui signifie qu'on a utilisé les fonctions de Windows APIs. Dans ce qui suit, nous allons faire une exploration de ces APIs.
Le langage de programmation Pascal sous l'environnement Delphi, permet d'exporter n'importe quelle API contenue dans un fichier DLL en spécifiant le nom de la fonction et le nom de la DLL. La syntaxe générale est comme suit :

```
function [nom de fonction] external [nom de dll] name  [nom de fonction original];
```

Comme on peut le remarquer, on peut donner à toute fonction de la DLL, un nom quelconque différent de son nom original et ce selon nos besoins.

a. dans la visualisation de réseau, nous avons utilisé les trois APIs suivantes :

WNetopenEnum, **WNetEnumRessource**, **WNetCloseRessource**.

La fonction **WnetopenEnum** effectue une énumération des ressources du réseau avec lesquels il existe une connexion.

Syntaxe :

```
function WNetOpenEnum(dwScope, dwType, dwUsage: DWORD;
  lpNetResource: PNetResource; var lphEnum: THandle): DWORD;
```

Paramètres:

`DwScope` : spécifie le but de l'énumération, ce paramètre peut être une des valeurs suivantes :

`RESOURCE_CONNECTED` : toutes les ressources connectées.

`RESOURCE_GLOBALNET` : toutes les ressources sur le réseau.

`RESOURCE_REMEMBERED` : toutes les connections persistant.

`DwType` : spécifie le type de ressource à énumérer, ce paramètre peut être une combinaison des valeurs suivantes :

`RESOURCETYPE_ANY` : tous les types de ressource.

`RESOURCETYPE_DISK` : toutes les ressources de type disque.

`RESOURCETYPE_PRINT` : toutes les ressources de type imprimante.

`dwUsage`: spécifie l'usage de la ressource à être énuméré, ce paramètre peut être une combinaison des valeur suivantes :

`0` : toutes les ressources.

`RESOURCEUSAGE_CONNECTABLE` : toutes les ressources connectables.

`RESOURCEUSAGE_CONTAINER` : toutes les ressources inclues.

`PnetResource`: pointe à une structure `NETRESOURCE` qui contient les informations sur les ressources connectées aux réseaux durant l'énumération de ces ressources.

La fonction **WnetEnumRessource** continue une énumération des ressources réseau commencé par **WnetopenEnum.**

Syntaxe :

```
function WNetEnumResource(
   hEnum: THandle;          // pointeur doit être retourné par WnetopenEnum
   var lpcCount: DWORD;
   lpBuffer: Pointer;       // pointeur vers le buffer résultat
   var lpBufferSize: DWORD // spécifie la taille de buffer
): DWORD;
```

Paramètres:

`lpcCount:` quand la fonction se termine avec succès. La variable pointé par ce paramètre contient réellement le nombre des ressources lues.

La fonction **WNetCloseRessource** fermer l'énumération des ressources du réseau qui commencé par **WnetopenEnum.**

b. dans la gestion des sessions, les deux APIs utilisées sont :

NetSessionEnum, NetSessionDel.

La fonction **NetSessionEnum** permet d'énumérer et fournit des informations sur toutes les sessions courantes établies sur le serveur.

Syntaxe :

```
function NetSessionEnum(servername: LPWSTR; UncClientName: LPWSTR;
  username: LPWSTR; level: DWORD; var bufptr: Pointer; prefmaxlen: DWORD;
  var entriesread: DWORD; var totalentries: DWORD;
  resume_handle: PDWORD): DWORD;
```

Paramètres:

`servername:` pointeur vers une chaîne qui spécifie le nom du serveur distant sur lequel la fonction est exécutée, si ce paramètre est NIL, l'ordinateur local est utilisé.

`UncClientName:` pointeur vers une chaîne qui spécifie le nom de la session de l'ordinateur pour lequel l'information sera rendu, si ce paramètre est NIL, cela signifie que toutes les sessions de l'ordinateur sur le serveur seront énumérées.

`username:` contient le nom de l'utilisateur qui a ouvert une session, NIL spécifie les sessions pour tous les utilisateur.

`level:` spécifie le niveau de l'information sur les sessions.

`Bufptr:` tampon qui reçoit les données, la taille de ce tampon dépend de la valeur du paramètre `level`.

`prefmaxlen:` spécifie la longueur maximale de données retournés, en multiple de 8 bits.

`entriesread:` contient le nombre total d'éléments énumérés actuellement.

`totalentries`: reçoit le nombre total d'entrées qui ont été énumérées et qui est utilisé pour continuer une recherche des sessions existantes.

La fonction **`NetSessionDel`** permet d'arrêter une session entre un serveur et un poste de travail.

Syntaxe :

```
function NetSessionDel(servername: LPWSTR; UncClientName: LPWSTR;
  username: LPWSTR):DWORD;
```

Paramètres:

`UncClientName`: contient le nom de l'ordinateur à déconnecter, NIL signifie que toutes les sessions de l'utilisateur seront terminées.

`username`: contient le nom de l'utilisateur dont la session sera terminé, NIL indique que les sessions de tous les utilisateurs du client spécifié seront terminé.

c. pour gérer le partage des ressources, il est nécessaire d'utiliser les trois APIs suivantes :

`NetShareEnum`, `NetShareAdd`, `NetShareDel`.

La fonction **`NetShareEnum`** permettre d'énumérer les ressources partagées et rapporte les informations sur chaque ressource partagée sur le serveur.

Syntaxe :

```
function NetShareEnum(servername: LPWSTR; level: DWORD; var butptr: Pointer;
  prefmaxlen: DWORD; var entriesread: DWORD; var totalentries: DWORD;
  resume_handle: PDWORD): DWORD;
```

La fonction **`NetShareAdd`** permet d'ajouter une ressource à l'ensemble des ressources partagées sur le serveur.

Syntaxe :

```
function NetShareAdd(servername: LPWSTR; level: DWORD;
  const buf: Pointer;
  parm_err: LPDWORD): DWORD;
```

Paramètres:

`buf`: un tampon doit être remplit par le programmeur spécifiant les informations sur le partage.

`parm_err`: qui reçoit l'index du premier membre de la structure de l'information de partage qui cause l'erreur.

La fonction **`NetShareDel`** permet de supprimer un partage de la liste des ressources partagées sur le serveur, en déconnectant toutes les connections à ce partage.

Syntaxe :

```
function NetShareDel(servername: LPWSTR; netname: LPWSTR;
  reserved: DWORD): DWORD;
```

Paramètres:

`netname`: spécifie le nom de partage à supprimer.

`reserved`: doit être zéro.

d. les APIs suivantes permettent de gérer les comptes utilisateurs ainsi que d'énumérer les groupes locaux :

NetUserEnum, NetUserAdd, NetUserDel, NetUserGetLocalGroups, NetLocalGroupEnum, NetLocalGroupAddMember, NetLocalGroupDelMember.

La fonction **NetUserEnum** permettre d'énumérer tous les comptes utilisateurs ainsi que les informations sur chaque compte.

Syntaxe :

```
function NetUserEnum (servername : LPWSTR; level : DWORD; filter : DWORD;
  var bufptr : Pointer; prefmaxlen : DWORD; var entriesread : DWORD;
  var totalentries : DWORD; var resume_handle : DWORD) : DWORD;
```

Paramètres:

`Filter`: spécifie un filtre de types des comptes à énumérer, une valeur zéro indique tous les types des comptes.

La fonction **NetUserAdd** permet d'ajouter un compte utilisateur et assigne un mot de passe et niveau de privilège.

Syntaxe :

```
function NetUserAdd (servername : LPWSTR; level : DWORD;
          buf : Pointer; // buffer utilisé pour les information de l'utilisateur.
          var parm_err : DWORD
) : DWORD;
```

la fonction **NetUserDel** permet de supprimer un compte utilisateur.

Syntaxe :

```
function NetUserDel (servername : LPWSTR;
  username : LPWSTR  // le nom de l'utilisateur à supprimer
) : DWORD;
```

La fonction **NetUserGetLocalGroups** rapporte une liste des groupes locaux auxquels un utilisateur spécifié appartient.

Syntaxe :

```
function NetUserGetLocalGroups (servername : LPWSTR;
  username : LPWSTR;  // spécifie le nom d'utilisateur.
  level : DWORD; // seulement zéro est valide.
  flags : DWORD;
  var bufptr : Pointer; prefmaxlen : DWORD;
entriesread : DWORD; totalentries : DWORD) : DWORD;
```

La fonction **NetLocalGroupEnum** permet d'énumérer tous les groupes locaux ainsi que les informations nécessaires pour chaque groupe.

Syntaxe :

```
function NetLocalGroupEnum(servername: LPWSTR; level: DWORD; var bufptr: Pointer;
  prefmaxlen: DWORD; var entriesread: DWORD; var totalentries: DWORD;
  var resumehandle: DWORD): DWORD;
```

La fonction **NetLocalGroupAddMember** permet d'ajouter un utilisateur ou groupe globale à un groupe local existant.

Syntaxe :

```
function NetLocalGroupAddMember (servername : LPCWSTR;
  groupname : LPCWSTR;  // spécifie le nom de groupe local.
  membersid : PSID    // spécifie l'identité de sécurité de l'utilisateur a ajouter.
   ) : DWORD;
```

La fonction **NetLocalGroupDelMember** permet de supprimer un membre d'un groupe local existant.

Syntaxe :

```
function NetLocalGroupDelMember (servername : LPCWSTR;
  groupname : LPCWSTR;
  membersid : PSID  // spécifie l'identité de sécurité de l'utilisateur a supprimer.
) : DWORD;
```

e. la fonction **GetNetworkParams** permet de récupérer certains paramètres globaux de la configuration du réseau. Cette fonction renvoi une structure `FIXED_INFO` qui contient les informations suivantes :

```
FIXED_INFO = record
    HostName: array [0..MAX_HOSTNAME_LEN + 3] of Char;     // le nom du PC
    DomainName: array[0..MAX_DOMAIN_NAME_LEN + 3] of Char; // le nom de domaine
    CurrentDnsServer: PIP_ADDR_STRING; // l'adresse IP de serveur DNS principale
    DnsServerList: IP_ADDR_STRING; // les adresses IP des autres serveurs DNS
    NodeType: UINT;  // type de noeud
    ScopeId: array [0..MAX_SCOPE_ID_LEN + 3] of Char; // Nom de serveur DHCP
    EnableRouting: UINT;  // si le routage est active
    EnableProxy: UINT; // si le PC comporte comme un proxy ARP
    EnableDns: UINT;  // si le DNS est active
  end;
```

Syntaxe :

```
function GetNetworkParams(pFixedInfo: PFIXED_INFO;
var pOutBufLen: ULONG //longueur de buffer
```

```
): DWORD;
```

f. concernant les statistiques sur les protocoles TCP/IP, nous avons utilisé les APIs suivantes :

`GetTcpStatistics` : permet de récupérer via une structure `MIB_TCPSTATS` enregistrée dans le MIB, des informations sur le protocole TCP comme :

- la configuration du RTO (Retransmission Time-Out)
- le nombre des connections actives
- des statistiques sur les segments envoyés et reçus.

`GetUdpStatistics` : permet de récupérer via une structure MIB_UDPSTATS les informations sur le protocole UDP comme :

- le nombre de datagrammes reçus et envoyés
- le nombre de ports UDP qui sont en écoute.

`GetIPStatistics` : permet de récupérer via une structure `MIB_IPSTATS` les informations sur le protocole IP dont :

- IP Forwarding activé ou non
- TTL (Time To Live)
- Des statistiques sur les datagrammes reçus et envoyés
- Le nombre d'interface
- Le nombre d'adresse IP associées à l'ordinateur
- Le nombre de route dans la table de routage

`GetICMPStatistics` : permet via une structure `MIB_ICMPSTATS` de récupérer des statistique sur les messages ICMP entrants et sortants.

g. la fonction **`GetIPForwardTable`** permet de récupérer un tableau de structure `MIB_IPFORWARDROW` contenant des informations sur chaque route de la table de routage. On récupère en effet pour chaque route :

- l'adresse IP de destination
- le masque de sous-réseau
- l'adresse IP du prochain saut
- l'index de l'interface
- des métriques (*RFC 1345*).

On peut ajouter et supprimer des entrées dans la table de routage avec les fonctions **`CreatetIPForwardEntry, DeleteIPForwardEntry.`**

h. finalement, pour programmer la routine Ping, on utilise un ensemble d'APIs qui sont résident dans la librairie "Icmp.dll", ces APIs sont :

- **`IcmpCreatetfile :`** permet d'ouvrir un port pour la communication et donne un pointeur sur ce port.
- **`IcmpSendEcho :`** envoyer une chaîne pour réaliser un Ping.
- **`IcmpCloseHandle :`** fermer un port déjà ouvert.

Et pour réaliser la communication entre les utilisateurs, la fonction **NetMessageBufferSend** permet d'envoyer un message vers un autre poste.

Syntaxe :

```
function NetMessageBufferSend(ServerNam : LPWSTR;
MsgName : LPWSTR;          // spécifie le destinataire
FromName : LPWSTR;         // spécifie l'émetteur
Buf : Pointer;             // Buffer pour stocker le message
BufLen : DWORD             // spécifie la taille de Buffer.
) : DWORD;
```

Nous somme contenté d'exposé dans ce mémoire, fonctions les plus importantes pour la réalisation d'une application pour l'administration des réseaux.

6. Description et test de l'application :

l'application que nous avons développé sert à l'administration d'un réseau. Elle est déstinée aux administrateurs débutants ou en apprentissage. Elle a des fonctions selon le modèle que nous avons élaboré, en découpant l'application en plusieurs fonctions.

Avant de commencer la description des détails de l'application, il faut faire une description sur les différents éléments que nous avons programmés.

Concerant les fenêtres, notre application utilise des fenêtres MDI (Multiples Document Interface) qui sont utilisée pour manipuler des fonctions qu'on peut visualiser en même temps.
Et maintenant, nous arrivons à la description de l'application et sa fonctionnalité.

L'interface contient un menu avec plusieurs options et une barre d'outil avec plusieurs icônes, chaque icône a une fonction prédéfinis ainsi que un ExplorerBar permettant de naviguer facilement sur les fonctions principale de l'application . Les diffrentes fonctions qui sont offerte par notre application sont :

- Visualisation de réseau : cette fonctionnalité permet de découvrir tous les ordinateurs connectés aux réseau local afin de permettre à l'administrateur de surveiller facilement le réseau .
- Gestion des sessions : elle permettre à l'administrateur de lister ou déconnecter toutes les sessions étabiles entre le serveur et d'autres ordinateurs du réseau.
- Gestion des ressources partagées : cette fonctionnalité permet le partage des ressources d'un serveur, afin de les mettre à la disposition des utilisateurs du réseau.
- Gestion des comptes : liste les compte utilisateur du serveur, stockés dans la base de données des comptes et on peut créer, supprimer et modifier ces comptes sur le serveur ou le domaine.
- Statistique et digonistique sur le réseau : on peut faire des diagonistic sur les élements du réseau à l'aide de l'outil ping et des statistiques sur les protocoles TCP/IP, elle permet aussi d'afficher la table de routage et de faire la mise à jour ainsi que voir la configuration globale du réseau .

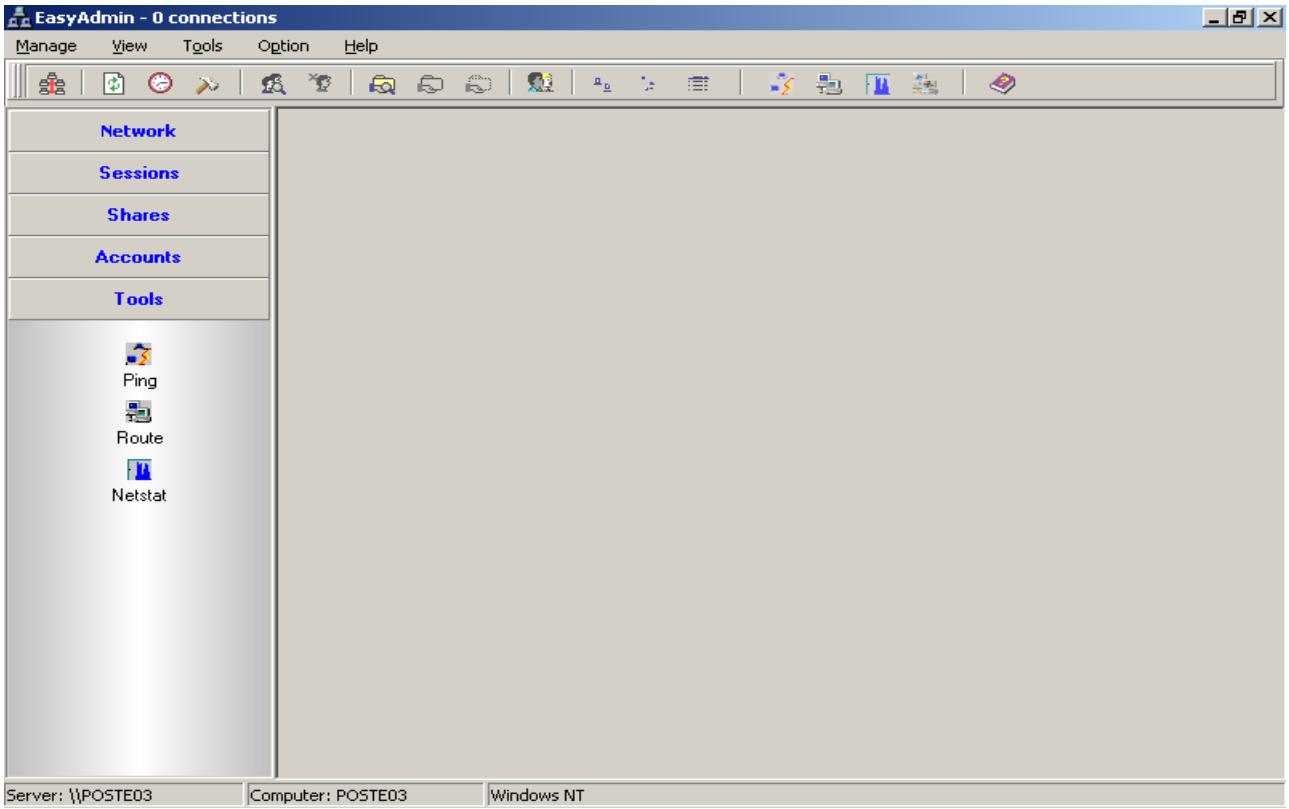

Fig.4.3 interface globale de l'application.

Finalement, l'application offre une aide pour assiter les utilisateurs de cette dernière afin de leur permettre une manipulation correcte de l'application.

La figure 4.3, répresente une vue globale de l'application.

6.1 Visualisation du réseau :

Cette partie offre une interface graphique qui facilite l'observation de tous les postes connectées au réseau. Si on sélectionne un poste dans l'interface, on peut effectuer certaines opérations sur ce poste à l'aide d'un menu contextuel. On peut sonder le poste avec la commande « ping » ou lui envoyer un message (similaire à la commande NetSend). On peut aussi obtenir des informations, tel que le nom et l'adresse IP associé à chaque poste.

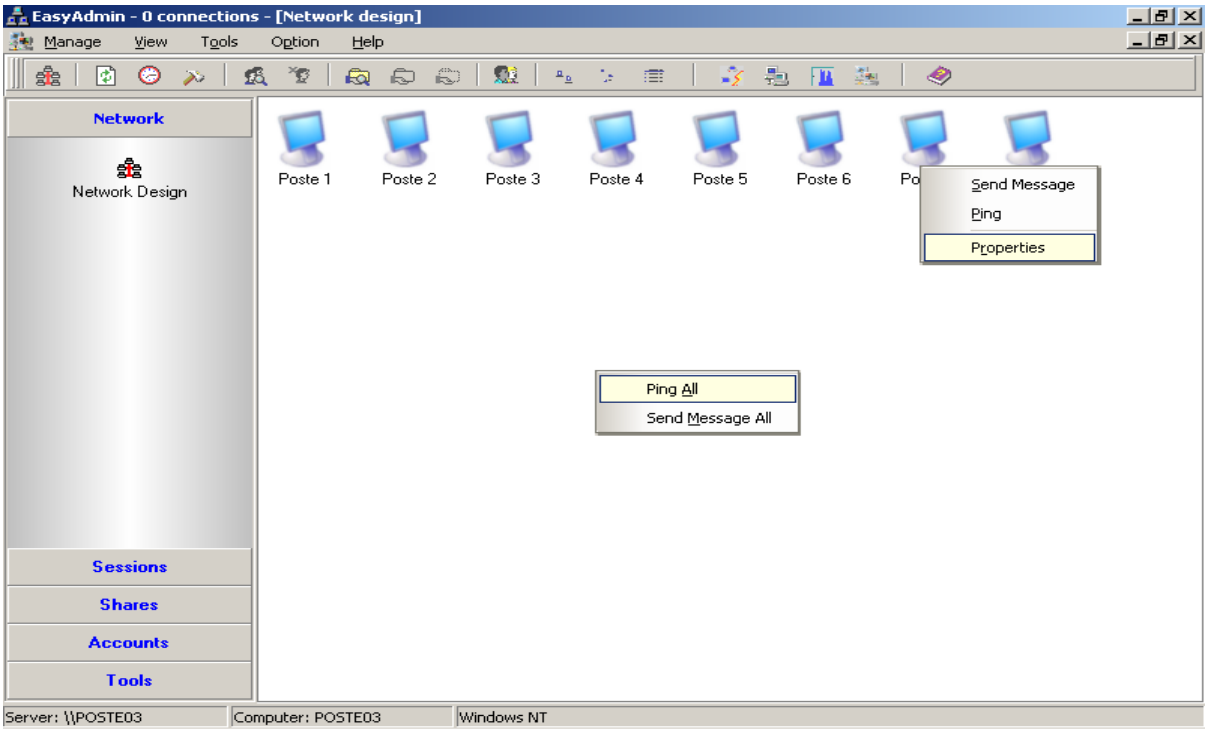

Fig.4.4 la détection des postes du réseau.

On a la possibilité de sonder tous les postes. Si, un poste répond, alors la couleur de ce poste est verte, sinon elle est rouge (figure 4.5). On peut émettre un message à toutes les postes à l'aide d'un autre menu contextuel. Si le poste reçoit le message alors on voit apparaître une icône qui représente une enveloppe sur le poste en question (figure 4.6).

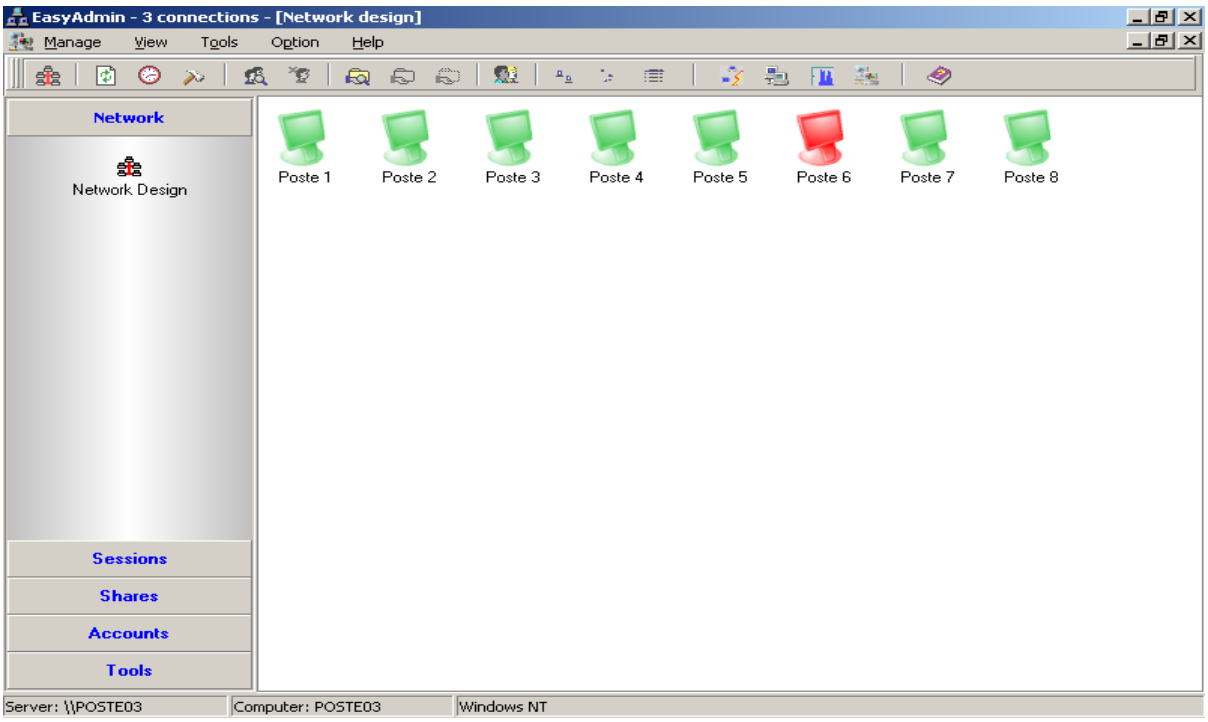

Fig.4.5 Test de connectivité des postes du réseau.

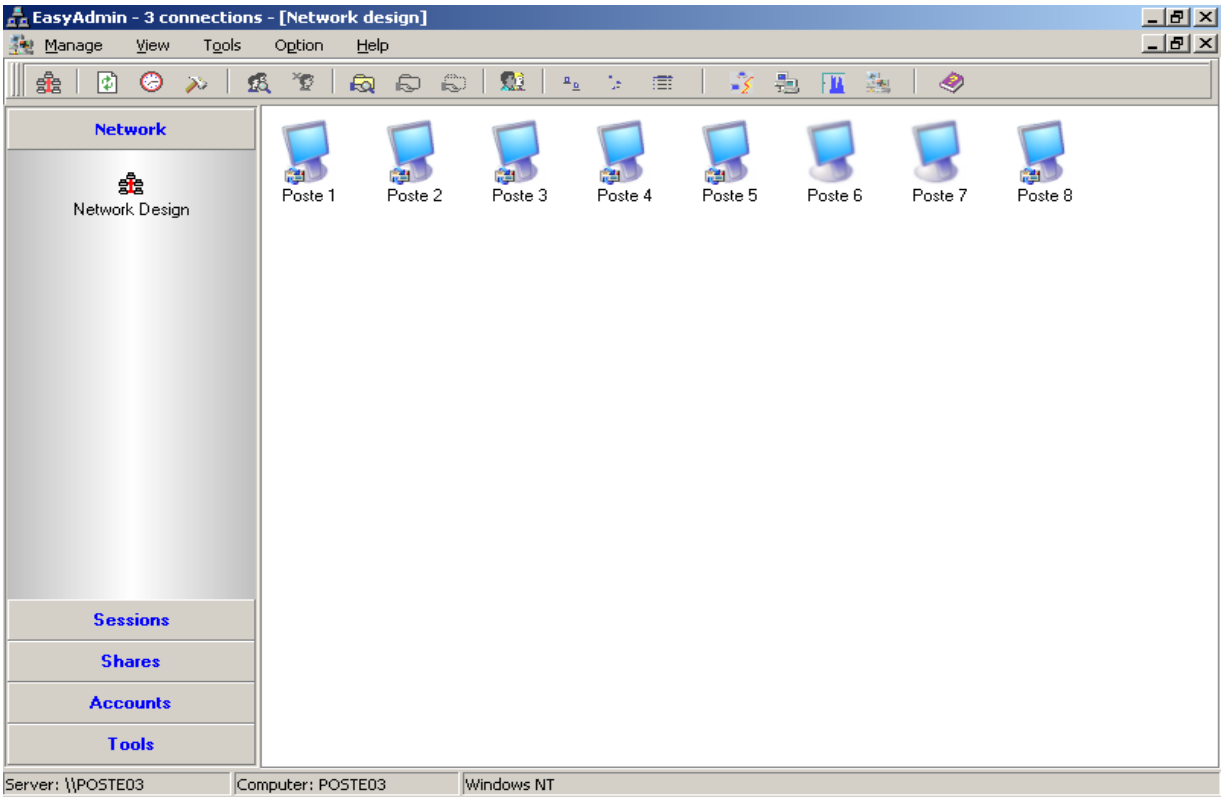

Fig.4.6 Emission d'un message à tous les postes du réseau.

6.2 Gestion des sessions :

Cette interface permet de contrôler les sessions ouvertes sur le serveur et d'obtenir les informations suivantes :

- *User Name* : le nom d'utilisateur de celui qui a ouvre la session.
- *Computer* : le nom de l'ordinateur sur lequel l'utilisateur a ouvre la session.
- *Opened* : le nombre de fichiers ouverts sur le serveur par l'utilisateur.
- *Connected time* : spécifie la durée de la connexion sur le serveur.
- *Idle time* : spécifie le temps d'inactivité sur le serveur.

Figure 4.7, illustre cette interface.

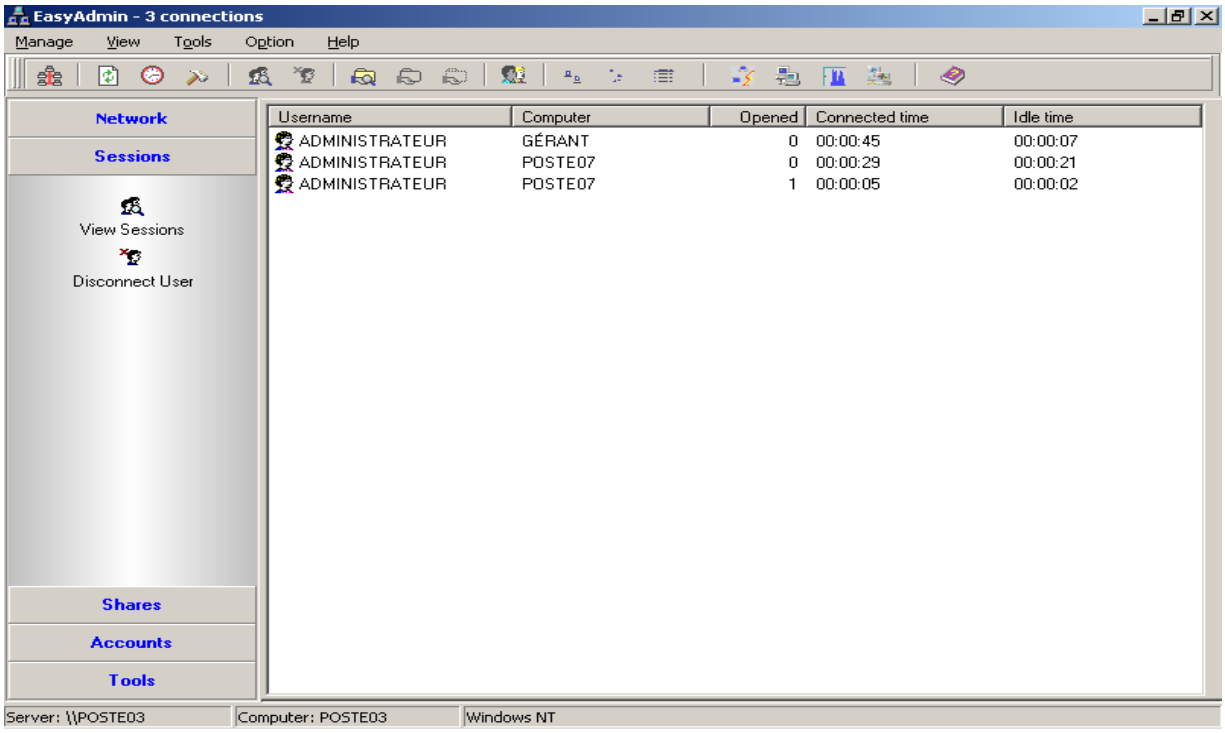

Fig.4.7 liste des sessions ouvertes sur le serveur.

On peut sélectionner un utilisateur et le déconnecter à partir de l'icône "Disconnect user".

6.3 Gestion des ressources partagées :

Cette interface affiche des informations sur toutes les ressources partagées du serveur. Elle fournit les noms de partage du dossier ou du périphérique ainsi que le chemin d'accès et les commentaires associés à chaque partage comme le montre la Figure 4.8 :

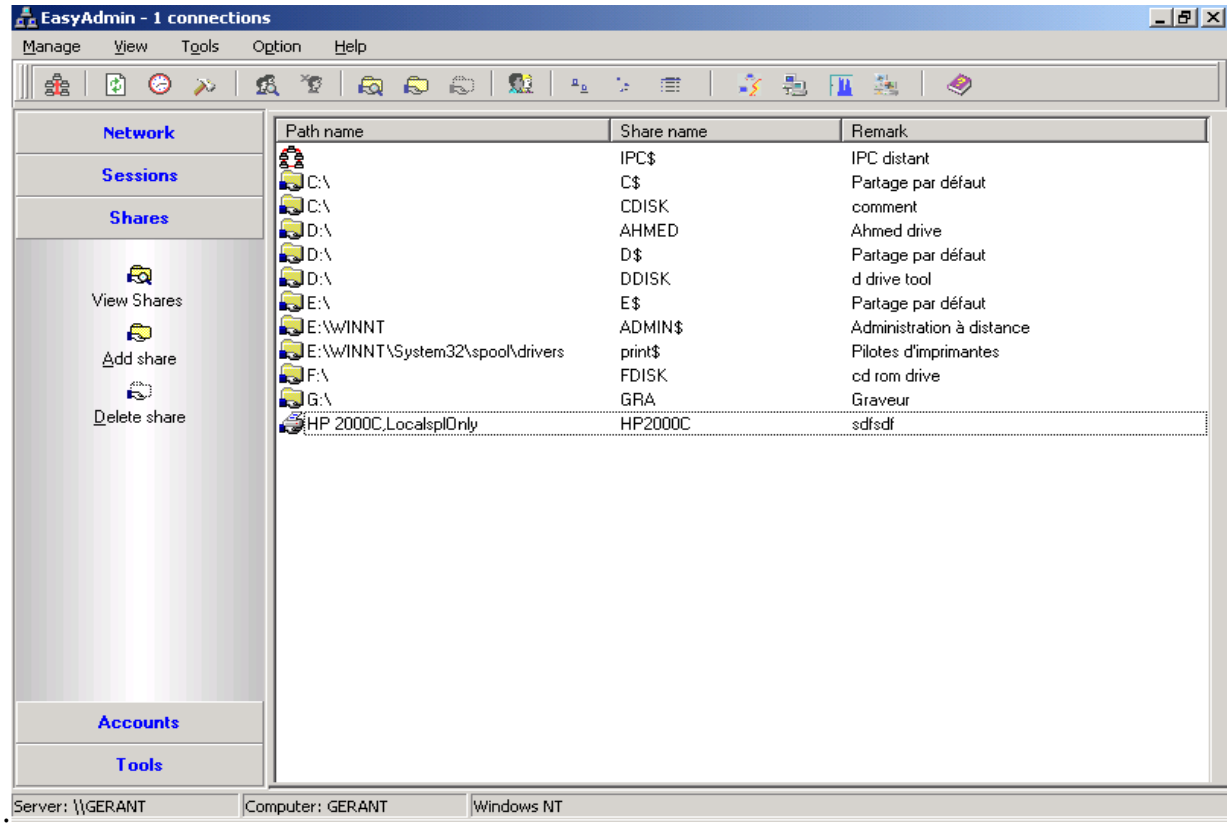

Fig.4.8 liste des ressources partagées sur le serveur.

Si on sélectionne un partage, on peut le supprimer ou le modifier. A l'aide de la boite de dialogue représenté par la Figure 4.9, on peut ajouter un partage en entrant les informations appropriées au partage.

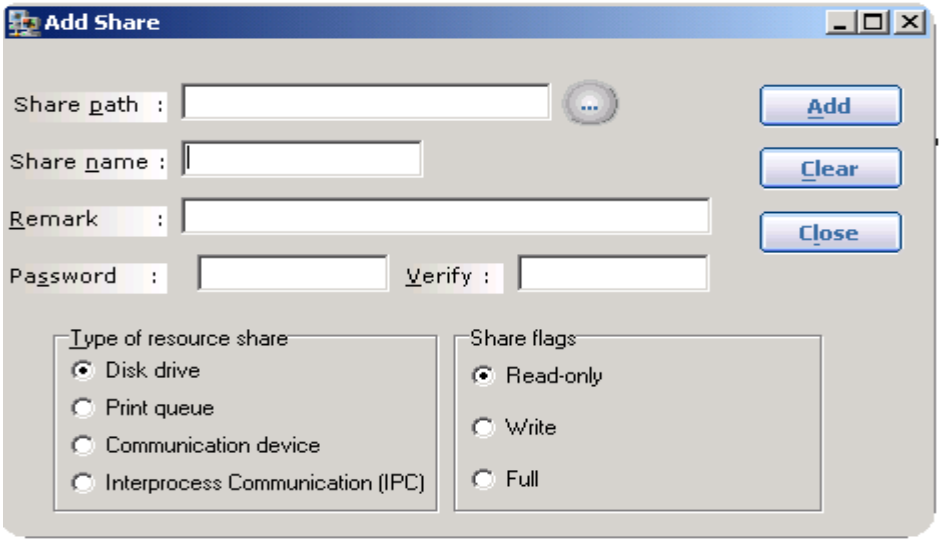

Fig.4.9 l'ajout d'un partage.

6.4 Gestion des comptes :

L'administrateur à besoin de gérer les comptes utilisateurs. Cette gestion peut se faire an choisissant l'icône correspondante dans la barre d'outil. La fenêtre de cette interface, représentée Figure 4.7, contient la liste des comptes utilisateurs du serveur ou du domaine.

Pour chaque compte, on peut avoir les informations suivantes :

- *User Name* : chaque utilisateur dan un domaine ou un ordinateur doit posséder un nom unique, ce nom peut comprendre jusqu'à vingt caractères.
- *Full Name* : ce champ optionnel permet de spécifier un nom détaillé de l'utilisateur.
- *Description* : ce champ est optionnel, vous pouvez par exemple, l'utiliser pour identifier la profession et le département de l'utilisateur.

On peut visualiser aussi dans la même interface les groupes locaux avec leurs noms et une description sur chaque groupe.

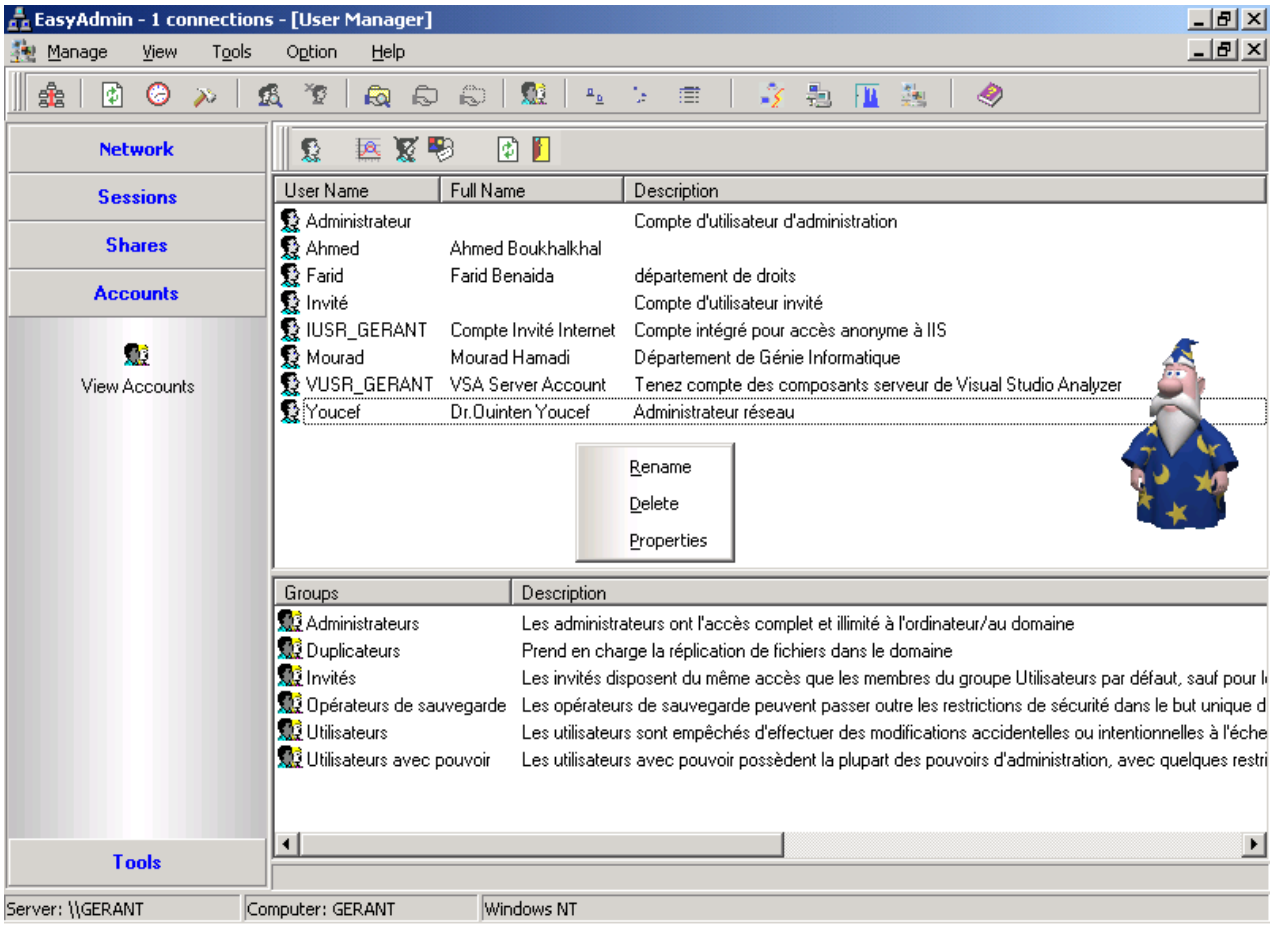

Fig.4.10 la gestion des comptes utilisateur.

Si on sélectionne un compte, l'interface nous propose un menu contextuel pour effectuer les opérations suivantes :

- *Rename* : renommer un utilisateur.
- *Delete* : supprimer un utilisateur
- *Propreties* : nous donne plus de détail sur l'utilisateur tel que le type de mot de passe autorisé soit :

  - ✓ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session.
  - ✓ L'utilisateur ne peut pas changer de mot de passe.
  - ✓ Les mots de passe n'expirent jamais.
  - ✓ Compte désactivé.

On peut aussi connaître à quel groupe appartient l'utilisateur. De plus on peut modifier certains champs, et à l'aide de l'icône New User on peut créer un nouvel utilisateur. Une boite de dialogue apparaît pour l'obtention des informations ci-dessous, comme le montre les figures suivantes :

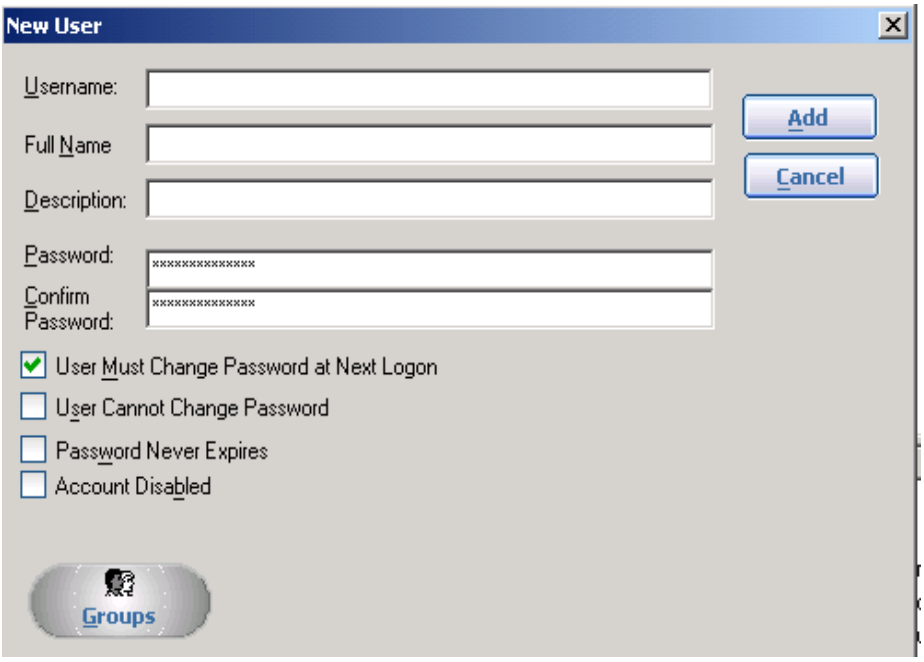

Fig.4.11 l'ajout d'un nouvel utilisateur.

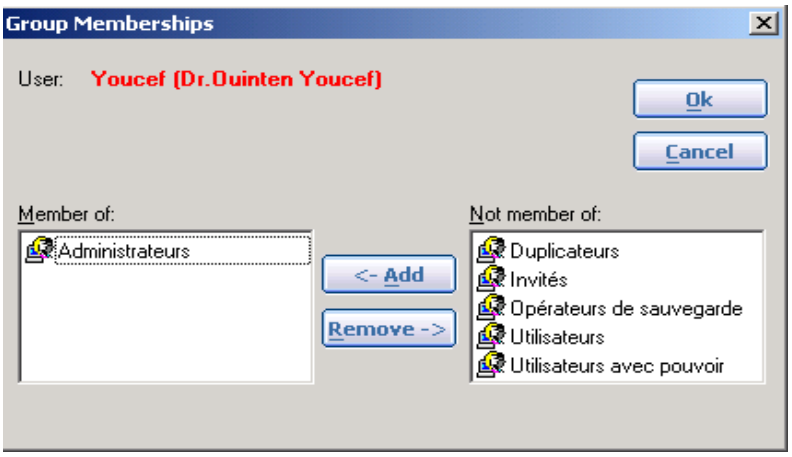

Fig.4.12 l'assignation aux groupes.

6.5 Statistiques et diagnostic sur le réseau :

Si on a besoin de statistiques sur le protocole TCP/IP, on peut choisir l'icône correspondante dans la barre d'outil. Figure 4.13, représente cette interface qui offre la possibilité d'obtenir des statistiques sur les protocoles TCP/IP soit TCP, UDP, IP, ICMP ainsi que les connexions ouvertes par les protocoles TCP, UDP et le trafic géré par la carte réseau, de plus on a la possibilité d'enregistrer ces statistiques dans un fichier texte que l'on peut ouvrir avec Le bloc-notes de Windows.

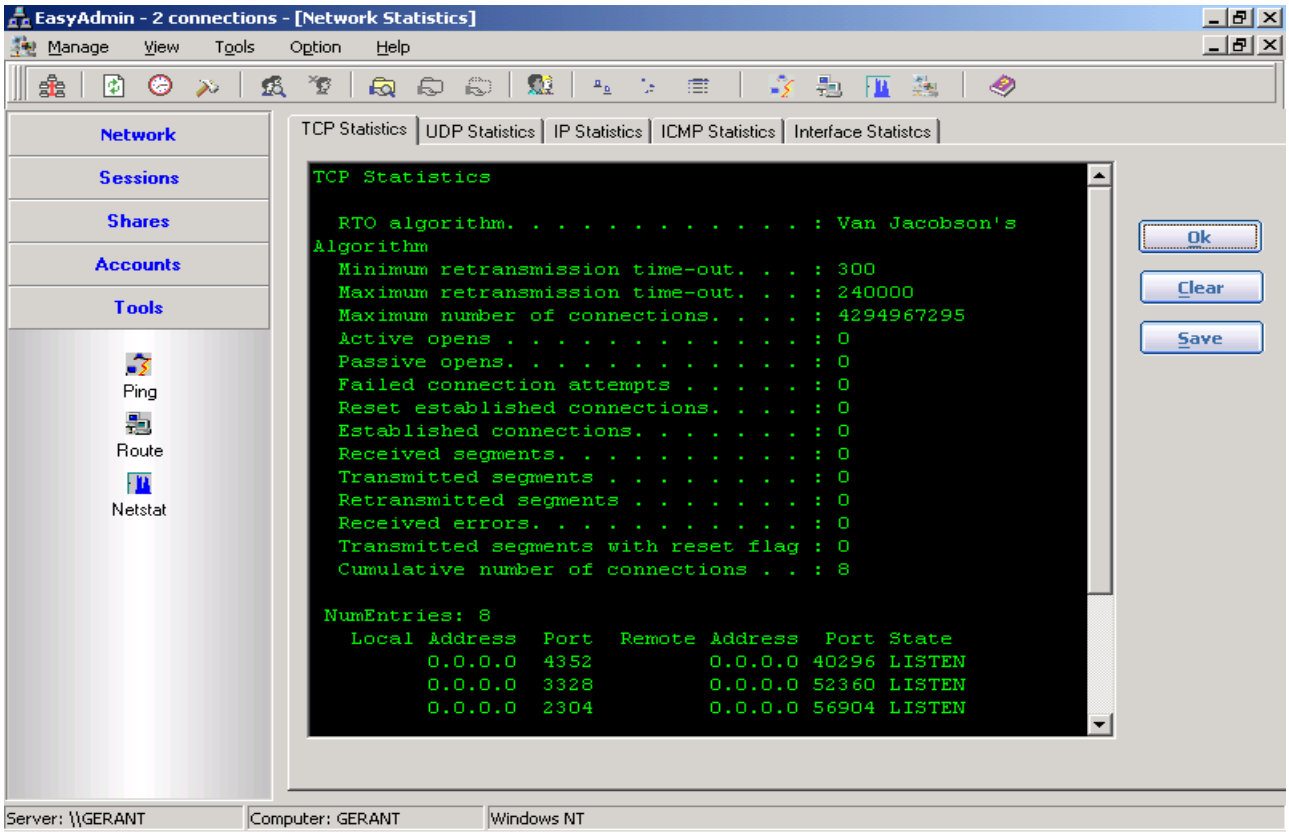

Fig.4.13 statistique sur les protocoles TCP/IP .

L'administrateur a, des fois, besoin d'effectuer des changements dans la table de routage, selon les besoins dans le réseau. Notre application offre une interface permettant de visualiser la table de routage et d'ajouter ou de supprimer une route d'une manière simple et rapide comme le montre Figure 4.14.

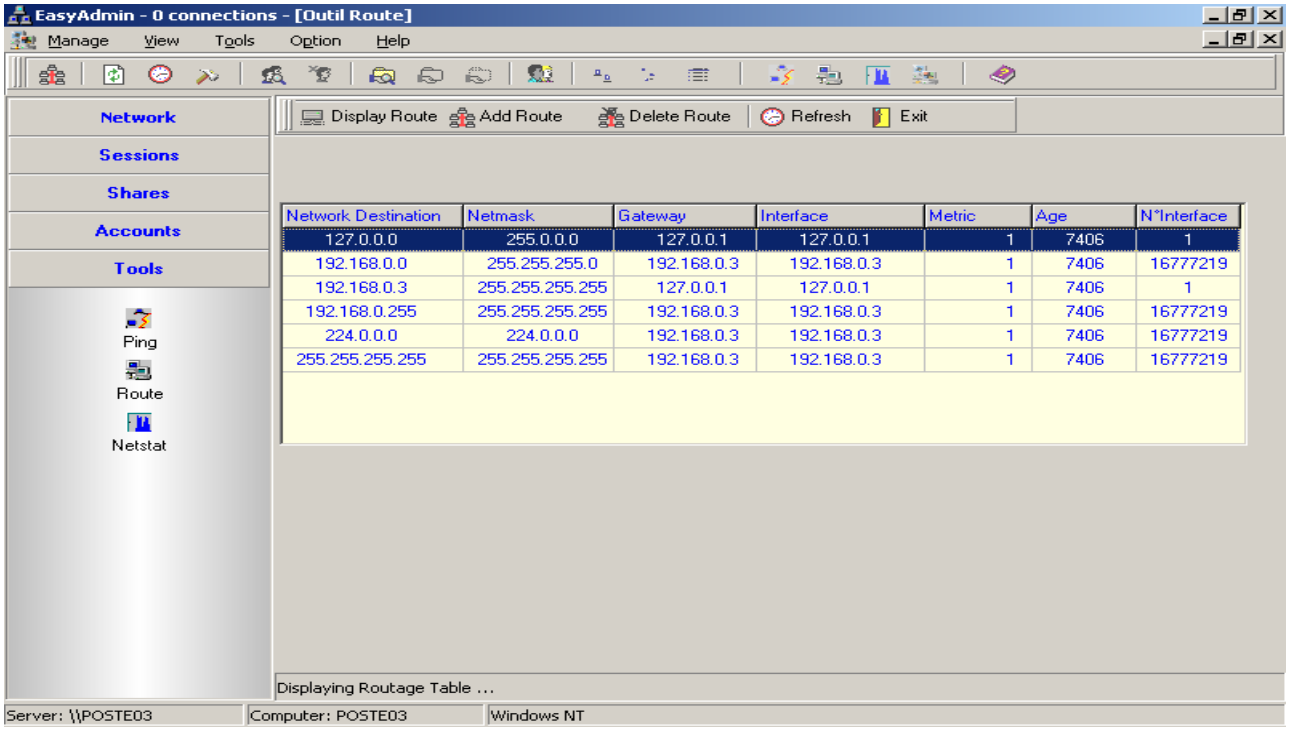

Fig.4.14 l'outil route.

Notre application offre aux administrateurs la possibilité d'obtenir des informations sur certains paramètres globaux du réseau. Comme illustré dans Figure 4.15, l'application nous permet d'obtenir les informations suivantes :

- Le nom du PC
- Le nom du domaine
- Les adresses IP des serveurs DNS
- Le type de nœud
- Le nom de serveur DHCP
- Si le routage est activé
- Si le PC comporte comme un Proxy ARP
- Si le DNS est active.

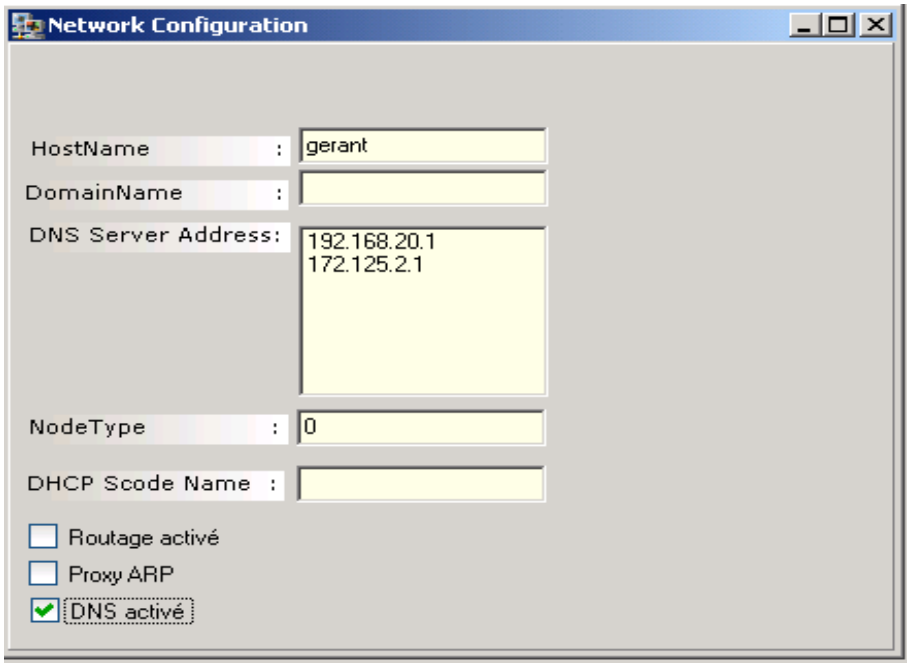

Fig.4.15 la configuration globale du réseau.

Les teste de connectivité du réseau est une opération presque quotidienne. On a souvent besoin de tester si un poste est connectée aux réseau ou non. Cette opération a été incluse dans notre application comme le montre Figure 4.16. On peut tester un seul poste comme on a la possibilité de tester plusieurs postes en spécifiant une plage d'adresses IP. Les adresses IP sont arrangées dans un tableau et une icône verte indique qu'un une poste est connecté tandis qu'une icône rouge indique que le poste ne répond pas.

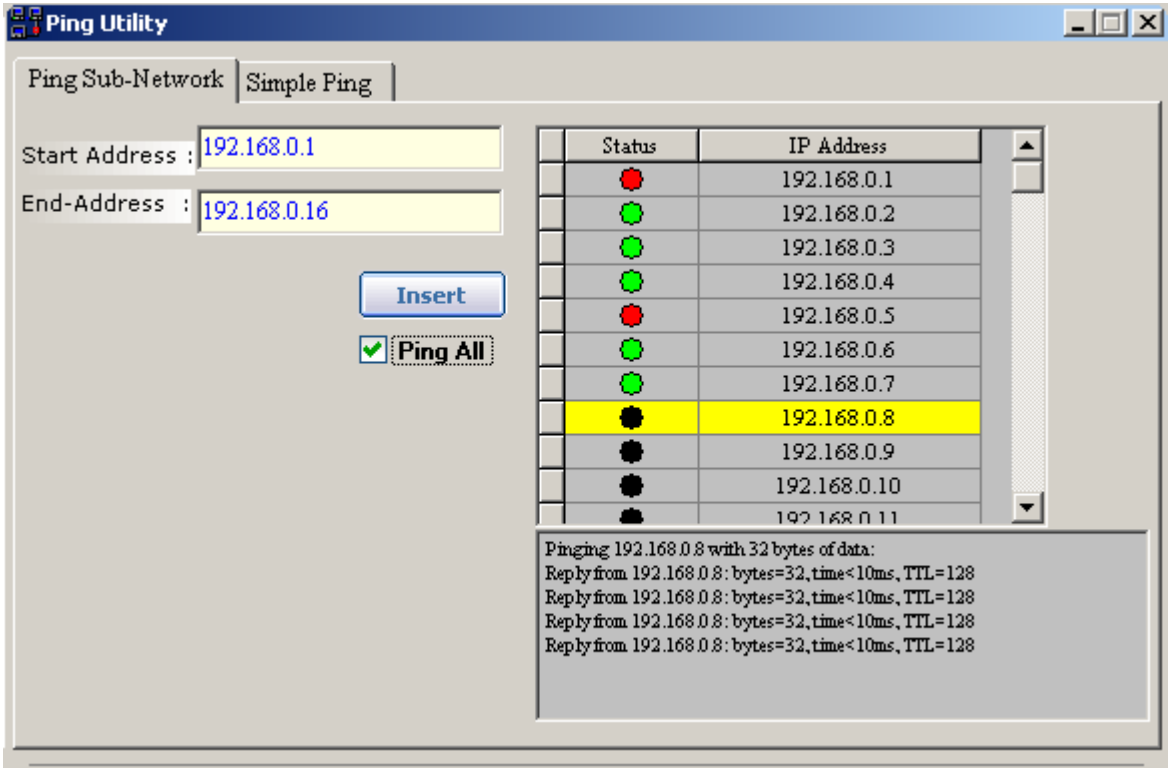

Fig.4.16 l'outil Ping.

De plus notre application offre la possibilité de rester en exécution, c'est-à-dire notre programme est résident, une icône apparaît dans la liste des programmes résidents. Si on clic avec le bouton droit de la souris sur cette icône, un menu contextuel apparaît avec les options suivantes :

- Fermer l'application
- Redémarrer Windows NT
- Arrêter Windows NT

Comme le montre la figure suivante:

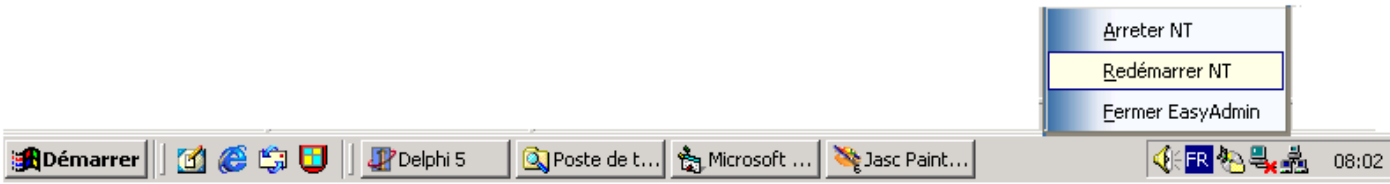

Fig.4.17 la permanence d'exécution de l'application.

Conclusion

La croissance exponentielle des réseaux et la complexité des équipements sont à l'origine de besoins des outils d'administration qui permettent leurs exploitations. On trouvera toujours un administrateur à qui, il manquera l'outil nécessaire pour réaliser une tâche particulière sur le réseau.
Les programmeurs réseau seront toujours confrontées aux progressions rapides des technologies d'information et de communication et interagissent lorsque de nouveaux besoins surgissent.
La programmation réseau est un domaine vaste, nouveau et en quelque sorte difficile à aborder pour les programmeurs dans le tiers-monde à cause du manque de documentations ou de sa cherté lorsqu'elle existe. Nous avons essayé à travers ce projet de fin d'étude de poser les concepts de base sur les réseaux et la programmation réseau pour encourager, éventuellement, d' autres à investir ce domaine.
Les APIs Windows présentent aux programmeurs la possibilité d'interagir avec le système d'exploitation et offrent des possibilités presque infinies.
Nous avons tenté dans ce projet d'implémenter certaines APIs qui concernent le réseau et d'interpréter leurs résultats dans une interface simple et conviviale. Nous avons découpé notre application en plusieurs parties. Une pour visualiser les postes de travail dans une interface graphique et de faire quelques opérations quotidiennes telles que Ping, émission d'un message et récolte de quelques informations. Une deuxième partie sert au contrôle des sessions ouvertes sur le serveur. Une autre partie concerne la gestion des ressources partagées et l'environnement des utilisateurs. Finalement, nous avons tenté d'implémenter l'équivalent des utilitaires Ping, Route, Netstat dans une interface simple et rapide.
L'application que nous avons développée n'est pas parfaite, elle peut évoluer dans le futur pour qu'elle soit mieux adaptée aux développements rapides des réseaux et répondre aux besoins de l'administrateur. Pour cela nous proposons ici quelques améliorations possibles à cette application.
Une amélioration possible est d'orienter l'application vers les services réseau, on peut contrôler les services et implémenter quelques services tel que Ftp, Telnet,…etc.
L'autre amélioration est d'utiliser certaines APIs concernant la gestion des utilisateurs, les groupes locaux et globaux ainsi que l'observation des événements survenus sur le serveurs.

Notre projet peut être considère comme un premier pas vers le développement de logiciels réseaux performants. Et nous espérons avoir réussi dans cette tache et que ce travail intéressera d'autres étudiants pour ajouter d'autres améliorations à cet édifice.

Références et bibliographie

[1] Pascal Nicolas, *Cours de réseaux*, Université d'angers, 2000.

[2] Jean -Pierre et Michelle claudé ,*Gestion des réseaux informatique*, Paris, Septembre 1993.

[3] Centre INRA de Corse, *http://www.corse.inra.fr/uic/resobur/page5-3.html*, 1997.

[4] Shreshtha Takshak of Honeywell Solutions Technology Lab, *www.developperIQ.com/ Magazinestories/03jun27dissectIP.php*, 2003.

[5] John Paul Mueller, *Windows 2000 le guide du programmeur*, Paris, 4éme trimestre, 2000.

[10] Gray Nebbett, *Le DICO référence API Windows NT/2000*, 19 rue Michel le comte 75003 Paris, 3éme trimestre 2000.

R.Simon, *Windows 95 Win32 programmation des API*, Paris, 1998.

Guy Pujolle, *Les réseaux*, Paris, 2003.

Philippe Gomez et Pierre Bichon, *Comprendre les réseaux d'entreprise*, Paris, 1995.

Gaig Hunt, *TCP/IP administration réseaux*, Paris, 1998.

Simon et Schuster Macmillan, *Windows NT 4.0 Server*, 19 rue Michel le conte, Paris, 1996.

Nouri Nabil et Bensemaoune Brahim, *Administration de réseau par le protocole SNMP*, Mémoire de fin d'étude pour l'obtention de diplôme d'ingénieur d'état en informatique, Université Amar Telidji Laghouat, 2003.

Webographie :

http://www.urec.cnrs.fr/cours/applis/admin98/sld047.html.

http://www.tulipe.cnam.fr/personne/duchien/poly.html.

http://www.ensimag.image.fr/cours/Exposes.Reseaux/administration/sommaire.html.

http://www.urec.cnrs.fr/cours/Wnt/wint-jres97.pdf.

http://raphaello.univ-fcompte.fr/NT/02-ConceptsETPlanification/ ConceptsETPlanification.htm.

http://www.iufm-fc.ac-montpellier/fc/documents/ntadministration/index.html.

http://www.iglooduhack.com/delphi-ip-helper.php.

http://www.msdn.microsoft.com.

http://www.mentalis.org/apilist.htm

http://delphi-jedi.org.