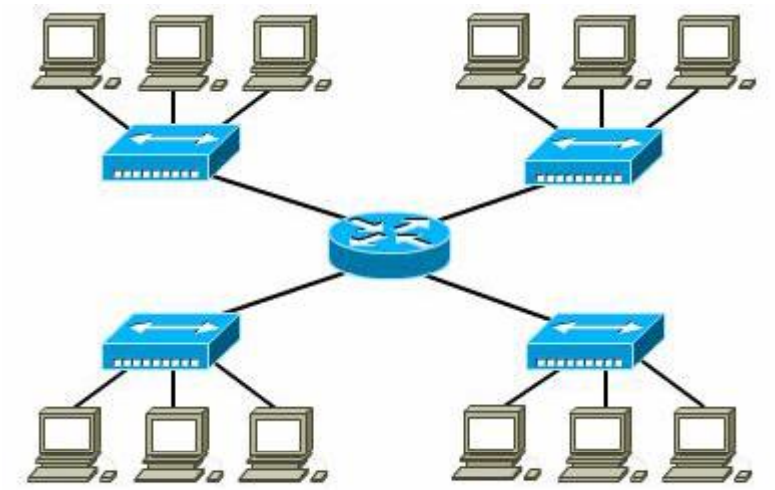
UNIVERSITE D'ANTANANARIVO
ECOLE SUPERIEURE POLYTECHNIQUE D'ANTANANARIVO
DEPARTEMENT GENIE ELECTRIQUE
FILIERE GENIE INDUSTRIEL

MISE EN PLACE D'UN RESEAU INTRANET



MEMOIRE DE FIN D'ETUDES EN VUE DE L'OBTENTION DU DIPLOME D'INGENIEUR EN GENIE INDUSTRIEL

Présenté et soutenu par : ANDRIHAJA Joseph
Sous la direction de : M^{r} RAKOTONDRASOA Justin

Promotion 2004 N°40 / 2004
Date de soutenance : 02 Août 2005

UNIVERSITE D'ANTANANARIVO
ECOLE SUPERIEURE POLYTECHNIQUE D'ANTANANARIVO
DEPARTEMENT GENIE MECANIQUE ET PRODUCTIQUE,
DEPARTEMENT GENIE ELECTRIQUE
FILIERE GENIE INDUSTRIEL

Mémoire de fin d'études en vue de l'obtention du diplôme d'Ingénieur en Génie Industriel

MISE EN PLACE D'UN RESEAU INTRANET

Président du jury : M^r^ SOLOFOMBOAHANGY

Membres du jury : M^r^ RAJAONARIVELO Jean André

M^r^ RAMELINA Arimonjy

M^r^ Yvon ANDRIANAHARISON

Présenté et soutenu par : M^r^ ANDRIHAJA Joseph.

Encadreur : M^r^ RAKOTONDRASOA Justin.

N°40/2004 Promotion 2004

INTRODUCTION

La croissance explosive de l'Internet a été largement présentée dans les nouvelles. Cependant, il y a une utilisation croissante plus rapide encore des technologies d'Internet qui transforme la manière que les sociétés utilisent pour entretenir la communication avec leurs employés, des clients, des fournisseurs, et des fournisseurs : Intranets. En bref, les organismes ont découvert que les utilisateurs peuvent utiliser les mêmes technologies qui rendent l'Internet réussi à leur réseau interne -- leur Intranet.

Le thème de notre travail consiste à la Mise en place d'un réseau intranet. Nous allons utiliser l'architecture Client/ Serveur. Pour cela nous utiliserons Windows 2000 Server sur le poste serveur.

Notre travail se divise en deux parties dont les suivantes :

- la première partie pour l'assimilation du concept du réseau local et ses technologies,
- la deuxième partie concerne l'administration du réseau intranet et ses applications.

CHAPITRE I

LE RESEAU LOCAL ET SES TECHNOLOGIES

I.1 Généralité

I.1.1 Généralités.

Un réseau informatique met en relation des ordinateurs comme un réseau téléphonique met en relation des personnes.

I.1.2 Modèle de communication OSI

Un modèle communication a été développé par l'ISO (International Standards Organisation) entre 1977et 1984. Il décrit la structure et le fonctionnement des protocoles de communications.

Ce modèle se nomme OSI (Open System Information). Il est constitué de sept couches. Chaque couche communique avec la couche correspondante des autres ordinateurs.
Lors de passage d'information d'une couche vers celle d'en-déssous, une en tête est ajouté aux données pour indiquer la provenance et la destination des informations.

Couche OSI	Nom de l'unité d'information
Application	données
Présentation	données
Session	données
Transport	Segment
Réseau	Datagramme
Liaison	Trame (ou paquet)
Physique	Bit

Tableau.I.1.2. Modèle en 7 couches de l'ISO

OSI Les différentes fonctions des 7 couches du modèle

- La couche physique (physical layer) : Assure le transport de l'information .Unité d'information [bit]

- La couche liaison (Line Layer) : Est responsable de l'acheminement des blocs d'information sans erreurs entre deux équipement adjacents du réseau. Blocs d'information [trames]
- La couche Réseau (Network layer) : Est responsable de l'acheminement des paquets de données qui transiteront à travers le système. Elle assure l'opération d'adressage, de routage des informations.
- La couche transport (transport layer) : Est responsable du contrôle du transport de bout à bout, au travers du réseau. Elle est responsable du transport des unités de données appelées messages. Elle contrôle le flux et découpe les messages en plusieurs paquets.
- La couche session : Elle prend en charge l'ouverture et la fermeture de session des utilisateurs
- La couche présentation : Elle représente les données transférées entre application et la structure des données
- La couche application : Elle exécute les applications et est responsable de la communication avec la couche 7 du récepteur

I.2 Interconnexion : Technologie élémentaire.

Pour réaliser la communication entre les ordinateurs, de supports de transmission sont nécessaire pour transporter les données. Parmi lesquels, nous citons les câbles paires torsadées et les fibres optiques qui sont le plus utilisées actuellement.

I.2.1 Les paires torsadées.

La paire torsadée est composée de 2 à 4 paires de fils torsadées sur toute sa longueur. C'est une meilleure protection contre les interférences électriques. On a deux types :

a)Les paires torsadées non blindées (Unshielded Twisted Pair : UTP)

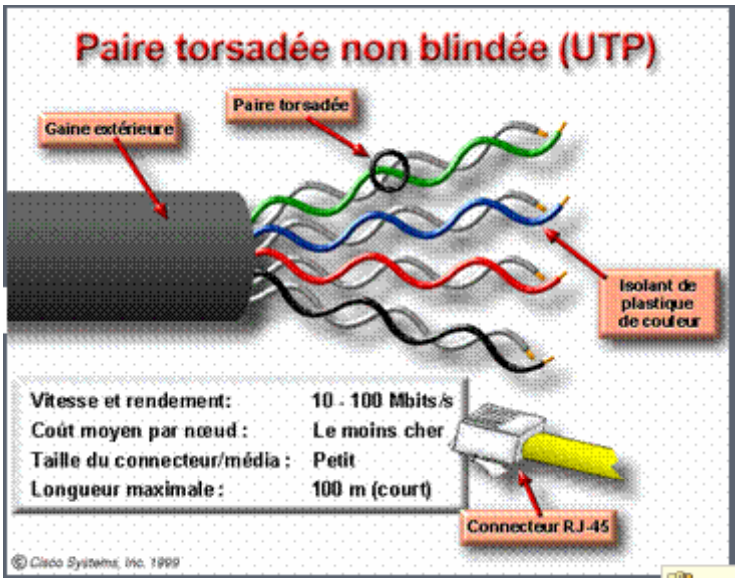


Fig.1.2.a : paire torsadée non blindée

b) Avantages et incovenients de paires torsadées non blindées.

- Il est facile à installer
- coûte moins cher
- n'occupe pas tout l'espace des conduits guide-fils
- moins de parasites sur le réseau
- capte davantage les interférences et les parasites électriques

c) Les paires torsadées blindées (Shielded Twisted Pair : STP)

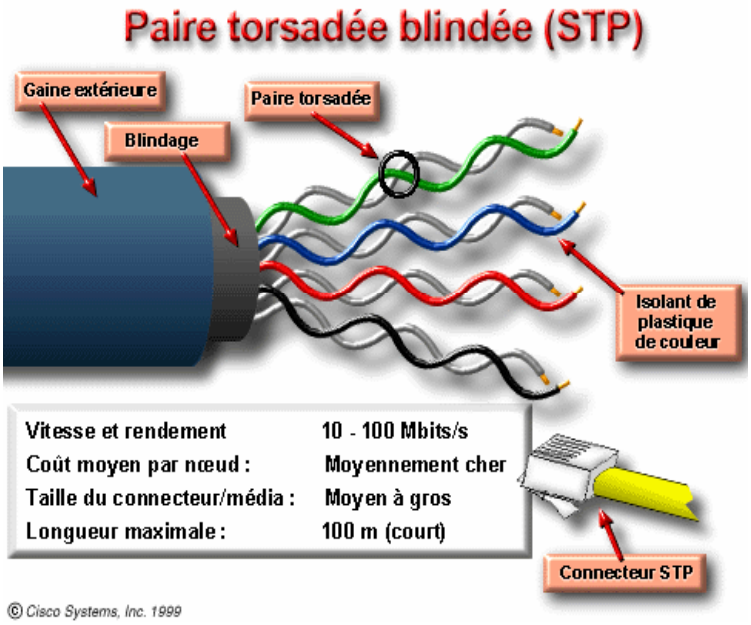


Fig.I.2.c : paire torsadée blindée.

Le câble à paires torsadées et blindées allie les techniques de blindage, d'annulation et de torsion de câbles.

d) avantages et incovenients de paires torsadées blindées.

Le câble à paires torsadées blindées présente tous les avantages et désavantages du câble à paires torsadées non blindées. Toutefois, le câble à paires torsadées blindées assure une plus grande protection contre toute interférence externe et est plus dispendieux que le câble à paires torsadées non blindées.

I.2.2 les fibres optiques

Quelques particularités de la fibre optique

-la plus utilisé est la fibre multimode 62.5/125.0µm

-usage d'un transducteur optique pour assurer la transformation entre le signal lumineux (en laser).

-distance maximal de 1,5km.

-Insensible aux perturbations électromagnétiques.

-vitesse de transmission jusqu'à 100Mbps.

-son principal désavantage est un coût élevé au mètre et la nécessité d'avoir un transducteur au raccordement de tous les appareils contenant de l'électronique (Serveur, switch, Routeur).

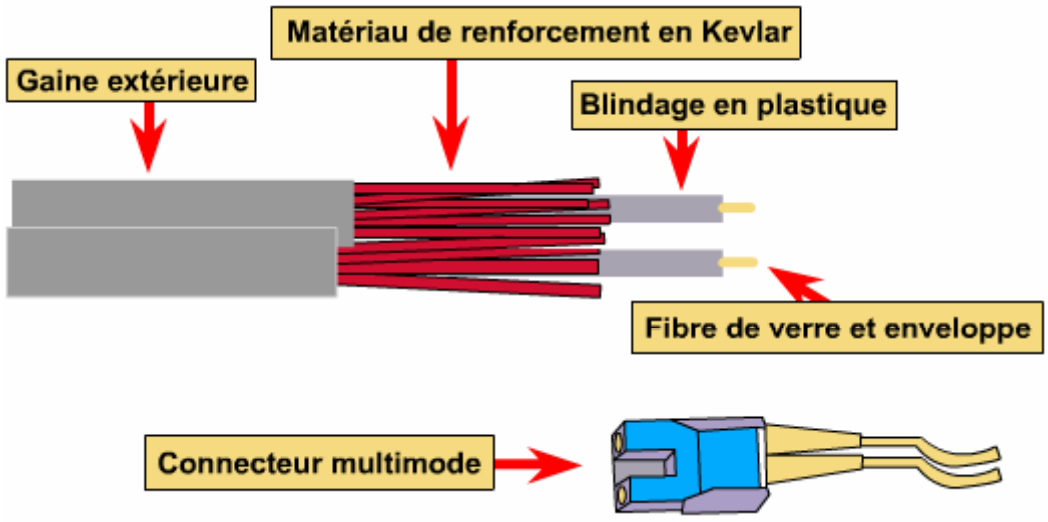


Fig.I.2.2 : fibre optique.

I-3 Les topologies d'un réseau local.

Il convient de distinguer la topologie physique de la topologie logique :
La topologie physique décrit la mise en pratique du réseau logique (câble etc.….) tandisque la topologie logique décrit le mode de fonctionnement du réseau, la répartition des nœuds et le type de relation qu'ont les équipements entre eux.

I-3.1 La topologie en anneaux.

Chaque nœud est relié au nœuds suivant et au nœuds précédents et forme ainsi une boucle : l'information transite par chacun d'eux et retourne à l'expéditeur.

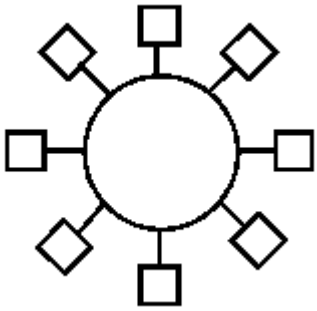


Fig.I.3.1 : la topologie en anneau.

I-3.2Les réseaux en bus.

Chaque nœud est connecté sur un bus. L'information passe devant chaque nœud et s'en va 'mourir' à l'extrémité du bus.

Fig.I.3.2 : la topologie en bus.

I-3.3 Les réseaux en étoile.

Chaque nœud est directement relié sur un nœud central : l'information passe d'un nœud périphérique au nœud central, celui-ci devant gérer chaque liaison.

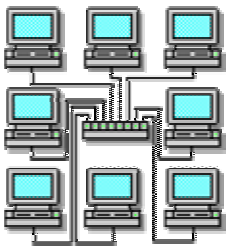


Fig.1.3.3 : la topologie en étoile.

I.4 La transmission dans les réseaux locaux.

Deux approches sont possibles pour les transports des éléments binaires provenant des applications :

-Soit l'information est véhiculée en bande de base

-Soit chaque type d'information se voit allouer une bande passante en fonction de ses besoins. Dans cette approche les signaux numériques sont modulés sur une porteuse

I.4.1 La transmission en bande de base.

Cette transmission envoie les signaux numériques sur un seul canal. Des transmissions multiples peuvent être envoyé sur ce canal au même instant en utilisant le technique de multiplexage. On utilise souvent des répéteurs. Car le signal tend à se dégénérer au fil de sa circulation.

I.4.2 Transmission en large bande.

La transmission en large bande s'appuis sur un signe analogique, une plage de fréquence et un support de communication (câble coaxial ou fibre optique) divisible en plusieurs canaux séparés par de petites bandes de fréquences inutilisées afin qu'un canal n'interfère avec un signal transmis sur ses voisins.

I.4.3 Codage électrique : Manchester Bi-phasé.

Le signal électrique parcourant le câble doit correspondre à des caractéristiques permettant de répondre à certains besoins.

-une immunité aux bruits électromagnétiques (parasites).

-pas de composant continue afin de diminuer les pertes électriques (effet joules).

-possibilité d'inverser la polarité.

Le code Manchester Bi-phasé a été adopté : il s'agit d'une modulation en bande base , c'est-à-dire que le signal binaire est transformé en un signal de type analogique sans être translaté en fréquence (par opposition a une signal radio).

Le code Manchester simple.

Il consiste à introduire dans le signal des transitions au milieu de chaque intervalles Δ par une front montant lorsque le bit a_i =0 et par un front descendant lorsque le bit a_i =1.

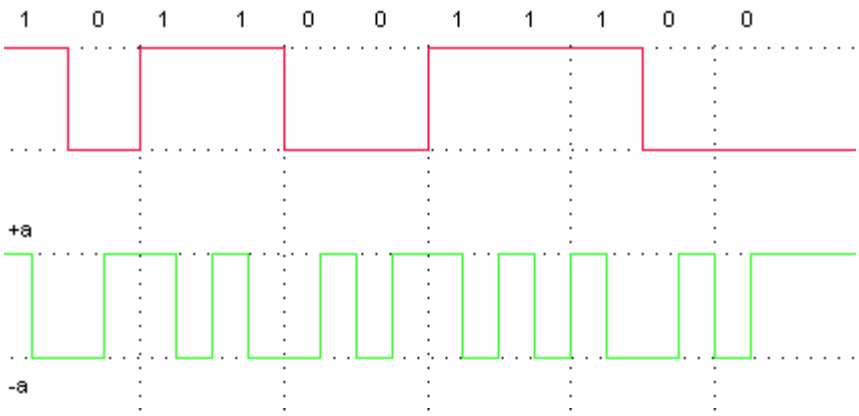


Fig.I.4.1 : le codage Manchester.

I.4.4 La carte réseau (NIC/Network Interface Card.)

Ce matériel permet la connexion d'une station au réseau. Sa fonction consiste à adapter l'unité hôte au média du réseau. Il convertit le signal en série provenant du câble en un signal parallèle pour être décodé ensuite.

La carte réseau doit être installée et configurée comme tout nouveau matériel du PC. Et comme toute configuration de la carte d'extension, elle a ses options de configuration :
Le numéros d'interruption IRQ (*Interrupt Request*) ; ligne sur laquelle un périphérique peut envoyer des signaux pour attirer l'attention du processeur lorsqu'il est prêt à recevoir ou envoyer des informations.
Le numéros de canal d'accès direct mémoire DMA cette option permet pour une carte DMA d'accéder directement au processeur c'est-à-dire que ses données sont immédiatement traitées
L'adresse port de base d'entrer – sortie :

Canal de transfert de données entre un périphérique et le microprocesseur. C'est pour adresser les données quand elles sont prêtes à être traitées

Car un signal en bande de base tend à dégénérer à la fin de sa circulation
L'adresse mémoire de base ; c'est une partie de la mémoire RAM attribuée à la carte si sa mémoire est insuffisante pour le traitement de donnée.

La communauté IEEE normalise une carte en lui adressant une adresse physique composée de 12 chiffres en hexadécimal.

A noter aussi que le performance du réseau dépendait de la carte puisqu'elle est responsable de l'envoi et réception des données sur le câble. En conséquence, le débit d'information transmise est celui de la carte.

Fig.I.4.2 : Carte réseau

I.4.5 Les méthodes d'accès

Une carte réseau doit « écouter » le câble du réseau (écouter si une fréquence circule, si une porteuse passe, si un signal défile, …), attendre que le câble soit libre (qu'il n'y ait pas ou plus de porteuse), émettre et retransmettre si les trames ont été détruites pendant le voyage. En bref, il faut éviter les collisions de paquets.

I.4.3.1 La méthode d'accès CSMA/CD.

La méthode d'accès CSMA/CD (Carrier-Sense Multiple Access / Collision Detection) impose à toutes les stations d'un réseau d'écouter continuellement le support de communication, pour détecter les porteuses et les collisions. C'est le transceiver (le mot valise « transmeter et receiver » qui écoute le câble, et qui lit les entêtes des paquets (de 64 octets à 1500 octets au maximum). La méthode d'accès CSMA/CD est relativement fiable et rapide pour les réseaux composés d'un nombre restreint de stations. Plus le nombre de station est important, plus le risque de collision croît, plus le nombre de collisions augmente, et plus les délais d'attente sont importants. Le nombre de collision peut « exploser » rapidement, le réseau saturer, si le nombre de station est excessif.

I.4.3.2 La méthode du passage du jeton.

La méthode du passage du jeton est une méthode propre aux réseaux en anneau. Les stations doivent attendre le jeton qui donne la permission de « parler », il y a des délais d'attente pour obtenir le jeton, mais il n'y a pas de collisions, donc pas de délais de retransmission. Le jeton est un paquet spécial qui passe de station en station, et qui autorise celle qui le détient à émettre.

Les stations sont ordonnées les unes par rapport aux autres, et la plus haut dans la hiérarchie a la responsabilité de surveiller le bon fonctionnement du jeton (la durée des trames pour parcourir l'anneau, le temps moyen de rotation, la suppression des trames qui sont revenues à leur expéditeur, l'avertissement des autres stations qu'il est toujours le superviseur,…), et éventuellement d'en créer un nouveau. Le superviseur d'un réseau Token Ring est d'abord la première station allumée sur le réseau, puis si celle-ci se déconnecte, il y a une l'élection du nouveau superviseur. Après une élection, c'est la station qui possède l'adresse MAC la plus grande qui est élue superviseur.

I.4.3.3 La méthode d'accès de la priorité de la demande.

La méthode d'accès de la priorité de la demande, aussi appelée DPMA (Demand Priority Access Method), est une méthode d'accès récente qui a été mise au point pour les réseaux mixtes en bus en étoile.

Les réseaux 100VG-AnyLAN (ETHERNET à 100 Mb/s) répondent à la norme IEEE 802.12 définie pour les réseaux en bus en étoile. Les réseaux 100VG-AnyLAN sont constitués de plusieurs concentrateurs (HUB), ou de répéteurs. Les concentrateurs sont reliés ensembles et forment une architecture « double », une architecture à deux niveaux, les concentrateurs forment entre eux un bus, comme une épine dorsale, et chaque concentrateur contient un anneau auquel sont reliées les stations. Ainsi, des données peuvent être transmises

simultanément, mais à l'intérieur de sous-ensembles différents. D'autre part le câblage d'un réseau 100VB-AnyLAN est constitué de quatre paires de fil ce qui permet quatre transmissions simultanées.

Les concentrateurs gèrent l'accès au réseau. Le réseau est composé du même nombre de sous-ensembles qu'il y a de concentrateurs. Chaque concentrateur s'occupe de son sous-ensemble. Le réseau est en quelque sorte segmenté en plusieurs parties. Les messages ne sont pas diffusés sur tout le réseau, mais seulement sur la partie concernée. La gestion de l'accès au réseau est centralisée (il y a autant de pôles centralisateurs que de concentrateurs).

Les concentrateurs interrogent tous les « nœuds terminaux » de la partie du réseau dont ils ont la charge, c'est à dire toutes les stations branchées sur leur anneau, et tous les concentrateurs auxquels ils sont reliés. L'interrogation des nœuds s'effectue à tour de rôle (méthode « round-robin »), et permet à chaque concentrateur de connaître les informations d'adressage et de routage de chacun :

- L'adresse des nœuds terminaux d'un même anneau
- Les plages d'adresse gérée par les concentrateurs proches
- L'état de fonctionnement de chacun des nœuds

La méthode d'accès de la priorité de la demande est une méthode d'accès à contention. La méthode d'accès de la priorité de la demande implique que deux ordinateurs peuvent se retrouver en situation de « rivaliser » pour obtenir le droit de « parler », mais cette méthode d'accès a l'avantage de permettre une configuration où certains types de données, définis à l'avance, ont la priorité sur d'autres. La priorité de certains types de données permet de résoudre les conflits ; quand deux demandes d'accès ont la même priorité, alors les deux demandes sont traités en alternance.

CHAPITRE II

LE PROTOCOLE TCP/IP

II.1 Le protocole TCP/IP.

TCP/IP est une suite de protocoles (utilisé sur Internet). Il signifie Transmission Control Protocol/Internet Protocol. Il représente la façon dont les ordinateurs communiquent sur Internet. Pour cela il se base sur l'adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. Etant donné que la suite de protocoles TCP/IP a été créée à l'origine dans un but militaire, elle doit répondre à un certain nombre de critères parmi lesquels :

- fractionnement des messages en paquets
- utilisation d'un système d'adresses
- acheminement des données sur le réseau (routage)
- contrôle des erreurs de transmission de données

La connaissance du système de protocole TCP/IP est nécessaire pour les personnes désirant administrer ou maintenir un réseau fonctionnant dans un système de protocoles TCP/IP.

II.1.1 comparaison entre le modèle TCP/IP et le modèle OSI.

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches :

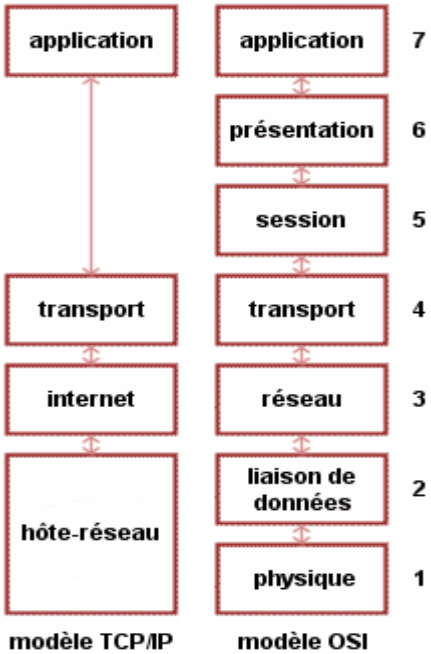


Fig.II.1.1 : le modèle à 4 couches

Voici les principaux protocoles faisant partie de la suite TCP/IP :

Modèle TCP/IP
Couche Application : Applications réseau
Couche Transport TCP ou UDP
Couche Internet IP, ARP, RARP
Couche Accès réseau FTS, FDDI, PPP, Ethernet, Anneau à jeton (Token ring)
Couche Physique

Tableau.I.1.1 : modèle tcp/ip.

II.1.2 le protocole TCP.

Le protocole TCP est basé en couche 4. Il ouvre une session et effectue lui-même le control d'erreur. Il est alors appelé "mode connecté".

Un segment TCP est constituée comme suit:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Port Source	Port destination
Numéro d'ordre	
Numéro d'accusé de réception	
Décalage données / réservée / URG / ACK / PSH / RST / SYN / FIN	Fenêtre
Somme de contrôle	Pointeur d'urgence
Options	Remplissage
Données	

Fig.II.1.2 : Un segment TCP

Signification des différents champs:

- *Port Source* (16 bits): Port relatif à l'application en cours sur la machine source
- *Port Destination* (16 bits): Port relatif à l'application en cours sur la machine de destination
- *Numéro d'ordre* (32 bits): Lorsque le drapeau SYN est à 0, le numéro d'ordre est celui du premier mot du segment en cours.
  Lorsque SYN est à 1, le numéro d'ordre est égal au numéro d'ordre initial utilisé pour synchroniser les numéros de séquence (ISN)

- *Numéro d'accusé de réception* (32 bits): Le numéro d'accusé de réception également appelé numéro d'acquittement correspond au numéro (d'ordre) du prochain segment attendu, et non le numéro du dernier segment reçu.
- *Décalage des données* (4 bits): il permet de repérer le début des données dans le paquet. Le décalage est ici essentiel car le champ d'options est de taille variable
- *Réservé* (6 bits): Champ inutilisé actuellement mais prévu pour l'avenir
- *Drapeaux (flags)* (6x1 bit): Les drapeaux représentent des informations supplémentaires:
    - URG: si ce drapeau est à 1 le paquet doit être traité de façon urgente.
    - ACK: si ce drapeau est à 1 le paquet est un accusé de réception.
    - PSH (PUSH): si ce drapeau est à 1, le paquet fonctionne suivant la méthode PUSH.
    - RST: si ce drapeau est à 1, la connexion est réinitialisée.
    - SYN: Le Flag TCP SYN indique une demande d'établissement de connexion.
    - FIN: si ce drapeau est à 1 la connexion s'interrompt.
- *Fenêtre* (16 bits): Champ permettant de connaître le nombre d'octets que le récepteur souhaite recevoir sans accusé de réception
- *Somme de contrôle* (Checksum ou CRC): La somme de contrôle est réalisée en faisant la somme des champs de données de l'en-tête, afin de pouvoir vérifier l'intégrité de l'en-tête
- *Pointeur d'urgence* (16 bits): Indique le numéro d'ordre à partir duquel l'information devient urgente
- *Options* (Taille variable): Des options diverses
- *Remplissage*: On remplit l'espace restant après les options avec des zéros pour avoir une longueur multiple de 32 bits

II.1.3 le protocole IP.

IP signifie "Internet Protocol", protocole Internet. Il représente le protocole réseau le plus répandu. Il permet de découper l'information à transmettre en paquets, de les adresser, de les transporter indépendamment les uns des autres et de recomposer le message initial à l'arrivée. Ce protocole utilise ainsi une technique dite de commutation de paquets. Il apporte, en comparaison à Ipx/Spx et Netbeui, l'adressage en couche 3 qui permet, par exemple, la fonction principale de routage.

Ce protocole travail en mode non connecté. Ainsi, avant et après le transfert de datagramme, IP il n'y a aucun échange d'information. C'est en vérifiant l'adresse de destination que le datagramme est délivré sinon il est retransmis à un gateway (passerelle : *ordinateur servant de liaison entre deux réseaux*).

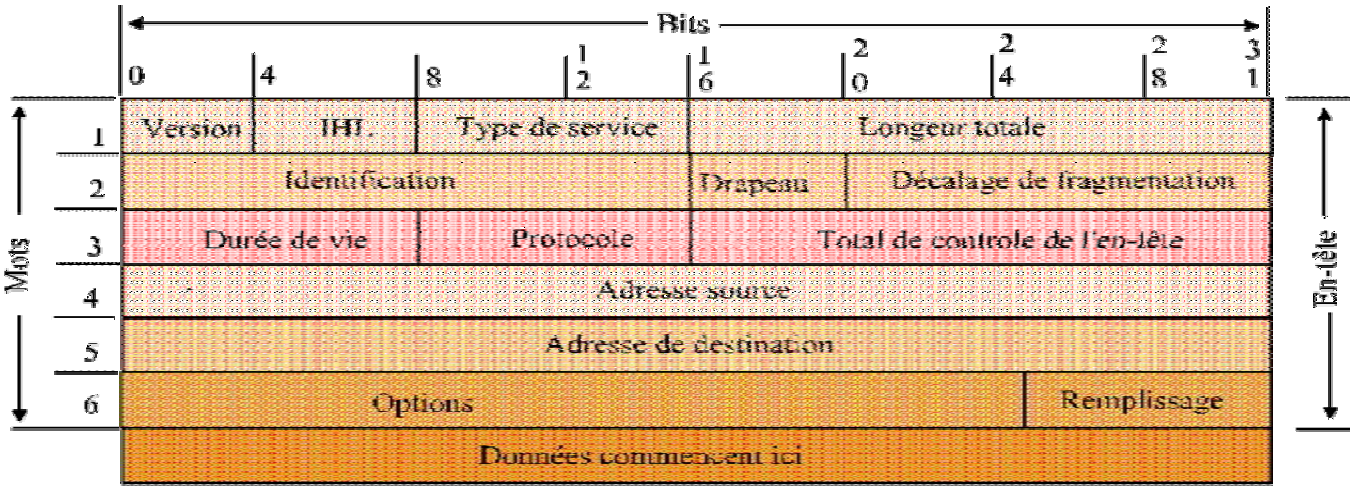


Fig.II.1.3 : En tête d'un datagramme IP.

Version (4 bits) : Le champ Version indique le format de l'en-tête Internet.

IHL (4 bits) Internet Header Lenght : taille de l'en-tête Internet en Mots de 32 bits. (Mimimun de 160 bits = 5 Mots de 32 bits)

Type de service (8 bits) : indique la qualité de service désiré, selon la valeur du champ.

Bits 0-2: Prioritée

- 111 - Network Control
- 110 - Internetwork Control
- 101 - CRITIC/ECP
- 100 - Flash Override
- 011 - Flash
- 010 - Immediate
- 001 - Priority
- 000 - Routine

Bits 3 : 0 = Délai normal, 1 = Faible délai

Bits 4 : 0 = Utilisation normale, 1 = Utilisation élevé

Bits 5 : 0 = Fiable, 1= Très fiable

Bits 6-7 : Réservé pour une utilisation future.

Longueur Total(16 bits)

- La longueur total est la longueur du datagramme, exprimé en octets, incluant l'en-tête (Longueur Total = Entête + Données).
- Le mécanisme de fragmentation est entièrement défini par les champs du datagramme IP. Le contrôle de la fragmentation et le réassemblage du datagramme est réalisé par trois champs de l'en-tête: IDENTIFICATION, DRAPEAUX et DECALAGE DE FRAGMENTATION.

Identification: 16 bits Champs d'indentification pour aider dans l'assemblage des fragments du datagramme.

Drapeaux(3 bits (Drapeaux de control))

Bit 0: réservé

Bit 1: (DF) 0 = Fragmenté, 1 = Non Fragmenté (Indique que le datagramme ne peut être fragmenté)

Bit 2: (MF)

- 0 = Dernier Fragment, 1 = Fragment à suivre
- Le bit MF est mis à un si le datagramme n'est pas le dernier fragement du message.

Décalage de fragmentation (Fragment offset)(13 bits)

- Ce champ indique à quel datagramme appartient ce fragment. les fragments sont comptés en unités de 8 octets. Ce format permet 8192 fragments de 8 octets pour un total 65,536 octets.

Durée de vie (8 bits) : indique en secondes, le temps maximal de transit du datagramme dans l'interconnexion de réseaux.

Protocole (8 bits) : indique quel protocole est utilisé dans la zone des données.

Total de contrôle de l'en-tête (16 bits) : Control d'erreur uniquement sur le champ d'en-tête

Adresse Source (32 bits) : Adresse IP source.

Adresse Destination(32 bits) : Adresse IP Destination.

Options: variable (selon les options choisies)

- Les options sont incluses essentiellement à des fins de test ou de mise au point. Le champ Options est codé entre 0 et 40 octets. Il n'est pas obligatoire, mais permet le "Tuning de l'entête IP". Afin de bien gérer les Options, cela doit commencer par un octet de renseignement. Voici le détail de cet octet :

- Le champ de Bourrage dépend des options choisies. Le champ Bourrage est de taille variable comprise entre 0 et 7 bits. Il permet de combler le champ option afin d'obtenir une entête IP multiple de 32 bits. La valeur des bits de bourrage est 0.

II.1.4 Les adressages IP.

Le protocole TCP/IP utilise des numéros de 32 bits, appelées adresse IP, on les note sous la forme xxx.xxx.xxx.xxx où les xxx s'écrivent sous forme de 4 numéros allant de 0 à 255 (4 fois 8 bits). Les ordinateurs s'identifient par ces adresses pour établir la communication entre eux.

Une adresse IP comporte deux parties: la "partie réseau" et la "partie hôte". Le format de ces parties différent d'une adresse IP à l'autre. Le nombre de bits d'adresse utilisé pour identifier le réseau et le nombre utilisé pour reconnaître l'hôte varient en fonction de "classe de l'adresse".

II.1.4.1 classe de l'adresse.

Classe A :r.n.n.n

Classe A :r.r.n.n

Classe A :r.r.r.n

(r – adresse réseau, n – adresse hôte)

II.1.4.2 Attribution des adresses IP.

Le but de la division des adresses IP en trois classes A,B et C est de faciliter la recherche d'un ordinateur sur le réseau. De cette facon, il est possible de rechercher d'abord le réseau

que l'on désire atteindre puis de chercher un ordinateur sur celui-ci. Alors on attribue les adresses IP selon la taille du réseau.

Classe Nombre de réseaux possibles Nombre d'ordinateurs maxi sur chacun

Classe	Nombre de réseaux possibles	Nombre d'ordinateurs maxi sur chacun
A	126	16777214
B	16384	65534
C	2097152	254

Tableau II.1.4.2 : nombre de réseau possible pour chaque classe.

Les adresses de classe A sont réservées aux très grands réseaux, tandis que l'on attribuera les adresses de classe C à des petits réseaux d'entreprise.

II.1.4.3 Adresses IP réservées.

Il arrive fréquemment dans une entreprise qu'un seul ordinateur soit relié à Internet, c'est par son intermédiaire que les autres ordinateurs du réseau accèdent à Internet (on parle généralement de Proxy). Dans ce cas, seul l'ordinateur relié à Internet a besoin de réserver une adresse IP auprès de l'INTERNIC. Toutefois, les autres ordinateurs ont tout de même besoin d'une adresse IP pour pouvoir communiquer ensemble de façon interne.

Ainsi, l'INTERNIC a réservé une poignée d'adresses dans chaque classe pour permettre d'affecter une adresse IP aux ordinateurs d'un réseau local relié à Internet sans risquer de créer de conflits d'adresses IP sur le réseau. Il s'agit des adresses suivantes:

· 10.0.0.1 à 10.255.255.254

· 172.16.0.1 à 172.31.255.254

· 192.168.0.1 à 192.168.255.254

Remarques :

On a les adresses par convention suivantes :

- Une adresse de diffusion « restreinte » ou « dirigée » contient un identificateur de machine où tous bits sont à 1.(ex: adresse réseau classe B 163.5.255.255 BroadCast)

§ Une adresse de diffusion « locale » ou « plein 1 » (« all 1s ») comporte les 32bits IP à 1. (Utiliser lors du démarrage)

§ L'adresse de Classe A de « boucle locale » (loopback) vaut 127.0.0.1. Elle est destiné

CHAPITRE III

LE SYSTEME D'EXPLOITATION WINDOWS 2000 SERVER

III.1 Définition d'un système d'exploitation

Le système d'exploitation est un ensemble de programmes très complexe permettant de gérer les périphériques entiers Il permet également de traduire machine pour être compréhensible par les utilisateurs. C'est un interpréteur de commande.

III.2 Présentation de windows 2000 server.

Au cœur d'un réseau, Windows 2000 fournit à toute entreprise les services qu'elle attend d'un système d'exploitation moderne : la gestion de fichiers et d'impression, la sécurité, l'accès à l'internent, la prise en charge du client, les services de communication et toute une gamme de services d'application et d'assistance.

Windows 2000 est plus stable moins aux sujet aux blocages, et il n'a besoin d'être redémarré que suite à quelque cas de reconfiguration.

En matière de sécurité, Windows 2000 adopte le protocole d'authentification kerberos. Quant un utilisateur se connecte au réseau, kerberos crée un billet (ticket) qui l'authentifie auprès de toutes les ressources du réseau auxquelles il souhaite accéder pendant toute la durée de sa session. Ainsi, le nombre de requêtes d'authentification que les serveurs de domaines doivent gérer diminue. Pour ce qui est de la sécurité des fichiers, Windows 2000 office le système de cryptage EFS (Encrypted File System) qu'on peut installer en tant qu'extension de NTFS.

III.3 Configuration requise pour Windows 2000 Server

Avant d'installer Windows 2000, on vérifie que éléments matériels figurent sur la liste de compatibilité matérielle (HCL, Hardware Compatibility List) de Windows 2000, car Microsoft fournit uniquement des pilotes testés pour les périphériques répertoriés dans cette liste. L'utilisation d'autres périphériques peut entraîner des problèmes pendant et après l'installation

Composant	Configuration requise
Processeur	Processeur Pentium 133Mhz ou supérieur

	Windows 2000 Server prend en charge jusqu'à quatre processeurs
Mémoire	256 Mo recommandés au minimum (128Mo pris en charge) 4Go au maximum
Espace disque dur	2 Go avec au minimum 1Go d'espace disponible
Affichage	Moniteur VGA (vidéo graphique ou à résolution Supérieure
Lecteur	Lecteur de CD-ROM 12x u plus rapide

Tableau.III.3 : la configuration matérielle pour Windows 2000 Server.

III.4 Installation de Windows 2000 Server.

L'installation de Windows 2000 Server se présente sous deux cas possible soit la nouvelle installation, soit la mise à niveau.

III.4.1 Les étapes d'installation de Windows 2000 Server à partir d'un CD-ROM

-Démarrage de l'ordinateur à partir du CD-ROM

-Sélection de l'option permettant d'installer une nouvelle copie de Windows 2000 Server

-Lire et accepter le contrat de licence

-Sélection de la partition sur laquelle on installe Windows 2000 Server

-Sélection du système de fichier

-Modification des paramètres régionaux

-Entrer le nom de l'administrateur et celui de la licence

-Entrer le nom de l'ordinateur et le mot de passe Administrateur local

-Sélectionner les composants facultatifs de Windows 2000 Server

-Sélection des paramètres de dates heure et fuseau horaire.

III.4.2 La mise à niveau de Windows 2000 Server

Plusieurs raisons amènent à préférer une mise à niveau de versions antérieures de Windows 2000 Server à une nouvelle installation. Tout d'abord, la configuration est plus simple lors d'une mise à niveau et les utilisateurs, paramètres, groupes, droits et autorisations existants sont conservés. En outre il n'y à pas à réinstaller les fichiers et les applications. Ce pendant il faut identifier la procédure de migration et sauvegarder les fichiers de données et les paramètres importants.

a)Indentification des procédures de mise à niveau de serveurs

A partir de	Mise à niveau
Un contrôleur principal de domaine ou un contrôleur secondaire de domaine exécutant Windows NT	Un contrôleur de domaine exécutant Windows 2000 Server
Un serveur membre exécutant Windows NT Server 3.5.1 ou 4.0	Un serveur membre exécutant Windows 2000 Server

Tableau.III.4.2 : Procédure de mise à niveau.

b)Sauvegarde des fichiers de données et des paramètres importantes.

On effectue les tâches suivantes :

-corriger les erreurs répertoriées dans l'observateur d'événements.

-sauvegarder tous les lecteurs.

-sauvegarder les registres.

-mettre à jour la disquette de réparation d'urgence.

-supprimez les détecteurs de virus' les services réseau d'autres éditeurs et les logiciels clients.

-déconnectez les câbles série onduleurs.

-conserve les requêtes d'interruptions pour les périphériques ISA (non plug-and-Play Industry Standard Architecture).

NOTE:

Pour l'installation de Windows 2000 Server après Windows xp, voir annexe2.

III.5 Les caractéristiques de Windows 2000 Server.

Windows 2000 fournit des services permettant à deux applications d'exploiter en même temps deux ou plusieurs processeurs. Il subdivise les processus en plusieurs unités d'exécution (les threads).

III.5.1 Traitement multimthread.

Quand un programme exécute une commande particulière (une impression, une communication avec un autre programme, un calcul de donnée une E/S vers un system d'exploitation de fichiers ou n'importe quelle autre tache), l'exécution de cette commande nécessite plusieurs étapes. Mais le processeur n'accorde l'attention à un programme que durant quelques cycles d'horloges aux mieux. Alors pour en accélérer l'exécution la commande est subdivisée en plusieurs petites tâches (threads). Un programme exécutable

engage un processeur qui, à son tour, génère un ou plusieurs threads capable d'exécuter plusieurs threads en même temps ; Windows 2000 optimise le temps de travail du processeur.

III.5.2 Traitement multitâche.

Un système d'exploitation multitâche donne l'impression que le processeur accorde son attention à plusieurs processus en même temps. Ce te tour de temps passe-passe peut se réaliser grâce au partage du temps du processeur. Les cycles d'horloge du processeur sont subdivisés et mis à la disposition de plusieurs threads à la fois grâce à un procédé nommée commutation de contexte (Context Switching). A un instant donné, seul un thread s'exécute réellement sur un microprocesseur, mais cet instant et si bref que l'exécution de plusieurs threads semble concurrente et simultanée.

III.5.3 Multitraitement (multiprocessing).

Le système d'exploitation Windows 2000 accord un niveau de priorité à chaque processus qu'il exécute. Il existe trente deux niveaux numérotés de 0 à 31. Plus le chiffre est élevé plus la priorité d'accès au multiprocesseur l'est également. Les processeurs en mode utilisateur ont un niveau de priorité allant de 0 à 15 et les processus en mode noyau de 16 à 31.

III.6 L'architecture du système d'exploitation Windows 2000.

III.6.1 Mode noyau.

Le mode noyau est le mode de fonctionnement privilégié des processus qui peuvent accéder au matériel et aux données du système. L'exécutif et la couche HAL de Windows 2000 fonctionnent en mode noyau.

Le mode noyau se compose de divers éléments qui sont regroupés en 5 catégories :
.l'exécutif Windows 2000 contrôle la gestion d'objets et la sécurité, et prend en charge le E/S des périphériques.

- les différents modules gestionnaires contrôles le mémoire virtuel
- les pilotes du périphérique établissement la communication avec les périphériques.
- le noyau proprement parler gère le CPU (Central Processing Unit)
- la couche d'abstraction du matériel (HAL) c'est la partie de l'exécutif qui communique véritablement.

III.6.2 Mode utilisateur

On appelle mode utilisateur (user mode) la partie du système d'exploitation sur laquelle l'utilisateur peur agir. Le mode utilisateur comprend un ensemble le sous-système

d'environnement, parmi lesquels se trouves POSIX win32 et OS/2. Les sous-systèmes d'exploitation permettent aux programmes écrits pour ces différents systèmes d'exploitation de fonctionner sous Windows 2000 Server sans recompilation particulière. Les sous système d'exploitation d'environnement win32 fournit les E/S d'écran et de clavier ainsi que plusieurs routines d'affichage et des bibliothèques de Windows.

Si une application client requiert l'accès au matériel, elle passe le contrôle au noyau, par l'intermédiaires de l'exécutif Windows 2000 ; la demande est alors interprétée et exécutée.

Entre l'exécutif est le plates-formes matérielle, la couche d'abstraction du matériel (HAL) fait office de médiateur. HAL refuse aux applications l'accès direct aux périphériques. Les pilotes, programmes chargés d'interpréter les commandes des applications qui son dépendants du matériel, sont contrôler par l'exécutif, il ne sont pas directement accessibles en mode utilisateur.

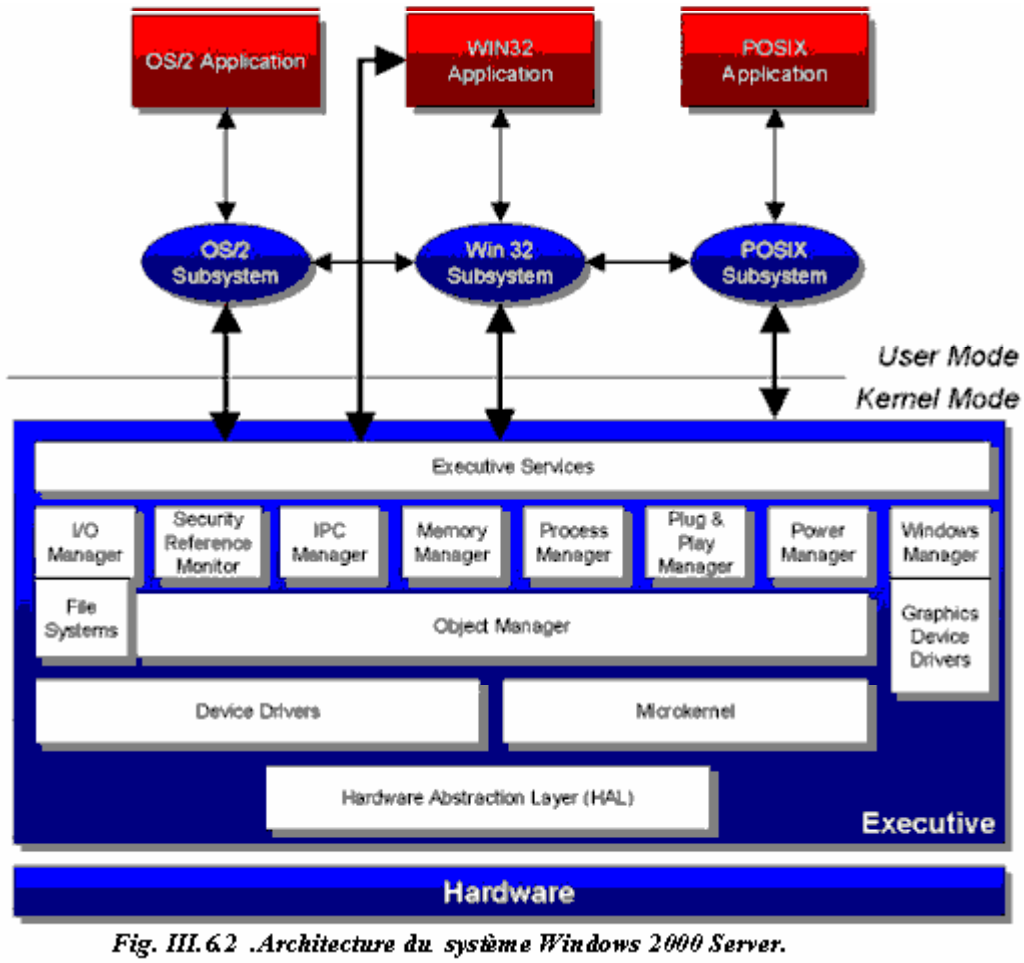


Fig. III.6.2 .Architecture du système Windows 2000 Server.

Fig.III.6.2 : Architecture du système windows 2000 server.

III. 7 L'architecture du réseau de Windows 2000 server.

III.7.1 La notion de domaine Windows 2000.

Domaine: Groupe de machines gérées sous Windows 2000 et Active Directory, reliées en réseau et pouvant être administrées comme une machine unique du point de vue des comptes d'utilisateur et de la politique de sécurité associée.

Le rôle principal d'un serveur Windows 2000 et de servir les utilisateur. La manières dont il remplit cette mission dépend de son mode de fonctionnement (Serveur autonome, serveur membre ou contrôleur domaine)

III.7.2 Le serveur autonome.

Un serveur Windows 2000 Server ne participant à un domaine est considéré comme serveur autonome. Il dispose sa propre base de donnés indépendant de nom d'utilisateur et de mot de passe.

III.7.3 Le serveur membres.

Un serveur Windows 2000 Server participant à un domaine est un serveur membre. Il authentifie tout utilisateur demandent une ressource qu'il héberge en se fiant à la base de données du domaine.

III.7.4 Les contrôleurs de domaines.

Ils forment la charpente d'un réseau, hébergent les comptes d'utilisateurs Active directory et prennent en charge la structuration et la gestion du réseau.

Un domaine Windows 2000 comprend les ordinateurs suivants :

Contrôleur de domaine avec Windows 2000 server.

Il peut y en avoir plusieurs. Chaque contrôleur possède une copie de l'annuaire, qui est maintenue a jour périodiquement par la réplication. Lorsqu'un utilisateur se connecte à un domaine, un contrôleur de domaine interroge son annuaire pour identifier l'utilisateur, et lui ouvre une session avec ses restrictions en vigueur.

Serveur membres Windows 2000 server.

C'est un serveur non configuré en contrôleur de domaine, il ne peut pas identifier les utilisateurs, sa fonction est de fournir des ressources partagées (dossiers ou imprimantes).

Ordinateur client Windows 2000 pro :

Ces ordinateurs permettent d'accéder aux ressources du domaine, ce sont les ordinateurs des utilisateurs.

CHAPITRE IV

ADMINISTRATION ET SECURITE DU RESEAU SOUS WINDOWS 2000 SERVER.

IV.I Gestion de fichier.

IV.I.1 Le système de fichier NTFS.

Le système de fichiers NTFS (Windows NT File System) de Microsoft® Windows® 2000 permet de stocker très efficacement des données sur une partition. Ainsi, on peut accorder des autorisations d'accès sur les dossiers et les fichiers afin de contrôler le niveau d'accès aux ressources dont bénéficient les utilisateurs. Le système NTFS optimise par ailleurs l'espace disque en permettant la compression de données et la configuration de quotas de disque.
En outre, il permet de crypter des données de fichier sur le disque dur physique à l'aide du système de cryptage de fichiers (EFS, Encrypting File System). Il est essentiel de maîtriser parfaitement le système NTFS et ses fonctions pour implémenter efficacement cette fonctionnalité de Windows 2000.

a) Présentation des autorisations NTFS.

Les autorisations NTFS ne sont disponibles que sur les partitions NTFS. Pour sécuriser des fichiers et des dossiers sur des partitions NTFS, on accorde des autorisations NTFS pour chaque compte d'utilisateur ou groupe d'utilisateurs qui doit accéder à la ressource. Les utilisateurs doivent bénéficier d'une autorisation explicite pour pouvoir accéder aux ressources. Si aucune autorisation n'est accordée, le compte d'utilisateur ne peut pas accéder au fichier ou au dossier. La sécurité NTFS s'applique, que l'utilisateur accède à un dossier ou à un fichier sur l'ordinateur ou par le biais du réseau.

b) Liste de contrôle d'accès.

Le système NTFS stocke une liste de contrôle d'accès (ACL, Access Control List) associée à chaque fichier et dossier contenus dans une partition NTFS. La liste ACL contient tous les comptes d'utilisateur, groupes d'utilisateurs et ordinateurs bénéficiant de l'accès au fichier ou au dossier, ainsi que le type d'accès qui leur est accordé. Pour qu'un utilisateur puisse accéder à un fichier ou à un dossier, la liste ACL doit contenir une entrée, appelée entrée de contrôle d'accès (ACE, Access Control Entry), pour le compte d'utilisateur, le groupe d'utilisateurs ou l'ordinateur auquel l'utilisateur est associé. L'entrée doit précisément autoriser le type d'accès

demandé par l'utilisateur afin que celui-ci puisse accéder au fichier ou au dossier. Si aucune entrée ACE n'existe dans la liste ACL, Windows 2000 ne permet pas à l'utilisateur d'accéder à la ressource.

Autorisation NTFS	Possibilités offertes à l'utilisateur
Lecture	Afficher les fichiers et les sous-dossiers contenus dans le dossier ainsi que les attributs, l'appropriation et les autorisations associés au dossier.
Écriture	Créer des fichiers et des sous-dossiers dans le dossier, modifier les attributs du dossier et afficher l'appropriation et les autorisations associées au dossier.
Afficher le contenu du dossier	Afficher le nom des fichiers et des sous-dossiers contenus dans le dossier.
Lecture et exécution	Parcourir les dossiers et effectuer les opérations permises par les autorisations Lecture et Afficher le contenu du dossier.
Modifier	Supprimer le dossier et effectuer les opérations permises par les autorisations Écriture, et Lecture et exécution.
Contrôle total	Modifier les autorisations, prendre possession d'un dossier, supprimer des sous-dossiers et des fichiers et effectuer les opérations permises par toutes les autres autorisations NTFS sur les dossiers.

Tableau.IV.1.1 : listes des autorisation NTFS.

c) Le système EFS(Encrypting File System)

Le système EFS permet d'appliquer un cryptage au niveau des fichiers pour les fichiers NTFS. La technologie de cryptage EFS repose sur l'utilisation d'une clé publique, s'exécute en tant que service système intégré et permet la récupération de fichiers à l'aide d'un agent de récupération EFS désigné.

Le système EFS permet aux utilisateurs de stocker les données sur le disque dur dans un format crypté. Une fois qu'un utilisateur a crypté un fichier, celui-ci demeure crypté tant qu'il est stocké sur le disque. Les utilisateurs peuvent utiliser le système EFS pour crypter des fichiers pour garantir leur confidentialité.

Le système EFS présente les caractéristiques principales décrites ci-dessous.

- Il fonctionne en arrière-plan et est transparent pour les utilisateurs et les applications.
- Il permet uniquement à l'utilisateur autorisé d'accéder à un fichier crypté. Le système EFS décrypte automatiquement le fichier à utiliser, puis le crypte de nouveau lorsqu'il est enregistré. Les administrateurs peuvent récupérer les données cryptées par un autre utilisateur. Ainsi, les données sont accessibles si l'utilisateur qui les a cryptées n'est pas disponible ou perd sa clé privée.
- Il intègre la prise en charge de la récupération des données. L'infrastructure de sécurité de Windows 2000 Server impose la configuration de clés de récupération de données. Vous pouvez utiliser le cryptage de fichiers uniquement si au moins une clé de récupération a été configurée sur l'ordinateur local. Le système EFS génère automatiquement les clés de récupération et les enregistre dans le registre lorsqu'il est impossible d'accéder au domaine.
- Il a besoin d'au moins un agent de récupération pour récupérer les fichiers cryptés. Vous pouvez désigner plusieurs agents de récupération pour gérer votre programme de récupération EFS. Chaque agent de récupération requiert un certificat d'agent de récupération EFS.

IV.2 Administration de disques.

IV.2.1 Le système DFS(Dictributed File System).

Le service DFS fournit un point de référence unique et une arborescence logique des ressources disque, quel que soit leur remplacement physique sur un réseau Windows 2000. L’utilisation de ce service pour partager les ressources réseau sur l’ensemble du réseau présente les avantages ci-dessous.

- Il organise les ressources. DFS utilise une arborescence qui contient une racine et des liens. Un lien DFS est une partie de la hiérarchie DFS. Chaque racine DFS peut comporter plusieurs liens sous-jacents, chacun pointant vers un dossier partagé.
- Il facilite la navigation. Un utilisateur qui navigue dans une arborescence DFS n'a pas besoin de connaître le nom du serveur qui stocke physiquement les ressources pour localiser une ressource réseau spécifique. Une fois connecté à une racine DFS, l'utilisateur peut parcourir toutes les ressources qui se trouvent sous cette racine et y accéder, quel que soit l'emplacement physique du serveur sur lequel se trouvent ces ressources.
- Il simplifie l'administration. DFS simplifie l'administration de plusieurs dossiers partagés. En cas de défaillance d'un serveur, vous pouvez modifier l'emplacement du dossier partagé d'un serveur à un autre sans que les utilisateurs ne s'en aperçoivent. Les utilisateurs continuent à employer le même chemin d'accès.
- Il maintient les autorisations. Un utilisateur peut accéder aux dossiers partagés par l'intermédiaire du système DFS, à condition de disposer de l'autorisation nécessaire.

IV.2.2 Windows 2000 Server gestion de ressources.

Windows 2000 Server prend en charge les disques dynamiques aussi bien que les disques de base :

IV.2.1.1 Disque de base.

Un disque de base peut contenir jusqu'à quatre partitions principales ou trois partions principales et une partition étendue

IV.2.1.2 Disque dynamique.

Un disque dynamique peut être formé d'un seul disque physique ou d'un ensemble de disque combinés pour créer, un volume miroir, un volume agrée par bandes ou un volume RAID-5.

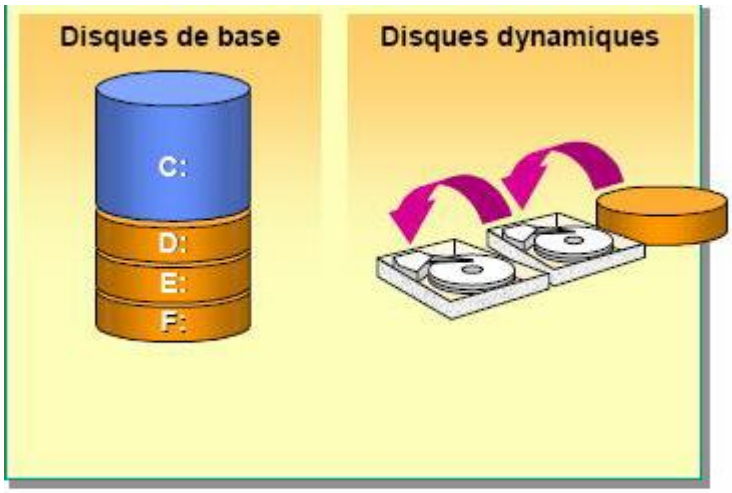


Fig.IV.2.1.2 : disques de base et disque dynamique.

IV.2.2.3 Tolérance de pannes.

La tolérance aux pannes se définit comme la capacité d'un système à trouver une compensation en cas de défaillance matérielle. Le standard en matière de tolérance aux pannes est connu sous le nom de RAID (Redundant Array of Inexpensive Disks).

Windows 2000 Server inclut la gestion logicielle de trois niveaux RAID:

Le niveau 0: Agregat par bandes de partitions,

Le niveau 1: mirroring de partitions,

Le niveau 5: Agregat par bandes avec parité.

IV.2.2.1 Mirroring de partitions.

Avec la mise en miroir, Windows 2000 Server écrira les mêmes données sur deux disques. Si l'un des deux tombe en panne, les données sont toujours disponibles sur l'autre.

IV.2.2.2 Agrégat par bandes avec parité.

Avec l'agrégat par bandes avec parité, Windows 2000 Server écrit les données sur une série de disques dynamiques (de 3 à 32).Les données ne sont pas dupliquées sur le disque, mais Windows 2000 Server enregistre des informations de parité (qu'il répartie équitablement sur les disques) qu'il peut ensuite utiliser pour régénérer les données manquantes si un disque tombe en panne.

IV.3 Gestion des comptes utilisateurs.

Un compte d'utilisateur contient les références propres à un utilisateur, et lui permet d'ouvrir une session soit sur le domaine pour accéder aux ressources réseau, soit sur un ordinateur particulier pour en utiliser les ressources. Chaque personne qui se connecte régulièrement au réseau doit disposer d'un compte d'utilisateur.

IV.3.1 Les types de comptes d'utilisateurs.

Type de compte d'utilisateur	Description
Compte d'utilisateur local	Permet à un utilisateur d'ouvrir une session sur un ordinateur particulier pour en utiliser les ressources. Les utilisateurs ne peuvent accéder aux ressources d'un autre ordinateur que s'ils disposent d'un compte distinct sur celui-ci. Ce type de compte d'utilisateur réside dans le Gestionnaire de comptes de sécurité (SAM, Security Accounts Manager) de l'ordinateur.
Compte d'utilisateur de domaine	Permet à un utilisateur d'ouvrir une session sur le domaine pour accéder aux ressources réseau. L'utilisateur peut accéder aux ressources réseau à partir de tout ordinateur du réseau, avec un même compte d'utilisateur et un même mot de passe. Ce type de compte d'utilisateur réside dans le service d'annuaire Active Directory.
Compte d'utilisateur prédéfini	Permet à un utilisateur d'effectuer des tâches administratives ou d'accéder provisoirement aux ressources réseau. Il existe deux comptes d'utilisateur prédéfinis, qu'il est impossible de supprimer : Administrateur et Invité. Les comptes d'utilisateur locaux Administrateur et Invité résident dans le Gestionnaire SAM, et les comptes d'utilisateur de domaine Administrateur et

	Invité résident dans Active Directory. Ces comptes prédéfinis sont automatiquement créés lors de l'installation de Windows 2000 et d'Active Directory.

*Tableau.IV.3.1 : les types de comtes d'utilisateur***.**

IV.3.2 Types de profils d'utilisateur.

Un profil d'utilisateur est créé à la première ouverture de session de l'utilisateur sur un ordinateur. Tous les paramètres propres à l'utilisateur sont automatiquement enregistrés dans le sous-dossier de cet utilisateur dans le dossier Documents and Settings (C:\Documents and Settings\utilisateur). Lorsque l'utilisateur ferme la session, son profil d'utilisateur est mis à jour sur l'ordinateur sur lequel il avait ouvert la session. Le profil d'utilisateur conserve donc les paramètres de bureau de l'environnement de travail de chaque utilisateur sur l'ordinateur local. Seuls les administrateurs système sont autorisés à modifier les profils d'utilisateur obligatoires. Les types de profils d'utilisateur sont présentés ci-dessous.

IV.3.2.1 Profil d'utilisateur par défaut

Ce profil est la base de tous les profils d'utilisateur. À l'origine, chaque profil d'utilisateur est une copie du profil d'utilisateur par défaut, qui est stocké sur tous les ordinateurs exécutant Windows 2000 Professionnel ou Windows 2000 Server.

IV.3.2.2 Profil d'utilisateur local

Ce profil est créé la première fois qu'un utilisateur ouvre une session sur un ordinateur, et est stocké sur l'ordinateur local. Toutes les modifications apportées au profil d'utilisateur local sont propres à l'ordinateur sur lequel les changements ont été effectués. Plusieurs profils d'utilisateur locaux peuvent exister sur un ordinateur.

IV.3.2.3 Profil d'utilisateur itinérant.

Ce profil est créé par l'administrateur système et stocké sur un serveur. Ce profil est disponible chaque fois qu'un utilisateur ouvre une session sur un ordinateur sur le réseau. Si un utilisateur apporte des modifications aux paramètres de bureau, son profil d'utilisateur est mis à jour sur le serveur lorsqu'il ferme la session.

IV.3.2.4 Profil d'utilisateur obligatoire.

Ce profil est créé par l'administrateur pour indiquer les paramètres particuliers d'un utilisateur ou d'utilisateurs, et peut être de type local ou itinérant. Un profil d'utilisateur

obligatoire ne permet pas à un utilisateur d'enregistrer des modifications apportées aux paramètres de son bureau. L'utilisateur peut modifier les paramètres du bureau de l'ordinateur sur lequel il a ouvert une session, mais ces modifications ne sont pas enregistrées lorsqu'il la ferme.

IV.4 Notion de groupes dans Windows 2000 Server.

Un groupe est un ensemble de comptes d'utilisateur. Les groupes permettent de simplifier la gestion de l'accès des utilisateurs et des ordinateurs aux ressources partagées. Ils permettent d'accorder des autorisations d'accès à plusieurs utilisateurs simultanément. Après avoir accordé l'autorisation d'accès à un groupe, vous pouvez lui ajouter des membres qui nécessitent cette autorisation.

IV.4.1 Groupes dans un groupe de travail.

Les caractéristiques des groupes dans un groupe de travail sont présentées ci-dessous.

- Ils sont créés sur des ordinateurs qui ne sont pas des contrôleurs de domaine. Cette caractéristique englobe les ordinateurs clients qui exécutent Windows 2000 Professionnel et les serveurs membres qui exécutent Windows 2000 Server ou Windows 2000 Advanced Server.
- Ils résident dans le Gestionnaire de comptes de sécurité (SAM, Security Accounts Manager), qui est la base de données de comptes de sécurité locale de l'ordinateur.
- Ils permettent d'accorder des autorisations sur les ressources et des droits pour des tâches système uniquement sur l'ordinateur sur lequel ils sont créés.

IV.4.2 Groupes dans un domaine.

Les caractéristiques des groupes dans un domaine sont présentés ci-dessous.

- Ils sont créés uniquement sur des contrôleurs de domaine.
- Ils résident dans le service d'annuaire Active Directory..
- Ils permettent d'accorder des autorisations sur des ressources et des droits pour des tâches système sur n'importe quel ordinateur du domaine.

Dans un domaine, Active Directory prend en charge différents types de groupes . Comme ces groupes sont stockés dans Active Directory, on peut les utiliser sur n'importe quel ordinateur du réseau. Le type de groupe détermine le type de tâche que on gére avec le groupe. Chaque type de groupe de domaine est pourvu d'un attribut étendue qui identifie dans quelle mesure le groupe s'applique au réseau.

IV.4.2.1 Types de groupes.

Il existe deux types de groupes dans Active Directory qui sont décrits ci-après.

a) Groupes de sécurité.

On utilise les groupes de sécurité à des fins de sécurité, par exemple pour octroyer des autorisations pour accéder aux ressources, pour envoyer des messages électroniques à plusieurs utilisateurs. L'envoi d'un message électronique à un groupe distribue le message à tous les membres du groupe. Les groupes de sécurité partagent donc les fonctionnalités des groupes de distribution.

b) Groupes de distribution.

Les applications utilisent des groupes de distribution comme listes pour des fonctions non liées à la sécurité, telles que l'envoi de messages électroniques à des groupes d'utilisateurs. On ne peut pas accorder d'autorisations aux groupes de sécurité. Même si les groupes de sécurité possèdent toutes les fonctionnalités des groupes de distribution, ceux-ci sont néanmoins requis, car ce sont les seuls que certaines applications peuvent lire.

IV.4.2.2 Étendues des groupes.

L'étendue d'un groupe détermine le champ d'utilisation du groupe dans les domaines.
L'étendue d'un groupe affecte les membres du groupe et l'imbrication des groupes.
L'imbrication correspond à l'ajout d'un groupe à un autre en tant que membre. Windows 2000 présente les trois étendues de groupes décrites ci-dessous.

a) Étendue de groupe globale.

On utilise cette étendue de groupe pour organiser les utilisateurs qui partagent les mêmes besoins d'accès au réseau. On peut utiliser un groupe global pour accorder des autorisations d'accès aux ressources situées dans un domaine quelconque.

- Les groupes globaux ont des adhésions limitées. On ajoute des comptes d'utilisateur et des groupes globaux uniquement à partir du domaine dans lequel est créé le groupe global.
- Les groupes globaux peuvent être imbriqués dans d'autres groupes. Cette fonction permet d'ajouter un groupe global à un autre du même domaine ou à des groupes universels et des groupes de domaine local appartenant à d'autres domaines.

b) Étendue de groupe de domaine local.

On utilise cette étendue pour accorder des autorisations sur des ressources de domaine situées dans le même domaine que celui dans lequel vous avez créé le groupe de domaine local.

La ressource peut résider ailleurs que sur un contrôleur de domaine.

- Les groupes de domaine local ont une adhésion illimitée. On ajoute des comptes d'utilisateur, des groupes universels et des groupes globaux d'un domaine quelconque.

- Les groupes de domaine local ne peuvent pas être imbriqués dans d'autres groupes. En d'autres termes, on ne peut ajouter un groupe de domaine local à un groupe, même si ce dernier appartient au même domaine.

c) Étendue de groupe universelle.

On accorde des autorisations sur les ressources connexes de plusieurs domaines. On utilise un groupe universel pour accorder des autorisations d'accès sur les ressources situées dans tout domaine.

- Les groupes universels ont une adhésion illimitée. Tous les groupes et comptes d'utilisateur de domaine peuvent être membres.
- Les groupes universels peuvent être imbriqués dans d'autres groupes de domaine. Cette fonctionnalité vous permet d'ajouter un groupe universel à des groupes de domaine local ou universels de tout domaine.

Les groupes de sécurité pourvus d'une étendue universelle ne sont disponibles que si le domaine est en mode natif. Le mode natif est appliqué lorsque tous les contrôleurs de domaine exécutent Windows 2000.

IV.4.3 Groupes intégrés et prédéfinis d'un domaine.

Les groupes prédéfinis pourvus d'une étendue globale sont situés dans le dossier Users. Les groupes intégrés pourvus d'une étendue de domaine local sont situés dans le dossier Builtin. Les groupes de domaine par défaut de Windows 2000 sont répertoriés ci-dessous.

a) Groupes de domaine local intégrés.

Ces groupes procurent aux utilisateurs des droits et autorisations prédéfinis leur permettant de réaliser des tâches sur des contrôleurs de domaine et dans Active Directory. Les groupes de domaine local intégrés sont uniquement situés sur des contrôleurs de domaine. On ne peut pas supprimer ces groupes.

b) Identités spéciales.

Ces groupes, également connus sous le nom de groupes spéciaux, permettent d'organiser automatiquement les utilisateurs pour l'utilisation du système. Les administrateurs ne leur affectent pas d'utilisateurs. Les utilisateurs sont membres par défaut ou en deviennent membres au cours d'une activité réseau. Les groupes système se trouvent sur tous les ordinateurs exécutant Windows 2000. Par exemple, lorsque des utilisateurs se connectent à un dossier partagé sur un ordinateur distant, ils deviennent membres du groupe Réseau. Les

groupes spéciaux ne sont pas visibles dans la console Utilisateurs et ordinateurs Active Directory.

c)Groupes globaux prédéfinis.

Ces groupes permettent aux administrateurs de contrôler facilement tous les utilisateurs appartenant à un domaine. Les groupes globaux prédéfinis sont uniquement situés sur des contrôleurs de domaine. Ces groupes résident dans le dossier Users de la console Utilisateurs et ordinateurs Active Directory.

IV.5 Audit des accès aux ressources système.

Windows 2000 permet de suivre les activités d'un utilisateur et d'un système d'exploitation sur un ordinateur. Pour être en mesure de détecter toute tentative de manipulation frauduleuse des données figurant sur le réseau par un intrus, on doit comprendre les procédures d'implémentation d'un audit et de contrôle des événements système.

Présentation de l'audit.

Dans Windows 2000, un audit désigne le suivi des activités d'un utilisateur et d'un système d'exploitation (appelées événements) sur un ordinateur. Lorsqu'un événement audité a lieu, Windows 2000 écrit l'enregistrement correspondant dans le journal de sécurité.

Stratégie d'audit.

Une stratégie d'audit définit les types d'événements de sécurité que Windows 2000 enregistre dans le journal de sécurité sur chaque ordinateur. Lorsqu'un événement a lieu sur un ordinateur, Windows 2000 l'écrit dans le journal de sécurité de cet ordinateur.
Définissez une stratégie d'audit pour un ordinateur afin d'effectuer les tâches suivantes :

- suivre le succès et l'échec des événements, par exemple les tentatives d'ouverture de session, les tentatives de lecture d'un fichier particulier par un utilisateur donné, les modifications apportées à un compte d'utilisateur ou aux membres d'un groupe, ou encore aux paramètres de sécurité ;
- réduire le risque d'utilisation non autorisée des ressources ;
- gérer l'enregistrement des activités des utilisateurs et des administrateurs.

IV.6 Les utilitaires de Windows 2000 Server.

Un administrateur doit surveiller les ressources système pour évaluer la charge de travail des ordinateurs, observer les modifications et les tendances liées à l'utilisation des ressources, tester les changements de configuration et recenser les problèmes.

IV.6.1 Présentation des journaux d’événements.

Les journaux d’événements permettent de surveiller les informations relatives au matériel, aux logiciels, à la sécurité et aux problèmes liés au système. On affiche ces journaux pour détecter les activités et les événements qui ont besoin d’être surveillés. Les journaux peuvent également être utilisés pour obtenir un historique des événements.

CHAPITRE V

L'INTRANET DANS UN RESEAU SOUS WINDOWS 2000 SERVER.

V.1 L'Intranet.

V.1.1 Définition :

Un Intranet est un ensemble de services Internet (par exemple un serveur web) internes à un réseau local. Il consiste à utiliser les standards client-serveur de l'Internet (en utilisant les protocoles TCP/IP), dont l'utilisation de navigateurs Internet (client basé sur le protocoles HTTP) et des serveurs web (protocole HTTP), pour réaliser un système d'information interne à une organisation ou une entreprise.

V.1.2 L'architecture Intranet.

Un intranet est généralement basé sur une architecture à trois niveaux composée:

- de clients (navigateur internet généralement) ;
- d'un ou plusieurs serveurs d'application (middleware): un serveur web permettant d'interpréter des scripts **CGI**, **PHP**, ASP ou autres, et les traduire en requêtes SQL afin d'interroger une base de données ;
- d'un serveur de **bases de données**.

De cette façon les machines clientes gèrent l'interface graphique, alors que les différents serveurs manipulent les données. Le réseau sert à véhiculer les requêtes et les réponses entre clients et serveurs.

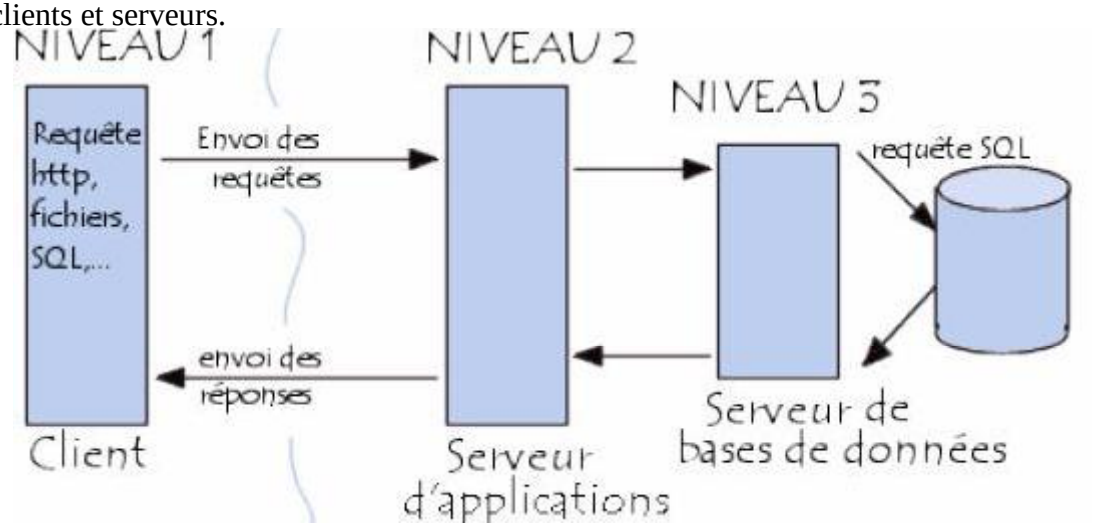


Fig.V.1.1: Schémas d'un architecture Intranet.

V.2 L'opportunité d'un Intranet au niveau d'une entreprise.

L'intranet est techniquement une forme de client-serveur qui s'appuie sur les protocoles standards d'internet.

Sur le plan organisationnel, avoir mis en place un intranet simplifie l'installation et l'administration des applications du système d'information de l'entreprise.

Un intranet facilite les projets de type collaboration de groupe, la publication de documents dynamiques, l'accès aux systèmes transactionnels. La mise en place d'un Intranet permet à chacun de devenir acteur par la mise en ligne de documents intéressant l'ensemble des collaborateurs de l'entreprise ou du service. La publication d'information sur l'intranet peut être à la limite très simple grâce aux fonction de publications au format web des logiciels que chacun a sur son micro (traitement de texte, tableur). Au delà de la vague médiatique d'Internet, un Intranet permet d'envisager des applications d'un autre type, tournées vers la circulation d'information et la communication directe entre les personnes et avec les directions.

Des documents de tous types (textes, images, vidéos, sons, ...) peuvent être mis à disposition sur un Intranet. Ainsi, un Intranet peut réaliser une fonction de *groupware* très intéressante, c'est-à-dire permettre un travail coopératif. Voici quelques unes des fonctions qu'un intranet peut réaliser:

- Mise à disposition d'informations sur l'entreprise (panneau d'affichage)
- Mise à disposition de documents techniques
- Moteur de recherche de documentations
- Un échange de données entre collaborateurs
- Annuaire du personnel
- Gestion de projets, aide à la décision, agenda, ingénierie assistée par ordinateur
- Messagerie électronique
- Forums de discussion, listes de diffusions, chat en direct
- Visioconférence
- Portail vers Internet

De cette façon un Intranet favorise la communication au sein de l'entreprise et réduise les erreurs dues à la mauvaise circulation d'une information. Pour éviter les conflits de version, l'information disponible sur l'intranet doit être mise à jour.

V.3 Avantages de l’Intranet.

V.3.1 Avantages.

Un intranet permet de constituer un système d'information à faible coût (concrètement le coût d'un intranet peut très bien se réduire au coût du matériel, de son entretien et de sa mise à jour, avec des postes clients fonctionnant avec des navigateurs gratuits, un serveur fonctionnant sous Windows 2000 Server avec le serveur web Apache et le serveur de bases de données MySQL).

D'autre part, étant donné la nature "universelle" des moyens mis en jeu, n'importe quel type de machine peut être connectée au réseau local, donc à l'intranet. On a :

- Partage : le pouvoir ne passe plus par la maîtrise de l'information
- Temps réel : disponibilité instantanée des informations
- Supprimer la paperasse
- Gain de temps : recherches facilitées
- Gérer les connaissances : pérennité, accessibilité, meilleure exploitation.

V.3.2 Les risques et les solutions correspondantes pour un Intranet.

L'intranet a pour vocation de diffuser des documents internes, qui peuvent être confidentiels. Une gestion adaptée des droits d'accès à l'information doit absolument être mise en place, pour garantir la confidentialité et l'intégrité des informations. Contrairement à internet où la sécurité est médiocre, un intranet bien conçu offre une très bonne sécurisation :

- Gestion des droits d'accès aux données de manière très sécurisée,
- gestion fine des droits : documents accessibles uniquement à certaines personnes suivant leur fonction, leur statut, ...

L’ouverture de l’Intranet vers l’Internet constitue à des risques d’intrusions de l’extérieur, parmi lesquelles les piratages, les virus et les vols de fichiers. L’installation et la mise à jour régulière d’un antivirus s’avère nécessaire .on doit aussi penser à la mise en place d’un pare-feu (*firewall*). Un pare-feu renforce la protection d’un serveur en bloquant l''accès de ce dernier aux utilisateurs non autorisés, que ce soit via un réseau ou Internet.

V.4 Le réseau Intranet sous Windows 2000 server.

V.1.1 Le serveur Web IIS (Internet Information Server).

Les Services Internet (IIS) pour Microsoft Windows 2000 mettent la puissance d'Internet à la portée de Windows. IIS permet de partager fichiers et imprimantes et de créer des applications permettant de publier en toute sécurité les informations qui amélioreront le fonctionnement d'une société. IIS constitue une base sure pour établir et déployer une solution de commerce électronique. IIS facilite également le déploiement d'applications critiques sur Internet.

Windows 2000 avec IIS permet d'effectuer les opérations suivantes :

- Configurer un serveur Web personnel.
- Partager des informations au sein d'une équipe.
- Accéder à des bases de données.
- Créer un Intranet pour une entreprise.

Il comprend les serveurs suivants:

- Web,
- FTP,
- Gopher,
- SMTP,
- NNTP,

On appelle «Web» (nom anglais «toile»), contraction de «*World Wide Web*» (d'où l'acronyme *www*), une des possibilités offertes par le réseau Internet, de naviguer entre des documents reliés par des liens hypertextes.
Le concept du Web a été mis au point au CERN (Centre Européen de Recherche Nucléaire) en 1991 par une équipe de chercheurs à laquelle appartenaient Tim-Berners LEE, le créateur du concept d'hyperlien, considéré aujourd'hui comme le père fondateur du Web.
Le principe de web repose sur l'utilisation d'hyperliens pour naviguer entre des documents (appelés «pages web») grâce à un logiciel appelé Navigateur (parfois également appelé *fureteur* ou *butineur* ou en anglais *browser*). Une page web est ainsi un simple fichier texte écrit dans un langage de description (appelé HTML), permettant de décrire la mise en page du document et d'inclure des éléments graphiques ou bien des liens vers d'autres documents à

l'aide de balises. Au-delà des liens reliant des documents formatés, le web prend tout son sens avec le protocole http permettant de lier des documents hébergés par des ordinateurs distants (appelés serveurs web, par opposition au client que représente le navigateur). Sur Internet les documents sont ainsi repérés par une adresse unique, appelée URL, permettant de localiser une ressource sur n'importe quel serveur du réseau internet.

Une URL (*Uniform Resource Locator*) est un format de nommage universel pour désigner une ressource sur Internet ou sur un Intranet.

· *Le nom du protocole* : c'est-à-dire en quelque sorte le langage utilisé pour communiquer sur le réseau. Le protocole le plus largement utilisé est le protocole HTTP (*HyperText Transfer Protocol*), le protocole permettant d'échanger des pages Web au format HTML. De nombreux autres protocoles sont toutefois utilisables (FTP,News,Mailto,Gopher,...)

· *Identifiant et mot de passe* : permet de spécifier les paramètres d'accès à un serveur sécurisé. Cette option est déconseillée car le mot de passe est visible dans l'URL

· *Le nom du serveur :* Il s'agit d'un nom de domaine de l'ordinateur hébergeant la ressource demandée. Notez qu'il est possible d'utiliser l'adresse IP du serveur, ce qui rend par contre l'URL moins lisible.

· *Le numéro de port :* il s'agit d'un numéro associé à un service permettant au serveur de savoir quel type de ressource est demandée. Le port associé par défaut au protocole est le port numéro 80. Ainsi, lorsque le service Web du serveur est associé au numéro de port 80, le numéro de port est facultatif.

· *Le chemin d'accès à la ressource :* Cette dernière partie permet au serveur de connaître l'emplacement auquel la ressource est située, c'est-à-dire de manière générale l'emplacement (répertoire) et le nom du fichier demandé Une URL a donc la structure suivante :

Une URL a donc la structure suivante :

Protocole	**Mot de passe**	**Nom du serveur**	**Port**	**Chemin**
http://	user:password@	Serveur.genieindustriel.espa.local	: 80	/w2k/

Tableau.V.4.1 : Représentation d'un URL.

V.1.2 Le nom de domaine(DNS ,Domaine Name System).

Chaque ordinateur directement connecté à Internet possède au moins une adresse IP propre. Cependant, les utilisateurs ne veulent pas travailler avec des adresses numériques du genre 194.153.205.26 mais avec des noms de machine ou des adresses plus explicites (appelées adresses FQDN) du type http://www.commentcamarche.net/.

Ainsi, un système appelé DNS (Domain Name System) est un systeme qui permet d' associer des noms en langage courant aux adresses numériques peu commode . On appelle résolution de noms de domaines (ou résolution d'adresses) la corrélation entre les adresses IP et le nom de domaine associé.

Un DNS est une base de données répartie contenant des enregistrements, appelés RR (Resource Records), concernant les noms de domaines. Le fonctionnement des serveurs de noms étant totalement transparent pour les utilisateurs. En raison du système de cache permettant au système DNS d'être réparti, les enregistrements de chaque domaine possèdent une durée de vie, appelée TTL (Time To Live, traduisez espérance de vie), permettant aux serveurs intermédiaires de connaître la date de péremption des informations et ainsi savoir s'il est nécessaire ou non de la revérifier.

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

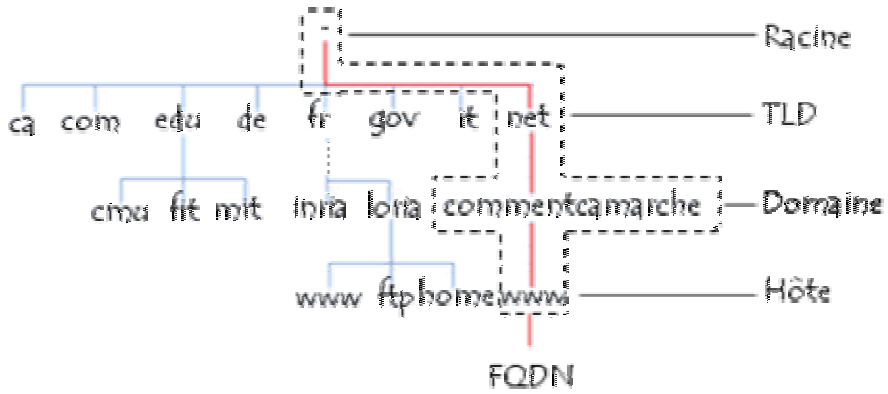


Fig.V.1.2 : la structure du système DNS.

On appelle «nom de domaine» chaque noeud de l'arbre. Chaque noeud possède une étiquette (en anglais «*label*») d'une longueur maximale de 63 caractères.

L'ensemble des noms de domaine constitue ainsi un arbre inversé où chaque noeud est séparé du suivant par un point («.»).
L'extrémité d'une branche est appelée ***hôte***, et correspond à une machine ou une entité du réseau. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré, ou le cas échéant dans le sous-domaine. Le mot «domaine» correspond formellement au suffixe d'un nom de domaine, c'est-à-dire l'ensemble des étiquettes de noeuds d'une arborescence, à l'exception de l'hôte.
Le nom absolu correspondant à l'ensemble des étiquettes des noeuds d'une arborescence, séparées par des points, et terminé par un point final, est appelé adresse FQDN (*Fully Qualified Domain Name*, soit *Nom de Domaine Totalement Qualifié*). La profondeur maximale de l'arborescence est de 127 niveaux et la longueur maximale d'un nom FQDN est de 255 caractères. L'adresse FQDN permet de repérer de façon unique une machine sur le réseau des réseaux. Ainsi ***www.commentcamarche.net.*** représente une adresse FQDN.

V.1.1.1 Les enregistrements DNS.

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

Nom de domaine	TTL	Type	Classe	RData
www.commentcamarche.net.	3600	A	IN	163.5.255.85

Tableau.V.5.1 : structure d'un nom de domaine.

Nom de domaine : le nom de domaine doit être un nom FQDN, c'est-à-dire être terminé par un point. Si le point est omis, le nom de domaine est relatif, c'est-à-dire que le nom de domaine principal suffixera le domaine saisi ;
Type : une valeur sur 16 bits spécifiant le type de ressource décrit par l'enregistrement. Le type de ressource peut être un des suivants :

- **A** : il s'agit du type de base établissant la correspondance entre un nom canonique et une adresse IP. Par ailleurs il peut exister plusieurs enregistrements A, correspondant aux différentes machines du réseau (serveurs).

- **CNAME** (*Canonical Name*) : il permet de faire correspondre un alias au nom canonique. Il est particulièrement utile pour fournir des noms alternatifs correspondant aux différents services d'une même machine.
- **HINFO** : il s'agit d'un champ uniquement descriptif permettant de décrire notamment le matériel (CPU) et le système d'exploitation (OS) d'un hôte. Il est généralement conseillé de ne pas le renseigner afin de ne pas fournir d'éléments d'informations pouvant se révéler utiles pour des pirates informatiques.
- **MX** (*Mail eXchange*) : correspond au serveur de gestion du courrier. Lorsqu'un utilisateur envoie un courrier électronique à une adresse (utilisateur@domaine), le serveur de courrier sortant interroge le serveur de nom ayant autorité sur le domaine afin d'obtenir l'enregistrement MX. Il peut exister plusieurs MX par domaine, afin de fournir une redondance en cas de panne du serveur de messagerie principal. Ainsi l'enregistrement MX permet de définir une priorité avec une valeur pouvant aller de 0 à 65 535 : www.commentcamarche.net. IN MX 10 mail.commentcamarche.net.
- **NS** : correspond au serveur de noms ayant autorité sur le domaine.
- **PTR** : un pointeur vers une autre partie de l'espace de noms de domaines.
- **SOA** (*Start Of Authority*) : le champ SOA permet de décrire le serveur de nom ayant autorité sur la zone, ainsi que l'adresse électronique du contact technique (dont le caractère « @ » est remplacé par un point).

Classe : la classe peut être soit **IN** (correspondant aux protocoles d'internet, il s'agit donc du système utilisé dans notre cas), soit **CH** (pour le système chaotique) ;
RDATA : il s'agit des données correspondant à l'enregistrement. Voici les informations attendues selon le type d'enregistrement :

- A : une adresse IP sur 32 bits ;
- CNAME : un nom de domaine ;
- MX : une valeur de priorité sur 16 bits, suivi d'un nom d'hôte ;
- NS : un nom d'hôte ;
- PTR : un nom de domaine ;
- SOA : plusieurs champs

V.1.1.2 Notion de zone.

Le système de nom de domaine (DNS, *Domain Name System*) permet de diviser un espace de noms DNS en zones. Ces zones stockent des informations

de nom relatives à un ou plusieurs domaines DNS. Pour chaque nom de domaine DNS inclus dans une zone, la zone devient la source de référence d'informations sur ce domaine.

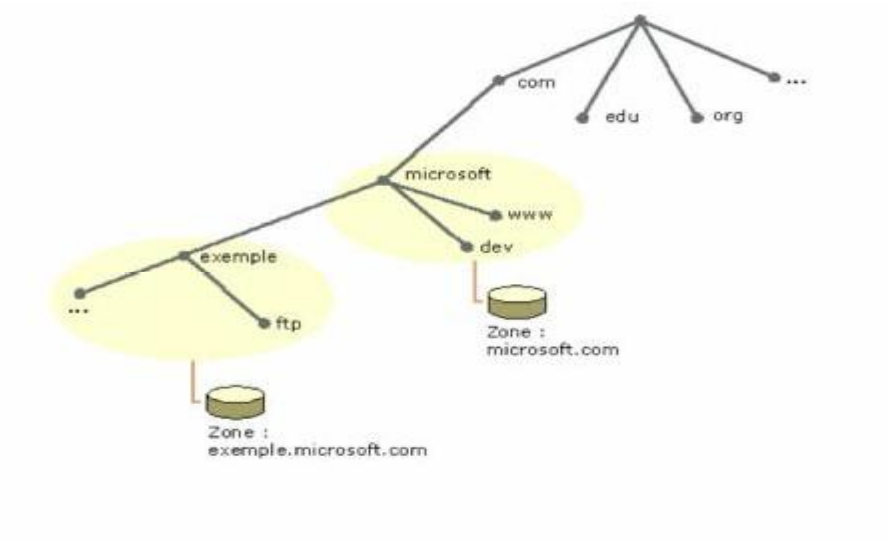


Fig.V.1.3 : Représentation d'une zone.

CHAPITRE VI

LES APPLICATIONS

VI.1 Mise en réseau des ordinateur du GI.

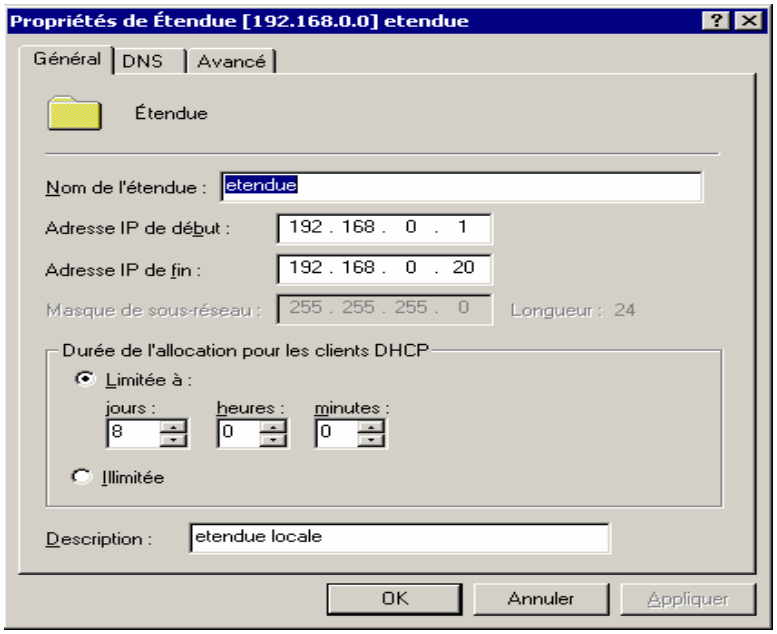
Nous allons le récapituler dans le tableau suivant.

	Adresse IP	Masque sous réseau
Poste1	192.168.0.30	255.255.255.0
Poste2	192.168.0.31	255.255.255.0
Poste3	EXEPTION	EXEPTION
Poste4	192.168.0.33	255.255.255.0
Poste5	192.168.0.34	255.255.255.0
Poste6	192.168.0.32	255.255.255.0
SERVEUR	192.168.0.1	255.255.255.0

Tableau VI.1 : les configurations IP des ordinateurs du GI

VI.2 Mise en place du serveur DHCP.

On a utilisé la console d'administration du serveur DHCP pour la mise en place de notre serveur DHCP. Le nom de notre étendue c'est « etendue » Ses propriétés sont illustrées par les figures suivantes :



Fig…VI.2.1

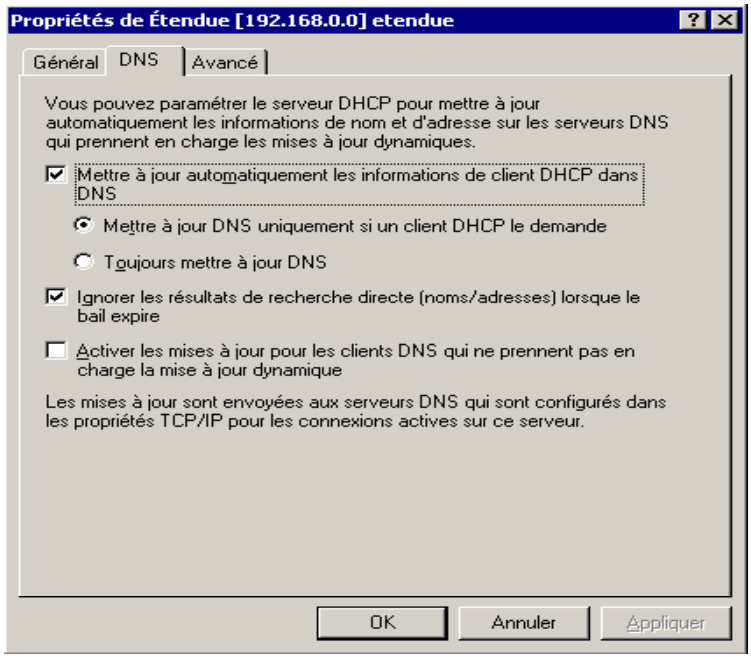
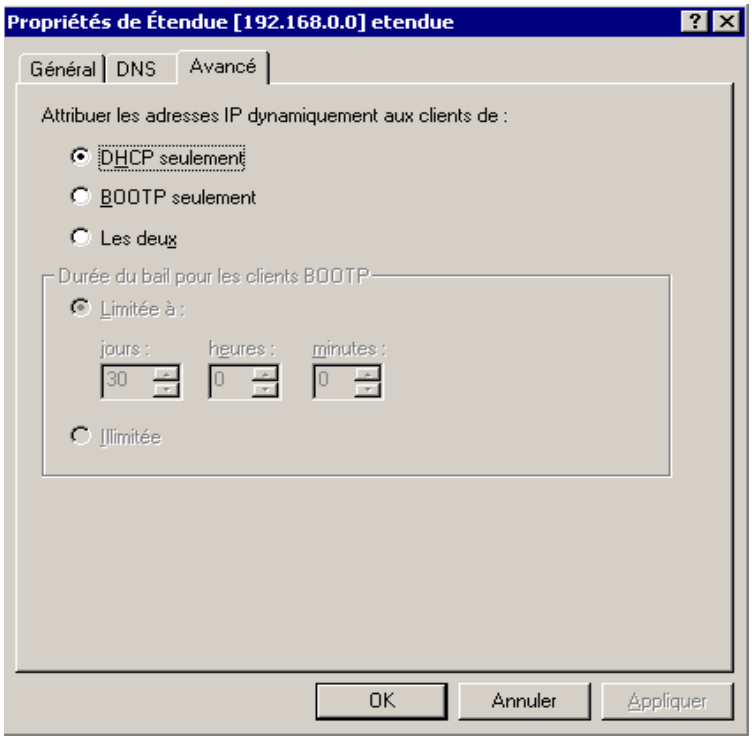
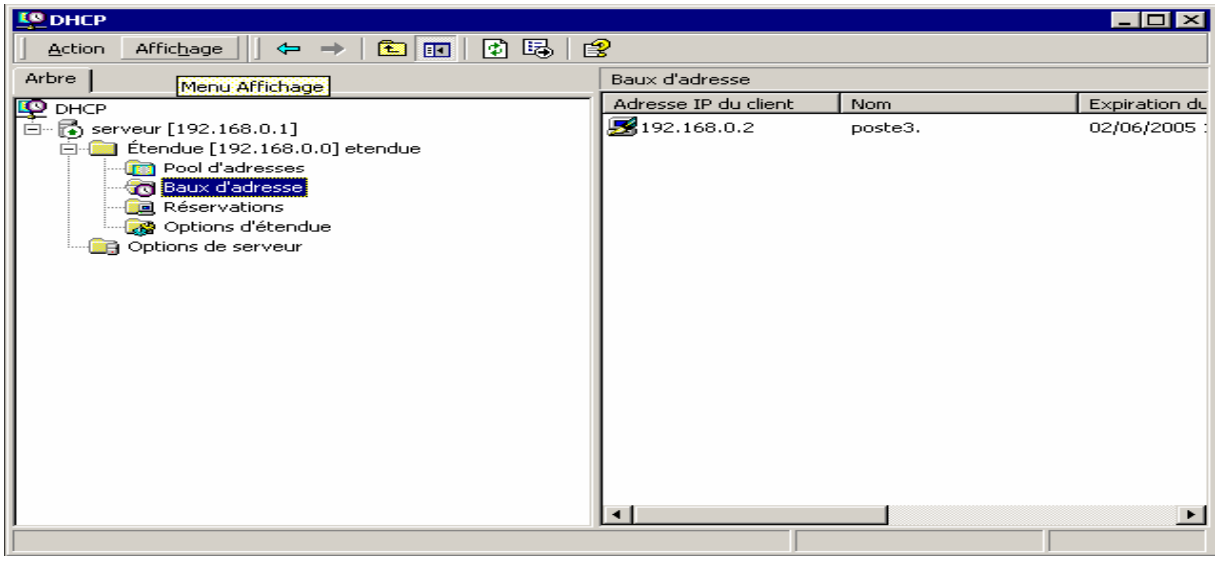


Fig.VI.1.3.





C'est seulement le poste3 que nous avons configuré pour recevoir de l'adresse dynamique. D'autre nouvel ordinateur peuvent être configuré ainsi et bénéficie de la connexion en réseau.

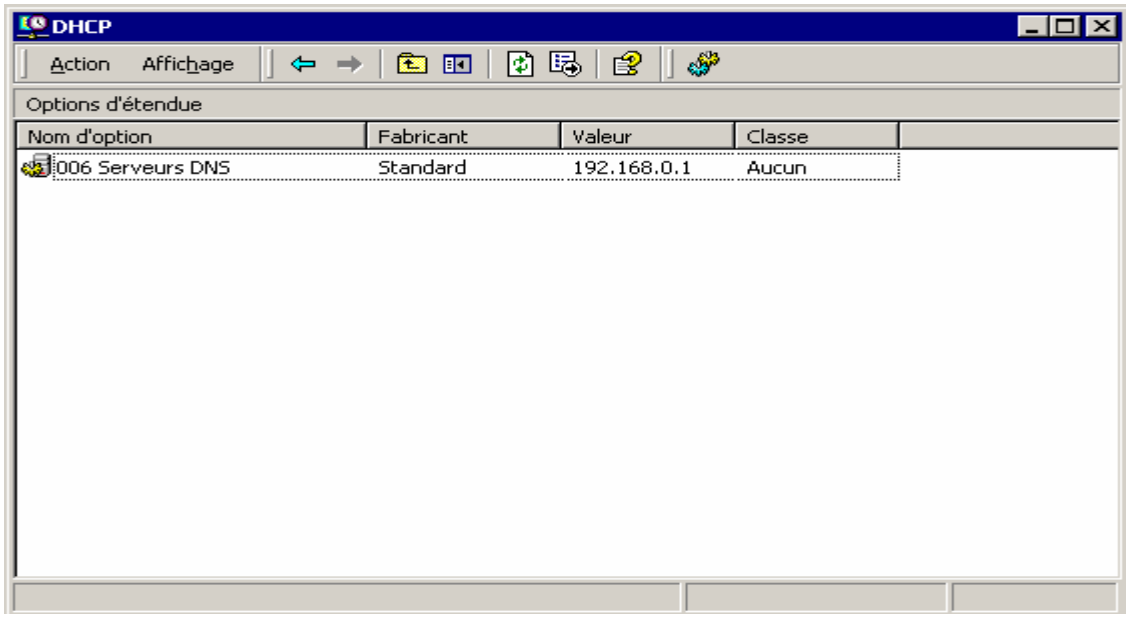


Fig.VI.2.3 : options d'étendue.

Nous n'avons pas ajouter aux options d'étendue de serveur WINS car les machines client exécute tous Windows xp ne nécessitant plus de résolution de nom NETBIOS. Pour les autres réseau WINS s'avère nécessaire.

VI.3 Mise en place du serveur DNS.

Avant d'installer un serveur DNS, il faut d'abord installer Active Directory. Au cours de l'installation on a les étapes suivantes :

- Choix du type de contrôleur: un nouveau contrôleur ou un contrôleur supplémentaire Dans notre cas, un contrôleur de domaine pour un nouveau domaine.
- Choix du type d'arborescence créée: nouvelle arborescence ou arborescence enfant Ici, une nouvelle arborescence.
- Pour une nouvelle arborescence, choix de l'intégration dans une forêt existante ou création d'une nouvelle forêt. Ici, création d'une nouvelle forêt.
- Choix du nom du domaine créé (nom complet).le notre c'est « genieindustriel.espa.local ».
- Choix du nom du domaine NetBIOS pour compatibilité avec les versions antérieures de Windows. «SERVEUR ».
- Emplacements de stockage des informations ADS .C:/WINNT/SYSVOL

C'est après une alerte relative à l'absence d'un serveur DNS pour le domaine « genieindustriel.espa.local » que commencent l'installation et la configuration du serveur DNS.

Apres un redémarrage on peut maintenant lancer le gestionnaire DNS.

VI.1.2 Les configurations de la résolution de nom.

Propriété DNS domaine.

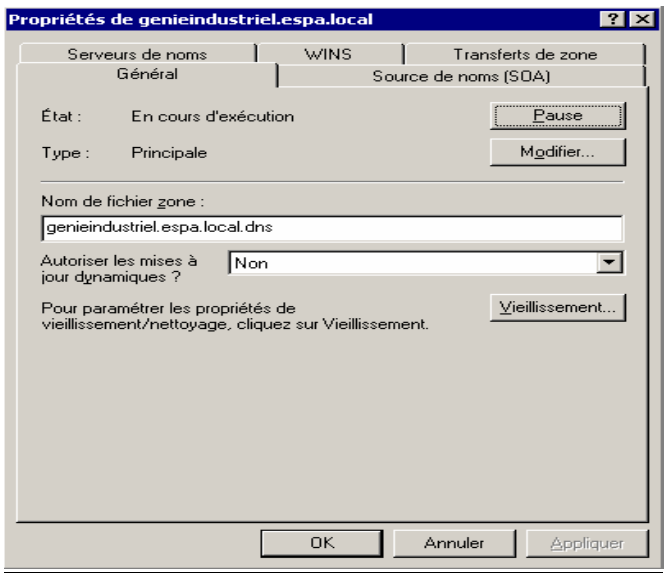


Fig.VI.2.1 : fichier du zone

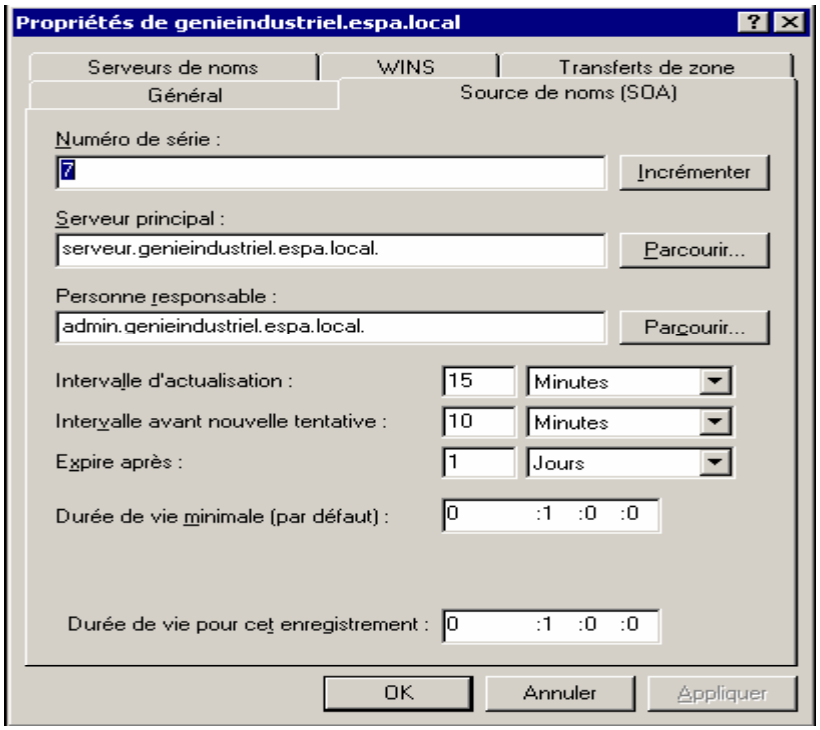


Fig.VI.2.2 : les propriétés du domaine avec l'enregistrement SOA.

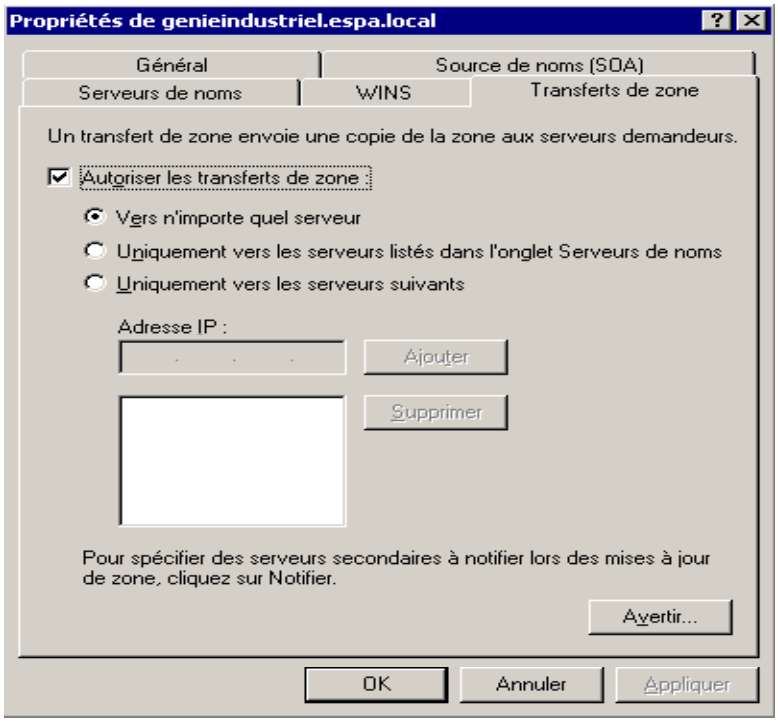


Fig.VI.2.3 : propriétés du transfert de zone

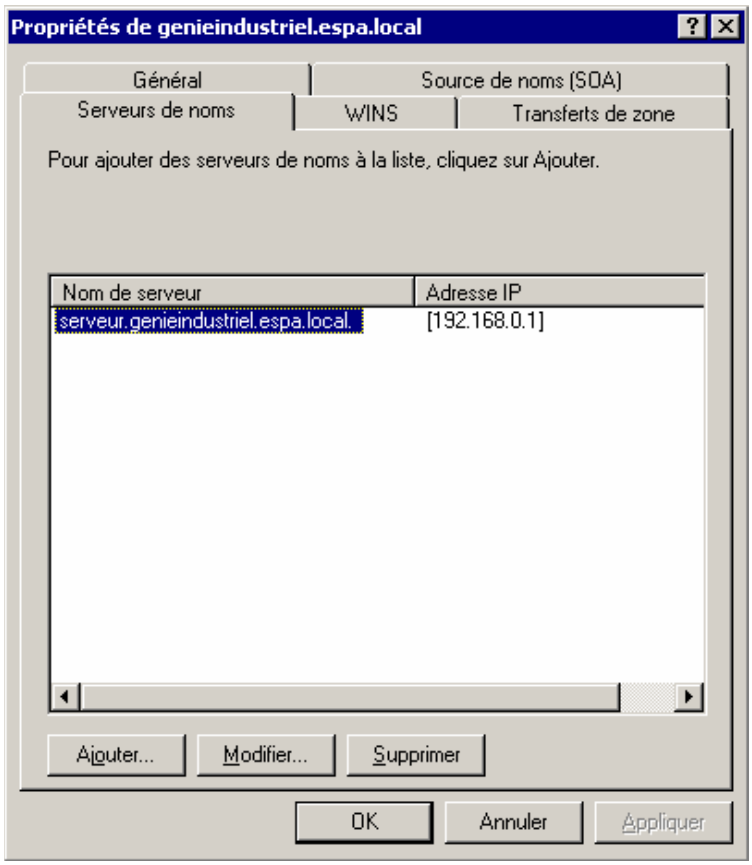


Fig.VI.2.4 : nom du serveur.

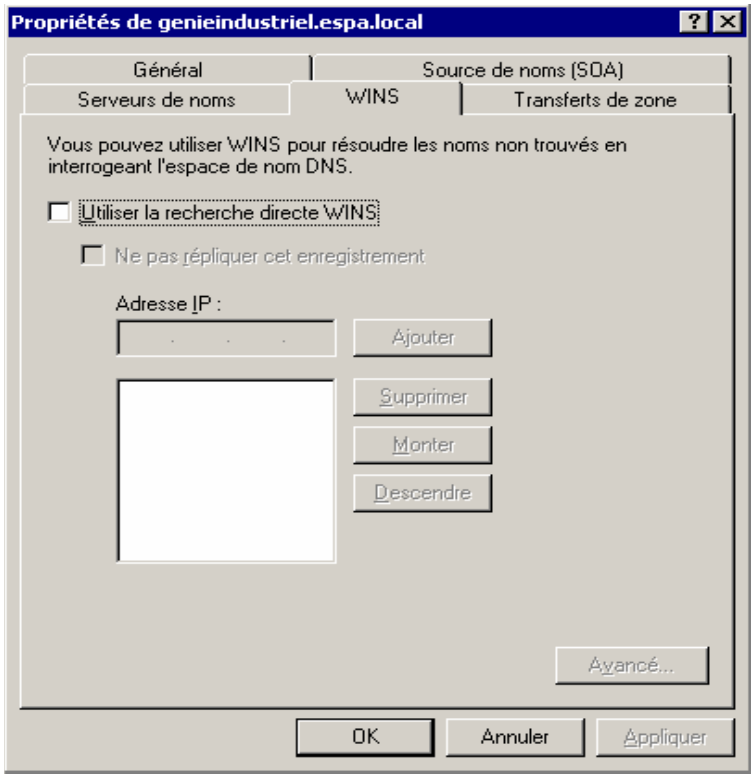


Fig.VI.2 : .WINS

Etat du DNS après configuration.

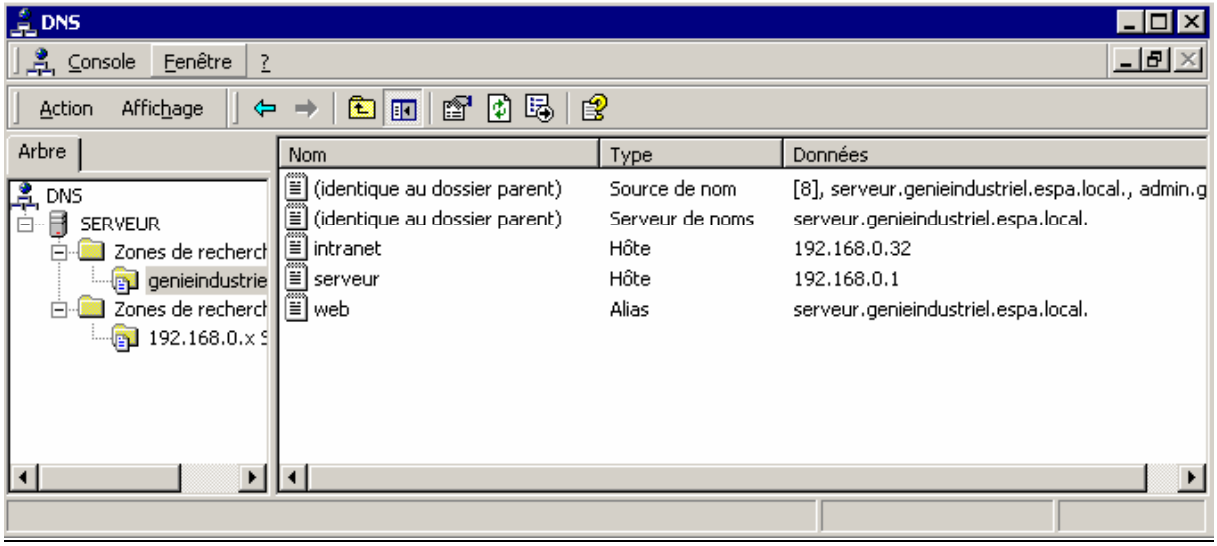


Fig.VI.2.6 : Zone de recherche directe.

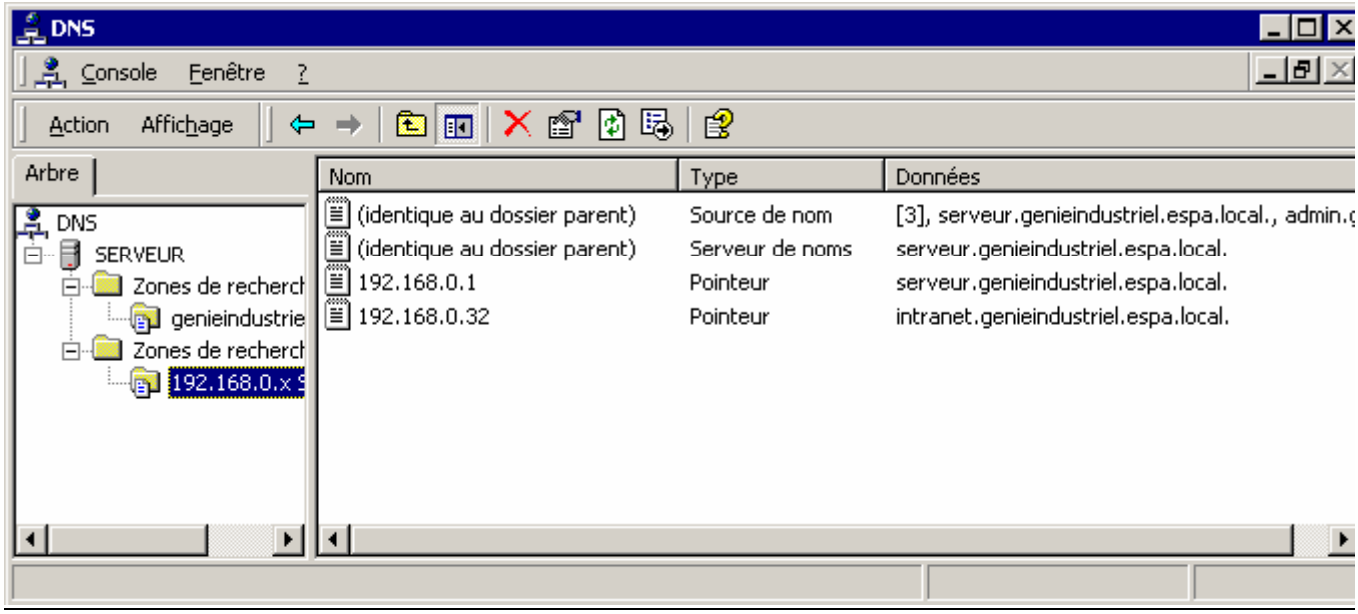


Fig.VI.2.7 : Zone de recherche inverse

Maintenant, en tapant l'adresse du serveur dans le navigateur Internet Explorer,on peut voir le page Web par défaut qui se trouve dans le répertoire du serveur. (C:/inetpub/www/).

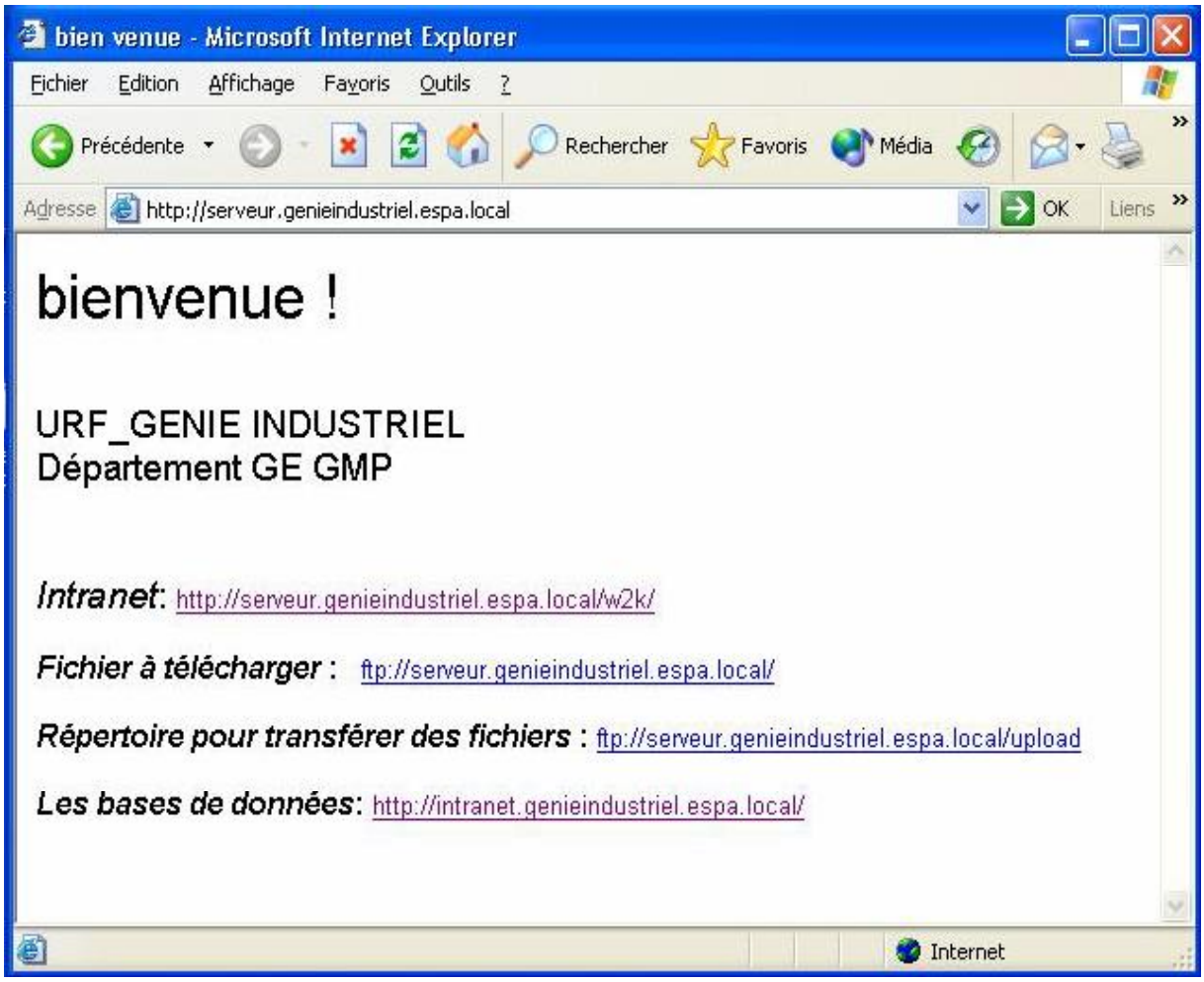


Fig.VI.2.8 : page par défaut sur le serveur web.

VI.3 Le serveur ftp.

VI.3.1Les propriétés du serveur ftp.

Nous avons crée deux répertoires de site ftp : l'une en lecture seul, c'est-à-dire que les clients ne peuvent pas supprimer ou modifier les fichier qui s'y trouve ;l'autre en lecture écriture,c'est là que les clients ont la possibilité de transférer,de modifier ou même supprimer leurs fichiers.

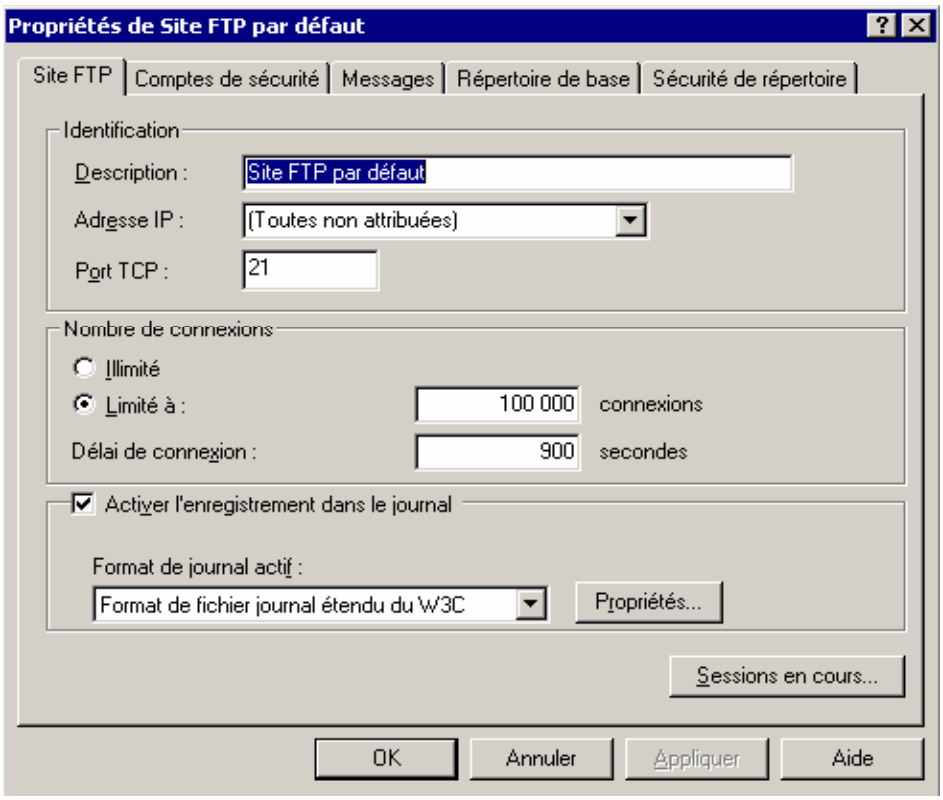


Fig.VI.3.1 : propriétés du site ftp par défaut

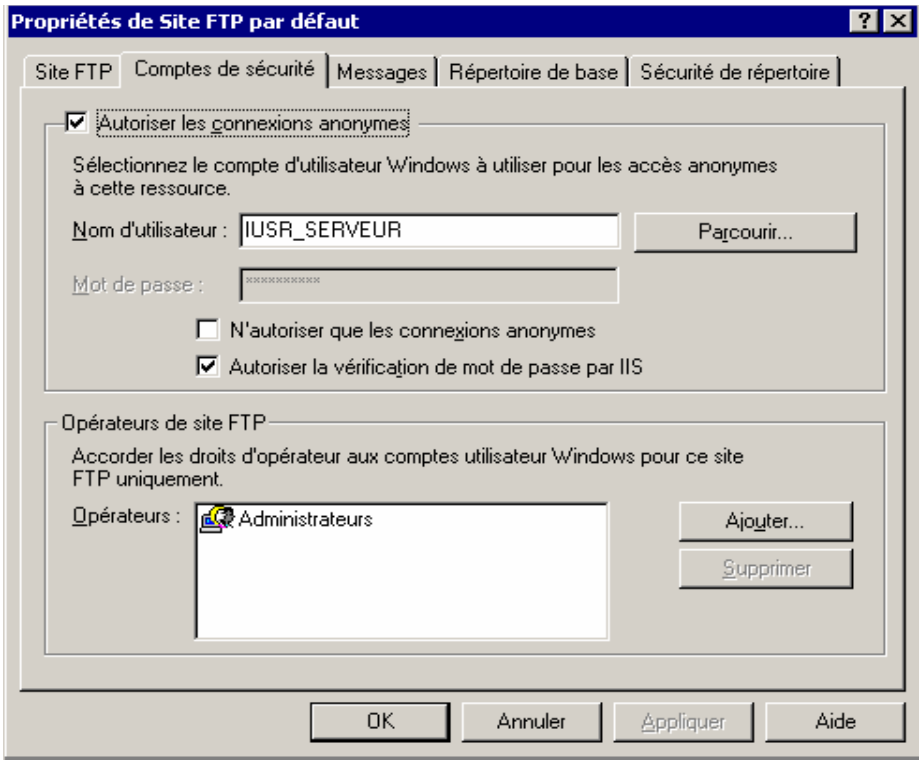
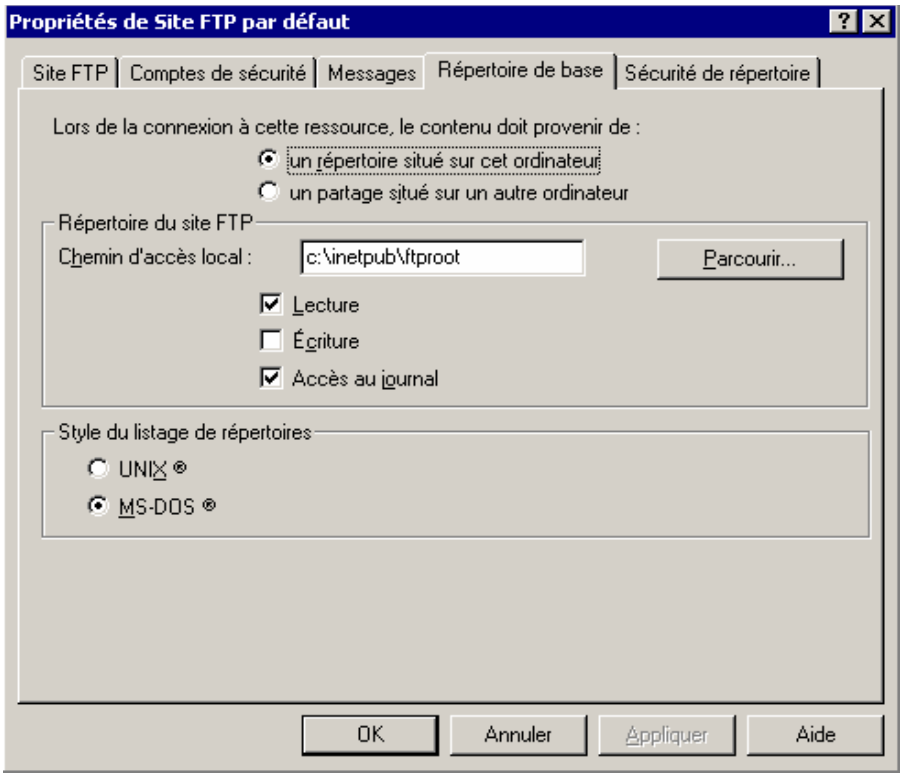


Fig.VI.3.2 : comptes de sécurité.



Fig….propriété du répertoire de base.

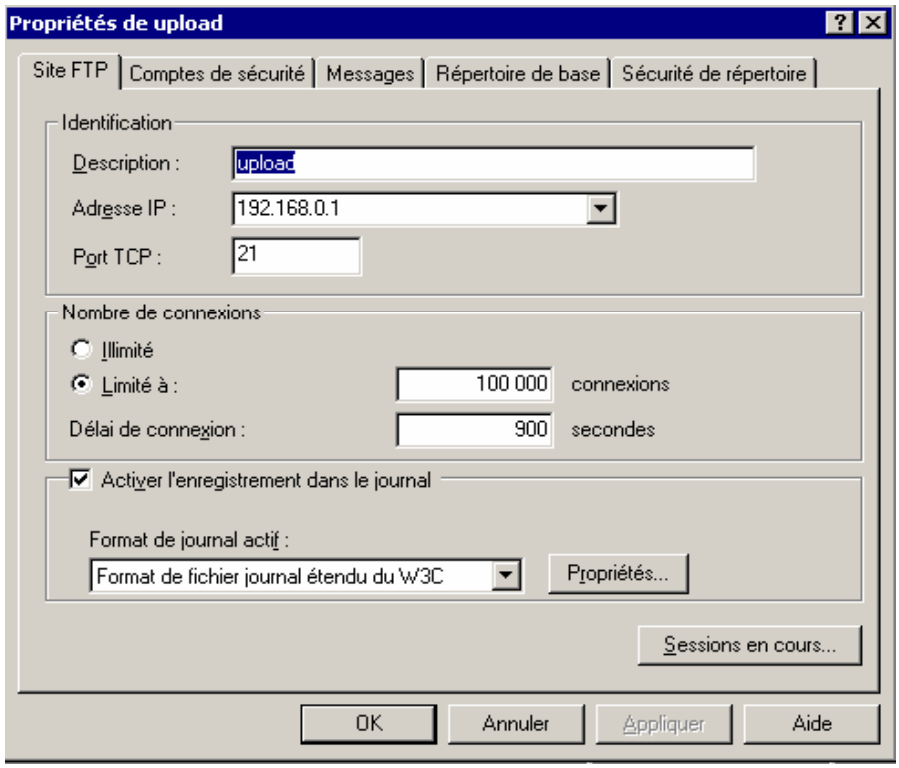


Fig.VI.3.3 : propriétés de upload.

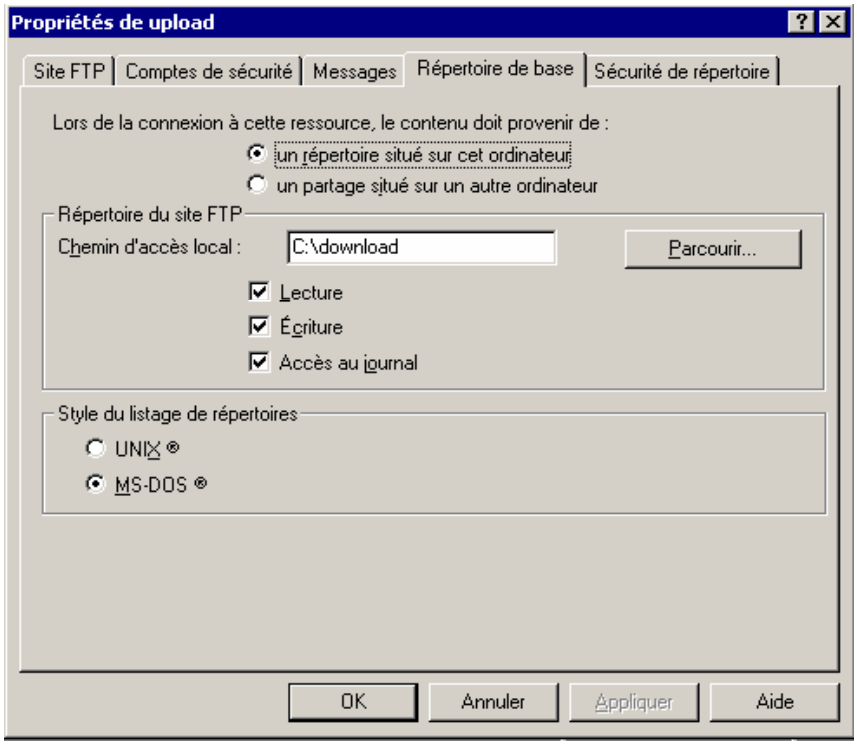
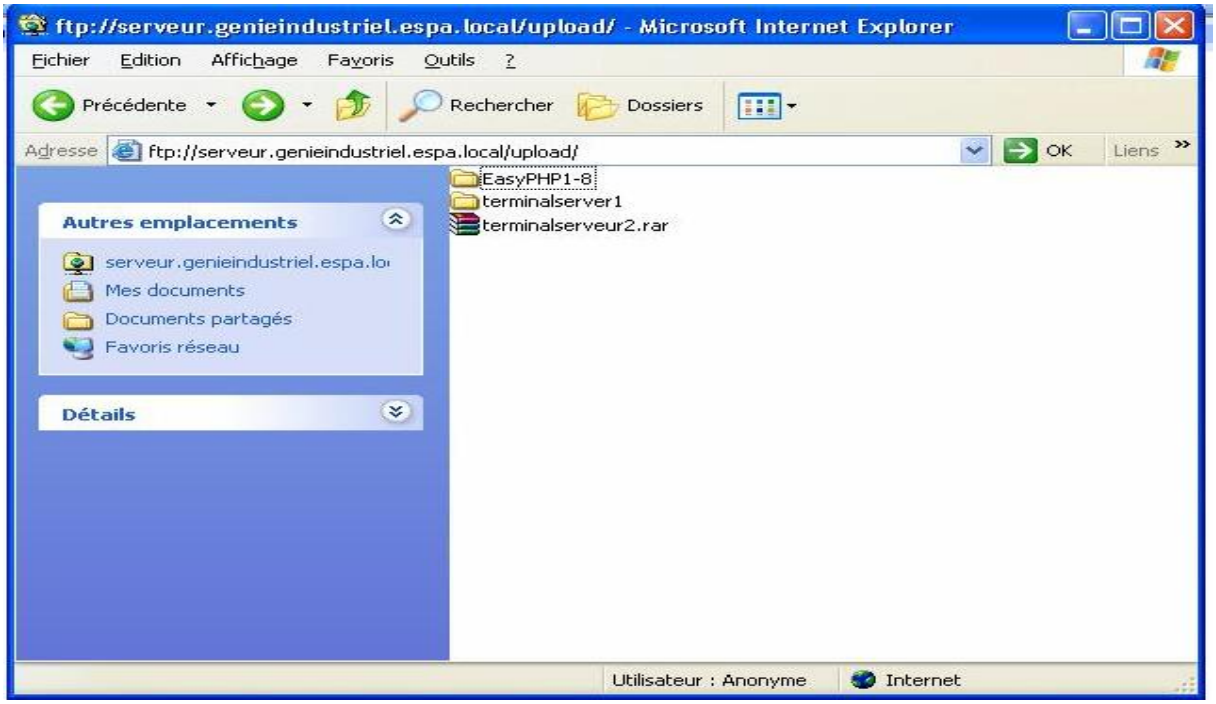


Fig.VI.3.4 : répertoire en lecture et écriture.

Transfert de fichier.

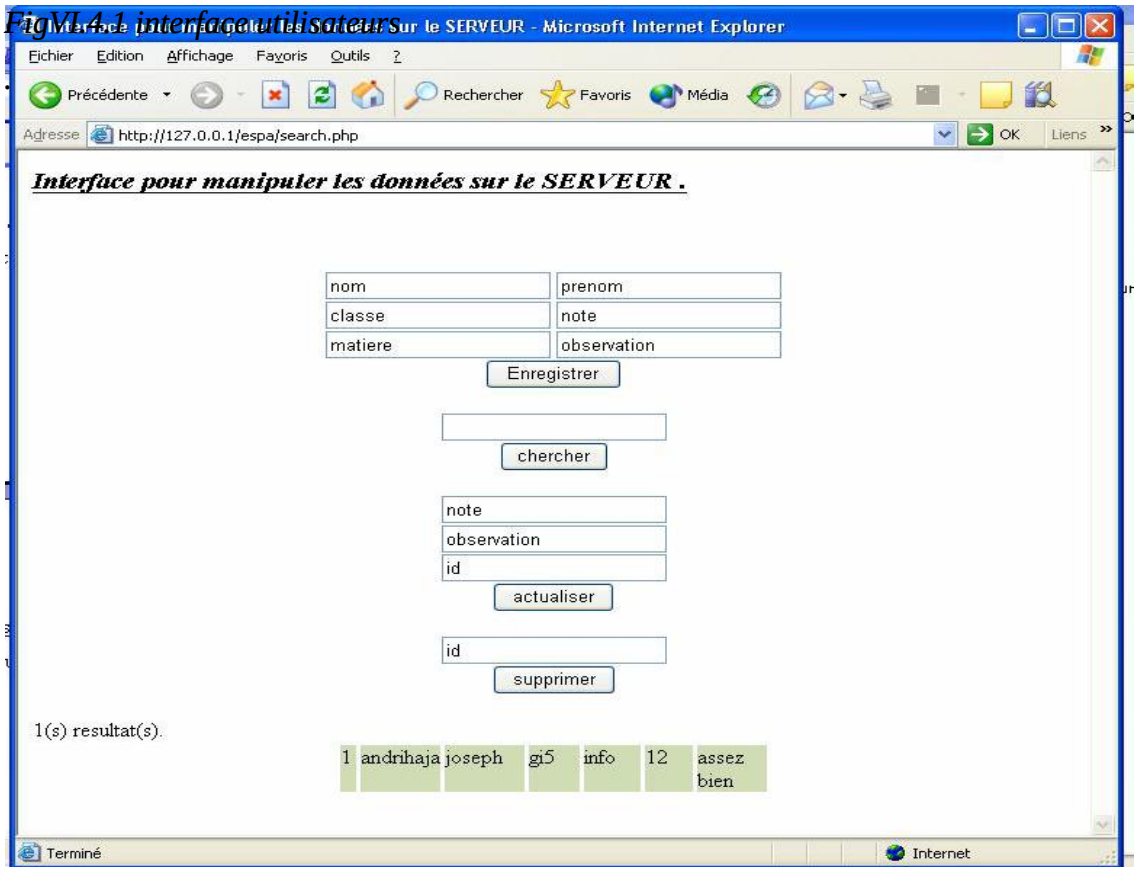
En naviguant on peut télécharger ou transférer des fichiers grâce au protocole ftp.



En double-cliquant sur un fichier ,le gestionnaire de téléchargement s'ouvre,et le client peut soit ouvrir ou enregistrer le fichier localement.

VI.4 Mise en place du serveur base de donnée avec Easyphp.

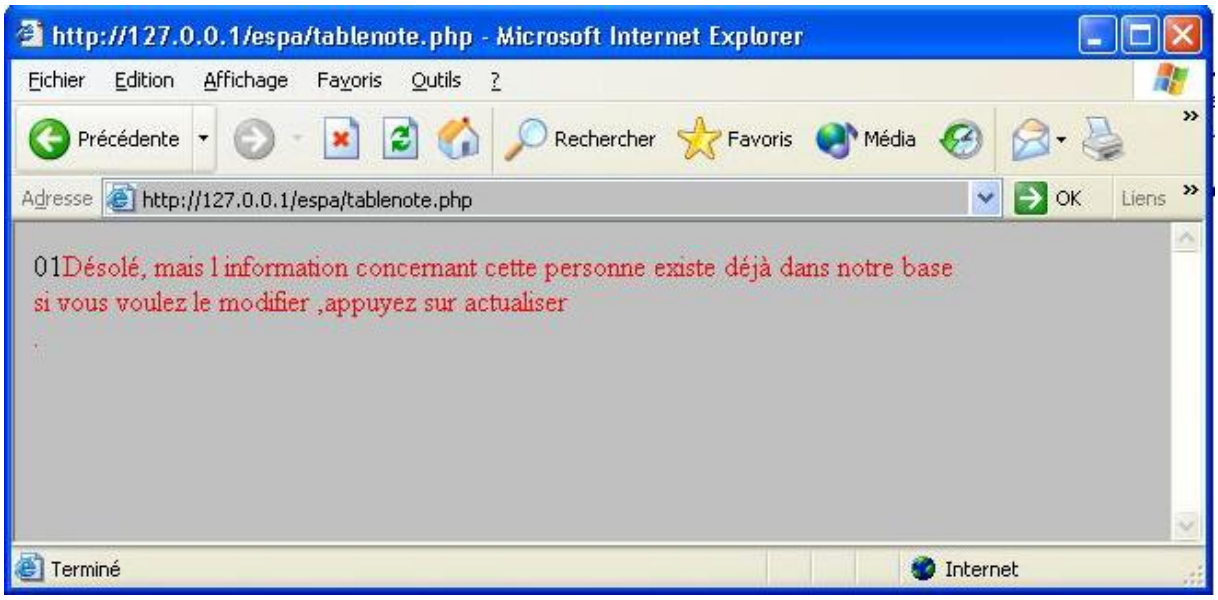
Nous avons installé Easyphp sur le poste6 pour en faire notre serveur de base de donnée. Avec php, on a créé l'interface suivante pour donner aux clients la possibilité de manipuler la base de donnée sur le serveur.



FigVI.4.1 interfaceutilisateurs

Ainsi un client peut enregistrer, chercher, modifier ou supprimer des bases de données selon ses besoins.

Nous avons conçu le programme de telle sorte que un enregistrement au même nom, prénom, classe et matière n'est pas accepté. Alors on demande si le client veut le modifier.



FigVI.4.2 : le code d'erreur.

(Voir le code source en annexe)

<u>En terme de coût.</u>

Considérons maintenant le coût de notre installation Intranet.

	Prix unitaire	nombre	somme
Ordinateur PIII	3 000 000 fmg	5	15 000 000 fmg
Ordinateur PVI	4 000 000 fmg	2	8 000 000 fmg
Câble UTP[m]	2500 fmg	1(20m)	50 000 fmg
Connecteur RJ45	2500 fmg	20	50 000 fmg
Carte réseau	75 000 fmg	5	375 000 fmg
hub	300 000 fmg	2	600 000 fmg

Les licences pour les systèmes d'exploitations (Windows 2000 Server et Windows XP) s'élèvent environ à 30 000 000 fmg.

CONCLUSION.

D’après notre étude nous avons constaté les fonctions pertinent d’un Intranet .La présence du serveur donne accès aux fonctions du Système d’Information. Cela a plusieurs applications bénéfiques au niveau d’un Entreprise dont la gestion du personnel, de la clientèle, des fournisseurs, des stocks,... EDI (échange de données informatisées). Plate-forme de travail coopératif, ingénierie simultanée, suivi de projets, gestion de connaissances. Espace de stockage de données, rubriques d'informations variées des données de l'entreprise, classées par thèmes ; notes et circulaires ; tableaux de bord ; aide à la décision ; et archives ; etc., jusqu'au journal interne Espaces d'informations volatiles, gestion et synchronisation d'agendas Annuaires.

La présence du butineur donne accès aux fonctions d'Internet :
Outils de travail collectif et de travail à distance :
Messagerie, par courrier électronique, avec ouverture sur l'extérieur
Salles de rencontres asynchrones, par forum ou liste de discussion.
Salles de rencontres synchrones, par irc.
Agenda de groupe
Téléphonie, visioconférence.
Recherche d'informations internes par un moteur.
Et accès au web !

Windows 2000 Server correspond bien à un système d’exploitation robuste et fiable pour l’administration d’un intranet.

Pourtant, il y a d’autre système qui mérite aussi l’attention .outre sa large possibilité en réseau, il a sa réputation d’être libre, c’est-à-dire gratuit. C’est le système Linux

ANNEXE 1 : Processus de démarrage Windows 2000

Processus de démarrage Windows 2000

Le processus de démarrage de Windows 2000 est similaire à celui de Windows NT4. Les fichiers mis en oeuvre restent identiques quelle que soit la version :

Etape 1 - La séquence POST - Power On Self Test

Test de la mise sous tension, de la quantité de mémoire, des composants matériels.

Chargement en mémoire de l'enregistrement d'amorçage principal (MBR).

Analyse de la table de partition.

Chargement et initialisation de Ntldr (bootstrap loader).

Etape 2 - Sélection du système d'exploitation

Ntldr fait passer le processeur du mode réel au mode mémoire linéaire 32 bits.

Ntldr démarre les pilotes de système de fichiers appropriés (FAT ou NTFS).

Ntldr lit Boot.ini et affiche les sélections.

Ntldr charge l'OS sélectionné.

Si Windows 2000 est sélectionné, Ntldr charge Ntdetect.com (sinon, Bootsect.dos).

Ntldr charge Ntoskrnl.exe, Hal.dll et la ruche "system".

Etape 3 - Chargement du noyau (Kernel)

Cette phase commence par le chargement de ntoskrnl.exe et du fichier Hal.dll. NTLDR va lire la ruche SYSTEM du registre et la mettre en mémoire puis va sélectionner la configuration matérielle et le control set qui seront utilisés pour ce démarrage. Si vous avez plus d'un profil matériel, vous pourrez faire la sélection à ce niveau. NTLDR va aussi charger tous les pilotes de périphériques dont la valeur de démarrage (dans le Registre : HKEY_LOCAL_MACHINE\SYSTEM \CurrentControlSet\Services) est 0x0.

Si vous ajoutez le switch /SOS dans le boot.ini, il vous sera possible de voir les pilotes chargés.

Etape 4 – Initialisation du noyau

Dès l'initialisation de ntoskrnl.exe, ce dernier crée le Clone control set en copiant le Control Set courant. Il va aussi créer la ruche HARDWARE dans le Registre en utilisant les informations collectées précédemment par ntdetect.com. Ntoskrnl.exe va ensuite initialiser les

pilotes de périphériques chargés précédemment, puis va scruter le registre pour les pilotes de périphériques qui ont une valeur de chargement de 0x1.

Etape 5 - Chargement des Services

Cette étape commence avec le chargement du processus Session Manager (smss.exe). Il va lancer les programmes présents dans l'entrée BootExecute du Registre ainsi que les sous-systèmes requis. Le sous-système Win32 va ensuite charger Winlogon.exe qui va lancer la LSA : Local Security Administration (Lsass.exe). La fenêtre Winlogon sera alors visible.
Le contrôleur de services (screg.exe) va ensuite scruter le Registre à la recherche de services qui ont une valeur de démarrage de 0x2 et va les charger. Les services doivent être lancés dans un certain ordre, en fonction de leurs dépendances vis à vis d'autres services.

Installation de Windows 2000 Server après Windows xp.

On peut installer win2k après winxp sur une autre partition, mais en s'installant win2k vire le boot d'xp , donc impossible de redémarrer xp .
La solution c'est de copier et collez 2 fichiers du cd de xp dans la partition d'amorçage (*C'est-à-dire la partition C:/*) du disque dur. Ce sont le fichier NTLDR et le fichier NTDETECT qui doivent se trouver dans /i386.

ANNEXE 2 : Kerberos

Kerberos V5.0 est le protocole d'authentification réseau de Windows 2000. Il succède à NT Lan Manager (NTLM). Associé à Active Directory, il rend Windows 2000 très différent de Windows NT 4.0 du point de vue de la gestion de la sécurité.
Deux points importants sont à signaler:

.L'authentification mutuelle: Cette fonctionnalité permet aux clients et serveurs, lors d'une communication d'informations, de vérifier l'authenticité de leurs identités respectives pour éviter les usurpations d'identité.

.L'approbation transitive: Si A fait confiance à B, et B fait confiance à C, alors A fait confiance à C.
-> En particulier, cette loi est vérifiée pour les approbations entre "Domaines Windows 2000".

BIBLIOGRAPHIE

[ ] ANDRIAMASITIANAHARIVONY : « Administration d'un réseau local sous WINDOWS NT 4.00 SERVER et mise en place d'un Intranet avec IIS. », mémoire, Dép. Eln. ESPA, A.U 2002

[ ] RAKOTONDRASOA Justin : « Réseau informatique. », cours 5ème Année, Dép. GE-GMP .ESPA, A.U 2004.

[ ] http://www.informatique-facile.net

[ ] http://www.zdc-fr.com/ccm/pratique/

[ ] http://www.faqxp.com/

[ ] http://www.lesproviders.com/arti/dossiers/

[ ] http://www.mines.inpl-nancy.fr/

[ ] http://www.ac-versailles.fr/etabliss/tice78/Reseau/reseau.html

[ ] http://www.dslvalley.com/

[ ] http://perso.wanadoo.fr/windows2000/resohardware.htm

[ ] http://www.evaluant.com/fr/societe/

[ ] http://www.commentcamarche.net/intranet/

[ ] http://solutions.journaldunet.com/

[ ] http://www.architectures-informatiques.com/cours/

[ ] http://www.figer.com/Publications/xpsec.htm

[ ] http://pro.winosoft.com/OutilsMajWeb.html

[ ] http://www.dicofr.com/cgi-bin/n.pl/dicofr/

[ ] http://www.01net.com/rdn?oid=191847

[ ] http://www.linux-france.org/prj/inetdoc/cours/

[ ] http://www.materiel.be/index_articles.php

[ ] http://www.cybersciences.com/Cyber/2.0/2_0.asp

[ ] http://www.oucs.ox.ac.uk/network/ethernet/win2k/index.xml

[ ] http://www.generation-nt.com/

[ ] http://www.themanualpage.org/reseau/index.php3

[ ] http://www.laboratoire-microsoft.org/

[ ] http://mi.cnrs-orleans.fr/Security

[ ] http://www.apache.org/

[ ] http://www.phpfrance.com/

[ ] http://dev.nexen.net/docs/mysql/chargement.html

[ ] http://www.phpwizard.net/projects/phpMyAdmin

LISTE DES FIGURES

TABLE DE MATIERE.

Nom : ANDRIHAJA
Prénom : Joseph
Adresse : Lot ITB 8 Ter Ambaniala Itaosy Tana 102.
Tel : 034 18 866 44 / 032 59 152 22
Titre : MISE EN PLACE D'UN RESEAU INTRANET
Nombre de pages : 61
Nombre de tableaux : 10
Nombre de figure : 31

Résumé.

Ce mémoire de fin d'étude nous a donné l'occasion d'assimiler les concepts du réseau local et d'intranet, d'embrasser le processus de fonctionnement du système d'exploitation Windows 2000 server. Il nous a aussi permis d'acquérir la connaissance du langage PHP du système de base de donnée MySQL.

Dans la première partie, on a développé le thème sur le réseau local et ses technologies.

Dans la deuxième partie, nous avons voir de plus prés l'administration d'un réseau local sous Windows 2000 Server, ses caractéristiques et les sécurités qu'il procure à un réseau. Et enfin,on a vu le principe de la mise en place d'intranet et les applications attendues

Abstract.

This memory gave us the opportunity to assimilate the concepts of the local area network and Intranet, to embrace the process of operation of the operating system Windows 2000 server. It also allowed us to acquire the knowledge of language PHP of the basic system of MySQL data.

In the first part, the topic on the local area network and his technologies is developed.

In the second part, we have to see moreover the administration of a local area network under Windows 2000 Server, its characteristics and the safety measures which it gets for a network. And finally, we saw the principle of the installation of Intranet and the awaited applications.

Rubrique: Intranet
Mot clé : Informatique, Réseau, Serveur.
Encadreur : RAKOTONDRASOA Justin