

Faculté des Sciences Exactes - Département Informatique

2^{ème} année Master Professionnel

Option : Administration et sécurité des réseaux

Mémoire de fin de cycle

En vue d'obtention d'un diplôme master professionnel en

Informatique

Thème :



**Configuration du réseau local
de l'entreprise NAFTAL Bejaia en vue de
partage des ressources informatiques via active
directory**

Présenté par :

M^{elle} Talbi berkahoum

Encadré par: M^r Albani.M

Membre de jury: M^r Touazi.D

M^r Salhi.N

Président de jury: M^r Badéche .A

Remerciements

Je tiens à remercier dieu tout puissant de m'avoir accordé santé et volanté pour accomplir ce travail.

Je tiens à remercier : tous ceux qui de près ou de loin, ont contribué

A l'élaboration de ce modeste travail.

Mes remerciements s'adressent essentiellement au personnel de l'entreprise sis djamaa

Pour sa disponibilité et orientations.

Mes remerciements aussi à mon promoteur Mr : Touazi pour son encadrement.

Je remercie également tout le personnel de l'entreprise NAFTAL ;

Mon encadreur Mr Albani sans oublier Mr Talbi qui mon setenu énormément durant la période du stage.

Je suis honoré par la présence de membres du jury d'avoir accepté ce

Travail en espérant qu'ils trouveront dans ce projet de quoi être satisfait

Et auront la gratitude de l'enrichir avec leurs critiques et corrections.

Berkahoum

Dédicace

Je dédie ce modeste travail aux êtres les plus chers de ma vie :

-A mes très chers parents qui ont attendu, et espérer ma réussite, ont toujours veillé sur moi avec beaucoup d'amour et de patience,

-A mes très chers frères et sœurs et toutes leurs familles ; sans oublier Fouzia en France et son mari massi.

-A mon très cher fiancé Anouar et toute la famille IDRI ;

- A mes collègues du travail C-E-M mixte souk-el-tenine .

-A toute ma famille : Oncles, Tantes, cousins, cousines

-A tous mes amis de l'enfance à ce jour

-A mes copines de chambre : B502

A tous ceux qui me connaissent de près ou de loin

Toutes ces valeurs m'ont donné confiance et espoir pour continuer les études et pour préparer ce travail.

Berkahoum

SOMMAIRE

Sommaire.....	i
Liste des figures.....	ii
Liste des tableaux.....	iii
Introduction générale	v
<u>Chapitre I</u> : notions générales sur les réseaux.....	
I.1.introduction	1
I.2 .définition d'un réseau informatique	1
I.3.l'objectif d'utilisations d'un réseau informatique.....	1
I.4. classifications des réseaux.....	1
I.4.1.classifications selon l'étendue géographique	1
I.4.1.1.les réseaux personnels (PAN).....	1
I.4.1.2.les réseaux locaux (LAN).....	2
I.4.1.3.les réseaux métropolitains (MAN).....	2
I.4.1.4.les réseaux étendus(WAN).....	2
I.4.2.classifications selon l'architecture.....	2
I.4.2.1.le réseau poste à poste.....	2
I.4.2.2.le réseau client/serveur.....	2
I.5.les topologies de réseau.....	3
I.5.1.la topologie en bus.....	4
I.5.2.la topologie en étoile	4
I.5.3 .la topologie en anneau.....	4
I.6.les supports de transmissions.....	5

I.7.les équipements d'interconnexions réseaux	7
I.8 .Architecture des réseaux.....	8
I.8.1.le modèle OSI.....	8
I.8.2.l'architecture TCP/IP.....	9
I.9.les protocoles	10
I.9.1.le protocole TCP/IP	11
I.9.2. le protocole IPX.....	12
I.9. 3.le protocole NetBeui.....	12
I.10. Attaques et moyens de sécurité réseau	12
I.10.1. Quelques types d'attaques	13
I.10.1.1. Attaque sur le réseau	13
I.10.1.2. Attaque sur le mot de passe.....	13
I.10.2. la politique de Sécurité réseau.....	13
I.10.3. Principe d'une politique de sécurité réseau.....	14
I.11.Solutions de Sécurité	14
I.11.1.Système de détection d'intrusions.....	14
I.11.2.Utilisations de sessions	15
I.11.3. Solution Antivirale	15
I.11.4. Solution Firewall.....	15
I.11.4.1. Firewall à filtrage de paquets.....	16
I.11.4.2. Firewall Applicatif.....	17
I.11.5. Annuaire	18
I.11.6. déploiement d'Active Directory	18

I.12.conclusion.....	19
Chapitre II: Etude de l'existant.....	
II. Présentation de l'entreprise NAFTAL de Bejaia	21
II.1. Missions et activités de l'entreprise NAFTAL.....	21
II .1.1. Ses Missions.....	21
II.1.2. Ses Activités	22
II.3.Organigramme général de l'entreprise NAFTAL Bejaia.....	23
II.4.1.Organisation de la GPL de Bejaia et ces différents départements	24
II.4.2. Le rôle de département informatique dans cette entreprise.....	24
II.4.3. L'architecture réseau de district GPL de Bejaia	24
II.5.Paramètres du serveur.....	26
II.5.1. Présentation des outils de travail.....	26
II.5.2. Les supports de transmissions	27
II.5.3. Gestion des utilisateurs et autorisations d'accès au réseau.....	28
II.6. Description du projet.....	28
II.6.1.Description des besoins	29
II.6.2. Synthèse des faiblesses.....	29
II.6.2. Solutions de sécurité réseau..	29
II.6.2.1. Active directory.....	30
II.6.2.2.Apple open Directory	30
II.6.2.3. Novell eDirectory server	30
II.6.2.4. Mandriva Directory server MDS.....	30
II.6.3. Le choix de la solution à entreprendre.....	30
II.6.4. Les caractéristiques d'Active Directory.....	31
II. 6.5. Structure d'Active directory.....	31
II.6.5. 1. Domaines.....	31
II.6.5. 2. Arbres de domaines.....	32

II.6.5. 3. Forêts.....	32
II.6.6. L'objectif global du projet	32
II.7. Conclusion.....	33
<u>Chapitre III : configuration</u>	
III.1.introduction.....	34
III.2.présentation de Windows server 2003.....	34
III.2.1. la famille Windows server 2003.....	34
III.2 .2.Installation Windows server 2003.....	34
III.3. installation d'Active directory	37
III.3.1.Reconnaissance des objets Active Directory.....	39
III.4.La configuration d'Active Directory.....	40
III.4.1. Contrôleur de domaine (Active directory).....	40
III.4.2. Création d'une unité d'organisation.....	41
III.4.3. Ajout d'un utilisateur dans active directory.....	43
III.4.4. Gestion des utilisateurs et autorisations d'accès.....	46
III.4.5. Rendre un utilisateur administrateur du domaine.....	47
III.5. Configuration de postes clients.....	50
III.6. La création de comptes utilisateurs	51
III.7. Spécification d'Horaires d'accès au compte utilisateurs	53
III.8. Le serveur de fichiers.....	55
III.8.1.Quesque' un serveur de fichiers ?.....	55
III.8.2. Installation et con figuration d'un serveur de fichiers.....	55
III.8.3. connexion d'un utilisateur au serveur de fichiers.....	58
III.9. le serveur d'impression.....	60
III.9.1.Quesq'un serveur d'impressions.....	60
III.9.2. Ajout et Partage d'une imprimante sur le réseau.....	61

III.10. Gérer les domaines et les approbations	64
III.11. Gérer les sites et les services	65
III.12. Le Serveur DNS.....	66
III.13. Le Serveur DHCP.....	67
III.14. La réservation d'une adresse IP	68
III.15. Conclusion70
Conclusion générale.....	
Bibliographie	vii

Liste des figures

Figure. I.1. -le câble coaxial	5
Figure I.2. - la paire torsadée.....	6
Figure I.3. -la fibre optique.....	6
Figure II.1. - Organigramme général de l'entreprise NAFTAL Bejaia.....	22
Figure II.2 - organigramme du district GPL Bejaia.....	23
Figure II. 3 - l'architecture du réseau informatique de district GPL BEJAIA..	24
Figure III.1 - Définition des stratégies systèmes.....	36
Figure III.2 – configuration du server	36
Fenêtre III.3 -le choix du type de configuration pour un premier serveur...37	
Figure III.4 - attribution d'un nom de domaine	38
Figure III.5 - Etablissement d'un rôle pour le serveur.....	39
Figure III.6 - Ajout d'une unité d'organisation.....	40
Figure III.7 - Création de l'unitéGPL	42
Figure III.8 -création des unités qui representent les deux departement	42
Figure III.9 - les objets crée au sein de la GPL	42
Figure III.10 - Création d'un utilisateur dans active directory	44
Figure III.11 - confirmation et validation mot de passe.....	44
Figure III.12 - liste des utilisateurs et ordinateurs crée au département informatique...45	
Figure III .13 - utilisateurs et ordinateurs crée au département commercial.....	46
Figure III.14 - rendre un utilisateur administrateur du domaine	47
Figure III.15 - propriété de l'utilisateur talbi	48
Figure III.16 - Ajout de propriété à l'utilisateur talbi.....	48
Figure III.17 - résultat de la sélection de l'administrateur du domaine.....	49
Figure III. 18 - validation de la sélection de l'administrateur du domaine.....	49
Figure III. 19 - modification du groupe du travail	50

Figure III.20 - Liste des réseaux Microsoft crée	51
Figure III.20 – voir Les ordinateurs du groupe du travail.....	51
Figure III.22 - résultat du Ping effectué entre les deux pc.....	52
Figure III.21 - Etapes de création d'un compte utilisateurs.....	53
Figure III.22 - le nom du compte utilisé.....	53
Figure III.23 - liste de compte utilisateurs crée.....	54
Figure III.24 - horaire d'ouverture de la session autorisée pour l'utilisateur Toula.....	55
Figure III.25 - horaire d'ouverture de session autorisé pour l'utilisateur talbi	55
Figure III.26 – l'assistant partage de dossiers	56
Figure III.27 - description et spécification des paramètres du partage	57
Figure III.28 -spécification des autorisations d'accès au partage.....	57
Figure III.29 - résumé de l'état de partage effectué.....	58
Figure III.30 -propriété de partage et les autorisations permises	58
Figure III.31 – autorisations permises pour tout le monde.....	59
Figure III. 32 - connexion d'un utilisateur au serveur de fichiers.....	60
Figure III.33. - etapes à suivre pour ce connecté à un bureau distant.....	60
Figure III.34. -Etablir la connexion bureau à distance.....	61
Figure III.35 -ajout de rôle serveur de fichiers et serveur d'impression.....	61
Figure III.36 – assistant ajout d'imprimante.....	62
Figure III.37 – le choix du type de l'imprimante à installer.....	63
Figure III.38 – recherche de l'emplacement à installé l'imprimante.....	64
Figure III.39 - l'imprimante est partagée	64
Figure III.40 - Gestion des domaines et des approbations.....	65
Figure III.41 - Gérer les sites et les services.....	66
Figure III.42- La configuration DNS d'une manière local.....	67

Figure III.43 - Configuration du server DHCP.....	68
Figure III.44 - La réservation d'une adresse IP.....	69
Figure III.45 - La réservation d'une adresse IP déjà existé.....	70

Liste Des Tableaux

TABLE I.1 - Tableau correspondance modèle TCP /IP et le modèle OSI.....	10
TABLE II.1- Tableau des paramètres serveur	24
TABLE II.2 - Equipement réseau de l'entreprise NAFTAL.....	25
TABLE II.3 - les supports de transmissions	25
TABLE III.1 - reconnaissances des objets active directory	37
TABLE III .2 - Mot pass des Utilstateurs créer pour departement informatiques...42	
TABLE III .3 - Mot pass des Utilstateurs créer pour departement commercial.....42	

Introduction générale

Introduction

La nécessité de faire communiquer les différents services d'une entreprise et/ou d'une organisation devient de plus en plus courante. En effet, L'évolution du réseau implique l'apparition de nouvelles technologies de l'information et de la communication (NTIC) ; permettant une souplesse de raccordement aux réseaux à lequel l'internet n'est pas étranger.

La notion de petits réseaux, puis de réseaux locaux (LAN) apparaît en premier lieu puis développer par la suite se forme de réseaux à grand distances.

Un réseau informatique offre des services et des ressources destinées à répondre aux besoins des utilisateurs, il permet de partager des dossiers, des ressources et d'avoir accès à celui -ci par le biais de compte utilisateur.

L'objectif de ses services et de rendre les dossiers et les ressources accessibles par tout le réseau et de définir les droits d'accès aux dossiers, aux fichiers et aux imprimantes.

Le thème de mon travail porte sur « **l'administration d'un réseau local via active directory** » Au sein de l'entreprise NAFTAL Bejaia.

- Ce modeste mémoire comporte une vue global sur l'ensemble des réseaux suivie d'une étude sur le réseau de l'entreprise NAFTAL ainsi que les ressources informatiques au niveau du département informatique de l'entreprise ; l'organisation du mémoire est comme suit :

- **Chapitre I** «Notions générales sur les réseaux » : ce chapitre présente une description générale sur les réseaux informatiques . aussi, propose des solutions pour la sécurité en réseau contre les intrus.et contre les accès non autorisé par le déploiement d'Active directory.
- **Chapitre II** « Etude de l'existant »: montre une brève étude sur le réseau NAFTAL .ainsi que les différent équipements et les ressources informatique qui dispose l'entreprise.
- **Chapitre III** « configuration » : se chapitre est consacré à la configuration est déploiement de l'annuaire active directory , la gestion des utilisateurs et le partage réseau des ressources informatique au sein de l'entreprise .ce chapitre est l'essentiel de ce mémoire il explique encore les différents rôles à gérer par l'administrateur réseau .

Ce mémoire ce termine par une conclusion qui donne un résumé sur le travail effectué ; glossaire, bibliographie .

CHAPITRE I :

Notions générales sur les réseaux informatiques

I.1. Introduction :

L'histoire des réseaux et des télécommunications pourrait se résumer à une perpétuelle course au débit ou ce qu'on appelle aussi largeur de bande. Le principe du réseau local est apparu dans les années 70 pour interconnecter les équipements de mini-informatique (terminaux, imprimantes, disques,.....).En effet, la plupart des échanges de données dans une entreprise s'effectue localement, voir par groupes de travail. C'est pourquoi, avec la généralisation des micro-ordinateurs à la fin des années 80, le réseau local à affirmé sa vocation.

I.2.Définition d'un réseau informatique :

Un réseau informatique est un ensemble d'élément matériel et logiciels relié entre eux dans le but de permettre aux utilisateurs de partager des ressources et d'échanger des informations sous forme numérique.

Un réseau est constituer d'équipement appelées nœuds .en fonction de leur étendue et de leur domaine d'applications, ces réseaux sont catégorisées.

I.3. l'objectif d'utilisations d'un réseau informatique :

L'objectif premier des réseaux est la mise en commun de ressources, assurant notamment :

- le **partage** de l'information .en informatique, celle-ci existe sous différentes formes : Fichiers ; documents ; données....
- La **communication** entre personnes grâce au courrier électroniques, la discussion en direct, ...
- La garantie de l'**unicité de l'information** lors d'une mise à jour de bases de données.
 - la mise en place d'outils de travail collaboratif.
 - La communication entre processus.

I.4.Classification des réseaux:

Un réseau est constituer d'équipement appelées nœuds .en fonction de leur étendue et de leur domaine d'applications, ces réseaux sont classifiés on distingue :

I.4 .1.Classification selon l'étendue géographique : on a

I.4 .1.1.les réseaux personnels(PAN):

La plus petite étendue de réseau est nommée en anglais Personale Area Network(PAN), centrée sur l'utilisateur, elle désigne une interconnexion d'équipements Informatiques dans un espace d'une dizaine de mètres de celui ci.

Il est appelé aussi réseau individuel ou réseau domestique. [2]

I.4 .1.2.les réseaux locaux (LAN) :

De taille supérieure, s'étendant sur quelques dizaines à quelques centaines de mètres, le local Area Network (LAN) , en français réseau local d'entreprise est une infrastructure de communications reliant des équipements informatiques variés, sur une aire géographique limitée, dans le but de partager des ressources communes. [2]

I.4 .1.3.les réseaux métropolitains(MAN) :

Le réseau métropolitain, ou Métropolitain Area Network (MAN), est également nommé réseau fédérateur .Il assure des communications sur des plus longues distances, interconnectant souvent plusieurs réseaux LAN.

I.4 .1.4.Les réseaux étendus(WAN) :

Les réseaux étendus sont capables de transmettre les informations sur des milliers de kilomètres à travers le monde entier. Le WAN (Wide Area Network) , le plus célèbre est le réseau public internet, dont le nom provient de cette qualité : Inter Networking ou interconnexion de réseaux. [2]

I.4.2.Classification selon l'architecture : on trouve

I.4.2.1.Le réseau poste à poste (peer to peer):

Chaque poste connecté est à la fois **serveur** lorsqu'il met ses ressources (imprimantes, dossiers) à disposition des autres postes, et **client** lorsqu'il bénéficie des ressources des autres postes.

Il n'existe pas de gestion centralisée des ressources du réseau.[3]

Les réseaux poste à poste ne nécessitent pas les mêmes niveaux de performance et de sécurité que les logiciels réseaux pour serveurs dédiés.

Tous les systèmes d'exploitation intègrent toutes les fonctionnalités du réseau poste à poste.

I.4 .2.2.Le réseau client / serveur :

Un ou plusieurs ordinateurs appelés serveur assurent des fonctions centralisées d'administration qui permettent d'authentifier des utilisateurs et de leurs accorder des permissions sur les ressources du réseau.

Les serveurs peuvent être spécialisés : serveur de fichiers, d'application, d'impression, de communication. Ils offrent des services à des programmes clients (client de messagerie, de base de données anti- virales, etc...). [3]

- les deux types de réseau présentent des **avantages dont on peut citer** :

- Le modèle client/serveur est particulièrement recommandé pour des réseaux nécessitant un grand niveau de fiabilité, ses principaux atouts sont :
- des ressources centralisées : étant donné que le serveur est au centre du réseau, il peut gérer des ressources communes à tous les utilisateurs, comme par exemple une base de données centralisée, afin d'éviter les problèmes de redondance et de contradiction .
- une meilleure sécurité : car le nombre de points d'entrée permettant l'accès aux données est moins important.
- une administration au niveau serveur : les clients ayant peu d'importance dans ce modèle, ils ont moins besoin d'être administrés.
- un réseau évolutif : grâce à cette architecture il est possible de supprimer ou rajouter des clients sans perturber le fonctionnement du réseau et sans modification majeure .

Le modèle *peer to peer* a :

- un coût réduit (pas de matériel évolué et donc cher, pas de frais d'administration)
- une grande simplicité (la gestion et la mise en place du réseau et des machines sont peu compliquées)

Note : l'« administration » d'un réseau ou de machines désigne :

- Gestion des utilisateurs et de la sécurité .
- Mise à disposition des ressources .
- Maintenance des applications et des données .
- Installation et mise à niveau des logiciels utilisateurs .

-Il existe un certain nombre d'**inconvénients** que l'entreprise doit connaître avant de faire son choix.

L'architecture client/serveur a tout de même quelques lacunes parmi lesquelles :

- un coût élevé dû à la technicité du serveur
- un maillon faible : le serveur est le seul maillon faible du réseau client/serveur, étant donné que tout le réseau est architecturé autour de lui ! Heureusement, le serveur a une grande tolérance aux pannes (notamment grâce au système RAID) .

Pour l'architecture poste à poste ce système n'est pas du tout centralisé, ce qui le rend très difficile à administrer ;

- La sécurité est moins facile à assurer, compte tenu des échanges transversaux
- Aucun maillon du système ne peut être considéré comme fiable.

Ainsi, les réseaux égal à égal sont préférentiellement utilisés pour des applications ne nécessitant pas un haut niveau de sécurité ni une disponibilité maximale (il est donc déconseillé pour un réseau professionnel avec des données sensibles).

I.5. Similitudes entre types de réseau :

Les différents types de réseaux ont généralement les points suivants en commun :

- Serveurs : ordinateurs qui fournissent des ressources partagées aux utilisateurs par un serveur de réseau
- Clients : ordinateurs qui accèdent aux ressources partagées fournies par un serveur de réseau
- Support de connexion : conditionne la façon dont les ordinateurs sont reliés entre eux.
- Données partagées : fichiers accessibles sur les serveurs du réseau
- Imprimantes et autres périphériques partagés : fichiers, imprimantes ou autres éléments utilisés par les usagers du réseau
- Ressources diverses : autres ressources fournies par le serveur.

I.5. les Topologies de réseau :

I.5.1. Topologie en bus :

Repose sur un câblage sur lequel viennent se connecter des nœuds (postes de travail, équipements d'interconnexions, périphériques...) .Il s'agit d'un support multipoints .Le câble est l'unique élément matériel constituant le réseau et seul les nœuds génèrent le signal. [4]

I.5.2. Topologie en étoile :

Cette topologie repose quand à elle, sur des matériels actifs ou chaque équipement est relié à un nœud central .Les performances d'un réseau en étoile dépende principalement du nœud central ; ce type de réseau est relativement efficace et économique .La plupart de réseau locaux fonctionne sur se principe ; en utilisant un Switch central reliant tout les ordinateurs au même nœud . [4]

I.5.3. Topologie en anneau : Dans ce type de topologie les ordinateurs sont placés en cercle sur un câble sans terminaison (en fait ils sont reliés par des câbles aller/retour à un

Concentrateur passif qui relie chaque ordinateur au suivant). Chaque Ordinateur joue le rôle de répéteur pour amplifier le signal et le faire repartir. La Méthode d'Accès à ce type de câblage est celle du passage de « jeton ». Pour pouvoir transmettre un ordinateur doit être en possession du jeton libre ce qui évite toute collision sur le réseau . [4]

I.6.les supports de transmission :

Un réseau suppose plusieurs équipements informatiques (ordinateurs fixes ou portables, divers équipements électroniques, téléphones, assistants numériques personnels...) situés à distance les uns des autres.

La première chose à mettre en œuvre pour constituer le réseau est la transmission des informations d'un équipement à l'autre : on utilisant des supports de transmission. C'est le support (généralement filaire, c'est-à-dire sous forme de câble, de plus en plus non filaire) qui relie les ordinateurs entre eux.

Les principaux supports physiques utilisés dans les réseaux locaux sont les suivants:

I.6.1 .avec fil :

- Le **câble coaxial** supporte un débit de 10 Méga bits par seconde (10 Mips) ; il est constitué d'un conducteur central en cuivre, d'un isolant puis d'un deuxième conducteur se forme de métal tressé, assurant le blindage et en fin d'une gaine isolante assurant la protection mécanique de l'ensemble comme se figure au dessus :



Figure. I.1. -le câble coaxial-

- La **paire torsadée** ressemble à un câble téléphonique. Suivant sa catégorie elle supporte de 10 à 100 Mbps sur 100 mètres.

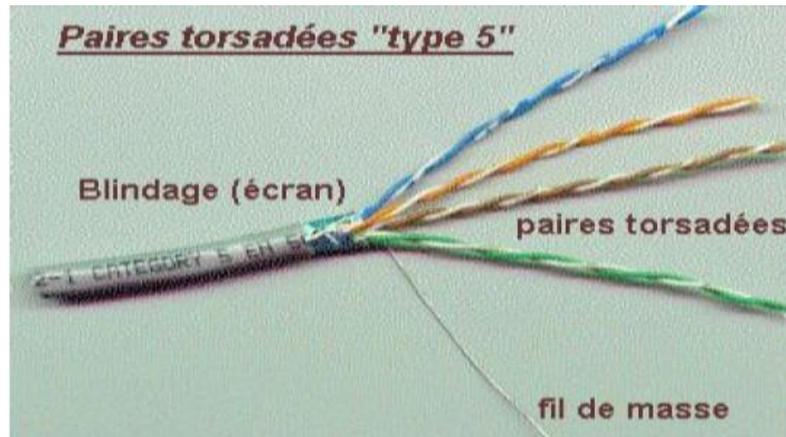


Figure I.2. – la paire torsadée -

- La **fibre optique** maintient un débit de 155 Mbps à 10 Gbps Sur plusieurs kms. La fibre transfère les données se forme d'impulsions lumineuse modulée. Il existe deux types de fibre optique :
 - La multi mode : utilisées pour les trop grandes distances.
 - La monomode : utiliser en local pour la connexion des appareils réseau. [4]



Figure I.3. -la fibre optique-

I.6.2 .Sans fil :

- a- Infra rouge** : L 'IrDA, appelé infrarouge, est encore aujourd'hui une technologie de transmission sans fil très répandue (PC portable, PDA, téléphone portable, etc.). Le protocole IrDA est conçu pour le transfert des données, en utilisant la lumière infrarouge. Avec une connectivité rapide, sans installation. Faible coût. sécurisation de transmission.

b- Bluetooth : La technologie Bluetooth est une technologie de réseaux sans fils d'une faible portée, de l'ordre de quelques dizaines mètres à un peu moins d'une

centaine de mètres, permettant de relier des périphériques (imprimantes, téléphones portables, appareils domestiques, oreillettes sans fils, souris, clavier, etc.) et des ordinateurs et assistants personnels (PDA) entre-deux sans liaison filaire.

Il a comme Avantages : Faible consommation d'énergie, Bonne gestion de la communication de la voix. Equipements de taille réduite. Technologie adaptée à la mobilité et un Faible coût.

Inconvénients : Nombre de périphériques limité dans un réseau Faible porté et un Débit limité.

c- Wifi : Le Wifi, pour Wireless Fidélité, est une technologie standard d'accès sans fil à des réseaux locaux. Le principe est d'établir des liaisons radio rapides entre des équipements et des bornes reliées aux réseaux Haut Débit. Grâce au Wifi, il est possible de créer des réseaux locaux sans fils à haut débit.

Le Wifi possède deux modes de fonctionnement :

Le mode infrastructure auquel se connectent toutes les stations (appareils équipés d'un équipement Wifi) à un point d'accès ou un routeur, et le mode ad-hoc où les stations se connectent les unes aux autres sans passer par un point d'accès.

d- Wi max : le Wi max est un standard de transmission sans fil à haut débit. Fonctionnant à 70 Mbit/s, il est prévu pour connecter les points d'accès Wifi à un réseau de fibres optiques, ou pour relayer une connexion partagée à haut débit vers de multiples utilisateurs.

Cette technologie apparue en France en décembre 2003 menace sur le papier le Wifi grâce à des débits théoriques sept fois supérieurs et une couverture qui s'étend jusqu'à 50 kilomètres là où les bornes Wifi se limitent à quelques centaines de mètres.

I.7.les équipements d'interconnexions réseau :

Un réseau local est constitué d'ordinateurs reliés par un ensemble d'éléments matériels et logiciels. Les éléments matériels qui permettent d'interconnecter les ordinateurs sont les suivants:

- **La carte réseau (parfois appelé coupleur):** Il s'agit d'une carte connectée sur la carte mère de l'ordinateur ou partie intégrante de la Carte mère qui relie à l'aide d'un câble ou d'ondes radios un ordinateur au reste du réseau. Sa vitesse était autrefois de 10 Mbps, la majorité du Parc est en 100Mbps et aujourd'hui les dernières cartes sont en 1 000 Mbps.
- **Les répéteurs :** permettant de régénérer automatiquement un signal ; ce qui permette de prolonger la portée du support.
- **Les concentrateurs (hubs),** permettant de connecter entre eux plusieurs hôtes. Ils sont non intelligents. Ils envoient le signal pour toutes les stations compris la station destinataire.
- **Les ponts (bridges),** permettant de relier des réseaux locaux de même types.
- **Les commutateurs (Switch)** permettant de relier divers éléments tout en segmentant le réseau, ils sont des hubs améliorés et plus intelligents envoient le signal directement à la station concernée.
- **Les passerelles (Gateway),** permettant de relier des réseaux locaux de types différents.
- **Les routeurs,** permettant de relier de nombreux réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de la façon optimale.
- **Les B-routeurs,** associant les fonctionnalités d'un routeur et d'un pont.

I.8 .Architecture des réseaux :

Grace à l'évolution des capacités réseaux, le traitement automatisé des informations a considérablement évolué depuis une quarantaine d'années succédant aux grands systèmes propriétaires centralisés, plusieurs architectures sont désormais possibles. [5]

I.8 .1.Le modèle OSI :

le modèle OSI (Open Système Interconnexion) : destiné à normaliser les échanges entre deux machines .il définit ainsi ce qui doit être une communication réseau complète.

L'ensemble du processus est ainsi découpée en sept couches hiérarchiques .Chaque couche se comporte comme un prestataire de service pour la couche immédiatement supérieure ; chacune d'elles ajoute un en-tête spécifique à la trame reçue. [5]

- **La couche(1) : physique**

Rassemble les moyens électriques, mécaniques, optiques ou hertziens par lesquels les informations sont transmises .Les unités sont donc des bits (0 ou 1) . [8]

- **La couche (2) : liaison de donnée**

Gère la fiabilité de transfert des bits d'un nœud à l'autre du réseau, comprenant entre autre les dispositifs de détection et correction d'erreur, ainsi que le système de partage des supports .L 'unité de donnée à ce niveau est appelée une trame. [8]

- **La couche (3) : réseau**

Aiguille les données à travers un réseau à commutation .L'unité de données s'appelle en général un paquet.

- **La couche(4) : transport**

Regroupe les règles de fonctionnement de bout en bout, assurant ainsi la transparence du réseau vis-à-vis des couches supérieures .Elle traite notamment l'adressage, l'établissement des connexions et la fiabilité de transport.

- **La couche(5) : session**

Réunit les procédures de dialogue entre les applications, établissement et interruptions de la communication , cohérence et synchronisation des opérations .

- **La couche(6) : présentation**

Traite les formes de représentation des données permettant la traduction entre machines différentes.

- **La couche(7) : application**

Source et destination de toute les informations à transporter , la couche application rassemble toutes les applications qui ont besoin de communiquer par le réseau : messagerie électronique ,transfert de fichiers ,gestionnaire de base de donnée,.....[5]

I.8.2.1'architecture TCP/IP :

Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à 4 couches ; dans laquelle les protocoles TCP et IP jouent un rôle prédominant, car ils en constituent l'implémentation la plus courante. Par abus de langage, TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

- **La couche accès réseau :**

Cette couche regroupe les couches physiques et liaison de données du modèle OSI.

- **La couche internet :**

Cette couche est la plus importante dans cette architecture ; elle réalise l'interconnexion des réseaux distants sans connexion, permet l'injection des paquets indépendamment les uns des autres jusqu'à la destination.

- **La couche transport :**

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

- **La couche application :**

Contrairement au modèle OSI, c'est la couche immédiatement supérieure à la couche transport , elle contient les protocoles de haut niveau Telnet , TFTP , http..... ;

Le point important pour cette couche est le choix du protocole de transport à utiliser.[8]

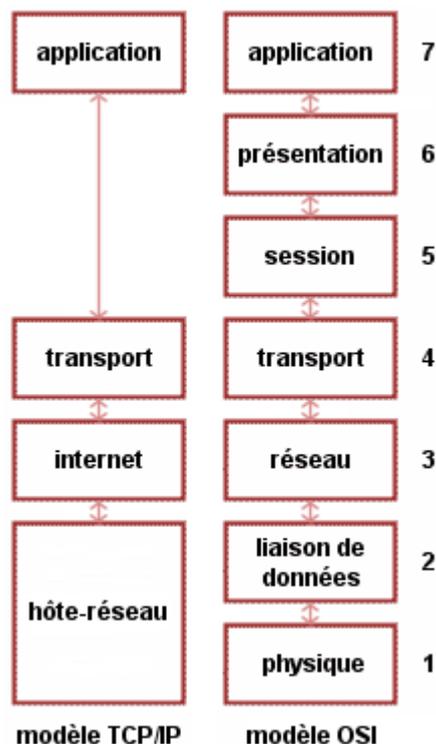


TABLE I.1. -correspondance du modèle OSI et TCP/IP-

I.9.les protocoles :

Un protocole est une méthode standard qui permet la communication entre deux machines.

Ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur le réseau. Parmi lequel on site :

I.9.1. TCP/IP : (Transmission Control Protocol / Internet Protocol) :

Défini la norme de communication, (en fait un ensemble de protocoles) des ordinateurs reliés à Internet.

Ce modèle définit les règles que les ordinateurs doivent respecter pour communiquer entre eux sur le réseau Internet. Nous vous proposons de découvrir plus en détails ses caractéristiques et son fonctionnement. [6]

Il existe d'autre protocole comme :

- **DNS** permet de retrouver une adresse IP en fonction d'un nom d'ordinateur (un peu comme un annuaire).
- **FTP** sert à transporter des fichiers d'un ordinateur à l'autre.
- **IRC** permet de créer des «salons» de discussion en direct.
- **ICQ** permet de savoir si quelqu'un est en ligne et de dialoguer avec lui.

- **NTP** permet de mettre les ordinateurs à l'heure par internet à 500 millisecondes près.
- **P2P** permettent de partager des fichiers à grande échelle.
- **NNTP** permet d'accéder à des forums de discussion sur des milliers de sujets différents.
- **SSH** permet d'avoir un accès sécurisé à des ordinateurs distants.
- **SMTP** permet d'envoyer des emails, et le protocole POP3 de les recevoir.

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

Système distribué de bases de données et de serveurs qui assure la traduction des noms de domaine utilisés par les internautes en numéros IP utilisables par les ordinateurs.

Mis au point pour permettre aux internautes d'utiliser des noms dans la rédaction des adresses (beaucoup plus facile à manipuler que des suites de chiffres).

Exemples :

nom : www.unice.fr

-> IP : 134.59.1.71

nom : bach.ebgm.jussieu.fr

-> IP : 134.157.50.1

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

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

Attention: Protocoles de transfert non sûrs, c'est-à-dire que les données circulent en clair sur le réseau.

I.9.2.le protocole IPX (Inter PAccket exchange):

Protocole de niveau réseau développé et commercialisé par la société Novell et intégré à son système d'exploitation réseau.

Les paquets XP peuvent être acheminées d'un réseau à l'autre aux couches trois et quatre du modèle de référence OSI(Open System Interconnexion).[7]

I.9.3.le protocole NetBeui :

Protocole plus rapide que TCP/IP et IPX, il est utilisé par les petits réseaux LAN, sa rapidité du traitement exprime son utilité. [7]

I.10. Attaques et moyens de sécurité réseau :

Le réseau local est le cœur de la majeure partie de l'activité informatique de nos organismes. A ce titre tout effort de sécurisation est nécessaire. Cette considération justifie à elle seule d'accorder une attention particulière à la sécurisation des réseaux locaux.

Par ailleurs, il est généralement estimé que la majorité des malveillances informatiques ont une origine complicité interne aux organismes (la malveillance constituant déjà la catégorie la plus significative des pertes par rapport aux deux autres accidents et erreurs). devant cette spécificité il est donc essentiel d'examiner dans une optique sécuritaire l'infrastructure du réseau local dès sa conception.

Il est donc nécessaire d'établir des configurations de systèmes d'exploitation comprenant leurs réseaux et multiples branches, sécurisés avec les techniques les plus sophistiquées en matière de « firewalls » et de contrôles d'accès. [17]

I.10.1. Quelques types d'attaques :

I.10.1.1. Attaque sur le réseau : les principales techniques d'attaques sur le réseau sont :

. **Le Sniffing :** technique permettant de récupérer toutes informations transitant sur le réseau. Elle est généralement utilisée pour récupérer les mots de passe des applications qui ne chiffrent pas leurs communications.

. **Usurpation d'identité (Spoofing) :** technique consistant à prendre l'identité d'une autre personne ou d'une autre machine. Elle est généralement utilisée pour récupérer des informations .

- absence d'un système de détection d'intrusion interne provoque l'accès non autorisé depuis l'extérieur

I.10.1.2. Attaque sur le mot de passe :

Les attaques sur les mots de passe peuvent consister à faire de nombreux essais jusqu'à trouver le bon mot de passe.

- Si aucun mécanisme n'est pris en considération pour lutter contre les attaques sur les mots de passe. Un intrus peut mener une attaque pour collecter les mots de passe afin d'accéder aux ressources matériels mises en question.
- La majorité des failles et incidents de sécurité sont dus à des erreurs humains, des utilisateurs sont encore inconscient ou ignorant des risques qu'ils encourent lors de l'utilisation d'un programme mal veillant.
- L'absence de session offre à l'intrus la possibilité de collecter un ensemble d'information sur la cible (nom d'utilisateur, partage).
- Les postes client sont intégrés dans le WORKGROUP, ou le compte d'accès par défaut est administrateur sur les postes client ce qui provoque Requêtes nombreuses provenant des postes clients qui veulent devenir le "maitre de Workgroups" .

I.10.2. La politique de Sécurité réseau :

La politique de sécurité est une démarche de toute entreprise visant à protéger son personnel et ses biens d'éventuels incidents de sécurité pour son activité. La politique de sécurité réseau fait éventuellement partie de la démarche sécuritaire de l'entreprise.

Tout d'abord, elle doit déterminer les éléments critiques qui est une tâche très délicate en passant par une analyse de risque qui consiste à identifier les ressources ou les biens vitaux de l'entreprise .Ces derniers peuvent être de plusieurs ordres : matériels ,données ,logiciels et personnes.

I.10.3. Principe d'une politique de sécurité réseau :

La politique de sécurité réseau vise à satisfaire les critères suivants :

- **Authentication** : information permettant de valider l'identité pour vérifier que la personne est celle qui prétend l'être .
- **Identification** : information permettant d'indiquer la personne inscrite.

- **Autorisation** : information permettant d'indiquer les ressources de l'entreprise auxquelles un utilisateur identifié aura accès ainsi que les actions autorisées sur ses ressources.

- **intégrité** : regroupe les mécanismes garantissant qu'une information n'a pas été modifiée ou altérée.

- **Disponibilité** : regroupe les mécanismes garantissant que les ressources de l'entreprise sont accessibles.

- **non-répudiation** : mécanisme permettant de prouver qu'un message a bien été envoyé par un émetteur et reçu par un récepteur.

La politique de sécurité réseau couvre les éléments suivants :

- **sécurité d'accès** : détermine la sécurité d'accès aux ressources de l'entreprise que soit localement ou via un accès distant, ainsi que la gestion des utilisateurs et leurs droit d'accès aux systèmes d'information de l'entreprise.

- **sécurité de l'infrastructure** : couvre la sécurité des équipements et des connexions réseaux.

- **sécurité de l'intranet face à internet** : couvre la sécurité logique des accès aux ressources de l'entreprise et l'accès aux ressources extérieures (internet) .

I.11. Solutions de sécurité réseau

Une bonne stratégie de sécurité vise à mettre en oeuvre des mécanismes de sécurité ; des procédures de surveillance des équipements de sécurité, des contrôles et audits de sécurité.

I.11.1. Système de détection d'intrusion (IDS) :

IDS sont des équipements logiciels ou matériels qui permettent de mettre en place des mécanismes de détection d'intrusion, un composant primordial pour les mécanismes de sécurité des réseaux. Grace à lui on peut détecter les tentatives d'attaques de l'extérieur.

Il est conseillé d'implanter un système de détection d'intrusion sécurisé . On distingue principalement deux catégories de système détection d'intrusion :

- **NIDS** : (Network Intrusion Détection System): est un détecteur d'intrusion réseau qui détecte les attaques réseau en se basant sur une base des signatures très à jour.
- **HIDS** : (Host Intrusion Détection System) : a pour objectif la surveillance de l'activité d'une machine en utilisant les fichiers de log du système et en contrôlant l'intégrité de celui-ci .Ces ondes s'insèrent entre les applications et le cœur du système d'exploitation pour protéger des applications ou des serveurs critiques.

Les solutions **IDS** (Intrusion Détection System) pour un réseau garantit une surveillance permanente du réseau.

I.11.2. Utilisation de sessions :

L'exigence d'avoir au moins deux sessions pour chaque poste dans un réseau local de l'entreprise , une pour l'utilisateur avec privilège restreint de préférence pour ne pas modifier la configuration initiale et la deuxième pour l'administrateur qui est le seul à pouvoir modifier les paramètres de base. Une authentification par Login et Mot de passe est obligatoire.

I.11.3. Solution Antivirale :

La protection antivirale consiste à appliquer une solution antivirus client/serveur. Cette solution consiste à installer un serveur antivirus sur les réseaux et de déployer sur chaque machine le client associé. Une telle solution permet de centraliser la tâche d'administration : mise à jour des fichiers des signatures et déploiement automatiquement sur les postes clients.

L'antivirus doit implémenter aux moins les fonctionnalités suivantes :

Exécution en tâche de fond, détection automatique, récupération des fichiers importants après une suppression accidentelle, filtrage du courrier électronique indésirable et mise à jour automatique.

I.11.4.Solution Firewall :

La solution de filtrage consiste à déployer trois niveaux de filtrage sur les ressources du réseau, comme écrit ci-dessous :

➤ Firewall à filtrage de paquets :

La majorité des équipements de routage actuels disposent d'une fonctionnalité de firewalling basé sur le filtrage de paquets. Cette technique permet de filtrer les protocoles, les sessions, les adresses sources, les ports sources et destination et même l'adresse MAC.

➤ Firewall State full Inspection:

Cette solution sera implémentée par un équipement firewall matériel qui agit en tant que passerelle, afin de garantir la sécurité entre le trafic du réseau interne, public et démilitarisé

Au niveau architecture du réseau, le firewall propose trois domaines de sécurité :

- Zone interne : Représente le réseau local de l'organisme. Cette zone contient le plus haut niveau de sécurité
- Zone externe : représente la zone publique par laquelle passe tout le trafic de destination internet.
- Zone démilitarisée : représente la zone contenant les serveurs visibles de l'extérieur dont l'accès est public.

➤ **Firewall Applicatif :**

Un Firewall applicatif sera installé sur tous les postes client et les serveurs afin de protéger en premier lieu des tentatives d'intrusion interne.

L'utilisation d'un firewall applicatif permet de contrôler les connexions depuis et vers ces machines, de renforcer la confidentialité des données et de se protéger contre les programmes malveillants.

On peut citer par exemple un Firewall : Mod_security et Mod_Proxy.

I.11.5. l'Annuaire :

Un annuaire permet de stocker des données légèrement typées, organisées selon des classes particulières et présentées dans un arbre.

On peut trouver des solutions d'annuaire comme LDAP, c'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leur valeur : la racine O «organisation», le sous ensemble d'une organisation ou « organisation Unit », le nom de domaine DC « Domain Component » et la personne Person « schéma standard pour une personne ».

Exemple : **Le service d'annuaire *Active Directory***

I.11.6. déploiement complet d'Active Directory :

Active directory fournit des services centralisés de Gestion des ressources et de la sécurité, il permet également l'attribution et l'application de stratégies.

Le contrôle d'accès peut être défini non seulement sur chaque objet de l'annuaire, mais aussi sur chaque propriété de chacun des objets. Active Directory fournit à la fois le magasin et l'étendue de l'application pour les stratégies de sécurité.

Une stratégie de sécurité peut inclure des informations de compte, telles que des restrictions de mot de passe applicables sur l'ensemble du domaine ou des droits pour des ressources de domaine spécifiques.

Les stratégies de sécurité sont mises en place par le biais des paramètres de stratégie de groupe. Ainsi les avantages d'Active directory est :

- Amélioration de la tolérance de pannes pour réduire les périodes d'indisponibilité.
- Amélioration de la sécurité.
- Amélioration de la productivité des utilisateurs.
- Réduction des tâches d'administration informatique.

I.12. Conclusion :

Ce chapitre a montré des notions sur les réseaux informatiques tel que les différents types de réseau, les modèles OSI et TCP/IP. Ainsi qu'une vue brève sur les solutions de sécurité d'un réseau au sein de l'entreprise.

Le chapitre qui suit va se porter sur une étude du réseau existant au sein de l'entreprise NAFTAL BEJAIA .

CHAPITRE II :
Etude De L'Existant
(NAFTAL GPL)



NAFTAL SPA [DISTRICT GPL BEJAIA]

Introduction

L'utilisation des réseaux informatiques est une condition indispensable pour la communication entre les différents secteurs De l'entreprise. Mais il est important d'assurer la sécurité du réseau informatique et cela n'est possible qu'avec un bon outil d'administration réseau comme Active Directory, qui été le sujet traité pendant mon stage au sein de l'entreprise NAFTAL Bejaia.

II. Présentation de l'entreprise NAFTAL de Bejaia

Historique :

Issue de SONATRACH, l'entreprise de raffinage et de la distribution des produits pétroliers (ERDP) a été créée par le décret N° 80/101 du 06 avril 1981. Entrée en activité le 1er janvier 1982, elle est chargée du raffinage et de la distribution des produits pétroliers.

En 1987, l'activité raffinage est séparée de l'activité distribution et dévolue à une nouvelle entité NAFTEC.

NAFTAL est désormais chargée uniquement de la commercialisation et de la distribution des produits pétroliers et dérivés.

En 1998, elle change de statut et devient Société par actions filiale à 100% de SONATRACH.

II.1. Missions et activités de l'entreprise NAFTAL

II .1.1. Ses Missions

NAFTAL a pour mission principale, la distribution et la commercialisation des produits pétroliers sur le marché national.

Elle intervient dans les domaines:



- *de l'enfûtage des GPL*
- *de la formulation de bitumes*
- *de la distribution, stockage et commercialisation des carburants, GPL, lubrifiants, bitumes, pneumatiques, GPL/carburant, produits spéciaux.*

II.1.2. Ses Activités

Les principales activités de l'entreprise NAFTAL sont :

- ❖ la commercialisation de carburants "terre" pour la motrice essence et diesel (Essence Normale, Essence Super, Essence super Sans plomb, Gas oil/ GPL/C)
- ❖ commercialisation des pneumatiques de grandes marques dans les catégories de véhicules les plus diverses : tourisme, camionnette, poids lourds.....
- ❖ commercialisation d' une gamme complète de lubrifiants qui couvre toutes les applications du secteur automobile et industriel.

- ❖ *le traitement du gaz naturel où gaz associés.*
- ❖ *le raffinage du pétrole.*
- ❖ *la liquéfaction du gaz naturel.*

II.3.Organigramme général de l'entreprise NAFTAL Bejaia

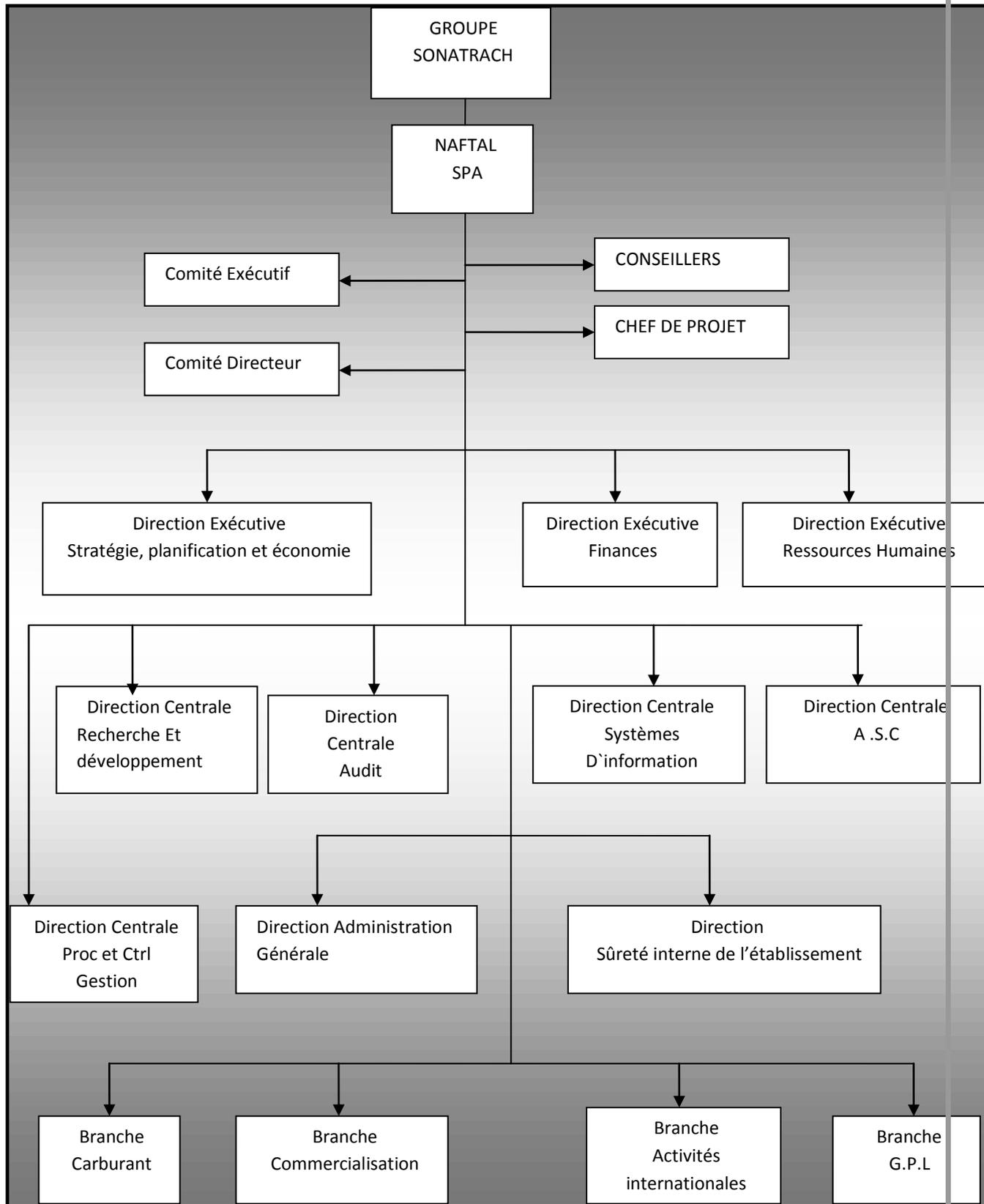


Figure II.1 . - Organigramme général de l'entreprise NAFTAL

Bejaia –

II.4. 1. Organisation de la GPL de Bejaia et ces différents départements :

La GPL de Bejaia se compose de plusieurs départements :

Informatique
commercial
comptabilité
exploitation
Technique
Personnel

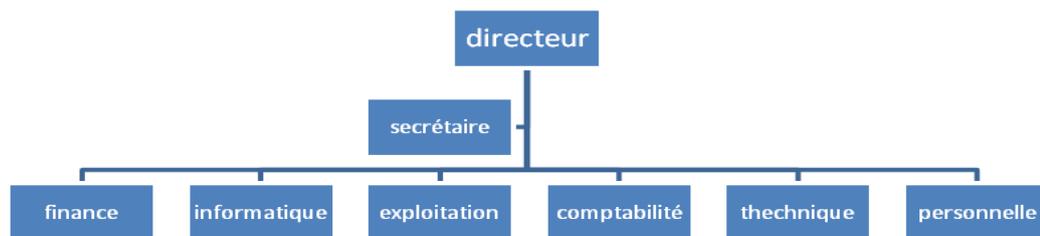


Figure II.2 - organigramme du district GPL Bejaia –

II.4.2. Le rôle de département informatique dans cette entreprise

1. **maintenance du matériel** : soit pour le côté software (installation des différents outils comme les systèmes d'exploitations et d'autres outils de gestion et de la messagerie ou bien hardware (diagnostiquer les différentes panne et leurs réparation)

2. **administration du réseau.**

II.4.3. L'architecture réseau de district GPL de Bejaia :

Le meuble de GPL de Bejaia se compose de 4 blocs séparés, dans chaque bloc se trouve un sous-réseau composé d'une armoire ou se trouve un Switch qui relie les différents ordinateurs avec un câble RJ45.

Et ces Switch sont reliés entre eux en cascade par des câbles en fibre optique .

Le serveur se trouve dans le département informatique et parmi ses services : FTP , DHCP et DNS (pour l'affectation des adresses IP automatiquement).

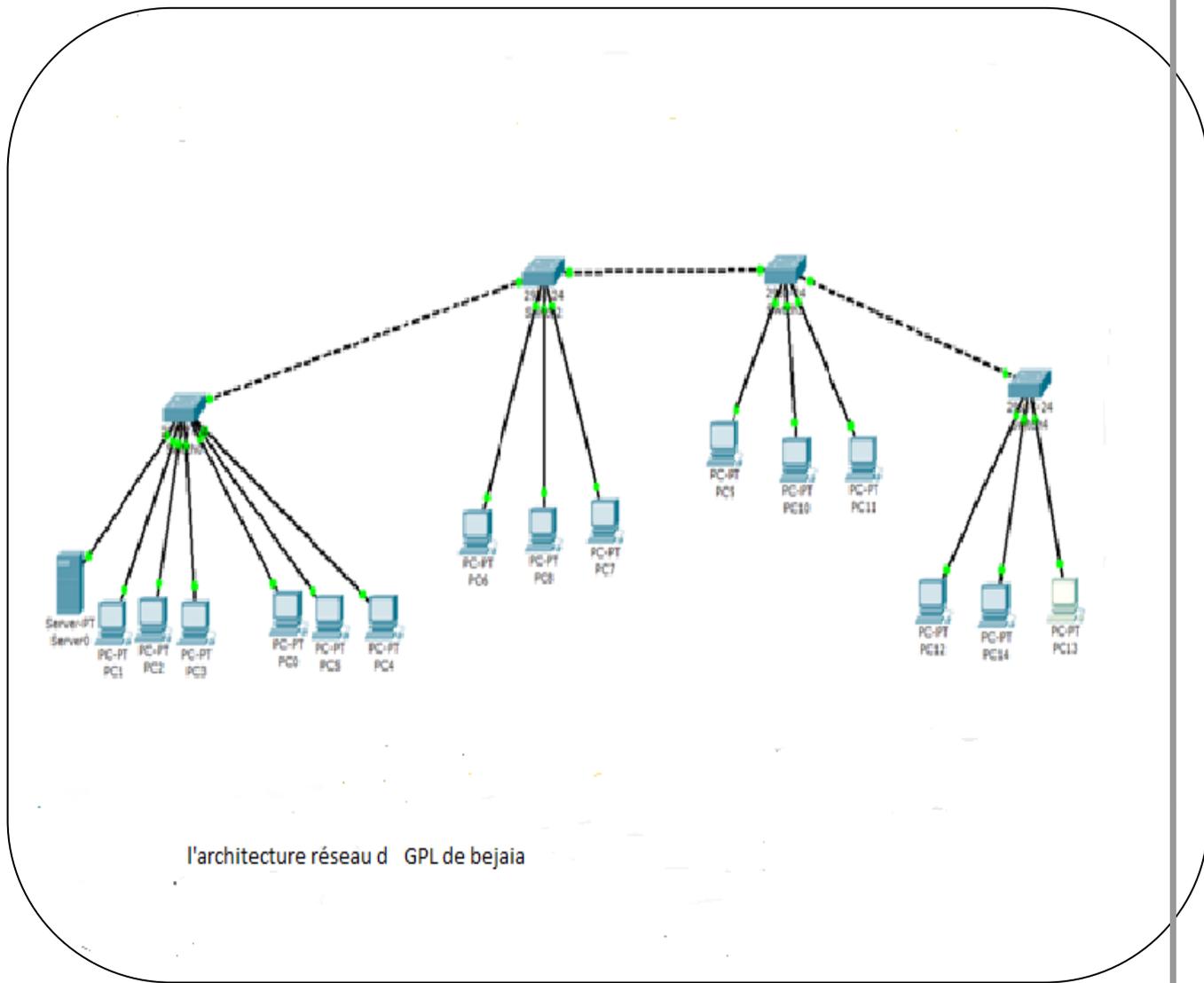


Figure II. 3 - l'architecture du réseau informatique de district GPL BEJAIA –

II.5. PARAMETRE DU SERVEUR :

NOM DU DOMAINE	DIST-BEJAIA.NAFTAL.LOCAL
----------------	--------------------------

NOM DU SERVEUR	SERV-BEJAIA
ADRESSE IP SERVEUR	10.48.148.10
MASQUE	255.255.252.0
PASERELLE	10.48.148.1
DNS	10.48.148.10
POOL D'ADRESSE IP DHCP	DEBUT 10.48.149.1 FIN 10.48.149.255
ISA SERVEUR	10.48.0.0 NON INSTALLE
MASQUE	10.48.255.255
ADRESSE IP STATIQUE	41.110.84.14
MASQUE	255.255.254.0

Figure II.1 - Tableau des paramètres serveur –

II.5.1. Présentation des outils de travail

L'entreprise NAFTAL dispose de plusieurs équipements réseau, le tableau ci-dessous montre les différents équipements qui existe dans se réseau, ainsi que leurs principaux caractéristiques.

EQUIPEMENT	N° SERIE
SERVEUR DELL POWEREDGE T610	CJKTJ4J
SWITCH CISCO 24 PORTS	FOC 1330 X0WU
SWITCH CISCO 24 PORTS	FOC 1330 X0W5
SWITCH CISCO 24 PORTS	FOC 1330 X1FV
SWITCH CISCO 24 PORTS	FOC 1330 X1AH
SWITCH CISCO 24 PORTS	FOC 1330 X1DN
SWITCH CISCO 24 PORTS	FOC 1330 X1FQ
SWITCH CISCO 24 PORTS	FOC 1330 X0SJ
SWITCH CISCO 24 PORTS	FOC 1330 X1A8

EQUIPEMENT	N° SERIE
ONDULEUR APC 450VA	AS 0920 160 632
ONDULEUR APC 450VA	AS 0918 260 560
ONDULEUR APC 450VA	AS 0920 160 684
ONDULEUR APC 450VA	AS 0920 160 629
ONDULEUR APC 450VA	AS 0920 160 630
ONDULEUR APC 450VA	AS 0920 160 635
ONDULEUR APC 450VA	AS 0920 160 694
ONDULEUR APC 450VA	AS 0920 160 659
ONDULEUR APC 450VA	AS 0920 160 597
ONDULEUR APC 450VA	AS 0920 160 734
ONDULEUR 1500 VA	AS 0926 230 425
ONDULEUR APC 450VA	AS 0918 260 484

TABLE II.2 - Equipement réseau de l'entreprise NAFTAL-

II.5.2. Les supports de transmissions

Pour relier les différents équipements qui sont utilisés dans le réseau ; NAFTAL opte pour deux types de média : le câble à paire torsadée RJ45 et la fibre optique, le tableau suivant récapitule les différentes caractéristiques de ces supports.

Désignation	Qté	UM
Prises réseaux RJ45 catégorie 6	118	U
Câble de postes souple 4 paires FTP3m catégorie 6	118	U
Fil de terre	0	M
Borne de terre	0	U
Câbles de fibre optique souple 6 brins	150m	U
Tiroir optique avec jarretières	2	UM
Connecteurs de fibre optique	0	M
Coupleur de fibre optique	4	U

Table II.3 - les supports de transmissions -

Quelques photos de la mise en place du réseau de GPL Bejaia :



- Armoire -



- Câblage-

- prise RJ 45 -

II.5.3. Gestion des utilisateurs et autorisations d'accès au réseau

Chaque employé possède un compte sur son *ordinateur* (dont les identifiants vous sont donnés à votre arrivée dans l'entreprise par le service informatique), sécurisé par un mot de passe. Lorsque l'*ordinateur* s'allume le nom d'utilisateur et le mot de passe sont demandés par le *serveur*. C'est lui qui s'occupe d'authentifier l'utilisateur et lui autoriser l'accès à son poste de travail.

Le *serveur* va également mettre à disposition des employés des dossiers partagés, accessibles à certains et pas à d'autre, selon le poste de l'employé.

Par exemple le service Comptabilité pourra mettre en commun les résultats financiers, tableaux de calculs et documents sur lesquelles plusieurs personnes travaillent en collaboration.

Ce dossier sera accessible seulement par le service comptabilité et la direction par exemple, mais pas par les autres.

Chaque service pourra avoir son propre dossier partagé. Le secrétariat pour avoir un dossier partagé avec tous les employés pour mettre à leur disposition des documents types, notes de frais...

II.6. Description du projet : La description du projet est le moyen consistant à définir les besoins de l'entreprise tout en se basant sur la distinction de ces faiblesses et de proposer d'éventuelles solutions qui remédieront à ces dernières :

II.6.1. Description des besoins

Après l'étude réalisée sur le réseau de l'entreprise NAFTAL (GPL Bejaia), on n'a constaté que le réseau district GPL Nécessite d'améliorations .en effet, la gestion des utilisateurs va devenir très difficile avec l'augmentation de nombre d'utilisateurs et des ressources partagées, Voici les principaux rôles, installé au serveur du siège de la GPL de Bejaia

- Contrôleur de domaine (Active Directory) .
- Serveur DNS : nécessaire pour le bon fonctionnement du réseau, obligatoire pour Active Directory.
- Serveur DHCP : pour attribuer les paramètres réseau automatiquement aux PC clients.
- Serveur WINS : pour permettre un bon fonctionnement des clients non XP / 2003

Les faiblesses du réseau employé dans l'entreprise NAFTAL sont principalement dues à l'absence d'un autre serveur pour la protection du réseau utilisé .en faite, l'architecture client server utilisé comporte de nombreux limites, avec le nombre des utilisateurs et des ressources partagées qui ne cesse d'augmenter, cette architecture client server nécessite la protection du serveur qui est une véritable source de tous les diffusions, nécessite un administrateur réseau compétant en informatique ;ainsi Il faut maintenir un serveur type par feu exemple ISA server pour la protection de réseau contre les menaces qui viennent d internet.

II.6.2. Solutions de sécurité d'un réseau :

Le déploiement d'un serveur d'annuaire contribue à la réduction des coûts administratifs, améliore la sécurité et offre aux utilisateurs un environnement de travail plus productif. En termes de compétitivité, les services d'annuaire constituent un élément essentiel pour les entreprises modernes. Il existe plusieurs technologies de service d'annuaire dont on peut citer :

II.6.2.1. Active directory

Active Directory vous permet de gérer vos ressources réseau de manière simple et centralisée. Cette gestion s'appuie sur la structure physique et logique de l'annuaire Microsoft. La structure physique concerne votre placement des contrôleurs de domaine, le contrôleur de

domaine eux-mêmes, les sites Active Directory, et bien d'autres choses encore. La structure logique, quant à elle, correspond à toute la partie logicielle et de structuration. On pourra notamment y intégrer les objets, les unités d'organisation (UO / OU), les domaines, les arborescences de domaine ou encore les forêts Active Directory. Pour créer ces objets logiques, Active Directory va se baser sur le schéma Active Directory. En effet, lorsque vous allez créer un objet, celui-ci va être validé ou non selon les informations que vous lui affectez avant d'être écrit dans la base Active Directory. [10]

II.6.2.2. Apple open Directory

Mac OS X server intègre open directory, Ce service d'annuaire et d'authentification réseau facile à employer permet de bénéficier d'information centralisée. Le serveur Open directory sur Open LDAP, le serveur LDAP Open source le plus répandu, et fournit des services d'annuaire pour mac ainsi que pour les environnements hétérogènes. [11]

II.6.2.3. Novell eDirectory server

C'est un éditeur de logiciel regroupant une vaste communauté de développeurs open sources, Novell eDirectory est un service d'annuaire LDAP fonctionnant sur des plateformes (linux, NetWare, Windows, ...) . [12]

II.6.2.4. Mandriva Directory server MDS

Produit développé par Lin box FAS (Free and Alter Soft) , la première version de MDS est la 2.10 ; elle est sortie avec une tout nouvelle interface adapté à la charte graphique de man driva. [12]

II.6.3. Le choix de la solution à entreprendre

Active directory est un service d'annuaire LDAP très répondu depuis son lancement , grâce à son caractère évolutif ,fiable ,souple et sécurisé ,mon choix est porté sur Active

Directory comme annuaire . de plus tout les services critiques du réseau fonctionnent sous Windows.

II.6.4. Les caractéristiques d'Active Directory Avec Windows server, active directory est devenu bien autre chose qu'un simple modèle de domaine de Windows, en voici les caractéristiques les plus répondues :

-Evolutivité : Active directory autorise des millions d'objets par domaine. Active directory permet de faire évoluer l'annuaire en fonction des exigences de l'activité et du réseau.

-Simplicité d'administration : Active directory repose sur des structures organisationnels hiérarchiques, celle –ci facilitent le contrôle des privilèges d'administration et d'autre paramètres de sécurité ; pour un utilisateur cela lui permet de localiser facilement des ressources réseau tel que les fichiers et les imprimantes.

- Intégration au DNS : Pour localiser les contrôleurs de domaines, les clients Active directory utilisent le DNS .Les zones DNS principales peuvent être stockées dans Active directory, l'ors de l'utilisation d'un service DNS Windows server ; autorisant la réplication vers d'autre contrôleurs de domaine Active directory . [16]

-Trafic LDAP signé et crypté : par défaut, les outils Active Directory signent et cryptent tous le trafic LDAP. Cela garantie que les données n'ont pas subie d'altération, et qu'ils proviennent d'une source connue.

-Souplesse et sécurité de l'authentification et des permissions : Active directory prend en charge plusieurs protocoles d'authentifications, comme Ker béros, SSL (Secure Socket Layer), ...

II. 6.5. Structure d'Active directory

II.6.5. 1. Domaines

Un domaine Active Directory (AD) est la principale frontière logique dans un annuaire. Pris séparément, un domaine AD ressemble beaucoup à un domaine NT. Les utilisateurs et les ordinateurs sont tous stockés et gérés dans les limites qu'il définit. Les domaines AD servent de limites de sécurité pour les objets et contiennent leurs propres stratégies de sécurité. Par exemple, chaque domaine peut appliquer aux utilisateurs des stratégies de mots de passe différentes. Un domaine étant une organisation logique d'objets, il peut aisément s'étendre sur plusieurs emplacements physiques.

Un domaine regroupe des ordinateurs, des périphériques, des utilisateurs. C'est une sorte de zone sécurisée, sur laquelle on ne peut pénétrer que quand on a été authentifié par le Contrôleur de Domaine.

II.6.5. 2. Arbres de domaines

Un arbre Active Directory est composé de plusieurs domaines reliés par le biais transitifs bidirectionnels, qui partagent un schéma et un catalogue global communs.

II.6.5. 3. Forêts

Une forêt est un groupe d'arbres de domaines interconnectés. Des approbations implicites existent entre les racines des arbres d'une forêt. Si tous les domaines et arbres de domaines ont en commun un même schéma et un même catalogue global, ils ne partagent en revanche pas le même espace de noms.

La structure d'Active Directory lui permet de gérer de façon centralisée des réseaux pouvant aller de quelques ordinateurs à des réseaux d'entreprises répartis sur de multiples sites.

II.6.6. L'objectif global du projet :

Après avoir étudié le réseau, Et choisit un annuaire Active directory, on va Tracer les objectifs et les étapes à suivre pour mettre en œuvre l'outil choisit .pour cela on a opté pour le plan suivant :

- La construction d'une infrastructure à base d'Active directory sous Windows 2003 Server.
- La création des domaines et sites , ainsi que les différentes stratégies de groupes .
- Création d'un s.réseau sous windows xp et puis le partage des fichiers et le partage d imprimantes.
- la gestion des utilisateurs au sein de l'entreprise et les autorisations d'accé au différentes ressources.

II.7. Conclusion

L'étude de l'existant nous à permet de ce familiariser avec le réseau actuel de NAFTAL et de l'étudier assez profondément et c'est se qui nous à permet de voir ses faiblesses, et conduit à proposé la solution pour palier à ces derniers.

Le chapitre suivant va être concrétisé à la description de la réalisation des différentes étapes, à savoir l'installation du matériel et de logiciel Active Directory et la configuration des différents services.

CHAPITRE III :

Configuration

III.1. Introduction

Ce chapitre sera consacré à la mise en œuvre et déploiement d'active directory au sein l'entreprise NAFTA, cette partie concerne les différents outils à utilisées plus particulièrement Windows 2003 server et puis définition des différents bases d'active directory à savoir les utilisateurs et groupes ,les sites et domaines .et puis je passe à la description des étapes d'installation et de configuration des différentes services à savoir DNS,DHCP ;

III.2. Présentation de Windows server 2003

Windows server 2003 est un système d'exploitation orienté serveur développé par Microsoft. Présenté le 24 avril 2003 comme le successeur de Windows serveur 2000, il est considéré par Microsoft comme étant la pierre angulaire de la ligne de produits serveurs professionnels Windows server système. Une version évoluer intitulée Windows server 2003 R2 à été finalisé le 6 décembre 2005. Son successeur, Windows Server 2008 est sortie le 4 février 2008.

Selon Microsoft, Windows Server 2003 est plus évolutif et fournit de meilleures performances que son prédécesseur Windows Server 2000.

III.2.1. La famille Windows server 2003

Héritant de la fiabilité de Windows 2000 server, les produits Windows 2003 Server intègrent une centaine d'améliorations demandées par les utilisateurs ; et représente une meilleure plateforme pour la mise en œuvre et développement .elle offre la fiabilité et la facilité d'administration.

Les produits de Windows 2003Server améliorent la sécurité grâce à internet information services 6.0, qui intègre des fonctionnalités de restriction d'accès et de sécurisation qui facilite la création, l'administration et l'exécution.

III.2.2. installation Windows server 2003

Windows server 2003 c'est le système d'exploitation installé au niveau de cette entreprise (NAFTAL) ; c'est un produit professionnel dont l'administration nécessite des connaissances

On commence par les étapes d'installation :

1 - Préparation

Nom du serveur, adresse IP, configuration matérielle, logiciels à installer, solutions de sauvegarde et anti-virus...

2 - Installation depuis le CD

Démarrage du serveur sur le CD d'installation, on suit l'assistant et c'est terminé. Puis il faut activer le produit par internet.

3 - Protection du serveur

Avant de faire quoique ce soit et d'exposer le serveur à des vulnérabilités, il convient de le protéger, on installant toutes les mises à jour nécessaires.

Ensuite il faut installer un logiciel Anti Virus, celui-ci devra être conçu pour un serveur, pas une station de travail.

5 - Installation des services supplémentaires

Voici les principaux rôles, installé au serveur du siège de la GPL de Bejaia

- Contrôleur de domaine (Active Directory) ;
- Serveur DNS : nécessaire pour le bon fonctionnement du réseau, obligatoire pour Active Directory.
- Serveur DHCP : pour attribuer les paramètres réseau automatiquement aux PC clients.
- Serveur WINS : pour permettre un bon fonctionnement des clients non XP / 2003

6 - Définition des stratégies systèmes

Afin de gérer la sécurité, mais aussi d'automatiser les choses, et si votre serveur est contrôleur de domaine (Active Directory) vous devez maintenant définir précisément les stratégies systèmes.

Combiné aux stratégies de groupes, Active directory permet une gestion des postes distants de façon complètement centralisée.

Si on souhaite utiliser Active Directory, DNS est très important. Le premier serveur Active Directory devra aussi faire office de DNS et les clients de ce domaine devront envoyer leurs requêtes à ce serveur, même si ceux ci doivent accéder à Internet (dans ce cas il faut configurer un redirecteur sur le serveur DNS.

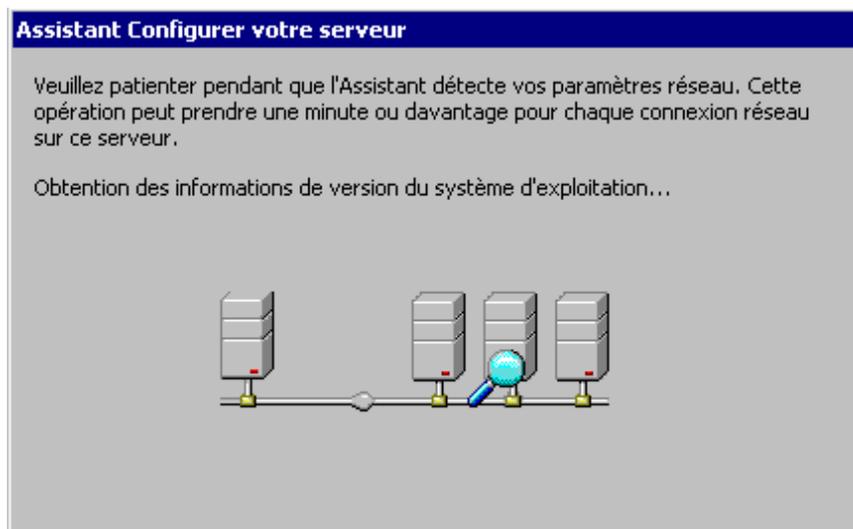


Figure III.1 - Définition des stratégies systèmes-

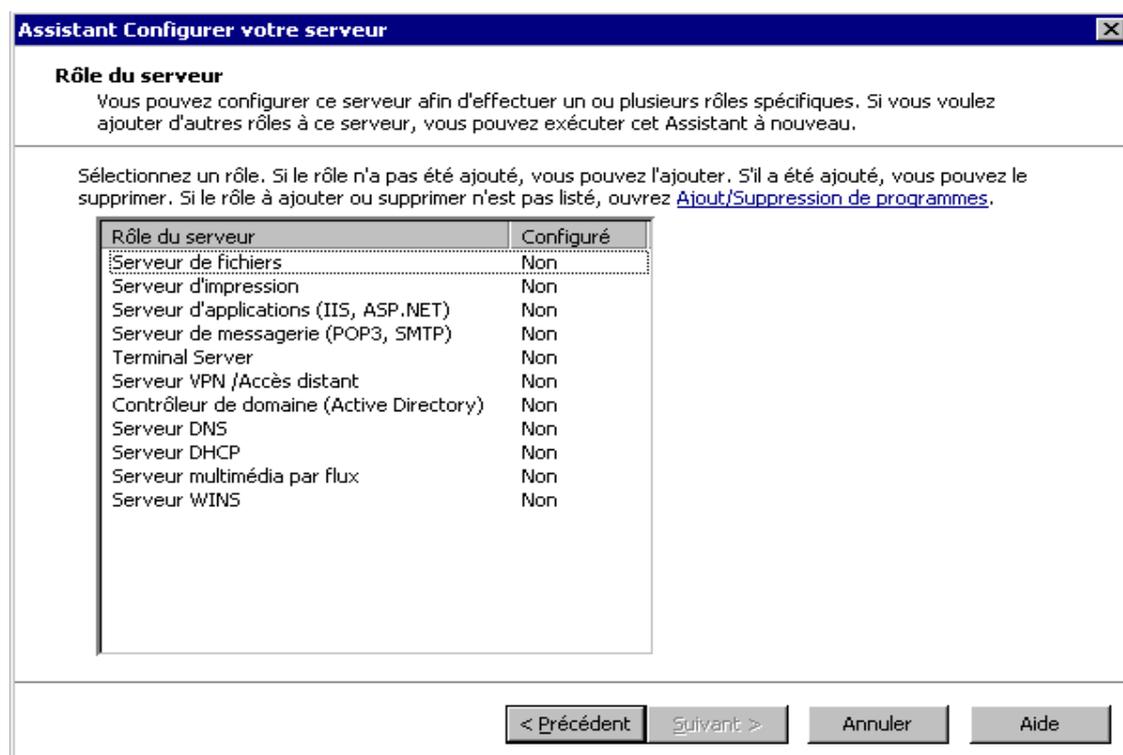


Figure III.2 – configuration du server -

III.3 .Installation d'Active Directory sous Windows server 2003

Active Directory Service (ADS) est le service LDAP implanté par Windows 2003 Server pour la gestion d'annuaires. Il est utilisé pour toutes les tâches d'administration demandant une forte implantation réseau et en particulier pour la création de domaines.

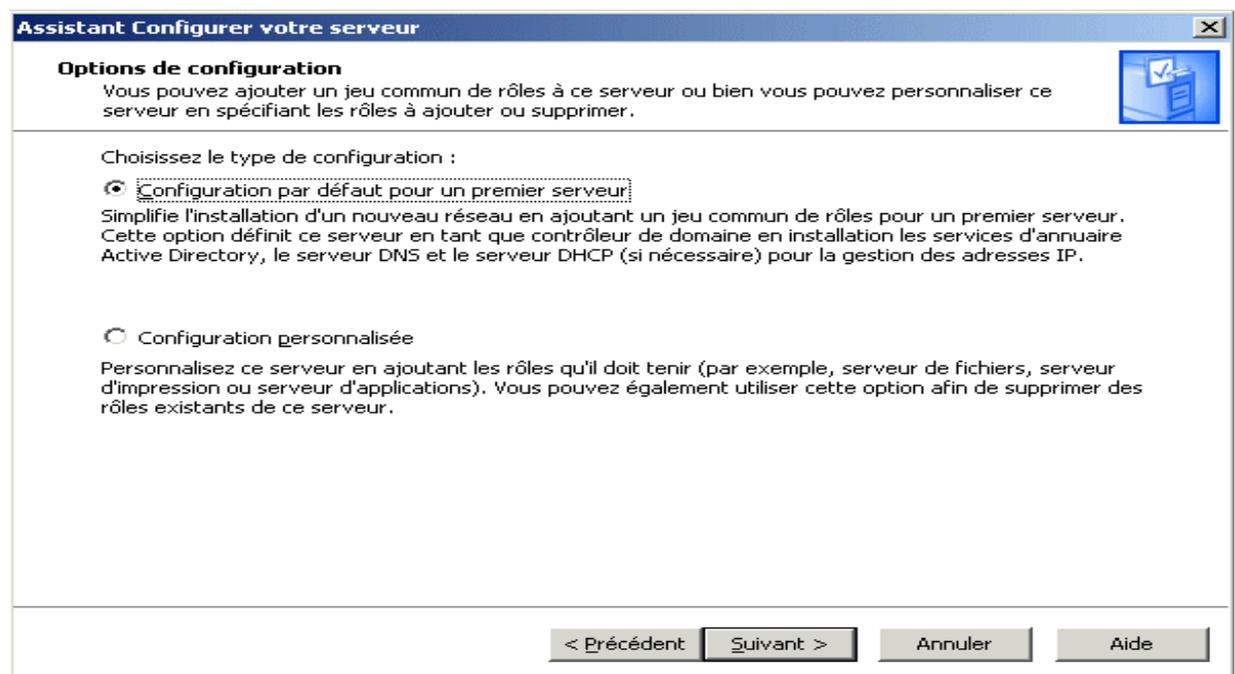
De base, ADS n'est pas installé sous Windows 2003. Au cours de son installation, un domaine devra être défini (exemple NAFTAL. Local), La machine d'installation pourra prendre différents rôles:

- premier contrôleur d'un nouveau domaine dans une nouvelle forêt,
- premier contrôleur d'un domaine enfant d'un domaine existant,
- premier contrôleur d'un nouveau domaine dans une forêt existante,
- contrôleur supplémentaire au sein d'un domaine existant

Pour installer Active Directory on utilise l'outil d'administration "Gérer votre serveur" qui simplifie l'installation sans poser les questions les plus pointues. Il installe et configure à minima AD, DNS et DHCP pour un nouveau domaine dans une nouvelle forêt.

Menu « Démarrer » .Tous les Programmes. Outils d'administration.

L'assistant "Gérer votre serveur», puis ajouter ou supprimer des rôles et on choisie configuration par défaut pour un premier serveur comme le montre la figure suivante :



Fenêtre III.3 -le choix du type de configuration pour un premier serveur-

Puis c'est la spécification d'un nom de domaine active directory, dans mon exemple j'ai pris comme domaine « NAFTAL. Local ».comme le montre la figure suivante :

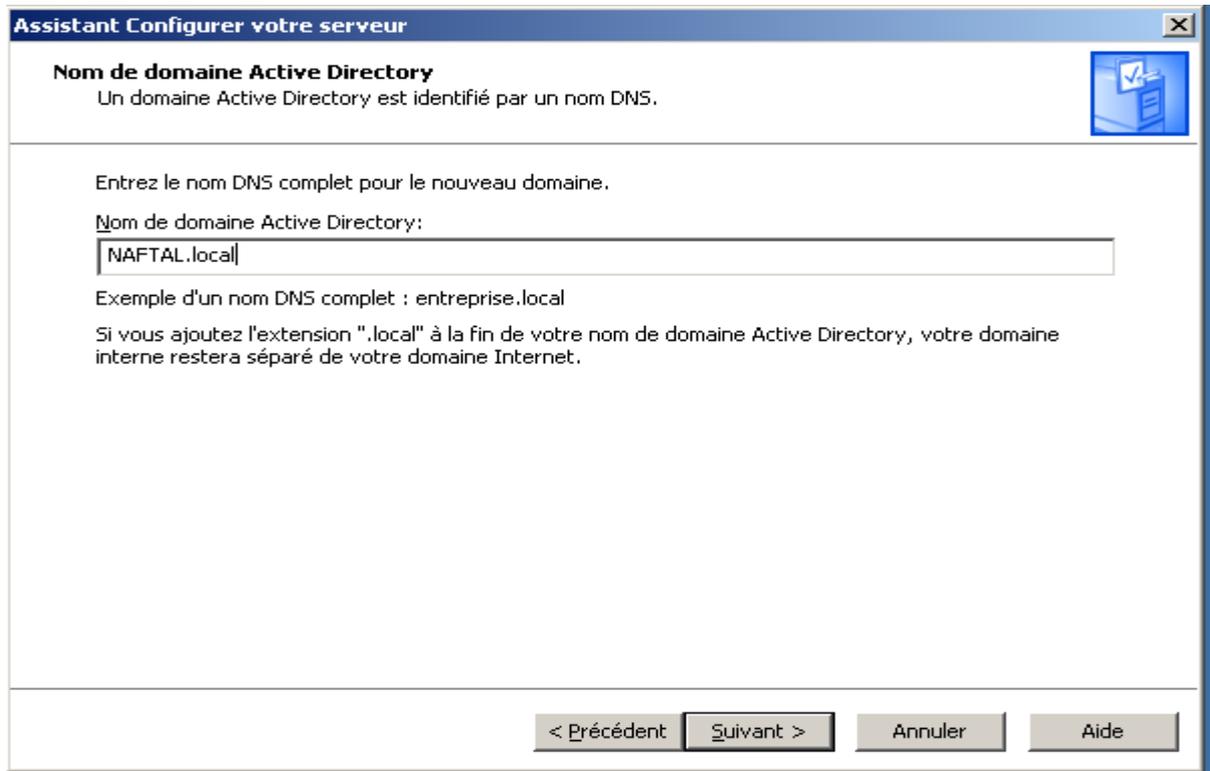


Figure III.4 - attribution d'un nom de domaine -

A la fin d'installation d'active Directory, on peut ajouter de différents rôles selon le besoin de l'administrateur réseau comme illustré dans la figure suivante :



Figure III.5 - Etablissement d'un rôle pour le serveur -

III.3.1.Reconnaissance des objets Active Directory

Les objets décrits dans le tableau suivant sont créés pendant l'installation du service Active Directory.

Icône	Dossier	Description
	Domaine	Le nœud racine du composant logiciel enfichable représente le domaine administré.
	Ordinateurs	Contient tous les ordinateurs Windows NT, Windows 2000, Windows XP et Windows Server 2003 qui font partie du domaine, ordinateurs exécutant Windows NT versions 3.51 et 4.0 inclus. Si vous procédez à une mise à niveau à partir d'une version antérieure, Active Directory migre le compte d'ordinateur vers ce dossier. Vous pouvez déplacer ces objets.
	Système	Contient des informations sur les systèmes et services Active Directory.

Comme on peut utiliser Active Directory pour créer les objets suivants.

Icône	Objet	Description
	Utilisateur	Un objet utilisateur est un objet principal de sécurité de l'annuaire. Un utilisateur peut se connecter au réseau avec ces informations d'identification et disposer d'autorisations d'accès.
	Contact	Un objet contact est un compte qui ne dispose d'aucune autorisation de sécurité. Vous ne pouvez pas vous connecter au réseau en tant que contact. Les contacts représentent les utilisateurs externes dans le cadre de la messagerie.
	Ordinateur	Un objet qui représente un ordinateur sur le réseau. Pour les stations de travail et serveurs Windows NT, il s'agit du compte d'ordinateur.
	Unité d'organisation	Les unités d'organisation (UO) sont utilisées comme conteneurs pour organiser de façon logique des objets d'annuaire tels que les utilisateurs, les groupes et les ordinateurs. Elles sont comparables aux dossiers que vous utilisez pour organiser les fichiers sur votre disque dur.
	Groupe	Les groupes peuvent contenir des utilisateurs, des ordinateurs et d'autres Ils simplifient la gestion d'un grand nombre d'objets.

	Dossier partagé	Un dossier partagé est un objet réseau qui a été publié dans l'annuaire.
	Imprimante partagée	Une imprimante partagée est une imprimante réseau qui a été publiée dans l'annuaire.

Table III.1 - reconnaissances des objets active directory –

III.4. La configuration d'Active Directory

III.4.1. Contrôleur de domaine (Active directory)

Ce rôle met en disposition de l'administrateur de différents services permettant de créer et de gérer les utilisateurs et les ordinateurs,

de définir et de modifier les domaines et les sites appropriés.

III.4.2. création d'une unité d'organisation

Pour créer une unité organisationnelle il suffit faire un clique droit sur notre domaine

->**nouveau** -> **unité d'organisation** comme illustré ci dessus :

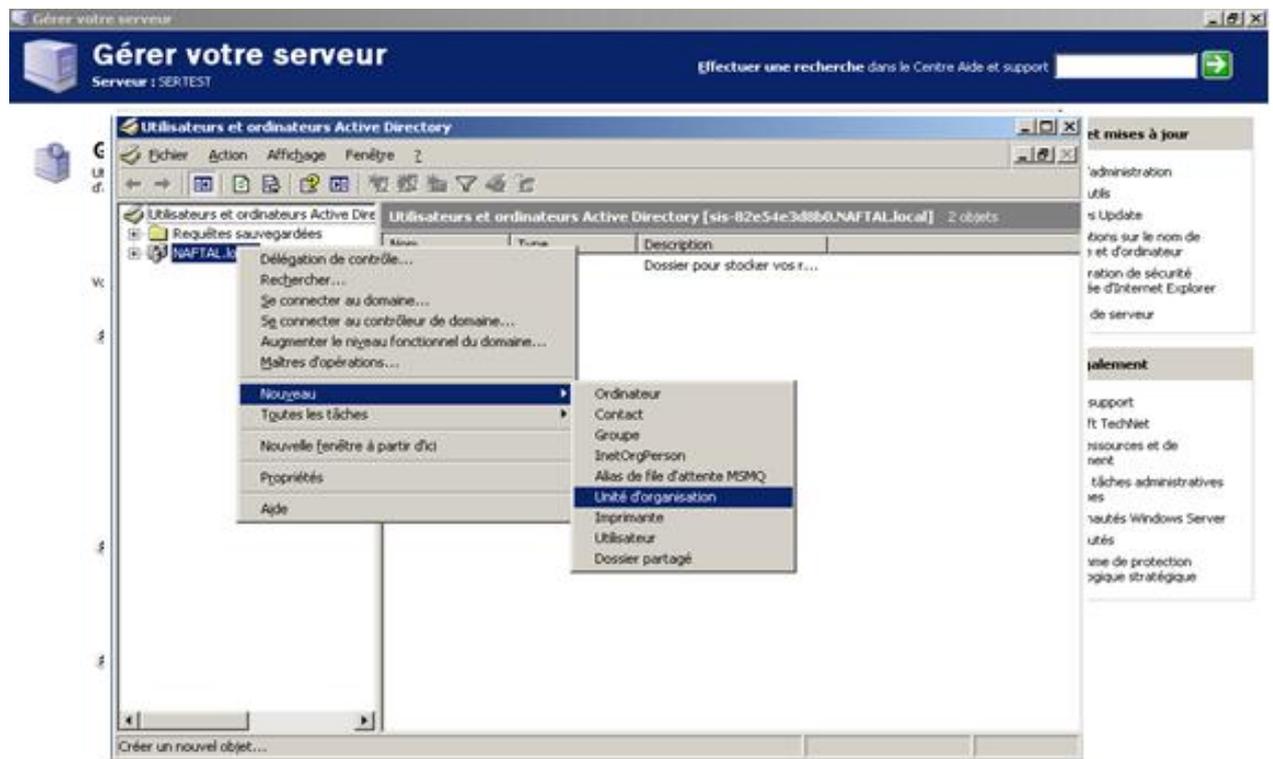


Figure III.6 - Ajout d'une unité d'organisation -

Cette procédure nous permet de regrouper des ordinateurs ou des utilisateurs dans une seule unité afin de pouvoir leur appliquer des procédures et des stratégies de groupes.

Dans notre cas on a nommé l'Unité Organisation racine : **GPL** ; comme se figure si dessous

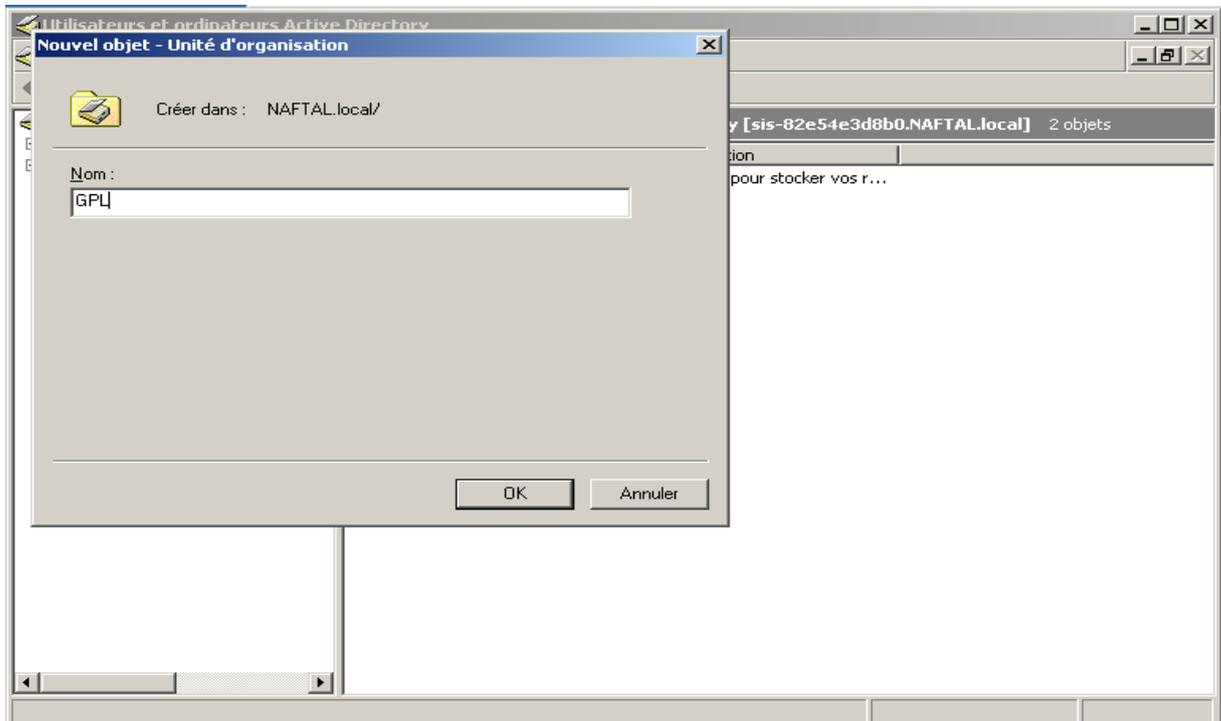


Figure III.7 - Création de l'unité GPL -

Ensuite, on a créé deux autres unités où chaque unité représente un département on a choisi **dept infom** (informatique) et **dept comerc** (commercial). Et puis créé et déplacé les utilisateurs et les ordinateurs sur lesquels on veut appliquer des stratégies de groupes, comme le montre l'image suivante :

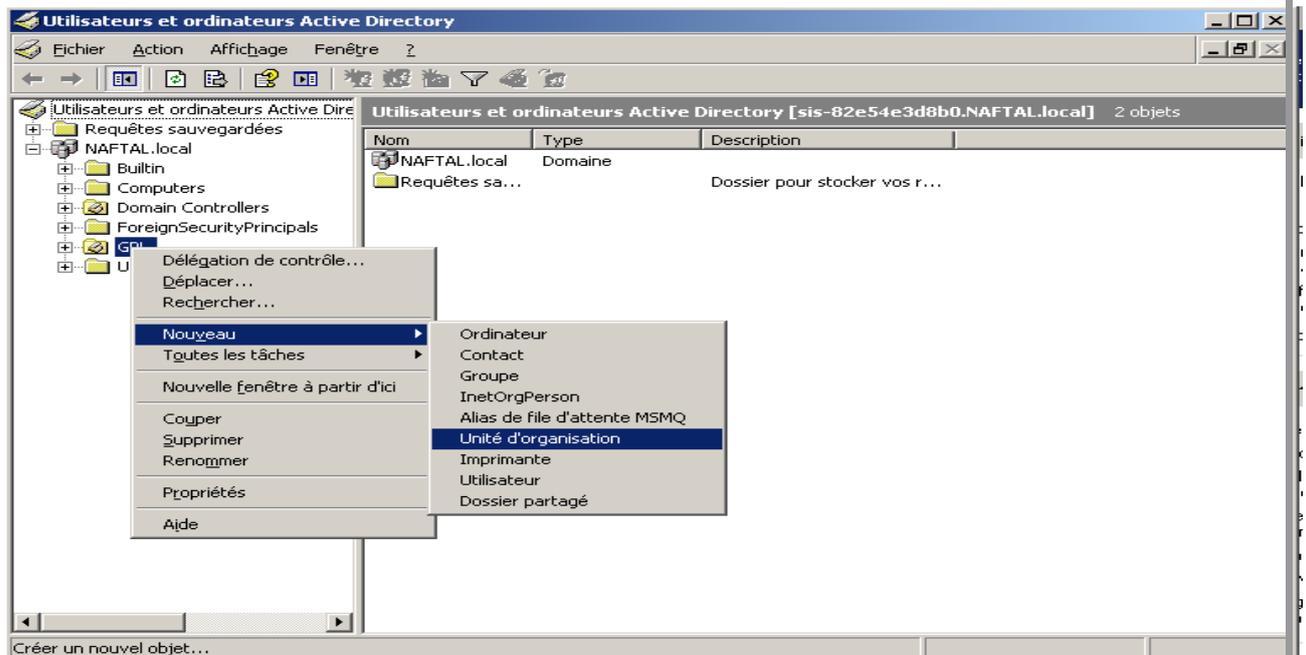


Figure III.8 - création des unités qui représentent les deux départements -

Une fois que l'utilisateur est appartenant à un département dans le contrôleur de domaine on doit l'ajouter à l'unité d'organisation pour lui attribuer des droits d'accès ainsi le partage de fichier et autres ressources a condition qu'il soit ajouté au domaine (dans ce cas NAFTA.L. Local). Pour cela voici les deux unités créées :

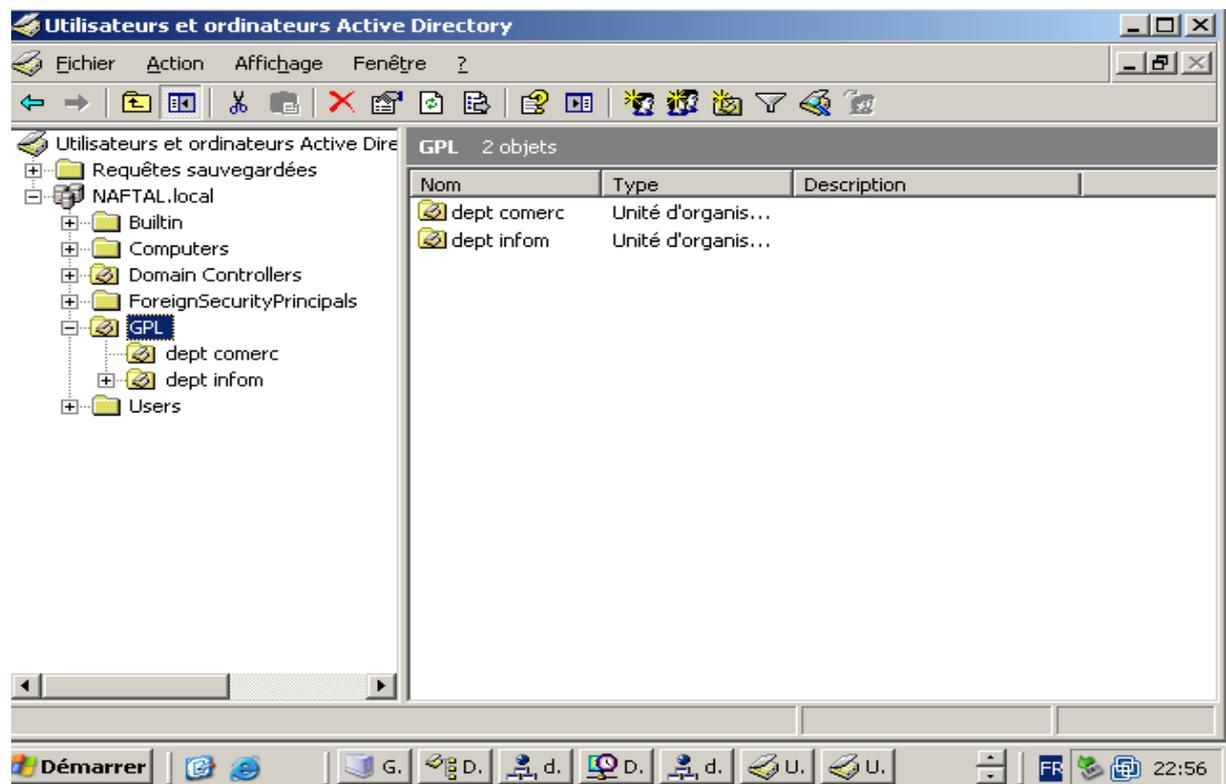


Figure III.9 – les objets créés au sein de la GPL -

III.4.3. Création d'un utilisateur dans active directory

Pour ajouter des utilisateurs à gérer dans active directory, on doit suivre les étapes suivantes :

Gérer des utilisateurs et des ordinateurs -> users -> nouvel utilisateur, puis on remplit les champs qu'il faut comme le montre la figure suivante :

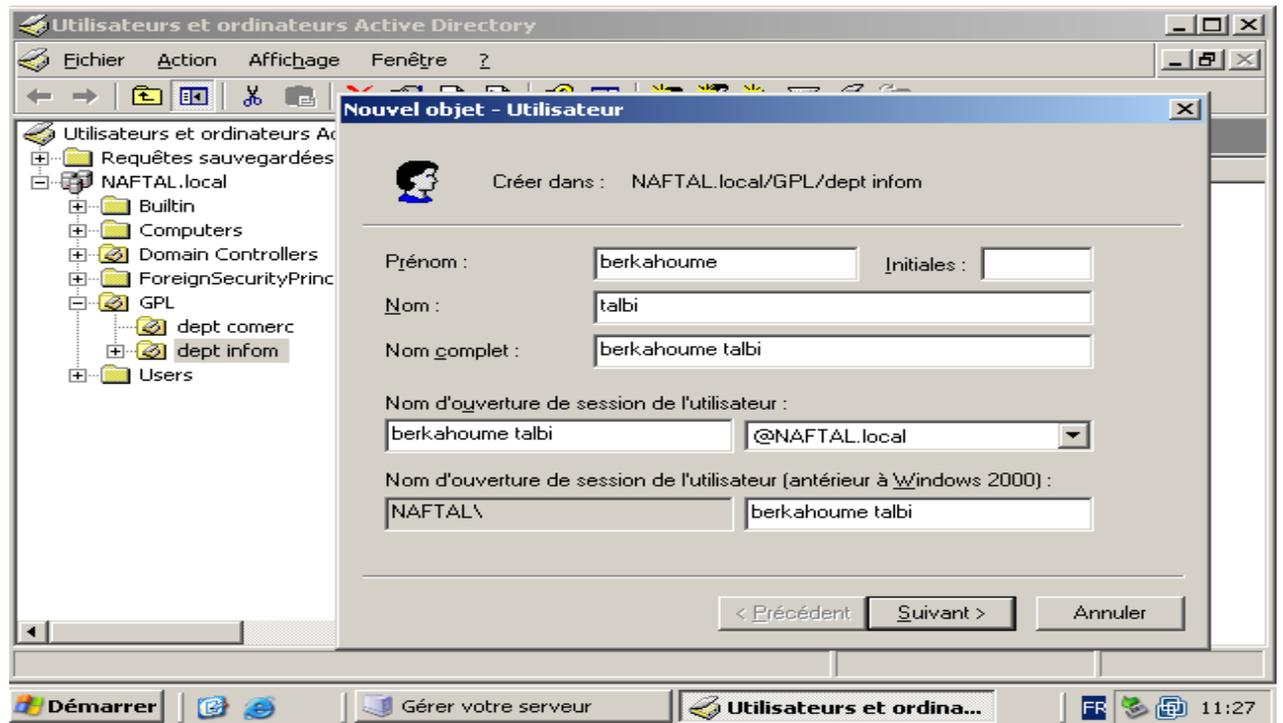


Figure III.10 - Création d'un utilisateur dans active directory

Et puis une fenêtre apparaît demande de spécifier un mot de passe pour cette utilisateur et en valide sur ok, la figure suivante doit apparaitre :

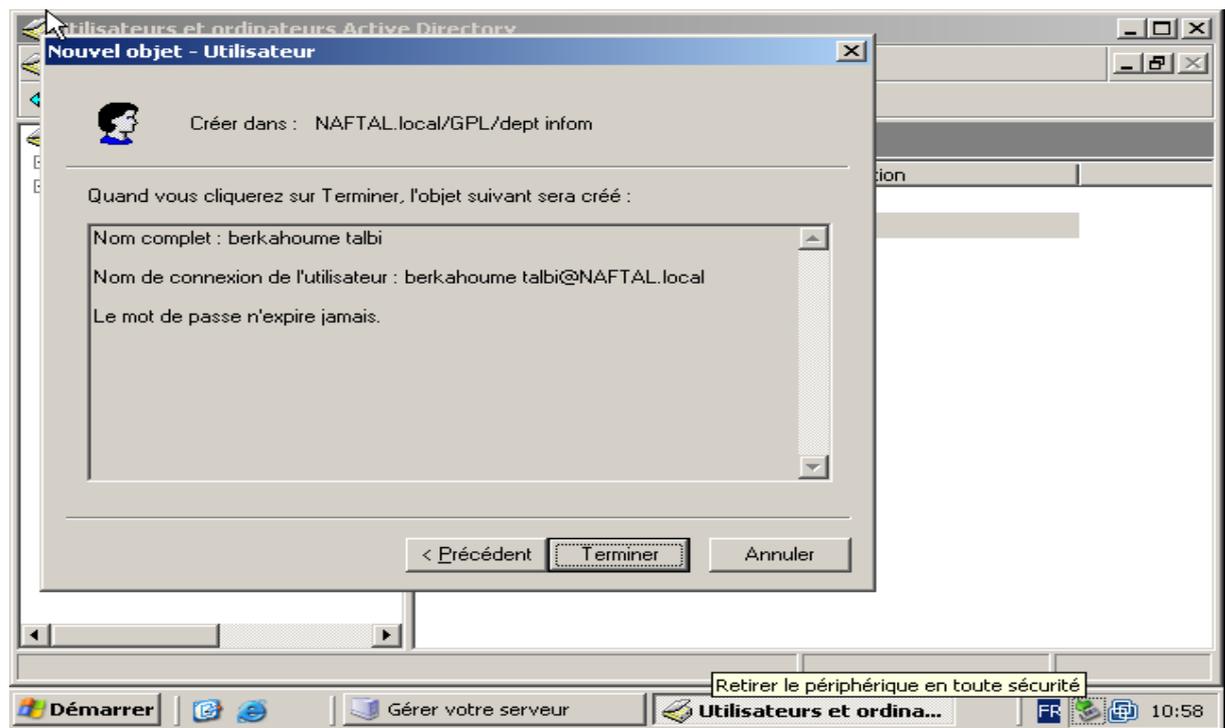


Figure III.11 - confirmation et validation mot de passe -

Pour chaque départements on a créer des utilisateurs et attribuer de mode passe pour pouvoir leurs spécifier des comptes utilisateurs et des autorisations d'accès au différentes ressources partagées de l'entreprise. Comme se figure sous les tableau suivants :

Utilisateurs	Mot de pass
Toula hassaine	Univ-06-inf 3
Stagiere informatique	Univ-06-inf 2
Talbi berkahoume	Univ-06-inf 1

Table III .2 - Mot pass des Utilisateurs créer pour departement informatiques –

Utilisateurs	Mot de pass
User 1 bika	Univ-06-com 1
Bellache tiwiza	Univ-06-com 2
Anouar idri	Univ-06-com 3

Table III.3 - Mot pass des Utilisateurs créer pour departement commercial –

Voici la liste des utilisateurs et ordinateurs crée à chaq'un des deux départements :

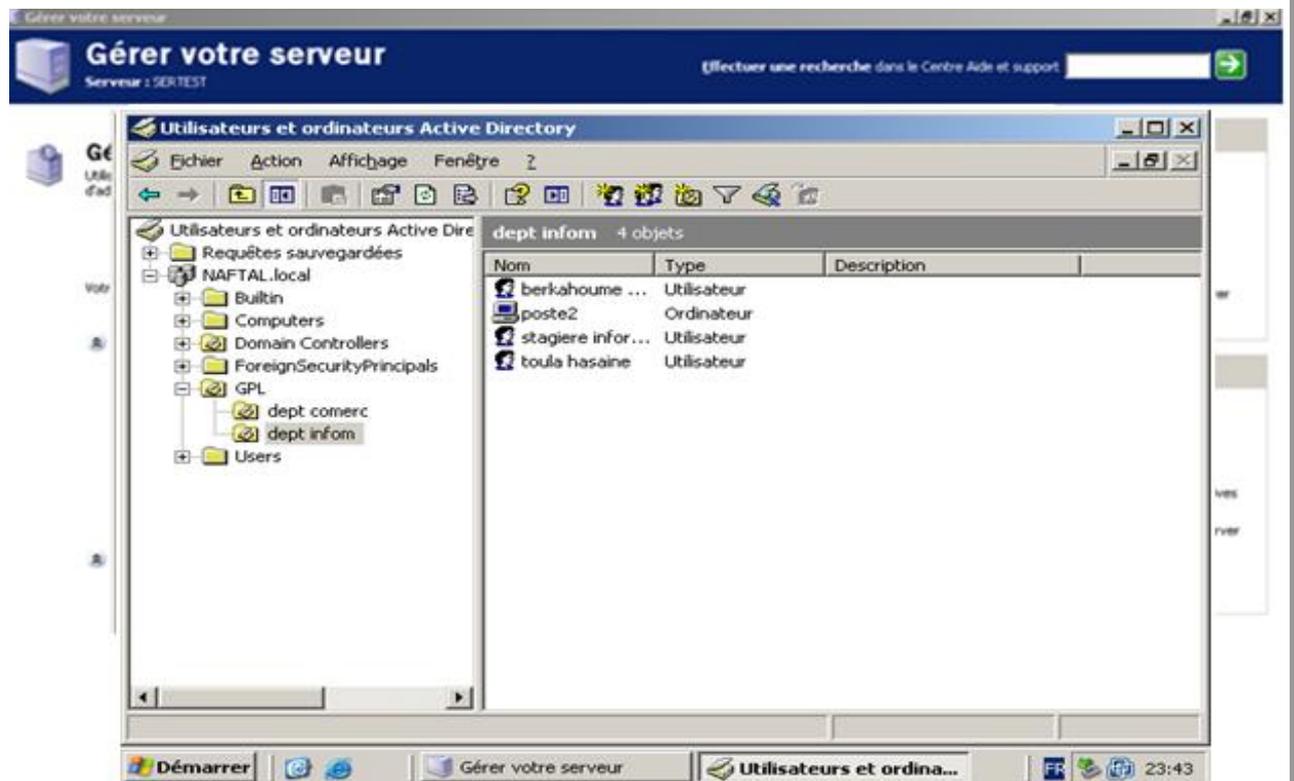


Figure III.12 - liste des utilisateurs et ordinateurs crée au département informatique -

les même étapes pour la création des utilisateurs dans le deuxième département qui est le département commercial, la figure suivante explique sa :

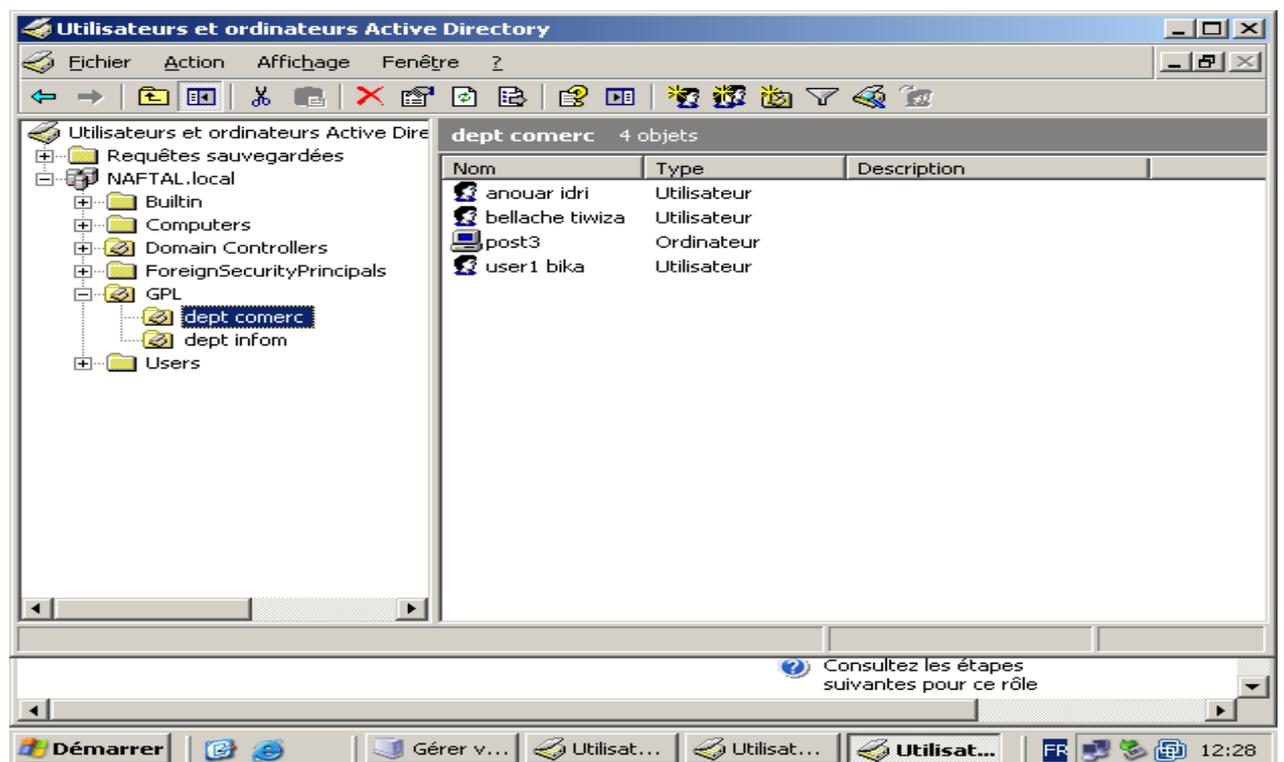


Figure III .13 - utilisateurs et ordinateurs crée au département commercial –

III.4.4. Gestion des utilisateurs et autorisations d'accès au ressources au sein de l'entreprise

Chaque employé possède un compte sur son *ordinateur* sécurisé par un mot de passe. Lorsque l'*ordinateur* s'allume le nom d'utilisateur et le mot de passe sont demandés par le *serveur*. C'est lui qui s'occupe d'authentifier l'utilisateur et lui autoriser l'accès à son poste de travail.

Le *serveur* va également mettre à disposition des employés des dossiers partagés, accessibles à certains et pas à d'autre, selon le poste de l'employé. Soit administrateur du domaine qui à l'accès à tout et à la possibilité de modifier les données par contre utilisateurs du domaine à le droit seulement de consulté les données mais pas les modifier ;

Chaque service pourra avoir son propre dossier partagé.

III.4.5. Rendre un utilisateur administrateur du domaine

Clique droit sur le nom de l'utilisateur choisit -> *propriété* ->

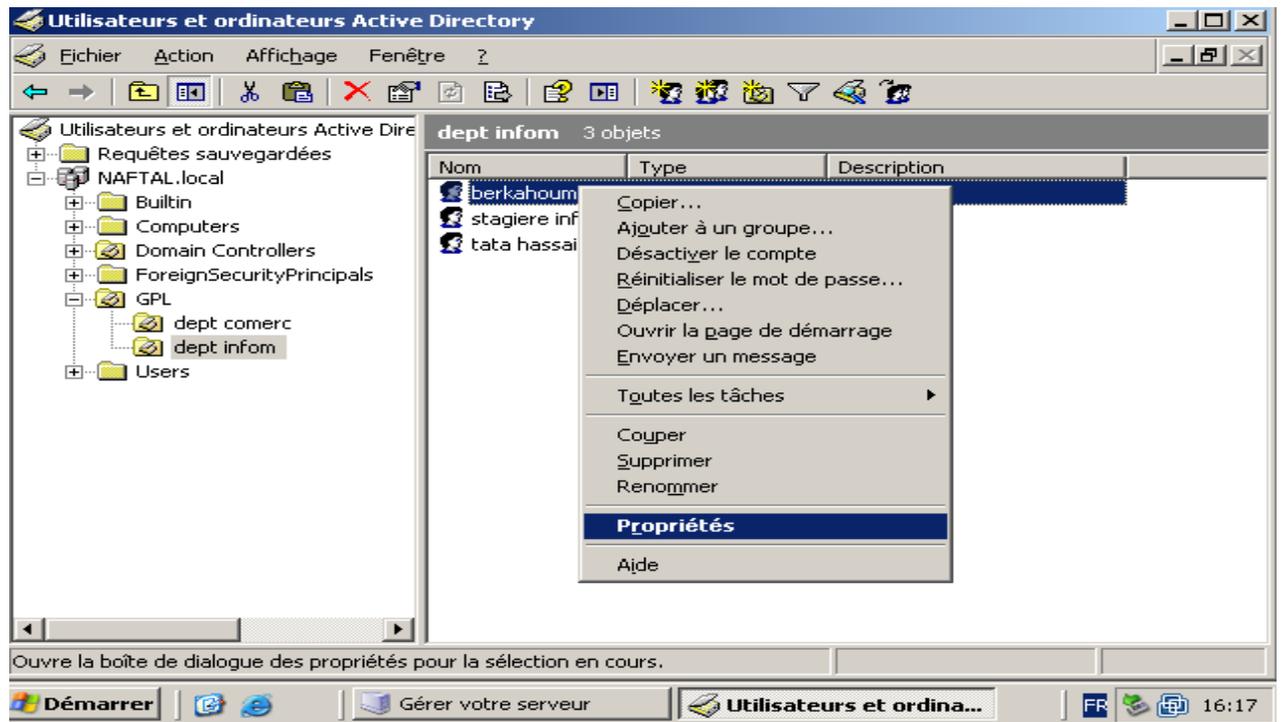


Figure III.14 - rendre un utilisateur administrateur du domaine -

La fenêtre suivante va apparaître ; elle donne une description sur les propriétés de l'utilisateur choisit comme si dessous :

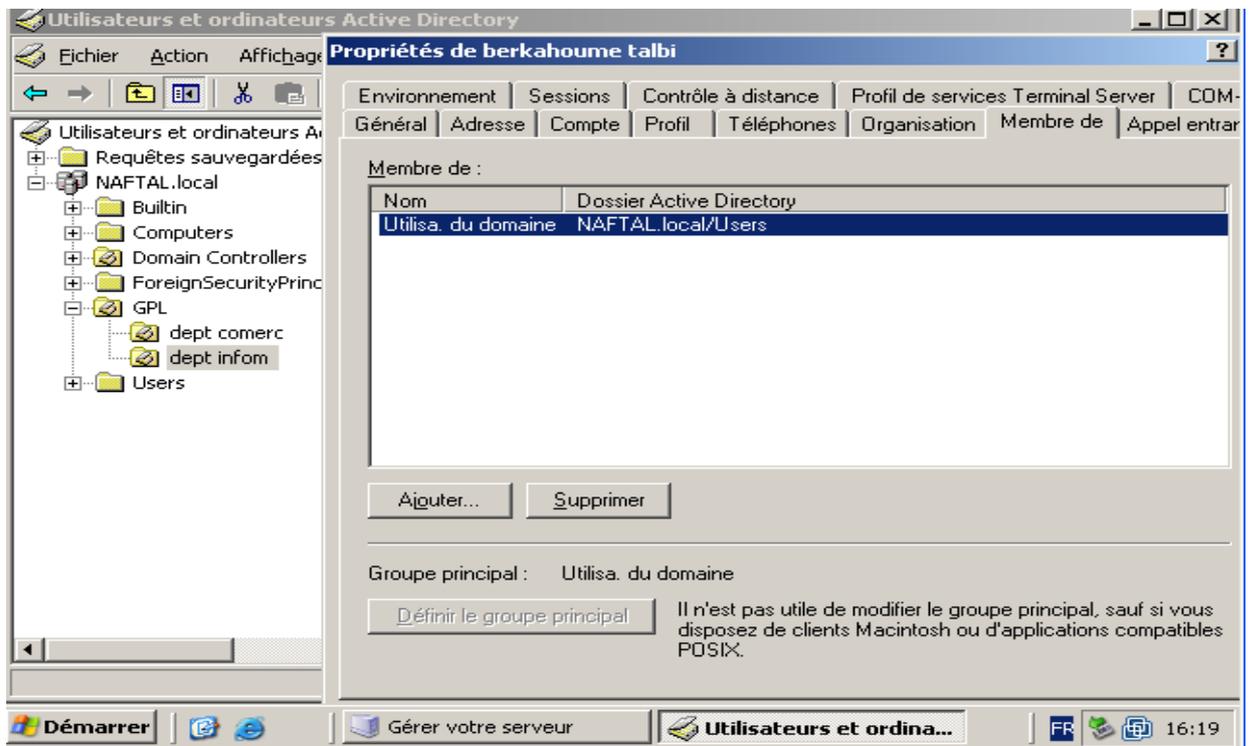


Figure III.15 – propriété de l'utilisateur talbi –

on clique sur le bouton membre de -> ajouter ->avancé

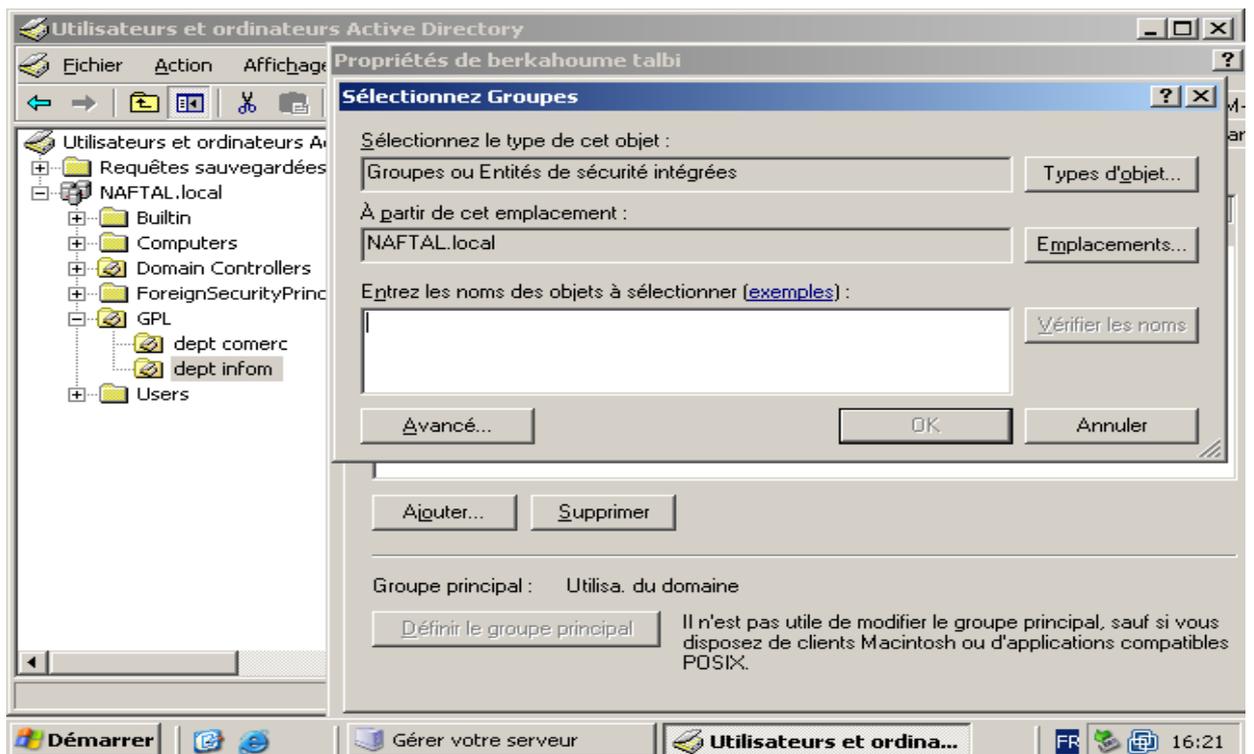


Figure III.16 - Ajout de propriété à l'utilisateur talbi -

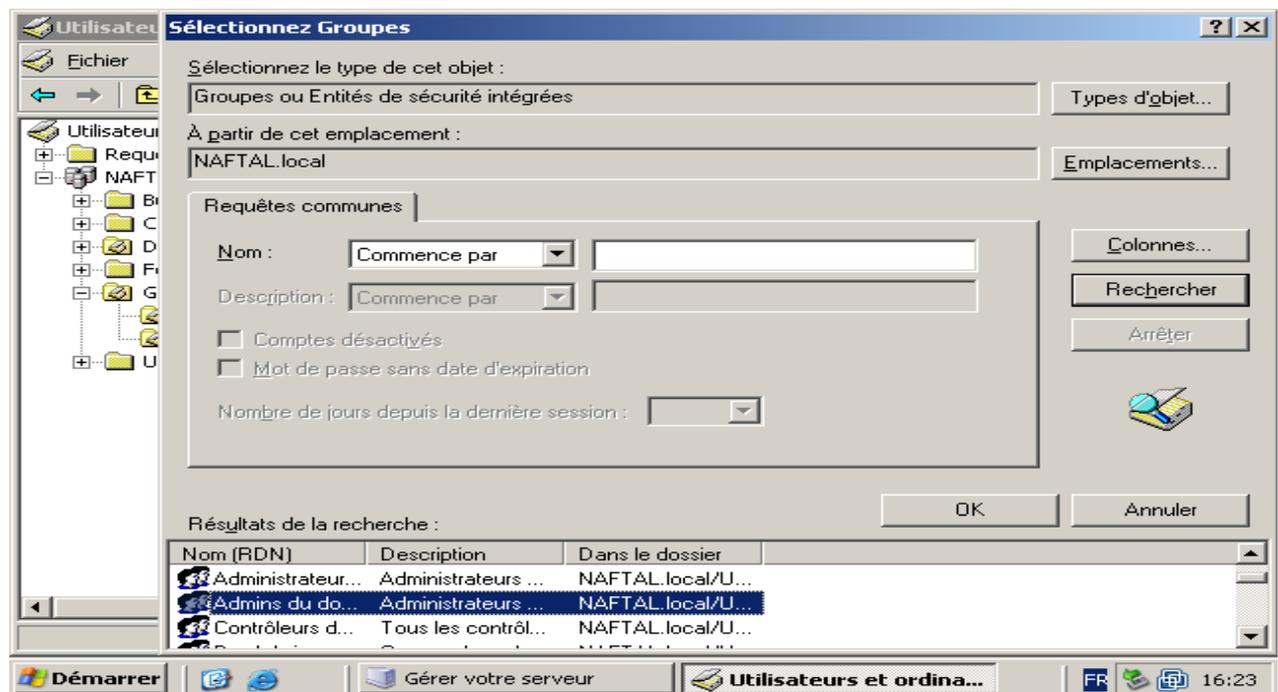


Figure III.17 - résultat de la sélection de l'administrateur du domaine -

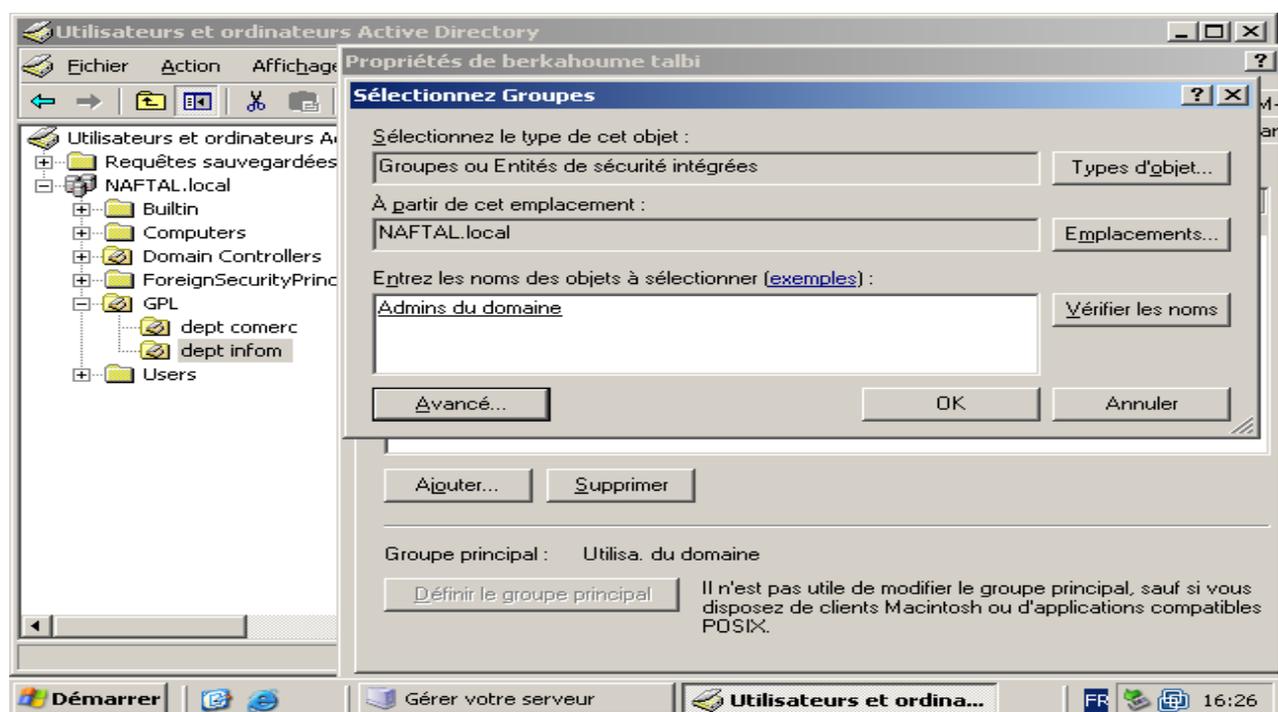


Figure III. 18 - validation de la sélection de l'administrateur du domaine -

Les autres utilisateurs vont restés que des utilisateurs membre du domaine ; ils ont des droits limitées par rapport à l'administrateur du domaine, ils peuvent seulement consulter les données partagées mai pas les modifiées.

III.5. Configuration et mise en œuvre d'un s.réseau sous Windows xp

J'ai créé d'abord un s.réseau sous Windows xp ; pour cela J'ai pris trois postes avec le serveur bien sur ET le même groupe du travail intitulé « MSHOME » ET le même domaine « NAFTAL. Local », puis les adresses IP sont comme suit :

@IP : 192 .168.0.113-> Poste1

@IP : 192 .168.0.114 -> Poste2

@IP : 192 .168.0.115 -> Poste3

@IP : 192.168.0.1 -> SERVEUR ; LA PASSRELLE @IP : 192.168.0.1

La figure suivante explique les étapes à suivre pour la modification du groupe du travail pour chaque poste : poste travail - > propriétés - > nom de l'ordinateur - > groupe du travail

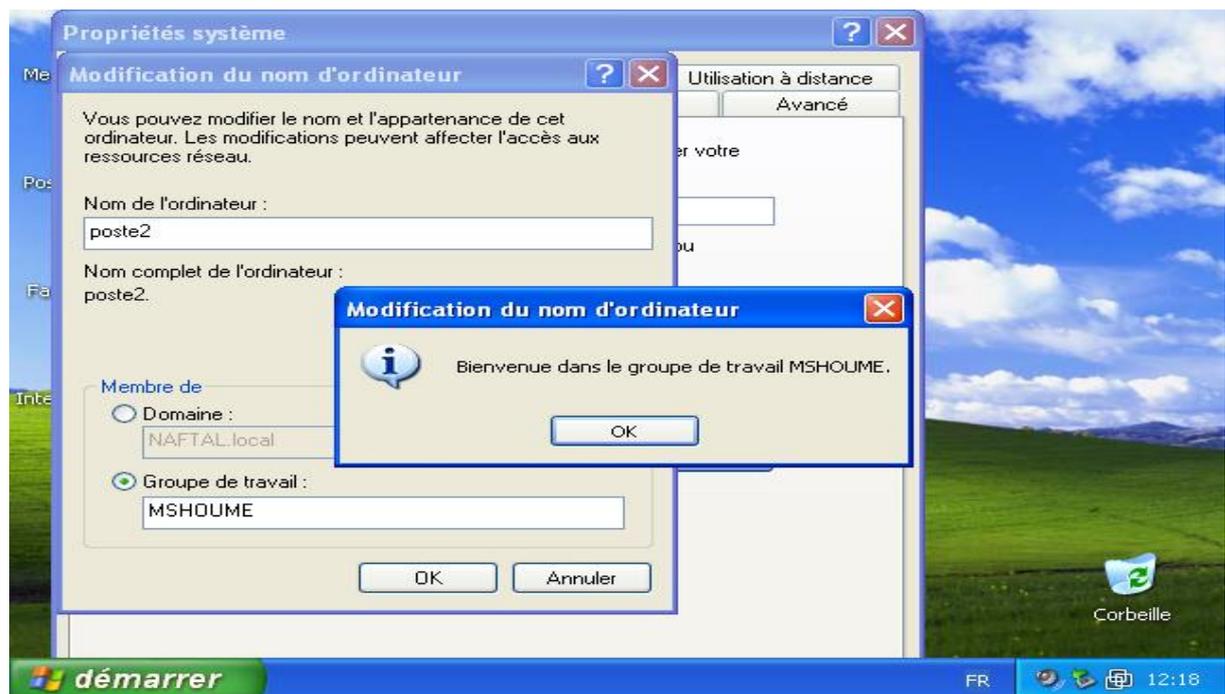


Figure III. 19 - modification du groupe du travail -

Une fois terminer il faut redémarrer les pc pour validé la modification effectuée.

Voici la listes des réseaux Microsoft crée :

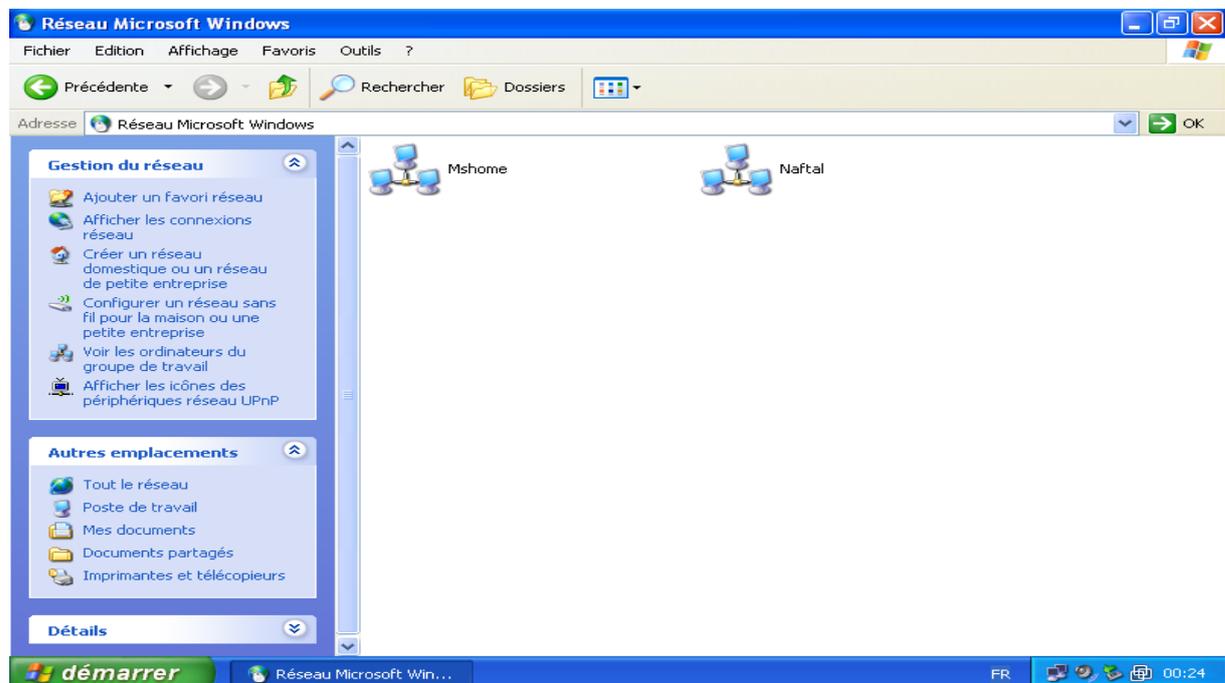


Figure III.20 - Liste des réseaux Microsoft crée -

Pour vérifié que les postes figure sur le même groupe du travail « MSHOME » on accède comme suit :

Menu démarrer - > Favoris réseau - > menu à gauche qui se figure - > voir les ordinateurs du groupe du travail. La figure si dessus va apparaitre :

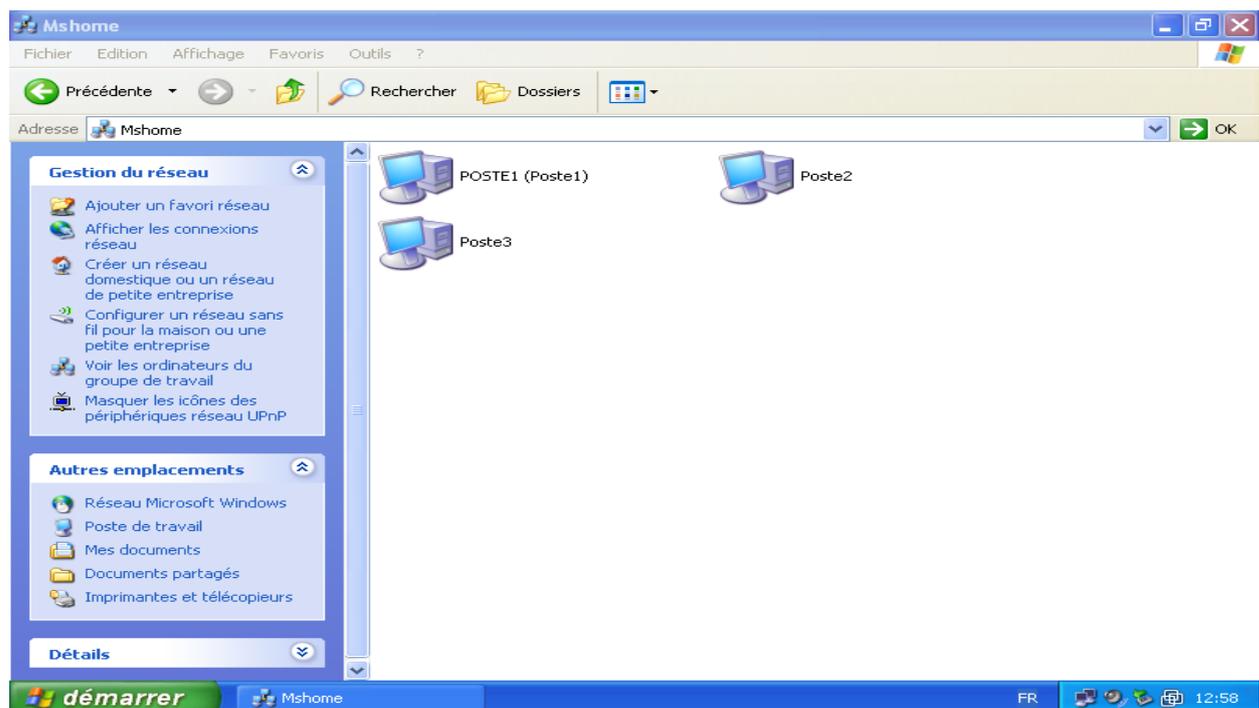
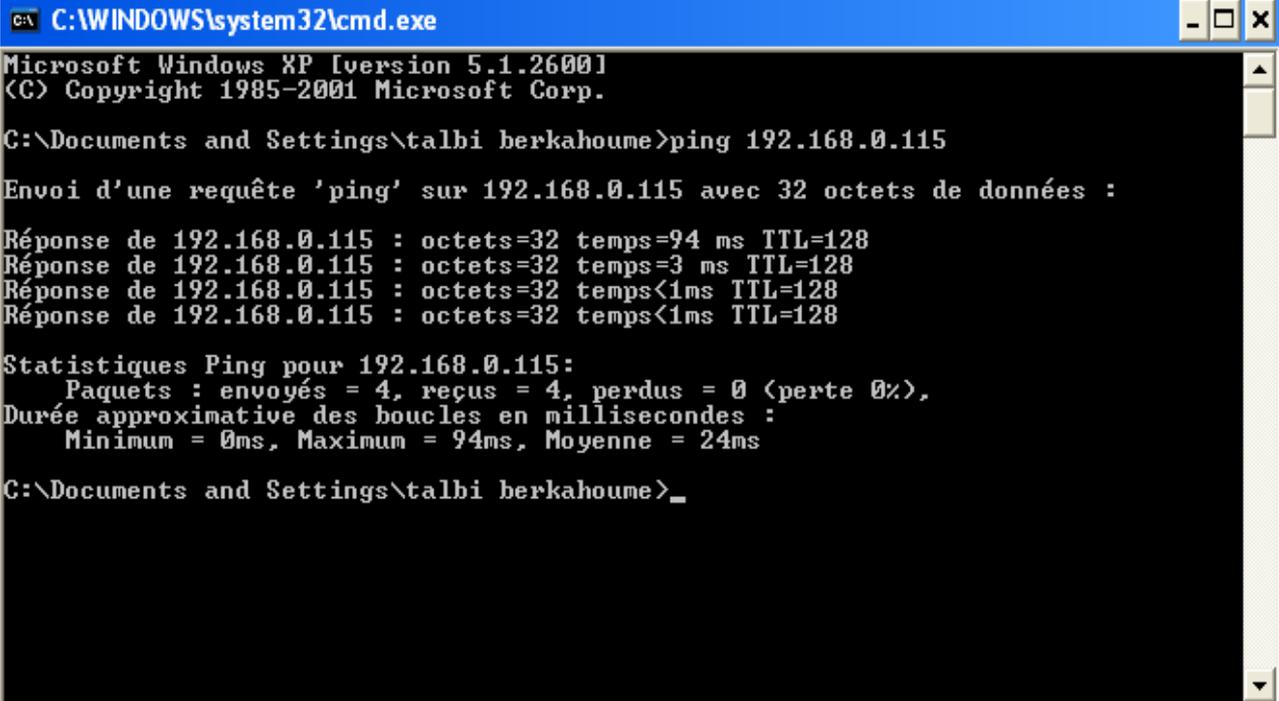


Figure III.21 – voir Les ordinateurs du groupe du travail -

On effectue un Ping pour s'assurer que tout marche bien. Depuis le poste 2 d'adresse IP 192.168.0.114 on Ping vers le poste 3 ayant l'adresse IP 192.168.0.115 et vice versa ; le résultat va apparaître sur les deux figure 22, figure 23 respectivement:



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\talbi berkahoume>ping 192.168.0.115

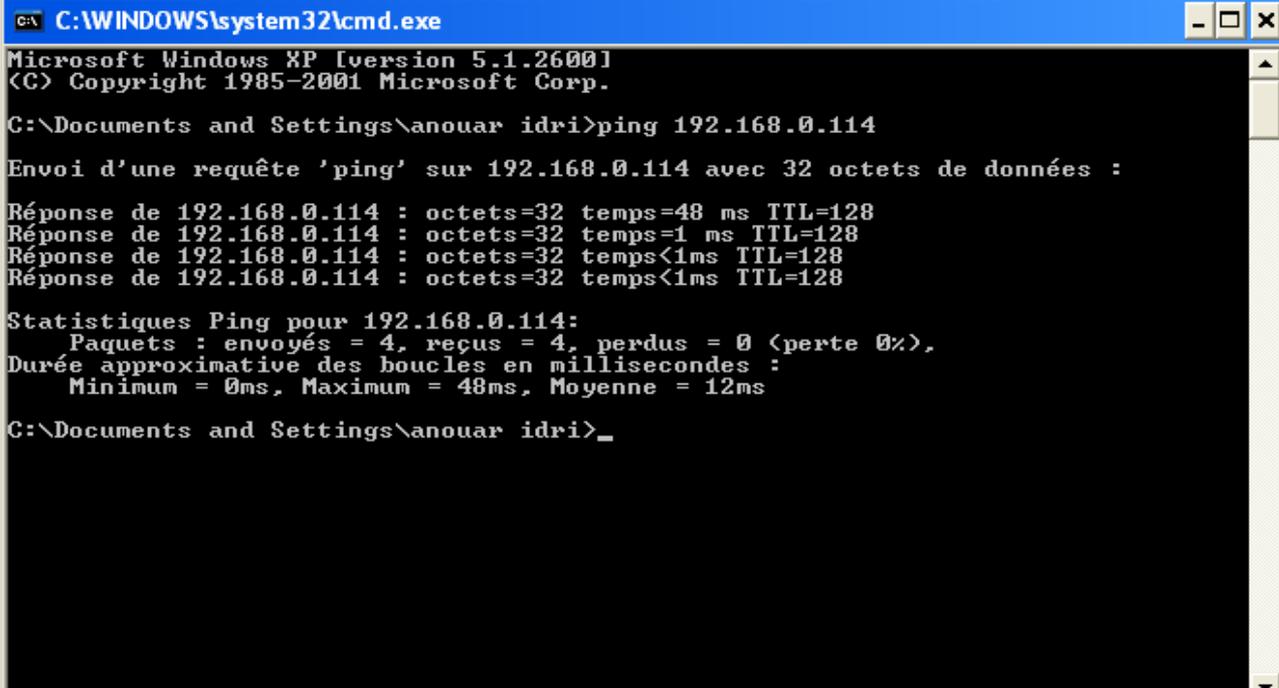
Envoi d'une requête 'ping' sur 192.168.0.115 avec 32 octets de données :

Réponse de 192.168.0.115 : octets=32 temps=94 ms TTL=128
Réponse de 192.168.0.115 : octets=32 temps=3 ms TTL=128
Réponse de 192.168.0.115 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.115 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.0.115:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 94ms, Moyenne = 24ms

C:\Documents and Settings\talbi berkahoume>_
```

Figure III.22 - résultat du Ping effectué entre les deux pc –



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\anouar idri>ping 192.168.0.114

Envoi d'une requête 'ping' sur 192.168.0.114 avec 32 octets de données :

Réponse de 192.168.0.114 : octets=32 temps=48 ms TTL=128
Réponse de 192.168.0.114 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.0.114 : octets=32 temps<1ms TTL=128
Réponse de 192.168.0.114 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.0.114:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 48ms, Moyenne = 12ms

C:\Documents and Settings\anouar idri>_
```

Figure III.23 - résultat du Ping effectué entre les deux pc –

III.6. La création de comptes utilisateurs

Chaque utilisateur doit posséder un compte sur son *ordinateur* sécurisé par un mot de passe. Lorsque l'*ordinateur* s'allume le nom d'utilisateur et le mot de passe sont demandés par le *serveur*.

Sur le même poste on peut créer autant de comptes que nécessaire selon le besoin des utilisateurs. Sur le pc client en accède de la façon suivante :

Démarrer -> paramètres -> panneau de configuration -> comptes utilisateurs

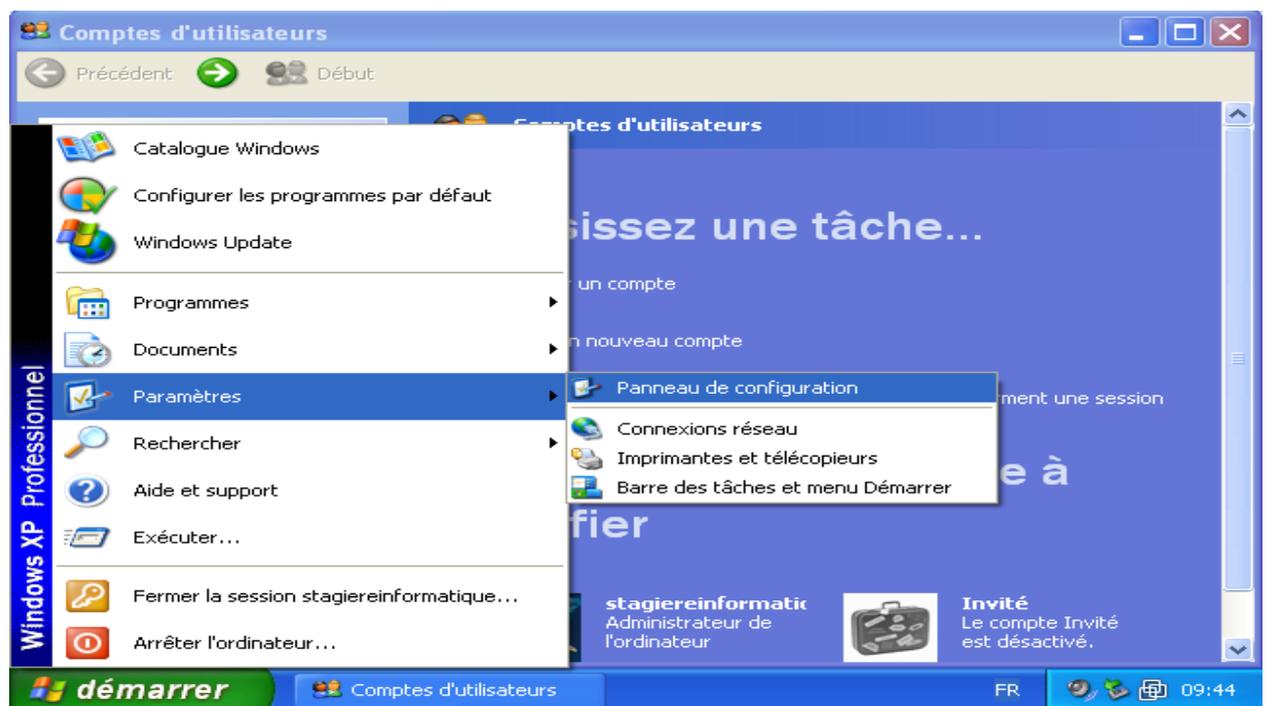


Figure III.24 - Etapes de création d'un compte utilisateurs –

La fenêtre suivante va apparaître, on donne un nom pour le compte utilisateur et on valide sur le bouton suivant

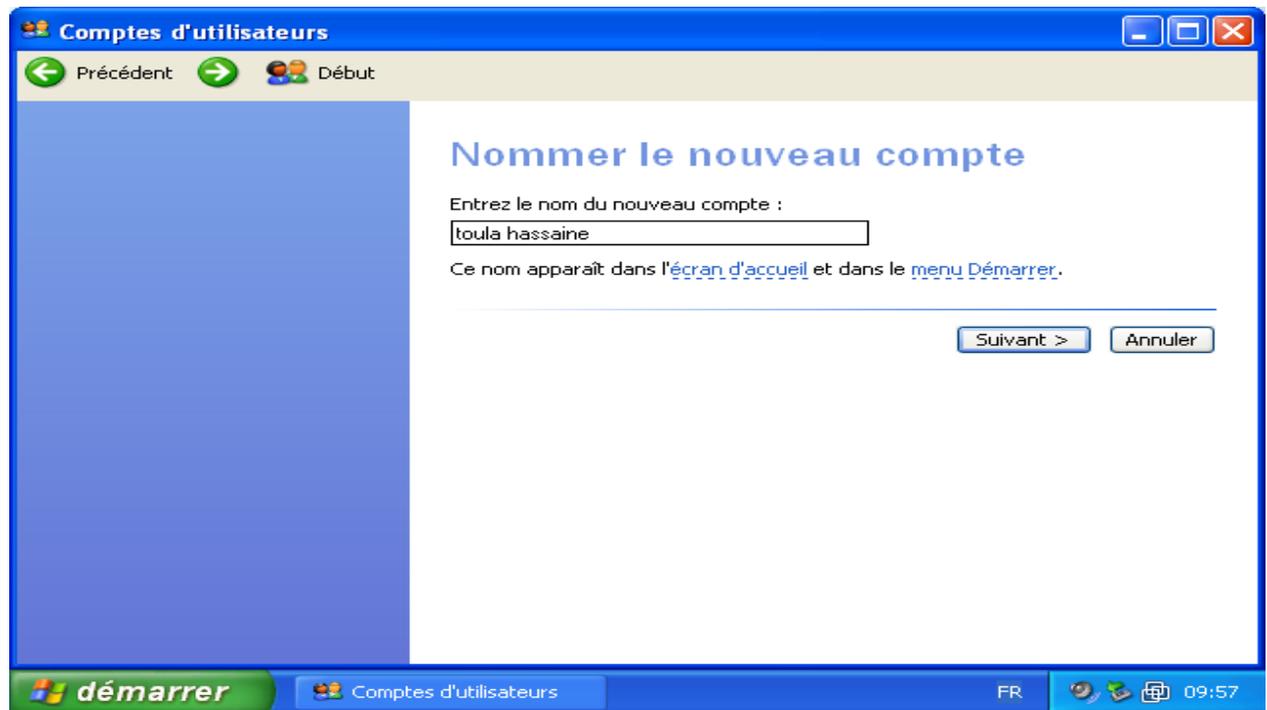


Figure III.25 – le nom du compte utilisé –

Pour terminer, la fenêtre suivante exprime la listes des comptes utilisateurs crée :

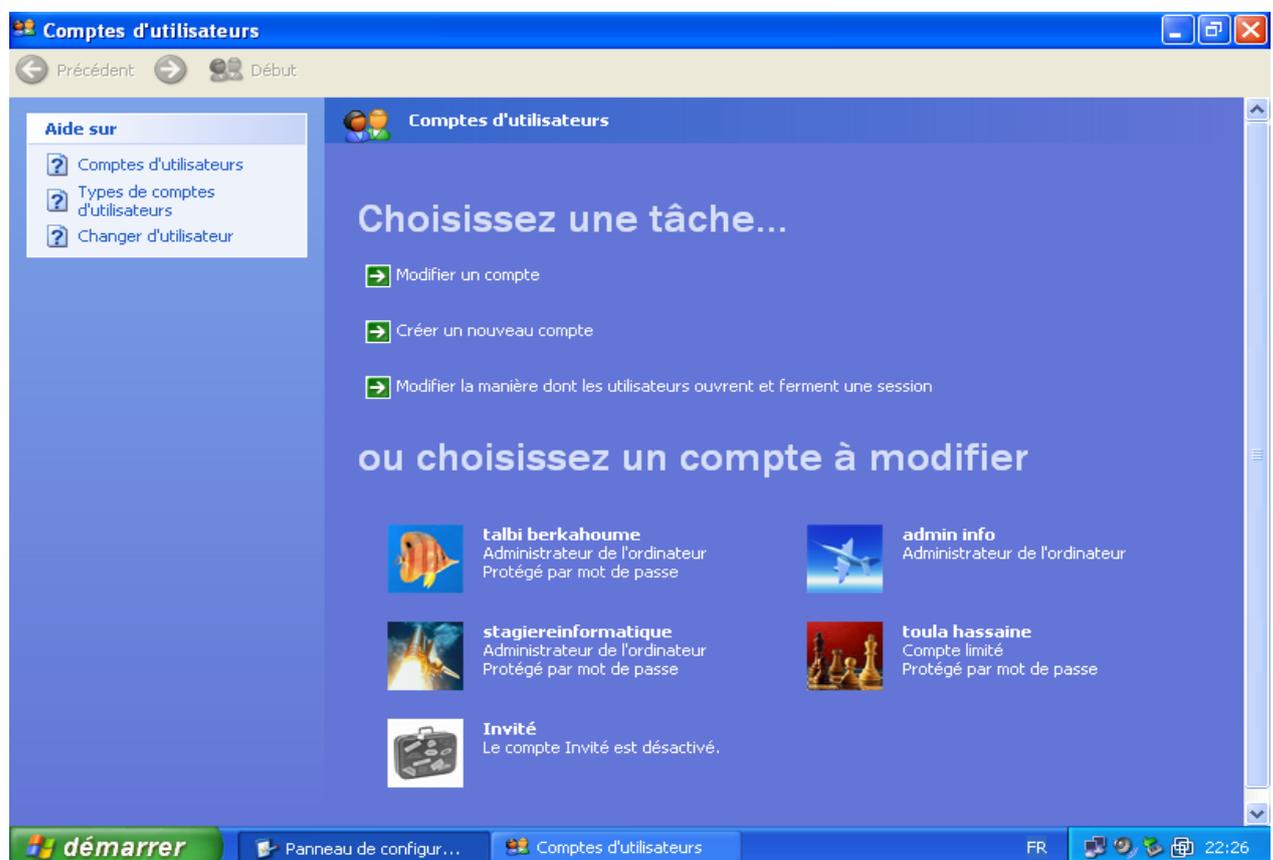


Figure III.26 – liste de compte utilisateurs crée -

III.7. Spécification d'Horaires d'accès au compte utilisateurs

Bien que cet outil soit intégré dans l'annuaire Active directory, l'administration du serveur sera effectuée d'une manière souple et performante ; pour chaque compte utilisateurs on peut le programmer des horaires d'ouverture de session journée et heure d'accès :

Pour Toula hassaine par exemple on peut lui programmer l'ouverture de session autorisée est pour mardi , de 11 :00 à 12 :00 ;

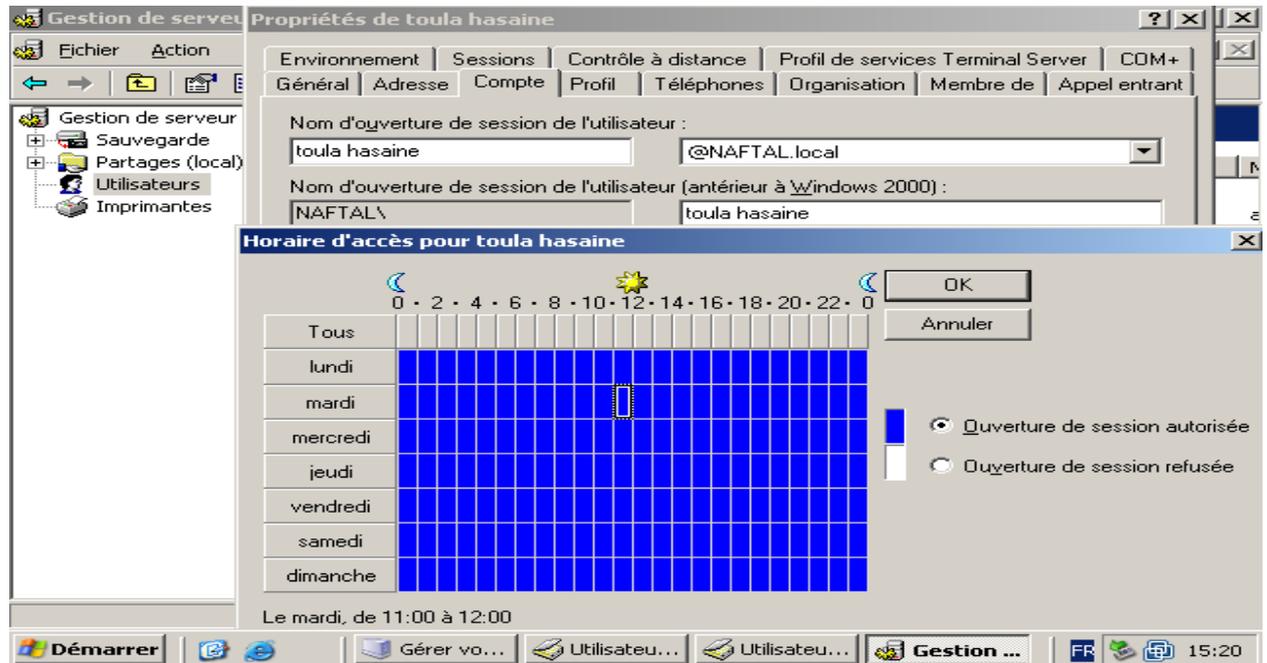


Figure III.27 - horaire d'ouverture de la session autorisée pour l'utilisateur Toula –

De même pour l'utilisateur talbi on accède de la façon suivante : Gestion de serveur -> utilisateurs -> propriétés -> compte -> horaire d'accès

La fenêtre ci-dessus va figurer :

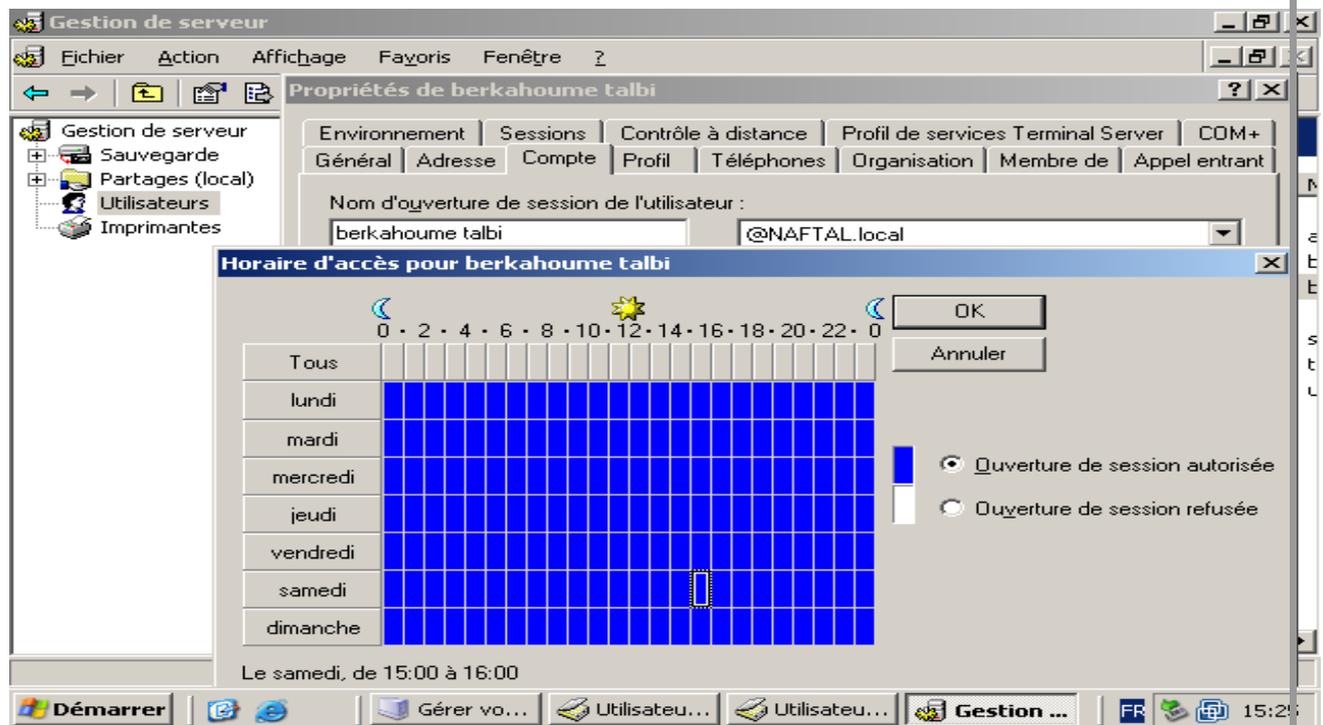


Figure III.28 - horaire d'ouverture de session autorisé pour l'utilisateur talbi -

III.8. Le serveur de fichiers

III.8.1. Qu'est-ce qu'un serveur de fichiers ?

Un serveur de fichiers sert à partager des données à travers un réseau LAN. Le serveur sert d'hébergeur et possède une grande capacité de stockage le plus souvent sécurisé au moyen d'un RAID matériel permettant la sauvegarde et la sécurisation des données. Le plus simple pour l'utilisateur est d'accéder à ses ressources grâce à un lecteur réseau accessible dans le poste de travail. La maintenance est ainsi facilitée pour l'administrateur qui de manière centralisée peut gérer toutes les sauvegardes. L'utilisateur peut accéder à ses ressources à partir de n'importe quel poste.

III.8.2. Installation et Configuration d'un serveur de fichiers

Le serveur de fichier est un rôle qu'on peut ajouter après l'installation d'Active Directory, en faisant le choix du partage d'un lecteur se trouvant sur le poste de travail d'administrateur et en modifiant les propriétés nécessaires pour permettre l'accès au partage à tous les utilisateurs. Pour partager un dossier sur le réseau en accède de la manière qui présenté a la figure si dessous :

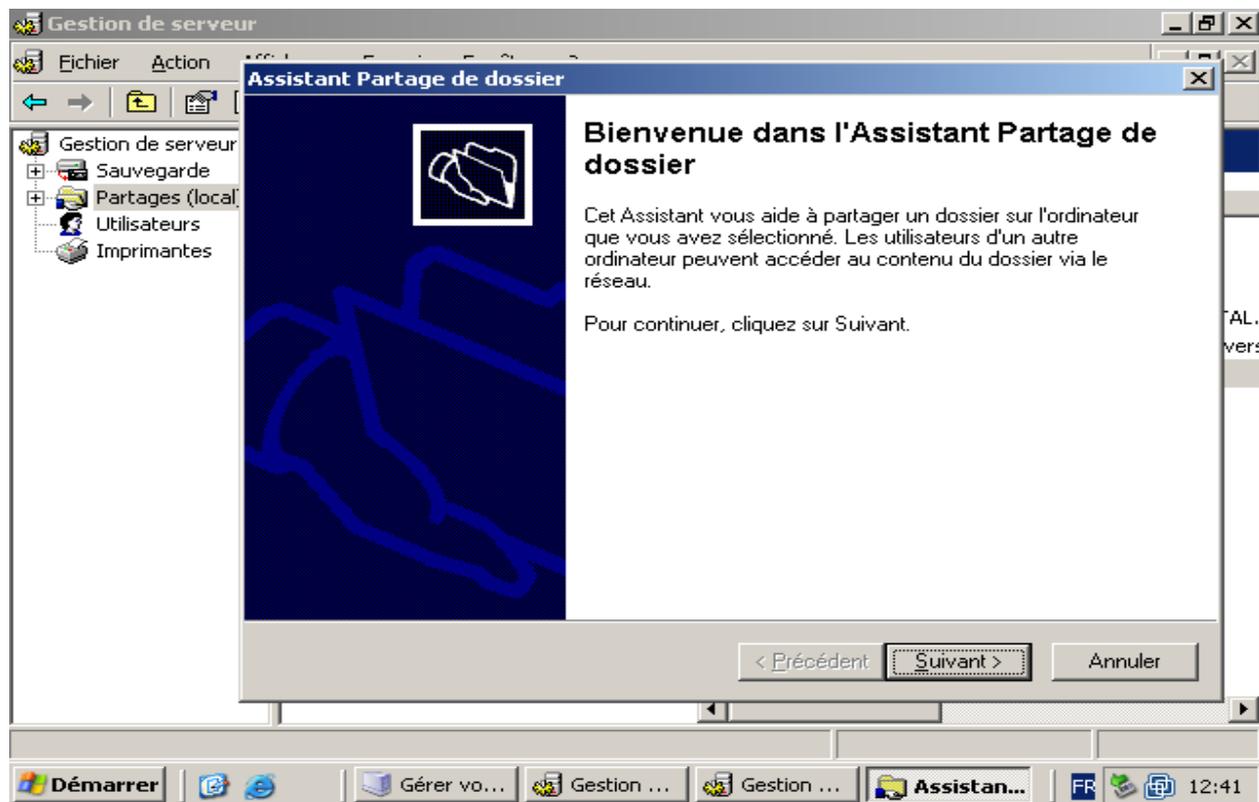


Figure III.29 – l'assistant partage de dossiers –

Une fois l'assistant est apparait on doit spécifier tout les paramètres décrivant le partage, le nom, le chemin d'accès,...

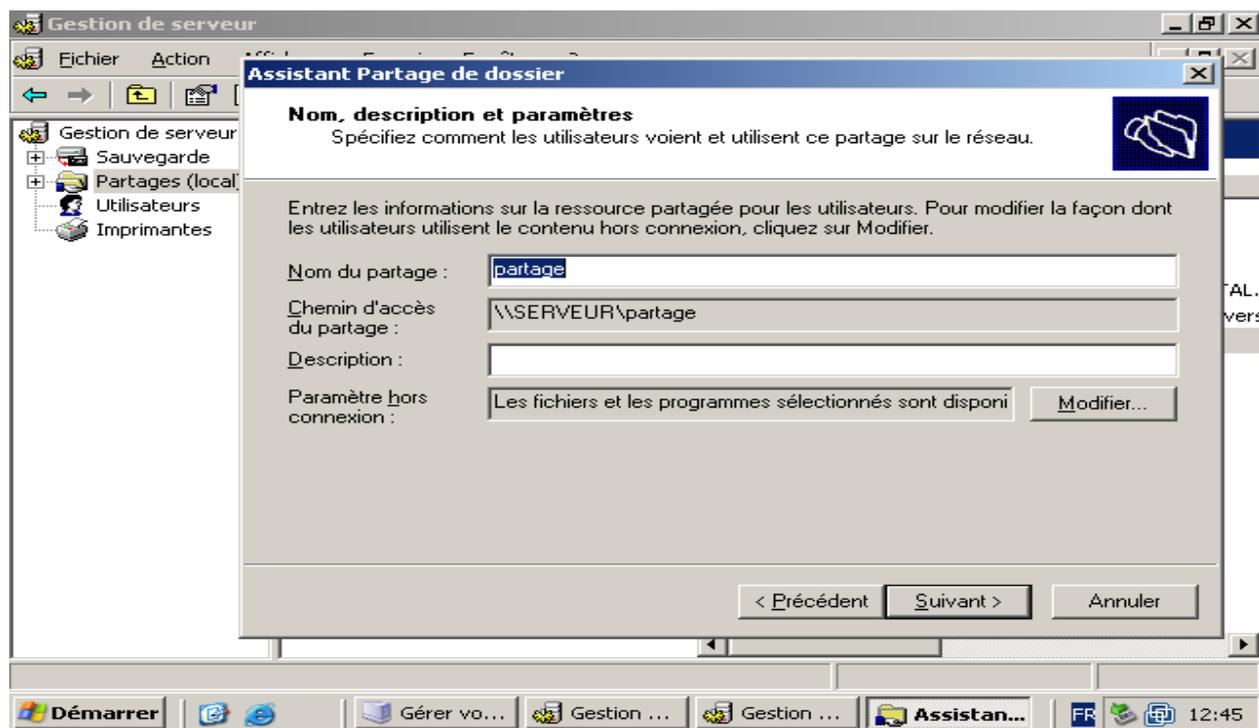


Figure III.30 - description et spécification des paramètres du partage -

Dans la fenêtre qui suit en attribue des autorisations d'accès au partage effectué :

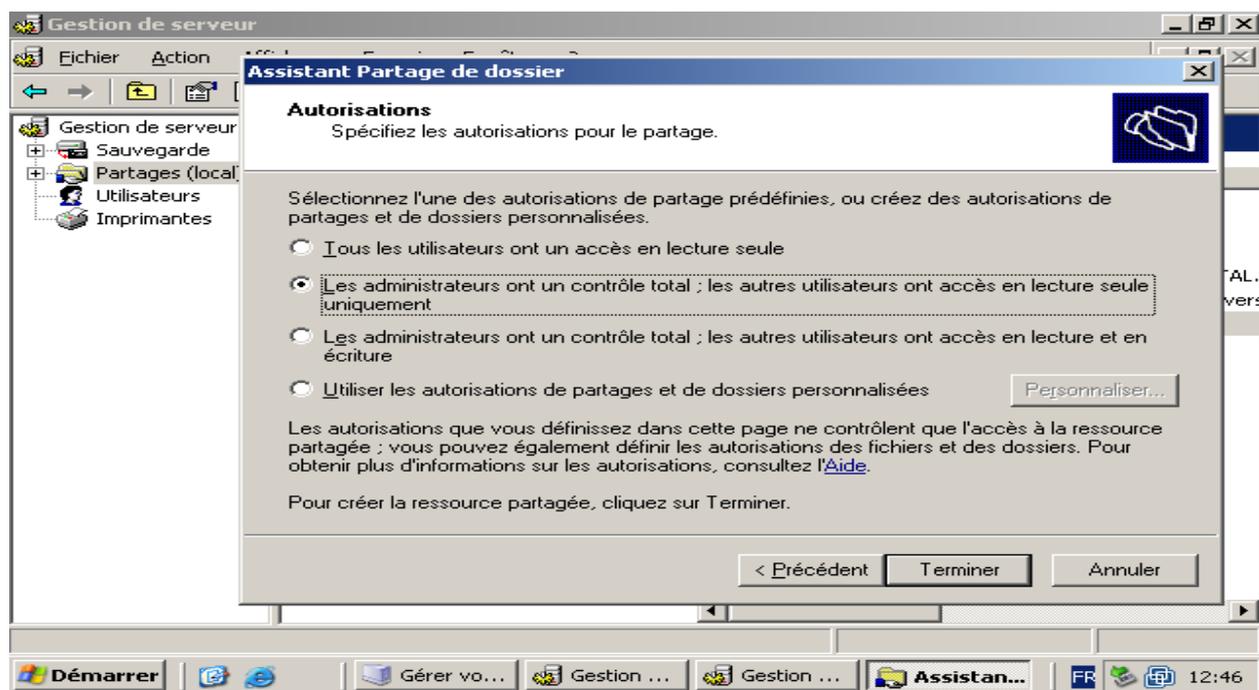


Figure III.31 – spécification des autorisations d'accès au partage

Pour terminer, une fenêtre partage réussi va apparaitre comporte un résumé concernant le nom du partage, chemin du dossier partagé ainsi que le chemin d'accédé au partage.

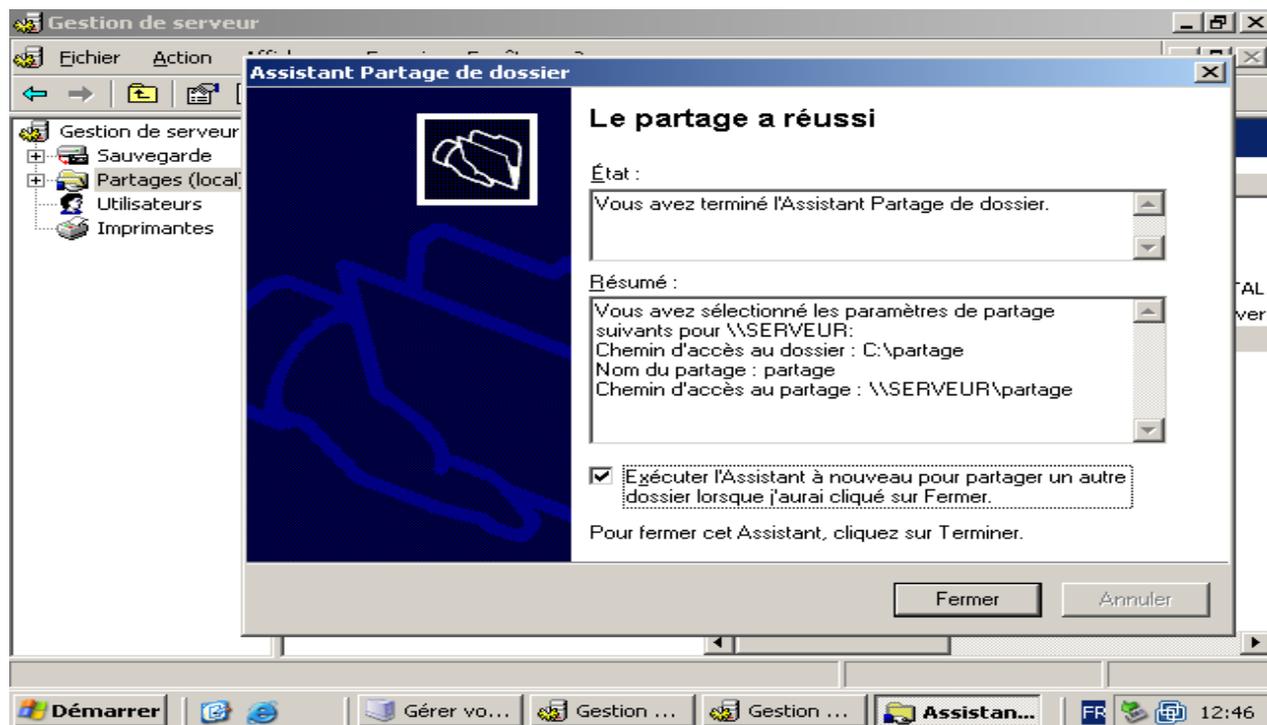


Figure III.32 - résumé de l'état de partage effectué -

Pour séparer les autorisations d'accès entre l'administrateur du domaine et l'utilisateur du domaine en accède comme suit :

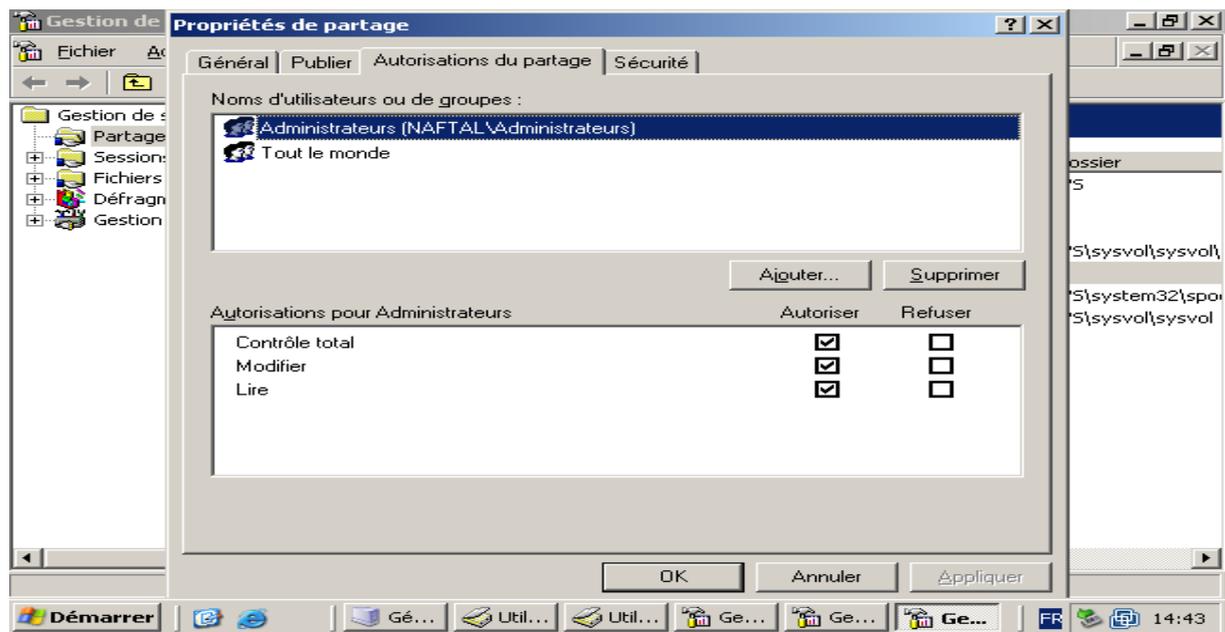


Figure III.33 -propriété de partage et les autorisations permises -

Pour les autres utilisateurs, les autorisations sont limitées à la lecture seulement.

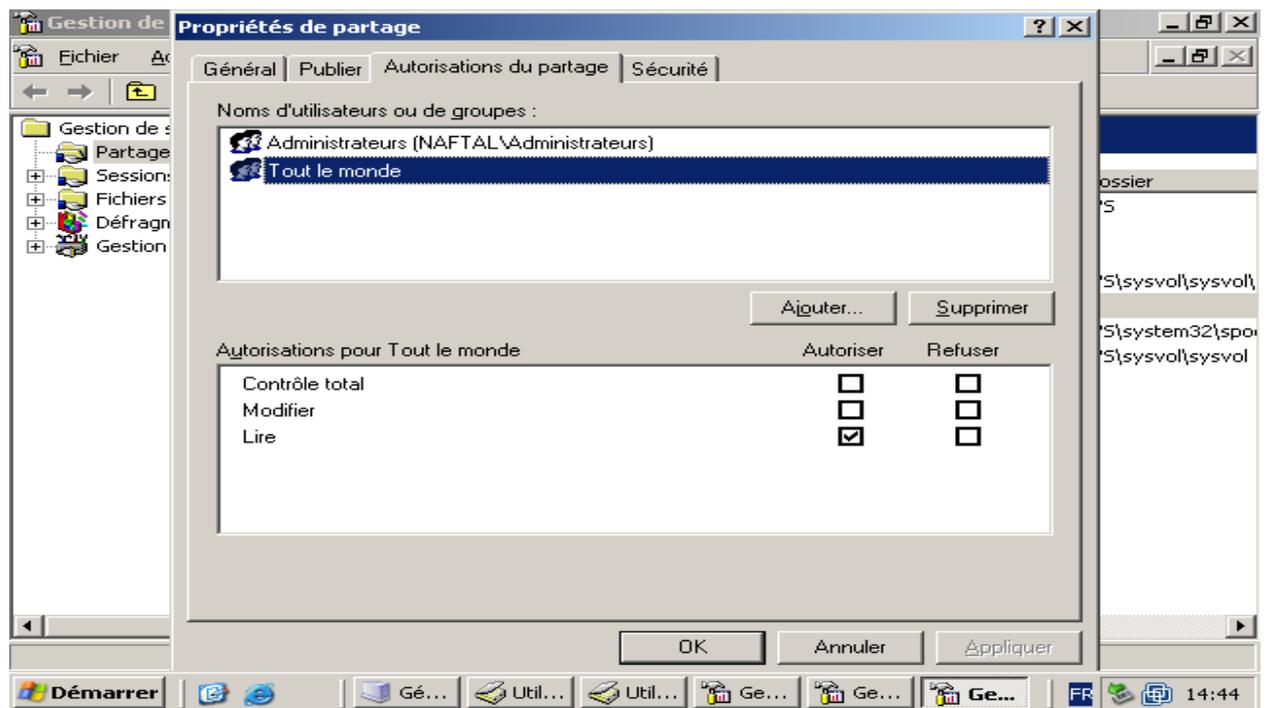


Figure III.34 – autorisations permises pour tout le monde -

Une fois le serveur à été configuré, dans notre cas pratique le serveur s'appel « SERVEUR »

Il suffit que l'administrateur ajoute les utilisateurs de la manière suivante :

Propriétés->autorisation ->ajouter ->avancer->rechercher.

III.8.3.connexion d'un utilisateur au serveur de fichiers

Les utilisateurs ont été choisis, à leurs tours ils doivent créer un lecteur réseau sur leur poste de travail comme le montre la figure suivante :

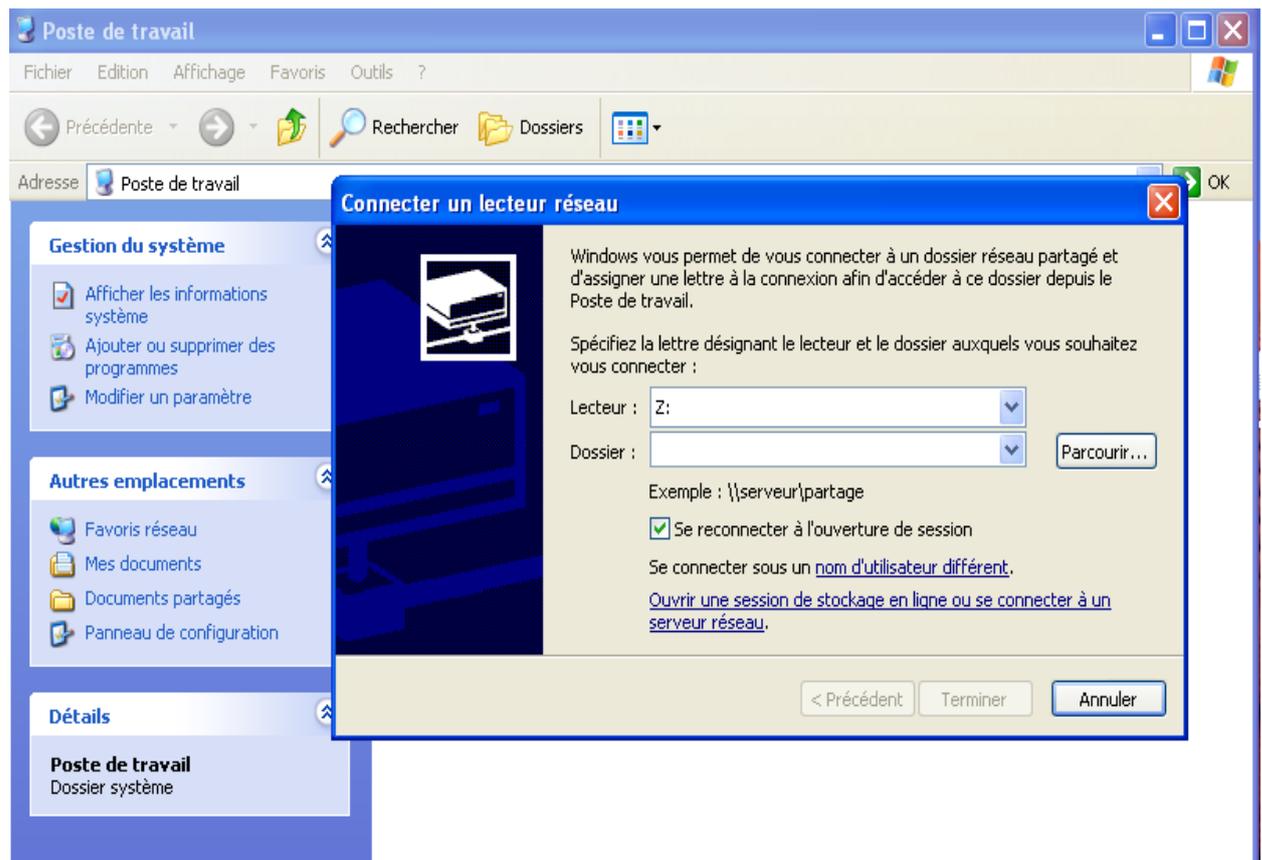


Figure III. 35 - connexion d'un utilisateur au serveur de fichiers –

Ou bien utilisé l'option **connexion bureau à distance** pour cela j'ai opté à l'installation d'un logiciel nommée **VNC (Virtual Network Controller)** qui permet de contrôler un ordinateur et

D'avoir l'accès a celui-ci à distance . Permet au serveur de visualisé l'écran de ses postes clients .

Pour avoir l'accès au pc du client distant depuis le serveur l'adresse IP et mot de passe sont demandé ; on accède selon les étapes suivantes :

On lance le logiciel vnc depuis le poste serveur puis ; tapez l'adresse ip dans mon exemple 192.168.0.115 (poste 3) ou bien 192.168.0.114 (poste2) ensuite s'authentifiez en tapant le mot de passe ; comme ci démontré sur la figure suivante (**Figure III.35**).

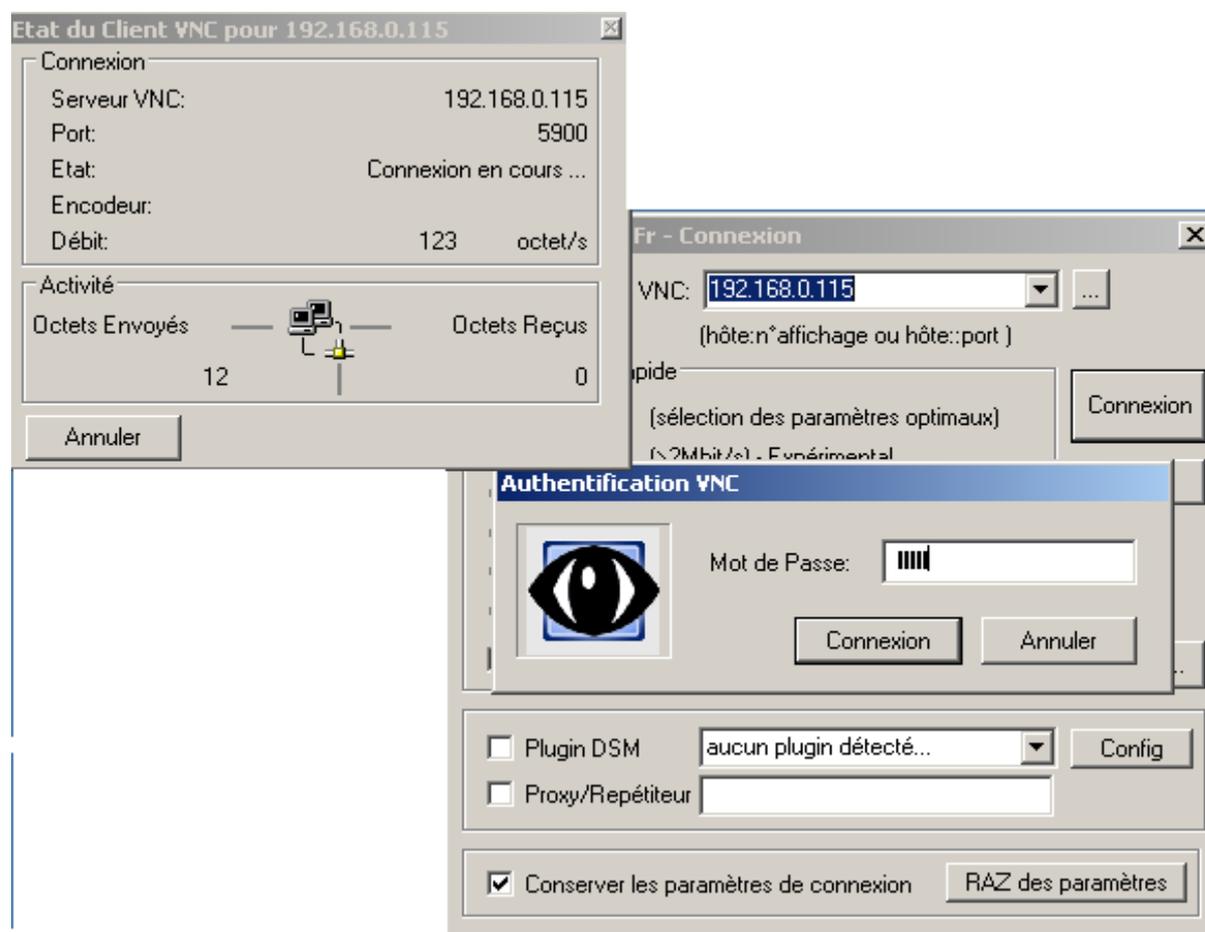


Figure III.36. – étapes à suivre pour se connecter à un bureau d'un ordinateur distant-

III.9. le serveur d'impressions

III.9.1. Qu'est-ce qu'un serveur d'impressions ?

Le serveur d'impression fournit et gère l'accès aux imprimantes réseau et à leur pilote ;

Le serveur peut être utilisé comme un serveur d'impression. En effectuant les étapes et les tâches suivantes :

- Ajouté une ou plusieurs imprimantes.
- Partagé des imprimantes pour permettre aux clients d'envoyer des travaux d'impression aux imprimantes.
- Ajouté, si nécessaire, des pilotes d'imprimante clients.

Le serveur d'impression est un rôle qu'on peut ajouter après l'installation d'Active Directory, comme se figure si dessus :

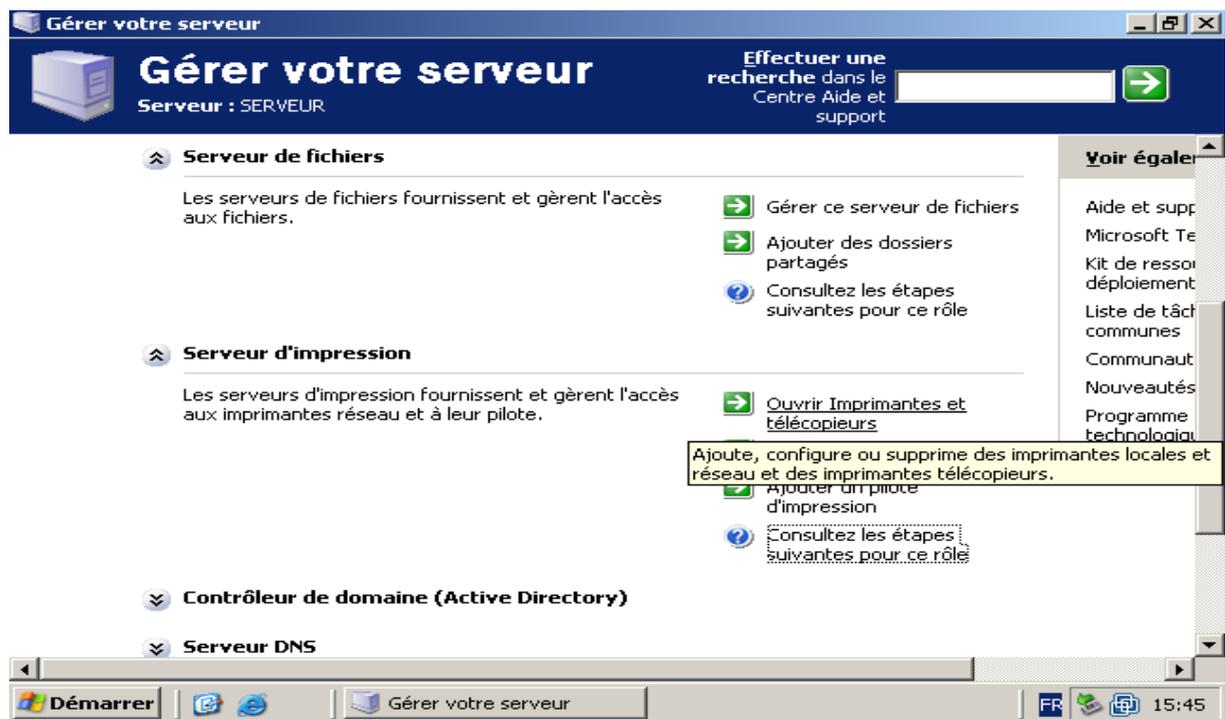


Figure III.37 – ajout de rôle serveur de fichiers et serveur d'impression –

III.9.2. Ajout et Partage d'une imprimante sur le réseau

Plusieurs ordinateurs sont utilisés dans l'environnement réseau, On partage l'imprimante connectée à un ordinateur SERVEUR avec les autres ordinateurs.

Il n'est pas nécessaire que les ordinateurs connectés au réseau soient tous équipés de la même version de Windows.

Lorsque les pc clients lancent l'impression, les données sont envoyées à l'imprimante par le biais du système serveur d'impression.

Les étapes d'ajout d'imprimante s'effectuent comme suit : Gérer serveur d'impression
-> assistant ajout d'imprimante ->

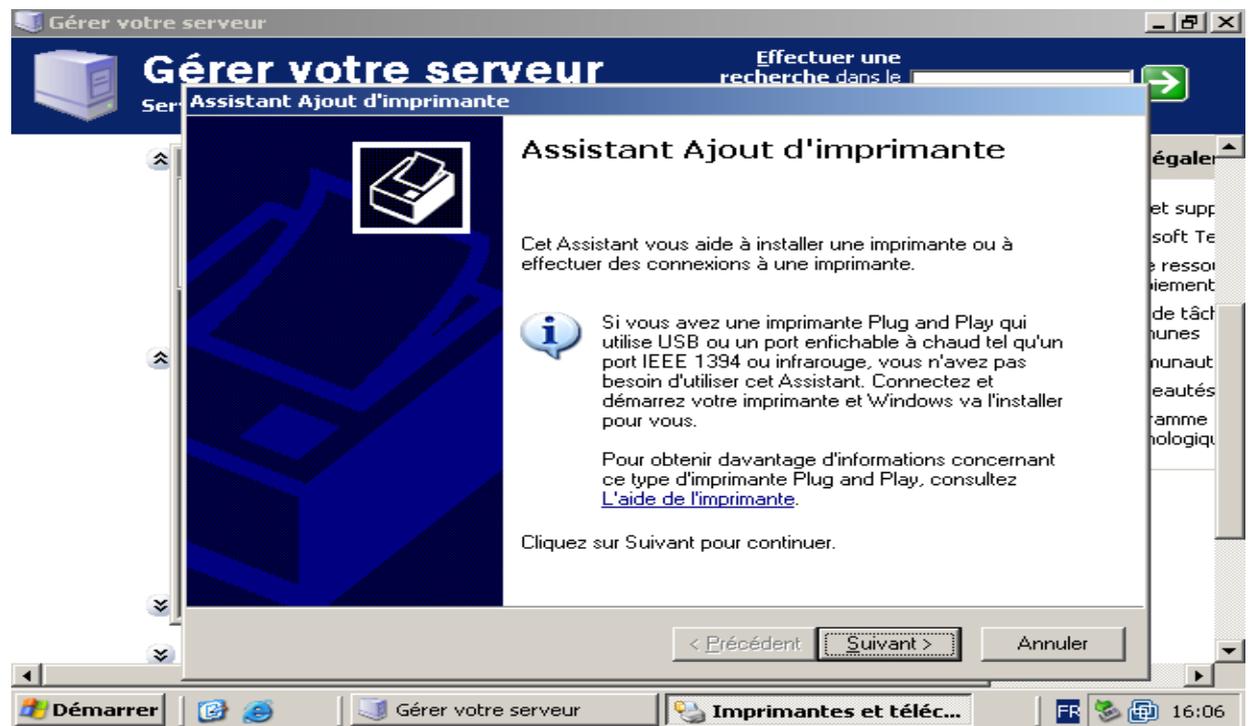


Figure III.38 – assistant ajout d'imprimante -

On fait un clique sur **suivant**, La fenêtre si dessous va figurer on sélectionne **une imprimante réseau ou imprimante connecté à un autre ordinateur**

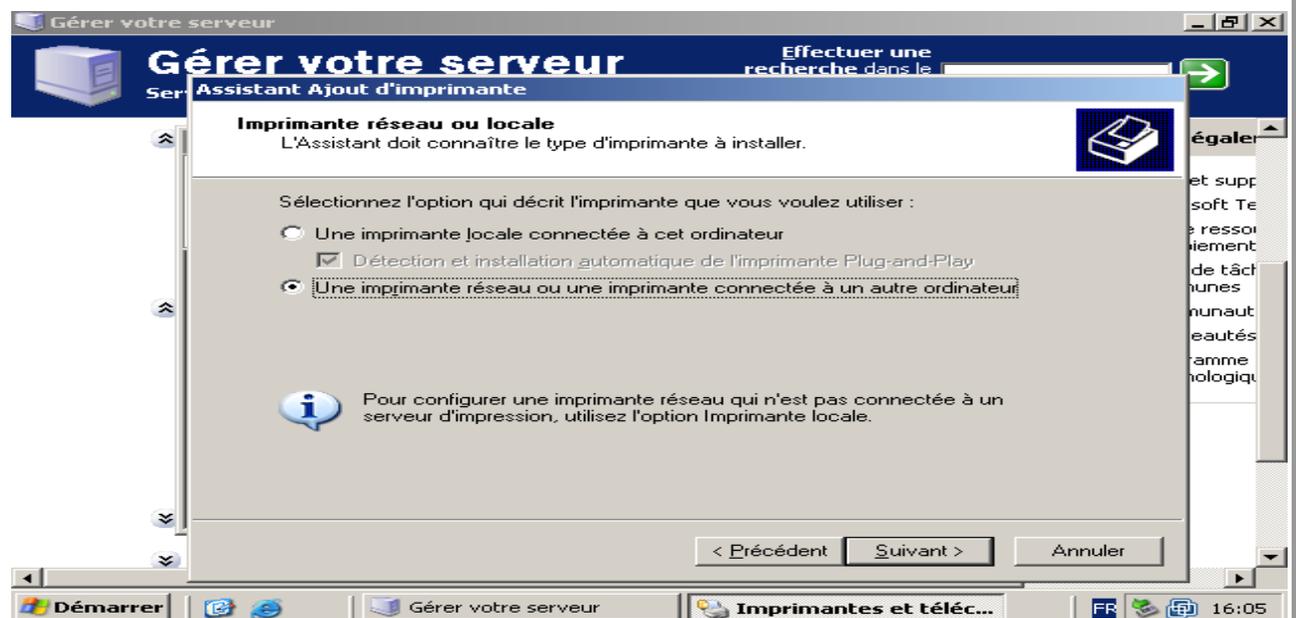


Figure III.39 – le choix du type de l'imprimante à installer -

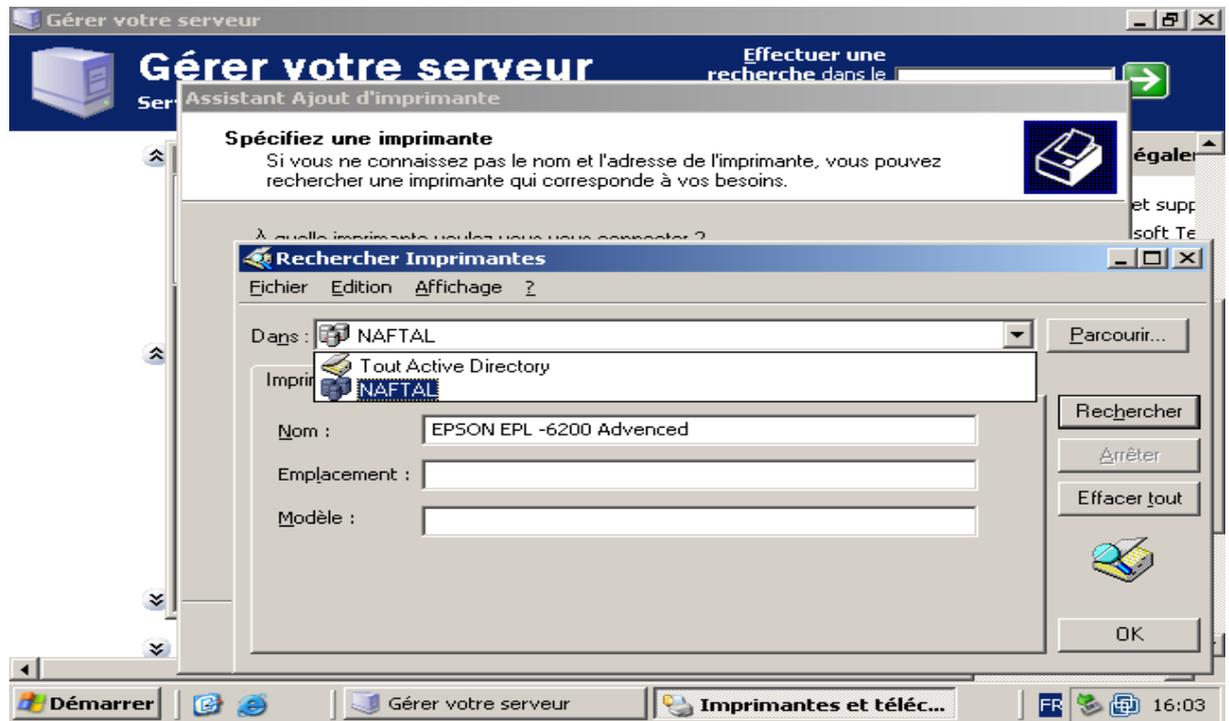


Figure III.40 – recherche de l'emplacement à installé l'imprimante -

Une fois terminer l'ajout, clique droit sur l'imprimante -> partage

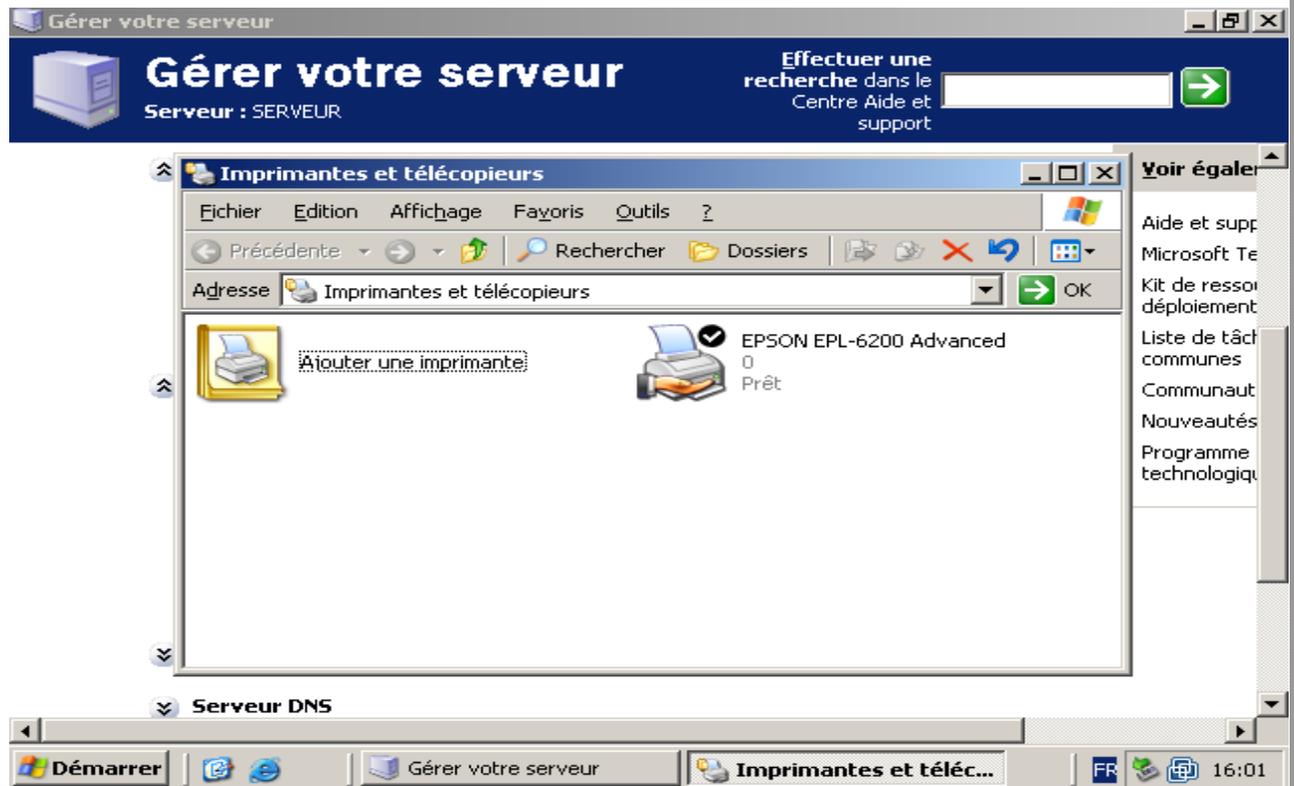


Figure III.41 - l'imprimante est partagée –

Une main se figure au dessus de l'imprimante partagée.

Remarque : Si une erreur s'est produite lors de l'impression par le système client sur une imprimante partagée, le message d'erreur de l'écran d'état d'imprimante s'affiche à la fois sur le système client et sur le système serveur d'impression. Lors d'une impression normale, l'écran d'état d'imprimante s'affiche uniquement sur le système client.

III.10. Gérer les domaines et les approbations

Ce service réalise l'administration des utilisateurs, des groupes d'utilisateurs et des ordinateurs d'un domaine (il leur a attribué un compte): Création, destruction et propriétés ;

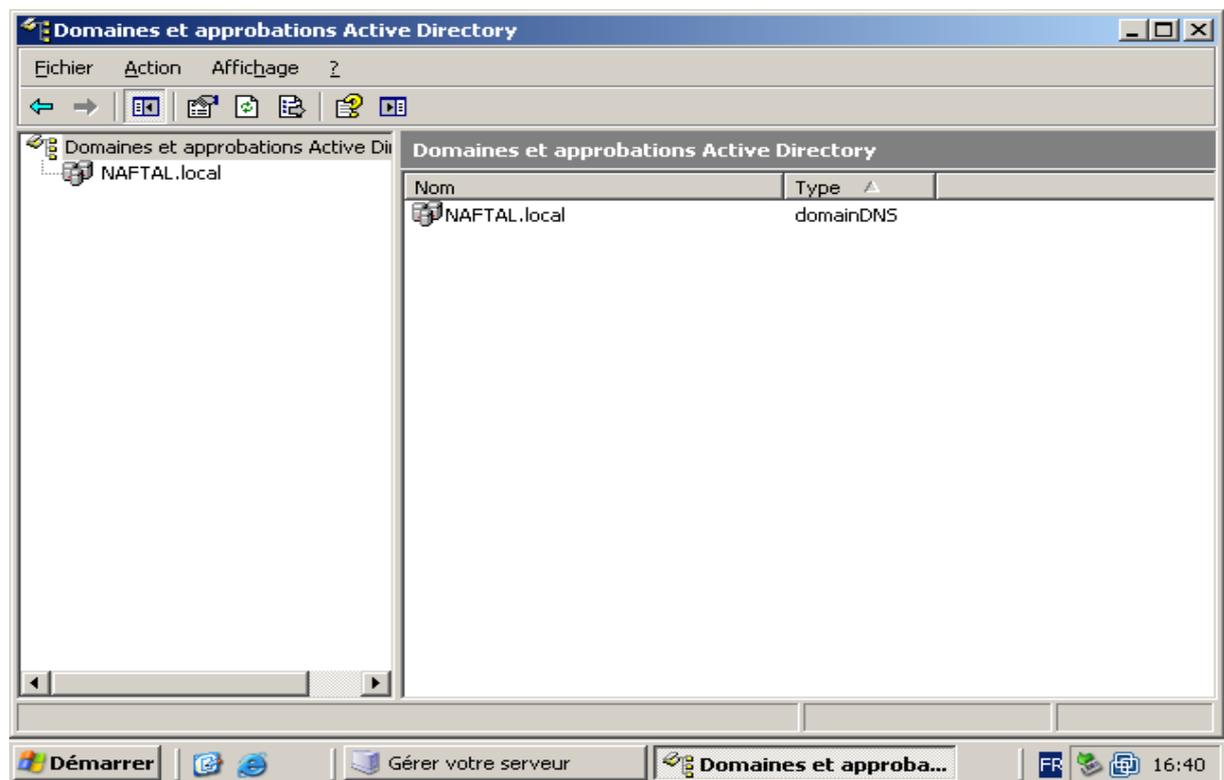


Figure III.42 - Gestion des domaines et des approbations –

III.11. Gérer les sites et les services

Ce composant nous fournit un affichage graphique de toutes les arborescences de domaines de la forêt. Grâce à cet outil, un administrateur peut gérer chaque domaine de la forêt, gérer des relations d'approbations entre domaines, configurer le mode d'opération pour chaque domaine (mode natif ou mixte) et configurer les autres suffixes UPN (User Principal Name) pour la forêt.

Lors de la création du premier contrôleur de domaine, on coche la case catalogue global une fois, mais si on veut répliquer les données alors on crée un deuxième contrôleur de domaine et on coche la case « catalogue global ».

Dans notre cas pratique à l'entreprise, on a créé une forêt nommée : NAFTAL et un domaine **NAFTAL.local** qui contient un site du même nom.

Et le site approprié contient le serveur d'hébergement SERVEUR, comme illustré ci dessus :

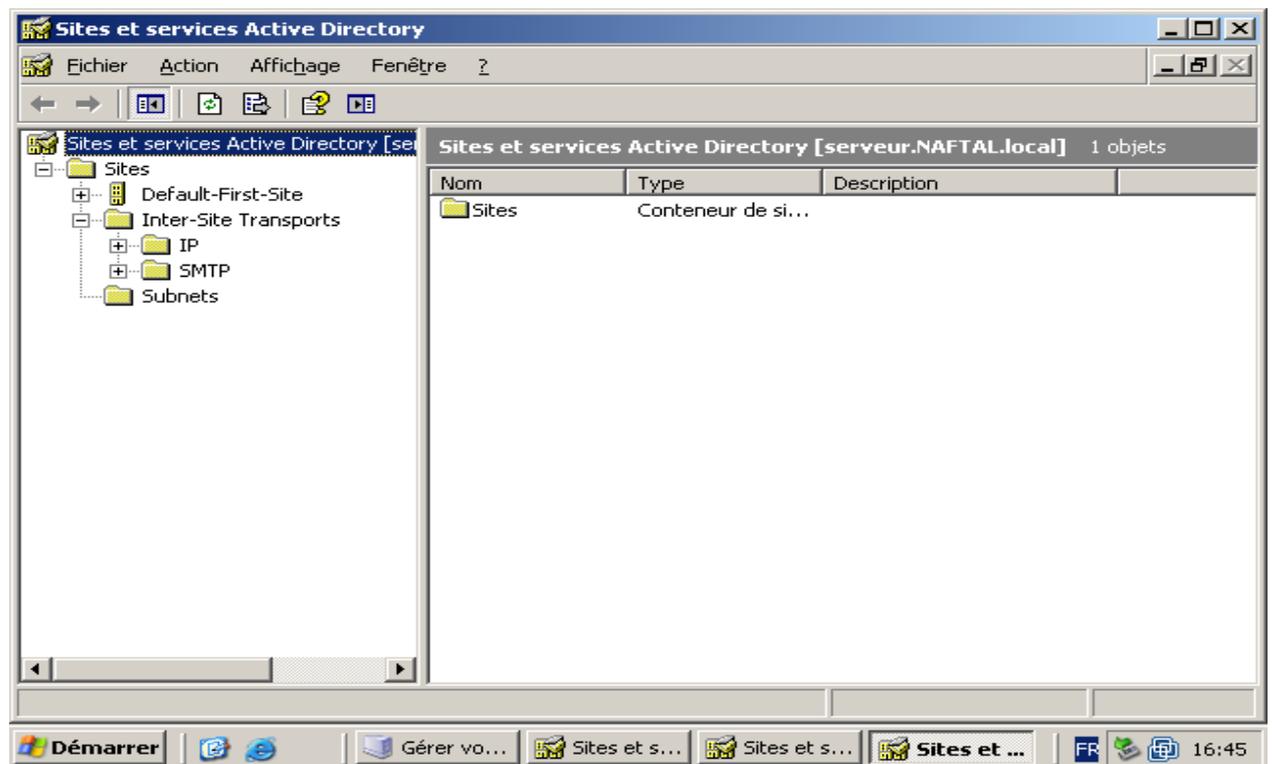


Figure III.43 - Gérer les sites et les services -

N.B : on peut déplacer notre serveur d'un site à l'autre, autrement dit on peut héberger plusieurs sites dans un même serveur.

III.12. Le Serveur DNS

On deux zones de recherche directe et inversée :

- Zone de recherche directe : se base sur la résolution nom vers adresse IP.

- Zone de recherche inversée : se base sur la résolution d'adresse IP vers nom.

Le DNS est configuré d'une manière locale, mais le serveur joue aussi le rôle d'un serveur **redirectionneur** afin de permettre l'accès à l'internet, ce serveur traduit toutes adresses DNS interne en une adresse DNS externe et vis-versa.

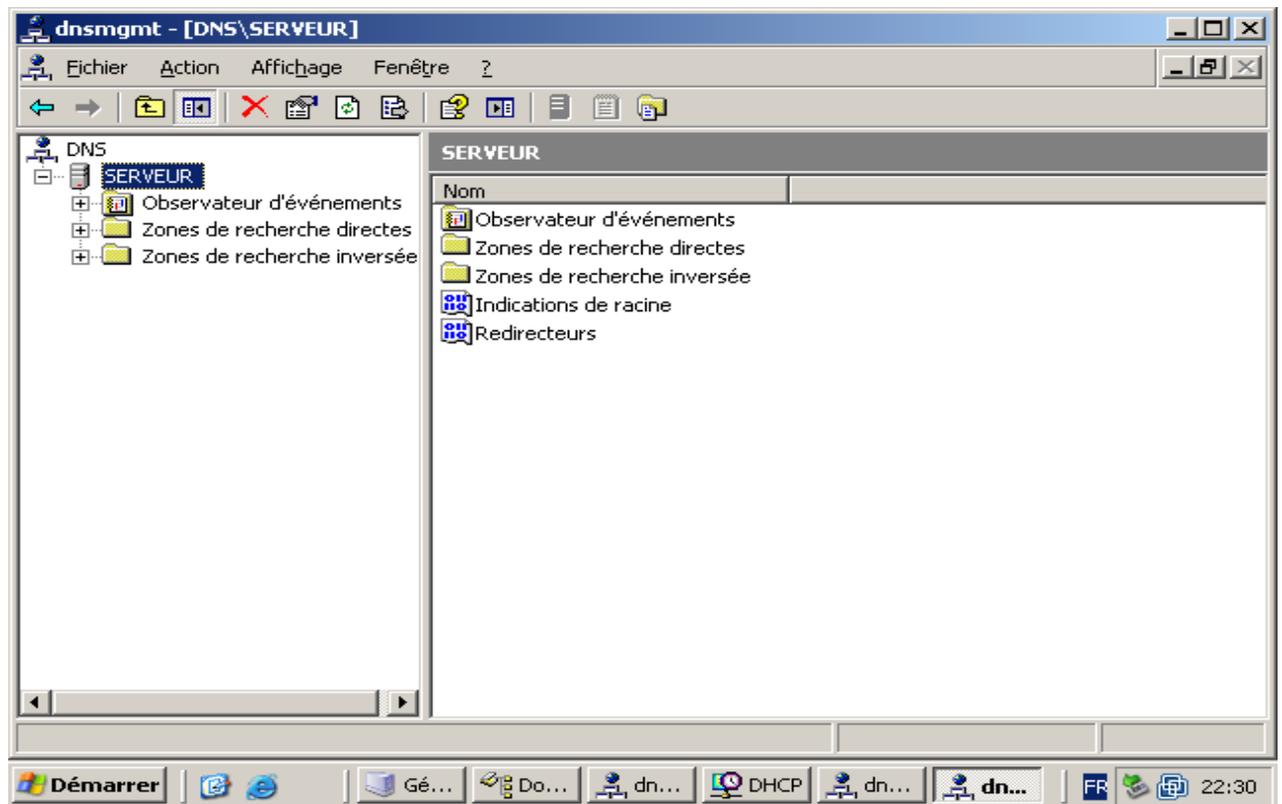


Figure III.44 - La configuration DNS d'une manière locale –

III.13. Le Serveur DHCP

On trouve une étendue qui est un groupage administratif d'adresses IP pour des ordinateurs sur un sous-réseau utilisant le service DHCP. L'administrateur crée d'abord une étendue pour chaque sous-réseau physique, puis utilise l'étendue pour définir les paramètres utilisés par les clients. Une étendue possède les propriétés suivantes :

- une plage d'adresses IP où inclure ou exclure les adresses utilisées pour les offres de bail de service DHCP ;
- un masque de sous-réseau, qui détermine le sous-réseau correspondant à une adresse IP donnée ;
- un nom affecté à l'étendue lors de sa création ;

- des valeurs de durée de bail, qui sont affectées aux clients DHCP recevant des adresses IP de manière dynamique ;
- des options d'étendue DHCP configurées pour être affectées aux clients DHCP, telles qu'un serveur DNS, l'adresse IP d'un routeur et l'adresse d'un serveur WINS ;
- des réservations, utilisées de manière optionnelle pour s'assurer qu'un client DHCP reçoit toujours la même adresse IP, comme le montre la figure suivante :

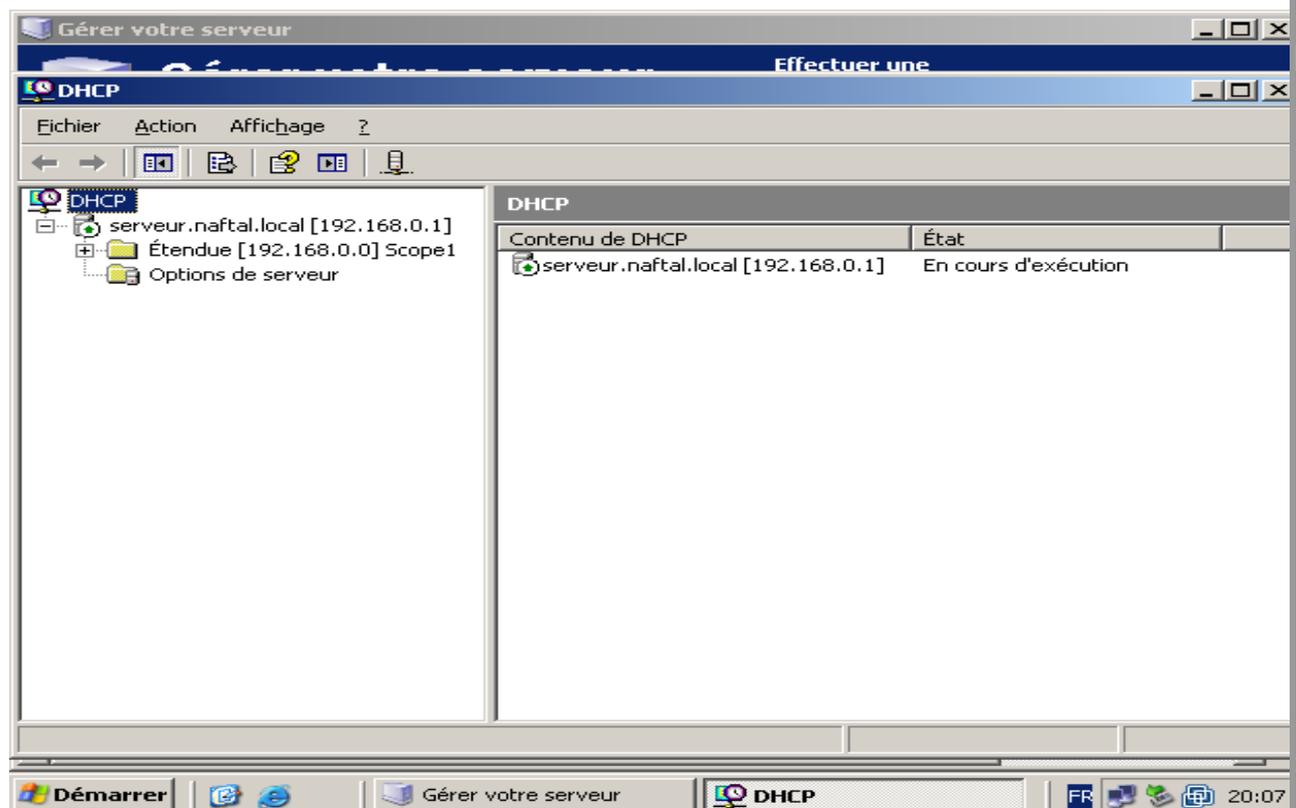


Figure III.45 - Configuration du server DHCP -

III.14. La réservation d'une adresse IP

La réservation d'une adresse IP se fait à l'aide de ses étapes :

Réservation->nouvelle réservation, puis il ya une fenêtre qui s'affiche, on doit introduire les informations nécessaires telle que l'adresse IP et l'adresse physique (mac) de la machine comme le montre la figure suivante:

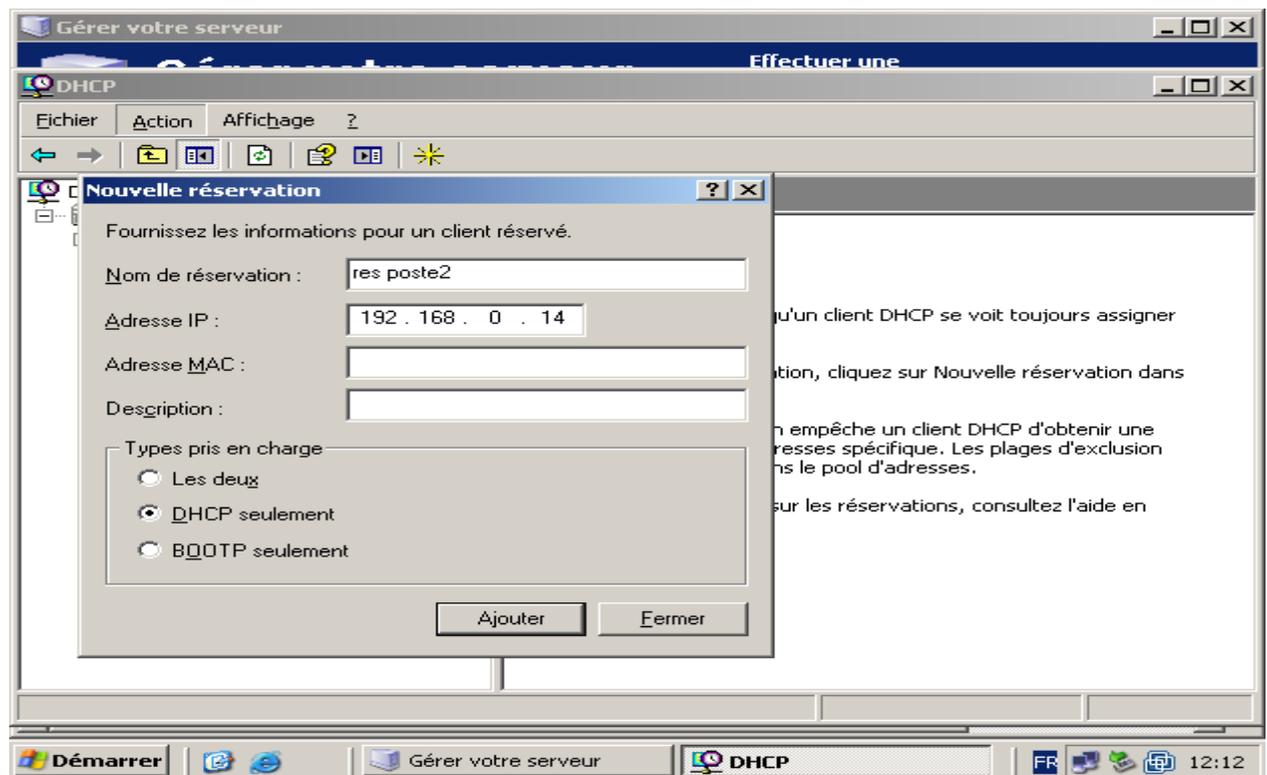


Figure III.46 - La réservation d'une adresse IP -

Remarque: Pendant le stage on a fait une réservation sur le serveur à l'un des deux utilisateurs qui se trouvent dans le domaine NAFTAL. Local, Par l'attribution d'une @IP et d'une adresse MAC de ce client, puis on a essayé de réserver la même adresse IP à l'autre utilisateur, alors un message d'erreur est affiché demandant de consulter le journal, car l'@IP est déjà réservée.

III.15.conclusion

Ce chapitre ma permit de découvrir l'environnement de Windows 2003 Server et de se familiariser avec ces différentes composants et services ; ceci ma permit de voir la puissance de cette environnement en terme de fonctionnalités à savoir l'organisation des ressources de l'entreprise et la gestion de ces utilisateurs en utilisant l'annuaire Active Directory.

Conclusion générale

Conclusion général

Dans le cadre de mon étude en matière de réseaux informatique à NAFTAL.et dans le but de mieux appréhender mes connaissances théoriques et les mettre en pratique, j'été amenés à réaliser mon travail qui a pour objectif la configuration et mise en ouvre d'un réseau local et partage réseau des ressources informatique au sein de l'entreprise sous Windows server.

Ainsi dans le cadre de ce travail, nous somme amenés à appliquer les notions et les différents concepts retenus en (Réseaux / Windows 2003Server).

En effet, le réseau informatique est indispensable à toute organisation car il facilite la transmission, la duplication, le partage des dossiers et des périphériques. Il permet aussi le traitement et la consultation des bases de données et une transmission rapide et fiable des données.

Ce projet à pour but d'assurer le fonctionnement optimal des ressources réseaux de l'entreprise et assurer à ses membres un accès rapide à l'information et un partage facile des données. D'où on constate que Le déploiement d'un service d'annuaire comme Active directory au sein d'une entreprise offre aux utilisateurs finaux un environnement de travail très fiable. Cet environnement permet aux administrateurs de bénéficier d'une sécurité et d'une facilité de gestion et aux utilisateurs d'effectuer leurs taches le plus efficacement possible.

Le travail qui à été réalisé n'est qu'un début d'implémentation, par rapport à tout ce qu'il ya à faire pour que l'administration réseau puisse être effective.

Glossaire

Protocole : spécification d'un dialogue entre plusieurs ordinateurs qui s'échange des données.

TCP/IP (Transmission contrôle protocole /Internet protocole) : représente l'ensemble des règles de communication sur internet ,se base sur la notion d'adressage IP .le faite de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données

IPX (inter PAC ket Xchange) : protocole de couche réseau développé et commercialisé par la société Novell et intégré à son système d'exploitation réseau.

LDAP : Protocole permettant l'interrogation et la modification des services d'annuaires.

Man driva (Mandrakesoft) : une société française éditrice du système d'exploitation Mandriva linux.

Open/LDAP : un annuaire informatique, il constitue une alternative libre à Microsoft Active directory.

Ker béros : protocole d'authentification réseau qui repose sur un mécanisme de clés secrètes et l'utilisation de tickets .

SSL : protocole de sécurisation des échanges sur internet ; devenu TLS par la suite.

TLS : norme de sécurisation par chiffrement du transport de l'information au sein des réseaux informatiques.

DNS (Domaine Name Système) : c'est un service permettant de traduire un nom de domaine en information de plusieurs types qui y sont associés notamment en adresse IP de la machine portant ce nom.

DHCP (Dynamique Host Configuration Protocole) :protocole réseau de configuration automatique des paramètres IP d'une station . en lui affectant automatiquement une adresse IP , le masque de sous réseau ,la passerelle et les paramétrages DNS .

WIFI : (Wireless Fidélité) : réseau local sans fils de type Ethernet permet d'obtenir des débits pouvant atteindre 11 MBIT /S .le matériel WIFI respecte la famille de norme 802.11 de L' IEEE pour la communication sans fil dans un réseau Ethernet.

BIBLIOGRAPHIE

- [1] Nathalie Bruneau et Thomas TAM ; Les illustrations de Les hauts débits en télécoms ; 1999 .
- [2] Philippe ATELIN, notions fondamentales sur les réseaux informatiques ; 2009 .
- [3] Christian Draux , Les réseaux.2006
- [4] Bertrand PETIT ; architectures des réseaux ,2006.
- [5] G. pugolle , les réseaux, EYROLLES ;1997 .
- [6] [http// :www. Labo-microsoft .org/articles /server.net](http://www.Labo-microsoft.org/articles/server.net)
- [8] Chabane.T ; mémoire, installation et configuration d'un réseau informatique, Bejaia, session 2006.
- [7] [http// :www.microsoft.com/france server /fourrant/server-isa.aspx](http://www.microsoft.com/france/server/fourrant/server-isa.aspx);2011
- [13] [http// :www.Labo-microsoft .org/articles /server/ISA2004](http://www.Labo-microsoft.org/articles/server/ISA2004);
- [9] <http://www.clusif.asso.fr> / Sécurité physique des éléments d'un réseau local , Clusif 2000 .
- [10] Riadh Abdel li , mémoire, université Virtuelle de Tunis.
- [11] [www .novell .com./fr-fr/directory/sysreqs.html](http://www.novell.com/fr-fr/directory/sysreqs.html)
- [12] [http://www.microsoft.com/france /server /windows server/editions .msp](http://www.microsoft.com/france/server/windows_server/editions.msp)
- [13] lefevre ,F.(2006);mise en place d'un server d'authentification LDAP. Université de LITORELLE ;
- [14] SUPINFO (2010) administration système et réseau .DUNOD
- [15] INTELLIGENT Teaching and Learning with computers:
[http://italc.sourceforge.net /home .PHP](http://italc.sourceforge.net/home.PHP).
- [16] Brown, T .2000 .Windows 2000server .campus press France .
- [17] les réseaux et l'informatique d'entreprise guide du décideur et de l'utilisateur pierre jacket .

Résumé

Mon projet consiste à répondre aux problèmes de partage des ressources informatiques au sein d'une entreprise. En particulier, j'ai étudié une solution permettant de centraliser les équipements et les ressources utilisées par les utilisateurs au sein de l'entreprise. En déployant un annuaire nommé active directory. Bien évidemment, j'ai constaté que Le déploiement d'un service d'annuaire comme Active directory au sein d'une entreprise offre aux utilisateurs finaux un environnement de travail très fiable. Cet environnement permet aux administrateurs de bénéficier d'une sécurité et d'une facilité de gestion et aux utilisateurs d'effectuer leurs tâches le plus efficacement possible.

Mots clés : partage de fichiers, gestion des utilisateurs, domaine, LDAP, active directory.

My project is responding to the problems of sharing computing resources within an enterprise. In particular, I studied a solution to centralize equipment and resources used by users within the enterprise. Deploying a directory named Active Directory. Of course, I found that the deployment of a directory service such as Active Directory within a company offers end users a work environment very reliable. This environment allows administrators to take advantage of security and ease of management and users to perform their tasks as efficiently as possible.

Key words: file sharing, user management, domain, LDAP, active directory.

