



Université François RABELAIS de Tours  
Ecole Polytechnique  
Département Informatique



# TP

# Administration

# Systeme

## Sous Windows 2000

(Bac + 5)



Microsoft  
**Windows 2000**

Ali Larab  
2003-2004



# SOMMAIRE

<b>INSTALLATION DE WINDOWS 2000 .....</b>	<b>4</b>
<b>1. INFORMATIONS UTILES ET PRE-INSTALLATION.....</b>	<b>4</b>
1.1. Informations utiles.....	4
1.2. C'est quoi Windows 2000 .....	4
1.3. Quelle version de Windows 2000 installer et sur quelle machine ?.....	4
1.4. Configuration matérielle nécessaire : .....	4
1.5. Différence entre partition primaire, secondaire, étendue et logique : .....	5
1.6. Différence entre FAT et NTFS : .....	6
1.7. RIS.....	6
1.8. Préparation de l'installation (Preliminaires) .....	7
<b>2. INSTALLATION .....</b>	<b>8</b>
Exercice N°1 : Installation de la version Serveur.....	8
Exercice N°2 : Installation de la version Client (W2k professionnel).....	10
Exercice N°3 : Configuration du 1 <sup>er</sup> serveur du réseau .....	11
Exercice N°4 : Rétrogradation d'un serveur.....	12
<b>TP N° 2 ET 3 :.....</b>	<b>13</b>
<b>CONFIGURATION DES SERVEURS.....</b>	<b>13</b>
<b>1. CONFIGURATION D'UN SERVEUR W2K.....</b>	<b>13</b>
1.1. Introduction .....	13
1.2. Définitions .....	13
1.3. Différentes configurations possibles de W2k Server .....	14
1.4. Que peut-on configurer avec l'Assistant de Configuration de votre serveur ? .....	15
1.5. Outils d'administration : .....	15
<b>ACTIVE DIRECTORY .....</b>	<b>16</b>
<b>2. ACTIVE DIRECTORY .....</b>	<b>16</b>
2.1. C'est quoi Active Directory : .....	16
2.2. Remarques :.....	16
2.3. Question : .....	17
2.4. Exercice 1 : Installer Active Directory.....	17
2.5. Remarque : .....	19
<b>3. GESTION DES MACHINES ET DES UTILISATEURS .....</b>	<b>20</b>
3.1. Création et gestion de comptes d'ordinateurs .....	20
Exercice N° 2 : Créer des comptes d'ordinateurs dans le composant « Utilisateurs et ordinateurs Active Directory » .....	20
Exercice N° 3 : Création d'un compte d'ordinateur à partir du poste client.....	21
Exercice N° 4 : Se connecter à un domaine.....	22
Exercice N° 5: Afficher et modifier les propriétés d'un compte d'ordinateur .....	22
Exercice N° 6: Activer/désactiver ou supprimer des comptes d'ordinateurs .....	22
Exercice N° 7: Déplacer des comptes d'ordinateur .....	23
3.2. Création et gestion des comptes d'utilisateurs .....	25
3.2.1. Option des comptes utilisateurs .....	25
3.2.2. Types de compte .....	26
3.2.3. Types d'utilisateur.....	26
Exercice 1 : Création d'un compte d'utilisateurs local.....	27
Exercice 2 : Création d'un compte d'utilisateur de domaine.....	28



Exercice 3 :Création d'un modèle de compte d'utilisateur.....	29
Exercice 4 : Définition des ordinateurs à partir desquels l'utilisateur peut ouvrir une session.....	29
Profil utilisateur :.....	30
<b>TP N°4 .....</b>	<b>31</b>
<b>4. INSTALLATION ET CONFIGURATION D'UN SERVEUR DNS.....</b>	<b>31</b>
4.1. Objectifs: .....	31
4.2. C'est quoi et pourquoi un DNS .....	31
4.3. Types de serveurs DNS .....	31
4.4. Installation d'un serveur DNS.....	32
Exercice N° 1 : Installer le serveur DNS.....	32
4.5. Activer le service DNS sur le réseau :.....	32
4.6. Configuration du serveur DNS.....	33
Exercice N° 2 : Configurer un serveur DNS principal.....	33
4.7. Ajout et gestion des enregistrements DNS.....	34
Exercice N° 3 : Ajouter des enregistrements d'adresses et de pointeurs .....	34
4.8. Mise à jour des propriétés d'une zone.....	35
<b>TP N° 5 .....</b>	<b>37</b>
<b>5. INSTALLATION ET CONFIGURATION D'UN SERVEUR DHCP.....</b>	<b>37</b>
5.1. Objectifs du TP : .....	37
5.2. Pourquoi un serveur DHCP.....	37
5.3. Présentation et fonctionnement d'un serveur .....	37
5.4. Installation et configuration d'un serveur et d'un client DHCP.....	38
Exercice N° 1 : Installation d'un serveur DHCP.....	38
Exercice N° 2 : Configuration d'un serveur DHCP .....	39
Exercice N° 3 : Configuration d'un client DHCP .....	40
5.5. Autoriser un serveur DHCP dans Active Directory .....	40
5.6. Réserveation d'adresses .....	41
5.6.1. Libération des adresses des clients.....	42
5.6.2. Active Directory et DNS :.....	42
5.7. Eviter les conflits d'adresses IP .....	43
<b>TP N° 3 .....</b>	<b>45</b>
<b>INSTALLATION D'UN SERVEUR D'IMPRESSION.....</b>	<b>45</b>
<b>1. INSTALLATION D'UN SERVEUR D'IMPRESSION.....</b>	<b>45</b>
<b>2. INSTALLATION D'UN SERVEUR TSE.....</b>	<b>47</b>
<b>TP N° 5 .....</b>	<b>48</b>
<b>LE PROFIT ERRANT .....</b>	<b>48</b>
<b>1. LE PROFIT ERRANT.....</b>	<b>48</b>
<b>2. UTILISER LES UTILITAIRES DE LIGNE DE COMMANDE .....</b>	<b>48</b>



## TP n° 1 :

# Installation de Windows 2000

## 1. Informations utiles et pré-installation

### 1.1. Informations utiles

Lorsque vous exécutez le programme d'installation de Windows 2000, vous devez donner des informations sur le mode d'installation et de configuration du système d'exploitation. Vous devez alors maîtriser certaines notions.

### 1.2. C'est quoi Windows 2000

Windows 2000 (ou simplement W2k) est un système d'exploitation multi-tâches et multi-utilisateurs. Il est développé par la firme Microsoft pour les PC et les serveurs. Actuellement il est le système d'exploitation le plus utilisé du grand public. C'est le successeur de Windows NT 4.0. Il a été réalisé officiellement en février 2000. Son interface ressemble à celle de NT 4.0 ou à celle de Windows 95. Par rapport à Windows NT 4.0, il est facile à configurer et offre un environnement entièrement nouveau (plus d'options).

### 1.3. Quelle version de Windows 2000 installer et sur quelle machine ?

Chacune des versions du système d'exploitation Windows 2000 (Professionnelle, Server, Advanced Server et DataCenter) a un objectif précis :

- **W2K Professionnel** : Conçu essentiellement pour les stations de travail et les postes clients de réseau. C'est cette version qui a remplacé Windows NT 4.0 Workstation.
- **W2K Server** : Conçu pour fournir des services et des ressources à d'autres systèmes du réseau. C'est elle qui remplace Windows NT 4.0 Server. Cette version est idéale pour les serveurs des fichiers et d'impression, les serveurs Web et les groupes de travail.
- **W2K Advanced Server** : Cette version prolonge les fonctionnalités de W2K Server. Elle reconnaît de très grandes quantités mémoires (64 Go) et jusqu'à 4 processeurs. Cette version est utilisée dans des réseaux de grandes entreprises et pour un travail intensif avec des bases de données.
- **W2K DataCenter Server** : C'est la version la plus évoluée de Windows 2000. elle reconnaît une mise en cluster plus complexe et jusqu'à 16 processeurs.

### 1.4. Configuration matérielle nécessaire :

- Minimum P133 MHz (PIII à 550 Mhz recommandé).
- 64 Mo de RAM pour la version professionnelle et 128 Mo pour la version Server (256 Mo recommandés au minimum, 4 Go maximum). La réactivité du système est proportionnelle à la quantité de mémoire.
- Minimum 2 Go (4 Go recommandés pour la version Server) d'espace disque sur la partition sur laquelle sera installé W2k dont 650 Mo d'espace libre pour la version professionnelle et 850 Mo d'espace libre pour la version Server.
- Carte réseau



- Carte vidéo SVGA

## 1.5. Différence entre partition primaire, secondaire, étendue et logique :

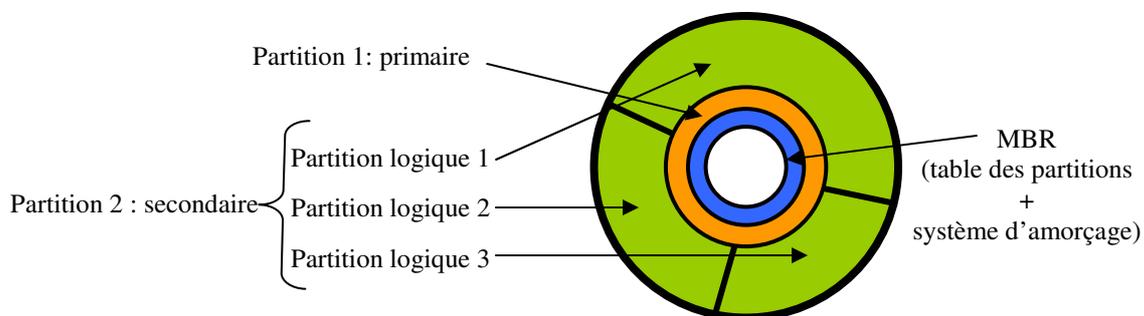
Un disque dur peut se décomposer en plusieurs **partitions primaires**. Le nombre de ces partitions primaires est limité à quatre (4). Afin de ne pas être limité par le nombre de partitions, il est préférable de désigner parmi ces partitions une en tant que **partition étendue** (ou **secondaire**), à l'intérieur de laquelle vous allez mettre des **partitions logiques** (jusqu'à 63 pour les disques IDE et jusqu'à 15 pour les disques SCSI).

Le **MBR** (Master Boot Recorder) : C'est une zone du disque très petite (512 octets), située sur les premiers secteurs du disque, avant la première partition physique. Le MBR est partagé en deux, la table des partitions et le système d'amorçage. Le MBR représente au disque ce que représente le secteur de boot à la partition (chaque partition a un secteur de boot).

Dans la **table des partitions** on enregistre les informations relatives aux partitions primaires : emplacement, taille, propriétés (cachée, amorçable). L'endommagement de cette partie fait perdre toutes les informations du disque.

Le **système d'amorçage** est un programme, stocké dans le MBR, exécuté par le BIOS au démarrage du PC pour lancer le système d'exploitation. Parfois il nous donne le choix du système d'exploitation avec lequel la machine démarre. Parmi ces systèmes un est mis par défaut. La commande `fdisk /mbr` sous DOS, sert à remettre le système d'amorçage par défaut (le réinstaller) sans effacer la table des partitions. Ceci sert par exemple à supprimer un virus situé dans le programme d'amorçage du MBR (ça ne marche pas avec les virus boot !).

Le **formatage** permet d'effacer le contenu du disque. Le formatage rapide efface seulement la table d'allocation des fichiers (partie permettant de localiser les fichiers sur le disque), par contre, le formatage bas niveau refait le découpage dès le début de la partition concernée. Il crée à nouveau les clusters (un cluster correspond à une unité d'allocation sur le disque. Minimum égal à un secteur et maximum 128 secteurs), écrit dans le secteur de boot de la partition le type du système de fichier et le nom de la partition, et il réécrit évidemment la table d'allocation des fichiers.



*Figure 1 : Structure d'un disque*



## 1.6. Différence entre FAT et NTFS :

Windows reconnaît seulement 3 systèmes de fichiers : FAT16, FAT32 et NTFS. Il ne peut donc pas lire les autres types de partitions.

<b>FAT32 (File Allocation Table)</b>	<b>NTFS (New Technology Filing System ou NT File System)</b>
C'est le système de fichier natif de Windows 98 et de Windows ME mais il est supporté par Windows XP/2000	C'est le système de fichier natif de Windows NT 2000 et de Windows XP. Il n'est pas compatible avec Win95 ni avec Win98. Les partitions formatées avec NTFS ne sont donc pas visibles sous DOS, Win9x ou Millenium. Elles ne peuvent donc être accédées qu'avec Windows NT/2000 ou XP.
Gère, en théorie, de moins de 1 Mo jusqu'à 1 To. Mais, avec Windows XP/2000, il ne supporte que 32 Go.	Gère des disques ayant des capacités comprises entre 10 Mo et 2 To. A cause de sa grande entête, NTFS ne peut pas être utilisé pour une disquette.
Adressage des clusters sur 32 bits.	Adressage des clusters sur 64 bits.
Taille maximale d'un fichier est de 4 Go.	Pratiquement pas de limite pour la taille des fichiers (2^64 clusters).
La table de référence des fichier est nommée FAT ( File Allocation Table). Elle a une taille fixe.	La table de référence des fichiers est nommée MFT (Master File Table). Elle une taille variable.
Le système NTFS est beaucoup plus performant que le système FAT. C'est un système de fichier de « journalisation » ; il est donc plus <b>sécurisé</b> , il reconnaît les erreurs ainsi que les mauvaises sections de disque et les corrige. NTFS supporte aussi les fichiers (dossiers) compressés, cryptés et les permissions d'accès aux fichiers, disque miroir ....	

La conversion de FAT en NTFS est possible grâce à la commande :

```
CONVERT volume /FS :NTFS
```

mais l'inverse n'est pas possible.

## 1.7. RIS

- Les services d'installation à distance (Remote Installation Service) permettent d'installer Windows 2000 Professionnel à distance, sans avoir à visiter chaque client. Pour pouvoir utiliser ce service, on doit le sélectionner lors de l'installation de W2k Server, quand Windows nous demande de choisir les composants Windows à installer.
- Pour créer une image de la machine sur le serveur, utilisez **RIPrep.exe** (\\NomDuServeurRIS\Reminst\Admin\I386\RIPrep.exe) qui permet de recueillir des informations sur la machine source (Paramètres, logiciels installés).



## 1.8. Préparation de l'installation (Preliminaires)

- Installation à partir du CD-ROM : Le CD-ROM d'installation fourni par Microsoft est bootable. Accédez au boot de votre PC et modifiez-le de telle manière à ce qu'il puisse booter avant tout sur le CD.
- Installation à partir du disque dur : recopiez le répertoire \i386 du CD d'installation sur le disque local C : dans le répertoire \install\ntwks, pour les postes clients, et sur \install\ntsrv pour le serveur.
- Vous devez posséder le CD des drivers. Sinon copiez la disquette de la carte réseau dans le répertoire \install\drivers\reseau et la disquette du pilote de la carte vidéo dans le répertoire \install\drivers\video.
- Clé de Windows Professionnel (client): **CWMC7-HB7Y2-MBQ9X-6BX4W-P7JQG**
- 
- Dans la salle des TP W2k, les PC. sont rangés par colonnes. Pour chacune des colonnes on installera 2 serveurs et 2 clients.



## 2. Installation

Remarque : Durant les installations, il faut lire attentivement les messages de Windows !

### Exercice N°1 : Installation de la version Serveur

- Après avoir rebooté à partir du CD d'installation de Windows 2000, créez une nouvelle partition d'environ 3 Go (2 Go minimum). Cette partition doit être formatée en NTFS. Donnez à cette partition le nom **groupe\_X** (où X est le n° de votre groupe).
- Sélectionnez cette partition puis appuyez sur *Entrer* ; Le programme d'installation formate la partition, examine le disque dur, puis copie les fichiers dans les dossiers d'installation de Windows 2000. A la fin de cette étape, l'ordinateur redémarrera automatiquement.
- Personnalisation du logiciel W2k : Par souci d'homogénéité, durant la configuration de Windows 2000 en mode GUI (*Graphical User Interface*), les étudiants doivent utiliser la même syntaxe.
  - o Votre nom : **Groupe-X**
  - o Utilisez le type de licence "**Par serveur**" avec 50 connexions.
  - o Nom d'ordinateur : **Serveur-X-Y** (où Y est le N° de la machine)
  - o Mot de passe : **mdp-serv-Y**Dans la réalité, le mot de passe doit être très compliqué et insignifiant pour qu'il soit difficilement devinable.
- Composants Windows à installer : laisser les composants par défauts. On en installera ce que dont on aura besoin dans les TP qui suivront.
  - \*
- A la fin de l'installation, Windows vous invite à configurer votre serveur. Avant de poursuivre cette configuration, installez la carte réseau de la présente machine (car les cartes réseau de certaines machines de la salle W2K ne sont pas détectées automatiquement par Windows 2000). Profitez l'occasion pour installer les autres drivers en suivant les différentes étapes du fichier "EtapasAsuivre.htm" du CD-ROM des drivers.
- Quand tout est fini, afin de laisser la machine opérationnelle pour les autres étudiants, accédez au fichier « boot.ini » et modifiez-le de telle sorte à ce qu'il nous donne le choix du système d'exploitation avec lequel la machine démarrera. Mettez l'ancien système, installé par les moniteurs, comme système de démarrage par défaut. Le fichier boot.ini devra ressembler à ceci :

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(3)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINNT="MS-W2k Server pour TP Admin_Syst
Groupe Y" /fastdetect
multi(0)disk(0)rdisk(0)partition(3)\WINNT="Microsoft      Windows      2000
professionnel" /fastdetect
```

\*



Remarques :

- 1- Pour des mesures de sécurité, à la fin de l'installation, au redémarrage de l'ordinateur accédez au BIOS et enlevez le boot sur CD-ROM.
- 2- Pensez aussi à changer les propriétés d'affichage (écran 600x800, mode 24 bits ...).
- 3- A chaque redémarrage, veuillez à démarrer avec notre système d'exploitation et non pas avec le système par défaut.



## Exercice N°2 : Installation de la version Client (W2k professionnel)

Les étapes sont relativement les mêmes que celles de l'exercice précédent, à l'exception de :

- Nom d'ordinateur : **Poste-X-Y** (où Y est le N° de votre machine)
- Mot de passe : **mdp-client-Y**
- Si Windows vous invite à adhérer à un « domaine » ou un « groupe de travail », choisissez, pour l'instant, de faire de votre ordinateur un membre d'un groupe de travail nommé « workgroup ». Plus tard, lors de la configuration du serveur, vous l'intégrerez au sein d'un domaine.
- Après l'installation, Windows affiche l'Assistant Identification Réseau qui vous aidera à connecter votre ordinateur au réseau. Cet assistant vous demande de spécifier qui peut ouvrir une session sur cet ordinateur. Il vous donne deux choix :
  - o Les utilisateurs doivent entrer un nom et un mot de passe pour utiliser cet ordinateur.
  - o Windows considère toujours que l'utilisateur suivant se connecte depuis cet ordinateur : (nom utilisateur, mot de passe).

L'option à choisir dépend de la stratégie que vous utilisez. Si une entreprise veut affecter un ordinateur à chaque employé et personne d'autre que ce dernier ne peut utiliser cet ordinateur, vous devez choisir la deuxième option. Mais dans notre cas (Ecole polytechnique), les étudiants utiliserons n'importe quel ordinateur disponible, choisissez alors le 1<sup>er</sup> cas.

- N'oubliez pas aussi d'installer les drivers et de changer le fichier « boot.ini » afin qu'il ressemble à ceci :

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(3)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(2)\WINNT="MS-W2k professionnel pour TP
Admin_Syst Groupe Y" /fastdetect
multi(0)disk(0)rdisk(0)partition(3)\WINNT="Microsoft Windows 2000
professionnel" /fastdetect
```

### Ouverture de session et compte utilisateur:

Pour pouvoir utiliser la machine sur laquelle doit travailler un utilisateur, il doit au préalable y ouvrir une session. Pour ceci il doit disposer du couple 'compte utilisateur-mot de passe'. Au cours de l'ouverture d'une session, W2K procède à l'authentification de l'utilisateur afin de vérifier son identité et de lui permettre ainsi d'accéder à toutes les ressources auxquelles il a le droit d'y accéder mais en fonction des autorisations qui lui ont été attribuées.



## Exercice N°3 : Configuration du 1<sup>er</sup> serveur du réseau

Après une installation "Standard" du serveur W2K, au redémarrage de la machine, la fenêtre "Configuration de votre serveur Windows 2000" s'ouvre automatiquement (cf. figure ci-dessous). Elle vous demande de configurer votre serveur.

Dans cet exercice, on va faire de l'une de nos machines (serveurs) notre premier contrôleur de domaine. Pour ceci, il faut choisir l'option 'Ceci est le seul serveur de mon réseau'.



Pour installer et configurer le présent serveur en tant que premier contrôleur de domaine, Windows a besoin de certaines informations :

Nom du domaine : **Polytech-Tours.**

Puisque nous possédons pas de nom de domaine public sur Internet, on ne va pas lui spécifier de nom du type NomDomaine.com . On le désignera comme étant '**local**'.

La procédure d'installation va durer plusieurs minutes. Le CD Windows 2000 Serveur vous sera demandé durant ce temps-là.

Si l'installation s'est bien déroulée, au redémarrage, Windows doit vous donner la possibilité de vous connecter au domaine 'Polytech-Tours'.



## Exercice N°4 : Rétrogradation d'un serveur

La commande « `dcpromo` » rétrograde un contrôleur de domaine en un serveur membre ou un serveur autonome (pour plus d'informations, voir TP suivant).

Si votre machine (contrôleur de domaine) est un serveur de catalogue global, vous devriez vous assurer que les utilisateurs de ce domaine peuvent accéder à d'autres catalogues globaux avant de supprimer Active Directory de l'ordinateur en question. Car les catalogues globaux sont utilisés pour traiter les ouvertures de session des utilisateurs.

Si votre serveur est le dernier contrôleur de domaine de votre domaine, après l'exécution de la commande `dcpromo`, le domaine n'existera plus et tous les comptes utilisateurs sur ce domaine seront supprimés.

Quand vous supprimez ce contrôleur de domaine, si vous avez des données cryptées, vous devez les décrypter avant de continuer, sinon elles ne seront plus jamais accessibles.

### Pratique :

Exécutez la commande `dcpromo` (Démarrer/Exécuter).

A la fin de l'exécution de cette commande, vous devez redémarrer l'ordinateur pour que les modifications prennent effet.

Si la commande `dcpromo` s'est bien exécutée, au redémarrage, vous constateriez qu'il n'y a plus de domaine 'Polytech-Tours'. Le système nous demande de (re) configurer le serveur.



## TP n° 2 et 3 :

# Configuration des serveurs

## 1. Configuration d'un serveur W2k

### 1.1. Introduction

La configuration du système se fait en fonction de son rôle sur le réseau. Pour ceci, généralement, on affecte les stations de travail et les serveurs à un **groupe de travail** ou un **domaine**.

### 1.2. Définitions

#### - Groupe de travail :

C'est un regroupement informel d'ordinateurs (10 ordinateur au Max car W2k professionnel par exemple prend en charge 10 connexions simultanées au Max) où chaque ordinateur est géré séparément. Si un ordinateur appartient à un groupe de travail, l'utilisateur peut ouvrir une session sur l'ordinateur local uniquement, car le compte utilisateur ne figure que dans la base de données de sécurité de l'ordinateur local. Chaque ordinateur d'un groupe de travail possède sa propre base de donnée de sécurité tandis qu'il n'existe qu'une seule base de données d'annuaire dans un domaine. Sur un groupe de travail, un utilisateur doit disposer d'un compte sur chaque ordinateur auquel il souhaite accéder.

#### - Domaine :

C'est un regroupement d'ordinateurs géré collectivement par des **contrôleurs de domaine** (le contrôleur de domaine est le serveur W2K qui gère l'accès au réseau) à l'aide de répertoires et ressources partagées. Chaque domaine est géré par un contrôleur de domaine. Ces ordinateurs qui forment un domaine partagent une zone commune de stockage des informations de sécurité. Un domaine permet donc de centraliser l'administration des ressources réseau. Il permet de :

- Ouvrir une session unique pour accéder aux différentes ressources réseau (fichiers, imprimantes, applications, ...).
- Avoir un compte utilisateur unique pour accéder à n'importe quel ordinateur.
- Faire une administration centralisée. Ce qui veut dire que, toutes les informations relatives aux comptes d'utilisateurs et aux ressources peuvent être gérées à partir d'un emplacement unique du domaine.
- Localiser simplement des données. Par exemple, le fait de publier une imprimante, permet aux utilisateurs de la sélectionner dans la liste des objets du domaine. Par contre, si elle n'est pas publiée, les utilisateurs peuvent toujours accéder à cette imprimante mais ils doivent en préalable en connaître l'emplacement.
- ...

⇒ En résumé :

Groupe de travail      décentralisation (chaque station gère et sécurise ses propres ressources).

Domaine              centralisation (la gestion et la sécurité sont gérés par un contrôleur de domaine. L'utilisateur peut se connecter sur n'importe quelle machine).



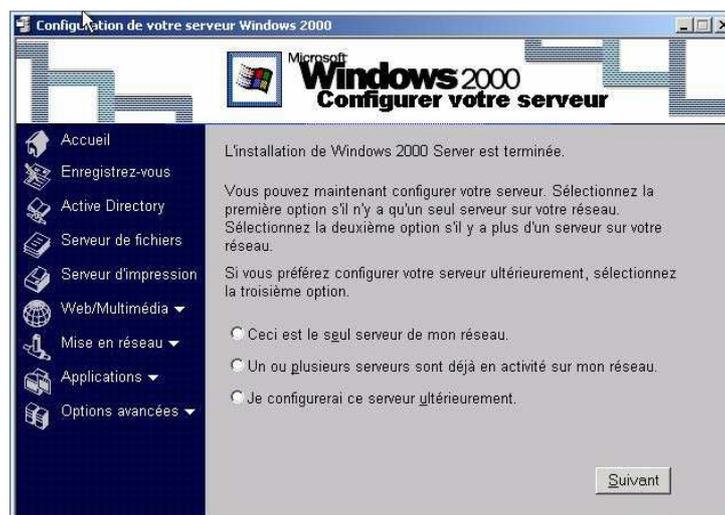
Une **arborescence** est une organisation hiérarchique des domaines. Lorsque on ajoute un domaine (exemple étudiant) à une arborescence existante (exemple : univ-tours.fr), il devient le sous-domaine d'un domaine de cette structure (etudiant.univ-tours.fr).

L'emplacement dans lequel W2k organise les informations relatives au membres d'un domaine est appelé **Active Directory** (service d'annuaire de W2k).

### 1.3. Différentes configurations possibles de W2k Server

Un serveur Windows 2000 est configuré selon les services qu'il offre. On peut lui ajouter ou enlever des services à tout moment grâce à l'utilitaire « **configurer votre serveur** » (Démarrer/Programmes/Outils d'administration/Configurer votre serveur).

Après une installation "Standard" du serveur W2K, quelques composants requièrent une phase de configuration. La fenêtre "**Configuration de votre serveur 2000**" s'ouvre automatiquement au démarrage de la machine. Si vous ne voulez pas faire cette configuration à l'instant même, vous pouvez la faire ultérieurement en cliquant sur "Démarrer/Programmes/Outils d'administration/Configurer votre serveur".



*La fenêtre Configuration du serveur*

W2K Server peut être configuré en tant que serveur membre, contrôleur de domaine ou serveur autonome.

- Un **serveur membre** fait partie d'un domaine mais ne stocke pas d'informations de répertoire .
- Un **contrôleur de domaine** est comme un serveur membre mais il stocke des informations de répertoire et rend des services d'authentification pour le domaine.
- Un **serveur autonome** ne fait pas partie d'un domaine et dispose de sa propre base de donnée utilisateur. Pour ouvrir une session sur ce serveur, c'est lui même qui fait l'authentification.



## 1.4. Que peut-on configurer avec l'Assistant de Configuration de votre serveur ?

Cet assistant vous permet de configurer les paramètres suivants :

- **Active Directory** : Configuration serveur en tant que contrôleur de domaine.
- **Serveur de fichiers** : Créer les dossiers partagés à stocker sur le serveur.
- **Serveur d'impression** : Configurer une imprimante locale ou réseau et la faire publier dans Active Directory.
- **Web/Multimédia** : Utilisation des services Internet pour configurer un site Web ou FTP sur le réseau intranet de votre entreprise.
- **Mise en réseau** : Pour sélectionner les services de gestion de réseau que vous souhaitez utiliser.
- **Application** : Pour configurer l'ordinateur en tant que serveur d'applications.
- **Options avancées** : Pour définir des configurations avancées (mise en file d'attente des messages, support technique de Windows 2000 ....).

## 1.5. Outils d'administration :

La section suivante recense les principaux outils graphiques d'administration. Pour accéder à ces outils, cliquez sur Démarrer/Programmes/Outils d'administration puis sélectionnez l'outil dont vous avez besoins.

Outil d'administration	Usage
Configurer votre serveur	Ajoute, supprime et configure les services Windows pour le réseau.
DNS	Gère le service DNS (Domain Name Service)
Domaines et approbation Active Directory	Gère les relations d'approbation entre domaines.
Utilisateurs et ordinateurs Active Directory	Gère les utilisateur, les groupes, les ordinateurs et d'autres objets de Active Directory.
Système de Fichier distribué (DFS)	Crée et gère les systèmes de fichier distribués qui connectent les dossiers partagés de différents ordinateurs.
Site et services Active Directory	Crée des sites pour gérer la réplication des informations utilisées pour Active Directory.
Stratégie de sécurité du contrôleur de domaine	Crée et gère les stratégies de sécurité du contrôleur de domaine actif.
Stratégie de sécurité locale	Gère les stratégies de sécurité de l'ordinateur local.
Gestion de l'ordinateur	Démarre et arrête les services, gère les disques et gère l'accès aux autres outils de gestion système.
performances	Affiche des graphes relatifs aux performances système et configure les journaux.
Observateur d'événements	Gère les événements et les journaux.
Moniteur réseau Microsoft	Surveille le trafic du réseau et résout les problèmes réseaux.
Gestionnaire des services Internet	Gère les serveurs Web, FTP et SMTP.
Routage et accès distant	Configure et gère le service de routage et d'accès distant qui contrôle les interfaces de routage, le routage IP dynamique et l'accès à distance.
Services d'authentification Internet	Gère l'authentification, les autorisations et les comptes des utilisateurs Internet distants.
DHCP	Configure et gère le service DHCP (Dynamic Host Configuration Protocol).



## Active Directory

### 2. Active Directory

#### 2.1. C'est quoi Active Directory :

Active Directory est le service d'annuaire de W2k. Il stocke les informations sur les objets réseau, fournit une structure hiérarchique qui facilite l'organisation des domaines et des ressources (fichiers, imprimantes ...) et offre des outils d'administration personnalisables qui facilitent et simplifient l'administration de ces ressources sur le réseau. Un seul compte d'utilisateur de domaine dans Active Directory est requis pour que l'utilisateur puisse accéder à l'ensemble des ressources réseau partagées du domaine. Parmi les objets que regroupe Active Directory, on trouve :

- Les comptes utilisateurs,
  - Les comptes groupes,
  - Les comptes machines,
  - Les imprimantes partagées,
  - Les dossiers partagés, ....
1. Pour installer Active Directory, il faut un volume NTFS et un serveur DNS, s'il n'y en a pas, l'assistant vous proposera d'en installer un.
  2. Après l'installation d'active Directory, votre serveur deviendra contrôleur de domaine. S'il y avait déjà un contrôleur de domaine sur le réseau, vous pouvez installer votre serveur en tant que contrôleur de domaine supplémentaire, d'un nouveau domaine enfant, d'une nouvelle arborescence ou d'une nouvelle forêt.
  3. Certains étudiants peuvent attendre donc la fin de la configuration des serveurs de leurs collègues pour qu'ils fassent de leurs serveurs des contrôleurs de domaines supplémentaires.

#### 2.2. Remarques :

1. Les domaines qui utilisent Active Directory ne peuvent fonctionner qu'avec un contrôleur de domaine.
2. Puisque tout contrôleur de domaine peut traiter les modifications de répertoire et les répliquer automatiquement dans d'autres contrôleurs de domaines, il est utile de configurer plusieurs contrôleurs de domaines pour un même domaine. Si un contrôleur tombe en panne, les autres contrôleurs peuvent prendre le relais pour gérer l'authentification ainsi que d'autres tâches critiques. Il est intéressant d'avoir au moins 2 contrôleurs de domaines. Cela permet une répartition des charges et aussi d'avoir une réplification de la base Active Directory (la base est distribuée).
3. Pour rendre un « serveur membre » « contrôleur de domaine », il suffit de lui installer le composant Active Directory au lieu de réinstaller tout le système d'exploitation. A l'inverse, on peut rétrograder un contrôleur de domaine au rang de serveur membre. Pour ceci on exécute la commande `dcpromo` (Démarrer/Exécuter).
4. **Duplication** : La duplication permet de mettre à jour la base d'annuaire d'Active Directory sur l'ensemble des contrôleurs du domaine. Elle se fait généralement 5 minutes après chaque modification. On peut lancer la duplication en mode manuel en choisissant dans la console « *Site et services d'Active Directory* », la fonction « *répliquer maintenant* ».



### 2.3. Question :

Votre ordinateur est-il membre d'un domaine ?

Réponse :

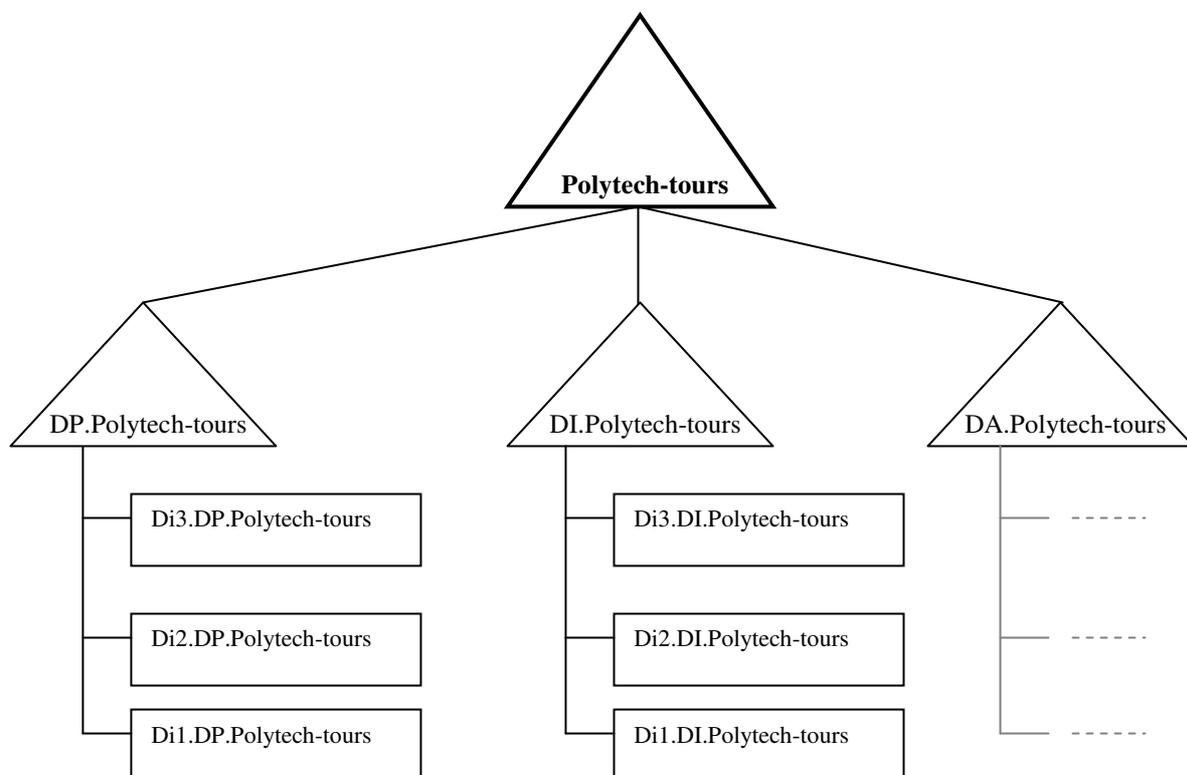
Quand vous appuyez sur Ctrl+Alt+Suppr puis sur « Option », si aucun domaine ne s'affiche dans la zone « se connecter à » alors votre ordinateur n'est membre d'aucun domaine.

### 2.4. Exercice 1 : Installer Active Directory

Avant d'installer Active Directory sur notre serveur, nous devons au préalable penser à l'architecture de notre réseau pour savoir s'il faut créer:

- Une nouvelle forêt
- Une nouvelle arborescence
- Un nouveau domaine enfant
- ...

Dans cet exercice, la première des choses qu'il faut faire est la création d'une nouvelle forêt et d'une nouvelle arborescence. Ceci se fera durant l'installation du premier contrôleur du domaine. Puis on créera de nouveaux domaines enfants du domaine « Polytech-Tours » suivant la figure ci-dessous. C'est durant l'installation des autres serveurs, qu'on installera les autres domaines enfants du domaine 'Polytech-Tours'. On créera dans cet exercice plusieurs sous-domaines enfants du domaine 'Polytech-Tours'. Ces domaines représenteront 3 départements de l'Ecole Polytechnique, DA pour département Aménagement, DI pour département Informatique et DP pour département Productique.





## 1. Installation d'Active Directory sur le premier serveur du domaine :

Pour configurer un serveur en tant que contrôleur de domaine, il faut lui installer Active Directory. L'installation d'Active Directory sur le premier serveur du domaine se fait de la même manière que celle de l'exercice N°3 (Configuration du 1<sup>er</sup> serveur du réseau) du précédent TP. Pour la configuration du premier contrôleur de domaine, sélectionnez la case « ceci est le seul serveur de mon réseau ».

## 2. Installation d'Active Directory sur les autres serveurs du domaine :

Pour installer Active Directory sur les autres serveurs, on suivra les étapes suivantes :

- Ouvrir la fenêtre « Configuration de votre serveur » puis cliquer sur « Active directory », sur « Démarrer l'assistant de configuration » puis sur « Suivant ».
- Puisqu'il y a déjà un contrôleur de domaine sur le réseau (celui du domaine Polytech-Tours), après l'ouverture de la fenêtre « Configuration de votre Serveur windows 2000 », il faut sélectionner la case 'un ou plusieurs serveurs sont déjà en activité sur mon réseau'. On installera donc notre serveur en tant que « Contrôleur d'un nouveau domaine enfant ».
- Puisqu'on ne créera pas de nouvelles arborescences, vous devez sélectionner la case « Créer un nouveau domaine enfant dans une arborescence de domaine existante ».
- Pour s'intégrer à un domaine existant, il faut donner le nom utilisateur et le mot de passe du domaine parent auquel on veut se connecter (Polytech-Tours).
  - Nom utilisateur : **Administrateur**
  - Mot de passe : **mdp-serv-Y** (ex mdp-serv-21)
  - Domaine : **Polytech-Tours**
- Avant de faire entrer le nom du nouveau domaine enfant, vous devez rentrer le nom DNS complet du domaine parent. Taper « **Polytech-Tours.local** » ou sélectionnez-le en appuyant sur le bouton « Parcourir ».
- Nom du nouveau domaine enfant :
  - Sur le 2<sup>ème</sup> serveur tapez : **DI** (le premier serveur est le serveur du domaine parent)
  - Sur le 3<sup>ème</sup> serveur tapez : **DP**
  - Sur le 4<sup>ème</sup> serveur tapez : **DA**
- Pour le nom DNS complet tapez :
  - **DI.Polytech-Tours.local**
  - **DP.Polytech-Tours.local**
  - **DA.Polytech-Tours.local**
- Nom NetBIOS: (pas plus de 14 caractères. Ce nom est utilisé pour les versions précédentes de Windows).
  - **DI**
  - **DP**
  - **DA**
- Emplacement de la base de données et journal : Pour des raisons de performance, il est préférable de stocker la base de données et le journal sur des disques durs distincts. Pour ce TP, on n'utilisera que la partition qui nous a été réservée on laissera donc l'emplacement par défaut (Lecteur:\WINNT\NTDS).
- Volume système partagé : idem, laisser le chemin par défaut. (c'est la liste du contenu de ce dossier, dossier Sysvol, qui est répliquée vers tous les contrôleurs de domaines dans le domaine).



Dans le cas où le serveur DNS n'est pas installé : ⇒ au moment où le système essaye de contacter le serveur DNS qui devait gérer le domaine « *DI.Polytech-Tour* » (ou *DP.Polytech-Tours*, ...) que nous venons de créer (pour voir s'il acceptera la MAJ dynamique), il ne le trouvera pas. On doit alors installer et configurer ce serveur DNS.

- Si vous utilisez des serveurs sur lesquels fonctionne une version antérieure à Windows 2000, choisissez « *Autorisation compatible avec les versions antérieures à Windows 2000* » sinon choisir l'autre option. Cette 2<sup>ème</sup> option est plus intéressante car elle ne permet pas de se connecter aux utilisateurs anonymes. Seuls les utilisateurs authentifiés peuvent lire les informations sur ce domaine.
  - Mot de passe d'administrateur pour restaurer le service d'annuaire : « **restor-annu-x-y** » où x et y sont les variables précédentes.
- 
- Autorisations : Choisissez « *Autorisations compatibles uniquement avec les serveurs Windows 2000* » car on n'utilise pas sur nos autres serveurs des versions antérieures à Windows 2000. cette option est plus intéressante car elle ne permet pas aux utilisateurs anonymes de se connecter.
  - Mot de passe administrateur de restauration des services d'annuaire : **mdp-restore-annu-X-Y** (ex. mdp restor-annu-1-20). Ce mot de passe sera utilisé si l'ordinateur démarrera en mode Restauration des Services d'Annuaire.
  - Le résumé des tâches effectuées s'affiche puis la configuration d'Active Directory commence (patience, elle peut prendre plusieurs minutes). A la fin de cette étape, Windows vous confirme la fin et le bon déroulement de l'installation d'Active Directory et vous demande de redémarrer la machine pour que les modifications prennent effet.
  - Au redémarrage, Windows vous donnera la possibilité de vous connecter soit au domaine « *Polytech-Tours* » soit à son sous-domaine « *DI* » (ou *DP* si vous êtes sur le 3<sup>ème</sup> serveur ...).

## 2.5. Remarque :

Si vous utilisez le programme *dcpromo.exe* (ou si vous exécutez à nouveau l'assistant d'installation d'Active Directory), cela supprimera Active Directory et votre serveur redevient un serveur autonome (ou membre d'un domaine).

La rétrogradation d'un serveur de domaine (contrôleur de domaine) le transforme en un serveur membre mais s'il est le dernier contrôleur de domaine, ça le transforme en serveur autonome.



### 3. Gestion des machines et des utilisateurs

#### 3.1. Création et gestion de comptes d'ordinateurs

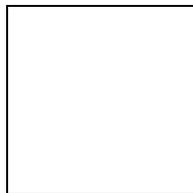
Les comptes d'ordinateurs sont stockés dans Active Directory sous forme d'objets. Ils vous permettent de contrôler l'accès au réseau et à ses ressources.

Nous verrons dans ce TP deux manières pour créer un compte d'ordinateur. La première se fait en créant des comptes d'ordinateurs dans le composant « Utilisateurs et ordinateurs Active Directory », la seconde, est la plus simple, se fait à partir du poste client.

#### Exercice N° 2 : Créer des comptes d'ordinateurs dans le composant « Utilisateurs et ordinateurs Active Directory »

Cette manière de créer un compte d'ordinateur se fait sur le serveur (le contrôleur du domaine). L'installation sur le poste client se fait à distance.

- 1- Ouvrir le composant « Utilisateurs et ordinateurs Active Directory » (Démarrer/programmes/Outils d'administration/Utilisateurs et ordinateurs Active Directory).
- 2- Dans l'arborescence de la console « Utilisateurs et ordinateurs Active Directory », cliquez du bouton droit sur le conteneur dans lequel vous souhaitez placer le compte ordinateur.
- 3- Cliquez sur 'Nouveau' puis sur 'Ordinateur' (cf. figure suivante). Sur la nouvelle boîte de dialogue 'Nouvel objet - Ordinateur' qui apparaît, entrez le nom de l'ordinateur client (ex Poste-1-19).



- 4- Cliquez sur « Modifier » si vous voulez autoriser un utilisateur ou un groupe différent des membres de Admins du domaine à effectuer cette opération (joindre cet ordinateur au domaine). Utilisez ensuite la boîte de dialogue « Sélectionner utilisateur ou groupe » pour sélectionner un compte d'utilisateur ou de groupe (vous pouvez sélectionner un compte d'utilisateur ou de groupe existant).



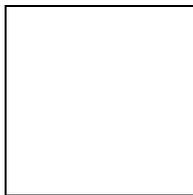
- 5- Si les systèmes Windows NT peuvent se servir de ce compte, cochez la case 'Autoriser les ordinateurs fonctionnant avec une version antérieure à Windows 2000 à utiliser ce compte'. Puis cliquez sur 'OK'.  
(Windows peut sauter les 2 étapes suivantes :)
- 6- Cochez la case 'Ceci est un ordinateur pris en charge', puis entrez l'Identifiant Unique Global (GUID) de l'ordinateur client (ou son l'UUID). Le GUID et l'UUID sont fournis par le fabricant. Le GUID a la forme cccccccc-cccc-cccc-cccc-cccccccccccc où c est un chiffre hexadécimal (ex. 601c59a3a78dd711ba3700c09f21d5ca). Vous pouvez avoir le GUID et l'UUID du poste client sur l'étiquette qui est collée derrière cette machine, vous pouvez aussi les trouver dans son BIOS.
- 7- Précisez quel serveur hôte effectuera l'installation à distance en choisissant l'une des options suivantes :
  - 'Tout serveur d'installation à distance disponible' : (dans ce cas, tout serveur disponible peut installer à distance l'ordinateur pris en charge.
  - 'Le serveur d'installation à distance suivant'
- 8- Cliquez sur 'Suivant' puis sur 'Terminer'.

**Remarque :** Si les outils d'installation à distance ne sont pas installé sur le serveur, il n'exécutera pas les étapes 6 et 7 (introduction du GUID et choix du serveur hôte qui effectuera l'installation à distance).

### Exercice N° 3 : Création d'un compte d'ordinateur à partir du poste client

Le moyen le plus facile pour créer un compte d'ordinateur est de le faire à partir du poste client. Pour ceci, il faut ouvrir une session sur l'ordinateur à configurer puis le joindre au contrôleur du domaine en suivant les étapes suivantes :

- 1- Ouvrir une session sur le poste client (station de travail ou serveur) à configurer.
- 2- Cliquez sur démarrer/paramètres/connexions réseau et accès à distance.
- 3- Cliquez sur identification réseau puis sur « Propriétés » dans l'onglet « Identification réseau ».
- 4- Dans « Membre de » choisissez « Domaine » et remplissez la zone avec le nom du domaine auquel vous voulez vous connecter (ex. Polytech-Tours).





- 5- Pour joindre le poste client au domaine, vous devez avoir l'autorisation de le faire. Utilisez alors le compte de l'Administrateur du contrôleur de domaine auquel vous voulez vous connecter.
- 6- Un message de bienvenue au domaine sera affiché. Vous devez redémarrer l'ordinateur pour que les modifications soient prises en comptes.
- 7- Au redémarrage, Windows vous donne le choix de connexion au domaine ou de travailler juste en local (sur l'ordinateur). Pour vous connecter au domaine, vous devez avoir les droits d'accès. Utilisez donc le compte d'un utilisateur du domaine.

Sur le serveur, si vous ouvrirez la fenêtre « Utilisateurs et ordinateurs Active Directory », vous trouverez dans le dossier « Computers » (ou Ordinateurs) le nom de l'ordinateur que vous venez de joindre au domaine.

#### **Exercice N° 4 : Se connecter à un domaine**

Vous pouvez travailler avec tout domaine de la forêt à condition de disposer des autorisations d'accès. Pour vous connecter à un domaine :

- Dans « Utilisateurs et Ordinateurs Active Directory », dans l'arborescence de la console, cliquez avec le bouton droit sur « Utilisateurs et ordinateurs Active Directory ». Sélectionnez ensuite « Se connecter au domaine ».
- La boîte de dialogue « Se connecter au domaine » affiche le domaine en cours (ou par défaut). Cliquez sur « Parcourir » et sélectionnez un domaine dans la boîte de dialogue « Rechercher le domaine ».

Les mêmes étapes sont valables pour se connecter à un contrôleur de domaine.

#### **Exercice N° 5: Afficher et modifier les propriétés d'un compte d'ordinateur**

Pour afficher et modifier les propriétés d'un compte d'ordinateur, procédez comme suit :

- Dans le menu « Outils d'administration », sélectionnez « Utilisateurs et ordinateurs Active Directory ».
- Dans l'arborescence de la console, développez le nœud du domaine en cliquant sur le signe '+' qui le **jouste**.
- Avec le bouton droit, cliquez sur le compte avec lequel vous vous souhaitez travailler, puis sélectionnez 'Propriétés'. La boîte de dialogue qui apparaît vous permet d'afficher et de modifier les paramètres du compte en question.

#### **Exercice N° 6: Activer/désactiver ou supprimer des comptes d'ordinateurs**

Pour activer/désactiver ou supprimer un compte d'ordinateur (si ce compte n'est plus nécessaire), procédez comme suit :

- Démarrer « Utilisateurs et ordinateurs Active Directory ».
- Dans l'arborescence de la console, cliquez sur le conteneur dans lequel se trouve le compte d'ordinateur en question. Ensuite cliquez sur le bouton droit sur cet ordinateur.
- Dans la fenêtre qui apparaît, faites votre choix. Sélectionnez 'Supprimer' pour supprimer le compte, 'Désactiver' pour désactiver le compte ou sur 'Activer' pour l'activer. Puis cliquez sur 'OK'.

Si le compte est précédé d'un X dans un cercle rouge, cela veut dire que le compte d'ordinateur est déjà désactivé.

Si le compte est en cours d'utilisation, vous ne pourrez pas le supprimer. Pour pouvoir le déconnecter, vous devez soit l'éteindre ou déconnecter sa session dans le dossier 'Session' dans la console « Gestion de l'ordinateur ».



## Exercice N° 7: Déplacer des comptes d'ordinateur

Généralement, les comptes d'ordinateurs sont placés dans les conteneurs suivants : Ordinateurs (Computers), Contrôleurs de domaines (Domaine Controlers) ou Unités d'organisation personnalisées. Mais vous pouvez leur changer de places (conteneurs). Pour cela, il faut suivre les étapes suivantes :

- Dans l'arborescence de la console « Utilisateurs et ordinateurs Active Directory », cliquez sur le conteneur dans lequel se trouve le compte d'ordinateur.
- Cliquez du bouton droit sur le compte d'ordinateur à déplacer, puis sélectionnez 'Déplacer'.
- Dans la boîte de dialogue 'Déplacer' qui apparaît, sélectionnez le conteneur dans lequel vous voulez placer l'ordinateur. Puis cliquez sur 'OK'.

*Exo 7 : Gérer des ordi*



**Question: Comment choisir le domaine auquel vous voulez vous connecter?**

**R :** Pour choisir le domaine auquel on veut se connecter sous W2K, après avoir appuyé sur Ctrl+Alt+Suppr, cliquez sur *option* (pour afficher la zone « *se connecter à* » afin de choisir l'un des domaine disponibles ou de se connecter tout simplement en local.

**Ouverture de session sur un domaine :**

Pour ouvrir une session sur un domaine W2K, après avoir appuyé sur ctrl+alt+suppr, l'utilisateur doit rentrer son **nom d'utilisateur** principal (nom d'utilisateur principal = nom d'ouverture de session suivi de @ et du suffixe du nom utilisateur, par exemple alice@etu.univ-tours.fr . Le @ et le suffixe sont à négliger, il suffit donc de taper par exemple alice) ainsi que son **mot de passe** puis appuyer sur **OK**.

**Question: Comment déterminer le type de réseau auquel vous appartenez ?**

**R :** Pour déterminer le type de réseau auquel vous appartenez, il faut afficher la boîte de dialogue des propriétés système en cliquant sur le bouton droit de la souris sur l'icône « Poste de travail » puis choisir l'onglet « Identification réseau ».



## 3.2. Création et gestion des comptes d'utilisateurs

En tant qu'administrateur, vous devez permettre aux utilisateurs de votre entreprise d'accéder aux diverses ressources réseau dont ils ont besoin. Les comptes d'utilisateurs permettent aux utilisateurs d'ouvrir des sessions et d'accéder aux ressources locales ou de domaine. Dans ce qui suit, on verra comment créer des comptes d'utilisateurs locaux et des comptes d'utilisateurs de domaine, et à en définir les propriétés.

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

Les noms d'ouverture de session et les noms complets des utilisateurs doivent être uniques. Les noms d'ouverture de session ne doivent pas dépasser 20 caractères. Il est formé d'une combinaison de caractères spéciaux et alphanumériques à l'exception des caractères suivant : " / \ [ ] ; = , + \* ? < > .

Attention : La zone de saisie vous permet de saisir plus de 20 caractères mais le système ne prend en considération que 20 caractères.

### 3.2.1. Option des comptes utilisateurs

Les options des comptes d'utilisateur permettent de contrôler dans quelle mesure un utilisateur accède au domaine ou à un ordinateur. Par exemple, vous pouvez limiter la plage horaire durant laquelle un utilisateur peut ouvrir une session sur le domaine, et les ordinateurs à partir desquels il peut ouvrir des sessions. Vous pouvez aussi indiquer la date d'expiration d'un compte d'utilisateur. Ces procédures permettent de maintenir la sécurité requise sur votre réseau.

#### a) Heures d'ouverture de session

Vous pouvez définir des heures d'ouverture de session pour les utilisateurs qui n'ont besoin d'accéder au domaine ou aux ordinateurs qu'à des heures particulières. Par exemple, vous pouvez définir pour les membres d'une équipe de nuit des heures d'ouverture de session qui ne leur permettent d'ouvrir des sessions que durant leurs heures de travail.

#### b) Ordinateurs à partir desquels les utilisateurs peuvent ouvrir une session

Par défaut, les utilisateurs peuvent ouvrir une session sur le domaine à partir de tout ordinateur du domaine. Vous pouvez configurer des options de compte pour préciser les ordinateurs à partir desquels les utilisateurs peuvent ouvrir des sessions. Ainsi, vous pouvez permettre à certains utilisateurs de n'ouvrir une session sur le domaine qu'à partir de leur ordinateur, par exemple les employés temporaires. Cette procédure empêche ces utilisateurs d'ouvrir une session sur les autres ordinateurs et d'accéder aux informations stratégiques stockées sur ceux-ci.

#### c) Expiration du compte

Vous pouvez définir une date d'expiration sur un compte d'utilisateur pour qu'il soit désactivé lorsque l'utilisateur concerné n'a plus besoin d'accéder au réseau. Par exemple, pour des raisons de sécurité, vous pouvez définir des comptes d'utilisateur pour les employés temporaires de telle sorte qu'ils expirent à la date de fin de leur contrat.



### 3.2.2. Types de compte

Trois types de comptes utilisateurs existent : compte d'utilisateur local, compte d'utilisateur de domaine et compte d'utilisateur prédéfini [Source : *documentation Microsoft*].

1. **Compte d'utilisateur local** : ce compte permet à un utilisateur d'ouvrir une session sur un ordinateur particulier pour en utiliser les ressources. Ce type de compte d'utilisateur réside dans le Gestionnaire de comptes de sécurité (SAM, Security Accounts Manager) de l'ordinateur. L'utilisateur qui a ce type de compte ne peut donc accéder aux ressources d'un autre ordinateur que s'il dispose d'un compte distinct sur celui-ci.  
Vous ne pouvez créer de comptes d'utilisateur locaux que sur des ordinateurs exécutant Windows 2000 Professionnel et sur des serveurs autonomes ou membres exécutant Windows 2000 Server ou Windows 2000 Advanced Server.  
Ne créez pas de comptes d'utilisateur locaux sur des ordinateurs faisant partie d'un domaine, car le domaine ne reconnaît pas les comptes d'utilisateur locaux et, de ce fait, le compte d'utilisateur ne permettrait d'accéder qu'aux ressources de cet ordinateur.
2. **Compte d'utilisateur de domaine** : ce compte permet à un utilisateur d'ouvrir une session sur le domaine pour accéder aux ressources réseau. L'utilisateur peut accéder aux ressources réseau à partir de tout ordinateur du réseau, avec un même compte d'utilisateur et un même mot de passe. Ce type de compte d'utilisateur réside sur un contrôleur de domaine dans le service d'annuaire Active Directory. Il est ensuite dupliqué automatiquement sur tous les autres contrôleurs de domaine. Vous pouvez créer le compte d'utilisateur de domaine dans le dossier Users par défaut, ou dans un autre dossier créé pour recevoir les comptes d'utilisateur de domaine.
3. **Compte d'utilisateur prédéfini** : ce compte permet à un utilisateur d'effectuer des tâches administratives ou d'accéder provisoirement aux ressources réseau. Il existe deux comptes d'utilisateur prédéfinis, qu'il est impossible de supprimer : Administrateur et Invité. Les comptes d'utilisateur locaux Administrateur et Invité résident dans le Gestionnaire SAM, et les comptes d'utilisateur de domaine Administrateur et Invité résident dans Active Directory. Ces comptes prédéfinis sont automatiquement créés lors de l'installation de Windows 2000 et d'Active Directory.

### 3.2.3. Types d'utilisateur

Quand vous créez un compte, Windows vous demande de spécifier quel type d'utilisateur choisir pour ce compte. 3 types existent, le type :

- **Standard** : un utilisateur possédant ce genre de compte peut installer des programmes sur l'ordinateur, il peut même modifier la configuration de cet ordinateur.
- **Restreint** : l'utilisateur de ce compte a des pouvoirs très restreints. Il peut juste accéder à la machine, l'utiliser et enregistrer son travail. Il ne peut ni installer des programmes ni modifier la configuration de l'ordinateur.
- **Autre** : ce compte est réservé généralement pour des administrateur secondaires ...



## Exercice 1 : Création d'un compte d'utilisateurs local

### 1) Sur le serveur :

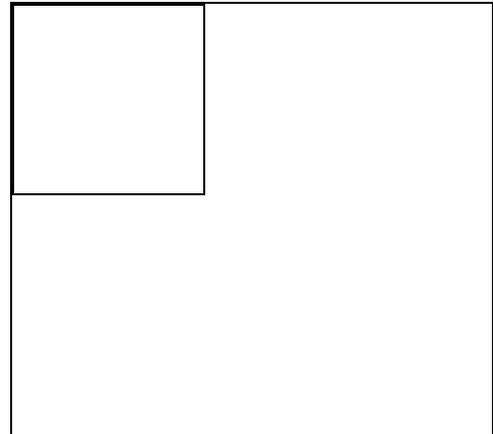
#### a) Si le serveur n'est pas un contrôleur de domaine

- Cliquer sur « Démarrer / Programmes / Outils d'administration / Gestion de l'ordinateur »
- Dans la console Gestion de l'ordinateur, développez « Utilisateurs et groupes locaux ».
- Cliquez avec le bouton droit sur le dossier « Utilisateurs », puis cliquez sur « Nouvel utilisateur ».

Pour le nom d'utilisateur, donnez : utilisateur-local1, utilisateur-local2,...

Pour le mot de passe, donnez : mdp-local1, mdp-local2,...

- Activez la ou les cases à cocher appropriées pour définir les restrictions du mot de passe.
- Cliquez sur « Créer » pour créer le compte d'utilisateur.



#### b) Si le serveur est un contrôleur de domaine

Si le serveur est un contrôleur de domaine alors il ne peut pas avoir des utilisateurs locaux ou des groupes locaux. Pour ajouter un utilisateur local, sur un poste client, à partir du contrôleur du domaine, suivez ces étapes :

- Ouvrez « Démarrer/ Programmes/ Outils d'administration/ gestion de l'ordinateur ».
- Cliquez avec le bouton droit sur l'entrée « Gestion de l'ordinateur » de l'arborescence de la console, puis sélectionnez « Se connecter à un autre ordinateur » dans le menu contextuel. Vous pouvez alors choisir le système (ou l'ordinateur) dont vous souhaitez gérer le compte local.
- Développez le nœud « Outils système » en cliquant sur le signe '+' qui le jouxte, puis sélectionnez « Utilisateurs et groupes locaux ».
- Cliquez avec le bouton droit sur « Utilisateurs » puis sélectionnez « Nouvel utilisateur ».

### 2) Sur le client :

Pour créer un compte d'utilisateur local sur un poste client, ouvrez « panneau de configuration / utilisateur et mot de passe ».

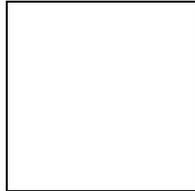
- a) Si l'ordinateur ne fait pas partie d'un domaine, cliquez sur « Ajouter ».
- b) Si l'ordinateur fait partie d'un domaine, vous ne pouvez ajouter que des utilisateurs de domaines existants en cliquant sur « Ajouter » dans « Utilisateurs et mot de passe ».
  - Pour ajouter un nouvel utilisateur local (qui n'a pas été ajouté au préalable par le contrôleur de domaine), cliquez sur l'onglet « Options avancées » puis cliquez sur le bouton « Avancé ». Dans « Utilisateurs et groupes locaux », cliquez sur « Utilisateurs », sur « Action », puis sur « Créer un utilisateur ».



## Exercice 2 : Création d'un compte d'utilisateur de domaine

Pour créer un compte d'utilisateur de domaine, suivez les étapes suivantes :

- À partir du menu « Outils d'administration », ouvrez la console « Utilisateurs et ordinateurs Active Directory », puis développez le domaine dans lequel vous souhaitez ajouter un compte d'utilisateur.
- Cliquez avec le bouton droit sur le dossier qui contiendra le compte d'utilisateur, pointez sur « Nouveau », puis cliquez sur « User ».



Une fenêtre s'ouvre. Elle contient les champs suivant :

**Prénom** : Prénom de l'utilisateur.

**Initiales** : Diminutif de l'utilisateur. Il ne s'agit pas d'une entrée obligatoire.

**Nom** : Nom de famille de l'utilisateur.

**Nom détaillé** : Nom complet de l'utilisateur. Ce nom doit être unique dans le dossier dans lequel vous créez le compte. Windows 2000 complète automatiquement cette option si vous avez entré des informations dans les zones Prénom ou Nom, puis affiche ce nom dans le dossier dans lequel se trouve le compte d'utilisateur dans Active Directory.

**Nom d'ouverture de session de l'utilisateur** : Nom d'ouverture de session unique de l'utilisateur établi en fonction des conventions de dénomination. Ce paramètre est obligatoire et doit être unique dans Active Directory. (*donnez : utilisateur1, utilisateur2,...*)

**Nom d'ouverture de session de l'utilisateur (avant l'installation de Windows 2000)** : Nom d'ouverture de session unique de l'utilisateur pour ouvrir des sessions à partir de versions antérieures de Microsoft Windows. Ce paramètre est obligatoire et doit être unique dans Active Directory.

La fenêtre du mot de passe contient les champs suivants :

**Mot de passe** : Mot de passe utilisé pour authentifier l'utilisateur. Pour plus de sécurité, affectez toujours un mot de passe. Le mot de passe est invisible lorsque vous le tapez : il est représenté par une suite d'astérisques (\*).



**Confirmer le mot de passe :** Confirmez le mot de passe en le tapant une seconde fois pour vérifier qu'il a été correctement entré. Il s'agit d'une entrée obligatoire.

**L'utilisateur doit changer de mot de passe à la prochaine ouverture de session :** Activez cette case à cocher pour que l'utilisateur change de mot de passe à la prochaine ouverture de session. Cette opération garantit que l'utilisateur est seul à connaître le mot de passe.

**L'utilisateur ne peut pas changer de mot de passe :** Activez cette case à cocher si plusieurs personnes utilisent le même compte d'utilisateur de domaine (Invité, par exemple) ou pour garantir le contrôle des mots de passe des comptes d'utilisateur. En procédant ainsi, seuls les administrateurs contrôlent les mots de passe.

**Le mot de passe n'expire jamais :** Activez cette case à cocher si vous voulez que le mot de passe ne soit jamais changé (par exemple pour un compte d'utilisateur de domaine qui sera utilisé par une application ou un service de Windows 2000).

**Le compte est désactivé :** Activez cette case à cocher pour empêcher l'utilisation de ce compte d'utilisateur (par exemple, pour le compte d'un nouvel employé qui n'a pas encore commencé à travailler).

### Attention :

L'option « L'utilisateur doit changer de mot de passe à la prochaine ouverture de session » a priorité sur l'option « Le mot de passe n'expire jamais ».

**Remarque :** Pour modifier les paramètres d'un compte utilisateur de domaine, il suffit de rouvrir la console « Utilisateur et ordinateur Active Directory », ouvrir le dossier « Users » (ou celui qui contient le compte utilisateur que vous voulez modifier) puis choisissez l'utilisateur concerné et modifiez ses paramètres (options).

## **Exercice 3 :Création d'un modèle de compte d'utilisateur**

Pour créer un modèle, créez un compte d'utilisateur de domaine ou copiez en un. Affectez un nom de compte unique, et n'oubliez pas d'activer la case à cocher **Le compte est désactivé** lorsque vous définissez les options de mot de passe.

## **Exercice 4 : Définition des ordinateurs à partir desquels l'utilisateur peut ouvrir une session**

Pour indiquer les ordinateurs à partir desquels un utilisateur peut ouvrir une session, suivez la procédure ci-dessous.

1. Ouvrez la boîte de dialogue « Propriétés » du compte d'utilisateur, puis, dans l'onglet « Compte », cliquez sur « Se connecter à ».
2. Cliquez sur « Les ordinateurs suivants ». Ajoutez les ordinateurs à partir desquels cet utilisateur peut ouvrir des sessions, en tapant leurs noms dans la zone « Nom » de l'ordinateur, puis cliquez sur « Ajouter ». Lorsque vous avez fini d'ajouter des ordinateurs, cliquez sur « OK ».



Quelques mesures de sécurité à prendre pour les comptes d'utilisateurs :

- Désactiver le compte invité.
- Limité les horaires d'accès à certains utilisateurs.
- Leur limiter aussi les ordinateurs auxquels il ont le droit d'accès et d'utilisation.
- Donner des dates d'expiration pour les utilisateurs temporaires.
- .....

**Profil utilisateur :**

Les profils utilisateurs contiennent les paramètres qui définissent l'environnement réseau, comme la configuration du bureau et les options de menu.



## TP N°4

### 4. Installation et configuration d'un serveur DNS

#### 4.1. Objectifs:

- A quoi sert un DNS,
- Installer un serveur DNS,
- Les techniques à exploiter pour configurer et gérer un DNS,
- Installation et configuration d'un serveur DNS secondaire,
- ....

#### 4.2. C'est quoi et pourquoi un DNS

**NB :**

Pour plus de détails, veuillez vous référer au TP d'Administration Système sous Unix.

**En résumé :**

Le DNS (Domain Name System) est un service de résolution de noms qui transforme les noms d'ordinateurs en adresses IP (et vice versa). DNS fonctionne avec la pile de protocole TCP/IP. Si vous l'intégrez aux fonctionnalités de mise en réseau suivantes : WINS (Windows Internet Naming Service), DHCP (Dynamic Host Configuration Protocol) et le service d'annuaire Active Directory, vous l'optimisez pour les domaines W2k.

#### 4.3. Types de serveurs DNS

Quatre types de serveurs DNS sont disponibles sous Windows 2000 : serveur principal intégré à Active Directory, serveur principal standard, serveur secondaire, et serveur de transmission. Ces types de serveurs peuvent être configurés sur tout serveur W2k. Tout domaine doit avoir un serveur DNS principal qui peut soit être intégré à Active Directory ou agir en serveur principal standard. On peut aussi associer à un domaine un serveur secondaire et un serveur de transmission. Les serveurs principaux doivent comporter des zones de recherche directes et inversées. Les recherches directes servent à résoudre les noms de domaines en adresses IP. Les recherches inversées sont nécessaires à l'authentification des requêtes DNS lors de la résolution des adresses IP en hôtes ou en noms de domaine.

1. **Serveur principal intégré à Active Directory** : Ce type de serveur DNS est pleinement intégré à Active Directory. Toutes les données DNS sont directement stockées dans l'annuaire.
2. **Serveur principal** : Ce type de serveur utilise une intégration partielle à Active Directory. Il conserve une copie master des enregistrements DNS et des fichiers de configuration du domaine. Ces fichiers sont stockés avec l'extension .DNS, généralement dans %systemRoot%\System32\Dns.
3. **Serveur secondaire** : Ce type de serveur fournit des services de sauvegarde au domaine. Il conserve une copie des enregistrements DNS provenant d'un serveur



principal. Il est mis à jour par transfert de zone. Il conserve ces informations jusqu'à ce qu'elles soient réactualisées ou qu'elles expirent.

4. **Serveur de transmission** : Ce type de serveur met des informations DNS en cache et passe les requêtes aux autres serveurs. Contrairement aux serveurs secondaires, les serveurs de transmission ne demandent pas de copies complètes des fichiers de base de données d'une zone. Ce qui fait que la base de données d'un serveur de transmission, au démarrage, ne contient aucune information.

#### 4.4. Installation d'un serveur DNS

Comme nous l'avons vu au TP précédent, Active Directory et DNS sont étroitement intégrés, au point où on doit installer DNS avant de pouvoir installer Active Directory. Les domaines Active Directory utilisent DNS pour implémenter leur hiérarchie et leur structure de dénomination. D'ailleurs, lors de l'installation (par défaut) d'un contrôleur de domaine, le système vous demande d'installer et de configurer DNS. C'est pour cette raison que tous les contrôleurs de domaine sont (généralement) serveurs DNS. Vous n'avez pas alors à réinstaller DNS dans la plupart des cas.

#### Exercice N° 1 : Installer le serveur DNS

Si vous n'avez pas installé déjà DNS sur votre contrôleur de domaine ou si vous voulez l'installer sur un serveur membre, suivez les étapes suivantes :

- 1- Ouvrez « Panneau de configuration » choisir « Ajout / suppression de programmes » puis « Ajouter Supprimer des composants Windows »,
- 2- Sélectionnez « Services de mise en réseau » puis cliquez sur « Détail »,
- 3- Sélectionnez « System de nom de domaine (DNS) ». Et enfin, cliquez sur « OK » puis sur « Suivant ».

A partir de maintenant, le service DNS doit démarrer automatiquement à chaque redémarrage de la machine.

#### 4.5. Activer le service DNS sur le réseau :

Pour activer DNS sur le réseau, il faut configurer les clients et les serveurs DNS. Concernant les clients, il faut leur indiquer les adresses IP des serveurs DNS du réseau. A l'aide de ces adresses, les clients peuvent communiquer avec les serveurs DNS n'importe où sur le réseau, même si les serveurs se situent sur des sous-réseaux différents.

Si le réseau utilise DHCP, vous devriez configurer DHCP pour qu'il travaille avec DNS (rappelez-vous de ce point pour le TP suivant).



## 4.6. Configuration du serveur DNS

### Exercice N° 2 : Configurer un serveur DNS principal

Après avoir installé le service serveur DNS sur le serveur, il faut configurer ce serveur (serveur principal) en procédant comme suit :

- 1- Ouvrir la console DNS (Démarrer/programmes/Outils d'administration/DNS),
- 2- Si le serveur que vous voulez configurer n'apparaît pas dans l'arborescence, vous devez vous y connecter en cliquant avec le bouton droit sur l'entrée 'DNS' de l'arborescence, puis sélectionnez « Connecter à l'ordinateur ». Deux (2) possibilités vous ont offertes : « Cet ordinateur » pour se connecter à un DNS sur l'ordinateur sur lequel on travaille, et « L'ordinateur suivant » pour se connecter à un serveur distant. Pour ce dernier cas, vous devez soit entrer le nom ou l'adresse IP du serveur distant.

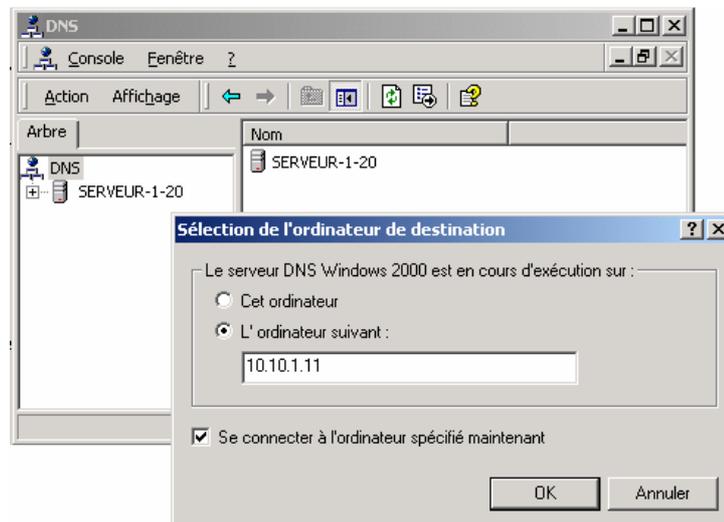


Figure 5.1 Se connecter à un serveur DNS distant

- 3- Dans la fenêtre « DNS », cliquez avec le bouton droit sur l'entrée du serveur, puis sélectionnez « Nouvelle zone » dans le menu contextuel. Ce qui fait démarrer « L'assistant Nouvelle Zone ».
- 4- A ce moment là, vous pouvez choisir le type de la zone que vous voulez créer (intégrée à Active Directory, zone principale standard ou zone secondaire standard). Pour de meilleures performances, choisissez une zone intégrée à Active Directory.
- 5- Sélectionnez « Zone de recherche directe », puis entrez le nom DNS complet de la zone (Polytech-Tours.fr ou DI.Polytech-Tours.fr ...).
- 6- Cliquez sur « Suivant » puis sur « Terminer ». La nouvelle zone est ajoutée au serveur et les enregistrements DNS de base sont automatiquement créés.
- 7- Créez des enregistrements supplémentaires pour tout ordinateur devant être accessible aux autres domaines DNS (voir point suivant).



## 4.7. Ajout et gestion des enregistrements DNS

Après avoir créé les fichiers de zones nécessaires, ajoutez des enregistrements aux zones. Les ordinateurs auxquels les domaines DNS et Active Directory doivent accéder doivent disposer d'enregistrements DNS. Parmi les types d'enregistrement DNS existants il y a :

- **A (Adresse)** : Mappe un nom de hôte en adresse IP. Si un ordinateur dispose de plusieurs cartes réseaux, il devrait avoir plusieurs enregistrements d'adresses.
- **CNAME (Canonic NAME)** : définit un alias pour un nom de hôte.
- **MX (Serveur de messagerie)** : indique le serveur de messagerie du domaine pour livrer correctement le courrier électronique.
- **NS (serveur de noms)** : indique le serveur de noms du domaine. Chaque serveur de noms (principal ou secondaire) doit être déclaré par cet enregistrement.
- **PTR (pointeur)** : crée un pointeur qui mappe une adresse IP en nom de hôte pour les recherches inversées.
- **SOA (autorité principale)** : Cet enregistrement est créé automatiquement lorsque vous ajoutez une zone. Il déclare l'hôte disposant de la plus grande autorité dans la zone. Il est donc la meilleure source d'information DNS de la zone. Chaque fichier de zone doit avoir un enregistrement SOA.

### Exercice N° 3 : Ajouter des enregistrements d'adresses et de pointeurs

Vous pouvez créer des enregistrements d'adresses et des enregistrements de pointeurs au même temps ou séparément. En cas de recherche inversée l'enregistrement 'A' mappe un nom de hôte en adresse IP et l'enregistrement 'PTR' crée un pointeur pour l'hôte.

Pour créer une nouvelle entrée d'hôte avec des enregistrements A et PTR (au même temps), procédez comme suit :

- Développez, dans la console DNS, le dossier « Zone de recherche directe » du serveur avec lequel vous voulez travailler,
- Cliquez avec le bouton droit sur le domaine à mettre à jour, puis choisissez « Nouvel hôte » dans le menu contextuel,
- Dans la fenêtre « Nouvel hôte » qui apparaît, entrez le nom et l'adresse IP de l'ordinateur qu'on veut ajouter (*voir figure 5.2 ci-dessous*).
- N'oubliez pas de cocher la case « Créer un pointeur d'enregistrement PTR » pour qu'il crée au même temps l'enregistrement PTR. Puis cliquez sur « OK ».

**Remarque :** De la même manière, vous pouvez créer seulement des enregistrements A, des enregistrements PTR, des alias CNAME, des serveurs de messagerie ou des serveurs de noms.

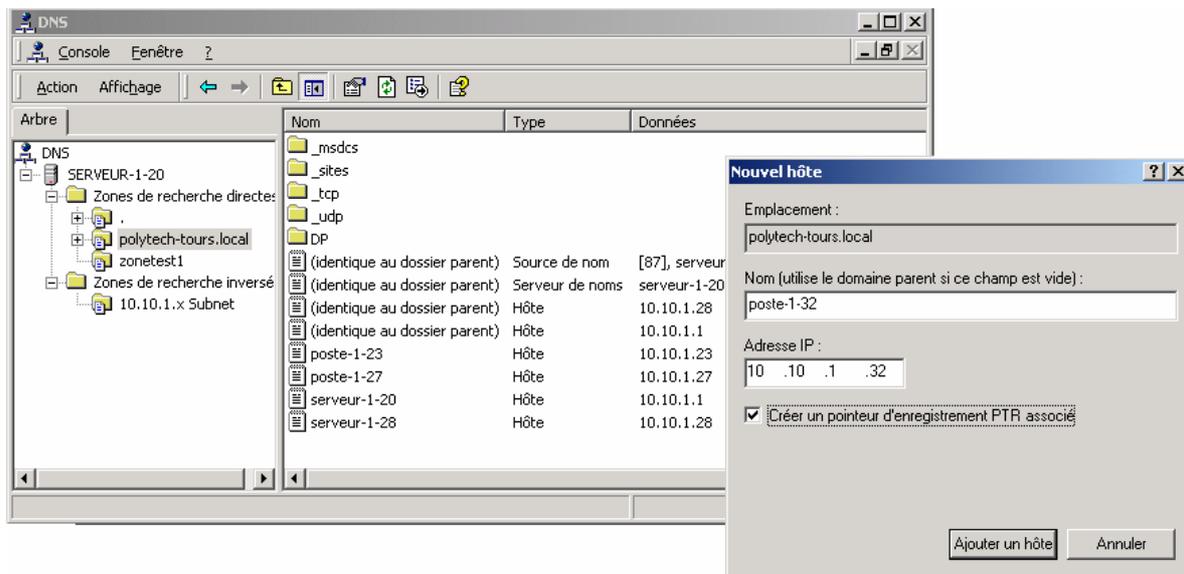


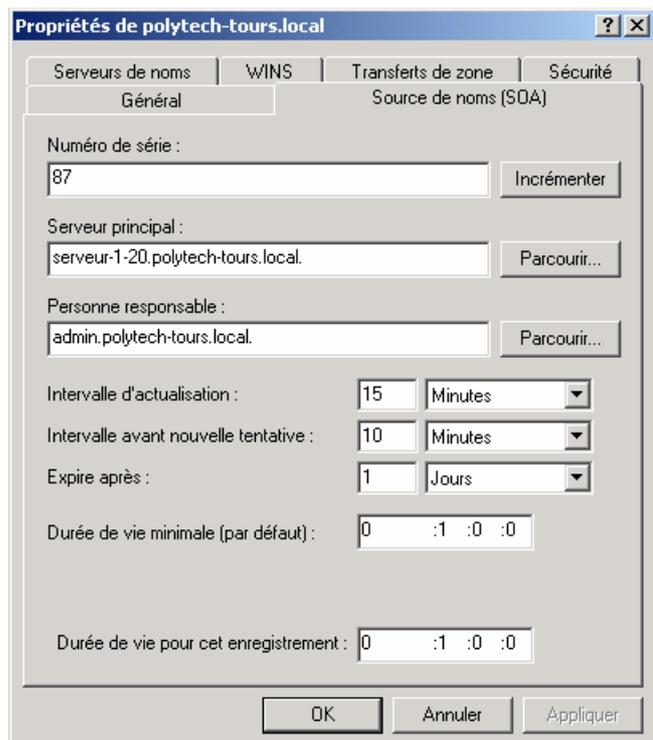
Figure 5.2 : Créer des enregistrement A et PTR simultanément avec l'option nouvel hôte

#### 4.8. Mise à jour des propriétés d'une zone

Pour configurer les propriétés d'une zone, procédez comme suit :

- Dans la console « DNS », cliquez avec le bouton droit sur la zone à mettre à jour, puis sélectionnez « Propriétés »,
- Modifiez les paramètres à changer puis cliquez sur « OK ».

Vous pouvez alors changer le nom du serveur principal de l'enregistrement SOA, l'adresse mail de la personne responsable à contacter, les intervalles de validité et d'expiration, les autorisations de transfert de zones, les autorisations de mises à jour dynamiques, les paramètres de sécurité...



**Remarques :**

- Chaque zone possède des propriétés distinctes.
- Le nom du serveur principal est suivi d'un point à la fin. Ce point sert à garantir que les informations du domaine ne sont pas ajoutées à l'entrée.
- Si vous changez l'adresse de la personne responsable du domaine remplacez l'arobase (@) par un point et terminez cette adresse par un point (ex. si l'adresse du responsable est Admin@Polytech-Tours.fr , mettez alors Admin.Polytech-Tours.fr.).
- Pour rendre dynamique la MAJ d'un serveur DNS, il faut mettre, dans l'onglet « général », le champ « autoriser les mise à jour dynamiques » à « OUI ».

**Autres remarques :**

- La commande « hostname.exe » permet de connaître le nom de hôte d'une machine.

```
F:\>hostname.exe
serveur-1-20
```

- Avec le système de serveur DNS, le fichier hosts (%systemRoot%\system32\drivers\etc\hosts) devient presque inutile. Lorsqu'un utilisateur cherche un nom d'hôte, W2k cherche d'abord dans le fichier 'hosts' de la machine. S'il n'y trouve pas de correspondance, il envoie une requête au serveur DNS. Si le serveur ne répond pas, 4 autres tentatives seront faites. S'il n'y aura aucune réponse, l'utilisateur reçoit un message d'erreur.
- L'utilitaire « nslookup.exe » permet de diagnostiquer le bon fonctionnement d'un serveur DNS.

```
F:\>nslookup
Serveur par défaut : localhost
Adresse : 127.0.0.1
>poste-1-23
Serveur: localhost
Address: 127.0.0.1
Nom:     poste-1-23.Polytech-Tours.local
Address: 10.10.1.23
```



# TP N° 5

## 5. Installation et configuration d'un serveur DHCP

### 5.1. Objectifs du TP :

- Comprendre le fonctionnement du service DHCP,
- Installer un serveur DHCP,
- Configurer un serveur et un client DHCP,
- Réserver des adresses et éviter des conflits d'adressage

### 5.2. Pourquoi un serveur DHCP

Quand le réseau est petit (une ou deux dizaines de machines) sa gestion est facile. Mais elle commence de plus en plus à se compliquer quand il y a de plus en plus de machines. Quand le nombre de machines de réseau devient très important ou quand les machines qui se connectent au réseau changent (portables), la gestion de ce réseau devient difficile. On pourra alors affecter à une machine, durant sa configuration, de fausses adresses de passerelles ou de serveur DNS. Il est même possible d'affecter de fausses adresses IP et de créer ainsi des conflits d'adresses (deux ou plusieurs machines qui ont la même adresse IP). Dans ce cas-là, une gestion automatique des machines s'avère plus efficace. C'est le rôle d'un serveur DHCP.

### 5.3. Présentation et fonctionnement d'un serveur

Un serveur DHCP (Dynamic Host Configuration Protocol) permet d'attribuer, à des postes clients, une adresse IP de manière dynamique (ou automatique). En plus d'une adresse IP, DHCP permet de donner à une machine cliente qui se connecte au réseau géré par un serveur DHCP, son masque de sous-réseau, l'adresse de la passerelle, la durée du bail (voir plus loin), un nom DNS...

Le DHCP utilise le modèle Client/Serveur dans lequel le serveur DHCP assure une gestion centralisée des adresses IP utilisées sur le réseau. Le client demande son adresse IP (ainsi que l'adresse de la passerelle...) au moment de son démarrage (à l'aide d'un message de broadcast). Les serveurs qui reçoivent cette demande choisissent leurs données dans leur pool d'adresses IP. Ils les proposent au client. Ce dernier doit renvoyer une requête DHCP au premier serveur qui lui répond où il lui dit qu'il accepte ces adresses et qu'il veut les garder. Le serveur lui renvoie alors un paquet de confirmation avec toutes les autres informations (adresse de la passerelle, celle du serveur DNS ...). Le client configurera alors ses paramètres réseaux avec ces informations qu'il vient de recevoir du serveur.

Parmi les paquets échangés entre le serveur et le client pour configurer ce dernier. Le paquet **DHCPDISCOVER** est le premier paquet émis par le client. Le serveur (ou les serveurs) répond (ent) alors par le paquet **DHCPOFFER**. Ce paquet contient des paramètres pour soumettre une adresse IP au client. Le client envoie le paquet **DHCPREQUEST** pour valider son adresse IP. Le serveur répond par un paquet **DHCPACK** avec l'adresse IP pour



confirmer au client l'attribution de cette adresse. Le serveur peut répondre aussi par un paquet **DHCPNAK** pour signaler au client que son bail (voir ci-dessous) est échu ou que la configuration réseau du client n'est pas bonne.

D'autres paquets peuvent être échangés entre le client et le serveur :

- **DHCPCLINE** : pour annoncer au serveur que l'adresse IP est déjà utilisée.
- **DHCPRELEASE** : pour libérer l'adresse IP du client.
- **DHCPINFORM** : le client demande, via ce paquet, au serveur des paramètres locaux (à ce moment le client a déjà son adresse IP).
- **DHCPACK** : quand le serveur reçoit le message d'acceptation du bail par le client, le serveur lui répond en lui précisant la durée

Les informations que reçoit le client du serveur (son adresse IP, adresse de la passerelle, adresse du serveur DNS...) ne sont valables que pour une certaine durée, appelée « **bail** ». Quand le bail d'un client arrive à son terme, ce client peut demander au serveur une prolongation du bail par un **DHCPREQUEST** (voir le paragraphe ci-dessous). Le serveur aussi peut demander au client s'il veut prolonger son bail (avec le paquet **DHCPNAK**). Si le serveur ne reçoit pas de réponse valide, annule l'attribution de l'adresse IP en question et rend cette dernière disponible.

Sur un réseau où des ordinateurs se branchent et se débranchent le plus souvent, il est intéressant d'utiliser des baux de courte durée. Par contre, si le réseau est constitué de machines fixes et très peu reboutées, il est plus intéressant d'utiliser des baux de longue durée et peut être de réserver aussi des adresses IP à chacune de ces machines.

#### NOTES :

1. Quand une machine cliente demande une adresse IP en envoyant le paquet **DHCPDISCOVER**, elle n'a pas encore d'adresse IP. Pour qu'elle puisse communiquer sur le réseau, elle met dans le paquet **DHCPDISCOVER** comme adresse source son adresse MAC et l'adresse IP 0.0.0.0. Elle envoie ce paquet vers toutes les machines (adresse MAC = FF FF FF FF FF FF, et adresse IP = 255.255.255.255 ).
2. Les serveurs répondent au paquet **DHCPDISCOVER** avec le paquet **DHCPOFFER** qui contient l'adresse MAC du client et l'adresse IP à attribuer au client.
3. Plusieurs serveurs répondent à la demande du client (paquet **DHCPDISCOVER**) mais le client ne prend qu'à une seule proposition, ça sera celle du serveur le plus rapide.
4. Les baux de courtes durée génèrent trop de trafic alors que les baux trop longs occupent des IP (les rends indisponibles). Ce dernier cas peut créer une pénurie d'IP quand les machines changent souvent alors que l'étendue (plage d'adresses IP à louer) n'est pas très grande.

## 5.4. Installation et configuration d'un serveur et d'un client DHCP

### Exercice N° 1 : Installation d'un serveur DHCP

L'installation d'un serveur DHCP est très simple. Pour cela, il faut ouvrir la fenêtre « Ajout-Suppression de programmes », choisir « Ajouter/Supprimer des composants Windows », puis choisir « Services de mise en réseau ». Cliquez sur « Détails » et cochez « Protocole DHCP », puis sur « OK ». A partir de maintenant, le service DHCP doit démarrer automatiquement à chaque réinitialisation du serveur.



## Exercice N° 2 : Configuration d'un serveur DHCP

Lorsque vous installez un nouveau serveur DHCP, les options de configuration sont automatiquement optimisées pour l'environnement réseau. Il faut tout d'abord s'assurer que l'adresse de votre machine est fixe car, un serveur DHCP doit avoir une **adresse IP fixe**.

Pour configurer un serveur DHCP, il faut commencer à l'autoriser sur le réseau existant afin d'éviter qu'un serveur non autorisé sur le réseau (serveur mal configuré ou un serveur bien configuré mais qui n'est pas sur le bon réseau) donne de mauvaises adresses IP. Pour **autoriser un serveur**, ouvrir la fenêtre DHCP (Outils d'administration / DHCP). Dans le menu « Action » choisir « Gérer les serveurs autorisés » puis cliquez sur « Autoriser ». Dans la fenêtre qui apparaît, entrez soit l'adresse IP soit le nom du serveur que vous voulez autoriser, puis cliquez sur « OK ».

Après l'autorisation, il faut créer une étendue. Une « **étendue** » est un pool (ou une plage) d'adresses IP qu'un serveur DHCP peut distribuer aux clients. Lors de la création d'une étendue, veuillez prendre en considération ce qui suit :

- Si vous avez plusieurs serveur DHCP, faites de telle sorte à ce qu'il n'y est pas une intersection entre leurs plages d'adresses. Puisque les serveurs DHCP ne s'échangent pas entre eux ce genre d'informations. Le fait d'avoir une intersection entre leurs étendues peut créer des conflits d'adresses.
- Pour chaque étendue, vous devez spécifier une adresse de début et une adresse de fin.
- Il devrait y avoir au moins une étendue par serveur, mais il est possible d'en créer plusieurs.
- N'oubliez pas d'exclure de votre étendue les adresses IP statiques de votre réseau, telles que celles des imprimantes ou des machines auxquelles vous avez donné des adresses IP fixes tels que les serveurs secondaires.

Pour créer une nouvelle étendue, dans la fenêtre « DHCP » (que vous avez ouvert tout à l'heure), dans le menu « Action », choisissez « nouvelle étendue ». Donnez un nom ainsi qu'une description à cette étendue. Puis, dans la nouvelle fenêtre qui s'ouvre, donnez l'adresse IP de début et l'adresse IP de la fin (vos machines peuvent donc prendre toutes les adresses IP qui se situe dans cet intervalle) ainsi que le masque de votre sous-réseau (vous pouvez aussi spécifier ce masque sous forme de longueur).

Assistant Nouvelle étendue

**Plage d'adresses IP**  
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Entrez la plage d'adresses que l'étendue peut distribuer :

Adresse IP de début : 10 . 10 . 1 . 12

Adresse IP de fin : 10 . 10 . 3 . 200

Un masque de sous-réseau définit le nombre de bits d'une adresse IP à utiliser pour les ID de réseau/sous-réseau, ainsi que le nombre de bits à utiliser pour l'ID d'hôte. Vous pouvez spécifier le masque de sous-réseau en terme de longueur ou comme une adresse IP.

Longueur : 24

Masque de sous-réseau : 255 . 255 . 0 . 0

< Précédent   Suivant >   Annuler



Après ça vous devez **exclure les adresses IP des machines qui ont des adresses statiques** (imprimantes, serveurs...). Pour exclure toute une plage d'adresse (sous-plage) au sein de la plage que vous avez spécifié, entrez l'adresse IP de début et l'adresse IP de la fin puis cliquez sur «Ajouter». Si vous voulez exclure une adresse unique faites rentrer seulement l'adresse de début.

Après avoir créé une étendue, il faut définir ses options. Les **options d'une étendue** permettent de préciser le fonctionnement des clients et de définir les paramètres TCP/IP par défaut. Ces options peuvent être l'adresse de la passerelle (ou routeur), l'adresse IP du serveur DNS que les clients doivent utiliser... Pour spécifier ces options, dans la console «DHCP» développez l'étendue concernée. Cliquez avec le bouton droit sur «Option de l'étendue» puis choisissez «Configurer les options». Dans la fenêtre qui s'ouvre, choisissez les options DHCP que vous voulez configurer. Si on utilise un serveur de domaine (c'est votre cas), il est conseillé d'utiliser ces 4 options : 003 pour l'accès à un routeur, 005 et 006 pour le serveur DNS et 015 pour le contrôleur de domaine qu'utiliseront les clients concernés par cette étendue. A chaque fois que vous sélectionnez une option, remplissez les champs nécessaires qui s'affichent en bas de la fenêtre.

Après avoir créé une étendue et défini ses options, vous devez finalement l'**activer** pour finir la configuration de votre serveur DHCP. Pour ce faire, cliquez avec le bouton droit sur l'étendue et choisissez «Activer» dans le menu contextuel. Vous avez remarqué peut être que la flèche rouge orientée vers le bas qui s'affichait devant votre étendue est remplacée par une flèche verte vers le haut. Cela signifie que votre étendue est activée et que votre serveur DHCP est prêt à distribuer des adresses IP aux clients.

### Exercice N° 3 : Configuration d'un client DHCP

La configuration d'un client DHCP est simple. Vous devez ouvrir la fenêtre «Propriétés du protocole Internet (TCP/IP)» et choisir, dans l'onglet «Général», les boutons radio «Obtenir des adresses IP automatiquement» et «Obtenir les adresses des serveurs DNS automatiquement».

Pour s'assurer que le service DHCP est activé, cliquez sur «Avancé». On peut aussi utiliser la commande «`ipconfig /all`» pour voir si le service DHCP est active.

#### Remarque :

A chaque démarrage, le client sollicite le serveur (ou les serveurs) DHCP du réseau pour qu'il lui affecte une adresse IP. Cette adresse IP lui sera affectée pour une durée déterminée appelée «bail». Si le client, au moment de sa réinitialisation, ne reçoit de réponse d'aucun serveur DHCP (même après 3 répétitions), il s'autoconfigure en s'affectant une adresse IP du type 169.254.xxx.xxx (ce type d'adresse s'appelle adresse APIPA (Automatic Private IP Addressing)). Ensuite il refait une tentative toutes les 5 minutes.

## 5.5. Autoriser un serveur DHCP dans Active Directory

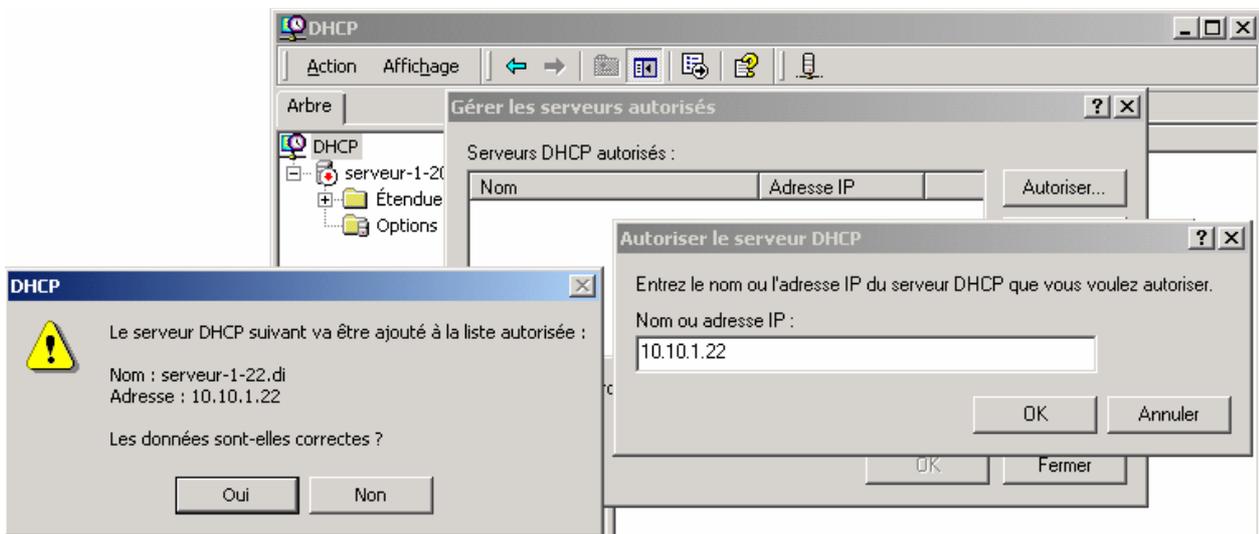
Pour pouvoir utiliser un serveur DHCP dans le domaine, vous devez d'abord l'autoriser dans le service d'annuaire Active Directory. Cela veut dire que à partir de ce moment vous autorisez à exécuter l'adressage IP dynamique dans le domaine.

Pour autoriser un serveur DHCP, dans l'arborescence de la console «DHCP», cliquez avec le bouton droit sur l'entrée concernant le serveur puis sélectionnez «Autoriser».



Pour supprimer l'autorisation, cliquez avec le bouton droit sur le serveur, puis sélectionnez « Interdire ».

Si vous utilisez la fenêtre « Gestion de l'ordinateur », cliquez avec le bouton droit sur « DHCP », puis sélectionnez « Autoriser » pour autoriser le serveur ou sur « Interdire » pour supprimer cette autorisation.



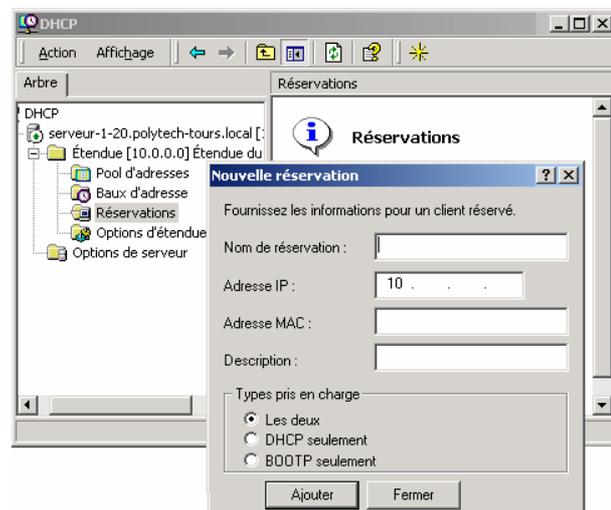
## 5.6. Réserveation d'adresses

On peut assigner une adresse permanente à un client bien déterminé. DHCP fournit plusieurs moyens pour ça. Parmi ces moyens, la réserveation d'adresses DHCP par client. Avec cette réserveation, le serveur DHCP fournit toujours la même adresse IP à ce client. Pour réserver une adresse DHCP à un client, procédez comme suit :

- Dans la console « DHCP », développez l'étendue avec laquelle vous travaillez, puis cliquez avec le bouton droit sur le dossier « Réserveation ». Choisissez « Nouvelle réserveation » dans le menu contextuel.
- Dans la fenêtre « Nouvelle réserveation » qui apparaît, donnez un nom à cette réserveation (un nom descriptif), l'adresse IP à réserver au client (cette adresse doit faire partie de la plage d'adresses valide de l'étendue sélectionnée) et l'adresse MAC de la carte réseau de l'ordinateur client (vous pouvez l'obtenir, à partir du client, à l'aide de la commande 'ipconfig /all').

### Remarque :

On peut supprimer une étendue globale et ajouter ou supprimer des étendues à cette étendue globale.





### 5.6.1. Libération des adresses des clients

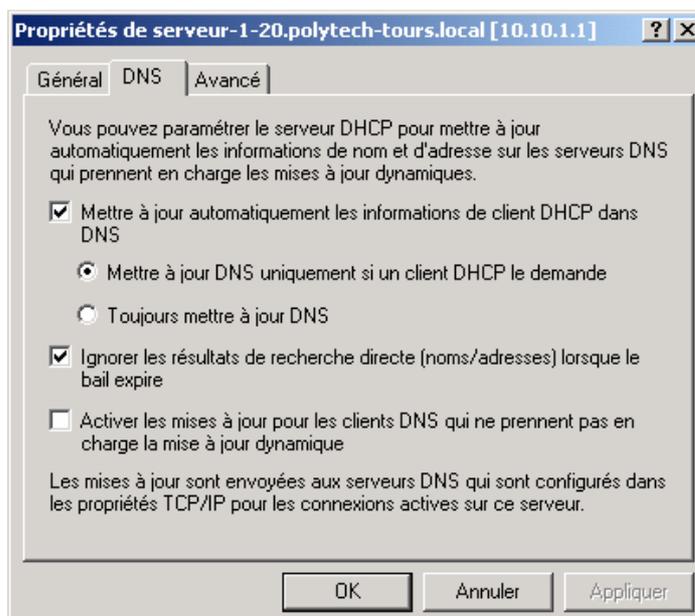
Quand on réserve des adresses à des clients, ces adresses ne sont pas automatiquement réassignées. Si l'adresse est déjà utilisée, vous devrez la libérer pour que le client approprié puisse l'obtenir. Pour forcer un client à libérer une adresse, on mettra fin à son bail ou on ouvre une session sur le client puis on tape la commande 'ipconfig /release'. Les clients ne basculent pas automatiquement sur l'adresse réservée. Si un client utilise une adresse IP différente, pour le forcer à libérer le bail en cours et à demander un nouveau, tapez la commande 'ipconfig /renew'.

### 5.6.2. Active Directory et DNS :

Avec Active Directory, tout contrôleur de domaine exécutant le service « Serveur DNS » peut gérer les mises à jour dynamiques. Grâce au protocole de mise à jour DNS, vous n'avez pas à enregistrer manuellement les clients DHCP dans le système DNS. Avec l'installation par défaut de DHCP, les clients DHCP Windows 2000 mettent automatiquement à jour leurs propres enregistrements DNS après réception d'un bail d'adresse IP.

Pour modifier et activer les paramètres de l'intégration DNS, dans la console « DHCP », cliquez avec le bouton droit sur le serveur avec lequel travailler, puis sélectionnez « Propriétés ». Dans l'onglet « DNS » de la fenêtre qui apparaît, modifiez ou activez les paramètres que vous voulez changer (propriétés de mise à jour du DNS : 'Toujours mettre à jour DNS', 'Mettre à jour DNS uniquement si un client DHCP le demande'...).

Quand le serveur DHCP alloue une adresse IP à une machine, il informe le DNS de la relation adresse IP ↔ Nom. Quand le bail expire, le serveur DHCP supprime cette relation.





## 5.7. Eviter les conflits d'adresses IP

Même quand vous faites des réservations d'adresses, des conflits d'adresses IP peuvent se produire. Si un conflit se produit entre deux ou plusieurs ordinateurs clients, un parmi les deux (ou tous les deux) peut être déconnecté du réseau. Pour détecter et éviter les conflits d'adresses IP :

- Dans la console « DHCP », cliquez avec le bouton droit sur le serveur avec lequel vous travaillez, puis sélectionnez « Propriétés ».
- Dans l'onglet « Avancé » de la fenêtre qui apparaît, donnez une valeur différente de zéro à « tentative de conflit ». Cette valeur représente le nombre de fois que le serveur vérifie qu'il n'y a pas de conflit pour l'adresse IP qu'il affectera au client. Cette vérification se fait en envoyant des pings (par le serveur) sur tout le réseau.



\*\*\*\*\*\_\*\*\*\*\*  
\*\*\*\*\* Fin du TP N° 3 \*\*\*\*\*  
\*\*\*\*\*\_\*\*\*\*\*



\*\*\*\*\*\_\*\*\*\*\*  
\*\*\*\*\* Début du TP N° 3 \*\*\*\*\*  
\*\*\*\*\*\_\*\*\*\*\*

## TP N° 3

### Installation d'un serveur d'impression

#### 1. Installation d'un serveur d'impression

Publier l'imprimante sur le serveur Polytech-tours.fr et non pas sur celui de Dep-Informatique.Polytech-tours.fr

Hklm .....



\*\*\*\*\*\_\*\*\*\*\*  
\*\*\*\*\* Fin du TP N° 3 \*\*\*\*\*  
\*\*\*\*\*\_\*\*\*\*\*



```
*****_*****  
***** Début du TP N° 4 *****  
*****_*****
```

## 2. Installation d'un serveur TSE

TSE (Terminal Server Edition) ⇒ l'installer pour les postes qui ont de petites configurations pour qu'ils puissent exécuter les application lourdes (telle l'exécution de Microsoft Office 2000 sur des machine qui ont de petites mémoires (quelques Mo de RAM) et des processeurs lent (60 MHz). L'exécution de l'application se fera sur le serveur TSE, on n'aura que le résultat sur l'écran du client. (voir petit polycopie Win2000 p15).

```
*****_*****  
***** Fin du TP N° 4 *****  
*****_*****
```



\*\*\*\*\*\_\*\*\*\*\*  
\*\*\*\*\* Début du TP N° 5 \*\*\*\*\*  
\*\*\*\*\*\_\*\*\*\*\*

## TP N° 5

### Le profit errant ....

#### 1. Le profit errant

Pour qu'un utilisateur ait un environnement identique sur n'importe quelle machine. Voir p23/25 du petit poly)

#### 2. Utiliser les utilitaires de ligne de commande

*Livre vert P 15*

\*\*\*\*\*\_\*\*\*\*\*  
\*\*\*\*\* Fin du TP N° 5 \*\*\*\*\*  
\*\*\*\*\*\_\*\*\*\*\*



**Les comptes que j'ai ajouté sur le serveur :**

Login : utilisateur-poste-19,  
pass : toto-poste-19

login : ali  
passe : toto-serv-19

**compte client sur le poste 19 (compte local seulement) :**

login : ali-poste-19 (le remplacer par user-poste-19)  
passe : toto-client-19

**poste 23 ( installation du client)**

nom : ali  
société : EPU-DI



- **Notes :**

-----\*

-

.....

