Client sur un domaine

stage personnes ressources réseau en établissement
janvier 2004

Formateurs : **Jackie DAÖN**
Franck DUBOIS

Médiapôle de Guyancourt Lycée de Villaroy – 2 rue Eugène Viollet Le Duc – BP31 – 78041 GUYANCOURT Cedex
Tel : 01 30 48 91 88 / Fax : 01 30 57 49 70 – www.mp-guyancourt.ac-versailles.fr
Franck.Dubois@ crdp.ac-versailles.fr Jackie.Daon@crdp.ac-versailles.fr

Sommaire

Préliminaires

A l'origine, les réseaux ont été conçus pour échanger rapidement, en quantité et à coût réduit, des données entre deux ou plusieurs stations de travail. Pour fonctionner en réseau, tout PC connecté intègre une carte adaptateur (ou carte réseau) sur laquelle vient se brancher un câble. Un logiciel spécifique, le gestionnaire de réseau, assure les fonctions de communication.

Du point de vue théorique, il existe deux grandes catégories de réseaux : le poste à poste et le traditionnel. La différence entre les deux réside dans la structure mise en œuvre pour faire communiquer les machines entre elles. Dans le réseau de type traditionnel, il existe une ou plusieurs stations dédiées, appelées serveurs (leur nombre varie selon la taille du réseau), dotées de bonnes performances, qui centralisent toutes les ressources partagées (données, imprimantes, sauvegarde, etc...). Autour de ces serveurs sont connectées des machines dites clientes : elles accèdent aux ressources du serveur mais, en aucun cas, ne mettent en commun leurs ressources. Les machines clientes peuvent ainsi utiliser l'ensemble des ressources que les serveurs mettent à disposition. Il existe donc une hiérarchie dite client/serveur où les machines clientes sont uniquement clientes et les machines serveurs exclusivement serveurs.

Nous nous proposons de décrire les différentes étapes de la configuration d'un poste client sur un réseau, constitué d'un domaine nommé Bourgogne.local, lequel possède au minimum un contrôleur de domaine nommé GEVREY tournant sous Microsoft Windows 2000 server.

Client sous Windows 9x

Configurations

Nous supposons que le poste client est sous Windows 98, que la carte réseau (de type Plug & Play) est déjà physiquement installée dans la machine et qu'elle a été correctement détectée par le système.

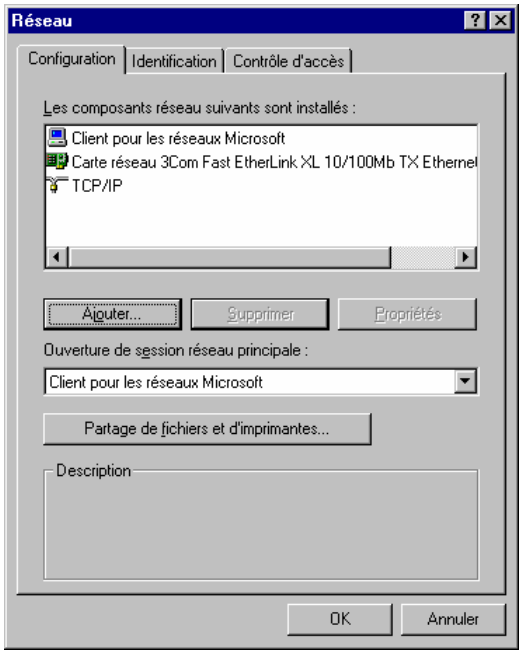
Accès à la configuration réseau

Une fois la partie matérielle du réseau installée (concentrateur, câbles de liaison, adaptateurs), il reste à mettre en place le logiciel de gestion du réseau et à définir sa configuration.

Un clic-droit sur l'icône du Voisinage réseau et le choix de la commande contextuelle Propriétés permet d'accéder aux éléments de la configuration réseau.
On obtient le même résultat en ouvrant l'icône Réseau du Panneau de configuration.

Il est nécessaire de :

- choisir un client réseau et un protocole,
- d'y lier un adaptateur,
- de définir un nom unique pour la station, et un type de contrôle d'accès aux ressources.

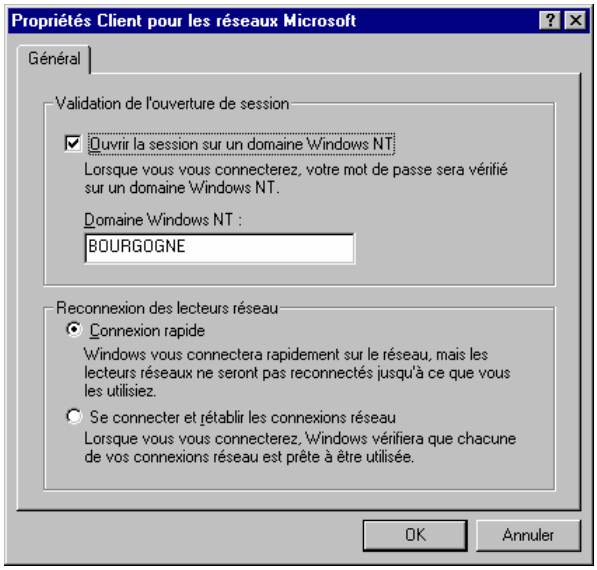


Propriétés du client réseau

On ouvre une session sur un domaine et non pas sur un serveur.

Le Client pour les réseaux Microsoft permet de se connecter à un domaine Windows NT.

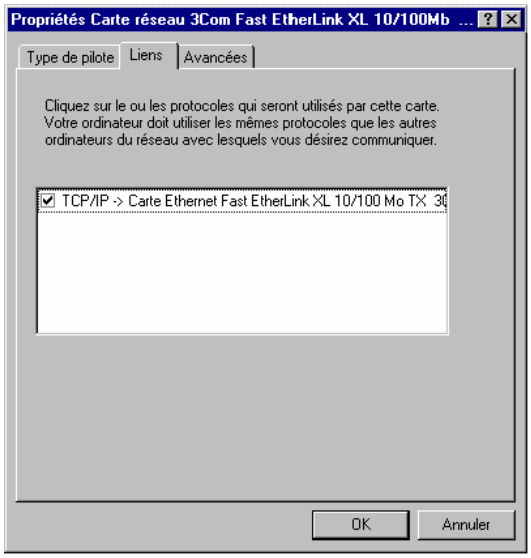
Lors de l'ouverture de session, c'est l'un des contrôleurs actifs du domaine qui validera l'accès de l'utilisateur au réseau par une vérification du nom et du mot de passe.

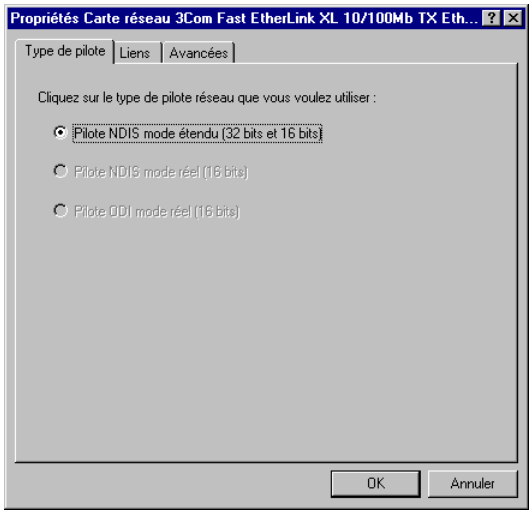


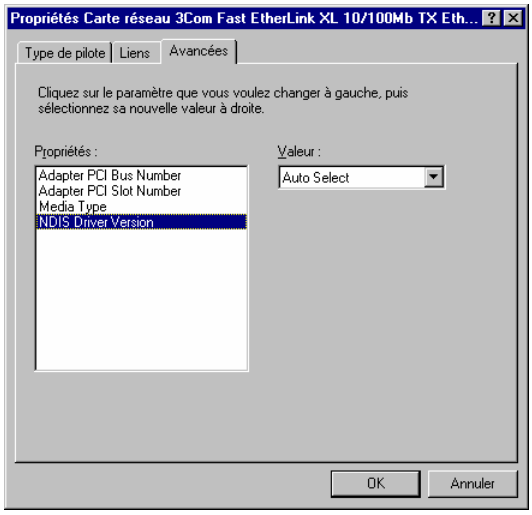
Propriétés de l'adaptateur réseau

Au moins un protocole doit être lié à l'adaptateur réseau.

Une carte réseau peut être liée à plusieurs protocoles réseau.







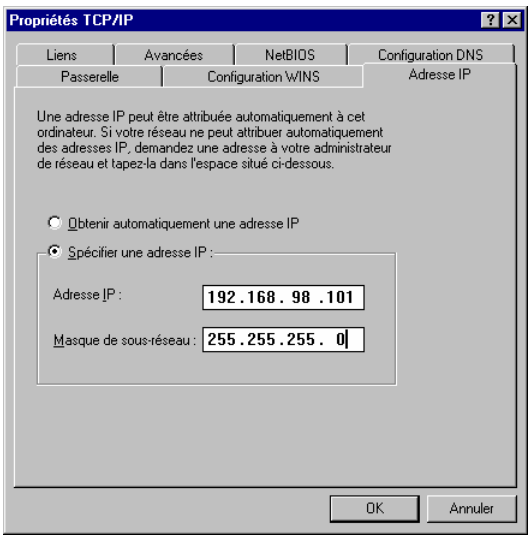
Propriétés du protocole réseau

Le choix s'est porté ici sur le protocole TCP/IP qui est maintenant le plus utilisé bien que n'étant pas très simple à configurer, mais ayant la grande qualité d'être un "langage universel" de communication informatique à travers le monde.

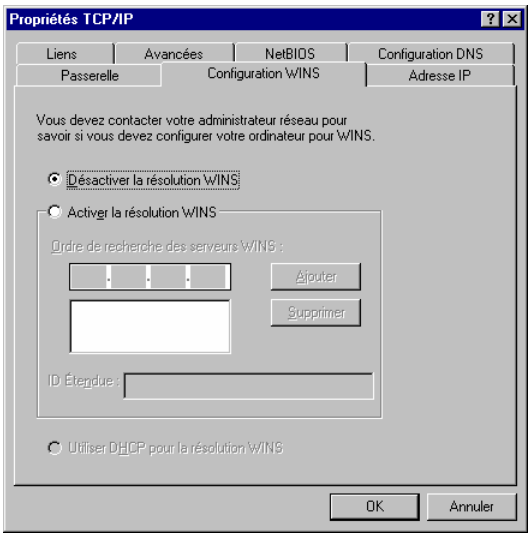
Le protocole TCP/IP attribue un numéro fixe à chaque ordinateur connecté. Ce numéro est appelé l'adresse IP. Dans le cadre du standard actuel (IPv4), les adresses sont codées sur 4 octets soit 32 bits.

Ainsi tout ordinateur utilisant TCP/IP se voit doté d'une adresse de type a.b.c.d , où a, b, c et d sont des nombres compris entre 0 et 255 (2^8 valeurs possibles).

Le masque de sous-réseau permet de savoir si deux machines sous TCP/IP sont ou non dans le même réseau IP.

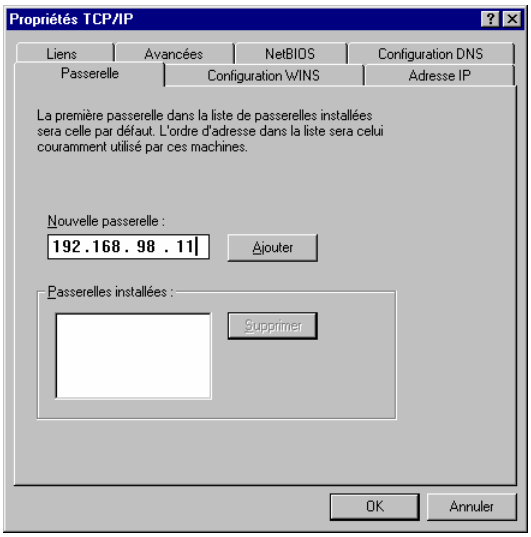


Si un serveur WINS (*Windows Internet Naming Service*) est présent sur le réseau, il faut le renseigner ici en spécifiant son adresse IP.



La passerelle est la "porte de sortie" du réseau IP. Typiquement un routeur.
Il est aussi caractérisé par une adresse IP qui lui est propre.

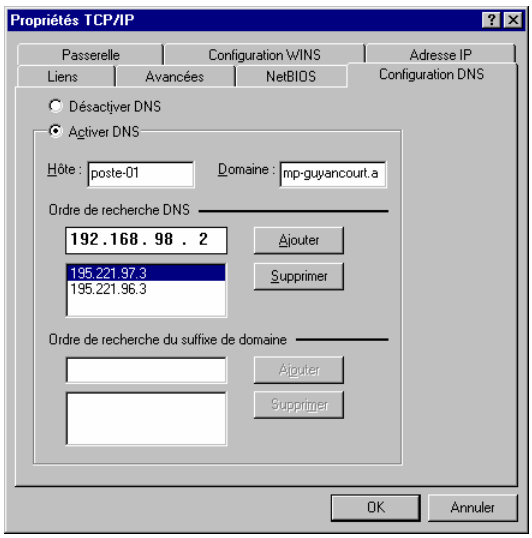
Attention :
Si l'on donne ici une liste de passerelles possibles, c'est toujours la première active dans la liste qui sera utilisée.



Si l'on veut utiliser Internet, il faut pouvoir résoudre les noms de domaine Internet en adresses IP.

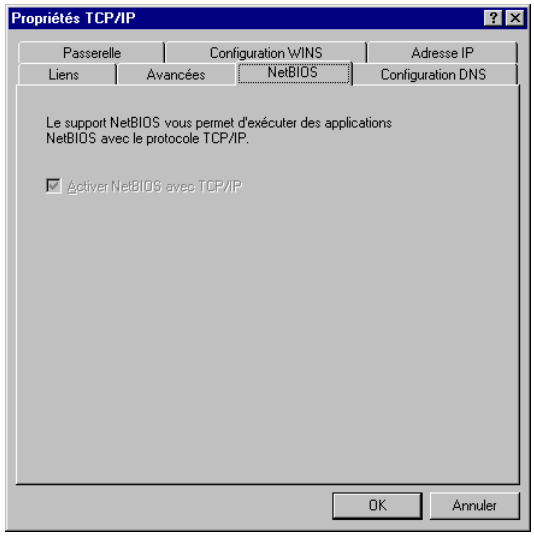
C'est le rôle des serveurs DNS (*Domain Name Service*).

Il faut donc indiquer ici l'adresse IP du serveur DNS d'Active Directory.



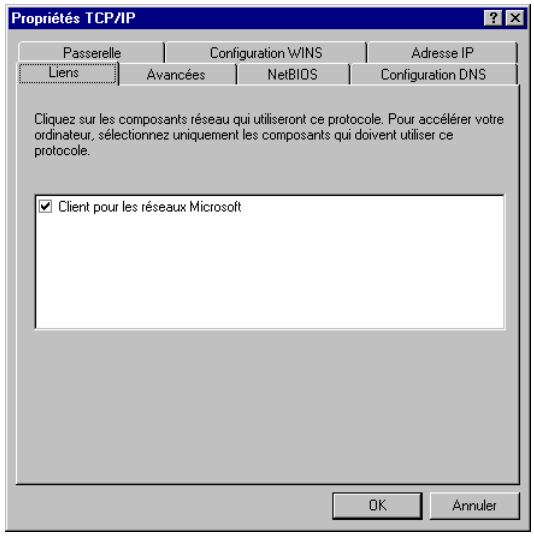
Les noms NetBIOS, qui sont les noms natifs utilisés dans un environnement de réseau Windows, sont utilisés lorsque les clients réseau Microsoft passent en revue le réseau.

Microsoft a rendu NetBIOS inséparable de TCP/IP dans Windows 9x.



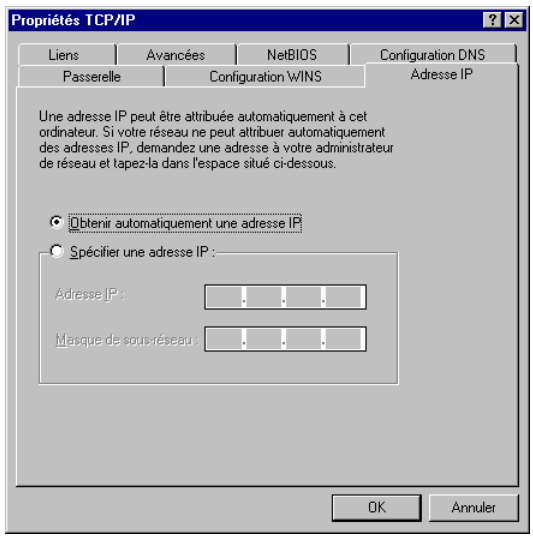
Nous avons vu que l'adaptateur réseau est lié au protocole, et nous constatons ici, que ce dernier est lui-même lié au Client réseau.

Ces trois éléments sont bien interdépendants.



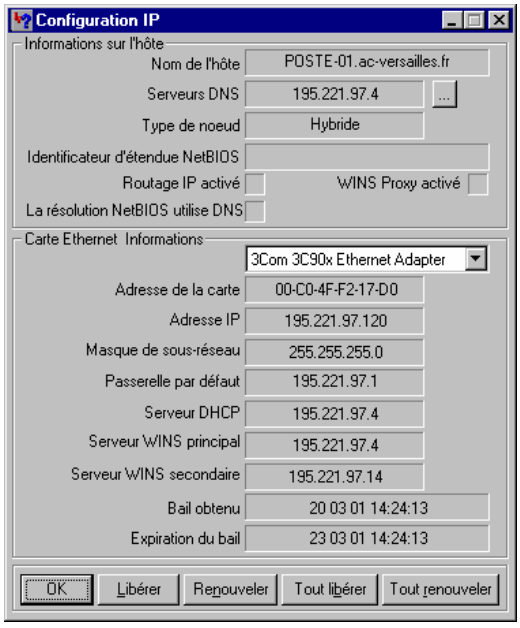
Il est possible que les différentes machines clientes du réseau reçoivent automatiquement leur configuration TCP/IP. Cela nécessite sur le réseau la présence d'un serveur DHCP (Dynamic Host Configuration Protocol).

Dans ce cas, il suffit de sélectionner le bouton permettant d'obtenir automatiquement une adresse IP.



Il est bon alors de vérifier dans les autres onglets qu'il ne reste pas de trace d'une ancienne configuration manuelle.

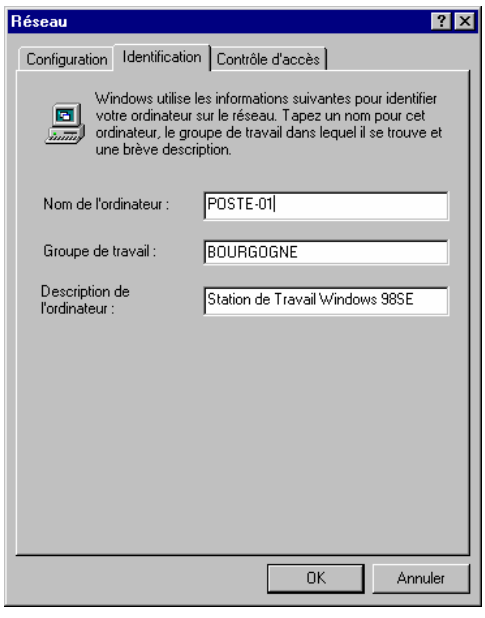
L'utilitaire **winipcfg.exe**, sous Windows 9x, permet de vérifier la configuration IP de la machine.



Identification de la machine sur le réseau

Il s'agit du nom NetBIOS.

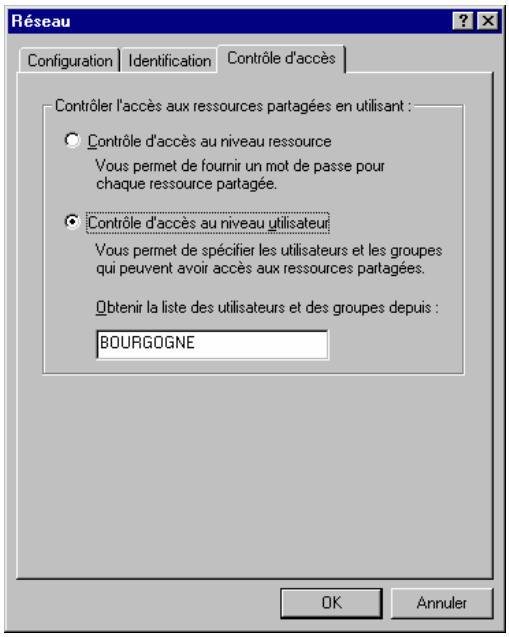
Le nom du groupe de travail est souvent identique à celui du domaine. Mais ce n'est pas une obligation.



Mode de contrôle d'accès aux ressources

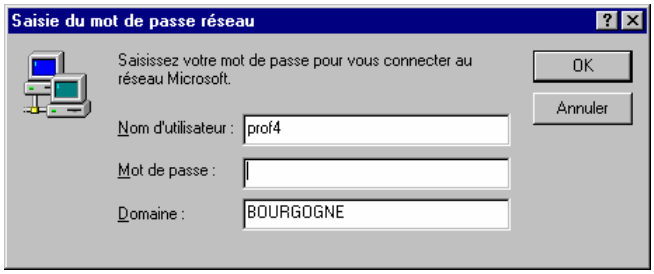
Le réseau poste à poste sous Windows 9x, ne permet pas de contrôler efficacement l'accès aux ressources partagées.
En effet, le contrôle d'accès se fait au niveau de la ressource elle même et ne propose qu'un accès en lecture uniquement, un accès complet en lecture et écriture ou un accès selon un mot de passe défini et à transmettre aux différents utilisateurs potentiels, ce qui en limite sérieusement l'efficacité.

Dans le cadre d'un domaine Windows NT, il est possible de contrôler l'accès aux ressources en fonction des utilisateurs et des groupes définis sur le domaine.



Ouverture de session sur le domaine

Lorsque la configuration de connexion au réseau est terminée, lors du démarrage d'un poste client, l'utilisateur est invité à donner son nom de connexion (login) et son mot de passe sur le domaine considéré.



Les informations fournies par l'utilisateur vont êtres contrôlées par un contrôleur de domaine, au niveau de sa SAM (*Security Account Manager*). Si l'utilisateur est reconnu, il va se voir affecter un jeton. Sinon il sera rejeté.

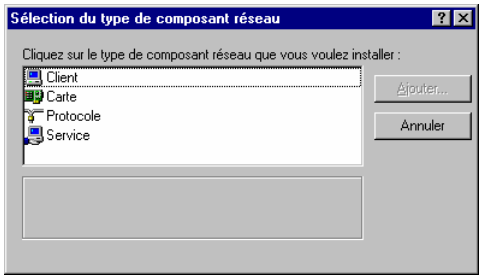
Le jeton de l'utilisateur va être utilisé pour contrôler ses actions dans le domaine. Il contient son SID (*Security Identification - identifiant unique attribué à un utilisateur et lui permettant d'accéder aux ressources d'un système informatique*), les SID de tous les groupes auquel il appartient et un certain nombre d'autres informations dont ses droits systèmes.
Il devient donc évident qu'un changement du contenu du jeton ne peut pas se faire de façon dynamique (création au moment de l'ouverture de session). Par exemple, un changement d'affectation de groupe ne prendra effet que lors de la prochaine ouverture de session.

Au niveau des ressources, les permissions et les droits qui leurs sont affectées, forment l'ACL (*Access Control List - Liste de Contrôle des Accès et Ressources par utilisateur, exploitée par les logiciels de gestion de réseaux*). Lorsqu'un utilisateur cherche à utiliser une ressource du domaine, le contrôleur de domaine va comparer le contenu de l'ACL de la ressource et du jeton de l'utilisateur. En fonction du résultat, l'utilisateur aura ou non accès à la ressource.
Les ACL ont des changements dynamiques. Il n'est heureusement pas nécessaire de redémarrer la ressource pour que les changements soient pris en compte.

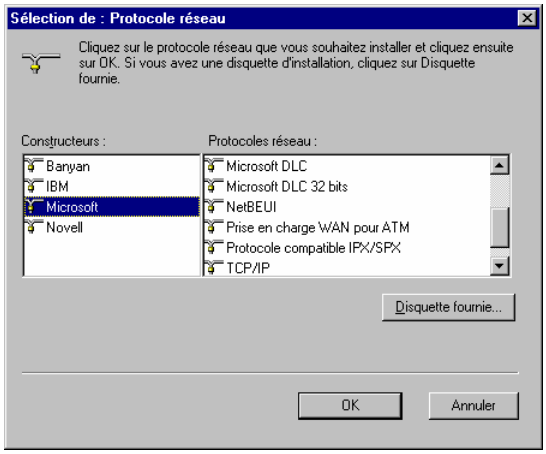
Ajout de composants réseau

Il est possible d'ajouter d'autres Clients réseau, d'autres protocoles, des cartes supplémentaires ou des services.

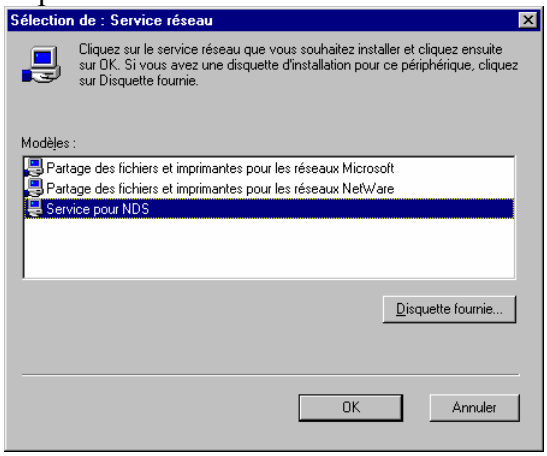
En cliquant sur le bouton Ajouter de l'onglet Configuration de l'icône Réseau, on obtient la fenêtre ci-contre.



Quelques protocoles Microsoft …



Le service de partage des fichiers et imprimantes.



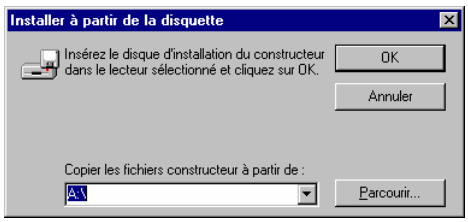
Ajout du service Base de registre distante Microsoft

Windows 9x intègre des outils permettant de gérer finement les stations et les utilisateurs, en local ou en réseau.

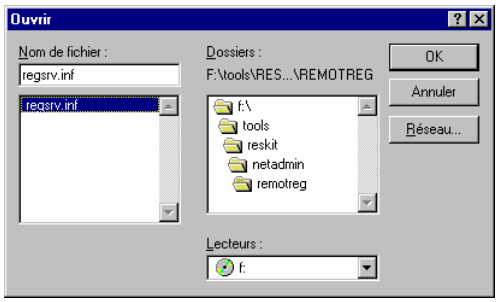
La mise en place de ces outils ouvre des possibilités intéressantes de gestion de salles pédagogiques. Mais ils prennent tout leur sens dans un environnement réseau. Il est par exemple possible à un utilisateur donné de retrouver son environnement sur n'importe quel poste du réseau. Ou encore de modifier les propriétés d'un poste via le réseau (pour une personne autorisée).

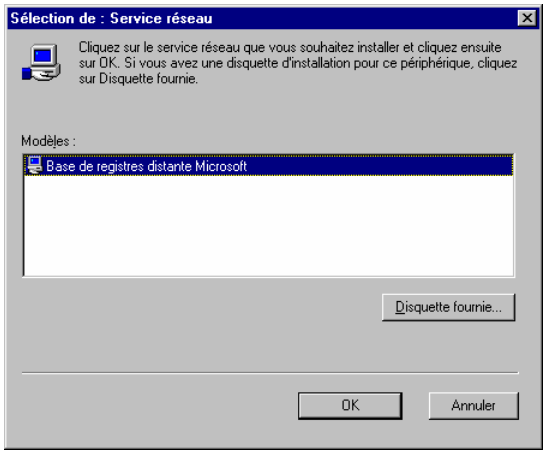
La mise en place des stratégies système passe par la modification de la Base de registres de Windows 9x et par l'installation du service de Base de registre distante.

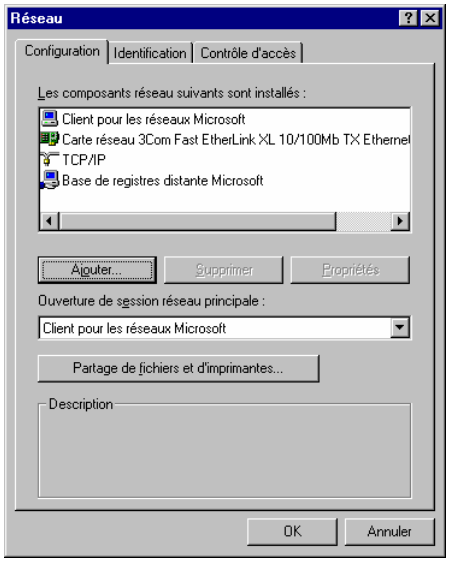
La base de registre distance est livrée dans les outils complémentaires de Windows 98.



Sur le CD-ROM, il faut localiser le fichier d'installation regserv.inf situé dans : TOOLS\RESKIT\NETADMIN\REMOTEREG







L'installation est maintenant terminée, il suffit de redémarrer le système pour que la nouvelle configuration soit prise en compte.

L'administration distante

Les outils de gestion à distance

- **Le Moniteur système**
  Il permet de contrôler les performances d'un ordinateur du réseau. On peut ainsi obtenir des informations relatives aux performances du système de fichiers ou des clients réseau par exemple.

- **L'Observateur réseau**
  Lorsque'on utilise les services Partage de fichiers et d'imprimantes, l'observateur réseau permet de créer, d'ajouter et de supprimer des ressources partagées sur des ordinateurs à distance, ainsi que de gérer les connexions aux ressources partagées.
  Cela se révèle utile pour connaître les connexions en cours sur un ordinateur donné ainsi que les fichiers qui y sont ouverts.

- **L'Editeur de stratégie système** (Poledit)
  Il permet d'éditer des entrées dans la Base de registre en temps réel d'un ordinateur distant. On peut également créer, éditer et gérer des stratégies système afin de contrôler les paramètres d'un ensemble d'ordinateurs sur le réseau.
- **L'Editeur de la Base de registre** (Regedit)
  Il permet de lire, de modifier, d'ajouter et de supprimer des valeurs directement dans la Base de registres d'un ordinateur distant.

Éléments nécessaires à l'administration à distance

Pour tirer parti des capacités d'administration à distance de Windows 9x, il faudra :

- Installer le service de Base de registre distante
- Activer la sécurité au niveau utilisateur et l'administration à distance sur chaque ordinateur que l'on souhaite gérer à distance.

message renvoyé lorsque les éléments nécessaires à l'administration à distance ne sont pas en place.

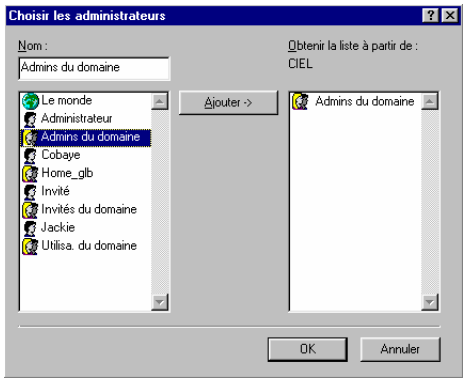
- Exécuter un protocole commun de réseau tel que le protocole compatible IPX/SPX, TCP/IP ou NetBEUI.
- Apprendre à maîtriser les outils d'administration à distance (qui ne sont pas sans risque !).

Lorsque l'administration à distance est activée sur un ordinateur, deux répertoires partagés spéciaux sont créés :

- ADMIN$ donne accès, aux administrateurs, au système de fichiers de l'ordinateur à distance.
- IPC$ fournit un canal de communication interprocessus (InterProcess Communication) entre les deux ordinateurs.

Définition des utilisateurs autorisés à administrer la station

Par défaut, l'administration à distance est activée automatiquement pour le groupe : Domaine admins (ce qui fonctionne correctement si le contrôleur de sécurité est un serveur NT en version US en non française !). Il faut donc commencer par rajouter les utilisateurs qui seront autorisés à administrer la station. Pour cela, aller dans le panneau de configuration, mots de passe, onglet administration distante et rajouter les utilisateurs souhaités (au minimum le groupe global **Admins du domaine** !).



Il faudra obligatoirement que ces opérations aient été réalisées sur tous les postes que l'on souhaitera administrer.

Client Windows XP Pro (ou Windows 2000 Pro)

Différences fondamentales entre Windows XP Home et Pro

Les ordinateurs sous Windows XP Édition familiale ne peuvent pas rejoindre des domaines. Pour cette raison, les fonctionnalités nécessitant un compte d'ordinateur dans le domaine, comme la stratégie de groupe, ne sont pas disponibles dans Windows XP Édition familiale.

En réseau, Windows XP Professionnel autorise jusqu'à dix connexions simultanées par partage de fichiers, alors que Windows XP Édition familiale n'en autorise que cinq.

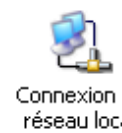
Configurations

Nous nous proposons de décrire les différentes étapes de la configuration d'un poste client Windows XP Pro sur un réseau, constitué d'un domaine nommé mpg.local, lequel possède un contrôleur de domaine nommé BigBoss tournant sous Microsoft Windows 2000 server.

Nous supposons que le poste client est sous Windows XP Pro, que la carte réseau installée dans la machine a été correctement détectée par le système.

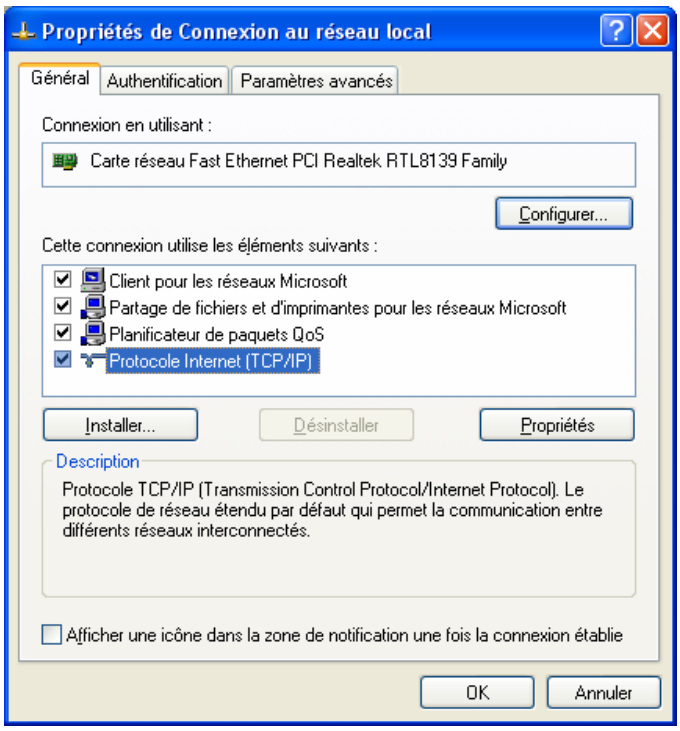
Accès à la configuration réseau

Un clic-droit sur l'icône du Favoris réseau et le choix de la commande contextuelle Propriétés permet d'accéder aux connexions réseau.



Un clic-droit sur l'icône du Connexion au réseau local et le choix de la commande contextuelle Propriétés permet d'accéder aux éléments de la configuration réseau.

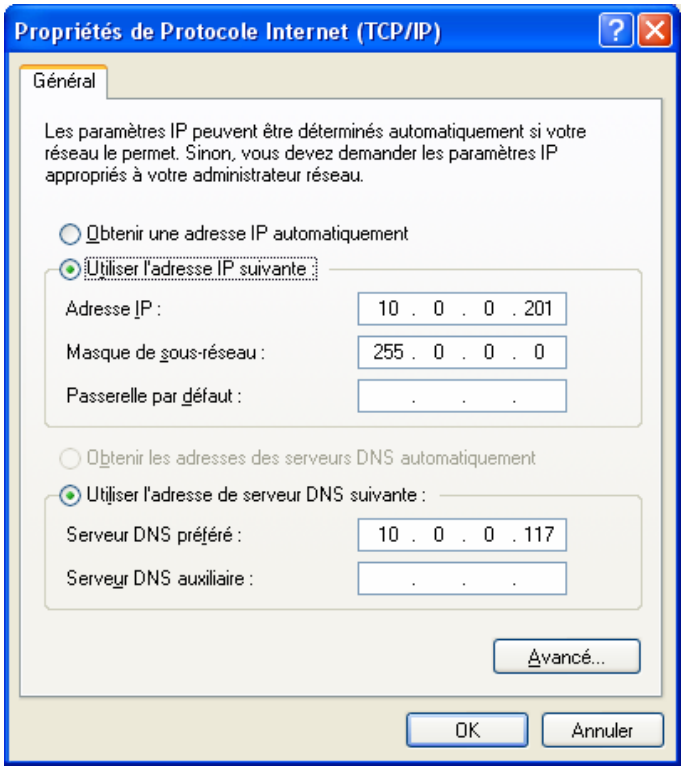
On accède ensuite facilement aux propriétés du protocole TCP/IP.



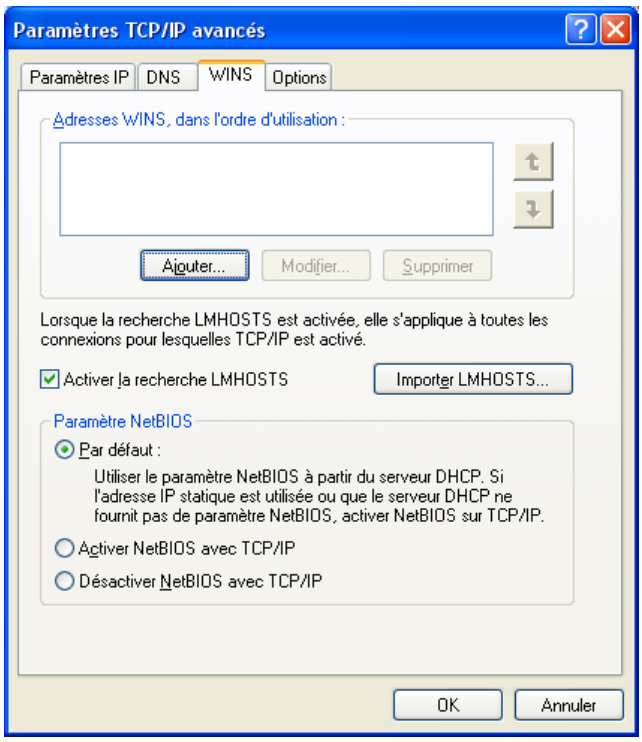
Propriétés du protocole réseau

Il est impératif de préciser dans la configuration l'adresse IP du serveur DNS du domaine.

Le bouton Avancé permet l'accès à d'autres éléments de la configuration TCP/IP.

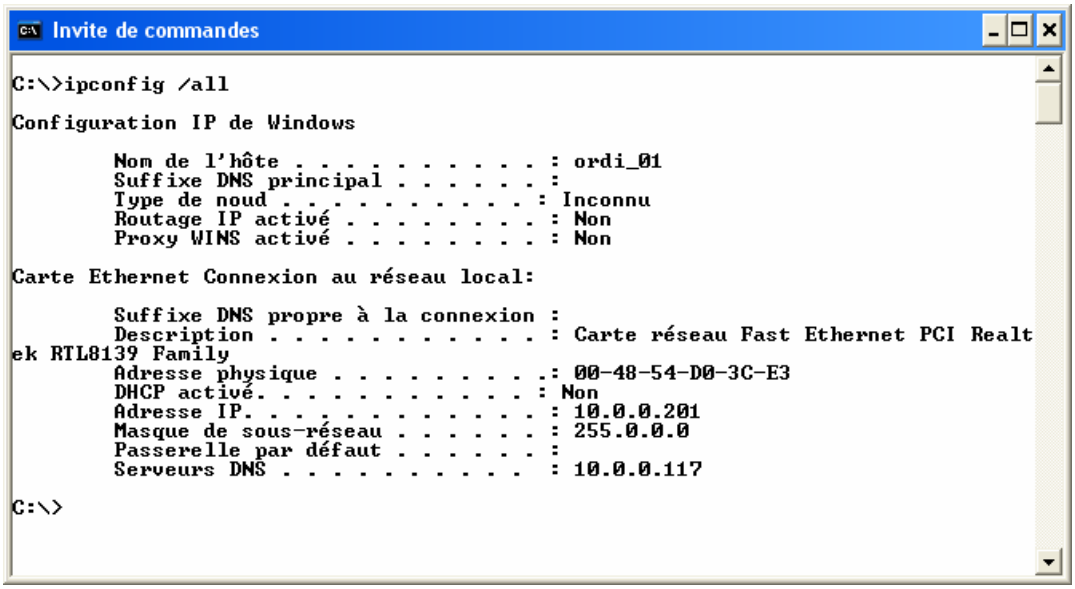


Tel le paramétrage des adresses WINS.



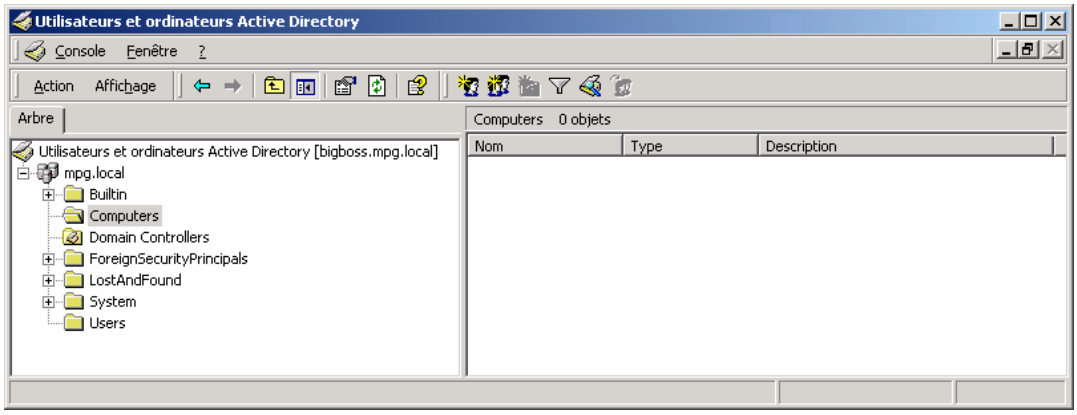
Il est également possible de désactiver NetBIOS avec TCP/IP.

Dans une fenêtre d'invite, la commande **ipconfig /all** permet de contrôler la configuration IP de la machine.



Joindre l'ordinateur au domaine

Initialement aucun ordinateur ne fait partie du domaine, comme le montre l'écran ci-dessous :

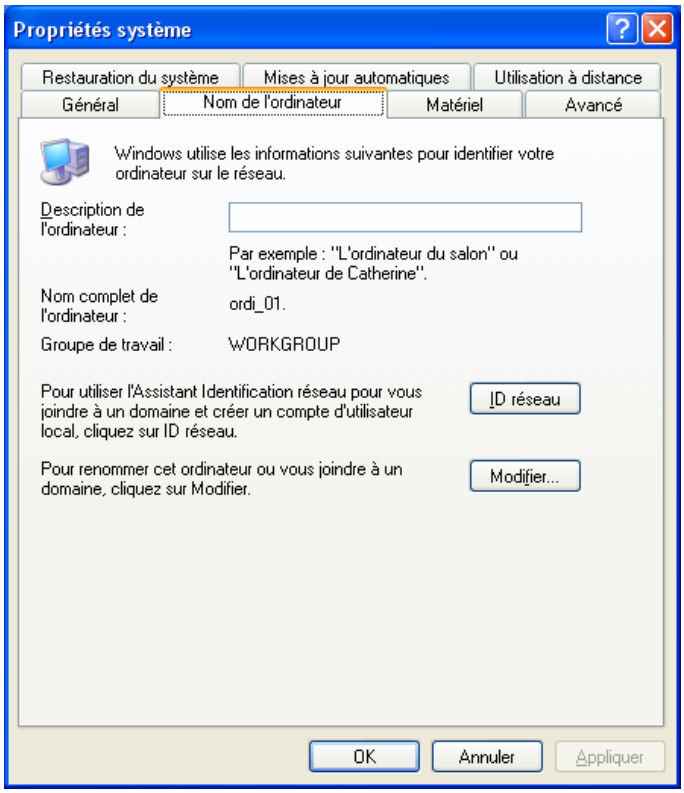


Poste de travail

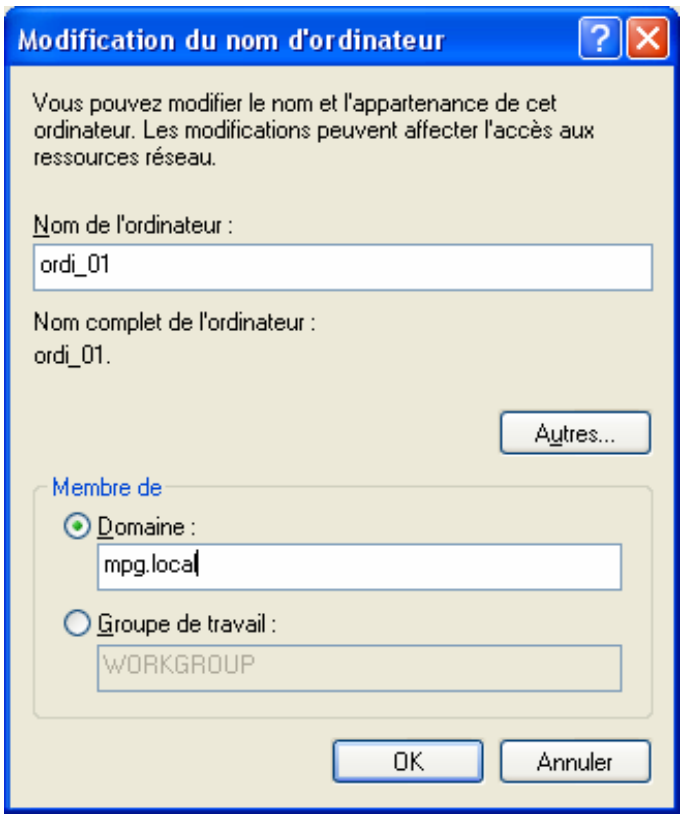
Un clic-droit sur l'icône du Poste de travail et le choix de la commande contextuelle Propriétés permet d'accéder aux Propriétés du système.

Ce qui va permettre de joindre l'ordinateur à un domaine

Par défaut l'ordinateur fait parti d'un WORKGROUP.

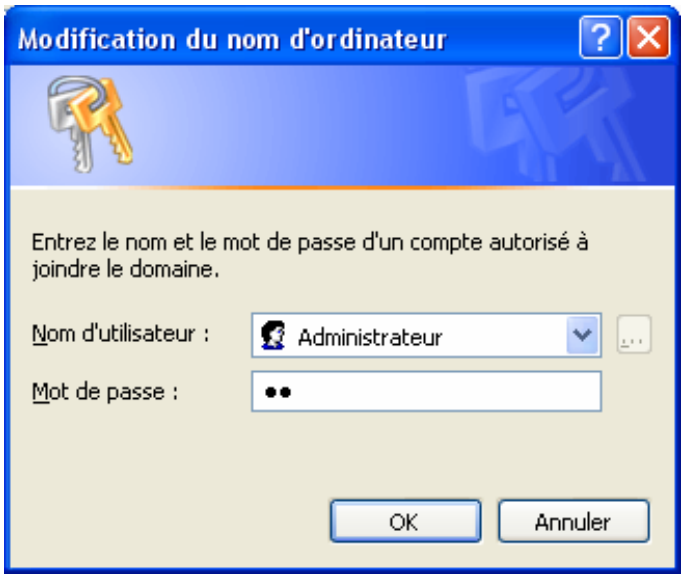


L'ordinateur va devenir membre du domaine mpg.local



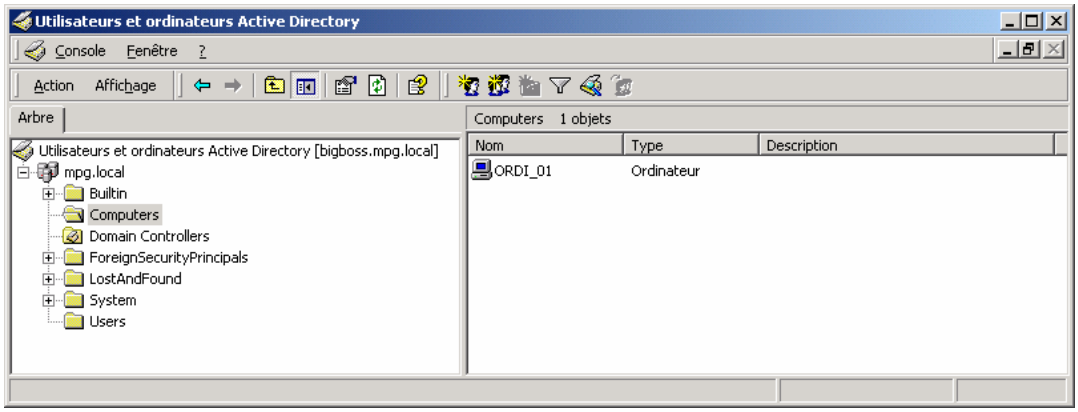
Un compte autorisé à joindre une machine au domaine est requis.

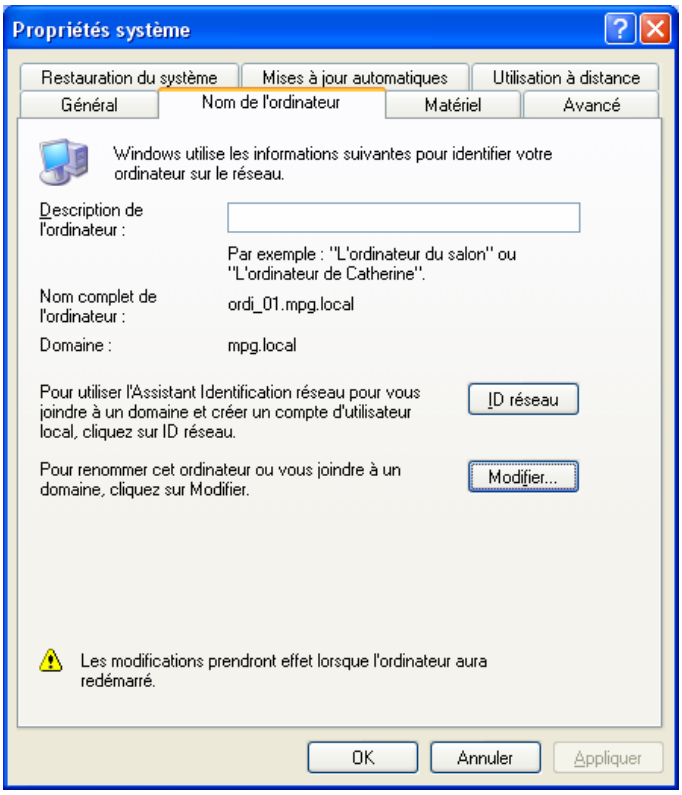
L'administrateur du domaine par exemple.

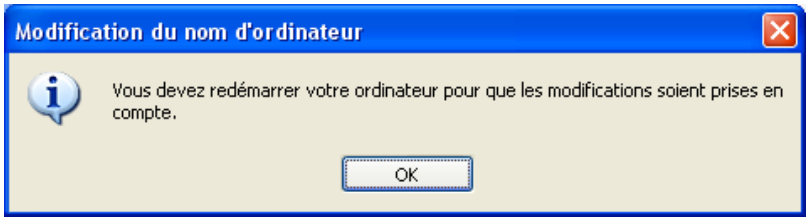


L'ordinateur est accepté dans le domaine.

Le compte de l'ordinateur a été créé dans Active Directory.







Ouverture de session

Vous pouvez ouvrir une session en tant qu'utilisateur local de l'ordinateur.

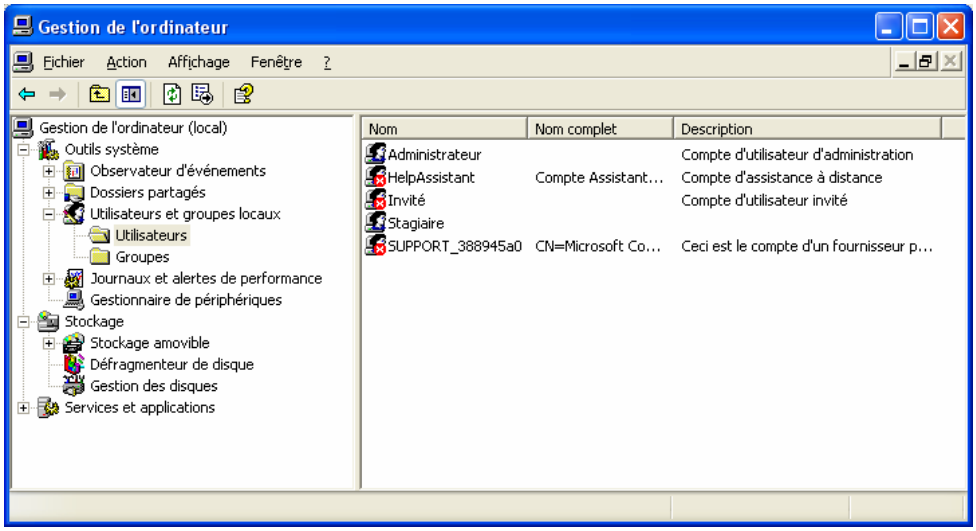
Ou en tant qu'utilisateur du domaine.

Autre forme possible.

Comptes utilisateurs et groupes locaux

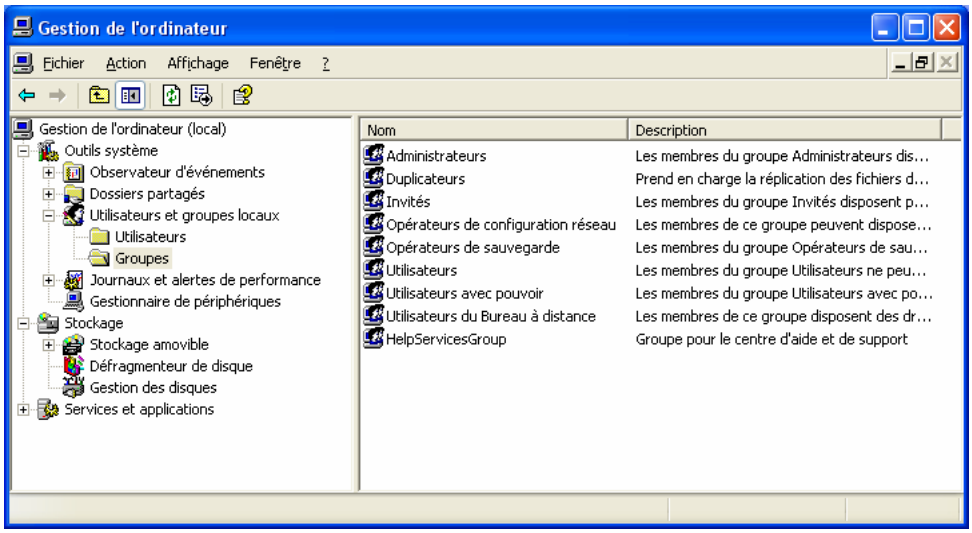
Un clic-droit sur l'icône du Poste de travail et le choix de la commande contextuelle Gérer permet d'accéder aux Utilisateurs et groupes locaux.

Les comptes utilisateurs



Administrateur	compte d'utilisateur d'administration. Il a un contrôle total sur l'ordinateur local.
HelpAssistant	compte d'assistance à distance.
Invité	compte d'utilisateur invité. Il est déactivé par défaut et il est conseillé de le laisser dans cet état.
SUPPORT_388945a0	compte d'un fournisseur pour les service Aide et support CN=Microsoft Corporation,L=Redmond,S=Washington,C=US

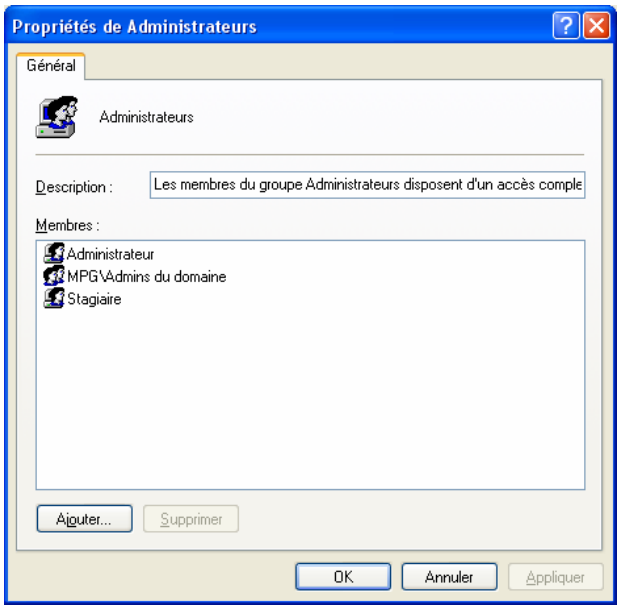
Les comptes de groupes



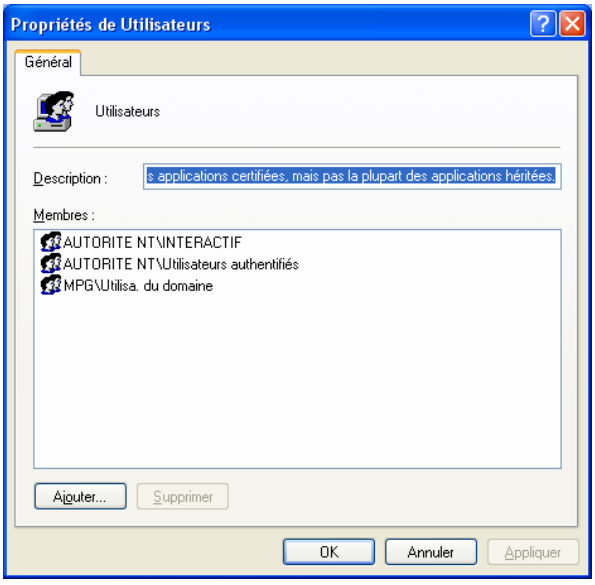
Administrateurs	Les membres du groupe Administrateurs disposent d'un accès complet et illimité à l'ordinateur et au domaine.
Duplicateurs	Prend en charge la réplication des fichiers dans le domaine.

Invités	Les membres du groupe Invités disposent par défaut du même accès que les membres du groupe Utilisateurs, à l'exception du compte Invité qui dispose d'autorisations restreintes.
Opérateurs de configuration réseau	Les membres de ce groupe peuvent disposer de certaines autorisations d'administration pour la configuration des fonctionnalités réseau.
Opérateurs de sauvegarde	Les membres du groupe Opérateurs de sauvegarde peuvent passer outre les restrictions de sécurité uniquement dans le but d'effectuer la sauvegarde ou la restauration de fichiers.
Utilisateurs	Les membres du groupe Utilisateurs ne peuvent pas effectuer de modifications système accidentelles ou intentionnelles. Ainsi, les utilisateurs peuvent exécuter les applications certifiées, mais pas la plupart des applications héritées.
Utilisateurs avec pouvoir	Les membres du groupe Utilisateurs avec pouvoir disposent de la plupart des droits d'administration, avec quelques restrictions. Ainsi, les utilisateurs avec pouvoir peuvent exécuter des applications héritées, ainsi que des applications certifiées.
Utilisateurs du Bureau à distance	Les membres de ce groupe disposent des droits nécessaires pour ouvrir une session à distance.
HelpServicesGroup	Groupe pour le centre d'aide et de support.

Le fait de joindre un domaine, ajoute dans le groupe local des Administrateurs, le groupe des administrateurs du domaine (Admins du domaine).



De même, le groupe des utilisateurs du domaine (Utilisa. du domaine) est ajouté au groupe local des Utilisateurs de l'ordinateur.



Créer un profil type pour tous les utilisateurs

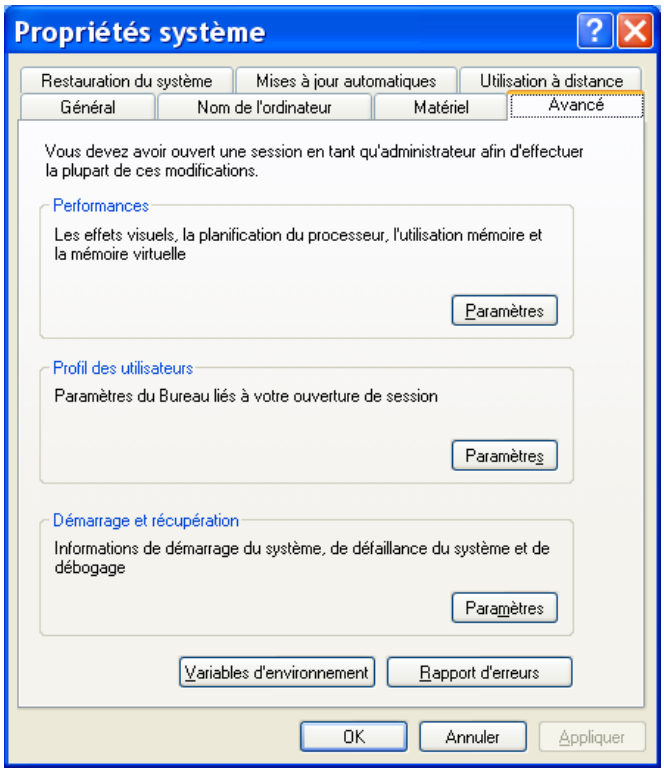
Procédure

1- En tant qu'administrateur, créer un compte temporaire Test par exemple.
2- Se connecter en tant qu'utilisateur Test.
Définir les paramètres de configuration de l'environnement de travail de l'utilisateur (Bureau, Menu Démarrer, …).
3- Se reconnecter en tant qu'administrateur , procéder aux dernières modifications du profil de l'utilisateur Test et copier ce profil sur celui de l'utilisateur par défaut (Default User).
4- Supprimer le compte de l'utilisateur Test.

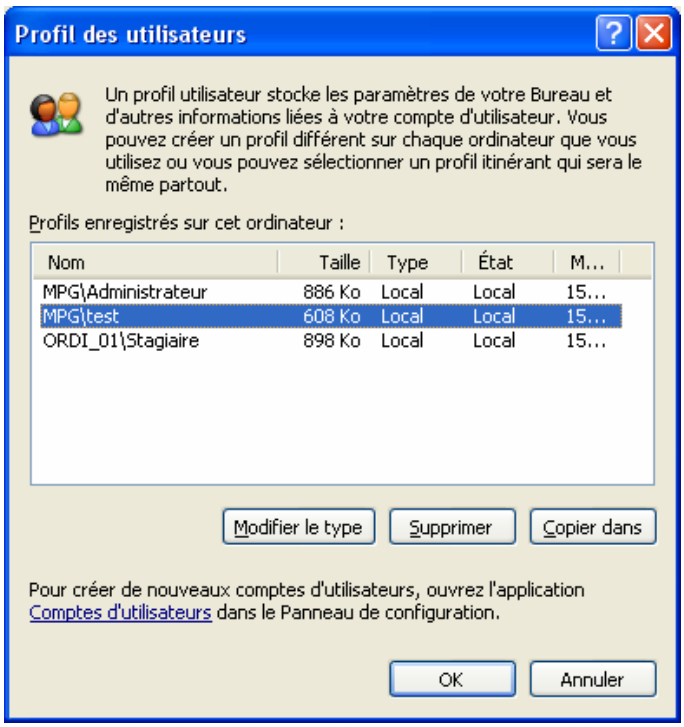
Copie d'un profil

Un clic-droit sur l'icône du Poste de travail et le choix de la commande contextuelle Propriétés permet d'accéder aux Propriétés du système.

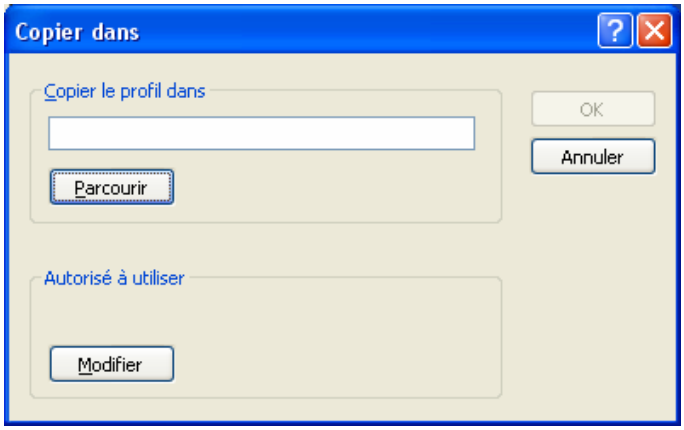
L'onglet Avancé permet d'accéder aux paramètres de bureau d'un profil utilisateur.



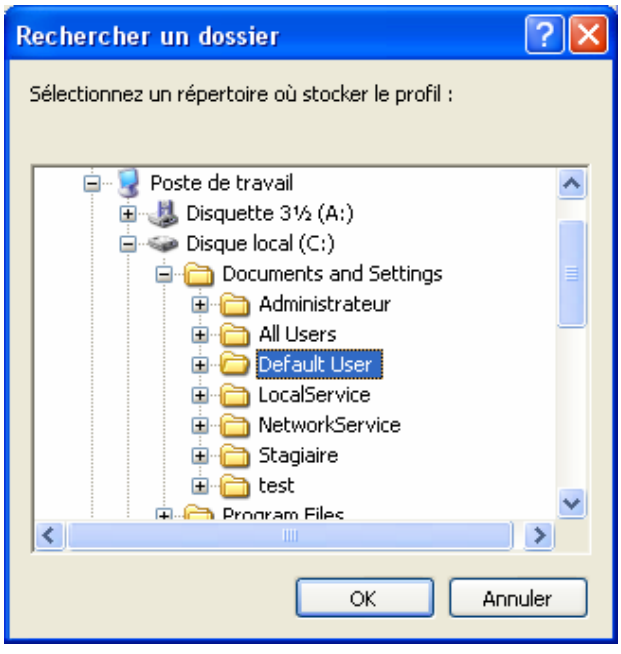
Copier le profil de l'utilisateur Test



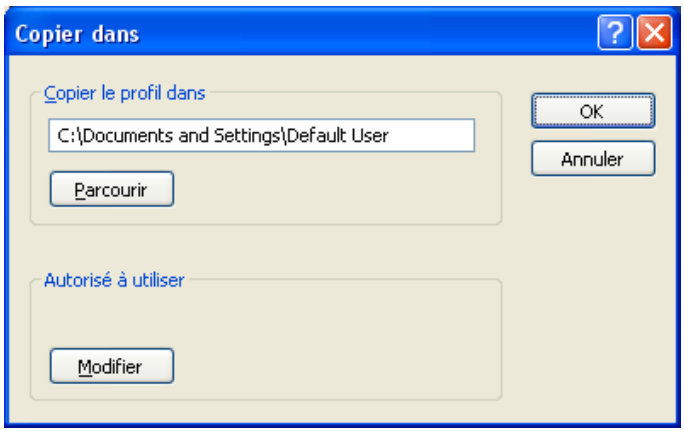
Utiliser le bouton Parcourir pour trouver la localisation du profil de l'utilisateur par défaut.



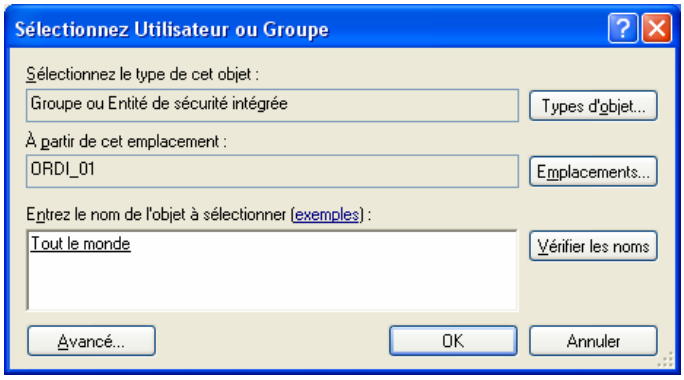
C:\Documents and Settings\Default User

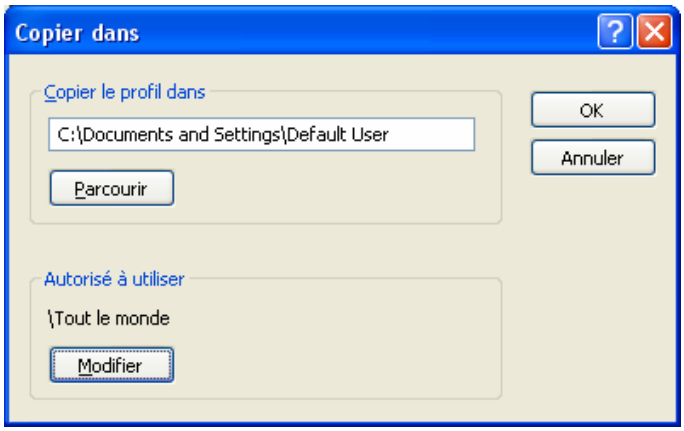


Utiliser le bouton Modifier …

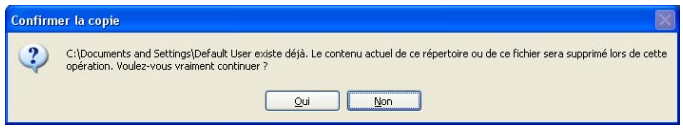


pour autoriser le groupe « Tout le monde » à utiliser ce profil après avoir choisi les types d'objets à rechercher dans l'ordinateur local.





Accepter le remplacement de l'ancien profil Default User par le nouveau.



Le profil par défaut est maintenant opérationnel pour tous les utilisateurs du domaine.