Nouvelle configuration du réseau local Miniplan

Claude-Éric Desguin

La mise en service, grâce au PRCI, d'un nouveau serveur HP Proliant ML350GS en avril 2008 a été l'occasion d'une mise à niveau du réseau local 'Miniplan'.

L'adresse IP attribuée à ce serveur est **192.168.11.3** (initialement son adresse était 192.168.11.11 mais il a été jugé préférable de lui attribuer une adresse dans la série 192.168.11.1 à 9, traditionnellement réservée aux serveurs) et son nom est **« pipserver »**, avec un descriptif **« Serveur PiP Production »**.

Il assure désormais *toutes* les fonctions de gestion du réseau local, y compris celles qui étaient jusqu'ici assurées par l'ancien serveur Windows 2000 (adresse IP **192.168.11.2**, dénomination **« serveur »**).

À l'examen de cet ancien serveur, il est apparu que :

- Le système d'exploitation Windows 2000 Server est fortement dégradé ;
- Le disque dur est physiquement endommagé ;
- Les supports originaux d'installation du système ont été égarés.

1. Première action :

La configuration initiale par défaut du nouveau serveur **« pipserver »** (initialement nommé « hpxxxxxx » d'après le n° de série de la machine) n'était pas optimale et a dû être entièrement refaite :

- Volume système redimensionné à **25 Go** au lieu de 7, valeur nettement insuffisante pour assurer la stabilité du système,
- Reconfiguration du système **« RAID »** (« Redundant Array of Independent Disks » ou *ensemble redondant de disques indépendants*) : les trois disques équipant le serveur ont été configurés pour une sécurité maximale (**« RAID5 »**) et non pour une vitesse maximale (**« RAID0 »**) comme initialement. Les trois disques sont désormais totalement redondants, ce qui signifie qu'en cas de dégradation accidentelle de données sur l'un d'eux, le contenu des deux autres sera utilisé pour réparer automatiquement le contenu du disque endommagé. (Voir http://www.commentcamarche.net/protect/raid.php3)
- Configuration du dispositif de **sauvegarde automatique** sur bandes magnétiques ; après une sauvegarde initiale de l'ensemble des données du système, une sauvegarde journalière différentielle automatique a été programmée chaque nuit à 23h59. « Différentielle » signifie que la sauvegarde journalière contiendra uniquement les différences par rapport à la sauvegarde précédente. Ceci économisera le volume utilisé sur la bande magnétique.

2. Deuxième action :

Nous avons ensuite procédé à une seconde opération visant à rassembler sur le nouveau serveur **« PipServer »** la totalité des fonctions de réseau auparavant assurées par l'ancien serveur **« Serveur »** très dégradé, et dont la mise hors service définitive est recommandée. Nous l'avons arrêté après en avoir sauvegardé tout le contenu récupérable (deux partitions sur trois sont en effet illisibles).

Parmi les tâches effectuées lors de cette opération était prévue la migration du domaine existant **« miniplan.bi »** vers le nouveau serveur. Malheureusement l'ancien serveur, trop dégradé, n'a pu répondre sans erreur à la demande de migration, qui s'est soldée par un échec. Nous avons donc dû créer un nouveau domaine **« pip »**, contrôlé par **« pipserver »** et géré à partir de ses outils d'administration. L'ancien domaine **« miniplan.bi »** a donc été arrêté en même temps que l'ancien serveur (rappelons toutefois que son contenu est sauvegardé).

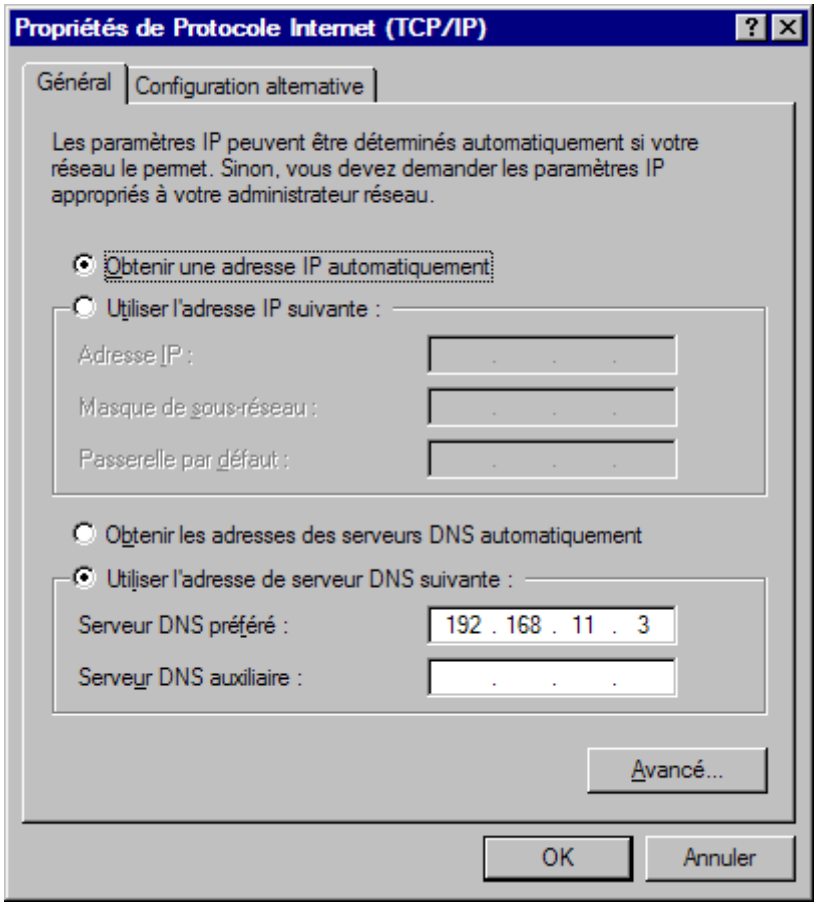
*(NB : un **domaine** est un ensemble de ressources sur un réseau Windows utilisant les mêmes règles de sécurité. Pour une machine isolée, le domaine est la machine elle-même. Pour un réseau, c'est une région définie par l'administrateur du réseau, incluant des machines, des utilisateurs, des groupes et des données partagées. Un domaine est géré par un **« contrôleur de domaine »**, en l'occurrence **« pipserver »**).*

Une documentation décrivant succinctement l'installation d'un serveur Windows 2003 est disponible sur le serveur lui-même. Voir
\\192.168.11.3\pip\documentation\doc_technique\InstallWindows2003Serveur.pdf

Note : la configuration du serveur a été effectuée grâce à l'appui à distance de M. Brice Servais, administrateur de réseaux qualifié en systèmes Microsoft (brice.servais@walkabout.be)

Changements à effectuer sur chacun des postes de travail

1. Configuration de la connexion au réseau :

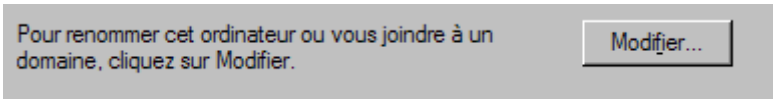


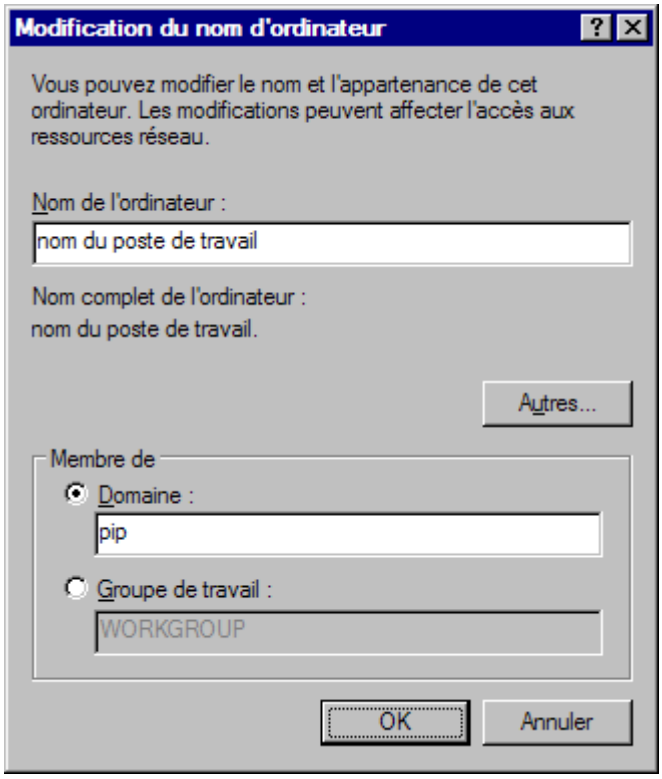
Les configurations antérieures attribuaient une adresse IP fixe à chaque poste de travail, ce qui occasionnait ne nombreux conflits d'adresse (la même adresse ayant été attribuée à plusieurs machines). L'adressage automatique éliminera ce problème. En effet, une adresse IP fixe n'est utile que pour les serveurs et autres ressources partagées de manière permanente, par exemple les imprimantes réseau.

Le **DNS** (**« Domain Name System »** ou gestion de l'adressage IP), auparavant délégué au fournisseur d'accès à Internet (196.2.12.200 et 196.2.8.205) pour chaque poste de travail, sera désormais assuré par « pip-server (192.168.11.3)». Ceci doit améliorer la performance du réseau, cette fonction étant désormais assurée localement et non plus par les DNS publics.

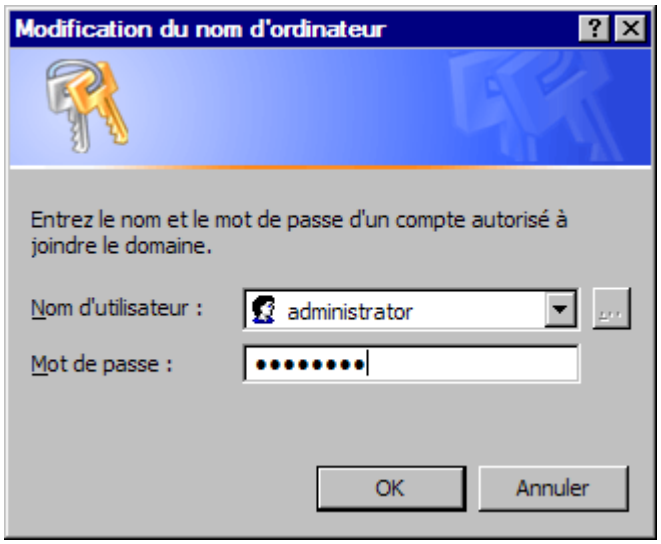
2. Inscription au domaine PiP (par l'administrateur du réseau) :

Dans les **« propriétés du poste de travail »**, sélectionner l'onglet **« Nom de l'ordinateur »**, ensuite le bouton **« Modifier »** :





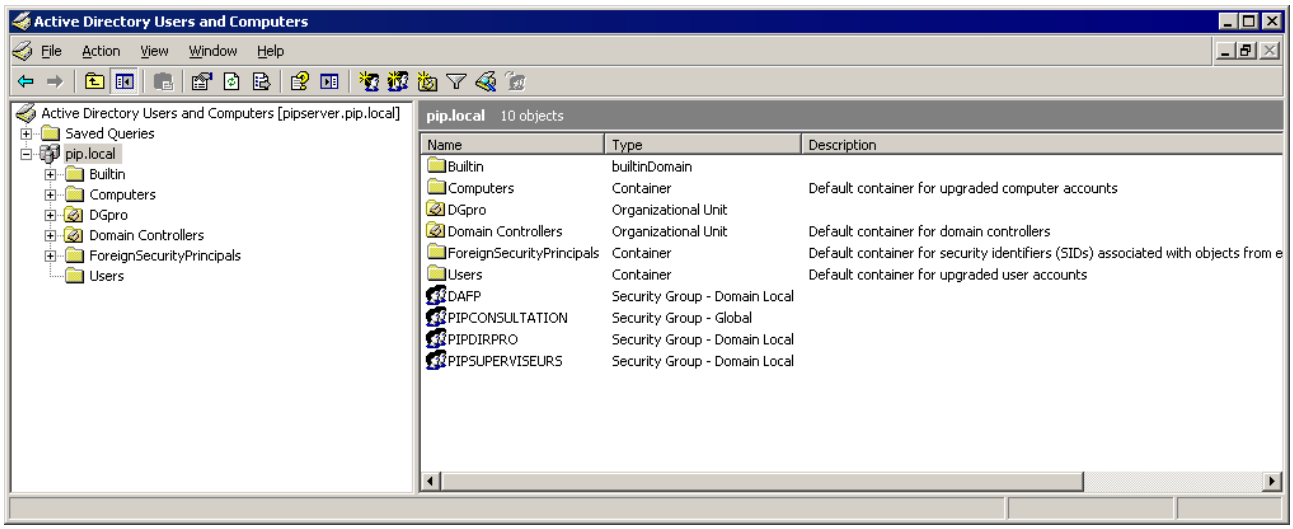
Procéder à l'inscription du poste de travail, opération qui nécessite que l'on s'authentifie comme administrateur du serveur (dont le mot de passe administrateur est identique à celui de l'ancien serveur aujourd'hui arrêté) :



(Un redémarrage de la machine sera ensuite nécessaire)

3. Accès aux ressources partagées PiP :

a) Groupes

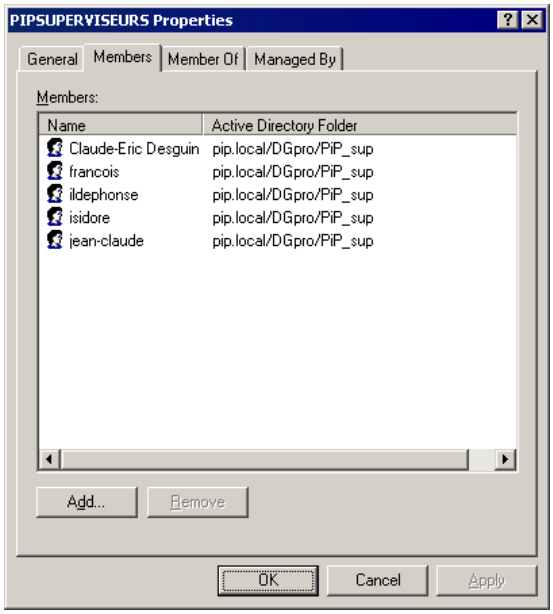


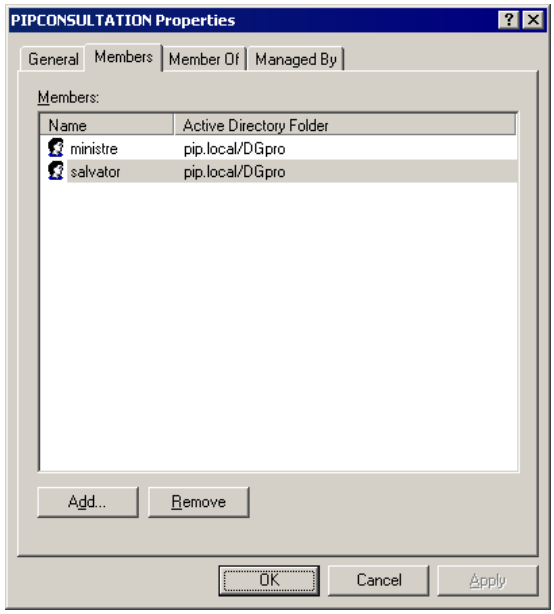
Dans le domaine « pip » ont été créés **4 groupes** d'utilisateurs authentifiés :

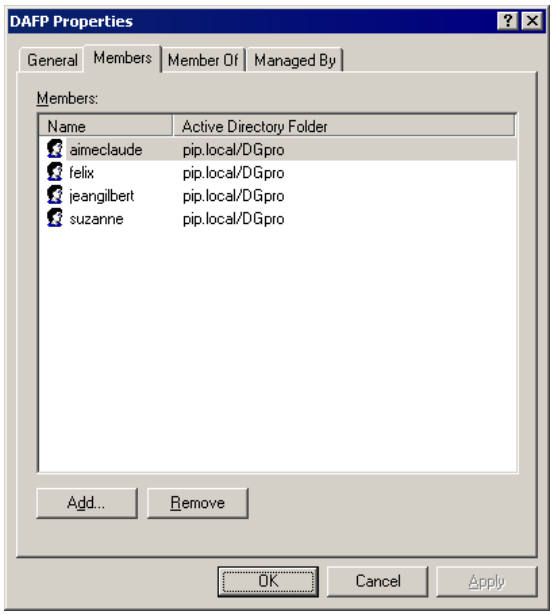
- **PIPSUPERVISEURS** : les utilisateurs chargés de superviser les travaux d'élaboration du PiP et de gérer la base de données.
- **PIPDIRPRO** : les utilisateurs chargés de la saisie et de la gestion des données PiP ainsi que de produire les états de sortie.
- **PIPCONSULTATION** : les utilisateurs autorisés à accéder à la base de données PiP en lecture seule (y compris l'impression des états de sortie).
- et **DAFP** : les cadres de la DAFP, avec des droits d'accès à définir ultérieurement.

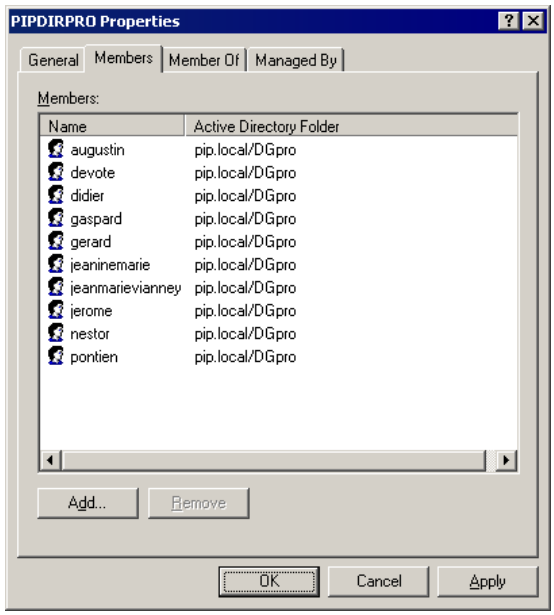
b) Utilisateurs

Les utilisateurs sont, pour le moment, répartis comme suit (l'administrateur du réseau pourra modifier cette liste ainsi que l'appartenance de chacun aux différents groupes) :



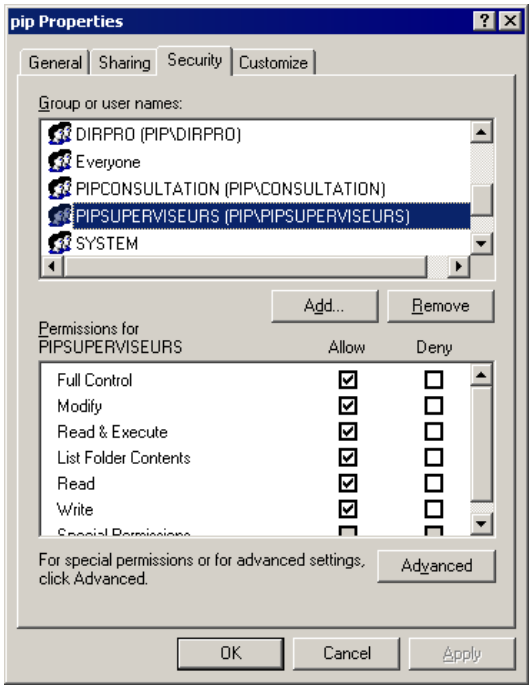


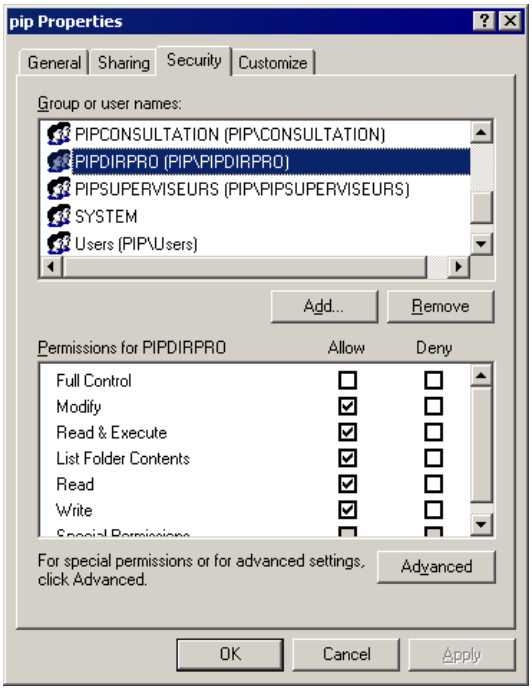


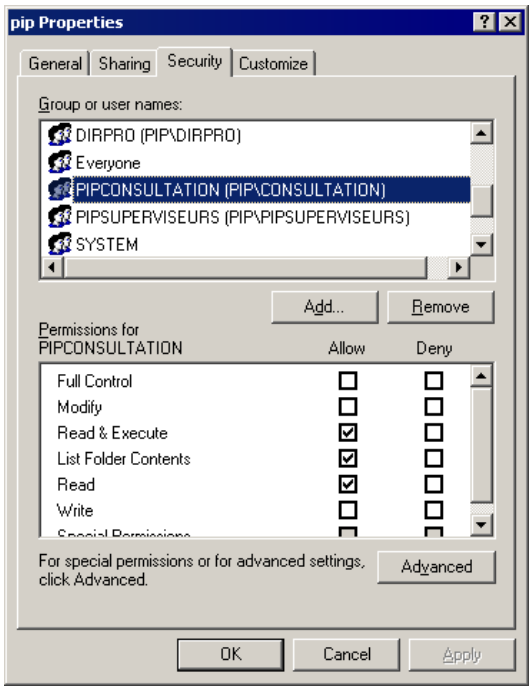


c) Privilèges

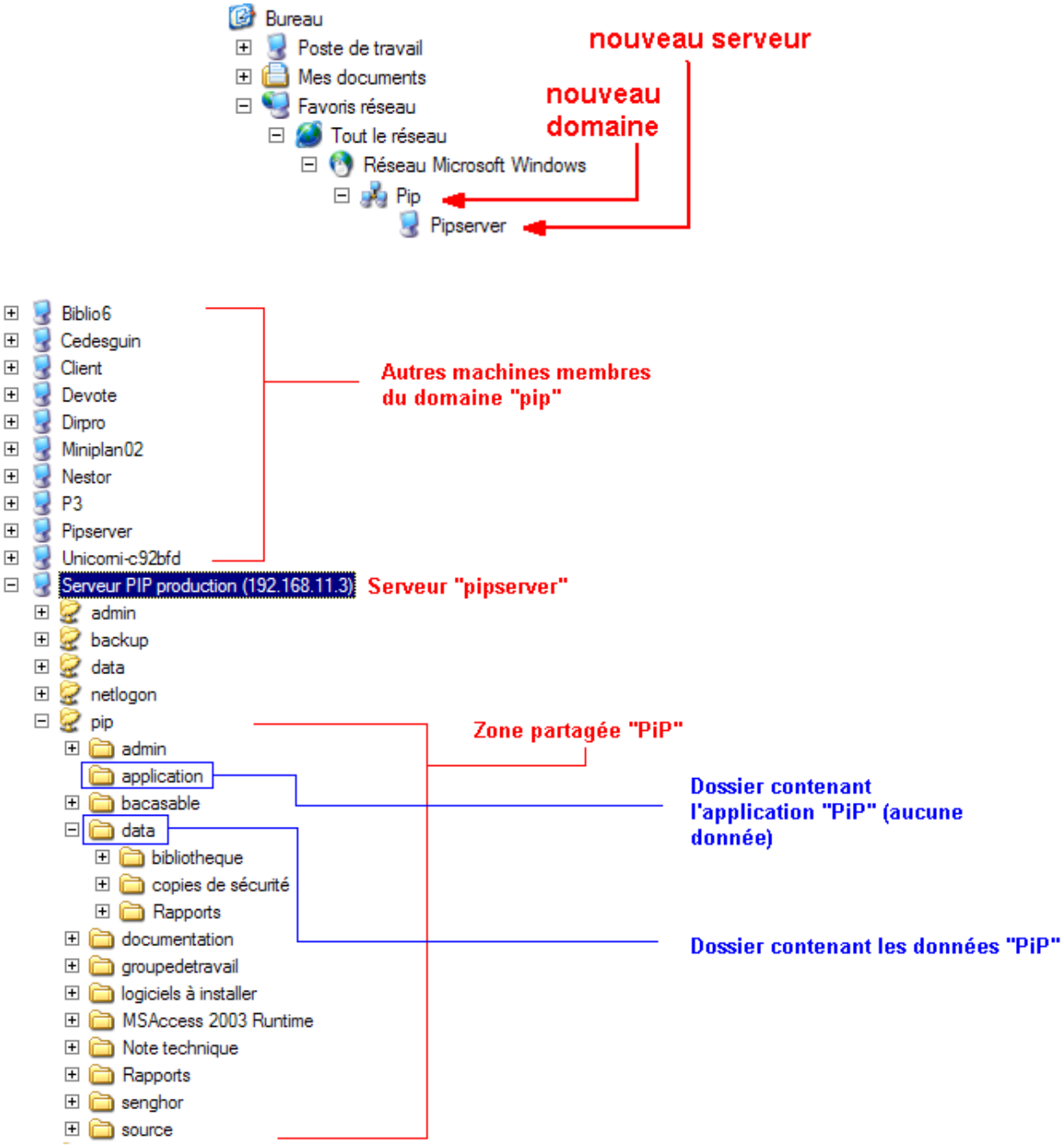
Les droits d'accès aux données partagées « pip » conférés aux groupes sont les suivants :







4. Les ressources partagées PiP :



Le dossier **« application »** sera donc celui auquel accéderont les utilisateurs authentifiés pour lancer l'application **« pip.mde »**, laquelle contient uniquement le programme et aucune donnée. Elle accède aux données contenues dans la base **« pipdata_exploitation2008.mde »** logée dans le dossier **« data »** de la zone partagée « pip ».

En raison des limitations imposées par Microsoft aux acquéreurs d'une licence Windows 2003 Server standard, et malgré le fait que ce système d'exploitation est spécialement destiné aux serveurs, seulement **cinq** utilisateurs peuvent accéder simultanément à une même ressource partagée (en l'occurrence l'application **« pip.mde »**). Une licence permettant 25 accès simultanés au lieu de 5 peut être acquise moyennant environ 2.500 € (modification purement administrative, aucun changement technique).

Dans l'état actuel des choses, on a donc recouru à un artifice consistant à dupliquer l'application **« pip.mde »** sous les noms de **« Copie de pip.mde »**, **« Copie (2) de pip.mde »**, **« Copie (3) de pip.mde »**, **« Copie (4) de pip.mde »** et **« Copie (5) de pip.mde »**, ainsi que sous une version compressée dans une archive nommée **« pip.zip »**. Cette version compressée et archivée présente l'avan-

tage suivant, décrit dans la note **« LISEZMOI.TXT »** figurant dans le dossier « application » et reproduite ci-dessous :

```
NOTE POUR ACCÉDER PLUS FACILEMENT AU PROGRAMME
==============================================

(Dossier "\\Pipserver\pip\application")

Dans certaines conditions (nombreux utilisateurs simultanés), des difficulté d'accès
aux exécutables "pip.mde", "pip_copie1.mde" et/ou "pip_copie2.mde" peuvent survenir.

Dans ce cas, il est recommandé d'effectuer un clic du bouton DROIT de la souris sur
l'archive "PIP.ZIP" et de choisir "EXPLORER" dans le menu contextuel. On ouvre ainsi
l'archive comme un dossier virtuel.

Dans ce dossier virtuel, double-cliquer sur "pip.mde" pour l'exécuter sous MSAccess
et poursuivre comme d'habitude. Ne pas tenir compte de l'avertissement indiquant que
la base de données est ouverte en lecture seule (cela ne concerne que la base appli-
cation, et non les données partagées).

La différence entre cette procédure et la procédure habituelle est que vous exécutez
non pas le programme localisé sur le serveur, mais une copie temporaire localisée sur
votre propre poste de travail. Ceci élimine le risque de conflit d'accès avec
d'autres utilisateurs tout en garantissant que vous utilisez bien la version la plus
récente de l'application.
```

Une fois l'application lancée, son exploitation se déroule conformément aux instructions du manuel utilisateur (« **Documentation base de données PiP** ») qui a fait l'objet d'une formation à l'ENA du 26 novembre au 7 décembre 2007.

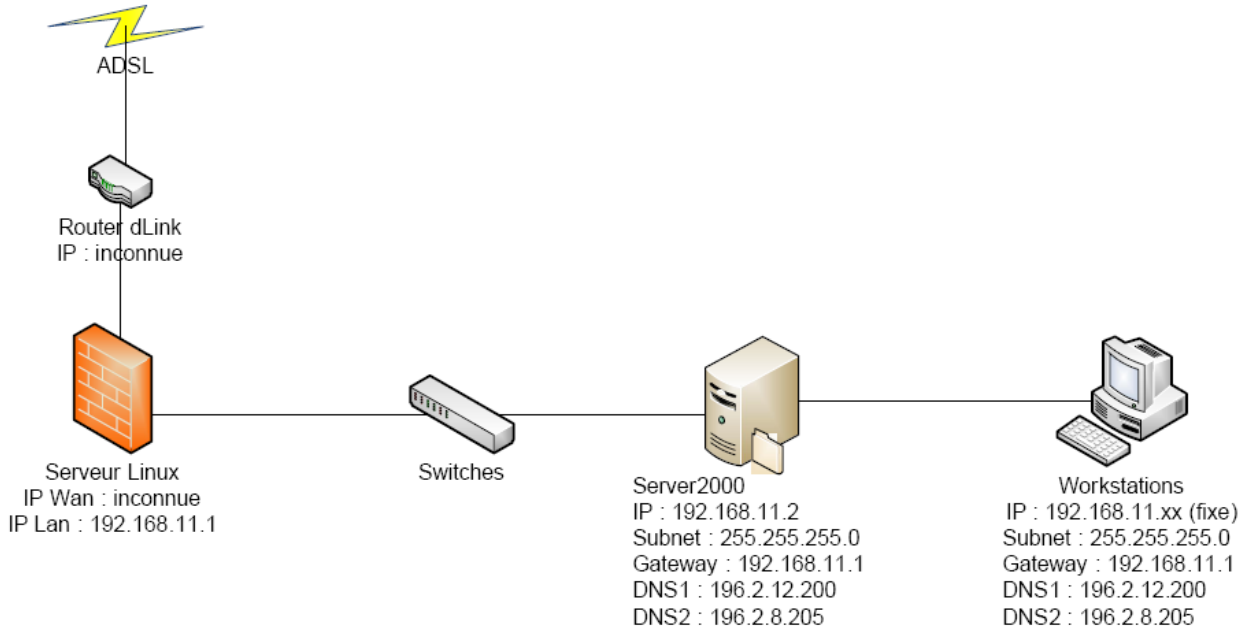
Dernière Minute

Une suite de sécurité Symantec/Norton, incluant antivirus, pare-feu et contrôle d'accès, a été installée le samedi 21 juin 2008 (en présence du responsable informatique du Miniplan) sur le serveur « pipserver ». Une actualisation des données d'identification des virus et autres logiciels malveillants a été effectuée immédiatement.

L'application a été paramétrée pour autoriser l'accès au serveur uniquement aux postes de travail affichant une adresse IP comprise dans la série précédemment spécifiée dans les paramètres du réseau local (entre 192.168.11.100 et 192.168.11.255). En d'autres termes aucun accès n'est possible en provenance d'un ordinateur n'appartenant pas au réseau local du Miniplan.

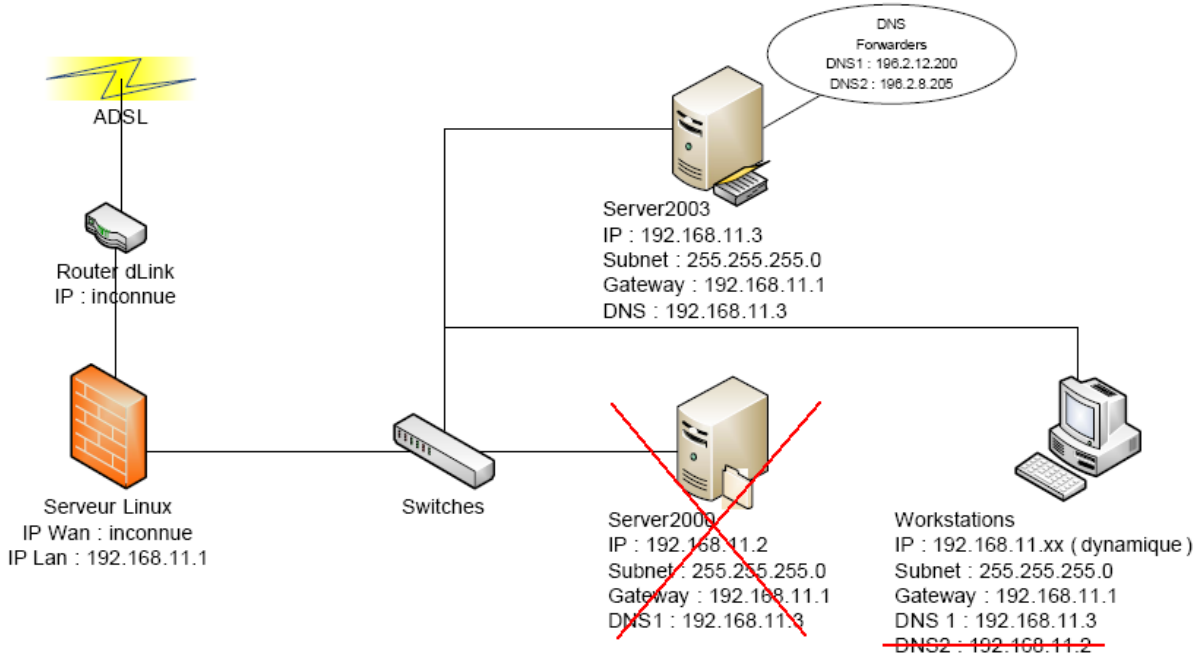
Le paramétrage du pare-feu comprend de nombreuses autres options qu'il conviendra d'administrer de manière optimale (plages horaires, utilisateurs déclarés ou bannis, adresse physiques, protocoles autorisés ou interdits, applications permises ou non, etc.)

Un effet collatéral de cette installation est la destruction de la sauvegarde du contenu de l'ancien serveur « serveur » (machine précédemment adressée « 192.168.11.2 ») : les nombreux virus et logiciels malveillants que cette sauvegarde contenait ont déclenché une action de nettoyage qui s'est soldée par la suppression pure et simple de cette sauvegarde. Une nouvelle sauvegarde pourra être effectuée au besoin après un indispensable nettoyage complet de la machine au moyen d'un logiciel antivirus actualisé ; ***nous insistons cependant sur les risques réels que présente le contenu des fichiers présents sur le disque de ce serveur. Sa remise en service est fortement déconseillée dans l'état où il se trouve, et la destruction de sa sauvegarde était tout simplement une mesure de salubrité indispensable.***



Situation actuelle :
- Pas de service DNS en local, les postes (server et workstations) font tous appel aux DNS publics.
- Server Linux fait firewall mais pas de controle dessus.

Resultat :
- trafic local hyper lent puisque toute requete, meme locale, est posee aux DNS publics qui ne connaissent rien du trafic local.



Situation Ideale :
- Services DNS en local sur les deux serveurs Windows, les postes (server et workstations) font tous appel aux DNS locaux.
- Services DNS locaux configures pour forward leur requetes aux DNS publics 196.2.12.200 et 196.2.8.205
- Server Linux fait firewall mais toujours pas de controle dessus.

Resultat :
- trafic local rapide puisque toute requete, publique ou locale, est posee aux DNS locaux qui ne forwardent aux publics que si la requete concerne un site en dehors de la zone miniplan.bi.
- iActive Directory et DNS se parlent
- Reseau protege