
Architecture réseau basée sur Windows 2000

Informations

Date *04.12.2001*
Etudiant *Yann Souchon*
Email *yann@linuxch.org*
Professeur *Gérald Litzistorf*

Mots clés

Active Directory, Kerberos, Audit, Réplication, Trust, IIS

Résumé

Ce document décrit les principaux éléments d'un réseau sous Windows 2000 avec un ou plusieurs domaines.

Conventions typographiques

Time New Roman	Police utilisée pour ce document en taille 12.
<i>Italique</i>	Utilisé pour les mots d'origine étrangère.
Gras	Utilisé pour la configuration ainsi que pour donner de l'importance à un mot.
→	Indique un renvoi sur une référence → Kerberos correspond au projet de semestre

Remerciements

Je tiens à remercier les personnes qui m'ont permis de réaliser ce document :

- M. Litzistorf pour sa rigueur et son intérêt.
- M. François-Xavier Marseille et M. Jean-Eric Cuendet pour leurs précieux conseils concernant le protocole Kerberos.

Les personnes que j'ai rencontrées dans l'école :

- Les camarades de classes des trois dernières années.
- Les collègues du laboratoire pour l'ambiance et la bonne humeur.

Et toutes les personnes qui m'ont soutenues :

- Mes parents, mon frère et mon amie qui m'ont encouragés durant toutes ces années.
- Mes amis, plus particulièrement M. Aurélien Porchet pour avoir relu et corrigé mon mémoire.

Annexes

1. Installation de Windows 2000 Server
2. Active Directory
3. Serveur de fichiers
4. Serveur DNS
5. Relations d'approbations
6. NetBIOS
7. Lightning Ethernet II
8. Différentes variantes d'accès à un serveur WEB
9. Analyse de protocole : Démarrage d'un ordinateur dans un domaine
10. Analyse de protocole : Authentification dans un domaine
11. Analyse de protocole : Différentes variantes d'accès à un serveur WEB

1	PRESENTATION DU MEMOIRE DE DIPLOME	5
2	AUTORISATIONS NTFS	6
2.1	INTRODUCTION	6
2.2	AUTORISATIONS LOCALES	7
2.2.1	Autorisations au niveau dossier	7
2.2.2	Autorisations au niveau fichier	7
2.2.3	Autorisations multiples	8
2.3	AUTORISATIONS DE PARTAGE	9
3	ACTIVE DIRECTORY	10
3.1	INTRODUCTION	10
3.2	COMPOSANTS	11
3.2.1	Objet et attribut (<i>Object and attribute</i>)	11
3.2.2	Compte d'utilisateurs (<i>Users account</i>)	12
3.2.3	Groupe d'utilisateurs (<i>Users group</i>)	13
3.3	STRUCTURE LOGIQUE	15
3.3.1	Domaine (<i>Domain</i>)	15
3.3.2	Unité d'organisation (<i>Organizational Unit</i>)	15
3.4	STRUCTURE PHYSIQUE	16
3.4.1	Contrôleur de domaine (<i>Domain Controller</i>)	16
4	KERBEROS	17
4.1	INTRODUCTION	17
4.2	GESTION DES CLES	20
5	ETAPE 1 : 1 DOMAINE	22
5.1	OBJECTIFS	22
5.1.1	Structure physique	22
5.1.2	Structure logique	23
5.2	SCENARIO 1 : DEMARRAGE D'UN ORDINATEUR DANS UN DOMAINE	27
5.3	SCENARIO 2 : AUTHENTIFICATION DANS UN DOMAINE	29
5.4	SCENARIO 3 : ACCES A UNE RESSOURCE PARTAGEE DANS UN DOMAINE	31
5.4.1	Principe	31
5.4.2	Configurations	32
5.5	SCENARIO 4 : AUDIT DE LA RESSOURCE PARTAGEE	35
5.5.1	Introduction	35
5.5.2	SID	36
5.5.3	Access Tokens	36
5.5.4	Descripteurs de sécurité	36
5.5.5	Principe	37
6	ETAPE 2 : 2 DOMAINES DANS UNE FORET	39
6.1	OBJECTIFS	39
6.1.1	Structure physique	39
6.1.2	Structure logique	41
6.2	ACTIVE DIRECTORY	44
6.2.1	Groupe d'utilisateurs (<i>Users group</i>)	44
6.2.2	Espace de noms (<i>Namespace</i>)	44
6.2.3	Noms (<i>Name</i>)	45
6.2.4	Nomination d'objets	45
6.2.5	Arbre (<i>Tree</i>)	46
6.2.6	Forêt (<i>Forest</i>)	47
6.2.7	Schéma	48
6.2.8	Catalogue global	49

6.3	SCENARIO 1 : DNS	50
6.4	SCENARIO 2 : REPLICATION	52
6.5	SCENARIO 3 : SITE	54
7	ETAPE 3 : 2 DOMAINES DANS 2 FORETS	56
7.1	OBJECTIFS	56
7.1.1	Structure physique	56
7.1.2	Structure logique	58
7.2	DNS	60
7.2.1	Nouveautés	60
7.2.2	<i>SRV record type</i>	60
7.2.3	<i>Dynamic DNS</i>	61
7.2.4	Zone de recherche	62
7.2.5	Vulnérabilité : Transferts de zone DNS	63
7.3	SCENARIO 1 : DNS	65
7.3.1	Principe	65
7.3.2	Ports utilisés	65
7.3.3	Configuration	65
7.4	SCENARIO 2 : TRUST	66
7.4.1	Principe	66
7.4.2	Ports utilisés	66
7.4.3	Configuration	66
7.5	SCENARIO 3 : REPERTOIRE CONFIDENTIEL	67
7.5.1	Principe	67
7.5.2	Ports utilisés	67
7.5.3	Configuration	67
8	ETAPE 4 : AUTHENTIFICATION SUR UN SERVEUR WEB	69
8.1	OBJECTIFS	69
8.1.1	Structure physique	69
8.1.2	Structure logique	69
8.2	SCENARIO 1 : SERVEUR WEB IIS 5.0	70
8.2.1	Principe	70
8.2.2	Authentification intégrée de Windows	70
8.2.3	Différentes variantes d'accès à un serveur WEB	71
8.2.4	Ports utilisés	72
8.2.5	Configuration	72
9	PROBLEMES GENERAUX RENCONTRES	74
9.1	PARTAGE DE FICHIERS ET D'IMPRIMANTES SOUS WINDOWS 2000 SERVER	74
9.2	LOCALISATION DU CONTROLEUR DE DOMAINE	74
9.3	FONCTION NAT ACTIVEE PAR DEFAUT SUR LE ROUTEUR LIGHTNING	74
9.4	IMPOSSIBLE D'ANALYSER LE TRAFIC DES ROUTEURS <i>LIGHTNING</i>	75
10	CONCLUSION	76

1 PRÉSENTATION DU MÉMOIRE DE DIPLÔME

De nos jours, beaucoup d'organisations et d'entreprises possèdent un système informatique composé de plusieurs ordinateurs. Ces systèmes informatiques sont connectés en réseau pour faciliter l'échange d'informations entre les différents utilisateurs.

La problématique de **l'échange d'informations** dans un réseau informatique reste la même quel que soit le système utilisé. Chaque utilisateur devra accéder à des ressources (fichiers, imprimantes, etc.) ou partager ses ressources pour travailler avec d'autres utilisateurs.

Dans ce travail de diplôme, l'étude se portera sur la problématique du partage de ressources, accessibles par certains utilisateurs **dans un réseau Windows 2000**.

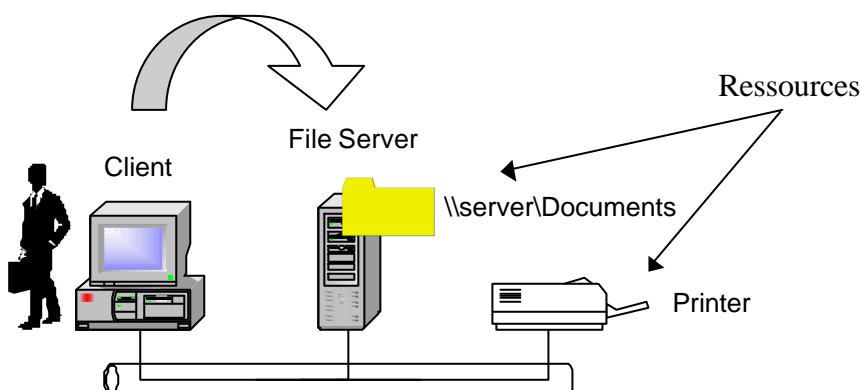
Lorsqu'on partage des ressources, la notion d'**autorisation** d'accès aux ressources intervient. Ces accès seront donc différents pour chaque utilisateur en fonction du travail qu'il doit effectuer.

Pour simplifier l'administration de ces autorisations, la notion de **groupes d'utilisateurs** permet de rassembler des utilisateurs qui possèdent les mêmes droits d'accès.

Par exemple, dans une école, les professeurs et les étudiants accèdent à un même répertoire partagé, appelé Documents, qui contient de la documentation.

Les professeurs ont les autorisations de **lecture et d'écriture** alors que les étudiants peuvent seulement **lire ces documents**. Pour illustrer cet exemple, la figure 1.1 représente un utilisateur qui veut accéder à un répertoire partagé.

FIGURE 1.1 : ACCÈS À UNE RESSOURCE PARTAGÉE



Le système d'exploitation imposé est **Windows 2000**. Il possède une gestion des ressources d'un réseau informatique, grâce à un annuaire centralisé appelé **Active Directory**. Ce travail de diplôme portera son étude principalement sur Active Directory et sur l'architecture réseau de Windows 2000.

2 AUTORISATIONS NTFS

2.1 INTRODUCTION

NTFS (*NT File System*) est le système de fichiers utilisé par Windows NT et 2000.

La différence principale entre ce système de fichiers et le système de fichiers de Windows 95/98 (FAT – *File Allocation Table*) est la gestion des autorisations.

Les **autorisations** (*permissions*) donnent aux utilisateurs la possibilité d'accéder à une ressource. Elles définissent le type d'accès aux ressources et les actions autorisées sur celles-ci.

Les **droits**, aussi appelés **privilèges**, permettent aux utilisateurs d'exécuter des tâches systèmes telles que l'ouverture d'une session locale, une sauvegarde, etc.

Les autorisations NTFS s'appliquent en toutes circonstances, dès qu'un utilisateur accède à un **fichier** ou à un **dossier** à partir d'un **poste de travail** ou du **réseau**.

Les autorisations attribuées au **niveau dossier** sont différentes de celles attribuées au **niveau fichier**.

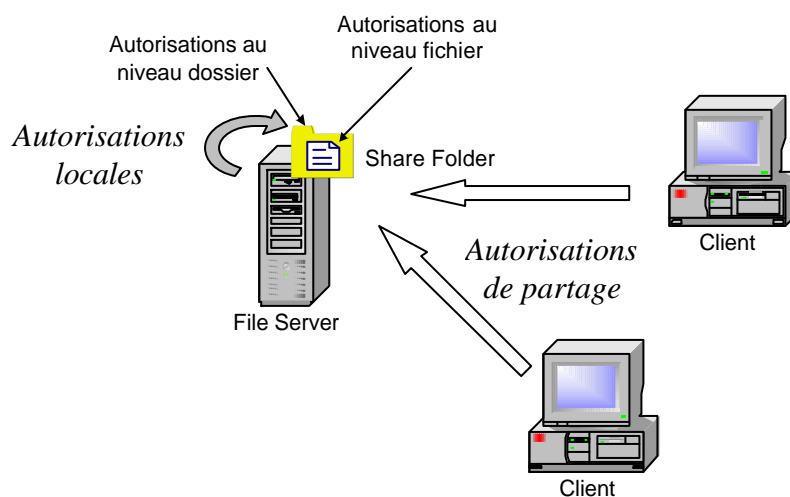
Dans un réseau, l'accès à un répertoire partagé peut s'effectuer soit depuis l'ordinateur où se trouve la ressource partagée, soit depuis le réseau. Ces accès sont appelés respectivement **autorisations locales** et **autorisations de partage**.

Pour résumer, il existe deux niveaux :

- **Les autorisations locales** : elles sont attribuées sur un poste de travail soit au niveau d'un dossier, soit au niveau d'un fichier.
- **Les autorisations de partage** : contrairement aux autorisations locales, elles sont attribuées depuis le réseau sur un répertoire partagé. En effet, il n'est pas possible de partager seulement un fichier.

La figure 2.1 illustre à quel niveau se trouvent ces autorisations. Lorsque les clients désirent accéder au répertoire partagé, ils doivent aussi bien satisfaire les autorisations de partage que les autorisations locales. Depuis le serveur de fichiers, seules les autorisations locales sont testées au niveau dossier et fichier.

FIGURE 2.1 : AUTORISATIONS NTFS



2.2 AUTORISATIONS LOCALES

2.2.1 Autorisations au niveau dossier

Il existe six types d'autorisations au niveau dossier ; elles permettent à l'utilisateur de :

- *Write* : créer de nouveaux fichiers et sous-dossiers dans le dossier, modifier les attributs du dossier (lecture seule, fichier caché, fichier système ou archive) et d'afficher le propriétaire et les autorisations du dossier.
- *Read* : consulter les fichiers et les sous-dossiers du dossier, et afficher le propriétaire, les autorisations et les attributs du dossier.
- *List Folder-Contents* : consulter le nom des fichiers et sous-dossiers du dossier.
- *Read & Execute* : se déplacer d'un dossier à l'autre pour accéder à d'autres fichiers et dossiers, et effectuer les opérations permises par les autorisations *Read* et *List Folder-Contents*.
- *Modify* : supprimer le dossier et d'effectuer les opérations permises par les autorisations *Write* et *Read & Execute*.
- *Full Control* : modifier les autorisations, s'approprier et supprimer des sous-dossiers et des fichiers, mais aussi effectuer les opérations permises par toutes les autres autorisations ci-dessus.

2.2.2 Autorisations au niveau fichier

Les autorisations locales au niveau fichier ne sont pas les mêmes que les autorisations au niveau dossier. Il en existe cinq types :

- *Write* : écraser le fichier, modifier ses attributs et afficher son propriétaire et ses autorisations.
- *Read* : lire le fichier et afficher les attributs, les propriétaires et les autorisations du fichier.
- *Read & Execute* : exécuter des applications et effectuer les opérations permises par l'autorisation *Read*.
- *Modify* : supprimer le fichier et effectuer les opérations permises par les autorisations *Write* et *Read & Execute*.
- *Full Control* : modifier les autorisations et s'approprier le fichier, mais aussi effectuer les opérations permises par toutes les autres autorisations ci-dessus.

2.2.3 Autorisations multiples

Lorsque l'utilisateur possède plusieurs autorisations sur le même dossier ou fichier, il y a deux règles importantes :

- **Le refus (*deny*) l'emporte sur toutes les autres autorisations.**
- **Les autorisations NTFS sont cumulatives.**
Par exemple, un utilisateur qui possède les autorisations de lecture sur un répertoire et qui est membre d'un groupe qui bénéficie des autorisations d'écriture, l'utilisateur profitera à la fois des autorisations de lecture et d'écriture sur ce répertoire.

Une troisième est importante :

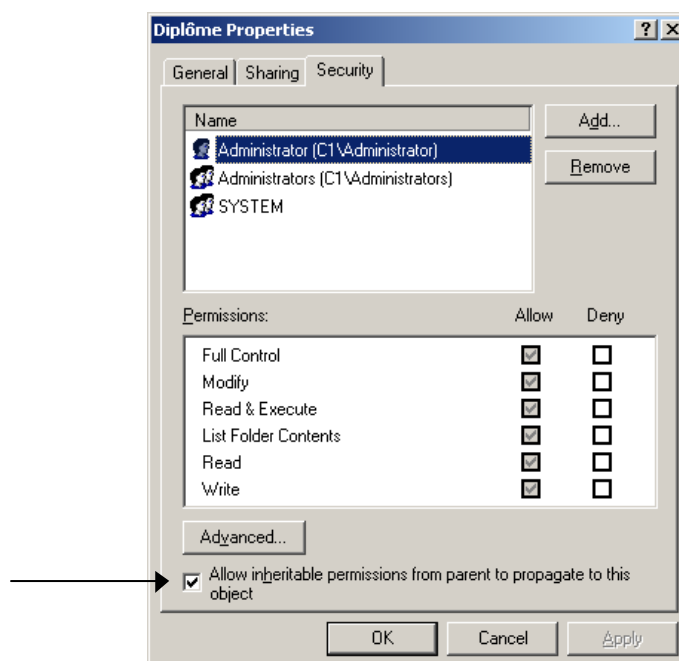
- **Les autorisations au niveau fichier sont prioritaires sur les autorisations au niveau dossier.**
Par exemple, un utilisateur qui possède les autorisations sur un fichier pourra y accéder à ce fichier même s'il n'a pas les autorisations sur le dossier dans lequel le fichier se trouve.

Remarque

Par défaut, **les autorisations mises sur un dossier parent sont transmises aux sous-dossiers et fichiers** qu'il contient.

La figure 2.2 illustre cette fonction activée par défaut (*Allow inheritable permissions from parent to propagate to this object*) sous Windows 2000.

FIGURE 2.2 : AUTORISATIONS RÉCURSIVES



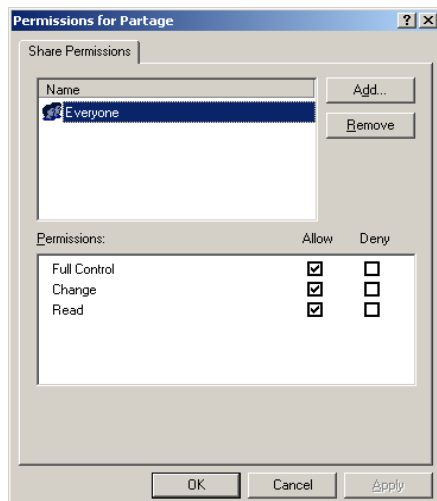
2.3 AUTORISATIONS DE PARTAGE

Les autorisations de partage s'effectuent au niveau du réseau. Il en existe trois types différents qui peuvent être utilisés sur une ressource partagée.

- *Read* : Les utilisateurs peuvent afficher le répertoire et les sous-répertoires et y accéder, lire les fichiers et exécuter les programmes.
- *Change* : Les mêmes autorisations que pour *Read*, mais, en plus, les utilisateurs peuvent créer des sous-répertoires et des fichiers, les modifier, et les supprimer
- *Full Control* : L'utilisateur a toutes les autorisations ci-dessous, mais en plus, il peut modifier les autorisations NTFS.

Les autorisations de partage sont illustrées par la figure 2.3.

FIGURE 2.3 : AUTORISATIONS DE PARTAGE



3 ACTIVE DIRECTORY

3.1 INTRODUCTION

Ce chapitre fournit une introduction à Active Directory.

Qu'est-ce qu'un service d'annuaire ?

Un annuaire est une source d'informations distribuée. Par exemple, un annuaire téléphonique contient des informations sur des abonnés au téléphone.

Dans un système informatique distribué ou un réseau informatique, l'annuaire contient des informations sur des ressources, comme des applications, des imprimantes, des bases de données, des ordinateurs, des comptes d'utilisateurs, etc.

Les utilisateurs veulent trouver et utiliser ces ressources, et les administrateurs veulent contrôler leur utilisation.

Quel est l'intérêt de disposer d'un service d'annuaire ?

Un service d'annuaire est l'un des éléments essentiels d'un système informatique. Il arrive souvent que les utilisateurs et les administrateurs ne connaissent pas le nom exact des ressources qui les intéressent. Avec un peu d'information sur cette ressource, ils peuvent interroger l'annuaire pour obtenir une liste des ressources correspondant à leur recherche.

Un service d'annuaire peut :

- Centraliser les ressources disponibles sur un réseau.
- Distribuer un annuaire à de nombreux ordinateurs au sein d'un réseau.
- Dupliquer un annuaire pour le rendre disponible à beaucoup d'utilisateurs et pallier une éventuelle défaillance.

Qu'est-ce que Active Directory ?

Active Directory est le service d'annuaire fourni par Microsoft. Il est intégré au système d'exploitation *Windows 2000 Server*. Grâce à lui, il est beaucoup plus facile de gérer et d'administrer un réseau informatique, car il peut contenir toutes les informations relatives aux ressources du réseau.

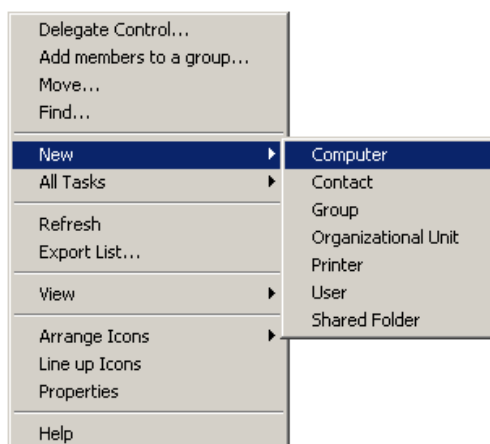
Par exemple, une petite entreprise de dix personnes n'aura peut-être pas besoin d'utiliser Active Directory. Par contre, lorsqu'on dépasse ce nombre de personnes, il devient très difficile de gérer les utilisateurs sur **chaque poste de travail**. Active Directory permet de **centraliser** la gestion des utilisateurs dans un réseau informatique.

3.2 COMPOSANTS

3.2.1 Objet et attribut (*Object and attribute*)

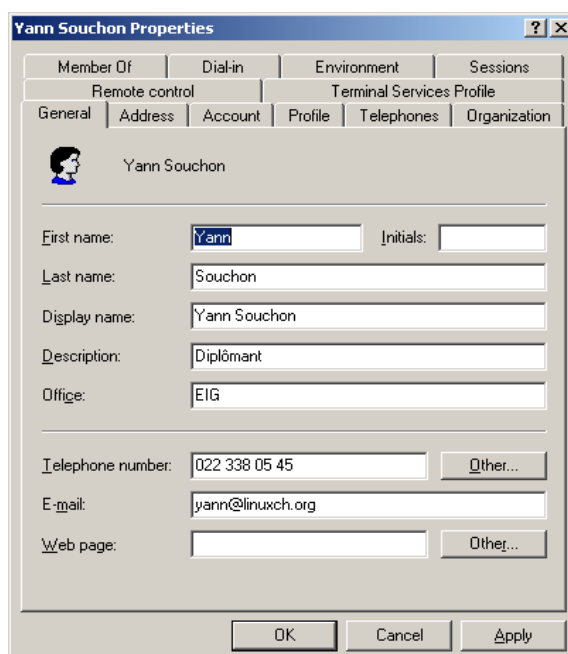
Dans la section précédente, les ressources correspondent aux éléments qui peuvent être stockés dans le service d'annuaire. Ces ressources constituent les **objets** d'Active Directory.

FIGURE 3.1 : OBJETS



Un objet est un ensemble d'attributs nommés et distincts qui représente une ressource réseau. Les **attributs** décrivent les caractéristiques des objets dans l'annuaire. Par exemple, les attributs d'un compte utilisateur peuvent être le prénom et le nom de l'utilisateur, ainsi que son adresse électronique.

FIGURE 3.2 : ATTRIBUTS DES OBJETS



Les objets peuvent être organisés en **classes**, autrement dit les regrouper en fonction d'une logique particulière. Les comptes d'utilisateurs, groupes et ordinateurs sont des exemples de classe.

3.2.2 Compte d'utilisateurs (*Users account*)

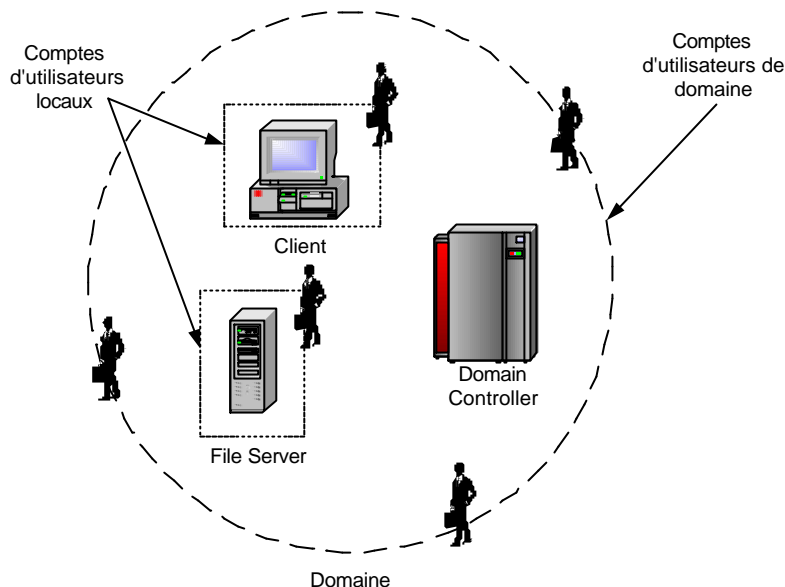
Un compte d'utilisateur donne à un utilisateur la possibilité de se connecter à un domaine afin d'accéder aux ressources réseau ou de se connecter à un ordinateur afin d'accéder aux ressources de cet ordinateur.

Il existe deux types de **comptes d'utilisateurs** :

- Comptes d'utilisateurs **locaux** : Ces comptes permettent uniquement aux utilisateurs de se connecter à l'ordinateur où un compte d'utilisateur local est présent et d'accéder à ses ressources.
Lorsqu'un compte d'utilisateur local est créé, Windows 2000 crée uniquement le compte dans la base de donnée locale de sécurité de cet ordinateur.
Windows 2000 ne transmet pas les comptes locaux sur le contrôleur de domaine.
Il n'est pas possible de créer des comptes d'utilisateurs locaux sur un contrôleur de domaine.
De plus, l'administrateur du domaine ne peut ni gérer les propriétés d'un compte d'utilisateur local, ni accorder d'autorisations d'accès aux ressources de ce domaine à moins qu'il ne se connecte à l'ordinateur local par le biais d'Active Directory de la manière suivante : *Active Directory Users and Computers*, puis en sélectionnant l'ordinateur concerné dans *Computers*. Ensuite, pour accéder à la gestion de l'ordinateur, il suffit de cliquer sur *Manage*.
- Comptes d'utilisateurs **de domaine** : Ces comptes d'utilisateurs de domaine permettent aux utilisateurs de se connecter au domaine et d'accéder aux ressources, quel que soit leur emplacement sur le réseau. Ils sont créés dans Active Directory sur le contrôleur de domaine, puis répliqués sur tous les contrôleurs du domaine.

La figure 3.3 illustre les différents types de comptes d'utilisateurs à l'intérieur d'un domaine.

FIGURE 3.3 : COMPTES D'UTILISATEURS



En plus de ces deux comptes d'utilisateurs, il existe un troisième type de compte appelé **compte intégré**. Ils sont créés automatiquement par Windows 2000. Les plus fréquents sont *Administrator* et *Guest*.

3.2.3 Groupe d'utilisateurs (*Users group*)

Un groupe est un ensemble de compte. Les groupes simplifient l'administration en permettant d'attribuer des **autorisations** et des **droits** à un groupe d'utilisateurs plutôt qu'à chaque compte d'utilisateur individuel.

Sur un ordinateur unique, les groupes d'utilisateurs sont appelés groupes **locaux**. Un groupe local sert à accorder des autorisations d'accès aux ressources de l'ordinateur sur lequel le groupe a été créé.

Dès que l'on possède un réseau d'ordinateur (domaine), il existe deux **types** de groupes :

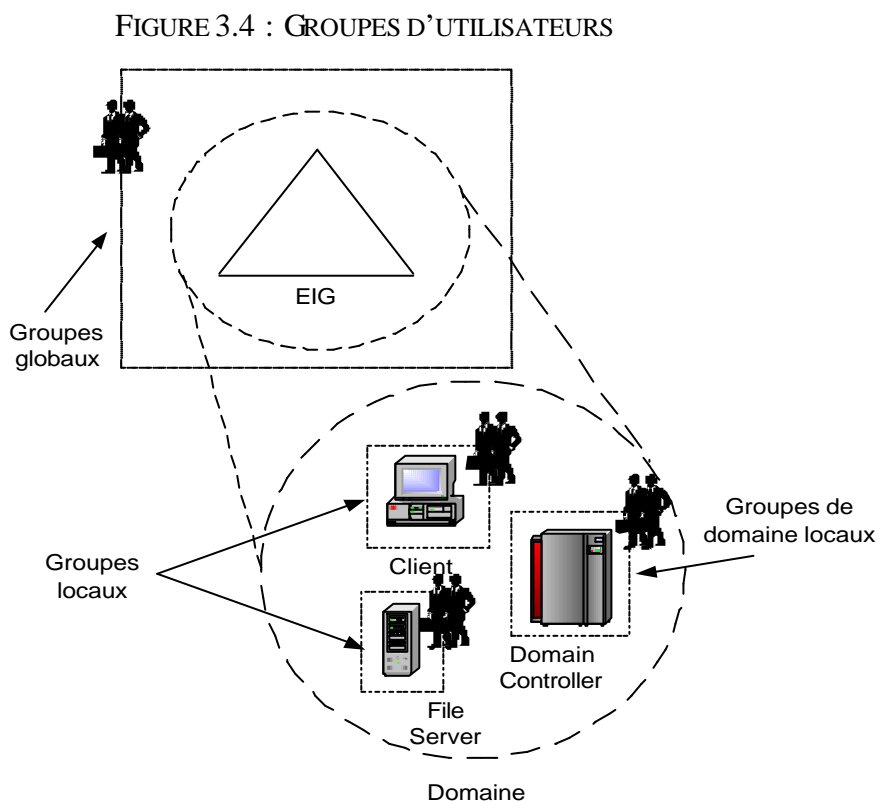
- Groupes de **sécurité** : Ces groupes permettent d'attribuer des autorisations d'accès aux ressources. Ils possèdent toutes les caractéristiques des groupes de distribution.
- Groupes de **distribution** : Ce type de groupe n'est pas utilisé dans ce travail de diplôme.

Après avoir défini le type du groupe, il faut spécifier l'étendue du groupe. Les étendues des groupes permettent d'utiliser les groupes de différentes façons pour attribuer des autorisations. L'étendue détermine à quel endroit du réseau on utilise le groupe pour lui attribuer des autorisations.

Deux **étendues des groupes** sont disponibles et sont résumés sous forme de tableau :

	Groupes de domaines locaux	Groupes globaux
Appartenance	Les membres sont issus de n'importe quel domaine	Les membres sont issus du domaine local
Accès aux Ressources	Les membres accèdent aux ressources du domaine local	Les membres accèdent aux ressources de n'importe quel domaine

La figure 3.4 illustre l'Ecole d'Ingénieurs de Genève sous forme de domaine (→ § 3.3.1). L'accès aux ressources est représentée par les trois étendues des groupes. De nouveau, il n'est pas possible de créer des groupes locaux sur un contrôleur de domaine.



3.3 STRUCTURE LOGIQUE

La **structure logique** d'Active Directory est représentée par les composants suivants : domaines et unités d'organisation.

3.3.1 Domaine (*Domain*)

Un **domaine** est défini par une limite de sécurité unique dans le cadre d'un réseau informatique tournant sous Windows 2000.

Active Directory est constitué d'un ou plusieurs domaines. Un domaine peut recouvrir plusieurs sites physiques. Chaque domaine a sa propre politique de sécurité et ses propres relations de sécurité avec les autres domaines.

3.3.2 Unité d'organisation (*Organizational Unit*)

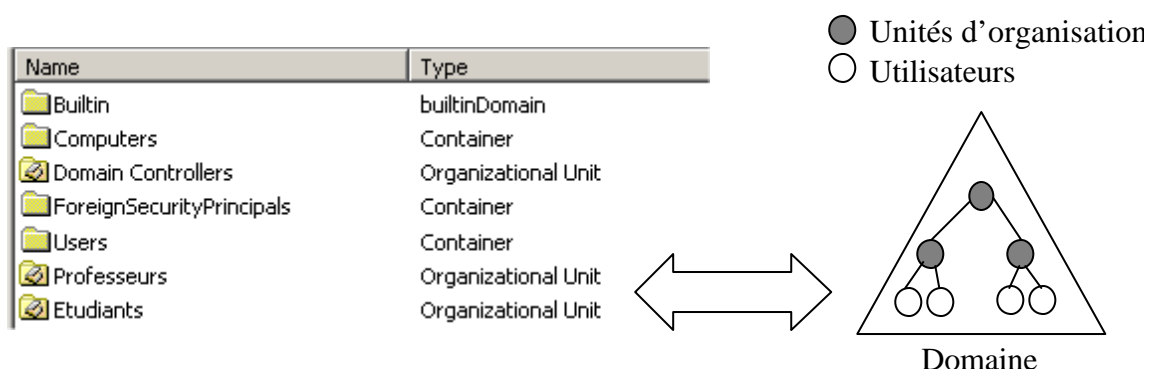
Une **unité d'organisation** est un conteneur qui sert à organiser les objets d'un domaine en groupes administratifs logiques qui reflètent la structure fonctionnelle. Une unité organisationnelle peut contenir des comptes d'utilisateurs, des groupes, des ordinateurs, des applications et des partages de fichiers, ainsi que d'autres unités d'organisation du même domaine.

Il est aussi possible de déléguer l'administration des utilisateurs et des ressources.

La figure 3.5 représente des unités d'organisation sous deux formes :

- La première est une capture d'écran d'Active Directory avec les cinq objets par défaut (*Buitin*, *Computers*, *Domain Controllers*, *ForeignSecurityPrincipals* et *Users*). Deux unités d'organisation sont ajoutées qui sont **Professeurs** et **Etudiants**.
- La seconde est un schéma de la première figure. L'avantage de cette figure est l'illustration de la hiérarchie des unités d'organisation. Par contre, les objets par défaut ne sont pas dessinés pour plus de clarté.

FIGURE 3.5 : UNITES D'ORGANISATION



3.4 STRUCTURE PHYSIQUE

3.4.1 Contrôleur de domaine (*Domain Controller*)

Un contrôleur de domaine est un ordinateur sur lequel est installé Windows 2000 Server et **Active Directory**.

Chaque contrôleur de domaine stocke soit une partie, soit toutes les informations d'Active Directory relatives à ce domaine, gère les modifications apportées à ces informations et les réplique vers les autres contrôleurs du même domaine.

Il s'occupe aussi **des ouvertures de session**, de **l'authentification** et de la recherche dans l'annuaire.

Il faut au minimum un contrôleur de domaine par domaine.

4 KERBEROS

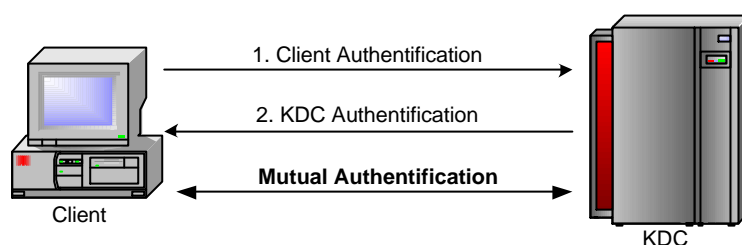
4.1 INTRODUCTION

Cette section introduit un petit rappel concernant Kerberos.

Kerberos est le protocole d'authentification utilisé par Windows 2000. Il permet d'authentifier différentes **entités**. Entité signifie que Kerberos est capable non seulement d'authentifier un simple utilisateur, mais surtout des clients, serveurs, etc. Ces entités sont appelées **clients Kerberos**. La figure 4.1 illustre ce protocole :

1. L'authentification d'un client (une entité) auprès du serveur Kerberos.
2. L'authentification du serveur Kerberos (une autre entité) auprès d'un client.

FIGURE 4.1 : AUTHENTIFICATION MUTUELLE AVEC KERBEROS



Lorsque les deux entités se sont authentifiées, on parle **d'authentification mutuelle**.

Kerberos repose sur l'utilisation de clé symétrique appelée **Long-Term Symmetric Key** ainsi que sur des clés de session (**session key**) qui permettent au client et au serveur Kerberos de dialoguer avec des messages chiffrés. Pour chiffrer ces messages à l'aide de clés symétriques, Kerberos utilise un chiffrement dérivé du **DES (Data Encryption Standard)** appelé **RC4-HMAC** sur 128 bits.

Active Directory intègre un serveur Kerberos, aussi appelé KDC qui possède la correspondance Client – Clé symétrique. Cette **clé symétrique**, qui est **le secret partagé**, est connue seulement du client et KDC.

Quelques termes importants pour la compréhension de ce protocole :

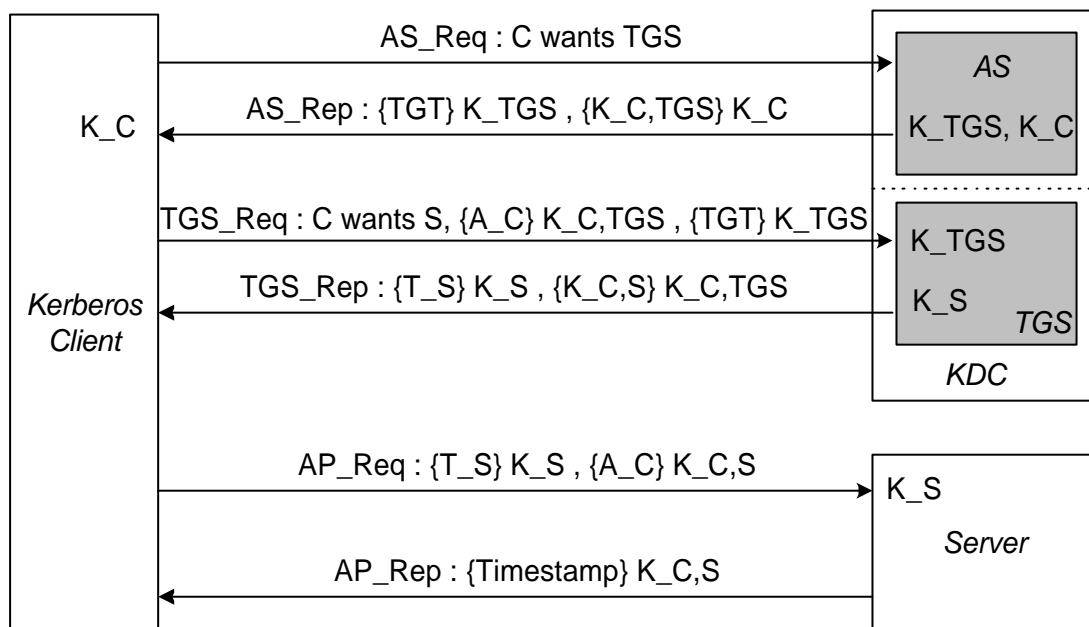
- **Key Distribution Center (KDC)** : le centre de distribution de clé est un service réseau qui accepte les requêtes de tickets émanant des clients Kerberos. Il comprend le service d'authentification (AS) ainsi que le service de délivrance des tickets (TGS).
- **Authentication Service (AS)** : le service d'authentification s'occupe d'authentifier les clients Kerberos et octroie un ticket (TGT) pour le TGS.
- **Ticket Granting Service (TGS)** : le service de délivrance des tickets, aussi appelé service de tickets, vérifie le TGT de l'utilisateur et accorde un ticket pour le service désiré.
- **Ticket Granting Ticket (TGT)** : le "ticket accordant le ticket" est le ticket qui est donné par l'AS pour le TGS.

Lorsqu'on installe un contrôleur de domaine (→ Annexe 1), deux services sont exécutés au démarrage. Ces services sont nécessaires au bon fonctionnement de Kerberos.

- *Centre de distribution des clés (KDC)* : ce service s'occupe de l'authentification des clients dans le domaine Windows 2000 grâce au protocole Kerberos. Il est divisé en deux sous-services : le service d'authentification (AS) et le service de délivrance des tickets (TGS).
- *Active Directory (AD)* : cet annuaire central gère les différents comptes utilisateurs, les ressources du domaine, etc., grâce au protocole LDAP.

La figure 4.2 illustre l'échange de paquets avec le protocole Kerberos entre un client et un serveur (de fichiers par exemple).

FIGURE 4.2 : ARCHITECTURE DÉTAILLÉE DE KERBEROS



Légende

{X}K_Y signifie que X est crypté avec la clé privée de Y
 {Z}K_V,W signifie que Z est crypté avec la clé de session entre V et W.

Voici un tableau qui résume les différentes abréviations utilisées (figure 4.2) :

- C : Kerberos Client
- K_TGS : TGS private key
- A_C : Client Authenticator
- K_S : Server private key
- ADR : Client Address
- S : Server
- K_C,TGS : TGS session key
- T_S : Ticket for Server
- K_C,S : Server session key
- Life : Ticket life length

Pour aider à la compréhension, les différentes clés que possède chaque entité dans leur **cache** sont indiquées à l'intérieur de l'illustration.

Ticket

Chaque ticket a la forme suivante : {S, C, ADR, Timestamp, Life, K_C,S} K_S
Il permet de donner au serveur S l'identité du client C ainsi que l'adresse de ce client ADR. Les tickets peuvent être utilisés plusieurs fois et ont une date limite de validité donnée par le *timestamp*.

Authentifieur

L'authentifieur a la forme suivante : {C, ADR, Timestamp} K_C,S.
Contrairement au ticket, il ne peut être utilisé **qu'une seule fois**. Il doit être généré à chaque fois que l'utilisateur souhaite utiliser un service (ressource). C'est l'utilisateur lui-même qui le génère.
L'authentifieur permet d'éviter les attaques de type *Replay* (un pirate ayant capturé le ticket et l'authentifieur renvoie ceux-ci pour accéder au service), il convient que le KDC garde une trace des authentifieurs déjà utilisés.

Remarques

- L'utilisation des *timestamps* suppose que les horloges du serveur et du client soient synchronisées.
- Il est possible de prouver l'identité du serveur au client, pour cela il suffit de renvoyer le *timestamp* du client incrémenté de un, le tout codé avec la clé de session. Un serveur pirate n'aurait pas pu décoder le ticket et donc se procurer le *timestamp* de l'authentifieur. On parle alors d'authentification mutuelle.

Utilitaires

Pour aider à mieux comprendre quels tickets sont stockés dans la cache de l'ordinateur, un utilitaire permet **d'afficher ce cache lorsque l'utilisateur s'est authentifié** dans le domaine Windows 2000. Il existe deux versions de cet utilitaire : **klist.exe** en mode texte et **kerbtray.exe** en mode graphique.

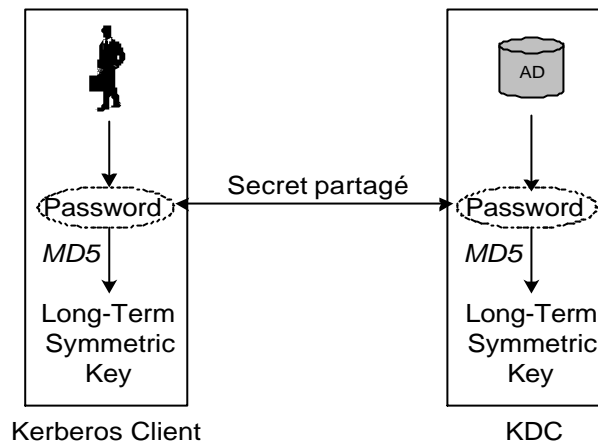
Source : Rapport du projet de semestre – **Kerberos**

- Chapitre 2.2

4.2 GESTION DES CLÉS

Dans le cas d'un **utilisateur**, le secret partagé est généré à partir d'une fonction de hachage (**MD5**) sur son mot de passe. Le KDC connaissant aussi le mot de passe de l'utilisateur, il peut, lui aussi, générer la même clé symétrique (figure 4.3). Cette manière facilite la gestion de son secret, car l'utilisateur peut changer d'ordinateur sans problème.

FIGURE 4.3 : SECRET PARTAGÉ ENTRE L'UTILISATEUR ET LE KDC



Dans le cas d'un **serveur** (par exemple un serveur de fichiers), il n'y a pas un mot de passe qui permette de générer la clé.

Dans la documentation officielle de Kerberos (RFC 1510), aucune information indique comment doit être générée cette clé.

Les extraits suivants sont tirés de la RFC :

- "The authentication servers maintain a database of principals (i.e., users and servers) and their secret keys." – § 1., page 5
- "Secret key: An encryption key shared by a principal and the KDC, distributed outside the bounds of the system, with a long lifetime. In the case of a human user's principal, the secret key is derived from a password." – § 1.3., page 10
- "The authentication server looks up the client and server principals named in the *KRB_AS_REQ* in its database, extracting their respective keys." – § 3.1.3., page 17
- "If keys are derived from user-typed passwords, those passwords need to be well chosen to make brute force attacks more difficult." – § 6., page 68

Dans notre cas, le "principal" correspond au serveur de fichiers. On peut remarquer que la RFC reste floue sur la façon dont cette clé symétrique est générée.

Concernant la gestion du secret, le problème n'est pas le même qu'avec un utilisateur. Il suffit que cette clé soit générée une fois et qu'elle reste secrète. La sécurité nécessaire pour atteindre cet objectif n'est pas défini dans la RFC :

- *"Principals must keep their secret keys secret. If an intruder somehow steals a principal's key, it will be able to masquerade as that principal or impersonate any server to the legitimate principal."* – § 1.2., page 8

D'après ces différents extraits, on peut penser que chaque implémentation de Kerberos peut définir **sa propre méthode pour partager le secret (la clé)**.

L'implémentation de Microsoft est de générer le secret sur le KDC, puis de le transmettre au serveur de fichiers. Ceci est réalisé lorsqu'on **ajoute le serveur dans le domaine** (*join a domain*, → Kerberos § 3.6.1).

Sources : RFC 1510 – **The Kerberos Network Authentication Service (V5)**
<http://sunsite.cnlab-switch.ch/ftp/doc/standard/rfc/15xx/1510>

Windows 2000 Magazine – **Kerberos Is on Guard in Windows NT 5**
InstantDoc ID : 138

5 ETAPE 1 : 1 DOMAINE

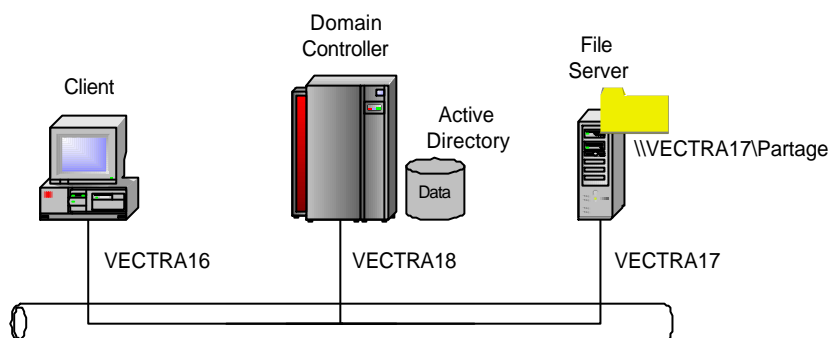
5.1 OBJECTIFS

L'objectif de ce scénario est d'étudier l'accès à une ressource dans un domaine Windows 2000 (*EIG-SOUCHON*).

- Un domaine avec un contrôleur de domaine (*VECTRA18*)
- Un serveur de fichiers avec un répertoire partagé (*VECTRA17*)
- Un client (*VECTRA16*)
- Un serveur DNS dynamique
- Quatre utilisateurs et deux groupes
- Trois adresses IP publiques

5.1.1 Structure physique

Disposant de trois ordinateurs, le réseau est mis en œuvre de la façon suivante :



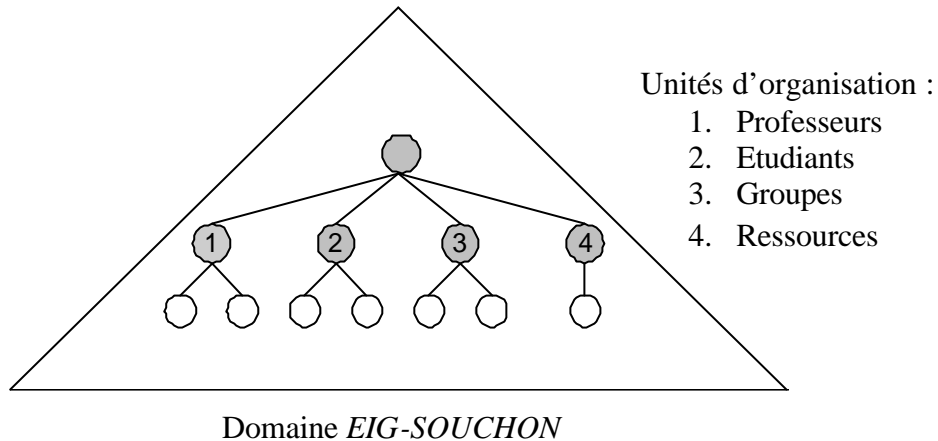
Ce tableau résume la configuration réseau des trois ordinateurs constituant le domaine.

<i>EIG-SOUCHON</i>	Client VECTRA16	Domain Controller VECTRA18	File Server VECTRA17
IP Address	129.194.187.57	129.194.187.59	129.194.187.58
Subnet Mask	255.255.252.0	255.255.252.0	255.255.252.0
Gateway	129.194.184.3	129.194.184.3	129.194.184.3
DNS Server	129.194.187.59	129.194.187.59	129.194.187.59
Operating System	Windows 2000 Professional	Windows 2000 Server	Windows 2000 Professional

5.1.2 Structure logique

La figure 5.1 illustre la configuration d'Active Directory. En plus des unités d'organisation créées par défaut, quatre unités d'organisation sont ajoutées (→ § 3.3.2). Ces unités d'organisation servent respectivement pour les utilisateurs (professeurs et étudiants), les groupes et les ressources.

FIGURE 5.1 : HIÉRARCHIE ACTIVE DIRECTORY



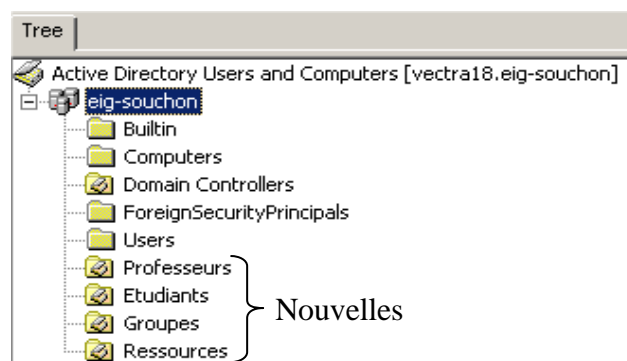
Après avoir créé ces quatre utilisateurs (→ § 3.2.2) et ces deux groupes (→ § 3.2.3), une ressource (répertoire) est partagée sur *VECTRA17*. Cela permet d'étudier les autorisations sur ce répertoire soit depuis un ordinateur client (*VECTRA16*), soit directement depuis le serveur de fichiers (*VECTRA17*).

VECTRA18 : Contrôleur de domaine

La configuration du contrôleur de domaine dans l'**annexe 2**.

- Créez quatre unités d'organisations nommées **Professeurs**, **Etudiants**, **Groupes** et **Ressources** (figure 5.2).

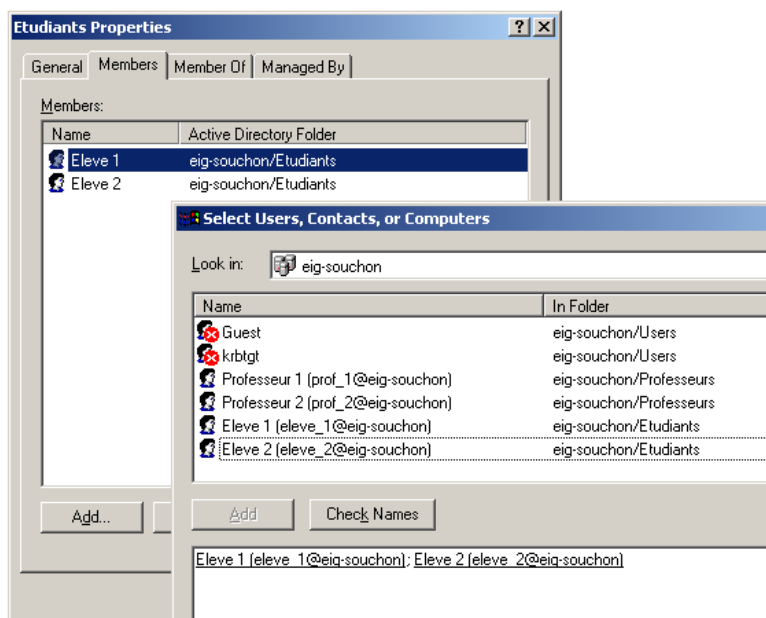
FIGURE 5.2 : QUATRE UNITES D'ORGANISATION SUPPLÉMENTAIRES



- Créez quatre utilisateurs nommés **eleve_1**, **eleve_2** dans **Etudiants** et **prof_1**, **prof_2** dans **Professeurs**.

- Créez deux groupes nommés **Etudiants** et **Professeurs** dans **Groupes**. Le type de groupe choisi est *Security* et l'étendue est *Domain Local*, car dans ce scénario, un seul domaine est utilisé.
- Ajoutez les quatre utilisateurs dans les deux groupes (figure 5.3).

FIGURE 5.3 : SÉLECTION DES UTILISATEURS DANS UN GROUPE



- Publier un répertoire partagé nommé **Repertoire Partage** dans **Ressources**. Le répertoire partagé se trouve sur *VECTRA17* (\\VECTRA17\Partage).

VECTRA17 : Serveur de fichiers

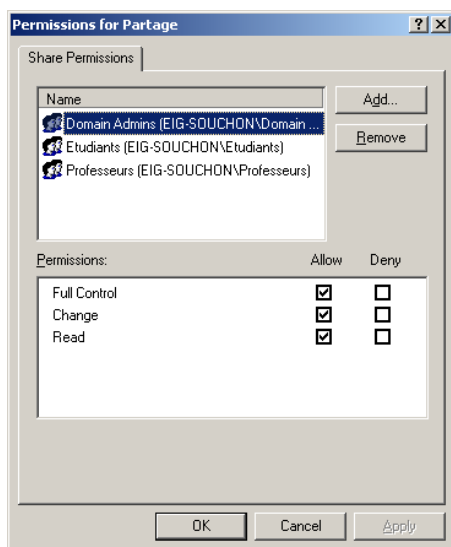
Pour partager un répertoire, il faut exécuter les opérations décrites dans l'**annexe 3**.

- Le nom du répertoire (*Share Name*) est **Repertoire Partage**.
- Les autorisations de partage sont résumées dans le tableau ci-dessous (→ § 2.3) :

	Groupe Etudiants	Groupe Professeurs	Groupe Domain Admins
<i>Read</i>	X	X	X
<i>Change</i>		X	X
<i>Full Control</i>			X

La figure 5.4 illustre les autorisations de partage après avoir configuré les groupes ci-dessus.

FIGURE 5.4 : AUTORISATIONS DE PARTAGE

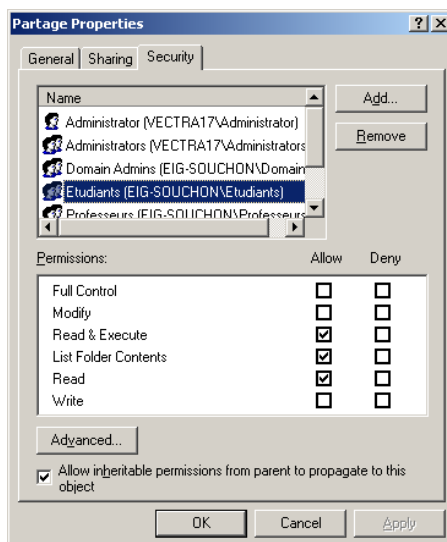


- Les autorisations locales sont décrites dans le tableau ci-dessous. On remarque qu'on peut être plus "précis" avec ces autorisations (→ § 2.2).

	Groupe Etudiants	Groupe Professeurs	Groupe Domain Admins
<i>List Folder Contents</i>	X	X	X
<i>Read</i>	X	X	X
<i>Read & Execute</i>	X	X	X
<i>Write</i>		X	X
<i>Modify</i>		X	X
<i>Full Control</i>			X

La figure 5.5 illustre ces autorisations locales.

FIGURE 5.5 : AUTORISATIONS LOCALES



En plus des trois groupes rajoutés, un utilisateur *Administrator* local et un groupe *Administrators* local sont présents par défaut .

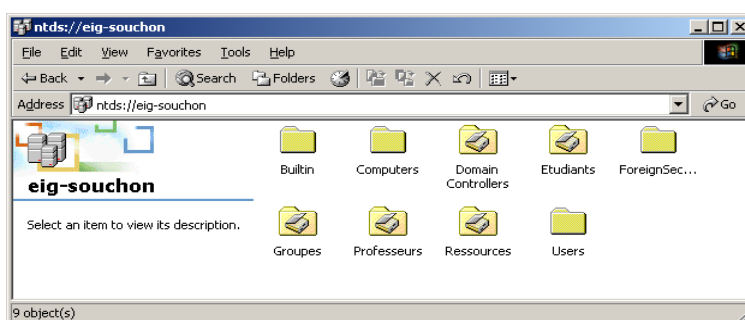
VECTRA16 : Client

Les tests sont effectués en s'authentifiant avec les différents utilisateurs des groupes créés sur le domaine *EIG-SOUCHON*.

L'accès à la ressource s'effectue par l'intermédiaire de *My Network Places – Entire Network – Directory – EIG-SOUCHON*. Cette méthode permet d'avoir accès à l'ensemble des éléments d'Active Directory.

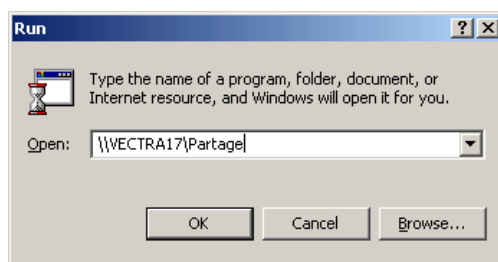
Seuls les comptes d'utilisateurs de domaine peuvent accéder à la ressource grâce à *Directory*. Les autres comptes, par exemple locaux, ne disposent pas de *Directory*. L'avantage de *Directory* est de pouvoir accéder à une ressource partagée sans devoir connaître le serveur qui l'héberge. Par contre, les ressources doivent être publiées dans Active Directory (→ Annexe 2).

FIGURE 5.6 : DIRECTORY



L'autre méthode est de taper directement l'adresse du serveur de fichiers à partir de *Start – Run... : \\VECTRA17\Partage*.

FIGURE 5.7 : RUN



Remarque

Chaque ordinateur du domaine fonctionne sans **NetBIOS**. Ce protocole propriétaire de Microsoft fonctionne sur le principe des *broadcasts*. L'annexe 6 décrit comment désactiver ce protocole (→ Kerberos Annexe 1, § 6.4).

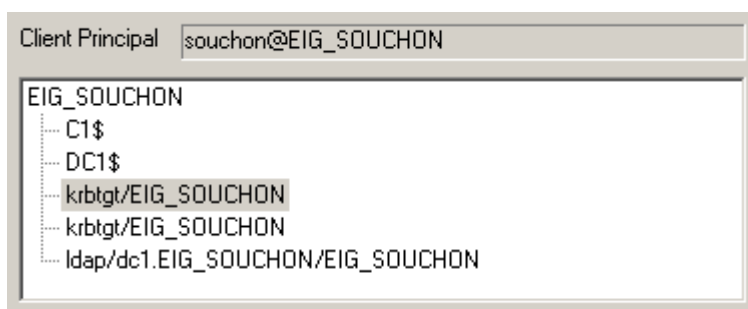
5.2 SCÉNARIO 1 : DÉMARRAGE D'UN ORDINATEUR DANS UN DOMAINE

Lorsqu'un ordinateur membre d'un domaine Windows 2000 démarre, il exécute une suite d'étapes nécessaires pour que tout fonctionne correctement. Il en existe huit différents. Ces étapes sont exécutées les unes à la suite des autres. Cette section en introduit cinq sur les huit. Par contre, le processus relatif à l'authentification est expliqué en détail.

1. **Connexion au réseau** : L'ordinateur commence par charger les protocoles TCP/IP. TCP/IP peut être configuré statiquement, c'est-à-dire que les paramètres sont rentrés manuellement sur l'ordinateur. La configuration statique est plutôt réservée pour des serveurs ou des routeurs. L'autre manière est de configurer TCP/IP dynamiquement. Pour cela, un serveur DHCP doit être présent sur le réseau pour attribuer ces paramètres.
2. **Localisation du contrôleur de domaine** : Lorsque l'ordinateur peut accéder au réseau, il doit localiser le contrôleur de domaine. Le client interroge le serveur DNS pour les enregistrements de ressources SRV (→ § 5.1.1). Ces enregistrements contiennent beaucoup d'informations concernant les contrôleurs de domaines (Création d'un canal sécurisé basé sur le protocole propriétaire SMB).
3. **Authentification Kerberos et création de la session** : Après avoir établi un canal sécurisé, le client doit s'authentifier à l'aide du protocole Kerberos. Pour commencer, il va demander un TGT au service d'authentification (AS). Ce TGT porte le nom *krbtgt/NOM_DU_DOMAINE*. Ensuite, il effectue trois demandes de tickets :
 - Un ticket pour **l'ordinateur lui-même** portant le nom de l'ordinateur plus un "\$" (par exemple C1\$).
 - Un deuxième ticket pour le **contrôleur de domaine** ayant le même type de nom que le ticket précédent.
 - Le troisième ticket est utilisé pour accéder à **Active Directory** grâce au protocole LDAP (*ldap/NOM_DU_DOMAINE*).

On parle **d'authentification mutuelle** lorsque l'utilisateur possède les tickets C1\$ et DC1\$. Ces tickets sont visibles dès l'ouverture d'une session sur un domaine et permettent soit d'authentifier les ordinateurs, soit d'accéder aux différents services. La figure 5.8 illustre ces tickets sur un client membre du domaine *EIG_SOUCHON*.

FIGURE 5.8 : TICKETS PRÉSENTS SUR UN CLIENT (C1)



Sur la figure 5.8, on remarque que le cache de l'utilisateur possède cinq tickets. Le ticket *krbtgt/EIG_SOUCHON* est présent **deux fois**, mais avec des *flags* différents.

4. **Synchronisation de l'horloge** : Pour que le protocole Kerberos fonctionne correctement, il faut que les ordinateurs membres du domaine possèdent une horloge synchronisée sur celle du contrôleur de domaine. En effet, Kerberos utilise la notion de *Timestamps*, qui est basée sur le temps. Le protocole NTP est utilisé.
5. **Mise à jour du DNS dynamiquement** : Le dernier processus lors du démarrage d'un ordinateur, est de mettre à jour le nom de la machine dans le serveur DNS. Cela simplifie grandement l'administration du serveur DNS (→ § 7.2.3).

Pour plus d'informations sur les processus lors du démarrage d'un ordinateur membre d'un domaine Windows 2000, Microsoft a publié une très bonne documentation appelée *Windows 2000 Startup and Logon Traffic Analysis*.

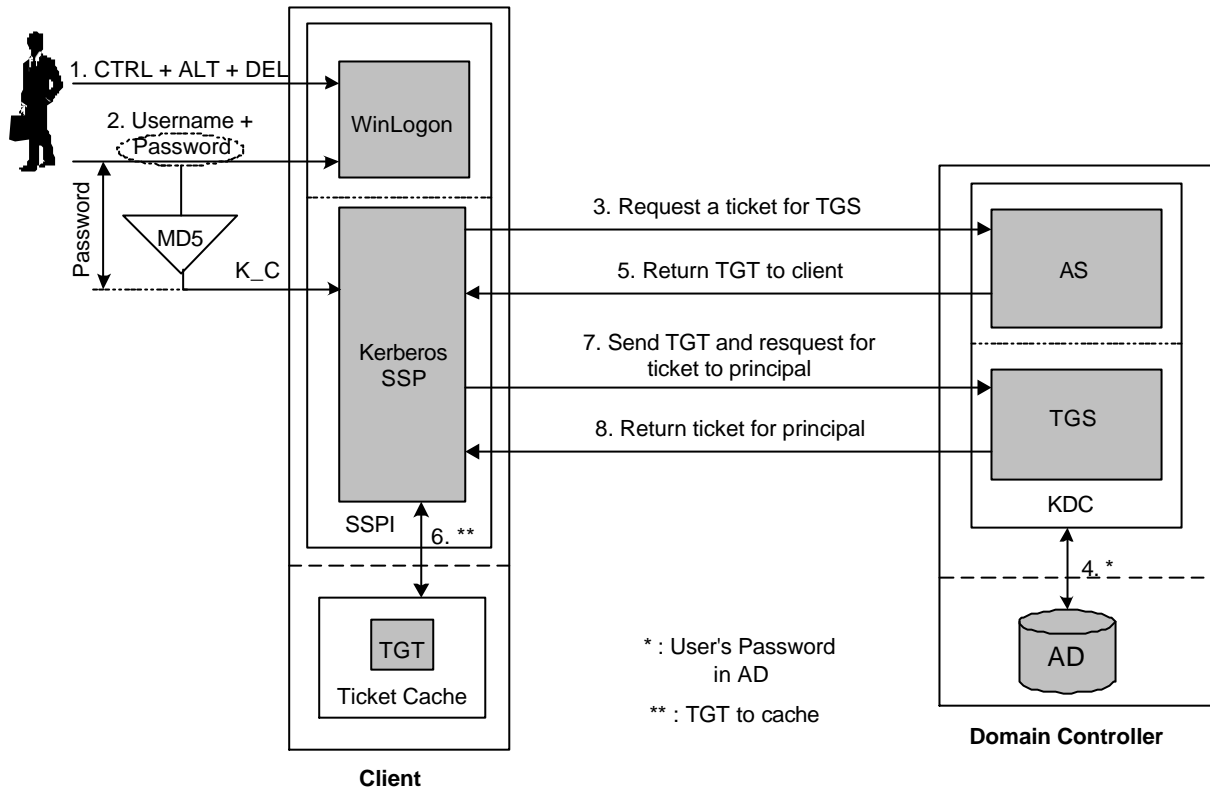
Annexe 9 : Une analyse de protocole correspondante à ce scénario est disponible en annexe. Elle est faite avec **Ethereal**.

Source : Microsoft TechNet – **Windows 2000 Startup and Logon Traffic Analysis**

5.3 SCÉNARIO 2 : AUTHENTIFICATION DANS UN DOMAINE

Cette section explique en détail les différentes étapes lorsque l'utilisateur désire ouvrir une session de travail dans le domaine.

FIGURE 5.9 : AUTHENTIFICATION DANS UN DOMAINE



1. L'utilisateur tape CTRL + ALT + DEL et la fenêtre de *WinLogon* apparaît. Chaque client Windows 2000 implémente une interface qui fournit des services de sécurité (SSPI - *Security Service Provider Interface*). *WinLogon* fait partie de ces services de sécurité ainsi que *Kerberos SSP*.
2. L'utilisateur rentre son nom d'utilisateur (*Username*) ainsi que son mot de passe (*Password*). Le client va lui aussi générer la clé *K_C* grâce au mot de passe.
3. *Kerberos SSP* fait une demande au service d'authentification (AS) pour obtenir un TGT.
4. De son côté, le KDC recherche le mot de passe de l'utilisateur concerné dans Active Directory. Grâce à ce mot de passe et à la fonction de hachage (MD5), il obtient la clé symétrique *K_C*.
5. Le service d'authentification envoie un TGT et une clé de session chiffrée avec la clé *K_C*. Grâce au TGT, l'utilisateur ne doit plus rentrer son mot de passe, car le TGT est **réutilisé** pour les autres authentifications. Tout devient **transparent** pour l'utilisateur.

6. Si le TGT est valable, le client va le mettre dans un cache qui stocke les tickets de l'utilisateur.
7. Pour finir, *Kerberos SSP* effectue plusieurs demandes pour des services différents (voir cette section précédente).
8. Pour chaque demande, le TGS envoie un ticket qui permet d'accéder au service correspondant.

Les étapes 7 et 8 sont effectués plusieurs fois, car le client doit posséder différents tickets.

Annexe 10 : Une analyse de protocole correspondante à ce scénario est disponible en annexe. Elle est faite avec **Ethereal**.

Sources : Windows 2000 Magazine – **How Kerberos Fits into the Windows NT 5.0 Security Model**
InstantDoc ID : 101

Microsoft TechNet – **Windows 2000 Startup and Logon Traffic Analysis**

Microsoft MSDN – **Secure Networking Using Microsoft Windows 2000 Distributed Security Services**
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2k/html/msdn_distsecserv.asp

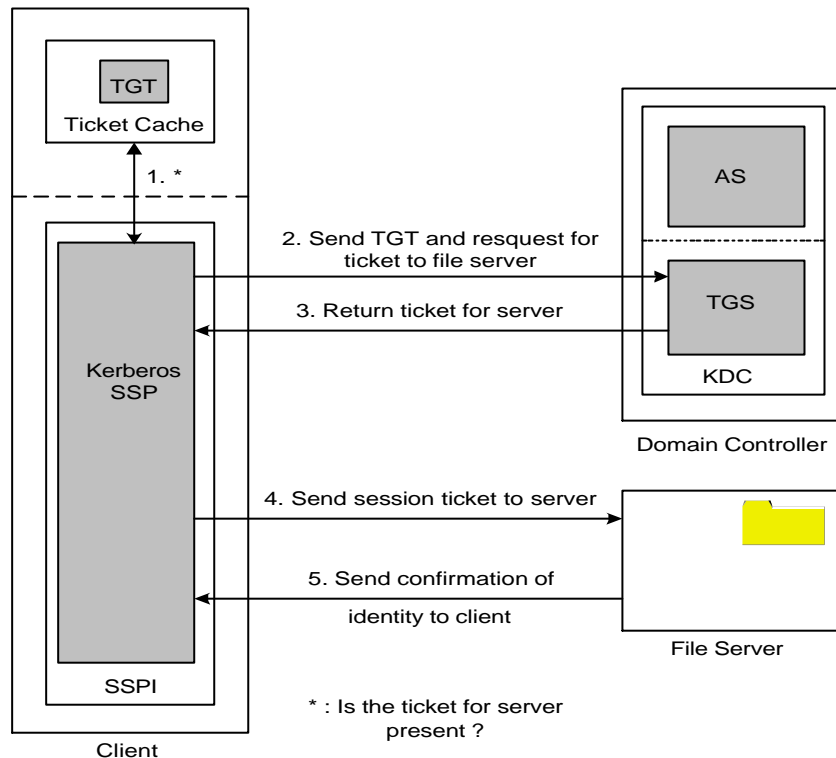
Ramapo Colleague – **Kerberos**
<http://ultrix.ramapo.edu/~fali/ecommm.html>

5.4 SCÉNARIO 3 : ACCÈS À UNE RESSOURCE PARTAGÉE DANS UN DOMAINE

5.4.1 Principe

Après avoir ouvert une session dans un domaine Windows 2000, l'utilisateur désire accéder à une ressource partagée. Cette ressource est représentée par un répertoire partagé sur un serveur de fichiers. Le client et le serveur de fichiers doivent être membre du domaine.

FIGURE 5.10 : ACCÈS À UNE RESSOURCE PARTAGÉE (DÉTAIL)



1. Lorsque l'utilisateur est authentifié sur le domaine, il désire accéder à la ressource partagée à l'aide de *Directory*. Pour cela, Kerberos SSP vérifie dans le cache si un ticket de session valide est présent pour le serveur de fichiers en question.
2. Si aucun ticket de session n'est présent, le TGT est envoyé au TGS pour un ticket de session qui permet d'accéder au serveur de fichiers.
3. Le service de délivrance des tickets renvoie un ticket de session pour pouvoir accéder au serveur. Le ticket de session peut être ensuite réutilisé pour des connexions futures sur le même serveur de fichiers s'il n'est pas expiré. La date d'expiration est définie par les polices de sécurité du domaine (→ Kerberos, Annexe 1 § 6.3).
4. Ensuite, le client envoie le ticket de session qu'il vient d'obtenir.

- Si le ticket de session est valide, le serveur de fichiers renvoie une confirmation.

Remarques

- Le ticket de session contient **une clé de session unique** créée par le KDC pour chiffrer les informations transférées entre le client et le serveur de fichiers.
- Le protocole Kerberos version 5 définit un champ chiffré dans les tickets de session pour transmettre les données d'autorisations (*Authorization Data*), mais l'utilisation de ce champ est laissée pour les applications.



Windows 2000 utilise ce champ pour transmettre les ID de sécurité (SID – *Windows Security ID*) qui représentent l'utilisateur et les groupes auxquels il appartient (→ § 5.5.2).

Ce champ est complété par le KDC lors de l'envoi du ticket de session (Paquet 3, figure 5.10). En effet, le KDC étant lié à Active Directory, il connaît les groupes auxquels l'utilisateur est membre.

- Grâce au champ qui contient les SID, le serveur de fichiers peut accepter ou refuser l'accès à sa ressource en fonction des autorisations de partage, et dans un deuxième temps, des autorisations locales.

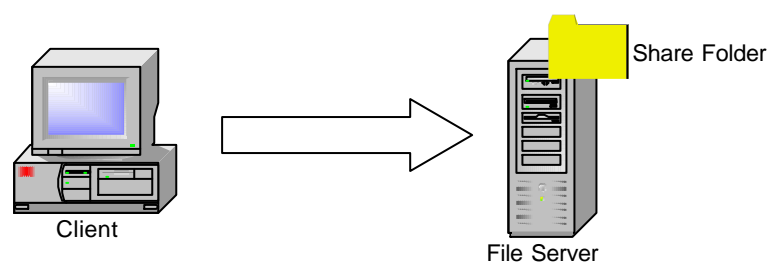
Sources : Windows 2000 Magazine – **How Kerberos Fits into the Windows NT 5.0 Security Model**
InstantDoc ID : 101

Microsoft MSDN – **Secure Networking Using Microsoft Windows 2000 Distributed Security Services**
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2k/html/msdn_distsecserv.asp

5.4.2 Configurations

Deux configurations d'autorisations sont possibles lorsqu'on accède à une ressource partagée.

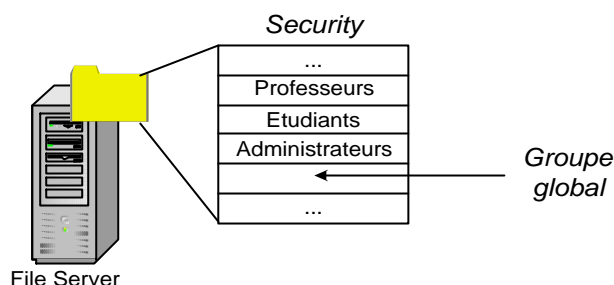
FIGURE 5.11 : ACCÈS À UNE RESSOURCE PARTAGÉE



1. Configuration triviale

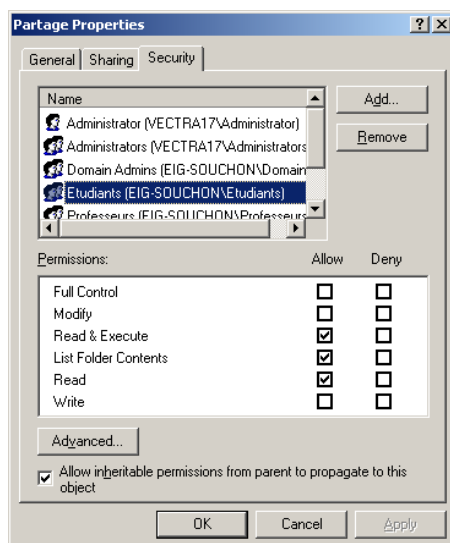
La configuration la plus simple à mettre en œuvre est d'ajouter **directement les groupes globaux** qui peuvent avoir accès au répertoire partagé.

FIGURE 5.12 : GROUPES GLOBAUX



Pour cela, il suffit d'aller dans les *Propriétés* du répertoire. Dans l'onglet *Security*, il suffit de faire *Add...* et d'ajouter les groupes d'utilisateurs (figure 5.13).

FIGURE 5.13 : CONFIGURATION TRIVIALE



Cette méthode est simple et facile à administrer si l'on possède **peu de groupes globaux**. Par contre, dans certains cas, un répertoire peut contenir plusieurs centaines de groupes globaux. Dans ce cas, l'administration se complique beaucoup et les **performances diminuent**.

En effet, lorsqu'un utilisateur accède au répertoire partagé, le serveur de fichiers doit tester **tous les groupes présents** dans l'onglet *Security* pour savoir quelles autorisations possèdent cet utilisateur.

2. Configuration AGDLP

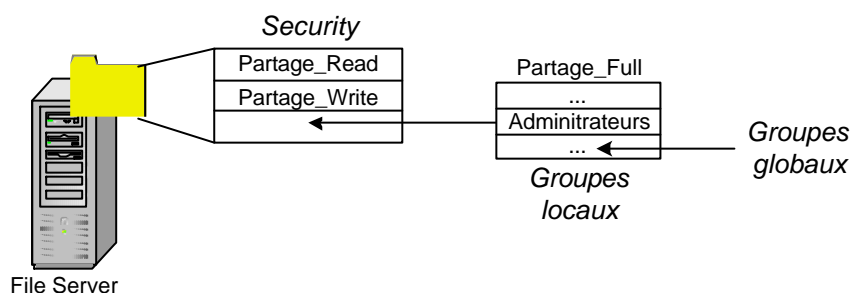
Cette configuration utilise les groupes locaux du serveur de fichiers ou les groupes de domaine locaux. Elle est **recommandée** par Microsoft :

The recommended strategy for using both global and domain local groups is to put user accounts (A) into global groups (G) and then to put global groups into domain local groups (DL) and assign resource permissions (P) to the domain local groups. This strategy (AGDLP) provides for the most flexibility and reduces the complexity of assigning access permissions to network resources.

- **AG** : Affecter des utilisateurs à des groupes globaux
- **DL** : Inclure des groupes globaux dans des groupes locaux au domaine
- **P** : Accorder les autorisations aux groupes locaux

Dans notre cas, on utilise les groupes locaux et non les groupes de domaines locaux.

FIGURE 5.14 : GROUPES GLOBAUX DANS GROUPES LOCAUX



Il faut créer **un groupe local par autorisation**. Dans notre exemple, on va créer trois groupes locaux correspondant aux trois autorisations *Read*, *Write* et *Full Control*.

Dans chaque groupe local, on ajoute des groupes globaux dont les autorisations correspondent à celle du groupe local.

Cette configuration permet d'avoir peu de groupes dans l'onglet *Security*, donc d'améliorer les performances.

5.5 SCÉNARIO 4 : AUDIT DE LA RESSOURCE PARTAGÉE

5.5.1 Introduction

L'**audit** permet le suivi des activités sur le réseau, appelé **événements**. Il est lié aux utilisateurs et au système. Tous ces événements sont enregistrés dans un journal de sécurité.

Par exemple, l'audit peut enregistrer les tentatives d'ouverture de session qui réussissent ou échouent, ainsi que les événements liés à la création, à l'ouverture ou à la suppression de fichiers ou de dossiers.

Chaque entrée dans le journal de sécurité fournit les informations suivantes :

- l'action qui a été exécutée
- l'utilisateur qui a exécuté l'action
- la réussite ou l'échec de l'événement et le moment auquel il s'est produit

Par défaut sous Windows 2000, la fonction d'audit est **désactivée**. C'est donc à l'administrateur de l'activer et déterminer les **événements** à auditer.

La stratégie d'audit peut être appliquée de différentes façons:

- **localement** : chaque ordinateur du domaine doit être configuré manuellement. Sur chaque ordinateur, des stratégies de sécurité locales (*Local Security Policy*) permettent de configurer la stratégie d'audit.
- **pour le domaine** : cette stratégie ne peut être configurée que sur le contrôleur de domaine. Le contrôleur de domaine possède des stratégies de sécurité pour le domaine (*Domain Security Policy*) qui permet d'appliquer ces stratégies à l'ensemble du domaine.



Lorsqu'une stratégie de sécurité est définie localement **et** pour le domaine, **c'est la stratégie du domaine qui est prioritaire sur la stratégie locale.**

Lorsqu'on définit une stratégie d'audit, il faut spécifier si l'on désire **auditer la réussite et/ou l'échec**.

La configuration des stratégies d'audit est expliquée en détail dans l'annexe 3.

Dans ce scénario, la stratégie d'audit est appliquée **localement** sur l'ordinateur dont on désire enregistrer certains événements. Dans notre cas, c'est le serveur de fichiers *VECTRA17* qui est configuré pour auditer **l'accès à sa ressource**.

Le choix de la stratégie est le suivant :

- **Toute personne** qui **réussit à lire** le document qui se trouve dans le répertoire partagé doit être auditée.
- **Toute personne** qui **réussit ou échoue l'écriture** du document est auditée.

5.5.2 SID

Les **identificateurs de sécurité** (SID – *Security IDentifier*) sont utilisés à la place des noms (qui ne peuvent pas être uniques) pour identifier les éléments (utilisateurs, groupes, ordinateurs, etc.).

Un SID est une clé numérique de longueur variable. Il se compose d'un numéro de révision, un identifiant d'autorité de 48 bits et d'un nombre variable de 32 bits appelé identificateurs relatifs (**RID** – *Relative IDentifier*). L'identifiant d'autorité indique l'entité qui a généré le SID. Le RID permet d'avoir un SID unique.

Grâce à *regedit.exe*, on peut visualiser le SID d'un ordinateur dans **HKEY_USERS**.

5.5.3 Access Tokens

Les **jetons d'accès** décrivent les privilèges requis pour accéder à une information.

La taille des jetons est variable puisque les utilisateurs ont des privilèges différents. Cependant, tous les jetons d'accès contiennent au moins les mêmes informations de base (figure 5.15).

On peut distinguer deux composants principaux dans un jeton d'accès :

- **Le SID de l'utilisateur** (*User Account SID*) et **les SID des groupes** (*Group N SID*) auquel il appartient.
- **Les privilèges** sont les droits associés au jeton d'accès. Par exemple, si le privilège d'ouvrir une session est présent dans le jeton d'accès, le processus qui y est rattaché permettra à l'utilisateur d'entreprendre cette action.

5.5.4 Descripteurs de sécurité

Les **descripteurs de sécurité** sont des éléments qui identifient un objet. D'une façon symétrique aux jetons pour les utilisateurs, ces objets possèdent une structure de données spécifiant les actions possibles et par qui elles le sont (figure 5.15).

La structure de données d'un descripteur se compose d'une zone d'en-tête qui contient le numéro de révision du descripteur et des drapeaux de contrôle spécifiant les attributs du descripteur. Le propriétaire de l'objet peut modifier ses autorisations d'accès.

Deux listes peuvent être attachées au descripteur :

- **DACL** (*Discretionary Access Control List*) permet de déterminer les actions qu'un utilisateur peut accomplir sur cet objet (**Qui peut faire quoi ?**). Ces actions sont représentées par des entrées de contrôle d'accès (**ACE** – *Access Control Entry*) qui sont illustrées sur la figure 5.15 :
 - Chaque entrée contient un type (*ACE Type*) qui autorise (*AccessAllowed*) ou refuse (*AccessDenied*) l'accès. Un troisième type (*SystemAudit*), utilisé par les SACL, archive les événements dans un journal d'audit (*Event Viewer*).
 - Le SID identifie l'utilisateur ou le groupe auquel cet ACE s'applique.
- **SACL** (*System Access Control List*) est une liste qui s'occupe d'enregistrer ce qu'un utilisateur a tenté de faire avec l'objet.

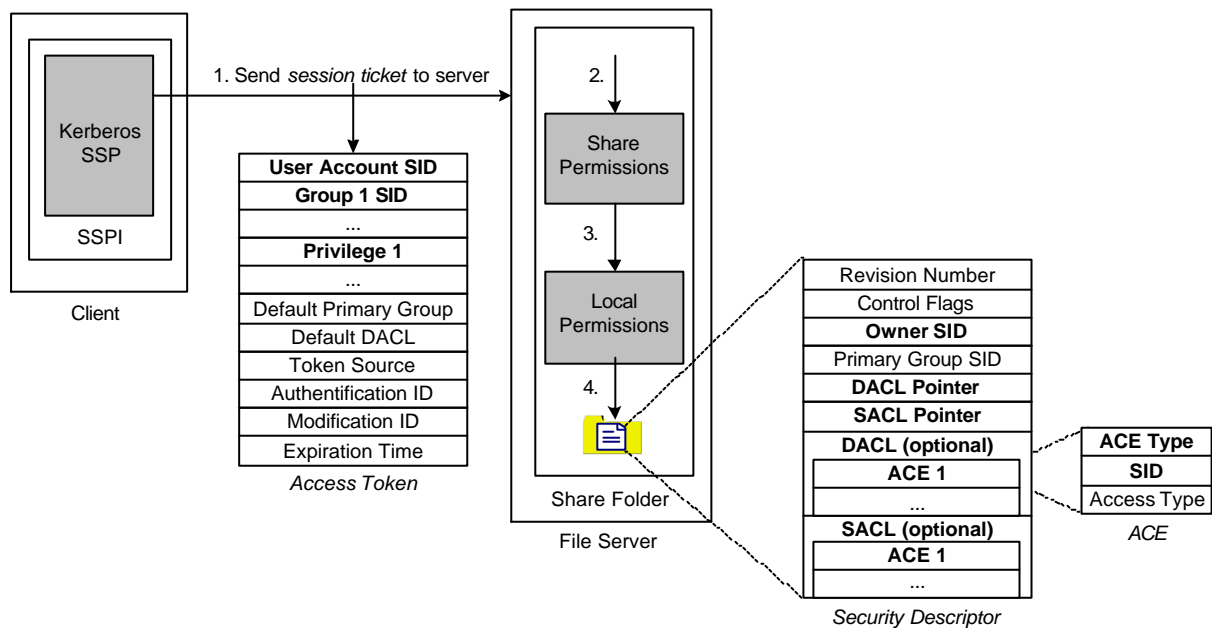
Remarques

- DACL
 - Si une DACL n'existe pas, tous les utilisateurs ont accès à l'objet.
 - Si une DACL existe mais ne contient pas d'ACE, personne n'a accès à l'objet.
- SACL
 - Si une SACL est vide, aucun audit n'est effectué.
 - Si une SACL contient des ACE de type *SystemAudit*, elle indique ce qui doit être audité selon que l'événement ait réussi et/ou échoué.

5.5.5 Principe

La figure 5.15 illustre tous les éléments qui interviennent lorsqu'on accède à une ressource qui est audité.

FIGURE 5.15 : ACCES A UNE RESSOURCE



1. Le client envoie son ticket de session qui contient les SIDs se trouvant dans les champs *Authorization Data* (→ § 5.4.1).
2. De son côté, le serveur vérifie grâce aux SID *User Account SID* et *Group N SID* si l'utilisateur a les autorisations de partage (→ § 2.3) suffisantes sur le répertoire partagé.

3. Le serveur va ensuite faire de même avec les autorisations locales (→ § 2.2) sur le dossier, et le fichier auquel l'utilisateur va accéder. Pour cela, il vérifie que les SID de l'utilisateur respectent les différentes ACE de la DACL.
Si le fichier possède une SACL non vide, le serveur va comparer les entrées de la SACL avec ce que l'utilisateur a tenté de faire et, si nécessaire, auditer ces tentatives.
4. Lorsque tous ces tests sont satisfaisants, l'utilisateur peut accéder à sa ressource.

Sources : Ecole d'Ingénieurs en informatique pour l'industrie – **Windows NT 4.0 Sécurité**
<http://www.e3i.univ-tours.fr/duac/winnt/uvnt2/uvnt2.htm>

Windows NT Magazine – **Windows NT Security, Part 2**
June 1998

6 ETAPE 2 : 2 DOMAINES DANS UNE FORÊT

6.1 OBJECTIFS

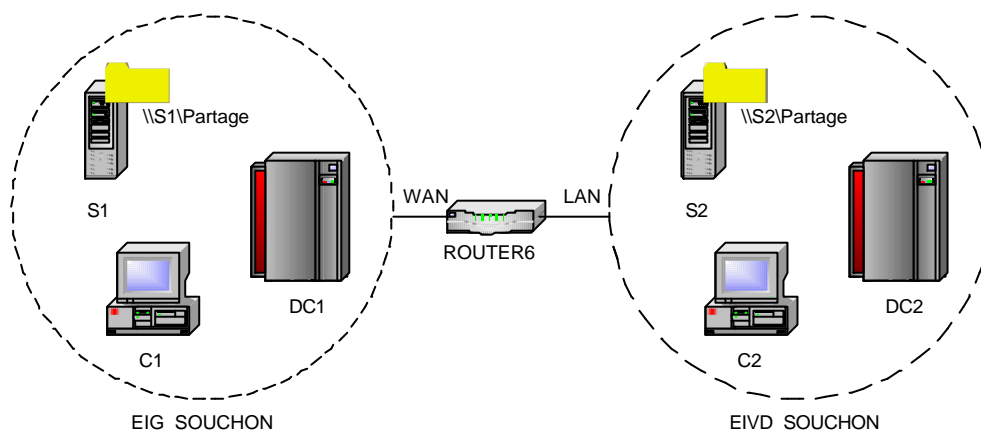
L'objectif de ce scénario est de simuler deux écoles (l'EIG et l'EIVD) en intranet. Chaque école correspond à un domaine Windows 2000, respectivement *EIG_SOUCHON* et *EIVD_SOUCHON*.

Chaque contrôleur de domaine fait office de serveur DNS privé pour son domaine.

- Deux domaines avec deux contrôleurs de domaine (*DC1*, *DC2*)
- Deux serveurs de fichiers avec chacun un répertoire partagé (*S1*, *S2*)
- Deux clients (*C1*, *C2*)
- Un routeur Lightning Ethernet II (*ROUTER6*)
- Deux serveurs DNS dynamiques
- Huit utilisateurs globaux et quatre groupes
- Deux zones d'adressages privées de classe C

6.1.1 Structure physique

Le schéma illustre la mise en œuvre du réseau décrit ci-dessus :



Chaque domaine utilise une zone d'adressage privée de classe C :

- *EIG_SOUCHON* : 192.168.1.0/24
- *EIVD_SOUCHON* : 192.168.2.0/24

Les deux tableaux ci-dessous représentent les configurations réseaux de chaque domaine.

<i>EIG_SOUCHON</i>	DC1	S1	C1
IP Address	192.168.1.10	192.168.1.11	192.168.1.12
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.1.1	192.168.1.1	192.168.1.1
DNS Server	192.168.1.10	192.168.1.10	192.168.1.10
Operating System	Windows 2000 Server	Windows 2000 Professional	Windows 2000 Professional

<i>EIVD_SOUCHON</i>	DC2	S2	C2
IP Address	192.168.2.10	192.168.2.11	192.168.2.12
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	192.168.2.1	192.168.2.1	192.168.2.1
DNS Server	192.168.2.10	192.168.2.10	192.168.2.10
Operating System	Windows 2000 Server	Windows 2000 Professional	Windows 2000 Professional

Le routeur possède **deux interfaces** (une pour chaque domaine), appelées *LAN* et *WAN*, avec chacune une adresse IP différente.

Le routeur doit aussi être configuré pour transmettre les paquets d'un domaine à l'autre. Pour cela, il faut ajouter deux routes qui permettent d'aiguiller le trafic.

Cette configuration réseau est décrite en détail dans le tableau suivant :

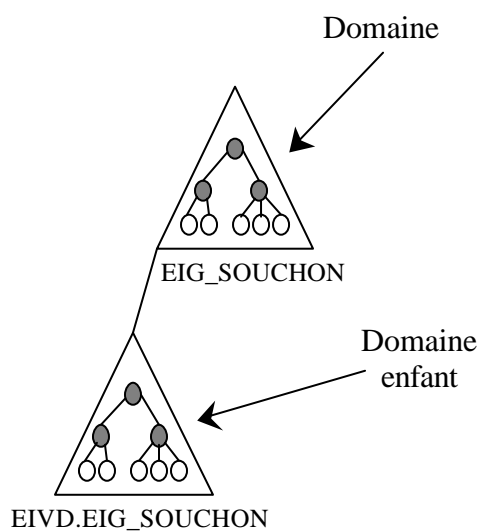
<i>ROUTER6</i>	Interface 1 (LAN)	Interface 2 (WAN)
IP Address	192.168.2.1	192.168.1.1
Subnet Mask	255.255.255.0	255.255.255.0

Routes	Destination	Gateway	Interface
<i>ROUTER6</i>	192.168.2.0/24	0.0.0.0	LAN
	192.168.1.0/24	0.0.0.0	WAN

6.1.2 Structure logique

Lorsqu'on désire mettre en place **deux domaines**, deux **variantes** sont possibles :

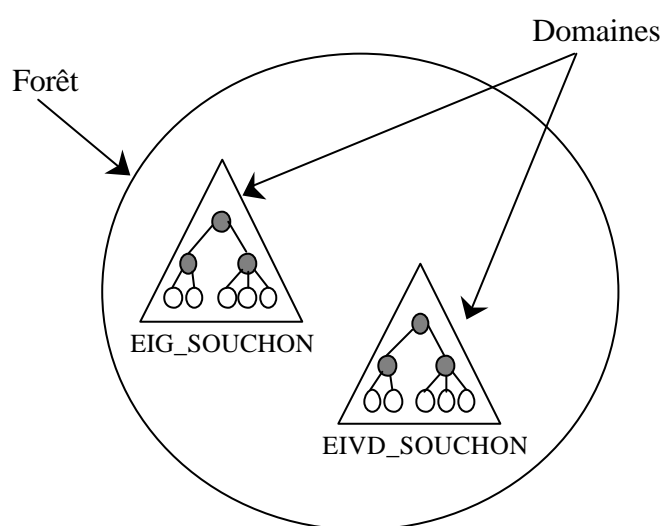
Variante 1 *Arbre de domaine et domaines-enfant*



Choix d'un arbre de domaine et de domaines-enfant :

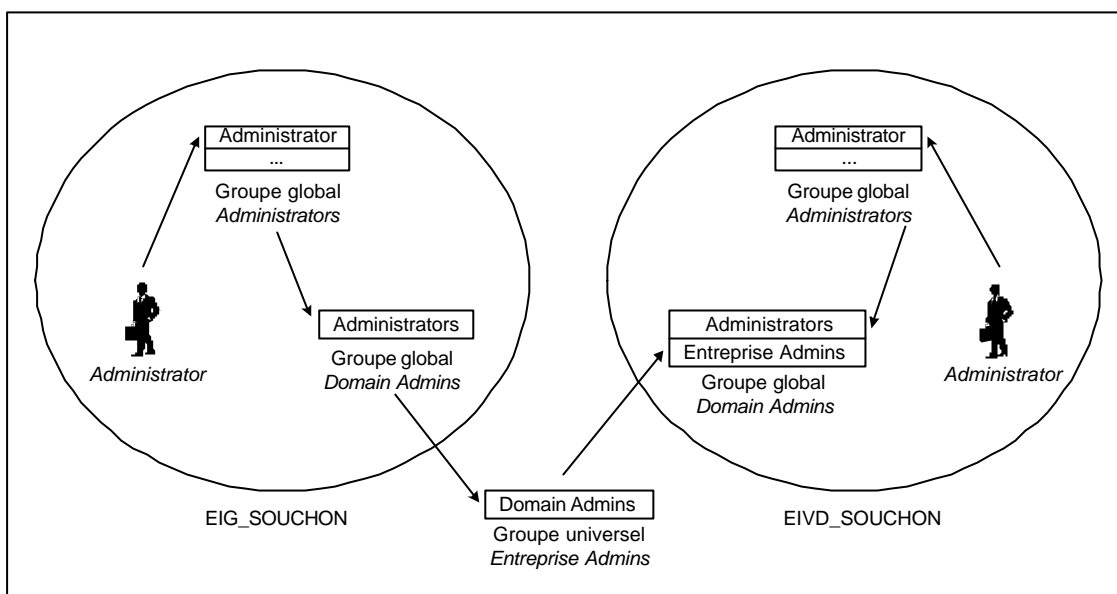
- Administration décentralisée
- Espace de noms contigu
- Administration localisée pour s'adapter à une langue ou un fuseau horaire différent.
- Partage un schéma, une configuration et un catalogue global.
- Le premier domaine possède tous les droits sur le deuxième domaine.

Variante 2 *Forêt de domaine*



Choix d'une forêt de domaine :

- Administration décentralisée
- Espace de noms non contigu
- Administration localisée pour s'adapter à une langue ou un fuseau horaire différent.
- Partage un schéma, une configuration et un catalogue global
- Par défaut, le premier domaine possède tous les droits sur le deuxième domaine (figure 6.1).

FIGURE 6.1 : GROUPE UNIVERSEL *ENTREPRISE ADMINS*

Par défaut, lorsqu'on rajoute un deuxième domaine (*EIVD_SOUCHON*) dans une forêt existante (*EIG_SOUCHON*), le **groupe universel** (→ 6.2.1) *Entreprise Admins* de la forêt est rajouté dans le groupe global *Domain Admins* de *EIVD_SOUCHON*. Cette astuce permet aux *Administrators* de l'EIG de pouvoir administrer aussi le domaine *EIVD_SOUCHON*.

Dans notre cas cela n'est pas souhaitable, car chaque école doit administrer **uniquement** son domaine respectif.

Par contre, il est possible de supprimer le groupe *Entreprise Admins* du groupe *Domain Admins* de l'EIVD.

Le choix s'est porté vers la **variante 2** pour une raison principale : les deux écoles doivent posséder **un espace de noms différent**.

Pour que la variante 2 soit mise en œuvre, les options d'installation des deux contrôleurs de domaine doivent être différentes. La marche à suivre détaillée est disponible dans l'annexe 1.

DC1 : Contrôleur de domaine

- *Domain Controller Type : Domain Controller for a **new domain***
- *Create Tree or Child Domain : Create a **new domain tree***
- *Create or Join Forest : Create a **new forest of domain trees***
- *New Domain Name : **DC1***
- *Configure DNS : Yes, install and configure DNS on this computer*
- *Permissions : Permissions compatible only with Windows 2000 servers*

Le premier contrôleur de domaine crée un nouveau domaine (*EIG_SOUCHON*), un nouvel arbre de domaine et une nouvelle forêt.

DC2 : Contrôleur de domaine

Les options sont identiques à la configuration de *DC1*, sauf :

- *Create or Join Forest : Place this new domain tree in an **existing forest***
- *New Domain Name : **DC2***

Le deuxième contrôleur de domaine doit aussi créer un nouveau domaine (*EIVD_SOUCHON*) et un nouvel arbre de domaine. Par contre, *DC2* doit être placé dans la forêt créée par *DC1*. Là aussi, un serveur DNS est obligatoire.

6.2 ACTIVE DIRECTORY

6.2.1 Groupe d'utilisateurs (*Users group*)

Dans le § 3.2.3, deux étendues de groupes sont expliqués. Ils interviennent au niveau du domaine. Il en existe une troisième qui agit au niveau **de la forêt : le groupe universel**.

	Groupes universels
Appartenance	Les membres sont issus de n'importe quel domaine
Accès aux Ressources	Les membres accèdent aux ressources de n'importe quel domaine

Les groupes universels gèrent la forêt de domaines. Par exemple, ils définissent qui a le droit d'ajouter un domaine dans la forêt ou encore qui a le droit de modifier le schéma (→ 6.2.7).

6.2.2 Espace de noms (*Namespace*)

Active Directory est essentiellement un espace de noms, comme c'est le cas de tout service d'annuaire. Par exemple, *td.unige.ch* pourrait être l'espace de noms utilisé par l'Ecole d'Ingénieurs de Genève.

N'importe quelle zone délimitée au sein de laquelle un nom donné peut être résolu constitue un espace de noms.

Active Directory repose sur le système de noms de domaine (DNS – *Domain Name System*) qui est aussi utilisé sur Internet.

Le principal avantage d'utiliser le DNS avec Active Directory est que les utilisateurs peuvent se connecter à des serveurs locaux en employant les mêmes règles d'attribution de nom que sur Internet.

Les espaces de noms existent sous deux formes :

- **Espace de noms contigu** : Dans une hiérarchie d'objets, le nom de l'enfant contient toujours le nom du domaine parent. Une arborescence est un espace de noms contigu.
- **Espace de noms non contigu** : Les noms d'un objet parent et d'un enfant du même objet parent ne sont pas directement liés les uns aux autres. Une forêt est un espace de noms non contigu.

6.2.3 Noms (*Name*)

Chaque objet dans Active Directory est identifié par un nom. Il y a deux sortes de noms :

- **Nom unique** : Chaque objet dans Active Directory possède un nom unique (DN – *Distinguished Name*). Le nom unique identifie le domaine qui contient l'objet, ainsi que le chemin d'accès complet permettant d'accéder à l'objet à travers la hiérarchie des unités d'organisation. Par exemple, ce nom unique identifie l'objet utilisateur « Yann Souchon » dans le domaine td.unige.ch :

/DC=ch/DC=unige/DC=td/OU=Etudiants /CN=Yann Souchon

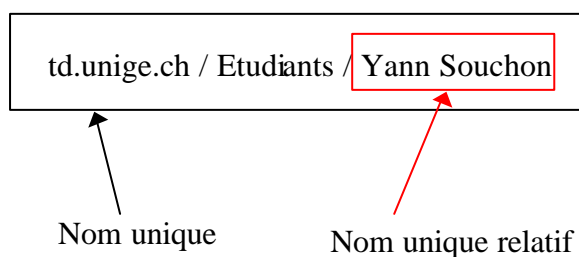
DC : Nom du composant du domaine

OU : Nom de l'unité d'organisation

CN : Nom courant

- **Nom unique relatif** : Le nom unique relatif (RDN – *Relative Distinguished Name*) d'un objet est la partie du nom qui constitue un attribut de l'objet. Dans l'exemple précédent, le nom unique relatif de l'objet utilisateur « Yann Souchon » est **CN=Yann Souchon**. Le nom unique relatif de l'objet parent est **CN=Etudiants**.

FIGURE 6.2 : NOM UNIQUE ET NOM UNIQUE RELATIF



6.2.4 Nomination d'objets

Un objet possède un seul nom, son nom unique (DN). Le DN identifie l'objet de manière unique et contient assez d'informations pour qu'un client puisse récupérer l'objet dans l'annuaire. Le DN d'un objet peut être très long et difficile à mémoriser. De plus, le DN d'un objet peut changer. Dans la mesure où le DN d'un objet est constitué de son nom unique relatif et de ses ancêtres, si un objet ou n'importe lequel de ses ancêtres change de nom, son DN changera.

Les DN sont difficiles à connaître et sujets à modification, il est utile de disposer d'autres moyens de récupérer des objets. Active Directory permet les requêtes par attributs, de telle sorte qu'on peut trouver un objet même si on ne connaît pas son DN exact ou s'il a changé. Pour simplifier le processus de recherche d'objets par requête, le schéma d'Active Directory définit deux propriétés :

- **Identificateur globalement unique d'objet** : L'identificateur globalement unique d'objet (GUID – *Globally Unique Identifier*) est un nombre codé sur 128 bits, garanti unique. Lorsqu'ils sont créés, les objets se voient attribuer un GUID. Le GUID ne change jamais, même si l'objet est déplacé ou renommé.
- **Nom principal d'utilisateur** : Le nom principal d'utilisateur (UPN – *User Principal Name*) est plus court que le DN et plus « convivial ». Le nom principal d'utilisateur est composé d'un nom abrégé pour l'utilisateur et du nom de l'arbre de domaines dans lequel se trouve l'objet utilisateur. Par exemple, l'utilisateur Yann Souchon de l'arbre td.unige.ch pourrait avoir l'UPN **souchon@td.unige.ch**.

6.2.5 Arbre (*Tree*)

Un arbre, aussi appelé arbre de domaine, est constitué de plusieurs domaines qui partagent **un même schéma** et **une même configuration**, formant un espace de nom contigu. Les domaines d'un arbre sont également liés entre eux par des relations d'approbation. Active Directory est un arbre ou un ensemble de plusieurs arbres. Il y a deux façons de visualiser un arbre : par le biais des relations d'approbation entre domaines ou par celui de l'espace de noms de l'arbre de domaines.

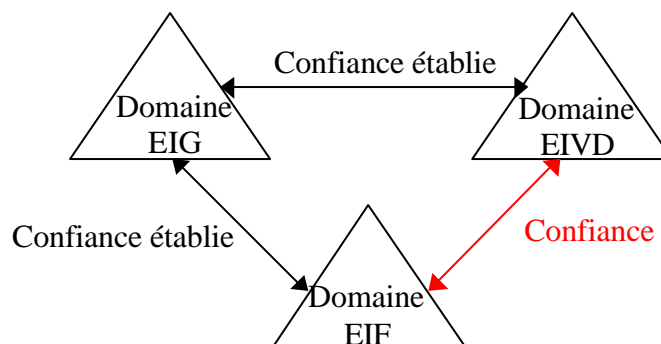
- Représentation des relations d'approbation

On peut dessiner un arbre de domaines en représentant les domaines individuels et leurs relations d'approbations mutuelles.

Windows 2000 établit des relations d'approbation entre domaines en se basant sur le protocole d'authentification Kerberos. L'approbation Kerberos est transitive et hiérarchique (→ Kerberos § 3.5.1).

La figure 6.3 représente trois domaines séparés. Chaque domaine, symbolisé par un triangle, correspond à un ensemble d'ordinateurs sous Windows 2000 avec un ou plusieurs contrôleurs de domaine. De plus, cette figure illustre les relations d'approbation qu'on peut avoir entre différents domaines.

FIGURE 6.3 : ARBRE DE DOMAINES PAR RELATIONS D'APPROBATION

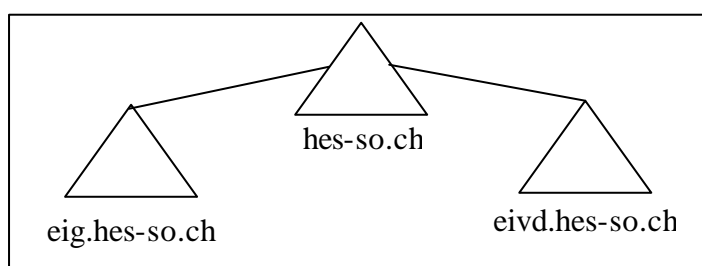


- Représentation de l'espace de noms

On peut aussi dessiner un arbre de domaine en fonction de son espace de noms. On détermine le nom relatif distinct d'un objet en suivant le chemin d'accès jusqu'à l'espace de noms de son arbre de domaines. Cette représentation est utile pour regrouper des objets selon une hiérarchie logique. L'avantage principal d'un espace de noms contigu est qu'une recherche approfondie à partir de la racine de l'espace de noms se fera dans l'ensemble de la hiérarchie.

Pour mieux comprendre, la figure 6.4 illustre un domaine principal (hes-so.ch) avec deux sous domaines qui sont l'Ecole d'Ingénieurs de Genève (EIG) et l'Ecole d'Ingénieurs du Canton de Vaud.

FIGURE 6.4 : ARBRE DE DOMAINES SOUS FORME D'ESPACE DE NOMS



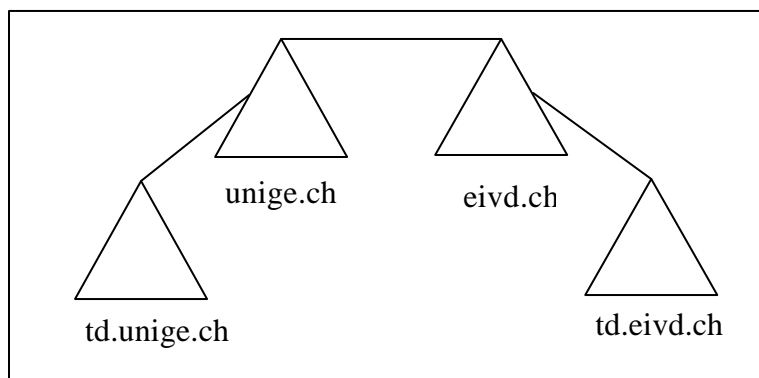
6.2.6 Forêt (Forest)

Une forêt est constituée d'un arbre ou de plusieurs arbres qui ne forment pas un espace de nom contigu. Tous les arbres d'une forêt partagent **un même schéma, une même configuration** et un **même catalogue global**.

De plus, ils s'accordent une confiance mutuelle par l'intermédiaire de relations d'approbation Kerberos transitives et hiérarchiques. Contrairement à un arbre, une forêt n'a pas besoin de nom distinct.

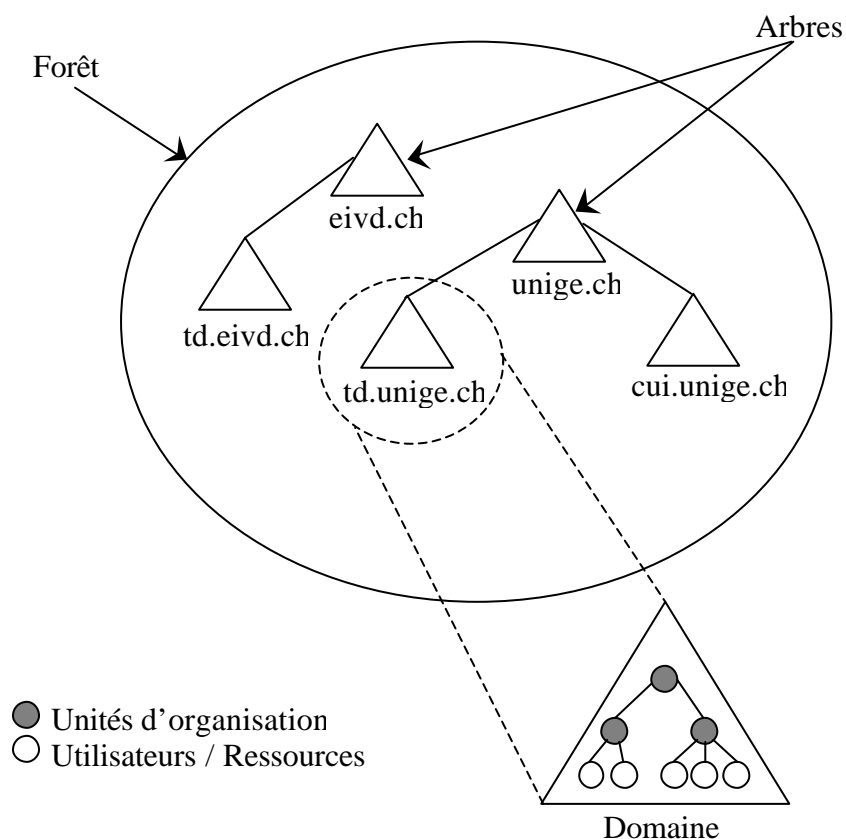
La figure ci-dessous montre deux domaines séparés avec un espace de nom non contigu.

FIGURE 6.5 : FORET DE DOMAINES



La figure 6.6 représente l'ensemble des différents éléments qu'on peut avoir dans une structure logique d'Active Directory. Pour compléter la figure, deux domaines (EIVD et UNIGE) illustrent la notion d'arbres avec deux sous-domaines pour UNIGE. L'ensemble forme une forêt.

FIGURE 6.6 : STRUCTURE LOGIQUE



6.2.7 Schéma

Le **schéma** d'Active Directory est une liste de définitions qui spécifie les types d'objets pouvant être stockés dans Active Directory et la nature des informations relatives à ces objets. Les définitions sont elles-mêmes stockées en tant qu'objets, afin que Active Directory puisse gérer les objets de schéma en appliquant les mêmes opérations de gestion que pour les autres objets de l'annuaire.

Il existe deux types séparés de définition dans le schéma : les **attributs** et les **classes**. Les attributs et les classes sont définis séparément. Chaque attribut est défini une seule fois et peut être utilisé dans plusieurs classes. Par exemple, l'attribut *Description* est utilisé dans de nombreuses classes, mais n'est défini qu'une seule fois dans le schéma.

Les classes, appelées aussi **classes d'objets**, décrivent les objets pouvant être créés dans Active Directory. Chacune d'elles est un regroupement d'attributs. Lors de la création d'un objet, les attributs stockent les informations qui décrivent l'objet.

Par exemple, certains programmes de messagerie comme *Microsoft Exchange* ou *Lotus Notes* modifient le schéma en rajoutant des nouvelles classes.

6.2.8 Catalogue global

Le catalogue global (GC – *Global Catalog*) permet aux utilisateurs et aux applications de trouver des objets dans l'arbre de domaines ou dans la forêt d'Active Directory pour peu qu'ils connaissent un ou plusieurs attributs de l'objet recherché.

Par défaut, le catalogue global est automatiquement créé sur le premier contrôle de domaine, appelé **serveur de catalogue global**.

Le catalogue global permet aux utilisateurs de trouver rapidement les objets qui les intéressent sans savoir quel domaine les contient.

Sources : Microsoft Press – **Windows 2000 Active Directory Services**

Document personnel – **Active Directory**
<http://perso.club-internet.fr/jegoup/AD.htm>

6.3 SCÉNARIO 1 : DNS

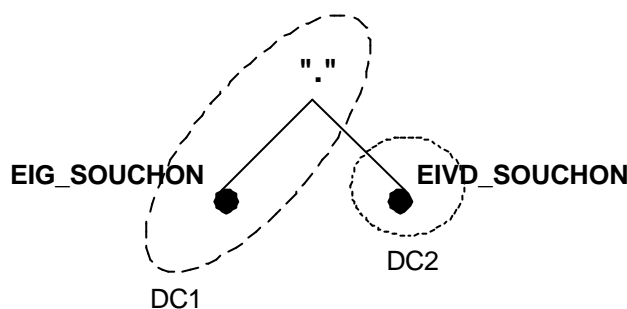
Après l'installation du premier contrôleur de domaine, on peut remarquer que la configuration du serveur DNS par défaut contient la zone correspondante au nom du domaine ainsi qu'une **zone d'adressage supplémentaire**. Cette zone d'adressage est une **zone root** représentée par un point ("."), c'est-à-dire qu'elle correspond au plus haut niveau dans la hiérarchie du DNS. Cette zone est créée car le réseau est totalement isolé d'internet, et que donc, par conséquent, Windows 2000 ne trouve aucun autre serveur DNS *root*.

La configuration du deuxième serveur DNS (sur le deuxième contrôleur de domaine) contient qu'une **seule zone**. Cette zone correspond au nom du domaine (*EIVD_SOUCHON* dans notre cas).

Dans la configuration des serveurs *root* (onglet *Root Hints*), le deuxième serveur DNS possède une entrée qui correspond au premier serveur DNS.

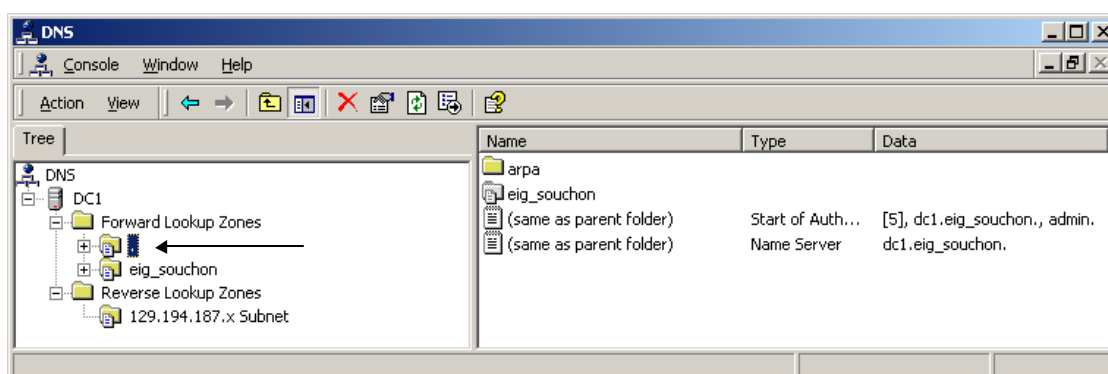
La figure 6.7 est le schéma de la configuration par défaut des serveurs DNS lorsqu'on installe deux contrôleurs de domaines dans la **même forêt et sans connexion internet**.

FIGURE 6.7 : CONFIGURATION DES SERVEURS DNS



Pour mieux comprendre, la figure 6.8 illustre la configuration du premier serveur DNS. La flèche montre la zone *root*.

FIGURE 6.8 : ZONE D'ADRESSAGE ROOT



La configuration décrite à la page précédente pose un **problème**. En effet, pour qu'on puisse accéder à un domaine depuis l'autre domaine, il faut que les serveurs DNS puissent travailler ensemble. Dans notre cas, seul le serveur DNS de *DC2* interroge *DC1* s'il ne connaît pas la réponse. Dans l'autre cas, comme *DC1* est un serveur DNS *root*, il ne peut pas interroger *DC2*.

Pour remédier à cela, il faut **supprimer la zone *root* (".")** de *DC1* en cliquant simplement sur la zone et ensuite sur *delete*.

DC1 peut maintenant interroger d'autres serveurs s'il ne connaît pas la réponse.

Deux variantes sont possibles pour que les serveurs DNS travaillent ensemble :

- Soit on utilise l'onglet ***Root Hints*** qui permet d'introduire des serveurs DNS *root*. Le serveur DNS interroge ces serveurs *root* lorsqu'il ne connaît pas la réponse.
- L'autre méthode est transmettre la requête à un autre serveur (onglet ***Forwarders***).

Comme aucun des deux serveurs DNS n'est un serveur *root*, le choix le plus approprié est la deuxième variante (→ Annexe 4).

6.4 SCÉNARIO 2 : RÉPLICATION

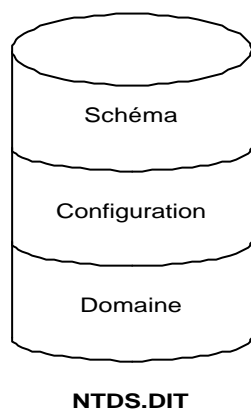
Ce scénario explique le principe de la réplication sous Windows 2000.

Dans le cas d'une forêt avec deux domaines, les deux contrôleurs de domaine doivent connaître l'ensemble des objets de la forêt. Pour cela, on utilise la **réplication**.

La réplication permet de maintenir à jour les données d'Active Directory. Chaque contrôleur de domaine possède un fichier sous forme de base de données qui possède l'ensemble des objets de son domaine. Ce fichier se trouve par défaut dans `\WINNT\NTDS\NTDS.DIT` (figure 6.9). Ce répertoire est modifiable à l'installation d'Active Directory (→ Annexe 1).

Le fichier NTDS.DIT se compose de trois parties :

FIGURE 6.9 : NTDS.DIT



- **Schéma** : Contient la définition de tous les objets et attributs qu'il est possible de créer dans Active Directory (→ 6.2.7). Répliquée sur tous les contrôleurs de domaine de la forêt.
- **Configuration** : Contient les informations concernant la structure d'Active Directory (domaines, sites, contrôleurs de domaine, etc.). Répliquée sur tous les contrôleurs de domaine de la forêt.
- **Domaine** : Tous les objets d'Active Directory sont stockés dans cette partie (*Users, Groups, Computers, etc.*). Répliquée au sein du domaine.

Qu'on utilise la variante 1 ou la variante 2, tous les contrôleurs de domaine partagent **le même schéma** et **la même configuration**. Ces deux parties sont **répliquées séparément**.

La partie **domaine** est spécifique à **chaque domaine**. Dans notre cas, *DC1* possède une partie **domaine1** et *DC2* **domaine2**, car *DC1* ne contient pas les mêmes objets que *DC2*.

La réplication intervient du fait des changements apportés à Active Directory :

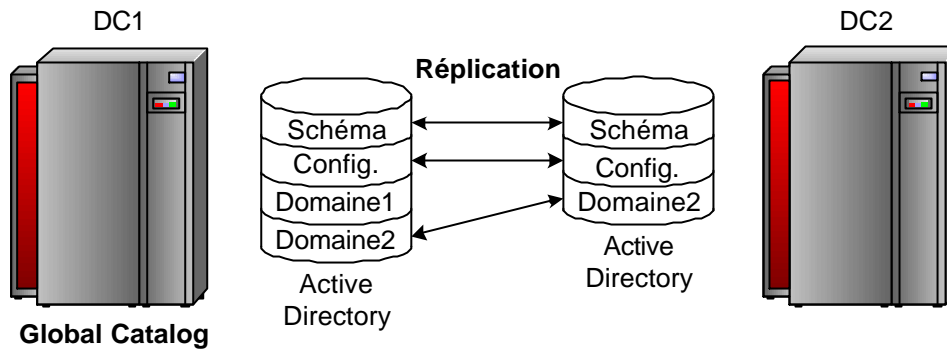
- Nouveaux comptes d'utilisateurs
- Changement d'attributs sur des objets
- Suppression d'objets

Temps entre chaque réplication :

- Toutes les 5 minutes par défaut lors d'une modification
- Toutes les heures en absence de modification
- Immédiate lors de réplication urgente (tout ce qui touche à la sécurité, par exemple verrouillage de comptes d'utilisateurs)

Par défaut, le premier contrôleur de domaine (*DC1*) est un **catalogue global** (→ § 6.2.8), c'est-à-dire qu'il contient sa partie domaine (domaine1) ainsi que la partie domaine de *DC2* (domaine2), comme l'illustre la figure 6.10. Par contre *DC2* ne l'est pas.

FIGURE 6.10 : REPLICATION DANS UNE FORET, CATALOGUE GLOBAL



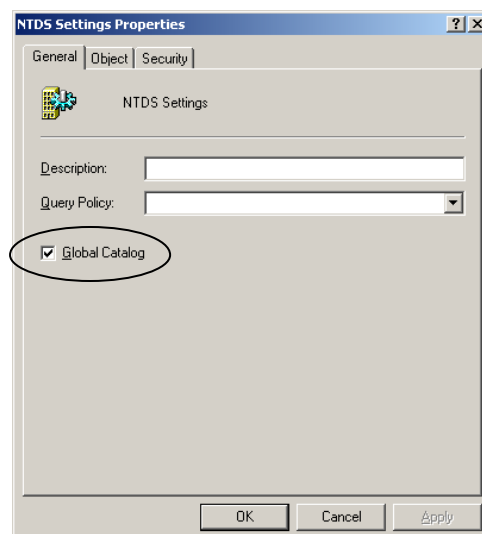
Dans notre cas, cela ne pose pas de problème de performance car la liaison entre les deux domaines est rapide.

Mais par exemple, si *DC1* et *DC2* seraient reliés par une liaison lente, il faudrait que *DC2* interroge *DC1* pour les objets qu'il ne connaît pas. Cela poserait un gros problème de performance.

En activant la fonction **Global Catalog** sur *DC1* et *DC2*, les deux contrôleurs de domaine se répliquent chacun leur partie **domaine**.

Pour qu'un contrôleur de domaine soit catalogue global, il faut simplement exécuter **Start – Programs – Administrative Tools – Active Directory Sites and Services**. Ensuite dans **Sites – Default-First-Site-Name – Servers**, sélectionnez le contrôleur de domaine (dans notre cas *DC2*) et affichez les **Propriétés** de **NTDS Settings** (figure 6.11).

FIGURE 6.11 : CATALOGUE GLOBAL



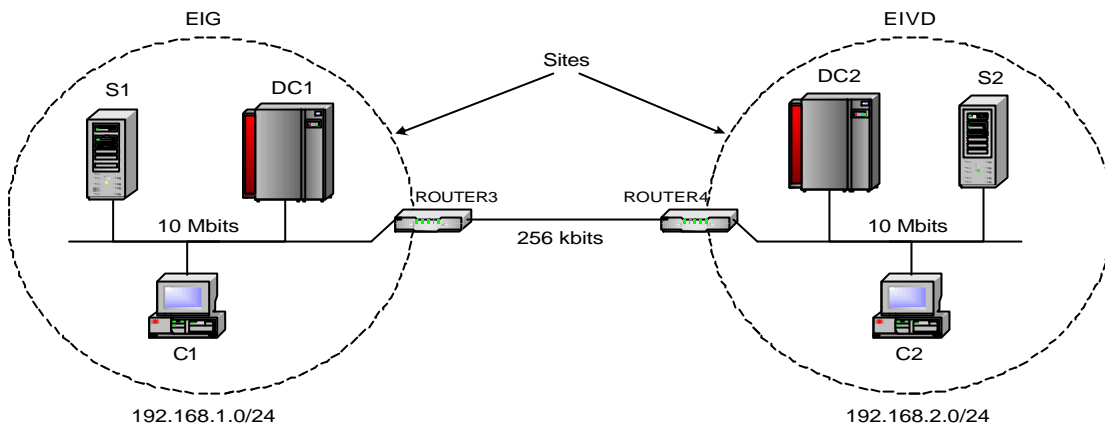
6.5 SCÉNARIO 3 : SITE

Ce scénario explique le principe du **site** avec un exemple (figure 6.12) qui illustre les deux écoles reliées par une liaison bas débit.



Attention, cette figure ne correspond pas à la structure physique de cette étape. La structure a été modifiée pour pouvoir expliquer la notion de site.

FIGURE 6.12 : SITES



Un site est une combinaison d'un ou plusieurs sous-réseaux IP connecté par une liaison haut débit.

Dans notre exemple, un site est représenté par un sous-réseau IP. A l'intérieur du site (intrasite), le réseau doit être d'un débit élevé (10 Mbits ou plus). Par contre, à l'extérieur des sites (intersites), la liaison est seulement de 256 kbits.

La création de deux sites possède deux avantages majeurs :

- **Optimisation de l'authentification**

Par défaut, lorsqu'on crée deux domaines dans une même forêt, un seul site est créé. De plus, seul le premier contrôleur de domaine (*DC1*) fait office de catalogue global.

Cette configuration par défaut introduirait un gros problème de performance. Par exemple, dix utilisateurs de l'EIG sont en dépassement à l'EIVD. Si ces utilisateurs s'authentifient les dix à la fois, ils devront patienter un moment avant qu'ils puissent travailler. En effet, ces utilisateurs faisant partit du domaine *EIG*, **DC2 devra aller interroger DC1** pour savoir si oui ou non ces utilisateurs peuvent accéder au domaine *EIVD*.

Pour résoudre ce problème, il faut premièrement déclarer *DC2* comme un **catalogue global**, ce qui va permettre à *DC2* de connaître les objets de *DC1*.

Cela ne suffit pas, car Windows 2000 ne définit pas d'une manière certaine que les dix utilisateurs utilisent *DC2* pour s'authentifier. Il est possible de voir sur un client la variable *LogonServer* (tapez **set | more** dans une console) qui définit sur quel contrôleur de domaine l'ordinateur s'authentifie.

C'est pour cela qu'il faut créer un site. **Tout site doit contenir au minimum un contrôleur de domaine avec un catalogue global.**

- **Configuration de la réplication intersite**

A l'intérieur d'un site, il n'est pas possible de configurer la réplication. Comme la réplication peut engendrer beaucoup de trafic (suivant les modifications), il faut que le réseau d'un site soit de bonne qualité. La réplication intrasite utilise le **protocole RPC** et s'effectue toutes les **cinq minutes**.

A l'extérieur des sites, la réplication est configurable en fonction de la bande passante à disposition. Il est possible de la compresser et de choisir un protocole entre RPC et SMTP (*Simple Mail Transfer Protocol*). SMTP possède deux avantages par rapport à RPC :

- SMTP peut être utilisé sur des **liaisons de mauvaises qualités**, car il supporte beaucoup mieux les **coupures**.
- Les **firewalls** possèdent très souvent le port SMTP (25) déjà ouvert, car SMTP est utilisé par presque tous les programmes de messageries.

Pour réduire le trafic sur la liaison intersite, on peut aussi configurer le **temps entre chaque réplication**

Dans cet exemple, un site représente un domaine. Mais on peut très bien avoir plusieurs domaines par site ou plusieurs sites par domaine.

Quelle est la différence entre un site et un domaine ?

Un domaine regroupe sous un même nom des ordinateurs ainsi que des ressources réseaux. Un site est un élément de la structure physique d'Active Directory alors qu'un domaine est un élément de la structure logique.

Comment un poste de travail trouve-t-il le site auquel il appartient ?

Un poste de travail trouve son site en présentant son numéro de sous-réseau au premier contrôleur de domaine qu'il contacte. Il détermine son numéro de sous-réseau en appliquant son masque de sous-réseau à son adresse IP. Le premier contrôleur de domaine contacté utilise le numéro de sous-réseau soumis pour localiser l'objet du site auquel appartient le poste de travail. Si le serveur courant n'appartient pas lui-même à ce site, il indique au poste de travail un autre serveur à contacter.

7 ETAPE 3 : 2 DOMAINES DANS 2 FORÊTS

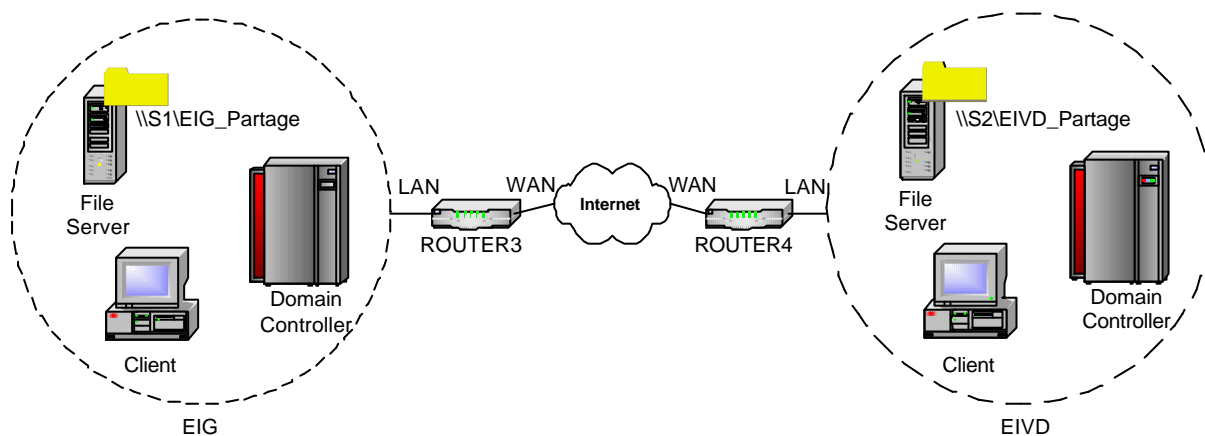
7.1 OBJECTIFS

L'objectif de ce scénario est de simuler deux écoles (l'EIG et l'EIVD) avec une connexion internet. Chaque école correspond à un domaine Windows 2000, respectivement *EIG* et *EIVD*.

- Deux domaines avec deux contrôleurs de domaine (*DC1*, *DC2*)
- Deux serveurs de fichiers avec chacun un répertoire partagé (*S1*, *S2*)
- Deux clients (*C1*, *C2*)
- Deux routeurs Lightning Ethernet II (*ROUTER3*, *ROUTER4*)
- Deux serveurs DNS dynamiques (*DNS1*, *DNS2*)
- Huit utilisateurs globaux et quatre groupes
- Deux zones d'adressages privées de classe C

7.1.1 Structure physique

Le schéma illustre la mise en œuvre du réseau décrit ci-dessus :



Chaque domaine utilise une zone d'adressage privée de classe C :

- *EIG* : 10.0.1.0/24
- *EIVD* : 10.0.2.0/24

Les deux tableaux ci-dessous représentent les configurations réseaux de chaque domaine.

<i>EIG_SOUCHON</i>	DC1	S1	C1
IP Address	10.0.1.10	10.0.1.11	10.0.1.12
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	10.0.1.1	10.0.1.1	10.0.1.1
DNS Server	10.0.1.10	10.0.1.10	10.0.1.10
Operating System	Windows 2000 Server	Windows 2000 Professional	Windows 2000 Professional

<i>EIVD_SOUCHON</i>	DC2	S2	C2
IP Address	10.0.2.10	10.0.2.11	10.0.2.12
Subnet Mask	255.255.255.0	255.255.255.0	255.255.255.0
Gateway	10.0.2.1	10.0.2.1	10.0.2.1
DNS Server	10.0.2.10	10.0.2.10	10.0.2.10
Operating System	Windows 2000 Server	Windows 2000 Professional	Windows 2000 Professional

La configuration des deux routeurs est décrite ci-dessous :

<i>ROUTER3</i>	Interface 1 (LAN)	Interface 2 (WAN)
IP Address	10.0.1.1	129.194.187.45
Subnet Mask	255.255.255.0	255.255.252.0

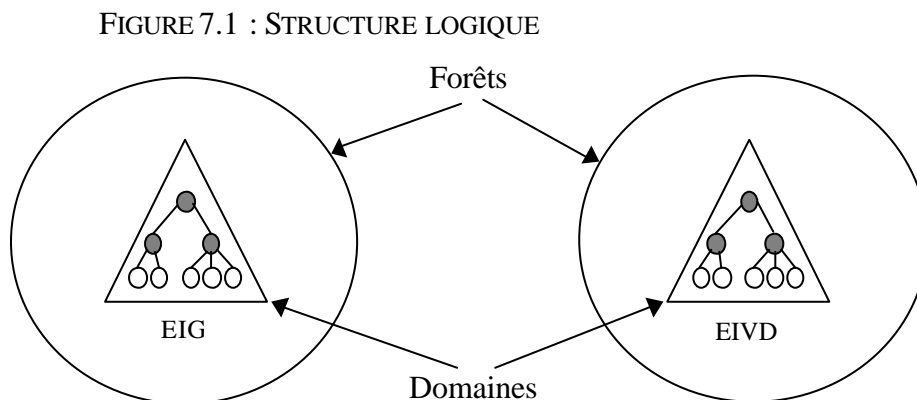
<i>ROUTER4</i>	Interface 1 (LAN)	Interface 2 (WAN)
IP Address	10.0.2.1	129.194.186.207
Subnet Mask	255.255.255.0	255.255.252.0

Routes	Destination	Gateway	Interface
<i>ROUTER3</i>	10.0.1.0/24	0.0.0.0	LAN
	129.194.184.0/22	0.0.0.0	WAN
	Default	129.194.184.3	WAN
<i>ROUTER4</i>	10.0.2.0/24	0.0.0.0	LAN
	129.194.184.0/22	0.0.0.0	WAN
	Default	129.194.184.3	WAN

7.1.2 Structure logique

Lorsqu'on installe les éléments d'un domaine Windows 2000 (structure logique), il est recommandé de respecter dans l'ordre les quatre étapes suivantes :

1. **Installation du serveur DNS** : La résolution DNS entre les deux domaines est très importante pour qu'Active Directory fonctionne correctement (→ § 7.3).
2. **Installation d'Active Directory** : La structure logique d'Active Directory est représentée ci-dessous.



Le choix de deux domaines dans deux forêts :

- Administration décentralisée
- Espace de noms non contigu
- Administration localisée pour s'adapter à une langue ou un fuseau horaire différent.
- Schémas, configurations et catalogues globaux indépendants
- Chaque administrateur gère sa forêt

Par rapport à la structure logique de l'étape 2 (→ 6.1.2), cette structure possède **deux avantages majeurs d'indépendances** :

- **Chaque école possède son propre schéma**, ce qui permet d'installer des applications qui le modifie sans déranger l'autre école (→ 6.2.7).
- **Chaque administrateur gère sa forêt**, ce qui n'était pas possible sans modification avec l'ancienne structure.

Pour créer cette structure, les options d'installation des deux contrôleurs de domaine doivent être identiques, à part le nom du domaine. Par exemple, pour *DC1* :

DC1 : Contrôleur de domaine

- *Domain Controller Type : Domain Controller for a new domain*
- *Create Tree or Child Domain : Create a new domain tree*
- *Create or Join Forest : Create a new forest of domain trees*
- *New Domain Name : DC1*
- *Configure DNS : No, I will install and configure DNS myself.*
- *Permissions : Permissions compatible only with Windows 2000 servers*



Ne pas oublier de changer le type des deux zones (directes et inverses) sur les deux serveurs DNS de chaque domaine. Maintenant qu'Active Directory est installé, **il est recommandé de les intégrer à Active Directory** (→ § 7.2.4).

Lorsque les zones sont intégrées à Active Directory, ajoutez les ordinateurs dans le domaine (*join a domain*, → Kerberos § 3.6.1). Le serveur DNS est mis à jour automatiquement dès que l'ordinateur joint le domaine.

3. **Configurations des relations d'approbations** : Pour que les utilisateurs puissent s'authentifier sur les deux domaines, il faut établir des relations d'approbations (*trust*) bidirectionnelles (→ § 7.4).
4. **Configuration d'un répertoire confidentiel** : Pour finir, un nouveau répertoire est partagé sur les serveurs de fichiers (→ § 7.5).

7.2 DNS

7.2.1 Nouveautés

Le service DNS permet la résolution de noms pour des clients. Grâce à cette fonction, les utilisateurs peuvent accéder à des serveurs en utilisant leur nom au lieu d'adresses IP difficiles à retenir. Active Directory fait appel au DNS pour l'attribution des noms de domaine et la localisation. Les noms de domaines Windows 2000 sont des noms DNS.

Windows 2000 intègre deux nouveautés principales dans son serveur DNS :

- **Les enregistrements de type SRV**
- **Le DNS dynamique**

7.2.2 *SRV record type*

Ce nouveau type d'enregistrement permet de localiser un **service** au moyen du serveur DNS. L'extension SRV est basée sur la RFC 2052.

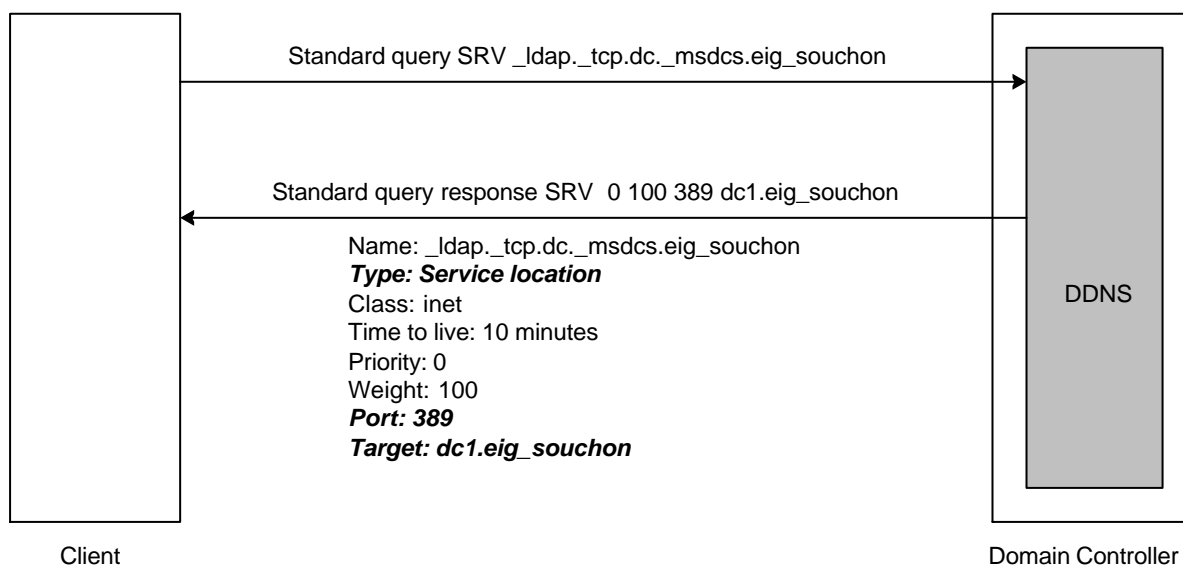
Le détail de la syntaxe avec les principaux champs est la suivante :

_Service._Proto.Name TTL Class SRV Priority Weight Port Target

- *Service* : le nom du service (*_http*)
- *Proto* : le protocole utilisé par le service (*_tcp*)
- *Name* : le nom du domaine où se trouve le service
- *Port* : le port du service
- *Target* : le FQDN de l'ordinateur

La figure 7.2 illustre un client qui désire connaître sur quel ordinateur se trouve le contrôleur de domaine. Le serveur DNS lui répond l'ordinateur qui fait office de contrôleur de domaine.

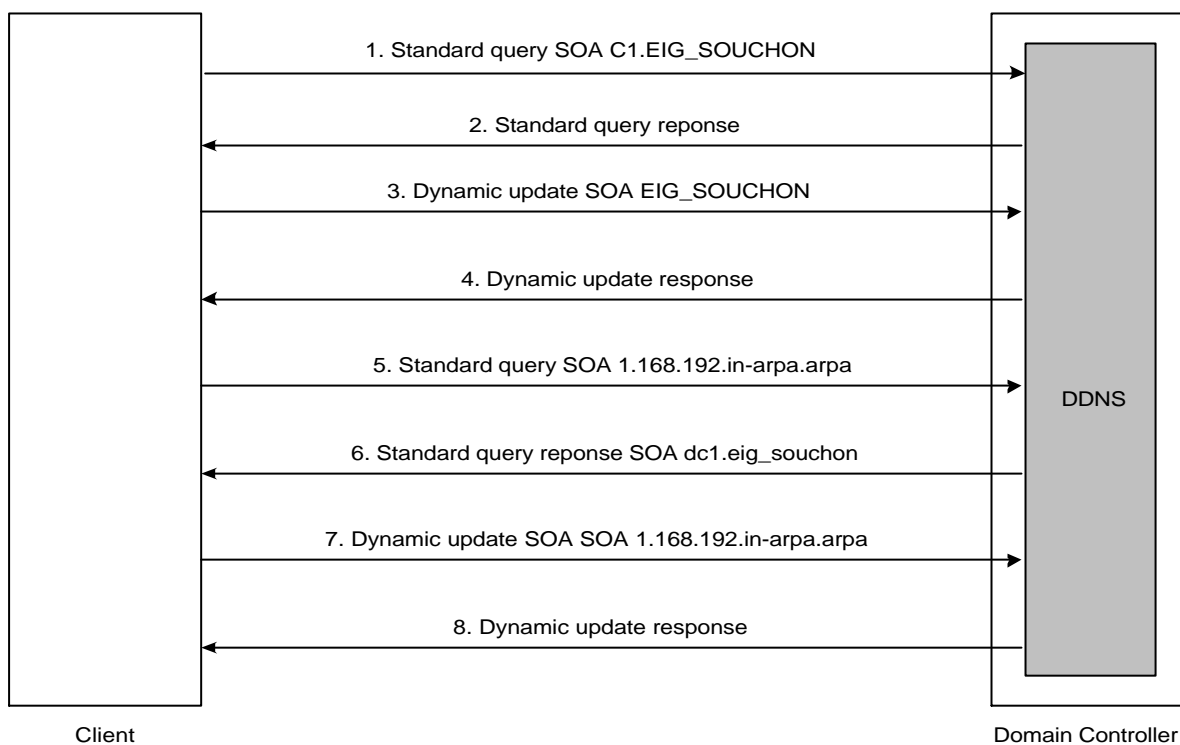
FIGURE 7.2 : LOCALISATION DU CONTRÔLEUR DE DOMAINE



7.2.3 Dynamic DNS

Windows 2000 Server utilise le **DNS dynamique** (DDNS – *Dynamic DNS*) , qui permet aux clients de s’inscrire directement auprès d’un serveur exécutant le service DNS et de mettre à jour le tableau DNS dynamiquement.

FIGURE 7.3 : MISE À JOUR DU DNS DYNAMIQUEMENT



1. Le client envoie une requête au serveur DNS pour connaître quel serveur gère la zone à laquelle il appartient.
2. Dans notre cas, c’est ce serveur DNS qui gère la zone *EIG_SOUCHON*. Le serveur DNS va donc lui renvoyer son adresse IP.
3. Le client va soit créer une nouvelle entrée, soit mettre à jour son adresse IP sur le serveur autoritaire.
4. Si le serveur accepte la demande du client, il va mettre à jour l’adresse IP de celui-ci.
5. – 8. Dans une deuxième partie (les quatre derniers paquets), le client effectue une requête inverse pour mettre à jour la zone inverse qui lui fait autoriter. Le principe est le même que pour une requête directe.

Le DNS dynamique réduit beaucoup **l’administration** du serveur DNS. En effet, chaque client Windows 2000 est capable de s’enregistrer dans le DNS automatiquement au démarrage (→ § 5.2).

Ce système fonctionne aussi bien avec des adresses IP statiques, qu'avec des adresses IP dynamiques dont l'attribution se fait grâce à un serveur DHCP (*Dynamic Host Configuration Protocol*).

Il existe deux types de mise à jour dynamique :

- ***Dynamic Update*** : Cette mise à jour peut être effectuée par **n'importe qui**. Chaque client possède une option par défaut qui effectue cette mise à jour (→ Kerberos, Annexe 1 § 2).
- ***Secure Dynamic Update*** : Les zones intégrées à Active Directory (→ § 7.2.4) peuvent être configurées pour effectuer une mise à jour sécurisée. Les listes de contrôles d'accès permettent de spécifier qui a le droit de mettre à jour le DNS. La mise à jour sécurisée est basée sur l'algorithme *GSS Algorithm for TSIG*. Cet algorithme est basé sur l'interface GSS-API (*Generic Security Service Application Program Interface*).

7.2.4 Zone de recherche

Le service DNS offre la possibilité de partager l'espace de noms en une ou plusieurs zones. L'espace de noms DNS représente la structure logique des ressources de votre réseau et les zones DNS fournissent une structure de stockage physique pour ces ressources.

Zone de recherche directe

Une zone de recherche directe permet les requêtes de recherche directe, qui font correspondre une adresse IP à un nom.

Si l'installation du serveur DNS s'effectue en même temps qu'Active Directory, une zone de recherche directe (intégrée à Active Directory) correspondant au nom est automatiquement créée.

Trois types de zone sont disponibles :

- ***Active Directory-integrated*** : Ce type de zone correspond à une copie maître d'une nouvelle zone. Elle utilise Active Directory pour stocker les fichiers de zones. L'administration s'effectue de manière automatique si les clients du domaine ont activé l'option *Register this connection's addresses in DNS* (→ Kerberos, Annexe 1 § 2).
Ce type de zone gère les listes de **contrôles d'accès** (ACL – *Access Control List*) qui permettent de spécifier les utilisateurs ou les groupes autorisés à modifier ces zones intégrées.
- ***Standard primary*** : Cette zone est aussi une copie maître d'une nouvelle zone. Par contre, elle est stockée dans un fichier texte standard. L'administration ne s'effectue donc pas automatiquement.
- ***Standard secondary*** : Ce type de zone correspond à un répliqua en lecture seule d'une zone maître existante et stockée dans un fichier texte standard.

Zone de recherche inversée

Une zone de recherche inversée n'est pas créée automatiquement. Cette zone effectue le travail inverse de la zone de recherche directe, c'est-à-dire qu'à partir d'un nom, elle trouve l'adresse IP.

Ce type de zone est utilisé dans certain cas comme par exemple *nslookup*, ou **encore pour que le protocole Kerberos fonctionne correctement** (→ Kerberos § 4.2).

Les types de zones sont **identiques** aux zones de recherche directe.

7.2.5 Vulnérabilité : Transferts de zone DNS

L'espace de noms d'Active Directory s'appuie sur DNS. Le serveur DNS qui lui est associé est donc une source majeure de renseignements. Par défaut, on peut effectuer des transferts de zone vers n'importe quel hôte distant.

Par exemple, grâce à l'utilitaire *nslookup*, un simple transfert de zone peut recenser une foule d'informations réseau intéressantes.

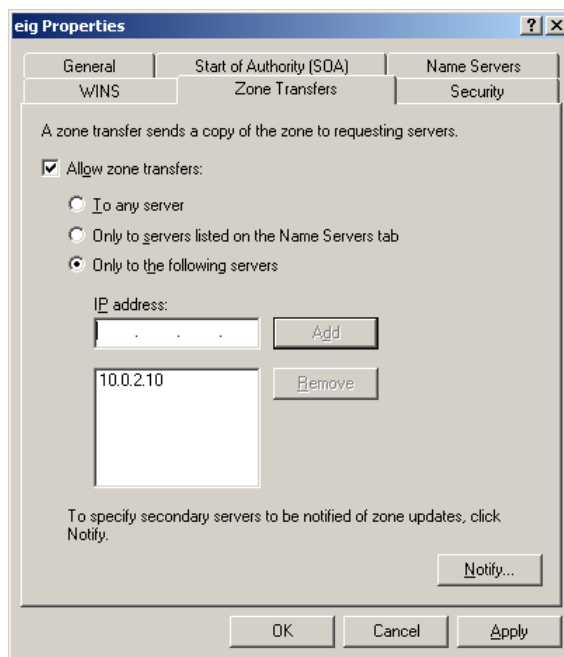
```
C:\>nslookup
Default Server: dc1.eig
Address: 10.0.1.10

> ls -d eig
[dc1.eig_souchon]
eig.          SOA   dc1.eig admin. (35 900 600 86400 3600)
eig.          A     10.0.1.10
eig.          NS    dc1.eig
...
_gc._tcp      SRV   priority=0, weight=100, port=3268, dc1.eig
_kerberos._tcp SRV   priority=0, weight=100, port=88, dc1.eig
_kpasswd._tcp SRV   priority=0, weight=100, port=464, dc1.eig
_ldap._tcp    SRV   priority=0, weight=100, port=389, dc1.eig
_kerberos._udp SRV   priority=0, weight=100, port=88, dc1.eig
_kpasswd._udp SRV   priority=0, weight=100, port=464, dc1.eig
C1            A     10.0.1.12
dc1           A     10.0.1.10
S1            A     10.0.1.11
eig.          SOA   dc1.eig admin. (35 900 600 86400 3600)
> exit
```

Pour bloquer ces transferts de zone DNS, il faut exécuter **Start – Programs – Administrative Tools – DNS**.

Cliquez ensuite sur chaque zone et affichez ces *Properties*, onglet *Zone Transfers* (figure 7.4).

FIGURE 7.4 : TRANSFERT DE ZONE DNS



Par défaut, Windows 2000 est configuré de façon à autoriser les transferts de zone vers n'importe quel serveur. Pour désactiver cela, choisissez l'option *Only to the following servers* et entrez l'adresse IP des serveurs autorisés à faire cela.

Source : Osman Eyrolles Multimedia – **Halte aux Hackers (Deuxième Edition)**

- Chapitre 6, Transferts de zone DNS

7.3 SCÉNARIO 1 : DNS

7.3.1 Principe

La configuration DNS des deux serveurs DNS (*DNS1* et *DNS2*) est essentielle pour qu'Active Directory fonctionne correctement.

Cette section explique en détail la configuration du DNS pour **le premier domaine**, car la configuration est identique pour le deuxième domaine.

Chaque serveur DNS gère **deux zones primaires** et possèdent **deux zones secondaires**.

<i>DNS1</i>	Zone primaire	Zone secondaire
Zone de recherche directe	eig	eivd
Zone de recherche inversée	10.0.1.0	10.0.2.0

<i>DNS2</i>	Zone primaire	Zone secondaire
Zone de recherche directe	eivd	eig
Zone de recherche inversée	10.0.2.0	10.0.1.0

Il est important que *DNS1* gère ces deux zones primaires et connaisse les deux zones de *DNS2* (zones secondaires). Cela permet au *DNS1* de ne pas aller interroger *DNS2* lorsqu'il ne connaît pas la réponse.

On parle de **réplication de zones DNS** lorsque deux serveurs DNS s'échangent leurs zones DNS.

Une fois que les zones primaires de *DNS2* sont stockées sur *DNS1*, il n'y a plus de trafic DNS entre les deux domaines, sauf lorsqu'il y a une **modification** sur une des zones primaires.

7.3.2 Ports utilisés

Pour que les deux serveurs DNS puissent s'échanger leurs zones (réplication), il faut spécifier sur les routeurs *Lightning* les ports utilisés. Les serveurs DNS utilisent les ports **UDP 53** et **TCP 53**. L'annexe 7 explique comment configurer ces ports.

7.3.3 Configuration

Commencez par créer les **deux zones primaires** sur chaque serveur DNS, et dans un deuxième temps, les **deux zones secondaires**.

L'annexe 4 décrit en détail la configuration des serveurs lorsqu'Active Directory n'est pas encore installé.

A ce niveau, pour être sûr que la configuration fonctionne correctement, effectuez des tests à l'aide des commandes *ping*, et *nslookup* qui permet d'interroger directement les serveurs DNS.

Ne pas oublier de changer le type des deux zones (directes et inverses) sur les deux serveurs DNS de chaque domaine lorsqu'Active Directory sera installé. **Il est recommandé de les intégrer à Active Directory.**

7.4 SCÉNARIO 2 : TRUST

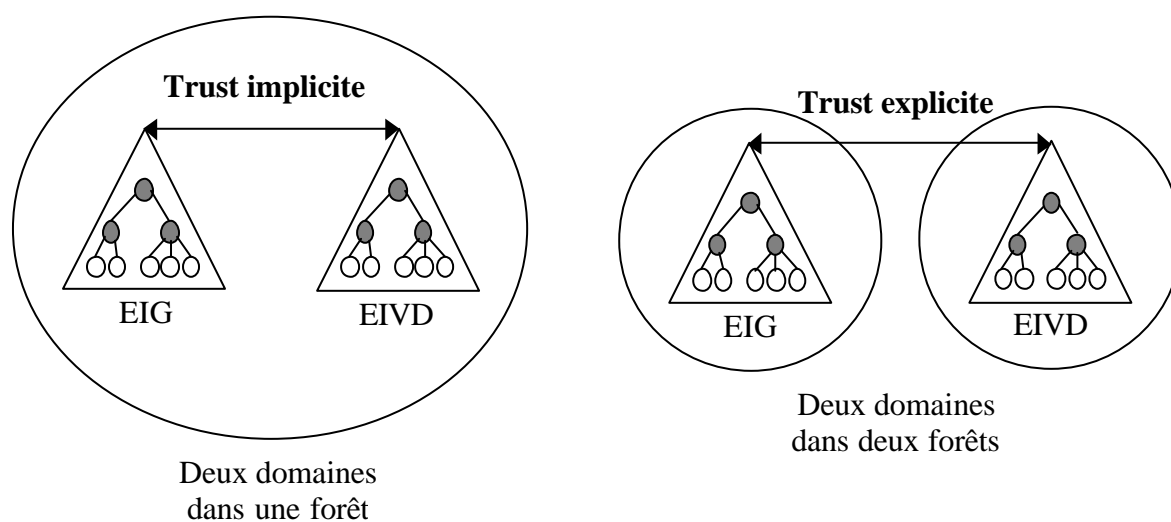
7.4.1 Principe

Le *trust* permet aux utilisateurs de s'authentifier depuis n'importe quel ordinateur sur un des deux domaines.

Par exemple, lorsqu'un utilisateur de l'EIG se déplace à l'EIVD, il pourra s'authentifier avec son compte d'utilisateur sur le domaine *EIVD*.

Contrairement à l'étape 2 où le *trust* est effectué d'une manière automatique (***trust implicite***) lorsqu'on ajoute le deuxième contrôleur de domaine, dans cette étape il faut établir le *trust* d'une manière manuelle (***trust explicite***). La figure 7.5 illustre ces types de *trust*.

FIGURE 7.5 : TRUST



7.4.2 Ports utilisés

Comme pour le DNS, il faut configurer les routeurs *Lightning* pour qu'ils acceptent le *trust*. Le *trust* utilise les ports **UDP 389** (LDAP – *Lightweight Directory Access Protocol*) et **TCP 445** (SMB – *Server Message Block*). L'annexe 7 explique comment configurer ces ports sur les routeurs *Lightning*.

7.4.3 Configuration

La configuration du *trust* s'effectue dans un sens à la fois. Elle est décrite en détail dans l'annexe 5.

7.5 SCÉNARIO 3 : RÉPERTOIRE CONFIDENTIEL

7.5.1 Principe

Ce scénario rappelle les différents objets à créer ainsi que les autorisations à appliquer et introduit la notion de **propriétaire**.

- Contrôleurs de domaine (*DC1* et *DC2*) : créez les mêmes comptes d'utilisateurs, groupes d'utilisateurs et répertoires partagés comme expliqués dans l'étape 1 (→ § 5).
- Serveurs de fichiers (*S1* et *S2*) : partagez les répertoires et créez les groupes locaux (AGDLP) correspondants (→ § 5.4.2).

Sur chaque serveur de fichiers, un nouveau répertoire est partagé. Par exemple, ce répertoire peut contenir les notes des étudiants dans des fichiers Excel. On parle alors de **répertoire confidentiel**, car à part les professeurs, **personne** (même les administrateurs) ne doit avoir accès à ce répertoire.

Pour que cela soit possible, il faut qu'un administrateur crée un répertoire et change le propriétaire de ce répertoire. En changeant de propriétaire, l'administrateur donne les pleins pouvoirs à ce nouveau propriétaire (dans notre cas, le groupe *professeurs*). Il est alors possible d'interdire l'accès à l'administrateur.

7.5.2 Ports utilisés

Par exemple, lorsqu'on désire ajouter des groupes globaux du domaine *EIVD* aux groupes locaux sur le serveur de fichiers *S1* et utiliser la ressource partagée correspondante, les trois ports suivants doivent être ouverts :

- **TCP 135** (MSRPC) : Ce port est utilisé pour localiser les groupes globaux.
- **TCP 389** (LDAP) : *S1* utilise ce port interroger *DC2*.
- **TCP 1027** (MSRPC) : Ce port est utilisé pour ajouter les groupes globaux du domaine *EIVD* dans les groupes locaux de *S1*.

La configuration de ces ports est décrite dans l'annexe 7.

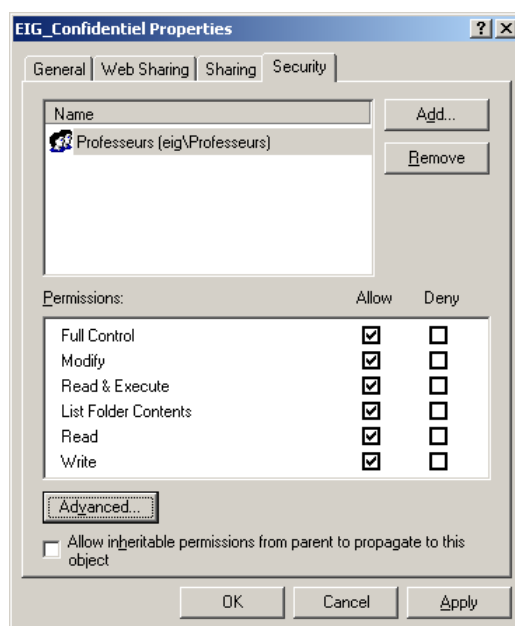
7.5.3 Configuration

Pour modifier le **propriétaire** (*owner*) d'un répertoire, il faut afficher les **Propriétés** du répertoire et cliquer sur l'onglet **Security**.

1. Désactivez l'option **Allow inheritable permissions from parent to propagate to this object** qui permet d'annuler la propagation des autorisations parentes.
2. Supprimez le compte ou le groupe d'utilisateurs qui possède toutes les autorisations grâce à **Remove**.

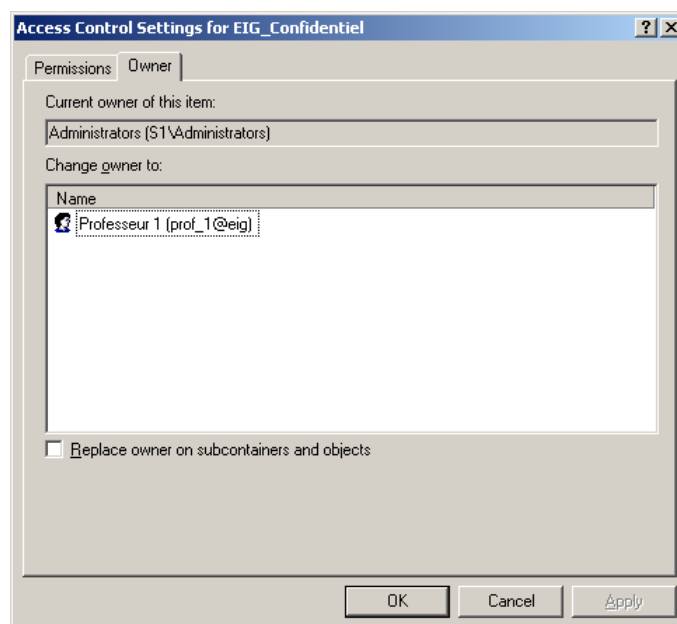
3. Ajoutez un nouvel utilisateur ou nouveau groupe avec toutes les autorisations (dans notre cas le groupe **Professeurs**). La figure 7.6 illustre cela.

FIGURE 7.6 : CHANGEMENT DE PROPRIÉTAIRE



4. Appuyez sur **Apply**. Essayez d'accéder au répertoire avec l'administrateur, le système retourne **Access is denied**.
5. En s'authentifiant avec un utilisateur (**prof_1**) faisant parti du groupe **Professeurs**, on s'aperçoit que le propriétaire (**owner**) du répertoire a changé (figure 7.7).

FIGURE 7.7 : NOUVEAU PROPRIÉTAIRE



8 ETAPE 4 : AUTHENTIFICATION SUR UN SERVEUR WEB

8.1 OBJECTIFS

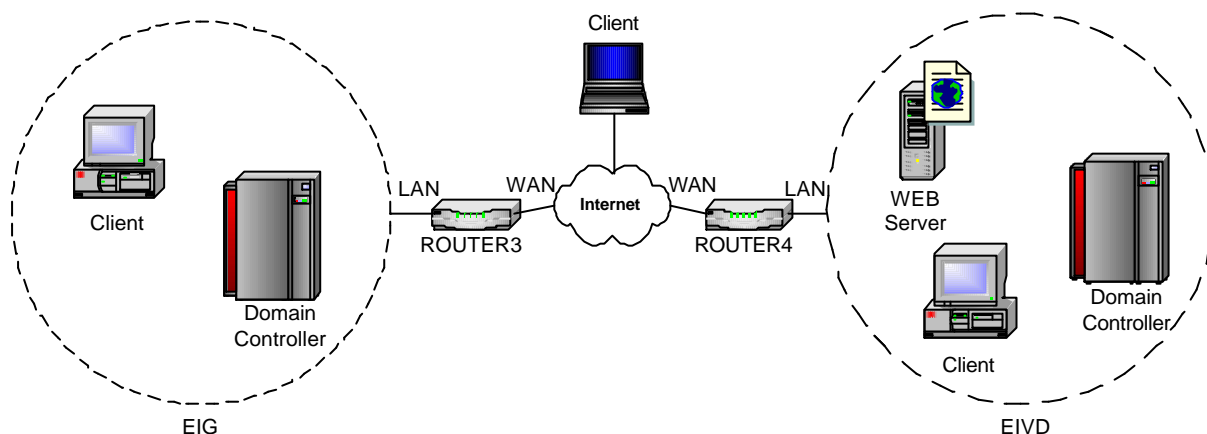
L'objectif de ce scénario est d'accéder depuis internet à un serveur WEB se trouvant en interne dans le domaine de l'EIVD.

Le serveur WEB utilise Active Directory pour authentifier les utilisateurs.

- Deux domaines avec deux contrôleurs de domaine (*DC1, DC2*)
- Un serveur WEB IIS 5.0 (*S2*)
- Deux clients (*C1, C2*)
- Deux routeurs Lightning Ethernet II (*ROUTER3, ROUTER4*)
- Deux zones d'adressages privées de classe C

8.1.1 Structure physique

Le schéma illustre la mise en œuvre du réseau décrit ci-dessus :



La configuration IP des ordinateurs et des routeurs Lightning est identique à celle de l'étape 3 (→ 7.1.1) avec en plus un **client externe** supplémentaire.

	Cext
IP Address	129.194.187.47
Subnet Mask	255.255.252.0
Gateway	129.194.184.3
DNS Server	129.194.4.6
Operating System	Windows 2000 Professional

8.1.2 Structure logique

La structure logique est identique à celle de l'étape 3 (→ 7.1.2).

8.2 SCÉNARIO 1 : SERVEUR WEB IIS 5.0

8.2.1 Principe

Le serveur WEB utilisé est celui livré avec Windows 2000 Professional, IIS 5.0 (*Internet Information Services*). Son FQDN est **www.eivd**.

Le serveur WEB doit être atteint de trois manières différentes :

- **Depuis le domaine *EIVD*** : le serveur WEB est accessible directement, car il se trouve dans le même domaine (ordinateur membre du domaine *EIVD*).
- **Depuis le domaine *EIG*** : Il faut configurer *ROUTER3* pour autoriser les ordinateurs du domaine *EIG* à y accéder (ordinateur membre du domaine *EIG*). De plus, *ROUTER4* doit autoriser les accès sur le port 80 de *S2*.
- **Depuis internet** : les clients externes doivent obligatoirement connaître l'interface externe de *ROUTER4* (129.194.186.207) pour y accéder. En effet, cette adresse IP n'est pas enregistrée dans un DNS externe. Par contre, il est possible de rajouter la ligne suivante dans le fichier `\WINNT\system32\drivers\etc\hosts` :

129.194.186.207 www.eivd

Lorsqu'un FQDN est tapé, l'ordinateur regarde d'abord dans ce fichier pour voir si l'adresse IP correspondante est présente, sinon il interroge le serveur DNS spécifié.

8.2.2 Authentification intégrée de Windows

Toute personne qui désire accéder au serveur WEB doit **s'authentifier**.

L'authentification choisie est ***Integrated Windows authentication***. C'est une méthode d'authentification sécurisée car le nom d'utilisateur et le mot de passe ne sont pas transmis en clair via le réseau. Le mot de passe est transmis en utilisant **une fonction de hachage**.

Ce type d'authentification peut utiliser **deux protocoles d'authentification** :

- **Kerberos v5** : protocole décrit dans le chapitre § 4.
- **NTLM** : ancien protocole propriétaire de Microsoft utilisé par les pre-Windows 2000 (→ Annexe 1).

Les trois manières d'accéder au serveur n'utilisent pas le même protocole d'authentification.

Le navigateur doit être **Internet Explorer 5.0 ou supérieur** pour que ce type d'authentification fonctionne.

8.2.3 Différentes variantes d'accès à un serveur WEB

L'étude comprend six variantes différentes pour accéder au serveur WEB :

1. Accès avec **etudiant_3** depuis le domaine *EIVD* en utilisant **IE 5.0**
2. Accès avec **etudiant_3** depuis le domaine *EIVD* en utilisant **IE 6.0**
3. Accès avec **etudiant_1** depuis le domaine *EIG* en utilisant **IE 5.0**
4. Accès avec **etudiant_3** depuis le domaine *EIG* en utilisant **IE 5.0**
5. Accès avec **etudiant_3** depuis internet en utilisant **IE 5.0**
6. Accès avec **etudiant_3** depuis internet en utilisant **IE 6.0**

Ces variantes sont illustrées sous forme de diagramme en flèches dans l'annexe 8. De plus, les différentes analyses de protocole faite avec **Ethereal** sont disponibles dans l'annexe 11.

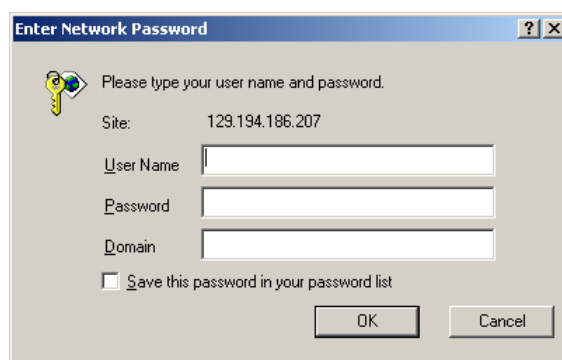
On peut remarquer **plusieurs choses** :

- *Negotiate / NTLM* : le deuxième paquet venant du serveur WEB propose au client **deux méthodes d'authentification** qui ne fonctionnent qu'avec *Internet Explorer 5.0* ou plus.
Negotiate négocie le protocole d'authentification (Kerberos ou NTLM) et *NTLM* utilise que le protocole NTLM.
- *KRB_Error* : lorsqu'on utilise *Internet Explorer 5.0* depuis l'un des deux domaines, Internet Explorer essaie d'obtenir un ticket pour accéder au serveur WEB grâce au protocole Kerberos. Le KDC lui renvoie **une erreur** *KRB5KDC_ERR_S_PRINCIPAL_UNKNOWN* qui signifie qu'il ne trouve pas le service demandé (dans notre cas HTTP). A part quelques informations trouvées sur les *newsgroups*, rien de très concret.
- *RPC Client / RPC Server* : ces deux paquets sont échangés entre le serveur WEB et le contrôleur de domaine qui possède l'utilisateur. Le serveur WEB va vérifier si le mot de passe que l'utilisateur a rentré (figure 8.1) est correct. Ces deux paquets sont **chiffrés** par le protocole NTLM.
- *Etudiant_1* ou *Etudiant_3* : le choix du contrôleur de domaine est **dépendant** du compte utilisateur. Par exemple, **etudiant_1** est géré par *DC1*, c'est donc lui qui va comparer si le mot de passe entré par l'utilisateur correspond au mot de passe dans Active Directory.
- *Internet Explorer 6.0* : lorsqu'on utilise cette version, le navigateur n'essaie plus d'obtenir des tickets au près du KDC grâce au protocole Kerberos. Il utilise **directement le protocole NTLM**.
- *Cext* : qu'on utilise *Internet Explorer 5.0* ou *6.0* depuis **internet**, seul le protocole NTLM est utilisé. En effet, **comme l'ordinateur ne fait pas parti d'un des domaines**, le protocole Kerberos ne peut pas être utilisé.

Remarques

- L'utilisateur **etudiant_1** provient du domaine *EIG*, alors que **etudiant_3** du domaine *EIVD*.
- Le navigateur affiche la fenêtre suivante (figure 8.1) lorsque le serveur WEB demande de s'authentifier.

FIGURE 8.1 : FENÊTRE D'AUTHENTIFICATION



Le champ **Domain** est obligatoire pour spécifier le domaine qui gère l'utilisateur.

8.2.4 Ports utilisés

Pour qu'on puisse accéder au serveur WEB, il faut spécifier sur *ROUTER4* le port **80**. De plus, il ne faut pas oublier d'ajouter une règle dans *Misc – NAT* sur *ROUTER3* pour le domaine *EIG* puisse accéder au serveur WEB :

Protocol :	tcp	Mapping :	mapto
Source :	10.0.1.0/24	To address :	129.194.186.207
Source Port :	any	To port :	http
Destination :	10.0.2.11/32	Type :	destination
Destination Port :	http		

Cette règle permet aux paquets venant de 10.0.1.0/24 (*EIG*) vers 10.0.2.11/32 (*www.eivd*) d'être envoyés vers 129.194.186.207. En effet, l'adresse de destination est redéfinie pour que les paquets arrivent sur l'interface externe du routeur de *EIVD*.

8.2.5 Configuration

La configuration est relativement simple :

1. Installez le serveur IIS 5.0 sur *S2*. Dans *My Computer – Control Panel – Add/Remove Programs – Add/Remove Windows Components*, cochez la case *Internet Information Services (IIS)*.
2. Lorsque le serveur WEB est installé, la première chose est d'appliquer le **patch** contre le virus **Nimda**. La référence de Microsoft est **Q301625**.

3. Grâce à la console MMC (*Snap-in : Internet Information Services*), dans *Default Web Site – Properties – onglet Directory Security*, cliquez sur *Edit...* de la partie *Anonymous access and authentication control*.
4. Désactivez *Anonymous access* et activez *Integrated Windows authentication*.
5. Dans *Forward Lookup Zones* du serveur *DNS2*, rajoutez dans la zone **eivd** un nouveau alias avec *NewAlias...* **www** qui pointe sur **s2.eivd**.

9 PROBLÈMES GÉNÉRAUX RENCONTRÉS

9.1 PARTAGE DE FICHIERS ET D'IMPRIMANTES SOUS WINDOWS 2000 SERVER

Après avoir installé et configuré Active Directory, il faut faire attention à **ne pas désactiver *File and Printer Sharing for Microsoft Networks*** dans la configuration de la carte réseau. Sinon, il est impossible d'ajouter des ordinateurs dans le domaine.

9.2 LOCALISATION DU CONTRÔLEUR DE DOMAINE

Sous Windows 2000, les noms des domaines sont des noms DNS. C'est pour cela qu'il faut **ne pas omettre de configurer sur chaque poste client le serveur DNS du domaine** (dans notre cas, le serveur DNS est installé sur le contrôleur de domaine, mais il peut très bien être sur un autre serveur).

Grâce au serveur DNS, le client peut ainsi obtenir les informations dont il a besoin pour localiser le contrôleur de domaine.

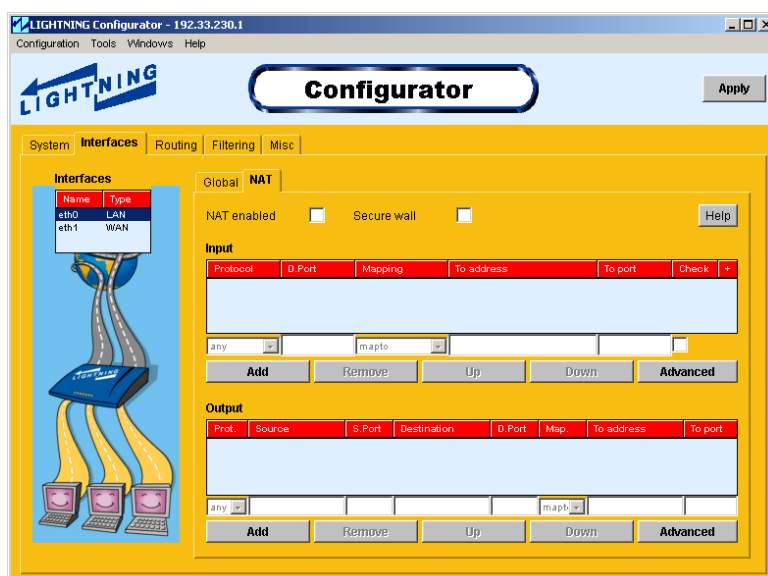
Le même problème se pose au moment où l'on **ajoute un deuxième contrôleur de domaine** (soit dans l'arbre de domaine, soit dans la forêt de domaine). En effet, le deuxième contrôleur de domaine doit aussi localiser le premier contrôleur de domaine soit pour joindre l'arbre de domaine, soit pour faire parti de la même forêt.

9.3 FONCTION NAT ACTIVÉE PAR DÉFAUT SUR LE ROUTEUR LIGHTNING

Il faut faire attention à désactiver l'option NAT dans la configuration du routeur Lightning (*firmware 3.0.1b*). En effet, cette option est activée par défaut lors du démarrage du routeur.

Elle est visible en utilisant l'utilitaire (**Ethernet II Configurator**) de Lightning livré avec le routeur dans l'onglet **Interfaces – NAT – NAT enabled**.

FIGURE 9.1 : LIGHTNING CONFIGURATOR



9.4 IMPOSSIBLE D'ANALYSER LE TRAFIC DES ROUTEURS <i>LIGHTNING</i>

L'ensemble des ordinateurs utilisés possède une carte réseau 10/100 Mbits et sont connectés sur un *hub* 10/100 Mbits.

Les routeurs *Lightning* possèdent deux interfaces, une à 10/100 Mbits (LAN) et l'autre à 10 Mbits (WAN).

Pour analyser le trafic des routeurs *Lightning*, **il faut que le driver la carte réseau de l'ordinateur en question travaille uniquement à 10 Mbits**. Pour une raison inconnue, le *hub* ne reproduit pas le trafic à 10 Mbits sur les interfaces à 100 Mbits.

10 CONCLUSION

Ce système d'exploitation est sorti le 25 août 1999 aux Etats-Unis. Aujourd'hui, deux *Service Pack* importants sont disponibles.

Le système est généralement stable. Durant ces trois mois, il n'a planté que une ou deux fois.

Au niveau protocole, Windows 2000 possède un grand avantage sur ses prédécesseurs car il utilise le protocole **DNS** pour localiser les différents ordinateurs d'un réseau. De plus, le protocole *NetBIOS* peut être désactivé, ce qui permet de réduire les *broadcasts*.

Un grand effort a été fait dans la sécurité. Windows 2000 utilise en standard le protocole **Kerberos** qui permet de chiffrer toutes les authentifications effectuées par les utilisateurs. Kerberos permet la mise en œuvre de **relations d'approbations** entre différents domaines. Par contre, l'interopérabilité avec d'autres systèmes est contestée car Windows 2000 utilise un champ supplémentaire pour transporter les SID qui n'est pas pris en compte dans l'implémentation standard de Kerberos.

Toutes les informations du réseau sont stockées dans un annuaire centralisé appelé **Active Directory**. Active Directory facilite la recherche et l'administration des ressources présentes dans un réseau.

L'**audit** fait partie de la sécurité de Windows 2000. Il permet d'enregistrer tout ce qui se passe sur un réseau du changement d'attributs jusqu'aux modifications d'autorisations.

La **réplication** est un élément essentiel lorsque Windows 2000 est utilisé dans plusieurs domaines. Elle permet de diminuer le trafic entre les domaines, car elle peut aller jusqu'à répliquer un simple attribut.

Beaucoup de particuliers utilisent Windows 2000, par contre peu d'entreprises ont migrés leur parc informatique sous Windows 2000. Il faudra, je pense, encore attendre un peu pour que le système possède un niveau de maturité plus important. La sortie prochaine du *Service Pack 3* devrait favoriser cela.

Sur le plan personnel, ce travail m'a permis de beaucoup mieux connaître Windows 2000 dans son ensemble. La comparaison avec d'autres systèmes est maintenant beaucoup plus claire qu'au début de la 5^{ème} année.

Windows 2000 est très vaste et très complet, il est donc impossible de l'étudier en douze semaines. De plus, l'évolution des systèmes d'exploitation utilisés pour des réseaux va très vite.

Le nouveau système de Microsoft, Windows XP, est déjà sorti alors que Windows 2000 commence à percer dans les grandes entreprises.

Pour finir, je dirais que Windows 2000 est une grande évolution dans les systèmes d'exploitation dédiés aux réseaux informatiques.

Yann Souchon