Administration des Systèmes et des Réseaux

- Partie Windows -

ESIAL 1A

Samson BISARO – 14 Mai 2008 -

Plan

- Historique de MS Windows
- Les systèmes de fichiers
- Notions de bases de Windows 2000
- La base des registres
- Adressage IP
- Serveur DNS
- Active Directory

Plan

- Historique de MS Windows
- Les systèmes de fichiers
- Notions de bases de Windows 2000
- La base des registres
- Adressage IP
- Serveur DNS
- Active Directory

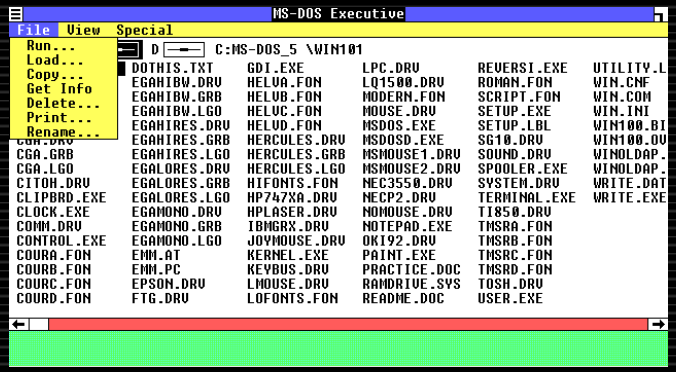
Historique de Windows

- **1984 : GEM** (Graphic Environment Manager)

Digital Research a été le premier à sortir en masse un environnement graphique pour PC. Il fera le succès des Atari. La version 4 couleur était donnée avec certains Amstrad PC… Microsoft s'en inspirera pour la suite.

- **1985 : Windows 1.0**

Première version de Windows, concept d'applications fenêtrées déjà utilisé par la firme Apple pour son propre système. On y retrouve aussi le gestionnaire de fichier GEM et quelques accessoires (calculatrice, notepad…), rien de plus. Le multi tâche reste encore un concept… Cette première version n'a pratiquement aucun succès auprès du public.



Historique de Windows

- **1987 : Windows 2.0**

Version pourvue d'un peu plus de caractéristiques avec l'apparition d'icônes, et de fenêtres superposables.
Système de développement viable (Excel, Word).
Version renommée plus tard Windows/286.

- **1990 : Windows 3.0**

Amélioration de l'interface graphique, support de 16 couleurs, capacité d'adressage mémoire de plus de 640K. Les éditeurs commencent a développer des applications pour Windows. Premier succès de Microsoft (+10 M ventes), Windows devient le système avec interface graphique le plus vendu dans l'histoire de l'informatique.

Historique de Windows

- **1992 : Windows 3.1 – 3.11**

Correction de nombreux bugs, support de polices True Type. le PC accueille les premiers composants multimédias. L'OLE (Object Linking and Embedding) fait son apparition permettant le partage de données entre application, ainsi que la fonction Redémarrage.

- **1992-1993 : Windows for Workgroups 3.1**

Windows pour Workgroups marque le début des ordinateurs en réseau sous Windows. Il permet de partager des fichiers et des imprimantes. Cette version est relativement stable par rapport à ces prédécesseurs. Entre autres innovations, le système d'exploitation supporte l'envoi de mail.

Historique de Windows

- **1994 : Windows NT 3.1 – NT 3.5**

Windows NT (New Technology) s'adresse au monde professionnel. Il intègre une architecture 32 bits, le multitâche préemptif, le support multi processeurs, supporte les toutes dernières technologies comme le Pentium, le TCP/IP, le format NTFS, et sécurise déjà le réseau.
OLE 2.0 augmente les performances et réduit les besoins mémoires.

- **1995 : Windows 95**

Révolution pour les utilisateurs. L'interface est complètement remaniée. Le plug and play fait son apparition. L'OSR2 de Windows 95 apporte un peu plus de stabilité à Windows. Même s'il n'est pas encore finalisé, on trouve de belles innovations avec le support des disques durs de grande capacité (FAT32) et surtout, il introduit les premiers éléments Internet.

Historique de Windows

- **1996 : Windows NT 4.0**

Interface de Windows 95, support d'Internet (IIS : Internet Information Server). Version beaucoup plus stable que la version NT 3.0 et plus performant, notamment au niveau de ses fonctionnalités réseau. Deux versions : Workstation & Server.
Apparition des Services Pack (6 au total, corrections de bugs, nouvelles fonctionnalités).

- **1998-1999 : Windows 98 – 98SE**

Version stable de Windows 95, intègre Internet, support de nouvelles technologies (DVD, USB, AGP, FireWire...) , outil de conversion du système de fichier de FAT16 en FAT32. La Seconde édition de Windows 98 n'est qu'une mise à jour des drivers et des applications comme Internet Explorer et Outlook Express. La correction des petites erreurs vient renforcer la stabilité du système. Le Dos est toujours présent.

Historique de Windows

- **2000 : Windows 2000 (NT 5.0)**

Windows 2000 a été longtemps repoussé car Microsoft voulait en faire l'outil d'une victoire définitive sur tous les systèmes concurrents, notamment Linux.
Perfectionnement des technologies réseaux, chiffrement des données dans NTFS, service d'annuaire (Active Directory), outils d'administration, amélioration de la sécurité...

- **2000 : Windows Millenium (ME)**

Millenium apporte de nouvelles fonctionnalités multimédia à Windows 98 en intégrant Windows Media Player et de nombreuses fonctions qui améliorent l'exploitation des données par les utilisateurs novices.
Version tournée vers le grand public.
Version de Windows comportant de nombreux bugs, très vite abandonnée.

Historique de Windows

- **2001 : Windows XP**

Fusion des versions NT et 9x, décliné en plusieurs versions (home, professional, server...), basé sur la stabilité de Windows 2000 et améliorant la simplicité d'accès aux données que l'on trouve dans Windows Me.

- **2003 : Windows Server 2003**

Evolution naturelle des serveurs Windows 2000, la famille Windows Server 2003 reprend les technologies déjà présentes dans Windows 2000 Server en les améliorant et en simplifiant la mise en œuvre.

- **2007 : Windows Vista**

Peu de recul à ce jour, mais avant de l'installer, acheter une grosse configuration ☹.

Plan

- Historique de MS Windows
- Les systèmes de fichiers
- Notions de bases de Windows 2000
- La base des registres
- Adressage IP
- Serveur DNS
- Active Directory

Les systèmes de fichiers

Généralités

Le système de fichiers d'un système a pour but d'**organiser les données** pour localiser les informations d'un disque dur.

Un disque dur est constitué de plusieurs plateaux circulaires tournant autour d'un axe. Les **pistes** (zones concentriques écrites de part et d'autre d'un plateau) sont divisées en quartiers appelés **secteurs** (d'une taille de 512 octets). Le formatage logique d'un disque permet de créer un système de fichiers sur le disque, qui va permettre à un système d'exploitation d'utiliser l'espace disque pour stocker et utiliser des fichiers. Le système de fichiers est basé sur la gestion des **clusters** (unité d'allocation, c'est-à-dire la plus petite unité de disque que le système d'exploitation est capable de gérer). Un cluster est constitué d'un ou plusieurs secteurs, plus la taille d'un cluster est importante, moins le système d'exploitation aura d'entités à gérer… Un fichier occupe un nombre entier de cluster, le gaspillage est d'autant plus grand qu'il y a de secteurs par cluster. On comprend alors toute l'importance du choix du système de fichiers.

Les systèmes de fichiers

- **Les types de systèmes de fichiers**

Système d'exploitation	Type de FS supporté
DOS	FAT16
Windows 95	FAT16
Windows 95 OSR2	FAT16, FAT32
Windows 98	FAT16, FAT32
Windows NT4	FAT, NTFS (version 4)
Windows 2000 / XP	FAT, FAT16, FAT32, NTFS (versions 4 et 5)

Les systèmes de fichiers

- **FAT16**

Le système **FAT** (File Allocation Table) a été conçu pour les partitions de faible capacité (< 500 Mo).

Pour des partitions de cet ordre de grandeur, FAT ne gaspille qu'une très faible quantité d'espace disque pour sa gestion interne.

Structure de la FAT très simple, mais absence de gestion de listes de contrôle d'accès (ACL) pour chaque fichier et chaque répertoire.

Le système FAT utilise une **table d'allocation de fichiers** :

index listant le contenu du disque pour mémoriser l'emplacement des fichiers.

Système 16 bits permettant un nom de fichiers de 8 caractères + 3 d'extension.

Le **VFAT** (Virtual FAT), système 32 bits, présent dès Windows 95, permet d'ôter cette limitation (255 caractères).

Taille maximale d'une partition FAT : 2 Go

Les systèmes de fichiers

- **FAT32**

Pour ôter la limitation de 2Go par partition de la FAT16, un nouveau système est apparu sous Windows 95 OSR2 : la **FAT32.**

Système 32 bits permettant l’allocation de 2 TO par partition, limités à 32 Go par MS pour favoriser l’utilisation de NTFS.

Les systèmes de fichiers

- **NTFS (New Technology File System)**

Permet une gestion de la sécurité local via les ACLS et de la casse des noms de fichiers, prend en charge la compression individuelle, permet la gestion des quotas disque (v5) , le cryptage de fichier par clé publique/clé privée.
NTFS intègre un mode transactionnel au niveau du système de fichiers : consistance des structures internes.

NTFS intègre un adressage 64 bits permettant un découpage plus fin des partitions en clusters : gain de place pour des fichiers de taille faible, taille accrue des partitions, pas de limitation du nombre de répertoire.

NTFS utilise une table appelée **MFT** (Master File Table) pour mémoriser les informations détaillées des fichiers (descripteur + journal).
Système journalisé.
La MFT représente une structure de stockage des données de la partition, et non une liste de clusters.

Plan

- Historique de MS Windows
- Les systèmes de fichiers
- Notions de bases de Windows 2000
- La base des registres
- Adressage IP
- Serveur DNS
- Active Directory

Notions de bases de Windows 2000

- **Système multitâches**

Capacité pour le système d'exploitation de gérer plusieurs programmes simultanément en attribuant tour à tour un pourcentage de temps CPU pour l'exécution des ces programmes : partage de la mémoire et des périphériques.

Deux implémentations du multitâche

- Multitâche **coopératif**

  Les programmes s'exécutent les uns après les autres selon l'ordre définit dans une file d'attente d'exécution. Chaque tâche dépend donc des autres.

  Problème : blocage d'une tâche : blocage des tâches suivantes, blocage du système possible.

  Implémentation présente dans les systèmes Windows 16 bits.

Notions de bases de Windows 2000

Deux implémentations du multitâche

- Multitâche **préemptif**

Chaque application dispose du CPU pendant un laps de temps prédéfini ou jusqu'à ce qu'une autre application ait une priorité plus importante.
Le système d'exploitation gère l'ordonnancement et l'attribution du temps CPU sans consultation des applications exécutées.

Si une application est bloquée alors libération de l'allocation du CPU prévue : pas de perte des autres applications ni blocage du système.

Notions de bases de Windows 2000

- **Le Multithreading**

Un thread est une unité d'exécution, un bout de programme (ou la totalité du programme si celui-ci ne propose pas le multithread).
Le multithreading est mis en œuvre lors du développement du programme.

A l'intérieur d'une même application, plusieurs tâches peuvent s'effectuer en pseudo-parallèle. (Ex : sous Word, correction orthographique et mise en forme en même temps que la saisi de texte.)

Notions de bases de Windows 2000

- **Le Multiprocessing**

Aptitude du système d'exploitation à utiliser les CPU présents dans la station de travail pour les faire travailler à la gestion du système Windows 2000 et à l'exécution des programmes.

Deux types de Multiprocessing :

- Multiprocessing Asymétrique (ASMP) : un CPU est réservé pour le système et les autres pour les applications.
- Multiprocessing Symétrique (SMP) : requête d'exécution du système et des applications réparties sur les différents CPUs. Quoi qu'il arrive, le système a toujours à disposition un pourcentage de temps CPU réservé.

Ces facultés sont grandement améliorées sous Windows 2000, il est même possible de lier un processus à un CPU donné via le gestionnaire de tâches.

Notions de bases de Windows 2000

- **Architecture de Windows 2000**

Système d'exploitation

- 32 bits
- Multitâches
- Multithread à architecture SMP

- Composé de systèmes d'exploitation en couches
- Systèmes client/serveur à base de micro-noyaux

Ces deux technologies ont permis de distinguer deux parties dans Windows 2000 : Le **mode exécutif** (mode noyau) et le **mode utilisateur** (mode applicatif)

Notions de bases de Windows 2000

- **Mode exécutif**

Le mode de l'exécutif regroupe l'ensemble des composants du système d'exploitation qui s'exécutent en mode noyau. Ces composants ou services

de l'exécutif sont prioritaires sur l'utilisation du CPU. Le noyau a une place prépondérante car il a à charge de fournir de la mémoire aux applications, de choisir les processus qui sont exécutés à un instant donné et de communiquer avec les périphériques. Les applications dépendent du noyau pour tous leurs besoins, ce qui évite qu'elles entrent en contact direct avec les périphériques, et ainsi provoquent une défaillance du système. Le noyau de Windows 2000 découle du noyau de NT4 avec des améliorations, comme la prise en charge de plusieurs sessions utilisateurs sur la même machine (Notion de Terminal Server), l'ajout de quotas de processeur pour les besoins d'Internet Information Server 5.

Notions de bases de Windows 2000

- **Mode exécutif (suite)**

Contrairement au noyau NT4, celui de 2000 prend en charge l'architecture WDM (Windows Driver Model). Il s'agit d'un nouveau modèle de pilote permettant d'utiliser les mêmes drivers sur 98 et sur 2000. L'architecture WDM permet l'exécution des applications en mode noyau, permettant ainsi une rapidité d'exécution.

Windows 2000 supporte également l'architecture EMA (Enterprise Memory Architecture) permettant ainsi l'allocation jusqu'à 32 Go de mémoire aux applications. (Intérêts pour les serveurs de BD par ex).

Le mode noyau est également doté d'un module Plug and PLay diminuant ainsi le temps de configuration du matériel. L'amélioration du noyau permet également à 2000 de fonctionner en clusters.

Notions de bases de Windows 2000

- **Mode utilisateur**

Le mode utilisateur regroupe les sous-systèmes protégés sur lesquels s'appuient les applications de l'utilisateur. Les processus en mode utilisateur n'ont pas d'accès directement aux matériels, ils sont limités à une zone mémoire affectée et sont traités avec un niveau de priorité bas.
Une des grandes évolutions du mode utilisateur est la présence dans le sous-système de sécurité d'Active Directory.

Plan

- Historique de MS Windows
- Les systèmes de fichiers
- Notions de bases de Windows 2000
- La base des registres
- Adressage IP
- Serveur DNS
- Active Directory

La base des registres

- **Fonctions de la base des registres**

Les fichiers du registre sont l'équivalent des fichiers de configuration win.ini, system.ini… que l'on retrouve sous Windows 3.x. A partir de Windows 9x, NT4 et 2000, la configuration du système, des logiciels et de l'environnement utilisateur est consignée dans le registre.

Ce registre est en fait constitué de deux fichiers : **user.dat** et **system.dat** Pour éditer ce registre, il faut utiliser l'outil **REGEDT32.EXE**.

L'éditeur de registre propose une vision arborescente de la configuration complète d'un poste.

Il intègre tous les paramètres du système :

- Composants du noyau
- Pilotes de périphériques
- Applications installées
- Profils utilisateurs
- Profils matériels
- Base des utilisateurs du système

La base des registres

Structure de la base des registres

Le contenu du registre est très variable d'un ordinateur à un autre mais on retrouve 6 « **clés** » principales :

- HKEY_CLASSES_ROOT (les classes et les objets)

  Arborescence contenant les paramètres les plus importants des programmes et gérant les extensions de nom de fichiers, la gestion de l'OLE « Object Linking and Embedding »

  (les liaisons avec les logiciels) et les serveurs ActiveX (composants utilisés en commun).

- HKEY_CURRENT_CONFIG (la configuration actuelle)

  Arborescence gérant les paramètres spécifiques au profil matériel courant tels que les pilotes de périphériques à charger et la résolution d'écran à adopter.

- HKEY_CURRENT_USER (paramètres de l'utilisateur)

  Arborescence gérant les paramètres spécifiques au profil utilisateur tels que les évènements système, apparences, couleurs...

La base des registres

- **Structure de la base des registres**

  - HKEY_LOCAL_MACHINE (l'équipement)

  Arborescence gérant les informations spécifiques à la machine telles que les profils utilisateurs, composants matériels, configuration réseau, paramètres de sécurité et système. Ces paramètres sont définis à l'installation du système et sont modifiés lors de changement dans la configuration.

  - HKEY_USERS (aperçu de tous les utilisateurs)

  Arborescence gérant les paramètres spécifiques aux utilisateurs.

  Décrit un environnement par défaut et contient une clé pour chaque utilisateur ayant ouvert une session.

  - HKEY_DYN_DATA (données dynamiques sous win2k)

  Arborescence gérant les données dynamiques chargées en RAM (usages répétés).

La base des registres

- **Problématique**

Le problème majeur de cette base de registre est que, suite à l'installation d'un programme, il se crée plusieurs clés dans divers endroits de la base de registre, or, à la désinstallation, les clés sont effacées (dans le meilleur des cas) mais l'arborescence reste.

Après installation et désinstallation de nombreux logiciels, le système ralentit.
Il faut au bout d'un certain temps réinstaller Windows ☹ ...

Plan

- Historique de MS Windows
- Les systèmes de fichiers
- Notions de bases de Windows 2000
- La base des registres
- Adressage IP
- Serveur DNS
- Active Directory

Adressage IP

- **L’adresse MAC**

Une **@MAC** (Medium Access Control) comporte 48 bits et est exprimée à l'aide de douze chiffres hexadécimaux. Le système hexadécimal est une façon abrégée de représenter les octets de huit bits qui sont stockés dans l'ordinateur. Il a été choisi comme identificateur, car il peut facilement représenter l'octet de huit bits à l'aide de deux symboles hexadécimaux.
Exemple : 00-B8-74-A3-51-F7

Les six premiers chiffres hexadécimaux, qui sont administrés par l'IEEE, identifient le fabricant ou le fournisseur et constituent donc l'identifiant unique d'organisation (OUI - Organizational Unique Identifier). Les six autres chiffres hexadécimaux forment le numéro de série d'interface ou une autre valeur administrée par le fournisseur. On dit parfois des adresses MAC qu'elles sont rémanentes (BIA - burned-in adresses) parce qu'elles demeurent en mémoire morte et sont copiées en mémoire vive lors de l'initialisation de la carte réseau.

Une @MAC est donc un identifiant physique unique pour toutes les cartes réseaux dans le monde. Elle est inscrite en usine de manière définitive dans la ROM.

Adressage IP

- **L’adresse IP dans le réseau TCP/IP**

Il existe deux versions d'**@IP** (Internet Protocol Adress) dans l'utilisation aujourd'hui. Presque tous les réseaux emploient l'adresse **IP version 4** (IPv4), mais un nombre croissant d'éducatif et les réseaux de recherches ont adopté l'adresse IP version 6 (IPv6).

L'adresse IP d'une machine est appelée une adresse logique.
Elle est **codée sur 32 bits soit 4 octets**. La notation consiste à indiquer chaque octet en décimal et à les séparer par des points “.”.
L’adresse IP d’un ordinateur est composée de deux parties :

La première partie est appelée **NetID**, correspond à **l’adresse du réseau**, aussi appelé **identifiant réseau**. L'identifiant réseau identifie les systèmes qui sont situés sur le même réseau physique. NetID doit être unique au segment local.

La deuxième partie est appelée **HostID**, correspond à **l’adresse de la machine sur le réseau**, aussi appelé **identifiant machine**. L'identifiant machine identifie un poste de travail, un serveur, un routeur, ou tout autre dispositif de TCP/IP dans un réseau. Le HostID pour chaque dispositif doit être unique à l'identifiant de réseau. Un ordinateur relié à un réseau de TCP/IP emploie le NetID et le HostID pour déterminer quels paquets il devrait recevoir ou ignorer et déterminer quels dispositifs doivent recevoir ses transmissions.

Adressage IP

- **L’adresse IP dans le réseau TCP/IP**

Exemple :

```
11000001  00110010  00101000  00011100
  193       50        40        28
```

193.50.40.28
NetID HostID

Chaque octet dans des chaînes d'une adresse IP est en valeur d'un minimum de 0 au maximum de 255. Le champ complet des adresses IP est de 0.0.0.0 à 255.255.255.255. Cela représente un total de 4.294.967.296 adresses IP possibles.

Adressage IP

Les classes d'adresses IP

Il y a 5 classes d'adresse IP, les **trois premières classes** (A, B et C) sont utilisées dans les réseaux standards.

Classe A :

1er octets : pour le réseau (NetID)

2,3, 4ème octets : pour les ordinateurs (HostID)

0XXXXXX1 -----> 01111110

L'adressage est de 1.0.0.1 à 126.255.255.254

L'adresse IP de classe A autorise 127 (2^7) réseaux de plus de 16 millions (2^{24}) de machines par réseau

Classe B :

1, 2ème octet : pour le réseau

3, 4ème octet : pour les ordinateurs

10XXXXXX -----> 10111111

L'adressage est de 128.0.0.1 à 191.255.255.254

L'adresse IP de classe B autorise 16384 (2^{14}) réseaux de plus de 65000 (2^{16}) de machines par réseau

Adressage IP

- **Les classes d’adresses IP**

Classe C :

1, 2, 3ème octet : pour le réseau

4ème octet : pour les machines

110XXXXX -----> 11011111

L'adressage est de 192.0.0.1 à 223.255.255.254

L'adresse IP de classe C autorise plus de 2 millions (2^{21}) de réseaux de 256 (2^{8}) machines par réseau

Classe D :

Cette classe d'adresse est réservée pour le multicast : la diffusion vers des machines d'un même groupe.

L'adressage est de 224.0.0.0 à 239.255.255.255

Le multicast est plutôt utilisé dans les réseaux de recherche. Il n'est pas utilisé dans le réseau normal.

Classe E :

Réservée pour le futur.

Elles ne devraient pas être employées sur des réseaux IP. Quelques organisations de recherche utilisent les adresses de la classe E pour des buts expérimentaux.

Adressage IP

Les classes d’adresses IP

127.0.0.1 : l'adresse pour localhost (machine locale) est une adresse IP spéciale : **loopback**, adresse logicielle et non physique.

Il s’agit d’un circuit fermé dans lequel un paquet de données est dirigé vers la couche réseau de la machine. On peut donc communiquer par le biais de cette interface comme si on était connecté à un ordinateur distant.

Un certain nombre d’adresses IP sont réservées pour des réseaux locaux connectés à l'Internet. Elles ne doivent pas être utilisées sur l'Internet car ces adresses sont "non routées", les paquets d'un ordinateur possédant une adresse privée ne seront pas transmis aux autres ordinateurs.

Adresses Interdites :

De 10.0.0.0 à 10.255.255.255 : réservées pour les réseaux privés.

De 172.16.0.0 à 172.16.255.255 : réservées pour les réseaux privés.

De 192.168.0.0 à 192.168.255.255 : réservées pour les réseaux privés.

De 127.0.0.0 à 127.255.255.255 : réservées pour le Loopback + pilotes réseaux.

Adressage IP

Les masques de réseaux

Un masque de réseau ou NetMask permet de savoir si une machine fait partie ou non du réseau.

Pour chaque Classe IP, on définit un masque de réseau associé :

Classe A - **255.0.0.0** (11111111.00000000.00000000.00000000)
Classe B - **255.255.0.0** (11111111.11111111.00000000.00000000)
Classe C - **255.255.255.0** (11111111.11111111.11111111.00000000)

La passerelle

Une passerelle ou Gateway est un équipement (machine, routeur) permettant à deux réseaux différents de communiquer. Certaines passerelles sont bidirectionnelles, d'autres unidirectionnelles.

Plan

- Historique de MS Windows
- Les systèmes de fichiers
- Notions de bases de Windows 2000
- La base des registres
- Adressage IP
- Serveur DNS
- Active Directory

Le serveur DNS

Généralités

TCP/IP permet d'associer des noms en langage courant aux adresses numériques grâce à un système appelé **DNS** (*Domain Name Service*).

On appelle **résolution de noms de domaines** (ou *résolution d'adresses*) la corrélation entre les adresses IP et le nom de domaine associé.

Ce système consiste en une hiérarchie de noms permettant de garantir l'unicité d'un nom dans une structure arborescente.

On appelle **nom de domaine**, le nom à deux composantes, dont la première est un nom correspondant au nom de l'organisation ou de l'entreprise, le second à la classification de domaine (.fr, .com, ...). Chaque machine d'un domaine est appelée **hôte**. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré (le serveur web d'un domaine porte généralement le nom *www*).

L'ensemble constitué du nom d'hôte, d'un point, puis du nom de domaine est appelé **adresse FQDN** (Fully Qualified Domain Name, soit Nom de Domaine Totalement Qualifié). Cette adresse permet de repérer de façon unique une machine.

Le serveur DNS

Généralités

Les machines appelées **serveurs de nom de domaine** permettent d'établir la correspondance entre le nom de domaine et l'adresse IP sur les machines d'un réseau. Chaque domaine possède ainsi, un serveur de noms de domaines, relié à un serveur de nom de domaine de plus haut niveau. Ainsi, le système de nom est une architecture distribuée, c'est-à-dire qu'il n'existe pas d'organisme ayant à charge l'ensemble des noms de domaines. Par contre, il existe un organisme (l'InterNIC pour les noms de domaine en .com,.net,.org et .edu par exemple). Le système de *noms de domaine* est transparent pour l'utilisateur.

Chaque ordinateur doit être configuré avec l'adresse d'une machine capable de transformer n'importe quel nom en une adresse IP. Cette machine est appelée Domain Name Server.

L'adresse IP d'un second Domain Name Server (secondary Domain Name Server) peut également être introduite: il peut relayer le premier en cas de panne.

Le serveur DNS

Généralités

Le serveur DNS de Windows 2000 supporte la mise à jour dynamique des enregistrements, soit par le client Windows 2000 lui-même, soit par le serveur DHCP lorsque le poste est client DHCP. D'où un gain de temps pour l'administrateur et le fait d'avoir une base DNS toujours à jour.

Le serveur DNS de Windows 2000 supporte également les enregistrements de type **SVR**. Ces derniers sont utilisés lorsqu'un client a besoin de localiser un serveur jouant un rôle précis. Chaque machine enregistre donc automatiquement, en plus de son nom d'hôte, la liste des rôles qu'elle joue.

Ex : un client désirant faire une recherche dans Active Directory va d'abord localiser un serveur LDAP auprès de son serveur DNS.

Le serveur DNS est également amélioré d'un point de vue **transfert de zone** : les zones DNS peuvent notamment s'intégrer à Active Directory.

Plan

- Historique de MS Windows
- Les systèmes de fichiers
- Notions de bases de Windows 2000
- La base des registres
- Adressage IP
- Serveur DNS
- Active Directory

Active Directory

- **Service d'annuaire**

Le rôle de la base d'annuaire d'Active Directory est de fournir des services, d'informer et de localiser des objets.

Fonctionnalités :

La base de données appelée **base d'annuaire** contient des **objets**. Les objets peuvent être des comptes utilisateurs, des groupes, des ordinateurs, des ressources (imprimantes, dossiers, applications)… Les domaines, les sites, les unités d'organisation (OU), et les stratégies de sécurité sont aussi considérés comme objets.

Active directory propose des fonctionnalités du Service d'annuaire au niveau des ressources réseau : permet de stocker, organiser, gérer et contrôler les objets.

Les objets permettent de réaliser une vue hiérarchique logique.

Un utilisateur peut accéder à une ressource via le réseau de façon transparente sans se soucier de la structure physique où la ressource est localisée.

Active Directory

- **Service d'annuaire**

Active Directory permet une administration centralisée et simplifiée, offrant une forte tolérance de pannes puisqu'il s'agit d'une **base d'annuaire distribuée**.

Toute modification d'annuaire est automatiquement copiée sur tous les contrôleurs de domaine d'un domaine (ex : AD-UHP). Ceci est possible grâce à une **réplication multi-maître** : tous les contrôleurs de domaine d'une domaine participent à la réplication et stockent la base de données Active Directory complète de leur domaine.

Un annuaire simplifie la recherche : les utilisateurs accèdent facilement aux objets tandis que les administrateurs gèrent ces objets. Un mécanisme de recherche et d'index, basé sur le protocole **LDAP** permet facilement de localiser les ressources publiées. La partition de domaine contient la liste de tous les objets du domaine. Un **catalogue global** contient les informations nécessaires pour localiser rapidement un objet de l'annuaire.

Active Directory

- **Service d'annuaire**

Active Directory fournit l'intégration du **sous-système de sécurité**. L'utilisateur se connecte une seule fois au réseau et le processus d'authentification (Kerberos v5) s'effectue en arrière plan à chaque nouvelle demande d'accès aux ressources.

La **sécurité distribuée** de Windows 2000 s'appuie sur l'infrastructure PKI (Public Key Infrastructure) qui met en place la cryptographie par clé publique pour contrôler et authentifier les deux partenaires d'une requête.

Active Directory s'appuie sur le concept d'espace de nommage Internet et intègre une ensemble de protocoles standards (TCP/IP, DNS, DHCP, SNTP, LDAP, LDIF, KERBEROS v5, certificats) : **interopérabilité** des différents systèmes d'exploitation et fait de cette base d'annuaire un composant réseau sur lequel toutes les applications peuvent s'appuyer.

Active Directory

- **Structure logique**

Composants de la base d'annuaire d'Active Directory :

- Forêt
- Arbre(s)
- Objets
- Domaines
- Unités d'organisation

Active Directory

- **Structure logique**

Un **domaine** regroupe des ordinateurs, partage la même base d'annuaire et représente une unité de réplication, une limite de sécurité (stratégies de comptes) et une unité d'administration.

Une **unité d'organisation** (OU) est une organisation logique représentant une structure géographique ou une structure par services (ex, OU=ESIAL) regroupant les objets d'un domaine. C'est un **conteneur** utilisé pour organiser les objets du domaine (comptes utilisateurs, ordinateurs, groupes, ressources...).

Une OU permet la délégation de pouvoir, simplifient la sécurité (visibilité par OU) et définissent une stratégie (groupes d'utilisateurs).

Active Directory

- **Structure logique**

Un **arbre** regroupe un ou plusieurs domaines Windows 2000 partageant un même espace de noms. Les noms de domaines correspondent à des noms DNS : le premier domaine créé est le **domaine racine** de la forêt.

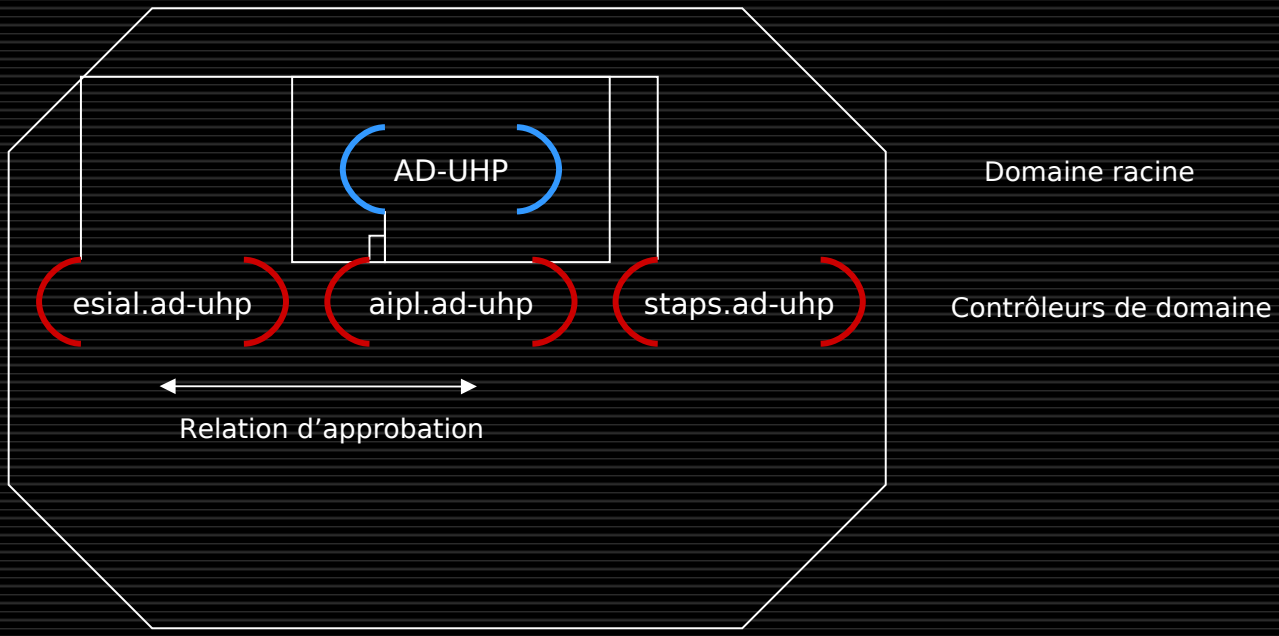
Lors de l'ajout d'un nouveau domaine à une arborescence, le nouveau domaine devient **domaine enfant** du domaine parent.

Une **forêt** est un ensemble d'une ou plusieurs arborescences. Tous les domaines d'une forêt partagent une configuration, un schéma et un catalogue global commun.

Les domaines d'une forêt sont reliés entre eux hiérarchiquement par des **relations d'approbation bidirectionnelles transitives**.

Active Directory

- **Structure logique**



Active Directory

- **Structure physique**

La structure logique permet d'organiser les objets et ressources réseau tandis que la structure physique est essentielle pour configurer et gérer le trafic réseau. Les **sites** et les **contrôleurs de domaine** sont les composants physiques de Active Directory. Leurs rôles est d'optimiser la réplication et les ouvertures de sessions ainsi que de localiser les objets.

Le contrôleur de domaine stocke la base d'annuaire et possède le service KDC (Key Distribution Center) distribuant les tickets d'accès aux services de réseau dans le cadre de l'authentification Kerberos V5.

Il gère les modifications d'annuaire et les duplique vers d'autres contrôleurs de domaine du même domaine.

Active Directory

- **A suivre : mise en place d'Active Directory au cours des TPs**

  - Installation de Windows 2000 client et serveur
  - Configuration d'un serveur DNS
  - Configuration d'Active Directory
  - Gestion des OU
  - Gestion des utilisateurs