



www.Mcours.com

Site N°1 des Cours et Exercices Email: contact@mcours.com

Administration Systèmes Windows

Campana Antoine – CNRS, UMR6134

La famille Windows

- Windows 3.1x
 - Workgroup.
- Windows NT Serveur
 - Notion de domaine Windows.
 - 98, NT Workstation.
- Windows 2000 Serveur
 - NT Workstation, 2000 Workstation
- Windows 2003 et 2003 R2 Serveur
 - Windows 2000, XP Pro, Vista business
- Windows 2008 Serveur
 - XP Pro, Vista business

Concepts Windows 2003

- **Active Directory**: service d'annuaire.
- **Architecture de sécurité**: prise en charge des cartes à puces, des clés de chiffrement publiques et privées et des protocoles liés à la sécurité.
- **IntelliMirror**: ensemble de fonctions de gestion des modifications et des configurations. Centralisation de l'administration.
- **Service Terminal Server**
- **Windows Script Host**

Concepts Windows 2003

Base de données de registre

- Base de données contenant les informations de configuration du système.
- Elle est composée de sous-arbres avec leurs clefs, leurs ruches et leurs valeurs.

Concepts Windows 2003

Base de données de registre

- **Hkey_local_machine**: Matériel, Système d'exploitation
- **Hkey_classes_root**: Données d'association de classes de fichiers, objets OLE
- **Hkey_current_user**: Profil de l'utilisateur courant
- **Hkey_user**: Profil de tous les utilisateurs
- **Hkey_current_config**: Profil matériel

Concepts Windows 2003

Base de données de registre

- Syntaxe des rubriques valuées:
nom:type de données:valeur
`DependOnService:REG_MULTI_SZ:Tcpip Nbtssys Streams`
- Types de données:
 - REG_BINARY: binaire
 - REG_DWORD: nombre de 4 octets
 - REG_EXPAND_SZ: variable
 - REG_MULTI_SZ: chaîne multiple
 - REG_SZ: caractères lisibles

Concepts Windows 2003

Le système de fichiers

- FAT (File Allocation Table)
 - 16 bits: 2 Go partition max, 8.3
 - 32 bits: 8 Go partition max, 255 caractères
 - Sécurité au niveau du partage

- NTFS (New Technologie File System)
 - Mini base de données de la partition
 - Partitions de 2 To
 - Attributs de fichiers, journaux
 - **Quotas (NTFS 5)**
 - **Cryptage (NTFS 5)**

Concepts Windows 2003

La famille Windows 2003 Server

- Microsoft Windows Server 2003
 - Standard Edition
 - Gère 4Go de RAM et 2 processeurs.
 - Entreprise Edition
 - Gère les processeurs Itanium 64 Bits, 32 Go de RAM sur x86 et 64 Go sur Itanium, 8 processeurs.
 - Datacenter Edition
 - 64 Go de RAM (x86) et 128 Itanium, 8 processeurs.
 - Web Edition
 - Conçu pour les sites Web. Pas d'AD.
 - 2 Go de RAM et 2 processeurs.

Concepts Windows 2003

Types et rôles des serveurs

- Contrôleurs de domaine et serveurs membres
- Rôles joués par les serveurs:
 - Serveur d'application
 - Serveur DHCP
 - Serveur DNS
 - Contrôleur de domaine
 - Serveur de fichiers
 - Serveur de messagerie (POP3, SMTP)
 - Serveur d'impression
 - Serveur d'accès distant/VPN
 - Serveur de nœud du cluster
 - Serveur de média en continu
 - Serveur de terminaux
 - Serveur WINS

Outils de gestion

- Outils supplémentaires
 - Outils de support de Windows Server 2003.
 - Suptools.msi sur le CD.
 - Adminpack.msi sur le CD.

- Outils d'usage fréquent
 - MMC
 - Panneau de configuration.
 - Outils graphiques d'administration.
 - Utilitaires à la ligne de commande.



Outils de gestion

Utilitaires à la ligne de commande

■ Utilitaires à connaître:

- ARP
- AT
- DNSCMD
- FTP
- HOSTNAME
- IPCONFIG
- NBTSTAT
- NET
- NETSH
- NETSTAT
- NSLOOKUP
- PATHPING
- PING
- ROUTE
- TRACERT.

■ Utilitaires NET:

- NET SEND
- NET START
- NET STOP
- NET TIME
- NET USE
- NET VIEW

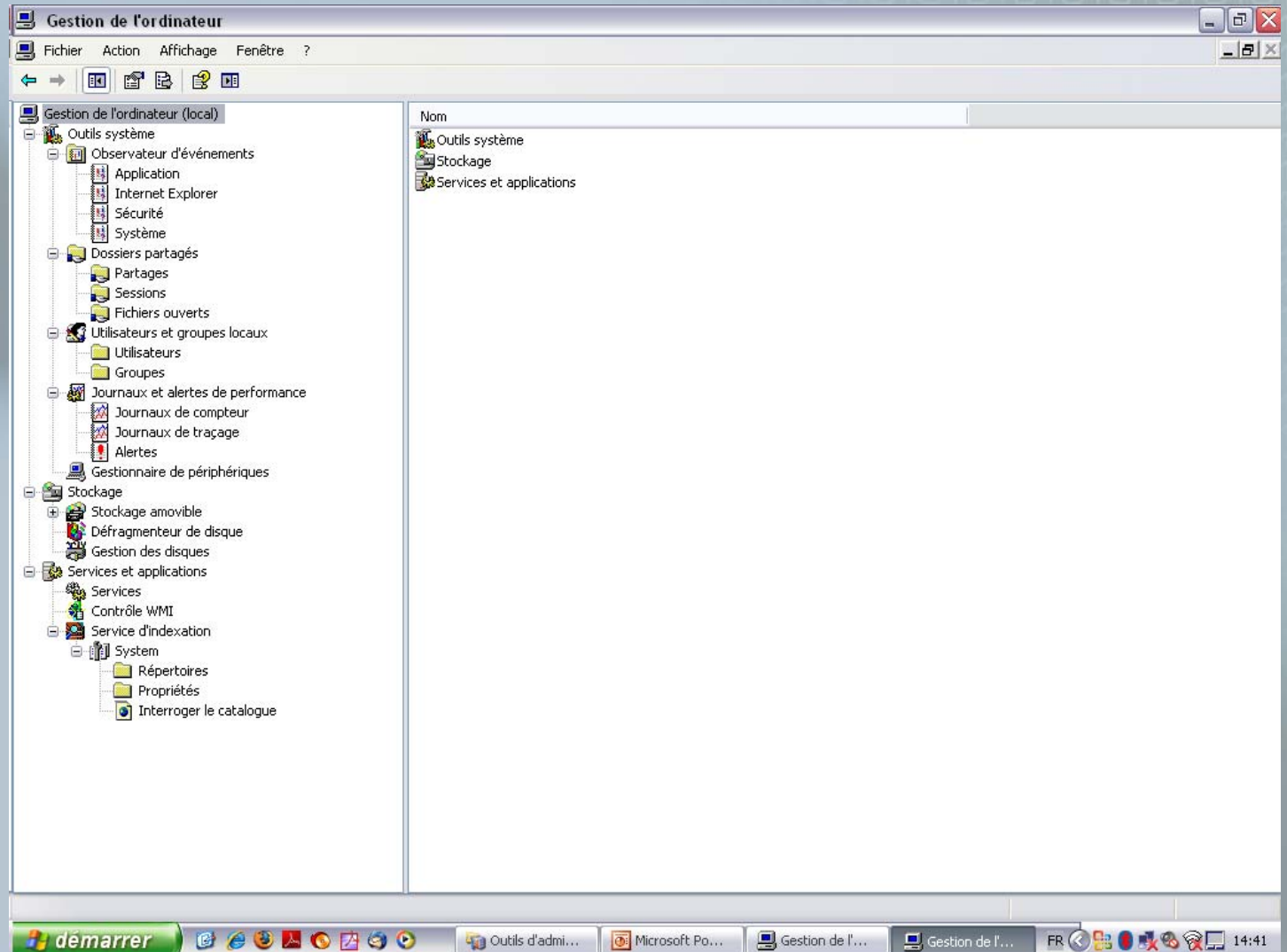
Outils de gestion

Console de gestion de l'ordinateur

- Gestion des sessions et des connexions des utilisateurs.
- Gestion de l'emploi des fichiers, des répertoires et des partages.
- Définition d'alertes administratives.
- Gestion des applications et des services de réseau.
- Configuration des périphériques matériels.
- Affichage et configuration des disques durs et des périphériques de stockage amovibles.

Outils de gestion

Console de gestion de l'ordinateur



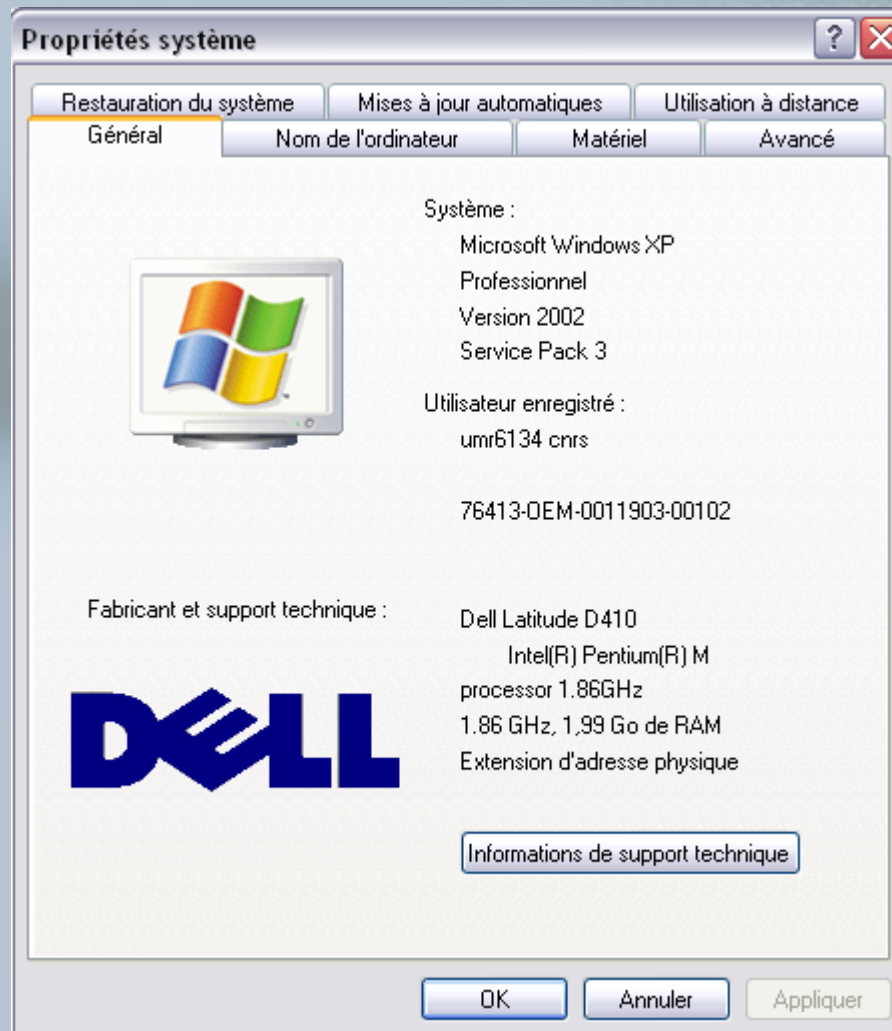
Outils de gestion

Utilitaire système

- Configurer les paramètres de performance, de mémoire virtuelle et de la base de registre.
- Gérer les variables d'environnement du système et de l'utilisateur.
- Fixer les options de démarrage et de récupération système.
- Gérer les profils matériels des utilisateurs.

Outils de gestion

Utilitaire système



Outils de gestion

- Gestion des périphériques et des pilotes matériels
 - Gestionnaire de périphériques.
 - Ajout/Suppression de matériels.
 - Assistant de mise à niveau matérielle.
- Gestion des bibliothèques dynamiques
 - regsvr32 nom.dll

Outils de gestion

- Gestionnaire de tâches.
 - taskmgr.exe
- Gestion des services système.
 - Penser à arrêter les services inutiles !
- Journaux d'évènements.

Performances du système

Surveillance

- Analyseur de performance
 - Journaux de compteur:
 - enregistre les données de performances à des intervalles de temps déterminés
 - Journaux de traçage:
 - enregistre les données chaque fois que l'évènement associé survient.
 - Alertes

Performances du système

Optimisation

- Performances des applications et Mémoire virtuelle
 - Utilitaire système
- Débit des données
 - Connexion réseau



Exemples de contrôles

- Contrôle de la mémoire
 - Mémoire/Octets disponibles
 - Mémoire/Octets dédiés
- Contrôle des performances du processeur
 - Processeur/%Temp processeur
 - Processeur/Longueur de la file d'attente
- Contrôle des accès disques
 - Disque Physique/%Temps du disque
- Contrôle de la bande passante et de la connectivité.
 - Réseau /Octets reçus/s
 - Réseau/Octets envoyés/s

Services d'assistance

- Centre d'aide et de support
- Mises à jour automatiques
 - Serveur de mises à jour (GPO)
- Accès à distance
 - Assistance à distance
 - Bureau à distance
 - Bureaux distants
- Configuration de l'horloge Windows
 - Protocole SNTP (Simple Network Time Protocol)

Installation de Windows

- 5 façons d'installer
 - Manuelle, à partir d'un CD –ROM ou d'un partage réseau.
 - Sans assistance, à l'aide d'un fichier réponse et d'un CD-ROM ou d'un partage réseau.
 - En utilisant Sysprep et un outil de gestion d'images disques.
 - Par le réseau, à partir d'un serveur RIS (Remote Installation Service)
 - Par les GPO ou avec Microsoft SMS (Systems Management Server)

Installation de Windows

- Configuration minimale recommandée
 - Un processeur Intel Pentium II 550 ou compatible
 - 256 Mo de Ram
 - Ecran SVGA 800x600
 - Clavier, souris
 - 2,5 Go de disque, 7200 tours/min
 - Lecteur de CD-Rom ou de DVD-Rom amorçable (12x)
- Consulter la HCL (liste des matériels compatibles)
 - <http://www.microsoft.com/hwdq/hcl/>

Installation de Windows

- Installer sur une partition NTFS
- Récolter les informations
 - Nom DNS (Domain Name System) de l'ordinateur.
 - Nom du domaine ou du groupe de travail.
 - Adresse Ip de l'ordinateur
- Gestion de licences
 - Par serveur.
 - Par périphérique et par utilisateur.

Installation de Windows

- Activation du produit
 - Office XP, XP et 2003 Server vendus au détail nécessite une activation.
 - Possibilité d'avoir des licences en volume à partir de 5 licences Microsoft.
- Disquettes d'amorçage
- Winnt.exe
- Winnt32.exe ou Setup.exe

Installation de Windows

- Installation sans assistance
 - Winnt.exe /u:[fichier de réponse] /s:[chemin]
 - Winnt32.exe /unattend:[nombre:fichier de réponse] /s:[chemin]
- Création d'un fichier de réponse
 - Assistant gestion d'installation
 - CD, \support\tools\deploy.cab
 - (regsvr32 cabview.dll)

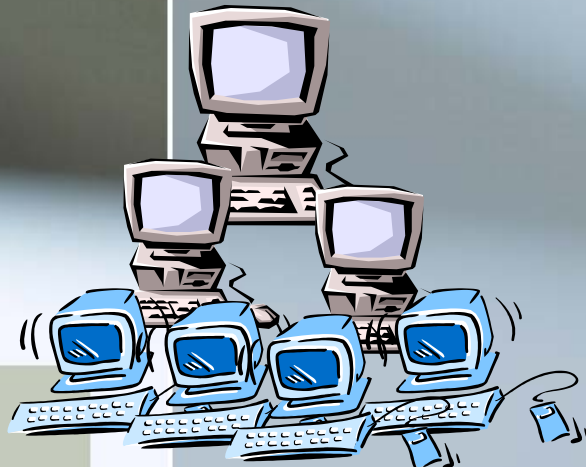
Installation de Windows

- Utilisation de Sysprep (deploy.cab)
 - Faire une installation type
 - Utiliser Sysprep
 - Faire une image disque et la propager à l'aide d'un gestionnaire d'image (ex: GHOST)
 - Démarrer la nouvelle machine.

Notion de domaine

- Regroupement logique d'ordinateurs (serveurs et autres) partageant les informations de sécurité et les comptes.
- Avantages:
 - Ouverture de session unique
 - Accès global aux ressources
 - Administration centralisée

Notion de domaine

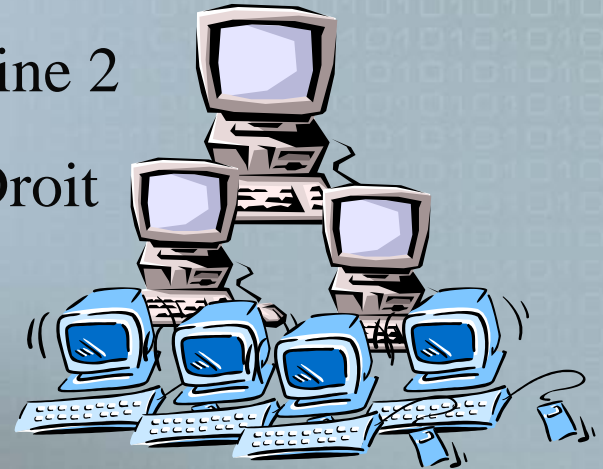


Domaine 1

Ufr Sciences

Domaine 2

Ufr Droit



Domaine 3

Ufr Lettres



Notion de domaine

■ Éléments constitutifs

Server Windows 2003



2000 WS



VISTA



XP Pro



DC



XP Pro



DC



Server Windows 2000



Active Directory

Notion de domaine

- DC: contrôleur de domaine
 - Serveur fonctionnant sous 2003 Server
 - Copie principale de la base de données d'annuaires.



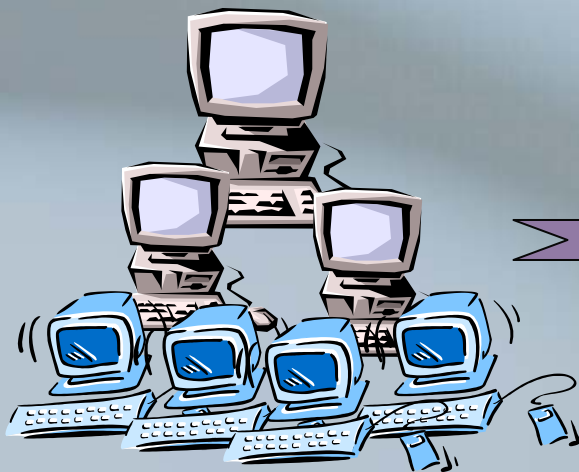
Relation d'approbation

- Relation d'approbation

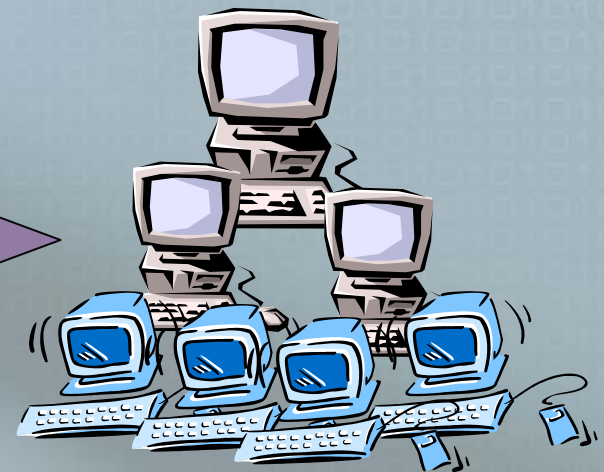
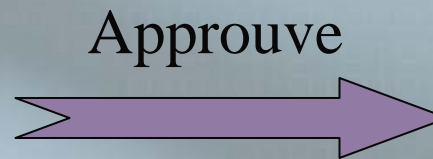
- lien entre 2 domaines, en fonction duquel l'un des domaines accepte les utilisateurs de l'autre sans authentifier une deuxième fois les demandes d'accès correspondantes.

Relation d'approbation

- l'un des domaines est dit *Approuvant* et l'autre *Approuvé*



Domaine Approuvant
Domaine des ressources

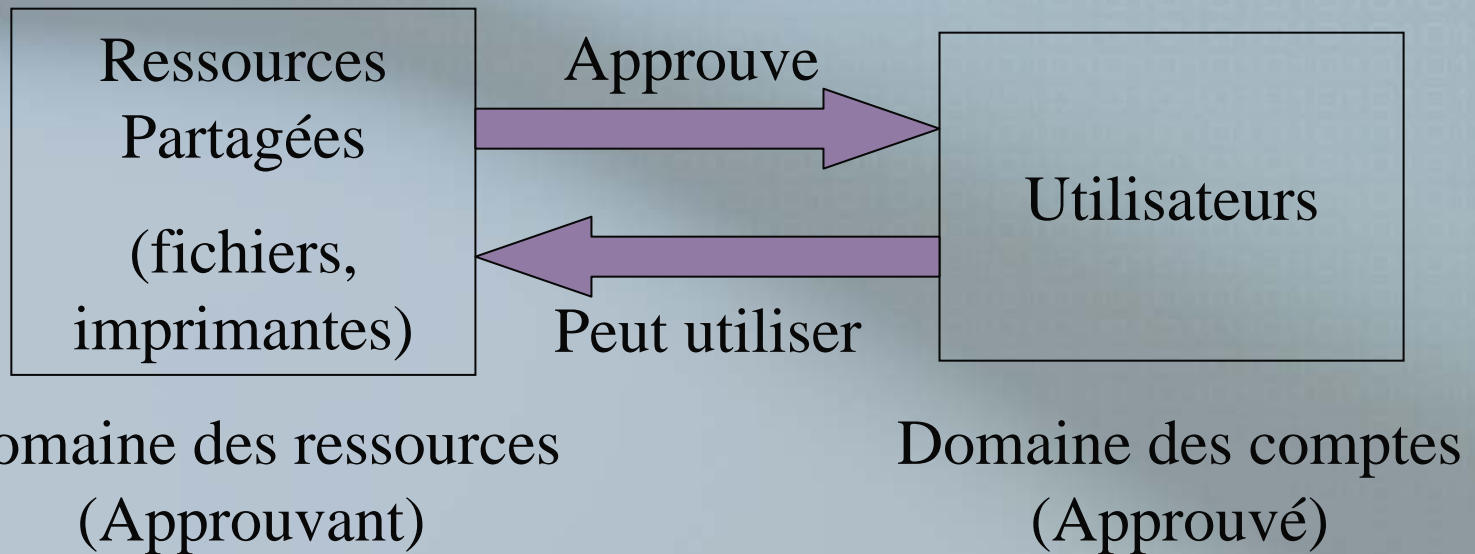


Domaine Approuvé
Domaine des comptes



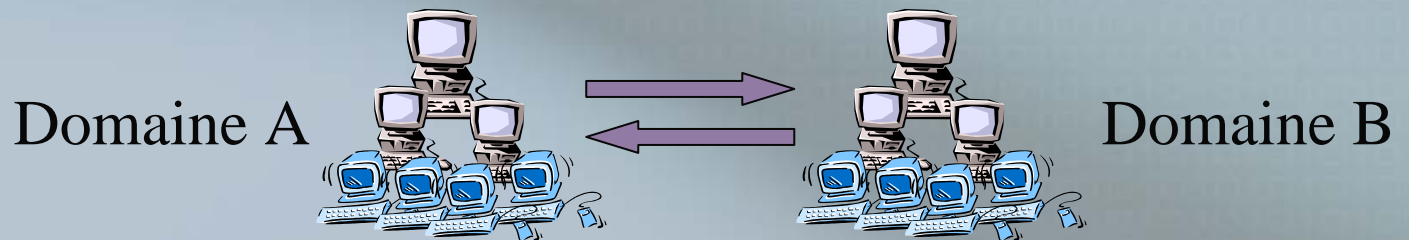
Relation d'approbation

- Les ressources du domaine *Approuvant* peuvent être utilisées par les Utilisateurs du domaine *Approuvé*



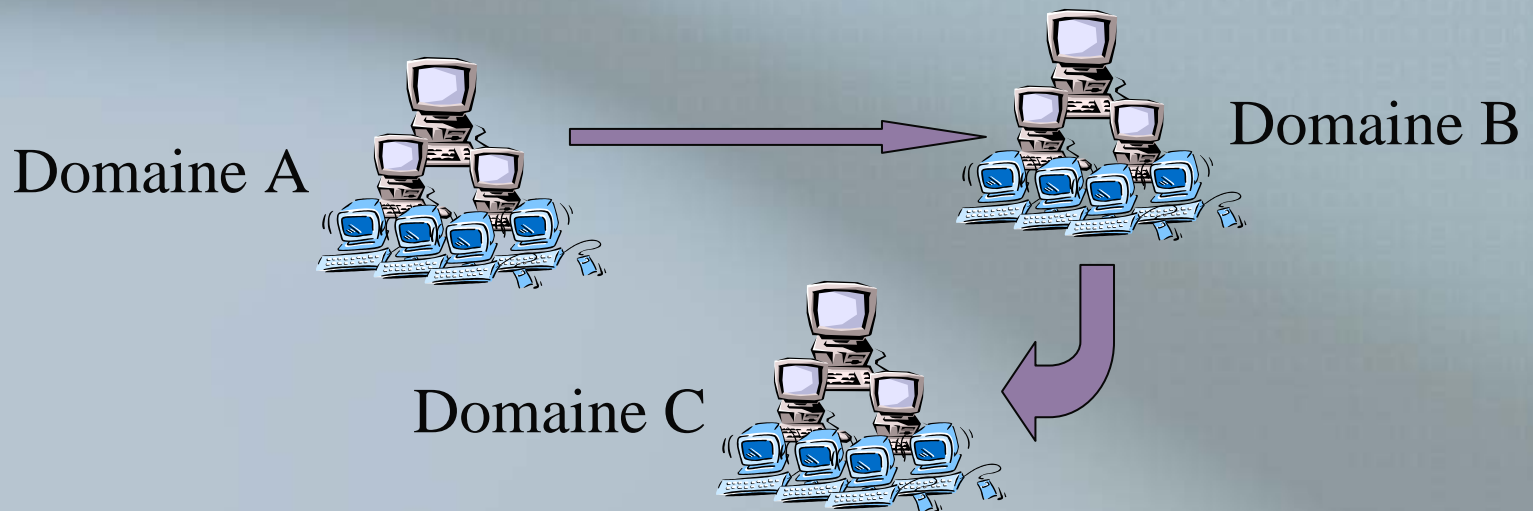
Relation d'approbation

- Relation à *sens unique* ou *réciproque*
 - A approuve B et B approuve A



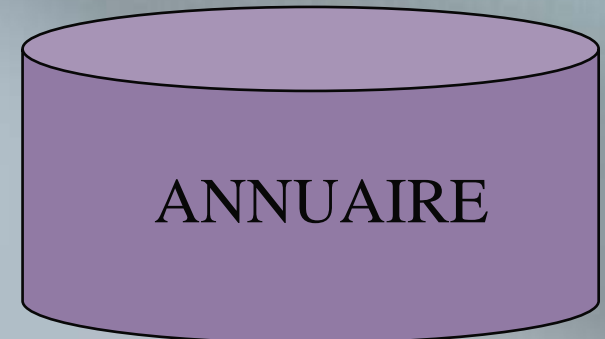
Relation d'approbation

- L'approbation n'est pas transitive
 - A approuve B, B Approuve C mais A n'approuve pas C



Annuaire réseau

- Base de données qui stocke des informations sur le réseau
- Stockage centralisé
 - Localisation et gestion améliorées
 - Objets: Machines, Utilisateurs, Groupes, Ressources, Infrastructure réseau



Annuaire réseau

- Le service d'annuaire permet de réaliser les opérations suivantes:
 - Assurer la sécurité des objets de la base de données
 - Réplication sur d'autres ordinateurs du réseau (disponibilité, panne)
 - Fragmenter l'annuaire pour augmenter le stockage

Annuaire réseau

- **X.500**: recommandation de l'IUT-T
 - IUT-T: Union Internationale des Télécommunications, agence des Nations Unies (V90).
 - ISO 9594: norme
 - IETF (Internet Engineering Task force)
- **LDAP** (Lightweight Directory Access Protocol), pas de norme iso, pure invention d'Internet

L'annuaire de NT 4.0

(pas d'active directory)

- Comptes utilisateurs
- Comptes de groupe
- Comptes de machine
- Relations d'approbation

www.Mcours.com

Site N°1 des Cours et Exercices Email: contact@mcours.com

L'annuaire de Windows 2003

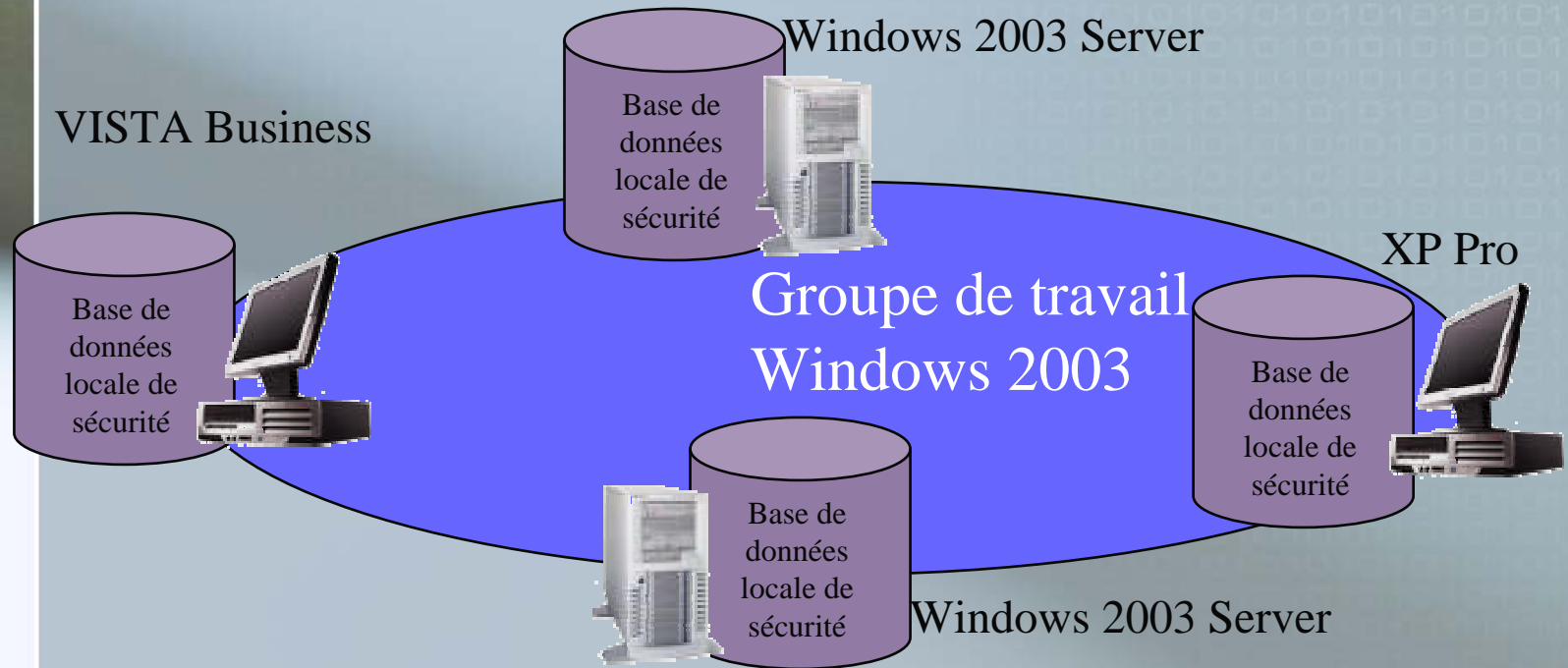
- Comptes utilisateurs
- Comptes de groupe
- Comptes machines
- Relations d'approbation
- Ressources réseaux (fichiers, imprimantes)
- Autres objets
- UO: unité organisationnelles (conteneur d'objet)

Groupes de travail et Domaines

- Groupe de travail
 - Regroupement logique d'ordinateurs en réseau partageant des ressources
 - Base de données locale (utilisateurs, informations de sécurité sur les ressources)



Groupes de travail et Domaines

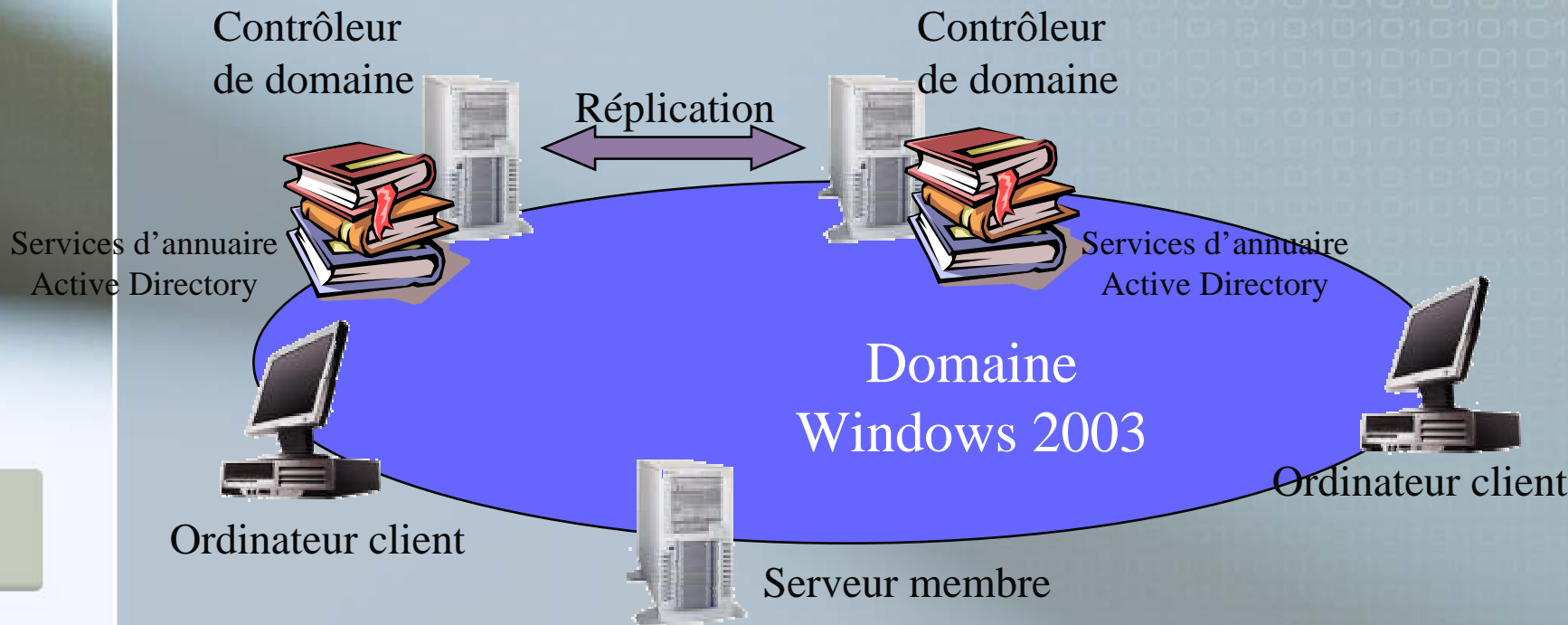


- Comptes locaux
- - de 10 ordinateurs

Groupes de travail et Domaines

- **Domaine Windows 2003**
 - Regroupement logique d'ordinateurs en réseau partageant une base de données d'annuaire centralisée
 - **Contrôleur de domaine**
 - Contient l'annuaire
 - Un seul type
 - Gère la sécurité du domaine

Groupes de travail et Domaines



- Administration centralisée
- Accès aux ressources via une connexion unique

Active Directory

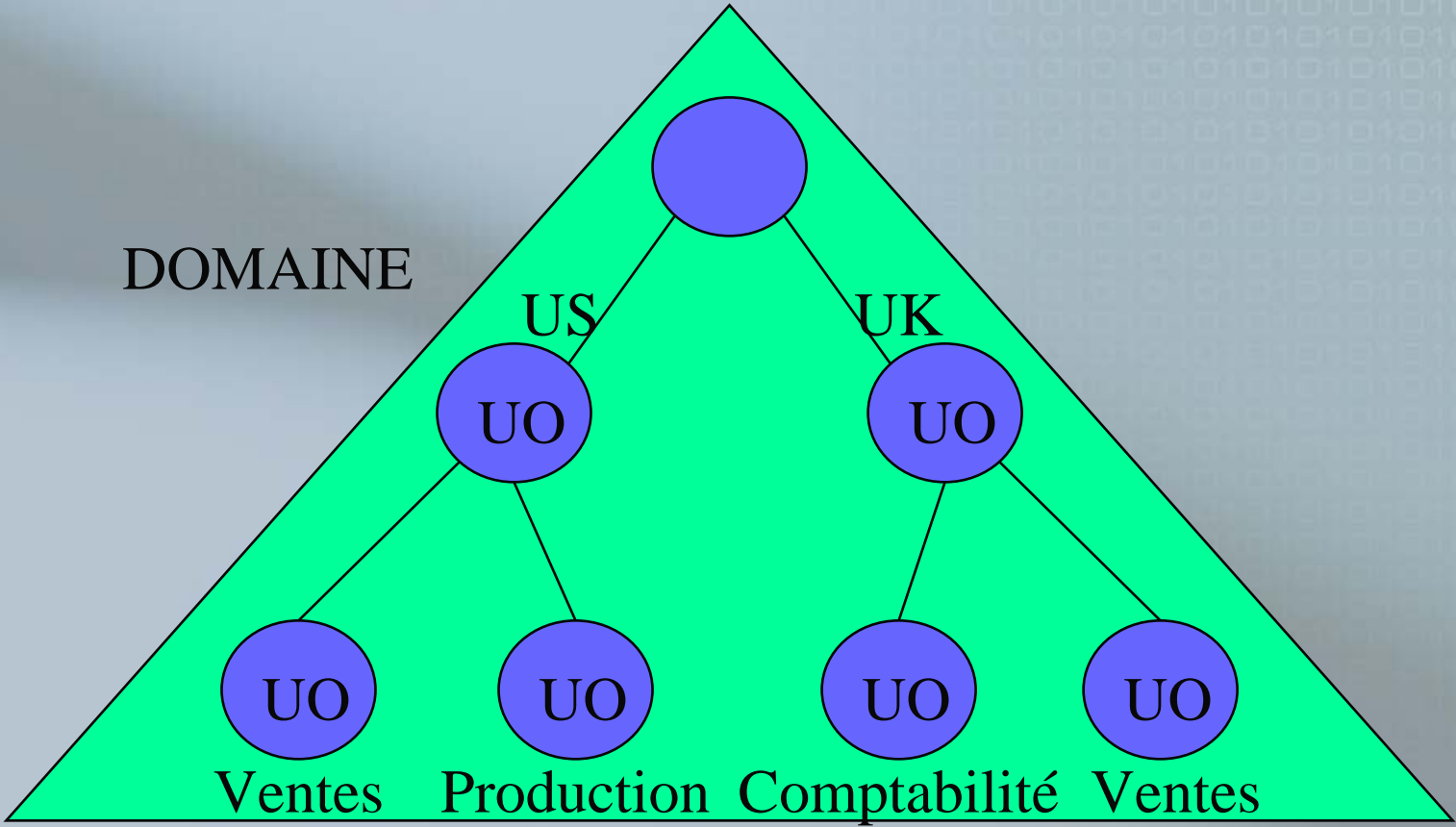
- Active directory est le service d'annuaire de Windows 2003
 - Annuaire des ressources
 - Services d'accès à l'annuaire
- Les ressources (utilisateurs, groupes, imprimantes, serveurs, règles de sécurité, ...) sont des **Objets**
 - Attributs
 - Classes

Active Directory

- Hiérarchie dans l'annuaire grâce à des UO au sein de domaines
 - On peut créer des utilisateurs, des groupes et autres ressources réseau au sein des UO
 - On peut déployer des stratégies d'utilisateurs et de machines par rapport aux UO
 - L'administration des objets contenus dans une UO peut être déléguée à des utilisateurs ou des groupes d'utilisateurs

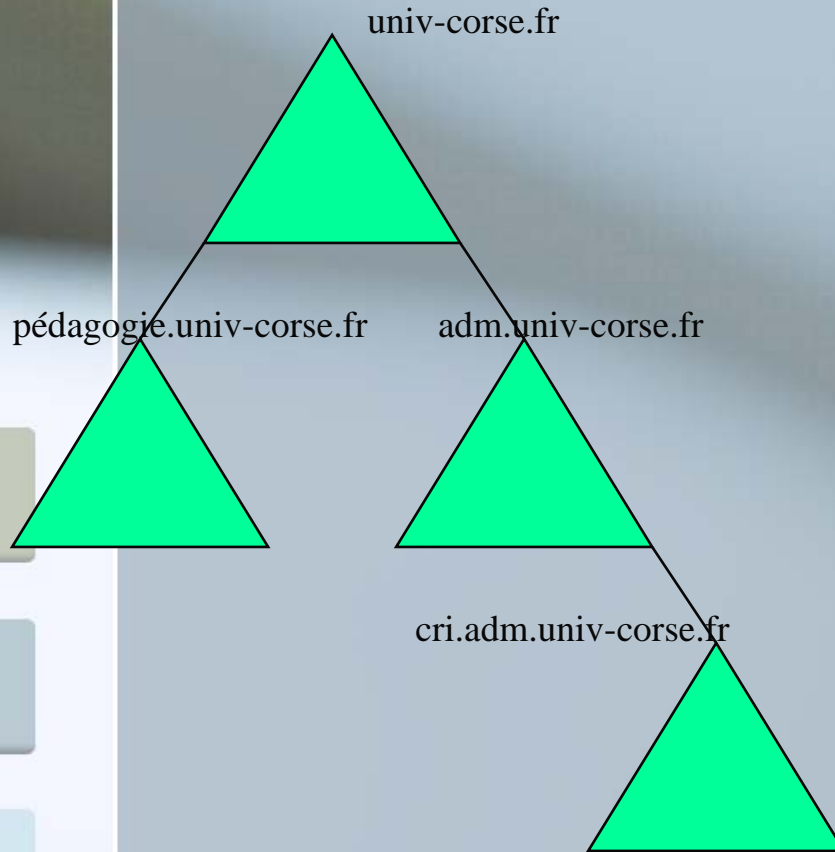
Active directory

Organisation



Active directory

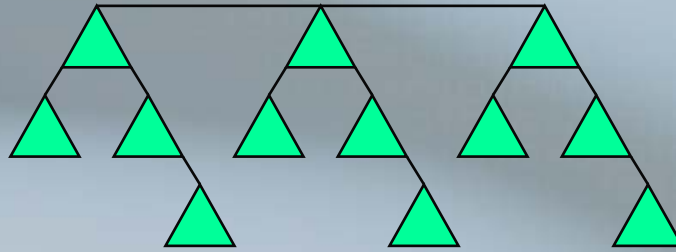
Arborescence



- Hiérarchie de domaines
- Espace de noms homogène
- Relations d'approbations
- Schéma commun
- Catalogue global listant tous les objets de l'arborescence

Active directory

Forêt



- ★ Une ou plusieurs arborescences
- ★ Espace de noms hétérogènes entre arborescences
- ★ Relations d'approbations
- ★ Schéma commun
- ★ Catalogue global listant tous les objets de la forêt

www.Mcours.com

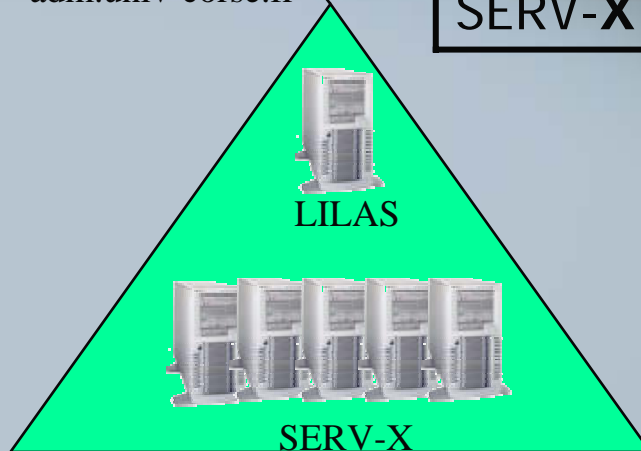
Site N°1 des Cours et Exercices Email: contact@mcours.com

Active directory

univ-corse.fr

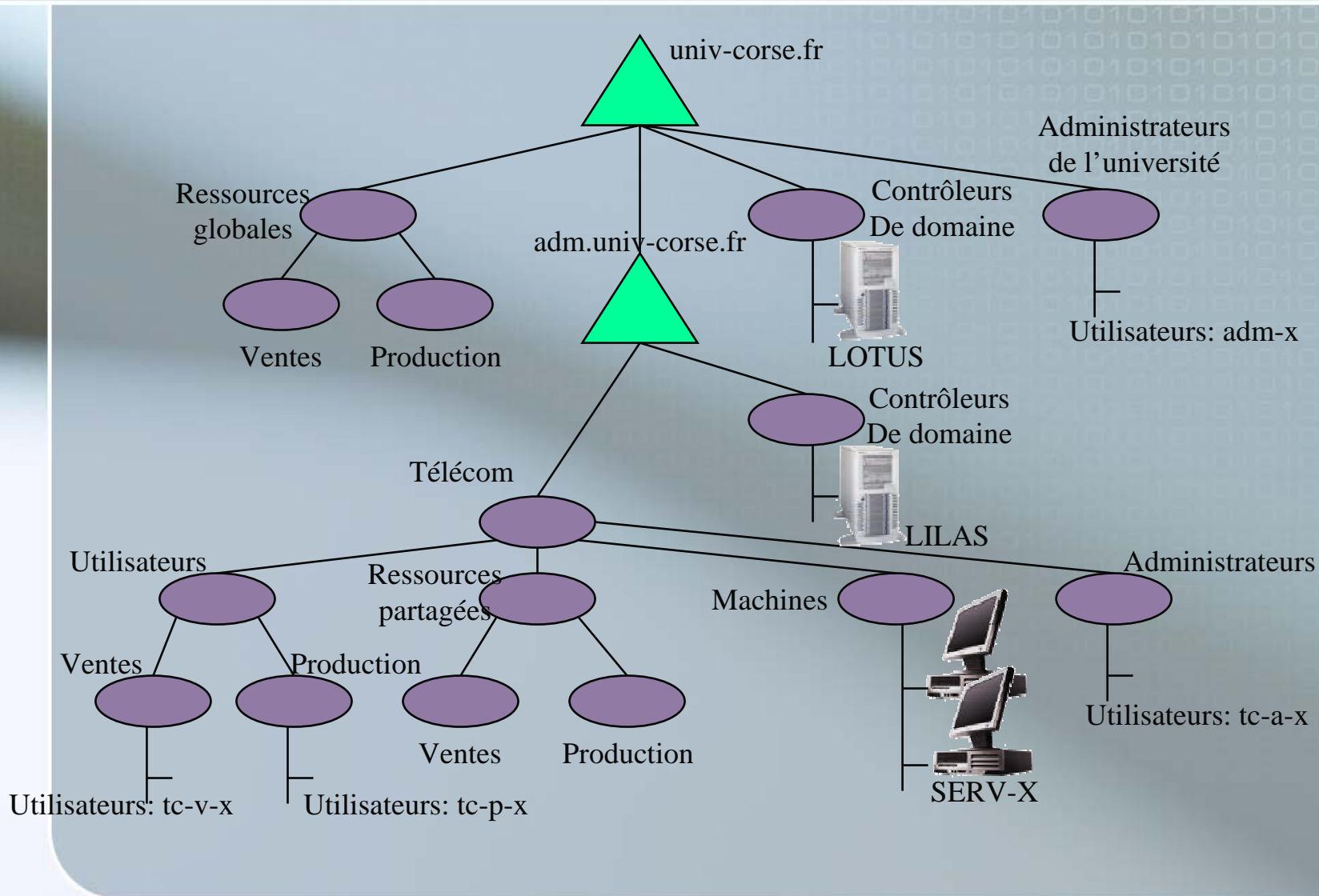


adm.univ-corse.fr



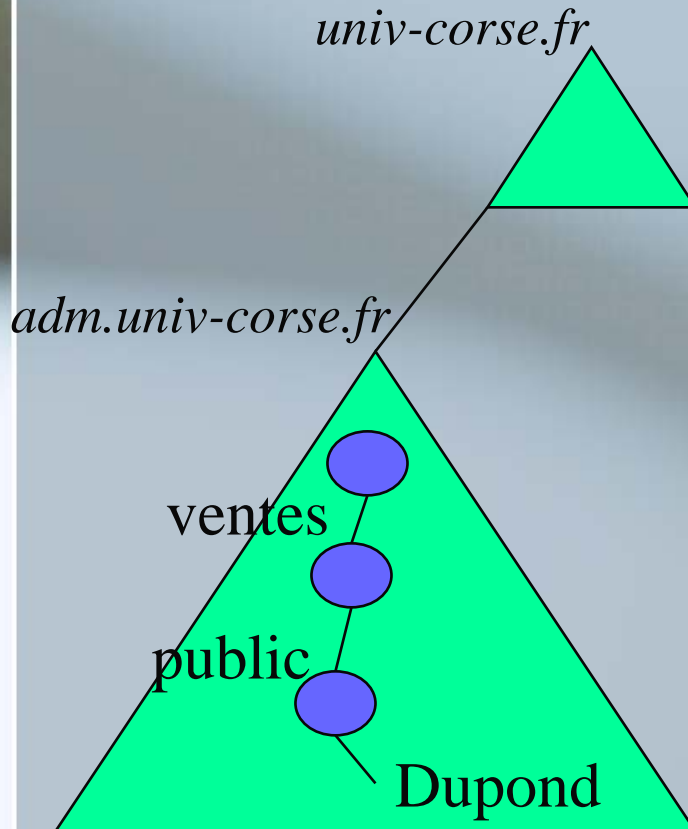
Nom	Type	Adresse IP
LOTUS	Contrôleur de domaine	Fixe
LILAS	Contrôleur de domaine	Fixe
SERV-X	Serveur membre	DHCP

Active Directory



Active directory

■ Nommer les objets



Nom unique (DN):

CN=Dupond, OU=public,
OU=ventes, DC=adm,
DC=univ-corse, DC=fr

CN: nom commun

OU: unité organisationnelle

DC: composant de domaine

Active directory

- Formats de noms

- RFC 822:

- `dupond@univ-corse.fr`

- URL HTTP:

- `http://udc.univ.priv/division/production/dupond`

- LDAP:

- `Ldap://udc.univ.priv/CN:dupond,OU=production,OU=division,DC=udc,DC=univ,DC=priv`

- UNC:

- `\\udc.univ.priv\division\production\dupond`

Active directory

- Le DIT (directory Information Tree):
 - Remplace la base de donnée SAM de NT.
 - Fichier ntds.dit dans %systemroot%\ntds équivalent du fichier sam.
 - Dans un domaine le fichier ntds.dit se duplique dans tous les contrôleurs de domaine.

Active directory

- Le Catalogue global:
 - Permet de trouver rapidement les informations.
 - Contient une réplique de chaque objet Active Directory, mais uniquement un petit nombre d'attributs.
 - Un par site.

Active directory

■ Le schéma:

- Défini les attributs obligatoires et optionnels que chaque classe d'objets peut posséder.
- Stocké sur tous les DC.
- Un seul contrôleur de schéma.
- Extensible
- Composant enfichable: Schéma Active Directory

Administration des utilisateurs et des groupes

- Généralités sur les groupes
 - Objets de l'annuaire ou bien objets locaux à la machine.
 - Contiennent des utilisateurs, des ordinateurs ou d'autres groupes.
 - Groupes de sécurité auxquels on peut attribuer des privilèges (permissions).
 - Groupes de distribution auxquels on ne peut pas attribuer de privilèges.

Administration des utilisateurs et des groupes

■ Étendue Globale

- Permissions sur des ressources situées dans tous les domaines.
- Ne contient que des membres du domaine sur lequel il est créé.
- Peut appartenir à des groupes locaux ou universels d'autres domaines.
- Peut contenir d'autres groupes locaux du même domaine ou des utilisateurs de son domaine.

Administration des utilisateurs et des groupes

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

- Étendue locale de domaine
 - Permissions attribuées uniquement sur les ressources du même domaine
 - Peut contenir
 - Autres groupes locaux de domaines du même domaine.
 - Groupes globaux de tous les domaines.
 - Groupes universels de tous les domaines.
 - Utilisateurs de tous les domaines.

Administration des utilisateurs et des groupes

- Étendue universelle
 - Uniquement si les domaines sont en mode natif.
 - Permissions attribuées sur les ressources de tous les domaines
 - Peut contenir:
 - Autres groupes universels d'autres domaines.
 - Groupes globaux de tous les domaines.
 - Des utilisateurs de tous les domaines.

Administration des utilisateurs et des groupes

- Groupes locaux prédéfinis
- Groupes locaux de domaine prédéfinis
- Groupes globaux de domaine prédéfinis



Administration des utilisateurs et des groupes

- Affectation de droits à un groupe au niveau du domaine
 - Stratégies de groupe (GPO) dans utilisateurs et ordinateurs Active directory.
- Affectation de droits localement
 - Stratégies locales dans outils d'administration.

Administration des utilisateurs et des groupes

Planification des groupes

- Noms de groupes parlants.
- Les groupes comparables doivent avoir des noms similaires.
- Des groupes globaux pour les utilisateurs et des groupes locaux pour les ressources.
- Mise en œuvre des groupes
 - Création, suppression, ajout d'utilisateurs

Administration des utilisateurs et des groupes

- Stratégie d'utilisation des groupes:

- A G DL P
- A G G DL P
- A G U DL P
- A G G U DL P

- Avec:

- A: Accounts
- G: Global
- DL: Domain Local
- U: Universel
- P: Permissions



Administration des utilisateurs et des groupes

- Création de comptes utilisateurs
 - Sur le domaine
 - Localement
- Administration d'un compte utilisateur
 - Localisation
 - Désactivation et Activation
 - Suppression
 - Transfert
 - Renommer
 - Réinitialisation de mot de passe
 - Déverrouillage

Administration des utilisateurs et des groupes

- Administration d'un compte utilisateur
 - Création de répertoires personnels sur un serveur
 - Créer le partage sur le serveur.
 - Permissions CT au groupe Utilisateurs.
 - Définir le chemin dans l'onglet Profil de l'utilisateur.
 - Utilisation de la variable %username%.
- Copie de comptes utilisateurs
 - Déploiement à partir d'un compte générique

Administration des utilisateurs et des groupes

■ Profils utilisateur

- Local: profil créé quand un utilisateur ouvre une session sur une machine. Ce profil est local à la machine.
- Itinérant: Profil créé par un administrateur et stocké sur un serveur. Le profil suit l'utilisateur sur toutes les machines.
- Obligatoire: Profil itinérant verrouillé. (ntuser.dat -> ntuser.man)

Administration des utilisateurs et des groupes

- Création de profils itinérants
 - \\serveur\profils\%username%
- Création de profils itinérants personnalisés
 - Créer un profil modèle.
 - Copier le modèle.

Administration des utilisateurs et des groupes

- Contenus d'un profil utilisateur
 - Application Data
 - Bureau
 - Cookies
 - Favoris
 - Local Settings
 - Menu Démarrer
 - Mes Documents
 - Modèles
 - Recent
 - SendTo
 - Voisinage d'impression

www.Mcours.com
Site N°1 des Cours et Exercices Email: contact@mcours.com

Gestion des disques

- Système de fichier

- FAT16

- Conçu pour les partitions <500 Mo, Gère jusqu'à 2 Go, pas d'ACL

- FAT32

- Partitions > 2 Go

- NTFS 5.0

- ACL, compression, quotas, cryptage par clé publique/clé privée

Gestion des disques

- MMC Gestion de l'ordinateur
- Disque de base (4 partitions max)
 - 4 partitions principales.
 - Ou 3 partitions principales et une partition étendue. Dans la partition étendue, on peut créer un ou plusieurs lecteurs logiques.

Gestion des disques

■ Disque dynamique

- Pas de partitions, des volumes.
- Tolérance de panne
- Pas de limite dans le nombre de volumes
- Extension de volumes NTFS

■ Types de volumes

- Volume simple
- Volume d'agrégat par bandes
- Volume réparti
- Volumes mis en miroir
- Volumes RAID 5

Gestion de disques

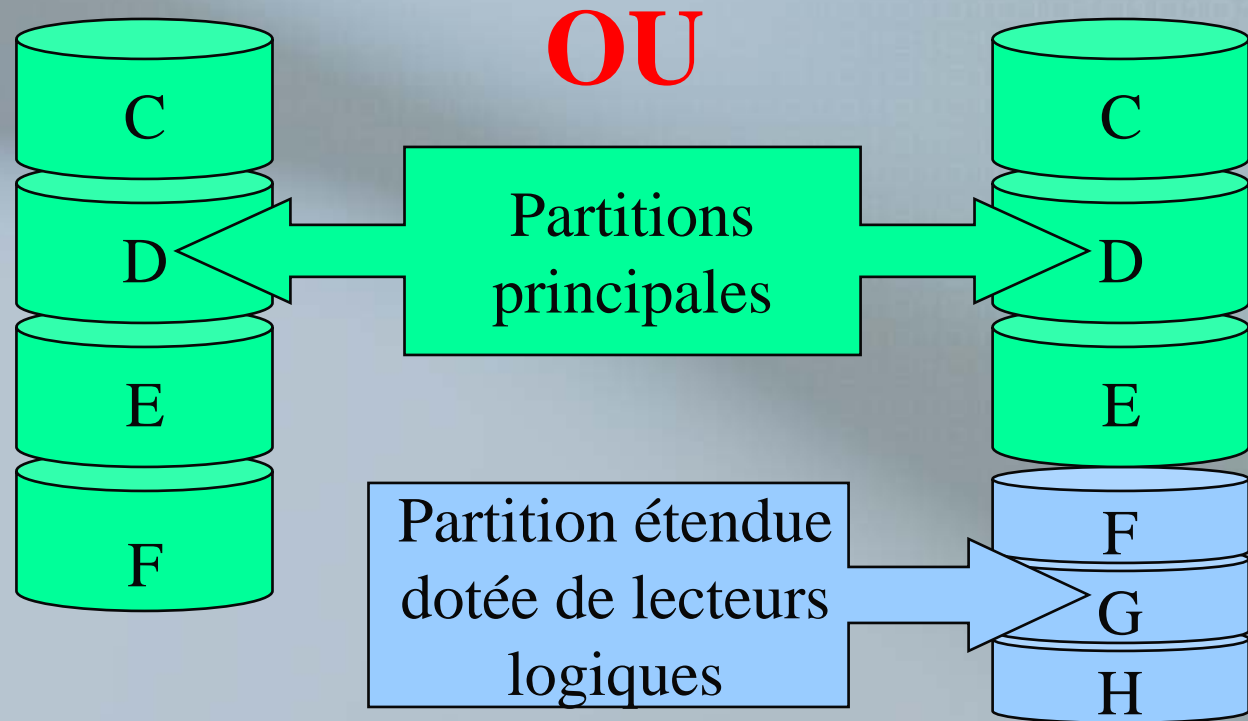
Configuration d'un disque dur

- Initialiser les disques au moyen d'un type de stockage
 - Stockage de base
 - Stockage dynamique
- Création de partitions ou de volumes
- Formatage du disque

Gestion de disques

Types de stockage

■ Stockage de base



Gestion de disques

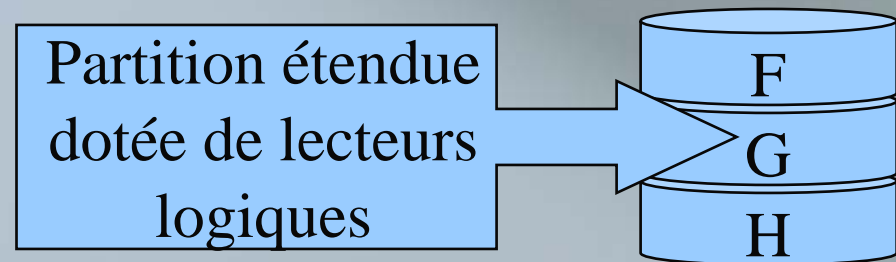
Types de stockage: **stockage de base**

- Partitions principale
 - 1 Partition active à la fois (fichiers d'amorçage du système).
 - Isolement de systèmes ou de données
 - La *partition système* sous Windows désigne la partition active.

Gestion de disques

Types de stockage: **stockage de base**

- Partition étendue
 - 1 seule par disque
 - Décomposée en secteurs logiques formatés au moyen d'un système de fichiers



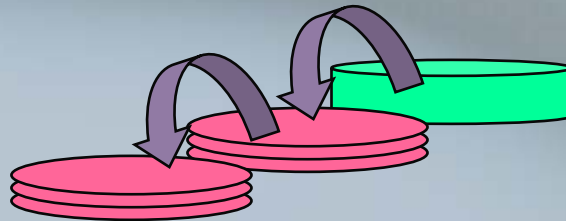
Gestion de disques

Types de stockage: **stockage dynamique**

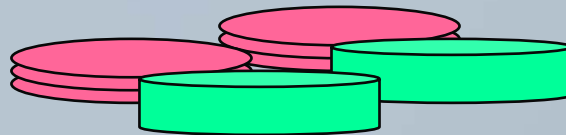
- Stockage dynamique
 - (Windows 2000 et +)



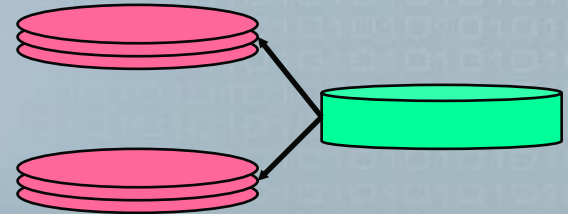
Volume simple



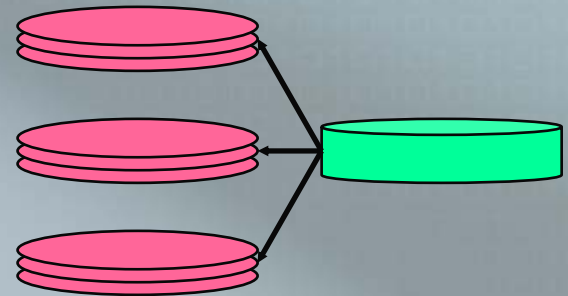
Volume fractionné



Volume en miroir



Volume agrégé par bande



Volume RAID-5

Gestion de disques

Types de stockage: **stockage dynamique**



Volume simple

- Contient l'espace disque d'un seul disque
- Pas de tolérance de panne

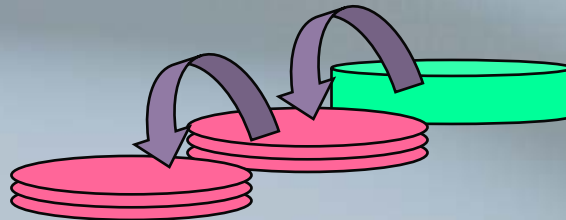


Gestion de disques

Types de stockage: **stockage dynamique**

www.Mcours.com

Site N°1 des Cours et Exercices Email: contact@mcours.com

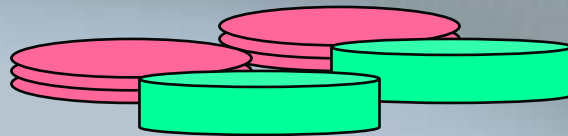


Volume fractionné

- Contient l'espace de plusieurs disques
- 32 disques max.
- Pas de tolérance de panne

Gestion de disques

Types de stockage: **stockage dynamique**

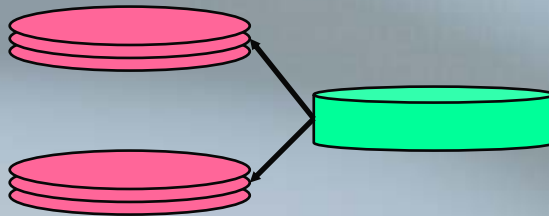


Volume en miroir

- 2 exemplaires identiques d'un volume simple sur 2 disques séparés.
- Tolérance de panne

Gestion de disques

Types de stockage: **stockage dynamique**

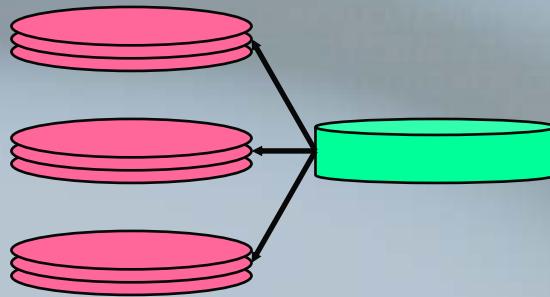


Volume agrégé par bande
Ou RAID-0

- Volume logique constitué des secteurs d'espace libres de plusieurs disques.
- Pas de tolérance de panne

Gestion de disques

Types de stockage: **stockage dynamique**



Volume RAID-5

- Agrégat par bande avec tolérance de panne.
- Minimum de 3 disques durs

Partage de dossiers

- Partages administratifs
 - C\$, D\$, E\$
 - Fournit un accès complet à l'administrateur sur les lecteurs. \\nom_ordinateur\C\$
 - Admin\$
 - Utilisé pour la gestion d'une station à travers le réseau. Il s'agit du répertoire %systemroot%
 - IPC\$
 - Ce partage sert pour la communication entre les processus. Il est utilisé notamment lors de l'administration à distance d'une station ou même lorsque on consulte un répertoire partagé.
 - Print\$
 - Est utilisé pour l'administration à distance des imprimantes.

Partage de dossiers

- 2 façons de faire:
 - Partage du dossier via l'option "Partager".
 - Partage du dossier via la mmc "Gestion de l'ordinateur".
- Autorisations de partage
 - Lecture
 - Modifier
 - Contrôle total

Permissions d'accès

- Permissions NTFS
 - Onglet sécurité dans Propriétés
- Permissions sur un dossier
 - Lecture
 - Afficher le contenu du dossier
 - Lecture et exécution
 - Ecriture
 - Modifier
 - Contrôle total



Permissions d'accès

- Permissions sur un fichier
 - Lecture
 - Ecriture
 - Lecture et exécution
 - Contrôle total
 - Modifier
- Permissions avancées

Permissions d'accès

- Application des permissions NTFS
 - NTFS/NTFS
 - Combinaison
 - Refus prioritaire
 - NTFS/Partage
 - Le plus restrictif des 2
 - Héritage

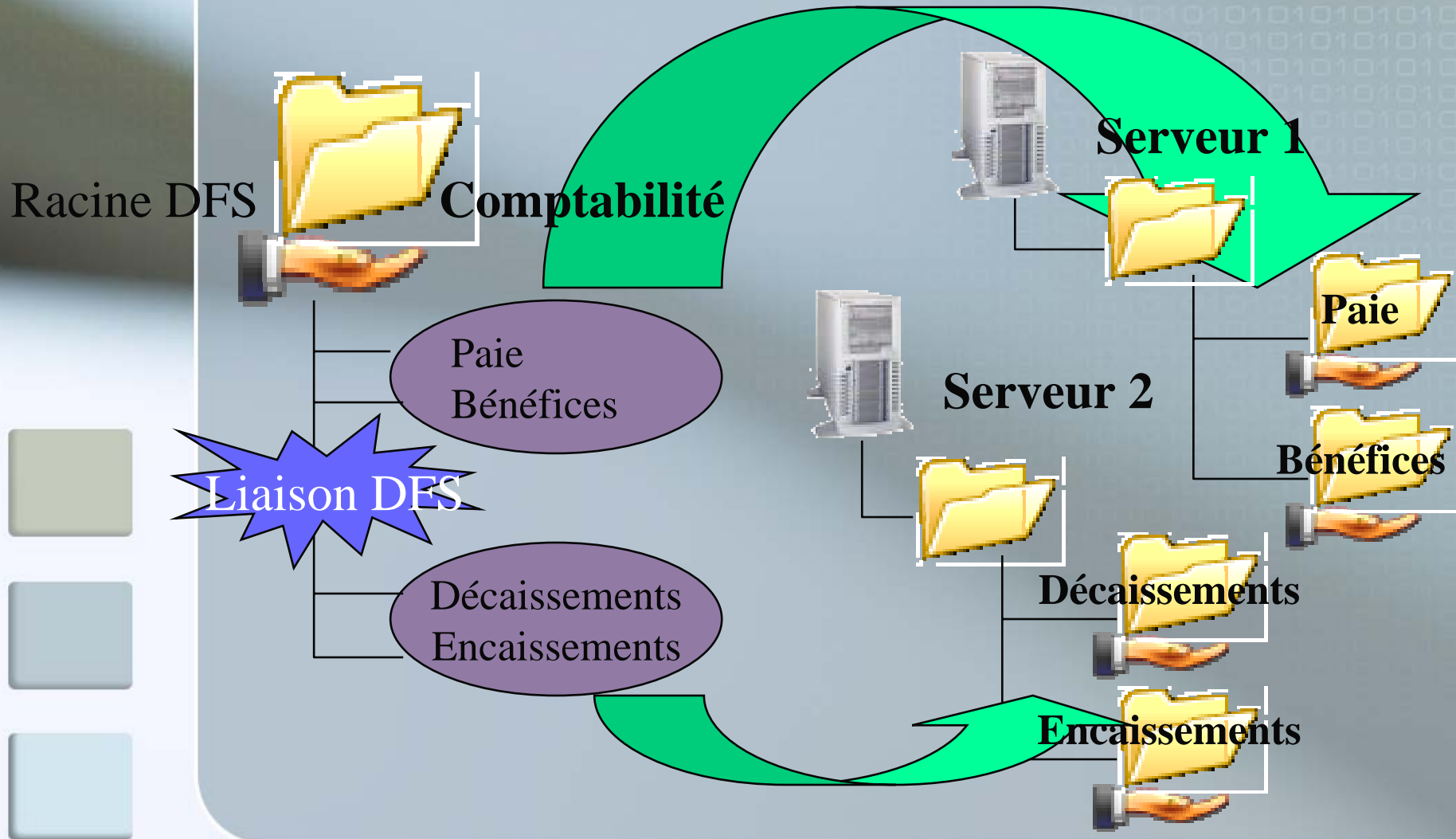
Systeme DFS

Distributed File System

- Permet de rassembler sous une arborescence unique et logique, plusieurs répertoires situés physiquement à différents endroits du réseau.
- DFS autonome (1 serveur).
- DFS à tolérance de panne (AD).

Systeme DFS

Distributed File system



Quotas et Compression

- Quotas de disques
 - Limiter la quantité de données que les utilisateurs peuvent stocker.
 - Propriétés du lecteur sélectionné.
- Compression de disques
 - Propriétés du fichier ou du dossier concerné.
 - Compact.exe à l'invite de commande
 - Attention à la copie !

Ressources d'impression

- Partage d'imprimante et publication ou pas dans l'AD.
- Sécurité.
- Options:
 - Pool d'impression
 - Gestion des priorités
- Gestion du spouleur.
- Administration via le Web:
 - <http://serveur/Printers>

Publication des ressources dans Active Directory

- Publication d'imprimantes
 - Simplifie la recherche et l'administration
- Publication de Partages
 - Simplifie la recherche
 - Mots clefs

Administration Windows 2003

Stratégies de groupe: présentation

- Elles servent à définir des configurations utilisateur et ordinateur pour:
 - Gérer l'environnement bureautique des utilisateurs
 - Appliquer une politique d'entreprise
 - Sécuriser le réseau

Administration Windows 2003

Stratégies de groupe: présentation

- Une stratégie de groupe peut être:
 - déployée sur des groupes d'utilisateurs et/ou d'ordinateurs.
 - Combinée.
 - Sécurisée.
 - Utilisée n'importe où dans l'entreprise.

Administration Windows 2003

GPO: structure

- Objet stratégie de groupe (GPO: Group Policy Object)
 - Conteneur (GPC) : objet Active Directory contenu dans le conteneur Policies
 - Modèle (GPT): dossier contenu dans:
 - %systemroot%\SYSVOL\sysvol\\policies
- Identifié par le GUID (global unique Identifier)
- GPO locale pour des machines individuelles
 - %systemroot%\System32\GroupPolicy

Administration Windows 2003

GPO: création

- Création de GPO liées
 - Dans "Sites et Services Active Directory" ou "Utilisateurs et Ordinateurs Active directory"

- Création de GPO non liée
 - À partir d'une MMC

- Console de gestion des stratégies de groupe.

Administration Windows 2003

Stratégies de groupe: Composant MMC

- Le composant permet l'édition d'une seule stratégie à la fois
- L'ensemble des paramètres se divisent en paramètres Utilisateurs et Ordinateur

ordinateur

utilisateur

Administration Windows 2003

GPO: configuration ordinateur

- Configuration de l'ordinateur

- Spécifie les paramètres applicables à l'ordinateur en fonction de son emplacement dans l'annuaire
- Appliquée au démarrage de l'ordinateur (boot)
- Indépendante du compte utilisateur de la session

ordinateur

Administration Windows 2003

GPO: configuration utilisateur

- Configuration de l'utilisateur
 - Spécifie les paramètres applicables à l'ordinateur selon l'emplacement de l'utilisateur courant dans l'annuaire
 - Appliquée lors de la connexion (logon)
 - Ces paramètres suivent l'utilisateur de machine en machine



utilisateur

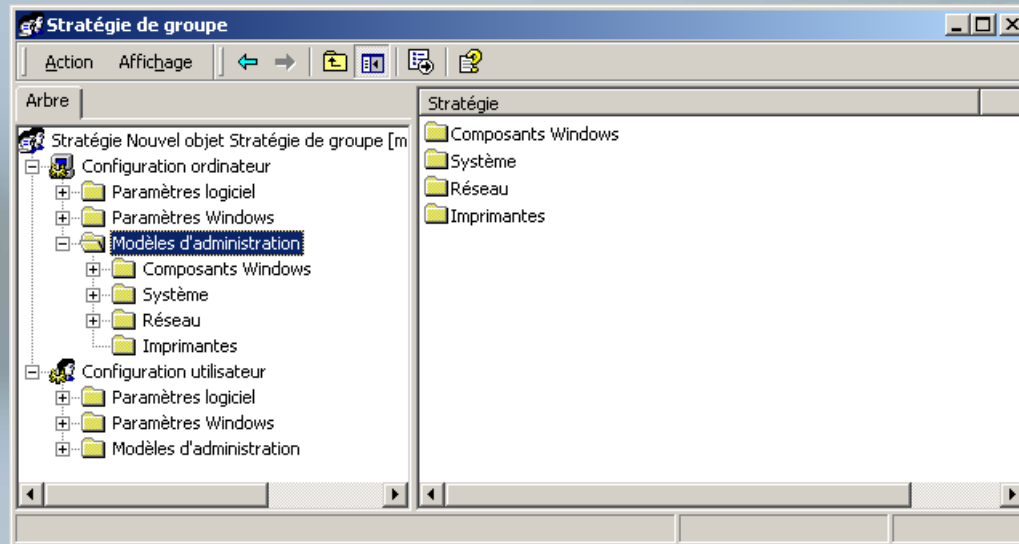
Administration Windows 2003

GPO: conflits de configurations

- Les configurations ordinateur et utilisateur entrent parfois en conflit
 - Bien que chaque configuration comporte de nombreux paramètres, des paramètres qui se recoupent sont très rares
 - Pour ces quelques paramètres, **ce sont ceux de la configuration de l'ordinateur qui sont appliqués**

Administration Windows 2003

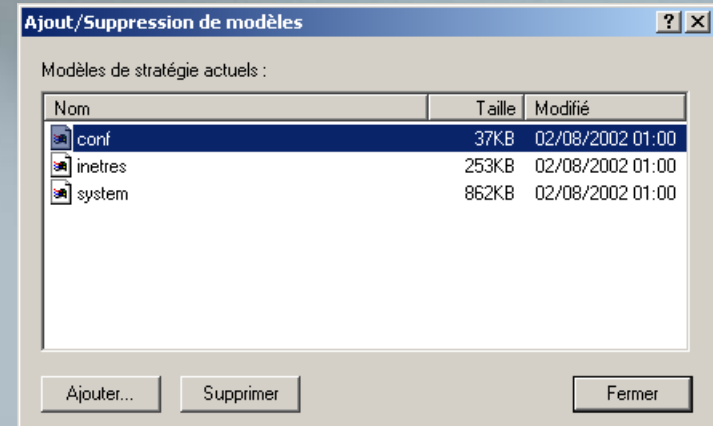
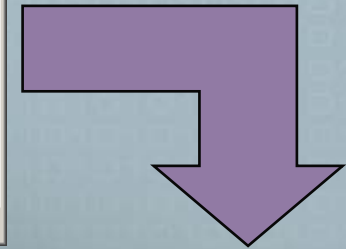
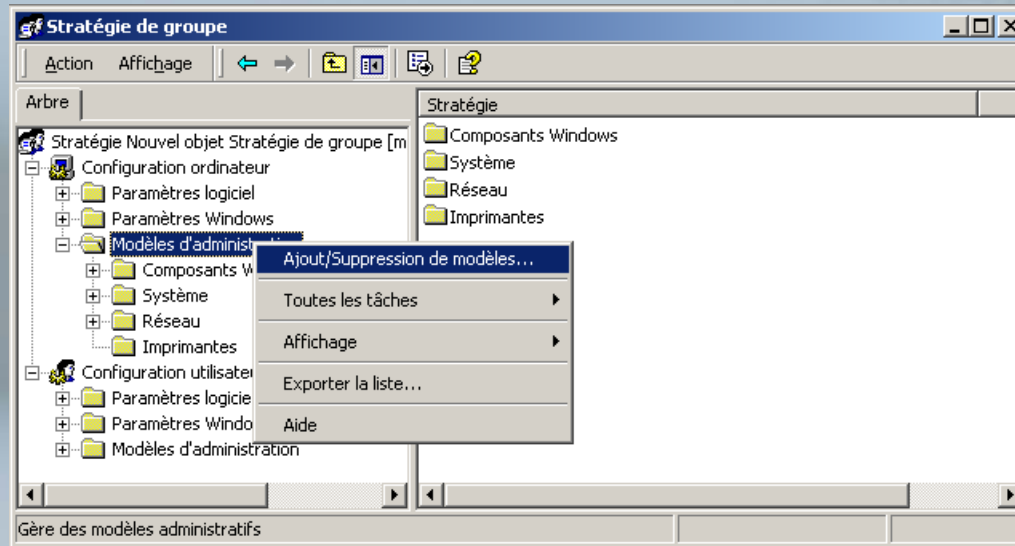
GPO: Modèles d'administration (1)



- L'extension "modèles d'administration" propose une interface graphique permettant de modifier les paramètres du registre
- Elle utilise des fichiers modèles indiquant les valeurs à configurer (System.adm, inetres.adm et conf.adm sont chargés par défaut)

Administration Windows 2003

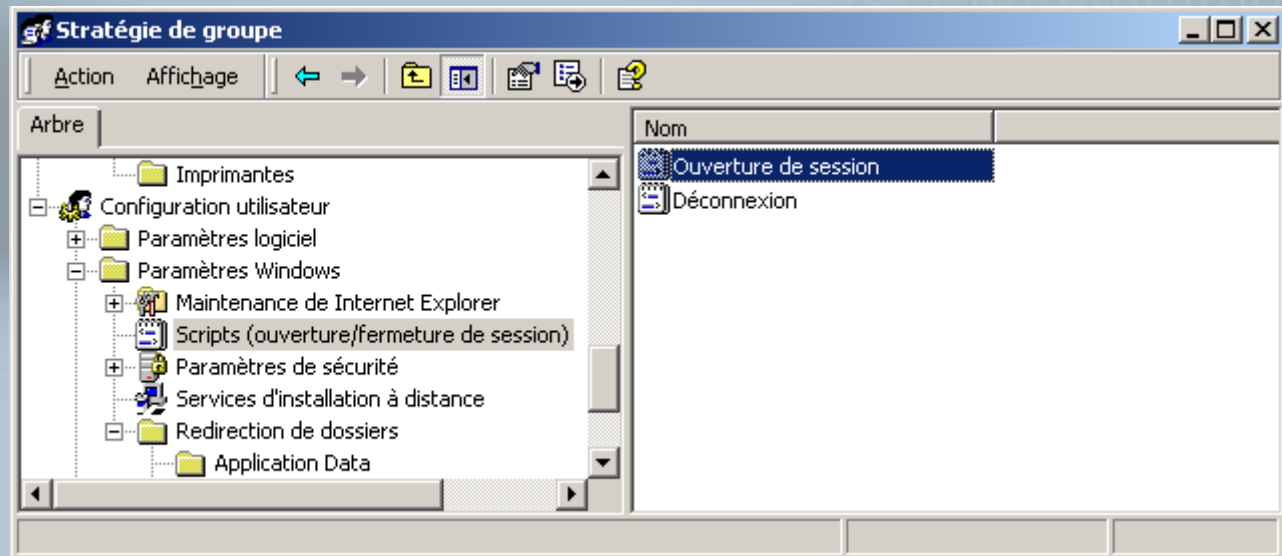
GPO: Modèles d'administration (2)



- Il est possible de charger de nouveaux modèles d'administration
- %systemroot%\inf

Administration Windows 2003

GPO: Scripts (1)



- L'extension Scripts associe un ou plusieurs scripts à un ordinateur ou à un utilisateur
 - Les scripts peuvent être développés en VB, Jscript et en format ligne de commande

Administration Windows 2003

GPO: Scripts (2)

- Les scripts de **démarrage/arrêt** s'appliquent aux **ordinateurs**
- Les scripts de **connexion/déconnexion** s'appliquent aux **utilisateurs**
- Pour intégrer un script à un objet GPO
 - Indiquer le chemin d'accès au script
 - Renseigner tous les paramètres à transmettre au script
 - Définir l'ordre d'exécution des scripts si nécessaire

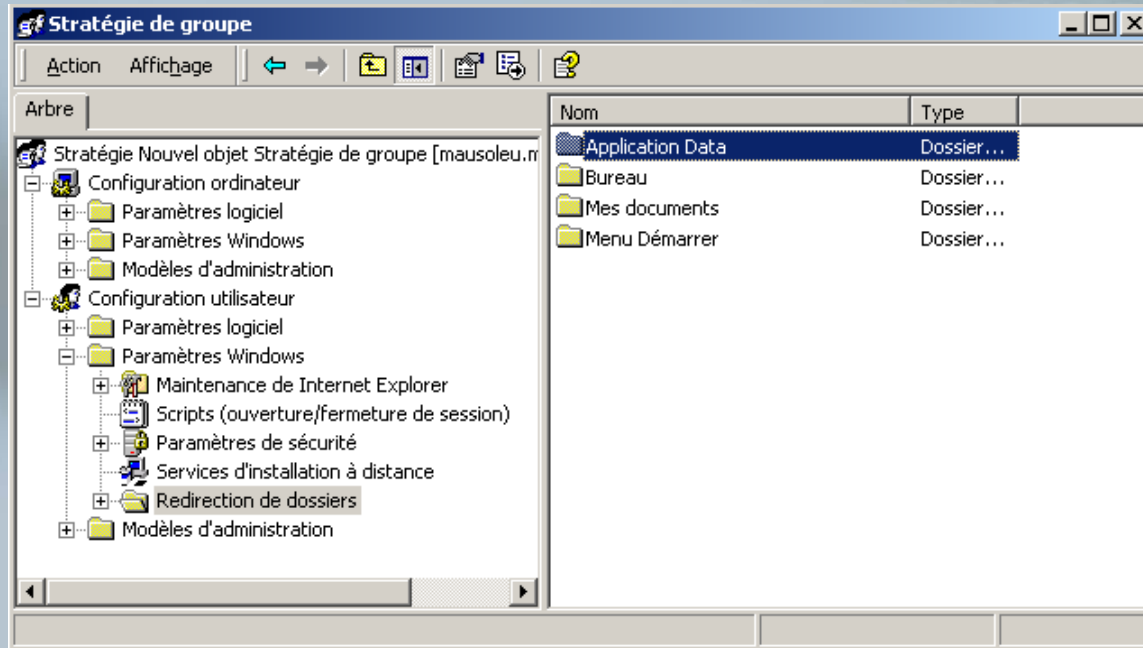
Administration Windows 2003

GPO: Stockage des Scripts (3)

- Un ordinateur doit pouvoir accéder au script pour l'exécuter
- Les scripts peuvent être placés:
 - dans le dossier Sysvol sur un contrôleur de domaine (idéal)
 - dans un serveur spécifique
 - `\\scriptserver.univ-corse.fr\Scripts\logon.vbs`
 - sur le poste local (rare)
 - `C:\scripts\localscript.cmd`

Administration Windows 2003

GPO: Redirection de dossiers

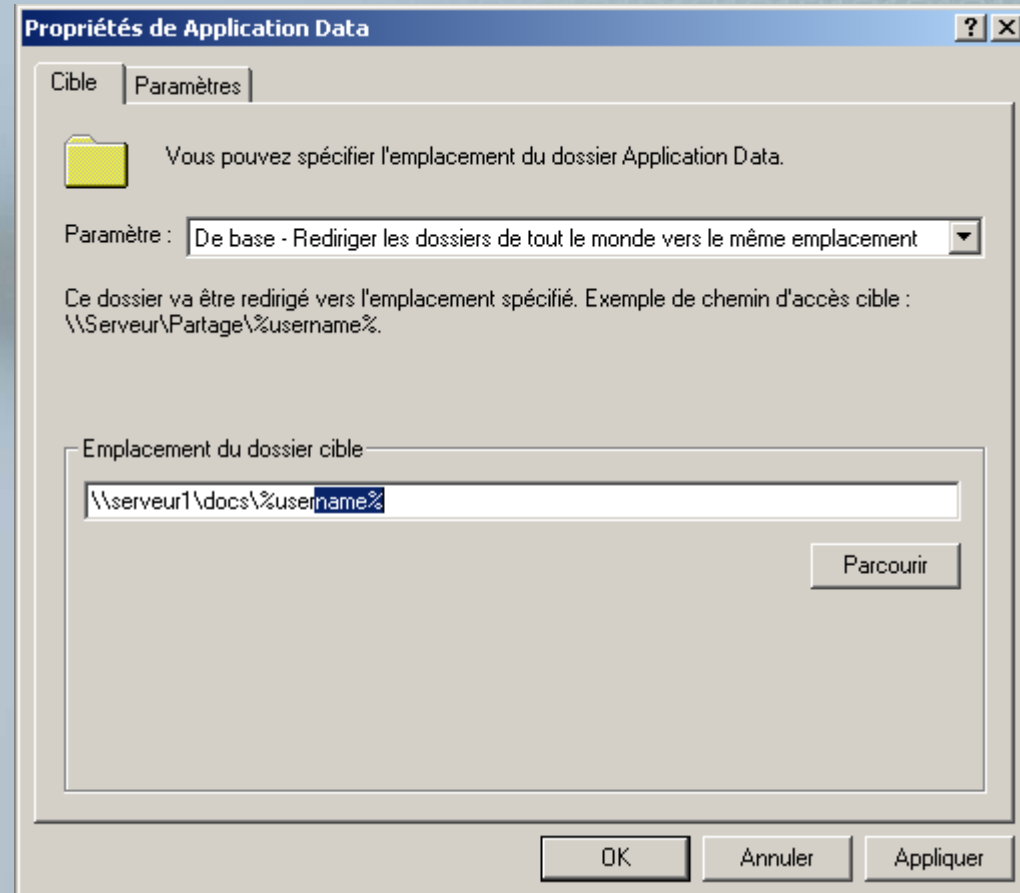


- L'option redirection de dossier fait pointer les dossiers spéciaux de l'utilisateur vers de nouveaux emplacements (local ou réseau)

Administration Windows 2003

GPO: Redirection de dossiers "de Base"

- Le paramétrage "de base" place tous les dossiers utilisateurs au même endroit
- Le paramètre %username% sert à les placer dans différents dossiers

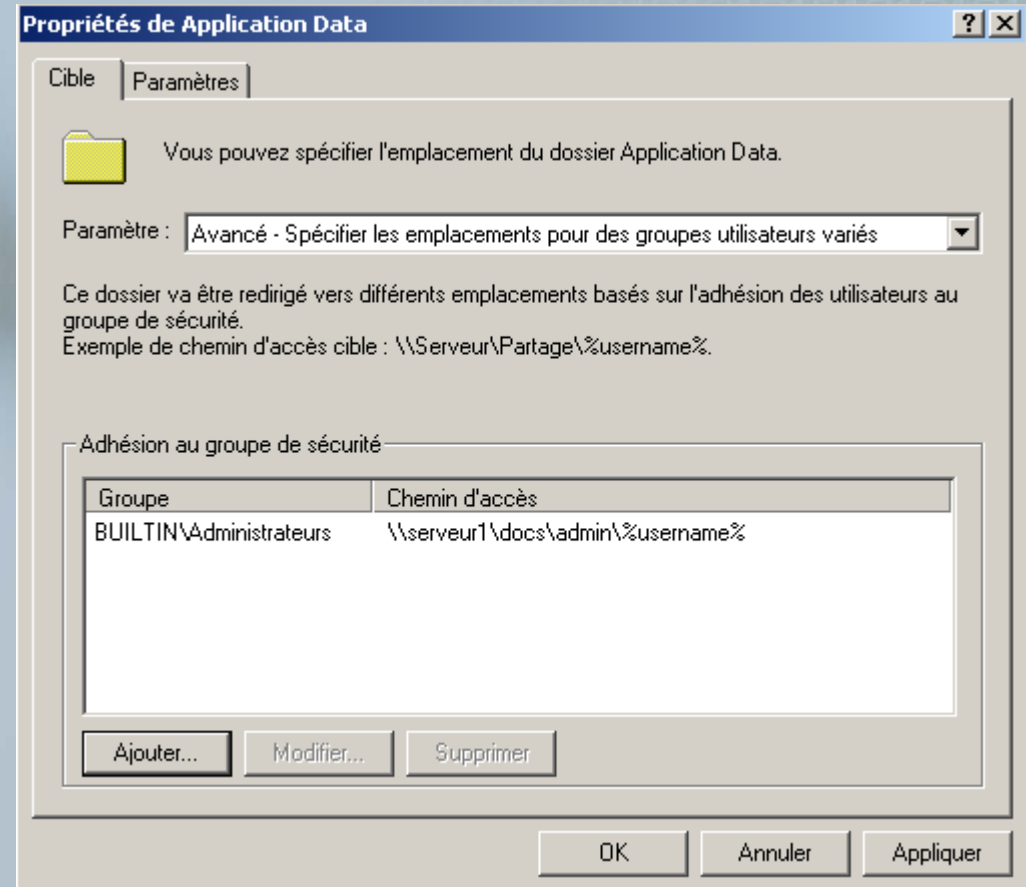


Administration Windows 2003

GPO: Redirection de dossiers "Avancé"

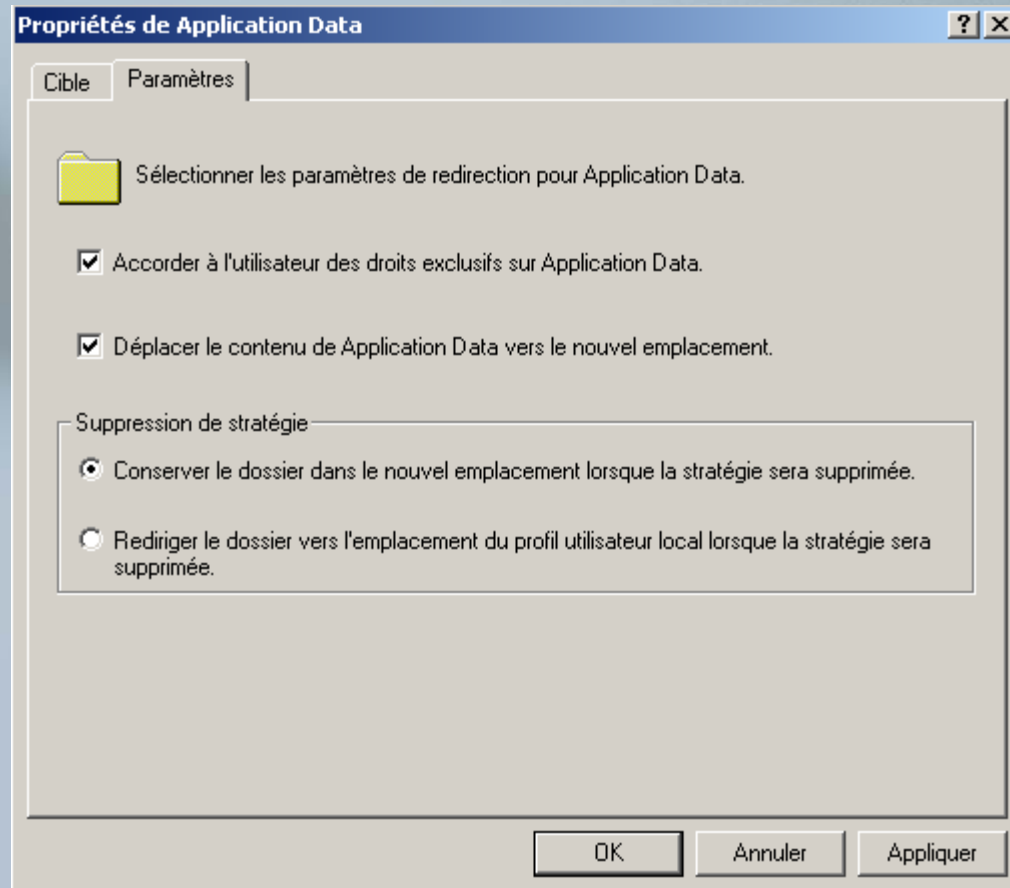
- Le paramétrage "Avancé" permet de définir différents dossiers destination selon l'appartenance de groupe

- Le paramètre %username% sert à les placer dans différents dossiers



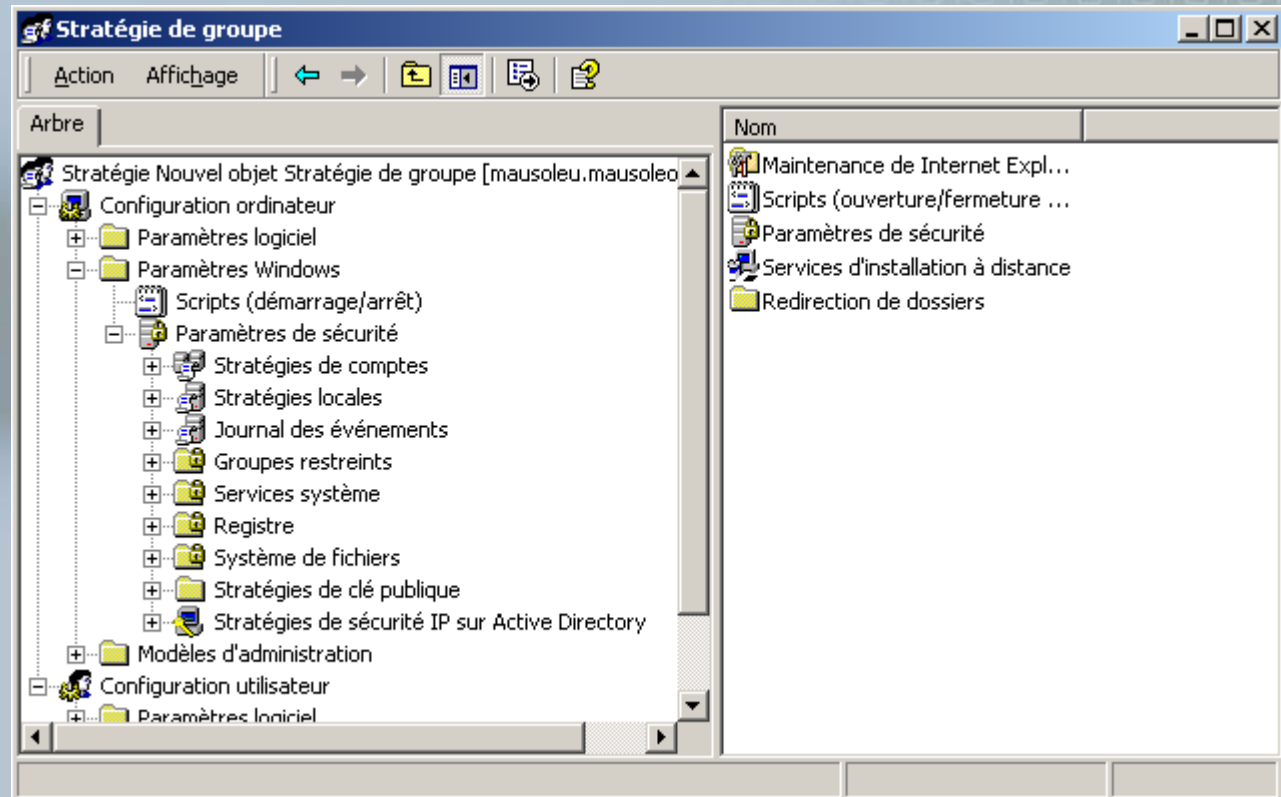
Administration Windows 2003

GPO: Redirection de dossiers, Paramètres



Administration Windows 2003

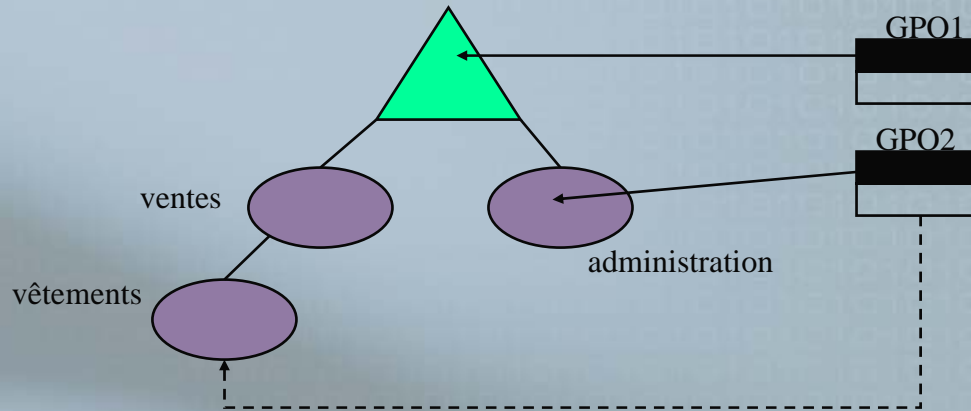
GPO: Paramètres de sécurité (1)



- Outils puissant permettant de renforcer les standards de sécurité de groupes d'ordinateurs

Administration Windows 2003

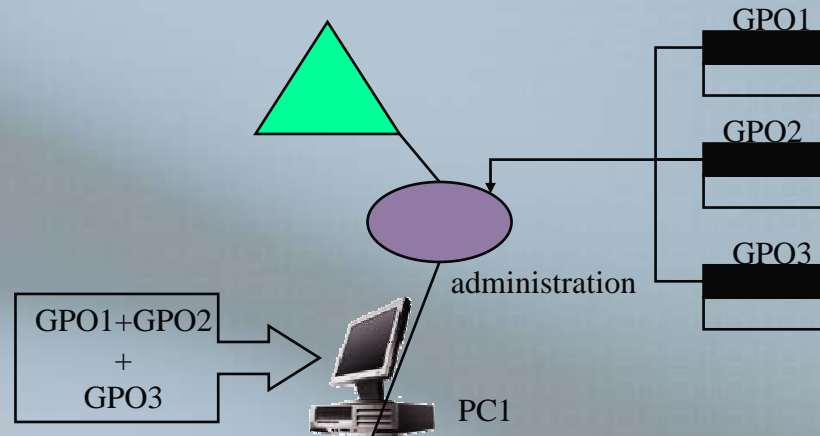
GPO: Liens



- Lorsque vous créez un GPO, un lien initial est établi, vous pouvez rompre ce lien et garder le GPO
- Vous pouvez lier les GPO aux autres domaines, OU et sites

Administration Windows 2003

GPO: Liens

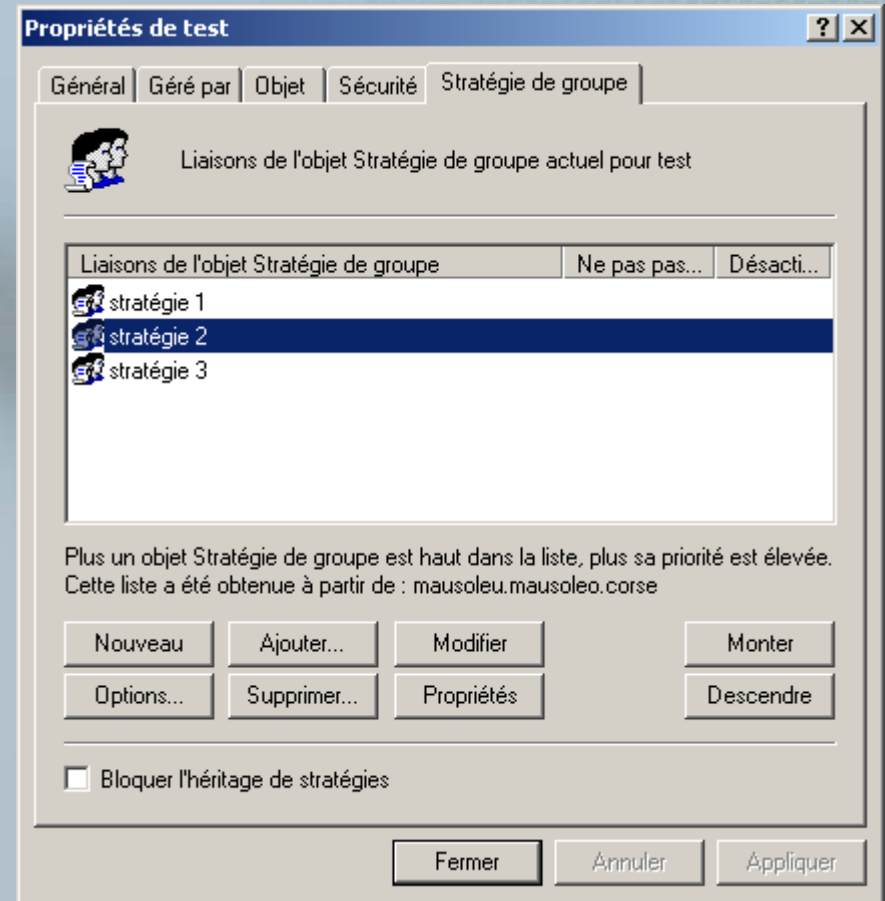


- Plusieurs GPO peuvent être liés aux domaines, OU et sites (utile pour compartimenter les stratégies).
- Les stratégies sont cumulatives.

Administration Windows 2003

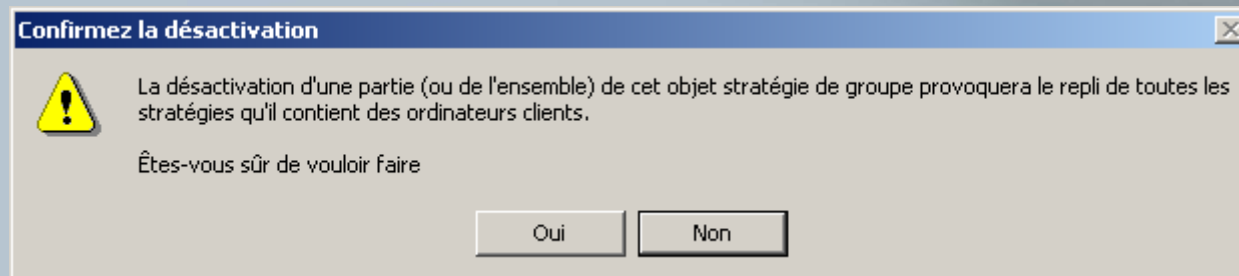
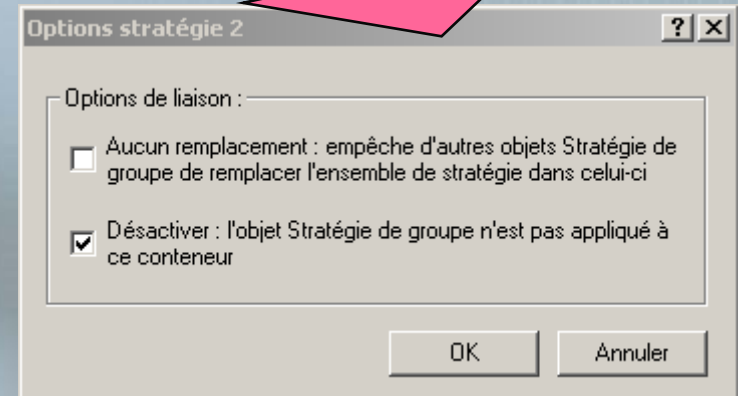
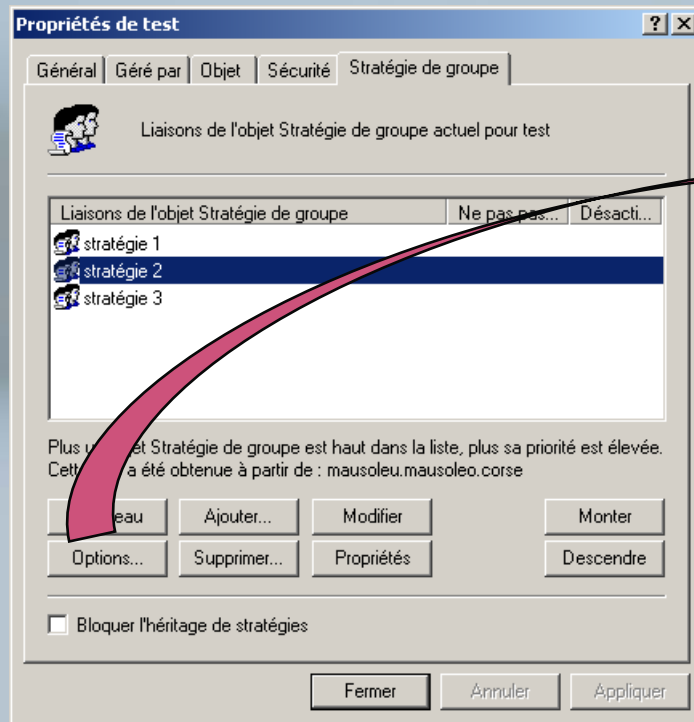
GPO: paramètres en conflit

- Les GPO du haut de liste sont prioritaires et prévalent



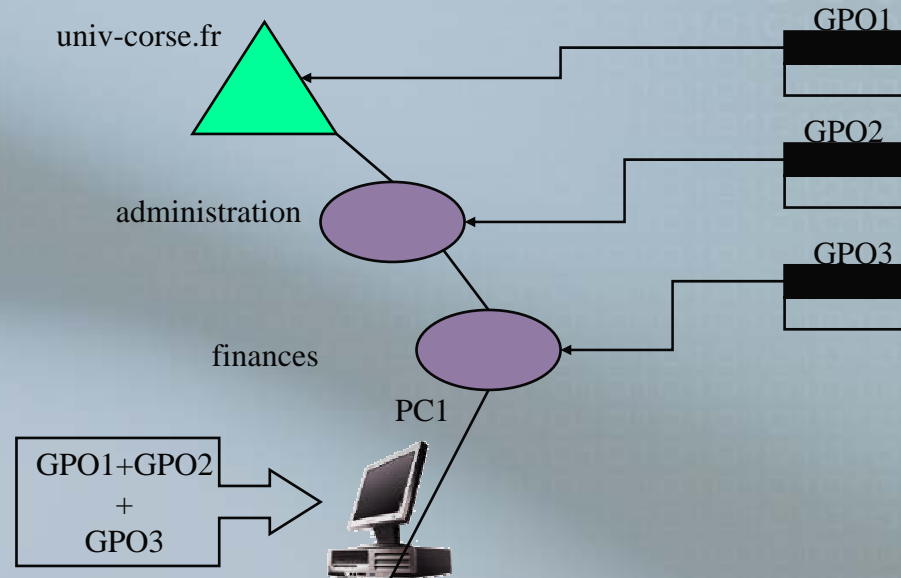
Administration Windows 2003

GPO: Désactivation des stratégies



Administration Windows 2003

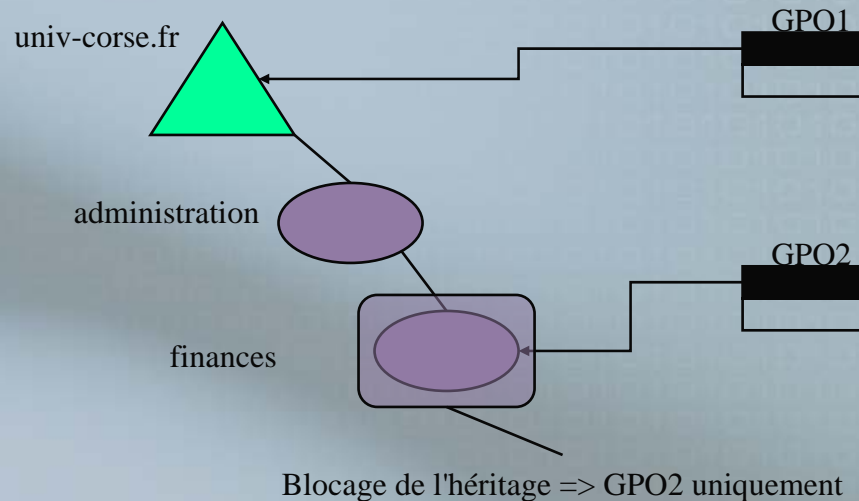
GPO: Héritage



- Un objet conteneur hérite aussi des stratégies des conteneurs parents.
- L'ordre d'application est Local Site Domaine OU.
- La dernière stratégie appliquée est prioritaire en cas de conflit

Administration Windows 2003

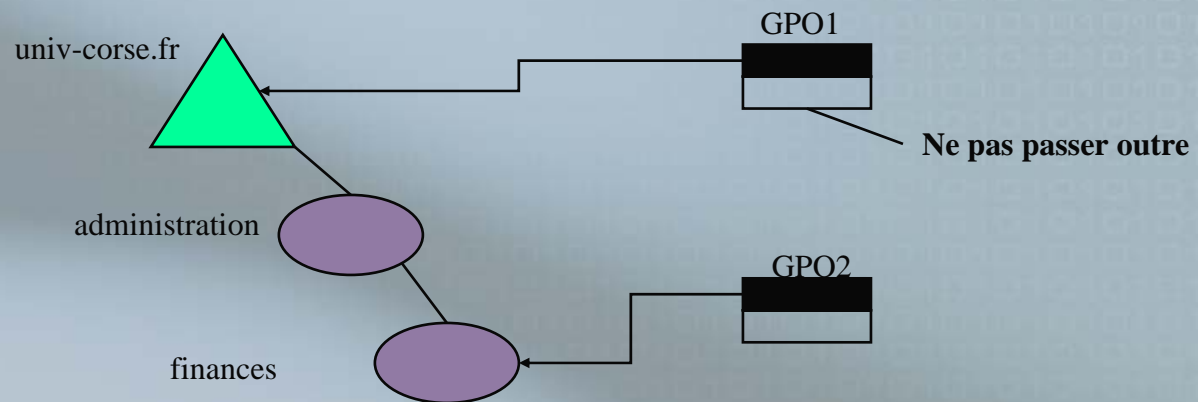
GPO: blocage de l'héritage



- Tout objet conteneur de l'AD peut bloquer l'héritage des GPO liés aux conteneurs parents.
- Seuls les GPO directement liés au conteneur affecteront son contenu

Administration Windows 2003

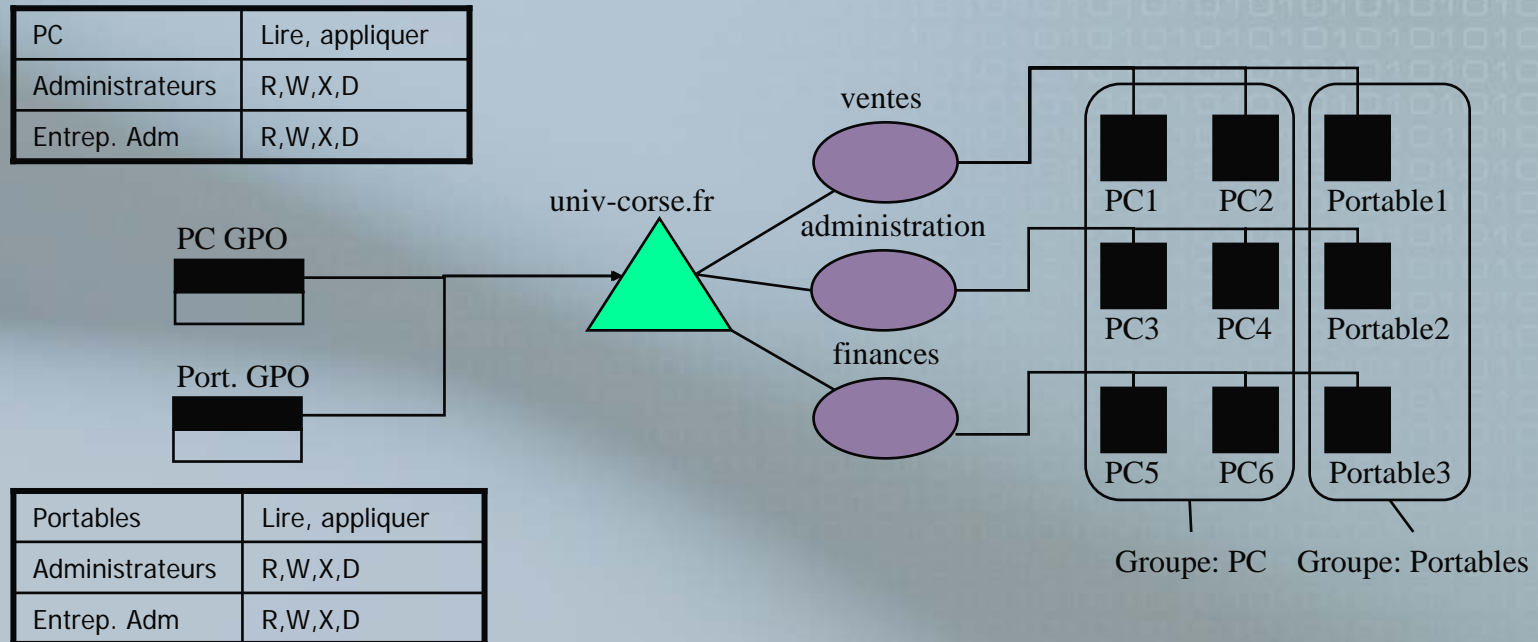
GPO: Ne pas passer outre



- L'option "Ne pas passer outre" empêche les GPO localisées plus bas dans l'arborescence de modifier des paramètres définis à un niveau supérieur.
- Cette option prévaut aussi sur le blocage de l'héritage.

Administration Windows 2003

GPO: Filtrage

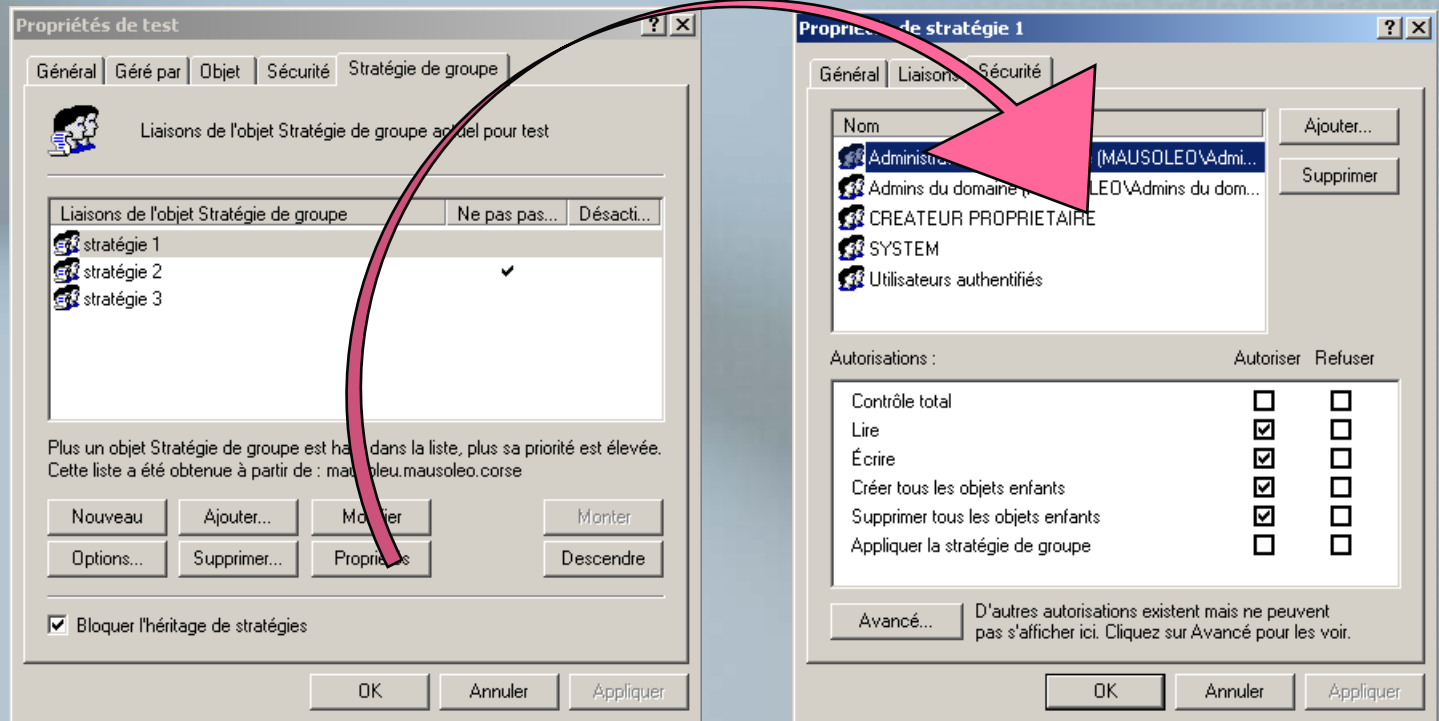


-La structure d'une stratégie de groupe peut être contrôlée par la DACL du GPO.

-Seuls les groupes ayant les autorisations appropriées peuvent appliquer l'objet stratégie.

Administration Windows 2003

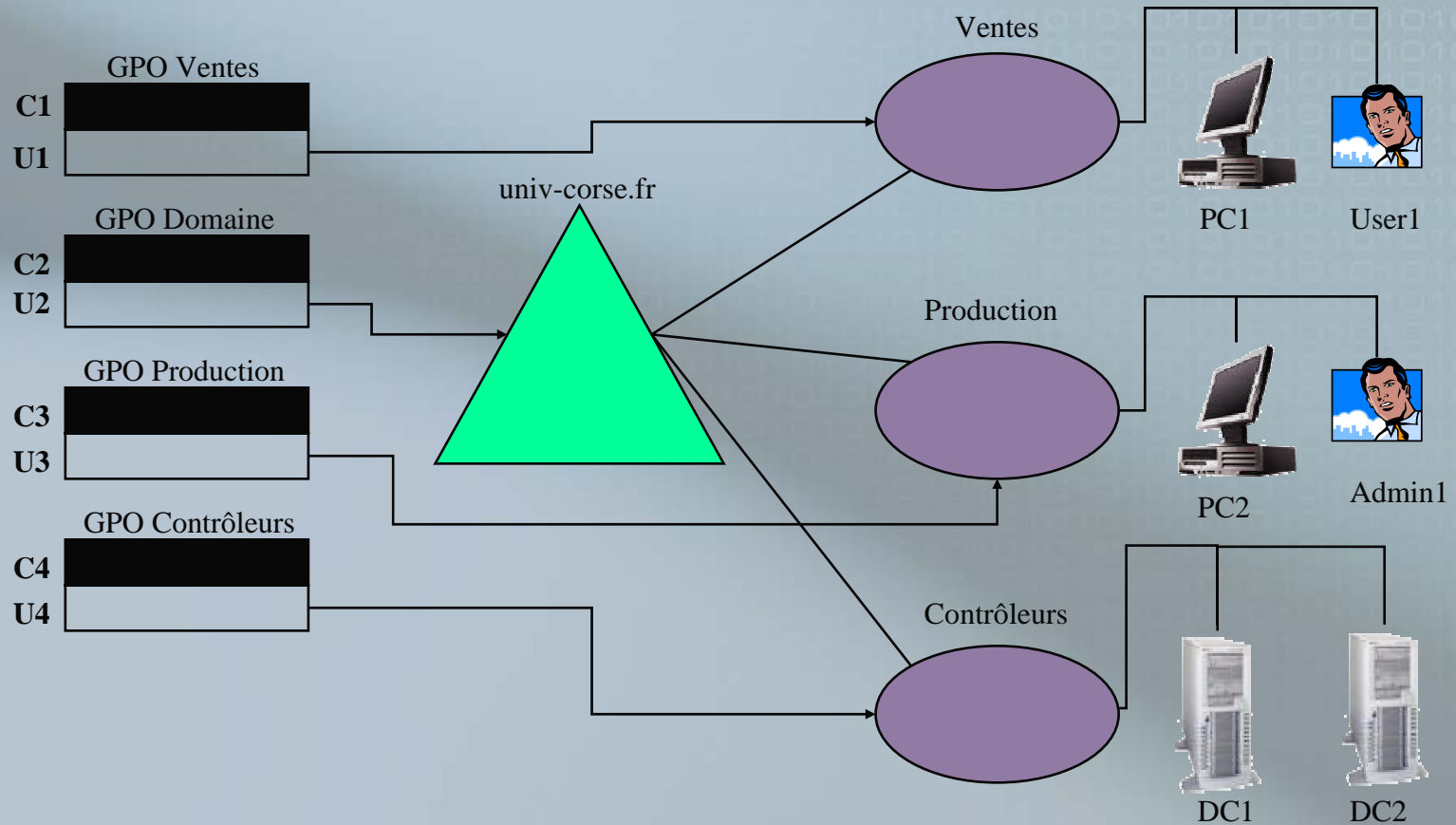
GPO: Filtrage (suite)



-Un ordinateur ou un utilisateur doit avoir la permission "Appliquer la stratégie de groupe" pour utiliser un GPO

Administration Windows 2003

GPO: Combiner les configurations



Administration Windows 2003

GPO: Combiner les configurations

■ Pour le PC1

- démarrage:
C2+C1
- login
 - User1: U2+U1
 - Admin1: U2+U3

■ Pour le DC1

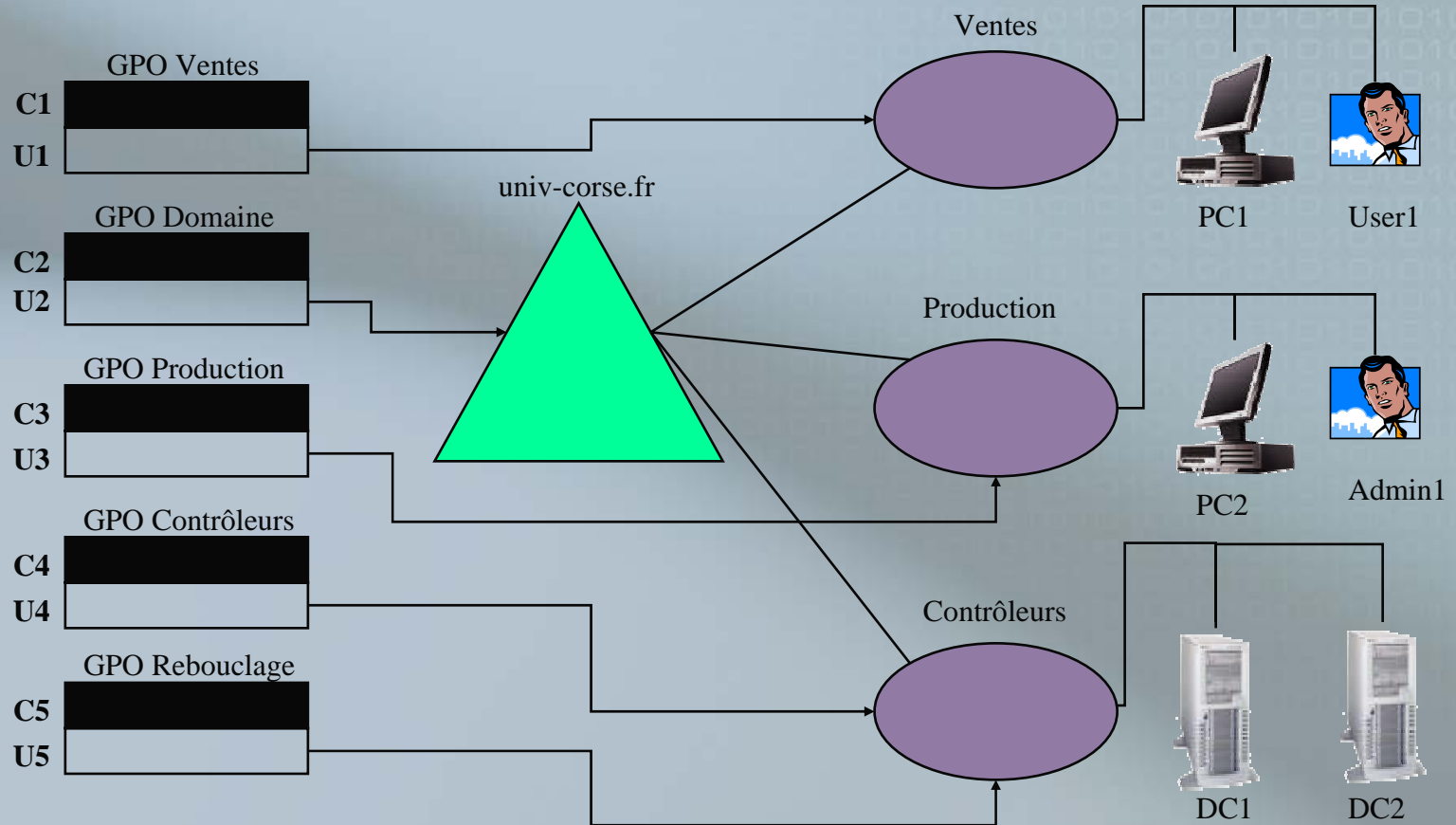
- démarrage:
C2+C4
- login
 - Admin1: U2+U3

■ Pour le PC2

- démarrage:
C2+C3
- Login
 - User1: U2+U1
 - Admin1: U2+U3

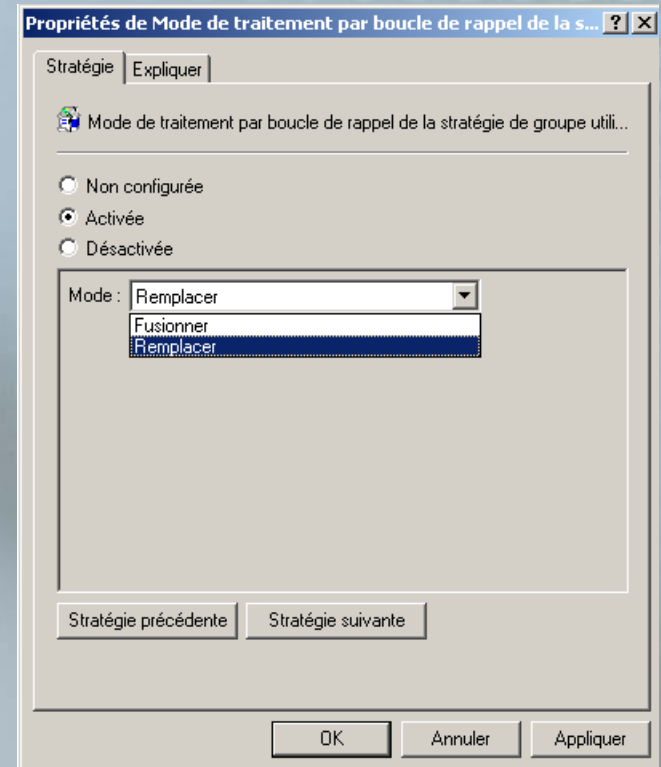
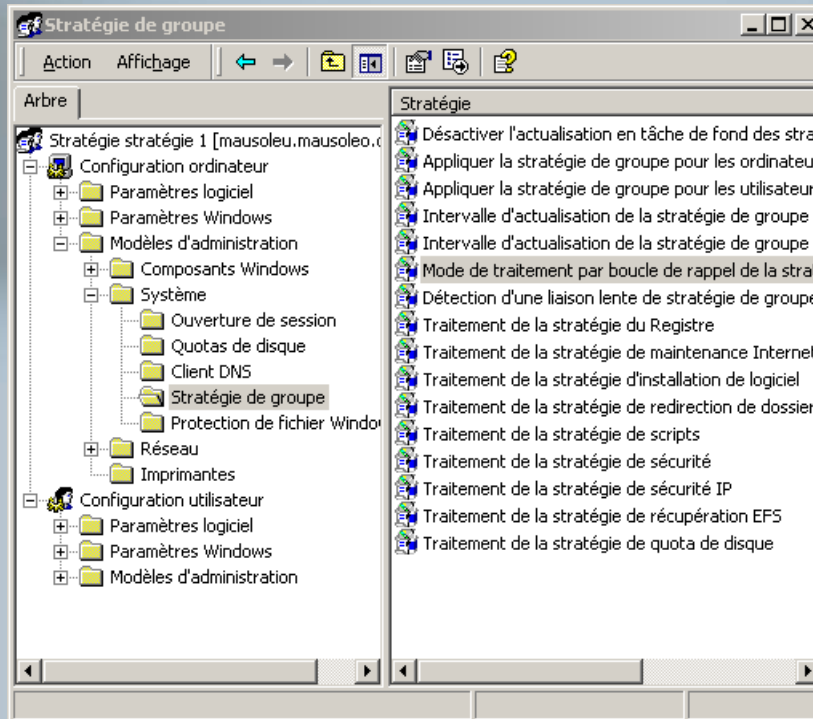
Administration Windows 2003

GPO: Processus de rebouclage



Administration Windows 2003

GPO: Processus de rebouclage



- Fusionner: C2+C4+C5 et U2+U3 + U2+U4+U5
- Remplacer: C2+C4+C5 et U2+U4+U5

Maintenance des GPOs

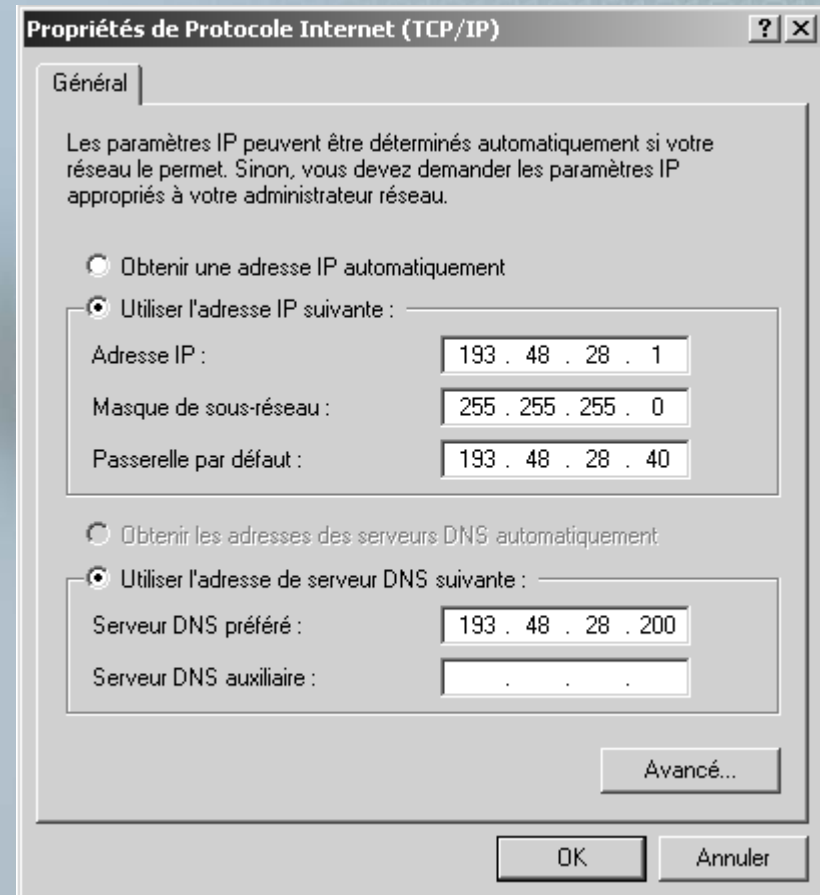
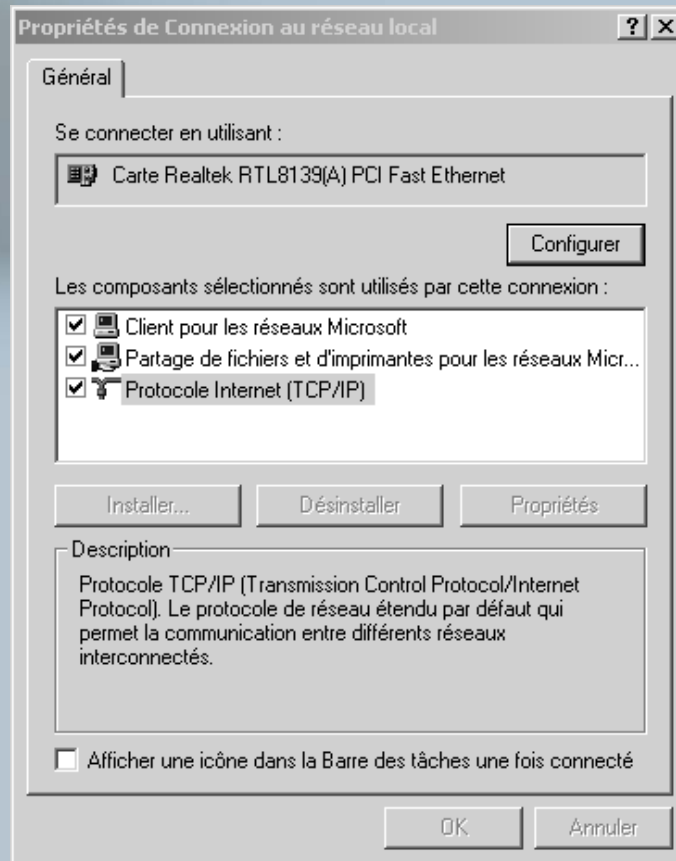
- Outils du support de Microsoft Windows 2000
 - Netdiag.exe
 - Replmon.exe
- Kit de ressources techniques Microsoft Windows 2000 server
 - Gpotool.exe
 - Gpresult.exe

Utilisation des GPOs

- Déployer des applications
- Appliquer des services packs
- Mettre à jour et supprimer des applications
- Affecter des scripts à des utilisateurs et à des ordinateurs
- Rediriger certains dossiers d'utilisateur ou de groupe
- Paramétrer les fichiers hors connexion
- Configurer l'environnement utilisateur

Protocoles et services réseau

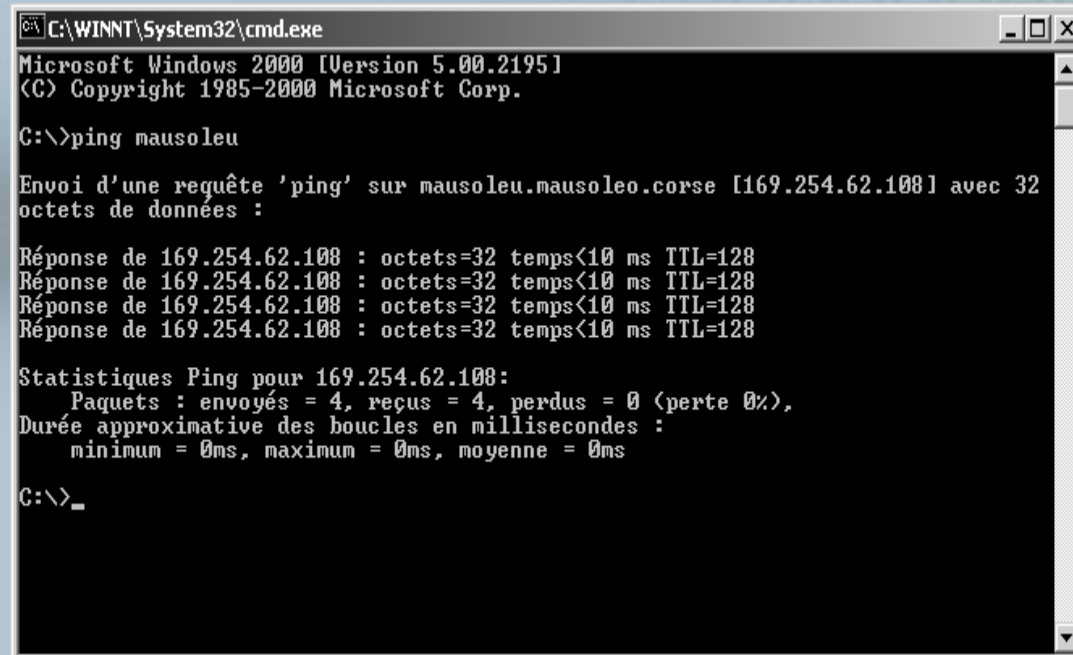
TCP/IP: configuration



Protocoles et services réseau

TCP/IP: dépannage et test

- Ping
- Ipconfig
- Hostname
- Route
- Tracert
- FTP
- Telnet



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping mausoleu

Envoi d'une requête 'ping' sur mausoleu.mausoleo.corse [169.254.62.108] avec 32
octets de données :

Réponse de 169.254.62.108 : octets=32 temps<10 ms TTL=128
Réponse de 169.254.62.108 : octets=32 temps<10 ms TTL=128
Réponse de 169.254.62.108 : octets=32 temps<10 ms TTL=128
Réponse de 169.254.62.108 : octets=32 temps<10 ms TTL=128

Statistiques Ping pour 169.254.62.108:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    minimum = 0ms, maximum = 0ms, moyenne = 0ms

C:\>_
```

Protocoles et services réseau

DHCP

- DHCP permet de centraliser la configuration des données TCP/IP et d'affecter dynamiquement les adresses IP.
- En plus de l'adresse IP, il est possible de télécharger sur le client DHCP plus de 50 paramètres supplémentaires, en particulier:
 - Le masque de sous-réseau, la passerelle par défaut, les serveurs WINS, les serveurs DNS.

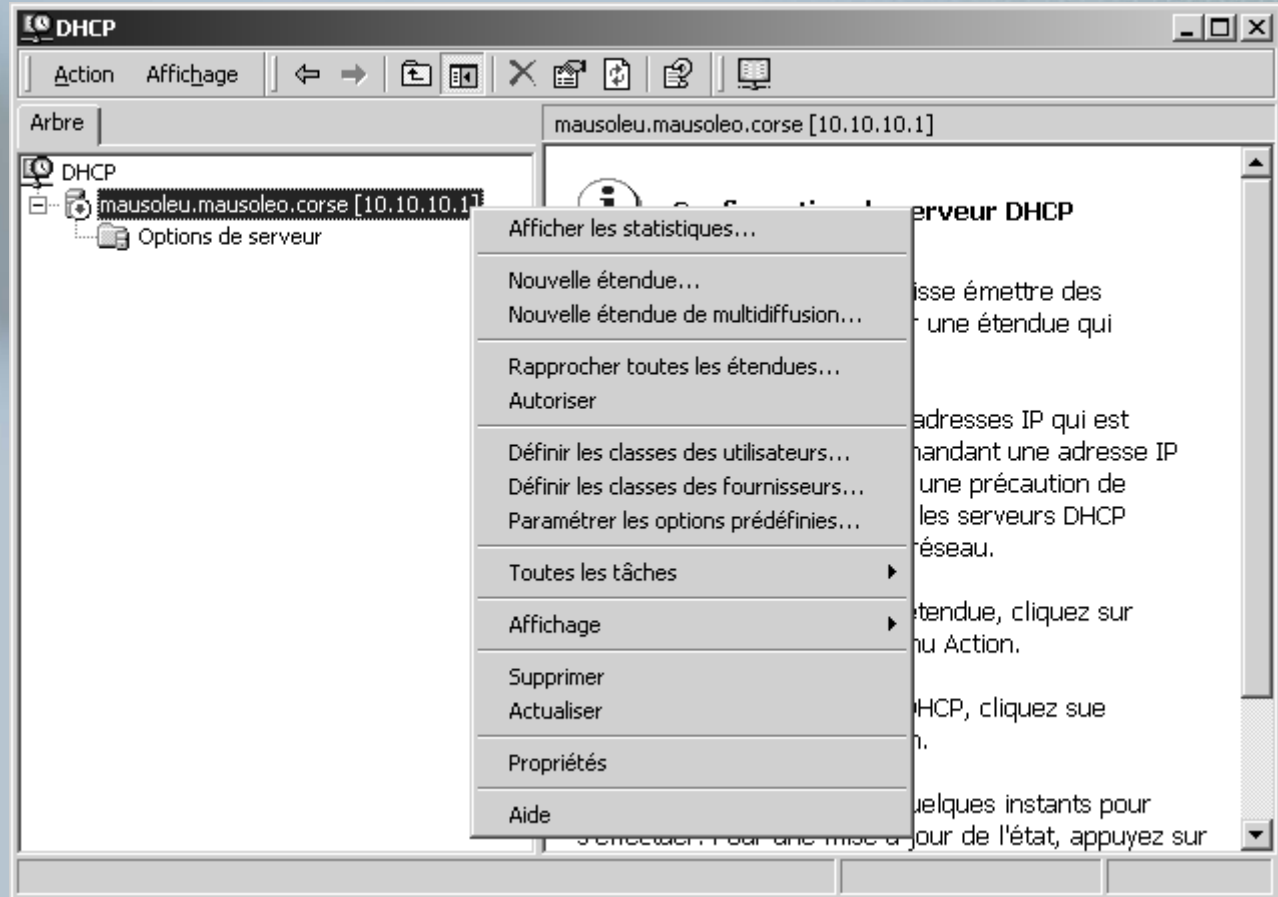
Protocoles et services réseau

DHCP

- Les adresses IP sont difficiles à suivre et à gérer
 - Sans DHCP une nouvelle adresse IP doit être affectée chaque fois qu'une machine est ajoutée
 - Vous devez vous assurer qu'elle est unique.
- DHCP rend plus facile les modifications futures du réseau
 - Nouveau routeur.
- Certaines sociétés manquent d'adresse IP
 - DHCP optimise l'utilisation des adresses IP

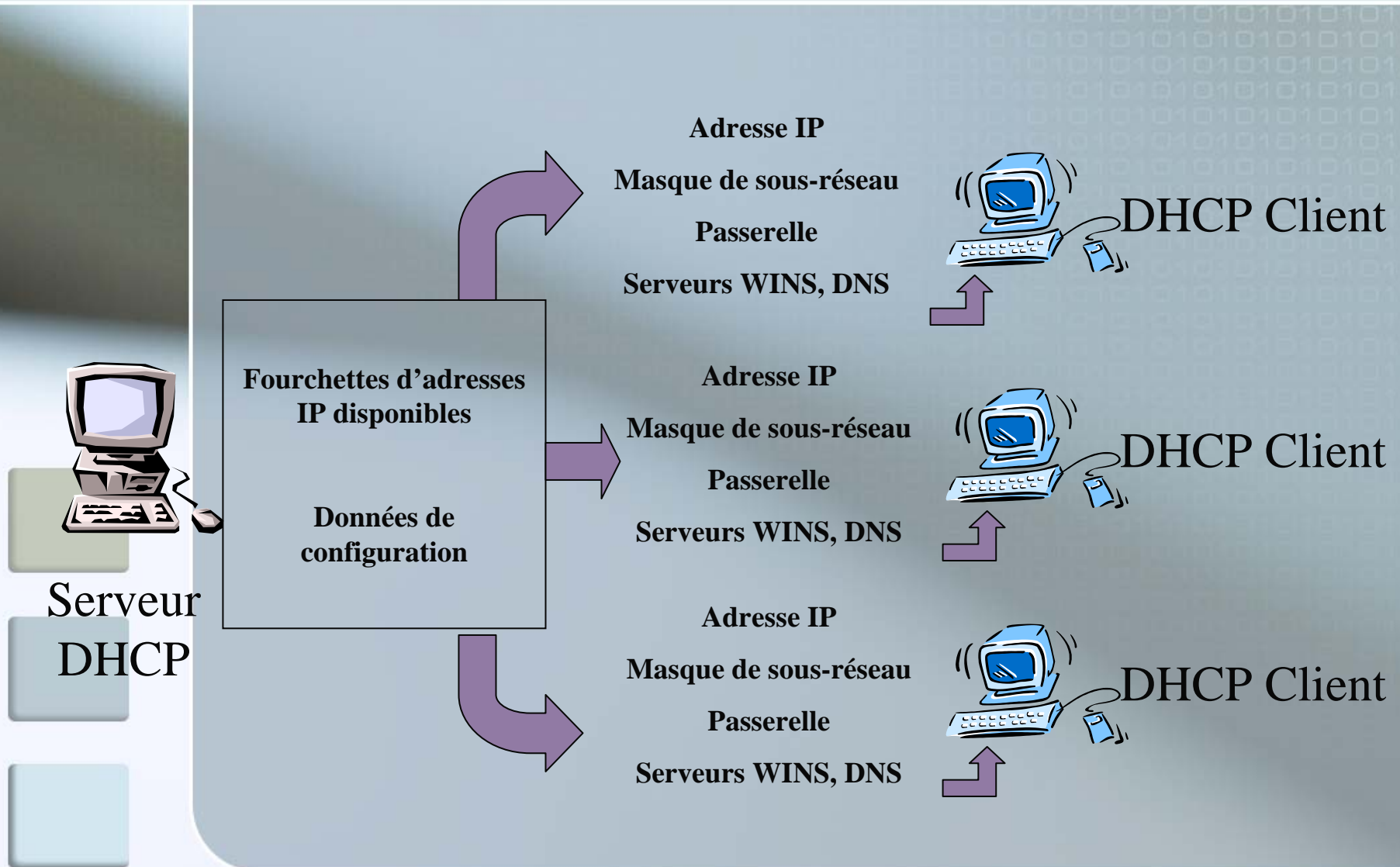
Protocoles et services réseau

DHCP



Protocoles et services réseau

DHCP: gestion centralisée



Protocoles et services réseau

DHCP: les clients

- Les clients DHCP peuvent être:
 - Windows 2000 Server et Professionnel, 2003
 - NT Server , NT Workstation, 2000, XP
 - Windows 95, 98, 3.11 (TCP/IP 32-bit)
 - Microsoft Network Client V 3.0 pour MS-DOS (TCP/IP 16-bit)
 - LAN Manager V 2.2c
 - Autres clients DHCP compatibles (UNIX, MacIntosh, etc...)

Un serveur 2003 DHCP ou WINS ne peut pas être un client DHCP

Protocoles et services réseau

DHCP: étendues

- Une étendue est la plage d'adresse IP mise à la disposition des clients DHCP
- Des plages d'adresse peuvent être exclues et des adresses statiques réservées aux ordinateurs non DHCP

Créer étendue - 193.48.28.175

Réserve d'adresses IP

Adresse de début : . . .

Adresse de fin : . . .

Masque de sous-réseau : . . .

Plage d'exclusion :

Adresse de début : . . .

Adresse de fin : . . .

Ajouter >

< Supprimer

Adresses exclues :

Durée de bail

Illimité

Limité à : 3 Jour(s) 00 Heure(s) 00 Minutes

Nom : _____

Commentaire : _____

OK Annuler Aide

Protocoles et services réseau

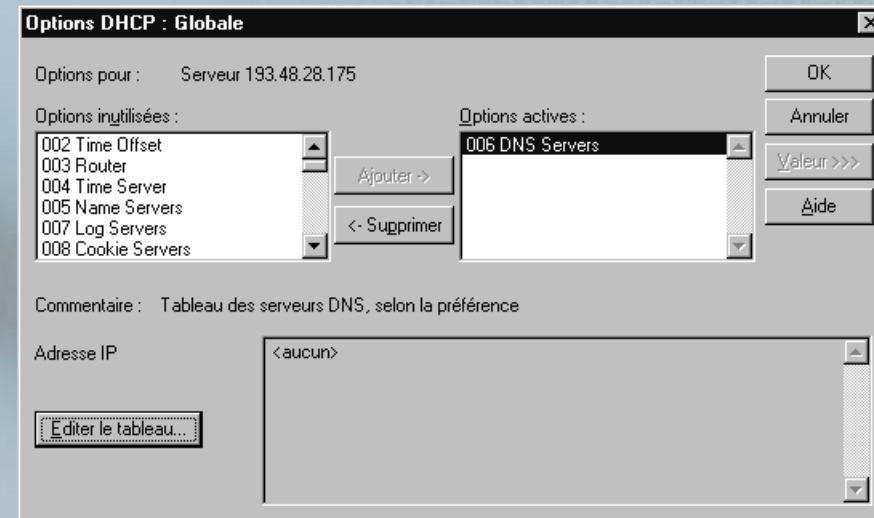
DHCP: baux

- Le serveur DHCP loue l'adresse IP avec un bail qui définit la durée d'utilisation de l'adresse IP par l'ordinateur client
 - La valeur par défaut est de 3 jours
- A 50% de la durée du bail, le client DHCP essaie automatiquement de renouveler le bail
 - Par un paquet DhcpRequest
- Si le renouvellement n'est pas possible, à 87,5% de la durée du bail, le client DHCP essaie d'obtenir une nouvelle adresse IP d'un autre serveur DHCP

Protocoles et services réseau

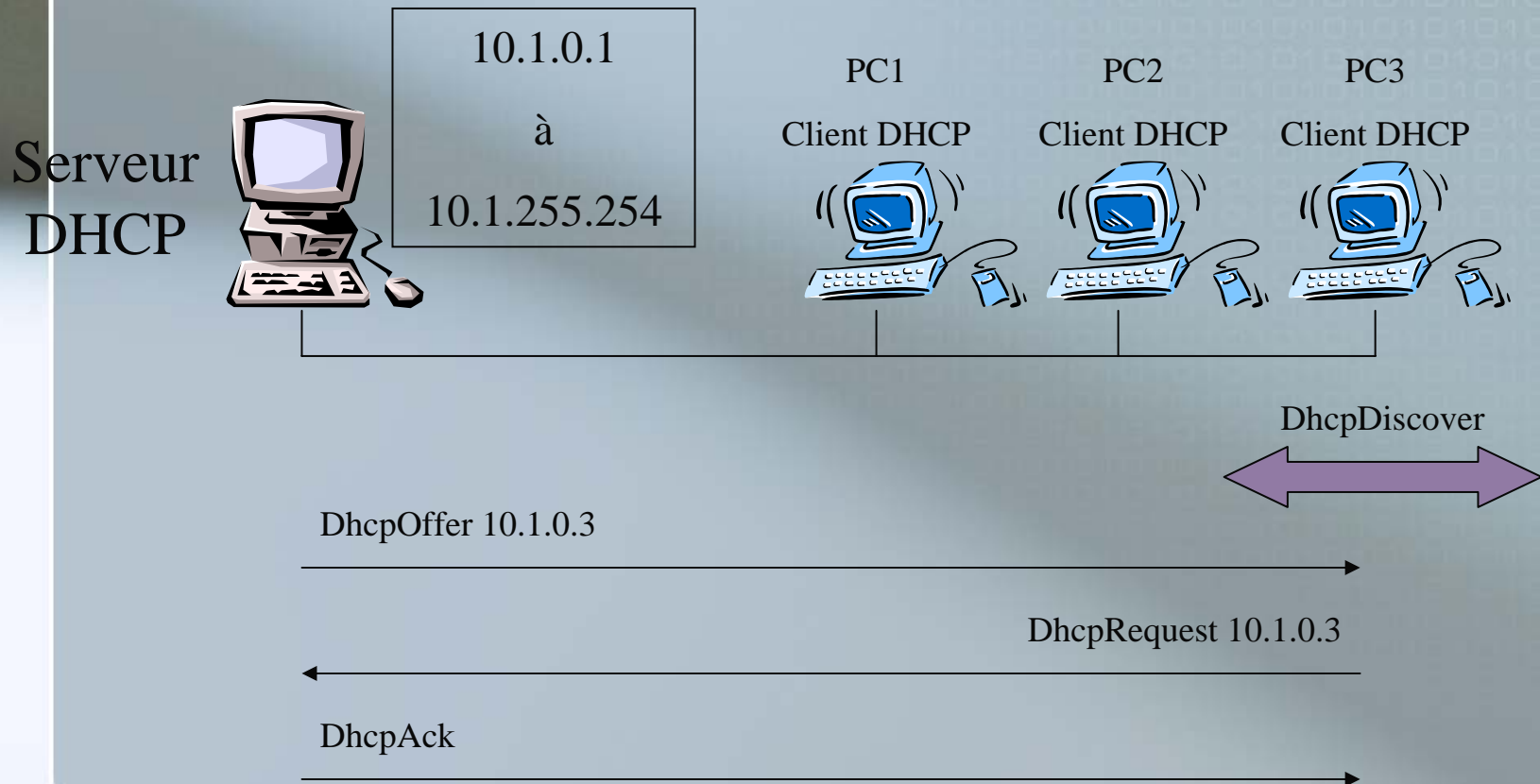
DHCP: options

- Les options DHCP peuvent être définies:
 - Globalement (pour toutes les étendues)
 - Pour une étendue (la plage d'adresses IP)
 - Pour un ordinateur spécifique (réservation statique)



Protocoles et services réseau

DHCP: obtention d'adresses



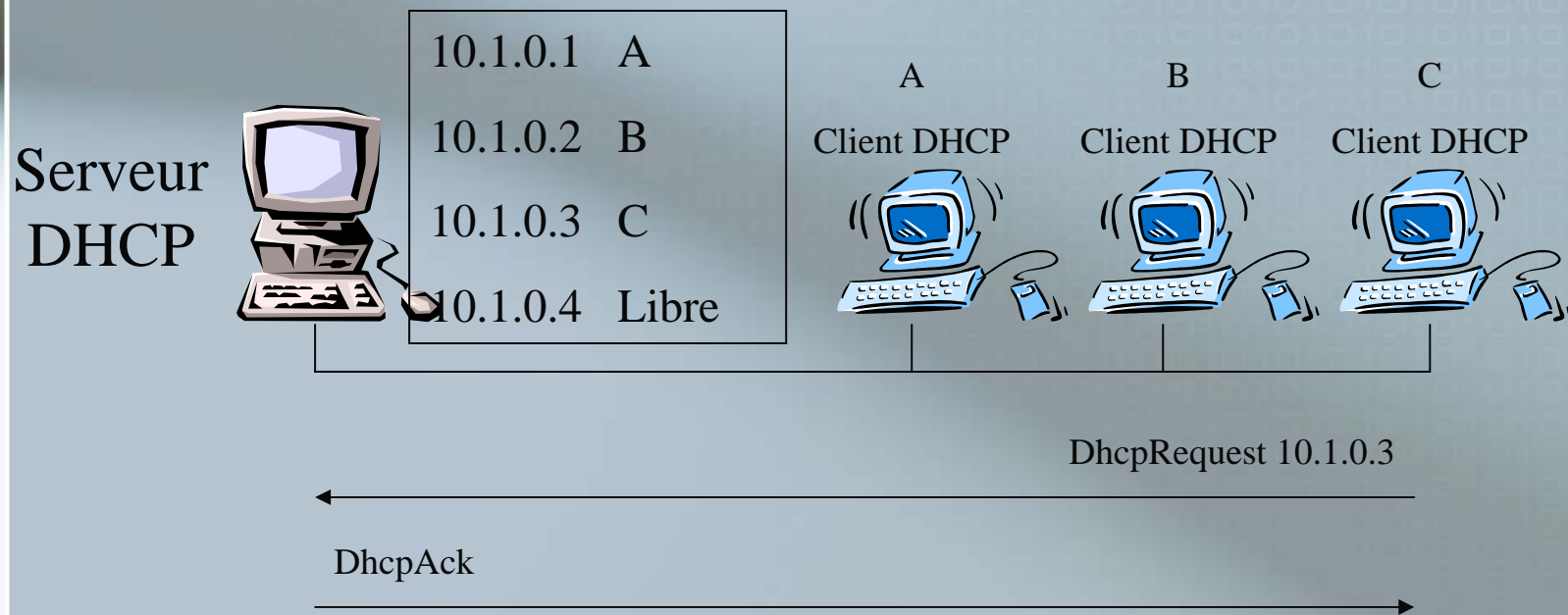
Protocoles et services réseau

DHCP: redémarrage du client

- Dans l'implémentation de Microsoft, quand un client est redémarré, il envoie un paquet DhcpRequest
 - Au lieu d'un DhcpDiscover
- Le DhcpRequest contient une requête pour l'adresse IP précédemment affectée
 - Le serveur DHCP essaiera de satisfaire le client
- Si l'adresse IP demandée n'est plus disponible, le client reçoit un DhcpNack et doit essayer à nouveau à partir de zéro.

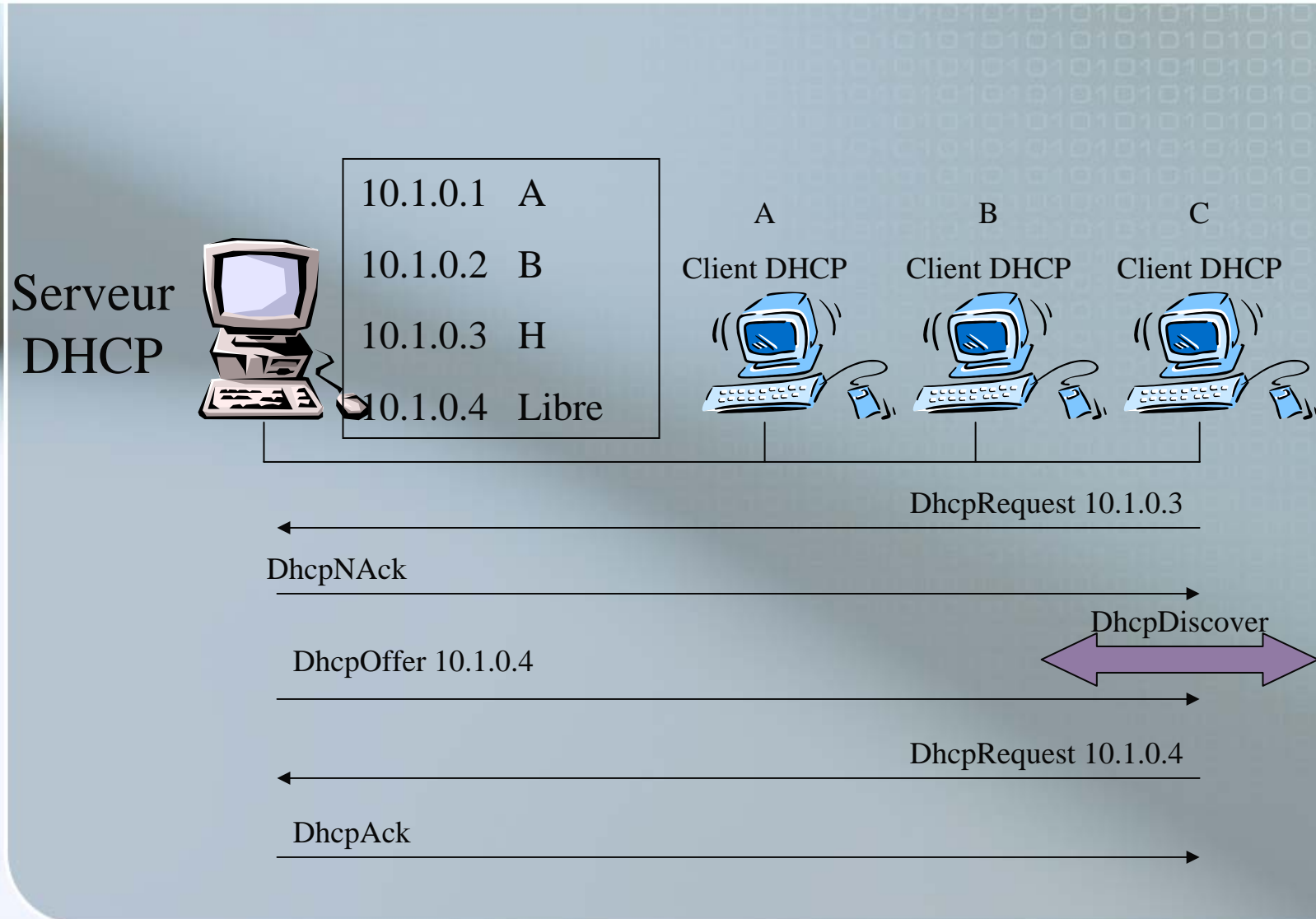
Protocoles et services réseau

DHCP: disponibilité d'adresse



Protocoles et services réseau

DHCP: indisponibilité d'adresse



Protocoles et services réseau

DHCP: si le serveur ne réponds pas ?

- Si un client ne reçoit pas un paquet DhcpOffer du serveur DHCP, il diffusera une requête 4 fois
 - A 2, 4, 6 et 8 secondes d'intervalle
- Si le client n'a toujours pas de réponse, il essaie encore 5 minutes plus tard
 - Jusqu'à ce que client reçoive un DhcpOffer, TCP/IP n'est pas lié
 - L'interface n'est pas connecté au réseau

Protocoles et services réseau

autoriser un serveur DHCP

- Autoriser un serveur DHCP
 - Pour éviter les conflits d'adresse IP. Et la prolifération de serveurs DHCP.
- Agent de relais DHCP
 - Passage des routeurs impossible pour les trames DHCP envoyées en broadcast par les clients.

Protocoles et services réseau

Maintenance du protocole IP et de DHCP

- Surveillance DHCP
- Dépannage DHCP
- Utilitaires TCP/IP
 - Ping
 - -t
 - -a
 - -n
 - -l
 - Pathping

Protocoles et services réseau

Maintenance du protocole IP et de DHCP

- Route
 - Print
 - Add
- Arp
 - -a
- Ipconfig
 - /all
 - /registerdns
 - /displaydns
 - /flushdns
 - /release
 - /renew
 - /showclassid <nom de la connexion réseau>
 - /setclassid <nom de la connexion réseau>

Protocoles et services réseau

Maintenance du protocole IP et de DHCP

- Netdiag
- Nslookup
- Netstat
 - -a
 - -e
 - -s
 - -r

Protocoles et services réseau

Maintenance du protocole IP et de DHCP

■ Nbtstat

- -a
- -A <adresse IP distante>
- -c
- -n
- -r
- -R
- -RR
- -S
- -S

Protocoles et services réseau

WINS (Windows Internet Naming Service)

- WINS a été conçu pour fournir une solution souple au problème de la localisation des ressources NetBIOS dans les réseaux TCP/IP routés.
- WINS fournit
 - Enregistrement dynamique des noms NetBIOS.
 - Résolution de noms NetBIOS efficace
 - Réduction des diffusions de requête de noms NetBIOS
 - Navigation transparente du voisinage réseau.
 - Duplication de la base de données WINS à travers LAN ou WAN.

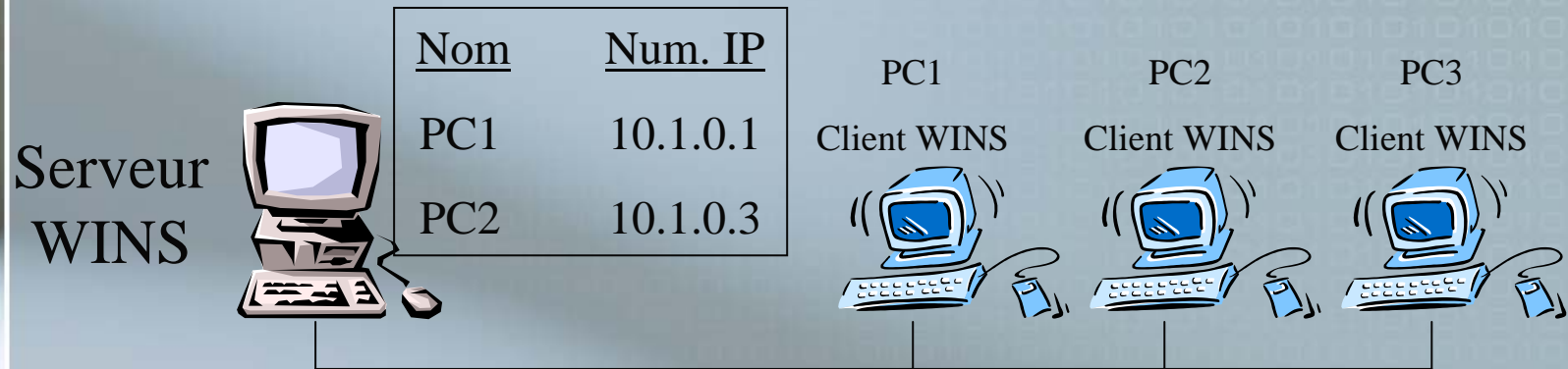
Protocoles et services réseau

WINS (Windows Internet Naming Service)

- WINS est supporté par 2003, 2000, NT, Windows 9x, Windows for Workgroups + TCP/IP 32-bit.
- WINS est un service de mappage de nom NetBIOS vers une adresse IP, c'est à dire un NBNS (NetBIOS Name Server).

Protocoles et services réseau

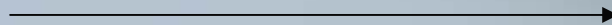
WINS: fonctionnement



Au boot: Je suis PC1, mon IP est 10.1.0.5



Merci, je l'écris



IP de PC1, svp ?

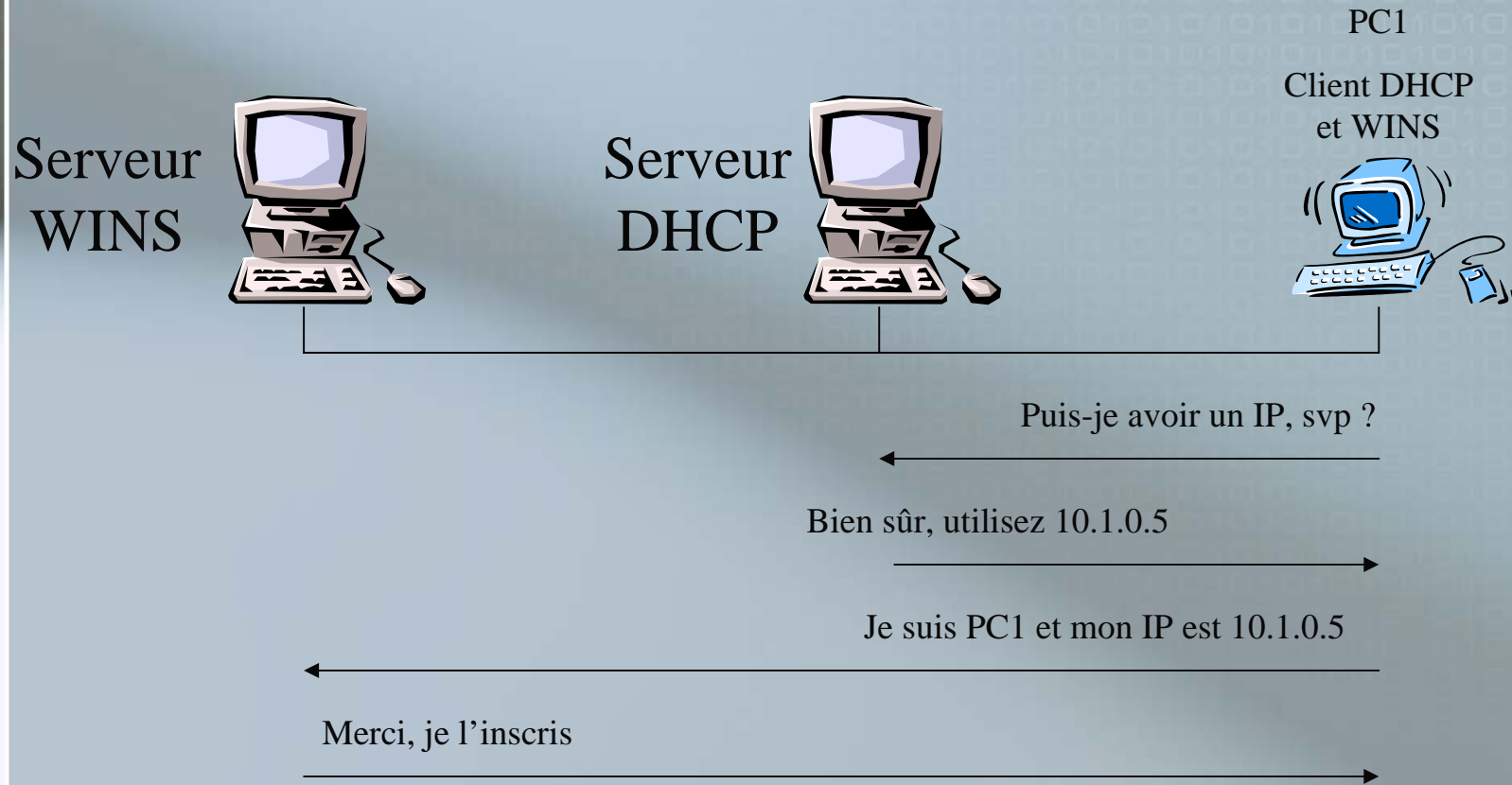


PC1 est 10.1.0.5



Protocoles et services réseau

WINS et DHCP



Protocoles et services réseau

WINS: duplication

- Il est important d'installer plusieurs serveurs WINS
 - Pour avoir une tolérance de panne
 - Pour distribuer la charge des requêtes de nom
- Normalement les serveurs WINS seront configurés pour dupliquer entièrement et réciproquement les bases de données
 - Un nom enregistré sur un serveur WINS A sera disponible sur un serveur WINS B

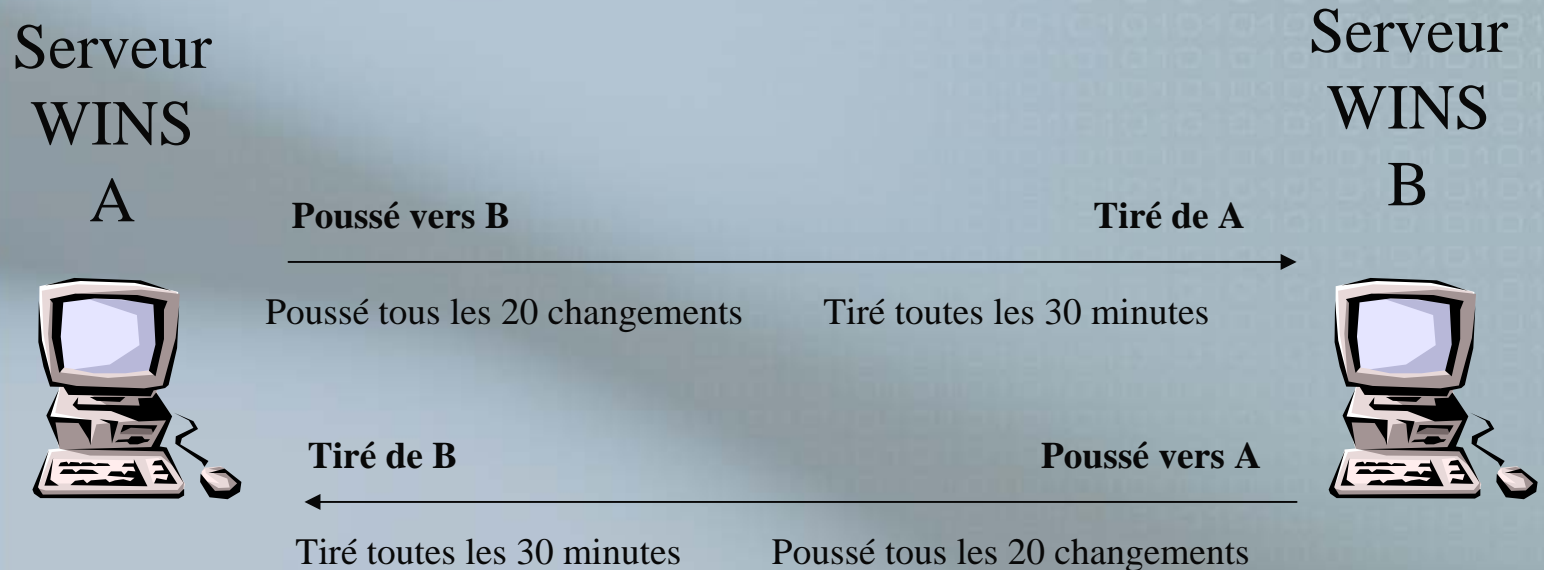
Protocoles et services réseau

WINS: Architecture de duplication

- Association de duplication
 - Le serveur A utilise le serveur B comme partenaire tiré ; le serveur B utilise le serveur A comme partenaire poussé
 - Le serveur A utilise le serveur B comme partenaire poussé ; le serveur B utilise le serveur A comme partenaire tiré
- Les serveurs WINS fusionnent leurs données
 - Seules les modifications sont dupliquées

Protocoles et services réseau

WINS: Architecture de duplication



Chaque relation peut avoir seulement poussé, seulement tiré ou les 2 ensembles

Protocoles et services réseau

WINS: le Client

- Un client WINS est généralement configuré avec les adresses IP de deux serveurs WINS
 - Le serveur WINS Primaire
 - Le serveur WINS secondaire
- Un client WINS fera 3 tentatives de communication avec le serveur primaire
 - Puis il essaiera le serveur WINS secondaire
- Les serveurs WINS primaires et secondaires doivent se dupliquer mutuellement

Protocoles et services réseau

WINS: le Client

- Lorsqu'un client WINS démarre, il envoie une requête d'enregistrement des noms
 - Nom d'ordinateur, nom d'utilisateur, nom de domaine ...
- Le 16ème caractère d'un nom NetBIOS définit le type de nom NetBIOS

Protocoles et services réseau

WINS: durée de vie

- Les noms sont stockés dans la base de données WINS avec des informations sur la durée de vie
- Les clients WINS renouvellent automatiquement leurs noms sur le serveur WINS avant l'expiration de la durée de vie
- Lorsqu'un ordinateur est arrêté correctement, le nom est enlevé de la base de données WINS

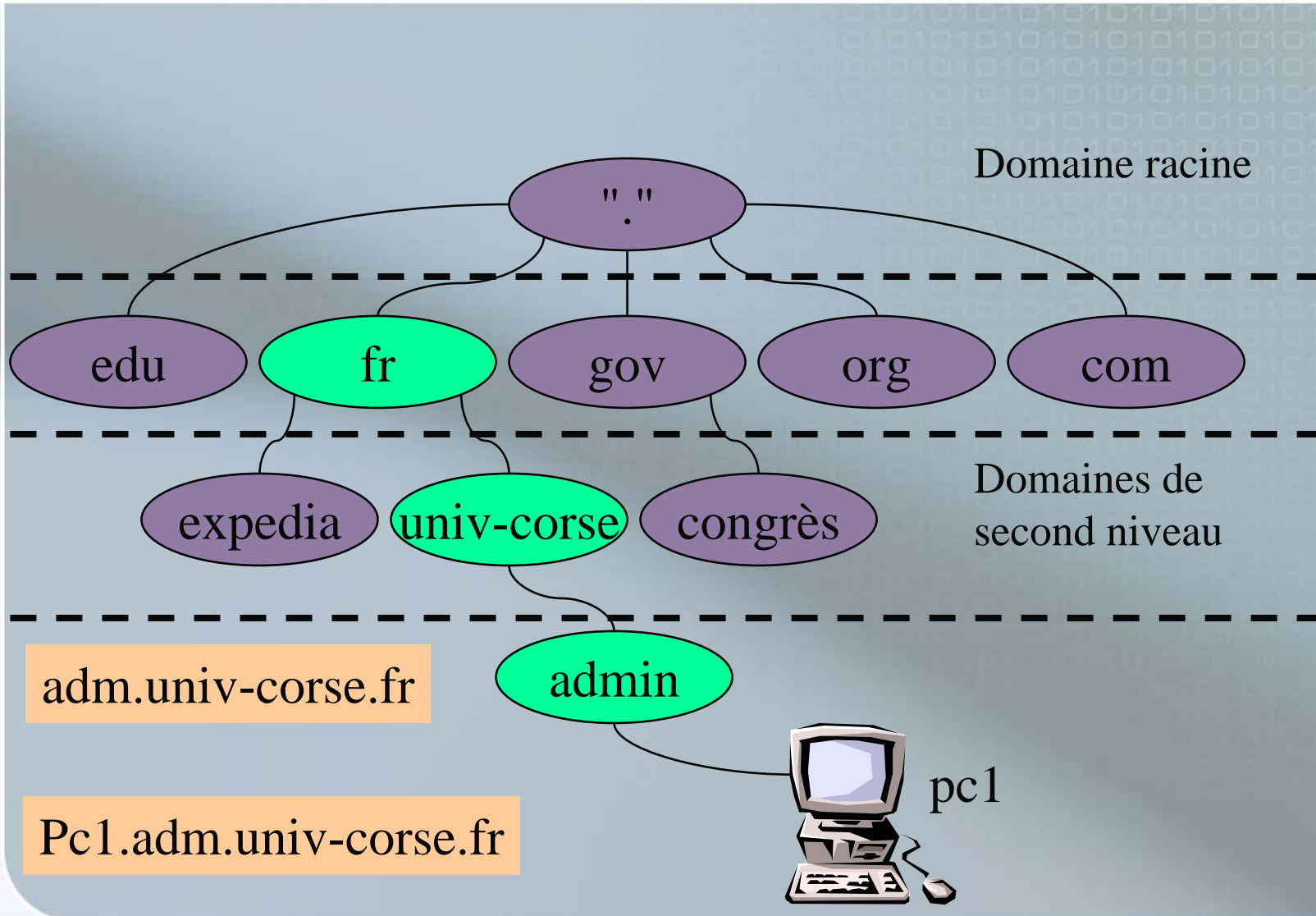
Protocoles et services réseau

DNS

- DNS *domain name space* donne la possibilité d'employer des noms familiers hiérarchiques afin de localiser aisément les ordinateurs et autres ressources sur un réseau TCP/IP
- Un serveur DNS peut être utilisé pour effectuer la résolution des noms
 - Un serveur DNS contient des mappages nom à adresse IP

Protocoles et services réseau

DNS: espace de nommage



Protocoles et services réseau

DNS: espace de nommage

- ROOT est administrée par le Centre d'information Réseau Internet (InterNIC: <http://www.internic.net>)
- Attribution de portion d'espace de nom aux organisations et aux entreprises qui se connectent sur Internet (Serveur DNS):
Nom de domaine

Protocoles et services réseau

DNS: espace de nommage

- Domaines administrés par l'InterNIC:
 - Domaines organisationnels: fonctions primaires ou activité de l'entreprise
 - com, edu, gov, mil, int, net, org, ...
 - Domaines géographiques:
 - fr, jp, nl, ...
 - Domaines inversés: in-addr.arpa

www.Mcours.com

Site N°1 des Cours et Exercices Email: contact@mcours.com

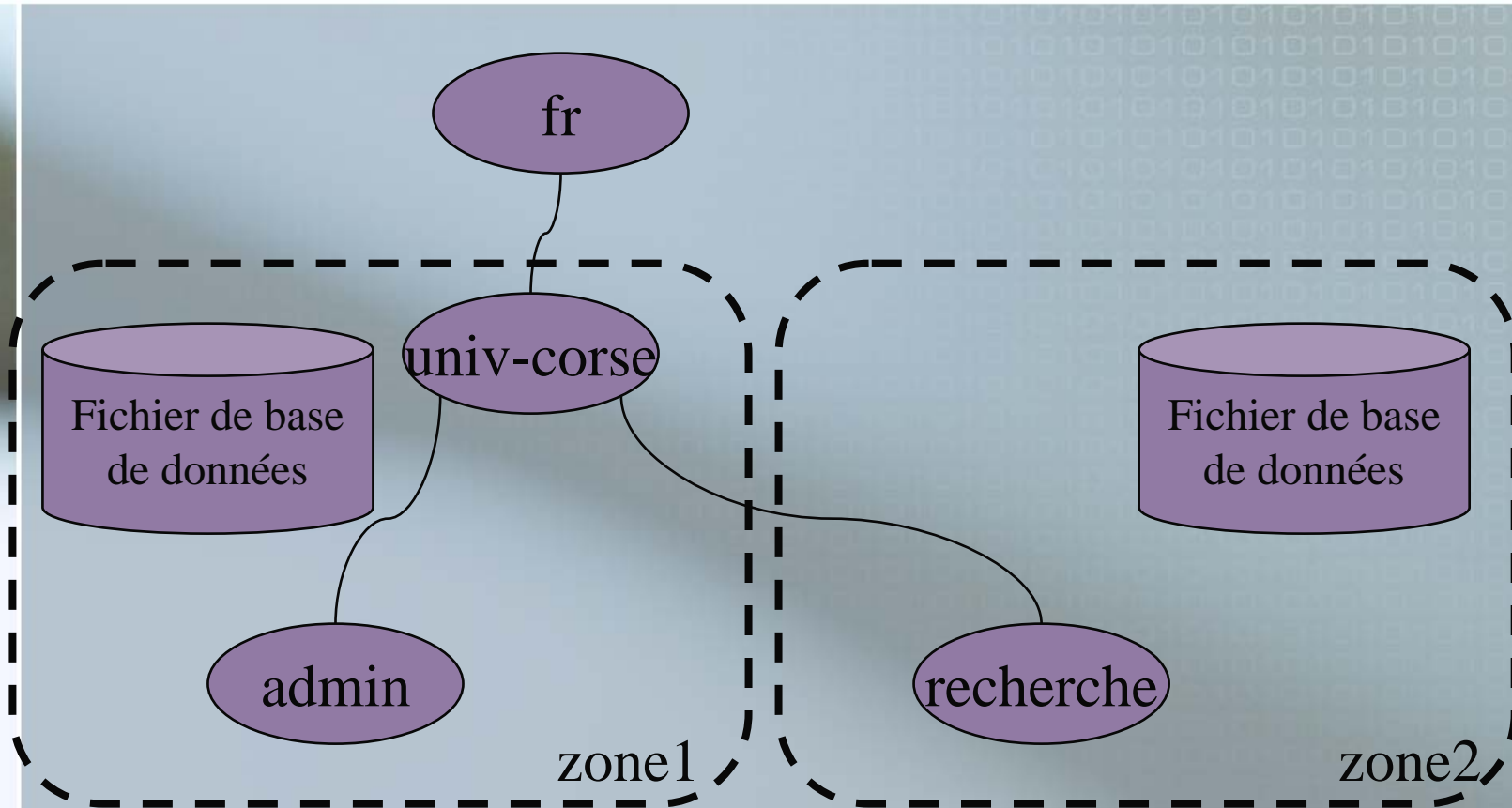
Protocoles et services réseau

DNS: espace de nommage

- Domaines "attribués":
 - Possibilité de créer des sous-domaines reflétant des groupements administratifs
 - Responsabilité de l'attribution de nom aux ordinateurs et aux périphériques réseaux à l'intérieur de leur domaine

Protocoles et services réseau

DNS: zones



Partitionner l'espace de nom de domaines en sections qu'il est possible de gérer.

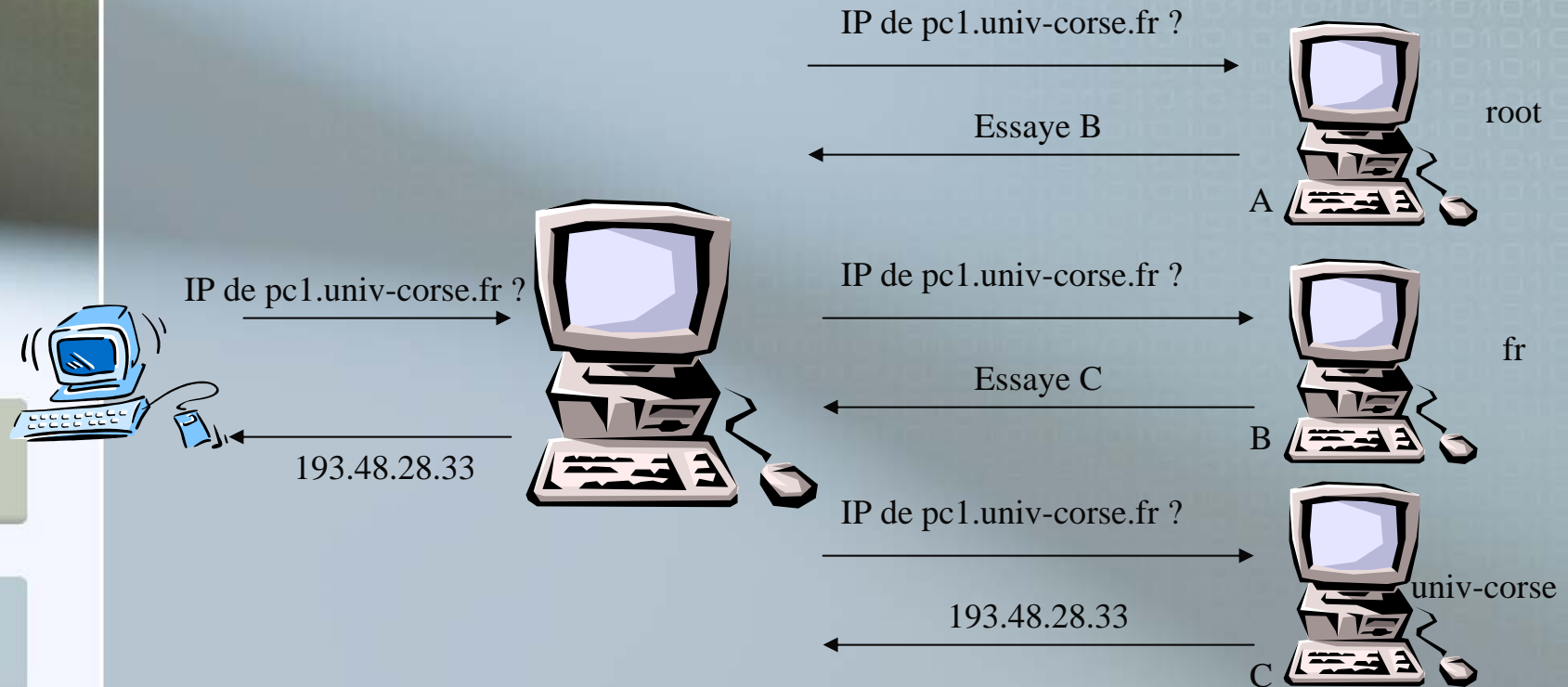
Protocoles et services réseau

DNS: quand est-il disponible?

- DNS peut ne pas être nécessaire dans un environnement Windows
 - WINS résout les noms
- DNS peut être utilisé dans un environnement mixte
 - Windows, UNIX, MacIntosh, etc...
- **DNS est essentiel dans Windows 2000 et 2003**

Protocoles et services réseau

DNS: résolution de nom



Protocoles et services réseau

DNS: structure

- La base de données DNS Microsoft est un ensemble de fichiers contenant le "mappage" nom-N°IP de l'hôte et les données d'informations DNS pour les postes TCP/IP du réseau (enregistrement des ressources)
 - Zone de recherche directe
 - Zone de recherche indirecte
 - Une par sous-réseau

Protocoles et services réseau

DNS: serveur primaire et secondaire

- Serveur primaire
 - Copie maître d'une zone (zone principale standard)

- Serveur secondaire
 - Duplicata d'une zone maîtresse (zone secondaire standard)
 - Tolérance de panne
 - Sous-réseaux
 - Sites distants (liaisons lentes)

- Enregistrement dans l'AD

Protocoles et services réseau

DNS: type d'enregistrement

- Nom d'hôte (A)
 - Mappage du nom d'hôte d'une machine à une adresse IP.
- Source de nom (SOA)
 - Indique quel serveur est serveur principal pour la zone.
- Serveur de nom (NS)
 - Indique quels sont les serveurs de noms qui ont autorité sur la zone.
- Alias (CNAME)
 - Création d'alias
- Serveur de messagerie (MX)
 - Spécifie quels sont les serveurs de messagerie.
- Pointeur (PTR)
 - Équivalent pour les zones de recherche inversée de l'enregistrement A.
 - Mappe une adresse IP à un nom FQDN.

Protocoles et services réseau

DNS: intégration WINS

www.Mcours.com

Site N°1 des Cours et Exercices Email: contact@mcours.com

- Un serveur DNS Windows 2000/2003 peut être configuré pour interroger un serveur WINS (pour la résolution de nom)

