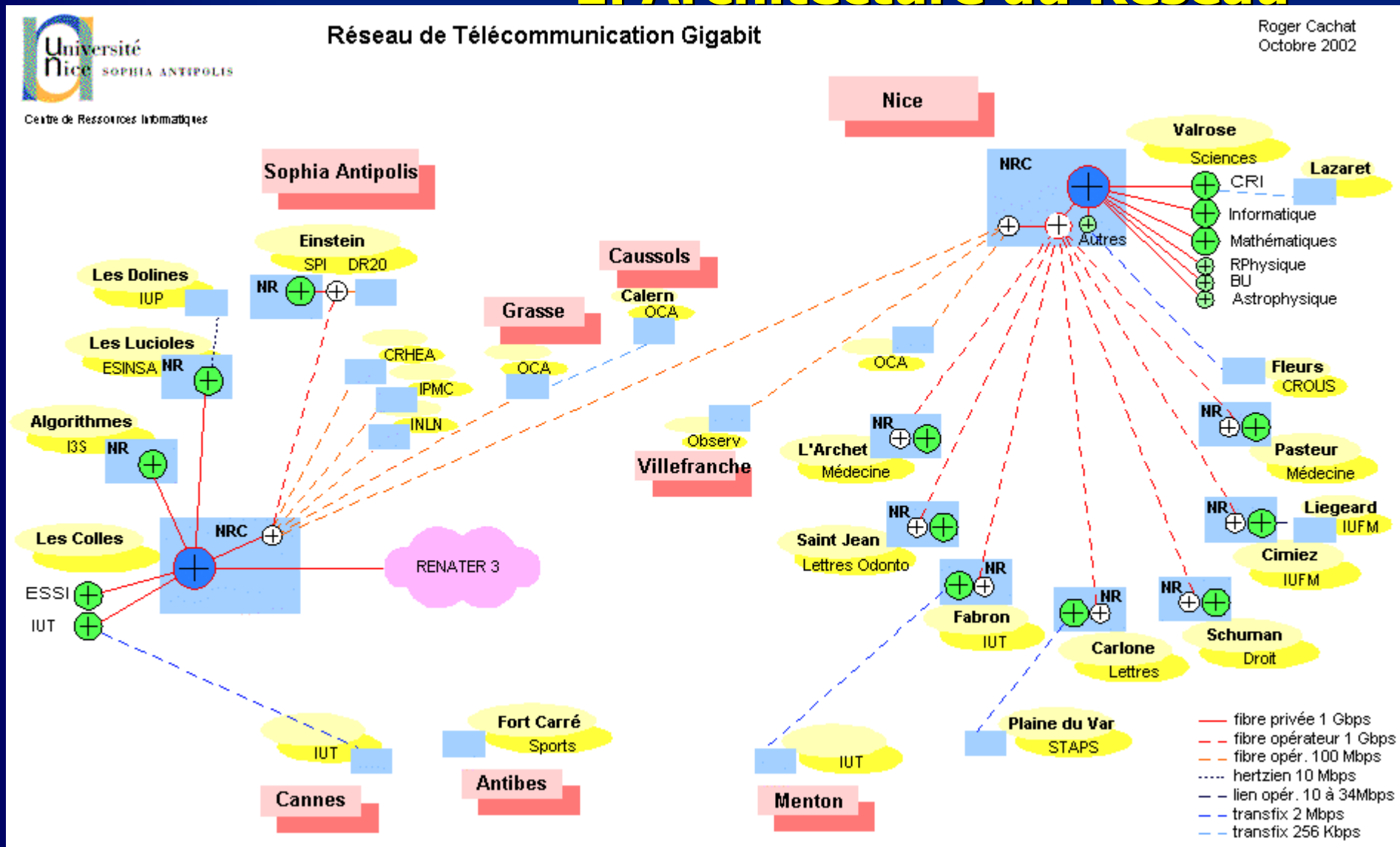
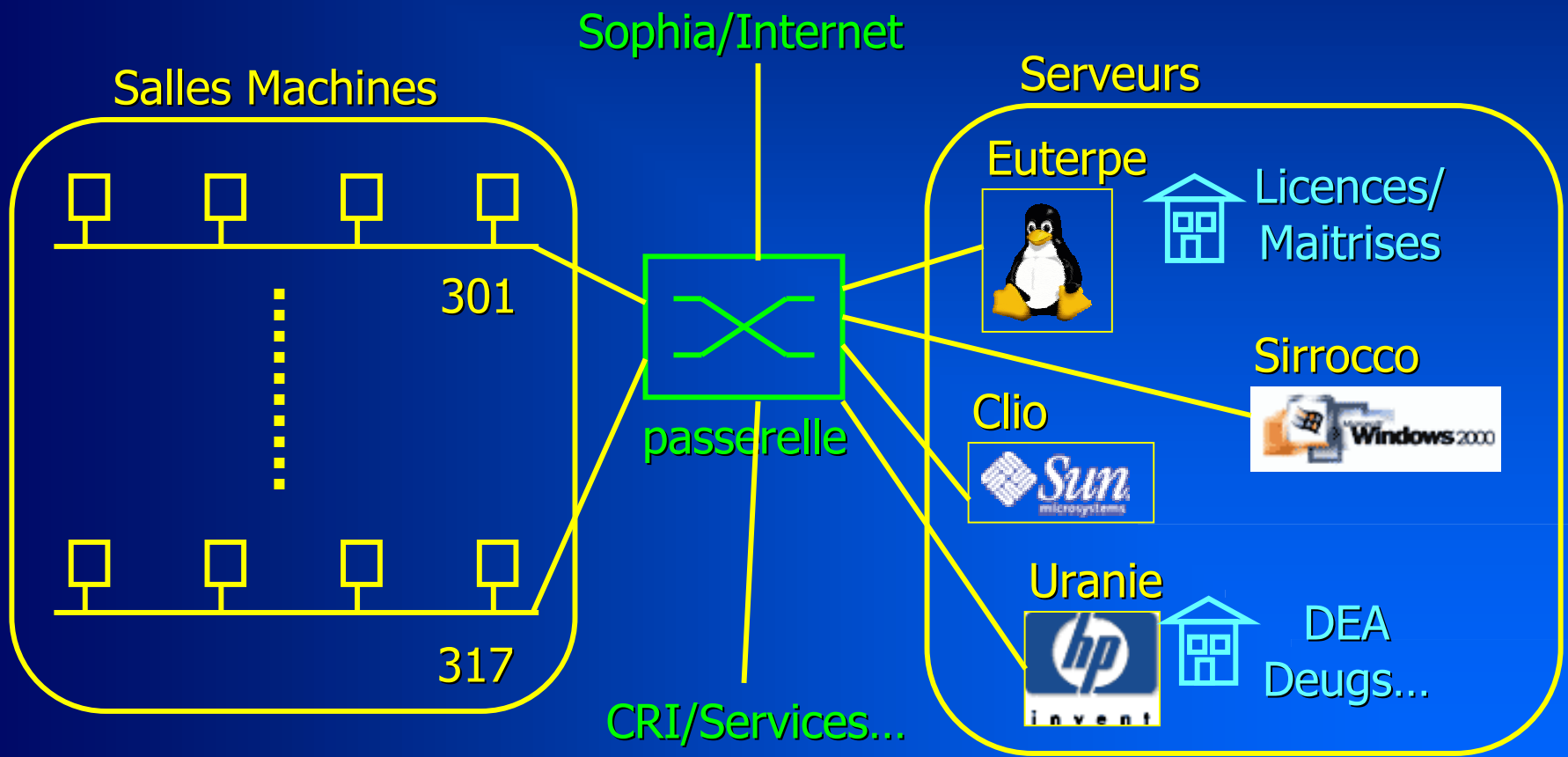
Plan du Cours

III-a. Environnement Réseau

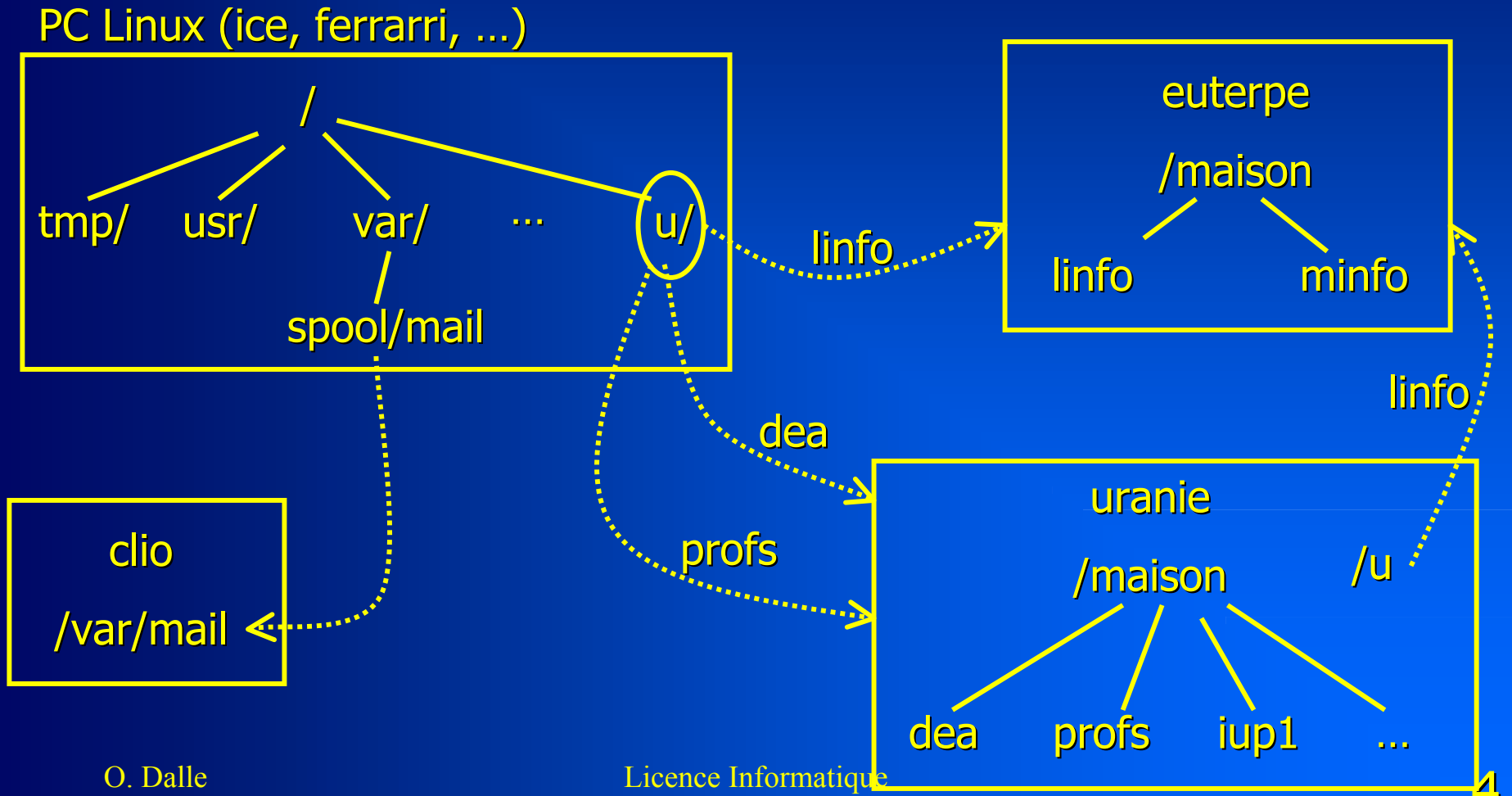
1. Architecture du Réseau



Architecture Locale



2. Partage de Fichiers : NFS



3. Connexion à distance

- Telnet, rlogin, rsh, rcp, ftp
  - Peu sûrs
    - les données circulent en clair (mot de passe, données)
    - authentification faible des machines
  - Assistance limitée pour X windows
    - obligation de "configurer le DISPLAY"
  - Aucune optimisation
    - gênant quand le réseau n'a qu'un faible débit (modem)

SSH

- Connexion sécurisée
  - Les transferts sont cryptés
  - "Empreinte digitale" des machines
    - Une machine ne peut pas se faire passer pour une autre
  - Authentification à l'aide de paires de clefs RSA
    - les clefs sont fabriquées par 2 : publique, privée
    - Principe : ce qui est codé par la clef publique ne peut être décodé que par la clef privée, et vice-versa
    - la clef privée est secrète : en principe elle ne doit jamais circuler sur le réseau
    - La clef publique est (doit être) librement accessible : elle sert soit à coder, soit à décoder les données sensibles

Le principe des clefs privées/publiques

- 1er cas d'utilisation : transmission d'un secret
  - permettre à un autre de m'envoyer un secret que je serai le seul à pouvoir décoder :
    1. (J'envoie ma clef publique)
    2. l'autre code le secret avec ma clef publique et m'envoie le résultat
    3. je décode avec ma clef privée

Principe des clefs privées/publiques (2)

- 2e cas d'utilisation : authentification
  - Je peux prouver que je détient la clef secrète :
    - Preuve de mon identité, car je suis (en principe) le seul à connaître la clef secrète
  - Principe d'utilisation :
    1. J'envoie un message codé avec ma clef secrète
    2. L'autre vérifie que le message est bien lisible lorsqu'il est décodé avec ma clef publique

Principe des clefs privées/publiques (3)

- L'authentification par clefs privée/publique
  - Le schéma précédent est trop simple !
    - Si quelqu'un intercepte un des messages codés avec ma clef privée, il peut le rejouer plus tard …
    - Le message doit donc changer à chaque fois
  - En pratique : l'autre lance un défi (challenge) :
    1. il m'envoie un message à usage unique qu'il a choisi (par exemple un nombre aléatoire), en clair.
    2. je code ce message avec ma clef privée et le retourne
    3. l'autre vérifie en décodant le message avec ma clef publique : si le message résultant est le même que l'original, alors l'authentification a réussi
    - Remarque : plusieurs protocoles similaires sont possibles (ex: l'envoi initial peut être codé avec ma clef publique)

Utilisation de SSH

- Les commandes ssh
  - ssh host [–l login]
    - Configure automatiquement le display !
  - scp host:fichier host:fichier
    - scp ice:tmp/mon_fichier ./toto/titi
    - scp mon_fichier ice:toto/titi
  - ssh-agent : mémorise les clefs privées
    - pas obligatoire, mais évite de ressaisir tout le temps la *passphrase*
  - ssh-add : enregistre une nouvelle clef privée auprès de l'agent
  - sftp : équivalent ftp
    - hélas pas toujours installé (SSH V2) …
  - ssh-keygen : fabrique des paires de clefs

Création des clefs SSH

- ssh-keygen –t type
  - type = 'rsa1' (SSH V1), 'rsa' (SSH v2) ou 'dsa' (SSH v2)
  - Chaque type produit 2 fichiers, en ~/.ssh/
    - rsa1 : identity (privée) + identity.pub (publique)
    - rsa2 : id_rsa + id_rsa.pub
    - dsa : id_dsa + id_dsa.pub
  - demande une "passphrase"
    - Les clefs privées sont stockées sous forme codée
    - il est conseillé de choisir quelque chose de long (> 10 caractère) et compliqué …

Installation des clefs SSH

- Sur les machines où l'on souhaite se connecter :
  - La (les) clefs publiques doivent être stockées dans le fichier ~/.ssh/authorized_keys
  - Exemple : pour autoriser l'accès à machineA depuis machineB (type rsa2)
    - Sur machineB : ssh_keygen –t rsa (si besoin)
    - copier le contenu du fichier
      machineB:~/.ssh/id_rsa.pub
      à la fin du fichier
      machineA:~/.ssh/authorized_keys
    - Attention : à ne pas écraser
      machineA:~/.ssh/id_rsa.pub !

Utilisation de l'agent SSH

- Lors du login (ex : .zlogin)
  - Lancer ssh-agent
  - SSH-AGENT affiche un script :
    - Ce script définit des variables d'environnement

```
~> ssh_agent
SSH_AUTH_SOCK=… ; export SSH_AUTH_SOCK
SSH_AGENT_PID=xxxx ; export SSH_AGENT_PID
```

    - Les shells qui exécutent ce script (.zshrc) savent ensuite comment contacter l'agent pour utiliser ses services
  - Lancer ssh-add pour enregistrer les clefs secrètes
- Dans chaque nouveau shell (.zshrc)
  - Exécuter le script (il faut l'avoir sauvé qq-part !)

Plan du Cours

I. Interface Graphique (Xwindows)
II. Interface Textuelle (zsh)
III. a - Environnement Réseau
III. b - Windows NT
1. Introduction
2. Caractéristiques
3. Architecture générale
4. Configuration d 'une machine NT
5. Fonctionnement en réseau
6. Protection des fichiers avec NTFS

IV. Outils de traitement de données
V. Installation de Linux

1. Introduction

- Unix ou NT ?
  - Les deux sont devenus incontournables !
    - Dans le monde professionnel
    - Chez les particuliers
- Il existe de plus en plus de passerelles
  - Pour utiliser les deux environnements en même temps sur un même poste de travail
  - Pas toujours très efficace…

2. Caractéristiques Générales

- NT = New Technology !

  The « high-end » Windows operating system in a family of Windows systems …

  - **Multi**-processus et multi-thread, péemptif à temps partagé
  - **Mono**-utilisateur
    - Mais serveur de ressources autres que calcul (fonctions réseau)
  - **Multi**-plate-forme
    - Capable de profiter d'architectures multi-processeurs

Caractéristiques Générales (suite)

- Sécurisé, niveau C2 de la *US DoD*
  - Identification (login)
  - Quota et contrôle sur l'usage des ressources
  - Traces des évènements
  - Mémoire virtuelle non partageable entre processus
- Système de fichiers robuste : NT File System (NTFS)
  - Protections
- Interface Windows bien connue …

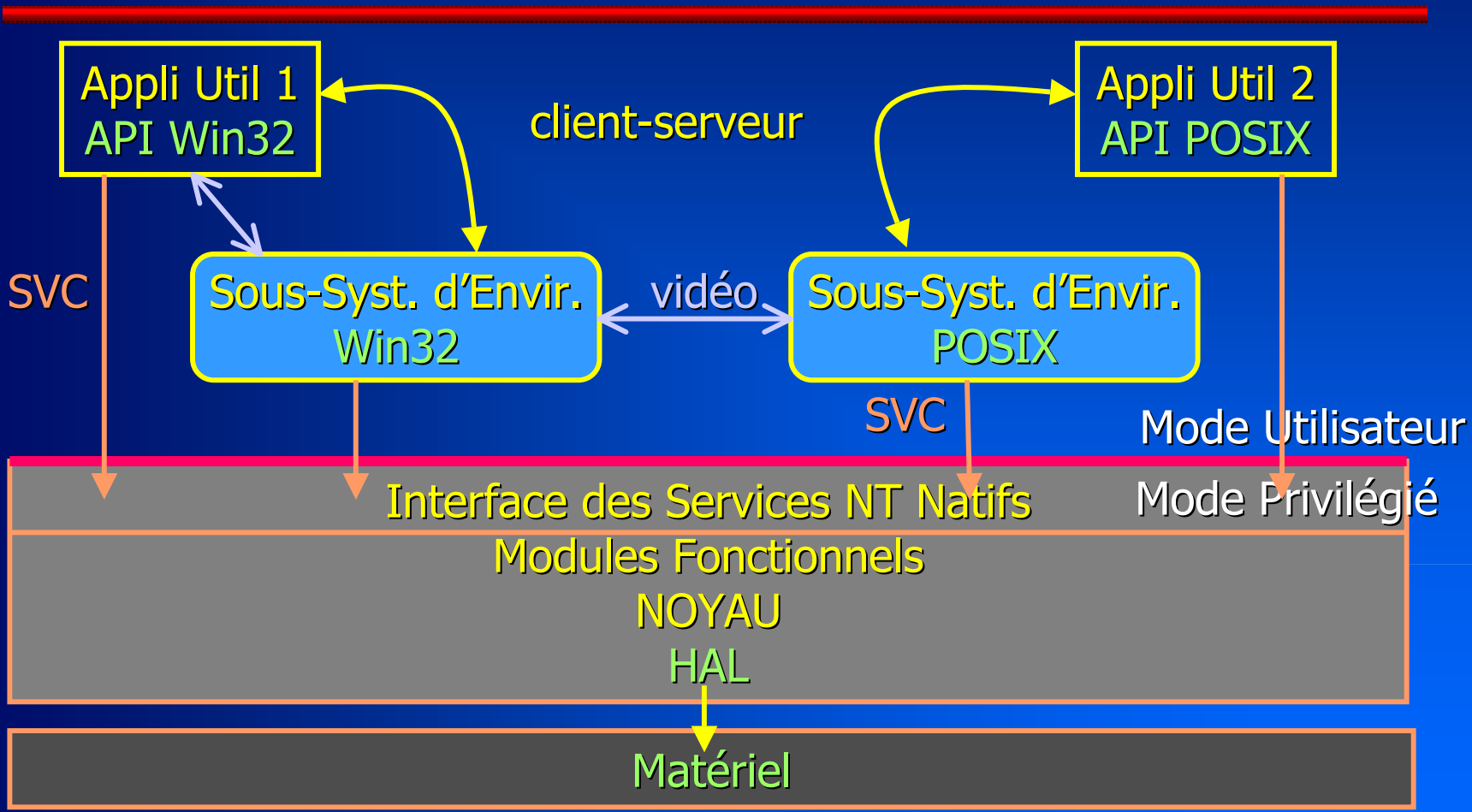
Différentes versions de NT

- NT 4.0
  - Workstation : Poste de travail
  - Server: + d'outils, Gestion hiérarchique de domaines de réseau
- NT 2000
  - Professional (version NT de Millenium)
  - Server : 1 à 4 CPU, 4Go RAM
  - Advanced Server : 1 à 8 CPU, 8 Go RAM, cluster (2 failover, 32 NLB)
  - Datacenter Server : 1 à 32 CPU, 64 Go RAM, cluster (4 failover, 32 NLB)
- XP : Fusion des branches 9x/Me et NT/2000

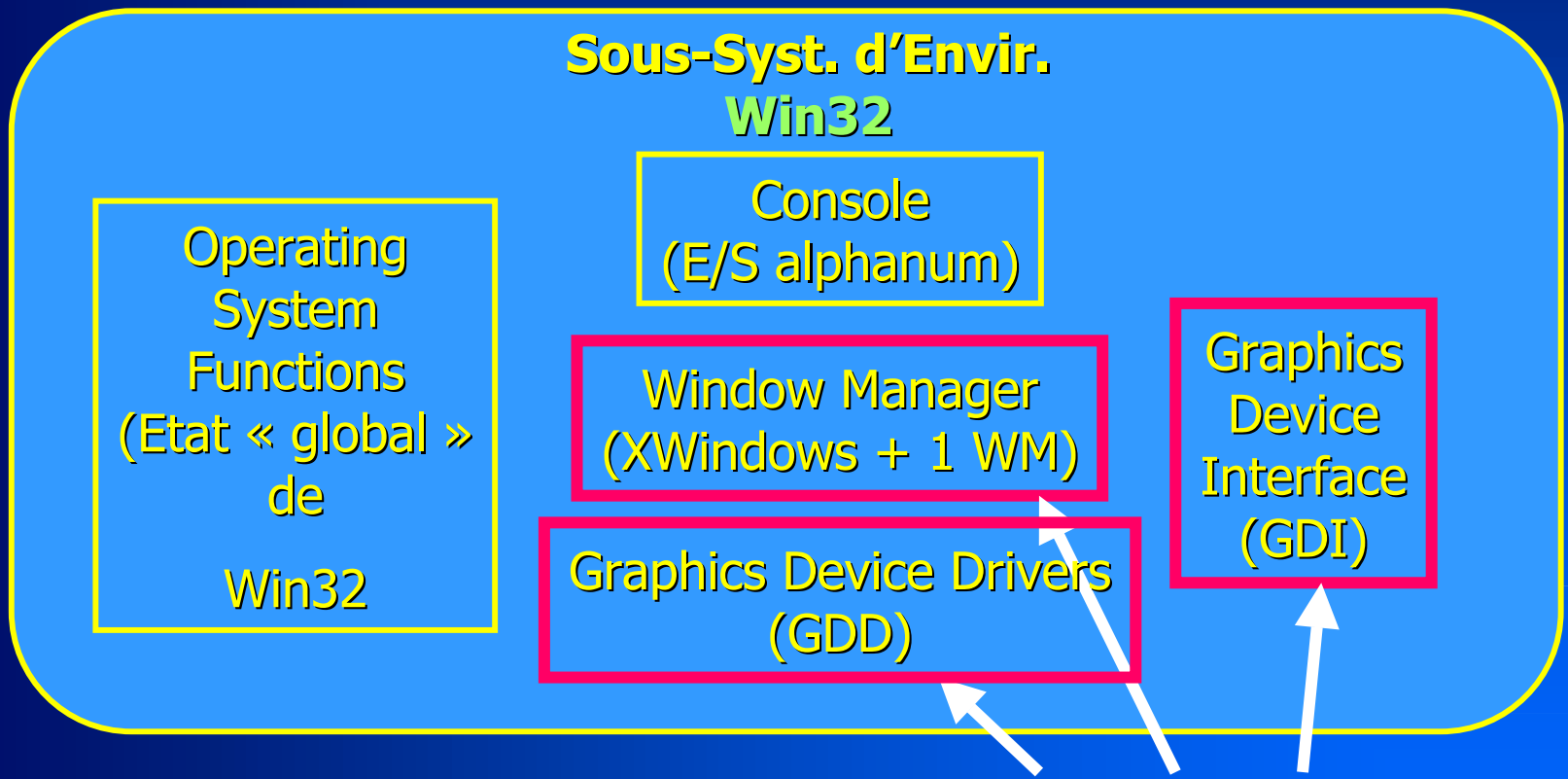
Les Améliorations de NT/2000

- Matériels supportés
  - Disques ATA, USB, IEEE 1394 (« Firewire »)
- Nouveaux services
  - Active Directory (« X500-like »)
  - Distributed File System
  - Kerberos
  - Quotas
  - Encrypted File System
- Clustering (Advanced et Data Server)
  - Mécanisme de « Failover » : tolérance aux pannes
  - NLB (Network Load Balancing) : répartition dynamique de charge

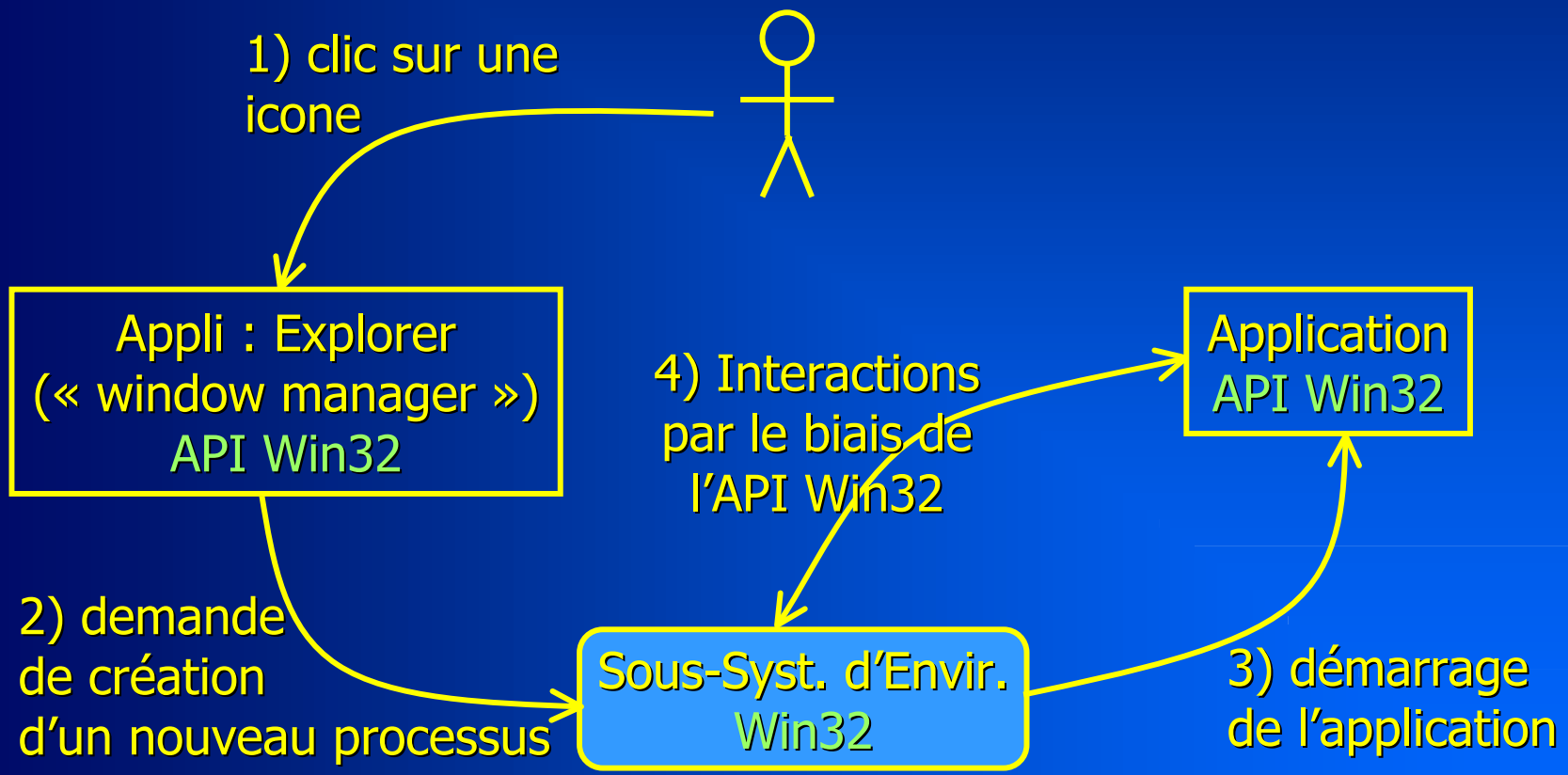
3. Architecture Générale



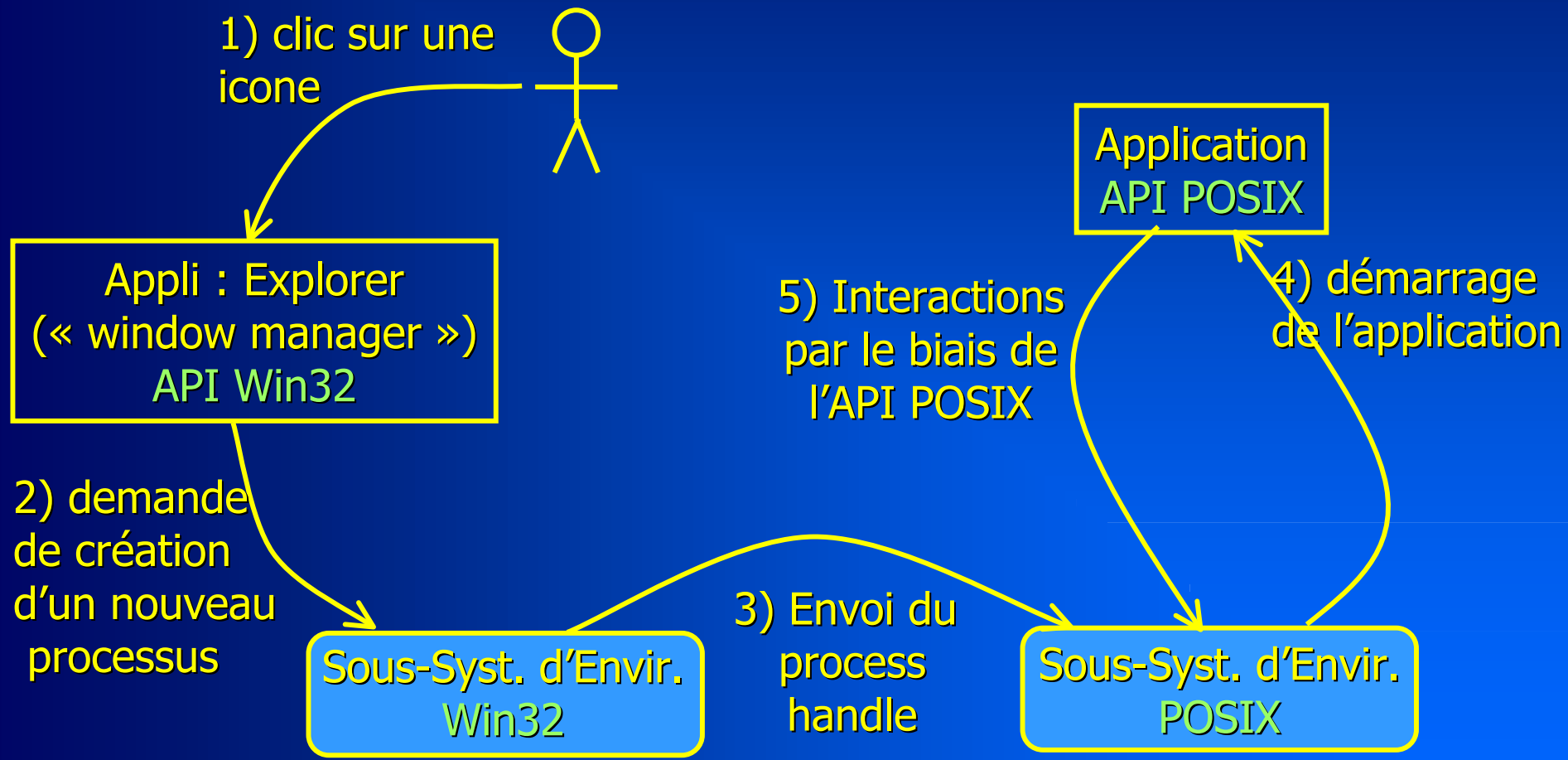
Le Sous-système d'environnement Win32



Démarrage d'une Application Interactive Win32



Démarrage d'une Application Interactive non Win32



Passerelles UNIX ↔ NT

- Serveur graphique :
  - client X11 sur NT : X-Win32, Exceed, WISE, …
  - « client » NT sur X11 : wincenter (Citrix)
- Système de fichiers : samba
- Executif UNIX sur NT :
  - sous-système d'environnement POSIX (propre à NT)
  - Cygwin32 : bibliothèque d'émulation POSIX pour les outils GNU
    - La dernière version est une vraie "distribution", avec notamment un serveur X11 XFree86
    - Emule une hiérarchie de fichier à la Unix

4. Configuration d'une Machine NT

a. La Base de Registre
b. Constitution d'un profile utilisateur

4a. La base de Registres

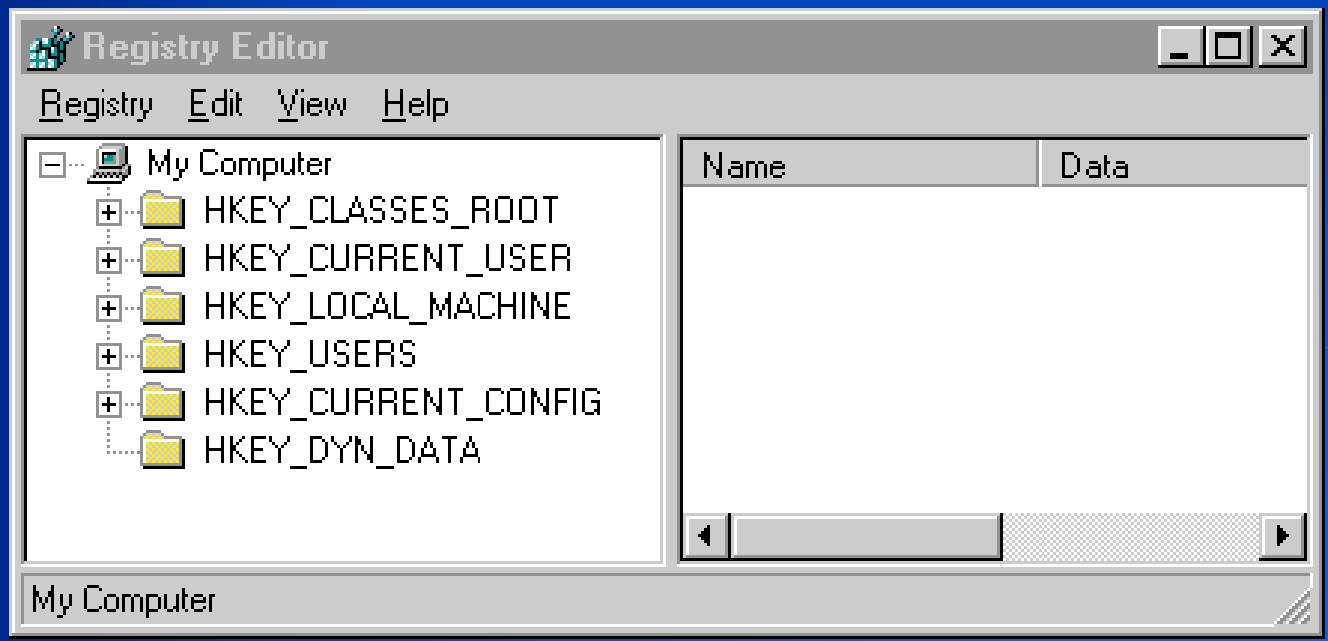
- Disparition des fichiers .INI
- Apparition d'une base d'informations : « the registry »
  - Système
  - Applications
  - Utilisateur
- Configurer le système, ses applications et utilisateurs :
  - Modifier des informations dans la base de registres
  - Plus de fichiers à modifier
  - ATTENTION : éviter de modifier la base manuellement !

La base de Registres (2)

- Contenu de la base de registres :
  - Une partie sauvegardée lorsque la machine est arrêtée
  - Le reste est reconstruit dynamiquement
- Editeurs pour le registry
  - regedit.exe (parfait pour recherche sur des valeurs)
  - regedt32.exe (parfait pour éditer des valeurs)

Organisation de la Base de Registres

- Organisation en sous-arbres (root-key)
- Chaque sous-arbre contient des clés, des sous-clés, des entrées

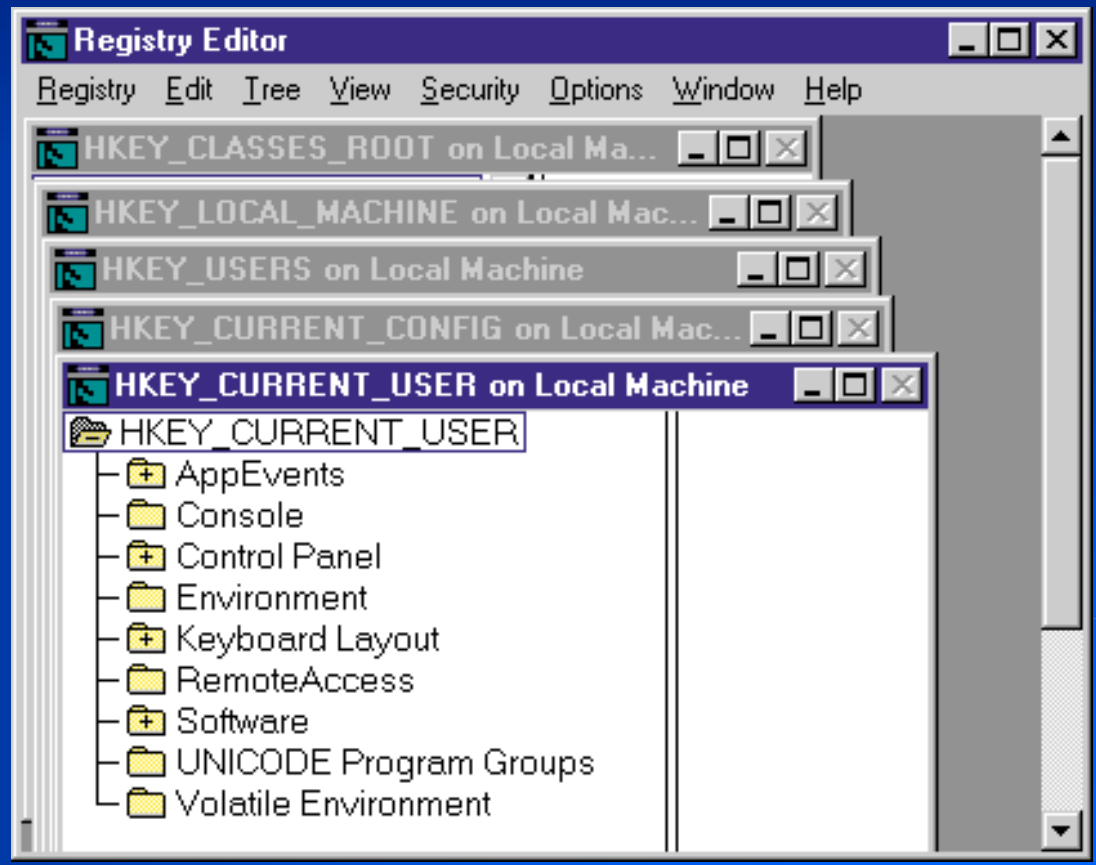


Organisation de la Base de Registres (2)

- Une entrée contient 3 champs :
  - Nom
  - Type
    - REG_SZ : simple chaîne de caractères
    - REG_DWORD : entier binaire sur 4 octets
  - Valeur

Edition de la Base de Registres

- Exemple avec regedt32



Ruches

- Certaines *root-key* ou *key* du registry sont sauvegardées dans des fichiers
  - En général, seul l'administrateur y a accès
- Ces parties de la base de registre sont appelées « ruches » (*hives*)
- Certaines root-key ne sont que des répliques d'autres
  - 2 root-key importantes :
    - HKEY_LOCAL_MACHINE
    - HKEY_CURRENT_USER

Type d'informations contenues dans les ROOT-KEY

- HKEY_LOCAL_MACHINE
  - Infos sur le matériel et les logiciels installés sur la machine
- HKEY_CLASSES_ROOT
  - Associations applications/fichiers et OLE (alias de HKEY_LOCAL_MACHINE\SOFTWARE\Classes)
- HKEY_USERS
  - Profiles d'utilisateurs
    - DEFAULT : le profile standard pour tout nouvel utilisateur
    - Profile pour l'utilisateur courant

Type d'informations contenues dans les ROOT-KEY

- HKEY_CURRENT_USER
  - Certaines des informations du profile de l'utilisateur courant
    - Configuration et apparence du poste de travail
    - Connexions réseau
    - Paramètres d'applications, …
  - Généralement un alias de HKEY_USERS**Sid_utilisateur**
- HKEY_CURRENT_CONFIG
  - Détails de la configuration courante pour les composants matériels
  - Alias de HKEY_LOCAL_MACHINE\System\CurrentControl\Set\HardwareProfiles\Current

Exemples

- Changement du fond d'écran par défaut
  - HKEY_CURRENT_USER\.DEFAULTS\ControlPanel\Desktop
    - Wallpaper:REG_SZ:xxx
- Message de Login personnalisé
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
    - LegalNoticeText:REG_SZ:xxx
- Valeur de la variable %systemroot%
  - Dans HKEY_LOCAL_MACHINE (rechercher la clef avec regedit)

4.b. Constitution d'un Profile Utilisateur

- Paramètre utilisateur
  - Nom, descriptif, mot de passe, groupes d'appartenance, restriction d'accès, etc
  - Localisation des éléments pour constituer le Profile
    - Chemin du profile personnel : par défaut %systemroot%\profiles\%username%
    - Mis en union avec %systemroot%\profile\AllUsers
    - Peut aussi dépendre d'une politique s'appliquant à la machine ou aux utilisateurs

Eléments du profile personnel

- Détails de la base de registre
  - ruche ntuser.dat (ou .man si « mandatory »)
    - AppEvents (actions associées aux évènements engendrés par des applictions)
    - ControlPAnel/Desktop (taille, fond, …)
    - Variables d'envionnement
    - Config clavier, imprimante(s), …

Eléments du profile personnel (2)

- Répertoires constituant l'environnement de travail
  - profiles\Application Data
  - profiles\Desktop : ce qui se trouve sur le bureau
  - profiles\Favorites : bookmarks
  - profiles\NetHood : voisinage réseau
  - profiles\Recents : documents récemment ouverts
  - profiles\StartMenu : contenu du menu démarrer
- Répertoire personnel
  - …\users\%username%

Eléments du profile personnel (3)

- Script de login
  - Récupère les variables d'environnement
    - %homedrive% : lecteur pointant sur le homedir
    - %homepath% : chemin vers homdir, sans référence au lecteur
    - %username% : login de l'utilisateur
  - Utile pour définir de nouvelles variables d'environnement, automatiser des initialisations,etc
  - Localisation par défaut :
    - %systemroot%\system32\repl\imports\scripts
    - login script a priori non modifiable

5. Machine NT sur un réseau

- Partage de ressources
- Organisation de type workgroup
- Organisation de type domaine
- Login (domaine)

Partage de Ressources

- Une machine NT peut rendre certaines de ses ressources accessibles par le réseau
  - Ce seront les seules ressources visibles des autres machines
  - Seul un utilisateur faisant partie des administrateurs peut rendre une ressource partageable
- Imprimante partagée
  - permissions de partage :
    - contrôle total
    - gestion de documents
    - imprimer
    - aucun accès

Partage de Ressources

- Partage de partition
  - Association
    - d'un « nom de partage »
    - de permissions de « partage » (contrôle total, modifier, lire, aucun accès)
    - Notation UNC (Universal Naming Convention) pour désigner la ressource :

\\nom_machine\nom_partage

Organisation de type WORKGROUP

- Compte en local
  - un utilisateur n'a qu'un seul endroit ou se connecter : en local sur une workstation NT
- Les utilisateurs de cette WS peuvent faire partie de groupes locaux

Organisation de type DOMAINE

- Un « Domaine » regroupe plusieurs machines en un ensemble « unificateur »
- Une machine **NT Server** joue le rôle de **Contôleur Principal du Domaine** (CPD)
  - Stockage
    - des informations d'identification
    - des profils
    - des homedirs
  - Application d'une politique aux utilisateurs
  - Un CPD peut être secondé par des CSD (contrôleurs secondaires)
  - Samba permet de faire tourner sur une machine Unix un émulateur de serveur NT

Fonctionnement en mode DOMAINE

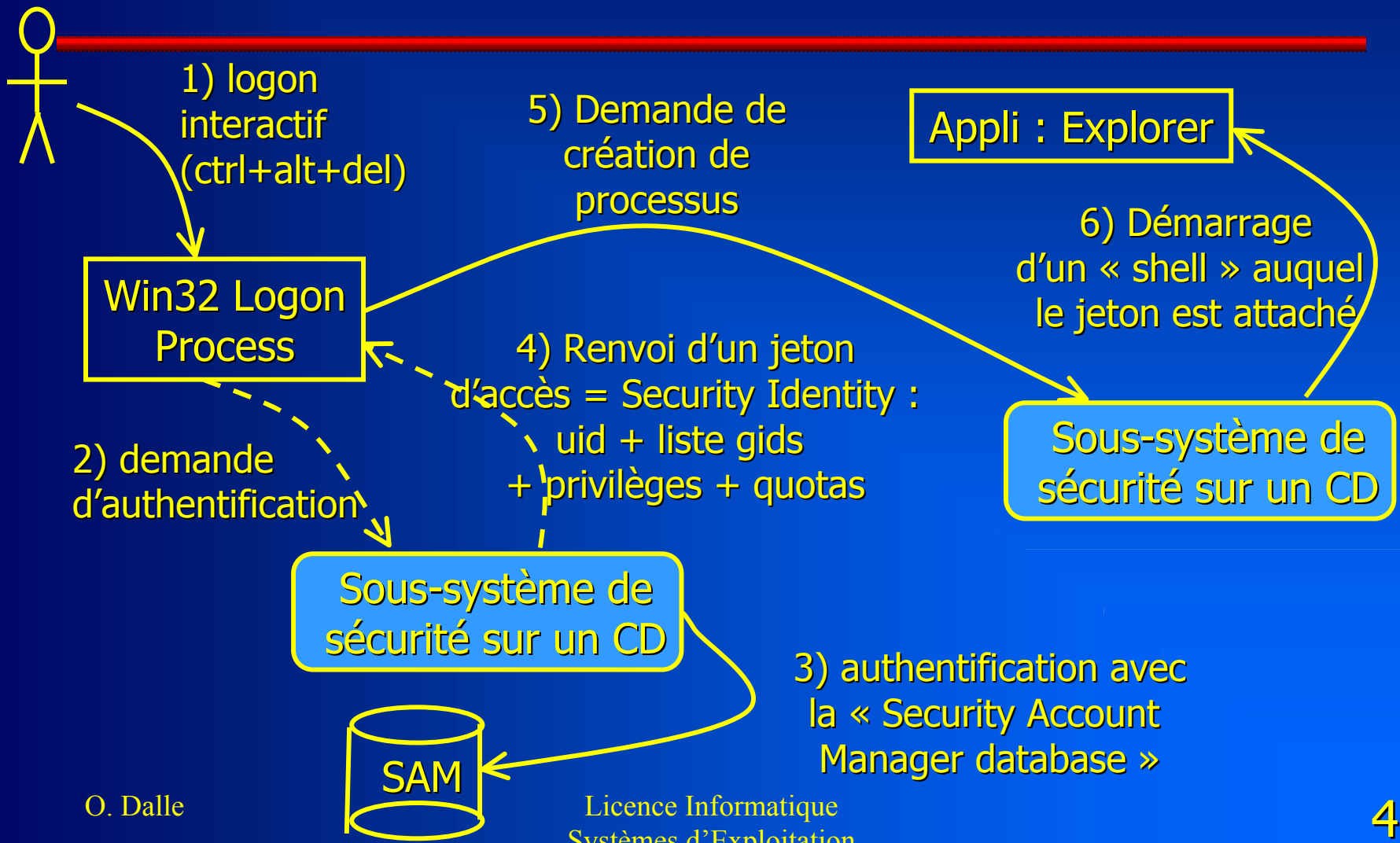
- Un utilisateur peut récupérer un profile unique
  - appelé **profile errant** ou **itinérant** (roaming profile)
  - accessible quelle que soit la machine (du domaine) où il se connecte

  ⇒connexion sur un domaine et non sur une machine
    - par défaut : \\svrCPD\Profiles\%username% \\svrCPD\Profiles\AllUsers
    - éventuellement : \\svrCPD\NETLOGON\{login script,NTCONFIG.POL}
  - profile obtenu par le réseau : connexion lente …

Fonctionnement en mode DOMAINE (2)

- Le profile est ensuite maintenu en local
  - A la déconnexion : mise à jour du profile sur le serveur
  - En cas d'inaccessibilité du serveur
    - Soit un profile local existe
    - Soit le profile part défaut est utilisé
    - Synchronisation éventuelle plus tard
- Possibilité de placer les utilisateurs dans des groupes d'utilisateurs globaux
  - Les groupes globaux peuvent être ajoutés aux groupes locaux des machines
- Possibilité d'établir des hiérarchies de domaines, basées sur des relations d'approbation (confiance)

Login dans un DOMAINE



6. Protection des fichiers avec NTFS

- NTFS ajoute des droits d'accès aux fichiers et répertoires
  - Système de fichiers FAT : pas de droits, tout est accessible à tout le monde

Types de Permissions

Permission	sur un fichier	sur un rép.
Lire (R)	ouvrir en lecture	lister
Ecrire (W)	modifier	ajouter
Exécuter (X)	exécuter prog	parcourir
Supprimer (D)	effacer	effacer
Changer les permissions (P)	modifier	modifier
Prendre possession (O)	nouveau prop.	nouveau prop.

Permissions d'accès « Standard » (prédéfinies)

Permission Standard	sur un fichier	sur un rép.
Aucun accès	-	-
Lister	RX	RX
Ajouter	-	WX
Ajouter et Lire	RX	RWX
Modifier	RWXD	RWXD
Contôle total	RWXDPO	RWXDPO

Mécanisme d'héritage

- Un objet créé dans un répertoire hérite des permissions
  - associées à ce répertoire
  - pour ce type d'objet (fic. ou rép.)
    - Les permissions d'un répertoire contiennent aussi des permissions « fichiers »

Différences par rapport à UNIX

- Un objet a un propriétaire, mais pas de groupe propriétaire
  - Mais un mécanisme d'ACL (cf. plus loin)
- Dans Unix les permissions des fichiers créés s'obtiennent généralement à partir du « umask »
  - Une notion d'héritage un peu similaire existe toutefois dans UNIX, grâce au bit « s » positionné sur les répertoires

Utilisateurs et Groupes

- Utilisateurs
  - Standard
  - Administrateur
- Groupes d'utilisateurs
  - Prédéfinis : Administrateurs, Opérateurs de compte, Invités, Admin. domaine, …
  - Définis par l'admin. : linfo, profs, …
  - Spéciaux :
    - Interactif : l'utilisateur de l'ordinateur
    - Réseau : utilisateurs en accès réseau
    - Créateur propriétaire : le créateur ou le propriétaire

Mécanisme des ACL

- A chaque objet est associé une ACL
  - Access Control List
  - Chaque élément de la liste = ACE
    - Access Control Element
  - Une ACE = { Groupe/utilisateur ; permissions }
  - Les ACEs et l'ACL se modifient
    - via l'**onglet sécurité** associé à l'objet
    - par la commande shell **cacl**
    - Remarque : permission P requise

Règles d'accès aux Objets du File System

- Les permissions **accordées**, sauf exception, sont **cumulatives**
- Au moment de l'accès :
  - Utilisateur identifié par son SID
    - UID + liste des gids auxquels il appartient
  1. Recherche dans ACL d'une ACE concernant son SID : « aucun accès » => accès (définitivement) refusé
  2. Sinon, recherche de permissions pour autoriser l'accès
     1. A l'aide d'autres ACE que celle concernant son SID