



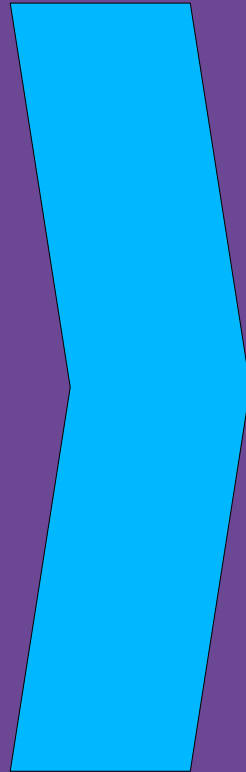
Cours d'administration Système

C. Gouinaud
Isima FX

But et contenu de ce cours :

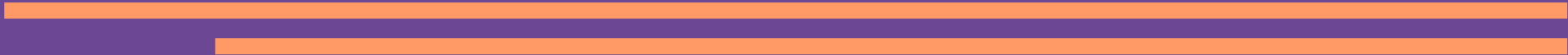
BUTS :

- Culture
- Autonomie
- Avenir



Contenus :

- Gestion des gens et annuaire
- Gestion des espaces disque et sauvegarde
- Gestion et maintenance des applications
- Réseaux et organisation des communications
- Modèle Ntiers et serveur
- Métier et sécurité



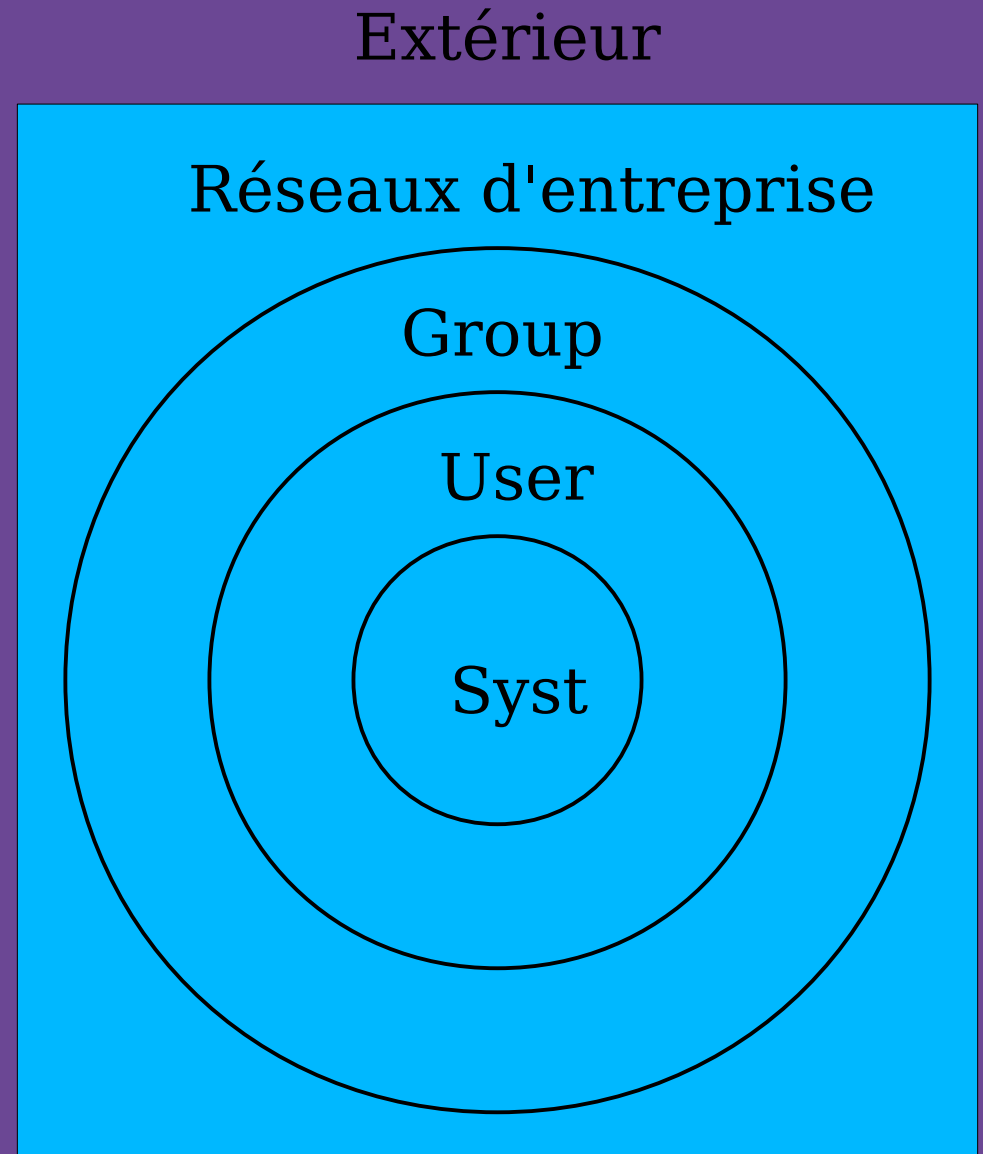
Introduction

- Ressources
 - Email, web
 - Application comptable ou courrier
 - Pupitre de commande
- Mettre à disposition en respectant
 - Sûreté
 - Confidentialité
 - Géographie – ubiquité

Amener les bons fichiers au bon endroit

Identification des personnes

- Accès interactif
- Accès au système de fichier
- Accès au applications fédérative
- Messagerie, workflow et intranet
- Accès externe et nomade

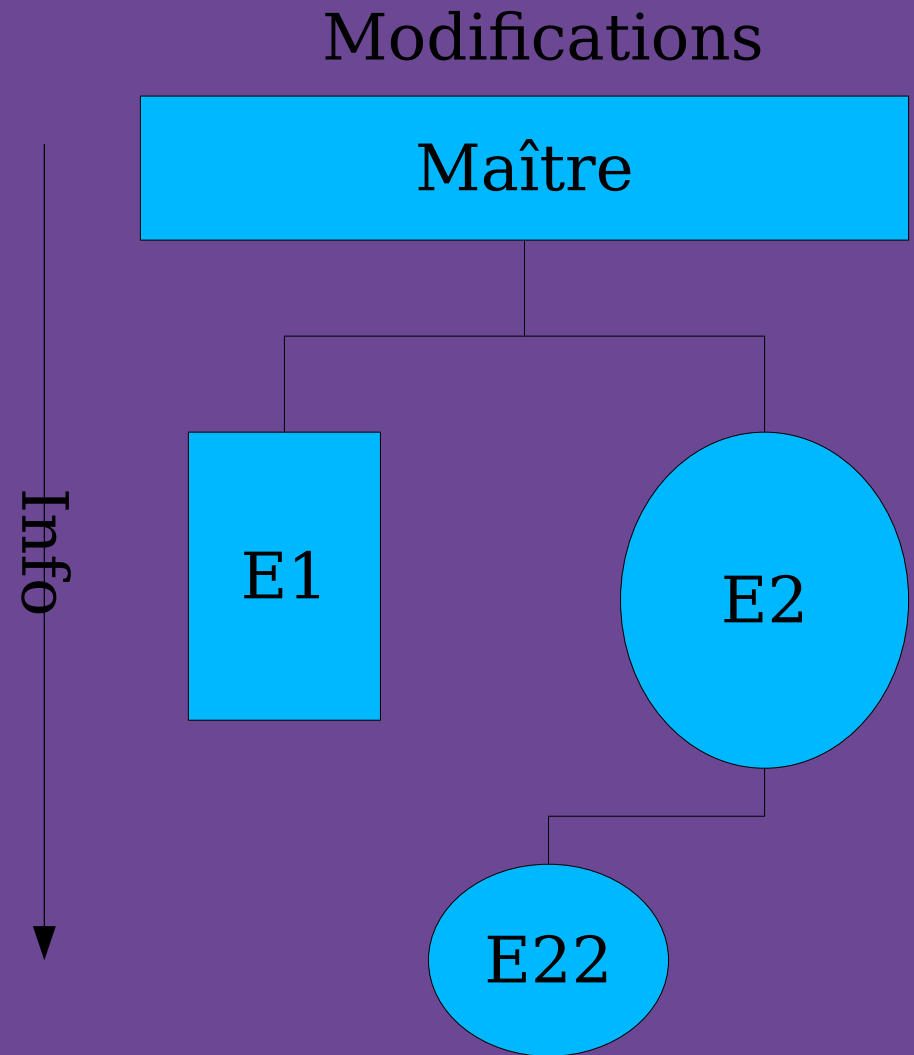


Identification - annuaire

- Un seul login
application, messagerie,
- Un seul mots de passe
Créer un sentiment de propriété (mail,
gestion de carrière, ...)
- Un seul annuaire d'entreprise
 - Identification – ldap, nis, edirectory, x500
 - Authentification – Radius, Tacas, kerberos

Stratégie d'annuaire

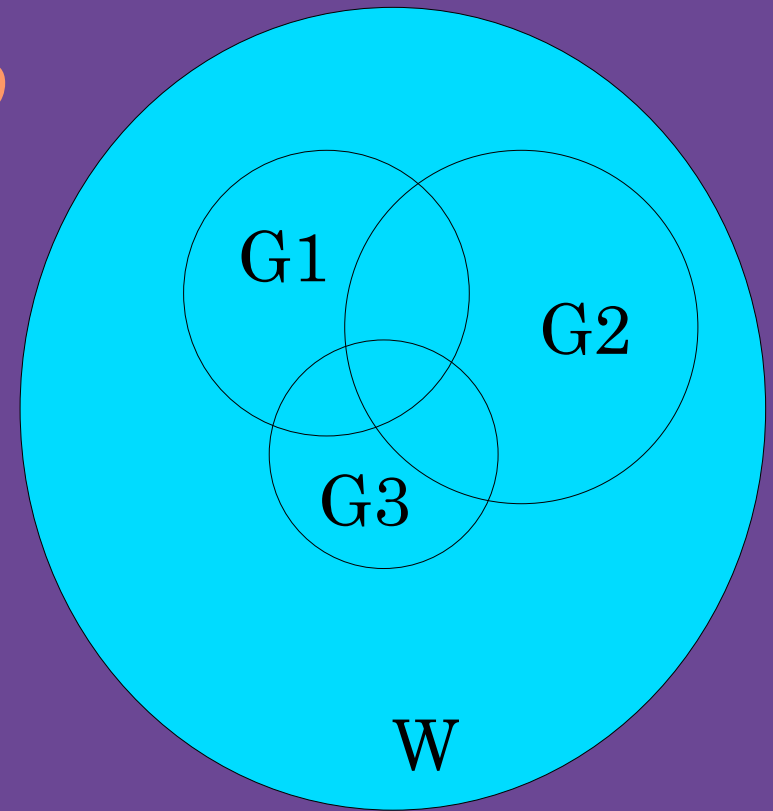
- X500
- LDAP
(X500 light)
- NIS
(transport de clef)
- Active directory
(ldap + kerberos)
- Autre



Regroupement - group

Contrôler les accès :

- Fichiers partagés
- Applications partagé (oracle, sap, ...)
- Rôle dans les Worflow (validation, ...)
- Moyen d'accès au réseau (Wifi, VPN)
- Accès au logiciel sous licence
-



Pour des regroupements de personnes !

Structure des groupes

- Un pour tous les utilisateurs
 - Un par rôle dans le système
 - Un par service
 - Un par niveau hiérarchique
 - Un par métier transversal (secrétariat, comptable, ...)
 - Un par communauté de travail (vente, ...) ou BU (projets)
 - Un par type de contrôle d'accès au moyen (VPN, intranet, serveur, ...)
-
-

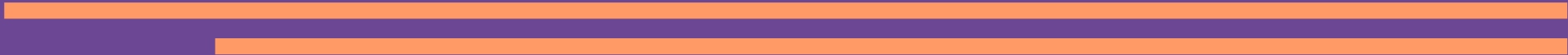
Régle de création :

- Nommage simple et significatif : scompta, svente, msecret, ...
 - Un groupe : un mail !
 - Données privés séparés (fichiers)
 - Liste et appartenance connus
 - Pas de login de groupe
 - Délégation de gestion (interface)
 - Utilisation transparente (fichiers)
-
-

Maintenance des groupes :

- Partagés sur tout les OS
 - Distribution centralisé
 - Mise en cohérence automatique
 - Gestion simple et automatisé
 - Création rapide et destruction à terme
 - Vérification automatique
 - Procédure d'attribution/révocation claire !
 - Pas de groupe admin à droit spéciaux !
-
-

Partie 2 – Gestion des espaces !



Matériel et force en présence

- Poste perso avec disque
- Serveur de fichier (NFS,CIFS,RFS,...)
 - PC et autres (360 Mo/s)
- NAS – network area storage
 - Serveur de fichier dédié (raid, scsci, sata)
- SAN – storage area network
 - réseau de stockage – disque en réseaux
 - Espace partagé entre plusieurs serveurs
 - Fiber channel, ISCSI, (10 gb/s)

AVOIR : www.emc.com

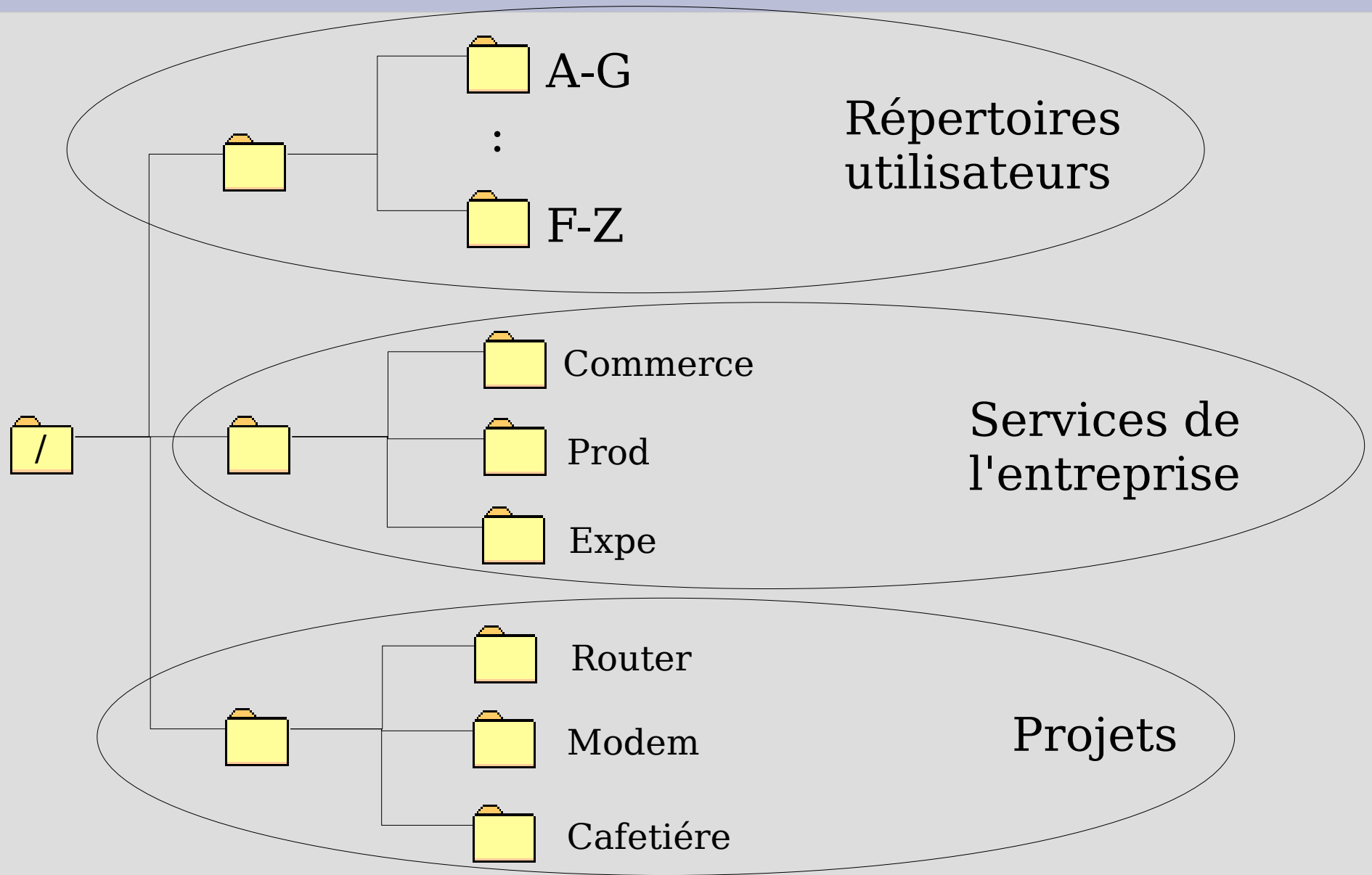
Espace disque

- On crée une arboréscence a 2 niveau
 - Niveau hierarchique => contenant les homes)
 - Niveau fonctionnel => contenant les groupes de travail effectif (BU)
- On rend cela transparent à l'utilisateur
 - Droits correctement fixés (groupe !)
 - Bureau explicite ... et non variable

Surêté des espaces (RAID)

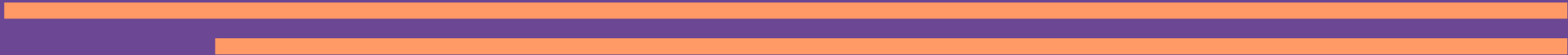
- Raid 0 (striping) $\text{espace} = \text{espace}$
- Raid 1 (mirroring) $\text{espace} / = 2$
- Raid 3 (checksum) 3 disque $\text{espace} * = 2/3$
- Raid 5 (checksum) $N+1$ disque $e^* = n / (n+1)$
- Raid matériel ou logiciel

Arborescence

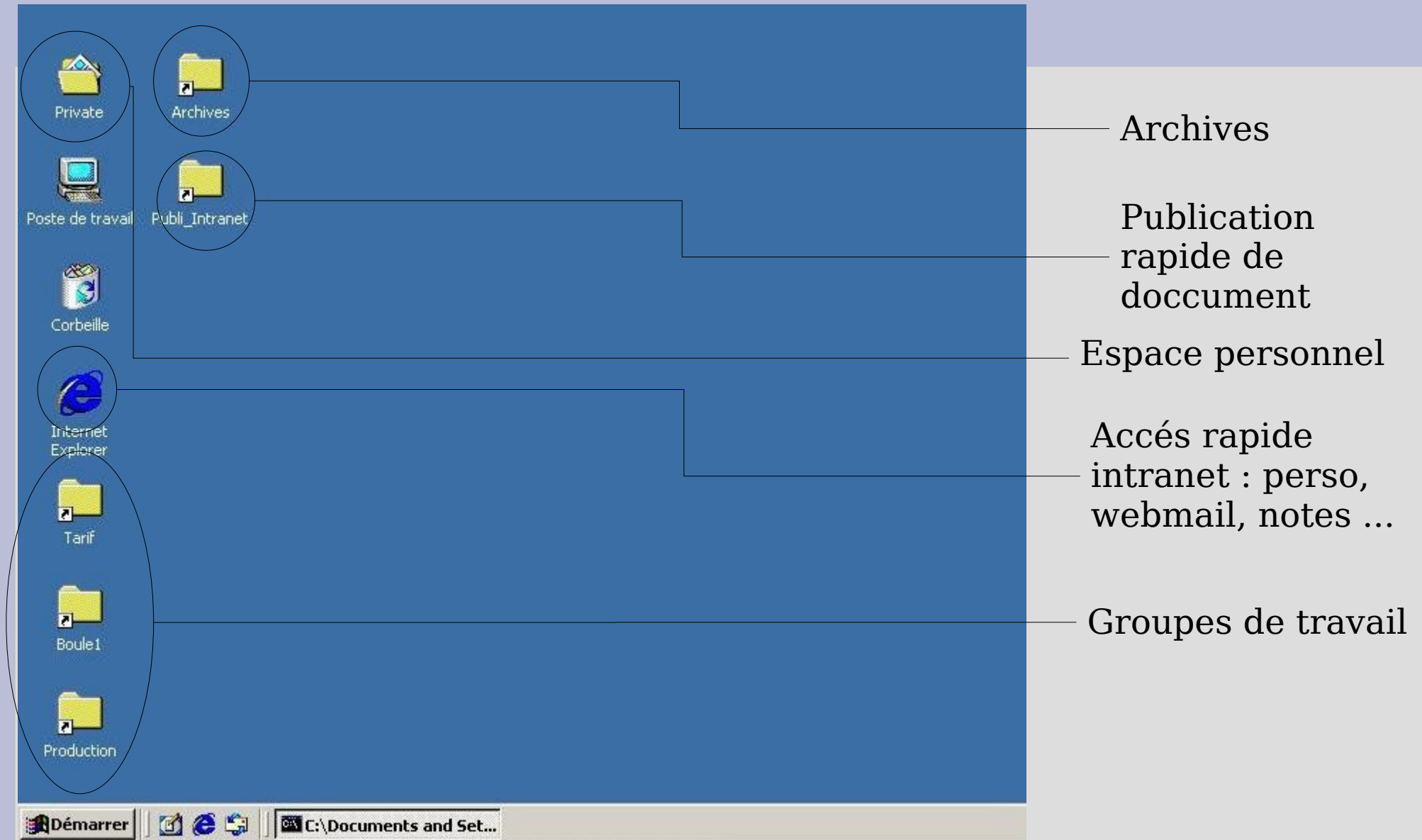


Régle pour l'espace

- Ne pas être hiérarchiste
- Règle du chemin minimal
- Regroupement de service
- Regroupement de communauté
- L'espace doit être borné (Quota)
- Ce bornage ne doit pas être un carcan



Bureau utilisateur



Archivage de données

- Débarrassé les disques
- Gardé une trace
- Ne pas confondre avec la sauvegarde

Nécessite une politique et des moyens

Archives

Les fichiers s'accumulent !

- Augmentation du coup de stockage
- Qui se souvient de ? Ou se trouve ?
- Augmentation des coup de sauvegarde
- Restoration problématique

=> On imprime tout !

Remède : politique d'archivage !

Règles d'archivage :

- Structure temporelle
 - Indexé par thème, projets et mots clef
 - Dupliquée sur du non réinscriptible
 - Contenu facilement accessible
 - Non compressés
 - Format originaux + vue !
 - Archivés les soft !
-
-

Stratégie d'archivage

- Volontaire : Basé sur les utilisateurs
 - Efficacité imprévisible
 - Forte variation entre individu
- Autoritaire : Basé sur des règles temporelles
 - Exploration des répertoire utilisateur
 - Stable au cours du temps

Existence d'une règle

accepté par tous validé par la

hierarchy !

Trucs et astuces !

- Archivage facile ! (façon poubelle)
Répertoire ou commande
 - Recherche facile
Interface Web !
 - Restoration facile
Validation délégué
 - Vérification de l'efficacité !
-
-

Sauvegarde

Motivation : coût de la perte
d'information

- Effacement accidentel
- Corruption volontaire
- Dysfonctionnement d'applications
- Panne matériel
- Perte ou vol de support

Analogie à un pb d'assurance !

Que sauvegarde t-on ?

- Les fichiers de bases de données
 - Les fichiers utilisateurs
 - Répertoires personnel
 - Emails, profils
 - Les configuration et déclarations
 - Annuaire (utilisateurs, machine)
 - Fichier de configuration, de logiciel ..
 - Les fichiers de système d'exploitation
-
-

Avec quoi ?

- Matériel
 - Filer = machine avec plein de disque
 - Lecteur de bande
 - Librairie = robot changeur de bande
- Logiciel
 - Intégrer avec une interface
 - Script + archiveur simple (tar, zip, dump)

Système de sauvegarde

- Dat
 - 20/40 giga
 - pas trop chère
 - Lecteur fragile
- DLT
- SLR
- SDLT

Quand ?

- Au moins une fois par jours
 - Sauvegarde incrémentale => diminution des volumes
 - Pas de perte > 1 jours
 - A un moment de faible activité
 - Peu de transaction
 - Peu de modif de fichiers
- 2 piege les BD et le MAIL => snapshot

Politique de sauvegarde !

Regroupe :

- Liste des volume sauvegarde
- Fréquence des sauvegarde
- Les moyens employes

Demande :

- Rôle de sauvegarde
- Calendrier prévisionnel



Calendrier

Semaine	1	2	3	4	1	2	3	4
L	K7_10	K7_2	K7_3	K7_4	K7_20	K7_6	K7_7	K7_8
M	K7_1	K7_2	K7_3	K7_4	K7_5	K7_6	K7_7	K7_8
M	K7_1	K7_2	K7_3	K7_4	K7_5	K7_6	K7_7	K7_8
J	K7_1	K7_2	K7_3	K7_4	K7_5	K7_6	K7_7	K7_8
V	K7_1	K7_2	K7_3	K7_4	K7_5	K7_6	K7_7	K7_8
S	K7_1	K7_2	K7_3	K7_4	K7_5	K7_6	K7_7	K7_8

Pratique de la restauration

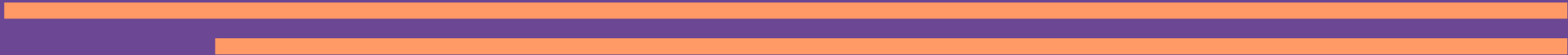
- Interrogatoire utilisateur
 - Dernière modification
 - Emplacement des fichiers
 - Coordonnées de l'utilisateur
 - Ne pas restaurer devant l'utilisateur
 - Plan de reprise après désastre
 - Réinstallation préalable
 - Plan de rechargement
 - Cahier de rôle
-
-

Partie 3 : Gestion des logiciels



Cahiers des charges logiciel

- Mise en autonomie
- Limité le nombre de logiciels
- Evité le doublonage (ex : 2 lecteur PDF)
- Homogénéïser les versions
- Evité les dépendance non indispensable
- Evité le clientélisme



Déploiement et mise à jour

- Configurer correctement les options
 - Former les utilisateurs
 - Ecrire un digest de la documentation
 - Vérifier la compatibilité avec :
 - le matériel (mémoire CPU(cpuhage))
 - les OS envisagés
 - les autres application
 - Les application mère
 - Récupérer les correctif existants (patch)
-
-

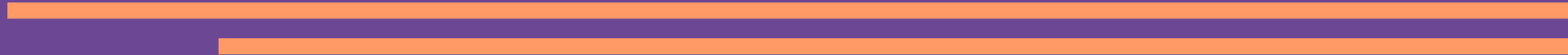
Configuration des logiciels

Ce fait :

- Par l'environnement
- Par la base de registre
- Par fichier de configuration (XML)

Problèmes :

- Mots de passe ?????
- Chemin relatif ...



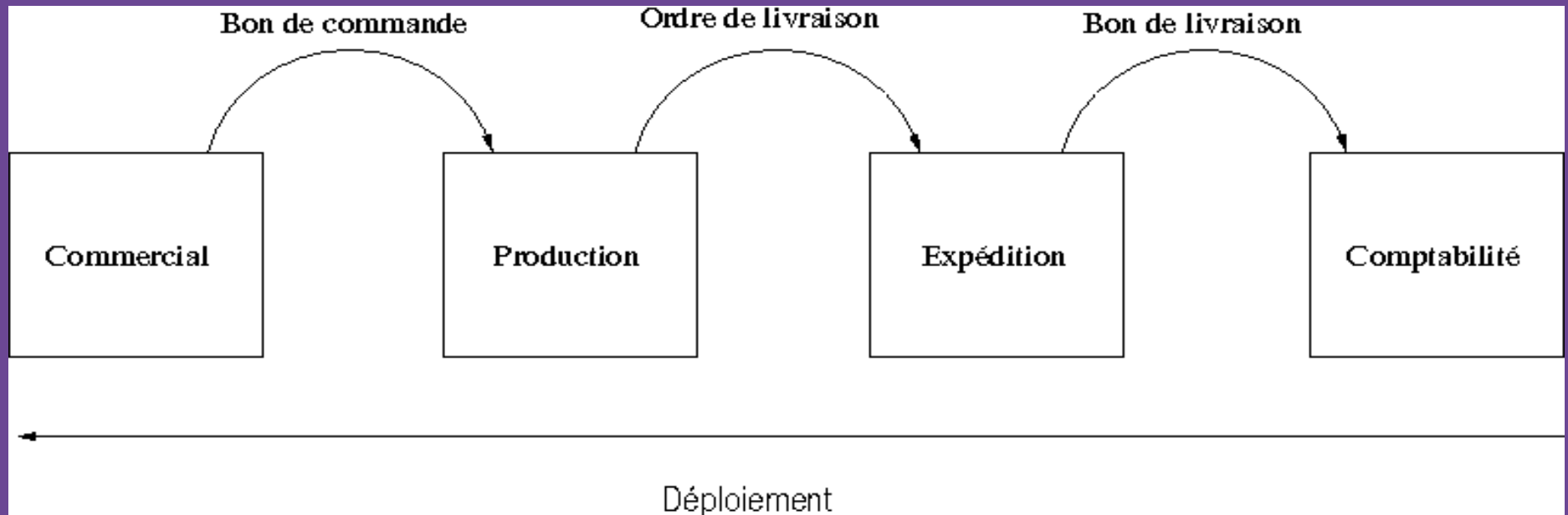
Stratégie de déploiement

- Vérifié la compatibilité ascendante et descendante
 - Choisir un jours (mercredi !)
 - Prévenir les utilisateurs !
 - Puis : par petit groupe
 - Bloquer l'application
 - Sauvegarder
 - Migrer les configurations utilisateur
 - Déployer
 - Déverrouiller
-
-

Service de logiciel

- Par fichier (/usr/local)
- Par auto installation (SMS)
- Par Serveur d'application (X11,RDP,ICA)
- A la main
 - Installation par défaut
 - La même partout
- ~~Avec GHOST~~

Mise à jours – Technique du bulldozer !



- En fonction du workflow
- En remontant la compatibilité
- Caché l'ancienne version

Maintenance logiciels

- Système d'exploitation
 - Patches, Pti, correctif
- Application
 - correctif
- Gestion d'incidents
 - Procédure
 - Rôle
 - Chaîne de traitement

Licence des logiciels

- Logiciel libre
 - Gain en terme de coût de possession
 - Changement d'échelle plus rapide
- Logiciel d'éditeur
 - Disponible
 - Documenter
 - supporter

Partie 4 : Organisation réseau



Réseaux – organisation

- Coopération systèmes (interactif, fichiers, bdd, dns,)
 - Entre ordinateurs
 - Transparent aux utilisateurs

Réseaux fiable et constant !

- Communication entre machines (mail, groupware, ...)
 - Processus entre utilisateurs
 - Entre utilisateurs mais asynchrone

Réseaux quelconque !

Réseaux – type de trafic

- Trafic interactif
X11, RDP, ICA, VNC, telnet, Ssh
- Trafic système
SGBD, NFS, SMB, CIF, DNS, YP,
KERBEROS, ldap, X500, snmp
- Trafic de communication
HTTP, HTTPS, FTP, SMTP, ...
Contraintes de délais, débit et connexion !

Réseaux – contrainte !

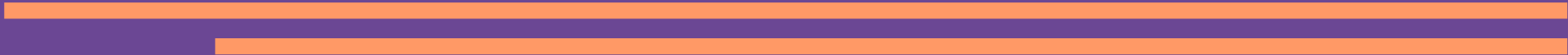
	Délais	Débit	Connexion	Type
Interactif	0.04	Constant	Permanente sur une session	LAN ou TDM
Système	0.8	Constant	Permanente	LAN ou MAN
Internet	30	Quelconque	QCQ	QCQ

Quelques définitions :

- LAN, MAN, WAN
- VLAN, VPN
- HUB, Switch, Router
- IDF

Réseaux – conceptions

- Concevoir un cablage isotrope
- Etablir un plan de contrainte
- Etablir un plan d'adressage
- Identifier toutes les liaisons et dépendance
- Documenté sérieusement sur papier

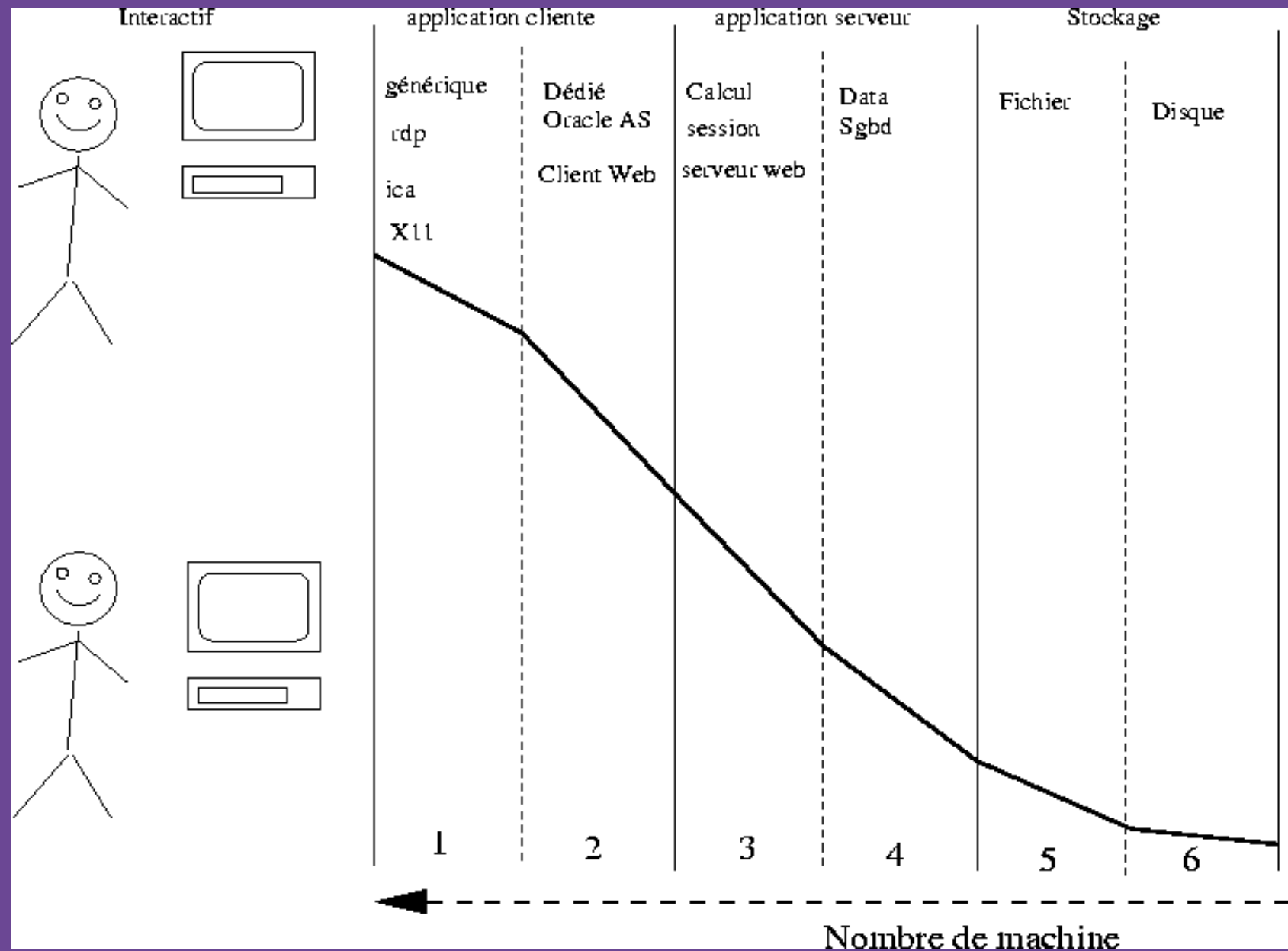


Rôle des serveurs

- Serveur : quoi c'est ?
 - Des programmes - oracle
 - Des ordinateurs – serveur de fichiers
 - Des machines – DEVWIN ou ETUD
- Deux extrêmes :
 - Mainframe + terminaux
 - Micro ordinateurs personnel



Modèle NTIERS



Mise en oeuvre des Ntiers

- Dupliquer les service fondamentaux
- Une business unit = un serveur à plusieurs service
- Limité au maximum le nombre de pièces
- Dimensionner largement chaque élément

Risque de pannes

- Dépendance accrue
Elle n'est qu'apparente
- Mais moins de machine
Moins de panne
- Risque de black-Out
Mesure = nombres d'heures perdus

Remède = surveillance

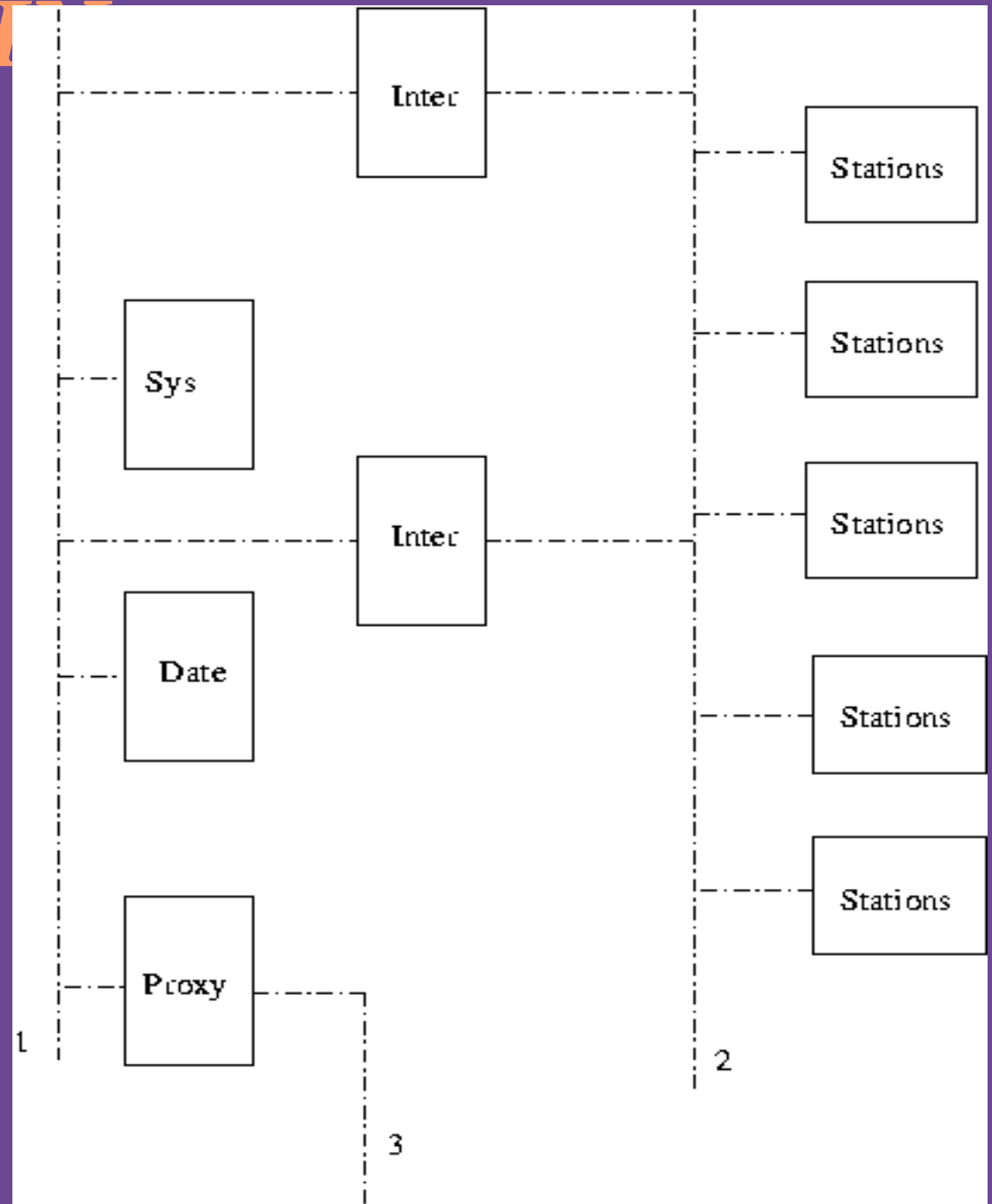
Différents type

- Serveur de fichier
- Serveur de base de données
- Serveur D'application
 - Interactif
 - Façon web service
- Serveur internet, web, mail, ftp

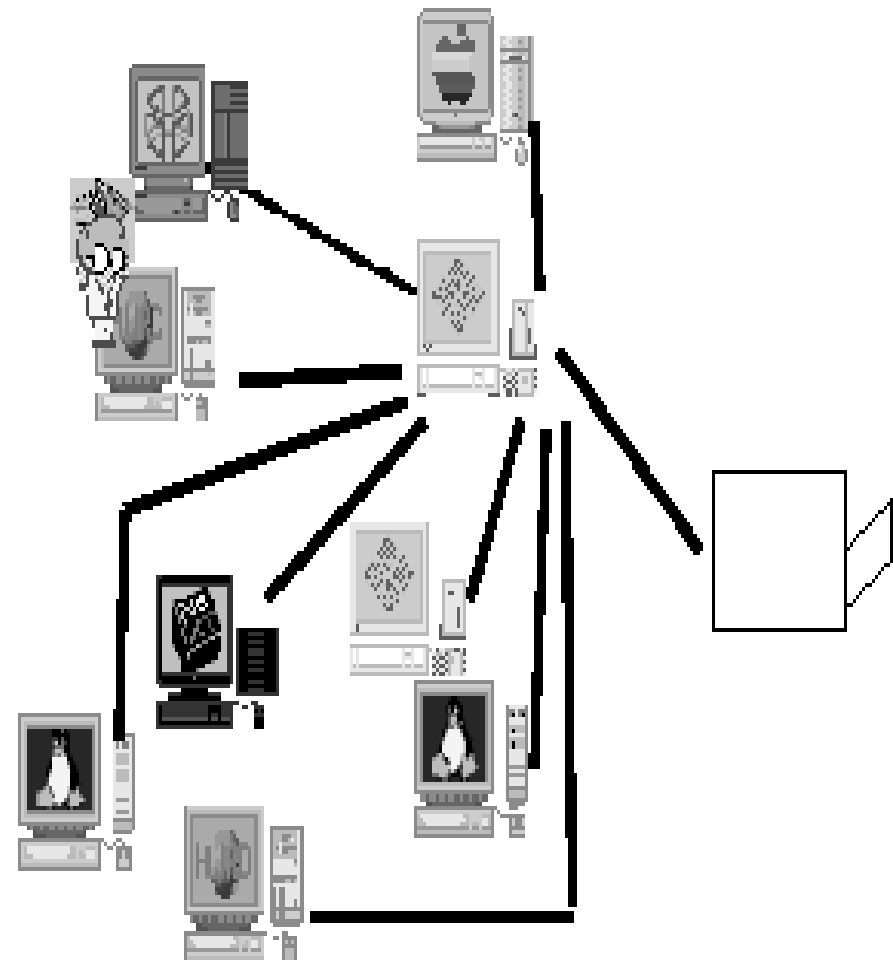
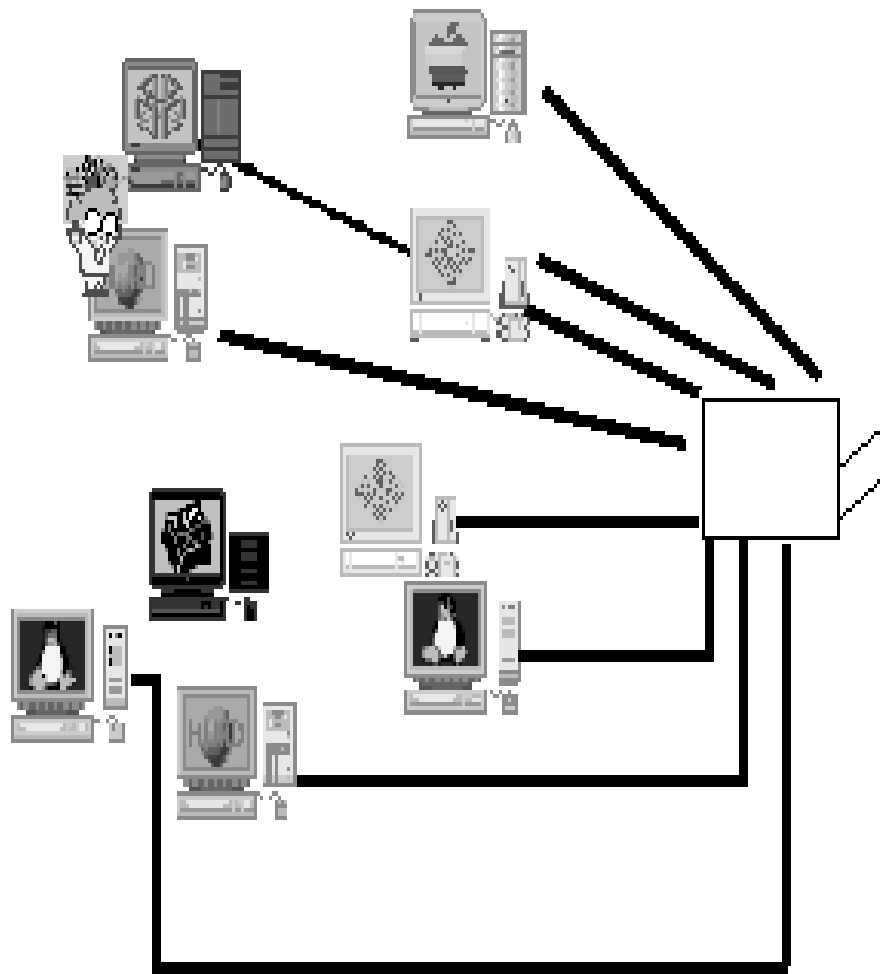
Différents rôle !

Modèle ISIMALT

- Inter serveur d'applications
- Sys serveur système
- Data serveur de sgbd
- Proxy serveur SMTP, HTTP, FTP, ...



Service d'impression



Chapitre 5 métier

- 3 type d'administrateur
 - Le tech
 - Le gourou
 - L'idiot
 - Déontologie
 - Protéger les données
 - Protéger la vie privé
 - Ne pas desinformé
 - Ne pas faire de clientélisme
-
-

Chapitre 6 sécurité

- Sécurité active
 - Protégé
 - Résisté
 - Filtré
- Sécurité passive
 - Inondation
 - Incendie
 - Vol

Mesure de protection

- Sauvegarde
 - Sécurisation des mots de passe
 - Complexité
 - Fréquences des changements
 - Sécurisation des système de fichier
 - Problème du partage
 - Problème de la manipulations des droits
 - Accès au sauvegarde
-
-

Sécurisation des applications

- Back door
 - Accès connus des programmeur
 - Ajouté par des virus ou spyware
 - remède filtrage externe :
- Bug connus permettant
 - L'injection sql
 - Les buffer overrun
 - Les dénis de services
 - remede : install non standart

Durcissement des système

- Restriction de l'accès physique
 - Restriction d'accès aux information de sécurité
 - Restriction d'accès au système de fichiers
 - Limitation des droits et application utilisateur
 - Installation de patch (correctif)
 - Recherche des anomalie
-
-

Filtrage des accès et virus

- Firewall
 - C'est ton meilleurs ennemie
 - C'est un trucs central
 - C'est contraire a la moral
 - Ca ne doit que filtré
 - Tcpwrapper
 - hosts.allow
 - hosts.deny
 - Utilisation de proxy
-
-

Protection physique

- Vols de données (VPN/GED)
- Inondation (where are th loo please !)
- Bris de matériel (range ton bordel)
- Incendie (eteind ton clop !)
- Vol et dégradations de matériel (ferme la porte !)

