TC131C - Introduction à Unix/Linux

Christophe Lohr

Automne 2018

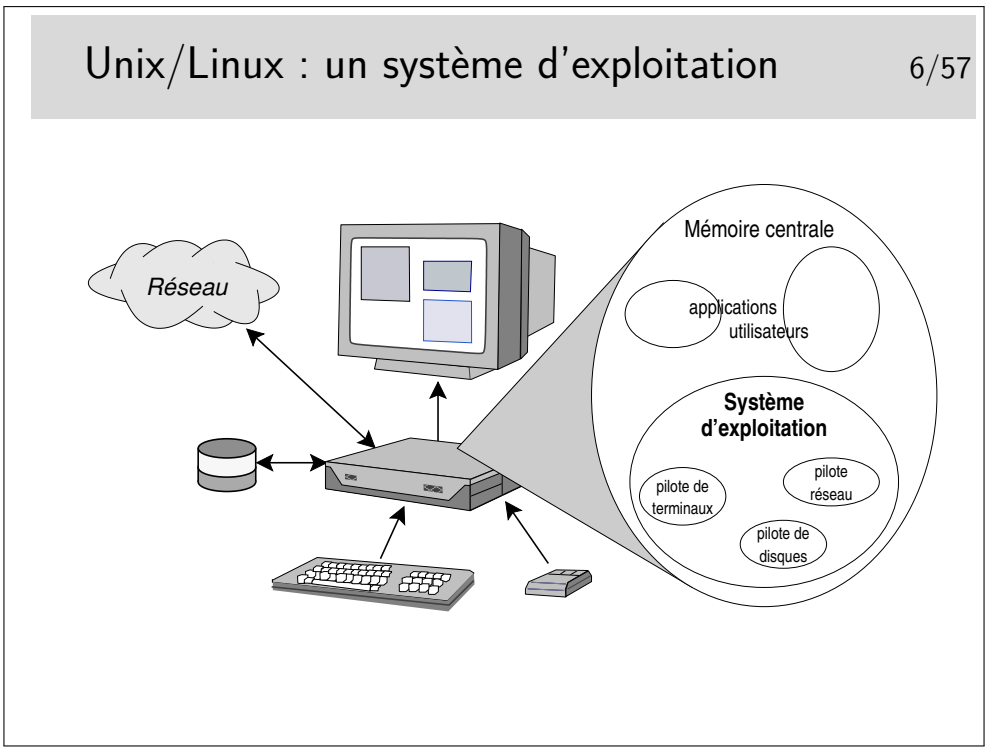
Grace Hopper - 1960

Dennis Ritchie & Ken Thompson - 1972

Sommaire

1 Introduction

1.1 Le système d'exploitation



Le système d'exploitation peut être vu comme une application particulière, chargée en mémoire centrale, très rapidement après la mise sous tension de la machine (juste après que que programme résidant en mémoire EEPROM se soit exécuté, ce qu'on appelle le BIOS dans l'architecture PC). Cette application permet d'utiliser l'ordinateur, elle gère les applications qui s'y déroulent et sert d'interface entre elles et les périphériques matériels. La mémoire centrale est chargée avec le Système d'exploitation d'une part et avec les programmes applicatifs lancés par les utilisateurs d'autre part. Le système d'exploitation contient des modules spécifiques aux périphériques qu'il sait contrôler, ce sont les pilotes (*drivers* en anglais)

1.2 Historique

Historique 8/57

- Unix naît officiellement le 1er janvier 1970 dans les laboratoires Bell AT&T : Ken Thompson et Dennis Ritchie
- Années 70 : développement d'Unix : 1973 langage C...
- Années 80 : deux filières
  - Univ. Berkeley : système Unix BSD (Berkeley Software Development)
  - AT&T : Unix Système V (déjà...), version commerciale standard
  - Sun (création 1983) et Digital (Dec) choisissent BSD : SunOS (jusqu'à la version 4) et Ultrix (Dec)
  - 1984 : Richard Stallman crée la Free Software Foundation et la Licence Publique Générale (GNU GPL)

Historique 9/57

- Années 90 : La version Système V s'impose, Sun s'y rallie (Solaris ou encore SunOS-5), Digital adopte une autre version développée par le consortium OSF, HP-UX (HP), AIX (IBM) sont des systèmes V.
- Un trublion apparaît : Linus Torvalds qui écrit le noyau Linux
- Les versions BSD continuent en logiciel libre : FreeBSD, OpenBSD...

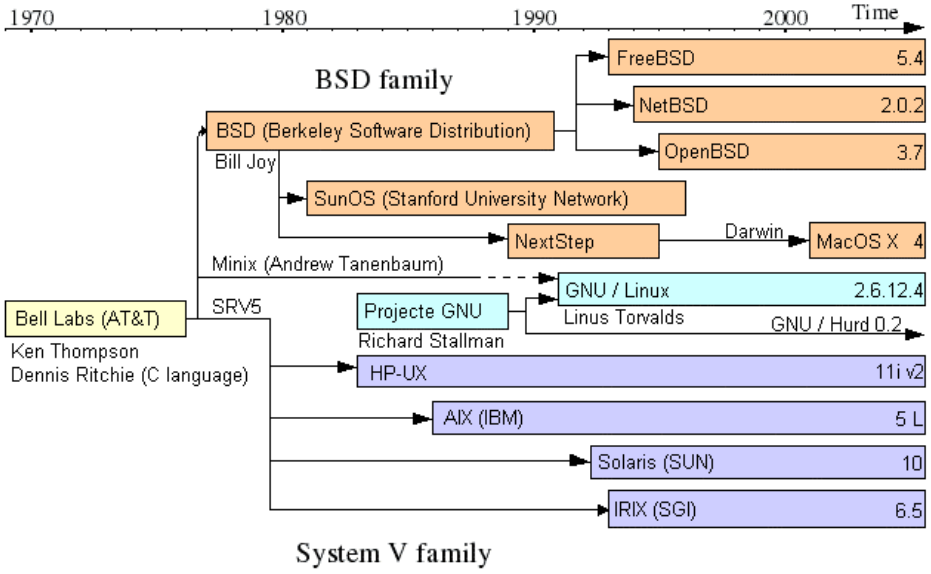
Pointeurs :

— `http://en.wikipedia.org/wiki/Unix`

— `http://virtual.park.uga.edu/hc/unixhistory.html`

— `http://www.princeton.edu/~hos/mike/transcripts/thompson.htm` (interview de Ken Thompson)

— http://www.unix.org/what_is_unix/history_timeline.html



1.3 De Unix à Linux

Linux : un système Unix 11/57

- Philosophie d'Unix :
  - (presque) tout s'utilise comme un fichier
  - "Do one thing, do it well" (Doug McIlroy, l'inventeur des *pipes Unix*) :
    - Write programs that do one thing and do it well.
    - Write programs to work together.
    - Write programs that handle text streams, because that is a universal interface.
- Caractéristiques d'un système d'exploitation Unix :
  - Multitâche (multi processus)
  - Multi utilisateurs
- Spécificités (de Linux et de tous les Unix) :
  - Son Système de Gestion de Fichiers
  - La gestion des processus
- → Linux c'est (une implémentation) Unix

...vocabulaire... 12/57

Linux (p.ex. Linux 3.2.0)

Le noyau, uniquement !

GNU/Linux

+ commandes Unix de base (implémentation de GNU)
copier un fichier, répertoire, permissions utilisateur..

une distribution Linux (p.ex. Ubuntu 12.04, Debian Wheezy)

+ organisation des fichiers, outils d'administration, applications

Sur clef USB :

— LinuxLive USB Creator `http://www.linuxliveusb.com/` (sous Windows)

— PenDriveLinux YUMI `http://www.pendrivelinux.com/yumi-multiboot-usb-creator/` (sous Windows)

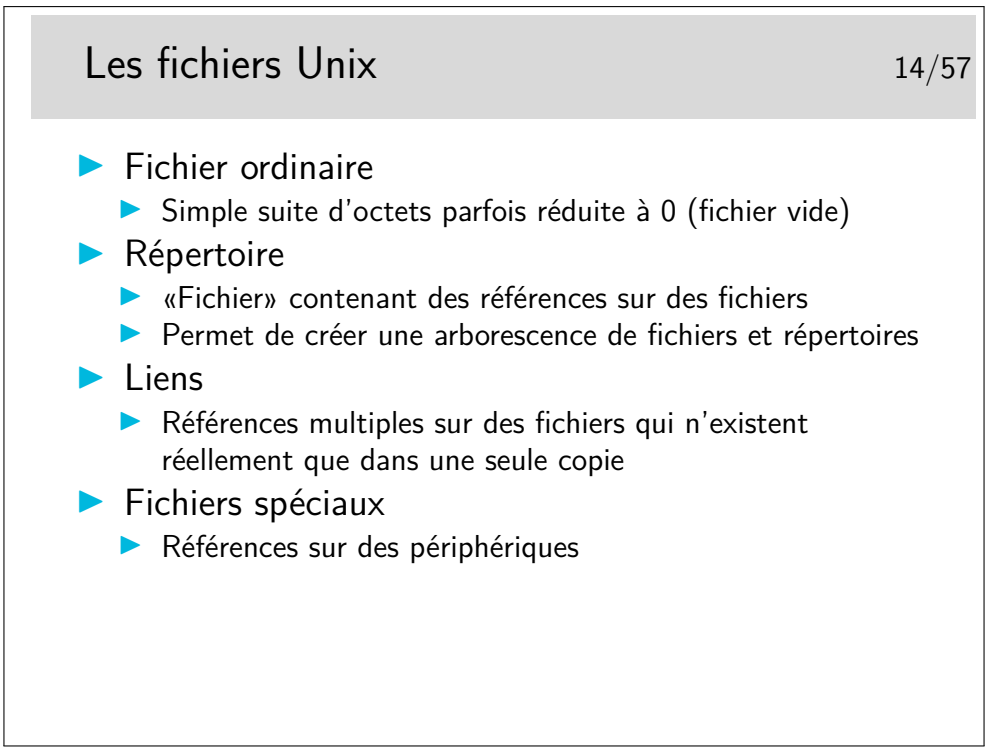
— Xboot `https://sites.google.com/site/shamurxboot/` (sous Windows)

— MultiBoot `LiveUSBhttp://liveusb.info/dotclear/` (sous Linux)

— etc.

2 Le système de fichiers

2.1 Structure, nommage, droits

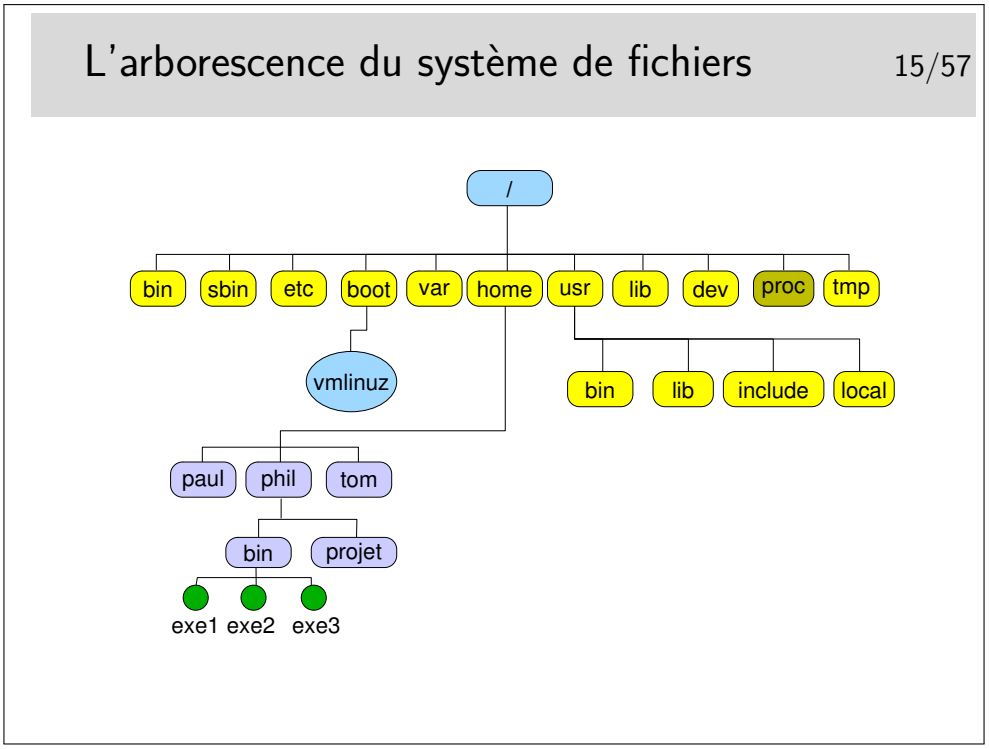


Il existe quelques autres types de fichiers pouvant apparaître dans l'arborescence :

— les sockets (type `s`) permettant la communication entre processus

— les tubes nommés (type `p` comme *pipe*) permettant aussi la communication entre processus

Les liens peuvent être de deux types : liens durs (version originale des liens sur Unix) et les liens symboliques (type l), version apportée par l'Unix de Berkeley (BSD) pour augmenter la portée des liens natifs (durs). Les liens durs ne peuvent être réalisés qu'entre références (nom dans un répertoire, on dit aussi entrée dans un répertoire) sur un même système de gestion de fichiers. Les liens symboliques peuvent passer les frontières physiques des système de fichiers.



— `/bin` et `/usr/bin` les commandes standards

— `/etc` fichiers d'administration

— `/sbin` commandes d'administration

— `/lib` et `/usr/lib` les bibliothèques (fichiers contenant les fonctions appelées par les commandes pour réaliser les opérations avec le système, exemple libc.a est la bibliothèque standard du langage C).

— `/dev` les fichiers spéciaux, référencent les périphériques du système (les *devices*).

— `/tmp` répertoire où sont créés les fichiers temporaires, il peut exister aussi /usr/tmp et /var/tmp.

— `/var/spool` répertoire où sont créées les files d'attente pour différents services tels que l'impression, le courrier électronique, etc.

— `/var/spool/cron` contient les travaux du service *cron* (voir cette référence dans le manuel de référence, faire man cron).

— `/usr/include` contient les fichiers d'entête standards des programmes en langage C.

— `/boot` répertoire contenant les composants du noyau du système.

— `/boot/vmlinuz` le noyau (le système-lui même en quelque sorte).

— etc.

Une organisation standardisée sous Unix : Filesystem Hierarchy Standard (`http://www.pathname.com/fhs/`).

Les fichiers - Le nommage

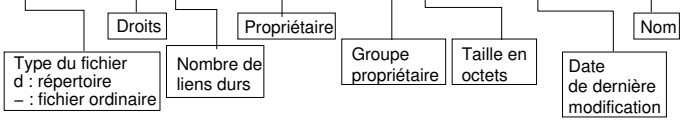
- Nommage abolu
  - par rapport à la racine, le nom commence par /
  - /home/phil/bin/exe1
- Nommage relatif
  - relatif au répertoire dans lequel on est :

home/phil/bin/exe1	si on est dans /
phil/bin/exe1	si on est dans /home
bin/exe1	si on est dans /home/phil
exe1	si on est dans /home/phil/bin

Visualiser le contenu d'un répertoire

- La commande ls
  - Exemple :

```
[bash]$ ls -l
total
-rwxr-xr-x    1   clohr   ens-rec     7790   avr 11 2005 essai
-rw-rw-r--    1   clohr   ens-rec     1122   avr 24 2005 essai.c
-rw-rw-r--    1   clohr   ens-rec  9869052   avr 25 2005 test
```



Les fichiers cachés 18/57

- Ce sont les fichiers dont le nom commence par un point
  - Exemple : .bashrc
- Par défaut les outils d'affichage du contenu des répertoires n'affichent pas les fichiers cachés
- Ce sont généralement des fichiers de configuration d'applications
- On peut les comparer à la base de registres sur des systèmes concurrents à Unix/Linux
- Il existe aussi des répertoires cachés, leur nom commence aussi par un point

Pour visualiser la liste des fichiers cachés il faut utiliser l'option `-a` de `ls`. Pour les outils graphiques de gestion de fichiers (les «explorateurs» dirions nous sous un autre système d'exploitation bien connu), il existe une option de paramétrage dans les menus de configuration (parfois appelés «*préférences*»).

Les répertoires «`.`» et «`..`» 19/57

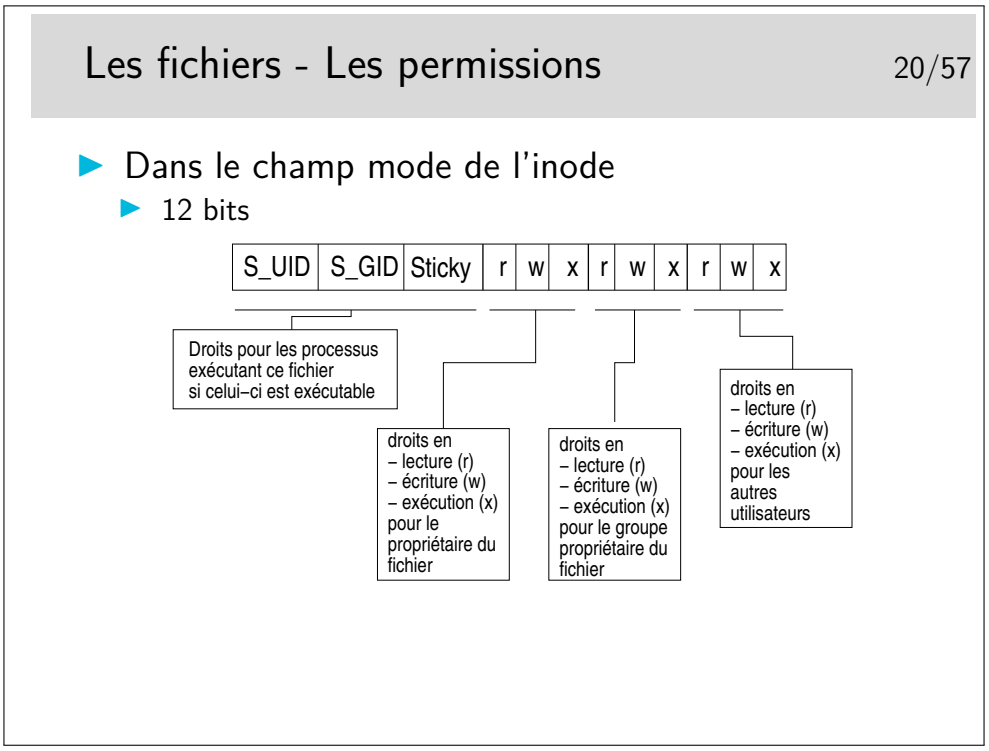
- Un répertoire n'est jamais vide, même à sa création, il contient déjà deux références sur des répertoires de nom «`.`» et «`..`»
  - Le répertoire «`.`» (point) constitue une référence sur le répertoire lui-même
  - Le répertoire «`..`» constitue une référence sur le répertoire immédiatement au dessus dans l'arborescence (le répertoire *père* en quelque sorte)
- Utilisation
  - Nommage sans ambiguïté d'un fichier local : `./test` par exemple
  - Nommage rapide d'un fichier au dessus : `../fichier` par exemple

Il arrive à beaucoup de gens d'écrire un petit fichier d'essai et de le nommer `test`. Après qu'il soit rendu exécutable, il est essayé... Et...Surprise ! le résultat n'est pas du tout celui attendu... Car la commande lancée, de nom `test`, n'est pas celle qu'on croit, il

s'agit de `/bin/test` et non le test du répertoire courant (si la variable d'environnement `PATH` ne contient pas le caractère « `.` » dans sa liste avant `/bin`).

Il suffit pour remédier à cela d'entrer alors la ligne de commande `./test` et le tour est joué.

En général, par défaut, le « `.` » ne figure pas dans la variable `PATH` pour des raisons de sécurité élémentaire et toute commande se situant dans le répertoire de travail (celui dans lequel on se trouve) doit se lancer avec la séquence `./nomFichier` (à moins que le répertoire de travail ne soit listé naturellement dans la variable `PATH`).



Si les droits en écriture/lecture/exécution sont assez évidents à comprendre il n'en va pas de même pour les trois premiers : `S_UID`, `S_GID` et le `Sticky bit` :

— Ces droits concernent les processus d'exécution du fichier, ils ne sont actifs qu'au moment où le fichier est en exécution. Ils précisent ce que le fichier (si l'on peut dire) a le droit de faire lorqu'il s'exécute.

— Lorsqu'une commande est lancée, si celle-ci correspond à un fichier exécutable, ces droits agissent comme suit :

  — si le bit *S_UID* est positionné, le processus d'exécution a les droits du propriétaire du fichier et non ceux de l'utilisateur qui a lancé la commande,

  — si le bit *S_GID* est positionné, le processus a les droits du groupe propriétaire du fichier

  — si le *sticky bit* est positionné, le processus ne sera pas purement et simplement effacé de la mémoire, il sera recopié en zone de swap et si la commande correspondant est rappelée, son rechargement en mémoire sera plus rapide. Ce n'est plus beaucoup utilisé.

Remarque importante : le *sticky bit* est maintenant utilisé sur des répertoires ouverts en lecture/écriture à tous pour restreindre le droit d'effacement des fichiers qui s'y trouvent

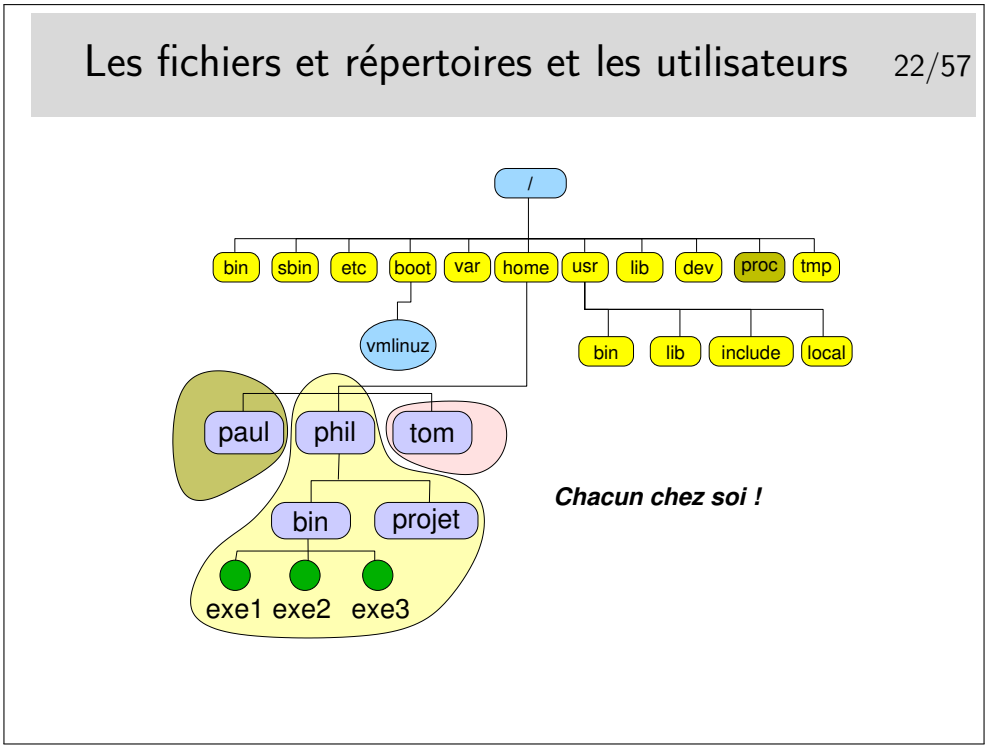
au seul propriétaire de ces fichiers. Cas des répertoires `/tmp`, `/var/tmp`, `/usr/tmp`. Voir aussi la notion d'attribut avec la commande `chattr`.

Les droits sur les répertoires 21/57

- Ce sont les mêmes types de droits que pour les fichiers : `r`, `w` et `x` et même `t`
- La sémantique associée est toutefois différente
- Droits :
  - `r` : le répertoire est lisible, on peut lister son contenu
  - `w` : le répertoire est «écrivable», on peut y créer des fichiers ou des répertoires
  - `x` : le répertoire n'est pas exécutable, il est accessible : on peut aller dedans, ou le traverser pour accéder à ce qu'il contient (fichiers, sous-répertoires)
  - `t` : le *sticky bit*, valable pour un répertoire ouvert en `w` à tout le monde, indique que seul un propriétaire de fichier peut supprimer ce fichier.

Si un répertoire est interdit de passage (i.e. le droit `x` est ôté), on ne peut pas s'y déplacer, on ne peut pas non plus descendre dans ses sous-répertoires, même si ceux-ci sont autorisés. Un droit `x` ôté est comme un obstacle infranchissable.

Si un répertoire à le droit `w` pour les utilisateurs non propriétaires, n'importe qui peut y créer un fichier, mais n'importe qui peut aussi supprimer ce fichier. Ce serait le cas pour les répertoires contenant les fichiers temporaires (`/tmp`, `/var/tmp`) si ceux-ci n'étaient pas munis du droit `t`.



Chacun chez soi... Et chacun maître chez soi. Si un utilisateur veut ouvrir son répertoire à tout le monde il en a le droit. Il a aussi le droit de fermer son répertoire à tous (même à lui même, ce qui est embêtant pour lui sur le moment, mais il peut modifier à nouveau les droits pour se ré-autoriser...).

Les répertoires ouverts en lecture sont visitables pour autant qu'ils aient le droit `x` positionné. Les répertoires `/tmp`, `/var/tmp`, `/usr/tmp` sont ouverts à tous et tous peuvent y créer des fichiers et les supprimer. Généralement ces répertoires sont munis du *sticky bit* afin de restreindre le droit d'effacement aux seuls propriétaires des fichiers.

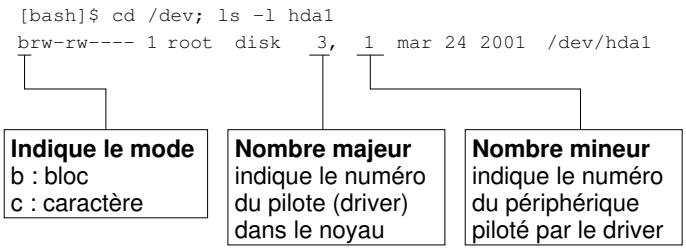
Il est donc possible de «se promener» dans la plus grande partie du système de fichiers. Seuls certains répertoires et fichiers sensibles sont interdits.

Les fichiers spéciaux 23/57

- Référencent des périphériques
  - Permettent les échanges (lectures/écritures) avec les pilotes des périphériques
  - Permettent le contrôle de ceux-ci
- Deux types
  - Les périphériques en mode bloc
    - les échanges se font par bloc d'octets (par «pages»)
  - Les périphériques en mode caractère appelé encore mode transparent (on dit plutôt mode *raw*)
    - les échanges se font octet par octet
  - Les disques sont plutôt en mode bloc, les terminaux en mode *raw*

Les fichiers spéciaux - le répertoire /dev 24/57

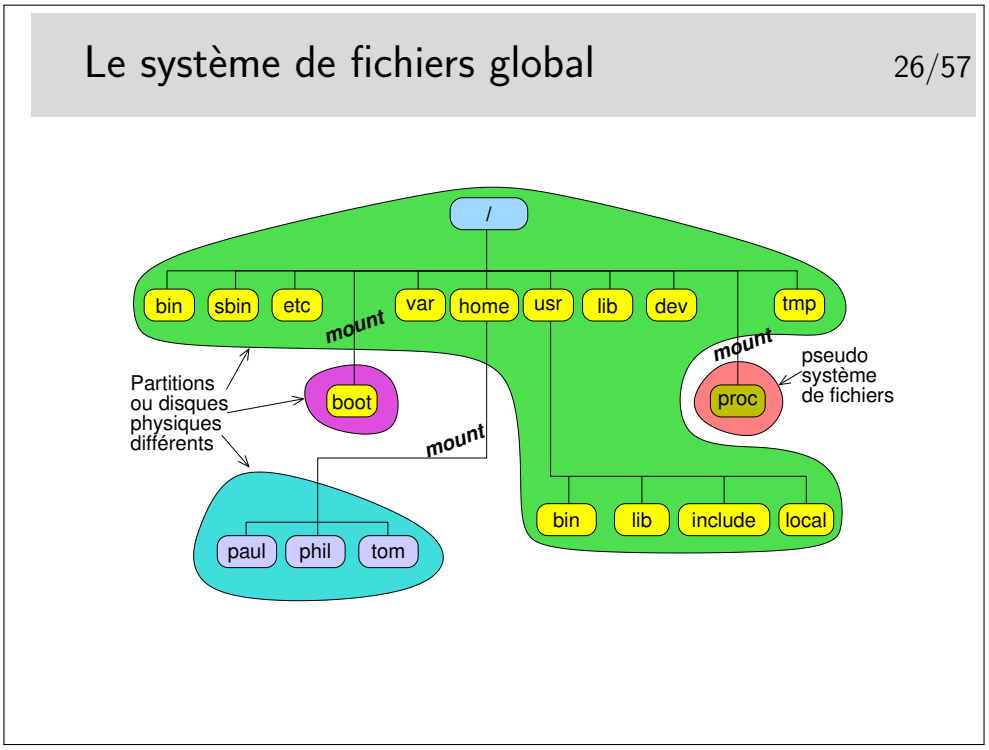
- Exemple d'entrée dans /dev



Ces fichiers sont créés par la commande `mknod`, ils peuvent être créés n'importe où mais en général on les trouve dans `/dev`.

Cette manière de voir les périphériques permet de considérer ceux-ci comme des fichiers (certes spéciaux, mais fichiers quand même), ainsi les échanges entre les applications et les périphériques se font essentiellement par des écritures et des lectures, comme pour des fichiers normaux.

2.2 Organisation sur disques



Le système de fichier global peut être constitué de plusieurs systèmes de fichiers de natures identiques ou différentes.

Dans le schéma ci-dessus on a choisi de créer 3 partitions formatées en système de fichier Linux (`ext2` ou `ext3`) :

- la partition racine avec `/bin`, `/etc`, `/var`, `/usr`, `/lib`, `/dev`, `/tmp`, ...
- une partition pour `/boot` (fait par défaut sous RedHat ou Debian par exemple)
- une partition pour les utilisateurs
- le système de fichiers proc est un pseudo système de fichiers, il n'existe pas sur disque mais est créé en mémoire vive. C'est en quelque sorte un point d'accès au noyau interne depuis le système de fichiers.
- à noter aussi l'existence du pseudo-système de fichiers `/sys` avec le noyau 2.6, donnant accès aux informations sur les «objets noyaux» tels que les bus et les drivers.

Les systèmes de fichiers sont raccrochés à la racine lors du lancement du système. D'abord le système crée la racine virtuelle qu'il nomme «`/`». Il raccroche dessus immédiatement le système de fichiers racine, puis ensuite il raccrochera les autres systèmes de fichiers selon l'ordre indiqué dans le fichier `/etc/fstab`.

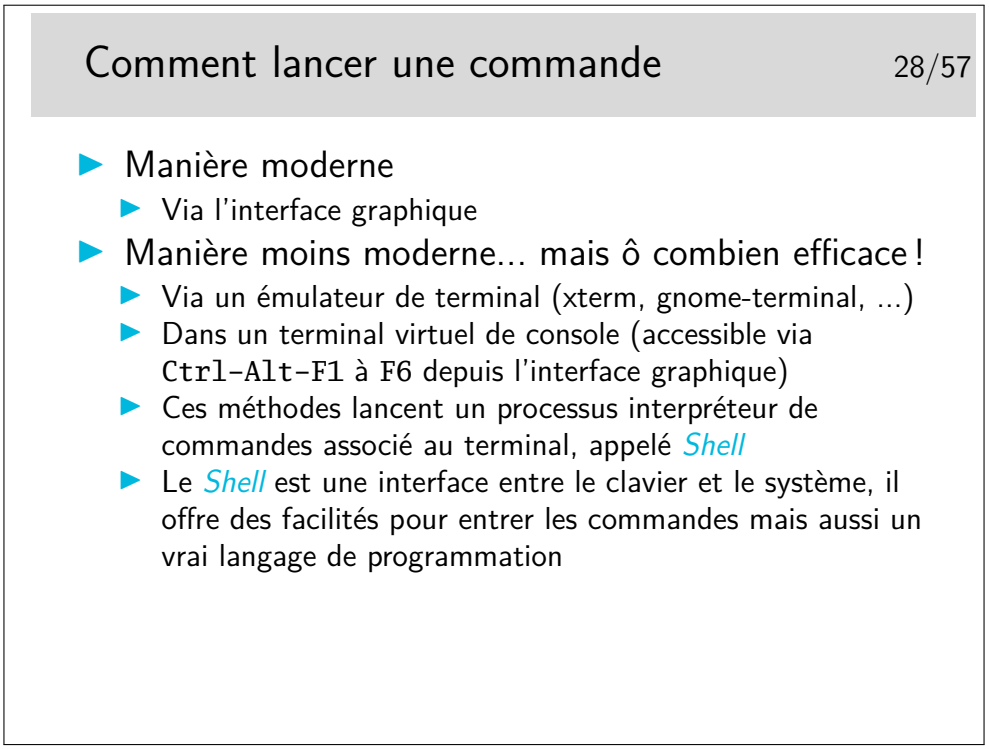
L'utilitaire permettant de raccrocher un système de fichiers à l'arborescence globale est la commande `mount`.

La question pertinente est de savoir combien de partitions il faut pour installer le système. On peut laisser la procédure d'installation faire seule mais les choix automatiques ne sont pas toujours satisfaisants.

Notons que lorsqu'un utilisateur insère un CD ou une clé USB, le volume apparaît alors comme par magie sur son bureau. Techniquement, c'est bien `mount` qui est utilisé (de façon cachée) par le gestionnaire de fichier.

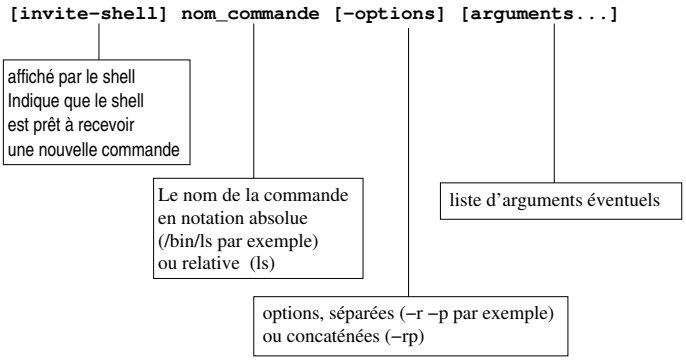
3 Utilisation courante

3.1 Les commandes et leur syntaxe



Les commandes 29/57

- Syntaxe générale



Les commandes - La variable PATH 30/57

- Le `PATH` est une variable d'environnement
- Contient la liste des répertoires où se trouvent les commandes que l'on peut appeler par leur nom relatif le plus court : `ls` au lieu de `/bin/ls` par exemple
- Ne pas croire le système lorsqu'il vous dit : «*command not found*», il se peut que votre variable `PATH` soit mal configurée...
- Configuration dans le shell directement ou dans `$HOME/.bashrc` :
  - `export PATH=$PATH:/usr/local/bin` (par exemple)

La variable `PATH` peut aussi être configurée dans `$HOME/.bash_profile` mais ce fichier n'est pas lu systématiquement quand on ouvre une fenêtre terminale. Il n'est lu que lors de la connexion (le *login*) dans une console virtuelle (que l'on accède à partir de l'interface graphique avec le jeu de touches clavier `<Ctrl-Alt-F1>`.

Si on modifie la variable `PATH` directement dans le Shell par la commande `export` ci-dessus, la modification est prise en compte dans le shell, évidemment, mais dans CE shell seulement... Pas dans le shell de la fenêtre terminal d'à côté par exemple, et c'est très

déconcertant pour le néophyte. Pour comprendre pourquoi une telle modification n'est pas vue immédiatement de tous les shells il faut savoir qu'un shell en cours d'exécution est avant tout un processus qui hérite des propriétés du processus «terminal» lui-même (le processus qui «dessine» la fenêtre à l'écran). Ces processus forment une arborescence et héritent leurs propriétés les uns des autres d'une manière descendante. Le processus «terminal» lance le processus Shell. Le processus Shell hérite de son «père», le terminal. Si on modifie les propriétés d'un processus, les modifications pourront être vue par des sous-processus mais pas par les processus au dessus dans l'arborescence. Ni à fortiori par ceux «à coté», ou dans une autre arborescence...

Pour qu'une modification d'environnement soit permanente il suffit qu'elle soit écrite dans un fichier de configuration pris en compte systématiquement lors du lancement du Shell. Le fichier personnel `.bashrc` est le plus approprié pour le shell `bash` ; et le fichier `.tcshrc` (ou `.tcsh.PERSO`) pour le shell `tcsh`.

Les commandes - Quelques raffinements 31/57

- Les commandes en arrière-plan (*background*)
  - la ligne de commande se termine par le caractère &
  - le shell lance la commande et redonne la main aussitôt sans attendre qu'elle se termine. La commande poursuit son exécution en arrière-plan
- Les redirections
  - redirection du fichier standard de sortie
    - *commande* > *fichier*
  - Redirection du fichier standard d'erreur
    - *commande* 2> *fichier*
  - redirection du fichier standard de sortie et d'erreur
    - *commande* > *fichier* 2>&1

Les commandes - Tubes de communication 32/57

- Pour réaliser des filtres
  - *commande1* | *commande2* | *commande3* ...
  - le texte normalement affiché par *commande1* est redirigé vers *commande2* (il est lu par *commande2* et n'apparaît pas à l'écran). Le résultat est envoyé vers *commande3* et ainsi de suite
  - Exercice :
    - afficher le contenu du répertoire `/usr` à l'aide de la commande `ls -l`
    - en utilisant un tube de communication et la commande `head`, n'afficher que les 5 première lignes du résultat précédent
    - en utilisant un autre tube et la commande `tail`, n'afficher que la dernière ligne du résultat précédent
    - Voir le manuel en ligne pour savoir comment utiliser ces commandes

C'est en fait la philosophie de base de l'utilisation d'Unix : une pléiade de petits utilitaires que l'on assemble au moyen de tubes pour réaliser une grande tâche. Le contraire des approches monolithiques.

Note : lors de l'exécution de `commande1 | commande2`, les deux programmes sont exécutés en parallèle. Sur d'autres systèmes mono-tâche comme MS-DOS, il y a d'abord l'exécution du premier programme en sauvegardant sa sortie dans un fichier temporaire, puis ensuite l'exécution du second programme en lisant le fichier temporaire...

Les commandes – Les jokers (*wildcards*) 33/57

- Un caractère spécial qui en remplace plusieurs...
  - Pour les noms de fichiers
  - Un genre d'expression rationnelle (mais non POSIX)
- Exemple : `rm *` (efface les fichiers du répertoire)
- Reconnus par le shell :
  - `?` : n'importe quel caractère
  - `*` : zéro ou plusieurs caractères
  - `[A1x]` : le caractère `A` ou `1` ou `x`
  - `[a-z]` : les caractère de `a` à `z` (code ASCII)
  - `{ab,ac}` : la chaîne `ab` ou `ac`

Les commandes Unix classiques 34/57

(liste non exhaustive...)

- Créer, naviguer parmi les fichiers et répertoires
  - `ls cd pwd cp mv rm mkdir rmdir`
- Afficher — éditer des fichiers
  - `more less` — `vi emacs touch`
- Filtres texte
  - `echo cat grep sort uniq sed tail tee head cut tr split paste printf`
- Comparaison de fichiers
  - `comm cmp diff patch`

Les commandes Unix classiques 35/57

...

- Administration basique (niveau utilisateur)
  - `chmod chown ps su w who`
- Communication
  - `mail telnet ftp finger ssh`
- Shells
  - `sh csh ksh zsh bash tcsh`

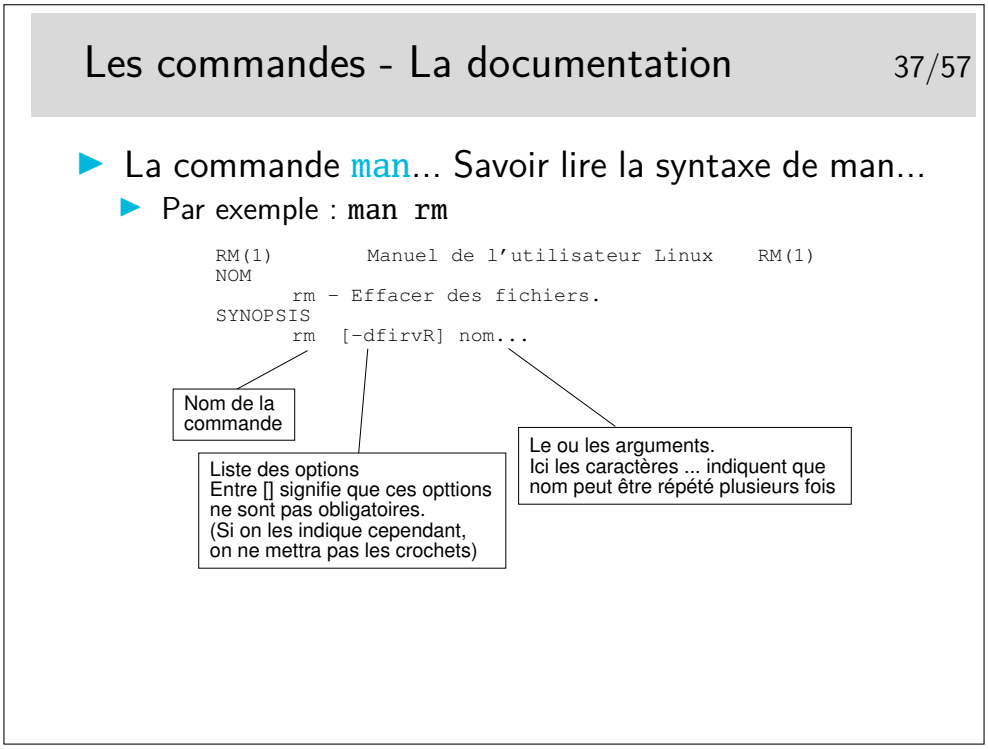
Ce ne sont quelques commandes classiques que tout utilisateur d'Unix finit par connaître par coeur au bout de quelque temps de pratique...

Même si il est évidemment difficile de les connaître toutes dans le détail, il est bon de savoir qu'elles existent et de savoir retrouver leur documentation en temps utile.

Ces commandes sont rangées typiquement dans `/bin` et `/usr/bin`

`http://en.wikipedia.org/wiki/List_of_Unix_programs`

3.2 La documentation



Les pages du «manuel» Unix, en ligne (Sun fournissait un gros classeur du man imprimé...).

La source d'information de référence incontournable. Ne pas poser une question dans les forums de discussion dont la réponse est dans le man... sous peine d'être bien mal accueilli :-)

Attention : les pages du man ne sont pas des cours ni des tutoriels, mais du condensé d'information. Chaque mot est important. Il est parfois difficile de se plonger dedans, mais les pages de man sont toutes rédigées selon la même manière, tant est si bien que lorsque l'on a pris le plis, il est relativement facile de s'y retrouver rapidement.

Le man est organisé en sections :

1. Commandes utilisateur
2. Appels système
3. Fonctions de bibliothèque
4. Fichiers spéciaux
5. Formats de fichier
6. Jeux
7. Divers
8. Administration système
9. Interface du noyau Linux

Chaque section possède une page d'introduction qui présente la section, disponible en tapant `man <num_section> intro`.

Les commandes - La documentation 38/57

- La commande `info`
  - alternative à `man`
  - généralement plus à jour
  - interface texte «à la emacs» avec menu
- La commande `apropos`
  - recherche les commandes «à propos de *xxxx*» (recherche dans les mots clefs des pages de man)

Note : les commandes *internes* au shell (p.ex. `cd pwd history` etc.) n'ont pas de page de `man` car ce ne sont pas des programmes, mais juste des mots clefs reconnus et interprétés directement par le shell. Ces commandes sont donc expliquées dans la documentation du shell lui-même. Par exemple, si vous cherchez de la documentation sur la commande `cd` et que vous avez *bash* comme shell, regardez dans le `man bash`. Une autre façon de faire est de taper `help cd` (En effet, `help` est une autre commande interne de *bash* qui affiche de la documentation sur les commandes internes de *bash*.)

Les outils de recherche de fichiers 39/57

- La commande `locate`
  - recherche les occurrences de la chaîne de caractères qui lui est passée en arguments dans une base de données mise à jour via la commande `updatedb`
- La commande `whereis`
  - Recherche le nom de commande passé en argument dans un certain nombre de répertoires standards
- La commande `which`
  - Recherche dans le `PATH` où se trouve la commande indiquée en argument
- La commande `find`
  - Recherche n'importe quoi n'importe où

4 Les processus

4.1 Environnement, cycle de vie

Les processus 41/57

- Le concept de processus
  - Dans une première approche on peut dire qu'un processus est un programme en cours d'exécution, dans un environnement donné, dans la mémoire centrale
- Notion d'environnement
  - Ensemble d'informations complémentaires au programme en exécution qui viennent paramétrer l'exécution
  - Essentiellement trois types d'information d'environnement
    - Les variables d'environnement
    - L'identité de l'utilisateur au nom duquel s'exécute le processus
    - Les fichiers ouverts (notamment ceux d'entrée/sortie standard)

Création d'un processus 42/57

- Un processus est toujours créé par le noyau, à la demande d'un autre processus
- Le processus qui demande la création est appelé le père, le processus créé est appelé le fils
- Le processus fils est créé en mémoire centrale dans une zone mémoire distincte du processus père
- Le processus fils est la copie intégrale du processus père. Mais un détail technique permet au développeur de différencier les instructions exécutées par le père de celles exécutées par le fils

Le fils est un clone du père mais il y a une mutation génétique... Le père demande la création du fils via une fonction de bas niveau (un appel système). Cette fonction rend 0 dans le processus fils et une valeur strictement positive dans le processus père. Cette

valeur dans le père est en fait le numéro de processus du fils. Le programmeur profite de cette différence pour différentier le code exécuté par les deux processus. Sinon les deux exécuteraient strictement la même chose.

Les variables d'environnement 43/57

- Chaînes de caractères, en majuscules par coutume
  - Syntaxe `NOM=valeur`
  - Regroupées dans un espace mémoire appelé «tableau des variables d'environnement»
  - Ce tableau est hérité par les processus fils et résiste à l'exécution d'une commande (voir plus loin)
- Quelques variables standard
  - `PATH`, `HOME`, `USER`, `LOGNAME`, `DISPLAY`, ...

Identité utilisateur associé au processus 44/57

- Deux identités d'utilisateur !
  - L'utilisateur réel : celui qui a lancé le processus, identifié par son numéro d'utilisateur dans `/etc/passwd` (*ruid : real user ID*)
  - L'utilisateur effectif :
    - Dans la majorité des cas il s'agit de l'utilisateur réel
    - Si le fichier exécuté (qui a donné naissance au processus) a le bit *S_UID* positionné (une lettre s apparaît à la place du x des droits du propriétaire du fichier) alors l'utilisateur effectif est le propriétaire du fichier exécuté (*euid : effective user ID*)
    - Attention : trou de sécurité potentiel, surtout si le fichier appartient à root
- Deux identités de groupe
  - Concept identique à ci-dessus : groupe réel, groupe effectif (bit *S_GID*)

Pendant l'exécution d'un fichier ayant le bit *S_UID* positionné on a les droits du propriétaire du fichier, les droits d'un autre utilisateur, sans lui demander... Mais si le fichier exécuté possède ce droit c'est que son propriétaire l'y a mis, car lui seul peut le faire, ou l'administrateur, ou une application malicieuse...

Tout utilisateur peut avoir chez lui de tels fichiers pour des raisons qui lui sont propres et pour que des applications qui lui sont personnelles puissent fonctionner pour tout le monde. L'administrateur peut toutefois demander aux utilisateurs de justifier la présence de tels fichiers, c'est son droit et peut être même son devoir.

De tels fichiers existent et appartiennent à root, l'administrateur. S'ils sont vulnérables à des attaques de type débordement de tampon (buffer overflow) alors la sécurité du système entier est gravement compromise.

Les fichiers standards d'entrée-sortie 45/57

- Trois fichiers standards
  - Le fichier standard d'entrée (descripteur 0, FILE Pointer stdin)
  - Le fichier standard de sortie (descripteur 1, FILE Pointer stdout)
  - Le fichier standard de sortie d'erreur (descripteur 2, FILE Pointer stderr)
- Ouverts par défaut lors du lancement d'un exécutable
- Associés virtuellement au clavier pour l'entrée standard et à l'écran pour les deux autres
- Ils peuvent être redirigés vers des fichiers réels ou des tubes de communication

Contrôle sur les processus 46/57

- Lister les processus
  - La commande `ps`
    - Nombreuses options : `ax`, `axl`, `axf`, `-ef`, etc.
  - La commande `top`
    - Comme `ps axu`, avec réaffichage régulier, plus des informations sur la charge et l'occupation mémoire
- Arrêter un processus
  - Si on a le contrôle (processus en premier plan dans un terminal)
    - Sans le tuer (arrêt momentané) : `<Ctrl-Z>`
    - En le supprimant : `<Ctrl-C>`
  - La commande `kill` (voir pages suivantes)

Sur certains systèmes les paramétrages des terminaux ou des émulateurs de terminaux sont tels que les associations de touches `<Ctrl-Z>` ou `<Ctrl-C>` ne fonctionnent pas. On peut le vérifier avec la commande `stty -a` qui affiche le paramétrage du terminal.

Exemple :

```
[bash]$ stty -a
speed 38400 baud; rows 25; columns 80; line = 0;
intr = ^C; quit = ^\; erase = ^H; kill = ^U; eof = ^D; eol = <undef>;
eol2 = <undef>; start = ^Q; stop = ^S; susp = ^Z; rprnt = ^R; werase = ^W;
lnext = ^V; flush = ^O; min = 1; time = 0;
...
```

Remarquer le paramètre `intr = ^C`, l'accent circonflexe indique la touche `<Ctrl>`. En fait, `intr` est le paramètre permettant de tuer rapidement un processus. Voir aussi `susp`. Et faire `man stty`.

On peut changer le paramétrage `intr` avec : `[bash]$ stty intr ^F`

Contrôle sur les processus : les signaux 47/57

- Un signal est une sorte d'interruption logicielle envoyée à un processus par le noyau après qu'un événement particulier soit intervenu
- L'événement peut être :
  - Une faute logicielle (division par 0, manipulation d'une adresse mémoire interdite, erreur d'alignement de donnée)
  - Terminaison d'un processus fils : par défaut (mais paramétrable) le père est prévenu
  - Intervention de l'utilisateur via le shell ou l'interface graphique pour tuer le processus ou le stopper ou autre (modification de la taille d'une fenêtre par exemple)
- Dans la plupart des cas le signal est fatal au processus

Les principaux signaux 48/57

Signal	Numéro	Fonction
HUP	1	Signal envoyé au processus en premier plan associé à un terminal lorsque celui-ci est fermé
INT	2	Envoyé depuis le clavier avec la combinaison de touches <CTRL-C> (par défaut)
QUIT	3	Envoyé depuis le clavier avec la combinaison de touches <CTRL-|> (par défaut)
KILL	9	Ne peut être intercepté, envoyé depuis le clavier via la commande `kill` (`kill -9` ou `kill -KILL`)
TERM	15	Envoyé via le clavier par la commande `kill` simple
SEGV		Erreur de segmentation, accès à une zone mémoire interdite
CLD		Terminaison d'un fils
WINCH		Modification de la taille de la fenêtre associée à l'application
STOP		Arrêt du processus sans le terminer. Envoyé via la combinaison de touches <CTRL-Z>
URG		Une données urgente a été reçue via le protocole TCP et est en attente de lecture (voir le cours sur la programmation réseau)
IO		Des données réseau sont arrivées et sont en attente de lecture. (voir le cours sur la programmation réseau)
USR1		Nom de signal utilisable par le développeur, à son gré
USR2		Nom de signal utilisable par le développeur, à son gré

Les raccourcis claviers (p.ex. <CTRL-C>) pour envoyer les signaux au processus en cours dans le shell sont paramétrés au niveau du terminal : `stty -a`.

La commande `kill` 49/57

- `kill` *[numéro_ou_nom_de_signal] numéro_processus | numéro_job*
- le numéro ou le nom de signal sera en général omis sauf si le résultat est négatif, auquel cas on pourra essayer le signal `KILL` (-9) qui ne peut pas être intercepté par le processus
- Le numéro de processus sera obtenu par `ps`
- Le numéro de job n'est valable que pour les processus en arrière plan (background) ou les processus stoppés. On peut le connaître avec la commande `jobs`
- Le programmeur d'application peut gérer l'arrivée des signaux (sauf le signal 9) et les ignorer ou les traiter de manière à ce que le processus se termine proprement ou ne se termine pas

Les processus zombies 50/57

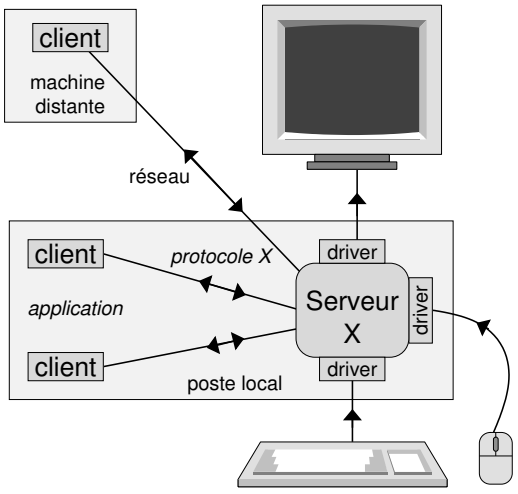
- Lorsqu'un processus fils se termine, son père doit acquitter la terminaison. C'est un problème de programmeur, pas d'utilisateur. Si l'acquittement n'est pas fait, le processus terminé reste dans la liste des processus (état `Z`), il est appelé «zombie»
- Un processus zombie est un processus fils pour lequel son père n'a pas acquitté la terminaison
- Le processus zombie est vidé de sa substance mais reste dans la liste des processus de la machine et peut être listé par `ps`
  - On ne peut plus le supprimer, il faut supprimer le père pour que le zombie disparaisse
  - Il est généralement dû à une erreur de programmation

En Shell (`sh`, `bash`, `ksh`) on peut récupérer le code de retour du exit du fils dans la variable `$?`.

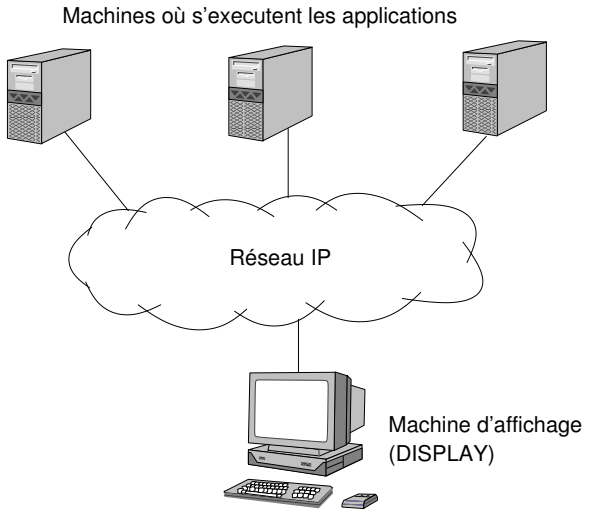
5 L'interface graphique X-Window

5.1 Client-serveur, authentification, bureau

X-Window - Principes 52/57



X-Window - Intrinsèquement Réseau



X-Window - Applications en réseau

- Toute application X peut s'exécuter sur une machine et s'afficher sur une autre
- La machine d'affichage est indiquée dans une option (`-display`) ou une variable d'environnement (`DISPLAY`)
  - Exemples :
  - `$ xterm -display lune:0.0`
  - `$ export DISPLAY=lune:0.0`
  - `$ xterm`
  - format du `display` : *adresseOuNomMachine* :*numServ*.*numEcran*

X-Window - Réseau et sécurité 55/57

- Par défaut il n'est pas possible d'afficher des fenêtres sur un «display» utilisé par un autre utilisateur si celui-ci n'a pas donné l'autorisation
- Les autorisations sont possibles avec la commande `xhost`
  - `xhost +terre`
  - autorise les «connexion graphiques» depuis la machine `terre`
  - authentification par adresse IP
- Autorisations avec la commande `xauth`
  - plus complexe mais plus *sûr*
  - fichier `.Xauthority`
  - autentifie un utilisateur (qui doit posséder le bon *cookie* de 128 bits)

X-Window - Le serveur et les applications 56/57

- Le serveur X sait gérer l'affichage mais il ne sait pas quoi ni comment afficher !
  - ce sont les applications qui l'informent via le protocole X
  - des librairies applicatives pour dessiner boutons, menu, assenceurs, etc. (*graphic toolkits*)
- Le serveur X reçoit tous les événements clavier et souris
  - il informe alors les applications de l'événement si celles-ci ont demandé qu'il leur soit envoyé
  - les applications traitent l'événement et décident de ce qu'il faut faire, elles demandent éventuellement des modifications d'affichage au serveur

X-Window - Une application très particulière

- Le gestionnaire de fenêtre ou *Window Manager*
  - le serveur X **ne sait pas gérer** les fenêtres ! ! ! !
  - une application spécifique est nécessaire pour
    - offrir des menus de fond d'écran
    - permettre de déplacer, iconifier, restaurer, supprimer les fenêtres et aussi modifier leur taille
    - C'est le **Window Manager**
  - Les Window Managers existent en grand nombre, il y en a pour tous les goûts
  - Les applications sont normalement compatibles avec tous les Window Managers (vœu pieux !)