



PLANNING DE DÉROULEMENT DU COURS

ENSEIGNANT

Nom (s) et prénom (s) : **BALLA MEKONGO Joseph Aubin**

Grade ou Qualification : **Ingénieur en Réseaux et Télécommunications**

Téléphone : **(+237) 691491991**

Courriel : **balla.aubin@yahoo.fr**

Objectifs du cours

Ce cours va permettre à l'étudiant(e) de maîtriser les concepts fondamentaux sur l'administration du système d'exploitation Windows.

À la fin de cet enseignement, l'étudiant doit être capable de :

1. Maîtriser les généralités sur les systèmes d'exploitation (Définition et rôle, l'évolution historique et les types de SE) ;
2. Maîtriser le système d'exploitation Windows et ses outils (Historique de Windows, présentation de Windows, logiciels et la sécurité sous Windows) ;
3. Maîtriser les systèmes de gestion des fichiers et le langage des commandes.



CONTENU DE L'ENSEIGNEMENT

CHAPITRE I : Généralités sur les systèmes d'exploitation CHAPITRE II : Présentation de Windows et ses outils

APPROCHE PEDAGOGIQUE

L'approche pédagogique est conçue pour impliquer l'étudiant dans la construction et l'utilisation des savoirs. Ce planning transmis à l'étudiant lui permet de préparer chaque séance de cours. Des travaux à faire lui sont donnés à la fin de chaque séance de cours afin de lui permettre d'assimiler l'unité d'enseignement.

Diverses stratégies sont utilisées dont : l'enseignement magistral interactif, les exercices pratiques, la méthode des cas, l'apprentissage par problèmes, le réseau de concepts etc.

Déroulement des exercices / cas pratiques et Méthode d'évaluation

Hormis les exercices d'application une liste d'exercices est intégrée à l'annexe du cours.

A chaque séance l'étudiant a droit aux exercices / TP à faire en salle, à la maison ou en équipe. Le(s) contrôle(s) continu(s) et l'examen final comptent chacun pour 50% de la note finale Le contrôle continu est constitué de :

- La présence et participation en salle ;
- L'évaluation en salle ;
- Travaux à faire à la maison ; ○ Les travaux d'équipes.



Cours des bases d'administration Windows

Chapitre 1 :	6
Généralités sur les systèmes d'exploitation	6
Introduction	6
I. Définition, Rôle et évolution historique des systèmes d'exploitation	6
1. Définition et rôle des SE	6
2. Evolution historique des systèmes d'exploitation	7
II. Les types des systèmes d'exploitation	8
1. Classification selon le nombre d'utilisateurs et de tâches exécutées	8
2. Classification selon le modèle	8
III. Description des tâches d'un système d'exploitation	9
1. La gestion de processus	9
2. La gestion de la mémoire	12
3. La gestion des fichiers	14
Chapitre 2 :	16
Présentation de Windows et ses outils	16
Introduction	16
I. Historique de Windows : De Windows 1.0 à Windows 11	16
1. Windows 1	16
2. Windows 2	16
3. Windows 3	17
4. Windows 95	17
5. Windows	

98.....	18
6. Windows 2000/ME (MILLENIUM)	
.....	18
PROPOSE PAR DIFFOUO TAZO EVARISTE	
7. Windows XP	
.....	19
8. Windows Vista	
.....	19
9. Windows 7	
.....	20
10. Windows 8/8.1	
.....	20
11. Windows 10	
21	
12. Windows 11	
21	
II. Exploration de Windows et de ses outils	22
1. Le processus de démarrage d'un ordinateur avec Windows comme SE.	
.....	22
2. Le Bureau (Desktop) de Windows	
.....	23
3. Manipulation de la souris	
.....	23
4. Bouton Démarrer et barre des tâches	
.....	24
5. Les fenêtres d'exploration de fichiers et les menus contextuels	
.....	24
III. La gestion des fichiers et des répertoires	25
1. Quelques définitions	
.....	25
2. Caractéristiques des fichiers et accès	
.....	25
3. Importance de la sauvegarde /compression :	
.....	27
IV. La gestion des programmes	28

1. Visualisation et désinstallation d'un programme installé sur la machine	28
2. Visualisation des processus (programmes en cours d'exécution).....	28
3. Arrêt d'un programme en cours d'exécution (Pas très recommandé).....	28
V. La Sécurité informatique sous Windows et entretien de l'ordinateur	31
A. La Sécurité informatique	31
B. L'entretien de l'ordinateur	34



Chapitre 1 : Généralités sur les systèmes d'exploitation

Introduction

Avant l'avènement des systèmes d'exploitation, la conception d'un programme nécessitait la connaissance parfaite du mode de fonctionnement de la machine. Le programmeur devait gérer au moindre détail le placement des programmes en mémoire en utilisant directement les adresses, l'exécution au niveau du processeur à savoir le chargement et la terminaison des programmes, l'affichage sur l'écran des résultats, etc. Cette tâche étant très complexe, et heureusement depuis plusieurs décennies on a dissocié la programmation de la machine et les systèmes d'exploitation ont vu le jour.

Un système d'exploitation (SE) est le centre de toute activité de traitement d'information sur un ordinateur. C'est un programme qui fait fonctionner les autres programmes ainsi que la partie matérielle de l'ordinateur. Il agit comme un intermédiaire entre l'utilisateur, les logiciels d'application et la partie matérielle de la machine.

Ce chapitre introduit les principes fondamentaux des systèmes d'exploitation, de sa structure et de son fonctionnement. Il traite l'ensemble des techniques matérielles et logicielles utilisées pour construire un SE.

I. Définition, Rôle et évolution historique des systèmes d'exploitation

1. Définition et rôle des SE

Le système d'exploitation (SE) est un ensemble de programmes qui réalise l'interface entre le matériel de l'ordinateur et les utilisateurs. Il prend en charge la gestion des ressources de la machine (**ressources physiques** : mémoire, unités E/S, UCT... et les **ressource logiques = virtuelles** : fichiers et bases de données partagés, canaux de communication logiques, virtuels...) et le partage de celles-ci. Les ressources logiques étant bâties par le logiciel sur les ressources physiques.

Le but principal d'un SE est de :

- Fournir un environnement où l'utilisateur puisse exécuter des programmes,
- Rendre le système informatique pratique pour l'utilisateur,
- Utiliser le matériel de façon efficace.

Chaque système d'exploitation possède une architecture selon le type de services qu'il devra fournir à l'avenir. À partir de ce qui précède, Le système d'exploitation joue plusieurs rôles :

- **Systèmes d'exploitation comme machine virtuelle (abstraite)** en présentant au programmeur une interface d'accès aux ressources de l'ordinateur (sous forme d'appels système). Ainsi le programmeur peut faire abstraction des détails de fonctionnement des ressources.
- **Systèmes d'exploitation comme gestionnaire (administrateur) de ressources** en gérant l'utilisation des ressources par différents utilisateurs et les éventuels conflits. Le système

d'exploitation d'un autre point de vue doit gérer un ensemble complexe d'élément (processeur, mémoire, timers, bus, interfaces réseaux) et cette gestion doit se faire de façon optimale.

2. Evolution historique des systèmes d'exploitation

La théorie des SE a été développée surtout dans les années 1960 . A cette époque, il y avait des machines très peu puissantes avec lesquelles on cherchait à faire des applications comparables à celles d'aujourd'hui (mémoire typique : 100 -500K). Ces machines devaient parfois desservir des dizaines d'usagers !

Les premiers ordinateurs ne possédaient pas vraiment de système d'exploitation. L'informatique moderne naît dans les années 1960. On peut résumer rapidement ses avancées autour de l'invention des notions suivantes :

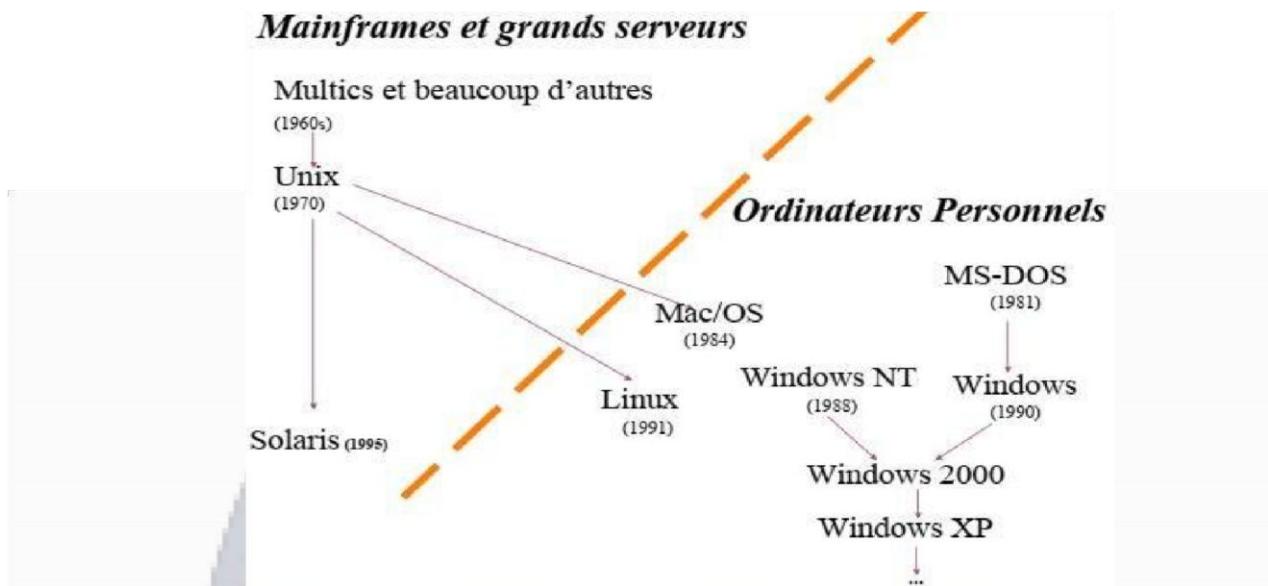
- Apparition des processeurs d'entrées-sorties ;
- Multiprogrammation, c'est à dire possibilité d'exécuter plusieurs programmes simultanément ;
- Compilateurs ;
- Temps partagé ;
- Mémoire paginée virtuelle. Elle permet de faire fonctionner un ensemble de programmes dont la taille est supérieure à celle de la mémoire physique ;
- Les communications.

L'évolution des systèmes d'exploitation au cours des dernières décennies le SE est passée par plusieurs étapes.

- Le début : routines d'E/S avec amorçage système ;
- Systèmes par lots simples ;
- Systèmes par lots multiprogrammés ;
- Systèmes à partage de temps ;
- Ordinateurs personnels ;
- SE en réseau ;
- SE répartis ;

Il faut noter que les fonctionnalités des systèmes simples se retrouvent dans les systèmes complexes. Les problèmes et solutions qui sont utilisés dans les systèmes simples se retrouvent souvent dans

les systèmes complexes. Ci-dessous une synthèse historique des SE.



II. Les types des systèmes d'exploitation

Les systèmes d'exploitation peuvent être classifiés Selon le nombre d'utilisateurs et de tâches exécutées et selon le modèle.

1. Classification selon le nombre d'utilisateurs et de tâches exécutées

On trouve ici : les SE Mono utilisateur et monotâche ; les SE mono utilisateur et multitâches et enfin les SE Multi utilisateurs et multitâches

2. Classification selon le modèle

Ici, le système d'exploitation se présente sous la forme d'un ensemble de primitives, chacun mettant en œuvre une partie du système. Lorsqu'un utilisateur donne un ordre au système d'exploitation, ce dernier doit appeler plusieurs primitives, chacune exécutant la partie qui lui incombe. On distingue trois principales manières d'organiser les primitives du système à travers les différents types de systèmes d'exploitation. Les différents modèles de systèmes d'exploitation sont : Les systèmes monolithiques ; Les systèmes à couches et Le modèle client -serveur. Ces types de systèmes sont : Les systèmes réseaux et les systèmes temps réel qui comprennent les Systèmes embarqués (Système temps réel dédié pour une application particulière) et les Systèmes distribués ou répartis (c'est un SE qui fonctionne entre ordinateurs et qui pousse l'usager à voir des ressources éloignées comme si elles étaient locales).

III. Description des tâches d'un système d'exploitation

L'existence d'une multitude de systèmes d'exploitation peut laisser penser qu'ils sont tous différents. Sachant que les systèmes sont conçus pour une gamme d'ordinateurs, il est plus judicieux de dire que les systèmes d'exploitation sont différents d'une gamme d'ordinateurs à l'autre. Ils se distinguent par l'interface qu'ils proposent et les algorithmes et stratégies qu'ils appliquent. Le principal objectif

d'un système est de gérer les composants de l'ordinateur. On retrouve par conséquent quatre tâches qui correspondent à :

a- La gestion de processus

- Création et suppression
- Ordonnancement (allocation du processeur à un processus)
- Synchronisation (accès aux données/ressources partagées)
- Communication (échange d'informations entre processus)
- Prévention, détection et résolution des interblocages

b- La gestion de la mémoire (Centrale et secondaire)

- Maintien d'une carte des zones occupées par processus
- Allocation/libération mémoire
- Stratégie d'allocation (pagination, segmentation, ...)

c- La gestion des fichiers / réseaux

Fichiers:

- Vision uniforme et organisée des données (arborescence)
- Masquage des détails de l'organisation physique

Réseau:

- Connexion à distance
- Partage de fichiers / périphériques
- Envoi / réception de messages

d- La gestion des Entrées/Sorties

L'OS comprend

- une interface standard pour les pilotes de périphériques (haut niveau);
- des pilotes liés à un matériel donné (bas niveau);
- des programmes de gestion des interruptions;
- des procédures de gestion des erreurs.

1. La gestion de processus

La principale tâche du système d'exploitation concerne l'allocation du processeur aux processus. Il s'agit de décider quel processus s'exécute à un moment donné, à quel moment interrompre le processus, quel sera le suivant, et de quoi il a besoin comme ressources pour son exécution. Le système d'exploitation doit gérer deux types de processus : les siens et ceux des utilisateurs.

Le système d'exploitation gère également les conflits dus à la concurrence et leurs solutions, en effet les processus peuvent utiliser des variables en commun. Le système doit par ailleurs offrir des primitives pour assurer la communication entre les processus ainsi que leur synchronisation. Pour finir le système d'exploitation doit parer aux erreurs et effectuer la correction des situations d'interblocage

entre processus en fournissant les mécanismes adéquats.

Mots-clés

Processus : Un processus est un programme en cours d'exécution auquel est associé un environnement processeur (Compteur Ordinal, Registre d'Etat, RSP , registres généraux) et un environnement mémoire appelés contexte du processus

Ressource : Une désigne toute entité dont a besoin un processus pour s'exécuter

Multiprogrammation : En Système d'Exploitation (SE), la multiprogrammation est la capacité d'un système d'exécuter à la suite plusieurs activités sans l'intervention de l'utilisateur. C'est une des premières capacités fournies par les SE dès la fin des années 1950.

Thread : Les threads sont des entités planifiées pour leur exécution par le processeur. Les threads autorisent les exécutions multiples dans le même environnement de processus avec une marge d'indépendance les uns par rapport aux autres.

Programme : C'est une suite ordonnée d'instructions élémentaires en vue d'accomplir une tâche donnée.

Concurrence : Les faits que deux ou plusieurs processus concourent à l'accès à une même ressource.

Ordonnancement : L'Ordonnancement est le fait d'agencer les processus par ordre de priorité.

Interblocage : C'est un état qui se produit lorsque deux processus concurrentes s'attendent mutuellement (l'un détenant la ressource que l'autre a besoin).

1.1. Processus et états

Tous les ordinateurs modernes sont capables de faire plusieurs tâches simultanément (exécuter un programme utilisateur par exemple et afficher du texte ainsi qu'effectuer des lectures sur disque, etc.). Dans un système multiprogrammé, le processeur bascule entre programme pour les servir en raison de petit laps de temps ; ce qui fait que le processeur puisse intervenir pour plusieurs programmes à raison d'une seconde simulant ainsi le parallélisme.

Le processeur physique commute entre les processus sous la direction d'un **ordonnanceur**. Dans le

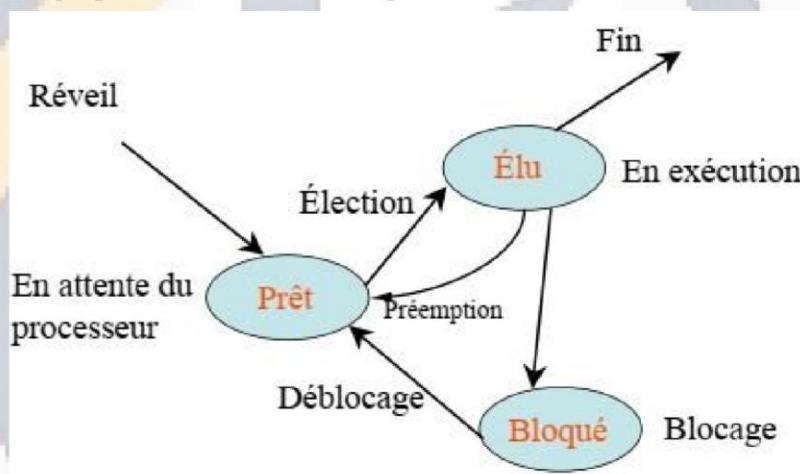


cas de systèmes à temps partagé, tous les processus progressent dans le temps, mais un seul s'exécute à la fois. Un processeur peut être partagé par plusieurs processus à l'aide d'un algorithme d'ordonnancement intervenant pour déterminer à quel moment arrêter de travailler sur un processus pour en servir un autre.

Un processus peut-être dans trois états différents : *élu*, *prêt*, *bloqué*. Lorsque le processus obtient le processeur et s'exécute, il est dans l'état élu. L'état élu est l'état d'exécution du processus ;

- Lors de l'exécution, le processus peut demander à accéder à une ressource. Il quitte alors le processeur et passe dans l'état bloqué. L'état bloqué est l'état d'attente d'une ressource autre que le processeur ;
- L'état prêt est l'état d'attente du processeur. Un processus est dit prêt s'il est suspendu en faveur d'un autre. Pour un processus prêt, il ne lui manque que la source processeur pour s'exécuter.

Ci-dessous la figure qui présente les états d'un processus.



1.2. Quelques politiques d'ordonnancement des processus

La politique d'ordonnancement détermine quel sera le prochain processus élu. Selon si la préemption est autorisée ou non, la politique d'ordonnancement sera de type préemptive ou non. Objectifs d'ordonnancement diffèrent selon les types de systèmes. Il existe plusieurs politiques. On peut avoir :

- **Premier Arrivé, Premier Servi :** Les processus sont élus selon l'ordre dans lequel ils arrivent dans la file d'attente des processus prêts. Il n'y a pas de réquisition. Comme avantages, on a la simplicité et l'inconvénient est que les processus de petit temps d'exécution sont pénalisés en termes de temps de réponse par les processus de grand temps d'exécution qui se trouvent avant eux dans la file d'attente.
- **Plus Court d'Abord :** L'ordre d'exécution des processus est fonction de leur temps d'exécution sans réquisition. Cette méthode remédie à l'inconvénient pour PAPS mais la difficulté réside dans la connaissance a priori des temps d'exécution des processus.
- **Politique par priorité :** Chaque processus possède une priorité. À un instant donné, le processus élu est le processus prêt de plus forte priorité. Deux versions selon si la réquisition est

autorisée ou non. La réquisition est admise et le processus couramment élu est préempté dès qu'un processus plus prioritaire devient prêt.

○ **Politique du tourniquet (round robin)** : C'est le Système en temps partagé. Ici, le temps est découpé en tranches, quantum de temps (10 – 100 ms). Lorsqu'un processus est élu, il s'exécute au plus durant un quantum de temps. Si le processus n'a pas terminé son exécution à l'issue du quantum de temps, il est préempté et il réintègre la file des processus prêts mais en fin de file. La valeur du quantum est un facteur important de performance (commutations de contexte).

2. La gestion de la mémoire

La mémoire est une ressource importante qui doit être gérée avec attention. Le Système d'Exploitation doit cohabiter dans la mémoire principale avec un ou plusieurs processus. La gestion de la mémoire prend en charge l'allocation de la mémoire aux processus. Elle doit également protéger la mémoire allouée au Système d'Exploitation contre des accès non autorisé. Pour ce faire le gestionnaire de la mémoire doit remplir plusieurs tâches :

- Connaître l'état de la mémoire (les parties libres et occupées de la mémoire). – Allouer de la mémoire à un processus avant son exécution.
- Récupérer l'espace alloué à un processus lorsque celui-ci se termine.
- Traiter le va-et-vient (swapping) entre le disque et la mémoire principale lorsque cette dernière ne peut pas contenir tous les processus.
- Posséder un mécanisme de calcul de l'adresse physique (absolue) car, en général, les adresses générées par les compilateurs et les éditeurs de liens sont des adresses relatives ou virtuelles.

En général, pour ne pas ralentir l'accès à la mémoire le calcul des adresses est réalisé par le matériel. Comme nous allons le voir, les techniques de gestion de la mémoire sont très conditionnées par les caractéristiques du système (monoprogrammé ou multiprogrammé) et du matériel (registres de base et limite). Nous passerons en revue un certain nombre de méthodes de gestion de la mémoire

Il existe différents types de mémoires, et différentes techniques de gestion de la mémoire.

Mots-clés

Mémoire virtuelle: C'est la mémoire que l'on crée sur le disque dur. Cette notion repose sur la traduction des adresses virtuelles en adresse physique de mémoires vives

Mémoire vive : C'est une partie de la mémoire où on trouve les programmes en cours d'exécution.

Mémoire morte: C'est une mémoire non volatile (c'est-à-dire le contenu de ce type de mémoire ne s'efface pas à la coupure de l'alimentation) dont le contenu était fixé lors de sa programmation. Au début ces mémoires étaient en lecture seule mais avec l'évolution de la technologie, des utilisateurs expérimentés peuvent les modifier.

Pagination : La pagination est une technique d'allocation de la mémoire qui fournit au processus des espaces d'adresses séquentielles à partir d'espaces mémoire discontinues.

Partition: C'est le fait de subdiviser la mémoire en partie de tailles fixes ou variables afin de mieux l'utiliser

Monoprogrammation : Se dit pour les systèmes d'exploitation n'exécutant qu'un seul programme à la fois (un seul processus possible dans la mémoire physique).

Multiprogrammation : Se dit lorsque le nombre de processus présents dans la mémoire d'un ordinateur à un instant donné dépasse 1.

La tâche principale de la gestion de la mémoire est de charger des programmes en mémoire pour qu'ils soient exécuté par le CPU

2.1.Gestion de la mémoire avec le principe de la pagination

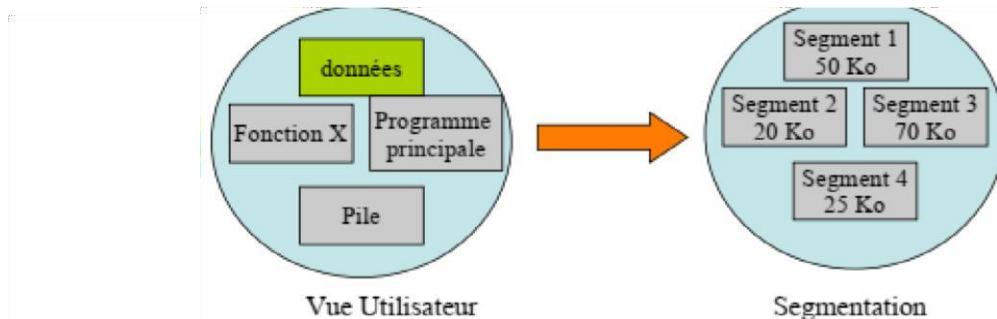
L'espace d'adressage du programme est découpé en morceaux linéaires de même taille appelés pages. L'espace de la mémoire physique est lui-même découpé en morceaux linéaires de même taille appelés case. La taille page = case – définie par le matériel (selon le SE elle varie entre 512 octets et 8192 octets). La pagination consiste donc à charger un programme en mémoire centrale (placer les pages dans les cases disponibles). Pour connaître à tout moment quelles sont les cases libres en mémoire centrale, le système maintient une table des cases.

La pagination constitue un découpage de l'espace d'adressage du processus qui ne correspond pas à l'image que le programmeur a de son programme : Données ; Programme principal ; Procédures séparées et la Pile d'exécution.

2.Gestion de la mémoire avec le principe de la segmentation

La segmentation est un découpage de l'espace d'adressage qui cherche à conserver la vue du programmeur. Lors de la compilation, le compilateur associe un segment à chaque morceau du programme compilé. Un segment est un ensemble d'emplacement mémoire consécutifs non sécable.

Les segments d'un même espace d'adressage peuvent être de taille différente.



2.3. Gestion de la mémoire avec le principe de la mémoire virtuelle

Le principe de la mémoire virtuelle est couramment implémenté avec la pagination à la demande. La taille du programme, des données et de la pile peut dépasser la mémoire disponible. Le SE garde en mémoire les parties du programme qui sont utilisées et stocke le reste dans le disque. Les pages des processus ne sont chargées en mémoire centrale que lorsque le processeur demande à y accéder.

À un instant donné, seules les parties de code et données utiles à l'exécution sont chargées en mémoire centrale. Ici, la répartition de la mémoire centrale est faite entre les processus et l'allocation peut être équitable ou fixe (Même nombre de cases quelle que soit la taille de l'espace d'adressage) ou proportionnelle (Proportionnellement à la taille des processus).

2. La gestion des fichiers

Le Système d'Exploitation gère l'allocation des mémoires de masse ainsi que l'accès aux données stockées (système de gestion de fichiers et notion de fichier). Il assure la conservation des données sur un support de masse non volatile.

Le SE offre à l'utilisateur une unité de stockage indépendante des propriétés physiques des supports de conservation : le fichier qui peut être logique (vue de l'utilisateur) ou physique et il assure la correspondance entre le fichier logique et le fichier physique (Structure de répertoire).

3.1. Le fichier logique

C'est un type de données standard défini dans les langages de programmation sur lequel un certain nombre d'opérations peuvent être réalisées : Création, ouverture, fermeture, destruction. Les opérations de création ou d'ouverture effectuent la liaison du fichier logique avec le fichier physique. Un ensemble

d'enregistrements, un type de données regroupant des données de type divers liées entre elles par une certaine sémantique inhérente au programme qui les manipule.

3.2. Le fichier physique

Il correspond à l'entité allouée sur le support permanent et contient physiquement les enregistrements définis dans le fichier logique. Le fichier physique est constitué d'un ensemble de blocs physiques qui doivent être alloués au fichier logique.

Différentes méthodes d'allocation de la mémoire secondaire : Allocation contiguë ; Allocation par zones et l'Allocation par blocs chaînés.

3.3. Le répertoire

La correspondance entre le fichier logique et le fichier physique est effectuée par le biais d'une table

appelée répertoire qui contient des informations de gestion des fichiers : Le nom logique du fichier ; Le type du fichier (Codé dans son nom logique à l'aide d'une extension) ; L'adresse physique du fichier (qui dépend de la méthode d'allocation mise en œuvre sur le disque) ; La taille en octets ou en blocs du fichier ; Le nom du propriétaire et Les protections appliquées au fichier. Le système de gestion de fichiers offre des primitives permettant de manipuler les répertoires.



Chapitre 2 : Présentation de Windows et ses outils

Introduction

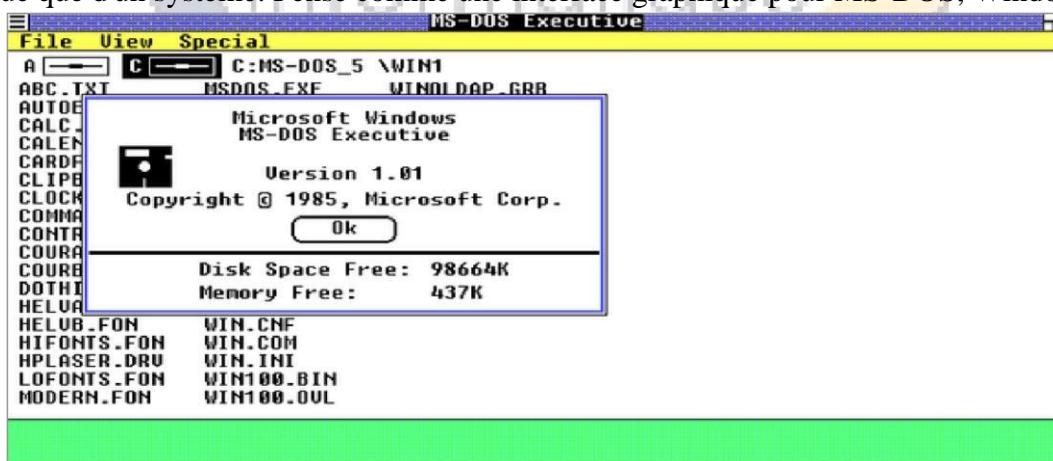
L'un des Systèmes d'exploitation le plus connu actuellement est le Système d'exploitation Microsoft Windows. La version actuelle est Windows 11. Windows est une interface graphique, c'est-à-dire basée sur une représentation graphique des objets manipulés (fenêtres, icônes, boutons, ascenseurs, etc.). Il est marqué par un certain nombre d'innovations. L'interface évoque un bureau facilement configurable.

I. Historique de Windows : De Windows 1.0 à Windows 11

Il y a plus d'une trentaine d'années, le 20 novembre 1985, naissait Windows 1.0 alors que les ordinateurs étaient loin d'être populaires. Aujourd'hui Windows 11, une mise à jour majeure du dernier système d'exploitation développé par Microsoft, sera bientôt installé sur des millions d'appareils. La version précédente, Windows 10 l'est quant à elle sur plus d'un milliard de machines. Nous allons ici présenter l'historique du système le plus utilisé dans le monde sur les ordinateurs personnels.

1. Windows 1

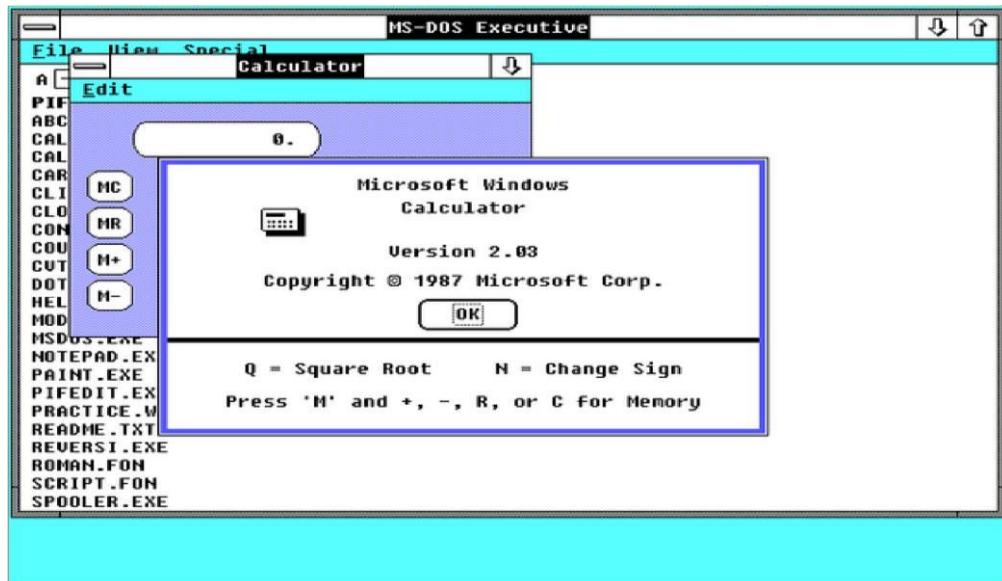
Le 20 novembre 1985, Microsoft présentait Windows 1.01. Il s'agissait plus d'une interface graphique que d'un système. Pensé comme une interface graphique pour MS-DOS, Windows 1.0



apporte une vraie touche visuelle et le support de la souris. Ci-après son interface.

2. Windows 2 Sortie en 1987, cette version corrige toutes les erreurs de la précédente mais ne cherche pas à réinventer la roue. Plus fluide, dynamique et plus simple à utiliser, c'est bien

avec cette itération que La firme est alors sommet de sa gloire lorsqu'elle lance Windows 95. L'OS est moderne, graphiquement impressionnant et inclut des nouveautés comme le 32-bits, Windows a réellement décollé. Ci-après son interface.



3. Windows 3

Cette version débarque en 1990 et signe le début du règne de Windows sur le monde informatique. C'est simple, nous avons là un véritable carton. Tout a été repensé et l'interface se veut plus moderne, plus simple. Les versions se succèdent, comme la 3.1 en 1993 qui a connu le plus de succès. Windows 3.x a notamment inclus le gestionnaire de programmes mais aussi Internet Explorer, logiciel qui servait à naviguer sur cette chose alors très mystérieuse qu'était Internet. Ci-après son interface.



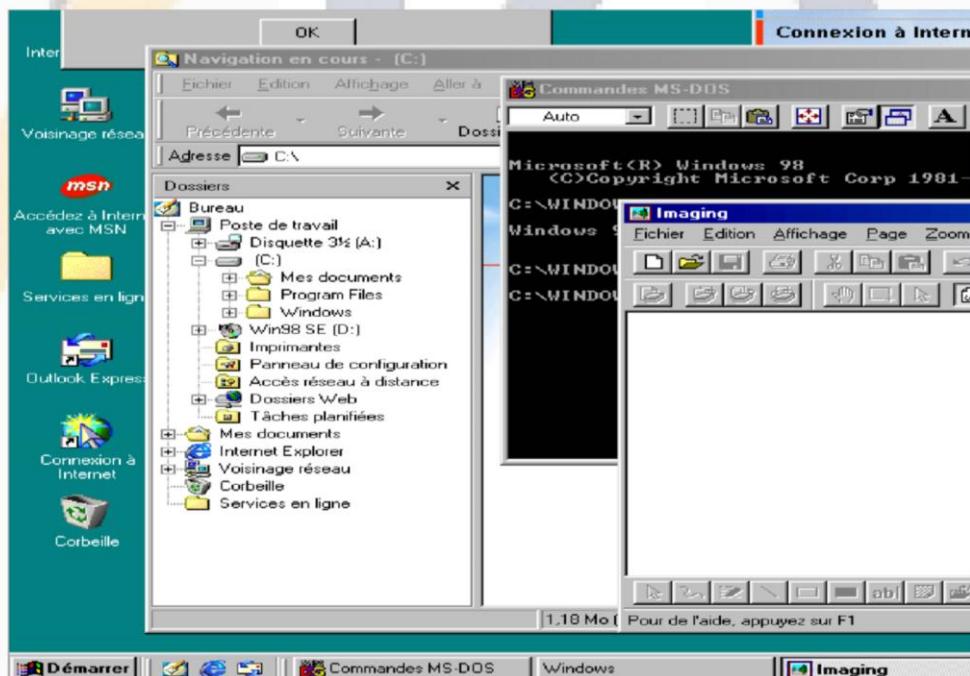
4. Windows 95

la barre des tâches, toujours présente aujourd'hui, ou encore le bouton Démarrer. Le succès est colossal et Microsoft s'installe confortablement dans son fauteuil de leader du monde informatique. Ci-après son interface.



5. Windows 98

Windows 95 étant un véritable carton, la version suivante se contente d'améliorer la formule par petites touches. Ici, l'accent est mis sur Internet, avec l'arrivée d'Outlook notamment. Ci-après son interface.



6. Windows 2000/ME (MILLENIUM)

Cette version sortie en 2000 reste dans la lignée de Windows 95 et 98. Le design commence à se faire un peu vieillot, mais ce qui agace le plus les utilisateurs, ce sont les bugs à répétition. Ci-après

son interface.



7. Windows XP

Sorti en 2001 le système est encore utilisé de nos jours par quelques irréductibles, même si considéré comme obsolète. En 2018, il était encore installé sur de nombreux ordinateurs malgré l'absence de support et donc de correctifs de sécurité. Son design est moderne et plaît au public . Ci-après son interface.



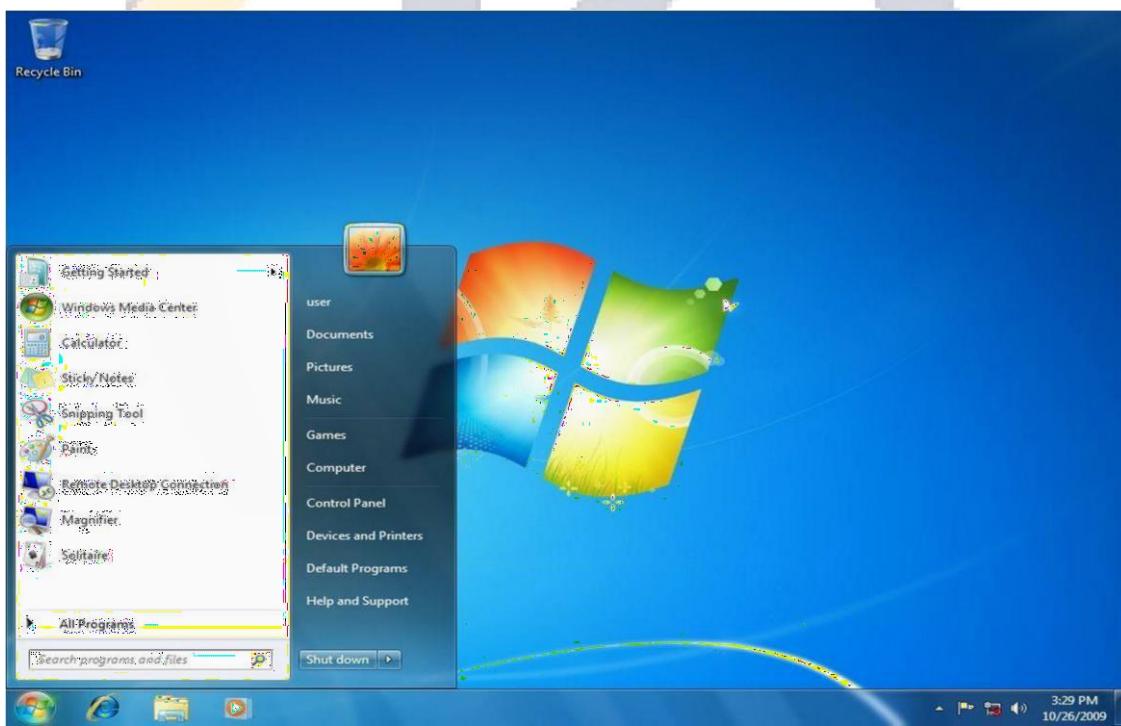
8. Windows Vista

Après le succès de XP, Microsoft lance Vista en 2007. L'intention était bonne : reprendre le succès d'XP en l'améliorant sur tous les points, notamment au niveau du design. Mais malheureusement Vista a eu beaucoup de bugs. Ci-après son interface.



9. Windows 7

Pour cette version qui sort en 2009, Microsoft remet tout à plat au niveau de la technique. Très appréciée, notamment par les joueurs, cette itération a été populaire pendant très longtemps . Ci après son interface.



10. Windows 8/8.1

Pour Windows 8, Microsoft ne peut plus ignorer l'essor des tablettes et autres appareils portables et dévoile un système utilisable sur les écrans tactiles. Le bouton et menu démarrer en font les frais. Un an plus tard, Windows 8.1 remet en place le bouton démarrer et ajoute la possibilité de démarrer sur le bureau pour éviter l'interface tactile.



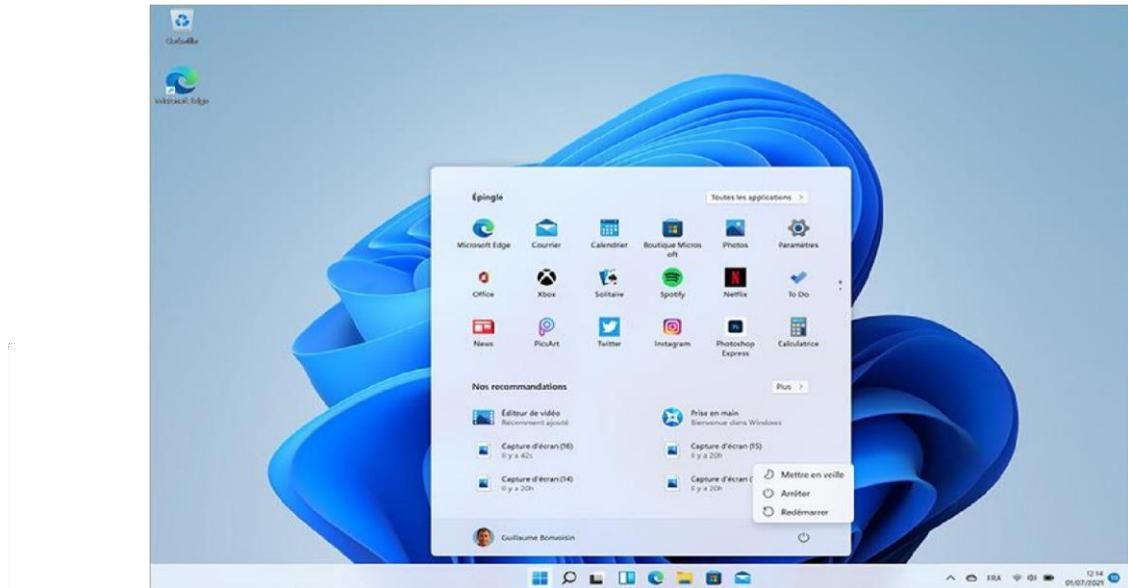
11. Windows 10

Windows 10 est apparu en 2015 et a tenté de garder ce qui était apprécié dans Windows 7 et de conserver ce qui a plu dans Windows 8, c'est-à-dire la possibilité d'utiliser le système au tactile. Le menu démarrer est de retour, avec les tuiles, et l'utilisateur garde la possibilité de passer en mode tablette (automatiquement ou manuellement) lorsqu'il souhaite utiliser l'ordinateur avec un écran tactile et sans clavier ni souris.



12. Windows 11

Avec Windows 11, annoncé et sorti en 2021, Microsoft chamboule complètement l'interface. Même si on retrouve la plupart des fonctionnalités, l'apparence change dès l'arrivée sur le bureau avec un menu démarrer centré par défaut (mais qu'il est possible de replacer à gauche).



II. Exploration de Windows et de ses outils

Windows est un système de fenêtres dimensionnables, déplaçables et superposables les unes sur les autres. Ces fenêtres contiennent des applications, des fichiers, ... Une seule fenêtre est active à la fois. C'est usuellement celle qui a sa barre de titre (son nom dans la partie supérieure) de couleur plus vive que les autres. Chacune des fenêtres peut être **fermée, réduite** en un bouton de la barre de tâches, ou représentée par une icône de raccourci sur le bureau. L'icône de raccourci est un simple dessin symbolisant l'application, le fichier,

Toute application, qu'elle soit ouverte ou réduite, est rappelée par un bouton sur la barre de tâches. Il est possible d'ouvrir plusieurs fenêtres en même temps (tant que le permet la mémoire vive de la machine), mais pas de travailler sur ces différentes fenêtres simultanément. L'intérêt d'ouvrir deux fenêtres est par exemple de voir le contenu de deux disques différents pour comparer ou assurer le transfert de données de l'un à l'autre.

Chaque fenêtre comporte un bouton Fermer dans son coin supérieur droit, sur lequel vous pouvez cliquer pour fermer la fenêtre et arrêter le programme. Pour réduire la fenêtre, on utilise le bouton Réduire. Le bouton Agrandir/Restaurer représente successivement une fenêtre couvrant l'écran et deux fenêtres se superposant. Le bouton Aide, parfois présent, permet d'obtenir de l'aide sur le contenu de la fenêtre, ou sur une zone particulière de celle-ci.

1. Le processus de démarrage d'un ordinateur avec Windows comme SE.

Lorsque l'on démarre son ordinateur, le processus commence par **le chargement du BIOS** (Basic Input-Output System) : Chargement automatique du compteur ordinal avec l'adresse de la

première instruction du BIOS et la gestion des périphériques vitaux (Pilotes du clavier, de l'écran en mode texte, des ports « série » et « parallèle » ; vérification de la mémoire et tous les composants vitaux).

L'étape suivante du processus est ***l'Amorçage*** : Ici, le BIOS recherche un secteur d'amorçage sur une disquette, un disque dur ou un CD-ROM (selon ses paramètres) ; Charge en mémoire la routine de lancement qu'il contient ; Charge le noyau du système d'exploitation à son emplacement définitif. L'étape finale du processus de démarrage est ***l'Exécution la procédure d'initialisation du système***

d'exploitation. : Recherche et exécution du fichier CONFIG.SYS pour l'installation de drivers particuliers ; Chargement de l'interprète du langage de commande COMMAND.COM ; Recherche et interprétation du fichier AUTOEXEC.BAT ; Interprétation des fichiers System.ini et Win.ini et Démarrage du bureau de WINDOWS.

2. Le Bureau (Desktop) de Windows

Lorsque Windows est lancé, la zone qui apparaît est appelée le bureau. Le bureau peut être personnalisé en y ajoutant des icônes de raccourcis vers les logiciels, les documents, les dossiers et fichiers, et en modifiant son aspect général via la couleur, le papier -peint, ... Placer des raccourcis sur le bureau constitue un moyen rapide d'accéder à des éléments souvent utilisés. Un Raccourci est une «Adresse» permettant d'accéder directement à un programme. Cette adresse représente un «raccourci» dans la mesure où elle permet d'éviter le passage par une cascade de menus et de sous menus dans le Menu Démarrer. On crée le raccourci d'un fichier grâce au clic droit, et en choisissant la commande Créer un raccourci. On peut ensuite le déplacer sur le bureau.



3. Manipulation de la souris

Le déplacement de la *souris* sur son *tapis* permet le déplacement à l'écran d'un *pointeur* de forme variable. On distingue les opérations suivantes :

Clic : appuyer une fois sur le *bouton gauche* de la *souris*. Cela permet de *sélectionner un fichier*, ouvrir un *menu*, choisir une *commande*, placer le *pointeur* dans le texte, ...

Double-clic : appuyer deux fois rapidement sur le *bouton gauche*. Cela permet d'*ouvrir un fichier*, lancer un *logiciel* par son *icône*, ...

Clic droit : appuyer une fois sur le *bouton droit* de la *souris*. Cela permet d'appeler le *menu contextuel*. Ce menu contient des *commandes* courantes que l'on applique à l'élément désigné. Par exemple, en *cliquant* sur un *fichier* avec le *bouton droit* de la *souris*, on peut choisir de *l'ouvrir*, de *le copier*, de le *supprimer*, de l'envoyer sur la disquette, ...

Cliquer-glisser : appuyer sur le *bouton gauche* de la *souris* et ne le lâcher qu'après avoir déplacé la

souris à l'endroit voulu. Cela permet de sélectionner des fichiers, sélectionner du texte, déplacer un objet, dessiner des formes, ...

4. Bouton Démarrer et barre des tâches

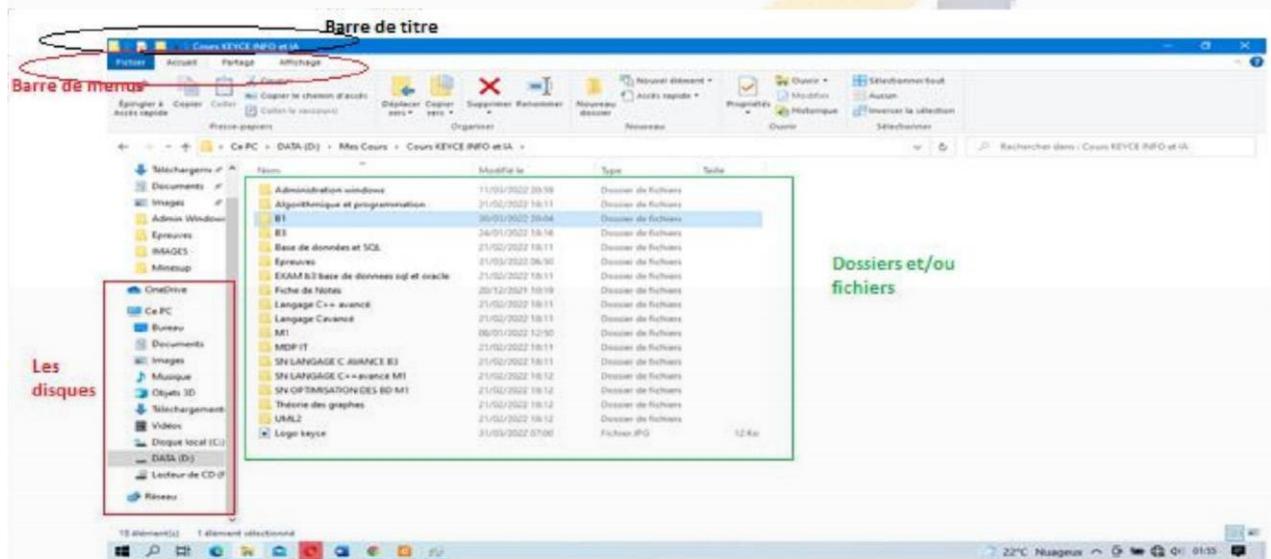
Au bas de l'écran se trouve la barre des tâches. Elle présente le bouton Démarrer ainsi que Les icônes de toutes les fenêtres



5. Les fenêtres d'exploration de fichiers et les menus contextuels

Une Fenêtre est un cadre dans le Bureau qui affiche le contenu d'un programme, d'un répertoire ou d'un fichier (créé par un traitement de texte par exemple). L'Explorateur de Windows nous propose de nous occuper de l'entreposage logique des données : Comment nommer tel fichier ? Dans quel dossier le ranger ? Dans quel dossier ranger ce dossier ? ...

On peut lancer l'Explorateur Windows à partir soit du bouton Démarrer ; soit du poste de travail ; soit de l'icône dossier placée sur la barre de tâche. Ses constituants sont les unités de stockages ; les dossiers et /ou les fichiers. La structure présentant les fichiers et dossiers dans l'Explorateur est appelée arborescence. Les objets de base de l'explorateur étant : la barre de titre, la barre de menu, et la barre d'outils.



Si on clique avec le bouton droit sur un fichier ou un dossier dans l'Explorateur, le menu qui apparaît affiche les commandes les plus fréquemment utilisées pour ce fichier ou ce dossier. On peut aussi cliquer avec le bouton droit sur un espace vide de la barre des tâches ou du bureau. Le menu sera différent car le contexte aura changé.

Le menu contextuel d'un fichier permet d'accélérer la première méthode de copie et de déplacement décrite ci-dessus. Les commandes Couper, Copier et Coller y sont accessibles beaucoup plus rapidement. Le menu contextuel permet aussi d'ouvrir rapidement le fichier sélectionné à l'aide du logiciel associé à l'extension du fichier. On peut aussi l'imprimer, éventuellement l'ajouter à une archive. La commande "Envoyer vers" permet d'en faire une sauvegarde sur disquette, d'en faire un raccourci sur le bureau, de le joindre comme "attache" à un message électronique, ...

Le menu contextuel permet aussi de changer l'affichage de vos dossiers. Son accessibilité par clic droit seulement sur le bureau Permet soit de : Définir la résolution de l'écran ; Personnaliser son fond d'écran et couleurs du thème ; Changer le type d'affichage des icônes (larges, petites, etc.) se trouvant sur le bureau ; Afficher les icônes selon un ordre choisi.

III. La gestion des fichiers et des répertoires

1. Quelques définitions

Le SE gère l'allocation des mémoires de masse ainsi que l'accès aux données stockées (système de gestion de fichiers et notion de fichier) et il assure la conservation des données sur un support de masse non volatile.

- Un **Fichier** est une unité logique de stockage d'information.
- Un **Système de gestion des fichiers (SGF)** est un ensemble des fonctionnalités mises en œuvre pour la gestion des fichiers dans un SE.
- Un **Répertoire** est une entité créée pour l'organisation des fichiers.

2. Caractéristiques des fichiers et accès

Un SGF doit être en mesure de créer, de supprimer, de renommer et de déplacer des fichiers et des répertoires. Il doit aussi gérer l'accès aux fichiers (protégé en écriture, etc.). Enfin, il doit s'occuper de l'organisation et de l'emplacement des fichiers. Les caractéristiques des fichiers sont :

- **Nommage des fichiers** : utilisation d'extensions (txt, jpg, mp3, exe, etc.).
- **Chemin d'accès** : Exemple : C:\Program Files\Microsoft Office 15\fichier.txt
- **Types de fichiers** : régulier, répertoire
- **Opérations sur les fichiers** : lecture, modification, etc.

Pour accéder à un fichier il faut fournir au système de fichiers les informations nécessaires pour le localiser sur le disque, c'est-à-dire lui fournir un chemin d'accès. Les systèmes modernes permettent aux utilisateurs d'accéder directement à une donnée d'un fichier, sans le parcourir de-

puis le début du chemin.

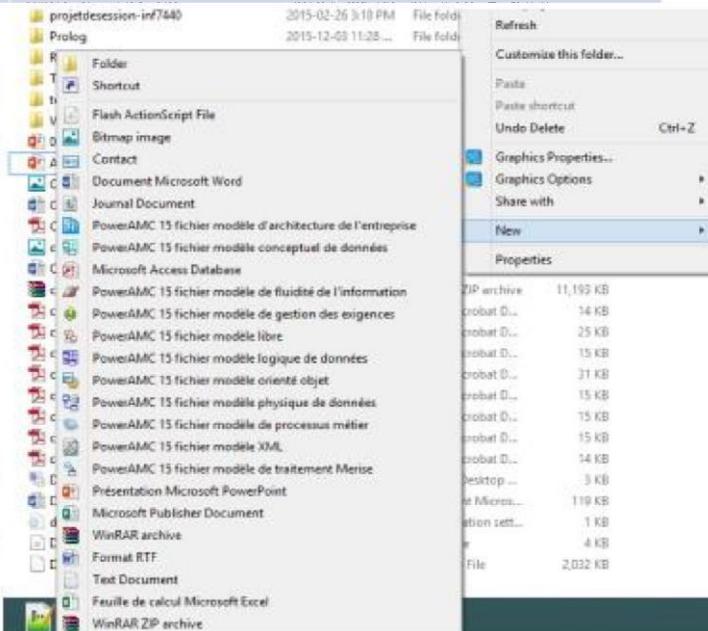
Exemples d'extensions de fichiers

Extension	Type du fichier	Application
.doc	Document texte	Word
.xsl	Tableur ou chiffrier	Excel
.ppt	Présentation	Power Point
.pdf	Document PDF	Adobe
.zip, .rar	Document compressé	WinRAR
.mp3, mp4, .wav, .avi	Audio, Vidéo	Lecteur Windows Média
.jpg, .bmp, .gif, .png	Images	Paint, explorateur windows

Comment créer un nouveau fichier/répertoire manuellement sous Windows.

Se positionner dans l'emplacement souhaité, ensuite réaliser l'une des opérations suivantes :

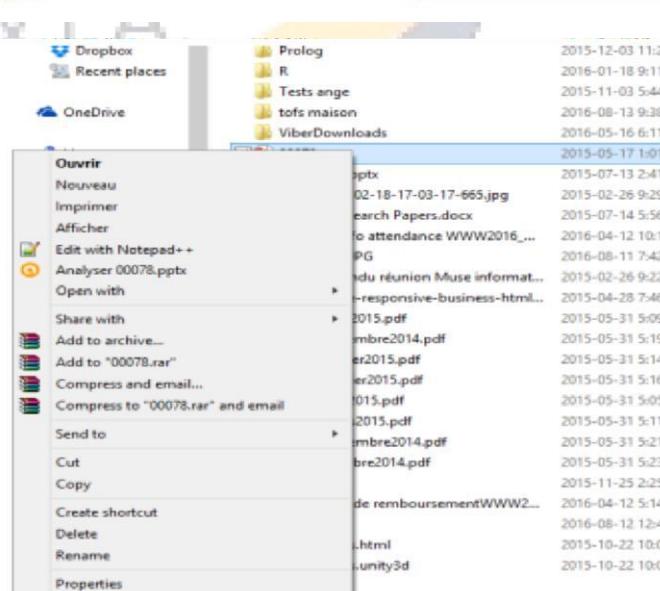
- Cliquez avec le bouton droit de la souris
- Allez dans le menu Nouveau
- Cliquez sur le type de fichier à créer



Comment manipuler un fichier/répertoire sous Windows.

Clic droit sur l'élément à manipuler puis:

- Ouvrir
- Renommer
- Supprimer
- Copier / Couper
- Créer un raccourci sur le bureau
- Etc.



Quelques raccourcis utiles:

- **Ctrl-c** : copier
- **Ctrl-x** : Couper
- **Ctrl-v** : Coller
- **Ctrl-a** : Tout sélectionner
- **Ctrl-z** : Annuler
- **Ctrl-y**: Rétablir
- **Ctrl-p**: Imprimer
- **Ctrl + clic gauche**: Conserver la sélection
- **Ctrl+Alt+Suppr** : Ouvrir le gestionnaire de tâche ou verrouiller l'ordinateur
- **F1**: Fiche d'aide
- **Touche Windows**: Ouvrir le menu démarrer
- **Touche Windows-L** : Verrouiller son ordinateur



Essayons quelques raccourcis utiles (pour gérer les fenêtres):

- **Alt+Tab** : passer d'une fenêtre à l'autre. Maintenez la touche Alt enfoncee et appuyez une ou plusieurs fois sur la touche Tab pour accéder à la fenêtre de votre choix.
- **Alt+Shift+Tab** : passer d'une fenêtre à l'autre (dans l'ordre inverse). Cette fois-ci, vous devez maintenir les touches Alt et Shift, et appuyer sur la touche Tab une ou plusieurs fois.
- **Windows+D** : masquer toutes les fenêtres. Pratique pour afficher brièvement le bureau.
- **Windows+Flèche vers le bas** : si la fenêtre occupe tout l'écran (fenêtre agrandie), elle retrouve une taille classique. Un deuxième clique sur **Windows+Flèche vers le bas** minimise la fenêtre.
- **Windows+Flèche vers le haut** : agrandir la fenêtre active.
- **Windows+Flèche vers la gauche** : pour placer la fenêtre sur la moitié gauche de l'écran.

3. Importance de la sauvegarde /compression :

- Les informations stockées dans les fichiers peuvent devenir partiellement ou entièrement irrécupérable à la suite d'une erreur, du bris d'un appareil ou d'un support, d'un feu, d'un vol, d'un acte de vandalisme ou de l'effet d'un virus.
- Le SE par l'intermédiaire du SGF est impuissant dans cette situation.

Solution: Prise de copie de sauvegarde

- L'utilisateur doit créer une copie de sauvegarde de l'information consignée sur support informatique (CD, DVD, clé USB ou disque dur externe).

- Les données (sauvegardées ou pas) peuvent devenir très volumineuses et ainsi occuper beaucoup d'espace mémoire.

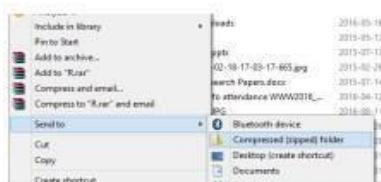
Solution: Compresser les données (zip, rar, etc.)

Importance de compression:

- Gagner de la place
- Regrouper plusieurs fichiers pour les envoyer par email

Comment s'y prendre ?

1. Sélectionner les fichiers à compresser
2. Clic droit sur l'un des fichiers
3. Choisir Envoyer vers... puis Dossier compressé



Exemple:

Fichier 27MB -> Fichier compressé 11 MB !!

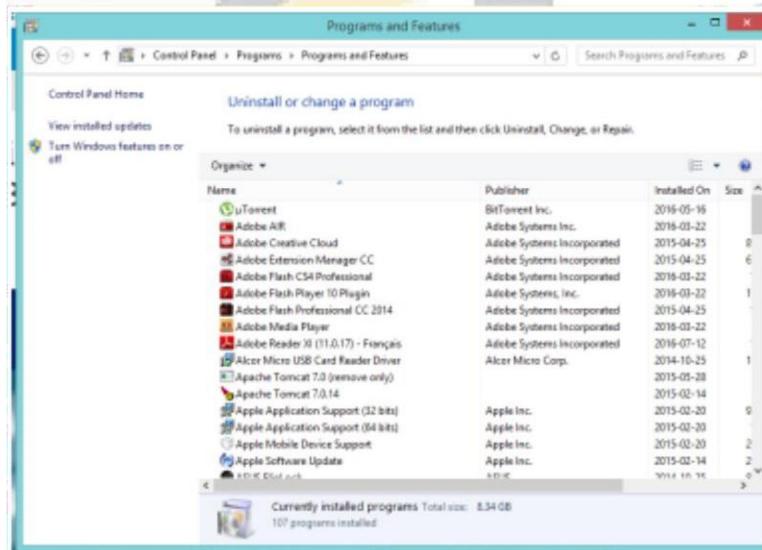
IV. La gestion des programmes

Le SE s'occupe tout seul d'allouer les ressources nécessaires pour chaque programme en cours d'exécution.

La gestion des programmes peut se faire manuellement. Les tâches effectuées étant entre autre :

- Visualisation des programmes installés sur la machine ;
- Désinstallation d'un programme ;
- Visualisation des processus (programmes en cours d'exécution) ;
- Arrêt d'un programme en cours d'exécution (Pas très recommandé) ;
- Visualisation de l'utilisation du processeur et de la RAM par chaque processus

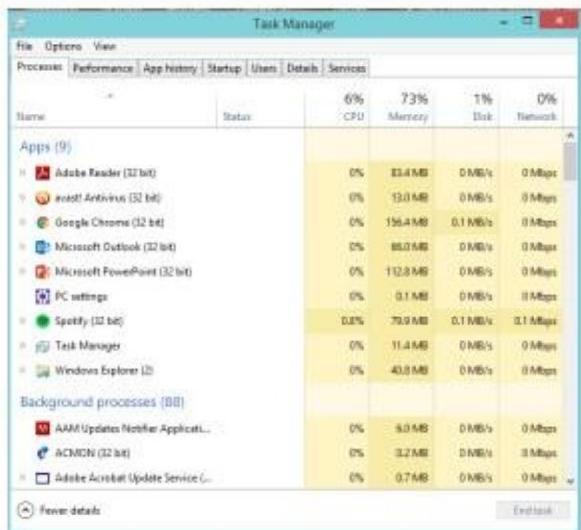
1. Visualisation et désinstallation d'un programme installé sur la machine



Accès

- Menu démarrer
- Rechercher: Panneau de contrôle
- Cliquez sur Programmes
- Cliquez sur Programmes et fonctionnalités
- Cliquez sur le programme que vous voulez désinstaller
- Cliquez sur désinstaller qui apparaît juste au dessus

2. Visualisation des processus (programmes en cours d'exécution)

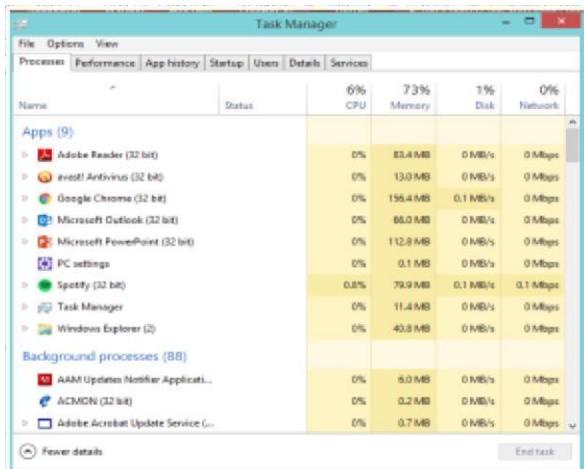


Accès

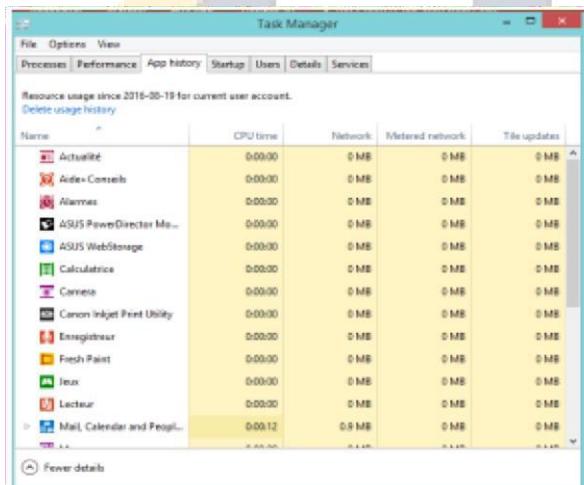
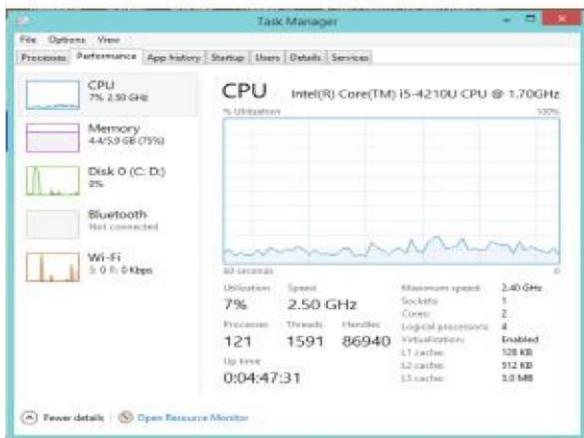
- Ctrl + Alt + Suppr
- Sélectionnez le gestionnaire de tâche

Vous avez la liste des programmes en cours d'exécution ainsi que leur consommation mémoire, CPU, etc.

3. Arrêt d'un programme en cours d'exécution (Pas très recommandé)



Exploration des onglets du gestionnaire de tâche



Name	Publisher	Status	Startup Impact
JD BubbleSound		Disabled	None
Adobe Creative Cloud	Adobe Systems Incorpor...	Enabled	Not measured
Adobe CSA Service Manager	Adobe Systems Incorpor...	Enabled	Not measured
Adobe Updater Startup Utility	Adobe Systems Incorpor...	Enabled	Not measured
ASUSWSLLoader.exe		Enabled	Not measured
avast! Antivirus	AVAST Software	Enabled	Not measured
Download		Disabled	None
Dropbox Update	Dropbox, Inc.	Enabled	Not measured
Fix PC problems and optimi...	Super PC Tools Ltd	Disabled	None
HDD Protection Monitor	STMicroelectronics	Enabled	Not measured
iOS(R) Dynamic Platform a...	Intel Corporation	Enabled	Not measured
iTunesHelper	Apple Inc.	Disabled	None
Juiced		Disabled	None
Lean Motion Control Panel	Lean Motion, Inc.	Disabled	None

- Sélectionnez un processus
- Cliquez sur fin de la tâche

Remarque: Lorsque vous quittez un programme de cette manière, toutes les données non enregistrées de ce programme sont perdues.

▪ Onglet performance

Visualisez en temps réel l'utilisation du CPU, de la mémoire vive, du disque dur, etc. Mesures de performances

▪ Historique des applications

Affiche l'activité cumulative pour chacune des vignettes d'applications.

Les applications qui utilisent plus de processus ou de données sont mises en surbrillance dans une couleur plus sombre

▪ Démarrage

Applications lancés automatiquement lors du démarrage de l'ordinateur.

Si votre ordinateur est lent ou si le processus de démarrage prend trop de temps, sélectionnez l'onglet Démarrage. Il affiche l'état du logiciel, si un programme est activé ou désactivé, et l'impact du logiciel sur la durée du démarrage de votre système.

- Utilisateurs

L'onglet Utilisateurs affiche l'utilisation de l'UC, de la mémoire, du disque et du réseau pour chaque compte d'utilisateur sur le système. Les options qui utilisent un pourcentage plus élevé de ressources sont mises en surbrillance.

- Détails

L'onglet Détails affiche des informations plus détaillées sur les processus.

- Services

L'onglet Services affiche les services en cours d'exécution.

Utilité du gestionnaire de tâches:

Le gestionnaire des tâches peut être particulièrement utile lorsqu'un programme ne répond plus ou pour fermer une session sans se déconnecter. En effet il permet d'envoyer des interruptions pour les forcer à se terminer rapidement. Il permet aussi de consulter des informations sur la connexion à Internet etc.

4. Exploration du panneau de configuration

Le panneau de configuration est l'endroit où sont rassemblés tous les paramètres (les réglages) de l'ordinateur.

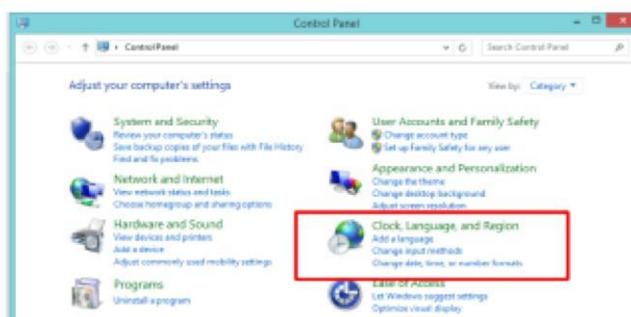
C'est un endroit à parcourir avec prudence : utile mais dangereux !

- Ne rien changer sans être sûr de ce que l'on fait ;
- Prendre note de ce qu'on fait pour marche arrière ;
- Annuler en cas du moindre doute.

Pour ouvrir le panneau de configuration : Menu Démarrer, Paramètres, Panneau de configuration ou, dans la barre de recherche du menu démarrer, tapez « panneau de configuration »

Par défaut, les éléments sont regroupés par catégories : Système et Sécurité, Réseau et Internet, Programmes, etc. Cliquez sur le nom d'un thème pour faire apparaître dans une nouvelle fenêtre tous les réglages qu'il propose.

- Régler la date et l'heure de votre ordinateur.
- Définir le fuseau horaire et autoriser le passage automatique à l'heure d'été.
- modifier les caractéristiques du clavier (français,...) En principe c'est correctement défini lorsque vous recevez votre ordinateur. Peut être utile si vous achetez un nouveau clavier.



V. La Sécurité informatique sous Windows et entretien de l'ordinateur

A. La Sécurité informatique

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation ou d'un poste seul sont uniquement utilisées dans le cadre prévu. La sécurité informatique consiste généralement en quatre principaux objectifs :

- L'intégrité, c'est-à-dire garantir que les données sont bien celles qu'on croit être
- La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources
- La disponibilité, permettant de maintenir le bon fonctionnement du système informatique
- La non répudiation, permettant de garantir qu'une transaction ne peut être niée

4.1. Les virus et les codes cachés

4.1.1. Les virus

Un virus est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé. Le véritable nom donné aux virus est CPA soit Code Auto-Propageable, mais par analogie avec le domaine médical, le nom de "virus" leur a été donné.

Le champ d'application des virus va de la simple balle de ping-pong qui traverse l'écran au virus destructeur de données, ce dernier étant la forme de virus la plus dangereuse. Ainsi, étant donné qu'il existe une vaste gamme de virus ayant des actions aussi diverses que variées, les virus ne sont pas classés selon leurs dégâts mais selon leur mode de propagation et d'infection. On distingue ainsi différents types de virus :

- les vers sont des virus capables de se propager à travers un réseau
- les troyens (chevaux de Troie) sont des virus permettant de créer une faille dans un système (généralement pour permettre à son concepteur de s'introduire dans le système infecté afin d'en prendre le contrôle)
- les bombes logiques sont des virus capables de se déclencher suite à un événement particulier (date système, activation distante, ...)

Depuis quelques années un autre phénomène est apparu, il s'agit des canulars (en anglais hoax), c'est-à-dire des annonces reçues par mail (par exemple l'annonce de l'apparition d'un nouveau virus destructeur ou bien la possibilité de gagner un téléphone portable gratuitement,...) accompagnées d'une note précisant de faire suivre la nouvelle à tous ses proches. Ce procédé a pour but l'engorgement des réseaux ainsi que la désinformation.

4.1.2. Concept d'antivirus

Un antivirus est un programme capable de détecter la présence de virus sur un ordinateur et, dans la mesure du possible, de désinfecter ce dernier. On parle ainsi d'éradication de virus pour désigner la procédure de nettoyage de l'ordinateur. Il existe plusieurs méthodes d'éradication :

- La suppression du code correspondant au virus dans le fichier infecté ;
- La suppression du fichier infecté ;
- La mise en quarantaine du fichier infecté, consistant à le déplacer dans un emplacement où il ne pourra pas être exécuté.

4.1.3. Les vers

Un ver est un programme qui peut s'auto-reproduire et se déplacer à travers un réseau en utilisant les mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier ...) pour se propager; un ver est donc un virus réseau. Les vers actuels se propagent principalement grâce à la messagerie (et notamment par le client de messagerie Outlook) grâce à des fichiers attachés contenant des instructions permettant de récupérer l'ensemble des adresses de courrier contenues dans le carnet d'adresse et en envoyant des copies d'eux-mêmes à tous ces destinataires. Ils se déclenchent lorsque l'utilisateur destinataire clique sur le fichier attaché.

Il est simple de se protéger d'une infection par ver. La meilleure méthode consiste à ne pas ouvrir "à l'aveugle" les fichiers qui vous sont envoyés en fichier attachés. Ainsi, tous les fichiers exécutables ou interprétables par le système d'exploitation peuvent potentiellement infecter votre ordinateur. Les fichiers

comportant notamment les extensions suivantes sont potentiellement susceptible d'être infectés : exe, com, bat, pif, vbs, scr, doc, xls, msi, eml. Pour tous les fichiers dont l'extension peut supposer que le fichier soit infecté (ou pour les extensions que vous ne connaissez pas) n'hésitez pas à installer un antivirus et à scanner systématiquement le fichier attaché avant de l'ouvrir.

4.1.4. Les chevaux de Troie

On appelle "Cheval de Troie" (en anglais trojan horse) un programme informatique effectuant des opérations malicieuses à l'insu de l'utilisateur. Le nom "Cheval de Troie" provient de la légende narrée dans l'Iliade (de l'écrivain Homère) à propos du siège de la ville de Troie par les Grecs. Un cheval de Troie (informatique) est donc un programme caché dans un autre qui exécute des commandes sournoises, et qui généralement donne un accès à la machine sur laquelle il est exécuté en ouvrant une porte dérobée (en anglais backdoor), par extension il est parfois nommé troyen par analogie avec les habitants de la ville de Troie.

A la façon du virus, le cheval de Troie est un code (programme) nuisible placé dans un programme sain (imaginez une fausse commande de listage des fichiers, qui détruit les fichiers au lieu d'en afficher la liste). Un cheval de Troie peut par exemple

- voler des mots de passe ;
- copier des données sensibles ;
- exécuter tout autre action nuisible ;
- ...

Pire, un tel programme peut créer, de l'intérieur de votre réseau, une brèche volontaire dans la sécurité pour autoriser des accès à des parties protégées du réseau à des personnes se connectant de l'extérieur.

Un cheval de Troie n'est pas nécessairement un virus, dans la mesure où son but n'est pas de se reproduire pour infecter d'autres machines. Par contre certains virus peuvent également être des chevaux de Troie, c'est-à-dire se propager comme un virus et ouvrir un « port » sur les machines infectées !

Détecter un tel programme est difficile car il faut arriver à détecter si l'action du programme (le cheval de Troie) est voulue ou non par l'utilisateur. Une infection par un cheval de Troie fait généralement suite à l'ouverture d'un fichier contaminé contenant le cheval de Troie et se traduit par les symptômes suivants :

- activité anormale du modem ou de la carte réseau : des données sont chargées en l'absence d'activité de la part de l'utilisateur ;
- des réactions curieuses de la souris ;
- des ouvertures impromptues de programmes ;
- des plantages à répétition ;

Pour se protéger de ce genre d'intrusion, il suffit d'installer un firewall, c'est-à-dire un programme filtrant les communications entrant et sortant de votre machine. Un firewall (littéralement pare-feu) permet ainsi d'une part de voir les communications sortant de votre machine (donc normalement initiées par des programmes que vous utilisez) ou bien les communications entrant. Toutefois, il n'est pas exclu que le firewall détecte des connexions provenant de l'extérieur sans pour autant que vous ne soyez la victime choisie d'un pirate. En effet il peut s'agir de tests effectués par votre fournisseur d'accès ou bien un pirate scannant au hasard une plage d'adresses IP.

Pour les systèmes de type Windows, il existe des firewalls non payants très performants :

- ZoneAlarm en version non professionnelle
- Tiny personal firewall

Si un programme dont l'origine vous est inconnue essaye d'ouvrir une connexion, le firewall vous demandera une confirmation pour initier la connexion. Il est essentiel de ne pas autoriser la connexion aux programmes que vous ne connaissez pas, car il peut très bien s'agir d'un cheval de Troie.

En cas de récidive, il peut être utile de vérifier que votre ordinateur n'est pas infecté par un troyen en utilisant un programme permettant de les détecter et de les éliminer (appelé bouffe-troyen). C'est le cas de The Cleaner, téléchargeable sur <http://www.moosoft.com>.

4.2. Autres problèmes de sécurité : les attaques

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Sur Internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont en réalité généralement lancées automatiquement à partir de machines infectées (virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire et plus rarement par des pirates informatiques. C'est la raison pour laquelle il est absolument impératif d'installer un pare-feu afin de faire barrière entre l'ordinateur et le réseau.

On appelle «attaque réseau» l'exploitation d'une faille (du système d'exploitation, d'un logiciel communiquant par le réseau ou bien même de l'utilisateur) à des fins non connues par la victime et généralement préjudiciables. Le but peut être de différentes sortes :

- obtenir un accès au système
- obtenir des informations personnelles sur l'utilisateur
- récupérer des données bancaires
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.)
- faire dysfonctionner un service
- utiliser le système de l'utilisateur comme «rebond» pour une attaque
- utiliser le système de l'utilisateur comme serveur FTP, lorsque le réseau sur lequel il est situé possède une bande passante élevée

4.2.1. Types d'attaques

Les attaques réseau consistent généralement à exploiter une vulnérabilité du système d'exploitation ou de l'une de ses applications en envoyant une requête spécifique, non prévue par son concepteur, ayant pour effet un comportement anormal conduisant parfois à l'accès au système tout entier.

Pour autant les erreurs de programmation contenues dans les programmes sont habituellement corrigées assez rapidement par leur concepteur dès lors que la vulnérabilité a été publiée. Il appartient alors aux administrateurs (ou utilisateurs personnels avertis) de se tenir informé des mises à jour des programmes qu'ils utilisent afin de limiter les risques d'attaques.

D'autre part il existe un certain nombre de dispositifs (pare-feu, systèmes de détection d'intrusions, antivirus) permettant d'ajouter un niveau de sécurisation supplémentaire.

Enfin dans la majeure partie des cas le maillon faible est l'utilisateur lui-même ! En effet c'est souvent lui, par méconnaissance ou dupé par un interlocuteur malicieux, qui va exécuter un fichier vénéré, donner des informations personnelles ou bancaires, etc. Ainsi, aucun dispositif de protection ne peut protéger l'utilisateur contre les arnaques, seuls bon sens, raison et un peu d'information sur les différentes pratiques peuvent lui éviter de tomber dans le piège !

4.2.2. Le hacking

Le terme «hacker» est souvent utilisé pour désigner un pirate informatique. Les hackers ayant l'intention de s'introduire dans les systèmes informatiques recherchent dans un premier temps des failles, c'est-à-dire des vulnérabilités nuisibles à la sécurité du système, dans les protocoles, les systèmes d'exploitations, les applications ou même le personnel d'une organisation ! Les termes de vulnérabilité, de brèche ou en langage plus familier de trou de sécurité (en anglais security hole) sont également utilisés pour désigner les failles de sécurité.

Pour pouvoir mettre en œuvre un exploit (il s'agit du terme technique signifiant exploiter une vulnérabilité), la première étape du hacker consiste à récupérer le maximum d'informations sur l'architecture du réseau et sur les systèmes d'exploitations et applications fonctionnant sur celui-ci.

Une fois que le hacker a établi une cartographie du système, il est en mesure de mettre en application des exploits relatifs aux versions des applications qu'il a recensées. Un premier accès à une machine lui permettra d'étendre son action afin de récupérer d'autres informations, et éventuellement d'étendre ses priviléges sur la machine.

La dernière étape du hacker consiste à effacer ses traces, afin d'éviter tout soupçon de la part de l'administrateur du réseau compromis et de telle manière à pouvoir garder le plus longtemps possible le contrôle des machines compromises.

4.2.3. Attaques par rebond

Lors d'une attaque, le pirate garde toujours à l'esprit le risque de se faire repérer, c'est la raison pour laquelle les pirates privilégient habituellement les attaques par rebond (par opposition aux attaques directes), consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer l'adresse IP réelle du pirate et d'utiliser les ressources de la machine servant de rebond. Cela montre l'intérêt de protéger son réseau ou son ordinateur personnel, car celui-ci se retrouve «complice» contre son gré de l'attaque et en cas de plainte de la victime, la première personne interrogée sera le propriétaire de la machine ayant servi de rebond.

Avec le développement des réseaux sans fils, ce type de scénario risque de devenir de plus en plus courant car si le réseau sans fil est mal sécurisé, un pirate situé à proximité peut l'utiliser pour lancer des attaques !

4.2.4. Ingénierie sociale

Le terme d'«ingénierie sociale» (en anglais «social engineering») désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct. L'ingénierie sociale est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs en se faisant passer pour une personne de la maison, un technicien, un administrateur, etc.

La meilleure façon de se protéger des techniques d'ingénierie sociale est d'utiliser son bon sens pour ne pas divulguer à n'importe qui des informations pouvant nuire à la sécurité de vos biens ou de votre entreprise.

4.2.5. Le scam

Le «scam» («ruse» en anglais), est une pratique frauduleuse d'origine africaine, consistant à extorquer des fonds à des internautes en leur faisant miroiter une somme d'argent dont ils pourraient toucher un pourcentage. L'arnaque du scam est issue du Nigéria, ce qui lui vaut également l'appellation «419» en référence à l'article du code pénal nigérian réprimant ce type de pratique.

L'arnaque du scam est classique : vous recevez un courrier électronique de la part du seul descendant d'un riche africain décédé il y a peu. Ce dernier a déposé plusieurs millions de dollars dans une compagnie de sécurité financière et votre interlocuteur a besoin d'un associé à l'étranger pour l'aider à transférer les fonds. Il est d'ailleurs prêt à vous reverser un pourcentage non négligeable si vous acceptez de lui fournir un compte pour faire transiter les fonds.

En répondant à un message de type scam, l'internaute s'enferme dans un cercle vicieux pouvant lui coûter plusieurs centaines d'euro s'il mord à l'hameçon.

B. L'entretien de l'ordinateur

Pourquoi entretenir son ordinateur ?

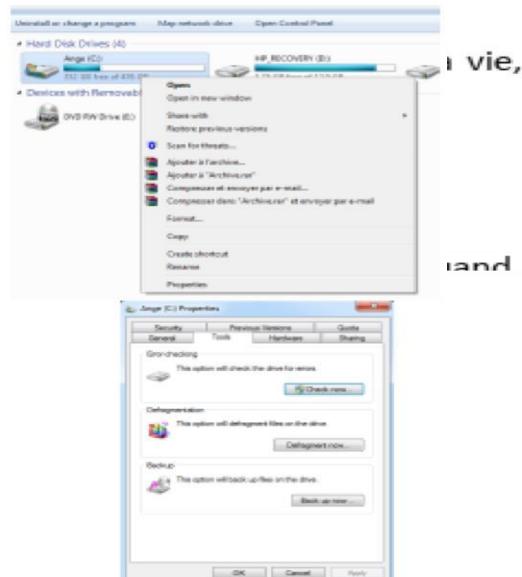
- L'empêcher de devenir trop lent
- Prolonger sa durée de vie
- Etc.

Les causes:

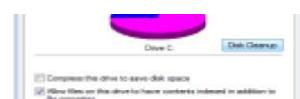
- Un conflit entre deux ou plusieurs logiciels
- trop de programmes lancés au démarrage.
- l'infection par des virus et logiciels malveillants
- l'accumulation des fichiers temporaires et cookies.
- manque d'espace libre sur le disque dur
- un ou plusieurs programmes ne sont pas à jour
- l'exécution de plusieurs logiciels à la fois (voir aussi les programmes qui fonctionnent en arrière-plan)
- le disque dur n'est pas fragmenté
- L'un des composants matériel de l'ordinateur est infecté (le disque dur, la barrette mémoire ou la carte graphique).

Défragmentation du disque

- Faites un clique-droit sur votre disque local (C:), puis cliquez sur Propriétés.
- Cliquez sur l'onglet Outils, puis cliquez sur « Défragmenter maintenant ».
- Sélectionnez un disque et lancer la défragmentation.
- Cet outil est sans risque pour l'ordinateur
- Permet d'accélérer l'ordinateur



- L'application procède alors au nettoyage du disque.



Chapitre 3 : Séances de travaux pratiques

ATELIER 1: INSTALLATION DE WINDOWS SUR UN PC

Objectif : Permettre à l'étudiant d'installer une version de windows

ATELIER 2 : MISE EN RESEAUX DE DEUX PC

Objectif : pouvoir effectuer un partage de fichiers entre deux PC dans lesquels windows est installé

Etape 1 : Renommer les deux PC à mettre en réseau.

Etape 2 : Insérer les adresses IP dans les cartes réseaux

Etape 3 : Configurer la découverte réseau

Etape 4 : Paramétriser le partage d'un fichier

ATELIER 3 : MANIPULATION DE QUELQUES COMMANDES DOS

Voici quelques commandes DOS

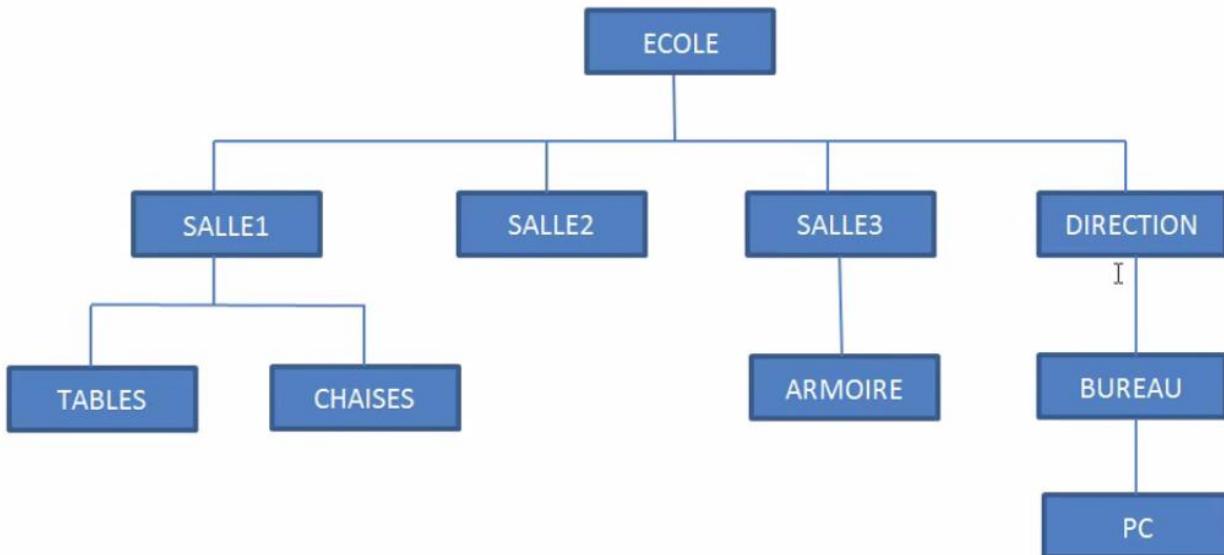
	Commande	<i>Interne/ Externe</i>	Description
1	CLS	I	Effacer l'écran
2	DIR	I	Afficher le contenu du répertoire en cours
3	TIME I	I	Afficher l'heure en cours
4	DATE	I	Afficher la date en cours
5	VOL	I	Afficher le volume du disque
6	VER	I	Afficher la version du DOS utilisé
7	DEL -----	I	Supprimer un ou plusieurs fichiers

8	COPY	I	Copier un ou plusieurs fichiers
9	MOVE	I	Déplacer un ou plusieurs fichiers
10	RENAME	I	Renommer un fichier
11	MKDIR MD	I	Créer un ou plusieurs répertoires
12	CHDIR CD	I	Se déplacer vers un autre répertoire
13	RMDIR RD	I	Supprimer un répertoire vide
14	TREE	E	Afficher tous les noms des dossiers et des fichiers.
15	XCOPY	E	Copier des fichiers et des dossiers
16	HELP	I	Lister les commandes disponibles et les paramètres
17	COPY CON EDIT	I E	Créer un fichier Créer un fichier et l'éditer
18	TYPE	I	Afficher le contenu d'un fichier
19	COMP	I	Comparer le contenu de 2 fichiers
20	EXIT	I	Quitter l'interpréteur de commande et revenir au niveau précédent

Exercice 1

Manipuler les commandes : cls, dir, time, date, vol, ver, exit.

Exercice 2 :



- 1/- Créer l'arborescence suivante
- 2/- Créer deux fichiers « fichier1 » et « fichier2 » dans le dossier « SALLE2 » par la commande « copy con ».
- 3/- Copier le fichier « fichier1 » dans le dossier « ARMOIRE »
- 4/- Déplacer le fichier « fichier1 » vers le dossier « PC »
- 5/- Renommer le fichier « fichier1 » par « exo1 » cd
- 6/- Supprimer le fichier « fichier1 » du dossier « SALLE2 »
- 7/- Afficher le contenu du fichier « fichier2 »
- 8/- Afficher l'arborescence créée
- 9/- copier le dossier « SALLE3 » et son contenu dans le dossier « TABLES»
- 10/- Supprimer le dossier « CHAISES »
- 11/- Supprimer le dossier « DIRECTION » et son contenu par une seule commande

ATELIER 4 : COMMANDES RESEAUX

Liste des principales commandes CMD

Ping

PING : Teste la connexion réseau avec une adresse IP distante

```
ping -t [IP ou host] ping -l 1024
[IP ou host]
```

- L'option -t permet de faire des pings en continu jusqu'à Ctrl-C.
 - Si vous avez précisé l'option -t vous pouvez à tout moment avoir des statistiques sans interrompre les requêtes ping en appuyant sur Ctrl+Attn (aussi nommé Ctrl+Pause)

Cette commande est aussi utile pour générer une charge réseau en spécifiant la taille du paquet avec l'option -l et la taille du paquet en octets.

Tracert

TRACERT : Affiche toutes les adresses IP intermédiaires par lesquelles passe un paquet entre la machine locale et l'adresse IP spécifiée.

```
tracert [@IP ou nom du host]
tracert -d [@IP ou nom du host]
```

Cette commande est utile si la commande ping ne donne pas de réponse, afin d'établir à quel niveau la connexion est défaillante.

IpConfig

IPCONFIG : Affiche ou rafraîchit la configuration réseau TCP/IP

```
ipconfig [/all] [/release [carte]] [/renew [carte]] [/flushdns] [/displaydns]
[/registerdns] [-a] [-a] [-a]
```

Cette commande, exécutée sans option, affiche l'adresse IP en cours, le masque réseau ainsi que la passerelle par défaut au niveau des interfaces réseau connues sur la machine locale.

- /all: Affiche toute la configuration réseau, y compris les serveurs DNS, WINS, bail DHCP, etc
...
• /renew [carte]: Renouvelle la configuration DHCP de toutes les cartes (si aucune carte n'est spécifiée) ou d'une carte spécifique avec le paramètre carte. Le nom de carte est celui qui apparaît avec ipconfig sans paramètre.
• /release [carte]: Envoie un message DHCPRELEASE au serveur DHCP pour libérer la configuration DHCP actuelle et annuler la configuration d'adresse IP de toutes les cartes (si aucune carte n'est spécifiée) ou d'une carte spécifique avec paramètre carte. Ce paramètre désactive TCP/IP pour les cartes configurées de manière à obtenir automatiquement une adresse IP.
• /flushdns: Vide et réinitialise le cache de résolution du client DNS. Cette option est utile pour exclure les entrées de cache négatives ainsi que toutes les autres entrées ajoutées de façon dynamique.
• /displaydns: Affiche le cache de résolution du client DNS, qui inclut les entrées préchargées à partir du fichier des hôtes locaux ainsi que tous les enregistrements de ressources récemment obtenus pour les requêtes de noms résolues par l'ordinateur. Le service Client DNS utilise ces informations pour résoudre rapidement les noms fréquemment sollicités, avant d'interroger ses serveurs DNS configurés.
• /registerdns: Actualise tous les baux DHCP et réinscrit les noms DNS.

NetStat

NETSTAT : Affiche l'état de la pile TCP/IP sur la machine locale

```
NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [intervalle]
```

- -a Affiche toutes les connexions et ports d'écoute (Les connexions côté serveur sont normalement inhibées).
- -e Affiche les statistiques Ethernet. Peut être combinée avec l'option -s.
- -n Affiche les adresses et les numéros de port sous forme numérique.
- -p proto Affiche les connexions pour le protocole spécifié par proto; proto peut être TCP ou UDP. Utilisé avec l'option -s pour afficher des statistiques par protocole, proto peut être TCP, UDP, ou IP.
- -r Affiche le contenu de la table de routage.
- -s Affiche les statistiques par protocole. Par défaut, des statistiques sur TCP, UDP et IP sont visualisées; l'option -p peut être utilisée pour spécifier un sous-ensemble du défaut.
- intervalle: Réaffiche les statistiques sélectionnées, avec une pause de "intervalle" secondes entre chaque affichage. Appuyez sur Ctrl+C pour arrêter l'affichage des statistiques.
- -abnov Affiche les processus qui utilisent la connexion internet (Adresse IP local, port, adresse IP distante et le PID du processus qui utilise la connexion ainsi que son nom).

Route

ROUTE : Affiche ou modifie la table de routage

```
ROUTE [-f] [commande [destination] [MASK masque réseau] [passerelle]]
```

- -f Efface les tables de routage de toutes les entrées de passerelles. Utilisé conjointement à une des commandes, les tables sont effacées avant l'exécution de la commande. □ -p Rend rémanente l'entrée dans la table après le reboot de la machine □ commande Spécifie une des quatre commandes :
 - DELETE: Efface un itinéraire. ○ PRINT: Affiche un itinéraire.
 - ADD: Ajoute un itinéraire.
 - CHANGE: Modifie un itinéraire existant.
- destination: Spécifie l'hôte.
- MASK: Si le mot clé MASK est présent, le paramètre suivant est interprété comme le paramètre masque réseau.
- masque réseau: Fourni, il spécifie la valeur de masque de sous-réseau à associer à cette entrée d'itinéraire. Non spécifié, il prend la valeur par défaut 255.255.255.255.
- passerelle: Spécifie la passerelle.
- METRIC: Spécifie le coût métrique pour la destination

Arp

ARP : Résolution des adresses IP en adresses MAC. Affiche et modifie les tables de traduction des adresses IP en adresses physiques utilisées par le protocole de résolution d'adresses ARP.

```
ARP -s adr_inet adr_eth [adr_if]  
ARP -d adr_inet [adr_if]  
ARP -a [adr_inet] [-N adr_if]
```

- -a Affiche les entrées ARP actives en interrogeant le protocole de données actif. Si adr_inet est spécifié, seules les adresses IP et physiques de l'ordinateur spécifié sont affichées. Si plus d'une interface réseau utilise ARP, les entrées de chaque table ARP sont affichées.
- -g Identique à -a.
- adr_inet Spécifie une adresse internet.
- -N adr_if Affiche les entrées ARP pour l'interface réseau spécifiée par adr_if.
- -d Efface l'hôte spécifié par adr_inet.
- -s Ajoute l'hôte et associe l'adresse Internet adr_inet avec l'adresse physique adr_eth. L'adresse physique est donnée sous forme de 6 octets hexadécimaux séparés par des tirets. L'entrée est permanente.
- adr_eth Spécifie une adresse physique.
- adr_if Précisée, elle spécifie l'adresse Internet de l'interface dont la table de traduction des adresses devrait être modifiée. Non précisée, la première interface applicable sera utilisée.

NbtStat

NBTSTAT : Mise à jour du cache du fichier Lmhosts. Affiche les statistiques du protocole et les connexions TCP/IP actuelles utilisant NBT (NetBIOS sur TCP/IP).

```
NBTSTAT [-a Nom Distant] [-A adresse IP] [-c] [-n] [-r] [-R] [-s] [S]  
[intervalle]
```

- -a (état carte) Liste la table de noms de la machine distante (nom connu).
- -A (état carte) Liste la table de noms de la machine distante (adresse IP).
- -c (cache) Liste le cache de noms distant y compris les adresses IP.
- -n (noms) Liste les noms NetBIOS locaux.
- -r (résolus) Liste les noms résolus par diffusion et via WINS.
- -R (Recharge) Purge et recharge la table du cache de noms distante.
- -S (Sessions) Liste la table de sessions avec les adresses destination IP.
- -s (sessions) Liste la table de sessions convertissant les adresses de destination IP en noms d'hôtes via le fichier hôtes.

Un Exemple : nbtstat -A
@IP

Cette commande renvoie le nom NetBIOS, nom du système, les utilisateurs connectés ...de la machine distante.

Telnet

TELNET

```
telnet <IP ou host>
telnet <IP ou host> <port TCP>
```

La commande telnet permet d'accéder en mode Terminal (Ecran passif) à un host distant. Elle permet également de vérifier si un service quelconque TCP tourne sur un serveur distant en spécifiant après l'adresse IP le numéro de port TCP. C'est ainsi que l'on peut tester si le service SMTP, par exemple, tourne sur un serveur Microsoft Exchange en utilisant l'adresse IP du connecteur SMTP et puis 25 comme numéro de port. Les ports les plus courants sont :

- ftp (21),
- telnet (23),
- smtp (25),
- www (80),
- kerberos (88),
- pop3 (110), □ nntp (119) □ et nbt (137-139).

Hostname

HOSTNAME : Affiche le nom de la machine

Ftp

FTP: Client de téléchargement de fichiers `ftp -`

`s:<file>`

- `-s` cette option permet de lancer des FTP en mode batch : spécifie un fichier textuel contenant les commandes FTP.

NsLookUp

NsLookUp: envoie des requêtes DNS sur un serveur DNS au choix `nslookup [domaine] [serveur dns]`

La commande NsLookUp permet d'envoyer des requêtes DNS à un serveur. Par défaut, si vous ne mettez pas le serveur DNS, la commande utilisera celui qui est configuré pour votre interface réseau (celui que

vous utilisez pour naviguer sur internet, par exemple) mais vous pouvez forcer l'utilisation d'un autre serveur.

Par exemple, pour demander au serveur DNS 10.0.0.3 l'adresse IP correspondante à l'adresse `www.commentcamarche.net`: `nslookup www.commentcamarche.net 10.0.0.3`

- Si vous ne précisez aucun paramètre pour nslookup, un shell s'ouvrira en attente de requêtes de votre part.

NetSh

NetSh: configurer le réseau sous Windows

Netsh (pour network shell en anglais) est un logiciel utilitaire qui présente une interface utilisateur en ligne de commande de type Win32 pour la gamme des systèmes d'exploitation Windows NT (NT, 2000, XP, 2003 Serveur, Vista, etc.) à partir de Windows 2000. Il permet la configuration du réseau, localement ou à distance.

Une utilisation classique de netsh est la réinitialisation de la pile TCP/IP à ses paramètres d'origine (Sous Windows 98, cette opération nécessitait la réinstallation de l'adaptateur TCP/IP). Dans ce mode, il faut fournir à la commande un fichier journal (log). Celui-ci sera rempli avec les valeurs affectées par netsh. Netsh permet aussi (entre autres) de changer l'adresse IP de la machine.

Exemples d'utilisation

Réinitialisation de la pile TCP/IP :

```
netsh interface ip reset C:\resetlog.txt
```

Adresse IP statique :

```
netsh interface ip set address "Connexion au réseau local" static  
123.123.123.123 255.255.255.0      Adresse IP dynamique : netsh interface ip set  
address "Connexion au réseau local" dhcp
```

EXERCICE D' APPLICATION : CREATION D'UN POINT D'ACCES VIRTUEL