Maintenance

Fait par

ALLOUTI Manale
MCHIOUER Soumia
MOUHIB Amine
NAANAA Imane
NAJEH Amine

Stagiaires en ista lazaret Oujda option réseaux informatiques groupe A 2007/2008

Sommaire

Avant tout…. Qu'est ce que la maintenance ??

95% des problèmes informatiques se situent entre le clavier et la chaise

La **maintenance** vise à maintenir ou à rétablir un bien dans un état spécifié afin que celui-ci soit en mesure d'assurer un service déterminé.

La **maintenance** regroupe ainsi les actions de dépannage et de réparation, de réglage, de révision, de contrôle et de vérification des équipements matériels (machines, véhicules, objets manufacturés, etc.) ou même immatériels (logiciels).

Maintenir c'est pas si facil, surtout dans notre domaine : l'informatique …..En fait il faut bien connaître l'architecture de l'ordinateur

Architecture de l'ordinateur

la carte mère

L'élément constitutif principal de l'ordinateur est la **carte mère** (en anglais « *mainboard* » ou « *motherboard* », parfois abrégé en « *mobo* »). La carte mère est le socle permettant la connexion de l'ensemble des éléments essentiels de l'ordinateur. Comme son nom l'indique, la carte mère est une carte maîtresse, prenant la forme d'un grand circuit imprimé possédant notamment des connecteurs pour les cartes d'extension, les barrettes de mémoires, le processeur, etc. Il existe plusieurs façons de caractériser une carte mère, notamment selon les caractéristiques suivantes :

- le facteur d'encombrement,
- le chipset,
- le type de support de processeur,
- les connecteurs d'entrée-sortie.

Facteur d'encombrement

On désigne généralement par ce terme (ou *facteur de forme*, en anglais *form factor*), la géométrie, les dimensions, l'agencement et les caractéristiques électriques de la carte mère. Afin de fournir des cartes mères pouvant s'adapter dans différents boîtiers de marques différentes, des standards ont été mis au point :

- **AT baby / AT full format** est un format utilisé sur les premiers ordinateurs PC du type 386 ou 486. Ce format a été remplacé par le format ATX possédant une forme plus propice à la circulation de l'air et rendant l'accès aux composants plus pratique.
- **ATX** : Le format ATX est une évolution du format Baby-AT. Il s'agit d'un format étudié pour améliorer l'ergonomie. Ainsi la disposition des connecteurs sur une carte mère ATX est prévue de manière à optimiser le branchement des périphériques (les connecteurs IDE sont par exemple situés du côté des disques). D'autre part, les composants de la carte mère sont orientés parallèlement, de manière à permettre une meilleure évacuation de la chaleur.
- **BTX** : Le format BTX (*Balanced Technology eXtended*), porté par la société Intel, est un format prévu pour apporter quelques améliorations de l'agencement des composants afin d'optimiser la circulation de l'air et de permettre une optimisation acoustique et thermique. Les différents connecteurs (connecteurs de mémoire, connecteurs d'extension) sont ainsi alignés parallèlement, dans le sens de circulation de l'air. Par ailleurs le microprocesseur est situé à l'avant du boîtier au niveau des entrées d'aération, où l'air est le plus frais.
- **ITX** : Le format ITX (*Information Technology eXtended*), porté par la société Via, est un format extrêmement compact prévu pour des configurations exigües telles que les mini-PC.

Ainsi, du choix d'une carte mère (et de son facteur de forme) dépend le choix du boîtier.

La carte mère contient un certain nombre d'éléments embarqués, c'est-à-dire intégrés sur son circuit imprimé :

- Le chipset, circuit qui contrôle la majorité des ressources (interface de bus du processeur, mémoire cache et mémoire vive, slots d'extension,...).
- L'horloge et la pile du CMOS.
- Le support du processeur.
- Le BIOS.
- Les bus.

Le chipset

On appelle **chipset** (en français *jeu de composants*) l'élément chargé d'aiguiller les informations entre les différents bus de l'ordinateur afin de permettre à tous les éléments constitutifs de l'ordinateur de communiquer entre eux.

Le **chipset** était originalement composé d'un grand nombre de composants électroniques, ce qui explique son nom. Il est généralement composé de deux éléments :

- Le **NorthBridge** (**Pont Nord** ou **Northern Bridge**, appelé également *contrôleur mémoire*) est chargé de contrôler les échanges entre le processeur et la mémoire vive, c'est la raison pour laquelle il est situé géographiquement proche du processeur. Il est parfois appelé **GMCH**, pour *Graphic and Memory Controller Hub*.
- Le **SouthBridge** (**Pont Sud** ou **Southern Bridge**, appelé également *contrôleur d'entrée-sortie* ou *contrôleur d'extension*) gère les communications avec les périphériques d'entrée-sortie. Le pont sud est également appelé **ICH** (*I/O Controller Hub*).

Horloge et pile du CMOS

L'**horloge temps réel** (notée **RTC**, pour *Real Time Clock*) est un circuit chargé de la synchronisation des signaux du système. Elle est constituée d'un cristal qui, en vibrant, donne des impulsions (appelés *tops d'horloge*) afin de cadencer le système. On appelle *fréquence de l'horloge* (exprimée en *MHz*) le nombre de vibrations du cristal par seconde, c'est-à-dire le nombre de *tops d'horloge* émis par seconde. Plus la fréquence est élevée, plus le système peut traiter d'informations.

Lorsque l'ordinateur est mis hors tension, l'alimentation cesse de fournir du courant à la carte mère. Or, lorsque l'ordinateur est rebranché, le système est toujours à l'heure. Un circuit électronique, appelé *CMOS* (*Complementary Metal-Oxyde Semiconductor*, parfois appelé *BIOS CMOS*), conserve en effet certaines informations sur le système, telles que l'heure, la date système et quelques paramètres essentiels du système.

Lorsque l'heure du système est régulièrement réinitialisée, ou que l'horloge prend du retard, il suffit généralement d'en changer la pile

Support du microprocesseur

Le processeur (aussi appelé *microprocesseur*) est le cerveau de l'ordinateur. Il exécute les instructions des programmes grâce à un jeu d'instructions. Le processeur est caractérisé par sa fréquence, c'est-à-dire la cadence à laquelle il exécute les instructions. Ainsi, un processeur cadencé à 800 MHz effectuera grossièrement 800 millions d'opérations par seconde.

La carte mère possède un emplacement (parfois plusieurs dans le cas de cartes mères multi-processeurs) pour accueillir le processeur, appelé **support de processeur**. On distingue deux catégories de supports :

- **Socket** (en français *embase*) : il s'agit d'un connecteur carré possédant un grand nombre de petits connecteurs sur lequel le processeur vient directement s'enficher.
- **Slot** (en français *fente*) : il s'agit d'un connecteur rectangulaire dans lequel on enfiche le processeur verticalement

Le processeur possède généralement un détrompeur, matérialisé par un coin tronqué ou une marque de couleur, devant être aligné avec la marque correspondante sur le support.

BIOS

Le BIOS (*Basic Input/Output System*) est le programme basique servant d'interface entre le système d'exploitation et la carte mère.Il est possible de configurer le BIOS grâce à une interface (nommée *BIOS setup*, traduisez *configuration du BIOS*) accessible au démarrage de l'ordinateur par simple pression d'une touche (généralement la touche *Suppr)*.

Les Bus

On appelle **bus**, en informatique, un ensemble de liaisons physiques (câbles, pistes de circuits imprimés, etc.) pouvant être exploitées en commun par plusieurs éléments matériels afin de communiquer.

Les bus ont pour but de réduire le nombre de « voies » nécessaires à la communication des différents composants, en mutualisant les communications sur une seule voie de données. C'est la raison pour laquelle la métaphore d'« autoroute de données » est parfois utilisée.

On distingue généralement sur un ordinateur deux principaux bus :

- le **bus système** (appelé aussi *bus interne*, en anglais *internal bus* ou *front-side bus*, noté *FSB*). Le bus système permet au processeur de communiquer avec la mémoire centrale du système (mémoire vive ou RAM).

- **le bus d'extension** (parfois appelé *bus d'entrée/sortie*) permet aux divers composants de la carte mère (USB, série, parallèle, cartes branchées sur les connecteurs PCI, disques durs, lecteurs et graveurs de CD-ROM, etc.) de communiquer entre eux mais il permet surtout l'ajout de nouveaux périphériques grâce aux connecteurs d'extension (appelés **slots**) connectés sur le bus d'entrées-sorties.

les connecteurs

On trouve des connecteurs :
1-de la mémoire vive (RAM)
2-d'extension :

Les **connecteurs d'extension** (en anglais **slots**) sont des réceptacles dans lesquels il est possible d'insérer des cartes d'extension, c'est-à-dire des cartes offrant de nouvelles fonctionnalités ou de meilleures performances à l'ordinateur. Il existe plusieurs sortes de connecteurs :

- Connecteur ISA (*Industry Standard Architecture*) : permettant de connecter des cartes ISA, les plus lentes fonctionnant en 16-bit
- Connecteur VLB (*Vesa Local Bus*): Bus servant autrefois à connecter des cartes graphiques
- Connecteur PCI (*Peripheral Component InterConnect*) : permettant de connecter des cartes PCI, beaucoup plus rapides que les cartes ISA et fonctionnant en 32-bit
- Connecteur AGP (*Accelerated Graphic Port*): un connecteur rapide pour carte graphique.
- Connecteur PCI Express (*Peripheral Component InterConnect Exress*) : architecture de bus plus rapide que les bus AGP et PCI.
- Connecteur AMR (*Audio Modem Riser*): ce type de connecteur permet de brancher des mini-cartes sur les PC en étant équipés

3 d'endrer/sortie
4 connecteur d'alimentation
5 connecteurs du disque dur

Les types de connexion

Actuellement, vous pouvez trouver sur le marché trois types de connexions pour les disques durs. Il y a :

- la connexion "**IDE**" (Integrated Drive Electronics), ce type de connexion est le plus couramment utilisée par les disques durs. Cependant, l'IDE est aussi utilisé par les lecteurs de CD-ROM et de DVD-ROM, mais aussi par certains périphériques de stockage. Les ordinateurs peuvent prendre en charge jusqu'à quatre périphériques IDE sur deux connecteurs, soit deux périphériques par connecteur. Les deux connecteurs sont appelés IDE 1 et IDE 2 .Les périphériques qui y sont connectés ; sont désignés comme "**maîtres**" (en anglais, "**master**") ou "**esclaves**" (en anglais, "**slave**"). Il faut noter qu'il existe aussi des versions améliorées du standard IDE, comme par exemple l'"**E-IDE**"(Enhanced-IDE).

-la connexion "**SCSI**" (Small Computer System Interface), ce type de connexion est plus rapide que l'IDE. Cependant, il exige l'installation d'une carte spéciale dans l'ordinateur .Tout comme l'IDE, ce type de connexion est aussi utilisé par d'autres périphériques (scanners, périphériques de stockage, etc.). Il existe aussi plusieurs types de SCSI, chacun d'eux ayant des caractéristiques spécifiques. Il y a par exemple, le Fast SCSI (parfois appelé SCSI-2), le Wide SCSI, etc

- la connexion "**IEEE 1394**" (Institute of Electrical and Electronics Engineers 1394), parfois appelé "**Fire Wire®**" ou "**i.LINK**", ce type de connexion prend en charge des taux de transfert beaucoup plus élevés que l'IDE et le SCSI. Ce standard est donc adapté aux périphériques qui nécessitent des taux de transfert important, comme les caméscopes numériques et bien sûr les disques durs. L'IEEE 1394 utilise un connecteur à six broches qui fournit les données et l'alimentation électrique aux périphériques (cependant, certains périphériques nécessitent une alimentation séparée). Ce type de connexion sera sans nul doute le standard dans les années à venir, notamment grâce à son taux de transfert élevé.

Alimentation de la carte mère

On peut dire que l'alimentation est le coeur de l'ordinateur sans elle rien ne fonctionne elle fait presque toujours partie de l'unité du boîtier même si on achète celui-ci separament elle est équipée d'un ventilateur dont le rôle consiste a évité tout surchauffe en évacuant l'air de l'intérieur vers l'extérieur.
Cette photo vous montre l'ensemble des composants présents sur une carte mère.
A Emplacement prévu pour l'alimentation électrique.
B Emplacement prévu pour le microprocesseur.
C Emplacements des barrettes de mémoire.
D Connecteur de la nappe vers le lecteur de disquettes.

E Connecteurs IDE1 et IDE2 qui servent à brancher, au moyen de nappes, le disque dur, le lecteur de CD ou de DVD et le graveur de CD.
F Connecteur AGP pour la carte graphique.
G Connecteurs PCI pour la carte son, la carte tuner TV, le modem interne, etc.
H Connecteurs ISA pour les anciennes cartes.
I Cavaliers qui servent pour divers réglages. Ces cavaliers ne sont pas toujours présents sur toutes les cartes mères. Consultez le manuel de votre carte pour effectuer les réglages.
J Connecteur du ventilateur principal.

le processeur

Un **processeur** est un ensemble matériel destiné, dans un ordinateur ou une autre machine, à interpréter et exécuter des traitements. Cet organe peut être **généraliste** et constituer le processeur central d'un ordinateur (par exemple, le **Pentium**) ou **spécialisé** dans des tâches particulières ; par exemple, un processeur **DSP** (Digital Signal Processor) est spécialisé dans le traitement des signaux numériques.
Le **processeur central** peut être vu comme le **cerveau** (c'est la partie la plus "intelligente") ou comme le **coeur** (qui pompe des instructions et expulse des données, et non du sang) de l'ordinateur ; il est aussi appelé :
- **UCT** (Unité Centrale de Traitement) ou **CPU** (Central Processing Unit) dans un gros système,
- **microprocesseur** dans un micro-ordinateur (processeur tenant tout entier sur **une seule puce de silicium** et contenant plusieurs millions de composants électroniques).
Le **processeur central** remplit les fonctions suivantes :
- Décodage et exécution des instructions contenues dans les programmes, en passant par un stockage intermédiaire dans des registres.
- Lecture/écriture des données en mémoire.
- Commande des autres éléments de l'ordinateur, contrôle des opérations d'entrée/sortie (clavier, souris,...), et gestion des unités de stockage et des périphériques.

Mémoires de masses

Lecteur disquette

Les lecteurs de disquettes (ou floppy), sont actuellement les supports amovibles de mémoire de masse de petite taille les moins répandus. En effet, la majorité des PC actuels ne le possèdent pas. La cause est bien vue leur petite capacité et leur fragilité, les disquettes, en particulier le format 3.5" 1.44M, sont un standard. Leur faible coût, leur facilité d'emploi et la possibilité d'écrire (à l'inverse des CD-ROM) ont permis un énorme nombre de vente. ***Ces lecteurs n'évoluent malheureusement plus beaucoup***, alors ils sont remplacés par les flashes disque ou ce qu'on nomme clé usb.
Les lecteurs de disquettes sont de conception relativement simple***. Un moteur rotatif fait tourner la disquette dans son support, à une vitesse donnée. Attention car celle-ci peut varier en fonction du type de disquette. Une tête de lecture va alors se placer sur les secteurs à lire. Celle-ci converti les données binaires en pulsion électromagnétiques lors de l'écriture, et inversement lors de la lecture. Le positionnement de la disquette est extrêmement grossier, ce qui ne permet pas un stockage dense des données sur le support***. En effet, la densité courante d'une disquette n'est que de ***135 TPI***. ***A l'inverse des disques dur, la tête de lecture est contact direct avec la disquette***. C'est en effet comme cela qu'est obtenu le meilleur résultat avec une technologie simple et peu coûteuse. D'autres part, la souplesse du support empêcherait toute tentative de maintenir la tête à une distance constante de la disquette. Le principal inconvénient est qu'à la longue la tête de lecture s'encrasse avec les particules issues de la disquette et peut générer des erreurs de lecture/écriture. Afin de lutter contre ce problème, il existe dans le commerce des kits de nettoyages de lecteurs de disquettes. Ils sont généralement composés d'une disquette composée d'une surface absorbante et d'un liquide de nettoyage. Il suffit d'imbiber la disquette et de forcer le lecteur à la lire.
La tête de lecture est composée de trois parties. La tête de lecture/écriture proprement dite, entourée de deux têtes d'effaçage. Ainsi, lorsqu'une zone est écrite, les deux têtes latérales se chargent de délimiter proprement la piste en effaçant toutes les traces parasites. Ce procédé autorise ainsi une tolérance d'erreur dans le positionnement de la tête de lecture. Si cette dernière n'est pas située exactement sur la piste, elle n'est pas gênée par les valeurs stockées sur les pistes mitoyennes.
Un élément appelé Head Actuator est chargé de déplacer la tête de lecture latéralement sur le disque. Un "Stepper Motor" est chargé de stopper ce déplacement à des points précis, correspondant aux différentes pistes. Ce procédé n'est pas nouveau, les anciens disques durs l'utilisaient déjà. Mais désormais, ils ne font plus appel à ce procédé. En effet, leur forte vitesse de rotation provoque un dégagement de chaleur tel que la dilatation fausserait le positionnement précis de la tête

Montage d'un lecteur de disquette

Commencez par définir la destination du lecteur, A: ou B:? ***Si vous utilisez un câble de connexion standard, doté de fil croisés entre les deux connecteurs des lecteurs, les paramétrages par défaut feront l'affaire***. Dans le cas contraire, il peut être nécessaire de modifier les jumpers situés sur la face arrière du lecteur.
Les fonctions DS0 et DS1 permettent respectivement de spécifier A ou B. Sachez toutefois qu'il est rare de rencontrer un tel cas.
Il faut ensuite repérer un emplacement libre correspondant au format du lecteur de disquette. Si aucun emplacement 3.5" n'est disponible, et que vous désirez monter un tel lecteur, vous pouvez vous procurer un kit adaptateur en vente dans le commerce. ***Un lecteur peut être monté horizontalement ou verticalement ,mais de préférence jamais à l'envers.*** En effet. dans cette position, le poids des têtes de lecture peut provoquer des erreurs d'écriture ou de lecture. Ensuite vissez correctement le lecteur, en utilisant au minimum quatre vis. Rappelez-vous que pour éjecter une disquette, vous appliquez un effort sur le lecteur lui-même, il serait ennuyez qu'il recule dans le PC.
Il est maintenant nécessaire de brancher le lecteur. ***Deux branchements sont nécessaires, d'une part l'alimentation électrique, d'autre part la nappe du câble de donnée***s. Les lecteurs 5.25" utilisent le gros connecteur électrique, alors que les 3.5" utilisent le petit. Vous trouverez facilement dans le commerce des adaptateurs si aucune prise du type requis n'est disponible.
Il existe deux types de connecteurs de données, le connecteur plat, en cours d'abandon et le connecteur à 34 pins. Le connecteur plat, généralement utilisé pour les lecteurs 5.25", dispose d'un détrompeur, le second pas forcément. Il faut savoir que le fil rouge de la nappe de câbles correspond à la pin 0 ou 1 du connecteur. Cette numérotation est presque toujours imprimée sur le circuit imprimé du lecteur de disquette. Dans le cas où cela ne serait pas spécifié, vous avez la possibilité de tâtonner. En effet, un connecteur branché à l'envers ne risque pas d'endommager le lecteur. Par contre, ne laissez aucun disquette à l'intérieur de celui-ci, elle risque d'être formatée de force, protection contre l'écriture ou pas. Si le connecteur est à l'envers, la LED du lecteur va rester allumée en permanence, ou au contraire, ne va pas s'allumer du tout.
Le câble de données se compose d'une natte de câble et de trois ou cinq connecteurs. Le premier, obligatoirement à pins, se place sur le contrôleur, sur le connecteur à 34 pins. Les autres connecteurs, s'ils sont au nombre de quatre, se gèrent par groupe de 2. ***Les 2 extrémités, situées après les fils croisés, représentent le lecteur A***. Il y a ainsi un connecteur plat et un connecteur à pins. Un seul des deux peut être utilisé, en fonction du lecteur que l'on possède. ***Les deux autres connecteurs représentent le lecteur B***. Sur les câbles récents, il n'est pas rare que les connecteurs plats soient purement et simplement supprimés. On trouve dans le commerce des adaptateurs pour lier un connecteur plat à une prise à pins. Pensez toujours au fil rouge qui doit absolument être lié à la pin n°0 ou 1.
Il arrive, sur certaines machines, que le câble n'ait pas de fils croisés. En ce cas, les lecteurs sont déclarés Master (A:) et Slave (B:). Cette opération s'effectue à l'aide de jumpers directement sur le lecteur. Il peut exister des modèles à 2 ou à 4 positions, ce dernier permettant de mettre jusqu'à quatre lecteurs. Ces jumpers portent l'appellation DS suivi d'un numéro. Le premier numéro correspond au premier lecteur, ainsi DS0 désigne le lecteur A.

Formatage d'une disquette

Il faut avant tout savoir que les capacités indiquées sur les boîtes de disquettes ne sont pas toujours réelles. Ainsi de nombreux fabricants indiquent 2Mo sur des disquettes de 1.44Mo en réalité. La valeur qu'ils indiquent est juste si l'on ne tient pas compte du système d'exploitation. En effet, un Macintosh utilisera une capacité de 1.6Mo sur cette même disquette. Lorsque vous devez formater une disquette, il convient de contrôler si votre lecteur de disquettes est compatible avec la disquette insérée. Ainsi de nombreux lecteurs 1.2Mo 5.25" endommagent les disquettes de 360ko. Cela est lié à une vitesse de rotation différente. Dans les autres cas, il suffit d'utiliser la commande Dos FORMAT. Elle dispose de deux syntaxes adaptées à la situation :
FORMAT d: /N:9 /T:40 ou FORMAT d: /F:360
d: nom du lecteur N: nombre de secteurs/piste T: nbr de pistes F: capacité
IL FAUT TOUJOURS FORMATER UNE DISQUETTE AVANT L'UTILISER

Manipulation de la disquette

La manipulation des disquettes doit suivre certaines règles très strictes. Si cela n'est pas fait, le risque de perdre des données est grand. Dans chaque boîte de disquette, on trouve un petit mode d'emploi illustré qui résume parfaitement les diverses choses à ne pas faire.

- ***Ne jamais approcher une disquette d'une source magnétique*** (aimant, ...). Les données sont elles-mêmes inscrites sur la disquette sous forme magnétique.
- ***Ne jamais laisser une disquette dans des conditions de température difficiles.*** En effet, elle pourrait gondoler, avoir de la condensation.

- ***Toujours remettre une disquette à l'abri après l'usage (étui, boîte, ..).*** Et surtout prendre garde à la poussière***, ne jamais toucher le disque lui-même***.
- ***Ne jamais plier une disquette*** ou la poser dans un endroit où cela pourrait être fait involontairement. Le risque existe aussi sur une disquette 3.5", la partie métallique pourrait être faussée.

Disque Dur (généralité)

Le disque dur est la mémoire de masse la plus répandue dans les PC depuis plusieurs années. Son fonctionnement est très proche de celui d'un lecteur de disquette. En effet, on y retrouve les principaux composants (têtes de lecture, moteur, ...). Afin de proposer une capacité nettement accrue, un certain nombre de points ont étés revus. En premier lieu, ***le disque est hermétiquement fermé dans le but d'empêcher toute saleté de gêner la lecture.*** Ensuite, ***les plateaux sont rigides***, d'où le nom de ce composant. ***Un cache est souvent intégré afin d'augmenter les performances générales du disque.*** L'offre actuelle diffère sur différents points: ***la capacité totale du disque, l'interface (IDE, SCSI,IEEE1394 ...***), ***le format et enfin les performances***.

Montage du disque dur

- ***Le montage d'un disque dur est extrêmement facile***.
- Avant tout, ***configurez le disque dur selon sa fonction, Master, Slave ou ID SCSI.***
- ***Trouvez un emplacement libre au format correspondant, généralement 3.5".***
- Placez ensuite le disque correctement et vissez-le à l'aide d'au moins quatre vis.
- Attention, si un disque peut être monté horizontalement ou sur la tranche, ne le montez jamais à l'envers (circuit imprimé vers le haut.). En effet, dans cette position, les têtes de lecture se rapprochent beaucoup trop des plateaux et un crash disque peut se produire suite à un faible choc.
- ***Reliez enfin les différents connecteurs, soit le connecteur de données et le connecteur électrique.***
- Dans le cas d'un disque externe, la connexion pourra s'effectuer soit à l'aide d'une interface SCSI ou parallèle.

N'oubliez pas alors de le configurer correctement et de charger les pilotes requis, si nécessaire.

Connectique

Les disques qui utilisent cette technologie ont besoin de connecteurs plats, au nombre de deux. ***Le petit*** connecteur, utilisé pour piloter le disque dur, ***possède 20 fils. Le grand connecteur***, utilisé pour le transfert de données, ***possède quand à lui, 34 fils***. Attention, il est souvent confondu avec un connecteur floppy qui est lui aussi à 34 fils. ***Le câble de contrôle est commun aux deux disques durs, alors que le câble de données est propre à chaque lecteur.*** Il faudra donc ne pas croiser les fils lors du montage, la carte contrôleur possédant trois connecteurs. Certains contrôleurs, plus anciens, disposaient d'un connecteur de contrôle par disque dur
Une fois le disque en place, il est encore nécessaire de le définir correctement dans le Bios. ***La première étape consiste à spécifier sa géométrie, soit le nombre de têtes, pistes et secteurs par pistes.*** Tout cela permettra au PC d'en calculer la capacité. ***La plupart des Bios récents disposent d'un mode AUTO qui permet de détecter la géométrie du disque au boot***. S'il a l'inconvénient de ralentir la procédure de démarrage, cela s'avère extrêmement pratique avec les disques amovibles

Smart : un auto diagnostic pour prévenir les pannes des disques durs

Les micro-ordinateurs de Compaq, IBM et HP peuvent aujourd'hui prédire le crash de leur disque dur. Grâce au système Smart. Le procédé n'est ni infaillible, ni standardisé, mais il constitue un gage de sécurité évident. Sans pour autant supprimer la mise en place d'une solution de sauvegarde.
Près de la moitié des pannes de nos disques durs peuvent être prédite. Grâce à la technologie Smart, aujourd'hui adoptée par les plus grand constructeurs. Un disque dur Smart est capable de s'auto diagnostiquer. ***Ce système , self-monitoring, analysis and reporting technology, part d'une idée simple. Il exploite des mécanismes déjà existants : les processus d'auto correction, intégrés, comme lui-même, au « firmware .***
Les fabricants connaissent tous les types de pannes des disque durs. Certaines, d'origine électronique, sont brusques et, de ce fait, imprévisibles. A l'inverse, ***les pannes mécaniques peuvent être anticipées.*** Elles proviennent d'une détérioration graduelle, dont les symptômes nous sont familiers : lenteur au démarrage ou erreurs de lecture, par exemple. ***Quand un disque dur rencontre ce type de problèmes, des mécanismes d'auto correction se mettent alors en branle.***
Smart surveille ainsi une dizaine d'éléments du disque susceptibles de défaillances. Appelés attributs en langage Smart, ils sont cotés de 100 (état neuf) à zéro. Smart diminue leur valeur proportionnellement à la gravité et à la fréquence de leurs défaillances. Quand la cote de l'un d'eux atteint une valeur seuil, fixée par le fabricant, Smart émet une alerte.

Le système révèle ici ses deux faiblesses principales.
D'abord, ce sont les fabricants de disques durs qui choisissent les attributs ainsi que leur valeur seuil. Ce qui interdit toute standardisation. Deux disques durs 3,5 ″ à trois plateaux, l'un Quantum l'autre Seagate , arborant tous deux le logo Smart, surveillent paramètres différents, étalonnés différemment. D'après ses fabricants, sélectionner tout cela par eux - même accroît la pertinence du système. Pour les constructeurs de PC, clients de plusieurs fabricants de disques, cela n'a aucune incidence sur la diligence avec laquelle le disque prévient l'utilisateur. En l'absence de tests, on s'en remettra à leur jugement.
Second point faible, Smart ne fait qu'émettre une alerte. Quasiment tous les PC sont commercialisés aujourd'hui avec des disques Smart, y compris les portables, dont les disques sont particulièrement exposés aux chocs. Mais, faute d'une infrastructure logicielle pour relayer leur alarme, un grand nombre de ces disques crieront demain dans le vide. « Le soft doit être quelque part, dans le BIOS, l'OS ou ailleurs. Or aujourd'hui, il est plutôt…nulle part », déplore-t-on chez Quantum. Ainsi les systèmes d'exploitation, comme Windows, OS/2 ou Net Smart eux même. Ils se contentent de laisser passer l'alerte.
Deux constructeurs ont pris les devants. IBM et Compaq ont développé des outils pour prévenir l'utilisateur (respectivement Prédictive failure analisis et intellis-Safe) et l'administrateur réseau (via IBM NetFinity et Compaq Insight Manager). Hewlett Packard apporte une réponse plus ouverte avec ses derniers Vectra : Norton smart Doctor (NSD).
Symantec esquisse avec ce logiciel minimaliste un début de « solution universelle «. Norton Smart Doctor se charge au démarrage du PC puis réside en mémoire. Il n'a qu'une fonction : se manifester 72 heures environ avant la mort du disque dur, par un message laconique encourageant l'utilisateur a effectué une sauvegarde.
Mais ce n'est qu'un début. NSD n'existe que pour Windows 95 (bientôt NT 4.0) et est uniquement vendu en OEM. De plus, il ignore le réseau; un logiciel résident, conforme à la norme DMI, devra prévenir l'administrateur. C'est toutefois un début prometteur, auquel s'intéressent Acer, Dell, Digital ou encore NEC.
Aux responsables informatiques de réclamer des solutions matérielles et logicielles Smart pour accélérer ce mouvement. Associé à une sauvegarde régulière, il peut, constituer une alternative économique à un système Raid pour un serveur d'entrée de gamme.

Lecteur CD

Le CD-ROM (Compact Disk - Read Only Memory) n'est autre qu'un disque compact audio amélioré, utilisable en lecture seule. Sa capacité usuelle est de ***650Mo,*** ce qui en fait une mémoire de masse conséquente, idéale pour des applications multimédias, tel que les encyclopédies. Le CD pèchent surtout par un temps d'accès trop lent pour certaines applications nécessitant beaucoup d'accès disque. Au fil du temps, le débit a augmenté de manière conséquente, ce qui le place au niveau d'un mauvais disque dur. Désormais vous pouvez trouver dans le commerce des CD inscriptibles (CD-R), réinscriptibles (CD-RW) et même des supports de plus grande capacité (DVD). Tous ces éléments sont décrits dans une autre page
Les lecteurs CD-Rom utilisent un faisceau laser pour lire les données inscrites sur le disque. Ainsi, les données ne sont pas lues par un procédé magnétique, comme les disques durs, mais plutôt par un procédé optique. Ce système est d'ailleurs bien plus proche de nos regrettés disques vinyle (regretté..., enfin pas ceux de Chantal Goya).
Au centre du disque est placée une surface réfléchissante, qui lui donne cet aspect si caractéristique. Une couche de résine, comportant des variations sur sa surface extérieure, la recouvre. On ne peut pas parler ici de sillons, mais plutôt de "trous". ***Le tout étant recouvert d'un film plastifié qui protège ces creux, évitant ainsi que des impuretés s'y logent. Le faisceau laser va frapper la surface du disque. Si aucun trou n'est rencontré, le faisceau est réfléchi par la surface métallisée, puis guidé par un jeu de prismes jusqu'à un capteur photosensible. Par contre, si un trou est rencontré, il va dévier le rayon laser qui ne pourra être réfléchi correctement. Le capteur photosensible ne recevra alors aucun signal. Ces deux états permettent ainsi un stockage d'informations binaires. Ces dernières sont ensuite envoyées au processeur qui les traite comme des données provenant d'une mémoire quelconque.***
Le laser proprement dit est un élément fixe qui ne se déplace pas le long du disque. En effet, il se contente d'émettre un faisceau qui est redirigé et concentré par une lentille en un point précis du CD. Cette lentille, ainsi que les prismes nécessaires à la lecture, sont placés sur un chariot mobile. Ce dernier parcours de manière linéaire la moitié de la diagonale du CD***. Dans la plupart des lecteurs CD, ces éléments ne sont pas accessibles, seul le support (tiroir) sort du lecteur.*** Par contre, la lentille peut être éjectée avec le tiroir sur certains lecteurs de très petite taille, pour les portables par exemple. En ce cas, ne la touchez jamais, si elle devait être sale ou pire encore désaxée, de graves erreurs de lecture s'ensuivraient.
Un des facteurs déterminant lors de l'achat d'un lecteur CD-ROM est sa vitesse. Le premier lecteur simple vitesse, possédaient un débit et un temps d'accès identique à un CD audio. Cette vitesse est nettement insuffisante pour une utilisation dans le domaine informatique. On trouve désormais des lecteurs: simple, double, triple, quadruple et …tuple vitesse. Les temps d'accès n'ont guère augmenté, alors que les débits sont nettement supérieurs. Un lecteur quadruple vitesse offre déjà des performances proches d'un mauvais disque dur.

CONNECTIQUE

La face arrière d'un lecteur CD comporte de nombreux connecteurs. On peut les répartir en trois catégories distinctes: ***l'interface de données, l'interface audio et le connecteur électrique.*** Ce dernier est un modèle à quatre broches, traité dans les pages relatives à l'alimentation électrique.
Les connecteurs audio sont plus ou moins standardisés. On trouve généralement une prise Jack sur la face avant du lecteur. Celle-ci pourra être utilisée pour y connecter un casque audio ou des haut-parleurs. ***La prise à quatre broches située sur la face arrière sert à lier la sortie son du lecteur à une carte son.*** Un câble prévu à cet effet est généralement fourni avec le lecteur. Si malgré un branchement correct sur un vieux lecteur (1x à 4x), aucun son n'est émis par la carte son, vous avez la chance d'avoir une interface son semi-propriétaire. Pas de panique, il suffit de réagencer les fils, généralement en les croisant par paires, pour que tout fonctionne correctement. Si vous utilisez des haut-parleurs directement connectés sur le lecteur, ne soyez pas étonnés par la qualité médiocre du son. En effet, l'amplificateur monté sur le lecteur est de qualité plus que discutable. Vous devrez pousser au maximum le volume, attrapant au passage tous les bruits internes du PC (moteur rotatif du disque dur, ...). Envisagez plutôt d'acquérir une carte son, le résultat en vaut la peine.

Les commandes

La face avant d'un lecteur CD proposent différents boutons de commande. Le plus important est celui permettant l'éjection du CD proprement dit. Si vous possédez un lecteur équipé d'un tiroir, veillez à ce qu'il ne rencontre pas d'obstacles. En effet, le moteur du tiroir pourrait être endommagé. Certains d'entre eux peuvent être fermés en poussant simplement le tiroir, mais attention, pas tous. Certains systèmes d'exploitation, tel Windows 95, permettent une éjection logicielle du CD. Les autres boutons permettent principalement de piloter les CD audio, il s'agit de pause, piste suivante, piste précédente. Certains lecteurs proposent même un affichage digital permettant de connaître la chanson traitée.

Les drivers

A l'inverse des disques durs, les lecteurs CD doivent être gérés par un pilote logiciel (driver), quelle que soit l'interface utilisée. Sous Dos, ce pilote se compose de deux fichiers: un fichier possédant l'extension SYS, fourni par le constructeur et le fichier MSCDEX.EXE fourni avec le Dos***. Le fichier SYS est propre à chaque CD et doit être placé dans le fichier CONFIG.SYS***. La syntaxe utilisée est généralement la suivante :

DEVICE=C:\DRIVERS\MTMIDE.SYS /D:CD01

La commande Device pourra être remplacée par DeviceHigh si un gestionnaire de mémoire est actif. Le paramètre /D: permet de donner un nom au lecteur CD, qui sera repris par MSCDEX. Ainsi, si plus d'un CD est installé sur votre PC, il faudra définir une ligne de commande pour chacun d'entre eux, même s'il s'agit de modèles identiques.
Le fichier MSCDEX.EXE doit être placé dans le fichier AUTOEXEC.BAT en utilisant la syntaxe suivante :
C:\DOS\MSCDEX.EXE /D:CD01 /L:F /X /S /M:64

Quoi après assemblage du pc??

il faut tout d'abord être sure d'isoler le dessous de la carte mère de la carcasse de la tour, en fixant les petits plots en plastique en dessous
Dans les cartes mères récentes ce n'est pas nécessaire de flasher le bios après assemblage mais on peut le faire après installation du SE

Installation du système d'exploitation

Pour cela il faut tout d'abord savoir lesquels parmi les SE existant peuvent être installés sur ce pc
En fait chaque système d'exploitation a une configuration minimale … (voir power point) et en plus que ça vérifier si le produit à une clé de licence.
Ensuite il faut régler le bios a ce qu'il boot avec le lecteur CD ou DVD selon le matériel présent.
Insérer le CD et redémarrer.
Exemple **Installation de Windows Vista: (DVD)** **voir power pointe**
A l'invite **«Appuyez sur n'importe quelle touche pour démarrer du CD-Rom ou DVD Rom »,** frappez une touche du clavier.

Patientez le temps du chargement des fichiers en mémoire. **(Windows is loading Files**)
1) Choisissez la langue de **Vista**
2) Cliquez sur **Installer**.
3) Saisissez votre clé-produit et cochez la case **Activer automatiquement Windows quand je serai en ligne**.
Remarque: La saisie de la clé-produit n'est pas obligatoire mais si aucune clé-produit n'est renseignée, **Vista** sera installée en version d'évaluation et cessera de fonctionner au bout de 30 jours d'utilisation.
Si malgré tout vous voulez tester **Vista** avant de l'installer définitivement, vous pouvez renseigner la clé-produit et activer **Vista** (avant la fin de la période d'évaluation) à partir du **Panneau de Configuration/Système**.
4) Patientez le temps que les termes du **Contrat de Licence** s'affichent.
Cochez la case **J'accepte les termes du contrat de licence** puis cliquez sur **Suivant**.
5) Choisissez le type d'installation.
Dans notre cas : **Installation Personnalisée**.
6) Choisissez la partition sur laquelle vous désirez installer **Vista**. Si la partition choisie est vierge (1ère installation), vous pouvez cliquer sur **Suivant**.
Dans le cas contraire, cliquez sur le **Options de Lecteurs (Avancées)** pour avoir accès aux fonctions de **Formatage**, **Création** et **Suppression** de partitions.
Remarque:
Si vous réinstallez **Vista** sans formater la partition qui accueillait l'ancienne version, le programme va effectuer une sauvegarde de la précédente installation dans un répertoire de la forme **Windows.00N**.
7) L'installation démarre.
On peut suivre sa progression grâce à la petite barre verte en bas de l'écran.
Soyez patient! Selon votre quantité de mémoire vive, il peut vous sembler que le programme d'installation s'est arrêté. Ce n'est pas le cas.
8) Premier redémarrage du PC.
Il vous est demandé une nouvelle fois de patienter.
9) Retour à l'interface du programme d'installation.
10) Affichage d'un écran noir (plus ou moins long) suivi d'un redémarrage du PC
11) Il vous est demandé de saisir un **Nom d'utilisateur** et éventuellement un **mot de passe** (conseillé pour des raisons de sécurité).
12) Entrez un nom d'ordinateur ou laissez celui proposé par défaut.
Choisissez un fond d'écran pour votre bureau parmi ceux proposés. (Ce fond d'écran sera bien sûr modifiable, par la suite, dans le **Panneau de configuration**).
13) Saisie des paramètres de mise à jour de **Windows Vista**.
Pour que votre ordinateur soit le moins possible exposé aux attaques virales, il est fortement conseillé d'appliquer les correctifs de sécurité dès qu'ils sont disponibles sur le site de **Microsoft**.
Choisissez **Utiliser les paramètres recommandés** pour activer la **mise à jour automatique**
14) Une nouvelle fois, il vous est demandé de patienter, le temps que Windows calcule l'indice de performance de votre ordinateur.

la maintenance

BASES DU DEPANNAGE

Qu'est-ce que dépanner ?

Un bon dépannage utilise des techniques éprouvées pour diagnostiquer et ensuite réparer les problèmes informatiques. La découpe logique du processus de dépannage en étapes le rend plus efficace.
Le processus de dépannage démarre avec l'identification du problème. Des informations doivent ensuite être rassemblées pour définir les causes. Ensuite, une solution est développée et mise en place. Enfin, on vérifie que la solution a fonctionné. Si le problème est résolu, le processus de dépannage se termine avec la documentation de la solution. Si le problème n'est pas résolu, le processus redémarre jusqu'à ce qu'une solution soit trouvée. Chaque étape est détaillée dans les chapitres suivants.

Identifier le problème

Dans cette étape, le problème est identifié. Pour cela, il faut analyser les symptômes, de façon à déterminer les causes possibles. Le résultat est un bilan détaillé qui décrit clairement le problème. Sans une bonne compréhension du problème, le technicien ne peut pas rassembler les bonnes informations pour développer une solution adéquate.

Collecter les informations

Une fois que le problème a été identifié, la prochaine étape est de collecter les informations pour qu'une solution puisse être développée. Un dépannage rapide et efficace implique la collecte d'informations fiables afin de trouver une solution adéquate. Les problèmes informatiques peuvent varier du simple au très complexe. Le problème peut devenir très compliqué si le technicien n'a pas la bonne information.
Aujourd'hui, les techniciens ont de nombreux outils disponibles pour les aider à diagnostiquer le problème. Ils peuvent utiliser des multimètres digitaux (DMM), des outils logiciels de diagnostic, et obtenir des informations de l'utilisateur final. Les techniciens peuvent aussi inspecter visuellement les systèmes à la recherche d'un composant cassé et guetter les symptômes d'un problème.
L'utilisateur final peut fournir des informations sur le fonctionnement antérieur du système. Le technicien peut ainsi connaître les changements effectués par l'utilisateur susceptibles de perturber le système. L'utilisateur peut aussi renseigner le technicien sur les modifications du système, les erreurs survenues ou la baisse de performance qui a conduit au problème.
Le technicien a besoin de savoir comment interroger efficacement l'utilisateur final. La liste ci-dessous comprend les questions classiques à poser :
L'erreur peut-elle être décrite? Ecrire la description du problème..
Y a t'il un message d'erreur? Les ordinateurs comprennent des outils d'autodiagnostic. Si l'un des auto-tests échoue, un message d'erreur est généré.
Demander à l'utilisateur final de se rappeler le message d'erreur ou recréer le. Dans le cas d'une erreur au POST (Power On Self Test), demander au client le nombre de bips entendus.
Le problème ou l'erreur se sont-ils déjà produits? Essayer d'établir un historique de l'évènement. Celui-ci peut permettre d'identifier les causes de l'évènement. Si le problème s'est produit auparavant, consulter les changements survenus précédemment.
Y a t il eu des changements récents sur le matériel ou le logiciel? Des modifications sensées corriger un problème précédent peuvent être la cause du problème actuel. L'ajout d'un matériel ou d'un logiciel peut créer des problèmes imprévus avec les ressources système.
NOTE : Rappelez-vous d'aborder l'utilisateur poliment et respectueusement. Quelques utilisateurs peuvent refuser d'admettre leurs erreurs. Un vrai professionnel établit la confiance afin que l'utilisateur se confie plus facilement.
L'erreur peut-elle être reproduite? Reproduire le problème aidera l'utilisateur final dans la description exacte de l'erreur. Le technicien sur site pourra donc constater de visu le problème.
Attention : Ne tentez pas de reproduire l'erreur s'il y a un risque de détérioration des composants. Ne tentez pas de reproduire un problème tel qu'un amorçage sur une alimentation.
Après avoir répondu aux questions et vérifié les réponses, le problème devra être caractérisé comme ***logiciel*** ou ***matériel***. Le problème pourra être circonscrit à un élément spécifique ou une partie du système. Une fois le problème caractérisé et circonscrit, le technicien peut ensuite développer une solution comme indiquée dans la section suivante.
Résolution des problèmes de serveur réseau :
Il y a quelques questions classiques concernant les problèmes de serveur réseau :

Jusqu'à quelle heure le serveur fonctionnait-il?
Qu'y a-t-il eu de changé avant?
Quel matériel a été récemment ajouté sur le serveur?
Quel logiciel a été récemment installé?
Qui a découvert le problème?
Où est le journal du serveur?
Comment la défaillance du serveur affecte-t-elle le fonctionnement de l'entreprise?

Utiliser vos sens pour répondre à ces questions :
La température de la salle serveur est-elle trop élevée?
Le taux d'humidité dépasse-t-il le taux maximum admissible des équipements?
Y a t il une odeur de brûlé?
Y a t il de la fumée?
Les alarmes du serveur ou de l'onduleur sonnent-elles?
Les leds des disques durs clignotent-elles?
La surface d'un des équipements réseaux est-elle chaude au toucher?
Les cordons d'alimentation sont-ils tous connectés?
Les câbles réseaux sont-ils déconnectés?
Les câbles SCSI sont-ils correctement connectés?
L'utilisation des sens est une technique classique de dépannage.
Les outils, tant matériels que logiciels, sont également importants dans cette optique.

Développer une solution

Créer une solution est la troisième étape du processus de dépannage. Le technicien évalue les données recueillies. Le technicien utilise ***l'expérience***, ***la logique***, ***le raisonnement*** et ***le bon sens*** pour développer une solution. Quelquefois, le diagnostic initial est faux, et la stratégie doit être revue
NOTE : le dépannage est une compétence acquise qui s'améliore avec le temps et l'expérience.

Mise en place de la solution

La quatrième étape dans le processus de dépannage est la mise en place de la solution. C'est essentiellement l'étape où le technicien travaille sur l'ordinateur. Le technicien essaie sa solution en manipulant des composants de l'ordinateur, qui peuvent être matériels ou logiciels. Un certain nombre d'éléments sont à prendre en compte dans la mise en place d'une solution :

- ***Toujours récupérer les données importantes avant d'effectuer tout changement pouvant endommager les données stockées dans l'ordinateur.***
- ***Toujours démarrer avec des choses simples.***
- ***Ne changer qu'une chose à la fois mais contrôler deux fois l'effet sur l'ordinateur.***
- Annuler tout changement faisant empirer le problème ou endommager davantage le système.

Le problème est-il résolu ?

Vérifier la résolution effective du problème est la 5e étape du processus de dépannage. Après la mise en place de la solution, le technicien est responsable et doit vérifier que le système fonctionne correctement. Le technicien peut effectuer des tests, contrôler visuellement, et vérifier que le système fonctionne normalement. Ensuite, le technicien doit solliciter l'utilisateur final afin de s'assurer de sa satisfaction.
Si le système fonctionne correctement, alors le processus de dépannage se termine normalement. Si le système ne fonctionne pas correctement, le technicien devra annuler tous les changements faits sur le système, et recommencer le processus de dépannage depuis le début. Si le technicien a besoin de plus d'information, le technicien devra retourner à l'étape d'identification du problème (***étape 1***).

Enregistrer le problème et la solution

Faire un document est l'étape finale du processus de dépannage. Il est important de toujours garder une trace de tous les changements introduits dans le système, en tant que résolution d'un problème. Cet enregistrement peut être le point de départ du dépannage des prochains problèmes. L'enregistrement peut également permettre l'élimination d'une catégorie entière de problèmes.

Enregistrer au fur et à mesure permet de suivre tous les changements ou modifications faits sur le système. Les prochains problèmes pourront être réparés plus facilement par un autre technicien. Le suivi des réparations est un outil inestimable de diagnostic et renseigne le technicien sur l'état de la machine.

LOGICIELS DE DIAGNOSTIC

Il existe de nombreux logiciels commerciaux disponibles comme aides à la réparation. Ces produits, connus comme logiciels de diagnostic, aident aussi à prévenir les pannes du système. Quelques-uns des programmes les plus connus sont inclus dans la liste suivante :

- **SpinRite** – http://grc.com/default.htm
- **Checkit** – http://www.hallogram.com/
- **PC Technician** – http://www.windsortech.com/
- **AMI Diags** – http://www.ami.com/
- **SiSoft Sandra (freeware)** – http://www.3bsoftware.com/

SpinRite : SpinRite est un programme de récupération des données à partir d'un disque dur défaillant. SpinRite est un programme indépendant qui est capable de se lancer sans le DOS. C'est un logiciel reconnu pour sa capacité à régler des problèmes difficiles. SpinRite peut aussi empêcher les pannes de disque dur. S'il est chargé avant une panne, il peut prévenir les utilisateurs d'un problème potentiel, et peut empêcher une défaillance en isolant les zones à problèmes. Les mauvaises zones sont repérées comme défaillantes. Si une zone est défaillante, elle ne peut pas être utilisée pour lire ou écrire des données.
Checkit : Checkit effectue des analyses du système et des tests. Il peut fournir au technicien des rapports sur la performance des composants matériels. Checkit peut effectuer des tests de bouclage en utilisant des bouchons. Il peut aussi vérifier le bon fonctionnement du CPU, des slots PCI, du DMA, du CMOS, du cache, du clavier et les premiers 64 mégaoctets de la RAM vidéo.
PC Technician : PC Technicien est un outil de diagnostic indépendant du DOS. PC Technicien peut effectuer des tests sur les ports parallèles, ports série, disque dur, le clavier, les cartes vidéo et la RAM.
AMI Diags : AMI Diags effectue des tests approfondis du système. AMI Diags peut fournir des rapports sur la mémoire, les ports série, les ports parallèles, les modems, les disques durs, le clavier, le BIOS, et les adaptateurs vidéo.
SiSoft Sandra : Sandra (analyseur de système, assistant de rapport et de diagnostic) est un programme libre qui fournit un ensemble d'outils diagnostic, qui peut aider au dépannage et à la mesure de performance. Sandra peut tester la performance des CPU, du modem, de la carte vidéo, de la mémoire, du BIOS et des disques durs

MAINTENANCE PREVENTIVE

Calque de l'anglais *preventive maintenance*, l'expression **maintenance préventive** désigne le remplacement, la révision, ou la réfection d'un élément matériel avant que celui-ci n'entraîne une avarie.

La définition donnée par l'AFNOR est la suivante : « Maintenance exécutée à des intervalles prédéterminés ou selon des critères prescrits et destinée à réduire la probabilité de défaillance ou la dégradation du fonctionnement d'un bien » (extrait norme NF EN 13306 X 60-319).

On peut subdiviser la maintenance préventive en quatre types :

- la **maintenance systématique** (angl. *scheduled maintenance*), maintenance obéissant à un échéancier (angl. *schedule*) établi en fonction du temps et du nombre d'unités d'exploitation;

Définition de la norme européenne : « Maintenance préventive exécutée à des intervalles de temps préétablis ou selon un nombre défini d'unités d'usage mais sans contrôle préalable de l'état du bien » (extrait norme NF EN 13306 X 60-319).

- La **maintenance programmée** (angl. *planned maintenance*), maintenance obéissant à un programme;

Définition de la norme européenne : « Maintenance préventive exécutée selon un calendrier préétabli ou selon un nombre défini d'unités d'usage» (extrait norme NF EN 13306 X 60-319).

- la **maintenance conditionnelle** (calque de l'anglais *conditional maintenance*), maintenance subordonnée à l'apparition d'indices révélateurs de l'état (angl. *condition*) d'un élément matériel. Consacrée par l'usage, cette expression est une traduction fautive, l'anglais *conditional* signifiant ici non pas « conditionnel » (au sens de

soumis à des conditions) mais « reposant sur l'état » du matériel (comme dans l'expression anglaise équivalente *condition-based maintenance*);

Définition de la norme européenne : « Maintenance préventive basée sur une surveillance du fonctionnement du bien et/ou des paramètres significatifs de ce fonctionnement intégrant les actions qui en découlent » (extrait norme NF EN 13306 X 60-319).

- la **maintenance prévisionnelle** (angl. *predictive maintenance*), maintenance partant de la surveillance de l'état du matériel et de la conduite d'analyses périodiques pour déterminer l'évolution de la dégradation du matériel et la période d'intervention. Le calque « maintenance prédictive » est à éviter car il n'y a pas lecture dans le marc de café.

Définition de la norme européenne : « Maintenance conditionnelle exécutée en suivant les prévisions extrapolées de l'analyse et de l'évaluation de paramètres significatifs de la dégradation du bien » (extrait norme NF EN 13306 X 60-319).

Généralités

Décharge électrostatique (ESD)

L'électricité statique est la concentration de charges électriques restant à la surface. Cette concentration peut bombarder quelque chose et l'endommager. Un tel bombardement est appelé une décharge électrostatique (ESD). L'électricité statique est le pire ennemi des fragiles composants d'un système informatique. C'est pourquoi il en sera question dans presque tous les modules de ce cours.
Au moins 3000 volts doivent être présents avant qu'une personne ne ressente une décharge. Si la décharge provoque une douleur ou fait du bruit, le voltage se situe probablement aux alentours de 10000 volts. La plupart des composants électroniques des ordinateurs fonctionnent avec moins de 5 volts. Un composant peut être endommagé avec moins de 3000 volts d'électricité statique.

Sacs antistatiques

Des matériaux d'emballage spéciaux sont utilisés pour les composants et cartes électroniques. Ces matériaux d'emballage sont composés de plastiques moulés spéciaux ou polystyrène pour les composants, et de sacs antistatiques pour les cartes. Ne pas enlever le composant de son emballage spécial avant qu'il ne soit prêt à être installé. Un sac antistatique peut être utilisé pour stocker temporairement des pièces et des composants, quand on démonte un ordinateur pour le nettoyer ou lors d'autres actions de maintenance préventive.

Bracelets antistatiques

Quand on travaille sur un ordinateur ou sur des composants individuels, un outil permet de réduire le risque d'ESD. Un bracelet antistatique, permet à l'électricité statique de s'évacuer ailleurs que sur un composant informatique sensible.

Avertissement : Un bracelet antistatique ne doit pas être porté lors du travail sur équipement à voltage élevé, tel que l'alimentation ou le moniteur CRT. Ces composants ne doivent être réparés que par un professionnel certifié. Le voltage et l'ampérage élevés dans les condensateurs pourraient se décharger sur le technicien. Une décharge électrique d'un appareil de voltage élevé peut être fatale.

Air comprimé

Deux autres éléments peuvent être utilisés quand on travaille sur un ordinateur : l'air comprimé ou le vaporisateur antistatique. Ces éléments peuvent être utilisés sur les sols, les bureaux, et dans certains cas sur l'équipement lui-même. Bien suivre les instructions de sécurité quand on utilise ces produits.

Etabli à la terre

Pour empêcher l'ESD, il est important de connaître les conditions dans lesquelles elle survient le plus fréquemment. Quand le taux d'humidité est bas, la potentialité d'ESD s'accroît considérablement. Si la température est fraîche ou s'il y a des tapis au sol, la potentialité est également plus élevée.

Un bon espace de travail doit comprendre un revêtement antistatique sur le sol, les établis mis à la terre avec un tapis antistatique, et des bracelets antistatiques. L'espace doit être propre, bien éclairé, et le taux d'humidité doit être maintenu entre 20 et 50%. Si tous ces éléments sont en place, le risque d'ESD sera fortement réduit.

Une fois que le boîtier de l'ordinateur a été ouvert, le technicien doit être au potentiel du boîtier en touchant une partie métallique exposée du boîtier. Si une partie peinte est touchée, cela peut ne pas avoir d'effet. Une fois que l'électricité statique a été déchargée sur le boîtier, relier le bracelet antistatique au boîtier pour prévenir de futures différences de potentiel. Un environnement sans ESD est crucial pour la maintenance préventive avec boîtier ouvert.

Il y a plusieurs choses qui peuvent engendrer les défaillances d'un système informatique. Les plus connues sont la formation de **poussière**, les **températures extrêmes**, et les **mauvaises manipulations**. Plus la poussière ou l'électricité statique seront importantes dans la zone où est placé le PC, plus il faudra le nettoyer souvent.

Si un ordinateur n'est pas régulièrement nettoyé, de la poussière peut se former sur les composants à l'intérieur de l'ordinateur, comme sur le ventilateur ou les circuits imprimés. Un ventilateur encrassé peut s'arrêter et faire chauffer le système. C'est surtout vrai avec les nouveaux CPU. Si le ventilateur du processeur arrête de fonctionner, l'ordinateur sera défaillant ou s'éteindra complètement, et le processeur peut être endommagé.

Pour ces raisons, il est important de garder l'intérieur de l'ordinateur propre. Pour bien nettoyer l'intérieur de l'ordinateur, débrancher l'unité et déplacer la loin d'un autre équipement. Utiliser une bouteille d'air comprimé en s'assurant d'éliminer toute la poussière à l'intérieur du casier. Cette opération devrait être effectuée **au moins une fois par an**, dans les **zones peu poussiéreuses**, et **deux ou trois fois par an** dans les **zones très poussiéreuses**. Cette opération poursuit deux objectifs. En enlevant la poussière, les composants motorisés fonctionneront plus efficacement, pour une période plus longue. De plus, la poussière se formant moins, Les risques relatifs à l'électricité statique seront moindres.

Les températures extrêmes doivent être évitées car elles sont dangereuses pour les ordinateurs. Si un système informatique surchauffe, plusieurs problèmes peuvent survenir, tels qu'un mauvais fonctionnement du système ou une perte des données. Pour empêcher cela, s'assurer que la ventilation du boîtier fonctionne correctement, et que la pièce est à une température modérée.

La dernière chose qui peut endommager un ordinateur est une mauvaise manipulation. Quand on déplace le système, il faut faire attention à ne pas perdre l'un des éléments internes. Si un composant bouge pendant que la machine est à l'arrêt, il pourra être endommagé quand on remettra la machine en marche.

Maintenance préventive pour les périphériques informatiques

Moniteur

L'écran est la pièce la plus visible de l'équipement, il est intéressant de le garder propre à la fois pour son aspect et sa fonctionnalité. Les concepts suivants s'appliquent à la fois sur les types d'écran LCD et CRT.
Quand on nettoie un écran, s'assurer que l'appareil est débranché. Utiliser un tissu humide avec un détergent doux, nettoyer tout l'écran, pour enlever toute formation de poussière. Pour enlever le résidu, prendre un autre tissu humidifié. Etre sûr de ne pas utiliser trop d'eau de façon à éviter les gouttes. Une fois que l'écran a été nettoyé, utiliser un tissu sec pour terminer. Faire attention en nettoyant l'écran du moniteur à ne pas le rayer.
Après avoir nettoyé le moniteur, s'assurer que le câble d'alimentation est rebranché en toute sécurité.
Avertissement : Si du liquide pénètre à l'intérieur de l'écran CRT pendant qu'on le nettoie, il est conseillé de le laisser s'évaporer. Ne jamais ouvrir un écran CRT.

Souris

Il existe deux types de souris : mécanique et optique..
Une souris mécanique peut fonctionner de façon incorrecte si elle devient sale. Quand la poussière s'introduit dans le boîtier de la souris, elle se répand sur les pièces amovibles de la souris. Ceci provoque une accumulation de poussière sur les rouleaux à l'intérieur de la souris. Le moyen le plus rapide de les nettoyer est d'enlever le plateau au bas de la souris, extraire la boule, et ensuite gratter doucement la poussière formée sur les rouleaux avec un ongle, ou un outil faiblement abrasif. Certaines personnes préfèrent utiliser de l'alcool isopropylique ou du méthanol avec un coton-tige.
Une souris optique a besoin d'un tissu humide pour nettoyer la surface du détecteur optique. Cependant, ceci peut engendrer des dommages et ne devra être fait que si c'est vraiment nécessaire. Bien débrancher la souris optique avant de la nettoyer. Les yeux doivent être protégés des émissions du laser

Clavier

Un clavier est l'élément le plus exposé de tous les autres composants du système informatique. La poussière se dépose sur le clavier, avec le temps. Le nettoyage périodique du clavier prolongera sa durée de vie et empêchera les dysfonctionnements. Les touches sur un clavier peuvent être enlevées, ce qui permet d'avoir un accès facile aux zones où la poussière s'est installée. On peut utiliser une brosse douce ou un morceau de coton pour enlever la poussière sous les touches. Utiliser de l'air comprimé pour enlever la poussière sous les touches. Cependant, il est nécessaire de garder le clavier vertical ou dans une position inclinée et souffler des jets d'air pour faire sortir la saleté et la poussière hors du clavier. Cela évitera l'amas de saleté dans les coins et autres endroits inaccessibles sous les touches.

Nettoyage des imprimantes

Les imprimantes ont beaucoup de pièces amovibles à l'intérieur. De ce fait, il y a donc un besoin important de maintenance. Les imprimantes produisent des impuretés qui ont besoin d'être nettoyées. Sinon, elles peuvent causer des dysfonctionnements dans l'imprimante.

Quand on travaille avec des imprimantes matricielles, c'est une bonne idée de nettoyer les rouleaux avec un tissu humide. Bien débrancher le câble d'alimentation avant d'appliquer un tissu humide.

Quand on nettoie une imprimante à jet d'encre, la pièce qui aura le plus besoin d'être nettoyée sera le mécanisme de prise du papier. Avec le temps, des particules de papier se déposent. Elles peuvent être enlevées avec un tissu humide quand l'unité est débranchée.

Les imprimantes laser ont d'habitude une maintenance moindre, sauf si elles se trouvent dans une zone poussièreuse ou sont d'une ancienne génération. Il faut utiliser un aspirateur spécial pour le toner. Si on utilise un appareil domestique, la poudre passera à travers le filtre et polluera encore plus. Il faut débrancher l'imprimante avant le nettoyage à cause des tensions élevées dans ce type d'imprimante.

Prendre en compte les aspects suivants concernant le papier et l'encre utilisés :

- **Choix du papier** : choisir le bon type de papier aidera l'imprimante à durer plus longtemps et imprimer de façon plus efficace. Dans la plupart des magasins de fournisseurs informatiques, différents types de papier sont disponibles. Chaque type de papier est clairement défini selon le type d'imprimante prévu : papier pour jet d'encre, papier pour imprimante laser, etc. Le fabricant de l'imprimante recommande généralement le bon type de papier dans le manuel de l'imprimante.
- **Choix de l'encre** : quand on choisit l'imprimante, il faut consulter le manuel de l'imprimante pour voir quelle marque et quel type d'encre le fabricant d'imprimante recommande. L'imprimante ne fonctionnera pas ou aura des dysfonctionnements en faisant baisser la qualité d'impression, si on installe le mauvais type d'encre. Essayer de remplir à nouveau la cartouche d'encre n'est pas une bonne idée puisque l'encre peut fuir. Toujours acheter les cartouches d'encre recommandées par le vendeur.

Scanners

La chose la plus importante à se rappeler quand on utilise un scanner, est de garder la surface du scanner propre. Si la poussière ou tout autre corps étranger rendent le verre sale, consulter le guide d'utilisateur pour les recommandations de nettoyage. Si le manuel ne fait aucune recommandation, essayer d'utiliser un produit pour nettoyer le verre et un tissu doux de façon à ne pas rayer le verre.
Si l'intérieur du verre devient sale, consulter le manuel pour ouvrir l'unité ou enlever complètement le verre du scanner. Si c'est possible, nettoyer les deux côtés, et les remettre dans le même sens qu'à l'origine dans le scanner

Maintenance préventive logicielle

Il y a différents utilitaires qui sont livrés avec DOS et Windows, qui aident à maintenir l'intégrité du système. S'ils sont utilisés régulièrement, les utilitaires suivants peuvent rendre le système plus rapide et plus efficace :

- **Scandisk** : cet utilitaire est utilisé soit pour vérifier l'intégrité des fichiers et répertoires, ou pour faire un contrôle approfondi du système en recherchant les erreurs physiques sur le disque. Il peut être utilisé sur n'importe quel disque formaté pouvant être lu par le système d'exploitation. Lancer ce programme quand le système n'est pas arrêté correctement ou au moins une fois par mois.

- **Défrag** : quand un programme est installé sur un ordinateur, il peut être stocké dans plus d'un endroit sur le disque dur. Ceci est connu sous le nom de fragmentation. La performance d'un lecteur fragmenté est moins importante que s'il n'est pas fragmenté. L'utilitaire optimise l'espace sur le disque de façon à ce que les programmes s'exécutent plus rapidement. Les techniciens lancent généralement cet utilitaire après l'utilisation de Scandisk.
- **CHKDSK / f** : cette commande est utilisée pour contrôler le système de fichiers et peut être comparé au Scandisk pour Windows 2 000 et XP. CHKDSK est une application DOS qui fonctionne en ligne de commande.
- **REGEDIT** : le Registre est une base de données qui maintient les données de configuration concernant le matériel et l'environnement du PC. REGEDIT est une commande pour les techniciens avancés. L'Editeur du registre fournit l'accès au registre avec une vue d'ensemble identique à l'explorateur Windows. Si quelque chose est changé dans le Registre, des erreurs sur le système ou des dysfonctionnements peuvent en découler. Une attention extrême est conseillée quand on utilise ce programme car il n'est pas possible d'annuler les modifications.

Responsabilités de l'utilisateur

Un utilisateur final d'un ordinateur peut faire plusieurs choses afin d'assurer le bon fonctionnement du système. Les utilitaires du système peuvent être utilisés afin d'améliorer les performances sur les points suivants :

- Gérer les applications
- Gérer les fichiers
- Sauvegarder des travaux

Gérer les applications Quand on installe des applications, utiliser l'utilitaire Ajouter / Supprimer des programmes. Certaines applications peuvent ne pas utiliser de protection à l'installation, et si le programme bloque en plein milieu de l'installation, ceci pourrait altérer le fonctionnement du système. L'utilitaire Ajouter / Supprimer des programmes peut être utilisé pour complètement effacer une application du système.

Gérer les fichiers et les répertoires Le système de gestion des fichiers d'un système d'exploitation est conçu pour stocker les données sous forme d'un arbre hiérarchique. Les disques durs doivent être organisé avec les fichiers de travail et les programmes dans des emplacements différents. Ceci rend les fichiers plus faciles à trouver et à récupérer.

Sauvegarder des travaux Du fait de la possible défaillance du système, les fichiers personnels doivent être sauvegardés régulièrement. Le meilleur moyen de sauvegarder des données est de faire une copie de celles-ci sur un média amovible (floppy disk, CD ou zip drive), et ensuite les stocker dans un endroit loin de l'ordinateur, de préférence dans un bâtiment différent. Si le bâtiment ou la maison brûle et que toutes les données récupérées sont à côté de l'ordinateur, tout est perdu. Ne pas utiliser toujours le même support. Utiliser plusieurs supports et créer de multiples copies des mêmes données, juste au cas où l'une serait défaillante.

Pare-feu

La plupart des personnes commencent à tirer partie de l'accès haut-débit permanent. Les utilisateurs du haut-débit doivent être informés des risques inhérents à la connexion d'un ordinateur au monde extérieur. Une faille de sécurité sur un ordinateur personnel peut permettre à un pirate de dérober des données ou d'utiliser l'ordinateur personnel afin de pirater d'autres ordinateurs.

Plusieurs possibilités s'offrent afin de minimiser les risques précités. Un pare-feu personnel est l'une de celles-là. Les pare-feux représentent la méthode la plus populaire pour protéger les réseaux locaux d'entreprise contre les attaquants externes. Un pare-feu est un système logiciel ou matériel utilisé pour empêcher les personnes non autorisées d'accéder aux données. Un pare-feu personnel est classiquement situé entre la connexion haut-débit et les ordinateurs locaux. Tout le trafic entre ces deux réseaux, qu'il soit composé de données informatiques, voix, ou vidéo est inspecté par le pare-feu. Un pare-feu personnel classique comprend les caractéristiques suivantes :

- Ferme la connexion haut-débit en cas de détection d'une tentative de piratage
- Permet aux différents membres de la famille de définir leurs propres niveaux de sécurité
- Enregistre tous les évènements relatifs à l'accès Internet

Maintenance corrective

Calque de l'expression anglaise *corrective maintenance* (autre traduction, plus conforme à l'esprit du français : « maintenance correctrice »).

La **maintenance corrective** désigne l'élimination d'une avarie ou d'une altération dans le fonctionnement d'un élément matériel (aussi appelé « bien » ou « entité » dans le jargon de la spécialité), par un des divers moyens que sont la réparation, la restauration à l'état antérieur, et le remplacement de l'élément matériel impliqué.

La définition de la norme européenne est la suivante : « Maintenance exécutée après détection d'une panne et destinée à remettre un bien dans un état dans lequel il peut accomplir une fonction requise» (extrait norme NF EN 13306 X 60-319).

Certains auteurs donnent l'expression « maintenance curative » (angl. *curative maintenance*) comme synonyme de « maintenance corrective », alors qu' elle n'est qu'une partie seulement de la maintenance corrective (celle qui se solde par la restauration de l'élément matériel à l'état antérieur), par opposition à une maintenance corrective dite « palliative » (ou, pour parler simplement, un dépannage provisoire). Cette dernière distinction est ignorée des auteurs de langue anglaise.

Une autre distinction opérée dans la maintenance corrective prend pour base le caractère immédiat ou différé de l'intervention, distinguant :

- la maintenance corrective immédiate (anglais : *immediate corrective maintenance*), effectuée tout de suite après la panne;
- la maintenance corrective différée (angl. *differed corrective maintenance*), retardée en fonction de règles de maintenance données

Problèmes d'alimentation

Les composants des ordinateurs sont vulnérables à différentes sortes de fluctuations électriques, et peuvent être endommagés par des décharges électriques. Les ordinateurs peuvent être endommagés ou détruits avec des décharges élevées comme la foudre ou de faibles décharges comme l'électricité statique. Les problèmes électriques pouvant causer des dommages sont répertoriés ci-dessous :

- **Coupures** : les coupures sont la perte complète d'alimentation pour un temps donné. Elles sont d'habitude la conséquence du mauvais temps, comme le vent violent, les éclairs ou les tremblements de terre.
- **Baisse d'intensité ou micro-coupures** : les baisses d'intensité sont une chute de l'alimentation. Une micro-coupure est une baisse d'intensité qui dure moins d'une seconde. Ces incidents apparaissent quand le voltage sur la ligne d'alimentation descend sous les 80 % du voltage normal. Des circuits surchargés peuvent provoquer ces incidents. Des baisses d'intensité peuvent aussi être causées intentionnellement par les fournisseurs d'énergie, cherchant à réduire l'alimentation mise en place par les utilisateurs, durant les périodes où la demande est forte. Les baisses d'intensité ou micro-coupures comptent pour une large part dans les problèmes d'alimentation, qui touchent les réseaux et les appareils informatiques.
- **Bruit** : le bruit est causé par des interférences venant de la radio, des générateurs et des éclairs. Le bruit perturbe l'alimentation, ce qui peut causer des erreurs dans un système informatique.
- **Pointes de tension** : une pointe de tension est une augmentation soudaine du voltage qui devient beaucoup plus élevé que les niveaux normaux. Si l'événement dure de une à deux secondes, on appelle cela une pointe de tension. Ceci est généralement causé par des éclairs, mais peut aussi apparaître lorsque l'alimentation secteur revient après une extinction.
- **Surtensions** : C'est une forte augmentation de voltage au-dessus du flux normal du courant électrique. Une surtension dure plus de 3 nanosecondes (milliardièmes de seconde). Cependant, les suppresseurs de surtension peuvent aider à défendre les composants informatiques contre de tels chocs.

Ayant vu les différents types d'alimentation qui peuvent causer des problèmes aux systèmes informatiques, il sera plus facile d'éviter que ces problèmes n'arrivent. La prochaine section abordera les différents types d'équipement qui peuvent être utilisés pour protéger les équipements contre des problèmes d'alimentation.

Suppresseur de surtensions et alimentations électriques

Trois appareils différents peuvent être utilisés pour protéger les équipements informatiques sensibles, contre certains événements liés à l'alimentation. Ils sont décrits dans les sections suivantes :

Suppresseurs de surtensions Egalement appelés protecteurs, les suppresseurs de surtensions, fonctionnent en dérivant le voltage supplémentaire au sol. Les suppresseurs de surtensions utilisent un composant appelé Varistor Oxide Metal (MOV) pour dévier le survoltage. Une tension de maintien déclenche le MOV. Si la tension est au-dessus du minimum, elle est déviée vers le MOV et évitera les composants informatiques. Cela garantit que le voltage alimentant un appareil reste en dessous d'un certain niveau. Les protecteurs sont majoritairement utilisés pour protéger le matériel des pointes de tension et des surtensions. Les suppresseurs de choc ont généralement un fusible à l'intérieur qui prévient les excès d'intensité. Un suppresseur de surtension est par contre inutile pendant les baisses d'intensité et les micro-coupures.

Fournisseurs d'alimentation en attente (SPS) Un fournisseur d'alimentation en attente (SPS) est équipé d'une batterie, qui alimente les appareils lorsque la tension chute en dessous de son niveau normal. La batterie est en attente durant le fonctionnement normal de l'unité. Quand la tension chute, la batterie fournit du courant continu, à un oscillateur qui le convertit en courant alternatif pour l'ordinateur. Le problème avec cet appareil est le temps qu'il met pour basculer sur la batterie. Si le composant de commutation fait défaut, la batterie ne sera pas capable d'alimenter l'ordinateur.

Fournisseurs d'alimentation ininterrompue (UPS) Un UPS est comparable au SPS. L'UPS utilise l'alimentation de la batterie tout le temps. L'alimentation arrivant dans l'unité recharge les batteries pendant qu'on les utilise. L'alimentation de la batterie est envoyée à un oscillateur, qui envoie le courant alternatif vers l'ordinateur. C'est un appareil qui protège contre les problèmes d'alimentation secteur. Un UPS fournit une alimentation limitée en cas de panne d'alimentation. D'habitude, un UPS fonctionne assez de temps pour sauvegarder et sortir avant que le manque d'alimentation ne stoppe la machine. Un UPS peut aussi protéger contre les baisses d'intensité ou micro-coupures. La raison pour laquelle la plupart des gens choisissent d'avoir un UPS, plutôt qu'un SPS, est le temps de basculement. Un UPS donne un courant constant sans retard.

Surtout, la meilleure solution pour l'alimentation électrique est d'avoir un immeuble correctement connecté à la terre, tout comme une batterie suffisante pour gérer tous les équipements en cas de rupture d'alimentation.

Merci bios

parmi les meilleures moyens qui nous aident a detecter les pannes c'est le bios :

Un programme de test du matériel le POST[1] est exécuté à chaque mise sous tension. S'il détecte un mauvais fonctionnement d'un des sous-ensembles de l'ordinateur il le signalera par l'émission de bips sonores où par l'affichage d'un message lorsque cela est possible.

Avant que la carte vidéo soit testée, configurée donc utilisable, le BIOS signale les erreurs par l'émission de BIP sonores (voir tableaux suivants) ainsi que par l'envoi d'un code vers le port E/S dont l'adresse est 80_H, ce port est présent sur des cartes de dépannage. Ces cartes affichent le code sur des afficheurs 7 segments. Ce type de cartes étaient très utiles pour déterminer le composant en panne sur les anciennes cartes mères, à l'heure actuelle la quasi totalité des fonctions d'une carte mères sont intégrées sur un ou deux chipsets.

BIOS AMI		
Nbre de bips	**Signification**	**Remède(s)**
1 court	Problème rafraîchissement de la mémoire	Vérifiez si les barrettes mémoires sont bien insérées, si oui changez les une par une. Si le problème persiste il faut changer la carte mère.
2 courts	Problème de parité mémoire	Idem précédemment.
3 courts	Erreur lors du test des 64 premiers Ko de la mémoire	Changer la première barrette mémoire, si le problème persiste changer la carte mère.
4 courts	Erreur de l'horloge système	Changer la carte mère
5 courts	Problème au niveau du processeur	Vérifiez s'il est bien inséré dans son support, si oui changez le processeur, si le problème persiste changer la carte mère.
6 courts	Erreur contrôleur clavier (8042 par exemple).	Si le circuit est sur support, on peut le changer, si il est soudé ou intégré dans il faut changer la carte mère.
7 courts	Le processeur provoque une exception en mode V86.	On peut essayer de changer le processeur mais le plus souvent cela provient du jeu de chipset, donc il faut changer la carte mère.
8 courts	Problème sur la carte vidéo lors d'un essai d'écriture/lecture dans la RAM vidéo.	Vérifiez que la carte vidéo est bien insérée dans son slot, si oui changez la carte vidéo.
9 courts	Erreur de checksum au niveau de la mémoire qui contient le BIOS	Si le circuit est sur support, on peut le changer (**!!! mettre la même version**), si il est soudé ou intégré dans il faut changer la carte mère.
10 courts	Erreur d'accès à la CMOS	Changer la carte mères
11 courts	Erreur d'accès à la mémoire cache externe	Vérifiez si les barrettes ou les CI correspondant à la mémoires caches sont bien insérés, si oui changez les si possible. Si le problème persiste il faut changer la carte mère.
1 long + 2 courts	Erreur vidéo	Vérifiez que la carte vidéo est bien insérée dans son slot, si oui changez la carte vidéo.

1 long + 3 courts	Erreur vidéo	Vérifiez que la carte vidéo est bien insérée dans son slot, si oui changez la carte vidéo.

Si aucun bip ne se fait entendre et si votre ordinateur ne démarre pas, vérifiez que le haut-parleur est correctement connecté à votre carte mère. Si oui, il faut vérifier l'alimentation soit en vérifiant que la led Power on est allumée ou mieux en mesurant avec un voltmètre le +5 V à la sortie de l'alimentation. Si c'est correcte, il faut enlever une à une toutes les cartes d'extension jusqu'à ce qu'un bip sonore soit émis. Si aucun son n'est émis lorsqu'il n'y a plus de cartes d'extension, il faut changer les barrettes mémoires, puis le processeur. Si le problème persiste toujours il faut changer la carte mère.

Lorsque la première série de test c'est correctement passée et que la carte vidéo fonctionne, un message d'erreur est le plus souvent affiché lors de la détection d'une erreur par le BIOS, voir ci-dessous les messages d'erreurs d'un BIOS AWARD :

8042 Gate -A20 Error

Le contrôleur du clavier 8042 ne fonctionne pas ou problème clavier. Essayez de changer le clavier; réinsérer correctement le composant 8042 dans sont support; changer le si possible.

Address line short

Problème logique dans le décodage d'une adresse mémoire. Il peut s'agir d'une perturbation magnétique, éteindre le PC et l'allumer trente secondes plus tard. Si le problème persiste changer la carte mère.

Bios ROM Checksum error

C'est une erreur de contrôle de la ROM du Bios. C'est à dire que le contrôle de la zone d'adresse F0000H-FFFFFH est incorrecte. Changer le BIOS si possible

Cache memory bad, do not enable cache!

Défaillance de la mémoire cache. La plupart du temps c'est la barrette de mémoire cache qui est mal insérée dans son connecteur.

CH-2 Timer error

Certaines cartes mères disposent de deux horloges. Ce message indique que la seconde horloge est défectueuse ou que les ressources qu'elle utilise (IRQ et adresse) sont en conflit avec un autre périphérique.

CMOS Battery has Failed

Ce message indique que la pile de la carte mère doit être changée.

CMOS checksum failure

Ce message indique généralement que les paramètres du Bios sont beaucoup trop "optimisés" ce qui peut entraîner un blocage du système en cours d'utilisation. Autre signification, il se peut aussi que la pile de la carte mère doive être changée. Si c'est le cas, pour le vérifier, il suffit d'éteindre l'ordinateur et de vérifier que les paramètres du Bios sont bien conservés.

CMOS memory size mismatch CMOS system options not set, CMOS time and date not set

Ces erreurs se produisent en général lorsque vous ajoutez des mémoires qui ne sont pas compatibles entres elles ou défectueuses. Parfois il suffit d'aller dans le Setup et d'indiquer la quantité de mémoire réelle.

DMA bus time out

Un périphérique a monopolisé les signaux du bus pendant une durée supérieure à la durée allouée (7,8 microsecondes). Cela signifie généralement que le périphérique incriminé est défectueux.

Keyboard error or no Keyboard present

Impossible d'initialiser le clavier. Il faut s'assurer que le clavier est correctement branché et qu'aucune touche n'est actionnée pendant l'initialisation.

FDD Controler Fail

Cause possible :
CMOS mal configurée
Contrôleur Ide absent/défectueux
Câble FDD mal branché ou câble d'alimentation disque mal branché
Lecteur de disquette défectueux

Floppy Disk Fail 80

Impossible de réinitialiser le lecteur de disquette. Vérifier que les câbles du lecteur sont bien branchés.

Floppy Disk Fail 40

Les paramètres du setup sont en contradiction avec le matériel installé.

HDD Controler failure

Cause possible :
CMOS mal configurée
Contrôleur Ide absent/défectueux
Câble ide mal branché ou câble d'alimentation disque mal branché
Disque dur défectueux

Hard Disk Fail

80La réinitialisation du disque dur a échoué.
40 Le diagnostic du contrôleur de disque dur a échoué.
20 Erreur d'initialisation du disque dur.
10 Impossible de "ré-étalonner" le disque fixe.
08 Vérification des secteurs défaillants.

De façon générale lorsque vous avez un problème avec le disque dur, vérifiez :
- Si il est correctement déclaré dans le SETUP,
- Si il est correctement connecté à la carte contrôleur ou à la carte mère, changer la nappe pour être sûr,
- Si il est correctement alimenté,
- Puis vérifiez avec FDISK que la partition d'amorçage est bien active.

Keyboard is locked out

Le Bios détecte que le clavier est verrouillé.

No ROM Basic ou **Missing Operating System** ou **please insert boot disk in drive**

Ce message indique qu'aucune unité de *boot* n'a été trouvée. La plupart du temps le problème provient du fait que le disque dur n'a pas été déclaré dans le Bios ou qu'il n'est pas partitionné ou pas formaté système ou que la partition principale n'est pas activée ou qu'il n'est pas correctement branché.

On board parity error

Erreur de parité dans la mémoire de la carte mère. Faites une vérification antivirale : les erreurs de parité sont la spécialité de certains virus. Cette précaution concerne également les messages suivants :

Off board parity error,Parity error
Memory parity error at XXXH
I/0 card patity error at XY.XH

Elle s'applique enfin aux deux messages **Offending address notfound** et **Offending segment,** qui indiquent une erreur plus grave encore puisque le segment mémoire corrompu ne peut être déterminé.

LES ANTIVIRUS : un outil de maintenance préventive et corrective

LES VIRUS

Qu'est-ce qu'un virus informatique ?

La définition *officielle* d'un virus est la suivante : Un virus est un petit programme qui est capable de se dupliquer sur des disques informatiques. Les virus peuvent (directement ou indirectement) **infecter** (être copier à partir de ou se copier dans) des fichiers exécutables, des fichiers système, voire dans des fichiers non exécutables utilisant des macros. Les virus ne sont pas des accidents ou des bugs de votre système. Ils sont écrits par des gens qui savent ce qu'ils font.

Quels sont les effets d'un virus ?

- Ces effets dépendent du virus qui infecte votre machine. Certains se contentent de prendre de plus en plus de place sur votre disque dur en se dupliquant jusqu'à saturation, d'autres exécuteront automatiquement certains programmes (par exemple, affichage inopiné d'une boite de dialogue) , d'autres, enfin, vont jusqu'à détruire toute ou partie des données sur votre disque (ce qui est beaucoup plus gênant).

Un virus peut-il endommager physiquement mon ordinateur ?

- **Non**. Un virus est un programme et agit sur d'autres programmes. Un virus ne peut pas faire imploser votre moniteur, arracher les composants d'une carte électronique, ou encore coincer les touches d'un clavier ou les boutons d'une souris. Si cela devait se produire sur votre machine, vous auriez plus de chance de découvrir la vérité en soupçonnant votre entourage ou en appelant un exorciste qu'en blâmant un pauvre virus innocent, incapable d'accomplir une telle prouesse. A moins que votre ordinateur ne soit équipé de bras et que le virus, par un miracle extraordinaire, ne lui donne l'instruction de s'auto baffer, il n'existe aucun risque pour que votre ordinateur soit physiquement endommagé sous l'impulsion d'un virus.

Les différents types de virus

- Il existe deux catégories de virus. Le premier type de virus regroupe les virus qui infectent des fichiers (FILE INFECTORS) dont l'action consiste à se lier à des programmes normaux. En règle générale, ces virus infectent arbitrairement les fichiers EXE et COM, mais certains peuvent également infecter des fichiers qui requièrent une exécution ou une interprétation tels que les fichiers SYS , OVL, OBJ, PRG, MNU et BAT. Il existe également au

moins un virus PC qui infecte des fichiers source en insérant du code dans des fichiers en langage C et qui reproduit les fonctions du virus dans n'importe quel programme qui utiliserait ce code source par la suite.

La deuxième catégorie de virus regroupe les virus qui infectent le code exécutable des zones systèmes d'un disque (SYSTEM ou BOOT-RECORD INFECTORS). Pour un PC, il y a des virus *ordinaires* qui n'affectent que les secteurs réservés au DOS et d'autres qui affectent le MBR (Master Boot Record : secteur #0 sur une disquette ou un disque dur et qui contient un petit programme exécutable affichant le message « disque non système »). Ces virus, une fois introduits dans un système, résident dans la mémoire de la machine.

Pour rendre cette classification un peu plus ardue à comprendre, certains virus sont capables d'infecter à la fois des fichiers et des secteurs systèmes (ex : le virus Tequila). Ces virus sont appelés MULTI-PARTITE ou BOOT-AND FILE.

En plus de ces deux grandes catégories de virus, les chercheurs spécialisés dans la lutte contre les virus ont identifié deux autres catégories distinctes de virus :

Les virus FILE SYSTEM (fichiers systèmes) ou CLUSTER (ex : Dir-II) qui modifient les tables d'entrées d'un répertoire de telle sorte qu'un virus est chargé et exécuté avant que le programme voulu ne le soit. Le programme n'est pas altéré, mais sa référence dans le répertoire est modifié. Certains considèrent ces virus comme étant une catégorie à part entière dans la classification des virus, alors que d'autres considèrent qu'ils sont une sous-catégorie des virus FILE-INFECTORS.

Les virus KERNEL (noyau) s'attaquent à des fonctions spécifiques des programmes qui constituent le noyau d'un système d'exploitation. Un virus FILE-INFECTOR qui peut infecter des fichiers noyau n'est PAS un virus KERNEL. Ce terme est réservé aux virus qui utilisent une spécificité des fichiers noyaux (par exemple, emplacement physique sur le disque).

- Nous allons maintenant examiner les différents modes de fonctionnement des virus :

✓ Les virus furtifs (STEALTH)

- Un virus furtif est un virus qui, lorsqu'il est actif, dissimule les modifications apportées aux fichiers ou aux secteurs boot. En règle générale, ce phénomène est rendu possible par le virus qui observe les appels aux fonctions de lecture des fichiers et falsifie les résultats renvoyés par ces fonctions. Cette méthode permet au virus de ne pas être détecté par les utilitaires anti-virus qui recherchent des modifications éventuelles apportées aux fichiers. Néanmoins, pour que cela soit possible, le virus doit être actif en mémoire résidente, ce qui est détectable par les anti-virus.

✓ Les virus polymorphes (POLYMORPHIC)

- Un virus polymorphe est un virus qui produit des copies variées de lui-même, mais qui restent opérationnelles. Ces stratégies ont été employées dans l'espoir que les utilitaires anti-virus ne puissent pas détecter toutes les instances du virus.

✓ Les virus compagnons (COMPANION)

- virus compagnon est un virus qui, au lieu de modifier un fichier existant, crée un nouveau programme qui est exécuté à l'insu de l'utilisateur au lieu du programme voulu. Le programme original est ensuite exécuté de telle sorte que tout apparaît normal à l'utilisateur. Sur un PC, ceci est généralement accompli en créant un nouveau fichier .COM portant le même nom que le fichier .EXE. Les anti-virus qui ne cherchent que les modifications apportées aux fichiers existants (vérificateurs d'intégrité) ne détecteront pas ce type de virus.

✓ Les virus "cavité" (CAVITY)

- Les virus cavités sont des virus qui écrasent une partie du fichier hôte qui est constitué d'une constante (en général, des 0) sans augmenter la taille du fichier et tout en préservant sa fonctionnalité.

✓ Les virus blindés (ARMORED)

- Un virus blindé est un virus qui utilise des astuces spéciales pour que son dépistage, son désassemblage et la compréhension de son code soient plus durs.

✓ Les virus souterrains (TUNNELLING)

- Les virus souterrains sont des virus qui appellent directement les vecteurs d'interruption du DOS et du BIOS, contournant ainsi tout programme de contrôle qui pourrait être chargé et avoir intercepté ces mêmes vecteurs dans le but de détecter l'activité d'un virus. Certains anti-virus utilisent cette même technique pour contourner un virus inconnu ou non détecté.

✓ Les virus compte-gouttes (DROPPER)

- Un virus compte-gouttes est un programme conçu pour *installer* un virus sur le système visé. Le code du virus est en règle générale contenue dans ce programme de telle manière qu'il ne sera pas détecté par un anti-virus qui, dans d'autres circonstances, détecte ce virus (le compte-gouttes n'est pas infecté par ce virus). Bien qu'assez rare, ce type de virus a été signalé à plusieurs reprises. Un compte-gouttes qui installe le virus seulement en mémoire (donc sans infecter de fichiers sur le disque) est parfois appelé un *injecteur*.

✓ Les bombes ANSI (ANSI BOMB)

- Une bombe ANSI est une séquence de caractères, généralement incluse dans un fichier texte, qui reprogramme certaines fonctions du clavier d'ordinateurs ayant une console ANSI (écran + clavier). On peut ainsi reprogrammer la touche Enter d'un clavier pour qu'elle exécute l'instruction format c : suivi de la fonction Enter.
Néanmoins, cette possibilité ne constitue pas une grande menace. En effet, il est rare pour un logiciel moderne d'exiger un ordinateur tournant sur une console ANSI. De même, peu de gens utilisent des logiciels qui envoient simplement la sortie sur le terminal, donc une bombe ANSI dans un Email ne reprogrammerait pas votre clavier.

Parallèlement à ces différents types de propagation, les virus se différencient également par leur vitesse de propagation (Nota : cette description ne s'applique qu'aux virus de fichiers) :

✓ Les infecteurs normaux

Un virus de fichier typique (ex : Jérusalem) infecte les programmes au fur et à mesure que ces derniers sont exécutés.

✓ Les infecteurs rapides

Un infecteur rapide est un virus qui, lorsqu'il est activé en mémoire, infecte non seulement le programme qui est exécuté mais également ceux qui sont simplement ouverts. Le résultat est que, si on lance un scan anti-virus ou un vérificateur d'intégrité, tout ou partie des programmes seront infectés.

✓ Les infecteurs lents

Le terme infecteur lent fait référence aux virus qui n'infecteront des fichiers que s'ils sont modifiés ou créés. Le but est de faire croire aux utilisateurs de vérificateurs d'intégrité que les rapports de modifications sont dues à des raisons légitimes.

✓ Les infecteurs occasionnels

Les infecteurs occasionnels sont des virus qui infectent de manière sporadique (par exemple, 1 fois sur 10 programmes exécutés, programmes dont la taille dépasse un certains nombres d'octets, etc.). En infectant moins souvent, ces virus réduisent la probabilité d'être découverts.

✓ Les vers (WORM)

Un ver informatique est un programme complet, qui est capable de répandre des copies, ou des segments, fonctionnelles de lui-même sur d'autres systèmes informatiques (en règle générale, via un réseau).
Contrairement aux virus, les vers n'ont pas besoin de programme hôte. Il existe deux types de vers : les vers de station de travail et les vers de réseaux.
Les vers de station sont entièrement contenus dans le système sur lequel ils tournent et ils utilisent les connexions réseaux pour se copier sur d'autres machines. Ceux qui se terminent après s'être copiés sur un autre système (il n'y a donc qu'un seul exemplaire du ver sur le réseau) sont parfois appelés *lapin*
Les vers de réseaux sont constitués de plusieurs parties (ou *segments*), chacunes tournant sur des machines différentes et qui utilisent le réseau pour communiquer. Ils se servent également du réseau pour se dupliquer. Les vers de réseaux qui possèdent un segment principal coordinant les actions des autres segments sont parfois appelés *pieuvres*

✓ Les macro virus

Par rapport aux virus décrits, les macro virus constituent une catégorie à part. En effet, ces virus ne sont pas spécifiques à un système d'exploitation et infectent indifféremment des ordinateurs tournant sous DOS, Windows (3.x, 95, 98,2000 et NT) ou Macintosh. De plus, ces virus n'infectent pas des programmes mais des documents.
Ces virus utilisent certaines fonctions du langage macro de MS Word pour infecter le modèle de base NORMAL.DOT. Dès qu'un document infecté est ouvert, le virus infectera ce modèle qui est la base de la majorité des autres documents et modèles de MS Word.
A leurs débuts, ces virus étaient sans danger et se contentaient d'afficher des boites de dialogues de manière inopinée. Aujourd'hui certains de ces virus ont un but destructeur et peuvent aller jusqu'à l'effacement pur et simple de fichiers.

Le mythe des virus par Email

✓ Les messages d'alerte

- Ce genre de mail vous rappelle-t-il quelque chose ?
  ATTENTION !!! ALERTE AU VIRUS !!! Si vous recevez un e-mail intitulé NE L'OUVREZ PAS. Le virus qu'il contient va effacer l'intégralité de votre disque dur. Faites suivre ce message à autant de personnes de votre connaissance. Ceci est un nouveau virus, très nocif et peu de gens connaissent son existence..
  Viennent ensuite les références de la personne bien informée qui a identifié ce virus (une personne du département recherche d'IBM, ou du département Vente de Microsoft, etc.) afin de donner une plus grande crédibilité à cette alerte.
- CES MAILS SONT DES CANULARS ! Il est impossible d'infecter son ordinateur par l'intermédiaire du texte d'un Email. Un Email n'est pas un programme mais un fichier **texte** qui ne contient aucune instruction exécutable. Il ne s'agit pas non plus d'un document pouvant contenir des macros, il n'existe donc aucun risque d'infection par un macro virus. Le terme virus ne veut pas dire qu'il s'agit d'organismes qui flottent dans l'univers virtuel d'Internet et qui pourrait infecter un ordinateur, à la manière du virus de la grippe infectant un être humain. N'oubliez pas qu'un virus requiert un programme hôte et non pas un simple fichier texte.

✓ Liste des faux virus

- AOL4Free
- Baby New Year
- BUDDYLST
- BUDSAVER.EXE
- Death69
- Deeyenda
- E-Flu
- FatCat
- Free Money
- Ghost
- Good Times
- Hairy Palms
- Irina
- Join the Crew
- Penpal Greetings
- Red Alert
- Returned or Unable to Deliver
- Time Bomb
- Win a Holiday
- World Domination

✓ Que faire si vous recevez un message d'alerte ?

- En tout premier lieu, il convient de ne pas faire suivre ce message. Vous contribueriez au gâchis de bande passante généré par ces Emails.
- Vous pouvez ensuite envoyer une réponse à l'expéditeur de ce message en lui expliquant que l'existence d'un tel virus est impossible, soit en résumant la discussion contenue dans cette page ou tout simplement en lui indiquant l'url de cette page. Il est en effet préférable d'informer le plus de monde possible sur ces canulars afin de faire cesser ces pratiques. Plus de gens seront au courant de ces supercheries, moins ces canulars circuleront sur le net.
- Restez courtois avec votre correspondant. La tentation d'être agressif est grande, surtout s'il s'agit du énième message d'alerte, mais gardez en mémoire que l'expéditeur est animé de bonnes intentions, et qu'il y a de fortes chances qu'il s'agisse de quelqu'un d'inexpérimenté.

✓ La transmission de vrais virus au moyen d'Email

- Le but de cette discussion est de vous montrer qu'il est impossible d'être infecter par un virus en **lisant** un mail, mais il existe néanmoins une possibilité d'envoyer un virus par Email : **par le biais d'un fichier attaché au document**
- En effet, un fichier attaché à un mail n'a rien à voir avec le mail lui-même. Si le mail est un fichier texte, le fichier attaché peut-être n'importe quel type de fichier, y compris un exécutable. Par contre, le téléchargement de ce fichier, en supposant qu'il soit infecté, n'est pas suffisant pour infecter votre ordinateur. Il vous faut d'abord l'exécuter pour démarrer l'infection.
    - **Il vous faut agir avec la plus grande prudence si vous recevez un fichier par mail!**

Les règles de prudence

- Ne démarrer jamais votre ordinateur à partir d'une disquette que vous n'auriez pas formaté vous-même. Un virus peut avoir été introduit dans le MBR qui infecterait votre ordinateur avant qu'un utilitaire anti-virus puisse être activé.
- Procurez vous un utilitaire anti-virus et **maintenez le à jour**. De nouveaux virus sont découverts tous les jours, et l'anti-virus que vous avez installé 3 mois auparavant est déjà obsolète. Pour exemple, le premier macro virus est apparu durant l'année 1998. En 2000, on en dénombre environ 4800, soit plus de 200 nouveaux macro virus par mois!
  Il est à noter que la plupart des fabricants d'anti-virus proposent des mises à jour gratuites de leur produit pendant une période définie.
- Certains lecteurs de mails permettent le démarrage automatique de certaines applications dans le cas de fichiers attachés aux mails. **Invalidez cette option** qui pourrait s'avérer catastrophique si le fichier en question était infecté.
- Soyez excessivement méfiant si vous recevez d'un inconnu un fichier qui pourrait contenir un virus (fichier exécutable de type EXE, COM, etc. ou document pouvant utiliser des macros, tels que les documents DOC ou XLS)
- N'exécuter jamais un programme que vous venez de télécharger, que ce soit par mail ou sur l'Internet, sans l'avoir préalablement scanné avec un anti-virus récemment mis à jour.
- Ne vous servez pas de disquettes qui n'auraient pas été préalablement scannées (surtout si ces disquettes ont l'habitude d'être prêtées).

LES ANTIVIRUS

Un **antivirus** (AV) est un logiciel censé protéger un micro-ordinateur contre les programmes néfastes appelés virus, vers, macro virus, etc.

Fonctionnement

Les principaux antivirus du marché se concentrent sur des fichiers de **signatures** et comparent alors la *signature génétique* du virus aux codes à vérifier. Certains programmes appliquent également la méthode dite **heuristique** tendant à découvrir un code malveillant par son comportement.
Autre méthode, l'**analyse de forme** repose sur du filtrage basé entre des règles regexp ou autres, mises dans un fichier junk. Cette dernière méthode peut être très efficace pour les serveurs de courriels supportant les regexp type postfix puisqu'elle ne repose pas sur un fichier de signatures.

Les antivirus peuvent balayer le contenu d'un disque dur, mais également la mémoire de l'ordinateur. Pour les plus modernes, ils agissent en amont de la machine en scrutant les échanges de fichiers avec l'extérieur, aussi bien en flux montant que descendant. Ainsi, les courriels sont examinés, mais aussi les fichiers copiés sur ou à partir de supports amovibles tels que cédéroms, disquettes, connexions réseau, clefs USB…

On distingue plusieurs types d'antivirus selon leur fonctionnement. La première méthode est celle du dictionnaire.

Dictionnaire

Les créateurs d'antivirus ayant préalablement identifié et enregistré des informations sur l'antivirus, comme le ferait un dictionnaire, l'antivirus peut ainsi détecter et localiser la présence d'un virus. Lorsque cela se produit, l'antivirus dispose de trois options, il peut :

1. tenter de réparer les fichiers endommagés en éliminant le virus ;
2. mettre les dossiers en quarantaine afin qu'ils ne puissent être accessibles aux autres dossiers ni se répandre et qu'ils puissent éventuellement être réparés ultérieurement ;
3. supprimer les fichiers contaminés.

Afin de maximiser le rendement de l'antivirus, il est essentiel d'effectuer de fréquentes mises à jour en téléchargeant des versions plus récentes. Des internautes consciencieux et possédant de bonnes connaissances en informatique peuvent identifier eux-mêmes des virus et envoyer leurs informations aux créateurs de logiciels antivirus afin que leur base de données soit mise à jour.

Généralement, les antivirus examinent chaque fichier lorsqu'il est créé, ouvert, fermé ou lu. De cette manière, les virus peuvent être identifiés immédiatement. Il est possible de programmer le système d'administration pour qu'il effectue régulièrement un examen de l'ensemble des fichiers sur l'espace de stockage (disque dur, etc).

Même si les logiciels antivirus sont très performants et régulièrement mis à jour, les créateurs de virus font tout aussi souvent preuve d'inventivité. En particulier, les virus « oligomorphiques », « polymorphiques » et plus récemment, « métamorphiques », sont plus difficiles à détecter.

Comportements suspects

Une autre approche pour localiser les virus consiste à détecter les comportements suspects des programmes. Par exemple, si un programme tente d'écrire des données sur un programme exécuté, l'antivirus détectera ce comportement suspect et en avisera l'usager qui lui indiquera les mesures à suivre.

Contrairement à l'approche précédente, la méthode du comportement suspect permet d'identifier des virus très récents qui ne seraient pas encore connus dans le dictionnaire de l'antivirus. Toutefois, le fait que les usagers soient constamment avertis, de fausses alertes peuvent les rendre insensibles aux véritables menaces. Si les usagers répondent « Accepter » à toutes ces alertes, l'antivirus ne leur procurera aucune protection supplémentaire. Ce problème s'est aggravé depuis 1997, puisque plusieurs programmes inoffensifs ont modifié certains fichiers exécutables sans observer ces fausses alertes. C'est pourquoi, les antivirus les plus modernes utilisent de moins en moins cette méthode.

Autres approches

L'*analyse heuristique* est utilisée par quelques antivirus. Par exemple, l'antivirus peut analyser le début de chaque code de toutes les nouvelles applications avant de transférer le contrôle à l'usager. Si le programme semble être un virus, alors l'usager en sera averti. Toutefois, cette méthode peut également mener à de fausses alertes. La méthode heuristique permet de détecter des variants de virus et, en communiquant automatiquement les résultats de l'analyse à l'éditeur, celui-ci peut en vérifier la justesse et mettre à jour sa base de définitions virales.

La *méthode du bac à sable* consiste à émuler le système d'exploitation et à exécuter le fichier lors de cette simulation. Une fois que le programme prend fin, les logiciels analysent le résultat du bac à sable afin de détecter les changements qui pourraient contenir des virus. En raison des problèmes de performance, ce type de détection a lieu habituellement pendant le balayage sur demande. Cette méthode peut échouer puisque les virus peuvent s'avérer non déterministes et résulter de différentes actions ou même peut-être d'aucune action lorsque exécuté. Il est impossible de le détecter à partir d'une seule exécution.

La *liste blanche* est une technique récente qui, contrairement à la liste noire bloquant des codes recensés dans ladite liste, empêche l'exécution de tous les codes informatiques à l'exception de ceux qui ont déjà été identifiés comme sûrs par l'administrateur de système. En suivant cette approche de déni par défaut, les limitations inhérentes au fait d'avoir à garder les signatures des virus à jour sont ainsi évitées. De plus, les logiciels jugés indésirables par l'administrateur du système sont empêchés d'exécution puisqu'ils ne sont pas sur la liste blanche. Puisque l'organisation des entreprises modernes possède de grandes quantités de logiciels sécuritaires, les limitations reliées à l'adoption d'une telle technique demeurent reliées à l'habilité de l'administrateur d'inventorier et de mettre à jour ladite liste. Une implantation valable de cette technique requiert donc des outils de gestion d'inventaire et de maintenance de la liste.

Problèmes dignes d'intérêt

- La propagation des virus utilisant les courriels comme vecteur d'infection (vers) pourrait être inhibée de manière plus efficace et moins dispendieuse sans installation d'antivirus supplémentaires si des bogues dans les logiciels de courrier électronique clients, qui permettent l'exécution non autorisé du code, étaient corrigés.
- La connaissance informatique chez les utilisateurs peut être un bon complément pour les logiciels antivirus. Le fait d'apprendre à ces derniers comment utiliser les ordinateurs de manière sécuritaire (par exemple, ne pas télécharger sur Internet et exécuter des programmes inconnus) ralentirait la propagation des virus et rendrait les logiciels antivirus presque inutiles.
- La création et la diffusion constantes des virus favorisent la vente d'antivirus. Certaines personnes pensent que les éditeurs d'antivirus font affaire avec des créateurs de virus afin de soutenir leur marché.
- Certains antivirus peuvent réduire de manière considérable la performance des ordinateurs, notamment lorsqu'ils résident en mémoire (analyse en temps réel). Les utilisateurs peuvent désactiver la protection antivirus pour surmonter la perte de performance, mais cela augmente le risque d'infection. Pour un maximum de protection, le logiciel antivirus doit être activé en tout temps, malgré la réduction des performances du système.
- Il est fortement déconseillé d'avoir plusieurs antivirus installés sur un même ordinateur, car cela pourrait l'endommager, en particulier s'ils résident en mémoire. Cette mise en garde n'est pas toujours mentionnée dans les manuels.
- Il est parfois nécessaire de désactiver temporairement la protection contre les virus lorsqu'on installe des mises à jour importantes telles que *Windows Service Packs* ou celles des pilotes de périphérique de cartes graphiques. Si la protection antivirus fonctionne en même temps, cela peut empêcher la mise à jour.
- Lors de l'acquisition d'un logiciel antivirus, une clause de souscription automatiquement renouvelée peut être prévue, de sorte que la carte de crédit de l'acheteur est automatiquement débitée. Par exemple, McAfee exige qu'un client se désabonne au moins 60 jours avant la fin de la souscription. Pourtant, McAfee ne fournit ni ligne téléphonique, ni un autre moyen afin de se désabonner directement depuis leur site Internet. Dans ce cas, le recours de l'abonné est de contester les frais avec la société émettrice de carte de crédit.
- Les antivirus sont souvent responsables de nombreux problèmes informatiques. Certains disent même qu'ils causent plus de tort que de bien à l'utilisateur au final. Néanmoins, un utilisateur novice ne peut s'en passer sans courir de grands risques.
- Il faut souvent configurer manuellement certains logiciels (décompression d'archives, gestionnaire de téléchargement, peer-to-peer, etc.) pour qu'ils fassent appel à l'antivirus.

Maintenance évolutive et maintenance adaptative

**** Une application peut évoluer, par exemple, à la suite de demandes d'utilisateurs pour modifier son comportement ou pour proposer de nouvelles fonctions.

La maintenance évolutive consiste ainsi - à améliorer (voire à redéveloper) des fonctions existantes d'une application, - à développer de nouvelles fonctionnalités pour faire face à de nouvelles exigences.

**** Une application dépend souvent d'autres applications. En informatique par exemple, un logiciel s'exécute en général au-dessus d'un système d'exploitation. Lorsque celui-ci évolue, il peut rendre nécessaire une adaptation du logiciel. La maintenance adaptative consiste à faire évoluer une application lorsque son environnement change, afin d'assurer sa continuité de fonctionnement.

TEST DE FIN DE L'EXPOSÉ **THEME : LA MAINTENANCE**

Les noms : - **-** **-**

- **-** **-**

Ce thème vous a plu ? : ☐OUI **☐NON** **☐UN PEU**

1) Quelles affirmations concernant le Chipset sont vraies :

- ☐ Il coordonne les échanges entre les composants de l'ordinateur.
- ☐ Il assure le débit constant des données traitées par le processeur
- ☐ Il doit être changé à chaque fois que l'on change de processeur

2) Quelles affirmations concernant les mémoires sont vraies

- ☐ La mémoire RAM permet de sauvegarder les données à l'arrêt de la machine.
- ☐ Elle est plus rapide d'accès que les disques durs
- ☐ On y stocke des informations pendant le fonctionnement de l'ordinateur.
- ☐ Ses temps d'accès se mesure en nanosecondes.

3) Quelles affirmations concernant les connecteurs d'extension sont vraies

- ☐ on peut y insérer des cartes dotant le PC de nouvelles fonctionnalités.
- ☐ Actuellement les constructeurs sont sur le point de proposer un nouveau connecteur : le VLB.
- ☐ Le connecteur AGP permet d'insérer des cartes graphiques et des cartes réseaux
- ☐ Les cartes mères récentes ne disposent plus de connecteurs ISA.

4) Quelles affirmations concernant la mémoire morte sont vraies

- ☐Le BIOS est logé dans une mémoire morte
- ☐Le shadowing consiste à copier le contenu d'une RAM dans une ROM
- ☐Une mémoire de type ROM peut être reprogrammé
- ☐Le flashage est une technique pour reprogrammer les EPROM.

5) citez les 6 étapes du dépannage d'une panne

1-
2-
3-
4-
5-
6-

6) citez 5 faux virus

1)…… 2)…… 3)……4)……5)……..

7) complétez le tableau suivant

BIOS AMI		
bips	**problème**	**remède**
4 bips courts		
10 bips courts		
1 bip long+2 bips courts		

8) Qu'est ce qu'une maintenance adaptative ?? :

……..
……..
……..

9) C'est quoi l'ESD ?

……..
……
……..……

10) Qu'est ce qu'un « DROPPER » ?

……..
……..