Démarrage d'un ordinateur de type PC avec Windows XP

Eric BERTHOMIER

19 janvier 2014

Collaborateurs : Franck Berger (Traduction & Relecture)
Yohann Radin (Relecture)

Résumé

Ce document est la traduction d'un document en anglais "The PC Boot Process - Windows XP".
Source : `http://www.gegeek.com/documents/cheat_sheets/Windows%20XP%20Boot%20Process.pdf`.

L'alimentation est mise sous tension	L'alimentation réalise un auto-test. Lorsque tous les niveaux de tension et de courants sont acceptables, l'alimentation indique qu'elle est stable en envoyant un signal de bon fonctionnement (Power Good) au processeur. Le temps écoulé entre l'allumage et l'envoi du signal est généralement entre 0.1 secondes et 0.5 secondes.
Le microprocesseur d'horloge reçoit le signal "Power Good"	Avec l'arrivée du signal "Power Good", le microprocesseur d'horloge arrête d'envoyer des signaux de reset au CPU permettant à celui-ci de démarrer les opérations.
Le CPU commence à exécuter le code situé dans la ROM du BIOS (Basic Input Output System).	Le CPU pointe dans la ROM du BIOS à l'adresse mémoire " FFFF :0000" soit 16 octets avant l'adresse de fin de la mémoire. Cette adresse ne contient qu'une instruction JMP (jump) qui pointe sur l'adresse réelle de la ROM du BIOS.
Le BIOS effectue un test basique du matériel principal pour vérifier les fonctionnalités de base.	Toute erreur qui pourrait apparaître à ce niveau dans le processus de boot sera transmis à l'utilisateur au travers de "code-beep"car la fonction vidéo n'a pas été encore initialisée.
Le BIOS recherche des périphériques qui auraient besoin de charger leurs propres routines BIOS.	Les périphériques vidéo sont un exemple courant de périphériques fournissant leur propre source de code BIOS. Pour se faire, les routines BIOS scannent les adresses mémoires de C000 :0000 à C780 :0000 pour trouver la ROM vidéo. Une erreur sur le chargement de la ROM de ce périphérique génère une erreur du type : **XXXX ROM Error** où XXXX représente l'adresse du segment du module qui a échoué.

Le BIOS teste si le démarrage du PC est un démarrage à froid ("cold-start") ou un reboot ("warm-start").

Pour savoir si le démarrage est de type reboot ou à froid, le BIOS teste la valeur des 2 octets situés à l'adresse mémoire : 0000 :0472. Toute autre valeur que 0x1234 indique un démarrage à froid.

- Dans le cas d'un démarrage à froid, le BIOS exécute un POST (Power On Self Test) complet.
- Dans le cas d'un démarrage en reboot, la vérification de la mémoire n'est pas réalisée.

Le POST peut être découpé en 3 phases :
- le test vidéo initialise l'adapteur vidéo, teste la carte vidéo et la mémoire vidéo puis affiche les informations de configuration ou les erreurs.
- le programme d'identification du BIOS affiche la version du BIOS, le fabriquant et la date.
- le test de Mémoire teste les barettes mémoires et affiche la quantité de mémoire installée.

Les erreurs pouvant intervenir durant la phase de POST peuvent être clasées en "Fatale" ou "Non-Fatale".
- Une erreur "non-fatale" affichera typiquement un message d'erreur sur l'écran et permettra au système de continuer son processus de démarrage.
- Une erreur "fatale" arrête le processus de démarrage de l'ordinateur et est généralement signalée par une série de beeps.

Le BIOS lit alors les informations de configuration stockée dans le CMOS.

Le CMOS (Complementary Metal Oxide Semiconductor) est une petite zone de mémoire (64ko) qui est maintenue par une pile (pile lithium ronde) attenante à la carte mère. Le plus important pour le BIOS est notamment que le CMOS contient l'ordre dans lequel les différents lecteurs doivent être examinés pour savoir s'ils contiennent un éventuel système d'exploitation, disquette en premier, cd-rom en premier ou disque dur en premier.

Fixed Disk

	Si le premier disque dit bootable (amorçable) est un disque dur, le bios examine le tout premier secteur de ce disque à la rercherche d'un Master Boot Record (MBR). Dans le cas d'une disquette, le BIOS recherche un secteur de boot dans le tout premier secteur.	Sur un disque dur, le MBR occupe toujours le premier secteur du disque dur (cylindre 0, tête 0, secteur 1). Sa taille est de 512 octets. Si ce secteur est trouvé, il est chargé en mémoire à l'adresse 0000 :7C00 et un test de signature est effectué. Une signature valide correspond à la valeur 55AAh dans les 2 premiers octets. L'absence de MBR ou une signature invalide arrête le processus de démarrage avec un message du type "NO ROM BASIC - SYSTEM HALTED". Un MBR est composé de 2 parties : – une table de partitions qui décrit l'architecture du disque physique – le code de chargement des partitions qui incluent les instructions permettant de continuer le processus de boot
MBR	Avec un MBR valide chargé en mémoire, le BIOS transfère le contrôle du processus de démarrage au code de chargement des partitions qui peut ainsi contenir plus que les 512 octets du MBR.	Le processus permettant l'installation de plusieurs OS sur un seul PC s'effectue souvent en remplaçant le code du chargeur de partitions par un programme de Boot (Boot Loader) qui permet à l'utilisateur de sélectionner la partition à charger lors de la prochaine étape du processus.
Table de Partitions	Le chargeur de partitions (ou le chargeur de boot (Boot Loader)) examine la table de partitions pour trouver une partition marquée comme Active. Le chargeur de partition recherche alors le tout premier secteur de la patition en tant que secteur de boot (Boot Record).	Le secteur de boot est composé de 512 octets et contient une table qui décrit les caractéristiques de la partition (nombre d'octets par secteur, nombre de secteurs par cluster, etc.) et aussi une adresse de saut permettant la localisation du 1er fichier de démarrage du système (IO.SYS en DOS)
Système d'Exploitation (Operating System)		
Secteur de Boot	Le secteur de boot de la partition active est testée en recherchant une signature de boot valide. Si cette signature est trouvée, le secteur est exécutant à l'image d'un programme.	Le démarrage de Windows XP est contrôlé par le fichier NTLDR (NT Loader (chargeur d'amorçage)) qui est un fichier système caché résidant dans la partition système. NTLDR va charger Windows XP en 4 phases : a. Phase initiale du chargeur de démarrage (Initial Boot Loader Phase) b. Sélection du sytème d'exploitation c. Détection du Matériel d. Sélection de la Configuration

Phase de chargement du NTLDR (NT Loader (chargeur d'amorçage))	Durant la phase de chargement du NTLDR, le processeur passe du mode réel au mode protégé. Ceci met le processeur en mode mémoire 32 bits et active la pagination. Il charge alors le driver du mini système de fichiers pour permettre au NTLDR de lire les fichiers de la partition formattée avec l'ensemble des fichiers systèmes supportés par Windows XP.	Windows XP supporte les partitions formatées en FAT16, FAT32 et NTFS.
NTLDR OS Selection BOOT.INI	Si le fichier BOOT.INI est trouvé à la racine du système de fichiers, NTLDR lira son contenu et le mettra en mémoire. Si le fichier BOOT.INI contient des entrées pour plus d'un système d'exploitation, NTLDR arrêtera la séquence de démarrage à ce niveau et proposera une liste de choix. Il attendra alors un certain temps pour que l'utilisateur puisse décider de son choix.	Si le fichier BOOT.INI n'est pas trouvé à la racine du système de fichiers, NTLDR continuera la séquence de démarrage et essaiera de charger XP à partir de la première partition du premier disque, typiquement C :\.
F8	Dans le cas où le système d'exploitation est Windows NT, 2000, ou un XP, l'appui de la touche F8 à ce stade permet d'interrompre la séquence de démarrage et de proposer différentes options de démarrage telles que *"Mode sans échec"* ou *"Dernière bonne configuration connue"*.	Après chaque séquence de démarrage réussie, XP crée une copie de la combinaison drivers et paramètres systèmes et l'enregistre sous le nom de *"Dernière bonne configuration connue"*. Cet enregistrement peut être utilisé pour démarrer le système par la suite dans le cas où l'installation d'un nouveau périphérique ait causé un échec au démarrage.
NTLDR Détection du Matériel	Si le système d'exploitation choisi est XP, NTLDR continuera le processus de démarrage en localisant et en chargeant le programme NTDETECT.COM pour réaliser une recherche du matériel.	NTDETECT.COM collecte la liste des composants matériels installés et retourne cette liste pour une inclusion prochaine dans le registre HKEY_LOCAL_MACHINE \HARDWARE.
NTLDR Sélection de la configuration	Si l'ordinateur possède plus d'un profil matériel, le programme NTLDR s'arrêtera à ce niveau et proposera le choix entre les *Profils materiel* / *Récuperation de configuration*.	Ne pas disposer de plusieurs configurations matérielles entraînera que le NTLDR sautera simplement cette étape et n'affichera pas de menu.

Chargement du Noyau (kernel)	Suite à la sélection du profil matériel (dans le cas où il existait), NTLDR commence à charger le noyau XP (NTOSKRNL.EXE (Windows NT Operating System Kernel)).	Durant le chargement du noyau (mais avant son initialisation), NTLDR reste maître de l'ordinateur. L'écran s'efface et une série de rectangles blancs apparaîssent en bas de l'écran. À ce moment, NTLDR charge aussi la couche d'abstraction du matériel (Hardware Abstraction Layer (HAL.DLL)) ce qui permettra d'isoler le noyau du matériel. Ces deux fichiers sont localisés dans le répertoire \system32.
NTLDR - Démarrage des drivers de périphériques	NTLDR charge maintenant les pilotes (drivers) de périphériques qui sont marqués comme des périphériques de démarrage. Avec le chargement de ces drivers, NTLDR abandonne le contrôle de l'ordinateur.	Chaque driver possède une entrée dans la base de registres sous HKEY_LOCAL_MACHINE \SYSTEM \Services. Chaque driver qui a une valeur "Start" pour l'entrée "SERVICE_BOOT_START" est considéré comme un périphérique de boot. Un point de progression est mentionné à l'écran pour chaque fichier chargé sauf si le commutateur */SOS* a été indiqué dans le fichier BOOT.INI. Dans ce cas, c'est le nom de fichier qui est affiché.
Initialisation du Kernel (noyau)	NTOSKRNL passe par deux phases dans son processus de démarrage la phase 0 et la phase 1. La phase 0 initialise juste ce qu'il faut du micro-noyau et des sous-systèmes exécutifs pour que les services de base nécessaires à l'achèvement de l'initialisation deviennent disponibles. Á ce stade, le système affiche un écran graphique avec une barre d'état indiquant l'état de charge.	XP désactive les interruptions durant la phase 0 et les active durant la phase 1. HAL est appelé pour préparer le contrôleur d'interruption (Interrupt Controller) ; le gestionnaire de mémoire (Memory Manager) ; le gestionnaire d'objets (Object Manager) ; le Moniteur de référence de sécurité (Security Reference Monitor) et le gestionnaire des tâches (Process Manager) sont initialisés. La Phase 1 débute quand HAL est appelé pour préparer le système à accepter les interruptions venant des différents périphériques. Si l'architecture matérielle comporte plus d'un processeur, les autres processeurs sont alors initialisés. L'ensemble des sous-systèmes exécutifs (Executive subsystems) sont initialisés dans l'ordre suivant : a. Gestionnaire d'Objets (Object Manager) b. Exécutif (Executive) c. Micro-noyau (Microkernel) d. Security Reference Monitor (A traduire) e. Gestinnaire de Mémoire (Memory Manager) f. Gestionnaire de Cache (Cache Manager) g. Appels de Procédures Locales LPCS h. Gestionnaire d'Entrées / Sorties (I/O Manager) i. Gestionnaire de Processus (Process Manager)

Gestionnaire d'Entrées / Sorties (I/O Manager)	L'initialisation du gestionnaire d'Entrées / Sorties débute le processus de chargement de l'ensemble des drivers systèmes. Reprenant là où le NTLDR s'était arrêté, il finit le chargement des périphériques d'amorçage. Ensuite, il crée une liste priorisée des pilotes et tente de les charger chacun à leur tour.	L'échec du chargement d'un pilote de périphérique (driver) peut entraîner un redémarrage avec la possibilité d'utiliser la *"Dernière bonne configuration connue"*.
SMSS	La dernière tâche de la phase 1 de l'initialisation du noyau est de lancer le sous-système gestionnaire de session (Session Manager Subsystem (SMSS)). SMSS est responsable de la création de l'environnement utilisateur et qui permet d'obtenir une interface utilisateur.	SMSS s'exécute en mode utilisateur, mais contrairement à d'autres applications en mode utilisateur, SMSS est considéré comme un "membre" ou "composant" de confiance du système d'exploitation et est également une application native du système (il utilise uniquement les fonctions exécutives de base). Ces deux caractéristiques permettent à SMSS de démarrer le sous-système graphique et le processus d'authetification.
win32k.sys	SMSS charge le pilote de périphérique win32k.sys qui implémente le sous-système graphique de Win32.	Peu de temps après le démarrage de win32k.sys, il passe l'écran en mode graphique. Le sous-système de Services démarre alors tous les services marqué "Démarrage automatique". Une fois l'ensemble des périphériques et des services démarrés, le processus de boot (démarrage) est considéré comme réussi et cette configuration est enregistrée en tant que *"Dernière bonne configuration connue"*.
Logon	Le processus de démarrage de XP ne peut être considéré comme terminé qu'une fois qu'un utilisateur a pu se connecter au système. Le processus est démarré par le programme WINLOGON.EXE qui est chargé en tant que service par le noyau et est suivi par l'éxécution de l'Autorité Locale de Sécurité (Local Security Authority (LSASS.EXE)) qui affiche une boîte de dialogue d'authentification.	La boîte de dialogue apparaît approximativement au moment où le sous-système Services démarre le service Réseau.