UEFI&BIOS相关

技术部培训

分区表

- 分区表的作用就是把一块单独的物理硬盘，划分成几个各自相对独立的区域，便于我们更方便的使用硬盘
- GPT和MBR是硬盘分区表的两种不同格式

MBR

- 主引导记录（Master Boot Record，缩写：MBR）
- 硬盘的0柱面、0磁头、1扇区(0,0,1)称为主引导扇区,是访问硬盘时所必须要读取的首个扇区


引导代码
（MBR）
分区表
（DPT）
结束标志
（55AA）

字节位移	占用字节数	值	描述
0x01BE	1 BYTE	0x80	引导指示符，指明该分区是否是活动分区；活动分区指示符是 0x80
0x01BF	1 BYTE	0x20	开始磁头
0x01C0	6 BIT	0x21	开始扇区，占用 6 位
0x01C1	10 BIT	0x00	开始柱面，占用 10 位，最大值 1023
0x01C2	1 BYTE	0x07	分区类型，NTFS 一般是 0x07
0x01C3	1 BYTE	0xFE	结束磁头
0x01C4	6 BIT	0xFF	结束扇区，占用 6 位
0x01C5	10 BIT	0xFF	结束柱面，占用 10 位，最大值 1023
0x01C6	4 BYTE	0x00080000	相对扇区数，从该磁盘的开始到该分区的开始的扇区偏移量，以扇区为单位
0x01CA	4 BYTE	0x00F0DF01	该分区的总扇区数

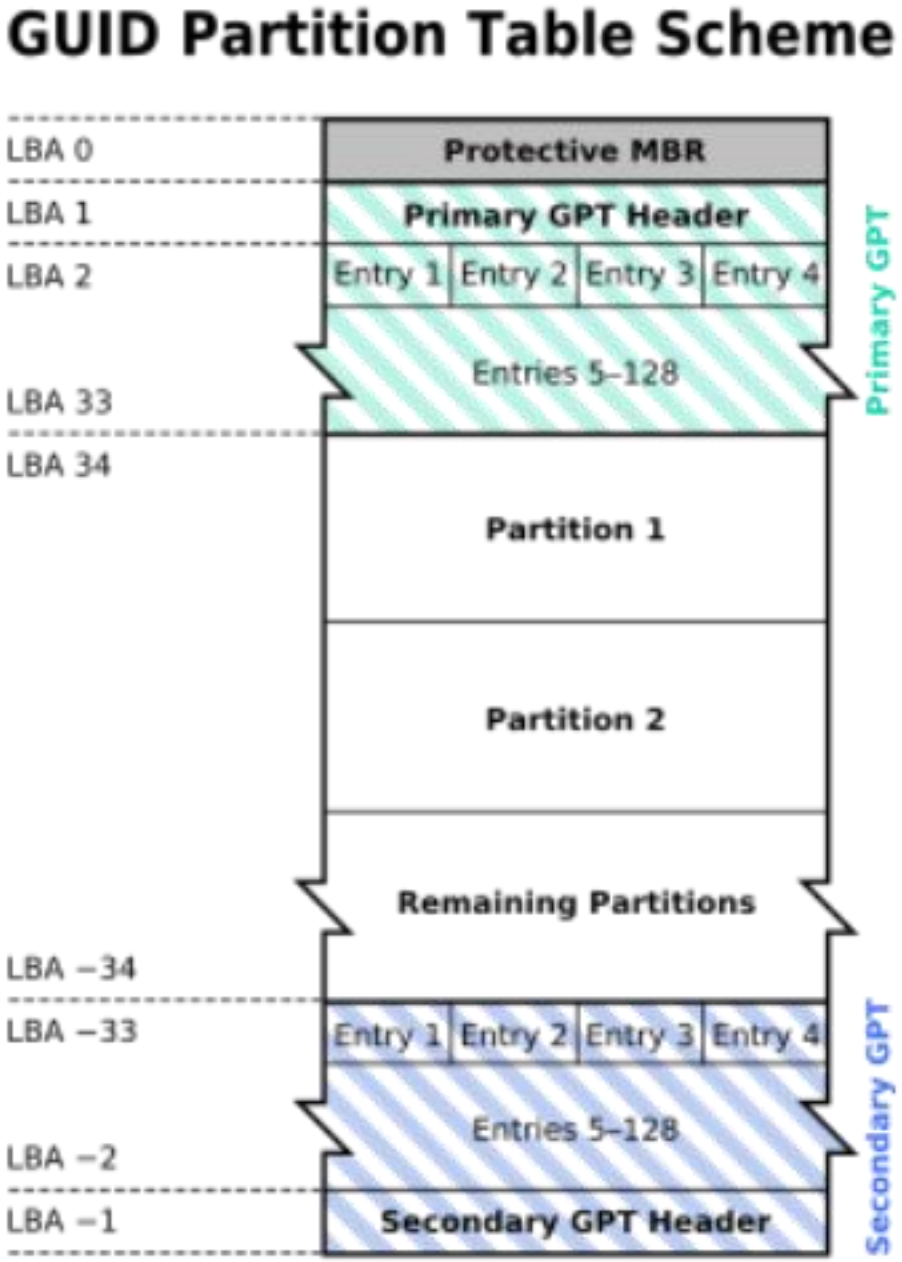
GPT（GUID Partition Table）

- GUID是一种由算法生成128 位二进制数唯一标识
- 保护MBR
- 分区表头

  签名+版本+分区表头大小+分区表头+硬盘GUID

- 分区表项

  GUID类型+GUID+开始扇区+结束扇区+分区名



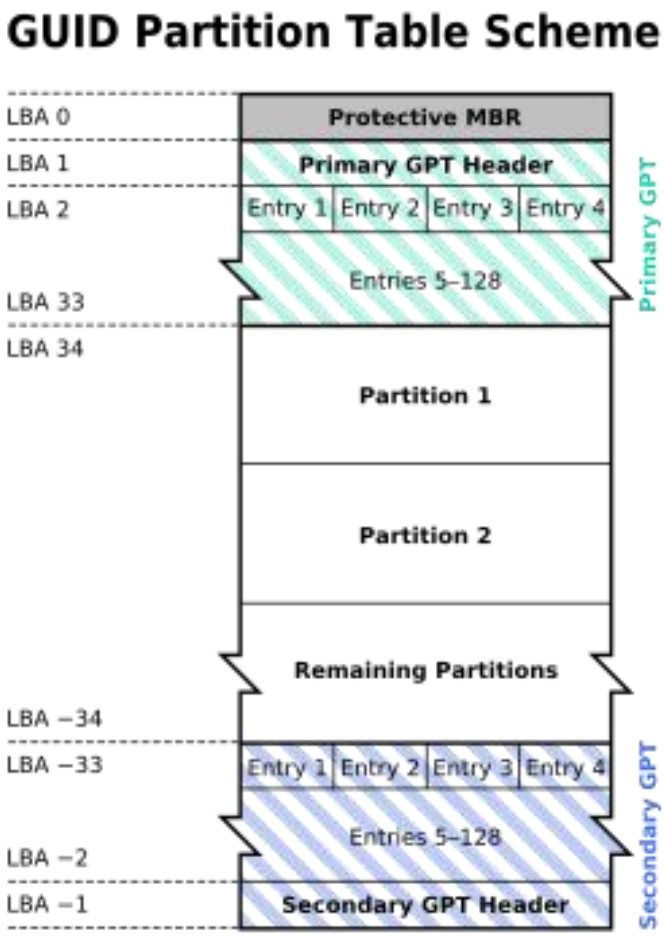
GUID类型	分区名
C12A7328-F81F-11D2-BA4B-00A0C93EC93B	EFI系统分区
E3C9E316-0B5C-4DB8-817D-F92DF00215AE	微软保留（MSR）分区
EBD0A0A2-B9E5-4433-87C0-68B6B72699C7	基本数据分区

GPT（GUID Partition Table）

- GUID是一种由算法生成的唯一标识
- 保护MBR
- 分区表头

  签名+版本+分区表头大小+分区表头+硬盘GUID
- 分区表项

  GUID类型+GUID+开始扇区+结束扇区+分区名



MBR

- 最多4个主分区（或3个主分区，1个扩展分区和无限制的逻辑驱动器）
- MBR区易损坏
- 16字节
- 最大2TB(512B)

GPT

- 理论上无限
- 更安全
- 128字节
- 最大8ZB(512B)

字节的次方单位

十进制前缀 (SI)			二进制前缀 (IEC 60027-2)		
名字	缩写	次方	名字	缩写	次方
千字节	KB	10^{3}	kibibyte	KiB	2^{10}
兆字节	MB	10^{6}	mebibyte	MiB	2^{20}
吉字节	GB	10^{9}	gibibyte	GiB	2^{30}
太字节	TB	10^{12}	tebibyte	TiB	2^{40}
拍字节	PB	10^{15}	pebibyte	PiB	2^{50}
艾字节	EB	10^{18}	exbibyte	EiB	2^{60}
泽字节	ZB	10^{21}	zebibyte	ZiB	2^{70}
尧字节	YB	10^{24}	yobibyte	YiB	2^{80}

BIOS

- Basic Input/Output System基本输入输出系统
- 通电引导阶段运行硬件初始化，以及为操作系统和程序提供运行时服务的**业界标准的接口固件。**
- BIOS这个字眼是在1975年第一次由CP/M操作系统中出现
- 最大BIOS提供商American Megatrends(AMI)

BIOS组成

- 自诊断程序
- CMOS设置程序
- 系统自举装载程序

- BIOS->自检(POST)->MBR->活动主分区->/bootmgr->系统引导

缺陷

- 汇编代码
- 只能识别MBR
- 16位运行方式，阻碍硬件发展

  屏幕： 640*480　4:3

  内存：只认前1MB

  CPU：32/64位保留16位运行模式

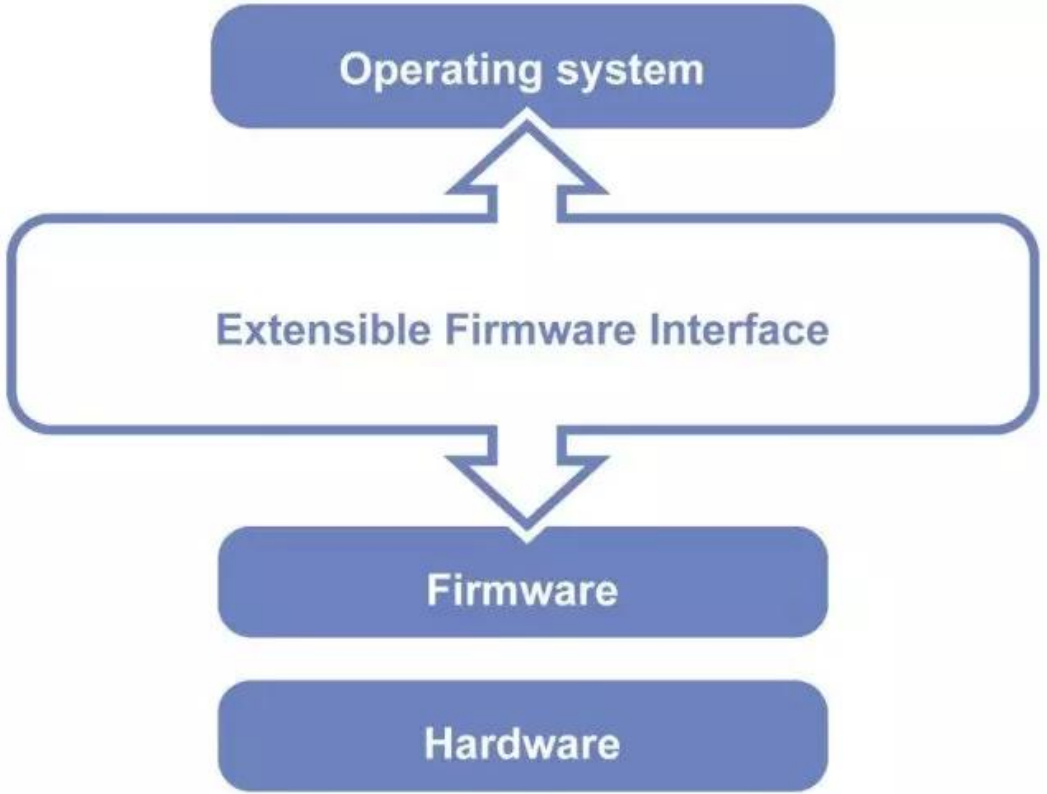
EFI

- Extensible Firmware Interface　可扩展固件接口
- 前身和基础——EFI，是由 Intel 开发和发布的
- 2007年，英特尔，AMD，微软和PC制造商就新的统一可扩展固件接口（UEFI）规范达成一致。UEFI 由 UEFI 论坛进行管理。

- IBV（独立BIOS厂商） AMI、Insyde、Phoenix
- IHV（独立硬件厂商） AMD、Apple、Dell、HP、IBM、Intel、联想
- ISV（独立软件厂商） 微软

UEFI

- Unified Extensible Firmware Interface统一可扩展固件接口
- 是一种个人电脑系统规格，用来定义操作系统与系统固件之间的软件界面，作为BIOS的替代方案
- 不像是BIOS那样是固件又是接口，UEFI只是一个接口



UEFI固件规范

- 兼容传统Legacy BIOS 模式（ CSM兼容性支持模块）

- 要求 支持UEFI的 固件必须能识别 GPT，也要求能识别 MBR，以保证向后兼容
- 必须能读取 FAT 格式的变种（ FAT16 和 FAT32等）
- 定义了一种可执行文件格式.efi，并要求所有支持 UEFI 的固件能够执行此格式的代码

ESP分区

- EFI System Partition

  GUID:　C12A7328-F81F-11D2-BA4B-00A0C93EC93B
- 本质上为FAT分区
- ├-BOOT　传统BIOS

  └EFI　　UEFI

UEFI 设置程序

- “UEFI 启动管理器是一种固件策略引擎，可通过修改固件架构中定义的全局NVRAM 变量来进行配置。启动管理器将尝试按全局 NVRAM 变量定义的顺序依次加载 UEFI 驱动和 UEFI 应用程序（包括 UEFI 操作系统启动装载程序）。”
- 使用NVRAM存储数据
- 启动管理器->ESP分区->.efi文件->系统引导

BIOS

- 汇编
- 16位
- 只可选取启动磁盘
- 引导文件与系统都在主分区
- BIOS->自检(POST)->MBR->活动主分区->bootmgr->系统引导

UEFI

- C语言
- 32/64位
- 有boot menu，可修改
- 引导文件独立分区（ESP）
- (自检)启动管理器->FAT分区->.efi文件->系统引导

windows引导

- BCD（boot configuration data）引导配置数据

  含有Windows操作系统的启动参数配置信息
- BCD文件可以用EasyBCD等查看编辑

BIOS启动windows10流程

- BIOS->MBR->活动的主分区->\bootmgr->\Boot\BCD->\Windows\system32\winload.exe

- Bootmgr is missing

UEFI启动Windows10流程

- .efi文件
- bootx64.efi 是计算机默认引导文件
  bootmgfw.efi 是 Windows默认引导文件

- UEF->ESP分区->\efi\boot\Microsoft\boot\bootmgfw.efi
  ->efi\Microsoft\BCD->\Windows\system32\winload.efi

参考链接

- http://bbs.wuyou.net/forum.php?mod=viewthread&tid=299643
- http://bbs.wuyou.net/forum.php?mod=viewthread&tid=303679&fromuid=396698
- https://blog.woodelf.org/2014/05/28/uefi-boot-how-it-works.html
- https://mp.weixin.qq.com/s/vVIa3Gc25VscX-QbZxLhhw
- https://zh.wikipedia.org/wiki/GUID%E7%A3%81%E7%A2%9F%E5%88%86%E5%89%B2%E8%A1%A8
- https://zh.wikipedia.org/wiki/BIOS
- https://zh.wikipedia.org/wiki/%E4%B8%BB%E5%BC%95%E5%AF%BC%E8%AE%B0%E5%BD%95