

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

00000000	03 C0 8E D0 BC 00 7C 8E C0 8E D8 BE 00 7C BF 00	3.....
00000010	06 B9 00 02 FC F3 A4 50 68 1C 06 CB FB B9 04 00Ph.....
00000020	BD BE 07 80 7E 00 00 7C 0B 0F 85 0E 01 83 C5 10~..
00000030	E2 F1 CD 18 88 56 00 55 C6 46 11 05 C6 46 10 00V.U.F...F..
00000040	B4 41 BB AA 55 CD 13 5D 72 0F 81 FB 55 AA 75 09	.A..U..}r...U.u.
00000050	F7 C1 01 00 74 03 FE 46 10 66 60 80 7E 10 00 74t..F.f'..~..t
00000060	26 66 68 00 00 00 00 66 FF 76 08 68 00 00 68 00	&fh....f.v.h..h.
00000070	7C 68 01 00 68 10 00 B4 42 8A 56 00 8B F4 CD 13	h..h...B.V.....
00000080	9F 83 C4 10 9E EB 14 B8 01 02 BB 00 7C 8A 56 00V.
00000090	8A 76 01 8A 4E 02 8A 6E 03 CD 13 66 61 73 1C FE	.v..N..n...fas..
000000A0	4E 11 75 0C 80 7E 00 80 0F 84 8A 00 B2 80 EB 84	N.u..~.....
000000B0	55 32 E4 8A 56 00 CD 13 5D EB 9E 81 3E FE 7D 55	U2..V...]}...>}.U
000000C0	AA 75 6E FF 76 00 E8 8D 00 75 17 FA B0 D1 E6 64	.un.v....u.....d
000000D0	E8 83 00 B0 DF E6 60 E8 7C 00 80 FF E6 64 00 75d.u
000000E0	00 FB B8 00 BB CD 1A 66 23 C0 75 3B 66 81 FB 54f..f..T
000000F0	43 50 41 75 32 81 F9 02 01 72 2C 66 68 07 BB 00	CPAu2....r,fh...
00000100	00 66 68 00 02 00 00 66 68 08 00 00 00 66 53 66	.fh....fh....fSf
00000110	53 66 55 66 68 00 00 00 00 66 68 00 7C 00 00 66	SfUfh....fh. ..f
00000120	61 68 00 00 07 CD 1A 5A 32 F6 EA 00 7C 00 00 CD	ah.....Z2... ...
00000130	18 A0 B7 07 EB 08 A0 B6 07 EB 03 A0 B5 07 32 E42.
00000140	05 00 07 8B F0 AC 3C 00 74 09 BB 07 00 B4 0E CD<.t.....
00000150	10 EB F2 F4 EB FD 2B C9 E4 64 EB 00 24 02 E0 F8+..d..\$...
00000160	24 02 C3 49 6E 76 61 6C 69 64 20 70 61 72 74 69	\$..Invalid parti
00000170	74 69 6F 6E 20 74 61 62 6C 65 00 45 72 72 6F 72	tion table.Error
00000180	20 6C 6F 61 64 69 6E 67 20 6F 70 65 72 61 74 69	loading operati
00000190	6E 67 20 73 79 73 74 65 6D 00 4D 69 73 73 69 6E	ng system.Missin
000001A0	67 20 6F 70 65 72 61 74 69 6E 67 20 73 79 73 74	g operating syst
000001B0	65 6D 00 00 00 63 7B 9A AE F7 6A EC 00 00 80 20	em...c{...j....
000001C0	21 00 07 FE FF FF 00 08 00 00 00 F0 DF 01 00 00	!.....
000001D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001F0	00 00 00 00 00 00 00 00 00 00 00 00 55 AAU.

引导代码
(MBR)

分区表
(DPT)

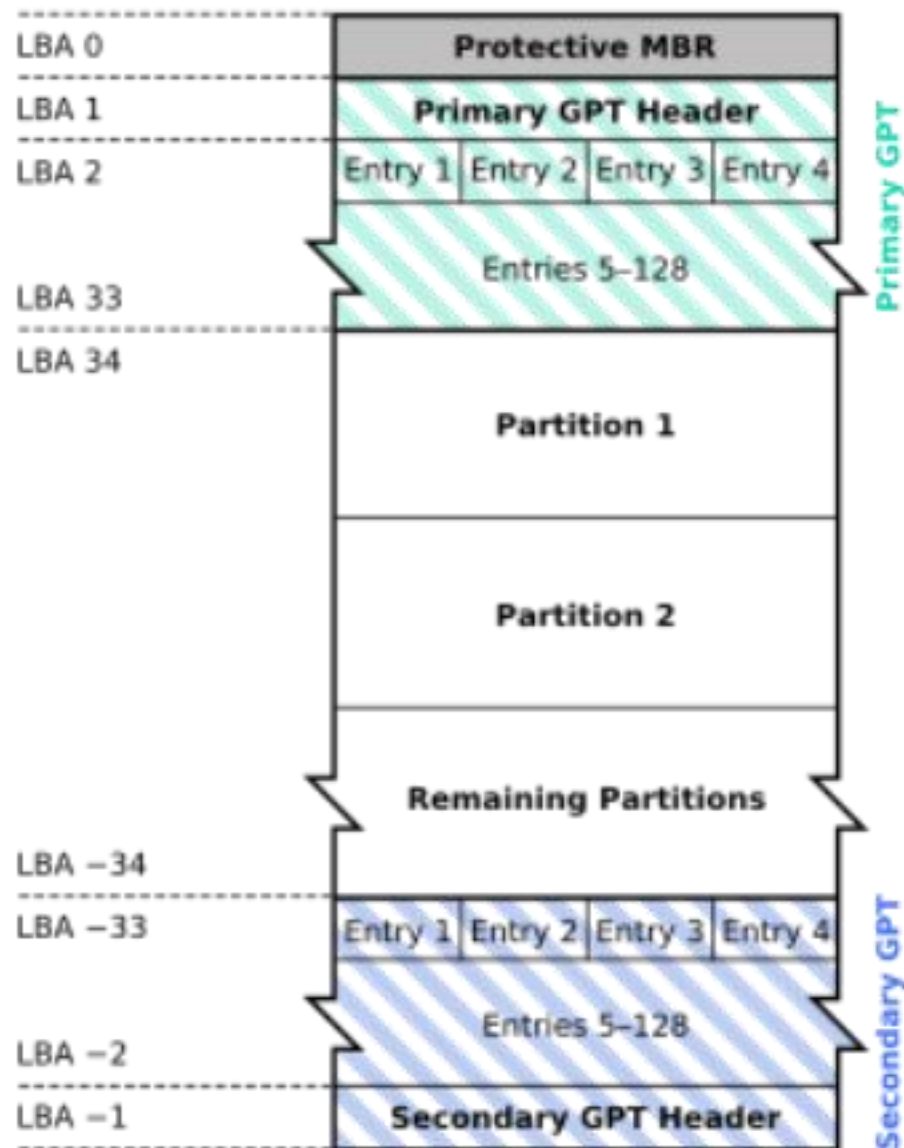
结束标志
(55AA)

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 Partition Table Scheme



GUID类型

- C12A7328-F81F-11D2-BA4B-00A0C93EC93B
- E3C9E316-0B5C-4DB8-817D-F92DF00215AE
- EBD0A0A2-B9E5-4433-87C0-68B6B72699C7

分区名

EFI系统分区

微软保留（MSR）分区

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

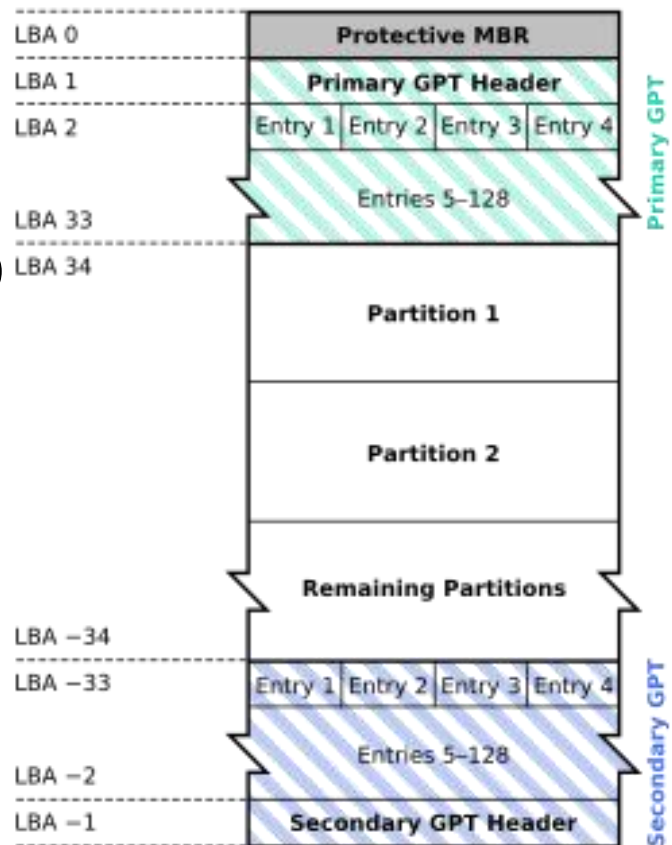
- 分区表头

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

GUID Partition Table Scheme



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

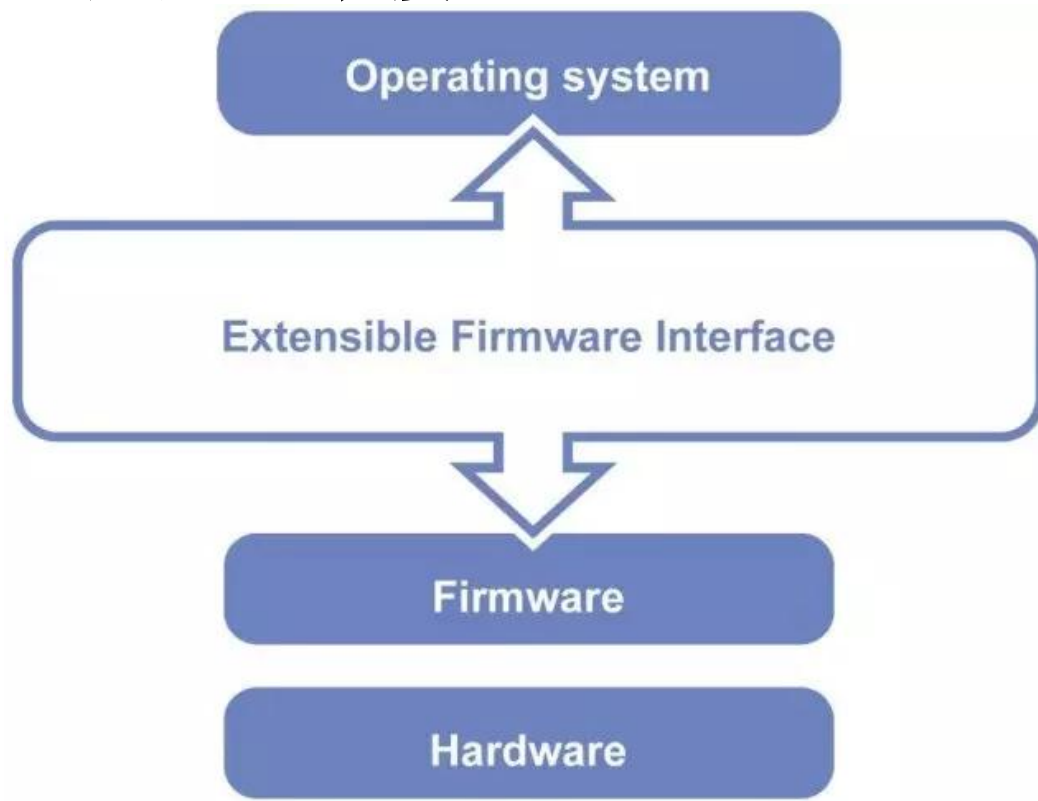
EFI

- 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/vVla3Gc25VscX-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>