硬盘主引导扇区、分区表和分区引导扇区(MBR、DPT、DBR、BPB)详解（转自无忧存储网）

http://simg.sinajs.cn/blog7style/images/common/sg_trans.gif (2011-10-07 21:46:14)

[[http://simg.sinajs.cn/blog7style/images/common/sg_trans.gif](javascript:;)转载▼](javascript:;)

|  |  |
| --- | --- |
| 标签：  [it](http://search.sina.com.cn/?c=blog&q=it&by=tag) | 分类： [IT\_硬盘及多系统](http://blog.sina.com.cn/s/articlelist_1439502415_7_1.html) |

硬 盘的主引导扇区，分区表，分区引导扇区(MBR、DPT、DBR、BPB)是电脑BIOS 自检完成后，操作系统开始引导系统前整个电脑运作过程中需要检查的重要参数，硬盘的主引导扇区，分区表，分区引导扇区(MBR、DPT、DBR、BPB) 参数错误可能导致系统无法启动或存储的数据丢失，这片文章我们介绍一下硬盘的主引导扇区，分区表，分区引导扇区(MBR、DPT、DBR、BPB)的详细 信息。

　 　硬盘的0柱面、0磁头、1扇区称为主引导扇区（也叫主引导记录MBR），该记录占用 512个字节，它用于硬盘启动时将系统控制权转给用户指定的、在分区表中登记了某个操作系统分区。MBR的内容是在硬盘分区时由分区软件（如FDISK） 写入该扇区的，MBR不属于任何一个操作系统，不随操作系统的不同而不同，即使不同，MBR也不会夹带操作系统的性质，具有公共引导的特性。但安装某些多 重引导功能的软件或LINUX的LILO时有可能改写它；它先于所有的操作系统被调入内存并发挥作用，然后才将控制权交给活动主分区内的操作系统（下 图）。

[](http://photo.blog.sina.com.cn/showpic.html#blogid=55cd104f0100xxcb&url=http://s4.sinaimg.cn/orignal/55cd104fhaeb5b0a84213)

MBR由三部分构成：

　　1．主引导程序代码，占446字节

　　2．硬盘分区表DPT，占64字节

　　3．主引导扇区结束标志AA55H

   　一、硬盘的主引导程序代码是从偏移0000H开始到偏移01BDH结束的446字节； 主引导程序代码包括一小段执行代码。启动PC 机时，系统首先对硬件设备进行测试，成功后进入自举程序INT 19H；然后读系统磁盘0柱面、0磁头、1扇区的主引导扇区MBR的内容到内存指定单元0：7C00 首地址开始的区域，并执行MBR程序段。

　　主引导代码实现下列功能：

　　1．扫描分区表查找活动分区；

　　2．寻找活动分区的起始扇区；

　　3．将活动分区的引导扇区读到内存；

　　4．执行引导扇区的运行代码。

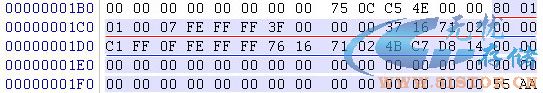
　　如果主引导代码未完成这些功能，系统显示下列错误信息：

　　Invalid partition table

　　Error loading operating system

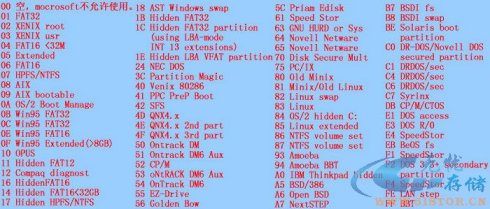
　　Missing operating system

　 　二、硬盘分区表DPT是从偏移01BEH开始到偏移01FDH结束的64字节（下图）； 硬盘分区表分为四小部分，每一小部分表示一个分区的信息，占16字节。在这里我们可以看出，硬盘的总分区数为什么不能大于4。其中可激活分区数不得大于 3，扩展分区数不得大于1，当前活动分区数必须小于等于1。

[](http://photo.blog.sina.com.cn/showpic.html#blogid=55cd104f0100xxcb&url=http://s11.sinaimg.cn/orignal/55cd104fhaeb5b87a06aa)

分区表的每一分区的第0个字节是自举标志，其值为80H时，表示该分区是当前活动分区，可引导，其值为00H时，表示该分区不可引导。

　　第4字节是分区类型（下图）。

[](http://photo.blog.sina.com.cn/showpic.html#blogid=55cd104f0100xxcb&url=http://s4.sinaimg.cn/orignal/55cd104fhaeb5bb7b6c13)

每 一分区的第1至第3字节是该分区起始地址。其中第1字节为起始磁头号（面号）；第2字 节的低6位为起始扇区号，高2位则为起始柱面号的高2位；第3字节为起始柱面号的低8位。因此，分区的起始柱面号是用10位二进制数表示的，最大值为 2^10 = 1024，因逻辑柱面号从0开始计，故柱面号的显示最大值为1023。同理，用6位二进制数表示的扇区号不会超过2^6 - 1 = 63；用8位二进制数表示的磁头号不会超过2^8 - 1 = 255。每一分区的第5至第7字节表示分区的终止地址，各字节的释义与第1至第3字节相同。这里我们假设一种极端的情况：如果让第5至第7字节的所有二进 制位都取1，就获得了柱面号、磁头号和扇区号所能表示的最大值，从而得到最大绝对扇区号为：

　　1024 × 256 × 63 = 16,515,072

　　这个扇区之前的所有物理扇区所包含的字节数为：

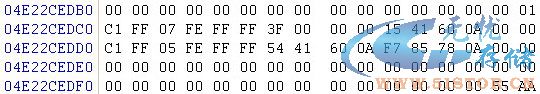
　　16,515,072 × 512Bytes ≈ 8.46GB。

　 　由此可知硬盘的容量设计为什么会有8.4GB这一档，分区表每一分区的第1至第3字节以 及第5至第7字节的数据结构已经不能满足大于8.46GB的大容量硬盘的需要。考虑到向下兼容的需要，业界并未对从DOS时代就如此定义的硬盘分区表提出 更改意见，否则改动所牵涉的面太广，会造成硬件和软件发展上的一个断层，几乎无法被业界和用户所接受。硬盘厂商解决这一问题的方法是定义了新的INT 13服务扩展标准。新的INT 13服务扩展标准不再使用操作系统的寄存器传递硬盘的寻址参数，而使用存储在操作系统内存里的地址包。地址包里保存的是64位LBA地址，如果硬盘支持 LBA寻址，就把低28位直接传递给ATA接口，如果不支持，操作系统就先把LBA地址转换为CHS地址，再传递给ATA接口。通过这种方式，能实现在 ATA总线基础上CHS寻址的最大容量是136.9 GB，而LBA寻址的最大容量是137.4GB。新的硬盘传输规范ATA 133规范又把28位可用的寄存器空间提高到48位，从而支持更大的硬盘。

　 　分区表每一分区的第8至第11字节表示该分区的起始相对扇区数（即该扇区之前的绝对扇区 个数），高位在右，低位在左；第12至第15字节表示该分区实际占用的扇区数，也是高位在右，低位在左；分区表这类数据结构的表达方式与机器中数据的实际 存储方式在顺序上是一致的，即低位在前，高位在后。因此，在从16进制向十进制作数值转换时，需将字段中的16进制数以字节为单位翻转调位，用4个字节可 以表示最大2^32个扇区，即2TB=2048GB。

系 统在分区时，各分区都不允许跨柱面，即均以柱面为单位，这就是通常所说的分区粒度。在未超 过8.4GB的分区上，C/H/S的表示方法和扇区数的表示方法所表示的分区大小是一致的。超过8.4GB的/H/S/C一般填充为FEH/FFH /FFH，即C/H/S所能表示的最大值；有时候也会用柱面对1024的模来填充。不过这几个字节是什么其实都无关紧要了。

　　扩展分区中的每个逻辑驱动器都存在一个类似于MBR的扩展引导记录（Extended Boot Record，EBR）（下图）。

[](http://photo.blog.sina.com.cn/showpic.html#blogid=55cd104f0100xxcb&url=http://s16.sinaimg.cn/orignal/55cd104fhaeb5bfd9822f)

扩 展引导记录包括一个扩展分区表和扇区结束标志55AA。一个逻辑驱动器中的引导扇区一 般位于相对扇区32或63。如果磁盘上没有扩展分区，那么就不会有扩展引导记录和逻辑驱动器。第一个逻辑驱动器的扩展分区表中的第一项指向它自身的引导扇 区；第二项指向下一个逻辑驱动器的EBR，如果不存在进一步的逻辑驱动器，第二项就不会使用，而被记录成一系列零。如果有附加的逻辑驱动器，那么第二个逻 辑驱动器的扩展分区表的第一项会指向它本身的引导扇区，第二个逻辑驱动器的扩展分区表的第二项指向下一个逻辑驱动器的EBR。扩展分区表的第三项和第四项 永远都不会被使用。

　　扩展分区表项中的相对扇区数是从扩展分区开始的扇区到该逻辑驱动器中第一个扇区的扇区数；占用的扇区数是指组成该逻辑驱动器的扇区数目。

      有时候在磁盘的末尾会有剩余空间，由于分区是以1柱面的容量为分区粒度的，那么如果磁盘总空间不是整数个柱面的话，不够一个柱面的剩下的空间就是剩余空间了，这部分空间并不参与分区，所以一般无法利用。

　　三、主引导扇区的最后两个字节（偏移1FEH和偏移1FFH），其值为AA55H，它表示该扇区是个有效的引导扇区，可用来引导硬磁盘系统。

　 　分区引导扇区DBR(DOS BOOT RECORD)是由FORMAT高级格式化命令写到该扇区的内容；DBR是由硬盘的MBR装载的程序段。DBR装入内存后，即开始执行该引导程序段，其主 要功能是完成操作系统的自举并将控制权交给操作系统。每个分区都有引导扇区，但只有被设为活动分区的DBR才会被MBR装入内存运行。

        DBR主要由下列几个部分组成：

　        　1．跳转指令，占用3个字节的跳转指令将跳转至引导代码。

        　　2．厂商标识和DOS版本号，该部分总共占用8个字节。

　        　3．BPB（BIOS Parameter Block， BIOS 参数块）。

        　　4．操作系统引导程序。

        　　5．结束标志字，结束标志占用2个字节，其值为AA55

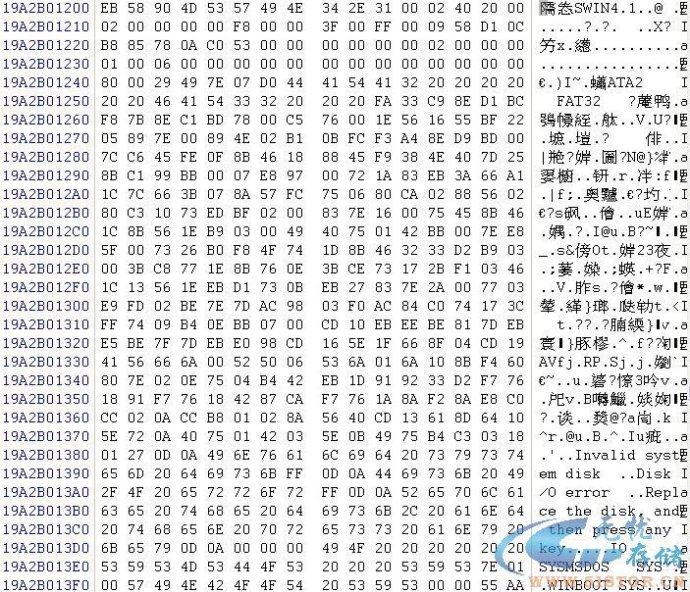
　　DBR中的内容除了第5部分结束标志字固定不变之外，其余4个部分都是不确定的，其内容将随格式化所用的操作系统版本及硬盘的逻辑盘参数的变化而变化。

　　一、FAT32的分区引导扇区

　 　为了使加载文件的操作更加灵活，加上FAT32文件系统采用"活动"的FDT表，，同时 考虑到引导程序的代码量和为今后发展保留适当的余量，FAT32文件系统分区引导扇区占据了6个扇区，只有前3个扇区作为系统的分区引导扇区，其余3个扇 区保留暂未使用。分区引导扇区对于操作系统的启动和磁盘文件的访问具有至关重要的作用；引导程序代码的损坏将导致操作系统不能正常启动，磁盘读写参数的破 坏将造成存储在磁盘上的文件不能正常读写。

　 　由于分区引导扇区的重要性，FAT32文件系统在在第一个分区引导扇区的6个扇区后的6 个扇区里保留了分区引导扇区的备份，在启动时操作系统可以对两份引导扇区进行比较，以便选择正确的引导扇区来引导系统。由于在磁盘正常工作过程中系统不再 对引导扇区的程序和数据进行修改，因此备份的分区引导扇区损坏的可能性非常小。

　　分区引导扇区的第一个扇区（图六）的前三个字节是一条跳转指令，然后是8个字节长的OEM ID（厂家标识）和版本号，其后是简称为BPB的BIOS参数块（BIOS Parameter Block）。

[](http://photo.blog.sina.com.cn/showpic.html#blogid=55cd104f0100xxcb&url=http://s11.sinaimg.cn/orignal/55cd104fhaeb5c3e2325a)

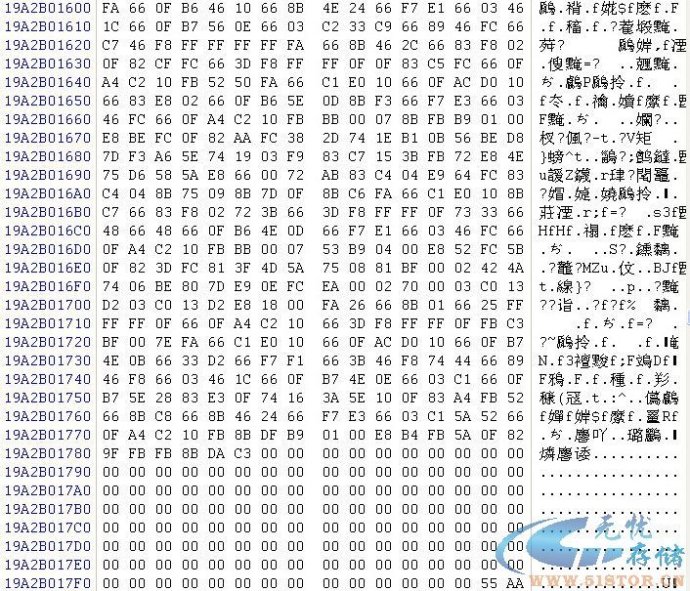
对于FAT32其各部分的意义如下表：  
[](http://photo.blog.sina.com.cn/showpic.html#blogid=55cd104f0100xxcb&url=http://s7.sinaimg.cn/orignal/55cd104fhaeb5c757b0e6)  
  
  
从偏移0x5A开始的数据为操作系统引导代码。这是由偏移0x00开始的跳转指令所指向的，此段指令在不同的操作系统上和不同的引导方式上，其内容也是不同的。

　　扇区的最后两个字节存储值为0x55AA的DBR有效标志，对于其他的取值，系统将不会执行DBR相关指令。

分 区引导扇区的第2个扇区作为文件系统相关参数存储标识扇区（下图），除了保存扇区的标识信 息（RraA（00H）和rrAa（1E4H））外，还可能在偏移地址1E8H处存储了文件系统有关的信息。其中扇区偏移地址1E8H～1EBH的4个字 节存储了逻辑磁盘中未使用的簇数，通常用于快速计算逻辑磁盘的剩余空间（典型的操作是在资源管理器状态栏上列出的"可用磁盘空间"参数），而 1ECH～1EFH 4个字节给出了逻辑盘中下一个可以分配给文件使用的空闲簇的簇号，这样操作系统可以不访问FAT表就直接获得磁盘剩余空间和可以分配的簇号。

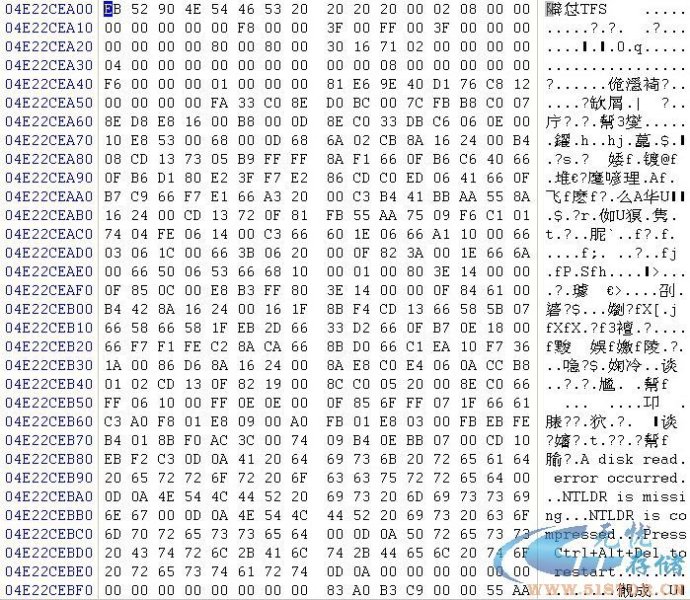
[](http://photo.blog.sina.com.cn/showpic.html#blogid=55cd104f0100xxcb&url=http://s8.sinaimg.cn/orignal/55cd104fhaeb5ccb3b9f7)

分区引导扇区的第3个扇区则存储了引导扇区的后一部分引导系统的程序代码（下图）。

[](http://photo.blog.sina.com.cn/showpic.html#blogid=55cd104f0100xxcb&url=http://s9.sinaimg.cn/orignal/55cd104fhaeb5db8231e8)

二、NTFS的分区引导扇区

　　对于NTFS分区来说，分区引导扇区DBR只占用一个扇区（下图），并且在该分区的最后一个扇区做了备份；NTFS的引导扇区也是完成引导和定义分区参数，NTFS分区的引导扇区不是分区的充分条件，它要求必须MFT中的系统记录如$MFT等正常该分区才能正常访问。

[](http://photo.blog.sina.com.cn/showpic.html#blogid=55cd104f0100xxcb&url=http://s1.sinaimg.cn/orignal/55cd104fhaeb5df7eede0)

其BPB参数如下表所示：  
[](http://photo.blog.sina.com.cn/showpic.html#blogid=55cd104f0100xxcb&url=http://s3.sinaimg.cn/orignal/55cd104fhaeb5e317aef2)