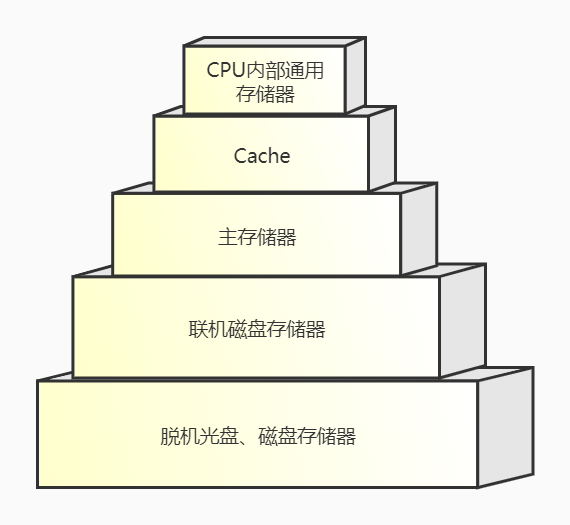
# 1.2计算机体系结构

## 1.2.2存储系统

### 1.存储器的层次结构

**计算机系统内的各种存储器：**CPU内部的通用寄存器组、CPU内的Cache（高速缓存）、CPU外部的Cache、主板上的主存储器、主板外的联机（在线）磁盘存储器以及脱机（离线）的磁带存储器和光盘存储器等。

**计算机的存储体系结构：**不同特点的存储器通过适当的硬件、软件有机地组合在一起形成计算机的存储体系结构。



图：存储系统的层次结构

其中，Cache和主存之间的交互功能全部由硬件实现，而主存与辅存之间的交互功能可由硬件和软件结合起来实现。

1.1虚拟地址和物理地址

虚拟地址对应虚存容量（比主存实际空间大得多）

物理地址对应主存容量

1.2层次结构

层次结构分为2种：主存-辅存、cache-主存。

构成三级存储层次：cache-主存-辅存。

### 2.存储器的分类

#### 1)按存储器所处的位置分类



按存储器所处位置可分为**内存**和**外存**。

**（1）内存（主存）**

**所处位置：**设在主机内或主机板上

**存放内容：**用来存放机器当前运行所需要的程序和数据，以便向CPU提供信息。

**与外存比较的特点：**容量小、速度快。

**（2）外存（辅存）**

**外存举例：**如磁盘、磁带和光盘等。

**存放内容：**用来存放当前不参加运行的大量信息，在需要时调入内存。

#### 2)按存储器的构成材料分类



按构成存储器的材料可分为**磁存储器**、**半导体存储器**和**光存储器**。

**（1）磁存储器**

**构成：**磁存储器是用磁性介质做成的。

**磁存储器举例：**如磁芯、磁泡、磁膜、磁鼓、磁带及磁盘等。

**（2）半导体存储器**

**根据所用元件可分为：**双极型和MOS型。

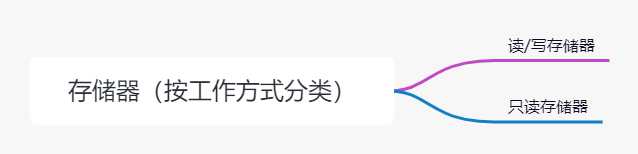
**根据数据是否需要刷新分为：**静态（Static Memory）和动态（Dynamic Memory）。

**（3）光存储器**

利用光学方法读/写数据的存储器。

**光存储器举例：**如光盘。

#### 3)按存储器的工作方式分类



按存储器的工作方式可分为**读/写存储器**和**只读存储器**。

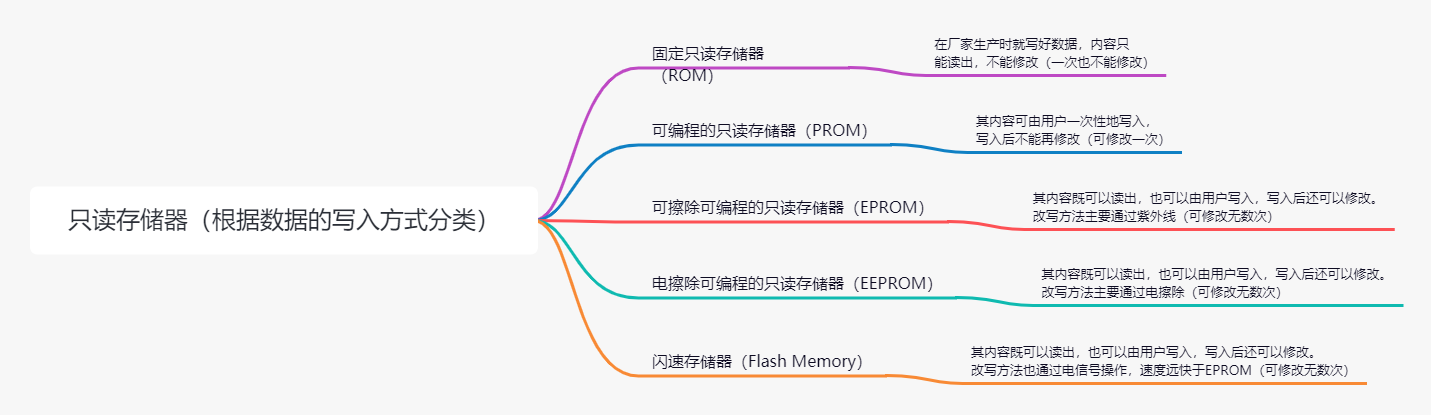
**（1）读/写存储器（Random Access Memory，RAM）**

它指既能读取数据也能存入数据的存储器。

**（2）只读存储器**

它指工作过程中仅能读取的存储器。

**根据数据的写入方式可分为：**ROM、PROM、EPROM和EEPROM等类型。



**①固定只读存储器（Read Only Memory，ROM）（不可修改）**

**特点：**在厂家生产时就写好数据的，其内容只能读出，不能改变。一般用于存放系统程序BIOS和用于微程序控制。

**②可编程的只读存储器（Programmable Read Only Memory，PROM）（可修改1次）**

**特点：**其中的内容可以由用于一次性地写入，写入后不能再修改。

**③可擦除可编程的只读存储器（Erasable Programmable Read Only Memory,EPROM）（可修改无数次）**

**特点：**其中的内容既可以读出，也可以由用户写入，写入后还可以修改。

**改写的方法：**写入之前先用紫外线照射15~20分钟以擦去所有信息，然后再用特殊的电子设备写入信息。

**④电擦除可编程的只读存储器（Electrically Erasable Programmable Read Only Memory,EEPROM）（可修改无数次）**

**与EPROM的异同：**与EPROM相似，EEPROM中的内容既可以读出，也可以进行改写。只不过这种存储器是用电擦除的方法进行数据的改写。

**⑤闪速存储器（Flash Memory），简称闪存（可修改无数次）**

**特点：**闪存的特性介于EPROM和EEPROM之间，类似于EEPROM，也可使用电信号进行信息的擦除操作。整块闪存可以在数秒内删除，速度远快于EPROM。

**与EEPROM的关系：**就其本质而言，Flash Memory属于EEPROM(电擦除可编程只读存储器)类型。它既有ROM的特点，又有很高的存取速度，而且易于擦除和重写，功耗很小。

**RAM和ROM区别：**

RAM是**随机存取存储器（random access memory）**，是计算机内部存储器中的一种，也是其中最重要的，计算机和手机中一般把其叫做（运行）内存，它的速度要比硬盘快得多，所以用运行程序在RAM中，而存放运行时不用的数据则在硬盘中，什么时候需要数据，便把数据从硬盘中拿到内存，但同时RAM断电会丢失数据，所以我们电脑如果断电了就会丢失原来正在运行的数据。所以，手机中的RAM和电脑中的RAM的概念是相同的，RAM即内存越大，能同时在内存中执行的程序就越多，性能一般是越好的。

ROM是**只读存储器（Read-Only Memory）**，也是计算机内部存储器中的一种，而硬盘是外部存储器。这就要从其发展历程说起，早期，乃至现在，我们的主要存储介质都是磁性存储，也就是磁盘，分为硬盘和软盘，硬盘不太适合做移动存储，因为其磁头容易损坏，不耐摔，而且体积较大，就算是缩小容量仍然很难缩小其体积，软盘虽然用作移动介质还算方便，但软盘容量过于小，不够用，而光盘虽然容量大但不易擦写，同时体积也不够小，这时就很适合使用半导体存储介质——ROM和RAM，ROM用来嵌入电脑主板或者做移动存储介质就很合适了，其体积够小，提供的容量可以比光盘和软盘的大，速度也更快，但成本相对更高，而且早期的ROM因为技术不成熟所以无法擦写，出厂后就只能读数据，所以叫只读存储器，后来随着技术的发展，在ROM的基础上出现了新的半导体存储介质EPROM和EEPROM，这两种可擦写，这就不符合ROM的命名，但是由于是在ROM的技术上衍变出来的，所以延用了一部分原来的叫法，此时非易失的半导体存储介质开始得以广泛应用，被大量用于电脑主板的bios和嵌入式存储，而后来在这两种技术的发展上又发展出了NAND FLASH闪存，这就是我们现在用的U盘中用到的技术，同样，因为其体积小，容量和速度均不错，现在手机存储中的emmc颗粒也是用的这种技术，所以有手机厂商就把手机的存储容量约定俗成为ROM，其继承ROM断电不丢失数据的特性，而且有着较快的速度。

RAM与ROM都属于内存，广义上内存指**Cache**、**ROM**和**RAM**三部分，其中Cache现在是做在CPU里面的，ROM在主板上，用来存放BIOS，装机内存指的是RAM。

**BIOS定义:**BIOS是英文"Basic Input Output System"的[缩略词](https://baike.baidu.com/item/%E7%BC%A9%E7%95%A5%E8%AF%8D)，直译过来后中文名称就是"基本输入输出系统"。在[IBM](https://baike.baidu.com/item/IBM/9190) PC兼容系统上，是一种业界标准的[固件](https://baike.baidu.com/item/%E5%9B%BA%E4%BB%B6/627829)[接口](https://baike.baidu.com/item/%E6%8E%A5%E5%8F%A3/2886384)。BIOS这个字眼是在1975年第一次由[CP/M](https://baike.baidu.com/item/CP/M/9092795)操作系统中出现。 BIOS是[个人电脑](https://baike.baidu.com/item/%E4%B8%AA%E4%BA%BA%E7%94%B5%E8%84%91/3688503)启动时加载的第一个软件。其实，它是一组固化到[计算机](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA)内[主板](https://baike.baidu.com/item/%E4%B8%BB%E6%9D%BF)上一个[ROM](https://baike.baidu.com/item/ROM)[芯片](https://baike.baidu.com/item/%E8%8A%AF%E7%89%87)上的[程序](https://baike.baidu.com/item/%E7%A8%8B%E5%BA%8F)，它保存着计算机最重要的基本输入输出的程序、开机后自检程序和系统自启动程序，它可从[CMOS](https://baike.baidu.com/item/CMOS/428167)中读写系统设置的具体信息。

#### 4)按访问方式分类



按访问方式可分为**按地址访问的存储器**和**按内容访问的存储器**。

**（1）按地址访问的存储器**

有**随机存储器**、**顺序存储器**和**直接存储器**。

**（2）按内容访问的存储器**

有**相联存储器**。

#### 5)按寻址方式分类



按寻址方式可分为**随机存储器**、**顺序存储器**和**直接存储器**。

**（1）随机存储器（Random Access Memory,RAM）**

这种存储器可对任何存储单元存入或读取数据，访问任何一个存储单元所需的时间是相同的。

**（2）顺序存储器（Sequentially Addressed Memory，SAM）**

访问数据所需要的时间与数据所在的存储位置相关，磁带是典型的顺序存储器。

**（3）直接存储器（Direct Addressed Memory,DAM）**

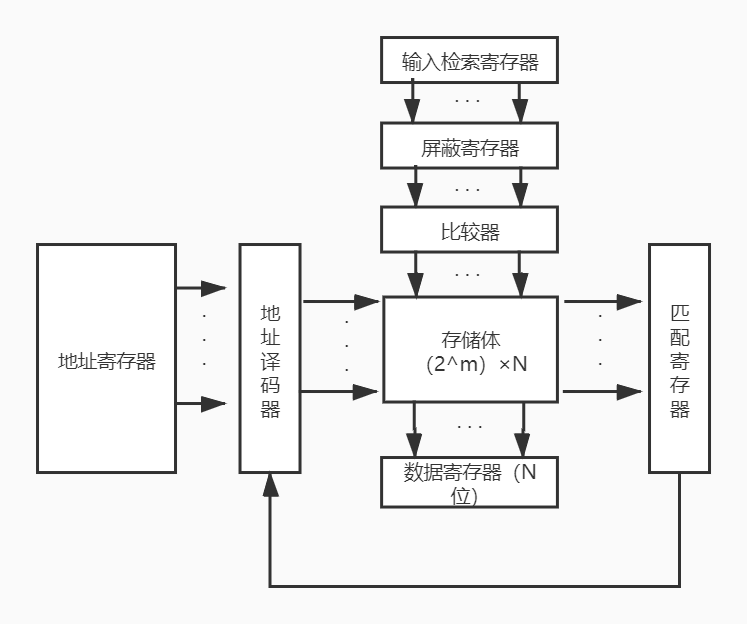
介于随机存取和顺序存取之间的一种寻址方式。磁盘是一种直接存取存储器，它对磁道的寻址是随机的，而在一个磁道内则是顺序寻址。

### 3.相联存储器（Content Addressable Memory，CAM）

**相联存储器特点：**按内容访问的存储器。

**工作原理：**当对其写入数据时，CAM能够自动选择一个未用的空单元进行存储；当要读出数据时，不是给出其存储单元的地址，而是直接给出该数据或者该数据的一部分内容，CAM对**所有**的存储单元中的数据**同时进行比较**并标记**符合条件的所有数据**以供读取。由于比较是同时、并行进行的，所以这种基于数据内容进行读/写的机制，其速度比基于地址进行读/写的方式要快许多。

**适用场景：**特别适合于信息的检索和更新。



图：相联存储器的结构框图

其中，输入检索寄存器用来存放要检索的内容（关键字），屏蔽寄存器用来屏蔽那些不参与检索的字段，比较器将检索的关键字与存储体的每一单元进行比较。为了提高速度，比较器的数量应很大。对于位比较器，应每位对应一个，应有2m×N个，对于字比较器应有2m个。匹配寄存器用来记录比较的结果，它应有2m个二进制位，用来记录2m个比较器的结果，1为相等（匹配），0为不相等（不匹配）。

**应用情况：**可用在高速缓冲存储器中，在虚拟存储器中用来作为段表、页表或快表存储器，用在数据库和知识库中。

### 4.高速缓存

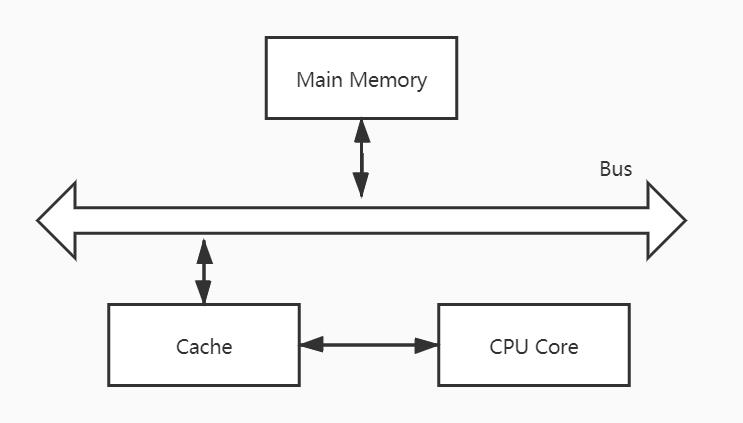
**存放内容：**高速缓存用来存放当前最活跃的程序和数据。

**特点：**

1. 位于CPU与主存之间。
2. 容量一般在几千字节到几兆字节之间。
3. 速度一般比主存快5-10倍，由快速半导体存储器构成（静态随机存储器SRAM）。
4. 其内容是主存局部域的副本，对程序员来说是透明的。

#### 1)高速缓存的组成

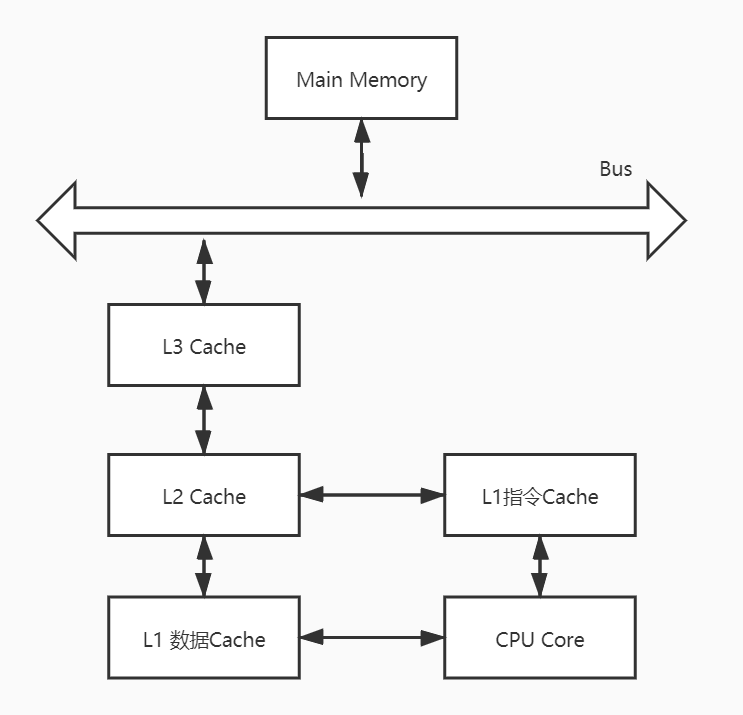
高速缓存（Cache）、主存（Main Memory）与CPU的关系如图所示：



图：高速缓存、主存和CPU的关系示意图

Cache存储器部分用来存放主存的部分拷贝（副本）信息。控制部分的功能是判断CPU要访问的信息是否在Cache存储器中，若在即为命中，若不在则没有命中。命中时直接对Cache存储器寻址；未命中时，要按照替换原则决定主存的一块信息放到Cache存储器的哪一块里。

现代CPU中Cache分为了多个层级，如图所示：



图：三级Cache示意图

在L1中还分数据Cache（D-Cache）和指令Cache（I-Cache）。它们分别用来存放数据和执行这些数据的指令，而且两个Cache可以同时被CPU访问，减少了争用Cache所造成的冲突，提高了处理器效能。

1.1.2主存和cache的基本结构

1. 主存

主存有2n个单元，地址码为n位，n=m+b：主存的块数M=2m块，块内的字节数（存储单元数即容量）B=2b

1. cache

cache地址码为（c+b），cache的块数为2c，块内字节数为2b与主存相同。cache中，每一块外加一个标记，指明它是主存的哪一块副本。

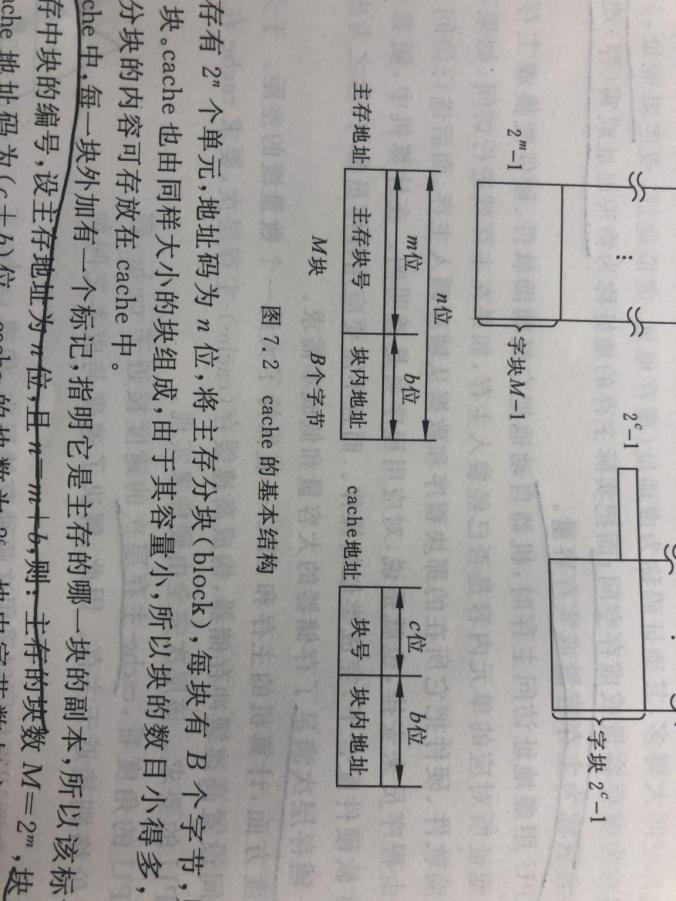


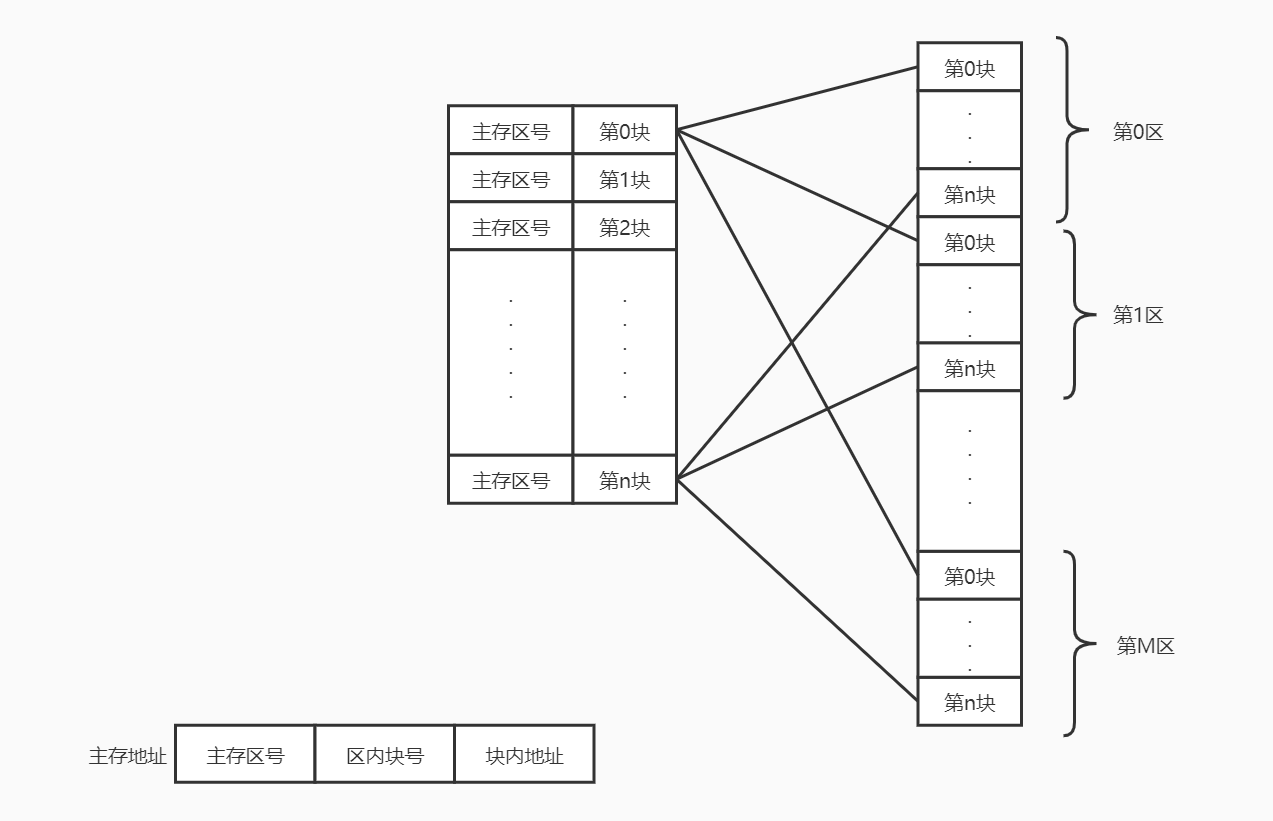
图 1主存和cacha的基本结构

#### 2)高速缓存中的地址映像方法

在CPU工作时，送出的是主存单元的地址，而应从Cache存储器中读/写信息。这就需要将主存地址转换成Cache存储器的地址，这种地址的转换称为地址映像。Cache的地址映像有以下三种方法：

**（1）直接映像**

直接映像指主存的块与Cache块的对应关系是固定的，如图所示：



图：直接映像示意图

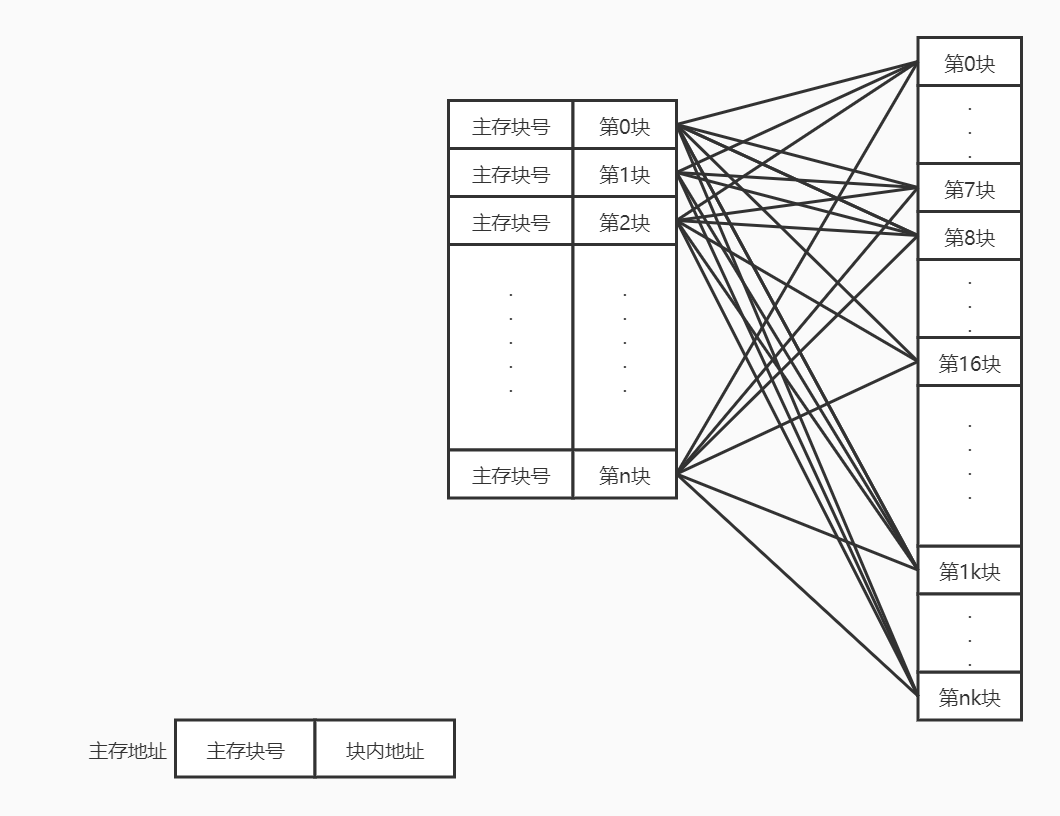
在这种映像方式下，由于主存中的块只能存放在Cache存储器的相同块号中，因此，只要主存地址中的主存区号与Cache中记录的主存区号相同，则表明访问Cache命中。一旦命中，由主存地址中的区内块号立即可得到要访问的Cache存储器中的块，而块内地址就是主存地址中给出的低位地址。

**优点：**地址变换简单。

**缺点：**灵活性差。例如，不同区号中块号相同的块无法同时调入Cache存储器，即使Cache存储器中有空着的块也不能利用。

**（2）全相联映像**

全相联映像如图所示。



图：全相联映像示意图

同样，主存与Cache存储器均分成大小相同的块。

**特点：**允许主存的任一块可以调入Cache存储器的任何一个块的空间中。

**地址变换过程：**利用主存地址高位表示的主存块号与Cache中相联存储器所有单元中记录的主存块号进行比较，若相同即为命中。这时相联存储器单元的编号就对应要访问Cache的块号，从而在相应的Cache块中根据块内地址访问到相应的存储单元。

**优点：**主存的块调入Cache的位置不受限制，十分灵活。

**缺点：**无法从主存块号中直接获得Cache的块号，变换比较复杂，速度比较慢。

**（3）组相联映像**

这种方式是前两种方式的折中。具体方法是将Cache中的块再分成组。

例如，假定Cache有16块，再将每两块分为1组，则Cache就分为8组。主存同样分区，每区16块，再将每两块分为1组，则每区就分为8组。

**组相联映像实现方式：**规定组采用直接映像方式而块采用全相联映像方式。也就是说，主存任何区的0组只能存到Cache的0组中，1组只能存到Cache的1组中，依此类推。组内的块则采用全相联映像方式，即一组内的块可以任意存放，也就是说，主存一组中的任一块可以存入Cache相应组的任一块中。

**实现过程：**通过直接映像方式来决定组号，在一组内再用全相联映像方式来决定Cache中的块号。由主存地址高位决定的主存区号与Cache中区号比较可决定是否命中。主存后面的地址即为组号。

#### 3)替换算法

**目标：**使Cache获得尽可能高的命中率。

**命中：**CPU从Cache中读到有用的数据称为命中。

**常用算法有如下几种：**

**（1）**随机替换算法

**原理：**用随机数发生器产生一个要替换的块号，将该块替换出去。

**优点：**简单易实现。

**缺点：**命中率较低。

**（2）**先进先出算法

**原理：**将最先进入Cache的信息块替换出去。

**优点：**易实现，系统开销小。

**缺点：**不能提高命中率。

**（3）**近期最少使用算法

**原理：**将近期最少使用的Cache中的信息块替换出去。

**优点：**有效的反映了程序的局部性。

**缺点：**需要独立的计数模块，系统开销大。

**（4）**优化替换算法

**原理：**这种方法必须先执行一次程序，统计Cache的替换情况。有了这样的先验信息，在第二次执行该程序时便可以用最有效的方式来替换。

**优点：**命中率最高。

**缺点：**需先执行一次程序，不现实。该算法是一种理想算法。

#### 4)cache和主存存储内容一致性

cache中保存的字块是主存中相应字块的一个副本。如果遇到写操作，就会遇到如何保持存储内容一致性问题，所以由3种写入方式。

1. 标志交换方式（写回法）：暂时只向cache写入，并用标志加以注明，直到经过修改的字块被从cache种替换出来时，才一次写入主存。特点：主存中的字块未经随时修改而可能失效。

（2）通过式写（写通法）：每次写入cache时也同时写入主存，使cache和主存保持一致。特点：能随时保持主存数据的正确性，但有可能增加多次不必要的向主存写入。

（3）当被修改的单元不在cache时，可以直接对主存进行，而不写入cache。

1. 有效位

机器刚启动时，有效位置0；在程序执行过程中，cache不命中时将指令块或数据块从主存中调入，并将此块的有效位置1。

1. cache的地址监听

输入输出设备向存储器写入数据时，若该地址与cache相应单元的标记相符且有效位为1，此时会造成cache和存储器数据不一致性。

解决方案：将cache的有效位置0，这样当CPU再访问时，需要去存储器再取数据。

1. **平均存取时间=h\*tC+（1-h）（tC+tM）**

h：命中率、tC：cache的存取时间、tM：主存的存取时间

#### 5)Cache的性能分析

Cache的性能是计算机系统性能的重要方面。命中率是Cache的一个重要指标，但不是最主要的指标。

**Cache设计目标：**在成本允许的条件下达到较高的命中率，使存储系统具有最短的平均访问时间。

设Hc为Cache的命中率，tc为Cache的存取时间，tm为主存的访问时间，则Cache存储器的等效加权平均访问时间ta为：

ta=Hctc+(1-HC)tm=tc+(1-HC)(tm-tc)

这里假设Cache访问和主存访问是同时启动的，其中，tc为Cache命中时的访问时间，（tm-tc）为失效访问时间。如果在Cache不命中时才启动主存，则

**ta=tc+（1-Hc）tm**

在指令流水线中，Cache访问作为流水线中的一个操作阶段，Cache失效将影响指令的流水。

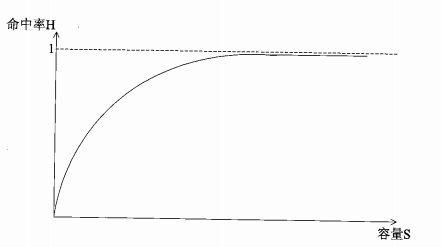
**提高Cache性能的一项重要措施：**降低Cache的失效率。

当Cache容量比较小时，容量因素在Cache失效中占有比较大的比例。

**降低Cache失效率的方法主要有：**

1. 选择恰当的块容量。
2. 提高Cache的容量
3. 提高Cache的相联度。

Cache的命中率与Cache容量的关系如图所示：



图：Cache容量与命中率的关系

Cache容量越大，则命中率越高，随着Cache容量的增加，其失效率接近0%（命中率逐渐接近100%）。但是，增加Cache容量意味着增加Cache的成本和增加Cache的命中时间。

#### 5)多级Cache

在多级Cache的计算机中，Cache分为一级（L1 Cache）、二级（L2 Cache）、三级（L3 Cache）等。

**访问顺序：**

1. CPU访存时首先查找L1 Cache。
2. 如果L1没有命中，则访问L2 Cache。
3. 直到所有级别的Cache都不命中，才访问主存。

通常要求L1 Cache的速度足够快，以赶上CPU的主频。

如果Cache为两级，则L1 Cache的容量一般都比较小，为几千字节到几十千字节；L2 Cache则具有较高的容量，一般为几百字节到几兆字节，以使高速缓存具有足够高的命中率。

### 5.虚拟存储器

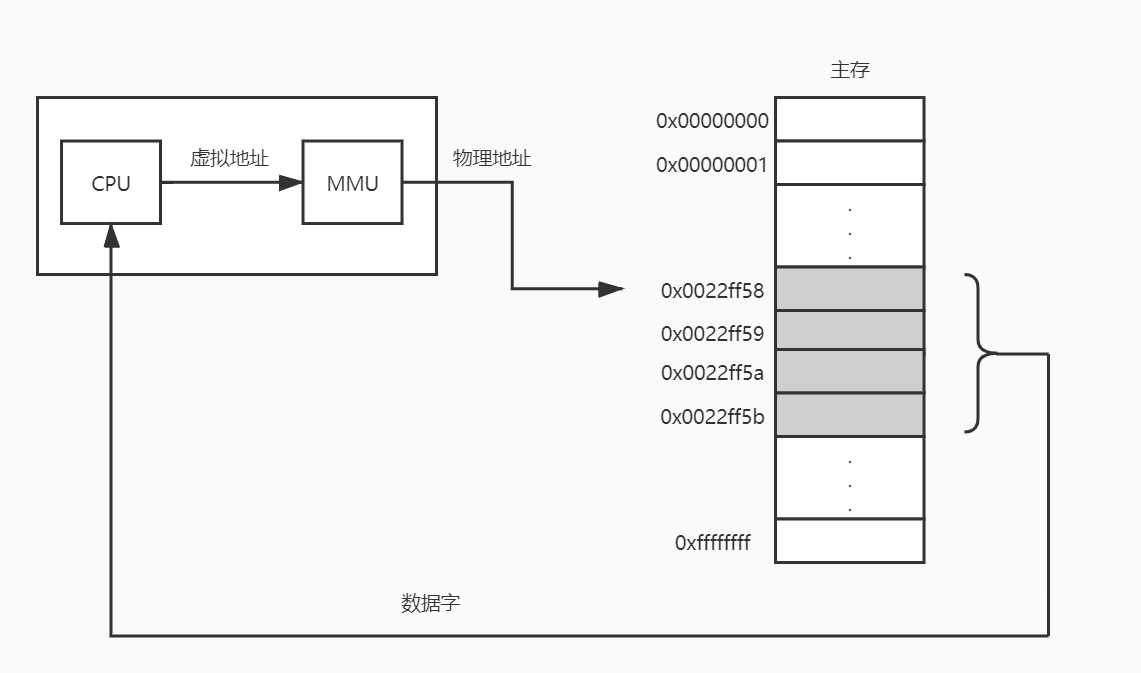
**主存存储器：**在概念上，可以将主存存储器看作一个由若干个字节构成的存储空间，每个字节（称为一个存储单元）有一个地址编号，主存单元的该地址称为物理地址（Physical Address）。

**访问主存数据流程：**当需要访问主存中的数据时，由CPU给出要访问数据所在的存储单元地址，然后由主存的读写控制部件定位对应的存储单元，对其进行读（或写）操作来完成访问操作。

现代系统提供了一种对主存的抽象，称为虚拟存储。

**虚拟存储：**使用虚拟地址（由CPU生成）的概念来访问主存，使用专门的MMU（Memory Management Unit）将虚拟地址转换为物理地址后访问主存。

设主存容量为4GB，则其简化后的访问操作和内存模型如图所示：



图：内存模型及使用虚拟地址访存示意图

虚拟存储器实际上是一种**逻辑存储器。**

**虚拟存储器实质：**对物理存储设备进行逻辑化的处理，并将统一的逻辑视图呈现给用户。

**优点：**用户在使用时，操作的是虚拟设备，无需关心底层的物理环境，从而可以充分利用基于异构平台的存储空间，达到最优化的使用效率。

### 6.外存储器

**用处：**用来存放暂时不用的程序和数据，并且以文件的形式存储。

CPU不能直接访问外存中的程序和数据，只有将其以文件为单位调入主存才可访问。

**外存储器构成：**主要由磁表面存储器（如磁盘、磁带）、光盘存储器及固态硬盘（采用Flash芯片或DRAM作为存储介质的存储器）构成。

#### 1)磁表面存储器

在磁表面存储器中，**磁盘**的存取速度较快，且具有较大的存储容量，是目前广泛使用的外存储器。

**磁盘存储器组成：**由盘片、驱动器、控制器和接口组成。

**（1）盘片：**用来存储信息。

**（2）驱动器：**用于驱动磁头沿盘径向运动以寻找目标磁道位置，驱动盘片以额定速率稳定旋转，并且控制数据的写入和读出。

**（3）控制器：**接收主机发来的命令，将它转换成磁盘驱动器的控制命令，并实现主机和驱动器之间数据格式的转换及数据传送，以控制驱动器的读/写操作。一个控制器可以控制一台或多台驱动器。

**（4）接口：**主机和磁盘存储器之间的连接逻辑。

硬盘是最常见的外存储器。一个硬盘驱动器内可装有多个盘片，组成盘片组，每个盘片都配有一个独立的磁头。所有记录面上相同序号的磁道构成一个圆柱面，其编号与磁道编号相同。将文件存储在硬盘上时尽可能放在同一圆柱面上，或者放在相邻柱面上，这样可以缩短寻道时间。

**磁道：**为了正确地存储信息，将盘片划成许多同心圆，称为磁道，从外到里编号，最外一圈为0道，往内道号依次增加。

**道密度：**沿径向的单位距离的磁道数称为道密度，单位为tpi（每英寸磁道数）。

**扇段或扇区：**将一个磁道沿圆周等分为若干段，每段称为一个扇段或扇区，每个扇区内可存放一个固定长度的数据块，如512B。

**位密度：**磁道上单位距离可记录的位数称为位密度，单位为bpi（每英寸位数）。

因为每条磁道上的扇区数相同，而每个扇区的大小又一样，所以每条磁道都记录同样多的信息。又因为里圈磁道圆周比外圈磁道的圆周小，所以里圈磁道的位密度要比外圈磁道的位密度高。最内圈的位密度称为最大位密度。

**硬盘的寻址信息组成：**由硬盘驱动号、圆柱面号、磁头号（记录面号）、数据块号（或扇区号）以及交换量组成。

**硬盘容量有两种指标：**

1. 非格式化容量

它是指一个磁盘所能存储的总位数。

非格式化容量=面数×磁道数×内圆周长×最大位密度

1. 格式化容量

它是指各扇区中数据区容量的总和。

格式化容量=面数×（磁道数/面）×（扇区数/道）×（字节数/扇区）

按盘片是否固定、磁头是否移动等指标，硬盘可分为移动磁头固定盘片的磁盘存储器、固定磁头的磁盘存储器、移动磁头可换盘片的磁盘存储器和温彻斯特磁盘存储器（简称温盘）。

#### 2)光盘存储器

**光盘存储器：**是一种采用聚焦激光束在盘式介质上非接触地记录高密度信息的新型存储装置。

根据性能和用途，光盘存储器可分为**只读型光盘（CD-ROM）**、**只写一次型光盘（WORM）**和**可擦除型光盘**。

（1）只读型光盘

是由生产厂家预先用激光在盘片上蚀刻不能再改写的各种信息，目前这类光盘的使用很普遍。

（2）只写一次型光盘

指由用户一次写入、可多次读出但不能擦除的光盘，写入方法是利用聚焦激光束的热能，使光盘表面发生永久性变化而实现的。

（3）可擦除型光盘

是读/写型光盘，它是利用激光照射引起介质的可逆性物理变化来记录信息。

**光盘存储器组成：**由光学、电学和机械部件等组成。

**光盘存储器特点：**记录密度高、存储容量大、采用非接触式读/写信息（光头距离光盘通常为2mm）、信息可长期保存（其寿命达10年以上）、采用多通道记录时数据传送率可超过200Mb/s、制造成本低、对机械结构的精度要求不高、存取时间较长。

#### 3)固态硬盘

**固态硬盘存储介质：**分为两种，一种是采用闪存（FLASH芯片）作为存储介质，另外一种是采用DRAM作为存储介质。

### 7.存储保护

5.1存储区域保护

1. 页表保护

每个程序都有自己的页表和段表，无论地址如何出错，也只能影响到分配给该程序的主存页面。页表保护是在生成主存地址前的保护。但若在地址变换过程中出现错误，形成错误主存地址，则保护无效。

1. 键保护

为主存的每一页分配一个存储键，相当于一把锁；为每道程序分配一个访问键，相当于一把钥匙。当访问主存的某一页时，访问键要和存储键相比较，若两键相符，则允许访问该页。

1. 环保护方式

按系统程序和用户程序的重要性和对整个系统正常运行的影响程度进行分环，赋予环号。环号越大，等级越低。操作系统的环号小与用户程序的环号。

环号小的可以去环号大的，同级环号也可以；环号大的去环号小的，则产生中断，由操作系统处理。

5.2访问方式保护

访问方式保护有RWE这3种方式及其逻辑组合。

5.3管理状态和用户状态

计算机执行程序时把工作状态分为2种，一种是执行操作系统或管理程序时所处的状态，称为管理状态；另一种是执行用户程序时所处的状态，称为用户状态。

为防止用户编辑出错而影响整个系统工作，在机器中设置了一些特权指令（只有操作系统等系统程序才能使用），假如在用户程序中出现特权指令，则在执行到该指令时立即中止执行并发出中断。