

4-1. 现代计算机系统需要存储层级的原因是为了提高计算机访问的速度与效率并降低成本。存储层级将不同速度与不同容量的存储设备分层,使得在计算机访问存储空间时,能根据所需要的特性选择最适合的存储介质进行操作。例如 SRAM 速度快, flash 容量大等等,因此计算机就能够较为快速访问内存或使用缓存,提高了整体的运行效率。

4-2. 过大的页:由于每个进程都要分配一个或多个完整的页,即使只需要使用一部分,因此导致了内存空间的浪费。
过小的页:页太小会使得需要维护更多的页表项,不仅占用大量内存空间,还可能增加页表访问的时间。

4-3. (1) 第0位 V: 表示 PTE(页表)是否是有效的,如果是0,表示尚未使用。

第1、2、3位 RWX: 表示该页是否可读、可写、可执行。

第4位 U: 表示是否在用户模式下能够访问该页, U=1 则能够访问。

第5位 G: 指定全局映射。

第6位 A: 表示虚拟页是否已经被读、写或提取(自上次A位被清除以来)。

第7位 D: 表示虚拟页是否已经被写入(自上次D位被清除以来)。

(2) 如果用户进程能够自由修改页表,那么也能够修改 RWX 位或 U 位,那么就能够访问用户进程不能访问的内存,破坏了权限机制。

(3) 如果 RWX 全部为0,该页表项会指向下一个等级的页表,也就是说说明该页表项不指向实际物理内存,还要进一步寻找下一级虚拟页表。

4-4.

(1) PMP 控制寄存器的 XWR 位主要作用是能够对页表条目进行更加精细的访问权限控制。由于页表条目也存在 XWR 位,因此处理器会将对应的位进行逻辑与运算从而确定该条目的访问权限。这意味着能够在硬件层面影响访问权限。

(2) A 位: (Address Matching) A 位表示如何对相关 PMP 寄存器的地址匹配模式进行编码。A=0 (OFF): 该条目被禁用;
A=1 (TOR): 表示任务范围的顶部边界; A=2 (NA4): 四字节区域自然对齐; A=3 (NAPOT): 2 次幂自然对齐。

L 位: 表示 PMP 条目是否被封锁 (Locked), 也即是否忽略对配置寄存器与相关地址寄存器的写入。

4-5.

(1) 页大小为 4KB, 说明 [11:0] 共 12 位作为偏移量; 因此页表条目共有 $2^{64-12} = 2^{52}$ 条。

每个条目使用 8 字节, 也就是 2^3 Byte , 所以页表需要的存储空间为: $2^3 \cdot 2^{52} \text{ Byte} = 2^{15} \text{ TB}$

(2) 只使用 48 位虚拟空间, 则页表所需空间: $2^3 \cdot 2^{48-12} \text{ Byte} = 512 \text{ GB}$ 。

(4) 多级页表能够随着进程占用内存空间的增大而对应地增多该进程的页表数目, 而不是在初始情况下就直接分配大量的空间。