

1. 简述现代计算机系统需要存储层级的原因。
2. 在页式虚拟存储中, 过大或过小的页分别会引起什么问题?

1) 需要存储层级的主要原因是为了解决存储器的速度与容量之间的矛盾。

不同的存储层次的数据传输速度不同, 一般来讲, 速度越快, 成本就越高, 容量就不宜太大。

采用多层存储器结构后, 处理器先访问速度最快的存储器, 数据不在该层级再往下一层

继续寻找, 可以有效缓解内存墙的问题。

- 2) 页过大:
- ① 进程需要的内存不一定总是刚好等于页面大小的整数倍, 因此在页面末尾浪费部分内存空间, 产生内存碎片。
 - ② 当需要将一个页面从物理内存中置换出去时, 要在磁盘中寻找足够大的空闲区域来存储, 页面过大会增加页面置换时间开销。
 - ③ 可用的存储进程的物理内存页面数减少, 导致大量的小型进程无法得到足够的页面。

页过小:

- ① 页面置换效率较低。
- ② 物理内存中可能无法找到足够大的连续空间来存储进程所需的页面, 导致留下许多未被使用的空闲内存。
- ③ 页面数增加, 导致页表项数目增加, 从而增加了页表的开销。

3. 页表条目除了保存物理页号外, 一般还包含各种状态和权限标记位, 它们为内存访问提供了各种细粒度的控制。例如, RISC-V 指令集的 Sv32 页表条目具有如下的形式:

31	20	19	10	9	8	7	6	5	4	3	2	1	0
PPN[1]	PPN[0]			RSW	D	A	G	U	X	W	R	V	
12	10			2	1	1	1	1	1	1	1	1	

- 1) 查阅 RISC-V 规范, 简要描述上述条目中的位 7 至位 0 具有什么功能。
- 2) 结合上述功能讨论: 如果用户进程能够自由修改自己的页表, 会发生什么问题?
- 3) 在 RISC-V 的虚拟内存管理中, 一个 X/W/R 位全部为 0 的有效页表条目有什么含义?

1) D - Dirty D 位为 1 时, 表明该页是否被改写, D 为 0 时对此页面进行写操作触发 Page Fault 异常

A - Accessed A 位为 1 表示该页可访问, 为 0 时不可访问, 否则触发 Page Fault 异常

G - Global 全局页面标识, 当前页可供多个进程共享

U - User 用户模式可访问

X W R 可执行, 可写, 可读

V - Valid 表明物理页在内存中是否分配好, 访问一个 V=0 页面会触发 Page Fault 异常

2) 如果用户进程能够自由地修改自己的页表, 则可以访问窃取其他进程的敏感信息。

还可以提升权限从而绕过系统的安全限制, 执行一些敏感操作等。

3) X/W/R 位全部为 0, 指针指向下一页表项。

4. RISC-V 的物理内存保护 (PMP) 机制允许硬件线程为特定的物理内存区域指定访问权限, 其配置寄存器有如下形式:



查阅 RISC-V 规范, 回答以下问题:

- 1) 在页表条目中已经存在 X/W/R 位的情况下, PMP 控制寄存器中的 X/W/R 位有什么作用?
- 2) 说明 PMP 配置寄存器中的 L 和 A 位有什么作用。

1) 页表条目中的 X/W/R 位是操作系统提供的软件控制机制, 而 PMP 是一种硬件支持的内存保护机制, 可以对系统代码、敏感数据等资源提供更强大的保护和隔离能力, 但需要更高的硬件成本和系统复杂度。

2) L-Lock 使能位: 0 时机器模式的访问都将成功, 用户模式的访问根据 R/W/X 判定是否成功, 1 时无法对表项进行相关修改。

A-地址匹配模式: 00 无效表项

01 使用相邻表项的地址作为匹配区间的模式。

10 区间大小为 4 字节的匹配模式。

11 区间大小为 2 的幂次方的匹配模式。

5. 回答以下问题:

- 1) 如果页大小为 4KB, 每个页表条目使用 8 字节空间, 内存系统按字节寻址, 则使用完整的 64 位虚拟地址时, 一个单级页表系统需要多大的空间用于存储页表?
- 2) 实际上, 多数真实系统仅限制使用 64 位系统的一部分位作为有效的访存空间, 例如 Sv48 即仅使用 48 位的虚拟地址空间, 则保持其他假设不变时, 一个单级页表系统存储页表所需要的空间被降低到多少?
- 3) 多级页表为什么可以降低虚拟内存系统的实际页表存储开销?

1) 一个页大小为 4KB, 即 2^{12} 位, 故需要 12 位来表示页内偏移量, 故需要用 $64-12=52$ 位来索引页号, 故一个页表可存储 2^{52} 个页表条目, 则一个单级页表需要空间: $2^{52} \times 8B = 32PB$

2) $2^{48} / 2^{12} \times 8 = 2^{36}B = 512GB$

3) 多级页表能够随着进程占用内存空间的增大对应地增多属于该进程的页表数目, 进程占用空间小时页表数目也少。