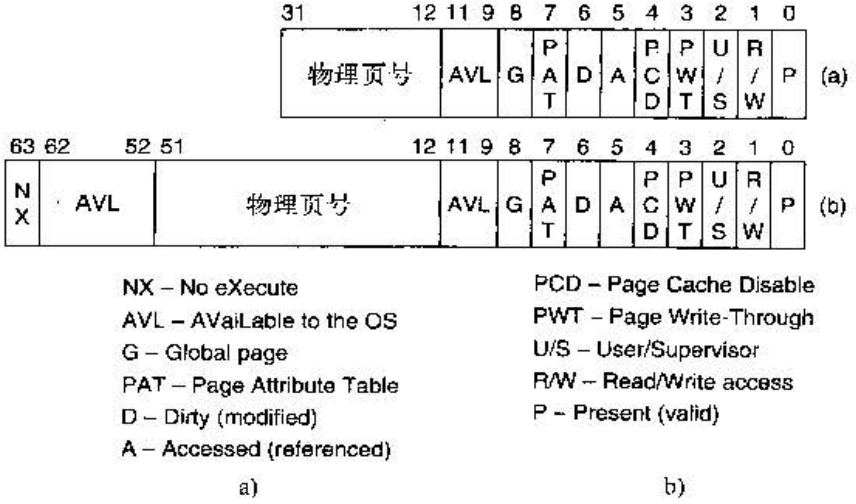

图11-33 一个a) Intel x86体系结构和b) AMD x64体系结构上的已映射页面的页表项（PTE）

每个页面失效都可以归入以下五类中的一类：

1) 所引用的页面没有提交。

2) 尝试违反权限的页面访问。

3) 修改一个共享的写时复制页面。

4) 需要扩大栈。

5) 所引用的页已经提交但是当前没有映射。

第一种和第二种情况是由于编程错误引起。如果一个程序试图使用一个没有一个有效映射的地址或试图进行一个称为访问违例（access violation）的无效操作（例如试图写一个只读的页面），通常的结果是，这个进程会被终止。访问破坏的原因通常是坏指针，包括访问从进程释放的和被解除映射的内存。

第三种情况与第二种情况有相同的症状（试图写一个只读的页面），但是处理方式是不一样的。因为页面已经标记为写时复制，存储管理器不会报告访问违例，相反它会为当前进程产生一个该页面的私有副本，然后返回到试图写该页面的线程。该线程将重试写操作，而这次的写操作将会成功完成而不会引发页面失效。

第四种情况在线程向栈中压入一个值，而这个值会被写到一个还没有被分配的页面的情况下发生。存储管理器程序能够识别这种特殊情况。只要为栈保留的虚拟页面还有空间，存储管理器就会提供一个新的物理页面，将该页面清零，最后把该页面映射到进程地址空间。线程在恢复执行的时候会重试上次引发页面失效的内存访问，而这次该访问会成功。

最后，第五种情况就是常见的页面失效。这种异常包含下述几种情况。如果该页是由文件映射的，内存管理器必须查找该页与内存区对象结合在一起的原型页表等类似的数据结构，从而保证在内存中不存在该页的副本。如果该页的副本已经在内存中，即在另一个进程的页面链表已经存在该页面的副本，或者在后备、已修改页链表中，则只需要共享该页即可。否则，内存管理器分配一个空闲的物理页面，并安排从磁盘复制文件页。

如果内存管理器能够从内存中找到需要的页而不是去磁盘查找从而响应页面失效，则称为*软异常*（soft fault）。如果需要从磁盘进行复制，则称为*硬异常*（hard fault）。软异常同硬异常相比开销更小，对于应用程序性能的影响很小。软异常出现在下面场景中：一个共享的页已经映射到另一个进程；请求一个新的全零页，或所需页面已经从进程的工作集移除，但是还没有重用。

当一个物理页面不再映射到任何进程的页表，将进入以下三种状态之一：空闲、修改或后备。内存管理器会立刻释放类似那些已结束进程的栈页面这样不再会使用的页面。根据判断映射页面的页表项中的上次从磁盘读出后的脏位是否设置，页面可能会再次发生异常，从而进入已修改链表或者后备链表（standby list）。已修改链表中的页面最终会写回磁盘，然后移到后备链表中。

内存管理器可以根据需要从空闲链表或者后备链表中分配页面。它在分配页面并从磁盘复制之前，