

缺页异常、受保护、非法地址.....

页错误(页故障) PAGE FAULT

下面我们介绍页错误，页故障这个概念，那么它的统称呢是 Page Fault。

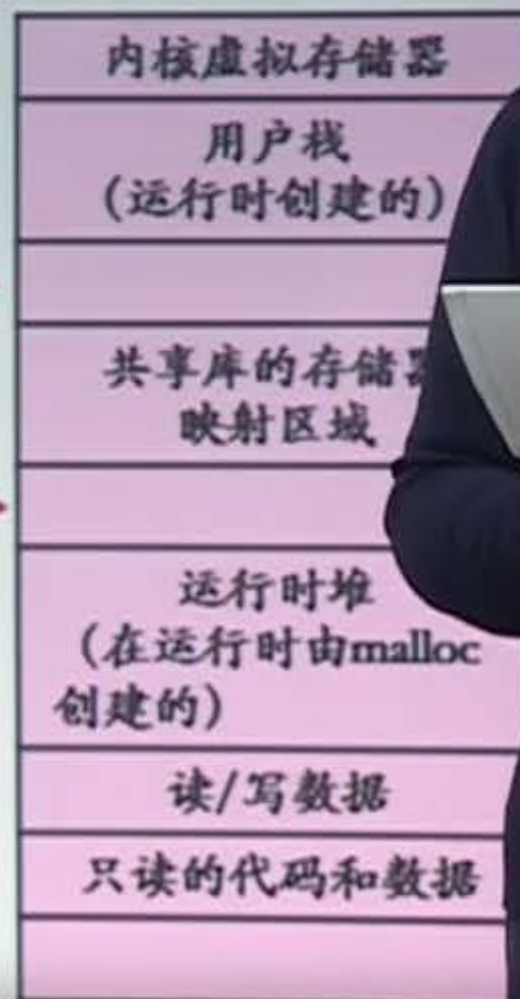
页错误PAGE FAULT

◎ 又称 页面错误、页故障、页面失效

◎ 地址转换过程中硬件产生的异常

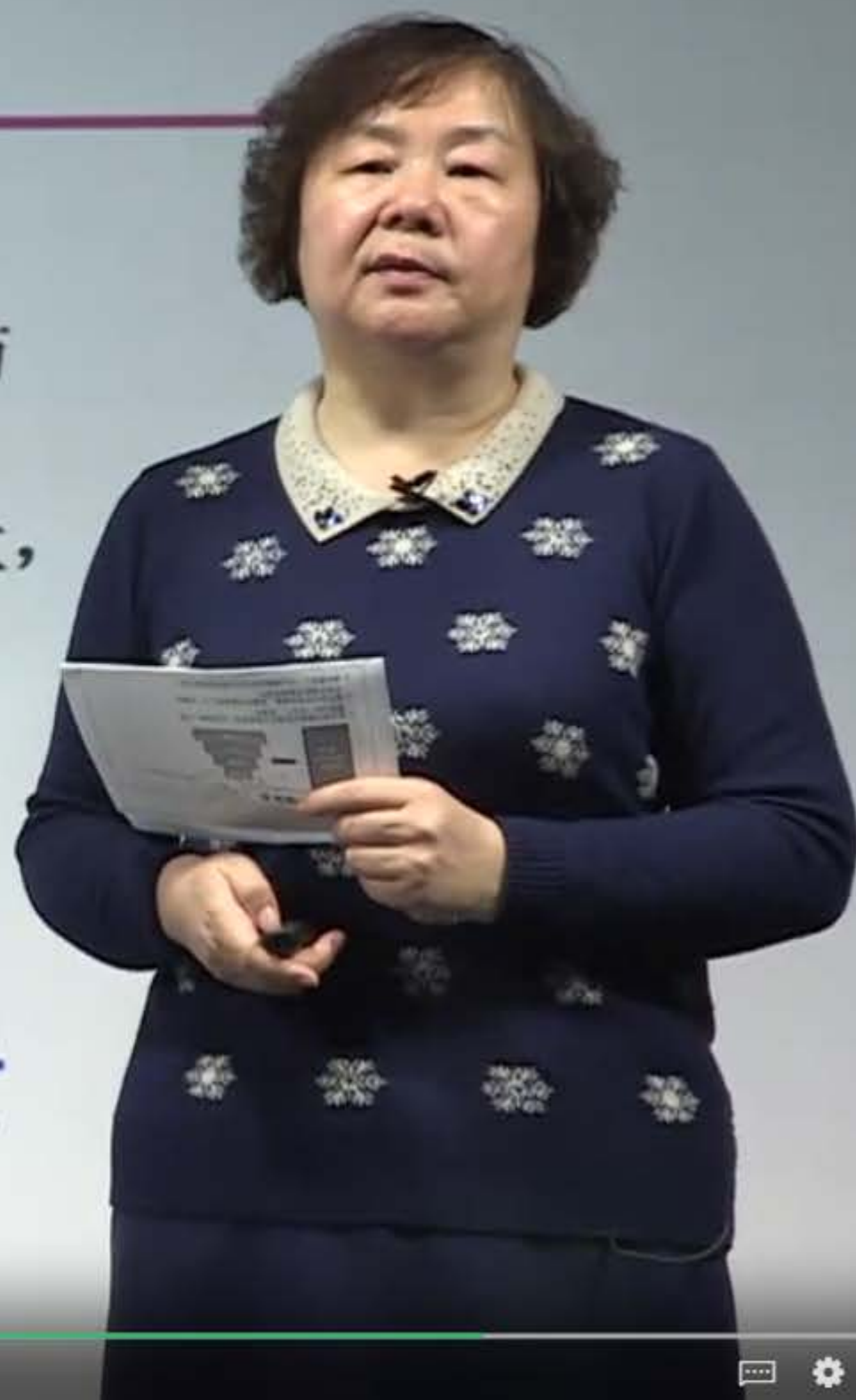
◎ 具体原因

- 所访问的虚拟页面没有调入物理内存
→ 缺页异常
- 页面访问违反权限（读/写、用户/内核）
- 错误的访问地址
-



缺页异常处理

- ◎ 是一种**Page Fault**
- ◎ 在地址映射过程中，**硬件**检查页表时发现所要访问的页面不在内存，则产生该异常——**缺页异常**
- ◎ **操作系统**执行**缺页异常处理程序**：获得磁盘地址，启动磁盘，将该页调入内存
 - ◎ 如果内存中有空闲页框，则分配一个页框，将新调入页装入，并修改页表中相应页表项的有效位及相应的页框号
 - ◎ 若内存中没有空闲页框，则要置换内存中某一页框；若该页框内容被修改过，则要将其写回磁盘



缺页异常处理

预取一些
页面

- 是一种**Page Fault**
- 在地址映射过程中，**硬件**检查页表时发现所要访问的页面不在内存，则产生该异常——**缺页异常**
- **操作系统**执行**缺页异常处理程序**：获得磁盘地址，启动磁盘，将该页调入内存。
 - 如果内存中有空闲页框，则分配一个页框，将新调入页装入，并修改页表中相应页表项的有效位及相应的页框号
 - 若内存中没有空闲页框，则要置换内存中某一页框；若该页框内容被修改过，则要将其

啊是这样一个想法，所以在缺页异常行处理过程中呢，我们可以在最后加一点点预取的功能。



下面我们介绍页错误，页故障这个概念，那么它的统称呢是 Page Fault。所谓页错误呢，有各种各样的说法：页面错误，页故障，页面失效。那么它通常指的是在地址转换的过程中，硬件发现了一些问题，然后产生了异常。那么我们知道第二讲我们讲过，产生异常之后呢就进入了操作系统，由操作系统呢来处理这样一些情况啊，所以这个机制呢，大家结合啊第二讲所讲的内容来理解。好，那么在地址转换过程中，硬件会发现什么样的问题呢？具体来说呢，有这么几个典型的问题。第一个是你要访问的虚拟页面还没有读入内存的，那么这个呢我们通常称之为叫做“缺页异常”，就是页面不在内存，所以简称缺页，啊缺页。还有一种情况呢，是你页面的这个访问呢违反了权限。比如说：在只读页面上做了写操作，比如说你用户进程访问到了这个系统相对的空间啊，就是说内核要访问的地方那可以，用户不能访问，那么用户要访问那个空间呢，那么也会产生异常。还有呢就是错误的访问地址啊，错误的访问地址。那么什么是错误的访问地址呢？我们来看一下，我们看一个示例，那么这个呢是一个地址空间啊，虚拟地址空间的图。那么我们这里头知道代码呀数据呀，或者是堆，或者是栈，以及引用到了一些共享库啊，或者是一些映射的地方，那么这是有内容的。但是如果你在访问过程当中的虚拟地址指向了这些没有内容的位置，实际上呢这些是相当于错误的访问地址。那么它产生了这样的一个异常，所以这是关于这个 Page Fault 的各种各样的具体原因。那我们就以缺页异常为例，来介绍一下它的处理过程。缺页异常首先它是一种 Page Fault，它是在地址的映射过程中，由硬件来检查页表的时候发现了这样一个问题。所要访问的这个页面不在内存，所要访问的页面不在内存，那么就产生了这样一个异常。产生异常之后我们知道，进入了操作系统所以呢，由操作系统来执行一个缺页异常的处理程序。那么这个程序呢，它要涉及到了方方面面的功能，我们这里简单的说一下它的主要的工作是通过获取到了磁盘地址，然后呢去启动磁盘，将该页调入内存，将这个页面调入内存。这是缺页异常处理程序的主要工作。但是我们知道缺页异常处理程序其实涉及了很多方面，大家请回忆一下在我们的这个第一讲当中，所讲的 Hello World 这个程序执行的过程当中，那么缺页的过程它要涉及到了进程的管理部分，内存的管理部分，还有磁盘就是相当于我们说文件系统，还有一些启动，驱动啊这样一些过程，所以整个操作系统的方方面面其实缺页异常处理程序都要涉及到，是一个非常重要的一段代码。当要把新的页面调入内存的时候呢就有两种可能性，第一种可能性就是内存当中有足够的空闲页框，所以呢你就可以分配一个

空闲页框 把新的页面调入。在调入完之后呢，你肯定要修改 页表当中的相应的页表项，比如说它的有效位原来是 0，就变成 1 了。页框号也要把这个分配给它的页框号填到页表项里头。但是第二种情况呢也会发生，因为内存可能会用完了，因此 内存中没有足够的空闲页框了，或者就没有空闲页框。那么我们要做的事情就是置换 内存当中的某一个页框，就把在内存中的某一个页框的内容，把它换到磁盘上，然后用这个页框来承接新调入的页面。那么这个页框如果选中这个页框，在内存的内容被修改过，那么这个时候呢，我们就要把它写回到磁盘。所以就是在缺页异常处理过程中要处理的几个问题。那我们前面讲过了，虚拟页式存储管理方案有两种方式，一种是请求调页，一种是 预先调页。那么实际上在这个过程中我们可以看到 它相当于是一个请求调页的一个场景，但是这个里头我们就可以增加一些 预取的功能。也就是在把 这个页面调入内存的同时，顺带的把相关的一些页面也都 调进内存。比如说像 Windows 它就会这么做，当要读入一段 页面，这个页面是代码内容的话，它会接着多读入几个页面。数据的话，它也会多读入几个页面，这样的话就可以 以便下一次缺页，啊就不容易发生了。啊是这样一个想法，所以在缺页 异常行处理过程中呢，我们可以在最后加一点点预取的功能。