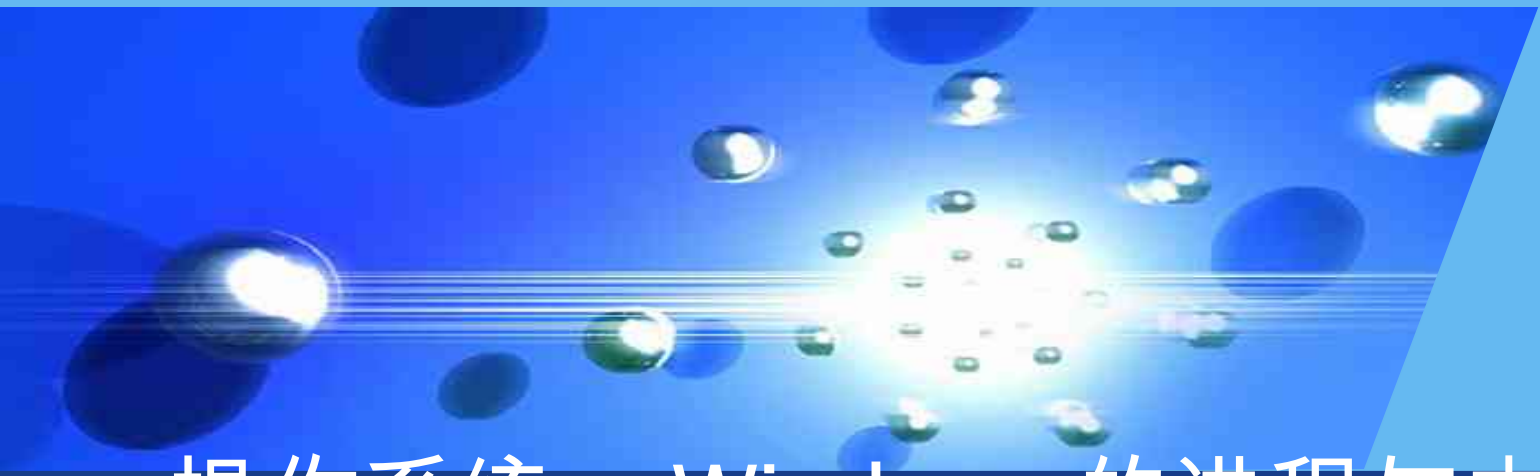
USTB



操作系统： Windows 的进程与内存管理

本章主要内容

1. Windows NT 相关概念
2. Windows 进程与线程
3. Windows 处理器调度机制
4. Windows 内存管理
5. 虚拟地址空间
6. 页面调度

7.1 Window NT (New Tech) 相关概念

- Windows NT 体系结构特点
  - Windows NT 是支持多处理器的操作系统
  - Windows NT 是完全 32 位操作系统
  - Windows NT 支持 16 位的 Windows 代码
  - Windows NT 对访问共享内存的进程有严格的安全限制
  - Windows NT 的系统内存空间只能在核心太被访问

7.1 Window NT 相关概念

- Windows 的管理机制
  - 核心态和用户态
  - Windows 操作系统的体系结构
    - windows 操作系统是由运行在用户态和核心态的一些构件组成的。
    - windows 的用户进程包括：
      - 操作系统支持进程
      - 服务进程
      - 应用程序
      - 环境子系统服务进程
    - windows 的核心服务包括：
      - windows 执行体
      - windows 内核
      - 驱动程序
      - 硬件抽象层
      - 窗口和图形系统

7.1 Window NT 相关概念

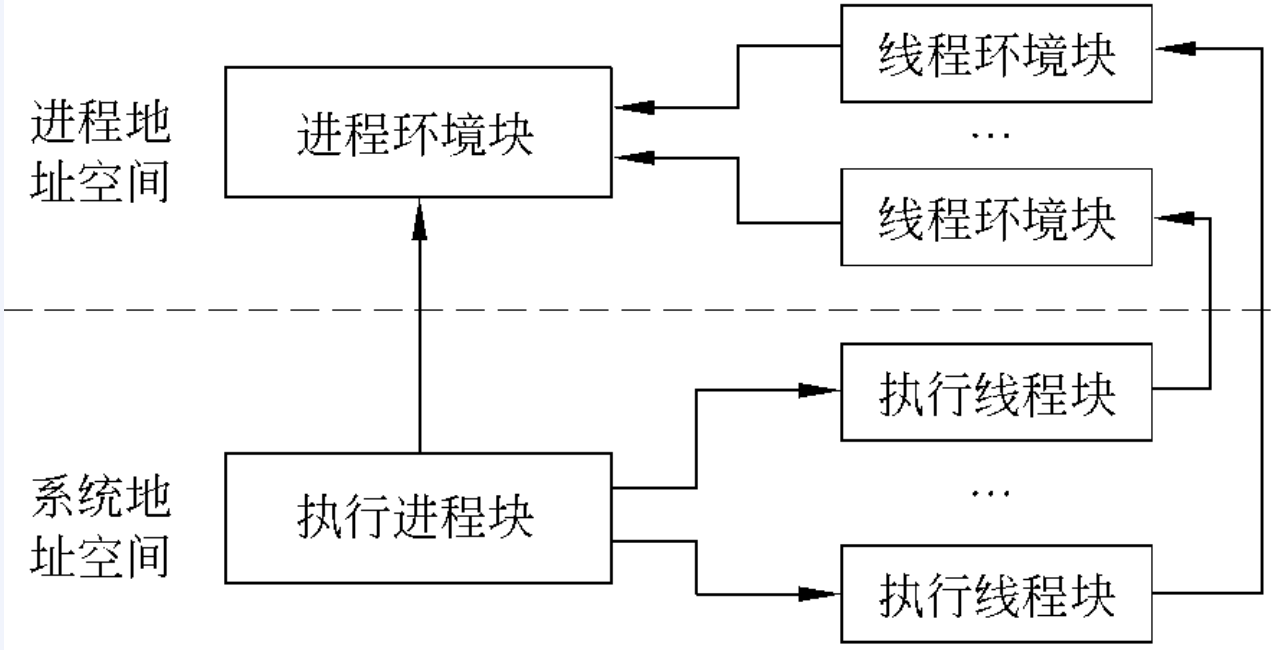
- 系统调用、中断和陷阱
  - Windows 利用系统服务陷阱来实现用户程序对系统服务调用。
  - Windows 利用中断陷阱机制来管理硬件设备
  - WIndows 利用意外陷阱机制来管理系统的出错状态
- 利用对象来共享系统资源
  - 必须通过对象服务来访问和修改对象封装的数据。
- 本地过程调用

7.2 Windows 进程和线程

- Windows 的进程和线程的定义
  - 每个进程都包含一个或多个线程， Windows 处理器调度的对象是线程。
  - Windows 进程包含以下 6 种信息：
    - 唯一的进程标志
    - 独立的虚拟地址空间
    - 映射到进程虚拟地址空间的执行代码和数据
    - 访问各种系统资源的对象句柄列表
    - 安全上下文
    - 至少包含一个可执行的线程
  - Windows 线程包含以下 4 种信息：
    - 唯一的线程标志
    - CPU 寄存器的状态数据
    - 两个线程栈，一个在用户态使用，一个在核心态使用
    - 一个供子系统、运行库和动态链接库使用的线程本地存储空间

7.2 Windows 进程和线程

- 进程和线程的关联
  - Windows 系统中，通过创建进程来为线程提供必要的上下文环境。
  - 通过创建线程来运行具体的程序。**执行进程块即进程控制块 PCB，进程地址空间即用户空间（目态），系统地址空间即核心态。**



7.2 Windows 进程和线程

❖Windows 进程的结构

表 7.1　Windows 进程的数据结构

执行进程块的数据项	功　　能
进程标志	唯一的进程标志号、父进程标志号、运行的映像文件(Image)名称
系统资源配额	对该进程所使用系统内存池以及分页文件的配额限制
虚拟内存管理	用来描述进程的哪些虚拟地址空间已被占用、哪些空间可以使用,以及进程虚拟内存管理的状态信息
工作集信息	该进程的虚拟地址空间中驻留在物理内存中的页面的集合
意外本地过程调用端口	当进程所属的线程出现意外时,进程管理器会通过本地过程调用发送意外信息到该进程,通过该端口接受意外信息进行相应的处理
调试本地过程调用端口	当进程所属的线程触发调试事件时,进程管理器会通过本地过程调用发送调试消息到该进程,通过该端口接受调试消息进行相应的处理

Windows 进程的结构（ 2 ）

续表

执行进程块的数据项	功　　能
访问安全描述	对访问该进程的安全设置
对象句柄表	指向该进程所有对象句柄
Windows 子系统进程信息	Windows 子系统调用该进程所需要的进程信息
核心进程块	它包含了 Windows 内核调度该进程的所属线程所需要的基本信息，如：分配给该进程的处理器时间、时间片大小、核心栈信息、进程基准优先级以及进程状态等
进程环境块	它驻留在进程地址空间中，提供映像调入器、堆管理器和其他运行在用户态的动态链接库所需要的进程信息，如程序映像的基地址、用户栈信息和线程的局部存储空间

7.2 Windows 进程和线程

Windows 线程的结构

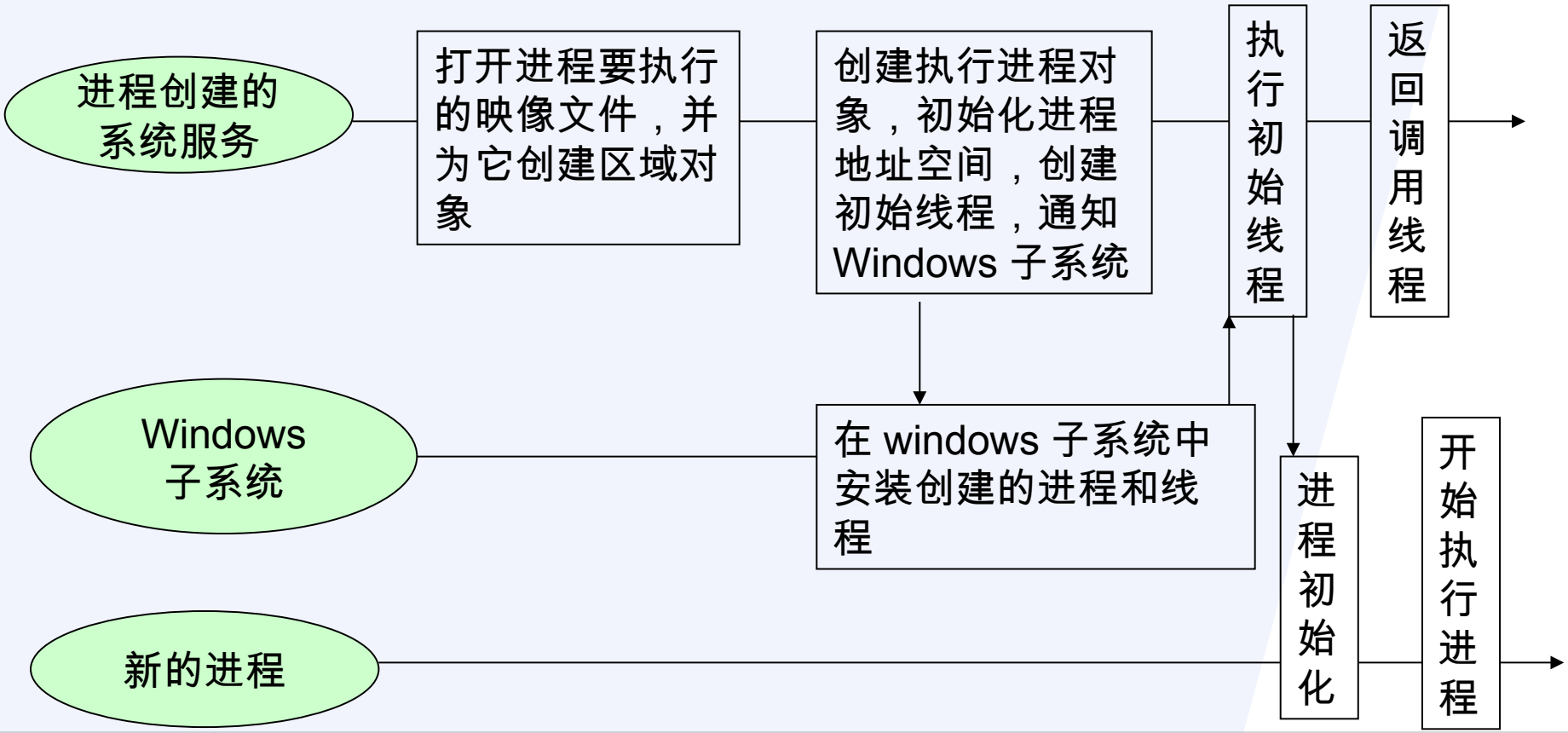
表 7.2 Windows 线程的数据结构

内　　容	功　　能
线程时间	线程创建和结束时间
所属进程标志	所属进程的标志
起始地址	线程起始例程的地址
访问安全控制	线程级别的访问安全控制信息
局部过程调用信息	线程处理局部过程调用的消息标志以及处理消息的地址
I/O 信息	等待处理的 I/O 请求包的列表
核心线程块	存储系统进行线程调度和同步的线程信息，如：该线程的可用执行时间、核心栈的地址、指向系统服务列表的指针、线程环境块的指针以及与处理器调度相关的信息：如调度优先级、时间配额、空闲处理例程
线程环境块	驻留在进程地址空间，存储用于映像调入器和 Windows 动态链接库所使用的线程上下文信息，如：线程的唯一标志、用户栈的地址以及指向所属进程的进程环境块

7.2 Windows 进程和线程

进程的创建

- 一般应用程序通过 CreateProcess 函数来创建一个新的 Windows 进程。



7.2 Windows 进程和线程

线程的创建

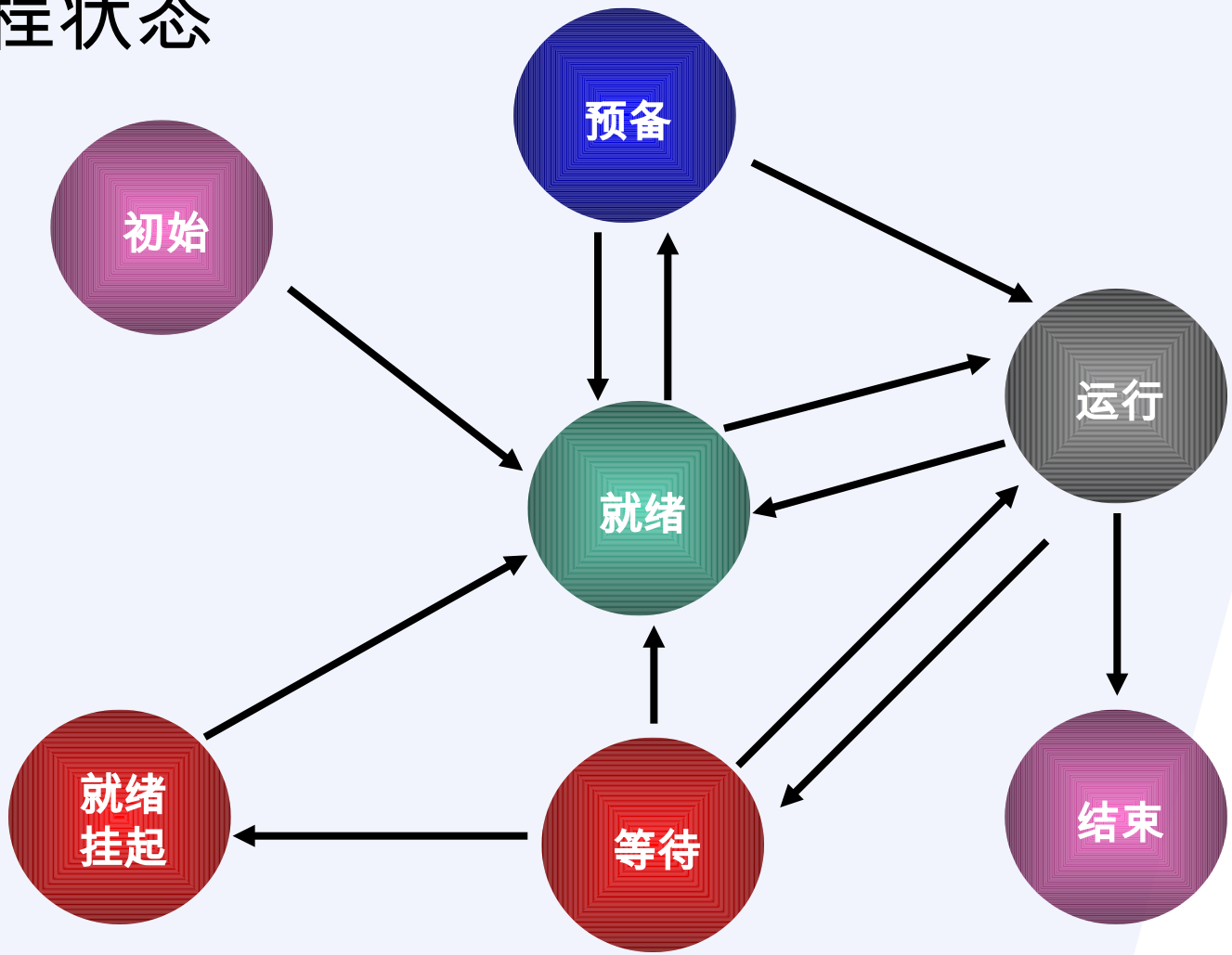
- 一般应用程序通过 CreateThread 函数来创建一个新的 Windows 线程。过程：
  - 在进程的地址空间为线程创建用户栈，并初始化运行上下文
  - 初始化线程的线程环境块
  - 创建执行线程对象
  - 通知 Windows 子系统新线程已被创建，子系统将新线程插入到相应进程的线程列表中
  - 新线程的句柄和标志被返回给调用的线程
  - 线程进入调度队列等待执行

7.3 Windows 处理器调度

- Windows 处理器调度的颗粒为线程，Windows 为每一个线程分配调度优先级。调度器根据优先级采用抢占式调度策略，让具有最高优先级的线程首先执行。
- 调度优先级
  - windows 系统使用 32 个优先级来表示线程要求执行的紧迫性。共分为 3 组：
    - 16 个实时优先级别
    - 15 个可变优先级别
    - 1 个系统优先级，为内存清零线程保留

7.3 Windows 处理器调度

- 线程状态



7.3 Windows 处理器调度

❖线程状态说明

表 7.3　线程状态的说明

状　态	含　义
就绪	表示一个线程已经准备就绪,等待运行。调度器查找线程库中处于就绪状态的线程,来决定下一个运行的线程
预备	表示一个线程已经被选择作为下一个运行的线程,如果条件满足,调度器会将上下文环境切换到该线程。但处于预备状态的线程也可能会被转换到就绪状态继续等待
运行	当调度器将上下文环境切换到一个进程,该线程就处于运行状态。当分配给线程的时间配额用完,或有更高优先级的线程抢占 CPU,它会让出处理器
等待	当一个线程需要等待必要的系统资源时,它会转入等待状态,直到系统资源就绪
就绪挂起	如果一个线程已经准备就绪,但运行它所需要的核心都在外存,它就进入就绪挂起状态,等待核心栈调入内存
终止	当一个线程完成执行后,它就进入了终止状态,对象管理器释放相应的执行进程块资源
已初始化	这是一个线程刚被创建时的内部状态

7.3 Windows 处理器调度

- 线程调度机制
  - 调度数据库
    - 用于记录处于就绪状态的线程
  - 时间配额
  - 调度算法
    - 基于优先级的抢占式调度算法
  - 上下文切换

7.4 Windows 内存管理

- 内存管理器
  - Windows 通过内存管理器来管理内存
  - 负责将虚拟地址映射到具体的物理内存
  - 当物理内存不够用时，将部分驻留内存数据交换到磁盘上

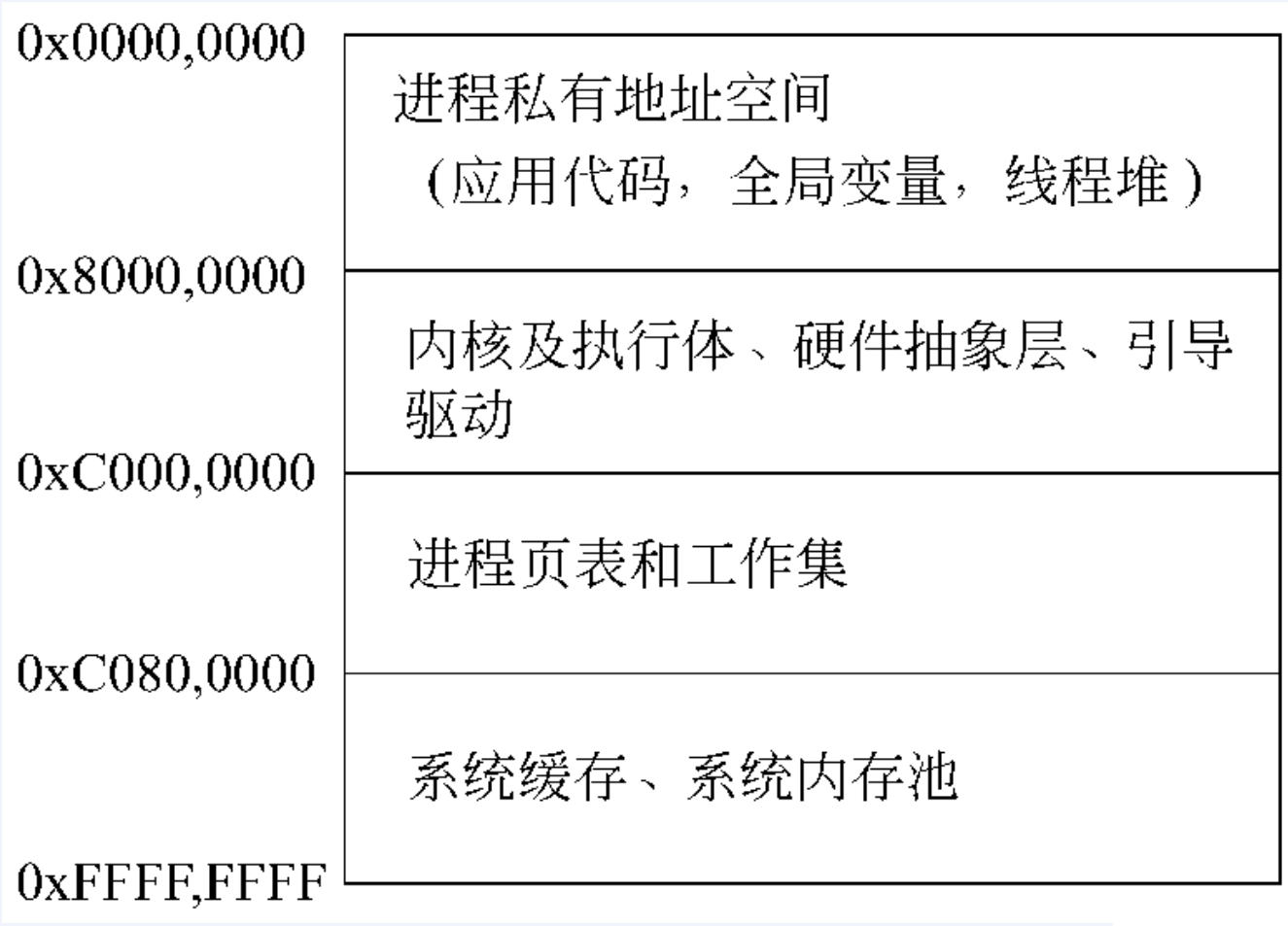
7.4 Windows 内存管理

内存管理机制

- 页
  - 内存管理器将虚拟内存空间划分成固定大小的单元：“页”，对于 X86 体系结构，页大小一般为 4KB
- 共享内存
  - 同一块物理内存在不同进程空间中的映射。
  - 对共享内存进行写时，采用“拷贝后写入”的方式。
- 堆管理
  - 用于管理小的内存分配
- 系统内存池

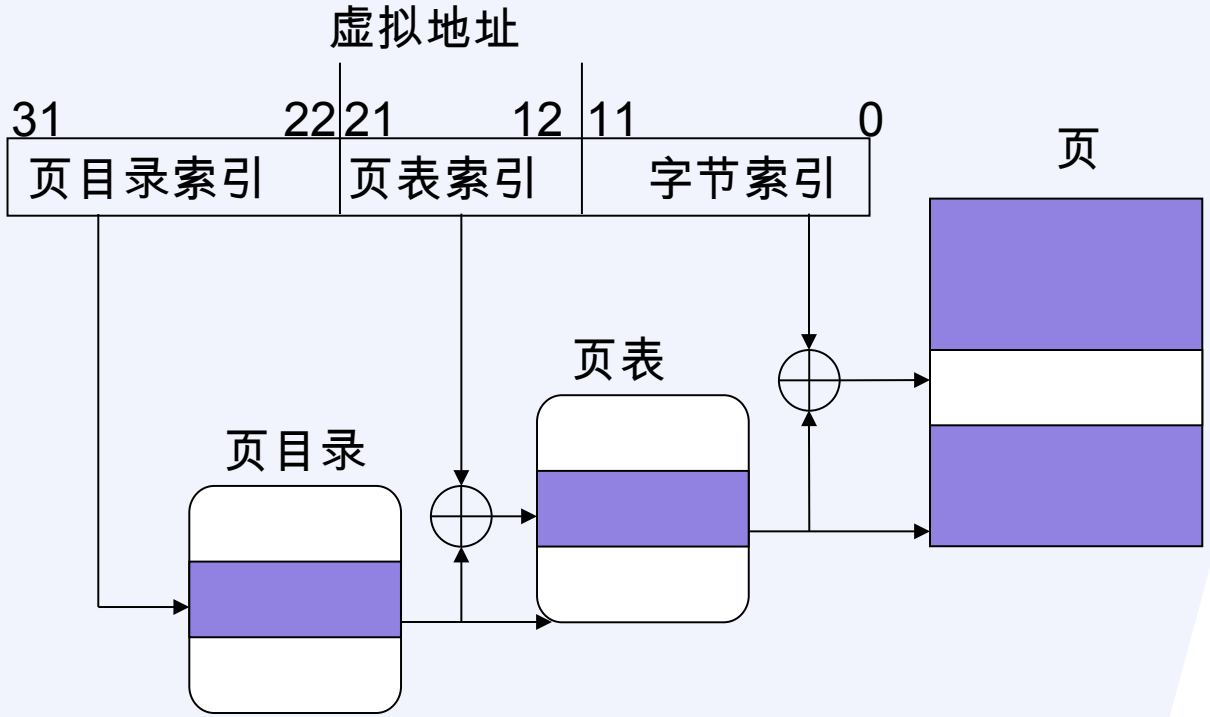
7.5 虚拟地址空间

❖虚拟空间布局



7.5 虚拟地址空间

- 虚拟地址转换
  - 其过程基本与 Linux 系统相同



7.6 页面调度

❖缺页处理

表 7.6　缺页处理的各种情况

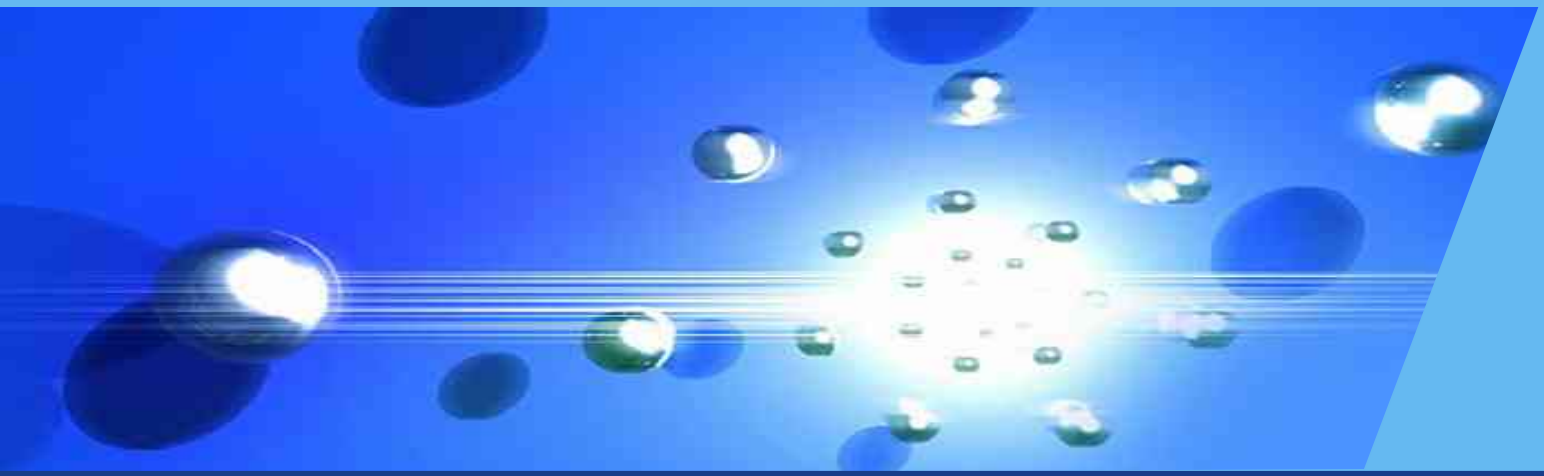
缺 页 原 因	处 理 方 式
被访问的页不在物理内存中,而在磁盘上的页文件或映射文件中	分配一个物理页从磁盘上读入该页,并将它记入工作集
该页被挂起或在修改页列表中	将该页转移到进程或系统的工作集
访问预留页或超出了分配的地址空间	访问错误
在用户态访问只能在核心态访问的页	访问错误
写入只读的页	访问错误
写入“先拷贝后写入”页	拷贝该页并将新的页作为进程的私有页,同时更新相应的映射和工作集
执行页中标明不能被执行的代码	访问错误

7.6 页面调度

- 工作集
  - 驻留在物理内存的虚拟页的集合
    - 进程工作集：描述一个进程中的所有线程引用的驻留在内存中的页面
    - 系统工作集：系统空间中可被分页的系统代码和数据驻留在物理内存中的部分
- 页面调度策略
  - Windows 系统采用请求式簇调度策略
  - Windows 系统采用“最久未使用”策略决定哪些虚拟页移出内存

7.6 页面调度

- 页框号和物理内存管理
  - 页框
    - 物理内存按照页的大小顺序划分成同样大小的单元
  - 页框号数据库
    - 用于描述整个物理内存的状态
    - 在数据库中，相同状态的物理页通过链表的形式连接在一起



结束