操作系统复习纲（名词解释版）

- 操作系统：是管理计算机硬件与软件资源的计算机程序，同时也是计算机系统的内核与基石。操作系统需要处理如管理与配置内存、决定系统资源供需的优先次序、控制输入与输出设备、操作网络与管理文件系统等基本事务。操作系统也提供一个让用户与系统交互的操作界面。

- 系统调用：运行在使用者空间的程序向操作系统内核请求需要更高权限运行的服务。 系统调用提供了用户程序与操作系统之间的接口。大多数系统交互式操作需求在内核态执行。

- 进程：计算机中已运行程序的实体。进程为现代分时系统的基本运作单位。

- 线程：是操作系统能够进行运算调度的最小单位。它被包含在进程之中，是进程中的实际运作单位。一条线程指的是进程中一个单一顺序的控制流，一个进程中可以并发多个线程，每条线程并行执行不同的任务。

- 进程同步：异步环境下的一组并发进程因直接制约而互相发送消息、进行互相合作、互相等待，使得各进程按一定的速度执行的过程。

- 管程：一种程序结构，结构内的多个子程序（对象或模块）形成的多个工作线程互斥访问共享资源。这些共享资源一般是硬件设备或一群变量。管程实现了在一个时间点，最多只有一个线程在执行管程的某个子程序。管程提供了一种机制，线程可以临时放弃互斥访问，等待某些条件得到满足后，重新获得执行权恢复它的互斥访问。

- 原子事务：事务中包含的程序作为系统的逻辑工作单位,它所做的对数据修改操作要么全部执行,要么完全不执行。

- 死锁：在多任务系统下，当一个或多个进程等待系统资源，而资源又被进程本身或其它进程占用时，就形成了死锁。【另一种解释是：如果所申请的资源被其他等待进程占有，那么该等待进程有可能再也无法改变其状态。】

- 虚拟内存：计算机系统内存管理的一种技术。它使得应用程序认为它拥有连续的可用的内存（一个连续完整的地址空间），而实际上，它通常是被分隔成多个物理内存碎片，还有部分暂时存储在外部磁盘存储器上，在需要时进行数据交换。与没有使用虚拟内存技术的系统相比，使用这种技术的系统使得大型程序的编写变得更容易，对真正的物理内存（例如 RAM）的使用也更有效率。

- 页错误：当软件试图访问已映射在虚拟地址空间中，但是目前并未被加载在物理内存中的一个分页时，由中央处理器的内存管理单元所发出的中断。通

常情况下，用于处理此中断的程序是操作系统的一部分。如果操作系统判断此次访问是有效的，那么操作系统会尝试将相关的分页从硬盘上的虚拟内存文件中调入内存。而如果访问是不被允许的，那么操作系统通常会结束相关的进程。

- 页面替换：在地址映射过程中，若在页面中发现所要访问的页面不在内存中，则产生缺页中断。当发生缺页中断时，如果操作系统内存中没有空闲页面，则操作系统必须在内存选择一个页面将其移出内存，以便为即将调入的页面让出空间。而用来选择淘汰哪一页的规则叫做页面置换算法。

- 设备驱动程序：是一个允许高级（High level）计算机软件（computer software）与硬件（hardware）交互的程序，这种程序创建了一个硬件与硬件，或硬件与软件沟通的接口，经由主板上的总线（bus）或其它沟通子系统（subsystem）与硬件形成连接的机制，这样的机制使得硬件设备（device）上的数据交换成为可能。

- RAID：其基本思想就是把多个相对便宜的硬盘组合起来，成为一个硬盘阵列组，使性能达到甚至超过一个价格昂贵、容量巨大的硬盘。根据选择的版本不同，RAID 比单颗硬盘有以下一个或多个方面的好处：增强数据集成度，增强容错功能，增加处理量或容量。另外，磁盘阵列对于计算机来说，看起来就像一个单独的硬盘或逻辑存储单元。简单来说，RAID 把多个硬盘组合成为一个逻辑扇区，因此，操作系统只会把它当作一个硬盘。RAID 常被用在服务器计算机上，并且常使用完全相同的硬盘作为组合。

- 总线、端口、控制器：
  - 总线指计算机组件间规范化的交换数据（data）的方式，即以一种通用的方式为各组件提供数据传送和控制逻辑。即一组线和一组严格定义的可以描述在线上传输信息的协议。同时采用多条线路才能传送更多数据，而总线可同时传输的数据数就称为宽度（width），以比特为单位，总线宽度愈大，传输性能就愈佳。总线的带宽（即单位时间内可以传输的总数据数）为：总线带宽 = 频率 x 宽度（Bytes/sec）。
  - 端口为计算机等的信息机器的硬件之间通信时的物理连接器形状、传送接收信号的方法（协议）等等的规格。主要可分为并行链接的和比特串行链接的。串行链接者相比起并行链接者，多得多使用同一电线作为信号控制线和电源供应线。
  - 控制器是用于操作端口、总线或设备的一组电子器件。

- 保护：指一种控制程序、进程或用户对计算机系统资源进行访问的机制。
- 保护域：当一个进程装入内存时，它们将为每个进程指派一个保护域。其指定了进程可以访问的资源。在一个对象上执行一个操作的权限是一种访问权限。一个域是一个访问权限的几何，每一个访问权限是一个有序对*<对象名，权限集>*，域之间允许存在交集，它们可以共享访问权限。
- 安全：计算机系统安全是指一系列包含敏感和有价值的信息和服务的进程和机制，不被未得到授权和不被信任的个人，团体或事件公开，修改或损坏。

目的是在保证信息和财产可被受权用户正常获取和使用的情况下，保护此信息和财产不受偷窃，污染，自然灾害等的损坏。由于它的目的在于防止不需要的行为发生而非使得某些行为发生，其策略和方法常常与其他大多数的计算机技术不同。

- 木马、后门、逻辑炸弹：
  - 木马是指计算机领域中指的是一种后门程序，是黑客用来盗取其他用户的个人信息，甚至是远程控制对方的计算机而加壳制作，然后通过各种手段传播或者骗取目标用户执行该程序，以达到盗取密码等各种数据资料等目的。
  - 后门指绕过软件的安全性控制，而从比较隐秘的通道获取对程序或系统访问权的黑客方法。在软件开发时，设置后门可以方便修改和测试程序中的缺陷。但如果后门被其他人知道（可以是泄密或者被探测到后门），或是在发布软件之前没有去除后门，那么它就对计算机系统安全造成了威胁。
  - 逻辑炸弹指一些嵌入在正常软件中并在特定情况下执行的恶意程式码。这些特定情况可能是更改档案、 特别的程式输入序列、或是特定的时间或日期。恶意程式码可能会将档案删除、使电脑主机当机、或是造成 其他的损害。逻辑炸弹这个名称正是因其发作时的恶意行为而来。
- 病毒、蠕虫：
  - 病毒是一种在人为或非人为的情况下产生的、在用户不知情或未批准下，能自我复制或运行的计算机程序；计算机病毒往往会影响受感染计算机的正常运作。
  - 蠕虫与计算机病毒相似，是一种能够自我复制的计算机程序。与计算机病毒不同的是，计算机蠕虫不需要附在别的程序内，可能不用使用者介入操作也能自我复制或执行。计算机蠕虫未必会直接破坏被感染的系统，却几乎都对网络有害。计算机蠕虫可能会执行垃圾代码以发动分散式阻断服务攻击，令到计算机的执行效率极大程度降低，从而影响计算机的正常使用；可能会损毁或修改目标计算机的档案；亦可能只是浪费带宽。（恶意的）计算机蠕虫可根据其目的分成 2 类：1）一种是面对大规模计算机使用网络发动拒绝服务的计算机蠕虫；2）另一种是针对个人用户的以执行大量垃圾代码的计算机蠕虫。