四级网络工程师高频考点随身学

目录

操作系统原理

第一章 操作系统概论

1.操作系统概述

- 操作系统是计算机系统中的一个系统软件，它是这样一些程序模块的集合——它们能有效地组织和管理计算机系统中的硬件及软件资源，合理地组织计算机的工作流程，控制程序的执行，并向用户提供各种服务功能，使用户能够灵活、方便、有效地使用计算机，并使整个计算机系统能高效地运行。
- 操作系统作为系统软件，位于软件系统的硬件之上，支撑软件之下。
- 从计算机应用角度看，操作系统是几乎人人都要使用的系统界面和接口；
- 而从软件设计和开发的角度看，操作系统起着系统软件开发基础和工具的作用；
- 而在黑客和网络攻击者看来，操作系统是他们要攻破的第一道防线；
- 从扩展角度看，将操作系统功能分成若干层次，每一个层次完成特定的功能，从而构成一个虚拟机。
- 在计算机系统中，集中了资源管理功能和控制程序执行功能的一种软件，称为操作系统。

2.操作系统特征

- **并 发 性**

并发性是指在计算机系统中同时存在若干个运行着的程序。

① 从宏观上看，这些程序在同时向前推进。

② 从微观上看，在单处理器的环境下，这些同时运行着的程序是交替在中央处理器上运行的。在多处理器系统的环境中，在处理器一级上，程序是并发执行的。

- **共 享 性**

共享性是指操作系统程序与多个用户程序共用系统中的各种资源。资源的共享性主要针对：

① 中央处理器：中央处理器是所有程序都必须使用的最重要的资源，操作系统必须采用恰当的调度策略，对多个并发程序分配处理器资源。

② 内存储器：任何一个程序必须首先调入内存之后，才能执行。

③ 外存储器：外存储器主要用来保存各种程序和数据。这些程序和数据一般以文件的形式存放在外存储器上。外存储器有各种类型，如硬盘、软盘、磁带、可读写光盘等。

④ 外部设备：计算机系统中的外部设备是供所有用户使用的，这些用户包括操作系统、系统用户（如管理员）和普通用户。

资源的共享一般有两种形式：互斥共享和同时共享。

① 互斥共享：系统中的有些资源比如打印机、磁带机、扫描仪、中央处理器、存储器等，虽然可以供多个用户程序同时使用，但是在一段特定的时间内只能由某一个用户程序使用。该资源正在被使用时，其他程序必须等待，并且在这个资源被使用完后才由操作系统根据一定的策略再选择一个用户程序占有该资源。通常把这样的资源称为临界资源。

② 同时共享：系统中还有一类资源在同一段时间内可以被多个程序同时访问。典型的可以同时共享的资源就是硬盘，可以重入的操作系统代码也是可以被同时共享的。

- **随 机 性**

操作系统的运行是在一种随机的环境下进行的。

随机性突出强调了在进行操作系统的设计与实现时要充分考虑各种各样的可能性。

操作系统本身应该稳定、可靠、安全、高效，实现程序并发和资源共享的目的。

3.操作系统结构设计

常见的操作系统体系结构有：

- 整体式结构
- 层次式结构
- 微内核（客户机/服务器）结构

① 运行在核心态的内核：内核提供所有操作系统基本都具有的那些操作，如线程调度、虚拟存储、消息传递、设备驱动以及内核的原语操作集和中断处理等。又称微内核。

② 运行在用户态的并以客户机/服务器方式运行的进程层：除内核部分外，操作系统所有的其他部分被分成若干个相对独立的进程，每一个进程实现一组服务，称为服务进程（用户应用程序对应的进程，虽然也以客户机/服务器方式活动于该层，但不作为操作系统的功能构成成分看待）。

4.一般指令和特权指令

- 运行模式通常分为用户模式和特权模式。
- 目态：为用户服务的用户模式；
- 管态：为系统专用的特权模式。
- 机器指令被划分为一般指令和特权指令。

① 特权指令包括输入输出指令、停机指令等，只有监控程序才能执行特权指令。

② 只能在内核态下运行。

③ 运行在该模式的代码，可以无限制的对系统存储、外部设备进行访问。（置程序计数器、清指令寄存器、清溢出标志）

④ 用户程序只能执行一般指令，在用户态下运行。

⑤ 一旦用户程序需要执行特权指令，处理器会通过特殊的机制将控制权移交给监控程序。

⑥ 如果用户程序在用户态下执行了特权指令，则引起访问中断，这也是 CPU 由用户态向核心态转换的方法。（置移位方向标志位）

5.研究操作系统的观点

- **软件的观点**

从软件的观点来看，操作系统是一种大型软件系统，它是多种功能程序的集合。作为一种大型软件系统，操作系统有软件的外在特性和内在特性。

- **资源管理的观点**

在计算机系统中，硬件和软件资源可以分成以下几部分：中央处理器、存储器（内存和外存）、外部设备和信息（文件）。操作系统就是负责记录谁在使用什么样的资源，系统中还有哪些资源空闲，当前响应了谁对资源的要求，以及收回哪些不再使用的资源等。

- **进程的观点**

采用进程的观点，操作系统可看作是由多个可以同时独立运行的程序和一个对这些程序进行协调的核心所组成。

- **虚机器的观点**

虚机器的观点将操作系统的功能分成若干个层次，每一层次完成特定的功能，从而构成一个虚机器，并为上一层次提供支持，构成它的运行环境。

- **服务提供者观点**

操作系统提供了一系列的功能和便利的工作环境为用户服务，所以可以把操作系统看作是服务提供者。为用户使用便利，该服务提供者提供了一组功能强大、方便、易用的广义指令（称为系统调用）。

6.操作系统提供的 3 类的接口

- 命令接口：提供一组命令供用户直接或间接操作。根据作业的方式不同，命令接口又分为联机命令接口和脱机命令接口。
- 程序接口：程序接口由一组系统调用命令组成，提供一组系统调用命令供用户程序使用。
- 图形界面接口：通过图标、窗口、菜单、对话框及其他元素和文字组合，在桌面上形成一个直观易懂，使用方便的计算机操作环境。

7.操作系统主要功能

- 进程管理（处理器管理）

① 进程管理的实质是对中央处理器进行管理，所以进程管理往往又称为处理器管理。

② 进程管理主要包括进程控制、进程同步、进程间通信和进程调度等几方面的内容。

③ 其中进程控制主要处理进程的创建、状态转换、进程撤销以及相关的进程资源的分配与回收等事务；

④ 进程同步主要处理进程之间的关系，包括进程的同步和互斥；

⑤ 进程间通信主要处理相互协作进程之间信息的交换问题；

⑥ 而进程调度则是按照一定的算法从就绪队列中挑选一个进程在处理器中真正执行它。

- 存储管理

存储管理的任务是管理计算机内存的资源。

存储管理有 3 个方面的功能：

① 内存的分配与回收：操作系统要为每个进程所占据的内存空间，在分配的过程中，还要尽可能提高内存资源的使用效能。

② 存储保护：必须考虑程序可能发生越界的情况，保护整个用户及计算机系统的程序运行。

③ 内存扩充：借助于虚拟技术在逻辑上增加进程运行空间的大小，这个大小比实际的物理内存大得多。操作系统把正在使用的页面保持在内存中即将使用的页面调入到内存中，用户就感受不到空间使用的限制。

- 文件管理

文件管理的任务是有效的支持文件的存储、检索和修改等操作，解决文件的共享、保密和保护问题，以使用户方便、安全地访问文件。

主要涉及 3 个方面：文件存储空间的管理、目录管理、文件系统的安全性。

① 管理磁盘空间和磁盘碎片整理都属于文件存储空间的管理；

② 目录管理的主要任务就是给出组织文件的方法，为每个文件建立目录项，并对众多的目录项加以有效的组织，以便为用户提供方便的按名存取；

③ 安全性包括文件的读写权限以及存取控制。

- 作业管理
- 设备管理
- 用户接口

从用户的观点来看，操作系统是用户与计算机系统之间的接口。因此，接口管理的任务是为用户提供一个使用系统的良好环境，使用户能有效地组织自己的工作流程，并使整个系统能高效地运行。

8.操作系统分类

- 按照用户界面的使用环境和功能特征的不同，一般可以把操作系统分为 3 种基本类型，即批处理系统、分时系统和实时系统。
- 随着计算机体系结构的发展，又出现了许多类型的操作系统，它们是个人操作系统、网络操作系统、分布式操作系统和嵌入式操作系统。

9.批处理操作系统特点

批处理操作系统的特点是成批处理。

- 优点：批量处理用户作业，作业流程自动化较高，资源利用率较高，作业吞吐量大，从而提高了整个系统效率。
- 缺点：用户不能直接与计算机交互，不适合调试程序。

10.分时操作系统特点

总体上看，分时操作系统具有多路性、交互性、独占性和及时性的特点。

- 多路性:指有多个用户在同时使用一台计算机。从宏观上看是多个人同时使用一个处理器，从微观上看是多个人在不同时刻轮流使用一个处理器。
- 交互性:指用户根据系统响应的结果提出下一个请求。用户直接干预操作每一步的进行。
- 独占性:指每个用户感觉不到计算机为其他人服务，就好像整个系统为他个人所独占一样。
- 及时性：指系统能够对用户提出的请求及时给予响应。

11.实时操作系统特点

- 实时操作系统（Real Time Operating System，RTOS)是指使计算机能在规定的时间内及时响应外部事件的请求，同时完成对该事件的处理，并能够控制所有实时设备和实时任务协调一致地工作的操作系统。
- 实时操作系统主要目标是:在严格时间范围内，对外部请求作出反应，系统具有高度可靠性。
- 实时系统为了能够实现硬实时或软实时的要求，除了具有多道程序系统的基本能力外，还具有实时时钟管理、过载防护和高可靠性的特点。

12.分布式操作系统特点

- 分布式操作系统是一个统一的操作系统，在系统中的所有主机使用的是同一个操作系统。
- 实现资源的深度共享。在网络操作系统中，由于各个主机使用不同的操作系统，不能随意地将一个计算任务从一台主机迁移到另一台主机执行。而在分布式系统中，通过统一的操作系统的调度，在某台主机上的一个计算任务可以迁移到另一台主机上执行，真正实现了处理机资源的共享。
- 透明性：整个分布式系统在用户眼里就像是一台具有强大功能的计算机系统。用户并不知道该分布式系统运行在多少台计算机上，各个主机地理位置上的差异对用户来讲是透明的，分布式操作系统屏蔽了这种差异。相应地，在网络操作系统中，用户能够清晰地感觉到本地主机和非本地主机之间的区别。
- 自治性：处于分布式系统中的各个主机都处于平等的地位，各个主机之间没有主从关系。一个主机的失效一般不会影响整个分布式系统。
- 分布式系统的优点在于它的分布式，分布式系统可以以较低的成本获得较高的运算性能。分布式系统的另一个优势是它的可靠性。

13.Android 操作系统特点

- Android 是一种基于 Linux 的自由及开放源代码的操作系统。
- 主要使用于移动设备，如智能手机和平板电脑，由 Google 公司和开放手机联盟领导及开发。
- 其特点就是支持移动应用和支持网络。

14.微内核（客户/服务器）结构的操作系统优点

① 高可靠性：系统服务或者设备驱动故障和与它们有关的运行任务是隔绝的；
② 高灵活性：当运行一个应用程序时，只需把选定的系统服务加载到系统中即可；
③ 适合分布式处理：一个精炼的微内核接口能够有演绎成更多模块的系统结构；
④ 提高了系统的可扩展性；
⑤ 可移植性；
⑥ 适用于对分布式处理的计算环境；
⑦ 融入了面向对象技术。

15.设备分配算法

在设备分配算法中，常采用的数据结构主要含 4 张表：
① 即系统设备表 SDT
② 设备控制表 DCT
③ 控制器控制表 COCT
④ 通道控制表 CHCT

16.程序状态字（PSW）

用一个专门的寄存器来指示处理器状态称为程序状态字（PSW），其包括的状态位有：
① 进位标志位（CF）
② 结果为零标志位（ZF）
③ 符号标志位（SF）
④ 溢出标志位（OF）
⑤ 陷阱标志位（TF）
⑥ 中断使能（中断屏蔽）标志位（IF）
⑦ 虚拟中断标志位（VIF）
⑧ 虚拟中断待决标志位（VIP）
⑨ IO 特权级别（IOPL）。

17.write（）

write（）会把参数 buf 所指的内存写入 count 个字节到参数 fd 所指的文件内。文件读写位置也会随之移动。若用户编程需要打印输出，需要系统调用 write（）。

第二章 操作系统运行机制

1.CPU 的构成与基本工作方式

一般的处理器由运算器、控制器、一系列寄存器以及高速缓存构成。

- 运算器实现任何指令中的算术和逻辑运算，是计算机计算的核心；
- 控制器负责控制程序运行的流程，包括取指令、维护 CPU 状态、CPU 与内存的交互等；
- 寄存器是指令在 CPU 内部作处理的过程中暂存数据、地址以及指令信息的存储设备，在计算机的存储系统中它具有最快的访问速度；
- 高速缓存处于 CPU 和物理内存之间，一般由控制器中的内存管理单元（Memory Management Unit，MMU）管理，它的访问 速度快于内存，低于寄存器，它利用程序局部性原理使得高速指令处理和低速内存访问得以匹配，从而提高 CPU 的效率。

2.CPU 状 态 的 转 换

- 在系统运行过程中，CPU 的状态是动态改变的，时而运行于管态，时而运行于目态，即管态和目态这两种状态可以相互转换。
- 目态到管态的转换

其转换的途径是通过中断或异常。中断响应时交换中断向量，新的中断向量中的 PSW 的 CPU 状态位标志为管态。

- 管态到目态的转换

可通过设置 PSW 指令（修改程序状态字），实现从操作系统向用户程序的转换。

当中央处理器处于管态时可执行包括特权指令在内的一切机器指令；当中央处理器处于目态时不允许执行特权指令。系统启动时，CPU 的初始状态为管态，然后装入操作系统程序。操作系统退出执行时，让用户程序在目态执行。

3.用户可见寄存器

- 用户可见寄存器通常对所有程序都是可用的，由机器语言直接使用。
- 它一般包括数据寄存器、地址寄存器以及条件码寄存器。

① 数据寄存器（Data Register)有时又称为通用寄存器，主要用于各种算术逻辑指令和访存指令，对具有浮点能力和多媒体能力的处理器来说，浮点处理过程的数据寄存器和整数处理时的数据寄存器一般是分离的。

② 地址寄存器（Address Register)用于存储数据及指令的物理地址、线性地址或者有效地址，用于某种特定方式的寻址。例如变址寄存器 (Index Register)、段指针（Segment Pointer)、栈指针（Stack Pointer)等。

③ 条件码寄存器保存 CPU 操作结果的各种标记位，例如算术运算产生的溢出、符号等，这些标记在条件分支指令中被测试，以控制程序指令的流向。一般来讲，条件码可以被隐式访问，但不能通过显式的方式修改。

4.中 断 与 异 常 的 概 念

1） 中断

- 中断是指 CPU 对系统中或系统外发生的异步事件的响应。中断是所有要打断处理器的正常工作次序，并要求其去处理某一事件的一种常用手段。
- 中断事件或中断源：引起中断的那些事件；
- 中断请求：中断源向处理器发出的请求信号；
- 中断处理程序：处理中断事件的程序；
- 中断断点：发生中断时正在执行的程序的暂停点；
- 中断响应：处理器暂停当前程序转而处理中断的过程；
- 中断返回中断处理结束之后恢复原 来程序的执行。
- 为了使得中断装置可以找到恰当的中断处理程序，专门设计了中断处理程序入口地址映射表，又称中断向量表。表中的每一项称为一个中断向量，主要由程序状态字 PSW 和指令计数器 PC 的值组成。

2） 异常

- 最早中断和异常并没有区分，都把它们叫做中断。随着它们的发生原因和处理方式的差别愈发明显，才有了现在的中断和异常之分。
- 中断是由外部事件引发的，而异常则是由正在执行的指令引发的。

5.中断与异常的分类

1） 中断系统可以分为两大组成部分：中断系统的硬件中断装置和软件中断处理程序。

● 硬件中断装置负责捕获中断源发出的中断请求，并以一定的方式响应中断源，然后将处理器的控制权移交给特定的中断处理程序。

● 中断处理程序则针对中断事件的性质而执行相应的一系列操作。

典型的中断包括：

● 时钟中断。由处理器内部的计时器产生，允许操作系统以一定规律执行函数，如时间片到时、硬件到时等。

● 输入输出（I/O)中断。由 I/O 控制器产生，用于通知一个I/O 操作的正常完成或者发生的错误。

● 控制台中断，如系统操作员通过控制台发出命令等。

● 硬件故障中断，由掉电、存储器校验错等硬件故障引起等。

2） 异常发生的时间以及位置具有确定性。

典型的异常包括：

● 程序性中断。在某些条件下由指令执行结果产生，例如算术溢出、被零除、目态程序试图执行非法指令、访问不被允许访问的存储位置、虚拟存储中的缺页等。

● 访管指令异常。目的是要求操作系统提供系统服务。

6.多级中断与中断优先级

1） 多级中断

● 从硬件上看，多级中断系统表现为有多根中断请求线从不同设备连接到中断逻辑线路上。

● 连接在不同中断请求线上的中断信号，表示它们有不同的中断级别。

● 中断信号的级别代表了该中断信号是否具有被优先处理的特权，以及这个特权的大小。

● 在多级中断系统中，硬件决定了各个中断的优先级别。

2） 多级中断的作用

● 对各类中断信号依据其紧急程度和重要性划分级别。在多级中断系统中，在同时有多个中断请求时，CPU 接收中断优先级为最高的那个中断，而忽略其中断优先级较低的那些中断。

● 解决如果有重要程度相当的多个中断信号同时到达时，如何选择首个被处理的中断信号的问题。在一般情况下，这两个中断信号具有同等的优先级。如果在同一中断级中的多个设备接口中同时都有中断请求时，一般有两种办法可以采用：

① 固定优先数：给每个设备接口安排一个不同的、固定的优先序。比如以该设备在总 线中的位置来定优先顺序，离 CPU 近的设备，其优先数高于离 CPU 远的设备。

② 轮转法：用一个表格，依次轮转响应，这是一个较为公平合理的方法。

7.系统调用与一般过程调用的区别

操作系统利用一种系统调用命令去调用所需的操作系统过程。因此，系统调用在本质上是应用程序请求操作系统核心完成某一特定功能的一种过程调用，是一种特殊的过程调用，它与一般过程调用有以下几方面的区别：

● 运行在不同的系统状态

一般过程调用，其调用程序和被调用程序都运行在相同的状态，即核心态或用户态；而系统调用与一般调用的最大区别就在于：调用程序运行在用户态，而被调用程序则运行在系统态。

● 状态的转换

一般过程调用不涉及系统状态的转换，可直接由调用过程转向被调用过程；但在运行系统调用时，由于调用和被调用过程工作在不同的系统状态，因而不允许由调用过程直接转向被调用过程，通常都是通过软中断机制先由用户态转换为核心态，在操作系统核心分析之后，转向相应的系统调用处理子程序。

● 返回问题

一般过程调用在被调用过程执行完后，将返回到调用过程继续执行。但是，在采用抢占式调度方式的系统中，被调用过程执行完后，系统将对所有要求运行的进程进行优先级分析。如果调用进程仍然具有最高优先级，则返回到调用进程继续执行；否则，将引起重新调度，以便让优先级最高的进程优先执行。此时，系统将把调用进程放入就绪队列。

● 嵌套调用

像一般过程调用一样，系统调用也允许嵌套调用，即在一个被调用过程的执行期间，还可再利用系统调用命令去调用另一个系统调用。一般情况下，每个系统对嵌套调用的深度都有一定的限制。

8.交互式操作系统

● 交互式操作系统是指用户交互式地向系统提出命令请求，系统接受每个用户的命令，采用时间片轮转方式处理服务请求，并通过交互方式在终端上向用户显示结果。

● FCFS(先来先服务)，最短作业优先，最短剩余时间优先，时间片轮转，最高优先级算法，多级反馈队列算法和最短进程优先都适用于交互式操作系统。

9.系统调用

- 为了从操作系统中获得服务，用户程序必须使用系统调用（system call），系统调用陷入内核并调用操作系统。
- 访管指令把用户态切换成内核态，并启用操作系统。当有关工作完成之后，在系统调用后面的指令把控制权返回给用户程序。
- 系统调用程序被看成是一个低级的过程，只能由汇编语言直接访问。
- 系统调用是操作系统提供给编程人员的唯一接口。

10.关闭中断响应

关闭中断响应指令属于特权指令，用户程序不能直接执行，必须要使 CPU 陷入核心态，由操作系统来执行该特权指令，因此该程序必须先发起访管中断，这是让 CPU 由用户态向核心态转换的方法。

11.程序并发执行特性

- 所谓程序并发执行是指两个或两个以上程序在计算机系统中同处于已开始执行且尚未结束的状态。
- 程序并发执行产生了一些和程序顺序执行时不同的特性：

① 并发程序在执行期间具有相互制约关系；
② 程序与计算不在一一对应；
③ 并发程序执行结果不可再现。

12.中断向量表

80x86 系统是把所有的中断向量集中起来，按中断类型号从小到大的顺序存放到存储器的某一区域内，这个存放中断向量的存储区叫做中断向量表，即中断服务程序入口地址表。

13.函数 open（）

open 是多种语言的一种函数，C 语言中 open()函数作用：打开和创建文件，是文件操作类系统调用。

14.进程控制块

进程控制块（PCB）的内容可以分成调度信息和现场信息两部分。

- 调度信息包括进程名、进程号、存储信息、优先级、当前状态、资源清单、“家族”关系、消息队列指针、进程队列指针和当前打开文件等;
- 现场信息只记录哪些可能会被其他进程改变的寄存器，如程序状态字、时钟、界地址寄存器等

第三章 进程线程模型

1.多道程序设计

- 所谓多道程序设计，就是允许多个程序同时进入内存并运行。多道程序设计是操作系统所采用的最基本、最重要的技术，其根本目的是提高整个系统的效率。
- 采用多道程序设计可以提高 CPU 的利用率。多道程序设计技术充分发挥了处理器与外围设备以及外围设备之间的并行工作能力，从而提高处理器和其他各种资源的利用率。
- 从宏观上看，CPU 与外部设备始终可以并行工作，这样使得 CPU 的运行效率达到最大化，不至于空闲。

2.多道程序设计环境特点

- 独立性
- 随机性
- 资源共享性

3.程序并发执行

- 所谓程序并发执行，是指两个或两个以上程序在计算机系统中同处于已开始执行且尚未结束的状态。
- 能够参与并发执行的程序称为并发程序。
- 引入程序并发执行，是为了充分利用系统资源，提高计算机的处理能力。
- 但是，程序并发执行产生了一些和程序顺序执行时不同的特性，概括如下：

① 并发程序在执行期间具有相互制约关系
② 程序与计算不再一一对应
③ 并发程序执行结果不可再现

4.进程和程序的区别

- 程序是构成进程的组成部分之一，一个进程的运行目标是执行它所对应的程序，如果没有程序，进程就失去了其存在的意义。
- 进程是由程序、数据和进程控制块（PCB）3 部分组成。
- 程序是静态的，进程是动态的。
- 程序的存在是永久的，进程的存在是暂时的，动态地产生和消亡。
- 一个进程可以执行一个或几个程序，一个程序亦可以构成多个进程。
- 进程具有创建其他进程的功能。被创建的进程称为子进程，创建者称为父进程，从而构成进程家族。
- 程序是指令、数据及其组织形式的描述，进程是程序的实体；

① 每一个进程都有它自己的地址空间，一般情况下，包括文本区域、数据区域和堆栈。
② 文本区域存储处理器执行的代码；
③ 数据区域存储变量和进程执行期间使用的动态分配的内存；
④ 堆栈区域存储着活动过程调用的指令和本地变量。

5.进程特性：

1） 并发性
可以同其他进程一道向前推进，即一个进程的第一个动作可以在另一个进程的最后一个动作结束之前开始。
2） 动态性
进程对应程序的执行过程，体现在两方面:
① 进程动态产生、动态消亡;
② 在进程生命周期内，其状态动态变化。
3） 独立性
一个进程是一个相对完整的资源分配单位。
4） 交往性
一个进程在运行过程中可能会与其他进程发生直接的或间接的相互作用。
5） 异步性
每个进程按照各自独立的、不可预知的速度向前推进。

6.3 状态进程模型

- 运行中的进程可以处于以下 3 种状态之一：运行、就绪、等待。
- 在任何时刻，任何进程都处于且仅处于 3 种状态之一。

1） 运行状态（Running）
① 运行状态是指进程已获得 CPU,并且在 CPU 上执行的状态。
② 在一个单 CPU 系统中，最多只有一个进程处于运行态。
2） 就绪状态（Ready）
① 就绪状态是指一个进程已经具备运行条件，但由于没有获得 CPU 而不能运行所处的状态。

② 一旦把 CPU 分配给它，该进程就可运行。

③ 处于就绪状态的进程可以是多个。

3) 等待状态（Waiting）

① 等待状态也称阻塞状态或封锁状态。

② 是指进程因等待某种事件发生而暂时不能运行的状态。

③ 系统中处于等待状态的进程可以有多个。

7.五状态进程模型

- 五状态进程模型中，进程状态被分成下列五种状态。
- 进程在运行过程中主要是在就绪、运行和阻塞 3 种状态间进行转换。
- 创建状态和退出状态描述进程创建的过程和进程退出的过程。

① 运行状态（Runing）:进程占用处理机资源；处于此状态的进程的数目小于等于处理机的数目。在没有其他进程可以执行时（如所有进程都在阻塞状态），通常会自动执行系统的空闲进程。

② 就绪状态（Ready）:进程已获得除处理机外的所需资源，等待分配处理机资源；只要分配处理机就可执行。

③ 阻塞状态（Blocked）:由于进程等待 I/O 操作或进程同步等条件而暂停运行时处于阻塞状态。

④ 创建状态（New）:进程正在创建过程中，还不能运行。

⑤ 结束状态（Exit）：进程已结束运行，回收除进程控制块之外的其他资源，并让其他进程从进程控制块中收集有关信息（如记账和将退出代码传递给父进程）。

8.七状态模型

1) 七状态进程模型把原来的就绪状态和阻塞状态进行了细分，增加了就绪挂起和阻塞挂起两个状态；这时原来的就绪状态和阻塞状态的意义也发生了一些变化：

① 就绪状态（Ready）:进程在内存且可立即进入运行状态；

② 阻塞状态（Blocked）:进程在内存并等待某事件的出现；

③ 阻塞挂起状态（Blocked，Suspend）:进程在外存并等待某事件的出现。

④ 就绪挂起状态（Ready，Suspend）:进程在外存，但只要进入内存，即可运行；

2) 在七状态进程模型中，新引入的状态转换有挂起和激活两类，意义有变化的转换有事件出现和进程提交两类。

- 挂起（Suspend）:把一个进程从内存转到外存；可能有以下几种情况：

① 阻塞到阻塞挂起：没有进程处于就绪状态或就绪进程要求更多内存资源时，会进行这种转换，以提交新进程或运行就绪进程。

② 就绪到就绪挂起：当有高优先级阻塞（系统认为会很快就绪的）进程和低优先级就绪进程时，系统会选择挂起低优先级就绪进程。

③ 运行到就绪挂起：对抢先式分时系统，当有高优先级阻塞挂起进程因事件出现而进入就绪挂起时，系统可能会把运行进程转到就绪挂起状态。

- 激活（Activate）:把一个进程从外存转到内存；可能有以下几种情况：

① 就绪挂起到就绪：就绪挂起进程优先级高于就绪进程或没有就绪进程时，会进行这种转换。

② 阻塞挂起到阻塞：当一个进程释放足够内存时，系统会把一个高优先级阻塞挂起进程激活，系统认为会很快出现该进程所等待的事件。

- 事件出现（Event Occurs）:进程等待的事件出现；如操作完成、申请成功等；可能的情况有：

① 阻塞到就绪:针对内存进程的事件出现。

② 阻塞挂起到就绪挂起:针对外存进程的事件出现。

- 提交（Admit）:完成一个新进程的创建过程，新进程进入就绪状态或就绪挂起状态。进入就绪挂起的原因是系统希望保持一个大的就绪进程表（挂起和非挂起）。

9.进程控制块（Process Control Block，PCB）

- 为了便于系统控制和描述进程的活动过程，在操作系统核心中为进程定义了一个专门的数据结构，称为进程控制块（Process Control Block，PCB）。
- PCB 是进程存在的唯一标志，当系统创建一个进程时，为进程设置一个 PCB，再利用 PCB 对进程进行控制和管理。
- 撤销进程时，系统收回它的 PCB，进程也随之消亡。
- PCB 的内容可以分成调度信息和现场信息两大部分：

① 调度信息供进程调度时使用，描述了进程当前所处的状况，它包括进程名、进程号、存储信息、优先级、当前状态、资源清单、“家族”关系、消息队列指针、进程队列指针和当前打开文件等。

② 现场信息刻画了进程的运行情况，由于每个进程都有自己专用的工作存储区，其他进程运行时不会改变它

的内容。所以，PCB 中的现场信息只记录那些可能会被其他进程改变的寄存器，如程序状态字、时钟、界地址寄存器等。一旦中断进程的运行，必须把中断时刻的内容记入 PCB 的现场信息。

10. PCB 的 3 种组织方式

- 线性方式
- 索引方式
- 链接方式

11. 进程控制原语

用于进程控制的原语一般有：创建进程、撤销进程、挂起进程、激活进程、阻塞进程、唤醒进程以及改变进程优先级等。

进程原语

1） 创建原语

- 一个进程可以使用创建原语创建一个新的进程，前者称为父进程，后者称为子进程，子进程又可以细建新的子进程，构成新的父子关系。从而整个系统可以形成一个树形结构的进程家族。
- 创建一个进程的主要任务是建立进程控制块 PCB。
- 具体操作过程是：先申请一空闲 PCB 区域，将有关信息填入 PCB，置该进程为就绪状态，最后把它插入就绪队列中。

2） 撤销原语

- 当一个进程完成任务后，应当撤销它，以便及时释放它所占用的资源。
- 撤销进程的实质是撤销 PCB。一旦 PCB 撤销，进程就消亡了。
- 具体操作过程是：找到要被撤销进程的 PCB，将它从所在队列中消去，撤销属于该进程的一切“子孙进程”，释放被撤销进程所占用的全部资源，并消去被撤销进程的 PCB。

3） 阻塞原语

- 某进程执行过程中，需要执行 I/O 操作，则由该进程调用阻塞原语把进程从运行状态转换为阻塞状态。
- 具体操作过程是：由于进程正处于运行状态，因此首先应中断 CPU 执行，把 CPU 的当前状态保存在 PCB 的现场信息中，把进程的当前状态置为等待状态，并把它插入到该事件的等待队列中去。

4） 唤醒原语

- 一个进程因为等待事件的发生而处于等待状态，当等待事件完成后，就用唤醒原语将其转换为就绪状态。
- 具体操作过程是:在等待队列中找到该进程，置进程的当前状态为就绪状态，然后将它从等待队列中撤出并插入到就绪队列中排队，等待调度执行。

12. 操作系统创建新进程

操作系统创建一个新进程的过程如下：

①申请空白 PCB;

②为新进程分配资源;

③初始化进程控制块;

④将新进程插入就绪队列，如果进程就绪队列能够接纳新进程，便将新进程插入到就绪队列中。

13. fork()函数

在 UNIX 类操作系统中，父进程通过调用 fork()函数创建子进程，子进程获得与父进程地址空间相同的一份拷贝，包括文本、数据和 bss 段、堆以及用户栈，fork()函数被调用一次，却返回 2 次：一次是在调用进程中，一次是在新创建的子进程中，

14. 线程的基本概念

- 在引入线程的操作系统中，线程是进程中的一个实体，是 CPU 调度和分派的基本单位。
- 线程自己基本上不拥有系统资源，只拥有一点在运行中必不可少的资源(如程序计数器、一组寄存器和栈)，但它可与同属一个进程的其他线程共享进程所拥有的全部资源。
- 在操作系统中再引入线程，则是为了减少程序并发执行时所付出的时间和空间开销，使操作系统具有更好的并发性。

15. 引入线程的好处

- 创建一个新线程花费时间少(结束亦如此)。创建线程不需另行分配资源，因而创建线程的速度比创建进程的速度快，且系统的开销也少。
- 两个线程的切换花费时间少。由于同一进程内的线程共享内存和文件，线程之间相互通信无须调用内核，故不需要额外的通信机制，使通信更简便，信息传送速度也快。
- 线程能独立执行，能充分利用和发挥处理器与外围设备并行工作能力。

16. Pthread 函数调用

线程调用	描述
pthread_create	创建一个新线程
pthread_exit	结束调用的线程
pthread_join	等待一个特定的线程退出
pthread_yiel	释放 CPU 来运行另外一个线程
pthread_attr	创建并初始化一个线程的属性结构
pthread_attr	删除一个线程的属性结构

17. 进程（线程）调度的时机

执行进程调度一般是在下述情况下发生的：

●正在执行的进程（线程）运行完毕；

●正在执行的进程（线程）调用阻塞原语将自己阻塞起来进入等待状态；

●正在执行的进程（线程）调用了阻塞原语操作，并且因为资源不足而被阻塞；或调用了唤醒原语操作激活了等待资源的进程（线程）；

●时间片用完；

以上都是在 CPU 为不可抢占方式下的引起进程调度的原因。在 CPU 方式是可抢占方式时，还有下面的原因：

●就绪队列中的某个进程（线程）的优先级高于当前运行进程（线程）的优先级时，引发进程（线程）调度。

18. 计算密集型 I/O 密集型

某些进程花费了绝大多数时间在计算上，而其他进程则在等待 I/O 上花费了绝大多数时间。前者称为计算密集型（Compute-Bound），也称为 CPU 密集型，后者称为 I/O 密集型（I/O-Bound），典型的计算密集型进程具有较长时间的 CPU 集中使用和较小频度的 I/O 等待。

19. 批处理检测指标

- 运行大量批处理作业的大型计算中心的管理者们为了掌握其系统的工作状态，通常检查 3 个指标：吞吐量、周转时间以及 CPU 利用率。
- 对于交互式系统，特别是分时系统和服务器，则有不同的指标。最重要的是最小响应时间和均衡性。
- 实时系统有着与交互式系统不一样的特性，所以有不同的调度目标。实时系统的特点是或多或少必须满足截止时间。
- 实时系统最主要的要求是满足所有的（或大多数）截止时间要求。
- 为了避免这些问题，进程调度程序必须是高度可预测的和有规律的。

20. 进程调度策略

操作系统中进程调度策略主要有：

① FCFS(先来先服务)
② 最短作业优先
③ 最短剩余时间优先
④ 时间片轮转
⑤ 最高优先级算法
⑥ 多级反馈队列算法
⑦ 最短进程优先

21. 交互式操作系统

- 交互式操作系统是指用户交互式地向系统提出命令请求，系统接受每个用户的命令，采用时间片轮转方式处理服务请求，并通过交互方式在终端上向用户显示结果。
- 多级反馈队列、时间片轮转和高优先级优先适用于交互式操作系统。
- 批处理系统常用的调度算法有：先来先服务、最短作业优先、最短剩余时间优先、响应比最高者优先；

22. linux 上进程的 5 种状态

① 运行状态
② 中断状态
③ 不可中断状态
④ 僵尸状态
⑤ 停止状态

23. 引起进程调度的原因

① 正在执行的进程执行完毕；

② 正在执行的进程调用阻塞原语将自己阻塞起来进入等待状态；

③ 正在执行的进程调用了阻塞原语操作，并且因为资源不足而被阻塞；或调用了唤醒原语操作激活了等待资源的进程；

④ 时间片已经用完；

⑤ 就绪对列中的某个进程的优先级高于当前运行进程的优先级。

24. 运行状态转换为就绪状态原因

在抢占式调度系统中，进程从运行状态转换为就绪状态的可能原因有：进程创建完成、时间片用完和被调度程序抢占处理机。

25. 引起进程阻塞的事件

引起进程阻塞的事件有请求系统服务、启动某种操作、新数据尚未到达与无新工作可做。

26. 引起创建进程的事件

在多道程序环境中，只有进程才能在系统中运行。因此，为使程序能运行，就必须为它创建进程。导致一个进程去创建另一个进程的典型事件，可以有以下四类：

① 用户登录：在分时系统中，用户在终端键入登录命令后，如果是合法用户，系统将为该终端建立一个进程，并把它插入到就绪队列中。

② 系统初始化：在批处理系统中，会创建 0 号、1 号系统进程。

③ 用户系统调用：用户采用系统调用创建进程。

④ 初始化批处理作业：在初始化批处理作业时，采用一个后台进程以便使新进程以并发的运行方式完成特定任务。设备分配不是会引起创建新的进程。

27. 管程

- 一个管程定义了一个数据结构和能为并发进程所执行（在该数据结构上）的一组操作，这组操作能同步进程和改变管程中的数据。
- 局部于管程的数据结构，只能被局部于管程的过程所访问，任何管程之外的过程都不能访问它；反之，局部于管程的过程也只能访问管程内的数据结构。
- 由此可见，所有进程要访问临界资源时，都必须经过管程才能进入，而管程每次只允许一个进程进入管程，从而实现了进程的互斥，但是管程无法保证本身互斥。

28. 可再入程序

- 可再入程序是由可重入代码组成的程序，可以被安全的并行执行，当该程序正在运行时，可以再次载入内存并执行它。
- 具有如下特点：它是纯代码的，即在执行过程中不可修改；调用它的进程应该提供属于它自己的数据区。

29. 进程调度功能

处理器调度负责动态地把处理器分配给进程。因此，它又叫分派程序或低级调度。它的主要功能是：

① 记录和保持系统中所有进程的有关情况及状态特征；

② 决定某个进程什么时候获得处理器，以及占用多长时间；

③ 把处理器分配给进程；

④ 收回处理器：将处理器有关的寄存器内容送入该进程的进程控制块内相应单元，以保护该进程的现场，并修改该进程的状态，从而使进程让出处理器。

30. 进程优先级

- 在进程调度算法中若采用最高优先级算法则会根据进程的优先级来决定进程调度的优先次序，分为静态优先级和动态优先级两种方法确定进程的优先级。
- 一般地，系统进程的优先级应高于用户进程的优先级；
- 若采用静态优先级，在进程创建时确定了优先级，进程运行期间优先级不会改变；
- 若采用动态优先级，在创建时先确定一个初始优先级，在进程运行中随着进程特性改变（如等待时间增长），不断改变先级。

31. 线程描述表

- 每个线程有一个唯一的标识符和一张线程描述表
- 线程描述表记录的信息有：线程 ID、指令地址寄存器、处理器寄存器，硬件设备寄存器，栈现场状态等少量线程私有信息。

32. 线程的实现机制

有 3 种途径：用户级线程、内核级线程、混合实现方式。

第四章 并发与同步

1.进程同步与进程互斥

- 进程同步：指多个进程中发生的事件存在某种时序关系，必须协同动作，相互配合，以共同完成一个任务。
- 进程互斥：指由于共享资源所要求的排他性，进程间要相互竞争，以使用这些互斥资源。

2.进程互斥解决方法

进程互斥的解决有两种做法：一是由竞争各方平等协商；二是引入进程管理者，由管理者来协调竞争各方对互斥资源的使用。

3.资源共享 3 个层次

- 互斥（MutualExclusion）：保证资源的互斥使用是指多个进程不能同时使用同一个资源，这是正确使用资源的最基本要求；
- 死锁（Deadlock）：避免死锁是指避免多个进程互不相让，避免出现都得不到足够资源的情况，从而保证系统功能的正常运行；
- 饥饿（Starvation）：避免饥饿是指避免某些进程一直得不到资源或得到资源的概率很小，从而保障系统内资源使用的公平性。

4.相互感知度划分：

相互感知的程度	交互关系	一个进程对其他进程的影响	潜在的控制问题
相互不感知（完全不了解其他进程的存在）	竞争（Competition）	一个进程的操作对其他进程的结果无影响	互斥、死锁、饥饿
间接感知（双方都与第 3 方交互，如共享资源）	通过共享进行协作	一个进程的结果依赖于从其他进程获得的信息	互斥、死锁、饥饿
直接感知（双方直接交互，如通信）	通过通信进行协作	一个进程的结果依赖于从其他进程获得的信息	死锁、饥饿

5.临界资源的访问过程

●进入区（Entry Section）：为了进入临界区使用临界资源，在进入区要检查可否进入临界区；如果可以进入临界区，通常设置相应的“正在访问临界区”标志，以阻止其他进程同时进入临界区。

●临界区（Critical Section）：进程中访问临界资源的一段代码。

●退出区（Exitt Section）：将“正在访问临界区”标志清除。

●剩余区（Remainder Section）：代码中的其余部分。

6.进程同步机制准则

- 空闲则入:任何同步机制都必须保证任何时刻最多只有一个进程位于临界区。当有进程位于临界区时，任何其他进程均不能进入临界区。
- 忙则等待：当已有进程处于其临界区时，后到达的进程只能在进入区等待。
- 有限等待：为了避免死锁等现象的出现，等待进入临界区的进程不能无限期地“死等”。
- 让权等待：因在进入区等待而不能进入临界区的进程，应释放处理机，转换到阻塞状态，以使得其他进程有机会得到处理机的使用权。

7.进程互斥的硬件方法

目前，在平等协商时通常利用某些硬件指令来实现进程互斥。硬件方法的主要思路是用一条指令完成读和写两个操作，因而保证读操作与写操作不被打断。依据所采用的指令的不同，硬件方法分成 TS 指令和 Swap 指令两种。

- TS(Test-and-Set)指令

TS 指令的功能是读出指定标志后把该标志设置为 TRUE。TS 指令的功能可描述成下面的函数。

```
Boolean TS (Boolean * lock) {
Boolean old;
old=*lock;  lock=TRUE;
return old;
}
```

利用 TS 指令实现的进程互斥算法是，每个临界资源设置一个公共布尔变量 lock，表示资源的两种状态：TRUE 表示正被占用，FALSE 表示空闲，初值为 FALSE。在进入区利用 TS 进行检查和修改标志 lock。有进程在临界区时，重复检查，直到其他进程退出时检查通过。所有要访问临界资源的进程的进入区和退出区代码是相同的。

TS 指令实现互斥的算法是：

① 测试锁变量的值，如为 1，则重复执行本命令，不断重复测试变量的值；

② 如为 0，则立即将锁变量测值置为 1，进入临界区；

③ 测试并设置指令是一条完整的指令，而在一条指令的执行中间是不会被中断的，保证了锁的测试和关闭的连续性；

④ 退出临界区时，将锁变量测试值设为 0。

2）Swap 指令（或 Exchange 指令）

Swap 指令的功能是交换两个字（字节）的内容。可用下面的函数描述 Swap 指令的功能。

```
Void SWAP(int*a, int*b){
Int temp;
temp=*a; *a=* b;*b =temp;
}
```

利用 Swap 指令实现的进程互斥算法是，每个临界资源设置一个公共布尔变量 lock,初值为 FALSE;每个进程设置一个私有布尔变量 key,用于与 lock 间的信息交换在进入区利用 Swap 指令交换 lock 与 key 的内容，然后检查 key 的状态;有进程在临界区时，重复交换和检查过程，直到其他进程退出时检查通过。

8.硬件方法优缺点

使用硬件方法实现进程互斥，

1） 优点有以下几个方面：

- 使用范围广：硬件方法适用于任意数目的进程，在单处理器和多处理器环境中完全相同；
- 简单：硬件方法的标志设置简单、含义明确，容易验证其正确性；
- 支持多个临界区：在一个进程内有多个临界区时，只需为每个临界区设立一个布尔变量；

2） 其缺点有：

- 进程在等待进入临界区时，要耗费处理机时间，不能实现“让权等待”；
- 由于进入临界区的进程是从等待进程中随机选择的，有的进程可能一直选不上，从而导致“饥饿”。

9.信号量

信号量是由操作系统提供的管理公有资源的有效手段。信号量代表可用资源实体的数量。属于低级通信方法

- empty 信号量表明的是空闲资源数目；
- full 信号量表明的是满的资源数目；
- mutex 信号量用于实现互斥访问。

10.PV 操作

1） PV 操作由 P 操作原语和 V 操作原语组成（原语是不可中断的过程）对信号量进行操作。

- P（S）：将信号量 S 的值减 1，即 S=S-1；如果 S>=0，则该进程继续执行；否则该进程置为等待状态，排入等待队列。
- V（S）：将信号量 S 的值加 1，即 S=S+1；如果 S>0，则该进程继续执行；否则释放队列中第一个等待信号量的进程。

2） 优点：

P、V 原语的执行，不受进程调度和执行的打断，从而很好地解决了原语操作的整体性。

3） 缺点：

- 一个信号量只能置一次初值，以后只能对之进行 P 操作或 V 操作。信号量机制功能强大，但使用时对信号量的操作分散，而且难以控制，读写和维护都很困难。
- 核心操作 P-V 分散在各用户程序的代码中，不易控制和管理；一旦错误，后果严重，且不易发现和纠正。

11.PV 处理过程

依据对临界区访问过程的分析，信号量机制中 P 原语相当于进入区操作，V 原语相当于退出区操作。下面来分析操作系统对这两个原语操作的处理过程。

- P 原语所执行的操作可用下面函数 wait(s)来描述。

```
wait(s)
{
-- s.count; //表示申请一个资源
If (s.count <0)//表示没有空闲资源
 {
调用进程进入等待队列 s.queue;
阻塞调用进程;
```

}
}

- V 原语所执行的操作可用下面函数 signal(s)来描述。

```
signal(s)
{
++s.count; //表示释放一个资源
if(s.count<=0)//表示有进程处于阻塞状态
{
从等待队列 s.queue 中取出头一个进程 P;
进程 P 进入就绪队列;
}
}
```

- 利用操作系统提供的信号量机制，可实现临界资源的互斥访问。
- 在使用信号量进行共享资源访问控制时，必须成对使用 P 和 V 原语。
- 遗漏 P 原语则不能保证互斥访问，遗漏 V 原语则不能在使用临界资源之后将其释放给其他等待的进程。
- P、V 原语的使用不能次序错误、重复或遗漏。

12.前趋关系

利用操作系统提供的信号量机制可实现进程间的同步，即所谓的前趋关系。

13.管程

- 一个管程是一个由过程、变量及数据结构等组成的集合，它们组成一个特殊的模块或软件包。
- 进程可在任何需要的时候调用管程中的过程，但它们不能在管程之外声明的过程中直接访问管程内的数据结构。
- 一个管程由 4 个部门组成：管程名称，共享数据的说明，对数据进行操作的一组过程和对共享数据赋初值的语句。
- 管程能保障共享资源的互斥执行。
- 为了保证管程共享变量的数据完整性，规定管程互斥进入;
- 进程间同步关系：一个管程定义了一个数据结构和能为并发进程所执行（在该数据结构上）的一组操作，这组操作能同步进程和改变管程中的数据。
- 任意时刻管程中只能有一个活跃进程，这一特性使管程能有效地完成互斥。

14. 解决进程通信 3 类方案

解决进程之间的大量信息通信的问题有 3 类方案：共享内存、消息机制以及通过共享文件进行通信，即管道通信。

1） 共享内存

在相互通信的进程之间设有一个公共内存区，一组进程向该公共内存中写，另一组进程从公共内存中读，通过这种方式实现两组进程间的信息交换。

2） 消息机制

进程在运行过程中，可能需要与其他的进程进行信息交换，于是进程通过某种手段发出自己的消息或接收其他进程发来的消息。

- 消息缓冲区通信机制

① 消息缓冲区，这是一个由消息长度、消息正文、发送者、消息队列指针组成的数据结构。
② 消息队列首指针 m_q，一般保存在 PCB 中。
③ 互斥信号量 m_mutex，初值为 1，用于互斥访问消息队列，在 PCB 中设置。
④ 同步信号量 m_syn，初值为 0，用于消息计数，在 PCB 中设置。

为实现消息缓冲通信，要利用发送消息原语（send)和接收消息原语（receive)。

① 发送消息原语 send(receiver，a)。

发送进程调用 send 原语发送消息，调用参数 receiver 为接收进程名，a 为发送进程存放消息的内存区的首地址。send 原语先申请分配一个消息缓冲区，将由 a 指定的消息复制到缓冲区，然后将它挂入接收进程的消息队列，最后唤醒可能因等待消息而等待的接收进程。

send 原语描述如下：send(R,M)

```
{
根据 R 找接收进程，如果没找到，则出错返回;
申请空缓冲区 P(s_b);
```

P(b_mutex);
取空缓冲区;
V(b_mutex);
把消息从 M 处复制到空缓冲区;
P(m_mutex);
根据 m_q，把缓冲区挂到接收进程的消息链链尾;
V(m_mutex);
V(m_syn);
}

其中，s_b 是空缓冲区个数，初值为 n,b_mutex 是空缓冲区的互斥信号量，初值为 1。

② 接收消息原语 receive(a)。

接收进程调用 receive 原语接收一条消息，调用参数 a 为接收进程的内存消息区。receive 原语从消息队列中摘下第一个消息缓冲区，并复制到参数 a 所指定的消息区，然后释放该消息缓冲区。若消息队列为空，则阻塞调用进程。

- 信箱通信

以发送信件以及接收回答信件为进程间通信的基本方式。

好处：发送方和接收方不必直接建立联系，没有处理时间上的限制。

发送方可以在任何时间发信，接收方也可以在任何时间收信。

规则：

① 若发送信件时信箱已满，则发送进程应被置成“等信箱”状态，直到信箱有空时才被释放。

② 若取信件时信箱中无信，则接收进程应被置成“等信件”状态，直到有信件时才被释放。

- 管道通信

① 管道通信是连接两个进程之间的一个打开的共享文件，专用于进程之间进行数据通信。

② 管道通信的基础是文件系统。

③ 在对管道文件进行读写操作的过程中，发送进程和接收进程要实施正确的同步和互斥，以确保通信的正确性。

④ 管道通信具有传送数据量大的优点，但通信速度较慢。

第五章 内存管理

1.存储体系构成

在计算机系统中层次化的存储体系是由寄存器、高速缓存、内存储器、硬盘存储器、磁带机和光盘存储器等装置构成的。

2.存储保护

- 存储保护的目的在于为多个程序共享内存提供保障，使在内存中的各程序只能访问其自己的区域，避免各程序间相互干扰。
- 特别是当某一程序发生错误时，不至于影响其他程序的运行，更要防止破坏系统程序。
- 存储保护的内容包括:保护系统程序区不被用户有意或无意的侵犯；不允许用户程序读写不属于自己地址空间的数据，如系统区地址空间、其他用户程序的地址空间。
- 地址越界保护

① 如果进程在运行时所产生的地址超出其地址空间，则发生地址越界。

② 地址越界可能侵犯其他进程的空间，影响其他进程的正常运行;也可能侵犯操作系统空间，导致系统混乱；

③ 发生越界时产生中断，由操作系统进行相应处理。

- 权限保护

① 对于允许多个进程共享的公共区域，每个进程都有自己的访问权限。

② 对属于自己区域的信息，可读可写。

③ 对公共区域中允许共享的信息或获得授权可使用的信息，可读而不可修改。

④ 未获授权使用的信息，不可读、不可写。

- 存储保护一般以硬件保护机制为主，软件为辅；
- 当发生地址越界或非法操作时，由硬件产生中断，进入操作系统处理。

3.静态重定位

- 在装入一个程序时，把程序中的指令地址和数据地址全部转换成绝对地址。
- 由于地址转换工作是在程序开始执行前集中完成的，所以在程序执行过程中就无须再进行地址转换工作，这种地址转换方式称为“静态重定位”。

4.动态重定位

- 在装入程序时，不进行地址转换，而是直接把程序装入到分配的内存区域中。
- 在程序执行过程中，每当执行一条指令时都由硬件的地址转换机构将指令中的逻辑地址转换成绝对地址。
- 这种方式的地址转换是在程序执行时动态完成的，故称为“动态重定位”。

5.分区存储管理

- 分区存储管理是能满足多道程序运行的最简单的存储管理方案。其基本思想是把内存划分成若干个连续区域，称为分区，每个分区装入一个运行程序。
- 分区的方式可以归纳成固定分区和可变分区两类。

1） 固定分区

① 固定分区是指系统先把内存划分成若干个大小固定的分区，一旦划分好，在系统运行期间便不再重新划分。

② 为了满足不同程序的存储要求，各分区的大小可以不同。

③ 由于每一分区的大小是固定的，就对可容纳程序的大小有所限制了。

④ 因此，程序运行时必须提供对内存资源的最大申请量；

⑤ 固定分区方案灵活性差，可接纳程序的大小受到了分区大小的严格限制。

2） 可变分区

① 可变分区是指系统不预先划分固定分区，而是在装入程序时划分内存分区，使为程序分配的分区的大小正好等于该程序的需求量，且分区的个数是可变的。

② 显然，可变分区有较大的灵活性，较之固定分区能获得更好的内存利用率。

③ 在可变分区管理方案中，随着分配和回收次数的增加，必然导致碎片的出现。

④ 解决碎片问题的办法是在适当时刻进行碎片整理，通过移动内存中的程序，把所有空闲碎片合并成一个连续的大空闲区且放在内存的一端，而把所有程序占用区放在内存的另一端，这一技术称为“移动技术”或“紧凑技术”或“紧缩技术”。

6.空闲分区的分配策略

这里介绍操作系统查找和分配空闲区的四种分配算法。

1）最先适应算法

- 最先适应算法,又称顺序分配算法。在这种分配算法中，当接到内存申请时，顺序查找分区说明表，找到第一个满足申请长度的空闲区，将其分割并分配。
- 此算法简单，可以快速做出分配决定。

2）最优适应算法

- 当接到内存申请时，查找分区说明表，找到第一个能满足申请长度的最小空闲区，将其分割并分配。
- 此算法最节约空间，因为它尽量不分割大的空闲区；其缺点是可能会形成很多很小的空闲区域，称作碎片。

3）最坏适应算法

- 当接到内存申请时，查找分区说明表，找到能满足申请要求的最大的空闲区。
- 基本思想：在大空闲区中装入信息后，分割剩下的空闲区相对也很大，还能用于装入其他程序。
- 优点：可以避免形成碎片；
- 缺点：分割了大的空闲区后，如果再遇到较大的程序申请内存时，无法满足要求的可能性较大。

4）下次适应算法

- 当接到内存申请时，查找分区说明表，从上一次分配的位置开始扫描内存，选择下一个大小足够的可用块。

7.分区的回收 4 种可能

1） 回收分区的上邻分区是空闲的，需要将两个空闲区合并成一个更大的空闲区，然后修改空闲区表。

方法如下：

如果空闲区表中第 i 个登记栏中的“起始地址+长度”正好等于S,则表明回收区有一个上邻空闲区。这时要修改第 i 栏登记项的内容:起始地址不变，长度为原长度加上 L,即：度=原长度+L

2） 回收分区的下邻分区是空闲的，需要将两个空闲区合并成一个更大的空闲区，然后修改空闲区表。

方法如下：

如果 S+L正好等于空闲区表中某个登记的栏目（假定为第i栏）所示分区的起始地址，则表明回收区有一个下邻空闲区。这时只要修改第i栏登记项的内容：

起始地址=S

长度=原长度+L

则第 i 栏指示的空闲区是回收区与下邻空闲区合并后的一个大空闲区。

3） 回收分区的上邻分区和下邻分区都是空闲的，需要将 3 个空闲区合并成一个更大的空闲区，然后修改空闲区表。

如果 S =第 i 栏起始地址+长度

S+L=第 k 栏起始地址

则表明回收区既有上邻空闲区，又有下邻空闲区。此时，必须把这 3 个区合并成一个空闲区登记入空闲区表中，只需使用一个登记栏目。具体修改方法如下：

第 i栏起始地址不变;

第 i栏长度为“i 栏中原长度+k栏中长度+L”；

第 k 栏的标志应修改成“空”状态。

于是,第t 栏中登记的空闲区就是合并后的空闲区，而第 k 栏成为空表目了。

4） 回收分区的上邻分区和下邻分区都不是空闲的，则直接将空闲分区记录在空闲区表中。

这时，应找一个标志为“空”的登记栏，把回收区的起始地址和长度登记入表，且把该栏目中的标志位修改成“未分配”，表示该登记栏中指示了一个空闲区。

8.覆盖技术

- 覆盖技术是指一个程序的若干程序段或几个程序的某些部分共享某一个存储空间。
- 未执行的程序段先保存在磁盘上，当有关程序段的前一部分执行结束后，把后续程序段调入内存，覆盖前面的程序段。
- 覆盖技术不需要任何来自操作系统的特殊支持，可以完全由用户实现；
- 覆盖可以从用户级彻底解决内存小装不下程序的问题。

- 覆盖技术利用相互独立的程序段之间在内存空间的相互覆盖，逻辑上扩充了内存空间，从而在某种程度上实现了在小容量内存上运行较大程序的目的。
- 覆盖技术主要用于系统程序的内存管理上。

9.交换技术

- 交换技术又称对换技术。在分时系统中，用户的进程比内存能容纳的数量要多，这就需要在磁盘上保存那些内存放不下的进程。在需要运行这些进程时，再将它们装入内存。
- 进程从内存移到磁盘并再移回内存称为交换。
- 交换技术是进程在内存与外存之间的动态调度，是由操作系统控制的。
- 系统可以将那些不在运行中的进程或其一部分调出内存，暂时存放在外存上的一个后备存储区（称为盘交换区 Swapping Area）中，以腾出内存空间给现在需要内存空间的进程，后者可能需要从外存换入内存，以后再将换出的进程调入内存继续执行。
- 交换技术多用于分时系统中。
- 交换技术利用外存来逻辑地扩充内存，它的主要特点是，打破了一个程序一旦进入内存便一直运行到结束的限制。

10.页式存储管理

- 页式存储器提供编程使用的逻辑地址由两部分组成：页号和页内地址。其格式为：

页号	页内地址

- 页式存储的地址结构确定了内存分块的大小，也就决定了页面的大小。
- 假定地址用 m 个二进制表示，其中页内地址部分占用 n 个二进制位，那么，每一个块的长度就是，也就是每一页有 2^n 个字节。这时，页号部分占用了 m-n 位，所以，最大的程序可允许有 $2^{(m-n)}$ 个页面。
- 从地址结构来看，逻辑地址是连续的。

11.存储空间的分配与回收

- 页式存储管理分配内存空间以物理页面为单位；
- 简单的内存分配表可以用一张“位示图”构成。
- 位示图中的每一位与一个内存块对应，每一位的值可以是 0 或 1，0 表示对应的内存块为空闲，1 表示已占用。
- 在进行内存分配时，先查看空闲块数是否能满足程序要求。若不能满足，则不进行分配，程序就不能装入内存；若能满足，则根据需求从位示图中找出一些为 0 的位，把这些位置成 1，并从空闲块数中减去本次分配的块数，然后按照找到的位计算出对应的块号。
- 当找到一个为 0 的位后，根据它所在的字号、位号，按如下公式就可计算出对应的块号：

块号=字号 ×字长+位号

- 把程序装入到这些内存块中，并为该程序建立页表。

12.页式存储管理的地址转换

- 为实现页式存储管理，系统要提供页表起始地址寄存器和页表长度寄存器以及要高速缓冲存储器的支持。
- 页表指出该程序逻辑地址中的页号与所占用的内存块号之间的对应关系；
- 页表的长度由程序拥有的页面数而定；
- 页表是硬件进行地址转换的依据，每执行一条指令时按逻辑地址中的页号查页表。若页表中无此页号，则产生一个“地址错”的程序性中断事件。若页表中有此页号，则可得到对应的内存块号，按计算公式可转换成访问的内存的物理地址。
- 物理地址的计算公式为：

物理地址=内存块号 ×块长+页内地址

- 根据二进制乘法运算的性质，一个二进制数乘以 2^n 结果实际上是将该数左移 n 位。所以，实际上是把内存块号作为绝对地址的高位地址，而页内地址作为它的低地址部分。

13.页表

1）多级页表

- 当系统支持 32 位的逻辑地址空间时，若页面大小为 4KB，则页表将包含 1M 个表项。假设每个表项由 4 字节组成，那么仅仅是为了存储页表就要为每个进程分配 4MB 的物理地址空间。假设用户地址空间为 2GB，页面大小为 4KB，则一个进程最多可以有 219 页。若用 4 字节表示一页的物理页号，则页表本身就占用 2MB，即需要 512 个页面存放。
- 存放页表的页面为页表页。一般来说，页表页可以不连续存放，因此需要对页表页的地址进行索引。

● 在大多数操作系统中采用二级页表，即由页表页和页目录一起构成进程页表。第一级表示页目录，保存页表页的地址;第二级表示页表页，保存物理页面号（即内存块号）。

● 在 Windows 操作系统中，页目录被称为页目录项（Page Directory Entry,PDE)，页表被称为页表项（Page Table Entry，PTE)。

2）散列页表

当地址空间大于 32 位时，一种常见的方法是使用以页号为散列值的散列页表。

其中每个表项都包含一个链表，该链表中元素的散列值都指向同一个位置。

这样，散列页表中的每个表项都包含3个字段：(a）虚拟页号，(b）所映射的页框号，(c）指向链表中下一个元素的指针。

3）反置页表

● 在反置页表中，每个物理页框对应一个表项，每个表项包含与该页框相对应的虚拟页面地址以及拥有该页面进程的信息。

● 因此，整个系统中只存在一个页表，并且每个页框对应其中一个表项。

● 由于一方面系统中只有一个页表，而另一方面系统中又存在着多个映射着物理内存的地址空间，因此需要在反置页表中存放地址空间标志符。这样就保证了一个特定进程的逻辑页面可以映射到相应的物理页框上。

14. 快表

● 为了提高存取速度，在地址映射机制中增加一个小容量的联想寄存器（相联存储器)，它由高速缓冲存储器组成。

● 利用高速缓冲存储器存放当前访问最频繁的少数活动页面的页号，这个高速缓冲器被称为“快表”，也称为转换检测缓冲器（Translation Lookaside Buffer，TLB)。

● 快表只存放当前进程最活跃的少数几页，随着进程的推进，快表的内容动态进行更新。

● 更新原理：当某一用户程序需要存取数据时，根据该数据所在的逻辑页号在快表中找出对应的内存块号，然后拼接页内地址，以形成物理地址；如果在快表中没有相应的逻辑页号，则地址映射仍然通过内存中的页表进行；在得到内存块号后需将该块号填到快表的空闲单元中；若快表中没有空闲单元，则根据置换算法置换某一行，再填入新得到的页号和块号。

● 查找快表和查找内存页表是并行进行的，一旦发现快表中有与所查页号一致的逻辑页号就停止查找内存页表，而直接利用快表中的逻辑页号。

● 例：假定访问内存的时间为 200ns,访问高速缓冲存储器的时间为 40ns，高速缓冲存储器为 16 个单元时，查快表的命中率为 90%。于是，按逻辑地址转换成绝对地址进行存取的平均访问时间为：

$$(200+40)\times 90\%+(200+200)\times 10\%=256(ns)$$

不使用快表需两次访问内存的时间为 200×2=400ns。可见使用快表与不使用快表相比，访问时间下降了 36%。

15. 虚拟存储器

● 实现虚拟存储器需要以下的硬件支持：

① 系统有容量足够大的外存。

② 系统有一定容量的内存。

③ 最主要的是，硬件提供实现虚-实地址映射的机制。

④ 缺页中断处理程序

⑤ 页表

● 在一个虚拟存储系统中，决定虚拟存储空间最大容量的要素是计算机系统地址位宽。

● 虚拟存储技术是动态的扩充内存容量。

● 虚拟存储器的工作原理如下：

① 当进程开始运行时，先将一部分程序装入内存，另一部分暂时留在外存；

② 当要执行的指令不在内存时，由系统自动完成将它们从外存调入内存的工作；

③ 当没有足够的内存空间时，系统自动选择部分内存空间，将其中原有的内容交换到磁盘上，并释放这些内存空间供其他进程使用。

16. 页表增加项

在使用虚拟页式存储管理时需要在页表中增加以下的表项：

页号——页面的编号。

● 有效位——又称驻留位、存在位或中断位，表示该页是在内存还是在外存。

● 页框号——页面在内存中时所对应的内存块号。

● 访问位——又称引用位或参考位，表示该页在内存期间是否被访问过。

- 修改位——表示该页在内存中是否被修改过。
- 保护位——是否能读/写/执行。
- 禁止缓存位——采用内存映射 I/O 的机器中需要的位。

其中，访问位和修改位可以用来决定置换哪个页面，具体由页面置换算法决定。

17.缺页中断

- 若在页表中发现所要访问的页面不在内存，则产生缺页中断。
- 当发生缺页中断时，操作系统必须在内存中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。
- 整个缺页处理过程简单阐述如下：

① 根据当前执行指令中的逻辑地址查页表的驻留位，判断该页是否在内存。

② 该页标志为“0”，形成缺页中断。保留现场。中断装置通过交换 PSW 让操作系统的中断处理程序占用处理器。

③ 操作系统处理缺页中断，寻找一个空闲的页面。

④ 若有空闲页，则把磁盘上读出的信息装入该页面中。

⑤ 修改页表及内存分配表，表示该页已在内存。

⑥ 如果内存中无空闲页，则按某种算法选择一个已在内存的页面，把它暂时调出内存。若在执行中该页面已被修改过，则要把该页信息重新写回到磁盘上，否则不必重新写回磁盘。当一页被暂时调出内存后，让出的内存空间用来存放当前需要使用的页面。页面被调出或装入之后都要对页表及内存分配表作修改。

⑦ 恢复现场，重新执行被中断的指令。当重新执行该指令时，由于要访问的页面已被装入内存，所以可正常执行下去。

18.页面调度 3 个策略

虚拟存储器系统通常定义 3 种策略进行页面调度：调入策略，置页策略和置换策略。

1）调入策略

- 虚拟存储器的调入策略决定了什么时候将一个页由外存调入内存之中。
- 在虚拟页式管理中有两种常用调入策略：

① 请求调页（Demand Paging):只调入发生缺页时所需的页面。实现简单，但易产生较多的缺页中断，容易产生抖动现象。

② 预调页（Prepaging):在发生缺页需要调入某页时，一次调入该页以及相邻的几个页。

2）置页策略

当线程产生缺页中断时，内存管理器还必须确定将调入的虚拟页放在物理内存的何处。用于确定最佳位置的一组规则称为“置页策略”。选择页框应使 CPU 内存高速缓存不必要的震荡最小。

3）置换策略

如果缺页中断发生时物理内存已满，“置换策略”被用于确定哪个虚页面必须从内存中移出，为新的页面腾出空位。

- 固定分配局部置换（Fixed Allocation，Local Replacement)。

① 可基于进程的类型，为每一进程分配固定的页数的内存空间，在整个运行期间都不再改变。

② 采用该策略时，如果进程在运行中出现缺页，则只能从该进程的 W 个页面中选出一个换出，然后再调入一页，以保证分配给该进程的内存空间不变。

- 可变分配全局置换（Variable Allocation，Global Replacement)。

① 采用这种策略时，先为系统中的每一进程分配一定数量的物理块，操作系统本身也保持一个空闲物理块队列。

② 当某进程发生缺页时，由系统的空闲物理块队列中取出一物理块分配给该进程。

③ 但当空闲物理块队列中的物理块用完时，操作系统才从内存中选择一块调出。

④ 该块可能是系统中任意一个进程的页。

- 可变分配局部置换（Variable Allocation，Local Replacement)。

① 同样基于进程的类型，为每一进程分配一定数目的内存空间。

② 但当某进程发生缺页时，只允许从该进程的页面中选出一页换出，这样就不影响其他进程的运行。

③ 如果进程在运行的过程中频繁地发生缺页中断，则系统再为该进程分配若干物理块，直到进程的缺页率降低到适当程度为止。

19. “抖动” 现象

如果刚被调出的页面又立即要用，因而又要把它装入，而装入不久又被选中调出，调出不久又被装入，如此反复，使调度非常频繁。这种现象称为“抖动”或称“颠簸”。

20.先进先出页面置换算法（First-In First-Out，FIFO）

- FIFO 算法简单，容易实现。
- 把装入内存的那些页面的页号按进入的先后次序排好队列，每次总是调出队首的页，当装入一个新页后，把新页的页号排入队尾。
- 由操作系统维护一个所有当前在内存中的页面的链表，最老的页面在表头，最新的页面在表尾。
- 当发生缺页时，置换表头的页面并把新调入的页面加到表尾。

21.最近最少使用页面置换算法（Least Recently Used,LRU）

- LRU 页面置换算法：在缺页发生时，首先置换掉最长时间未被使用过的页面；
- 最近最少使用页面置换算法总是选择距离现在最长时间内没有被访问过的页面先调出。
- 实现这种算法的一种方法是在页表中为每一页增加一个“计时”标志，记录该页面自上次被访问以来所经历的时间，每被访问一次都应从“0”开始重新计时。
- 当要装入新页时，检查页表中各页的计时标志，从中选出计时值最大的那一页调出（即最近一段时间里最长时间没有被使用过的页），并且把各页的计时标志全置成“0”，重新计时。
- 当再一次产生缺页中断时，又可找到最近最久未使用过的页，将其调出。

22.举例说明页面置换算法

- A:某程序在内存中分配 3 个页面，初始为空，所需页面的走向为 4，3，2，1，4，3，5，4，3,2,1,5，**采用 FIFO 算法**，请计算整个缺页次数。

下面用“时间长-页”表示在内存时间最长的页面，“时间中-页”其次，“时间短-页”表示在内存时间最短的页面。x 表示缺页，√表示不缺页。

页面走向	4	3	2	1	4	3	5	4	3	2	1	5
时间段-页	4	4	2	1	4	3	5	5	5	2	1	1
时间中-页		4	3	2	1	4	3	3	3	5	2	2
时间长-页			4	3	2	1	4	4	4	3	5	5
	x	x	x	x	x	x	x	√	√	x	x	√
	1	2	3	4	5	6	7			8	9	

① 开始时，内存中 3 个页面初始为空，故产生第 1 个缺页中断，需要把页面 4 调入。同样产生第 2 个缺页中断，需要把页面 3 调入。产生第 3 个缺页中断，需要把页面 2 调入。

② 此时 3 个内存页面全满。在需要页面 1 时，发现页面4 时间最长，故产生第 4 个缺页中断，把页面 4 换出，页面1 调入。接着又需要页面 4，于是产生第5个缺页中断，把页面 3换出，页面4调入。后面又需要页面3，于是产生第 6个缺页中断，把页面 2换出，页面3调入。接着又需要页面 5，于是产生第7 个缺页中断，把页面1换出，页面5调入。

③ 下面需要页面 4，正好在内存。接着需要页面 3，也正好在内存。后面需要页面 2，于是产生第 8 个缺页中断，把页面 4 换出，页面2 调入。接着需要页面 1，于是产生第9 个缺页中断，把页面 3 换出，页面1 调入。最后需要页面 5，正好在内存。整个操作结束，共产生缺页中断 9 次。

B:在上述例子中**采用 LRU 算法**，请计算整个缺页次数。

同样，用“时间长-页”表示未使用时间最长的页面，“时间中-页”其次，“时间短-页”表示未使用时间最短的页面。

页面走向	4	3	2	1	4	3	5	4	3	2	1	5
时间段-页	4	3	2	1	4	3	5	4	3	2	1	5
时间中-页		4	3	2	1	4	3	5	4	3	2	1
时间长-页			4	3	2	1	4	3	5	4	3	2
	x	x	x	x	x	x	x	√	√	x	x	x
	1	2	3	4	5	6	7			8	9	10

共缺页中断 10 次。

C:在上述例子中采用 **OPT 算法**，请计算整个缺页次数。

最长时间以后才会用到的页面，用“时间长-页”表示，“时间中-页”其次，“时间短-页”表示最短时间会用到的页面。

页面走向	4	3	2	1	4	3	5	4	3	2	1	5
时间段-页	4	3	2	1	1	1	5	5	5	2	1	1
时间中-页		4	3	3	3	3	3	3	3	5	5	5
时间长-页			4	4	4	4	4	4	4	4	4	4
	x	x	x	x	√	√	x	√	√	x	x	√
	1	2	3	4			5			6	7	

共缺页中断 7 次。

23.贝莱迪异常

当分配给进程的物理页面数增加时，缺页次数反而增加。这一现象称为贝莱迪异常（BeladyAnomaly）现象，FIFO 页面置换算法会产生异常现象。

24.缺页中断率

- 假定一个程序共有 n 页，系统分配给它的内存块是 w 块（m、n 均为正整数，因此，该程序最多有 m 页可同时被装入内存。如果程序执行中访问页面的总次数为 1 其中有 F 次访问的页面尚未装入内存，故产生了 F 次缺页中断。现定义：

$$f=F/A$$

把 f 称为“缺页中断率”。

- 显然，缺页中断率与缺页中断的次数有关。因此，影响缺页中断率的因素如下：

① 分配给程序的内存块数
② 页面的大小
③ 程序编制方法
④ 页面置换算法

25.虚拟存储管理的性能问题

- 引入虚拟存储管理，把内存和外存统一管理，其真正目的，是把那些访问概率非常高的页放入内存，减少内外存交换的次数。
- 在虚存中，页面可能在内存与外存之间频繁地调度，有可能出现抖动或颠簸。
- 颠簸是由于缺页率高而引起的。
- 此外，一般进程在一段时间内集中访问一些页面，称为“活动”页面，这是与程序的局部性有关的。如果分配给一个进程的内存物理页面数太少，使得该进程所需要的“活动”页面不能全部装入内存，则进程在运行过程中可能会频繁地发生缺页中断，从而产生颠簸。
- 采用工作集模型，可以解决颠簸问题。

26.段式存储管理

- 系统将内存空间动态划分为若干个长度不同的区域，每个区域称作一个物理段。每个物理段在内存中有一个起始地址，称作段首址。
- 将物理段中的所有单元从 0 开始依次编址，称为段内地址。
- 用户程序的逻辑地址由段号和段内地址两部分组成。
- 内存分配时，系统以段为单位进行内存分配，为每一个逻辑段分配一个连续的内存区（物理段）。逻辑上连续的段在内存中不一定连续存放。
- 段式存储管理是为程序的每一个分段分配一个连续的内存空间。
- 空闲区的分配也可以采用首先适应算法、最佳适应算法、最坏适应算法。
- 在进行动态地址转换时，硬件提供段表起始地址寄存器、段表长度寄存器等支持。

27.页表项内容

在虚拟页式存储管理系统中，每个页表项中必须包含的是：

①有效位：用于指明表项对地址转换是否有效；

②读写位：如果等于 1，表示页面可以被读、写或执行。如果为 0，表示页面只读或可执行；

③访问标志：处理器只负责设置该标志，操作系统可通过定期地复位该标志来统计页面的使用情况；

④修改位：当处理器对一个页面执行写操作时，就会设置对应页表项的 D 标志。处理器并不会修改页目录项中的 D 标志。

28.页式分配的优点

①由于它不要求作业或进程的程序段和数据在内存中连续存放，从而有效地解决了碎片问题。

②动态页式管理提供了内存和外存统一管理的虚存实现方式，使用户可以利用的存储空间大大增加。这既提高了主存的利用率，又有利于组织多道程序执行。

29.请求分页的外存

在请求分页的外存（磁盘）分为两部分：

- 用于存放文件的文件区和用于存放对换页面的对换区。
- 由于与进程有关的文件都放在文件区，故凡是未运行的页面都应该从文件区调入。

30.内存管理方案

要能与虚拟存储技术结合使用的内存管理方案必须具有如下特性：

- 一是使用动态内存地址，内存中的进程要是可以移动的；
- 二是不能要求全部程序加载入内存，进程才能运行的。

31.管理空闲内存方法

通常用于管理空闲物理内存的方法有：空闲块链表法、位示图法、空闲页面表。

32.程序局部性

- 程序局部性原理是指程序在执行时呈现出局部性规律，即在一段时间内，整个程序的执行仅限于程序中的某一部分。相应地，执行所访问的存储空间也局限于某个内存区域。
- 空间局部性是指一旦程序访问了某个存储单元，其附近的存储单元也将被访问，程序代码执行具有顺序性。
- 时间局部性是指如果程序中的某条指令一旦执行，则不久之后该指令可能再次被执行；如果某数据被访问，则不久之后该数据可能再次被访问，也就是说程序中存在大量的循环。

33.移动技术

移动技术可以集中分散的空闲区，提高内存的利用率，便于作业动态的扩充内存。采用移动技术要注意以下问题：

①移动技术会增加系统的开销；

②移动是有条件的。

在采用移动技术时应该尽可能减少需要移动的作业数和信息量。

在内存中可以将进程从低地址区域移到高地址区域，可以将进程从高地址区域移到低地址区域。

34.链接

链接是指把所有编译后得到的目标模块连接装配起来，再与函数库相连接成一个整体的过程。

35.页式存储管理

- 页式存储管理将内存空间划分成等长的若干区域，每个区域的大小一般取 2 的整数幂，称为页框。
- 系统将程序的逻辑空间按照同样大小也划分成若干页面，称为逻辑页面也称为页，大小与页框相同。
- 虚拟页面在物理空间上不要求连续存放。

第六章 文件管理

1.文件的定义

- 文件可以被解释为一组带标识的、在逻辑上有完整意义的信息项的序列。
- 这个标识为文件名，信息项构成了文件内容的基本单位。
- 信息项是构成文件内容的基本单位，这些信息项是一组有序序列，它们之间具有一定的顺序关系；
- 文件提供了一种将数据保存在外部存储介质上以便于访问的功能。为了方便用户使用，每个文件都有特定的名称。
- 文件名称的长度因系统而异。
- 有的文件系统不区分文件名的大小写，而有的则加以区分。
- 有的操作系统对不同的后缀有特定的解释，而有的则没有统一的规定。
- 一般地，文件建立在存储器空间里，以便使文件能够长期保存。即：文件一旦建立，就一直存在，直到该文件被删除或该文件超过事先规定的保存期限。

2.文件的分类

1) 按文件的用途分类

① 系统文件
② 库函数文件
③ 用户文件

2) 按文件的组织形式分类

① 普通文件
② 目录文件
③ 特殊文件

3) 一些常见的文件分类方式

- 按文件的保护方式可划分为：只读文件、读写文件、可执行文件、无保护文件等。
- 按信息的流向分类可划分为：输入文件、输出文件和输入输出文件等。
- 按文件的存放时限可划分为：临时文件、永久文件和档案文件等。临时文件，即记有临时性信息的文件;永久性文件，即其信息需要长期保存的文件；档案文件，即保存在作为“档案”用的磁带或光盘等永久性介质上以备查证和恢复时使用的文件。
- 按文件所使用的介质类型分类可划分为：磁盘文件、磁带文件、卡片文件和打印文件等。
- 还可以按文件的组织结构分类。比如，由用户组织的文件称逻辑文件，逻辑文件可采用流式文件和记录式文件两种组织方式。而文件在存储介质上的组织方式是文件的物理结构(物理文件)，常用的组织方式有顺序文件、链接文件和索引文件等。

4) UNIX 类操作系统中文件的分类

- 在 UNIX 类操作系统中，文件系统包括 3 种类型的文件：

① 普通文件。这是内部无结构的一串平滑的字符所组成的文件。
② 目录文件。这是由文件目录项所构成的文件。
③ 特殊文件。在 UNIX 类操作系统中，把 I/O 设备也看成是一种文件——特殊文件。

- 文件系统分类的目的是:对不同文件进行管理，提高系统效率；同时，提高文件系统的用户界面友好性。

3.文件逻辑结构分类

可以把文件划分成 3 类逻辑结构:无结构的字符流式文件、定长记录文件和不定长记录文件构成的记录树，定长记录文件和不定长记录文件可以统称为记录式文件。

1) 流式文件

- 流式文件是有序字符的集合，其长度为该文件所包含的字符个数，所以又称为字符流文件。
- 在流式文件中，构成文件的基本单位是字符。
- 可以认为流式文件就是一串有开头和结尾的连续字符；
- 流式文件无结构。所以用户对流式文件可以方便地进行操作。
- 源程序、目标代码等文件属于流式文件。UNIX 类系统采用的是流式文件结构。

2) 记录式文件

- 记录式文件是一组有序记录的集合。在记录式文件中，构成文件的基本单位是记录。
- 记录是一个具有特定意义的信息单位，它由该记录在文件中的逻辑地址（相对位置）与记录名所对应的一组键、属性及其属性值所组成，可按键进行查找。
- 记录式文件可分为定长记录文件和不定长记录文件两种。

● 在定长记录文件中，各个记录长度相等。在检索时，可以根据记录号 i 及记录长度 L 就可以确定该记录的逻辑地址。

● 在不定长记录文件中，各个记录的长度不等，在查找时，必须从第一个记录起一个记录一个记录查找，直到找到所需的记录。

● 记录式的有结构文件可把文件中的记录按各种不同的方式排列，构成不同的逻辑结构，以便用户对文件中的记录进行修改、追加、查找和管理等操作。

4.文件物理结构分类

常用的文件物理结构有顺序结构、链接结构、索引结构和 I 节点结构。

1） 顺序结构（连续分配）

● 顺序结构又称连续结构，它把逻辑上连续的文件信息依次存放在连续编号的物理块中。这是一种逻辑记录顺序核物理记录顺序完全一致的文件。

● 在顺序结构中，一个文件的目录项中只要指出该文件占据的总块数和起始块号即可。

● 优点：

① 由于从文件的逻辑块号到物理块号的变换，知道了文件在文件存储设备上的起始块号和文件长度，就能很快进行存取。

② 且顺序结构支持顺序存取和随机存取。

● 对于顺序存取，顺序结构的存取速度快。

● 缺点：

① 文件不能动态增长。对于顺序结构的文件，不利于文件插入和删除。

② 随着文件不停地被分配和被删除，空闲空间逐渐被分割为很小的部分，最终导致出现存储碎片，虽然空间满足，但由于不连续且都是小碎片而无法分配。

2） 链接结构（不连续分配）

● 链接结构的实质就是为每个文件构造所使用磁盘块的链表。

● 使用这种链接结构的文件，将逻辑上连续的文件分散存放在若干不连续的物理块中。

● Windows 的 FAT 文件系统采用的是链接结构，但将所有链指针集中存放。

● 优点：

① 解决存储碎片问题，有利于文件动态扩充；

② 有利于文件插入和删除，提高了磁盘空间利用率。

③ 方便链接结构的文件动态扩充。

● 缺点：存取速度慢，不适于随机存取文件；

① 磁盘的磁头移动多，效率相对较低；

② 存在文件的可靠性问题，比如指针出错，文件也就出错了；

③ 链接指针需要占用一定的空间。

● 链接结构的文件所使用的物理块是不连续分配的，所以一个链接结构的文件的所有物理块在磁盘上是分散分布的。

● 与顺序结构的文件相比，在访问一个链接结构的文件时需要更多的寻道次数和寻道时间。

3） 索引结构

● 索引结构的文件把每个物理盘块的指针字集中存放在被称为索引表的数据结构中的内存索引表中。

● 优点：

① 索引文件结构保持了链接结构的优点，又解决了其缺点。

② 索引结构文件既适于顺序存取，也适于随机存取。

③ 可以将有关逻辑块号和物理块号的信息全部保存在了一个集中的索引表中。

④ 索引文件可以满足文件动态增长的要求，也满足了文件插入、删除的要求；

⑤ 索引文件还能充分利用外存空间。

● 缺点：

① 会引起较多的寻道次数和寻道时间；

② 索引表本身增加了存储空间的开销。

4） 索引结构的实例——I 节点

● I 节点是一种多级索引文件结构。

● I 节点最早出现在 UNIX 操作系统中，是多级索引结构文件在 UNIX 中的具体实现。

● 掌握了 I 节点也就掌握了多级索引文件结构的工作原理。

- I 节点的基本思想是，给每个文件赋予一张称为 I 节点的小表，在这张小表中列出了文件属性和文件中各块在磁盘上的地址
- I 节点的文件结构，既适合小文件使用，也可供大型文件使用，灵活性比较强。这种文件结构占用的系统空间比一般多级索引结构的文件要少。

5.外存储设备

- 外存储设备通常由驱动部分和存储介质两部分组成。
- 外存储设备存取的过程方式因各种具体存储设备而异，不过也有一定共性。
- 外存储设备存取的过程大致如下：读状态-置数据-置地址-置控制-再读状态。

6.磁盘计算

- 在随机存取设备中，磁盘是一种典型的随机存取设备。
- 磁盘设备允许文件系统直接存取磁盘上的任意物理块。
- 磁盘一般由若干磁盘片组成，每个磁盘片对应两个读/写磁头，分别对磁盘片的上下两面进行读写。
- 磁盘上每个物理块的位置可用柱面号（磁道号）、磁头号和扇区号表示，这些地址与物理块号一一对应。其计算公式如下：

① 已知物理块号，则磁盘地址：

柱面号=[物理块号/(磁头数 ×扇区数）]

磁头号=[(物理块号 mod(磁头数× 扇区数))/扇区数]

扇区号=(物理块号 mod(磁头数× 扇区数）)mod 扇区数

② 已知磁盘地址：

物理块号=柱面号 ×(磁头数 × 扇区数)+磁头号 × 扇区数+扇区号

- 磁头臂是沿半径方向移动的。
- 访问磁盘时，首先要移动磁头臂到相应柱面（磁道）上，然后旋转盘片将指定磁头定位在指定扇区上，最后控制磁头对扇区中的数据进行读写。
- 一次访盘时间由寻道时间、旋转定位时间和数据传输时间组成；
- 寻道时间由于是机械动作，因而所花费的时间最长，传输时间花费时间最短。

7.文件存取方式

- 在用户面前，文件呈现的是文件的逻辑结构，这与用户使用文件的方式相适应；
- 在存储介质面前，文件呈现的是文件的物理结构，这与文件所使用存储介质的特性有关；
- 文件的存取方式是文件的逻辑结构和物理结构之间的映射或变换机制；
- 文件常用的存取方法有:顺序存取和随机存取两种方式。

① 顺序存取：按从前到后的次序依次访问文件的各个信息项。

② 随机存取：又称直接存取，即允许用户按任意的次序直接存取文件中的任意一个记录，或者根据存取命令把读写指针移到文件中的指定记录处读写。

- UNIX 类操作系统的文件系统采用了顺序存取和随机存取两种方法。

8.文件目录

- 在一个计算机系统中保存有许多文件，用户在创建和使用文件时只给出文件的名字，由文件系统根据文件名找到指定文件。
- 为了便于对文件进行管理，设置了文件目录，用于检索系统中的所有文件。
- 文件系统的一个特点是“按名存取”，即用户只要给出文件的符号名就能方便地存取在外存空间的该文件的信息，而不必了解和处理文件的具体物理地址。

9.文件目录块（FCB）

- 文件控制块 FCB 是系统为管理文件而设置的一个描述性数据结构。FCB 是文件存在的标志，它记录了系统管理文件所需要的全部信息。
- FCB 通常应包括以下内容：文件名、文件号、用户名、文件地址、文件长度、文件类型、文件属性、共享计数、文件的建立日期、保存期限、最后修改日期、最后访问日期、口令、文件逻辑结构、文件物理结构，等等，
- 其中文件名、文件大小、文件创建时间和磁盘起始地址是文件控制块中必须保存的信息。
- 在文件控制块中的信息可以分成文件存取控制信息、文件结构信息和文件管理信息。

10.目录文件

- 多个文件的文件控制块集中在一起组成了文件的目录。
- 通常，文件目录以文件的形式保存起来，这个文件就被称为目录文件。目录文件是长度固定的记录式文件。
- 在目录文件中，每个文件的文件控制块又称为目录文件中的目录项。

● 有时，为了节省内存的空间，就把目录文件保存在外存储器上，在需要时才把目录文件调入内存。

11.目录结构

1） 一级目录结构

● 在系统中设置一张线性目录表，表中包括了所有文件的文件控制块，每个文件控制块指向一个普通文件，这就是一级目录结构；

● 一级目录结构是一种最简单、最原始的文件目录结构。

● 有了一级目录，文件系统就可实现对文件空间的管理和按名存取。

● 一级目录表中各文件只能按连续结构或顺序结构存放，因此，文件名与文件必须一一对应，限制了用户对文件的命名，不能重名。

● 优点：简单，容易实现。

● 缺点：搜索效率较低，文件平均检索时间长。

2） 二级目录结构

● 为克服一级目录结构中文件目录命名中的可能冲突，并提高对目录文件的检索速度，一级目录被改进扩充成二级目录。

● 在二级目录结构中，目录被分为两级：

① 第一级称为主文件目录（Main File Directory，MFD),给出了用户名和用户子目录所在的物理位置；

② 第二级称为用户文件目录（User File Directory，UFD)，又称用户子目录，给出了该用户所有文件的 FCB。

● 优点：解决了文件的重名问题，可以实现用户间的文件共享，查找时间也降低了。

● 缺点：增加了系统的开销。

3） 树形目录

● 把二级目录的层次关系加以推广，就形成了多级目录，又称树形目录结构。

● 在树形目录结构中，最高层为根目录，最低层为文件。

● 根目录是唯一的，由它开始可以查找到所有其他目录文件和普通文件。根目录一般可放在内存。从根结点出发到任一个非叶结点或叶结点（文件）都有且仅有一条路径，该路径上的全部分支组成了一个全路径名。

● 树形目录结构的优点是便于文件分类，且具有下列特点：

① 层次清楚。

② 解决了文件重名问题。

③ 查找搜索速度快。

12.全路径名&相对路径

有两种根据路径名检索的方法，一种是全路径名，另一种是相对路径。

● 全路径名

① 使用全路径名检索的方法，需要从根目录开始，列出由根到用户指定文件的全部有关子目录，全路径名又称为“绝对路径名”。

② 缺点：不方便，影响访问速度，耗费时间。

● 相对路径

① 用于检索的路径名只是从当前目录开始到所要访问文件的一段路径，即以当前目录作为路径的相对参照点。

② 优点：检索路径缩短，检索速度提高。

13.目录项分解法

● 为加快目录检索可采用目录项分解法，即把目录项（FCB)分为符号目录项（次部）和基本目录项（主部）两部分。

● 符号目录项包含文件名以及相应的文件号；

● 基本目录项包含了除文件名外文件控制块的其他全部信息；

● 例子：

假设一个文件控制块有 48 字节，符号目录项占 8 字节，其中文件名占 6 字节，文件号占 2 字节；基本目录项占 48-8=40 字节。设物理块的大小为 512 字节。

在进行目录项分解前，一个物理块可以存放 512/48≈10 个文件控制块。在进行目录项分解后，一个物理块可以存放 512/8=64 个符号目录项，或者 512/40≈12 个基本目录项。

如果一个目录文件有 128 个目录项，那么分解前 128×48/512=12，即需要 12 个物理块存放该目录文件。

在进行目录项分解后，符号目录文件占 128×8/512=2，即需要 2 个物理块存放符号文件。基本目录项占 128×40/512=10，即需要 10 个物理块存放基本目录文件。

下面，计算查找一个文件的平均访盘次数。

分解前：(1+12)/2=6.5 次。

分解后：(1+2)/2+1=2.5 次。

- 目录项分解法的优点：减少了访问磁盘的次数，提高了文件目录检索速度。

14.存储空间分配与回收

在设计空闲空间登记表的数据结构时，一般有四种不同的方案可以考虑，下面分别介绍。

1）位示图

- 位示图法的基本思想是，利用一串二进制位（bit)的值来反映磁盘空间的分配使用情况。
- 在位示图中，每一个磁盘中物理块用一个二进制位对应，如果某个物理块为空闲，则相应的二进制位为 0;如果该物理块已分配了，则相应的二进制位为 1;
- 在申请磁盘物理块时，可在位示图中从头查找为 0 的位，如果发现了为 0 的位，则将其改为 1，同时返回该二进制位对应的物理块号。
- 在归还不再使用的物理块时，则在位示图中将该物理块所对应的二进制位改为 0，表示这块物理块恢复为空闲状态。
- 优点：

① 对空间分配情况的描述能力强。一个二进制位就描述一个物理块的状态；

② 位示图占用空间较小，因此可以复制到内存，使查找既方便又快速；

③ 适用于各种文件物理结构的文件系统。

2）空闲块表

- 空闲块表是专门为空闲块建立的一张表，该表记录外存储器中全部空闲的物理块，包括每个空闲块的第一个空闲物理块号和该空闲块中空闲物理块的个数；
- 空闲块表方式特别适合于文件物理结构为顺序结构的文件系统。

3）空闲块链表

- 将外存储器中所有的空闲物理块连成一个链表，用一个空闲块首指针指向第一个空闲块，随后的每个空闲块中都含有指向下一个空闲块的指针，最后一块的指针为空，表示链尾，这样就构成了一个空闲块链表；
- 在空闲块链表模式中对空间的申请和释放是以块为单位的。申请空间时从链首取空闲块，空间释放时将物理块接入链尾。
- 空闲块链表法节省内存，但申请空间和回收空间的速度较慢，实现效率较低。

4）成组链接

对链接表的一个改进方案是将 n 个空闲盘块的地址存放在第一个空闲块中，其余 n-1 个空闲盘块是实际空闲的。

假设每 100 个空闲块为一组。第一组的 100 个空闲块块号放在第二组的头一块中，而第二组的其余 99 块是完全空闲的。第二组的 100 个块号又放在第 3 组的头一块中。依此类推，组与组之间形成链接关系。在最后一组的块号中第 2 个单元填“0”，表示该块中指出的块号是最后一组的块号，空闲块链到此结束。在这个空闲块链中，不足 100 块的那个组的块号通常放在内存的一个专用块中。这种方式称为成组链接。

15.回收和分配算法

1） 分配一个空闲块

查 L 单元内容（空闲块数）:

当空闲块数>1，i:=L+空闲块数;

从 i 单元得到一空闲块号;

把该块分配给申请者;

空闲块数减 1。

当空闲块数=1，取出 L+1 单元内容（一组的第一块块号或 0);

取值=0，无空闲块，申请者等待;

取值≠0，把该块内容复制到专用块;

该块分配给申请者;

把专用块内容读到主存 L 开始的区域。

2） 归还一块

查 L 单元的空闲块数；

当空闲块数<100，空闲块数加 1；

j：=L+空闲块数；

归还块号填入 j 单元。

当空闲块数=100，把主存中登记的信息写入归还块中；

把归还块号填入 L+1 单元；

将 L 单元置成 1。

16.记录的成组

● 把若干个逻辑记录合成一组存放在一个物理块的工作称为“记录的成组”，每块中的逻辑记录个数称为“块因子”。

● 由于信息交换以块为单位，所以要进行成组操作时必须使用内存的缓冲区，该缓冲区的长度等于要进行成组的最大逻辑记录长度乘以成组的块因子。

17.建立文件

● 用户首先调用文件系统的“建立文件”操作，在请求调用该操作时提供所要创建的文件的文件名及若干参数:用户名、文件名、存取方式、存储设备类型、记录格式、记录长度，等等。

● 建立文件系统调用的一般格式为：create(文件名，访问权限，(最大长度))。

● 建立文件的具体步骤如下：

① 检查参数的合法性：

文件名是否符合命名规则，若是，则进行下一步②；否则报错，返回。

② 检查同一目录下有无重名文件：

若没有，则进行下一步③;否则报错，返回。

③ 在目录中有无空闲位置：

若有，则进行下一步④;否则，不成功返回。

有的系统可能要为此文件申请数据块空间（申请一部分或一次性全部申请）。

④ 填写目录项内容：

包括:文件名、用户名、存取权限、长度置零、首地址等。

⑤ 返回。

18.打开文件

● 打开文件，是使用文件的第一步，任何一个文件使用前都要先打开，即把文件控制块 FCB 送到内存。

● 打开文件系统调用的一般格式为:fd=open(文件路径名，打开方式)。

● 打开文件时，系统主要完成以下工作：

① 根据文件路径名查目录，找到 FCB 主部。

② 根据打开方式、共享说明和用户身份检查访问合法性。

③ 根据文件号查系统打开文件表，看文件是否已被打开。

如果是，共享计数加 1;否则，将外存中的 FCB 主部等信息填入系统打开文件表空表项，共享计数置为 1。

④ 在用户打开文件表中取一空表项，填写打开方式等，并指向系统打开文件表对应表项。返回信息：文件描述符 fd，这是一个非负整数，用于以后读写文件。

19.读文件

● 打开文件后，就可以读取文件中的信息。

● 读文件系统调用的一般格式为：read(文件名，(文件内位置)，要读的长度，内存目的地址)。

● 隐含参数：文件主。

● 读写方式可为读、写和既读又写等。

● 读文件时，系统主要完成以下工作：

① 检查长度是否为正整数：

若是，则进行下一步②;否则，转向⑩。

② 根据文件名查找目录，确定该文件在目录中的位置。

③ 根据隐含参数中的文件主和目录中该文件的存储权限数据，检查是否有权读。

若是，则进行下一步④;否则，转向⑩。

④ 由文件内位置与要读的长度计算最末位置，将其与目录中的文件长度比较，超过否？若是，则转向⑩；否则，进行下一步⑤。也可将参数中的长度修正为目录中的文件长度。

⑤ 根据参数中的位置、长度和目录中的映射信息，确定物理块号、需要读出的块数等读盘参数（参数准备完毕后，进行物理的读盘操作，读盘操作可能要进行多次）。

⑥ 根据下一块号读块至内存缓冲区。

⑦ 取出要读的内容，也许要进行成组的分解，将取出的内容送至参数中的内存目的地址。

⑧ 根据块内长度或起始块号+块数，确定还读下一块吗？同时确定下一块块号：

若是，则转向⑤;否则，进行下一步⑨。

⑨ 正常返回。

⑩ 错误返回，返回相应错误号。

20.写文件

- 写文件系统调用的一般格式为：write(文件名，记录键，内存位置)。
- 把内存中指定单元的数据作为指定的一个记录写入指定文件中，系统还将为其分配物理块，以便把记录信息写到外存上。

21.关闭文件

- 文件关闭后一般不能存取，若要存取，则必须再次打开。
- 关闭文件系统调用的一般格式为：close(文件名)。
- 系统根据用户提供的文件名或文件描述符，在该文件的文件控制块上做修改。

22.删除文件

- 删除文件系统调用的一般格式为：delete(文件名)。
- 系统根据用户提供的文件名或文件描述符，检查此次删除的合法性，若合法，则收回该文件所占用的文件控制块及物理块等资源。

23.指针定位

- 指针定位的一般格式为：seek(fd，新指针的位置)。
- 指针定位时，系统主要完成以下工作：

① 由 fd 检查用户打开文件表，找到对应的入口；

② 将用户打开文件表中文件读写指针位置设为新指针的位置，供后续读写命令存取该指针处文件内容。

24.文件的保护

文件系统经常采用建立副本和定时转储的方法来保护文件。

1） 建立副本

- 对文件建立副本，是保护文件不受破坏的有效方法。
- 一般用于短小且极为重要的文件。

2） 定时转储

- 定时转储的含义是，每隔一定的时间就把文件转储到其他的存储介质上。
- UNIX 系统就是采用定时转储的方法保护文件，以提高文件的可靠性。
- 按照转储内容可分为增量转储和全量转储。增量转储是指备份自上一次转储以来更改过的文件。
- 按照转储方式可分为物理转储和逻辑转储。

① 物理转储是从磁盘的第 0 块开始，将全部磁盘块按序输出到另一介质上，直到最后一块复制完毕。

② 而逻辑转储是从一个或几个指定的目录开始，递归地转储其自给定日期（例如，最近一次增量转储或全量转储的日期）后有所更改的全部文件和目录。

3） 规定文件的存取权限

规定用户使用文件的权限的方法有两种：

- 采用树形目录结构。

凡能得到某级目录的用户就可得到该级目录所属的全部目录和文件，按目录中规定的存取权限使用目录或文件。

- 存取控制表。

列出每个用户对每个文件或子目录的存取权限。

25.存取控制矩阵

- 在存取控制矩阵方式中，系统以一个二维矩阵来实施文件的存取控制。
- 在这个二维矩阵中，其中一维代表所有的用户，另一维代表所有的文件。
- 两维交叉点所对应的矩阵元素则是某一个用户对一个文件的存取控制权限，包括读 R、写 W 和执行 E，当然，还可以有其他的划分形式。

26.二级存取控制

- 对文件实施存取控制的另一种方法是二级存取控制。
- 二级存取控制方法中设立两个存取级别。

① 在第一级，把用户按某种关系划分为若干用户组，进行对访问者的识别；

② 在第二级，进行对操作权限的识别。

- 常用的文件保密措施还有隐蔽文件目录、设置口令与使用密码等。

27.UNIX 系统内部数值

- 读（Read)操作（R)；
- 写（Write)操作（W)；
- 执行（eXecute)操作（X)；
- 不能执行任何操作（--)。
- UNIX 系统内部使用数值来表示上述的文件属性每一个属性与文件属性中的一个二进制位相对应。如果该存取权限设置了，对应的二进制位就是 1，如果该存取权限没有设置，对应的二进制位是 0。
- 例：a.out 的权限属性 rwxr--xr--x 用二进制来表示就是 111101101。在 UNIX 中常使用八进制的形式表示，于是 a.out 的这个权限是 755。

28.提高文件系统性能的方法

常见的技术措施有如下几种：块高速缓存、磁盘空间的合理分配和对磁盘调度算法进行优化。

1） 块高速缓存

其基本思想是，系统在内存中保存一些磁盘块，这些磁盘块在逻辑上属于磁盘，内存的这一区域被称为块高速缓存。

块高速缓存的内容需要定期写回到磁盘上，以保存对磁盘块的修改。

2） 合理分配磁盘空间

在磁盘空间中分配块时，应该把有可能顺序存取的块放在一起，最好在同一柱面上。

这样可以有效地减少磁盘臂的移动次数，加快了文件的读写速度，从而提高了文件系统的性能。

3） 磁盘的驱动调度

磁盘是一种高速旋转的存储设备。磁头沿着盘片直径方向移动，同时对指定磁道上的扇面中的数据进行读写操作。当多个访盘请求在等待时，系统采用一定的策略，对这些请求的服务顺序进行调整安排，使寻道时间和延迟时间都尽可能小的那个访问请求可以优先得到服务，并降低若干个访问者的总访问时间，增加磁盘单位时间内的操作次数。其目的在于降低平均磁盘服务时间，从而实现公平、高效的访盘请求。

29.磁盘调度算法

1） 磁盘的存取访问时间

磁盘的存取访问时间由 3 部分组成：

- 寻道时间，即将磁头移动到相应的磁道或柱面所需的时间；
- 旋转延迟时间，即一旦磁头到达指定磁道，必须等待所需要的扇区旋转到读\头下的时间；
- 传输时间，即信息在磁盘和内存之间的实际传送时间。
- 一次磁盘服务的总时间就是以上 3 个时间之和。要使磁盘服务尽可能地快，就需要操作系统提供合适的磁盘调度算法，以改善磁盘服务的平均时间。

2） 设计磁盘调度算法应当考虑两个基本因素：

- 公平性：一个磁盘访问请求应当在有限时间内得到满足。
- 高效性：减少设备机械运动所带来的时间开销，增加磁盘缓存。

3） 磁盘驱动调度

磁盘驱动调度由“移臂调度”和“旋转调度”两部分组成。

- 移臂调度

根据访问者指定的柱面位置来决定执行次序的调度，称为“移臂调度”。移臂调度的目的是尽可能地减少操作中的寻找时间。

- 一般可采用以下几种移臂调度算法：先来先服务调度算法（FCFS)、最短寻道时间优先调度算法（SSTF)、 扫描算法（SCAN)、循环扫描算法（C-SCAN)。

30.先来先服务调度算法（FCFS)

- 即按照访问请求的次序为各个进程服务，这是最公平而又最简单的算法，但是效率不高。
- 因为磁头引臂的移动速度很慢，如果按照访问请求发出的次序依次读写各个磁盘块，则磁头引臂将可能频繁大幅度移动，容易产生机械振动，亦造成较大的时间开销，影响效率。

31.最短寻道时间优先调度算法（SSTF）

- SSTF 算法以寻道优化为出发点，优先为距离磁头当前所在位置最近磁道（柱面）的访问请求服务。
- 这种算法改善了平均服务时间，但也存在缺点：假设某一段时间外磁道请求不断，则可能有内磁道请求长时间得不到服务，缺乏公平性。

32.扫描算法（SCAN）

- 这种算法因其基本思想与电梯的工作原理相似，故又称电梯算法。
- SCAN 算法也是一种寻道优化的算法，它克服了 SSTF 算法的缺点。
- SSTF 算法只考虑访问磁道与磁头当前位置的距离，而未考虑磁臂的移动方向，而 SCAN 算法则既考虑距离，也考虑方向，且以方向优先。
- 这种算法比较公平，而且效率较高。

33.文件分配表（FAT）

- FAT 是一个简单的文件系统，最初为 DOS 操作系统设计，适用于小容量的磁盘，具有简单的目录结构。
- 为了向后兼容，也为了方便用户升级，目前新版本的 Wmdows 仍然提供对 FAT 的支持。
- FAT 文件系统总共有 3 个版本：FAT-12、FAT-16 和 FAT-32，取决于用多少二进制位表示磁盘地址。
- FAT 文件系统以簇为单位进行分配，所以 FAT-16 文件系统表示用 16 位（2 字节）表示簇号。

34.文件系统执行 close（）

执行“关闭”操作时，文件系统主要完成如下工作：

① 将活动文件表中该文件的“当前使用用户数”减 1；若此值为 0，则撤销此表目，并保存文件控制块写入磁盘或者缓存；

② 若活动文件表目内容已被改过，则表目信息应复制到文件存储器上相应表目中，以使文件目录保持最新状态；

③ 卷定位工作，一个关闭后的文件不能再使用，若要再使用，则必须再次执行“打开”操作。

第七章 I/O 设备管理

1.设备管理

- 设备管理是操作系统的主要功能之一，它负责管理所有输入输出设备以完成期望的数据传设备管理；
- 由于计算机系统中存在着大量的输入/输出设备，其性能和应用特点可能完全不同。所以要建立一个通用的、一致的设备访问接口，使用户和应用程序开发入员能够方便地使用输入/输出设备。

2.设备管理的主要任务

- 设备管理的主要任务有：缓冲区管理、设备分配、设备处理、虚拟设备以及实现设备独立性。
- 操作系统主要通过缓冲技术、中断技术和虚拟技术来解决 I/O设备系统的性能；
- 操作系统需要在设备管理和系统的其他部分之间提供简单而易于使用的接口；
- 对于设备拥有者而言，多用户多任务环境中的设备使用应该通过协调避免冲突，设备不能被破坏。

3.设备的分类

1）按设备的使用特性分类

按设备的使用特性分类，可以分为 I/O 设备和存储设备。

- I/O 设备：

① 是计算机与外部世界交换信息的设备。

② 输入设备是计算机用来接受指令和数据等信息的设备（键盘、鼠标等）；

③ 输出设备是计算机用来传送处理结果的设备（显示器、打印机等）；

④ 在计算机数据采集和过程控制等应用中，各种传感器、传动器、模拟/数字转换器、数字/模拟转换器等也属于 I/O 设备；

⑤ 调制解调器、网络适配器（网络接口卡）等数据通信设备也属于 I/O 设备，这类设备用于构建计算机网络通信系统。

- 存储设备：

① 是计算机用来存放信息的设备，例如磁带、磁盘、光盘、U 盘等各种外存设备。

② 其中，可移动的磁带或磁盘在用于不同机器间传送数据时也可看作是 I/O 设备。

2）按设备的信息组织方式来划分

按信息组织方式来划分设备，可以把 I/O 设备划分为字符设备（character device)和块设备(block device)。

- 字符设备

① 键盘、终端、打印机等以字符为单位组织和处理信息的设备；

② 字符设备通常以字符为单位发送或者接收字符流，而不存在任何块结构。

③ 字符设备不可寻址，所以没有任何寻址操作。除磁盘以外的大多数设备，例如网络接口卡、打印机、鼠标等可看作字符设备。

- 块设备

① 磁盘、磁带等以数据块为单位组织和处理信息的设备

② 基本特性：能够随时读写其中的任何一块而与所有别的块无关。

③ 外存类设备通常是块设备，因其记录长度通常为一个数据块，例如磁盘的扇区或者由若干扇区组成的簇。

3）按设备的共享属性分类

按设备的共享属性可以将设备分为共享设备、独占设备和虚拟设备。

- 共享设备

共享设备是指在一段时间内允许多个进程使用的设备。磁盘是典型的共享设备。

- 独占设备

独占设备也称为独享设备，是指在一段时间内只允许一个进程使用的设备。独占设备的使用效率低是造成死锁的条件之一。

- 虚拟设备

虚拟设备是指利用虚拟技术把独占设备改造成可由多个进程共享的设备。SPOOLing 系统是一种非常重要的虚拟设备技术。

4.I/O 设备的控制方式

有程序直接控制方式、中断控制方式、DMA 方式和通道控制方式。

5.程序直接控制方式（PIO(Programmed I/O，程控 I/O)方式）

- 指由用户进程直接控制内存或 CPU 和外围设备之间进行信息传送的方式，
- 也称为“忙-等”方式、轮询方式或循环测试方式，控制者是用户进程。

- 过程

① 用户进程从外围设备输入数据时，通过 CPU 发出启动设备准备数据的启动命令(通常是把一个启动位为 1 的控制字通过数据总线写入设备的控制寄存器中)。

② 用户进程进入测试等待状态。在等待时间，CPU 不断地用一条测试指令检查设备的状态寄存器是否为完成状态（通常是检测状态寄存器的完成位是否为1)，而外围设备只有将输入数据送入数据缓冲寄存器之后，才将该寄存器置为完成状态。

③ 当 CPU 检测到设备的状态寄存器为完成状态，则从设备的数据缓冲寄存器读取数据到内存或 CPU。

④ 反之，当用户进程需要向输出设备输出数据时，也必须同样发出启动命令和等待设备准备好之后才能输出数据。

- 优点：CPU 和外设的操作能通过状态信息得到同步，而且硬件结构比较简单；
- 缺点：CPU 效率较低，传输完全在 CPU 控制下完成，对外部出现的异常事件无实时响应能力。

所以，程序直接控制方式只适用于那些 CPU 执行速度较慢，而且外围设备较少的系统，如单片机系统。

6.程序直接控制的关键部件

I/O 设备数据传送控制方式中，实现程序直接控制方式需要的关键部件包括设备状态寄存器、地址总线和数据总线、设备控制寄存器、设备数据缓冲区和地址译码器。

7.中断控制方式

- 中断是在发生了一个异常事件时，调用相应处理程序（通常称为中断服务程序）进行服务的过程。
- 中断服务程序与中断时 CPU 正在执行的进程是相互独立的，相互不传递数据。
- 优点：

① CPU与外设在大部分时间内并行工作，有效地提高了计算机的效率。

② 具有实时响应能力，可适用于实时控制场合。

③ 及时处理异常情况，提高计算机的可靠性。

8.中断控制方式的处理过程

- CPU 通过数据总线发出命令，启动外设工作，当前进程阻塞，调度程序调度其他进程；
- 外设数据准备好，置位中断请求触发器；
- 若此时接口中断屏蔽触发器状态为非屏蔽状态，则接口向 CPU 发出中断请求（IR)；
- CPU 接受中断请求（设备控制器的功能)，且中断为允许中断状态，则中断判优电路工作；
- 中断判优电路对优先级最高的中断请求给予响应（INTA)，CPU 中断正在执行的其他进程，转而执行中断服务程序。所以需要的关键部件是：中断控制器、地址总线和数据总线、设备控制器。

9.DMA（直接内存访问)方 式

- 目的：

① 减少 I/O 数据交换消耗的处理时间；

② 提升高速的外围设备以及成组交换数据的速度。

- DMA 方式的数据块传送过程可分为 3 个阶段:传送前预处理、数据传送、传送后处理。

① 预处理阶段——由 CPU 执行 I/O 指令对 DMAC 进行初始化与启动。

② 数据传送阶段——由 DMAC 控制总线进行数据传输。当外设数据准备好后发 DMA 请求，CPU 当前机器周期结束后响应 DMA 请求，DMAC 从 CPU 接管总线的控制权，完成对内存寻址，决定数据传送的内存单元地址，对数据传送字进行计数，执行数据传送的操作。

③ 后处理阶段——传送结束，DMAC 向 CPU 发中断请求，报告 DMA 操作结束。CPU 响应中断，转入中断服务程序，完成 DMA 结束处理工作，包括校验数据，决定是否结束传送等。

- DMA 方式一般用于高速传送成组的数据。
- 优点：

① 操作均由硬件电路实现，传输速度快；

② CPU 仅在初始化和结束时参与，对数据传送基本上不干预，可以减少大批量数据传输时 CPU 的开销；

③ CPU 与外设并行工作，效率高。

- 局限性：

① DMA 方式在初始化和结束时仍由 CPU 控制；

② 在大型计算机系统中，为了进一步减轻 CPU 的负担和提高计算机系统的并行工作程度，除了设置 DMA 器件之外，还设置了专门的硬件装置——通道。

10.DMA 控制的关键部件

实现 DMA控制方式需要的关键部件包括:DMA控制器、地址总线和数据总线。

11.通道控制方式

● 通道（channel）是一个特殊功能的处理器，它有自己的指令和程序，可以实现对外围设备的统一管理和外围设备与内存之间的数据传送。

● 引入通道的目的：是为了进一步减少数据输入输出对整个系统运行效率的影响。

● 按照信息交换方式分类

① 选择通道

是一种高速通道，在物理上它可以连接多个设备，但是这些设备不能同时工作；

选择通道主要用于连接高速外围设备，如磁盘、磁带等，信息以成组方式高速传输；

优点：以数据块为单位进行传输，传输率高；

缺点：通道利用率低。

② 数组多路通道

当某个设备进行数据传送时，通道只为该设备服务；

当设备在执行寻址等控制性动作时，通道暂时断开与这个设备的连接，挂起该设备通道程序，为其他设备服务；

优点：数据块为单位进行传输，传输率高；又具有多路并行操作的能力，通道利用率高。

缺点：控制复杂。

③ 字节多路通道

是一种简单的共享通道，在分时的基础上为多台低速和中速设备服务。

特点:各设备与通道之间的数据传送是以字节为单位交替进行的，各设备轮流占用一个短的时间片；多路并行操作能力与数组多路通道相同。

12.通道的功能

● 接受 CPU 的指令，按指令要求与指定的外围设备进行通信。

● 从内存读取属于该通道的指令，并执行通道程序，向设备控制器和设备发送各种命令。

● 组织外围设备和内存之间进行数据传送，并根据需要提供数据缓存的空间，以及提供数据存入内存的地址和传送的数据量。

● 从外围设备得到设备的状态信息，形成并保存通道本身的状态信息，根据要求将这些状态信息送到内存的指定单元，供 CPU 使用。

● 将外围设备的中断请求和通道本身的中断请求，按序及时报告 CPU。

13.I/O 系统硬件结构

● 计算机 I/O 系统硬件结构主要包含 3 部分：适配器和接口部件、设备控制器、设备硬件。

14.I/O 软件分层

一般可以分为四层：中断处理程序，设备驱动程序，与设备无关的操作系统软件，用户级软件（指用户空间的 I/O 软件）。

15.与设备无关 I/O 软件功能

① 设备驱动程序的统一接口

② 设备命名：在操作系统的 I/O 软件中，对 I/O 设备采用了与文件统一命名的方法，即采用文件系统路径名的方法来命名设备。

③ 设备保护：对设备进行必要的保护，防止无授权的应用或用户的非法使用，是设备保护的主要作用。

④ 提供一个与设备无关的逻辑块

⑤ 缓冲：对于常见的块设备和字符设备，一般都使用缓冲区。

⑥ 存储设备的块分配：在创建一个文件并向其中填入数据时，通常在硬盘中要为该文件分配新的存储块。

⑦ 独占设备的分配和释放

⑧ 错误处理

一般而言，所有设备都需要的 I/O 功能可以在与设备独立的软件中实现。这类软件面向应用层并提供一个统一的接口。

16.典型的 I/O 技术

● 在 I/O 设备管理中，为了提高设备和 CPU 的效率，引入了各种技术。

● 经常使用技术有：缓冲技术、设备分配技术、SPOOLing 技术、DMA 与通道技术。

17.缓冲技术

● 为了解决中央处理机和外部设备的速度不匹配和负荷不均衡问题，为了提高各种设备的工作效率，增加系统中各部分的并行工作速度

● 缓冲技术是计算机系统中常用的技术。一般，数据到达速度和离去速度不匹配的地方都可以通过设置缓冲区，以缓解处理机与设备之间速度不匹配的矛盾，并减少对 CPU 的 I/O 中断次数从而提高资源利用率和系统效率。

18.设备分配技术

1） 设备分配算法的数据结构

● 在设备分配算法的实现中，常采用的数据结构主要含四张表。

① 系统设备表 SDT(System Device Table)：登录了该设备的名称、标识及设备控制表 DCT 的入口地址等相关的信息。

② 设备控制表 DCT(Device Control Table)：在 DCT 中充分体现出了设备的各方面特征，以及与该设备相连的设备控制器的情况，并保存了控制器块的入口位置。

③ 控制器控制表 COCT(Controller Control Table)：用于登录某控制器的使用分配情况及与该控制器相连的通道的情况。

④ 通道控制表 CHCT(Channel Control Table)：反映了通道的情况，系统中的每个通道都有一张 CHCT。

2） 设备分配的原则

● 设备分配的总原则：一方面要充分发挥设备的使用效率，同时又要避免不合理的分配方式造成死锁、系统工作紊乱等现象，使用户在逻辑层面上能够合理方便地使用设备。

● 考虑设备的特性和安全性

设备的特性是设备本身固有的属性，一般分为独占、共享和虚拟设备等；

● 从安全性方面考虑：

① 安全分配方式：安全，效率比较低，CPU 与 I/O 设备串行工作、

② 不安全分配方式两种：提高了运行效率，但存在造成死锁的可能，因此设备分配程序中应该增加预测死锁的安全性计算，在一定程度上增加了程序的复杂性。

● 设备分配策略

与进程的调度相似，设备的分配也需要一定的策略，通常采用先来先服务（FIFO)和高优先级优先等策略。

① 先来先服务策略：当多个进程同时对一个设备提出 I/O 请求时，系统按照进程提出请求的先后次序，把它们排成一个设备请求队列，并且总是把设备首先分配给排在队首的进程使用。

② 高优先级优先策略：给每个进程提出的 I/O 请求分配一个优先级，在设备请求队列中把优先级高的排在前面，如果优先级相同则按照 FIFO 的顺序排列。

3） 独占设备的分配

独占设备每次只能分配给一个进程使用，这种使用特性隐含着死锁的必要条件，所以在考虑独占设备的分配时，一定要结合有关防止和避免死锁的安全算法。

4） 共享设备的分配

① 共享设备是可由若干个进程同时共享的设备，例如磁盘。

② 通常，共享型设备的 I/O 请求来自文件系统、虚拟存储系统或输入输出管理程序，其具体设备已经确定，因而设备分配比较简单，即当设备空闲时分配，占用时等待。

19.虚拟设备

● 系统中独占设备有限，不能满足多个进程，因而引起大量进程由于等待某些独占设备而阻塞，造成系统“瓶颈”。

● 申请到独占设备的进程运行期间利用率低，设备常处于空闲状态。

● 从而引入虚拟设备技术。

● 实现这一技术的软、硬件系统被称为 SPOOLing(Simultaneous Peripheral Operation On Line,外围设备同时联机操作）系统。

20.SPOOLing 技术

● SPOOLing 技术是一种同时的外围设备联机操作技术，通常称为“假脱机技术”。

● SPOOLing 系统的 3 大组成部分：输入井和输出井、输入缓冲和输出缓冲、输入进程 SPi 和输出进程 SPo。

21.提高 I/O 性能的技术

● 通过应用缓冲技术，解决传输速度差异的问题。

● 通过应用异步 I/O 技术，使 CPU 不必等待 I/O 的操作结果。

● 通过应用 DMA 和通道部件，使 CPU 与这些部件能并行执行。

● 通过应用虚拟设备技术，减少进程阻塞时间，提高独占设备的利用率。

22.设备表作用

● 为了实现设备的独立性，系统必须设置一张逻辑设备表，用于将应用程序中所用的逻辑设备名映射为物理

设备名。

- 在该表每个表目中有 3 项：逻辑设备名、物理设备名和设备驱动程序入口地址。
- 系统设备表 SDT，在 SDT 中每个接入系统中的设备都有一个表目项。登录了设备的名称，标识设备控制表 DCT 的入口地址等相关信息。
- 全面反映了系统中的外设资源的情况，逻辑设备与物理设备之间对应关系等。

23.设备独立层

设立设备独立层的主要目的是用于实现用户程序与设备驱动器的统一接口、设备命令、设备保护、以及设备分配与释放等，同时为设备管理和数据传送提供必要的存储空间。

24.“准备就绪”信号

- 在程序控制 I/O 方式中，输出设备的主要作用是通过输出设备输出数据；
- 若输出设备向处理机返回“准备就绪”信号，则表示输出缓冲区已空或者可以向输出缓冲区写数据，CPU 可以向输出设备再次提供输出的数据。

25.外部设备命令传递

当用户使用外部设备时，其控制设备的命令传递途径依次为：

用户应用层→设备独立层→设备驱动层→设备硬件。

26.高速缓存

- 高速缓存不是缓冲，在计算机存储系统的层次结构中，介于中央处理器和主存储器之间的高速小容量存储器。
- 它和主存储器一起构成一级的存储器。
- 高速缓冲存储器和主存储器之间信息的调度和传送是由硬件自动进行的。

27.键盘的 I/O 控制

- 键盘的工作原理是由键盘控制器专门来完成的，当键盘控制器收到数据后通过中断控制器 IRQ1 引脚向 CPU 发送中断请求。
- 当 CPU 响应中断后就会调用键盘中断处理程序来读取控制器中的键盘扫描码。因此键盘的 I/O 控制是通过中断方式来实现的。

第八章 死锁

1.死锁、饥饿和活锁

- 死锁是指在多道程序中，一组进程中的每个进程均无期限的等待被该组进程中的另一个进程所占有且永远不会释放的资源。
- 饥饿是指一个可运行的进程尽管能继续执行，但被调度器无限期地忽视，而不能被调度执行的情况。饥饿可以通过先来先服务资源分配策略来避免。
- 活锁指的是任务或者执行者没有被阻塞，由于某些条件没有满足，导致一直重复尝试，失败，尝试，失败。
- 活锁和死锁的区别在于活锁的实体是在不断的改变状态，活锁有可能自行解开，死锁则不能。

2.死锁产生的原因

产生死锁的原因主要有两个：

- 一是竞争资源，系统提供的资源数量有限，不能满足每个进程的需求；
- 二是多道程序运行时，进程推进顺序不合理。

3.产生死锁的四个条件

1） 互斥条件

资源是独占的且排他使用。进程互斥使用资源，即任一时刻一个资源只能给一个进程使用，其他进程若请求一个资源而该资源被另一进程占有时，则申请者等待，直到资源被占用者释放。

2） 不可剥夺条件

又称不可抢占或不可强占。进程所获得的资源在未使用完毕之前，不能被其他进程强行剥夺，而只能由获得该资源的进程自愿释放。

3） 请求和保持条件

又称部分分配或占有申请。进程每次申请它所需要的一部分资源，在申请新的资源的同时，继续占用已分配到的资源。

4） 循环等待条件

又称环路等待。在发生死锁时，必然存在一个进程等待队列 $\{P_1, P_2, \cdots, P_n\}$，其中$P_1$等待 P_2 占有的资源，P_2 等待 P_3 占有的资源，…，P_n等待P_1占有的资源，形成一个进程等待环路。环路中每一个进程已占有的资源同时被另一个进程所申请，即前一个进程占有后一个进程所请求的资源。

4.死锁检测

- 操作系统可定时运行一个“死锁检测”程序，该程序按一定的算法去检测系统中是否存在死锁。
- 检测死锁的实质是确定是否存在“循环等待”条件，检测算法确定死锁的存在并识别出与死锁有关的进程和资源，以供系统采取适当的解除死锁措施。

5.死锁预防

- 在设计系统时确定资源分配算法，限制进程对资源的申请，从而保证不发生死锁。
- 具体的做法是破坏产生死锁的四个必要条件之一：

① 破坏“互斥条件”：可以通过采用假脱机（SPOOLing）技术，允许若干个进程同时输出；

② 破坏“不可剥夺”条件：如果资源没有被等待进程占有，那么该进程必须等待，在其等待过程中，其资源也有可能被剥夺；

③ 破坏“请求和保持”条件：可以采用静态分配资源策略，将满足进程条件的资源一次性分配给进程，也可以采用动态资源分配，即需要资源时才提出申请，系统在进行分配；

④ 破坏“循环等待”条件：进程申请资源时，必须严格按照资源编号的顺序进行，否则系统不予分配。

6.死锁避免

- 死锁避免的基本思想是：系统对进程发出的每一个系统能够满足的资源申请进行动态检查，并根据检查结果决定是否分配资源；如果分配后系统可能发生死锁，则不予分配，否则予以分配。
- 这是一种保证系统不进入死锁状态的动态策略。

7.安全与不安全状态

如果操作系统能保证所有的进程在有限时间内得到所需的全部资源，则称系统处于“安全状态”，否则说系统是不安全的。

- 安全状态是指：如果存在一个由系统中所有进程构成的安全序列{P1，…，Pn}，则系统处于安全状态。一个进程序列{P1，…，Pn}是安全的，如果对于其中每一个进程 Pi（$1 \leqslant i \leqslant n$），它以后尚需要的资源量不超过系统当前剩余资源量与所有进程 pj（$j<i$）当前占有资源量之和。系统处于安全状态则不会发生死锁。
- 如果不存在任何一个安全序列，则系统处于不安全状态。不安全状态一定导致死锁，但不安全状态不一定是死锁状态。即系统若处于不安全状态则可能发生死锁。

8.银行家算法

- 银行家算法是一种最有代表性的避免死锁的算法，又被称为“资源分配拒绝”法。
- 安全序列计算过程：

① 分别求出各进程所需最大资源数量(a)、已分配资源数(b)、缺少资源数(c)和资源剩余可分配量(d)；

② 拿 c 和 d 进行比较:

d>c:满足分配，此时 d1=d-c;

否则不满足，寻找下个可满足的进程;

③ 进程分配运行后释放该进程资源,则 d2=d1+a=d+b;

④ 按此步骤继续计算寻找可分配进程，直至完成所有进程分配。

9.死锁解除法

死锁解除法可归纳为两大类：

- 剥夺资源：使用挂起/激活机制挂起一些进程，剥夺它们占有的资源给死锁进程，以解除死锁。经常使用的方法有还原算法和建立检查点。
- 撤销进程：撤销死锁进程，将它们占有的资源分配给另一些死锁进程，直到死锁解除为止。撤销代价的标准有进程优先数、进程类的外部代价和运行代价，即重新启动进程并运行到当前撤销点所需要的代价。

10.资源分配图化简方法

1） 在资源分配图中，找出一个既非等待又非孤立的进程结点 P_i，由于 P_i 可获得它所需要的全部资源，且运行完后释放它所占有的全部资源，故可在资源分配图中消去所有的申请边和分配边，使之成为既无申请边又无分配边的孤立结点。

2） 将 P_i 所释放的资源分配给申请它们的进程，即在资源分配图中将这些进程对资源的申请边改为分配边。

3） 重复 1)、2）两步骤，直到找不到符合条件的进程结点。

- 经过化简后，若能消去资源分配图中的所有边，使所有进程都成为孤立结点，则该图是可完全化简的；否则为不可化简的。
- 所有的化简顺序将导致相同的不可化简图。可以证明，系统处于死锁状态的充分条件是，当且仅当该系统的资源分配图是不可完全化简的。

11.独占设备预防死锁

- 对于系统中的独占设备，为预防出现死锁，一般需要避免动态分配锁。也就说，锁应该采用静态分配。
- 死锁预防的一种措施，就是定时重试和定时放弃锁。
- 为了避免多个进程同时获取锁，因此锁的分配必须是采用加锁的互斥方式。
- 死锁预防，在系统设计时确定资源分配算法，保证不发生死锁。
- 具体的做法是破坏产生死锁的 4 个必要条件之一，其中破坏“循环等待”条件主要是通过“资源有序分配法”来解决死锁。

计算机网络

第一章 网络技术基础

1.ARPANET

- ARPANET 为美国国防高等研究计划署开发的世界上第一个运营的封包交换网络，它是全球互联网的始祖。
- ARPANET 是计算机网络技术发展中的一个里程碑，它的研究对促进网络技术发展和理论体系的形成起到了重要的推动作用，并为 Internet 的形成奠定了坚实的基础。

2.无线自组网（Ad hoc）

- 无线自组网（Ad hoc）是在无线分组网的基础上发展起来的；
- 是一种特殊的无线、自组织、对等、多跳、移动的网络；
- 它采用一种不需要基站的“对等结构”移动通信网络；
- 它在军事和特殊应用领域有着重要的应用前景。

3.Windows NT 操作系统

- Windows NT 3.1 操作系统是微软公司开发的一种闭源系统，采用 32 位的操作系统，可以提供全面的网络服务功能。
- Windows NT 4.0 是在 Windows NT 3.5 基础上改进的版本，由于采用客户机/服务器的工作模式，Windows NT 操作系统可以分为两部分：Windows NT Server 与 Windows NT Workstation。

4.Microsoft Windows 操作系统

- Microsoft Windows是微软公司制作和研发的一套桌面操作系统；
- Windows采用了图形化模式 GUI，比起之前的DOS需要键入指令使用的方式更为人性化；
- Windows 是闭源系统，并不向用户开放源代码。

5.Unix 操作系统

- Unix 是一种典型的操作系统，主要用于服务器端；
- 1969年，AT&T公司的Kennethl.Thompson用汇编语言编写了 Unix的第一个版本V1，目的是为开发新软件的程序员提供一个工具。
- Unix 作为工业标准已经被很多计算机厂商接受，并广泛应用于大型机、中型机、小型机、工作站与微型机上，特别是工作站中几乎全部采用 Unix 系统。
- TCP/IP 作为 Unix 的核心部分，使 Unix 与 TCP/IP 共同得到了普及与发展。
- Unix 是针对小型机环境开发的操作系统，采用的是集中式、分时、多用户的系统结构。
- 1993 年，Unix 国际和开放系统基金会（OSF)合作，成立了公共开放软件环境（COSE)组织，为 Unix 的标准化打下基础。

6.Linux 操作系统

- Linux 是一套免费使用和自由传播的类 Unix 操作系统。
- Linux 继承了 Unix 以网络为核心的设计思想，是一个性能稳定的多用户网络操作系统，可以作为服务器使用。
- Linux 是基于 GNU 开源的操作系统。
- Linux 的核心部分是其内核，提供 KDE 用户界面。
- 常见的 Linux 发行版主要包括 RedHat、Mandrake、Slackware、SUSE、TurboLinux、Debian、Caldera、Ubuntu，以及国内的蓝点、红旗 Linux 等。

7.计算机网络特征

- 建立计算机网络的主要目的是实现计算机资源的共享。
- 互联的计算机是分布在不同地理位置的多台独立的“自治计算机”。互联的计算机之间没有明确的主从关系，每台计算机都可以联网或脱网工作。
- 联网计算机之间的通信必须遵循共同的网络协议。

8.计算机网络分类

- 按覆盖的地理范围划分，可以分为以下 4类：广域网、城域网、局域网与个人区域网。
- 按照覆盖距离从大到小排列：

① 广域网（Wide Area Network,WAN)：覆盖100～1000km的网络。

② 城域网（Metropolitan Area Network，MAN)：覆盖10～100km的网络；

③ 局域网（Local Area Network，LAN)：覆盖 10m~10km的网络；

④ 个人区域网（Personal Area Network,PAN）：连接用户计算机身边 10m之内计算机、打印机、PDA与智能手机等数字终端设备的网络。

9.无线传感器网（WSN）

- 由部署在监测区域内大量的廉价微型传感器结点组成，通过无线通信方式形成的一个多跳的自组织的网络系统。
- WSN 是一种分布式传感网络，它的末梢是可以感知和检查外部世界的传感器。
- WSN 中的传感器通过无线方式通信，因此网络设置灵活，设备位置可以随时更改，还可以跟互联网进行有线或无线方式的连接。通过无线通信方式形成的一个多跳自组织的网络。
- 无线传感器网使用的无线通信技术主要包括 IEEE802.11 标准的 WLAN、IEEE 802.15.4 标准的无线个人区域网（6LoWPAN）技术、蓝牙（Bluetooth）技术、ZigBee 技术。

10.网络拓扑结构

- 拓扑学是将实体抽象成与其大小、形状无关的“点”，将连接实体的线路抽象成“线”，进而研究“点”“线”“面”之间的关系。
- 计算机网络拓扑是通过网中节点与通信线路之间的几何关系表示网络结构，反映网络中各实体之间的结构关系。
- 计算机网络拓扑是指通信子网的拓扑结构。

11.网络拓扑分类

基本的网络拓扑有五种：星形、环形、总线形、树形与网状。

- **星形拓扑**

星形拓扑结构的主要特点是：

① 节点通过点-点通信线路与中心节点连接。

② 中心节点控制全网的通信，任何两节点之间的通信都要通过中心节点。

③ 星形拓扑结构简单，易于实现，便于管理。

④ 网络的中心节点是全网性能与可靠性的瓶颈，中心节点的故障可能造成全网瘫痪。

- **环形拓扑**

环形拓扑结构的主要特点是：

① 节点通过点-点通信线路连接成闭合环路。

② 环中数据将沿一个方向逐站传送。

③ 环形拓扑结构简单，传输延时确定。

④ 环中每个节点与连接节点之间的通信线路都会成为网络可靠性的瓶颈。环中任何一个节点出现线路故障，都可能造成网络瘫痪。

⑤ 为了方便节点的加入和撤出，控制节点数据传输顺序，保证环的正常工作，需要设计复杂的环维护协议。

- **总线形拓扑**

总线形拓扑结构的主要特点是：

① 所有节点连接到一条作为公共传输介质的总线，以广播方式发送和接收数据。

② 当一个节点利用总线发送数据时，其他节点只能接收数据。

③ 如果有两个或两个以上的节点同时发送数据时，就会出现冲突，造成传输失败。

④ 总线形拓扑结构的优点是结构简单，缺点是必须解决多节点访问总线的介质访问控制问题。

- **树形拓扑**

树形拓扑结构的主要特点是：

① 节点按层次进行连接，信息交换主要在上、下节点之间进行，相邻及同层节点之间通常不进行数据交换，或数据交换量比较小。

② 树形拓扑可以看成是星形拓扑的一种扩展，树形拓扑网络适用于汇集信息。

- **网状拓扑**

网状拓扑结构的主要特点是：

① 节点之间的连接是任意的，没有规律，故又被称为无规则型。

② 网状拓扑的优点是系统可靠性高，广域网一般都采用网状拓扑。

网状拓扑结构复杂，必须采用路由选择算法、流量控制与拥塞控制方法。

12.数据传输速率

- 数据传输速率是每秒钟传输构成数据的二进制比特数；
- 单位为比特/秒（bit/second）记作 bps。
- 对于二进制数据，数据传输速率为：

$$S=1/T\ (bps)$$

其中，T 为发送 1 比特所需的时间。

1B=8b

1kbps=1*10^3bps

1Mbps≈1*10^3Kbps

1Gbps≈1*10^3Mbps

1Tbps≈1*10^3Gbps

● 奈奎斯特准则指出：如果间隔为π/ω（ω=2πf），通过理想通信信道传输窄脉冲信号，则前后码元之间不会产生相互窜扰。因此，对于二进制数据信号的最大数据传输速率 Rmax与通信信道带宽B（B=f，单位Hz）的关系可以写为：

$$R_{max}=2*f\ (bps)$$

对于二进制数据，如果信道带宽 S=f=3000Hz，则最大数据传输速率为 6000bps。

13.误码率

误码率是指二进制码元在数据传输系统中被传错的概率，它在数值上近似等于：

$$P_e=N_e/N$$

其中 A 为传输的二进制码元总数，I 为被传错的码元数。

● 误码率是衡量数据传输系统在正常工作状态下的传输可靠性的参数。

● 对于实际的数据传输系统，需要根据实际情况提出误码率要求。在数据传输速率确定后，误码率越低，传输系统设备越复杂、造价越高。

● 对于实际的数据传输系统，如果传输的不是二进制码元，需要折合成二进制码元来计算。

14.数据报（DG）与虚电路（VC）

● 分组交换技术可以分为两类：数据报（Datagram，DG）与虚电路（VirtualCircuit，VC）。

● 数据报方式主要有以下几个特点：

① 同一报文的不同分组可以经过不同的传输路径通过通信子网。

② 同一报文的不同分组到达目的主机时可能出现乱序、重复与丢失现象。

③ 每个分组在传输过程中都必须带有目的地址与源地址。

④ 数据报方式的传输延迟较大，适用于突发性通信，不适用于长报文、会话式通信。

⑤ 数据报是报文分组存储转发的一种形式，在数据报方式中，分组传输前不需要在源主机与目的主机之间预先建立“线路连接”。

● 虚电路方式主要有以下几个特点：

① 在每次传输分组之前，在源主机与目的主机之间建立一条虚电路。

② 所有分组都通过虚电路顺序传输，分组中不必携带目的地址、源地址等信息。分组到达目的主机时不会出现乱序、重复与丢失现象。

③ 分组通过虚电路上的每个路由器时，路由器只需要进行差错检测，而不需要进行路由选择。

④ 路由器可以与多个主机之间通信建立多条虚电路。

15.网络协议的概念

● 计算机网络是由多个主机组成，主机之间需要不断地交换数据。

● 为了在主机之间有条不紊地交换数据，每个主机都必须遵守一些事先约定好的规则。这些规则精确地规定交换数据的格式和时序。

● 这些为网络数据交换而制定的规则、约定与标准被称为网络协议（Protocol）。

16.网络协议组成 3 要素

① 语法：即用户数据与控制信息的结构和格式，以及数据出现的顺序。

② 语义：即解释控制信息每个部分的意义，它规定了需要发送何种控制信息，以及完成的动作与所作的响应。

③ 时序：即对事件发生顺序的详细说明。

17.网络体系结构

● 为了保证网络中大量计算机之间有条不紊地交换数据，入们必须制定大量的协议，构成一套完整的协议体系。

● 对于结构复杂的网络协议体系来说，最好的组织方式是层次结构模型。

● 计算机网络中引入了一个重要的概念——网络体系结构。

● 网络体系结构采用层次结构的方法具有以下优点：

① 各层之间相互独立。

② 灵活性好。

③ 易于实现和标准化。

18.OSI 各层的主要功能

- 1974 年，ISO(国际标准化组织,主要从事网络协议标准化工作)发布著名的 ISO/IEC 7498 标准，它定义了网络互联的七层框架，即开放系统互联（Open System Internetwork，OSI）参考模型
- OSI 参考模型结构包括以下 7 层：物理层、数据链路层、网络层、传输层、会话层、表承层和应用层。

1） 物理层（Physical Layer）

① 物理层是 OSI 参考模型的最底层。

② 物理层利用传输介质为通信的网络主机之间建立、管理和释放物理连接，实现比特流的透明传输，为数据链路层提供数据传输服务。

③ 物理层的数据传输单元是比特。

2） 数据链路层（DataLinkLayer）

① 数据链路层的低层是物理层，相邻高层是网络层。

② 数据链路层在物理层提供比特流传输的基础上，通过建立数据链路连接，采用差错控制与流量控制方法，使有差错的物理线路变成无差错的数据链路.

③ 数据链路层的数据传输单位是帧。

3） 网络层（Network Layer）

① 网络层相邻的底层是数据链路层，高层是传输层

② 网络层通过路由选择算法为分组通过通信子网选择最适当的传输路径，实现流量控制、拥塞控制与网络互联的功能。

③ 网络层的数据传输单元是分组（Packet）

4） 传输层（Transport Layer）

① 传输层相邻的低层是网络层，高层是会话层。

② 传输层为分布在不同地理位置的计算机的进程通信提供可靠的端-端（end-to-end)连接与数据传输服务。

③ 传输层向高层屏蔽了低层数据通信的细节。

④ 传输层的数据传输单元是报文（Message)。

5） 会话层（Session Layer）

① 会话层相邻的低层是传输层，高层是表示层。

② 会话层负责维护两个会话主机之间连接的建立，管理和终止，以及数据的交换。

6） 表示层（Presentation Layer）

① 表示层相邻的低层是会话层，高层是应用层。

② 表示层负责通信系统之间的数据格式变换、数据加密与解密、数据压缩与恢复。

7） 应用层（Application Layer）

① 应用层是参考模型的最高层。

② 应用层实现协同工作的应用程序之间的通信过程控制。

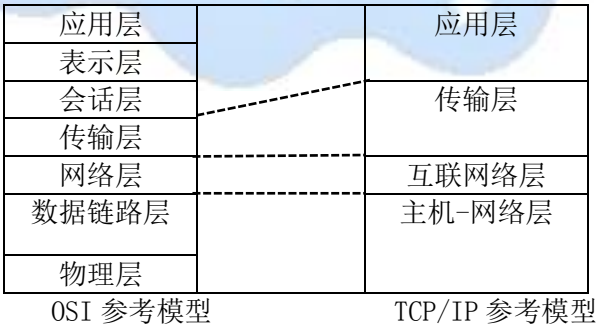
19.TCP/IP 协议

- TCP/IP 协议参考模型是由美国国防部指定使用的协议。
- TCP/IP 协议具有独立于特定的网络硬件，可以运行在局域网、广域网。

20.TCP/IP 应用层与 OSI 对应关系

从功能的角度来看：

- TCP/IP 参考模型的应用层与 OSI 参考模型的应用层、表示层、会话层对应；
- TCP/IP 参考模型的传输层与 OSI 参考模型的传输层对应；
- TCP/IP 参考模型的互联网络层与 OSI 参考模型的网络层对应；
- TCP/IP 参考模型的主机-网络层与 OSI 参考模型的数据链路层和物理层对应。



OSI 参考模型 TCP/IP 参考模型

21.TCP/IP 各层的主要功能

TCP/IP 参考模型从高到低可以分为 4 个层次：应用层（Application Layer)、传输层（Transport Layer)、互

联网络层与主机-网络层。

1） 主机-网络层（Host-to-network Layer）

主机-网络层是 TCP/IP 参考模型的最底层，它负责通过网络发送和接收 IP 分组。

2） 互联网络层（Internet Layer）

- TCP/IP 参考模型互联网络层的协议是 IP 协议。
- IP 协议是一种不可靠、无连接的数据报传送服务协议，它提供的是一种“尽力而为（best-effort）”的服务。(ICMP 也在网络层)
- 互联网络层的协议数据单元是 IP 分组。
- 互联网络层的主要功能包括如下：

① 处理来自传输层的数据发送请求。
② 处理接收的分组。
③ 处理网络的路由选择、流量控制与拥塞控制。

3） 传输层

- 传输层是负责在会话进程之间建立和维护端-端连接，实现网络环境中分布式进程通信
- 传输层定义两种不同的协议：

① 传输控制协议（Transport Control Protocol，TCP）

TCP 是一种可靠的、面向连接、面向字节流（Byte Stream）的传输层协议。TCP协议提供比较完善的流量控制与拥塞控制功能。

② 用户数据报协议（User Datagram Protocol，UDP）。

UDP 是一种不可靠的、无连接的传输层协议。

4） 应用层

- 应用层是 TCP/IP 参考模型中的最高层。
- TCP/IP 应用层主要有如下的基本协议。

① 远程登录协议（Telnet）。
② 文件传输协议（File Transfer Protocol，FTP）。
③ 简单邮件传输协议（Simple Mail Transfer Protocol，SMTP）。
④ 超文本传输协议（Hyper Text Transfer Protocol，HTTP）。
⑤ 域名服务（Domain Name System，DNS）。
⑥ 简单网络管理协议（Simple Network Management Protocol，SNMP）。
⑦ 动态主机配置协议（Dynamic Host Configuration Protocol,DHCP）。

22.计算机网络形成发展 4 个阶段

① 第一阶段是计算机网络技术与理论准备阶段；
② 第二阶段是计算机网络的形成阶段；
③ 第三阶段是网络体系结构的研究阶段；
④ 第四阶段是 Internet 应用、无线网与网络安全技术研究的发展阶段。

23.总线型局域网的特点

- 所有结点都通过网卡连接到作为公共传输介质的总线上。
- 总线通常采用双绞线或同轴电缆作为传输介质。
- 所有结点可以通过总线发送或接收数据，但是一段时间内只允许一个结点通过总线发送数据。结点之间按广播方式通信，一个结点发出的信息，总线上的其他结点均可“收听”到。
- 由于总线作为公共传输介质为多个结点所共享，就可能出现同一时刻有两个或两个以上结点通过总线发送数据的情况，因此会出现冲突而造成传输失败。
- 在总线型局域网的实现技术中，必须解决多个结点访问总线的介质访问控制问题。

第二章 局域网基础

- 早期的局域网主要是令牌环网。
- 20世纪80年代，局域网领域出现 Ethernet与Token Bus、Token Ring三足鼎立的局面，并且各自都形成了相应的国际标准。
- 21 世纪，Ethernet 已成为局域网领域的主流技术。
- 介质访问控制（MAC）是所有“共享介质”类型的局域网都必须解决的共性问题。早期 Ethernet是用一条作为总线的同轴电缆连接多台计算机，对应的物理层协议是 10BASE-2与10BASE-5。

1.局域网

- 局域网设计目标是覆盖一个公司、一所大学、一幢办公楼的有限地理范围，它的基本通信机制与广域网是完全不同的。
- 局域网拓扑结构主要分为总线形、环形与星形结构;传输介质主要采用双绞线、同轴电缆、光纤与无线介质。
- 目前应用最广泛的局域网类型是 Ethernet,它已成为局域网领域占统治地位的技术。传统以太网是共享介质类型的局域网,其核心是随机争用共享介质的访问控制方法,即带有冲突检测的载波侦听多路访问 CSMA/CD 方法。

2.局域网的 3 种类型

1) 采用带有冲突检测的载波侦听多路访问(Carrier Sense Multiple Access/Collision Detection，CSMA/CD)访问控制方法的总线形 Ethernet，简称为“以太网”。

2) 采用令牌控制的令牌总线形（Token Bus）局域网，简称为“Token Bus”或“令牌总线网“。

3) 采用令牌控制的令牌环形（Token Ring）局域网，简称为“Token Ring”或“令牌环网”

- 3 种局域网的共同之处：

① 体系结构都遵循：IEEE 802 层次结构模型。
② 传输介质主要采用同轴电缆、双绞线与光纤。
③ 采用共享介质的方式发送和接收数据帧。
④ 介质访问控制都采用分布式控制方法，局域网中没有集中控制的主机。

- 3 种局域网的不同之处

从物理结构的角度来看，Ethernet 与 Token Bus 是针对总线形的局域网设计，而 Token Ring 是针对环形拓扑的局域网设计。

3.CSMA/CD 与 Token Bus、Token Ring 的比较

- CSMA/CD 方法的主要特点

① CSMA/CD 介质访问控制方法算法简单，易于实现。
② CSMA/CD 是一种随机访问控制方法，适用于对传输实时性要求不高的办公环境。
③ CSMA/CD 在网络通信负荷较低时表现出较好的吞吐率与延迟特性。但是，当网络通信负荷增大时，由于冲突增多，网络吞吐率下降、传输延迟增加。

●Token Bus、Token Ring 的主要特点：

① Token Bus 与 Token Ring 中主机适用于对数据传输实时性要求较高的应用环境，如生产过程控制领域。
② Token Bus 与 Token Ring 在网络通信负荷较重时，表现出很好的吞吐率与较低的传输延迟，因此适用于通信负荷较重的应用环境。
③ Token Bus 与 Token Ring 环的维护过程复杂，实现起来困难。

4.高速 Ethernet

- 传统的局域网技术建立在共享介质的基础上，网中的所有主机共享一条共用的通信传输介质。
- 介质访问控制方法用来保证每个主机都能“公平”地使用传输介质。

5.IEEE 802 协议标准

- IEEE 802 协议标准的分类（3 类）

① IEEE 802.1 标准：定义局域网体系结构、网络互联，以及网络管理与性能测试;
② IEEE 802.2 标准：定义逻辑链路控制 LLC 子层的功能与服务;
③ 定义不同介质访问控制技术的相关标准。

- 介质访问控制标准的发展

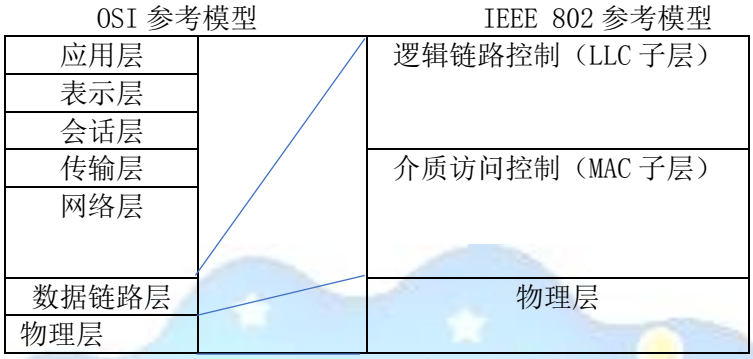
目前应用最多和正在发展的标准主要有 4 个，其中 3 个是无线局域网的标准。

- 4 个主要的介质访问控制协议标准如下：

① IEEE 802.3 标准：定义 CSMA/CD 总线介质访问控制子层与物理层的标准。
② IEEE 802.11 标准：定义无线局域网访问控制子层与物理层的标准。
③ IEEE 802.15 标准：定义近距离个人区域无线网络访问控制子层与物理层的标准。

④ IEEE 802.16 标准：定义宽带无线城域网访问控制子层与物理层的标准。

6. IEEE 802 参考模型与 OSI 参考模型



- IEEE 802 标准的设计者提出将数据链路层划分为两个子层：逻辑链路控制（Logical Link Control,LLC）子层与介质访问控制（Media Access Control，MAC）子层。
- 不同的局域网在 MAC 子层和物理层可以采用不同协议，而在 LLC 子层必须采用相同的协议。
- 不管局域网的介质访问控制方法与帧结构，以及采用的物理传输介质有什么不同，LLC 子层统一将它们封装到固定结构的 LLC 帧中。

7. CSMA/CD 的发送流程

为了有效地实现多个主机访问公共传输介质的控制策略，CSMA/CD 的发送流程可以简单概括为 4 步：先听后发，边听边发，冲突停止，延迟重发。、

8. Ethernet 帧结构

- Ethernet 帧结构一般包含前导码、帧前定界符、目的地址、源地址、类型/长度、数据(从低层来的数据或者从高层来的数据)、帧校验字段。
- 在 Ethernet 帧结构中，前导码由 64 位（8B）的 10101010…101010 比特序列组成。
- 帧前定界符是 8 位（1 字节）的 10101011。
- 目的地址与源地址均采用了 6 个字节 48 位，分别表示帧的接受结点与发送结点的硬件地址，硬件地址一般称为 MAC 地址、物理地址或 Ethernet 地址。
- 数据字段表示网络层使用的协议类型。数字字段的最小长度为 46B，最大长度 1500B。
- Ethernet 帧的最小长度是 64B，最大长度是 1518B。
- 其中前导码和帧前定界符是为了满足接收电路的要求，保证接收电路在目的地址字段到达之前进入稳定状态，二者在接收后不需要保留，也不计入帧头长度中。

9. 交换式以太网

- 交换式以太网的核心设备是以太网交换机，它可以在多个端口之间建立多个并发连接，实现多结点之间数据的并发传输，从而可以增加网络带宽，改善局域网的性能与服务质量，避免数据传输冲突的发生。

10. 交换机具有如下 4 个基本功能

① 建立和维护一个表示 MAC 地址与交换机端口号对应关系的映射表。
② 在发送主机与接收主机端口之间建立虚连接。
③ 完成帧的过滤与转发。
④ 执行生成树协议，防止出现环路。

11. 交换机的交换方式

交换机的交换方式主要有 3 种类型：直接交换、存储转发交换与改进直接交换。

1） 直接交换方式

① 在直接交换（CutThrough)方式中，交换机只要接收并检测到目的地址字段，立即将该帧转发出去，而不进行差错校验。帧出错检测任务由目的主机完成。
② 优点是:交换延迟时间短。
③ 缺点是:缺乏差错检测能力。

2） 存储转发交换方式

① 在存储转发交换方式中，交换机首先要完整地接收帧，并进行差错检测。
② 如果接收帧正确，则根据帧目的地址选择对应的输出端口号，然后转发出去。
③ 优点是:具有帧差错检测能力，并支持不同输入速率与输出速率端口之间的帧转发。
④ 缺点是:交换延迟时间将会增长。

3） 改进直接交换方式

① 改进的直接交换方式则将前两者结合起来，在接收到 Ethernet 帧的前 64 字节后，判断帧头字段是否正确，如果正确就转发出去。

② 对于短的 Ethernet 帧，交换延迟时间与直接交换方式比较接近;对于长的 Ethernet 帧，由于仅对帧的地址字段与控制字段进行差错检测，因此该方式的交换延迟时间将会减少。

12.交换机交换带宽计算

● 交换机交换带宽的计算方法是:

端口数 ×相应端口速率（全双工模式再乘以2)。

● 例如，一台交换机有 24 个 100Mbps 全双工端口和 2 个 1000Mbps 全双工端口，如果所有的端口都工作在全双工状态，那么交换机的交换带宽为：

S=24×2×100Mbps+2×2×1000Mbps=4800Mbps+4000Mbps=8800Mbps=8.8Gbps

13.虚拟局域网

● IEEE 公布关于 VLAN 的 IEEE802.1Q 标准。虚拟局域网（Virtual LAN，VLAN）是建立在局域网的基础上，以软件形式在局域网交换机上实现逻辑工作组的划分与管理，工作组中的结点不受物理位置的限制。

● 虚拟局域网的组网方法包括：

① 用交换机端口定义虚拟局域网；

② 用 MAC 地址定义虚拟局域网；

③ 用网络层地址定义虚拟局域网；

④ 基于广播组的虚拟局域网。

● 虚拟局域网的优点有：方便网络用户管理，减少网络管理开销、提供更好的安全性、改善网络服务质量。

14.快速以太网

● 快速以太网（Fast Ethernet）是一类新型的局域网，采用 IEEE 802.3u 标准；

● 数据传输速率可以达到 100Mbps，是标准以太网的数据传输速率的 10 倍。

● 具体包括两种技术：100BASE-T 和 100VG－AnyLAN。

● 快速以太网技术可以有效的保障用户在布线基础实施上的投资，它支持 3、4、5 类双绞线以及光纤的连接，能有效的利用现有的设施。

15.100ASE-T 的 3 种物理层标准。

● 100BASE-TX

① 100BASE-TX 使用两对 5 类非屏蔽双绞线 UTP 或 2 对 1 类屏蔽双绞线 STP。

② 1 对双绞线用于发送，而另一对双绞线用于接收。因此，100BASE-TX 是一个全双工系统，每个主机可以同时以 100Mbps 的速率发送与接收数据。

● 100BASE-T4

① 100BASE-T4 使用 4 对 3 类非屏蔽双绞线 UTP，其中 3 对用于数据传输，1 对用于冲突检测，只能用于半双工。

● 100BASE-FX

① 100BASE-FX 使用 2 芯的多模或单模光纤，是一种全双工系统。100BASE-FX 主要用作高速主干网，从主机到集线器的多模光纤的长度可以达到2km。

16.千兆以太网

● 千兆以太网又称为吉比特以太网。

● GE标准——IEEE 802.3z。

① GE 的传输速率达到了 1000Mbps,但仍保留传统 Ethernet 的帧格式与最小、最大帧长度等特征。

② IEEE 802.3z 标准定义了千兆介质专用接口（Gigabit Media Independent Interface,GMII），将 MAC 子层与物理层分隔开。物理层实现 1000Mbps 速率时使用的传输介质和信号编码方式的变化，不会影响 MAC 子层。

● 目前流行的 GE 物理层标准：

① 1000BASE-CX——使用两对屏蔽双绞线，双绞线最大长度为 25m。

② 1000BASE-T——使用 4 对 5 类非屏蔽双绞线，双绞线最大长度为 100m。

③ 1000BASE-SX——使用多模光纤，光纤最大长度为 550m。

④ 1000BASE-LX——使用单模光纤，光纤最大长度为 5km。

⑤ 1000BASE-LH——使用单模光纤，光纤最大长度为 10km。

⑥ 1000BASE-ZX——使用单模光纤，光纤最大长度为 70km。

17.局域网物理层（LAN PHY)标准

LANPHY 标准根据所使用的传输介质分为两类:光纤与双绞线。

● 基于光纤的物理层协议

10GBASE-SR——多模光纤，最大长度为 300m

10GBASE-LRM——多模光纤，最大长度为 220m。
10GBASE-LX4——单模光纤，最大长度为 10km。
10GBASE-LR——单模光纤，最大长度为 25km。
10GBASE-ER——单模光纤，最大长度为 40km。
10GBASE-ZR——单模光纤，最大长度为 80km。

- 基于双绞线的物理层协议

① 10GBASE-CX4:6 类 UTP 或 STP 双绞线，双绞线最大长度为 15m。
② 10GBASE-T：6 类 UTP 或 STP 双绞线，双绞线最大长度为 100m。

18.无线局域网技术

- 无线局域网技术以微波、激光与红外线灯无线电报作为传输介质，部分或全部代替传统局域网中的同轴电缆、双绞线与光纤，是对有线局域网的补充和扩展；
- 可以采用无基站的“对等结构”移动通信模式，如无线自组网（Ad hoc）。
- 无线局域网采用冲突避免的载波侦听多路访问（CSMA/CA）方法来解决介质访问控制问题。无线局域网采用的扩频技术有跳频扩频和直接序列扩频两种。
- 目前，无线局域网标准是 IEEE 802.11 系列标准。

19.无线局域网 4 个应用领域

1） 作为传统局域网的扩充。
2） 建筑物之间的互联。
3） 移动主机漫游访问。移动数据终端设备与无线局域网基站——接入点（Access Point，AP）设备之间可以实现漫游访问（Nomadic Access），也可以通过对等的 P2P 方式实现漫游。
4） 无线自组网。无线自组网络（Ad hoc)采用的是一种不需要基站的“对等结构”移动通信模式。Ad hoc 中所有联网设备可以在移动过程中动态组网。

20.扩频技术

- 无线局域网使用的是无线传输介质，按采用的传输技术可以分为 3 类：红外线局域网、扩频局域网和窄带微波局域网。
- 扩展频谱通信简称扩频通信，其特点是传输信息所用的带宽远大于信息本身带宽。
- 常用的扩频技术有跳频扩频和直接序列扩频。
- IEEE 802.11 规定跳频通信使用 2.4GHZ 的工业、科学与医药专用的 ISM 频段。
- 直接序列扩频的所有接收点使用相同的频段，发送端与接收端使用相同的伪随机码。

21.AAA 服务器

- AAA 是验证、授权和记账(Authentication、Authorization、Accounting)3 个英文单词的简称，是一个能够处理用户访问请求的服务器程序，提供验证授权以及帐户服务，主要目的是管理用户访问网络服务器，对具有访问权的用户提供服务。
- AAA 服务器通常同网络访问控制、网关服务器、数据库以及用户信息目录等协同工作。
- 同 AAA 服务器协作的网络连接服务器接口是 “远程身份验证拨入用户服务 (RADIUS)”。

22.IEEE 802.1X

- IEEE 802.11：

① 无线局域网（WLAN）的介质访问控制协议及物理层技术规范。
② IEEE 802.11 的 MAC 层协议定义了 14 种管理帧，例如信标帧、探测帧、关联帧、认证帧等，主要用于无线主机与 AP 之间建立关联。

- IEEE 802.12 ：需求优先的介质访问控制协议。
- IEEE 802.15：采用蓝牙技术的无线个人网技术规范。
- IEEE 802.16：宽带无线连接工作组，开发 2~66GHz 的无线接入系统空中接口。

23.无线接入技术

- 无线局域网（WLAN）接入：IEEE 802.11 标准；近距离。IEEE 802.11 标准重点在解决局域网范围的移动节

点通信问题。

表 1-4　　无线局域网 3 种版本标准的比较

版本名称	所定义的技术	数据传输速率
IEEE 802.11	定义了使用红外、跳频扩频与直接序列扩频技术	1Mbit/s 或 2Mbit/s
IEEE 802.11a		54Mbit/s
IEEE 802.11b	定义了使用直序扩频技术	1Mbit/s、2Mbit/s、5.5Mbit/s 与 11Mbit/s

- 无线城域网（WMAN）：IEEE 802.16 标准；远距离；采用 WiMAX 技术，可以在 50km 范围内提供最高 70Mbit/s 的传输速率。IEEE 802.16 标准的重点是解决建筑物之间的数据通信问题。

表 1-5　　IEEE 802.16 系列主要标准的基本情况及比较

协议标准	使用频段	信道条件	固定/移动	信道带宽/MHz	传输速度/Mbit/s	额定小区半径/km
IEEE 802.16	10～66GHz	视距	固定	25/28	32～134	<5
IEEE 802.16a	<11GHz	非视距	固定	1.25/20	75	5～10
IEEE 802.16d-2004	10～66GHz <11GHz	视距＋非视距	固定	1.25/20	75	5～15
IEEE 802.16e-2005	<6GHz	非视距	固定 移动＋漫游	1.25/20	30	若干

- 无线网格网（Ad hoc）技术
- Ad hoc 网是一种不需要基站的“对等结构”移动通信模式。它的特征是“多跳的、无中心的、自组织无线网络”，又称为多跳网、无基础设施网或自组织网。
- Ad hoc 技术有两个发展方向：一是在军事和特定行业发展和应用的基础上产生的无线传感器网络（WSN）；另一个是向民用的接入网领域发展，出现了无线网格网（WMN）。
- 无线接入技术主要有：
- WLAN、WiMAX、Wi-Fi、WMAN 和 Ad hoc 等。

24. 万兆以太网

- 万兆以太网采用的是双绞线和光纤传输介质，只采用全双工的传输方式。
- 万兆以太网最长传输距离可达 80 公里，且可以配合 10G 传输通道使用，足够满足大多数城市城域网覆盖。
- 2002 年，IEEE 802 委员会正式批准万兆以太网标准，即 IEEE 802.3ae。

25. 物联网

- 物联网是新一代信息技术的重要组成部分，也是“信息化”时代的重要发展阶段。
- 物联网顾名思义就是物物相连的互联网，其中包含两层意思：

① 物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；

② 其用户端延伸和扩展到了任何物品与物品之间，进行信息交换和通信，也就是物物相息。

26. IEEE 802.11g

- IEEE 802.11工作组近年来定义了新的物理层标准IEEE 802.11g。
- 与以前的IEEE 802.11协议标准相比，IEEE 802.11g草案有以下两个特点：

① 在 2.4GHz 频段使用正交频分复用（OFDM）调制技术，使数据传输速率提高到 20Mbps 以上；

② 能够与 IEEE 802.11b 的 Wi-Fi 系统互联互通，可共存于同一 AP 的网络里，从而保障了后向兼容性。

27. 以太网地址

- 以太网地址即物理地址、MAC 地址，它是 48 位的 Ethernet 物理地址编码方法。
- 为了统一管理 Ethernet 的物理地址，保证每块 Ethernet 网卡的地址都是唯一的。IEEE 注册管理委员会（RAC）为每个网卡生产商分配物理地址的前 3 个字节，后面的 3 个字节由生产网卡的厂商自行分配。

第三章 Internet 基础

1. Internet

- Internet 是全球最具影响力的互联网络，它是将多个物理网络通过路由器相互连接而形成的。
- 从网络设计者角度考虑，Internet 是一个计算机互联网络；
- 从使用者角度考虑，Internet 是一个信息资源网。Internet 屏蔽了各个不同网络的差异和内部结构，使用户比较简单、一致地面对大量主机提供的信息资源和服务。

2. 路由器

- 路由器是 Internet 种最重要的设备，它是网络与网络之间连接的桥梁。
- 它主要的功能是：维护路由表信息（路由表决定着 IP 数据报发往何处），转发所收到的 IP 数据报，为投递的 IP 数据报选择最佳路径。

3. IP 地址

IPv4的地址长度为32bit，每8位为一组，用点分十进制表示；

每 8位为一组，每组最大取值为 $2^8-1=255$，每组取值范围为 0-255。

表 3-1　　A、B、C 类地址的比较

地址类型	主机地址范围	可分配的网络数	每个网络内可分配的最大主机数
A 类	1.0.0.0～127.255.255.255	$2^7=128$	$2^{24}-2=16\,777\,214$
B 类	128.0.0.0～191.255.255.255	$2^{14}=16\,384$	$2^{16}-2=65\,534$
C 类	192.0.0.0～223.255.255.255	$2^{21}=2\,097\,152$	$2^8-2=254$

4. Internet 的接入方式

几种常用的通过广域线路接入 Internet 的方法：

1）通过电话网接入

- 用户的计算机和 ISP 处的远程访问服务器（Remote Access Server，RAS)通过调制解调器（Modem〉与电话网相连。
- 用户在访问 Internet 时，通过拨号方式与 RAS 建立连接，借助 RAS 访问 Internet。

2） 利用 ADSL 接入

- 为了解决大容量的信息传输问题，引入非对称数字用户线路 ADSL。
- ADSL 使用比较复杂的调制解调技术，在普通的电话线路进行高速的数据传输：在数据的传输方向上，ADSL 分为上行和下行两个通道。
- 下行通道的数据传输速率远远大于上行通道的数据传输速率，即“非对称”性。
- ADSL 的上行速率可以达到 16~640kbps，下行速率可以达到 1.5~9Mbps。
- ADSL 调制解调器的网桥和路由器功能使单机接入和局域网接入都变得非常容易。
- 优点：ADSL 所需要的电话线资源分布广泛，具有使用费用低廉、无须重新布线和建设周期短的特点，尤其适合家庭和中小型企业的互联网接入需求。

3）使用 HFC 接入

- 传统的有线电视网使用同轴电缆作为传输介质。
- 混合光纤/同轴电缆网（Hybrid Fiber Coaxial，HFC)：信号首先通过光纤传输到光纤节点，再通过同轴电缆传输到有线电视网用户。
- 利用 HFC，网络的覆盖面积可以扩大到整个大中型城市，信号的传输质量可以大幅度提高。
- HFC 也采用非对称的数据传输速率。
- 一般的上行传输速率在 10Mbps 左右，而下行传输速率在 10~40Mbps 之间。
- HFC 采用共享式的传输方式，所有通过 Cable Modem 的发送和接收使用同一个上行和下行信道，因此，HFC 网上的用户越多，每个用户的实际可以使用的带宽就越窄。

4）通过数据通信线路接入

- 数据通信网是专门为数据信息传输而建的网络，如果需要传输性能更好、传输质量更高的接入方式，可以考虑数据线路接入。
- 数据通信网的种类很多，DDN、ATM、帧中继等网络都属于数据通信网：这些数据通信网由电信部门建设和管理，用户可以租用。

5. IP 协议

- Internet 是将提供不同服务、使用不同技术、具有不同功能的物理网络互联起来而形成的一个互联网。

- IP(Intemet Protocol)作为一种互联网协议，运行于互联层，屏蔽各个物理网络的细节和差异。
- 它不对所连接的物理网络作任何可靠性假设，使网络向上提供统一的服务。
- IP 协议精确定义了 IP 数据报格式，并且对数据报寻址和路由、数据报分片和重组、差错控制和处理等作出了具体规定。

6.IP 服务特点

运行 IP 协议的互联层可以为其高层用户提供的服务有如下 3 个特点：

① 不可靠的数据投递服务。

② 面向无连接的传输服务。

③ 尽最大努力投递服务。

7.IP 互联网的特点

IP 互联网是一种面向非连接的互联网络，它对各个物理网络进行高度的抽象，形成一个大的虚拟网络。

- IP 互联网隐藏了低层物理网络细节，向上为用户提供通用的、一致的网络服务。
- IP 互联网不指定网络互联的拓扑结构，也不要求网络之间全互联。一个网络只要通过路由器与 IP 互联网中的任意一个网络相连，就具有访问整个互联网的能力。
- IP 互联网能在物理网络之间转发数据，信息可以跨网传输。
- IP 互联网中的所有计算机使用统一的、全局的地址描述法。
- IP 互联网平等地对待互联网中的每一个网络，不管这个网络规模是大还是小，也不管这个网络的速度是快还是慢。

8.ARP 协议的基本思想

- 以太网一个很大的特点就是具有强大的广播能力。
- 针对这种具备广播能力、物理地址长但长度固定的网络，IP 互联网采用动态联编方式进行 IP 地址到物理地址的映射，并制定了相应的协议——ARP。
- ARP 请求信息和响应信息的频繁发送和接收必然对网络的效率产生影响。为了提高效率，ARP 协议实现过程中经常采用高速缓存技术。

9.IP 数据报格式

- IP 数据报是 IP 协议单元使用的数据单元，它的格式可以分为报头区和数据区两大部分，其中数据区包括高层需要传输的数据，而报头区是为了正确传输高层数据而增加的控制信息。
- 报头区主要包括：版本与协议类型域、长度域、服务类型域、生存周期域、头部校验和域、地址域、选项+填充域。其中报头长度域以 32 位的双字为单位；
- 生存周期（TTL）域用于防止数据报在 Internet 中无休止地传递；
- 头部校验和域用来保证 IP 数据报报头的完整性；
- 选项域主要用于控制和测试两大目的。
- 报头中有两个表示长度的字段，一个为报头长度，一个为总长度。报头长度以 32b 双字为单位，指出该报头区的长度。在没有选项和填充的情况下，该值为“5”。一个含有选项的报头长度则取决于选项域的长度。但是，报头长度应当是 32b 的整数倍，如不是，需在填充域加 0 凑齐。
- 总长度以 8b 字节为单位，表示整个 IP 数据报的长度（其中包含头部长度和数据区长度）。

10.MTU 与分片

- 根据网络使用的技术不同，每种网络都规定了一个帧最多能够携带的数据量，这一限制称为最大传输单元（Maximum Transmission Unit，MTU）。
- 一个 IP 数据报的长度只有小于或等于一个网络的 MTU，才能在这个网络中进行传输。
- 当一个数据报的尺寸大于将发往网络的 MTU 值时，路由器会将 IP 数据报分成若干较小的部分，称为分片，然后再将每片独立地进行发送。
- 与未分片的 IP 数据报相同，分片后的数据报也由报头区和数据区两部分构成，而且除一些分片控制域（如标志域、片偏移域）之外，分片的报头与原 IP 数据报的报头非常相似。
- 一旦进行了分片，每片都可以像正常的 IP 数据报一样经过独立的路由选择等处理过程，最终到达目的主机。
- 以太网的 MTU 为 1500 字节，一般 IP 首部为 20 字节，UDP 首部为 8 字节，数据的净荷（payload）部分预留是 1500-20-8=1472 字节。如果数据部分大于 1472 字节，就会出现分片现象。

11.分片控制

- 在 IP 数据报报头中，标识、标志和片偏移 3 个字段与控制分片和重组有关。
- 标识：是源主机赋予 IP 数据报的标识符。目的主机利用此域和目的地址判断收到的分片属于哪个数据报，以便数据报重组。分片时，该域必须不加修改地复制到新分片头的报头中。

- 标志字段：用来告诉目的主机该数据报是否已经分片，是否是最后一个分片。
- 片偏移字段：指出本片数据在初始 IP 数据报数据区中的位置，位置偏移量以 8 个字节为单位。由于各分片数据报独立地进行传输，其到达目的主机的顺序是无法保证的，而路由器也不向目的主机提供附加的片顺序信息，因此，重组的分片顺序由片偏移提供。

12.源路由

- 源路由是指 IP 数据报穿越互联网所经过的路径是由源主机指定的，它区别于由主机或路由器的 IP 层软件自行选路后得出的路径
- 源路由选项是非常有用的一个选项，可用于测试某特定网络的吞吐率，也可以使数据报绕开出错网络。
- 源路由选项可以分为两类，一类是严格源路由选项，一类是松散源路由选项。

① 严格源路由选项:严格源路由选项规定 IP 数据报要经过路径上的每一个路由器，相邻路由器之间不得有中间路由器，并且所经过路由器的顺序不可更改。

② 松散源路由选项:松散源路由选项只是给出 IP 数据报必须经过的一些“要点”，并不给出一条完备的路径，无直接连接的路由器之间的路由尚需 IP 软件的寻址功能补充。

13.ICMP 差错控制

- ICMP 作为 IP 层的差错报文传输机制，最基本的功能是提供差错报告。
- ICMP 差错报文有以下几个特点：

① 差错报告不享受特别优先权和可靠性，作为一般数据传输。在传输过程中，它完全有可能丢失、损坏或被抛弃。

② ICMP 差错报告数据中除包含故障 IP 数据报报头外，还包含故障 IP 数据报数据区的前 64 比特数据。

③ ICMP 差错报告是伴随着抛弃出错 IP 数据报而产生的。

- ICMP 出错报告包括目的地不可达报告、超时报告、参数出错报告等。

14.RIP 和 OSPF 路由选择协议

- 应用最广泛的路由选择协议有两种，路由信息协议（RIP)和开放式最短路径优先协议（OSPF)。
- RIP 协议利用向量-距离算法，而 OSPF 则使用链路-状态算法
- 在互联网设计和管理过程中，网络管理员可以根据互联网的具体环境选择路由表的建立方法。一般来说，静态路由比较适合于在小型、单路径、静态的 IP 互联网环境下使用；
- RIP 协议比较适合于小型到中型、多路径、动态的 IP 互联网环境；
- 而 OSPF 协议比较适合较大型到特大型、多路径、动态的 IP 互联网环境。

15.RIP(路由表项问题)

当路由器 Ri 收到 Rj 的路由报文信息时，满足下列条件之一，则须修改 Ri 的路由表：

① Rj 列出的某表目 Ri 中没有。则 Ri 路由表中须增加相应的表目，其“目的网络”是 Rj 表目中的“目的网络”，其“距离”为 Rj 表目中的距离加 1，而“路径”则为 Rj。

② Rj 去往某目的地的距离比 Ri 去往该目的地的距离减 1 还小。这种情况说明 Ri 去往某目的网络如果经过 Rj，距离会更短。于是，Ri 需要修改本表目，其“目的网络”不变，“距离”为 Rj 表目中的距离加 1，“路径”为 Rj。

③ Ri 去往某目的地经过 Rj，而 Rj 去往该目的地的路径发生变化。则：A 如果 Rj 不再包含去往某目的地的路径，则 Ri 中相应路径须删除；B 如果 Rj 去往某目的地的距离发生变化，则 Ri 中相应表目“距离”须修改，以 Rj 中的“距离”加 1 取代之。

16.RIP 协议（收敛问题）

为了解决慢收敛问题，RIP 协议采用了以下解决对策：

- 限制路径最大“距离”对策。

① RIP 协议规定“距离”的最大值为 16，距离超过或等于 16 的路由为不可达路由。

② 在使用 RIP 协议的互联网中，每条路径经过的路由器数目不应超过 15 个。

- 水平分割对策
- 保持对策。
- 带触发刷新的毒性逆转对策。

17.IP 组播特点

- 组播是一种允许一个或者多个发送方发送单一数据包到多个接收方的网络传输方式。
- 在 Internet 上进行组播就叫 IP 组播，IP 组播具有以下几个明显的特点：

① 组播使用组地址。在组播网中，每个组播组拥有唯一的组播地址（D 类 IP 地址），组播数据包可以送到标识目的主机的组地址，发送方不必知道有哪些成员，它自己不必是组成员，对组成员中主机的数

目和位置也没有限制。主机不需要和组成员以及发送方协商，可以任意加入和离开组播组。

② 动态的组成员。组播组中的成员是动态的。

③ 底层硬件支持的组播。

- Internet 组管理协议（IGMP）运行于主机与主机直接相连的组播路由器之间，实现所连网络组成员关系的收集与维护。
- 组播路由协议是 IP 组播协议体系中最核心的内容。IP 组播路由协议包括：距离矢量组播路由协议（DVMRP），开放最短路径优先的组播扩展（MOSPF），以及协议独立组播-密集模式（PIM-DM）。
- 组管理协议包括 Internet 组管理协议（Internet Group Management Protocol，IGMP)和 Cisco 专用的组管理协议（CGMP)。

18.IGMPvX

- IGMPv1 定义了基本的组成员查询和报告过程；
- IGMPv2 在 IGMPv1 的基础上添加了组成员快速离开的机制。
- 目前通用的是 IGMPv3。IGMPv3 中增加的主要功能是成员可以指定接收或指定不接收某些组播源的报文。
- IGMP Snooping 技术可在二层设备上形成组成员和接口的对应关系。

19.IPv4 局限性

① 地址空间的局限性。

② IP 协议的性能问题。

③ IP 协议的安全性问题。

④ 自动配置问题。

⑤ 服务质量（QoS)保证问题。

20.IPV6 表示方法

- IPv6 的 128 位地址按每 16 位划分为一个位段，每个位段被转换为一个 4 位的十六进制数，并用冒号“：”隔开，这种表示法称为冒号十六进制(colon hexadecimal)表示法。
- 若 IPv6 地址中出现多个连续的 0，通过压缩前导 0 来简化表示。使用零压缩法时，只能压缩前导 0。不能把位段内的有效 0 压缩掉。
- 双冒号表示法：将 IPv6 地址中连续位段的 0 简写为“：：”。双冒号“：：”在一个地址中只能出现一次。
- 确定“：：”之间到底被压缩了多少位 0，可以用 8 减掉地址中剩余的位段数，再将结果乘以 16 即可。
- IPv6 前缀长度表示法：“地址 / 前缀长度”来表示。
- 在 IPvv6 中，回送地址一般是 0：0：0：0：0：0：0：1。

21.IPv6 扩展头

- 逐跳选项头：类型为 0，由中间路由器处理的扩展头，目前主要有两个选项，即巨型有效载荷选项和路由器警告选项。
- 目的选项头：类型为 60，用于为中间结点或目的结点指定数据报的转发参数。
- 路由头:类型为 43，用来指出数据报在从源结点到达目的结点的过程中，需要经过的一个或多个中间路由器。
- 分片头：类型为 44。由源结点给出分片数据报中数据部分相对原始数据的偏移量、是否是最后一片标志及数据报的标识符，目的结点用这些参数进行分片数据报的重组。
- 认证头：类型为 51。用于携带通信双方进行认证所需的参数。
- 封装安全有效载荷报头：类型为 52。可以与认证头结合起来使用，也可以单独使用。

22.传输控制协议 TCP

- 从 TCP 的用户角度看，TCP 可以提供面向连接的、可靠的（没有数据重复或丢失）、全双工的数据流传输服务。它允许两个应用程序建立一个连接，然后发送数据并终止连接。
- TCP 使用窗口机制进行流量控制。
- TCP 提供的服务特征：

① 面向连接（Connection Orientation)。TCP 提供的是面向连接的服务。

② 完全可靠性（Complete Reliability)。TCP 确保通过一个连接发送的数据正确地到达目的地，不会发生数据的丢失或乱序。

③ 全双工通信（Full Duplex Communication)。一个 TCP 连接允许数据在任何一个方向上流动，并允许任何一方的应用程序在任意时刻发送数据。

④ 流接口（Stream Interface)。TCP 提供了一个流接口，应用程序利用它可以发送连续的数据流。

⑤ 连接的可靠建立与优雅关闭（Reliable Connection Startup & Graceful Connection Shutdown)。

为确保连接建立和终止的可靠性，TCP 使用了 3 次握手（3-Way Handshake)法。

23.用户数据报协议 UDP

- 用户数据报协议 UDP 位于传输层；
- 可靠性远没有 TCP 高；
- 从用户的角度看，用户数据报协议 UDP 提供了面向非连接的、不可靠的传输服务。它使用 IP 数据报携带数据，但增加了对给定主机上多个目标进行区分的能力。
- 利用 UDP 协议传送的数据有可能会出现丢失、重复或乱序现象；
- 优点：运行的高效性和实现的简单性。

24.NAT 的主要技术类型

- NAT 的主要技术类型有 3 种，它们是静态 NAT（Static NAT）、动态 NAT（Pooled NAT）和网络地址端口转换 NAPT（Port-Level NAT）。
- 网络地址端口转换 NAPT

网络地址端口转换是目前最常使用的一种 NAT 类型，它利用 TCP/UDP 的端口号区分 NAT 地址映射表中的转换条目，可以使内部网中的多个主机共享一个（或少数几个）全局 IP 地址同时访问外部网络。

25.各类路由

- 源路由：指 IP 数据报穿越互联网所经过的路径是由源主机指定的。
- 记录路由：指记录下 IP 数据报从源主机到达目的主机所经过路径上各个路由器的 IP 地址。
- 主机路由：指对单个主机（而不是网络）指定一条特别的路径。
- 默认路由：一种特殊的静态路由，指的是当路由表中与包的目的地址之间没有匹配的表项时路由器能够做出的选择，默认路由会大大简化路由器的配置，减轻管理员的工作负担，提高网络性能。

第四章 Internet 基本服务

1.客户机/服务器模式

- 在分布式计算中，这种一个应用进程被动地等待，而另一个应用进程通过请求启动通信的模式就是客户机/服务器交互模式。
- 实际上，客户机（Client）和服务器（Server）分别指两个应用进程。客户机向服务器发出服务请求，服务器作出响应。客户机发出请求，该请求经互联网传送给服务器。一旦服务器接收到这个请求，就可以执行请求指定的任务，并将执行的结果经互联网回送给客户机。

2.C/S 模式解决的主要问题

1） 标识一个特定的服务

- 在 TCP/IP 互联网中，服务器进程通常使用 TCP 协议或 UDP 协议的端口号作为自己的特定标识。
- 在服务器进程启动时，它首先在本地主机注册自己使用的 TCP 或 UDP 端口号。
- 在客户机进程需要访问某个服务时，可以通过与服务器进程使用的 TCP 端口建立连接（或直接向服务器进程使用的 UDP 端口发送信息）来实现。

2） 响应并发请求

为解决多个请求同时到达服务器的问题。服务器必须具备处理多个并发请求的能力。为此，服务器可以有以下两种实现方案：

- 重复服务器（Iterative Server）方案。

① 该方案实现的服务器进程中包含一个请求队列，客户机请求到达后，首先进入队列中等待，服务器按照先进先出（First In First Out）的原则顺序作出响应。

② 重复服务器对系统资源要求不高，重复服务器解决方案一般用于处理可在预期时间内处理完的请求，针对面向无连接的客户机/服务器模型。

- 并发服务器（Concurrent Server）方案。

① 并发服务器是一个守护进程（Daemon），在没有请求到达时它处于等待状态。一旦客户机请求到达，服务器立即再为之创建一个子进程，然后回到等待状态，由子进程响应请求。当下一个请求到达时，服务器再为之创建一个新的子进程。其中，并发服务器叫作主服务器（Master），子进程叫作从服务器（Slave）。

② 并发服务器解决方案具有实时性和灵活性的特点。

③ 并发服务器解决方案通常对主机的软硬件资源要求较高。一般用于处理不可在预期时间内处理完的请求，针对面向连接的客户机/服务器模型。

3） 服务器进程的安全问题

- 由于服务器进程的特殊地位，它需要经常性地读取系统文件、保存日志、访问保护数据，具有相当高的特权。因此，
- 它必须承担保障系统安全性的责任，负责实施系统访问和保护策略。

3.对等计算模型

- 对等计算（PeertoPeer,P2P）可以简单地定义成通过直接交换来共享计算机资源和服务，而对等计算模型在应用层形成的网络通常称为对等网络。
- 网络中的每一台计算机既能充当网络服务的请求者，又能对其他计算机的请求作出响应，提供资源与服务。通常这些资源和服务包括:信息的共享与交换、计算资源（如 CPU 的共享）、存储资源（如缓存和磁盘空间的使用）等。

4.四种对等计算模型

对等计算模型主要有四种：集中目录式结构、分布式非结构化 P2P 网络结构、分布式结构化 P2P 网络结构和混合式 P2P 网络结构。

- 集中目录式结构：

① 以一个中心服务器来负责记录共享信息以及回答这些信息的查询。

② 采用集中式拓扑结构的 P2P 系统被称为第一代 P2P 系统，其代表性的软件有 Napster 和 Maze。

- 分布式非结构化 P2P 网络结构：

① 采用随即图的组织方式形成一个松散的网络；

② 支持复杂查询，比如带有规则表达式的多关键字查询、模糊查询等；

③ 分布式非结构化拓扑的 P2P 网络模型中，每个结点都具有相同的功能，既是客户机又是服务器，因而结点也被称为对等点；

④ 这种拓扑的网络中多采用洪泛方式查询和定位资源；

⑤ 采有分布式非结构化拓扑的 P2P 即时通信软件的典型代表有 Gnutella、Shareaza、LimeWire 和 BearShare。

- 分布式结构化 P2P 网络结构：

① 采用基于 DHT（分布式散列表）的分布式算法和路由算法组成一个网络结构；
② 目前采用分布式结构化拓扑的 P2P 网络系统有 Pastry、Tapestry、Chord 和 CAN。

- 混合式 P2P 网络结构：

① 混合式结合了集中式和分布式 P2P 网络的优点进行优化网络结构。
② 混合式拓扑的 P2P 网络系统有 Skype、Kazaa、eDonkey、BitTorrent 和 PPLive。

5.混合式 P2P 网络 3 种结点

●用户结点。

普通的结点就是用户结点，它不具有任何特殊的功能。

●搜索结点。

搜索结点处理搜索请求，从其子结点中搜索文件列表。这些结点必须有较高的网络连接速度，而且往往需要采用高性能的处理器。

●索引结点。

① 要以连接速度快、内存充足的结点作为索引结点。
② 索引结点保存可以利用的搜索结点信息、搜集状态信息以及尽力维护网络的结构。
③ 一个结点既可以是搜索结点又可以是索引结点。

6.层次型命名机制

- 层次型命名机制（Hierarchy Naming）就是在名字中加入结构，而这种结构是层次型的。
- 层次型命名机制将名字空间划分成一个树状结构，树中的每一结点都有一个相应的标识符，主机的名字就是从树叶到树根（或从树根到树叶）路径上各结点标识符的有序序列。

7.TCP/IP 互联网域名

- 在 TCP/IP 互联网中所实现的层次型名字管理机制叫作域名系统（Domain Name System,DNS）。
- 域名系统的命名机制叫作域名（DomainName）。完整的域名由名字树中的一个结点到根结点路径上结点标识符的有序序列组成，其中结点标识符之间以“.”隔开。
- 例：域名“cs.nankai.edu.cn”由 cs、nankai、edu 和 cn 四个结点标识符组成（根结点标识符为空，省略不写），这些结点标识符通常被称为标号（Label）,而每一标号后面的各标号叫作域（Domain）。在“cs.nankai.edu.cn”中,最低级的域为“cs.nankai.edu.cn”,代表计算机系;第 3 级域为“nankai.edu.cn”代表南开大学;第二级域为“edu.cn”，代表教育机构;顶级域为“cn”，代表中国。

8.Internet 顶级域名分配

顶级域名	分配给	顶级域名	分配给	顶级域名	分配给
com	商业组织	mil	军事部门	int	国际组织
edu	教育机构	net	网络支持中心	国家代码	各个国家
gov	政府部门	org	非营利性组织		

9.域名服务器

- 解析系统的核心是 TCP/IP 域名服务器，是一组既独立又协作的域名服务器
- 域名服务器实际上是一个服务器软件，运行在指定的主机上，完成域名-IP 地址映射。有时候，也把运行域名服务器软件的主机叫作域名服务器，该服务器通常保存着它所管辖区域内的域名与 IP 地址的对照表。
- 请求域名解析服务的软件叫域名解析器。在 TCP/IP 域名系统中，一个域名解析器可以利用一个或多个域名服务器进行名字映射。
- 树形的域名服务器的逻辑结构是域名解析算法实现的基础。
- 域名解析采用自顶向下的算法，从根服务器开始直到叶服务器，在其间的某个结点上一定能找到所需的名字-地址映射。

10.域名解析的两种方式

- 递归解析（Recursive Resolution ），要求域名服务器系统一次性完成全部名字-地址变换。
- 反复解析（Iterative Resolution），每次请求一个服务器，不行再请求别的服务器。

11.提高域名解析效率的 3 种方法

1） 解析从本地域名服务器开始
2） 域名服务器的高速缓冲技术

- 在互联网中，域名服务器采用域名高速缓冲技术可极大地减少非本地域名解析的开销。
- 为了保证缓冲区中域名-IP 地址映射关系的有效性，通常可以采用以下两种策略：

① 域名服务器向解析器报告缓冲信息时，需注明这是“非权威性的”（nonauthcmtative）的映射，并且给出获取该映射的域名服务器 IP 地址。

② 对高速缓冲区中的每一映射关系都有一个最大生存周期（Time To Live，TTL），它规定该映射关系在缓冲区中保留的最长时间。一旦某映射关系的 TTL 时间到，系统便将它从缓冲区中删除。

3） 主机上的高速缓冲技术

高速缓冲机制不仅用于域名服务器，在主机上也可以使用。

12.域名系统对象类型

类型	意义	内容
SOA	授权开始	标识一个资源记录集合（称为授权区段）的开始
A	主机地址	32 位二进制 IP 地址
MX	邮件交换机	邮件服务器名及优先级
NS	域名服务器	域的授权名字服务器名
CNAME	别名	别名的规范名字
PTR	指针	对应于 IP 地址的主机名
HINFO	主机描述	ASCII 字符串，CPU 和 OS 描述
TXT	文本	ASCII 字符串，不解释

13.远程登录协议（Telnet）

● Internet 中的用户远程登录是指用户使用 Telnet 命令，使自己的计算机暂时成为远程计算机的一个仿真终端的过程。

● 远程终端协议（Telnet 协议）。它是 TCP/IP 协议的一部分，精确地定义了本地客户机与远程服务器之间的交互过程。

● Telnet 协议引入了网络虚拟终端（Network Virtual Terminal,NVT）为了解决系统的差异性，他提供了一种标准的键盘定义，用来屏蔽不同计算机系统对键盘输入的差异性。

● Telnet 采用了客户机/服务器模式

14.FTP 客户机/服务器模型

● FTP 采用客户机/服务器模式，客户机与服务器之间利用 TCP 建立连接。

● FTP 是一个交互式会话系统，控制连接用于维持会话，负责在客户机和服务器之间传送 FTP 命令和响应。

● FTP 客户机和服务器之间要建立双重连接，一个是控制连接，一个是数据连接。

① 控制连接以通常的客户机/服务器方式建立。

② 数据连接用于传输数据。

● 当用户访问提供匿名服务的 FTP 服务器时，匿名账户和密码是公开的，如果没有特殊声明，通常用“anonymous”作为账号，用“guest”作为口令。

15.数据连接建立的两种模式

●主动模式（一般为默认模式）：

当客户机向服务器发出数据传输命令时，客户机在 TCP 的一个随机端口上被动打开数据传输进程，并通过控制连接利用 PORT 命令将客户机的数据传输进程所使用的端口号发送给服务器，服务器在 TCP 的 20 端口上建立一个数据传输进程，并与客户机的数据传输进程建立数据连接。

●被动模式：

当客户机向服务器发出数据传输命令时，通过控制连接向服务器发送一个 PASV 命令请求进入被动模式。服务器在 TCP 的一个端口上被动打开数据传输进程，并通过对 PASV 命令的响应将服务器数据传输进程使用的端口通知给客户机。客户机在 TCP 的一个随机端口上以主动方式打开数据传输进程，与服务器端的数据传输进程之间建立数据连接。

16.FTP 常用命令

命 令	描 述
USER username	向服务器发送用户名
PASS password	向服务器发送口令
PORT $n_1, n_2, n_3, n_4, n_5, n_6$	客户机 IP 地址（n_1, n_2, n_3, n_4）和端口号
PASV	请求使用被动模式建立数据连接
LIST filelist	请求服务器返回当前远程目录下的目录和文件
TYP Etype	说明文件类型：A 表示 ASCII 码，I 表示图像

命 令	描 述
REST marker	指明传输文件的起始点
RETR file name	检索一个文件
STOR file name	存储一个文件
ABOR	放弃先前的 FTP 命令和数据传输
QUIT	从服务器注销

17.FTP 协议文件传输方式

FTP 协议支持两种文件传输方式：文本文件传输和二进制文件传输。

1） 文本文件传输

- FTP 协议支持两种文本文件类型的传输，即 ASCII 码文件类型和 EBCDIC 文件类型。
- ASCII 码文件类型是系统的默认方式，文本文件以 NVT ASCII 码形式在数据连接中传输。这要求发方将本地文本文件转换成 NVT ASCII 码形式，而收方则将 NVT ASCII 码再还原成本地文本文件。
- EBCDIC 文件类型的文本文件传输要求两端都是采用 EBCDIC 编码的系统。

2） 二进制文件传输

文件系统不对文件格式进行任何变换，按照原始文件相同的位序以连续的比特流方式进行传输，确保拷贝文件与原始文件逐位一一对应。

18.FTP 用户接口命令

命令	描述
ftp	进入 ftp 会话
quit,bye	退出 ftp 会话
open host [port]	建立与指定 ftp 服务器的连接，可指定连接端口
close	中断与服务器 ftp 的连接
passive	进入被动传输方式
restart marker	从指定的标志 marker 处重新开始 get 或 put
ascii	使用 ascii 类型传输方式
binary	使用二进制文件传输方式
cd remote-dir	进入远程主机目录
cdup	进入远程主机目录的父目录
pwd	显示远程主机的当前工作目录
Is[remote-dir][local-file]	显 7K 远程目录 remote-dir,并存入本地文件 local-file
dir[remote-dir][local-file]	显示远程主机目录，并将结果存入本地文件 local-file
mk dirdir-name	在远程主机中建目录
rm dirdir-name	删除远程主机目录
get remote-file[local-file]	将远程主机的文件 remote-file 传至本地硬盘的 local-file
mge tremote-files	传输多个远程文件
put local-file[remote-file]	将本地文件 local-file 传送至远程主机
mput local-files	将多个文件传输至远程主机
delete remote-file	删除远程主机文件
help[cmd]	显示 ftp 内部命令 cmd 的帮助信息，如 helpget

19.电子邮件系统

- 电子邮件系统不但可以传输各种文字的文本信息，而且还可以传输图像、声音、视频等多媒体信息。
- 电子邮件系统采用客户机/服务器工作模式。
- 电子邮件应用程序的两项最基本功能为：创建和发送邮件以及接收、阅读和管理邮件。
- 在 TCP/IP 互联网中，邮件服务器之间使用简单邮件传输协议（Simple Mail Transfer Protocol,SMTP）相互传递电子邮件。

- 而电子邮件应用程序使用 SMTP 协议向邮件服务器发送邮件，使用 POP3（Post Office Protocol）协议或 IMAP（Interactive Mail Access Protocol）协议从邮件服务器的邮箱中读取邮件，
- 目前，尽管 IMAP 是一种比较新的协议，但支持 IMAP 协议的邮件服务器并不多，大量的服务器仍然使用 POP3 协议。

20.简单邮件传输协议 SMTP

- 简单邮件传输协议 SMTP 只规定发送程序和接收程序之间的命令和应答；
- SMTP 邮件传输采用客户机/服务器模式；
- 常用的 SMTP 命令

命令	描述
HELO<主机域名>	开始会话
MAILFROM:<发送者电子邮件地址>	开始一个邮递处理，指出邮件发送者
RCPTTO:<接收者电子邮件地址>	指出邮件接收者
DATA	接收程序将 data 命令后面的数据作为邮件内容处理，直到<CR><LF>.<CR><LF>出现
RSET	中止当前的邮件处理
NOOP	无操作
QUIT	结束会话

21.SMTP 邮件传递过程 3 阶段：

1） 连接建立阶段。

在这一阶段，SMTP 客户机请求与服务器的 25 端口建立一个 TCP 连接。一旦连接建立，SMTP 服务器和客户机就开始相互通报自己的域名，同时确认对方的域名；

2） 邮件传递阶段。

利用 MAIL、RCPT 和 DATA 命令，SMTP 将邮件的源地址、目的地址和邮件的具体内容传递给 SMTP 服务器，SMTP 服务器进行相应的响应并接收邮件；

3） 连接关闭阶段。

SMTP 客户机发送 QUIT 命令，服务器在处理命令后进行响应，随后关闭 TCP 连接。

22.邮局协议 POP3

POP3 是邮局协议 POP 的第 3 个主要版本，它允许用户通过 PC 机动态检索邮件服务器上的邮件；

POP3 只对邮件服务器上的邮件提供下载和删除的操作；

POP3 采用客户机/服务器模式；

POP3 的命令和响应也采用 ASCII 字符串的形式；

23.常用的 POP3 命令

命 令	描 述
USER<用户邮箱名>	客户机希望操作的电子邮箱
PASS<口令>	用户邮箱的口令
STAT	查询报文总数和长度
list[<邮件编号>]	列出报文的长度
RETR<邮件编号>	请求服务器发送指定编号的邮件
DELE<邮件编号>	对指定编号的邮件作删除标记
NOOP	无操作
RSET	复位操作，清除所有删除标记
QUIT	删除具有“删除”标记的邮件，关闭连接

24.用户检索 POP3 过程

1） 认证阶段。

邮件服务器中邮箱具有权限，只有授权才能访问，因此，在 TCP 连接建立之后，通信的双方随即进入认证阶段。客户机程序利用 USER 和 PASS 命令将邮箱名和密码传送给服务器，服务器据此判断该用户的合法性，并给出相应的应答。一旦用户通过服务器的验证，系统就进入了事务处理阶段；

2） 事务处理阶段。

在事务处理阶段，POP3 客户机可以利用 STAT、LIST、RETR、DELE 等命令检索和管理自己的邮箱，服务器在完成客户机请求的任务后返回响应的命令。但服务器在处理 DELE 命令请求时并未将邮件真正删除，只是给邮件作了一个特定的删除标记。

3） 更新阶段。

当客户机发送 QUIT 命令时，系统进入更新阶段。POP3 服务器将作过删除标记的所有邮件从系统中全部真正删除，然后 TCP 关闭连接。

25.电子邮件报文格式

RFC822 和多用途 Internet 邮件扩展协议（Multipurpose Internet Mail Extensions，MIME）对电子邮件的报文格式作出了具体规定。

1） RFC822

- RFC822 将电子邮件报文分成两部分，一部分为邮件头（Mail Header），另一部分为邮件体（Mail Body），两者之间使用空行分隔。
- 邮件头是一些控制信息，如发信人与收信人的电子邮件地址、发送日期等。
- 邮件体是用户发送的邮件内容，RFC822 只规定它是 ASCII 字符串。
- 邮件头由多行组成，每行由一个特定的字符串开始，后面跟有对该字符串的说明，中间用“隔开。

2） 多用途 Internet 邮件扩展协议 MIME

- 为了使电子邮件能够传输多媒体等二进制信息，MIME 对 RFC822 进行了扩充。
- MIME 协议继承了 RFC822 的基本邮件头和邮件体模式，但在此基础上增加了一些邮件头字段，并要求对邮件体进行编码，将 8 位的二进制信息变换成 7 位的 ASCII 文本。
- 主要增加的邮件头字段包括：

① MIME-Version:表明该邮件遵循 MIME 标准的版本号。目前的主要标准为 1.0。

② Comem-Type:说明邮件体包含的数据类型。MIME 定义了七种邮件体类型和一系列的子类型，这七种类型为：text（文本）、message（报文）、image（图像）、audio（音频）、video（视频）、application（应用）和 multipart（多部分）。

③ Content-Transfer-Encoding:指出邮件体的数据编码类型。由于电子邮件需要传输多媒体等二进制信息，因此，必须定义一种机制把亡进制数据编码成 7 位 ASCII 文本。MIME 推荐的编码方式包括带引见符的可打印编码（Quoted-Printable）和基数 64 编码（base64）。

26.Web 的基本概念

- Web 是 TCP/IP 互联网上一个完全分布的信息系统，最早由欧洲核物理研究中心的 Tim-Berners Lee 主持开发，其目的是为研究中心分布在世界各地的科学家提供一个共享信息的平台。
- Web 服务采用客户机/服务器工作模式；
- 它以超文本标记语言 HTML（Hyper Text Mark up Language）与超文本传输协议 HTTP（Hyper Text Transfer Protocol）为基础，为用户提供界面一致的信息浏览系统。
- 在 Web 服务系统中，信息资源以页面（也称网页或 Web 页面）的形式存储在服务器（通常称为 Web 站点）中；
- 页面到页面的链接信息由统一资源定位符 URL（Uniform Resource Locators）维持。

27.Web 浏览器

- Web 的客户机程序称为 Web 浏览器（Browser），它是用来浏览服务器中 Web 页面的软件。
- 从浏览器的结构上讲，浏览器由一个控制单元和一系列的客户单元、解释单元组成。
- 控制单元是浏览器的中心，它协调和管理客户单元和解释单元。

28.HTTP 请求报文&应答报文

1） HTTP 请求报文

① HTTP 请求报文包括一个请求行和若干个报头行，有时还可能带有报文体。

② 报文头和报文体以空行分隔。请求行包括请求方法、被请求的文档以及 HTTP 版本。

2） HTTP 应答报文

① HTTP 应答报文包括一个状态行和若干个报头行，并可能在空行后带有报文体。

② 状态行包括 HTTP 版本、状态码、原因等内容。

29.HTML 标记

- 段落标记用<P>表示
- 图像标记用<IMG>标记
- 超链接标记用<A>标记

30.SSL 协议

- SSL（安全套接层）及其继任者传输层安全（TLS）是为网络通信提供安全及数据完整性的一种安全协议。
- https 是以安全为目标的 HTTP 通道，简单讲是 HTTP 的安全版。即 HTTP 下加入 SSL 层，https 的安全基础是 SSL。
- 如果用户想在 Web 网站上使用 SSL 协议，则 URL 头必须采用 https 开始。

31.浏览器安全问题

浏览器是用户在电子商务活动中最常用的工具，用户在浏览 Web 站点及与 Web 站点进行交互最为关心的便是安全问题，通常考虑的安全问题包括以下几个方面：

- 如何保护自己的计算机：为了保护用户的计算机免受非安全软件的危害，浏览器通常将 Internet 世界划分成几个区域；
- 如何验证站点的真实性：利用 Web 站点传来的证书可以验证站点的真实性；
- 如何避免他人假冒自己的身份在 Internet中活动：用户可以从 CA安全认证中心申请自己的证书，并将该证书装入浏览器，利用其在 Internet 上表明自己的身份；
- 在与 Web 站点交互敏感信息时如何避免第三方偷看或者篡改等：在安全通道中使用安全套接层 SSL 技术。

第五章 新型网络应用

1.即时通信（IM）系统

- 1996 年 11 月，以色列 Mirabils 公司推出了世界上第一款即时通信软件 ICQ（I Seek You,网络寻呼机），宣告了“即时通信（Instant Messaging，IM）”这一概念的诞生。
- 即时通信系统是一种基于 Internet 的通信服务，可提供近实时的信息交换和用户状态跟踪。
- 2000 年，IMPP 工作小组提交的关于即时通信系统的 RFC 草案，获得了 IETF 的批准，成为正式的 RFC 文件。
- IETF 批准的 RFC2778 给出了一个抽象的呈现与即时消息系统模型，描述了即时通信系统的功能，勾勒出了即时通信系统的模型框架。
- 一个即时通信系统通常包括两种服务

① 一种是呈现服务（Pesence srvice），用户之间相互订阅并获取彼此的状态变更信息；

② 另一种是即时消息服务（istant message srvice），用于用户之间相互收发短消息。

- 即时通信系统一般采用两种通信模式

① 用户/服务器模式，在用户/服务器模式中，消息的发送和接收需要通过服务器中转，主流的即时通信软件的文本消息大多使用用户/服务器模式。

② 用户/用户模式。消息的发送和接收采用直接的点对点的通信方式，文件传送等大数据量业务通常使用用户/用户模式。

2.即时通信协议

- 微软 MSN采用 MSNP协议；
- AOL 采用 OSCAR 协议；
- QQ 采用自己设计的私有协议
- 由于各厂商自己定义的协议互不开放，因此造成彼此间互不兼容，无法互联互通。
- 即时通信开放的协议主要代表有两个

① 一个是基于 SIP 协议框架的 SIMPLE 协议簇

② 一个是基于 JABBER 协议框架的 XMPP 协议簇。

③ SIMPLE 协议是对 SIP 协议的扩展，以使其更好地支持即时消息服务。

④ XMPP 协议簇是基于 XML 语言定义的即时消息协议。

3.SIP(会话初始化协议)

- SIP 是 IETF 于 1999 年提出的一个信令控制协议，主要内容在 RFC3261 中进行定义；
- SIP 协议位于应用层，目标是方便地创建、管理和终止用户之间的会话。
- SIP 协议主要是为 IP 网络设计的，可以运行于 TCP、UDP、SCTP 等各种传输层协议之上。但是，SIP 协议本身并不关心承载网络，因此 SIP 协议也可工作在 ATM、帧中继等承载网中。

4.SIP 系统

1） SIP 用户的地址以“SIP”开始，后面类似于 E-mail 地址。

2） 例如可以使用 sip：miyname@my-company.com 表示一个 SIP 用户，该用户处于 mycompany.com 域中，在 mycompany.com 域中的名字为 myname。

3） SIP 地址是一个全局性的地址，SIP 系统通过这种统一名字标识符定位和查询 SIP 用户。

4） 按逻辑功能区分，SIP 系统由 4 种元素组成，它们是用户代理（user agent，UA）、代理服务（proxy server）、重定向服务器（redirect server）和注册服务器（registrar）。

- 用户代理：

① 用户代理由两个部分组成：一部分是用户代理客户机（User Agent Client，UAC），另一部分是用户代理服务器（User Agent Server UAS）。

② UAC 负责发起呼叫，UAS 负责接收呼叫并作出响应。

③ UAC 和 UAS 共同组成 UA，存在于用户终端之中。

④ 用户通过 SIP 用户代与 SIP 系统交互，其存在的形式多种多样，如计算机上的即时通信软件、专用的软电话（phone）等。

- 代理服务器:

① 代理服务器负责接收用户代理发来的请求，根据网络策略将请求发给相的服务器，并根据收到的应答对用户作出响应。

② 代理服务器是一个中间元素，既有客户机的性质又有服务器的性质，同时还具有名字解析能力。

③ 代理服务器分为有状态代理服务器和无状态代理服务器。

④ 有状态代理服务器需要存储接收到的请求、回送的响应和它转发的请求，而无状态代理服务器一旦转发请求和响应后就忘记所有的信息。

- 重定向服务器：重定向服务器是一个规划 SIP 呼叫路径的服务器。
- 注册服务器:用于接收和处理用户端的注册请求，完成用户地址的注册。

5.SIP 消息

1） SIP 消息组成

- 由一个起始行（start-line）、消息头（message-header）、一个标志消息头结束的空行 CRLF）和可选的消息体（messagebody）组成。
- 其中，消息头由一个或多个字段组成。

2） SIP 消息包括两种类型：

- 从客户机到服务器的请求消息（request）

① 在请求消息中，起始行为请求行。

② 请求行中一般包括请求方法、请求的 SIP 用户地址和 SIP 的协议版本。

③ 在 SIP 协议中有 6 种请求方法，它们是 INVITE、ACK、OPTIONS、BYE、CANCEL 和 REGISTER。

请求方法	功能
INVITE	邀请用户或服务器参加一个会话
ACK	UA 向服务器证实它已经收到了对 INVITE 请求的最终响应。ACK 只和 INVITE 一起使用
OPTIONS	请求关于服务器能力的信息。如果服务器认为它能与用户联系，则可用一个能力集响应
BYE	用户终止一次会话，既可由主叫 UA 发送，也可由被叫 UA 发送
CANCEL	取消一个挂起的呼叫
REGISTER	向定位服务器注册 UA 的相关信息

- 从服务器到客户机的响应消息（response）

① 响应消息中，起始行为状态行。

② 状态行中一般包括 SIP 的版本号、状态码和一句对该状态的文本描述信息。

6.SIMPLE 协议

- SIMPLE 协议是一组能够提供即时消息服务的通信协议。
- 它由 IETF 的 SIMPLE 工作组制定，基本上与 RFC2778 定义的即时消息系统模型保持一致。
- SIMPLE 协议通过对 SIP 协议进行扩展，使其支持即时消息服务。
- SIMPLE 增加了 NOTIFY、SUBSCRIBE 和 MESSAGE 方法支持即时通信。

① MESSAGE：用来发送一次性的短消息，即寻呼机模式的即时消息。

② SUBSCRIBE：用于观察者（watcher）向服务器订阅其他用户的呈现信息。

③ NOTIFY：在用户的呈现信息发生改变时，服务器使用 NOTIFY 方法向该用户的订阅用户发送呈现信息。

7.XMPP 系统

- XMPP 协议是一种基于 XML 的即时通信协议；
- XMPP 协议的系统架构沿袭了 E-mail 系统的架构；
- XMPP 系统架构主要由 3 种实体组成：XMPP 客户、XMPP 服务器和 XMPP 网关：

① XMPP 服务器间相互通信，形成一个由 XMPP 服务器组成的分布式网络；

② XMPP 网关负责 XMPP 与非 XMPP 系统之间的互联，可以使 XMPP 客户和非 XMPP 客户进行通信；

③ XMPP 客户通过 Internet 接入 XMPP 系统，可以通过 XMPP 系统与其他客户进行通信（如果存在 XMPP 网关，XMPP 客户也可以和非 XMPP 客户进行通信）。

8.XMPP 系统特点

① 用户/服务器中转模式:XMPP 使用用户/服务器通信模式，而不是有些即时消息系统采用的用户/用户模式。从一个用户客户机端发给另一个用户客户机端的 XMPP 即时消息都必须通过服务器中转。

② 分布式网络系统:XMPP 的网络体系结构与 E-mail 系统类似，XMPP 客户和服务器组成一个分布式的网络处理系统，即时消息和呈现信息在这些 XMPP 客户和服务器之间传输。XMPP 地址和 E-mail 地址形式一样（如 stpeter®jabber,org），因此，从一个用户地址即可得知该用户所属的 XMPP 服务器。

③ 简单客户机端:XMPP 的目标之一是必须支持简单客户机端，将复杂性从用户端转移到服务器端。XMPP 系统架构要求用户端必须支持的功能：通过 TCP 套接字与 XMPP 服务器进行通信、解析组织好的 XML 信息包、理解消息数据类型。(目前 Google 的 Google Talk 和 Jive Message 都采用 XMPP 协议)。

④ XML 数据格式:XML 是 XMPP 系统的核心，几乎能表述任何一种结构化数据。

9.XMPP 协议

- 寻址方案

① XMPP 通信系统具有统一的寻址方案，XMPP 用户地址的格式必须符合 RFC2396 统一资源标识符的语法规定。

② 由于历史原因，XMPP 地址也被称为 JID（JabberID，Jab-ber 标识）。

③ JID 用于标识即时消息用户和用户连接的资源，它由域标识符、结点标识符、资源标识 3 部分组成，形如 node@domaia/resource。其中，域标识符是唯一必需的，通常表不 XMPP 服务器或 XMPP 网关，必须是一个合法的 DNS 域名；结点标识符是一个可选项，以“@”符号分割放在域标识符之前。结点标识符通常是一个使用 XMPP 服务的一个用户；资源标识符也是一个可选的标识符，表示具体的资源。资源标识符放在域标识符之后，并以“/”分隔。

- XML 流与 XML 节（Stanza）

① XMPP 是一套基于 XML 流的协议；

② XMPP 流中的“节”有 3 种类型，它们是消息（message）、呈现（presence）和查询（1/Q，Info/Query）。

③ 消息节表示传输的消息，其中消息的接收方、发送方可以使用 to、from 等关键字表明；

④ 呈现节用来表明用户的状态（如在线、离线等）。当用户的状态改变时，用户端就会在用户到服务器的流中插入一个呈现节，用于表明自身的状态；

⑤ 查询节是一种请求/响应机制。一个实体发送请求，另外一个实体接收请求并进行响应。

10.即时通信实例

- 腾讯 QQ、网易泡泡、新浪 UC、微软 MSN 和雅虎 Messenger 等都曾经是非常流行的即时通信软件。
- 除了实时消息交换和状态跟踪之外，即时消息系统一般还提供一些附加功能，如音频/视频聊天、应用共享、文件传输、文件共享、游戏邀请、远程助理、白板等。

11.QQ 用户登录过程

① 客户端每次登陆时会访问记录上次登陆服务器的地址的记录文件，如果成功则不会重发 DNS 请求。

② 在 QQ 通信中，用户必须先登录后才可以进行互相发送信息等操作。

③ QQ 聊天通信信息是加密的，每次登陆时 QQ 客户机会向服务器获取一个会话密钥。

④ 客户端会从服务器端获得好友列表，以建立点对点的联系。

⑤ QQ 采用的通信协议以 UDP 为主，辅以 TCP 协议。

12.P2P 文件共享

- 文件共享是指用户主动地在网络上分享自己主机中的文件或者目录。
- P2P 文件共享起源于 1999 年的音乐分享网站 Napster。Napster 采用的是集中式的对等网络结构。
- eDonkey2000 继承了前者共享文件系统的优点，并为文件增加了哈希（Hash）信息。
- 最初的 BT 系统需要中心服务器存放用户的信息，该服务器被称为 Tracker 服务器。
- BT 系统要求文件的发布者制作一个被称为“种子”文件的.torrent 文件，该文件包含了 Tracker 服务器的相关信息和发布者共享文件的信息。
- 下载者通过发布者提供的种子文件连接到 Tracker 服务器，并通过 Tracker 服务器获取其他下载者（包括发布者）的 IP 地址和端口号。
- 下载的人越多，BT 系统提供的带宽越大，下载速度也就越快。在后续的版本中，BT系统加入了 DHT的支持，以实现无 Tracker服务器的文件传输。
- 在 20 世纪 60 年代，美国著名社会心理学家米尔格伦（Stanley Milgram）提出了“六度分隔（Six Degrees of Separation）”理论。这就是著名的“小世界假设”。六度分隔理论为 P2P 文件共享系统中的结点的快速发现和资源快速发现提供了理论基础。

13.文件共享实现方式

- 如 FTP 文件共享、NFS 网络文件系统共享、Windows 共享文件夹以及正在流行的 P2P 文件共享等。
- 在 FTP 文件共享中，用户将需要共享的文件传送到 FTP 服务器，其他用户使用该文件时需要通过 FTP 服务器进行下载；
- 在 NFS 网络文件系统中，用户可以将自己主机上的文件或目录共享出来，其他用户需要使用时，只需将该文件或目录挂接在自己的文件系统下，像使用本地文件一样使用远程主机上的文件；
- Windows 共享文件夹是微软针对 Windows 系统开发的文件共享机制，它通常使用 NetBIOS 和 NetBEUI 协议将文件夹共享给其他用户使用。
- NetBIOS 是由微软公司开发，工作于网络层驱动接口和传输层驱动接口之间，支持 254 个并发通信话路，名字服务可以采用 UDP 协议。

14.Maze 系统

- Maze 系统是一个功能非常强大的 P2P 文件共享系统，属于混合式的 P2P 网络系统。
- Maze 系统参考了 Kerberos 协议，采用了分布式认证机制。
- 为了促使用户更多地共享资源，Maze系统采用了 Maze 积点和 Maze星级技术。

- 该系统采用了以六度分隔理论为基础的网络链接关系，能够支持在线资源搜索和文件目录视图，可以进行多点下载和断点续传，支持跨防火墙的文件共享与下载。
- Maze 系统中的用户被称为 Peer,每个 Peer 相当于一个传统 FTP 服务器与一个 FTP 客户端的结合体。整个系统除了多个 Peer 外，还包括集中式的用户管理服务器、文件目录服务器、索引和检索服务器、心跳服务器。

① 用户管理服务器实现用户注册与身份认证；

② 文件目录服务器负责收集每个 Peer 共享的目录列表并将它们存入集中式的目录数据库；

③ 索引和检索服务器读取目录数据库中的数据，为所有共享文件目录建立索引并提供 XML 方式的检索接口；

④ 心跳服务器负责维护在线用户的列表。

15.互联网协议电视（IPTV）

- 用户可以采用两种方式使用 IPTV 服务，一种是计算机方式，另一种是网络机顶盒加普通电视机方式。
- 电视类服务是与电视业务相关的服务，如视频点播、直播电视和时移电视等；
- 通信类服务是指基于 IP 的语音服务、即时通信服务和电视短信服务等；
- 增值服务是指电视购物、互动广告和在线游戏等增值类服务。

16.视频点播（Video on Demand，VOD）

- 视频点播（Video on Demand，VOD）也被称为交互式电视点播系统。
- 本质上讲，VOD 是一种基于 IP 网络的利用机顶盒作为接收终端，电视机作为显示设备的视频点播系统。

17.VOD 的服务类型

VOD 的服务类型分为 3种：

1） 就近式点播电视 NVOD:在支持就近式点播电视系统中，每个视频流间隔一定的时间就发送同样的内容，用户选择距最近的某个时间起点进行收看。

2） 真实点播电视 TVOD:真实点播电视支持即点即放,每个视频流只为一个特定的用户服务。

3） 交互式点播电视 IVOD:交互式点播电视不仅可以支持即点即放，而且还可以让用户对视频流进行交互式的控制。

18.媒体内容分发技术

- 媒体内容分发网络（Media Content Delivery Network，MCDN）技术是 IPTV 大规模应用的重要技术保障。
- MCDN 关键技术包含以下几个方面。

① 内容发布:借助于索引、缓存、流分裂和组播等技术，将内容发布或投递到距离用户最近的远程服务点处。

② 内容路由：是整体性的网络负载均衡技术。内容路由技术通过内容路由器中的重定向以及媒体位置注册机制，在多个远程服务点上均衡用户的请求，保证用户请求得到最近内容源的响应。

③ 内容交换:根据内容的可用性、服务器的可用性以及用户的背景，利用应用层交换、流分裂、重定向及宽带媒体分发策略等技术，智能地平衡负载流量。

④ 性能管理:通过内部和外部监控系统，获取网络部件的状态信息。同时，性能管理还测量内容发布的端到端性能（如包丢失率、延时时间、平均带宽、启动时间和帧速率等），保证网络处于最佳的运行状态。

⑤ IP 承载网：MCDN 充分利用高速交换、汇聚层路由转发、接入层带宽保障、组播路由及服务质量等 IP 网络技术，为 IPTV 应用提供可靠 IP 网络平台。

19.VOIP 可以实现的通信方式

- VoIP（VoiceoverIP）也称为 IP电话，是利用 IP网络实现语音通信的一种通信手段，是基于IP网络的语音传输技术。
- VoIP 系统可以将源用户的电话语音数字化，通过压缩、打包后利用 IP 网络传输给目的用户。
- 目的用户收到数据包后，将数据解压并还原成声音。
- 利用VOIP可以实现的通信方式包括：PC-to-PC,PC-to-Phone,Phone-to-Phone,PC-to-Pad,Pad-to-Phone，PC到IP网关，IP网关到 IP网关。

20.VoIP 系统组成

VoIP 系统有 4 个基本组件，它们是终端设备（Terminal）、IP 电话网关（Gateway）、网守（Gatekeeper）和多点控制单元（MultipointControlUnit,MCU）

1） 终端设备

● 终端设备是直接和用户接触的设备。VoIP 中的终端设备有多种类型，其中包括传统的语音电话终端、ISDN 终端、多媒体 PC 等。

2） IP 电话网关

● IP 电话网关是 VoIP 系统的关键设备，是 IP 网络和电话网络之间的桥梁。

IP 电话网关的基本功能如下：

① 号码查询

② 建立通信连接

③ 信号调制

④ 信号压缩和解压

⑤ 路由寻址

3） 网守

● 网守是一个中央控制实体，在 VoIP 系统中起管理作用。

● 网守是 VoIP 系统中的消息控制中心，可以进行呼叫控制、地址解析、呼叫授权、身份验证、集中账务和计费管理、存留呼叫详细记录等操作。

● 同时，网守还可以像实时网管一样监控网络、平衡负载、管理带宽以及提供与现有系统的接口。

4） 多点控制单元

● 多点控制单元 MCU 的功能在于利用 IP 网络实现多点通信，使得 VoIP 系统能够支持 3 个或 3 个以上端点参与的多点会议。

● MCU 通常由两部分组成，分别是多点控制器（Multipoint Controller,MC）和多点处理器（Multipoint Processor，MP）。

● MC 主要负责呼叫信令的处理和会议的控制；

● MP 则提供多点会议中媒体流的集中处理，主要负责混音、交换等处理工作。

21.RTCP 报文

根据所携带的控制信息不同，RTCP 报文分为 5 种类型，分别是 SR、RR、SEDS、BYE 和 APP。

● SR（sender report，发送者报告）：该类型报文中含有活动端的发送和接收统计信息。

● RR（receiver report，接收者报告）：该类型报文中含有非活动端的接收统计信息。

● SDES（source description items,源描述项）：该类型报文中含有对数据源的描述信息。例如，数据源的 CNAME 和 SSRC 的映射关系等。

● BYE（goodbye,离开报告）：参与者结束通信时使用该类型报文通知其他参与者。

● APP（application-specificfunctions，特定应用）：用于特定应用功能的一类 RTCP 报文。

22.Skype

● Skype 融合了当前热门的两大技术——VoIP 技术和 P2P 技术，主要提供 IP 网络电话、即时消息、文件传输、用户搜寻等功能。

● Skype 还能有效地突破防火墙的限制。

① SkypeClient：SkypeClient 是 Skype 系统的客户机端，简称为 SC。

② SuperNode:SkypeNode 是 Skype 系统中的超级结点，简称为 SN。在 Skype 系统中，Super-Nodc 是动态生成的，其作用就像 Internet 中的核心路由器。

③ LoginServer:LoginServer 是 Skype 系统中的登录服务器，简称为 LS。LS 登录服务器存储着用户的用户名和密码，负责用户登录时的合法性认证。同时，它还要负责用户名的全局唯一性管理。

④ HostCache 简称为 HC，是一个 SN 的 IP 地址和端口对的列表。它由 SC 建立，并会经常更新。

⑤ BaddyList:BaddyList 是一个用户的好友列表。

⑥ Encryption:加密处理。Skype 采用了 256 位的 AES 加密算法。同时，Skype 采用 1536～2048 位的 RSA 算法对 AES 使用的对称密钥进行协商。

⑦ Codecs:编码方式。Skype 米用了 GloballPSounci 公司的宽带编码技术 iLBC 和 iSAC。这两种编码技术允许频率在 50~8000Hz 的语音通过。

⑧ Port:Skype 系统采用的端口。SC 可以使用 TCP 和 UDP 进行端口监听，这些端口值在 SC 的连接对话框设置。在安装客户机端软件时，SC 会随机选择一个端口号。除此之外，SC 也可以在 HTTP 的 80 端口和 HTTPS 的 443 端口进行监听。

⑨ NAT/FirewalhSC 采用各种 STUN 和 TURN 技术来判定它在哪种类型的 NAT 和防火墙之后，以便进行 NAT 或防火墙穿越。

23.Skype 的特点

1） 高清晰音质:从理论上说，使用 Skype 可以听到人类可以听到的所有声音频率，而普通电话只能听到 300~3000Hz 以内的声音。较宽的频率范围保证了高保真度的声音品质。

2） 高度保密性:Skype 终端之间传送的声音和消息都是经过加密处理的。Skype 采用 AES 加密算法，密钥长度为 256 位，是 AES 可选密钥长度里最长的（因此也是最安全）。AES 的会话密钥利用 2048 位的 RSA 算法生成，可以确保密钥的安全性。同时，用户登录时，系统会利用用户的私钥进行身份验证。

3） 免费多方通话:Skype 支持最多 5 人的多方会议呼叫，而且所有的通话都采用端到端加密。因此，Skype 比较适宜于商务会谈和其他会谈。

4） 跨平台：Skype 提供不同操作系统下的发行版本，包括 Windows、Linux 以及 MacOS 等。

24.搜索引擎组成

搜索引擎构成一般都由 4 个部分组成，即搜索器、索引器、检索器和用户接口。

- 搜索器

搜索器通过逐个访问 Internet中的 Web站点来采集 Web网页信息，并建立该站点的关键字列表。人们常把搜索器建立关键字列表的过程称为网络爬行。

- 索引器

索引器的功能是理解搜索器所搜索的信息，从中抽取出索引项，用于表示文档以及生成文档库的索引表。

- 检索器

检索器的功能是根据用户的查询要求在索引库中快速检出文档，进行文档与查询的相关度评价，对将要输出的结果进行排序。同时，检索器还应具有某种用户相关性反馈机制。

- 用户接口

① 用户接口的作用是输入用户查询、显示查询结果、提供用户相关性反馈机制。

② 用户输入接口可以分为简单接口和复杂接口两种：

③ 简单接口只提供用户输入查询词的文本框;

④ 复杂接口可让用户对查询进行限制，如逻辑运算（与、或、非等）、相近关系（相邻、NEAR等域名范围（.edu.com等）、出现位置（标题、内容等）、信息时间、长度等。

25.LAMP 网站架构

- LAMP 网站架构是目前国际流行的 Web 框架，该框架包括：Linux 操作系统，Apache 网络服务器，MySQL 数据库，Perl、PHP 或者 Python 编程语言，所有组成产品均是开源软件，是国际上成熟的架构框架。
- 该架构起源于 Linux 平台，由于是开源软件，建设成本很低。

26.IPSec

- IPSec 是为网络层提供安全的一组协议。
- 在 IPSec 协议族中有两个主要的协议：身份认证头（AH）协议和封装安全负载（ESP）协议。
- SA（安全协定）定义的逻辑连接是一个单工连接，也就是说，连接是单向的。SA 是由一个 3 元组确定的。
- ESP 头部采用 32 位顺序号字段组成。

第六章 网络管理与网络安全

1.网络管理

- 在网络管理中，一般采用网络管理者-网管代理模型。管理者实质上是运行在计算机操作系统之上的一组应用程序，代理位于被管理的设备内部。
- 一个管理者可以和多个代理之间进行信息交换。
- 网络管理一般采用集中式网络管理或者分布式网络管理。
- 集中式网络管理模式和分布式网络管理模式是网络系统在发展过程中自然形成的两种管理模式，它们各有特点，适用于不同的网络系统结构和不同的应用程序。

2.网络管理资源分类

分为硬件资源和软件资源。

- 硬件资源是指物理介质、计算机设备和网络互联资源。物理介质通常是物理层设备、如网卡、双绞线等；计算机设备包括打印机和存储设备及其他计算机外围设备。常用的网络互联设备有中继器、网桥、路由器、网关等；
- 软件资源主要包括操作系统、应用软件和通信软件。

3.网络安全管理作用

采用多层防卫手段，将受到侵扰和破坏的概率降到最低、提供迅速检测非法使用和非法入侵初始点的手段，核查跟踪入侵者的活动、提供恢复被破坏的数据和系统的手段，尽量降低损失和提供查获入侵者的手段。

4.网络故障管理

网络故障管理包括检测故障、隔离故障和纠正故障 3 个方面，应包括典型的功能有维护并检测错误日志、接收错误检测报告并作出响应、跟踪与辨认错误、执行诊断测试、纠正错误。

5.网络管理的目标

- 网络管理目标是通过合理的网络配置与安全策略，保证网络安全、可靠、连续与正常运行，当网络出现异常时及时响应并排除故障；通过网络状态监控、资源统计与性能分析，对网络做出及时调整与扩充，以便优化网络性能 。

6.网管模型

国际标准化组织（ISO）定义的网管模型包括 4 个部分：组织模型、信息模型、通信模型与功能模型。

- 组织模型描述网管系统的组成部分与结构；
- 信息模型描述网管系统的对象命名与结构；
- 通信模型描述网管系统使用的网管协议；
- 功能模型描述网管系统的主要功能。

7.网管功能域

- 网络管理功能模型就是常说的网管功能域。
- 网管功能域定义的是主要的网管功能，并将这些功能划分为 5 个部分：

① 配置管理（Configuration Management）
② 故障管理（Fault Management）
③ 性能管理（Performance Management）
④ 安全管理（Security Management）
⑤ 记账管理（Accounting Management）

1） 配置管理

- 配置管理用于实现网络设备的配置与管理，主要是网络设备参数与设备之间的连接关系。
- 配置管理的主要内容包括:标识网络中的被管对象（表示网络设备），识别网络拓扑结构（生成拓扑图），修改设备配置（工作参数、连接关系）。

2） 故障管理

- 故障管理用于发现与解决网络中的故障，目的是保证网络连续、可靠地运行并提供服务。
- 故障管理的主要内容包括：故障检测（通过轮询机制或告警信息），故障记录（生成故障事件、告警信息或日志），故障诊断（通过诊断测试或故障跟踪），故障恢复（通过设备更换、维修或启用冗余设备）。

3） 性能管理

- 性能管理用于测试网络运行中的性能指标；
- 目的是检验网络服务是否达到预定水平，找出已发生的问题或潜在的瓶颈，通过数据分析与统计来建立性能分析模型，以便预先报告网络性能的变化趋势，并为网管决策提供必要的依据。
- 性能参数包括网络的吞吐率、利用率、响应时间、传输延时等。
- 性能管理可分为两个部分:性能监控与网络控制。其中，性能监控是指收集网络状态信息，网络控

制是指为改善性能采取的措施。

4） 安全管理

- 安全管理用于保护网络中的资源的安全，以及网管系统自身的安全性。
- 安全管理的主要内容包括:控制与维护对网络资源的网管访问权限，安全服务设施的建立、控制与删除，与安全措施有关的信息分发，与安全有关的事件通知，与安全有关的网络操作的记录、维护与查阅等，以及网络防病毒等。

5） 记账管理

- 记账管理用于监视与记录用户对网络资源的使用，以及计算网络运行成本与用户应交费用
- 记账管理的主要内容包括：统计网络资源使用情况（通信量、利用率等），确定计费方法（采用包月、计时、按流量等），计算用户账单（根据资源、时段、费率等），分析网络运营成本与资费变更影响等。

8.网络管理系统（NMS）

- 网络管理系统通常简称网管系统，它是用来实现网管功能的软件或硬件系统。
- 从逻辑结构上来看，网管系统通常包括 3 个部分:管理对象、管理进程与管理协议

① 管理对象（Managed Object）是经过抽象的网络元素，对应于网络中具体可以操作的数据；

② 管理进程（Management Process）是负责对网络设备进行管理与监控的软件，它安装在网络中的网管工作站与各种网络设备中。

③ 管理协议（Management Protocol）负责在网管工作站与网络设备的管理进程之间通信，传输信息包括发送的操作命令与返回的操作结果。

9.SNMP 协 议

- 1987 年，IETF 制定了简单网关监控协议（Simple Gateway Monitoring Protocol，SGMP）。SGMP 是一种监控网关或路由器的协议，SNMP 协议在 SGMP 的基础上发展起来。

① 1989 年，IETF 制定 SNMP 第一个版本（snmpv1），它是一种设计简单、易于实现的协议，但没有考虑安全问题；

② 1993 年，IETF 制定 SNMP 第二个版本（snmpv2），增加了操作类型与支持多种传输层协议，在提高安全性和更有效性地传递管理信息方面加以改进，具体包括提供验证、加密和时间同步机制；

③ 1998 年，IETF 制定 SNMP 第 3 个版本（snmpv3），提供了安全性与改进的框架结构。

- SNMP 是一种应用层的网络协议，面向 Internet 的网管协议。
- SNMP 在传输层采用支持无连接服务的 UDP 协议，在传输管理信息之前不需要建立连接。
- SNMP 协议采用轮询监控方式，管理器定时向代理请求获得管理信息，并根据返回信息判断是否发生异常。
- SNMP 是 TCP/IP 协议族中的重要协议，它的成功与 TCP/IP 协议是分不开的。

10.CMIP 协 议

- ISO 制定的是通用管理信息服务（Common Management Information Service，CMIS）与通用管理信息协议（Common Management Information Protocol,CMIP）。
- CMIP 是基于 OSI 模型的网络管理协议，致力于解决异构互联网络中的网络管理问题。
- CMIS/CMIP建立在 OSI模型的基础上，两者共同提供通用的网管服务。
- CMIP协议负责实现具体的网管操作，这些操作需使用 CMIS定义的各种服务原语。
- CMIP是一种应用层的网络协议。
- CMIP系统包括两个组成部分:CMIP客户机与服务器。
- CMIP协议采用委托监控的方式，管理者只需向代理发送监控请求，代理将会自动监视指定的管理对象，并在异常事件发生时向管理者告警。这种监控方式的特点是开销小、反应快。

11.网络安全服务基本功能

网络安全服务应该提供以下基本保障。

1） 可用性

可用性是指，尽管存在可能的突发事件（例如停电、自然灾害、事故或攻击等）情况下，网络仍然可处于正常运转状态，用户可使用各种网络服务。

2） 机密性

机密性是指，保证网络中的数据不被非法截获或被非授权访问，保护敏感数据和涉及个入隐私信息的安全。

3） 完整性

完整性是指，保证数据在网络中传输、存储的完整，数据没有被修改、插入或删除。

4） 不可否认性

不可否认性是指，确认通信参与者的身份真实性，防止对已发送或已接收的信息否认现象的出现。

5） 可控性

可控性是指，能够控制与限定网络用户对主机系统、网络服务与网络信息资源的访问和使用，防止非授权用户读取、写入、删除数据。

12.可信计算机系统评估准则（TESEC）

- 美国国防部公布了《可信计算机系统评估准则》TCSEC，将计算机系统的安全可信度从低到高分为 D、C、B、A 四类共七个级别：D 级，C1 级，C2 级，B1 级，B2 级，B3 级，A1 级。
- （最小保护）D 级：该级的计算机系统除了物理上的安全设施外没有任何安全措施，任何入只要启动系统就可以访问系统的资源和数据，如 DOS，Windows 的低版本和 DBASE 均是这一类（指不符合安全要求的系统，不能在多用户环境中处理敏感信息）。
- （自主保护类）C1 级：具有自主访问控制机制、用户登录时需要进行身份鉴别。
- （自主保护类）C2 级：具有审计和验证机制（(对 TCB）可信计算机基进行建立和维护操作，防止外部入员修改）。如多用户的 UNIX 和 ORACLE 等系统大多具有 C 类的安全设施。
- （强制安全保护类）B1 级：引入强制访问控制机制，能够对主体和客体的安全标记进行管理。
- B2 级：具有形式化的安全模型，着重强调实际评价的手段，能够对隐通道进行限制。（主要是对存储隐通道）
- B3 级：具有硬件支持的安全域分离措施，从而保证安全域中软件和硬件的完整性，提供可信通道。对时间隐通道的限制。
- A1 级：要求对安全模型作形式化的证明，对隐通道作形式化的分析，有可靠的发行安装过程。（其安全功能，依次后面包含前面的）

13.信息传输安全

信息传输安全是指保证信息在网络传输过程中不被泄露、篡改与伪造。

- 截获信息。信息从源结点开始传输，中途被攻击者非法截获，目的结点没有接收到该信息，因而造成信息在传输途中丢失。
- 窃听信息。信息从源结点传输到目的结点，但是中途被攻击者非法窃听。
- 篡改信息。信息从源结点传输到目的结点的途中被攻击者非法截获，攻击者修改信息或插入欺骗性的信息，并将篡改后的信息发送给目的结点。
- 伪造信息。在这种情况下，源结点并没有信息要传送到目的结点。攻击者冒充源结点用户，将伪造的信息发送给目的结点。

14.网络攻击的分类

网络攻击可以有两种分类方法：主动攻击与被动攻击、服务攻击与非服务攻击。

1） 主动攻击与被动攻击

- 被动攻击主要以收集信息为目的，信息的合法用户难以察觉这种活动，例如嗅探、漏洞扫描、信息收集等。
- 主动攻击不但进入对方系统搜集信息，同时要进行破坏活动，例如拒绝服务、信息篡改、窃取信息、欺骗攻击等。
- 无论是主动攻击还是被动攻击，后果的严重程度有所区别，但是都是属于非法入侵的行为。

2） 服务攻击与非服务攻击

- 服务攻击是指攻击者对 E-mail、FTP、Web 或 DNS 服务器发起攻击，造成服务器工作不正常，甚至造成服务器瘫痪。
- 非服务攻击不针对某项具体应用服务，而是针对网络设备或通信线路。攻击者可能使用各种方法对网络设备（例如路由器、交换机、网关、防火墙等）与通信线路发起攻击，使得网络设备出现严重阻塞甚至瘫痪，或者造成线路阻塞，最终使网络通信中断。

15.DDoS 攻击的特征

主要有以下几点：

- 被攻击主机上可能有大量等待应答的 TCP 连接。
- 网络中充斥着大量的无用数据包，并且数据包的源地址是伪造的。
- 大量无用数据包造成网络拥塞，使得网络工作不正常，甚至瘫痪。
- 被攻击主机可能在攻击发起之后的短短几秒钟后就处于瘫痪状态。
- 攻击服务器与傀儡机都是在不知情的情况下参与攻击行动，而真正的攻击者早已消失。

16.对称加密与非对称加密

- 常用的加密技术可以分为两类：对称加密（Symmetric Cryptography）与非对称加密（Asymmetric Cryptography）。
- 在传统的对称密码系统中，加密用的密钥与解密用的密钥相同，密钥在通信中需要严格保密。
- 在非对称加密系统中，加密用的公钥与解密用的私钥不同，加密用的公钥可以向大家公开，而解

密用的私钥需要保密。

17.典型的对称加密算法

1） 数据加密标准

数据加密标准（Data Encryption Standard，DES）是最典型的对称加密算法，它是由 IBM 公同提出、经 ISO 认定的国际标准。

2） DES

DES 是一种典型的分组密码，它将数据分解成固定大小的分组，以分组为单位进行加密或解密。DES 每次处理一个 64 位的明文分组，并且每次生成一个 64 位的密文分组。DES 算法采用 64 位密钥长度，其中 8 位用于奇偶校验，用户可使用其余的 56 位。

3） 3 重 DES

3 重 DES（triple DES，3DES）是针对 DES 安全问题的改进方案。

4） 高级加密标准

- 高级加密标准（Advanced Encryption Standard，AES）是后来出现的一种对称加密算法。
- AES 将数据分解成固定大小的分组，以分组为单位进行加密或解密。
- AES 的主要参数是：分组长度、密钥长度与计算轮数。分组长度与密钥长度可以是 32 位的整数倍，范围是128～256位。AES规定分组长度为 128位，密钥长度可以为128、192或256位，根据密钥长度分别称为：AES-128、AES-192或AES-256。

5） 其他对称加密算法主要包括 IDEA、Blowfish、RC2、RC4、RC5、CAST 等。

18.公钥密码基本特征

- 公钥密码的基本特征是加密密钥与解密密钥不同，并且无法由加密密钥推导出解密密钥。
- 公钥密码技术提供了两个密钥：公钥与私钥。其中，公钥是可以公开的密钥；私钥是需要严格保密的密钥。
- 公钥密码技术使用的加密与解密算法公开。公钥密码的加密与解密算法是基于数学函数，而不是像对称密码那样地基于位模式的简单操作。
- 公钥密码的出现对保密性、密钥分发与认证等都有深远的影响。

19.公钥密码的应用领域

公钥密码技术	主要应用领域
RSA	数据加密、数字签名与密钥交换
EGG	数据加密、数字签名与密钥交换
DSS	数字签名
ElGamal	数字签名
Diffie-Heilman	密钥交换

20.典型的非对称加密算法

1） RSA

- 1977年，Ron Rivest、Adi Shamir与Leonard Adleman 设计了一种加密算法，并用3 人的姓氏首字母命名该算法。
- RSA 的理论基础是寻找大素数相对容易，而分解两个大素数的积在计算上不可行。
- RSA 算法的安全性建立在大素数分解极其困难的基础上。

2） 椭圆曲线密码（ECC）

- 1985 年，椭圆曲线密码由 Neal Koblitz 和 Victor Miller 分别提出；
- 其安全性建立在求解椭圆曲线离散对数的困难性上。
- 在同等密钥长度的情况下，ECC 算法的安全性要远高于 RSA 算法等。

3） 其他非对称加密算法主要包括 DSS、ElGamal 与 Diffie-Hellman 等。

21.公钥基础设施（PKI）

- PKI 是利用公钥加密和数字签名技术建立的安全服务基础设施，以保证网络环境中数据的秘密性、完整性与不可抵赖性。
- PKI 是一种针对电子商务、电子政务应用，利用非对称加密体系，提供安全服务的通用性网络安全基础设施。
- PKI 系统对用户是透明的，用户获得加密和数字签名服务时，无须知道 PKI 是如何管理证书与密钥。
- PKI 建立的安全通信信任平台与密钥管理体系，能够为所有网络应用提供加密与数字签名服务，实现 PKI 系统的关键是密钥的管理。

- PKI 的主要任务是确定用户可信任的合法身份。这个信任关系是通过公钥证书来实现。公钥证书就是用户身份与所持有公钥的结合，这是由可信任的第 3 方权威机构（认证中心）来确认。

22.数字签名

- 在网络环境中，通常使用数字签名来模拟日常生活中的亲笔签名。
- 数字签名将信息发送人的身份与信息传送相结合，以保证信息在传输过程中的完整性，并提供信息发送者的身份认证，防止信息发送人抵赖行为的发生。
- 利用非对称加密（例如 RSA 算法）进行数字签名是最常用的方法。
- 非对称加密算法（例如 RSA 算法）效率比较低，并对加密的信息块长度有一定的限制。在使用非对称加密算法进行数字签名前，通常先使用单向散列函数或哈希函数（Hashing Function 签名信息进行计算，生成信息摘要，并对信息摘要进行签名。
- 目前，广泛应用的数字签名算法是消息摘要（Message Digest5,MD5）。它是 Rivest 于 1994 年发表的一种单向散列算法，可对任意长度的数据生成 128 位的散列值，也叫作不可逆指纹。
- MD5 算法没有对数据进行加密或修改，只是生成一个用于判断数据完整性与真实性的散列值。
- 因此，利用数字签名可验证数据在传输过程中是否被篡改，同时确认发送放的身份，防止信息交互中的抵赖现象发生。

23.TCP/IP 协议安全机制

- 在主机-网络层（数据链路层对应它的一部分）中，主要的安全协议包括 PPTP、L2TP 与 UF 等。
- 在互联层（或网络层）中，最主要的安全机制是 IPSec 的两个组成协议，即认证头部（AH）与封装安全有效载荷（ESP）。
- 在传输层中，主要的安全协议包括 SSL、SSH 与 SOCKS 等。
- 在应用层中，针对不同网络服务或应用的安全机制比较多，例如用于增强 Web 安全的 S-HTTP、用于保障邮件安全的 S/MIME、用于电子商务安全交易的 SET 等。
- S/MIME 主要支持功能有：加密的数据、签名的数据、透明签名的数据、签名并加密的数据。

24.IPSec

- IPSec 主要包括 3 个组成部分：认证头（Authentication Header,AH）、封装安全负载（Encapsulating Security Payload，ESP）与密钥管理协议。
- 其中，AH 协议可提供数据源身份认证、数据完整性认证，以及可选的抗重放数据包功能；
- ESP 协议可提供 AH 协议的所有功能与数据加密服务；
- 密钥管理协议用于通信双方之间协商安全参数，例如工作模式、认证或加密算法、密钥与生存期等。
- 实际上，AH 与 ESP 协议都是网络层的安全协议，而密钥管理协议是应用层的安全协议。

25.安全套接层（SSL）协议

- SSL 协议使用非对称加密体制和数字证书技术，可保护信息传输的秘密性和完整性。SSL 是国际上最早应用于电子商务的一种网络安全协议。
- 同期，Microsoft 公司开发了类似的 PCT 协议。鉴于 SSL 与 PCT 不兼容的现状，IETF 发布了传输层协议（Transport Layer Security，TLS），希望推动传输层安全协议的标准化。

26.SSL 协议特点

- SSL 可用于 HTTP、FTP、TELNET 等，但是目前主要应用于 HTTP 协议，为基于 Web 服务的各种网络应用中的客户机与服务器之间的用户身份认证与安全数据传输提供服务。
- SSL 处于端系统的应用层与传输层之间，在 TCP 之上建立一个加密的安全通道，为 TCP 协议的数据传输提供安全保障。
- 当 HTTP 协议使用 SSL 时，HTTP 请求、应答报文格式与处理方法不变。不同之处在于：应用进程产生的报文通过 SSL 加密后，再通过 TCP 连接传输；在接收方的 TCP 软件将加密的报文传送给 SSL 解密后，再发送给应用层的 HTTP 协议。
- 当 Web 系统采用 SSL 时，Web 服务器的默认端口号从 80 变换为 443，Web 浏览器使用 https 代替常用的 http。
- SSL 主要包含两个协议：SSL 握手协议（SSL Handshake Protocol）与 SSL 记录协议（SSL Record Protocol），SSL 握手协议实现双方的加密算法协商与密钥传递；SSL 记录协议定义 SSL 数据传输格式，实现对数据的加密与解密操作。

27.PGP 协议

- PGP 协议于 1995 年开发，包括电子邮件的加密、身份认证、数字签名等安全功能。
- PGP 用来保证数据在传输过程中的安全，它的设计思想与数字信封是一致的。
- PGP 数字签名能够保证邮件的完整性、身份认证与不可抵赖性，数据加密可以保证邮件内容的机密性。

- 它主要由 5 种服务组成：鉴别、机密性、压缩、电子邮件的兼容性和分段，支持多语种安装平台。
- 数字签名使用 DSS/SHA 或 RSA/SHA 算法，报文加密采用 CAST 或 IDEA，或使用 Diffie-Hellman 的 3DES 或 RSA 算法。
- PGP 也提供了公共密钥认证机制，但是这个机制完全不同于通用的认证中心（CA）。PGP 公共密钥通过委托网站进行认证，它也可以通过互联网上的 PGP 公共密钥服务器发布。

28.电子支付安全（SET）协议

- 电子商务是以 Internet 环境为基础，在计算机系统支持下进行的商务活动。
- 电子商务是基于浏览器/Web 服务器工作模式，实现网上购物和在线支付的一种新型商业运营模式。
- SET 使用了对称加密与非对称加密体系，以及数字信封、数字签名、信息摘要技术与双重签名技术，以保证信息在 Web 环境中传输和处理的安全性。

29.防火墙主要功能

- 检查所有从外部网络进入内部网络的数据包。
- 检查所有从内部网络流出到外部网络的数据包。
- 执行安全策略，限制所有不符合安全策略要求的数据包通过。
- 具有防攻击能力，保证自身安全性的能力。

30.网络防火墙构成

常用防火墙有 3 种：包过滤路由器、应用级网关和电路级网关。

1） 包过滤路由器

- 包过滤路由器依据一套规则对收到的 IP 包进行处理，决定是转发还是丢弃。
- 包过滤路由器也称为屏蔽路由器（Screening Router），它是被保护的内部网络与外部网络之间的第一道防线。
- 包过滤规则通常基于部分或全部报头内容。
- 路由器按照设置的分组过滤规则（即访问控制表），检查每个分组的源地址、目的地址，决定该分组是否应该转发。例如，对于 TCP 报头信息，可以是源地址、目的地址、协议类型、IP 选项、源端口号、目的端口号、TCPACK 标识等。
- 包过滤路由器只工作于传输层也可以工作于应用层。
- 应用级网关也叫代理服务器，它在应用级的通信中扮演着一个消息传递者的角色。应用级网关不足之处在于它在每次连接中有多余的处理开销，处理数据时开销较大。
- 电路级网关不允许一个端到端的直接 TCP 连接。

31.入侵检测系统的基本功能

① 监控、分析用户和系统的行为；
② 检查系统的配置和漏洞；
③ 评估重要的系统和数据文件的完整性；
④ 对异常行为的统计分析，识别攻击类型，并向网络管理入员报警；
⑤ 对操作系统进行审计、跟踪管理，识别违反授权的用户活动；

32.网络蠕虫

- 网络蠕虫的权威定义是:一种无须用户干预、依靠自身复制能力、自动通过网络进行传播的恶意代码。
- 具有以下几个特点：冲击力度大，已导致很多部门的网络遭到严重破坏；大量通过垃圾邮件群发，利用系统漏洞快速传播。

33.蠕虫和病毒的区别

主要表现在以下几个方面：

- 蠕虫是独立的程序，而病毒是寄生到其他程序中的一段程序。
- 蠕虫是通过漏洞进行传播，而病毒是通过复制自身到宿主文件来实现传播。
- 蠕虫感染计算机，而病毒感染的是文件系统。
- 蠕虫会造成网络拥塞甚至瘫痪，而病毒破坏计算机的文件系统。
- 防范蠕虫可通过及时修复漏洞的方法，而防治病毒需要依靠杀毒软件来查杀。

34.认证中心（Certification Authority，CA）

- 为了解决公共密钥可能会遭受第 3方的主动攻击，在实际当中引入了一个可信媒介----认证中心。
- 认证中心（Certification Authority，CA）验证一个公共密钥是否属于一个特殊实体。
- 认证中心负责将公共密钥和特定实体进行绑定，它的工作是证明身份的真实性和发放证书，
- 国际电信联盟（ITU）和 IETF 制定了认证中心的标准。

- CA 具有以下作用：

① CA 验证实体（个入、路由器等）的身份。

② 一旦 CA 验证了实体的身份，CA 就可以产生一个证书，将这个公共密钥和身份进行绑定。

35.信息存储安全措施

信息存储安全措施至少要包括 3 类：

① 社会的法律政策、企业的规章制度及网络安全教育；

② 技术方面的措施，如防火墙技术、防病毒、信息加密、身份确认以及授权即设置访问权限等；

③ 审计与管理措施，包括技术与社会措施。主要有实时监控、提供安全策略改变的能力以及对安全系统实施漏洞检查等。

36.Caesar 密码加密

- Caesar 密码加密方法为，对每一个字母用它之后的第 3 个字母来代换，明文空间和密文空间都是 26 个英文字母的集合。
- Caesar 密钥取值范围为 1-25，最大的可能取值是 25。

37.密文攻击

- 唯密文攻击指的是在仅知已加密文字的情况下进行穷举攻击。
- 已知明文攻击指攻击者掌握了某段明文和对应密文，推断加密方式，从而破解后段密文的攻击方式。
- 选择明文攻击是指攻击者不仅已知加密算法和密文，而且还能够通过某种方式让发送者在发送的信息中插入一段由他选择的信息。
- 选择密文攻击的密码分析者事先任意搜集一定数量的密文，让这些密文透过被攻击的加密算法解密，透过未知的密钥获得解密后的明文。

38.背包加密算法

背包加密算法是一种公钥加密算法，该算法中背包的物品总重量是公开的，所有可能的物品也是公开的，但是背包中的物品却是保密的，它是一个 NP 难度问题。目前大多数一次背包体制均被破译了，一次背包已不安全了。

39.Blowfish 算法

- Blowfish 算法是由 Bruce Schneier 设计的一种对称分组密码；
- Blowfish 是一个可变密钥长度的分组密码算法，分组长度为 64 位；
- Blowfish 算法所有的运算都是 32 位字的加法和异或，仅有的另一个运算是每轮的四个查表。

40.RC5 算法

- RC5 算法是 Ron Rivest 设计的一种堆成加密算法，它是参数可变的分组密码算法；
- 3 个可变的参数是：分组大小、密钥大小和加密轮数。
- 在此算法中使用了 3 种运算：异或、加和循环。

41.X.509 公共密钥证书

- 在 X.509 公共密钥证书中，主题名是实体的身份，其公钥与证书相关，以 DN 格式表示；
- 版本字段是 X.509 说明书的版本号；
- 合法时期表示证书有效期的起止时间；
- 发行者名是签发证书CA身份，以 DN格式[RFC-2253]表示。

42.数字版权管理

数字版权管理主要采用的技术为数字水印、版权保护、数字签名和数据加密。