**操作系统原理**

**一、操作系统概述**

1.操作系统

（1）概念：是计算机系统的一个**系统软件**，能有效地组织和管理计算机系统中的硬件和软件资源，**合理（公平对待不同用户程序，不发生“死锁”和“饥饿”）**组织计算机工作流程，控制程序的执行，并向用户提供各种服务功能，使用户能灵活、方便、有效地使用计算机，并**使整个计算机系统高效运行（高效使用计算机）**；位于硬件之上，支撑软件（软件的编制和维护）之下。

数据结构可动态更新

A.应用角度看主要作用：提供人机交互接口（提供给用户的接口是命令输入和系统调用）；

B.软件开发角度看作用：软件开发的基础平台；

C.安全保护角度看作用：第一道安全防线；

D.系统发展角度看作用：虚拟机和扩展机

（2）特性

A.并发性：执行期间具有相互制约关系；程序与计算不再一一对应；结果不再现并发过程失去封闭性；（**宏同微交**）

B.共享性：CPU、内外存储器、外部设备；（磁带机投影仪扫描仪为独占设备）

同时共享：硬盘、可重入代码 互斥共享：临界区、中断服务

C.随机性（异步性）：不能对运行程序及硬件设备的情况作出假定；何时退出？假死？中断？关机？重启？

（3）功能：

A.进程管理：对CPU进行管理。包括进程控制（创建、撤销结束进程以及控制运行时候的各种状态转换）、进程同步（处理进程之间同步或互斥关系）、进程间通信（信息交换）和进程调度（按照一定算法从就绪队列中挑选一个进程让CPU执行它）；

B.存储管理：管理计算机内存资源。包括回收与分配内存、存储保护（考虑程序可能发生越界的情况）和内存扩充（借助虚拟技术在逻辑上增加进程运行空间）；

C.文件管理：文件存储空间的管理（管理/创建/删除/命名文件）；文件目录管理；文件系统的安全性（读写和存取权限）

D.设备管理：除CPU和内存之外的所有输入输入设备，复杂外部设备分配和故障处理。技术包括：中断技术、通道技术、虚拟设备技术和缓冲技术。

E.用户接口（作业管理）：

（4）常见的操作系统：Ubuntu、Windows、Unix、DOS、BSD、Android（基于Linux移动应用支持网络）

2.操作系统分类：

按页面使用环境和功能特征

（1）**批处理系统BAT**：分单道批处理系统和多道批处理系统，其中多道批处理**效率**和吞吐量较高但缺少人机交互性；指令有特权指令和一般指令；成批处理、资源利用率高

（2）**分时系统**：多路性（多用户共同）、交互使用系统；**独占性**（用户感觉）；及时性

（3）**实时系统**：多路性，及时性，交互性，**可靠性，有过载防护能力**

按计算机体系结构分类：

（1）个人操作系统

（2）网络操作系统：主从关系明显；有限制共享资源；

（3）分布式操作系统：统一配置，所有主机使用一个操作系统；资源共享；相互通信；透明性：自治性（地位平等）：可靠性

（4）嵌入式操作系统：成本低

交互式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，并通过交互方式在终端上向用户显示结果。**多级反馈、时间片轮转和高优先级适用于交互式操作系统**。

3.操作系统结构：

（1）整体式结构：功能划分成多模块；

（2）层次式结构：单向调用，同层不调用；

（3）微内核结构（C/S结构）：将大多数的操作系统由用户进程实现；分割成多个部分，每一部分只处理一方面的功能，如文件服务、进程服务与服务器通信；特点：高可靠性、高灵活性、**适合分布式处理**、可移植性强、融入面向对象技术，但效率低，不适合频繁通信；微内核具备：线程调度、虚拟存储、消息传递、设备驱动、内核原语操作以及中断处理（屏蔽中断）。

4.指令：

（1）特权指令：包括输出指令、停机指令等，只有在监控程序才能执行特权指令，**只能在内核状态（管态）下运行**（屏蔽中断、关闭中断）；

（2）一般指令：**用户态下运行**（关机、读文件、设置时间），**管态下也可以执行**。如果用户程序在用户态（目态）执行特权指令，则引起**访管中断**，这也是CPU由用户态向核心态转换的方法。

5.

（1）临界资源：

（2）可重写入代码：硬盘，内存；

（3）不可重用资源：时间片到时、硬件时钟到时

6.三类接口可供用户使用：

（1）命令接口：提供一组命令供用户间接/直接操作；

（2）**程序调用（系统调用）**：一组**系统调用**命令组成，是操作系统提供给编程人员唯一接口，调用命令供用户程序使用；（用户编程需要打印输出，提供指令：write()）

Open()文件操作类系统调用fork()进程控制类系统调用

（3）图像界面接口（图标和菜单）：图标、**菜单、窗口**，形成一个直观易懂，使用方便的计算机操作环境，**终端窗口采用命令行**。

7.设备分配算法中，数据结构主要包含四个表分配顺序是：**系统设备表（SDT）、设备控制表（DCT）、控制器控制表（COCT）、通道控制表（CHCT）**。

8.程序状态字（PSW，专门的寄存器指示处理器状态）

（1）包含：CPU工作状态码（指明管/目态）；条件码（指令结果）；终端屏蔽码（是否允许中断）；

（2）状态标志：CF（有进位）、ZF（为零）、SF（符号）、OF（溢出）、TF（陷阱）、IF（中断屏蔽）、VIF（虚拟中断）、VIP（虚拟自断待决）、IOPL（IO特权级别）

9.研究操作系统观点：软件的观点、资源管理观点、进程观点、虚拟机观点、服务提供者观点

10.文件权限：

二进制：000 000 000

文件所有者 同组用户 其他用户

各部分转换为十进制后其含义：0 无权限

1 X执行

2 W写入

4 r读取

**二、操作系统运行机制**

1.CPU中的存储器

（1）用户可见寄存器：主要用于各种算术逻辑指令和访问指令（数据寄存器、地址寄存器、条件码寄存器）

（2）控制和状态寄存器：用于控制处理器的操作（程序计数器PC、指令寄存器IR、程序状态寄存器PSW）

2.中断与异常的分类

（1）中断：（外部事件引起的）时钟中断；输入输出中断（键盘输入）；控制台中断；硬件故障中断；网卡上数据区满（数据传输完成）；（堆栈溢出）；（被0除）

（2）异常：（内部事件引起的）程序性中断（执行指令产生的结果）；访管指令中断（被清零）；

3.系统调用

（1）概念：运行在用户态（CPU在用户程序中执行）被调用程序在系统态（CPU在系统程序中执行）；系统调用可嵌套使用，即一个被调用过程执行期间还可以调用另一个，一般可多次调用但不能无限制调用；

（2）分类：进程控制类（创建/终止进程）、文件操作（打开）、进程通信类、设备管理类（请求/释放设备）、信息维护类（时间日期）；

（3）参数传递：由陷入指令自带参数（只能携带几个）；通过寄存器传递参数（内存开辟专门的堆栈传递参数）；

（4）一般调用在，被调用过程执行结束后，会直接返回调用程序；系统调用在结束调用，首先会对所要求的进程进行优先级分析，若调用进程不具备高优先级则会产生重新调度；

**三、进程线程模型**

1.多道程序环境特点：独立性；随机性（输入输出都是随机的）；资源共享（导致执行速度制约）。

2.进程

（1）概念：计算机**程序（指令、数据组成）**关于**数据**集合上的一次运行**活动**，是资源分配的基本单位；

（2）特点：并行性；独立性（独立资源分配单元）；异步性（不可预知速度的向前推行）；动态性；交往性。

（3）组成：PCB、指令和数据三部分组成；

（4）进程控制块（PCB）

A.组成：进程名、进程号、存储信息、进程标识符、**进程优先级、进程当前状态**、资源清单、**消息队列指针、进程队列指针**、打开当前文件等**调度信息**和PSW、时钟、界地址寄存器等**现场信息**；

B.组织方式：线性方式、索引方式、链接方式、队列方式（就绪队列、等待队列、运行队列）；

C.特征：是进程的灵魂；**必须常驻内存；**PCB的运行状态只可以通过操作系统读取。

（5）进程控制：通过原语实现对进程在整个生命周期中各种状态间的转换；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。

（6）创建进程：

A.步骤：申请空白PCB；为新进程分配资源；初始化PCB；**将新进程插入就绪队列末尾**。

B.创建进程的时机：用户登录；系统初始化；用户系统调用；初始化批处理作业。

3.进程状态及转换

（1）三状态模型：运行状态、就绪状态、等待状态（阻塞状态）。

其中**运行状态转换到就绪状态**有3种可能性：时间片用完；进程创建完成；**被调度程序强占CPU**（对于非强制式是：“**一个进程运行结束**”）；

**运行状态转换阻塞状态**：请求系统服务、启动某种操作、新数据尚未到达、无新工作可做。

（2）五状态模型：运行、就绪、阻塞、创建、结束。

Linux上进程有五种状态：运行、中断、不可中断、僵尸状态、停止状态。

（3）七状态模型；运行、就绪、阻塞、创建、结束、激活（外->内）、挂起（内->外）。

4.线程

（1）概念：进程中的实体，不能独立于进程存在；是CPU调度和分派的基本单位；不同的线程可以执行相同的程序；同一进程中各线程共享内存空间；自己不拥有系统资源，只拥有一点运行中必不可少的资源；每个线程有一个标识符和一张线程描述表，记录了线程执行的**寄存器和用户栈**等现场；

（2）特点：花费开销少、切换花费时间少、内部通信快、能独立工作；

（3）线程操作含义：

pthread\_join：等待一个特定的线程退出；pthread\_yield：线程让出CPU（主动释放）；

pthread\_creat：创建线程库函数； pthread\_exit：结束一个线程的库函数

5.CPU调度分类：高级调度（创建进程）、中级调度（调入内存）、低级调度（分配CPU）。

6.调度

（1）功能：记录系统中所有进程执行状态；从就绪队列中选出一个CPU分配给它；选中PCB有关现场信息（PSW、通用寄存器等）送往CPU的寄存器中，让他占用执行。

（2）时机：CPU资源让出来不一定调度，CPU资源占用一定不调度；可强占方式（当优先级高的进程运行存在时，立即进行调度，转让CPU资源）与不可强占方式（进程执行完毕才释放CPU）。

（3）调度算法：**先来先服务FCFS**（**不可强占**）；**最短时间作业算法**SJF；**轮转法RR**；**最高响应比优先算法**HRRF（介于FCFS与SJF之间的折中算法，即考虑等待时间又不使长作业等待时间过长）；多级反馈队列。**操作系统不能在运行中动态改变进程调度算法。**

**四、存储管理方案**

1.进程互斥的解决办法：竞争各方平等协商；引入进程管理者

2.计算机中资源共享的程序可分为三个层次：

（1）互斥；利用硬件解决的互斥方法简单、支持多个临界区、适用范围广；不能实现“让权等待”；

（2）死锁：

（3）饥饿：

3.临界资源分成四个部分：

（1）进入区：（P原语）；while TS(&lock)

（2）临界区：访问临界资源的一段代码；n=fetch(balance)

（3）退出区：（V原语）lock=FLASE

（4）剩余区：代码其余的部分output(list)

4.进程同步机制应遵循的准则：空闲则入、忙则等待、有限等待、让权等待。

5.信号量

（1）**只能通过初始化**和**两个标准的原语**来访问；

（2）**初始化可指定一个非负整数值**，表示空闲资源总数；若为**负值，其绝对值表示当前等待临界区的进程数**；P(empty) V(full)

（3）同步：信息量empty，初始值K；信号量full，初始值0

互斥：信号量mutex，初始值为1.（占用为1空闲为0）

（4）系统直接通信时，发送原语：**send(receiver,message)**

6.管程

（1）定义了一个数据结构和能为并发进程所执行的一组操作。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什么的过程中直接访问管程数据结构；管程能保障共享资源互斥执行；是一种同步机制；将共享变量及对共享变量的操作封装在一起

（2）任一时刻中，管程中只有一个活跃进程；所有临界区转换成管程，则只许一个进程使用临界区内代码。管程本身无法保证互斥；

（3）管程对象：共享的数据结构和一组操作过程。

（4）为解决进程同步关系，引入条件变量，在条件变量上实施P、V操作；

7.进程间的通信

（1）**共享内存**：用于多个进程**并发执行且相互通信**，适合传输大量信息；设置一个公共内存区，一组向其中写，一组从公共内存读；**不需要在系统中产生多份相同的拷贝。**

（2）**消息机制**：利用内存中若干缓存区组织成**队列**，依赖进程或基础框架来调用实际执行的代码；缓冲区中包括：消息缓冲区、消息指针、互斥信息量、同步信息量、发送和接收原语。

（3）**管道通信**：通过两个进程，打开一个共享文件，实现进程间的通信；字符流形式联系，不足**是通信速度较慢**。

（4）信箱通信：发送进程首先创建一个链接两个进程的通信机制，然后把向信息送入该机制；发送进程和接受进程不直接联系，接收进程可以在任何时刻从该机制中取出信息。

8.**PV操作可以实现两个进程互斥、进程同步和进程前趋关系**；PV同步机制缺点：可读性差、不利于修改和维护、正确性差；P操作一次减一，V操作一次加一。

9.可以实现进程互斥的算法：Peterson算法、TS指令、Swap或Exchange命令、信号量；

10.进程之间的关系有：

相互感知 交互关系 一个进程对其他进程的影响 潜在控制问题

相互不感知 竞争 两进程的结果无影响 互斥、死锁、饥饿

直接感知 通信协作 一个进程依赖其他进程 死锁、饥饿

间接感知 共享协作 一个进程依赖其他进程 互斥、死锁、饥饿

11.地址重定位：将逻辑地址转换成绝对地址；动态重定位（每条指令执行时；需要软件硬件相互配合实现，其中硬件包括基址寄存器和一个地址转换线路组成）和静态重定位（程序执行前已转换好地址）。

12.内存管理

（1）单一用户管理：一个时间内，一个用户进程独占内存；

（2）**分区管理**：固定分区；可变分区（**空闲分区策略**：**最先适应算法、最优适应算法、最坏适应算法、下次适应算法**）；可以满足多道程序设计且设计上最简单；内存使用不充分、较为严重碎片、不能提供虚拟内存、受物理内存不足限制。

利用**移动技术**，可以实现碎片整合；利用**交换技术**，在**磁盘上保存**内存放不下的**进程（代码、PCB和数据**），需要时再装入内存中，是由操作系统控制。

（3）**页式管理**：把一个逻辑地址连续分散存放到几个不连续的内存区域。不要求作业或进程的程序段和数据在内存中连续存放，从而有效解决“碎片”多的问题；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，提高了存储空间利用率；页面大小可以改变但用户不可以动态改变页面大小。通常管理空闲物理内存的方法有：空闲块链表法、位示图、空闲页面表。

A.空闲块的分配和回收：采用主存分配表、位示图和页表方式；页表中，存储块号与页号一一对应，一级页表共需访问内存2次完成数据提取；二级页表每执行一条指令至少需要访问3次内存；

B.快表（TLB）存放在高速缓存（介于主存和CPU之间的存储器，高速缓存器与内存之间信息调度和传送是通过硬件完成的）中；页式虚拟存储管理，部分页在内存中，其余在外存中（磁盘文件区），需要用到：请求调用页和预调页策略。

C.置换策略有：固定分配局部置换、可变分配全局置换、可变分配局部置换；（固定/可变指：块数是否可变；局部/全局：指作业以内或外）

D.页面置换算法：

FIFO：会出现Belady现象，随着分配给进程的物理页面增加，缺页率增加；

**LRU：最近最久未使用算法，需要记录访问位；**

LFU：最近最不经常使用算法，当前时间访问次数最少，需要访问计数器；

NRU：最近未使用页面置换算法，**需要记录访问位**；

CLOCK：时钟算法，**需要记录访问位**；

理想页面置换算法

（4）**段氏管理**：存储以段划分；

（5）**段页式管理**：先分段、再分页、每页对应块、可连续可不连续存储。

**其中，页式、段氏式和段页式管理可以与虚拟存储技术结合使用。**

13.链接：提高检索速度、节省存储空间的软链接，把所有编译后得到的目标模块连接装配起来，再与函数库想连接成一个整体的过程。

14.虚拟页面存储管理

（1）存在问题：页面抖动、Belady现象、缺页中断、**页面写错误**。

（2）解决办法：采用工作集算法可以缓解页面抖动（操作系统为每一个进程保持一个工作集，工作集随时间而变化，每个进程提供与工作集大小相等的物理界面）

（3）需要的硬件支持：足够大内外存；虚拟地址到物理地址映射机制；缺页中断处理机制。

15.碎片：

（1）内碎片：分配出内存，没有得到利用。固定分区、页式、段页式

（2）外碎片：内存空间无法满足分配要求。可变分区、虚拟段式。

16.进程中断，选中一个页面进行淘汰时，只需将页面移除，修改页面有效位，其余标志位不变；

当创建一个新进程，装入一个页面，对应页表项中的：内存号、驻留位、访问位需要修改；

当页面被修改时，需要修改的位：访问位、修改位；

将页面调入内存，需要修改位：内存号、驻留位、访问位。

17.虚拟存储器

（1）在虚拟存储系统中，进程的部分程序装入后便可运行；

（2）虚拟存储技术允许用户使用比物理内存更大的存储空间；

（3）虚拟内存必须有硬件支持。

18.程序的局部性分空间局部性和时间局部性，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。

**五、文件系统设计与实现技术**

1.文件分类

（1）按用途分：系统文件、用户文件、库函数文件；

（2）按**组织形式：普通文件、目录文件、特殊文件**（Unix中I/O设备被视为特殊文件）；

（3）保护方式：只读文件、读写文件、可执行文件、无保护文件；

（4）存放实限分类：临时文件、永久文件、档案文件；

（5）组织结构：逻辑文件（用户可见；**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）、物理文件（存放在磁盘上：顺序文件、链式文件、索引文件）

2.文件物理结构：即文件存储的结构；顺序结构、链接结构、索引结构；

存储介质 磁带 磁盘

物理结构 连续结构 **连续** 链接 **索引（多级索引）**

存取结构 顺序 顺序 顺序 顺序

**随机** **随机**

3.磁盘

（1）寻访时间：寻道时间（最长）、延迟时间、传输时间（最短）；

（2）磁盘调度：FCFS、SSTF（最短寻道时间，容易引起饥饿现象）、SCAN（电梯算法，来回服务）、C-SCAN（循环扫描，单向）

4.文件目录：实现按名存取，包含文件名和文件的起始地址，用以建立文件名（<255字符）与存储地址的对应关系；必须信息：FCB、文件结构信息和文件管理信息。

（1）FCB包含：文件名、文件号、用户名、文件物理地址、文件长度、口令、修改/访问/建立时间；

（2）管理形式分：一级目录、二级目录、树型目录（搜索快；层次清楚；解决不用用户文件重命名问题；用户不可以创建根目录）

（3）路径名搜索：全路径名和相对路径（加快搜索速度）；

5.存储空间的**分配与回收（文件存储空间的管理方法）**：位示图、空闲块表、空闲链表、**成组链接表（UNIX）**。

6.文件系统

（1）优化：块高速缓存；合理分配磁盘时间；磁盘驱动调度；目录项分解；

（2）FAT：是文件分配表；链接结构；FAT16表示16位簇号，支持8个字符文件名；

（3）安全：建立副本、定时转存、规定文件的存取权限。

（4）文件存储空间：分配单位数据块；

（5）从用户角度：建立文件系统的目标是实现“按名存取”；

从系统角度：看文件系统主要关注文件存储位置；

7.打开文件时，系统要完成的：

（1）根据文件名查找目录，找到FCB；（打开文件第一步，继续open()操作，将FCB写入内存）

（2）根据打开方式，共享说明和用户身份检查，访问合格性；

（3）根据文件号，打开文件表，看文件是否被打开；

（4）在用户打开文件中取一空表项，填写打开方式等，并指向系统打开文件表对应的表项；

8.物理结构：是文件的逻辑块到磁盘号的转换；

9.外存储存取过程：读状态-->置数据->置地址->置控制->读状态

10.创建文件操作过程：检查文件名是否合法；同目录下是否重名；目录中是否有空闲位置；填写目录项内容（文件名、用户名、存取权限、长度置零、首地址）；

11.文件描述符：内核利用文件描述符来访问文件。文件描述符是非负整数，打开现存文件或新建文件时，内核会返回一个文件描述符，读写文件也需要使用文件描述符来指定待读写的文件。实际上，它是一个索引值，指向[内核](https://baike.baidu.com/item/%E5%86%85%E6%A0%B8)为每一个进程所维护的该进程打开文件的记录表。当程序打开一个现有文件或者创建一个新文件时，内核向进程返回一个文件描述符。

12.对文件的操作：

（1）关闭文件操作：系统根据用户提供的文件名/文件标识符查找FCB；在该FCB的相关内容做修改；置FCB为“非活跃”；写回磁盘。

（2）删除文件操作：查找文件；检查删除合法性；收回FCB资源；收回文件存储空间。

（3）访问文件：首次访问时通常访问文件路径名，之后对文件访问通常使用文件描述符。

**六、I/O设备管理**

1.设备分类

（1）按共享属性：独占设备、共享设备（磁盘）、虚拟设备；

（2）按信息组织方式分类：块设备（磁盘/磁带，一般512B-4KB）；字符设备（键盘、显示器、打印机）；

2.I/O硬件：CPU和主存（中央部分）；接口；外围设备控制器（内有寄存器）；外围设备

3.I/O设备数据传输控制方式：

（1）**程序直接控制方式**：“忙-等待”

（2）**中断控制方式**：实现了主机和外围设备的并行工作；CPU是不是会跑去看数据是否可以输入输出；适用于**键盘以字符为单位读取**方式；关键硬件中断控制器、地址总线和数据总线、设备控制器；

（3）**DMA**：对输入/输出设备由DMA完成，在DMA控制器的作用下，设备和主存之间可以批量进行数据交换，而不用CPU干预；“窃取”总线控制权；适用于**对块设备的存取**；DMA控制器、地址总线和数据总线；

（4）**通道控制方式**：工作在内存中；实现外围设备的统一管理和外围设备与内存之间的数据传输；所需CPU干预更少；可以实现CPU、通道和输入输出设备三者之间的并行操作；适用于现代计算机内的大量数据交换；主要限于与**I/O操作有关的指令**和程序；通道控制器、地址总线、数据总线、设备控制器和通道程序代码；分数据选择通道、字节多路通道和数组多路通道。

4.I/O软件分层：中断处理程序（设备硬件）；设备驱动程序；与设备无关的系统软件（设备独立层）；用户控件的I/O软件（用户层）

5.设备无关层实现功能（提供一致的系统调用）

（1）统一命名：实现逻辑设备命名与物理设备的转换；

（2）设备保护；

（3）缓冲：对不同速度的设备使用缓冲区来匹配；

（4）提供与设备无关的逻辑块；

（5）独占设备的分配和释放；

（6）出错处理：向用户报告出错处理情况；

（7）存储设备的块分配。

6.I/O设备管理

（1）设备表：建立逻辑设备与物理设备之间的对应关系；

（2）设备管理任务：缓冲区管理、设备分配（需要考虑：设备固有属性；设备分配算法；设备分配安全性；设备独立性）、设备处理、虚拟设备以及实现设备独立。

（3）引入技术：缓冲技术、设备分配技术、SPLOOING技术、DMA技术、通道技术。

（4）缓冲池管理：实现进程访问缓冲区同步。

7.**SPOOLING组成**：**输入井和输出井**、**输入进程和输出进程**、**输入缓冲区和输出缓存区**。

**七、死锁**

1.死锁：在对资源的管理、分配和使用不当，会产生死锁现象；

（1）产生原因：竞争资源；进程推进顺序不合理。（**没有“调度不合理”的原因**）

（2）产生**必要条件**：互斥条件（**资源互斥使用**）；不可剥夺条件（**已分配资源不可剥夺**）；请求和保持条件（申请占有一部分资源，继续占用已分配的资源，**部分分配资源**）；循环等待条件（前一个进程拥有后一个进程所请求的资源，**资源申请形成环路**）；

（3）进入阻塞状态，无法被唤醒。

2.饥饿：当等待时间进程推迟和响应带来明显影响时；

3.活锁：“忙等待式”，没有阻塞，可被调动，但无进展（不主动放弃CPU）；

饥饿：“阻塞状态”，没有阻塞，但被无限推后，（主动放弃CPU）；

4.解决死锁方法

（1）预防死锁：“资源有序分配法”；SPOOLing系统的建立；一次分配所有资源；剥夺其他进程的资源。（**静态分配，分配时加锁**）

（2）避免死锁：银行家算法；

（3）死锁检测：定时运行资源分析程序；

（4）剥夺资源法、撤销进程法和重启。

5.几种死锁类型：

（1）同类资源死锁：“P1申请一页内存，P2申请一页资源…….”；

（2）不同类资源死锁：“P1拥有设备A请求设备B，P2拥有设备B请求A”；

（3）PV操作互斥死锁：“P1、P2先进行同步信号量P操作，再进行互斥信号量P操作”；

（4）临时资源死锁：“P1等待P2发来信件Q后向P2发送信件R，P2等待P1发来信件R后向P1发送信件Q”。

**计算机网络**

**一、网络技术基础**

1.网络分类：

（1）宽带城域网（MAN）：双环光纤传输；FDDI；（2）无线局域网（WLAN）；（3）无线自组网（Ad hoc）（自组织；对等；无线网络）；（4）无线传感网（WSN）：Ad hoc与传感器技术结合；（5）无线网状网（WMN）：用于扩大范围；对Wimax和WLAN的补充

2.操作系统

（1）Unix操作系统：小型机、C语言（第一版本由汇编语言编译）、部分开源；集中式、多用户，多任务，分时操作系统；贝尔公司开发；

I**BM—AIX SUN公司—Solaris HP—HP-UN**

（2）Linux操作系统：继承了Unix以网络为核心的设计，核心部分：内核；开源操作系统；版本很多；由不同组织管理维护；不是Unix操作系统的变种。

**Red Hat**

（3）Windows NT是微软公司开发的闭源系统；采用32位操作系统，可以提供全面的网络服务功能；基于不对等结构，分Windows NT Sever和Windows NT Workstation。

3.拓扑结构

（1）环型拓扑：传输延时确定；

（2）网状拓扑：广域网普遍使用；

4.数据报方式和虚拟电路方式

（1）数据报方式（分组存储转发）：同一报文不同分组可以通过不同的传输路径；不同分组可能会出现乱序、重复和丢弃现象；分组均携带源地址和目的地址；延迟大，不适宜报文会话式；

（2）虚电路方式：传输之前在源节点和目的节点之间建立逻辑连接；每个结点可以与任意结点建立多条虚电路连接，不需要路由选择；一次通信所有分组通过虚电路顺序传输，分组不需要携带目的地址和源地址等信息；结点只进行纠错。

5.网络体系结构

（1）ISO建立的OSI（开放系统互联）模型：

A.物理层（透明传输比特流）、数据链路层（MAC&LLC）、网络层（选择路由**IPSec**）、传输层（端到端服务）、会话层、表示层（加密/解密）、应用层（提供应用进程交换和远程操作）；

（2）TCP/IP模型：IETF制定的

A.主机-网络层、**互联层（IP/ARP/ICMP）、传输层（TCP\UDP）、**

**应用层**（FTP\HTTP\RIP\NFS\SMTP\Telnet\**SNMP\CIMP**\**PGP\S/MIME**\）

B.开放式网络协议标准；与网络硬件无关；每一层服务上一层

6.计算机网络：以能够相互**共享资源**方式互联起来的**自治**计算机系统集合。

7.**ARPANET**：Internet的始祖，是世界范围内的广域网，是世界上开发的第一个运营的封包交换网络（分组交换网络技术），是**美国国防部高级研究计划局**研究的网络。

**二、局域网技术**

1.局域网三要素：

（1）网络拓扑：总线型、环型、星型；

（2）传输介质：双绞线、同轴电缆（最早）、光纤和无线信道；

（3）介质访问：按照介质访问控制方式分为**共享介质**和**交换局域网**。其中：

共享介质（总线型局域网：利用CSMA/CD避免冲突；环型局域网：利用令牌环控制冲突）

2. IEEE 802

（1）对象：OSI的**物理层和数据链路层**。专门从事**局域网**的标准化工作。（不同局域网中，MAC和物理层可以不同，LLC（介质访问控制层）必须相同）

（2）分类：

802.3：定义CSMA/CD**总线型**介质访问MAC和物理层标准（**以太网标准**）；

802.4：定义令牌环网的协议标准；

802.11：无线局域网标准；

802.15：无线个人区域网介质访问MAC和物理层标准；

802.16：宽带无线局域网。

3.共享以太网

（1）概念：核心是集线器；ALOHA网络是基础；总线型局域网；核心技术：CSMA/CD；

（2）帧结构：

**间导码7B 帧前定界符1B|目的地址6B源地址6B类型2B|数据46-1500B校验位4B（CRC）**

（接收同步，不计帧头） （帧头；类型：网络层协议） （帧长64-1518B）

（3）以太网物理地址：长度48位，十六进制，两两一组，共6组；前三组生产公司，后三组生产商分配流水号，可分配地址2^47，第一位1则为组/广播；为0才可以分配给生产商。

4.高速局域网标准（MAC层与原标准兼容，仅定义物理层标准）

（1）802.3u：Fast Ethernet，百兆以太网；

（2）**802.3z**：Gigabit Ethernet，千兆以太网，定义多模光纤或屏蔽双绞线；

802.3ab：Gigabit Ethernet，千兆以太网，定义单模光纤或非屏蔽双绞线；

采用GMII分隔物理层和MAC层；与传统以太网的帧格式一致；

（3）802.3ae:10Gigabit Ethernet，万兆以太网，使用光纤传输，只有全双工模式，不存在介质访问控制，传输距离不受冲突检测的限制。

（4）802.3ba：40/100Gigabit Ethernet（40Gbps网络使用波分复用技术，100GPS物理接口类型）

5.**交换式局域网**

（1）概念：典型的是交换式以太网，核心设备：以太网交换机（专用/共享端口）；可以在**多个端口**之间建立多个并发连接，实现多结点之间的并发连接，

（2）帧转发方式：**直接交换**；**存储转发**；**改进直接交换**（接收一帧前64B，检测由主机进行）；

（3）**虚拟局域网（VLAN）**组网方式：用交换机**端口定义**；MAC**地址定义**；基于**网络层地址（IP）**定义；基于**广播组**定义。

6.无线局域网

（1）按物理层传输方式分类：**红外、直接序列扩频、跳频广播、微波**；

（2）红外无线局域网IR、跳频扩频FSSS（将频带划分为多个信道，使用2.5GHZ的ISM频段）、直接序列扩频DSSS（所有接受结果使用相同频段通信）、窄带微波无线局域网。

（3）802.11定义的两种访问方式：**无争用服务、争用服务**；MAC层采用CSMA/CA避免冲突；支持AP访问模式和漫游访问模式；802.11管理帧为**探测帧和认证帧**；采用层次结构模型；**MAC层主要功能是对无线环境的访问控制；物理层定义了红外、调频扩频与直接序列扩频的数据传输标准。**

（4）802.11协议族：

802.11a: 5HZ 54M

802.11b: 2.4HZ **11M**（跳频）

**802.11g: 2.4HZ 54M**

802.11n: 5G 100M

（5）网络结构为：端站（有无线网卡的用户结点）、接入点（AP）、接入控制器（AC在WLAN与外部网络之间充当网关作用）、AAA服务器（计费、认证、授权；802.11认证有三种：基于IEEE 802.1x的认证、基于PPoE的认证和基于Web的认证）

6. 1000BASE-SX:多模光纤 1000BASE-CX:屏蔽双绞线

1000BASE-LX:单模光纤 1000BASE-T:非屏蔽双绞线

100BASE-FX:单/多模光纤

7.不能够通信的原因：不在一个虚拟子网中；不在一个子网中。

8.总线局域网的特点：所有结点都通过网卡连接到作为公共介质的总线上，通常采用双绞线或同轴电缆作为传输介质；所有的结点都可以发送或接收数据，但在一段时间内只允许一个结点通过总线发送数据（即半双工形式）；当一个结点通过总线以“广播”方式数据时，其他结点只能以“收听”方式接收数据；由于总线作为公共传输介质被多结点共享，因此会出现冲突现象。

**三、Internet基础**

1.互联网构成：通信线路（基础设备）、**路由器**（主要设备，**主要功能：维护路由表信息；转发IP数据报；选择最佳路径**）、**主机**（信息资源和服务的载体）和**信息资源。IP协议是Internet中的主要协议。**

2.**Internet的接入方式**：

（1）电话线接入；

（2）ADSL接入：使用电话线路，完成非对称数据用户线路，ADSL调制解调器：具备网桥、路由器和调制解调的功能；

（3）HFC接入：有线电视网接入（混合光纤/同轴电缆），非对称数字用户线路；

（4）数据通信线路接入：（成本高）

3.IP协议

（1）定义：**IP数据报格式、对数据寻址和路由、数据报分片和重组、差错控制和处理**等。

（2）IP服务特点：**不可靠服务；面向无连接；尽最大努力投递；（一般不随意丢弃报文）**

（3）IP网络特点：**隐藏底层物理网络细节；不制定拓扑结构，不要求网络之间全部互联；在物理网络之间转发数据，信息可以跨网传输；公平对待互联网中每一个网络；使用同一的地址描述法。**

4.IP地址（A\B\C\D\E类地址）

（1）特殊IP地址：网络地址；广播地址（直接广播/有限广播：255.255.255.255）；回送地址（127.0.0.0）；本地地址（A:10.0.0.0/8;B:172.16.0.0/12;C:192.168.0.0/16）

（2）若要发送广播：源地址是本机，目的地址：网络号不变，主机号全为1.

5.地址解析协议ARP

（1）工作在互联层，能够实现IP到MAC的解析；

（2）工作原理：以广播形式发送请求报文（ARP请求），单播响应；

（3）通过高速缓存技术避免大量请求报文出现，提高有效性；拥有计时器的目的是保证主机ARP表的正确性。

6.**IP数据报格式**

（1）组成：报头区和数据区；

（2）数据报各字段及其功能：版本和协议类型；长度；服务类型；生存周期；头部校验和域（保证报头完整性，没有数据区校验字）；

（3）报头长度：32bit双字节为单位；总长度以8bit字节为单位。包含与分片和重组有关：**标识（原数据是谁）、标志（是否是最后一片）**和片偏移（顺序重组）

7.IP封装、**分片**（MTU:最大传输单元，一帧携带最多能携带的数据量。）**和重组**。

8. **IP数据报选项**

（1）目的：控制和测试；

（2）选项数据：

A.源路由：严格路由（严格按照路径转发）；松散路由（规定主要路由）；

B.记录路由：记录经过的所有路由IP；

C.时间戳

9.**差错与控制**

一个ICMP报文对应一个数据报

（1）**ICMP差错控制报文**：拥塞控制（源抑制报文）、路由控制（重定向报文）；

（2）**请求/应答对：**回应请求与应答（用于测试目的主机或路由器的可达性）、时间戳请求与应答（同步时间）、掩码请求与应答；

（3）ICMP特点：**不享受优先权和不享受特别的可靠性；报告伴随丢弃；报文包含IP数据报头和数据前64比特数据**。

（4）当路由器收到IP数据报，对IP数据报进行检测，当对其首部进行校验后发现数据报存在错误时，将抛弃该数据报。

10.**路由器与选择**

（1）特殊路由：默认路由、待定主机路由（制定到达的主机）

（2）**RIP协议**（路由器信息协议）：采用**V-D算法**（距离-矢量算法），简单、中小型网络、多路径、动态IP互联网环境；距离按跳数计算；慢收敛（解决：限制路径最大距离；水平分割对策；保持策略；带触发刷新的毒性逆转对策）

（3）**OSPF协议：**采用**L-S算法**（链路-状态算法），大型网络、多路径、动态IP互联网环境；每个路由都有一个LSA，最终获得一个LSDB（链路状态数据图），收敛比V-D算法快。

11.IP组播技术：

（1）特点：使用组地址（D类地址）；动态组播地址，成员也是动态；不仅通过IP层，还与要底层硬件支持功能。

（2）相关协议：组播管理协议（IGMP,CGMP）、组播路由协议。

IGMP：Internet制定的，一方面主机通过本地路由器主动加入；一方面ICMP协议路由器会周期查询。组播路由由：源地址、组地址、入接口和出接口组成（前三个进行匹配）。

12. IPv6

（1）地址：128位（IPv4:32位）；送回地址（0:0:0:0:0:0:0:1）；

（2）数据报格式：一个基本头（固定40B）、多个扩展头和一个高层协议数据单元组成。

（3）扩展头种类：**逐跳选项报头**；目的选项报头；**路由报头**（强制数据报经过指定路由）；分片头；

13.TCP与UDP：

（1）TCP:面向对象，可靠，全双工。（使用窗口机制进行流量控制；RTT算法进行数据丢失与重发；连接端口用12位二进制表示）

（2）UDP:非面向连接，不可靠，高效率。（应用程序提供可靠性保障）

14.NAT：内外网地址翻译。分类：静态NAT、动态NAT、网络地址端口转换**NAPT**（多个内网主机共享一个全局IP地址，同时访问外部网络）

15.MTU：1500字节；一般IP首部为20字节，UDP首部为8字节，数据的净荷部分预留是1472字节；如果超出1472字节，就会出现分片现象。

**四、Internet基本服务**

1.应用进程响应并发请求分类：

（1）**重复服务器**：“先进先出”原则；

（2）**并发服务器**：每来一条请求，创建一个子进程。

2.对等计算机模型（P2P）基本结构：

（1）**集中式**（Napster，服务器通常**只存储目录**和**索引信息**）；（2）**分布式非结构化**（无中心节点；**随机图**；支持复杂查询；模糊查询；利用**TTL机制**控制**泛洪**；Gnutella）；（3）**分布式结构化**（无中心节点；采用分布式散列表**DHT**；支持精确关键字匹配查询；可扩展；维护复杂；**pastry; tapestry; chord; CAN**）；（4）**混合式结构**（**索引结点**维护**搜索结点**在**搜索用户**结点；skype; BT; pplive）

3.域名解析方式：

（1）分类：**递归解析**（一次完成）、**反复解析**（分层多次解析）；

（2）每一个域名服务器至少知道根服务器的**IP地址**及其父节点服务器的**IP服务地址**，才能解析。（**本地域名服务器IP地址**）

（3）提高域名解析的效率：解析从本地域名服务器开始；在域名服务器使用高速缓存技术；在主机上采用高速缓冲技术。

4.域名对象类型：

A—主机；MX—邮件交换；PTR—指针；CNAME—别名；SOA—授权开始；

HINFO—描述主机信息

5.远程登录中，网络虚拟终端利用**NVT格式**将不同的用户本地终端统一起来。

6.FTP服务

（1）C/S模型，利用TCP建立双向连接（一个控制连接/一个数据连接）；

（2）建立联系方式：**主动模式**（服务器主动，使用**PORT**命令将端口发送给服务器）；**被动模式**（服务器被动，向服务器发送**PASV**命令）

（3）FTP文件格式传输方式：文本文件传输（ASCII）；二进制文件传输（BINARY，不对文件格式进行任何变化，按照原始文件相同的位序以连续比特流方式进行传输）；

（4）FTP口令描述：delete—删除远程主机上的文件命令；pwd—显示远程主机的当前工作目录；

7.电子邮件系统

（1）**SMTP**：服务器之间的传递；主要目的是实现发送邮件的。

（2）POP3/IMAP：向邮件服务器进行读取（认证阶段、事务处理、更新阶段Quit）；

（3）电子邮件报文格式：RFC822、MIME.

（4）命令：PASS—用户邮件口令（认证）；STAT—查询报文总数和长度； REST—复位，删除标记，中止当前操作；NOOP—无操作（事务处理）

8.Web服务

（1）HTML：页面规范，解释单元，能够对请求和返回进行页面翻译，显示内容；

（2）HTTP：客户机和服务器之间的传输协议，建立在TCP连接上，面向对象协议，精确定义了请求/相应报文；

（3）URL：页面地址，统一资源定位器；

（4）安全性：**SSL协议**（工作在传输层协议；位于TCP/IP协议与各类应用层协议之间）（浏览器安全性）（防止第三方偷看内容；防止第三方篡改）；CA证书（Web服务器）（证明自己）

（5）浏览器组成：控制单元（解释键盘/鼠标输入命令）、客户单元、解释单元组成。Web服务器不但需要保存大量的Web页面，而且需要接受和处理浏览器的请求，实现HTTP服务器功能。Web服务器不具备编辑Web页面的功能。

9.安全性：

（1）如何保护自己的计算机：浏览器将Internet世界划分成几个区域；

（2）如何验证站点真实性：利用Web站点传来的证书；

（3）如何避免他人假冒自己：用户可以在CA安全认证中心申请自己的证书，放在浏览器中；

（4）在与Web交互敏感信息时如何避免第三方篡改或偷看：使用安全套接层技术SSL技术；

（5）保证传输机密性：将Web站点放入可信站点区可保证信息传输的机密性；

（6）防止病毒传播：使用SSL技术。

9.网络蠕虫：独立、通过漏洞传播、早期利用电子邮件传播、自我复制和主动传播；木马是没有复制能力的。

**五、新型网络应用**

1.即时通信（IM）

（1）由IMPP工作组提出；IETF批准成为正式RFC文件；有RFC2778文件描述功能；该文件未提出即使通信系统必须使用同一标准。

（2）模式：客户机/服务器；客户机/客户机

2. QQ

（1）客户机的两种聊天方式：UDP主/TCP辅；服务器中转（无法直接通信）；

（2）采用自己私有的即时通信协议；

（3）每次登陆时客户机会获得一个来自服务器的会话密钥。

3.即时通信协议（基于SIP的SIMPLE；基于JABBER的XMPP）

（1）**SIP：工作在应用层**；**IEFT提出**；可在TCP/UDP上传输；支持多种信息类型（文件、视频、图像）；用于创建、修改和释放一个或多个用户会话；**分类**（用户代理、代理服务器、重定服务器（用于规划SIP路径服务器，可与其他服务器共存一个设备中）、注册服务器）；**SIP消息组成**（起始行、消息头、一个标志消息头的空行、消息体）；SIP定义的**6种请求消息**（INVITE：邀请用户/服务器参加一个会话；ACK；OPTIONS:获取服务器相关能力；BYE:终止一次会话；CANCLE:取消挂起呼叫；REGISTER）；**SIP消息通常可分为2类**，**从客户机到服务器的请求消息**和**从服务器到客户机的响应消息**。

（2）SIMPLE：以SIP为基础，不需建立会话，支持多媒体会话；IEFT的SIMPEL工作组制定；IM消息以message命令为载体传输，每条IM由单独message命令传输，彼此独立。

（3）**XMPP：工作在应用层;基于JABBER协议**；由IEFT制定；由4个RFC文档组成；设计上延续E-mail系统；包含用户客户端、XMPP服务器、XMPP协议网管；**XML是其核心**，统一选址方案，实体地址叫做JID。

（4）基本服务：呈现服务和即时消息服务。

4.网络文件共享

（1）NFS（网络文件系统）：Linux\Windows上均可使用；与主机操作系统无关；采用C/S结构；若想远程计算B的某一个文件系统：”mount:B:/usr/lib(远程主机目录)/usr/lib(本机目录)”

（2）NFS服务器共享出来的文件或目录都记录在/etc/exports文件中。

5.Windows LAN文件共享：Windows2000以前的系统使用NetBIOS协议；以后使用CIFS协议

6.P2P文件共享

（1）P2P:起源于Napster；BT（中心服务器tracker存放用户信息；种子文件：**.torrent**，包含存储用户信息和共享文件的信息）；源于MIT开源系统；加入DHT以实现无tracker服务器的文本传输；基于“六度分隔理论”、“世界最小理论假设”、“瓦斯特领导理论”。

（2）Maze：支持即时通信；参考Kerberos机制；在线资源搜索和文件目录视图；支持多点下载和断点续传；基于积点的资源交易体系；有种子机制；分布式认证机制（类似于信用卡机制）；类似URL表示文件位置；混合型P2P系统；包括集中式的用户管理服务器（注册、登录）、目录收集服务器、检索服务器、心跳服务器和种子服务器。

（3）P2P不支持种子机制；BT系统不支持积点机制；P2P可以实现用户之间直接传输；BT后期系统能够实现无Tracker服务器的文件传输；P2P与BT相互不兼容。

5.IPTV

（1）业务种类：近式点播（NVOD，多个视频流依次间隔发送同样的内容）、真实点播电视（TVOD）和交互式点播（IVOD）;

（2）媒体内容分发（MCDN）技术组成：

A.内容发布：借助相关技术，将内容发布或投递到距离用户最近的远程服务点；

B.内容路由：网络负载均衡技术，重定向路由器以请求最近内容源响应；

C.内容交换：根据内容可用性、服务器可用性等，利用应用层交换技术，智能平衡负载流量；

D.性能管理：保证网络处于最佳状态，测量内容发布的端到端性能。

6.VOIP（基于IP网络的语音传输技术）：

（1）组成：终端设备、**网关**（号码查询、建立通信、信号调制、压缩和解压缩、路由寻址）、多点控制单元（多终端）、**网守（**中央控制实体，负责用户注册和管理；消息控制中心；确定网关地址；计费管理；留存呼叫详细记录）

（2）Skype：利用VOIP和P2P技术；混合式网络结构；AES算法作为密钥，密钥长度256bit；加密保存好友列表；支持免费多方通信；采用iLBS和iSAC编码技术；系统中SN是动态生成的；可以进行NAT穿越。

7.搜索引擎组成：搜索器、检索器、索引器、用户接口。

8.ICQ、AOL采用OSCAR通信协议。

9.网管模型：（一般采用网络管理者-网管代理模型，管理者实际是运行在计算机操作系统上的一组应用程序，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）

（1）组织模型描述网管系统的组成部分；

（2）信息模型描述网管系统的对象命名；

（3）通信模型描述网管系统的管理协议；

**六、网络管理与网络安全**

1.网络管理

（1）管理对象：物理介质、计算机设备和网络互连设备（硬件资源）；操作系统、应用软件和通信软件（软件资源）；

（2）目标：用户及运营商对网络的有效性、可靠性、开放性、综合性、安全性和经济性。（3）模型：集中式管理和分布式管理（时效好）

2.网络管理功能

（1）**配置管理**：包含两阶段：网络初次运行的初始配置管理阶段和网络正常运行的工作配置管理阶段；负责网络建设、业务展开和配置维护，达到网络性能最优；包括：设置系统中有关路由操作的参数、被管理对象的名字管理、初始化或关闭被管对象、根据要求收集系统当前状态的有关信息、获取系统重要变化信息、更改系统配置、**生成网络拓扑**。

（2）故障管理：发现和排除故障；维护和监测错误日志；接收错误响应；跟踪辨别错误；

（3）**性能管理**：计算机网络性能；**收集统计信息**；监控网络使用状况；维护网络使用状况；

（4）计费管理

（5）安全管理：对授权机制、访问控制、加密和解密关键字的管理。

3.网络管理协议：

（1）CMIS和**CMIP：**由**IOS**制定；所用功能都要映射到应用层；采用报告机制（**委托管理制）**；实施复杂且花费高；

（2）**SNMP**：**工作在应用层；IETF制定**；遵循ISO的管理模型，可以应用于**TCP/IP环境下**；**收集数据的方式有轮询**（不断收集，按顺序存储在**MIB**中，时效低）**和基于中断**（时效高，需要转发大量信息，消耗管理设备资源时间，改进：trap）两种；SNMP第一版安全性差；第二版提供验证、加密和时间同步机制，在安全性和更有效的传递管理信息方面加以改进；

4.信息安全等级

（1）美国制定（DOD5200.28-STD）：

**非安全保护类：**D（客户机系统）；**自主保护类：**C1、C2（存取控制，以用户为单位）

**强制性安全保护类：B1（标记安全保护）B2（结构化安全保护）B3（安全域机制保护）**A1

（2）中国制定：自主保护级、指导保护级、监督保护级、强制保护级、专控保护级

5.OSI安全框架（X.800）中安全攻击类型

（1）被动攻击：不更改信息，**窃听检测，内容泄漏，流量分析**（重在预防）；

（2）主动攻击：更改信息，**消息篡改，DOS攻击，消息重放，拒绝，伪装**（重在检测）；

（3）服务攻击：针对特定服务攻击；**邮件炸弹；端口攻击；分布式拒绝服务攻击**；

（4）非服务攻击：基于网络层或底层协议漏洞攻击；**源路由攻击，地址欺骗，NetXray攻击**。

6.对称密码

（1）DES：分组长度64位，分组置换，密钥长度56位；美国NIST采纳；

（2）三重DES：多个密钥对DES进行三次加密；

（3）高级加密（AES）：分组长度128，分组置换，密钥长度128,192或256位，性能不低三重DES；

（4）Blowfish算法：可变长度密钥，分组长度64；

（5）RC5：分组长度和密钥长度均变。

7.非对称密钥（公钥密码）

（1）RSA算法：发明者姓名命名；分组密码；加密强度取决于密钥长度（概率加密方法）；质数值越大，破解越难；

（2）ElGamal算法：公钥密码体制和椭圆曲线加密体系；基于离散对数；常用于数字签名；密文是明文的两倍。

（3）背包加密算法：目前一次背包不安全；

8.密钥的验证：认证中心（CA），验证实体身份；产生证书，将公钥和身份绑定；证书由CA进行数字签名；认证后公钥的发布不受限制；保管用户的公钥；

9.认证技术

（1）消息认证的方法：认证消息来源；认证信息的完整性；认证信息的序号和时间。

（2）认证模式：单向和双向；

（3）认证函数：信息加密函数；信息认证码；散列函数（Hush，消息通过散列函数生成摘要。MD5同步处理可得到128位摘要）

（4）数字签名：防止抵赖

（5）身份认证：口令认证、持证认证和生物识别；协议有Kerberos（对称密钥；TCP/IP环境下；美国麻省理工）、X.509（公钥体制；CCITT制定）

10.安全电子邮件（**应用层**）

（1）PGP：数字签名采用DSS/SHA或RSA/SHA；压缩：ZIP；兼容：64-BASE

（2）S/MIME：支持数据加密和数字签名；

11.**IPSEC：网络层**安全协议；将互联层改造为逻辑连接的层；主要有**身份认证头（AH）**协议（对于发送方提供源身份认证和数据完整性，没有提供秘密性）和**封装安全负载（ESP）**协议（提供源身份认证和数据完整性，提供了秘密性）；源主机与网络主机进行握手并建立网络逻辑连接，该逻辑通道成为安全协议（SA）；**SA定义的逻辑连接是单工的，三元组**。

12.防火墙分类：

（1）包过滤路由器：根据IP数据包进行处理，决定转发或丢弃；

（2）应用级网关：代理服务器；

（3）电路级网关：不允许端到端直接TCP连接；

（4）堡垒主机。

13.公钥加密和数字签名技术建立的安全基础设施为：PKI

14.密钥分发中心（KDI）：是一个独立的可信的服务器；对称密钥；知道每个用户的密文，可一次性方法密钥，与客户通过密文传输。

15.安全电子交易协议SET是一种应用于Internet环境下，以信用卡为基础的安全电子交付协议，它给出了一套电子交易的过程规范。通过SET协议可以实现电子商务交易中的加密、认证、密钥管理机制等，保证了在Internet上使用信用卡进行电子购物的安全。主要目的是解决信用卡电子付款的安全保障性问题，这包括：保证信息的机密性、保证信息安全传输、不被窃听，只有收件人才能得到和解密信息。（常用于电子商务应用中；防止交易数据被篡改；需要认证中心的支持；验证交易双方的身份）