全国计算机技术与软件专业技术资格(水平)考试

2004 年下半年 网络工程师 上午试卷

为了满足广大学员及网友的强烈要求，现特定编制 2004 年下半年网络工程师试题详解。

●内存按字节编址，地址从 A4000H 到 CBFFFH，共有__(1)__个字节。若用存储容量为 32K×8bit 的存储芯片构成该内存，至少需要__(2)__片。（操作系统->存储地址计算）

(1)A.80K B.96K C.160K D.192K

(2)A.2 B.5 C.8 D.10

解答：CBFFFH-A4000H＝27FFFH 将 16 进制换算为 10 进制为

$2*16^4+7*16^3+15*16^2+15*16+15=163839$

163839/1024=160K

160K/32K=5

答案:（1）C、（2）B。

●中断响应时间是指__(3)__。（硬件知识->中断处理）

(3)A.从中断处理开始到中断处理结束所用的时间

B.从发出中断请求到中断处理结束所用的时间

C.从发出中断请求到进入中断处理所用的时间

D.从中断处理结束到再次中断请求的时间

解答：中断响应时间是从中断请求到中断处理，注意指的是响应时间

答案：C

相关知识点：计算机必须能够对微处理器外面发生的事情作出响应。例如，当按动键盘上一个按键，或时钟的报时信号来到，或软盘驱动器工作完毕发出中断信号时，均将引起微处理器的注意并处理相应事件，这就是中断。

中断的作用：

① 能充分发挥处理机的使用效率：因为输入输出设备可以用中断的方式同 CPU 通讯，报告其完成 CPU 所要求的数据传输的情况和问题，这样可以免除 CPU 不断地查询和等待，从而大大提高处理机的效率。

② 提高系统的实时处理能力：因为具有较高实时处理要求的设备，可以通过中断方式请求及时处理，从而使处理机立即运行该设备的处理程序（也是该中断处理程序）。

中断信号：发生某个事件时发出的信号

中断处理程序：处理中断信号所指示的那个工作程序

中断源（中断事件）：引起中断的那个事件

中断码：

中断信号是发送给中央处理机并要求它处理的，但处理机又如何发现中断信号呢？为

此，处理机的控制部件中增设一个能检测中断的机构，称为中断扫描机构。通常在每条指令执行周期内的最后时刻扫描中断寄存器，询问是否有中断信号到来。若无中断信号，就继续执行下一条指令。若有中断到来，则中断硬件将该中断触发器内容按规定的编码送入程序状态字 PSW 的相应位（IBM 中是 16~31 位），称为中断码。

中断的类别：

① 硬件故障中断(不可屏蔽中断)：电源故障中断

② 输入/输出中断：键盘、计时器、显示器、磁盘 I/O 中断

③ 程序性中断：除法错误中断，溢出中断，还包括：断点中断、单点中断(调试用)

④ 外部中断：对 CPU 而言，它的外部非通道式装置所引起的中断。如：时钟中断，操作员控制台中断，多机系统中 CPU 到 CPU 通讯中断

⑤ 软中断（访管中断）：用户程序和操作系统之间只有一个相通的“ 门户 ”，这就是访管指令，如利用 INT n 中断指令（SVC）发生的中断，可以实现对 OS 功能的访问(调用)。

这五类中断又可按中断方式不同划为：

①自愿中断：是正在运行的程序的期待的事件，这种事件是由于执行了一条访管指令而引起的。(只有访管中断是它自愿)

②强迫性中断：是由随机事件引起的，并非由程序设计人员事先安排的。

中断进入：

中断允许

CPU 响应后

保护现场(主要是标志位) PSW 入栈

保护断点(现行的代码段寄存器 CS 和指令计数 IP) 入栈

处理机从外部设备获悉中断类型，然后就把相应的表中项目送入 IP 与 CS

返回：

如果中断例行程序执行时可能改变某些寄存器的值，那么中断例行程序首先要保留初值，执行结束后恢复它们，最后通过执行一条叫“ IRET ” 中断返回指令，去恢复保留在推栈上的 IP、CS 以及各标志之值，从而使中断例行程序结束。

中断优先级：

在多级中断系统中，很可能同时有多个中断请求，这时 CPU 接受中断优先级为最高的那个中断，忽略其中断优先级较低的那些中断

●若指令流水线把一条指令分为取指、分析和执行三部分，且三部分的时间分别是 $t_{取指}$=2ns，$t_{分析}$=2ns，$t_{执行}$=1ns。则 100 条指令全部执行完毕需__(4)__ns。(硬件知识->指令系统)

(4)A.163　　B.183　　C.193　　D.203

解答：100 条指令全部执行完毕所需要时间=100*$T_{取指}$+ $T_{分析}$+ $T_{执行}$=203ns

答案：D

相关知识点：假设指令的解释分取指、分析与执行 3 步，每步的时间相应为 $T_{取指}$、$T_{分析}$、$T_{执行}$，

(1) 分别计算下列几种情况下，执行完 100 条指令所需时间的一般关系式：

(i) 顺序方式。

(ii) 仅“ 执行 $_k$ ”与“ 取指 $_{k+1}$ ”重叠。

(iii) 仅“执行$_k$”、“分析$_{k+1}$”、“取指$_{k+2}$”重叠。

(2) 分别在 $T_{取指}=T_{分析}=2, T_{执行}=1$ 及 $T_{取指}=T_{分析}=5, T_{执行}=2$ 两种情况下，计算出上述结果

解答：见 表 1-1

指令执行情况	执行完 100 条指令所需要的时间	
顺序方式	$100*(T_{取指}+T_{分析}+T_{执行})$	
仅“执行$_K$”与“取指$_{K+1}$”重叠	$T_{取指}+100*[T_{分析}+(T_{执行}, T_{取指最大者})]$	
仅“执行$_K$”、“分析$_{K+1}$”、“取指$_{K+2}$”重叠	$T_{取指}+T_{分析}+100*T_{执行}$	
指令执行情况	$T_{取指}=T_{分析}=2, T_{执行}=1$	$T_{取指}=T_{分析}=5, T_{执行}=1$
顺序方式	500	1200
仅“执行$_K$”与“取指$_{K+1}$”重叠	402	705
仅“执行$_K$”、“分析$_{K+1}$”、“取指$_{K+2}$”重叠	104	507

表 1-1

●在单指令流多数据计算机（SIMD）中，各处理单元必须__(5)__。（硬件知识->指令系统）

(5)A.以同步方式，在同一时间内执行不同的指令

B.以同步方式，在同一时间内执行同一指令

C.以异步方式，在同一时间内执行不同指令

D.以异步方式，在同一时间内执行同一指令

解答：SISD 也就是单指令流单数据流，传统的顺序处理机(串行机)。

SIMD 也就是单指令流多数据流，阵列处理机，并行处理机。

MISD 也就是多指令流单数据流，采用流水结构的计算机。

MIMD 也就是多指令流多数据流，多处理机

答案：B

●单个磁头在向盘片的磁性涂层上写入数据时，是以__(6)__方式写入的。（硬件知识->存储介质）

(6)A.并行 B.并－串行 C.串行 D.串－并行

解答：由于是单个磁头因此是串行的。

答案：C

●容量为 64 块的 Cache 采用组相联的方式映像，字块大小为 128 个字，每 4 块为一组。若主容量为 4096 块，且以字编址，那么主存地址应为__(7)__位，主存区号应为__(8)__位。（硬件知识->主存配置）

(7)A.16 B.17 C.18 D.19

(8)A.5 B.6 C.7 D.8

解答：主容量为 $4096=4*1024=2^2*2^{10}=2^{12}$，而 Cache 字块大小为 128 个字节则 $128=2^7$，因此主存地址应为 12+7=19 位，由于 Cache 的容量为 64 块，因 Cache 的地址=组号+组内地

址，Cache 的整个容量=64 块乘以每块大小=64* 2^7 = 2^{13}（即 13 位表示），又因为每块大小为 2^7 （即用 7 位表示，组内地址），因此组号地址为 6 位。

答案：(7)D，(8)B。

相关知识点：存储介质：

凡是明显具有并能保持两种稳定状态，并且能够方便地与电信息转换的物质和器件，均可作为存储介质。

（1）磁芯存储器

（2）半导体存储器：

60 年代后期发展起来的存储技术，采用集成化技术，将存储单元电路及其外围电路直接做在半导体芯片上，然后封装在管壳内。分为两类：一类是双极型半导体存储器，它的特点是速度快，功耗大，集成度较低，一般主要用作大型机的告诉缓冲存储器（Cache）；另一种是 MOS 存储器（Metal Oxide Semiconductor Memory）,它的特点是集成度高，功耗小，速度较低，适合于作各类计算机的主存储器。

MOS 型 RAM 有静态与动态之分。静态存储单元电路：以 MOS 晶体管触发器构成存储单元的电路，当没有外界信号作用时，触发器可以长久保持其所处的某种稳定状态。

动态存储单元电路：利用 MOS 晶体管极电容（或 MOS 电容）上充积的电荷来存储信息，电容上的电荷不能长久保存，需要周期地对电容进行充电，以补充泄露的电荷。动态存储单元电路是由多时钟脉冲控制，在动态情况下工作。

（3）磁表面存储器：

是将薄层的磁性材料沉积在某一基体上，并以相对于磁头运动的方式来存取信息的装置。如磁盘、磁带、磁卡等。

（4）光盘存储器：

利用激光在磁性薄膜上产生的热磁效应以实现信息的记录。

高速缓存

高速缓冲存储器（Cache）：用于解决 CPU 与内存之间的速度不匹配。

（1）Cache 的基本结构：Cache 由存储体、地址映像和替换机构组成

①Cache 存储体：存储体是存储单元的集合，用于存放信息，一般由半导体静态存储器构成。

②地址映像：地址映像的作用是把 CPU 送来的主存地址转换成 Cache 地址。有三种地址映像方式：直接映像、全相联映像和组相联映像。

直接映像：指每个主存页只能复制到某一固定的 Cache 页中。

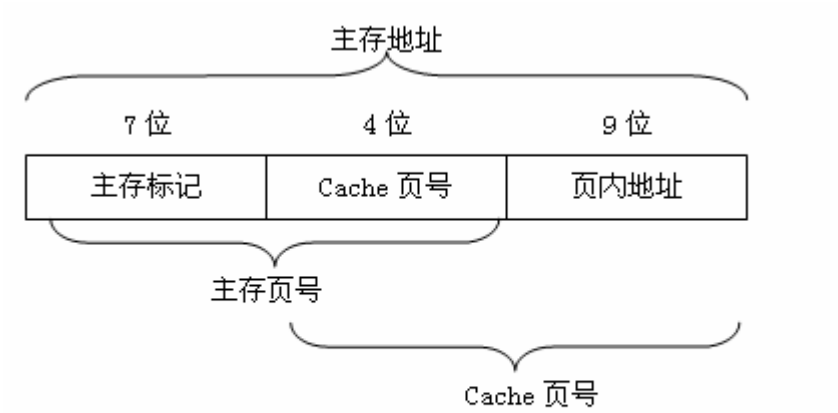


图1 地址映像方式一直接映像

全相联映像：指主存的每一页可以映像到 Cache 的任意一页。

图2地址映像方式一全相联映像

组相联映像：是直接映像和全相联映像的折中方案，它将 Cache 分为若干组，同时将主存分为若干组，每组内的页数与 Cache 的组数相同，其规律是主存中的各页与 Cache 的组号有固定的映像关系，但可以自由映像到对应的 Cache 组中的任意一页。即组间采用直接映像，而组内的页为全相联映像。

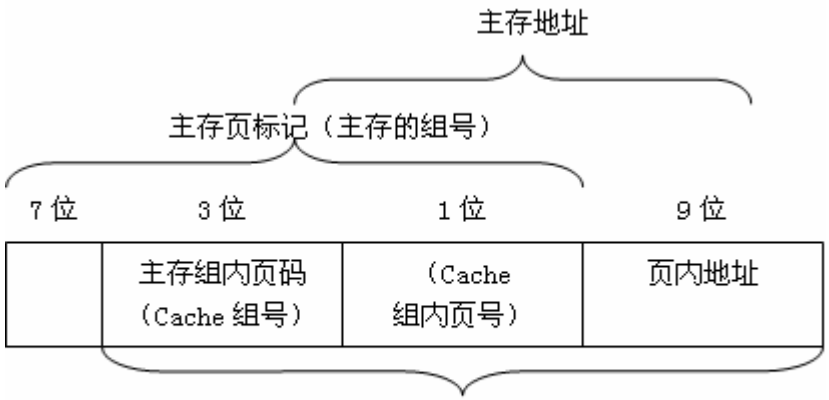


图3地址映像方式一组相联映像

③替换机构：当 CPU 访问 Cache 未命中时，应从主存中读取信息，同时写入 Cache 中，若 Cache 未满，直接写入，若已满，则需要进行替换，替换机构由硬件组成，并按替换算法

进行设计，常用的算法有先进先出算法（FIFO）和最近最少使用算法（LRU）

（2）Cache 的读写操作：

①读操作：访存时，将主存地址同时送主存和 Cache，一则启动对主存的读操作，二则在 Cache 中按映像方式从中获取 Cache 地址，并将主存标记与 Cache 标记比较：若相同，则命中，从 Cache 中读出数据。若不同，则未命中，则从主存中读取数据，并按某种替换算法更新 Cache。

②写操作：

写回法：信息暂时只写入 Cache，并用标志加以注明，直到该页需要从 Cache 中替换出来，才一次写入主存。

写直达法：信息写入 Cache 时同时也写入主存。

辅存设备的性能和容量计算

辅存设备的主要性能指标：

（1）记录密度

道密度：单位长度的道数，单位 TPI 或 TPM

位密度（线密度）：单位长度磁道所能记录的二进制信息的位数，单位 bpi。

（2）存储容量

存储容量指存储设备所能存储的二进制信息总量，一般以位（bit）或字节（byte）为单位。存储容量取决于盘面数，盘面大小和存储密度。

（3）平均寻址时间

读/写头接到读/写命令从起始位置到达指定的位置所需的全部时间称为寻址时间。寻址时间包括两部分：一是将读/写头移动到指定的道的时间——找道时间 T_S；二是找到道后，读/写头要等待存储介质上的指定区旋转到其下方所需的等待时间 T_W。

平均寻址时间 $T=T_{SA}+T_{WA}=（T_{SMAX}+T_{SMIN}）/2+（T_{WMAX}+T_{WMIN}）/2$

（4）数据传输率

指单位时间存储器读/写的二进制信息量。

（5）误码率

出错信息位数和读出的总信息位数之比。

磁盘的非格式化容量=W×3.14×d×m×n 其中 w 为位密度，d 为最内圈直径，m 为记录面数，n 为面磁道数。

磁盘的格式化后容量=n×t×s×b 其中 n 为保存数据的总盘面数，t 为每面磁道数，s 为每道扇区数，b 为每扇区的字节数。输入输出结构和设备。

●软件开发中的瀑布模型典型地刻画了软件生存周期的阶段划分，与其最相适应的软件开发方法是(9)。（软件工程->结构化分析）

(9)A.构件化方法　　B.结构化方法

C.面向对象方法　　D.快速原型方法

解答：瀑布模型特点：阶段的顺序性和依赖性，推迟实现的观点，质量保证

存在问题：不适合需求模糊的系统

快速原型模型特点：快速开发工具，循环，低成本。种类：渐进型和抛弃型

螺旋模型特点：瀑布模型+快速原型+风险分析，迭代过程

一个螺旋式周期包括：

确定目标，选择方案，选定完成目标的策略

风险角度分析该策略
启动一个开发阶段
评价前一步的结果，计划下一轮的工作

答案: B

●下述任务中，不属于软件工程需求分析阶段的是(10)。（软件工程->需求分析）

(10)A.分析软件系统的数据要求　　B.确定软件系统的功能需求
C.确定软件系统的性能要求　　D.确定软件系统的运行平台

解答：软件工程中包含需求、设计、编码和测试四个阶段,其中需求工程是软件工程第一个也是很重要的一个阶段。

一、需求分析

需求开发又分为需求获取、需求分析、编写规格说明书和需求验证。以下列出和讲解分析常规的步骤，当然应按照项目的大小和特点等实际情况我们应该自己确定合适的步骤

1．需求获取

确定需求开发过程确定如何组织需求的收集、分析、细化并核实的步骤，并将它编写成文档。

2．需求分析

绘制关联图、创建开发原型、分析可行性、确定需求优先级、为需求建立模型、编写数据字典、应用质量功能调配。

3．编写规格说明书

项目视图和范围文档包含了业务需求，而使用实例文档则包含了用户需求

4．需求验证

审查需求文档、依据需求编写测试用例、编写用户手册、确定合格的标准

二、需求管理

需求开发的结果应该有项目视图和范围文档、使用实例文档、软件需求规格说明及相关分析模型。经评审批准，这些文档就定义了开发工作的需求基线。

答案： D

●软件设计的主要任务是设计软件的构造、过程和模块，其中软件结构设计的主要任务是要确定(11)。（软件工程->结构设计）

(11)A.模块间的操作细节　　B.模块简的相似性
C.模块间的组成关系　　D.模块间的具体功能

解答：结构化设计的核心是“自上向下逐步求精 ”的模块化设计方法，是对每个模块的组成关系进行详细设计。

答案：C

●系统测试是将软件系统与硬件、外设和网络等其他因素结合，对整个软件系统进行测试。(12)不是系统测试的内容。（软件工程->测试方法）

(12)A.路径测试　B.可靠性测试　　C.安装测试　　D.安全测试

解答：系统测试包括（1）测试环境①硬件环境②软件环境③数据环境④网络环境。
（2）功能测试内容①模拟现场测试②应用现场测试。(安全测试与安装测试等)
（3）性能测试（可靠性测试）而路径测试是在开发阶段时进行的测试。

答案：A

●项目管理工具中，将网络方法用于工作计划安排的评审和检查的是　(13)　。（软件工程->项目管理基础知识）

（13）A.Gantt 图 B.PERT 网图 C.因果分析图 D.流程图

解答：常用的制定进度计划的工具主要有 Gantt 图和工程网络两种。Gantt 图具有悠久历史、直观简明、容易学习、容易绘制等优点，但是，它不能明显地表示各项任务彼此间的依赖关系，也不能明显地表示关键路径和关键任务，进度计划中的关键部分不明确。因此，在管理大型软件项目时，仅用 Gantt 图是不够的，不仅难于做出既节省资源又保证进度的计划，而且还容易发生差错。

工程网络不仅能描绘任务分解情况及每项作业的开始时间和结束时间，而且还能清楚地表示各个作业彼此间的依赖关系。从工程网络图中容易识别出关键路径和关键任务。因此，工程网络图是制定进度计划的强有力的工具。通常，联合使用 Gantt 图和工程网络这两种工具来制定和管理进度计划，使它们互相补充、取长补短。

进度安排是软件项目计划的首要任务，而项目计划则是软件项目管理的首要组成部分。与估算方法和风险分析相结合，进度安排将为项目管理者建立起一张计划图。

项目管理方法分为四个发展阶段：Gannt 图阶段、确定性网络计划技术阶段，如关键路径法 CPM（Critical Path Method）等、概率型网络计划技术阶段，如计划评审技术 PERT (Program Evaluation and Review Technique)和多因素随机网络计划技术阶段，如考虑资金因素的 PERT/COST，考虑活动风险的图评审技术 GERT(Graphics Evaluation and Review Technology)和风险评审技术 VERT(Venture Evaluation and Review Technology)，以及多种资源（资金、人力等）约束下的网络优化等等。

答案: A

●在结构化分析方法中，数据字典是重要的文档。对加工的描述是数据字典的组成内容之一，常用的加工描述方法 (14)。（软件工程->结构化分析）

（14）A、只有结构化语言 B、有结构化语言和判定树

C、有结构化语言和判定树和判定表 D、判定树和判定表

解答：数据字典是关于数据的信息的集合，是对数据流图中包含的所有元素的定义的集合。而加工条目是对数据流图中每一个不再分解的基本加工的精确说明，常用的加工逻辑描述方法有三种：结构化语言、判定表和判定树。

答案：C

●CMM 模型将软件过程的成熟度分为 5 个等级。在 (15) 使用定量分析来不断地改进和管理软件过程。（软件工程->过程管理）

（15）A、优化级 B、管理级 C、定义级 D、可重复级

解答：CMM 把软件开发组织的能力成熟度分为 5 个可能的等级。除了第 1 级外，其他每一级由几个关键过程方面组成。每一个关键过程方面都由公共特性予以表征。CMM 给每个关键过程规定了一些具体目标。按每个公共特性归类的关键惯例是按该关键过程的具体目标选择和确定的。如果恰当地处理了某个关键过程涉及的全部关键惯例，这个关键过程的各项目标就能达到，这就表明该关键过程实现了。这种分级的思路在于把一个组织执行软件过程的成熟程度分成循序渐进的几个阶段，这与软件组织提高自身能力的实际推进过程相吻合。这种成熟度分级的优点在于级别明确而清楚地反映了过程改进活动的轻重缓急和先后顺序。这一点很重要，因为大多数软件组织只能在某一段时间里集中开展少数几项过程改进活动。如果按管理、组织和工程三个方面分类，则 CMM 的关键过程方面分布如下表所示

CMM 的关键过程方面分布

类别 / 等级	管理	组织	工程
CMM1：初始级			
CMM2：可重复级	需求管理 软件项目策划 软件项目追踪和监督 软件分包管理 软件质量保证 软件配置管理		
CMM3：定义级	集成式软件管理 组间协调	组织过程定焦 组织过程定义 培训	软件产品工程 对等审查
CMM4：定量管理级	定量过程管理		软件质量管理
CMM5：优化级		技术变更管理 过程变更管理	缺陷预防

答案: A

●在面向数据流的设计方法中，一般把数据流图中的数据流划分为__(16)__两种。（软件工程->设计方法）

（16）A、数据流和事物流　　B、变换流和数据流

C、变换流和事物流　　D、控制流和事物流

解答：数据流图用于抽象描述一个软件的逻辑模型，数据流图由一些特定的图符构成，"变换流"：由输入 、输出 、变换（或称处理）三部分组成，是一顺序结构。"事物流"：它的某个加工，分离成许多发散的数据流，形成许多加工路径，并且根据输入值选择其中一个路径来执行。（这人加工称为事务处理中心）。

答案：C

●__(17)__属于第三层 VPN 协议。（网络知识>网络安全协议）

（17）A、TCP　　B、IPsec　　C、PPOE　　D、SSL

解答：隧道协议工作在 ISO 网络模型的层次可以把 VPN 分为第二层隧道协议（如 PPTP、L2F、L2TP、MPLS、UTI）和第三层隧道协议（如 GRE 和 IPSec）。第四层隧道协议最著名的是 SSL，现已成为远程访问 VPN 的新宠。除了具备与 IPSec VPN 相当的安全性外，还增加了访问控制机制，客户端只需要拥有支持 SSL 的浏览器即可，可以说是零配置，非常适合远程用户访问企业内部网。不过这类产品对非 Web 应用的支持不够理想。不管怎样，SSL VPN 是一种低成本、高安全性、简便易用的远程访问 VPN 解决方案，具备相当大的发展潜力。随着越来越多的公司将自己的应用转向 Web 平台，SSL VPN 会得到更为广泛的应用。

答案 B

●下图所示的防火墙结构属于__(18)__。（网络知识>防火墙）

（18）A、简单双宿主主机结构　　B、单 DMZ 防火墙结构

C、带有屏蔽路由器的单网段防火墙结构　　D、双 DMZ 防火墙结构

解答：防火墙最常用于一个组织的内部网络和互联网之间，在单层结构中，一台主机实现所有功能，并且与需要它控制访问的所有网络相连接。这种方法通常适用于对价格敏感或者只有两个网络互联的情况。它的优点在于，那台主机上的防火墙可以监控一切事情。在需要实行的安全策略比较简单，并且接入的网络也不多的情况下，这种结构是十分划算并且容易维护的。它最大的缺点是容易受执行缺陷（Implementation Flaw）以及配置错误的影响——由于这种结构的特性，只要有一个缺陷或者错误，就可以使防火墙失效。

在多层结构中，防火墙功能需要一定数量的主机来实现，而且通常采用级联方式，并且它们之间有 DMZ 网络。这种结构比单层结构更难设计和操作，但是它能够通过多样化的防御措施而提供更强的安全性。我们建议在每台防火墙主机中使用不同的防火墙技术，虽然这样的花费也更高。这样可以避免在不同的层中出现相同的执行缺陷和配置错误。这种结构最常见的设计方法就是在一个 DMZ 网络中接入一个由两台主机互联而组成的互联网防火墙。

答案：B

●电子商务交易必须具备搞抵赖性，目的在于防止（19）（网络知识>电子商务）

（19）A、一个实体假装成另一个实体

B、参与此交易的一方否认曾经发生过此次交易

C、他人对数据进行非授权的修改、破坏

D、信息从被监视的通信过程中泄漏出去。

解答：我们先理解什么是电子签名，需要从传统手工签名或盖印章谈起。在传统商务交易中，为了保证交易的安全与真实，一份书面合同或公文需要由当事人或负责人签字或盖章，以便让交易双方识别是谁签的合同，并能保证签字或盖章的人认可合同的内容，在法律上才能承认这份合同是有效的。而在电子商务的虚拟世界中，合同或文件是以电子文件的形式表现和传递的，在电子文件上，传统的手写签名和盖章是无法进行的，这就必须依靠技术手段来替代。从法律上讲，签名有两个功能：即标识签名人和表示签名人对文件内容的认可。因此联合国贸发会的《电子签名示范法》中对电子签名作如下定义："指在数据电文中以电子形式所含、所附或在逻辑上与数据电文有联系的数据它可用于鉴别与数据电文相关的签名人和表明签名人认可数据电文所含信息。"；而在欧盟的《电子签名共同框架指令》中对电子签名的定义是："以电子形式所附或在逻辑上与其他电子数据相关的数据，作为一种判别的方法"。不同的法律对电子签名的定义可能有所不同,但其实质是一样的。因此，能够在电子文件中识别双方交易人的真实身份，保证交易的安全性和真实性以及不可抵赖性，起到与手写签名或者盖章同等作用的电子技术手段，即可称之为电子签名。

实现电子签名的技术手段目前有多种，比如基于公钥密码技术的数字签名；或用一个独一无二的以生物特征统计学为基础的识别标识，例如手印、声音印记或视网膜扫描的识别；手书签名和图章的电子图象的模式识别；表明身份的密码代号（对称算法）；基于量子力学的计算机等等。但比较成熟的，世界先进国家目前普遍使用的电子签名技术还是基于 PKI 的数字签名技术。由于制定法律的技术中立性原则，目前电子签名法中所提到的签名，一般指的就是"数字签名"。它是电子签名的一种特定形式。

所谓数字签名就是利用通过某种密码运算生成的一系列符号及代码组成电子密码进行"签名"，来代替书写签名或印章，对于这种电子式的签名在技术上还可进行算法验证，其验证的准确度是在物理世界中与手工签名和图章的验证是无法相比的。数字签名在 ISO7498-2 标准中定义为：附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据和变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人（例如接收者）进行伪造。美国电子签名标准（DSS，FIPS186-2）对数字签名作了如下解释：利用一套规则和一个参数对数据计算所得的结果，用此结果能够确认签名者的身份和数据的完整性。根据这些定义，数字签名已成为目前电子商务、电子政务中应用最普遍、技术最成熟、可操作性最强的一种电子签名方法。它是采用了规范化的程序和科学化的方法，用于鉴定签名人的身份以及对一项电子数据内容的认可。它还能验证出文件的原文在传输过程中有无变动，确保传输数据的完整性、真实性和不可抵赖性。

答案：B

●知识产权一般都具有法定的何护期限，一旦保护期限届满，权利将自行终止，成为社会公从可以自由使用的知识。（20）权受法律保护的期限是不确定的，一旦为公众所知悉，即成

为公众可以自由使用的知识。（知识产权）

（20）A、发明专利　　B、商标　C、作品发表　D、商业秘密

解答：知识产权：是基于自己的智力活动创造的成果和经营管理活动中的经验、知识而依法享有的权利。它包括著作权、邻接权、商标权、商号权、商业秘密权、产地标记权、专利权、集成电路布图设计权等各种权利。

商业秘密：是指不为公众所知悉，能为权利人带来经济利益，具有实用性并经权利人采取保密措施的技术信息和经营信息。受法律保护的期限是不确定的，一旦为公众所知悉，即成为公众可以自由使用的知识。

商标权：是指商标所有人在法律规定的有效期内，对其经商标主管机关核准注册的商标享有的独占的、排他的使用和处分的权利。只有经商标局核准注册的商标，才享有商标权并依法予以保护。商标权的取得，我国实行统一注册原则和申请在先原则。

发表权：即决定作品是否公之於众的权利。发表权、使用权和获得报酬权的保护期为五十年，截止于作品首次发表后第五十年。的１２月３１日，但作品自创作完成后五十年内未发表的，本法不再保护。

答案：D

●甲、乙两人在同一时间就同样的发明创造提交了专利申请，专利局将分别向各申请人通报有关情况，并提出多种解决这一问题的办法，不可能采用（21）的办法。（专利权）

（21）A、两申请人作为一件申请的共同申请人

B、其中一方放弃权利并从另一方得到适当的补尝

C、两件申请都不授予专利权

D、两件申请都授予专利权

解答：专利申请申请人就一项发明创造要求获得专利权的，应当按照专利法及其实施细则的规定向专利局 提出专利申请两个以上的申请人分别就同样的发明创造申请专利的，专利权授予最先申请的人。

答案：D

●《计算机软件产品开发文件编制指南》（GB8567-88）是（22）标准。（标准化知识）

（22）A、强制性国家 B、推荐性国家 C、强制性行业 D、推荐性行业

解答：对需要在全国范围内统一的技术要求，制定国家标准；对没有国家标准而又需要在行业范围内统一的技术要求，制定行业标准。行业标准不得与有关国家标准相抵触。有关行业标准之间应保持协调、统一，不得重复。

国家标准　（GB XXX-XXXX　或　GB/T XXX-XXXX）

强制性国家标准代号--GB；

推荐性国家标准代号--GB／T；

强制性行业标准代号--××；

推荐性行业标准代号--××／T，

推荐性行业标准的代号是在强制性行业标准代号后面加“/T”，例如农业行业的推荐性行业标准代号是 NY/T。行业标准代号由国务院标准化行政主管部门规定。行业标准的编号由行业标准代号、标准顺序号及年号组成。行业标准归口部门应在行业标准发布后三十日内，将已发布的行业标准及编制说明连同发布文件各一份，送国务院标准化行政主管部门备案。 备案的行业标准如违反国家有关法律、法规和强制性国家标准，国务院标准化行政主管部门责成行业标准归口部门限期改正或停止实施，行业标准实施后，应根据科学技术的发展和经济建设的需要适时进行复审；复审周期一般不超过五年，确定其继续有效、修订或废止。一个简单记忆法：凡是“GB”（“国家”拼音的一个字母）就是国家标准，否则是行业标准，凡是“T”（“推荐”拼音的第一个字母）就是推荐标准。

答案：A

●虚拟存储管理系统的基础是程序的（23）理论，这个理论的基本含义是指程序执行时往往会不均匀地访问主存储器的单元。根据这个理论，Denning 提出了工作集理论。工作集是进程运行时被频繁地访问的页面集合。在进程运行时，如果它的工作集页面都在（24）内，能够使该进程有效地运行，否则会出现频繁的页面调入/调出现象。（操作系统->存储管理方案）

（23）A、全局性　　B、局部性　　C、时间全局性　　D、空间全局性

（24）A、主存储器　B、虚拟存储器　C、辅助存储器　　D、U 盘

解答：虚拟存储器，为了扩大容量，把辅存当作主存使用，所需要的程序和数据由辅助的软件和硬件自动地调入主存，对用户来说，好像机器有一个容量很大的内存，这个扩大了的存储空间称为虚拟存储器。

按写分配：当写 Cache 不命中时把该地址相对应的块从主存调入 Cache。

段式管理：指把主存按段分配的存储管理方式。

页式管理：指把存储空间按页分配的存储管理方式。

段页式管理：指将存储空间按逻辑模块分成段，每段又分成若干个页，访存通过一个段表和若干个页表进行的存储管理方式。

块表：在 Cache 中为确定地址映象关系而建立的一张逻辑表，此表反映出主存单元与 Cache 单元的对应关系。当采用不同的地址映象方式时，块表的格式各不相同。

页表：用于记录每个页的主存页号、表示该页是否已装入主存的装入位等信息的表称为页表，它是虚拟页号与物理页号的映象表。

段表：用于指明各段在主存中位置的表，表中包括段基址、装入位和段长等信息。

固件：把固定不变的常用软件固化在硬件中，如写入 ROM 存储器中，称为固件。固件是介于硬件和软件之间的实体。其设计方法类似于软件，而实现形态上则类似于硬件。

访问局部性：CPU 对局部范围存储器地址的访问频繁，而对此范围之外地址的访问甚少的现象称为访问局部性。

直接映象：指一个主存块只能映象到 Cache 中惟一一个指定块的地址映象方式。

全相联映象：指每个主存块都可映象到任何 Cache 块的地址映象方式。

组相联映象：指将存储空间分成若干组，各组之间是直接映象，而组内各块之间则是全相联映象。

全写法：又称写直达法，当出现写操作 Cache 命中时，将数据既写入 Cache 又写入主存。

写回法：当出现写操作 Cache 命中时，将数据只写入 Cache 而不写入主存。

答案：（23）B,(24) A

●在 UNIX 操作系统中，若用户键入的命令参数的个数为 1 时，执行 cat$1 命令；若用户键入的命令参数的个数为 2 时，执行 cat>>$2<$1 命令。请将下面所示的 Shell 程序的空缺部分补齐。（网络操作系统->UNIX 命令）

```
case （25） in
     1) cat $1 ; ;
     2)cat>>$2<$1 ; ;
     )echo ‘default…..’
esac
```

(25)A、$$　　B、$@　　C、$#　　D、$*

解答：shell 是提供到 UNIX 操作系统的接口的一个命令编程语言。它的特征包括控制流原语、参数传递、变量和字符串替换。还可获得如 while、if then else、 case 和 for 这样的构造。在 shell 和命令之间可以有双向通信。可以把字符串值参数、典型的文件名字和标志传递给命令。命令设置的返回值可用来决定控制流，而来自命令的标准输出可用作 shell 输

入。

控制流 - case

case 记号提供一种多路分支。例如，

```
case $# in
  1) cat >>$1 ;;
  2) cat >>$2 <$1 ;;
  *) echo \'usage: append [ from ] to\' ;;
esac
```

是一个 append 命令。在调用时带有一个实际参数如

```
append file
```

$# 是字符串 1 并使用 cat 命令把标准输入复制到 file 的末端。

```
append file1 file2
```

添加 file1 的内容到 file2 上。如果提供给 append 的实际参数数目不是 1 或 2 则打印指示正确用法的一个消息。

答案：C

●设信道的码元速率为 300 波特，采用 4 相 DPSK 调制则信道的数据速率为 (26) b/s.

（网络知识->数据速率的计算）

(26)A、300 B、600 C、800 D、1000

解答：首先掌握几个概念

1) 数据传输速率--每秒传输二进制信息的位数，单位为位/秒，记作 bps 或 b/s。

2) 计算公式: S=1/T*log2N(bps) .....(1)

式中 T 为一个数字脉冲信号的宽度(全宽码)或重复周期(归零码)单位为秒；N 为一个码元所取的离散值个数。通常 N=2K，K 为二进制信息的位数，K=log2N。N=2 时，S=1/T，表示数据传输速率等于码元脉冲的重复频率。

2)信号传输速率--单位时间内通过信道传输的码元数，单位为波特，记作 Baud。

计算公式: B=1/T (Baud) .....(2)

式中 T 为信号码元的宽度，单位为秒.

信号传输速率,也称码元速率、调制速率或波特率。

由(1)、(2)式得： S=B*log2N (bps) .....(3)

或 B=S/log2N (Baud) .....(4)

模拟信号无论表示模拟数据还是数字数据,在传输一定距离后都会衰减。克服的办法是用放大器来增强信号的能量，但噪音分量也会增强，以至引起信号畸变。数字信号长距离传输也会衰减，克服的办法是使用中继器，把数字信号恢复为"0、1"的标准电平后继续传输。

例如：采用四相调制方式，即 N=4，且 T=833x10-6 秒，则

S=1/T*log2N=1/(833x10-6)*log24=2400 (bps)

B=1/T=1/(833x10-6)=1200 (Baud)

3).信道容量

(1)信道容量表示一个信道的最大数据传输速率，单位：位/秒(bps)

信道容量与数据传输速率的区别是，前者表示信道的最大数据传输速率，是信道传输数据能力的极限，而后者是实际的数据传输速率。像公路上的最大限速与汽车实际速度的关系一样。

(2)离散的信道容量

奈奎斯特(Nyquist)无噪声下的码元速率极限值 B 与信道带宽 H 的关系：B=2*H (Baud) .....(5)

奈奎斯特公式--无噪信道传输能力公式：(2002 年网络设计师上午题 (10))

C=2*H*log2N (bps) .....(6)

式中 H 为信道的带宽，即信道传输上、下限频率的差值，单位为 Hz；N 为一个码元所取的离散值个数。

例如 1：普通电话线路带宽约 3kHz，则码元速率极限值 。

B=2*H=2*3k=6kBaud ；

若码元的离散值个数 N=16，则最大数据传输速率 C=2*3k*log216=24kbps。

(3)连续的信道容量

香农公式--带噪信道容量公式：

C=H*log2(1+S/N) (bps) .....(7)

式中 S 为信号功率，

N 为噪声功率，

S/N 为信噪比，通常把信噪比表示成 10lg(S/N)分贝(dB)。

例如：已知信噪比为 30dB，带宽为 3kHz，求信道的最大数据传输速率。

$\because\ 10\lg(S/N)=30\ \therefore\ S/N=10^{(30/10)}=1000$

$\therefore\ C=3k\log_2^{(1+1000)}\approx 30kbps$

4)码元：构成信息编码的最小单位，二进制编码的码元为 1 位二进制数，即 1 个比特。一个‘A’字符的 ASCII 码 01000001B 就是由 8 个码元构成。 一个码携带的信息量由码元取的离散的状态值个数决定。若码元取 0 和 1 两个离散状态值，则一个码元携带 1 比特(bit)信息。若码元可取 4 个离散状态值(如四进制，4 个离散状态值为 3、2、1、0)，则一个码元携带 2 比特信息。码元携带的信息量 n(比特)与码元取的离散值个数 N 有如下 n = log 2 N.

补充

5).误码率--二进制数据位传输时出错的概率。

它是衡量数据通信系统在正常工作情况下的传输可靠性的指标。在计算机网络中，一般要求误码率低于 10-6，若误码率达不到这个指标，可通过差错控制方法检错和纠错。

误码率公式：

Pe=Ne/N .....(8)

式中 Ne 为其中出错的位数；

N 为传输的数据总数。

信道利用率=发送数据时间/(传输时间+发送数据时间)

例：假设传送信道是可靠的，数据传送速率为 4kbit/s，信道传播时延为 20ms，帧处理时间及应答帧长度可忽略不计，试问帧长在什么范围内才能使信道利用率达到 50%?

解答：信道利用率=发送数据时间/(传输时间+发送数据时间)

50%=发送数据时间/(20ms×2+发送数据时间)

发送数据时间=40ms，帧长=4k/s×40ms=160bit

而本题由因为采用 4 相，码元所带比特数 n =log 2 N=2，C=2*H*log2N

(bps)=2*300*log22=600b/s

答案：B

●光纤通信中使用的复用方式是(27)EI 载波把 32 个信道按(28)方式复用在一条 2.048Mb/s 的高速信道上，每条话音信道的数据速率是 (29) (网络知识-多路复用)

(27) A、时分多路 B、空分多路 C、波分多路 D、频分多路

(28) A、时分多路 B、空分多路 C、波分多路 D、频分多路

（29）A、56Kb/s　　B、64Kb/s　　C、128 Kb/s　　D、512Kb/s

解答：光纤使用波分多路复用技术，EI 载波把 32 个信道按时分多用复用技术复用到一条线路上，**注意此题要看清楚题，许多考生一看到“32 个信道”就选频分多路，**每条信道的数据速率为 2048*1000/32=64K。

答案：（27）C、（28）A、（29）B。

●用户 A 与用户 B 通过卫星链路通信时，传播延迟为 270ms，假设数据速率是 64Kb/s，帧长 4000bit，若采用停等流控协议通信，则最大链路利用率为（30）；（网络知识->链路利用率）

若采用后退 N 帧 ARQ 协议通信，发送窗口为 8，则最大链路利用率可以达到（31）。

（30）A、0.104　　B、0.116　　C、0.188　　D、0.231

（31）A、0.416　　B、0.464　　C、0.752　　D、0.832

解答：利用公式，信道利用率=发送数据时间/(传输时间+发送数据时间)

发送时间=4000/64000*1000=62.5ms,传输时间=270*2=540ms，

信道利用率=62.5/(540+62.5)=62.5/602.5=0.104

后退 N 帧(Go-Back-N)协议的基本原理：因为后退 N 帧协议的发送窗口大于 1，而接收窗口=l。这就是说接收方只能按序接收。在后退 N 帧协议中，发送窗口大于 1，接收窗口等于 1。发送方一次可以连续发多帧，但接收方只能按序接收，也就是前一帧没有正确接收时，就不能接收它的下一帧。这样，当接收方检测出失序的信息帧后，要求发送方重发最后一个正确接收的信息帧之后的所有未被确认的帧；或者当发送方发送了 n 个帧后，若发现该 n 帧的前一帧在计时器超时后仍未返回其确认信息，则该帧被判定为出错或丢失，此时发送方就不得不重新发送该出错帧及其后的 n 帧。当发送窗口为 8 时，则其最大利用率为 8*0.104=0.832。

答案：（30）A，（31）D

●HDLC 是一种（32）协议。（网络知识->HDLC 协议）

（32）A、面向比特的同步链路控制

B、面向字节数的异步链路控制

C、面向字符的同步链路控制

D、面向比特的异步链路控制

解答：HDLC（High-Level Data Link Control）高层数据链路协议，是面向比特的通信协议，以比特作为传输的基本单位。HDLC 帧结构、内容：

F A C　INFO　FCS F

符号 定 义 长度（bit） 内 容

F 标志域 8 用特殊的位模式 01111110 作为标志确定帧首、帧尾。

A 地址域 8 标识从站的地址。

C 控制域 8 用控制域的格式区分信息帧、管理帧、无编号帧三种帧。

INFO 信息域 任 意 透明、编码独立的数据信息。只有信息帧和某些无编号帧含有信息域。

FCS 帧校验序列域 16 采用循环冗余校验（CRC）除标志域外的所有其他域的校验序列。

HDLC 帧类型：1）信息帧（I 帧）：用于实现信息的编号传送，其控制段的第一位为 0，它具有发送序号 N(S)，用于标明所发送信息帧的序号，只有信息帧才有此序号。还有捎带的肯定应答信号 N(R)，用于标明预期接收的帧的序号，并对以前收到的帧进行确认。P/F：询问/终止位。2）管理帧（S 帧）：用于实现流量和差错控制。控制字段的前两位为 10。只含有接收序号 N(R)，作用同 I 帧的 N(R)。不包含信息段。3）无编号帧（U 帧）：用于链路控制。无 N(S),N(R)字段。

答案：A

●帧中继网络没有采用流量控制机制，只有拥塞控制功能。采用显式信令控制时，如果 LAP-D

帧中的 FECN 比特置 1，则表示 (33)。（网络知识->流量与拥塞控制）

(33) A、在帧的传送方向上出现了调整
B、在与帧传送方向上出现了拥塞
C、在两个传送方向上同时出现了拥塞
D、没有出现拥塞

解答：帧中继是继 X.25 后发展起来的数据通信方式。从原理上看，帧中继与 X.25 及 ATM 都同属分组交换一类。但由于 X.25 带宽较窄，而帧中继和 ATM 带宽较宽，所以常将帧中继和 ATM 称为快速分组交换。

帧中继保留了 X.25 链路层的 HDLC 帧格式但不采用 HDLC 的平衡链路接入规程 LAPB(Link Access Procedure - Balanced)，而采用 D 通道链路接入规程 LAPD (Link Access Procedure on the D-Channel)。LAPD 规程能在链路层实现链路的复用和转接，所以帧中继的层次结构中只有物理层和链路层。与 X.25 相比，帧中继在操作处理上做了大量的简化。帧中继不考虑传输差错问题，其中节点只做帧的转发操作，不需要执行接收确认和请求重发等操作，差错控制和流量控制均交由高层端系统完成，所以大大缩短了节点的时延，提高了网内数据的传输速率。帧中继的帧结构类似与 HDLC 的帧格式，不过没有控制字段，帧中继的帧格式中，标志字段 F 和帧校验序列 FCS 的作用与 HDLC 中的类似。F 字段用以标志帧的起始和结束，其比特模式为 01111110,可采用 0 比特插入法实现数据的透明传输。FCS 字段用于帧的验错，若传输中出错，则有接收端将之丢弃并通知发送端重发，数据链路连接标识符 DLCI 由高、低两部分共 10 比特组成，用于唯一表示一个虚连接。命令／相应位 C/R 与高层应用有关，帧中继本身并使用。扩展地址位 EA 为“0”表示下一字节仍为地址，为“1” 表示地址结束，用于对地址字段进行扩展。对于 2 字节地址，其 EA0 为“0”、EA1 为“1”。发送方将前向显示阻塞通知位 FECN 置为"1"，用于通知接收方网络出现阻塞；接收方将反向显示阻塞通知位 BECN 置"1"，用于通知发送方网络出现阻塞。可丢弃位 DE 由用户设置，若置“1”，表示当网络发生阻塞时，该帧可被伏先丢弃。

答案：A

●ATM 网络采用了许多通信量管理技术以避免拥塞的出现，其中 (34) 是防止网络过载的第一道防线。（网络知识->ATM 网络）

(34)A、连接许可 B、选择性信元丢弃 C、通信量整型 D、使用参数控制

解答：选择性信元丢弃，通信量整型，使用参数控制都在连接以后所采取的方法，连接许可是最先、最有效的方法。

答案：A

●IP 交换是一种利用交换硬件快速传送 IP 分组的技术。一台 IP 交换机由 (35) 三部分组成。IP 交换机初始化后为每一个物理连接建立一个默认的 (36)，相邻的 IP 交换机通过这些默认通信交换路由信息和数据分组，为了进行第三层的路由选择，IP 交换控制器必须根据 (37) 等信息对网络数据流进行分类并加上数据流描述符。（网络知识->IP 交换技术）

(35) A、ATM 交换模块、IP 交换控制器和交换机管理协议
B、RF 交换模块、IP 交换控制器和路由器管理协议
C、X.25 交换模块、IP 交换控制器和交换机管理协议
D、IPX 交换模块、IP 交换控制器和路由器管理协议

(36) A、帧中继交换通道 B、ATM 交换通道 C、X.25 交换通道 D、IPX 交换通道

(37) A、源和目标 IP 地址、MAC 地址
B、源 IP 地址、ATM VPI/VCI
C、目标 IP 地址、TCP/UDP 端口号
D、源和目标 IP 地址、TCP/UDP 端口号

解答：IP 交换（IPSwitching）： IP 交换是 IPSILON 公司提出的 ATM 网络上传送 IP 分组的技术，其核心是 IP 交换机。IP 交换机由 ATM 交换机和 IP 交换控制器组成。IP 交换控制器又分为路由软件和控制软件两部分。ATM 交换机和 IP 交换控制器之间采用 RFC1987 通用交换机管理协议（GSMP）， IP 交换机之间采用 RFC1953 Ipsilon 流管理协议（IFMP）。 总之，ATM 和 IP 都是当今最热门的技术之一，是建立三网互连的关键。ATM 解决了信息高速、高质量的传输问题，IP 解决了网络互通问题，只有将二者融合、互补，充分发挥其优势，真正的信息高速公路才能成为现实。IP 交换机是一种配置交换硬件的 IP 路由器，具有缓冲路由选择功能。IP 交换技术最初由 Ipsilon 网络开发而成。IP 交换设备可以识别长数据包流并可能在第 2 层转换这些流，从而绕开了路由器并提高了吞吐量。IP 交换技术综合使用快速 ATM 硬件和 IP，这样保留了 IP 无连接特性。为达到交换功效，还提供了一种连接 IP 流和 ATM 标签的机制。IP 交换技术下，每个源/目的数据包流都分配到一个标签。IP 交换机处理流中的初始数据包，是通过将这些数据包传送到属于 IP 交换机组成部分的标准路由器模块中而实现的。

答案：(35) A，36 (B)，37 (D)

IETF 定义的多协议标记交换（MPLS）是一种第三层交换技术，MPLS 网络由_(38)_组成，负责为网络流添加/删除标记的是_(39)_。

(38) A.标记交换路由器和标记边缘路由器
B.标记分发路由器和标记边缘路由器
C.标记分发路由器和标记传送路由器
D.标记传送路由器和标记交换路由器

(39) A.标记分发路由器　　B.标记边缘路由器
C.标记交换路由器　　D.标记传送路由器

解答：MPLS 的基本原理：

多协议标记交换技术(MPLS:MultiProtocol Label Switching)，MPLS 是一种特殊的转发机制，它为进入网络中的 IP 数据包分配标记，并通过对标记的交换来实现 IP 数据包的转发。标记作为 IP 包头在网络中的替代品而存在，在网络内部 MPLS 在数据包所经过的路径通过交换标记（而不是看 IP 包头）来实现转发；当数据包要退出 MPLS 网络时，数据包被解开封装，继续按照 IP 包的路由方式到达目的地，MPLS 网络包含一些基本的元素。在网络边缘的节点就称作标记边缘路由器(LER:Label Edge Router),而网络的核心节点就称作标记交换路由器（LSR：Label Switching Router）。LER 节点在网络中提供高速交换功能。在 MPLS 节点之间的路径就叫做标记交换路径(LSP:Label Switched Path)。一条 LSP 可以看作是一条贯穿网络的单向隧道。

MPLS 的工作流程可以分为三个方面：即网络的边缘行为、网络的中心行为以及如何建立标记交换路径。

1. 网络的边缘行为

当 IP 数据包到达一个 LER 时，MPLS 第一次应用标记。首先，LER 要分析 IP 包头的信息，并且按照它的目的地址和业务等级加以区分。

在 LER 中，MPLS 使用了转发等价类(FEC:Forwarding Equivalence Class)的概念来将输入的数据流映射到一条 LSP 上。简单地说，FEC 就是定义了一组沿着同一条路径、有相同处理过程的数据包。这就意味着所有的 FEC 相同的包都可以映射到同一个标记中。

对于每一个 FEC，LER 都建立一条独立的 LSP 穿过网络，到达目的地。数据包分配到一个 FEC 后，LER 就可以根据标记信息库(LIB:Label Information Base)来为其生成一个标记。标记信息库将每一个 FEC 都映射到 LSP 下一跳的标记上。如果下一跳的链路是 ATM，则 MPLS 将使用 ATM VCC 里的 VCI 作为标记。

转发数据包时，LER 检查标记信息库中的 FEC，然后将数据包用 LSP 的标记封装，从标记信息库所规定的下一个接口发送出去。

2. 网络的核心行为

当一个带有标记的包到达 LSR 的时候，LSR 提取入局标记，同时以它作为索引在标记信息库中查找。当 LSR 找到相关信息后，取出出局的标记，并由出局标记代替入局标记，从标记信息库中所描述的下一跳接口送出数据包。

最后，数据包到达了 MPLS 域的另一端，在这一点，LER 剥去封装的标记，仍然按照 IP 包的路由方式将数据包继续传送到目的地。

3. 如何建立标记交换路径

建立 LSP 的方式主要有两种：

(1)“Hop by Hop (逐跳寻径) ”路由

一个 Hop-by -Hop 的 LSP 是所有从源站点到一个特定目的站点的 IP 树的一部分。对于这些 LSP，MPLS 模仿 IP 转发数据包的面向目的地的方式建立了一组树。

从传统的 IP 路由来看，每一台沿途的路由器都要检查包的目的地址，并且选择一条合适的路径将数据包发送出去。而 MPLS 则不然，数据包虽然也沿着 IP 路由所选择的同一条路径进行传送，但是它的数据包头在整条路径上从始至终都没有被检查。

在每一个节点，MPLS 生成的树是通过一级一级地为下一跳分配标记，而且是通过与它们的对等层交换标记而生成的。交换是通过标记分配协议(LDP:Label Distribution Protocol)的请求以及对应的消息完成的。

(2)显式路由

MPLS 最主要的优点就是它可以利用流量设计“引导”数据包。MPLS 允许网络的运行人员在源节点就确定一条显式路由的 LSP（ER-LSP），以规定数据包将选择的路径。ER-LSP 从源端到目的端建立一条直接的端到端的路径。MPLS 将显式路由嵌入到限制路由的标记分配协议的信息中，从而建立这条路径。

答案：(38) A，(39) B。

● DHCP 协议的功能是 (40)。在 Linux 中提供 DHCP 服务的程序是 (41)；DHCP 服务将主机的 MAC 地址和 IP 地址绑定在一起的方法是在 (42) 文件中添加“host 主机名{|hardware Ethernet xx.xx.xx.xx.xx.xx fixed-address 192.168.0.9}”配置项；创建 DHCP 租用文件的命令是 (43)；通过运行 (44) 命令可以设置在操作系统启动时自动运行 DHCP 服务。

(网络操作系统->LINUX 命令，常见 windows 网络操作命令)

(40) A.为客户自动进行注册　　B.为客户机自动配置 IP 地址
　　C.使 DNS 名字自动登录　　D.为 WINS 提供路由

(41) A./etc/networks/dhcpd　　B./usv/sbin/dhcp
　　C./etc/networks/dhcp　　D./usr/sbin/dhcpd

(42) A./etc/dhcpd.conf　　B./etc/dhcp.conf
　　C./networks/dhcpd.conf　　D./networks/dhcp.conf

(43) A.touch/var/state/dhcp/dhcpd.leases
　　B.address/var/state/dhcp/dhcpd.leases
　　C.nat/var/state/dhcp/dhcp.leases
　　D.resolve/var/state/dhcp/dhcp.leases

(44) A.ipconfig　　B.touch　　C.reboot　　D.chkconfig

解答：Linux 下的网络命令

1) rcp 命令

rcp 代表“ remote file copy ”（远程文件拷贝）。该命令用于在计算机之间拷贝文件

2) ftp 主机名/IP

其中“主机名/IP”是所要连接的远程机的主机名或 IP 地址

最常用的命令有：

ls 列出远程机的当前目录

cd 在远程机上改变工作目录

lcd 在本地机上改变工作目录

ascii 设置文件传输方式为 ASCII 模式

binary 设置文件传输方式为二进制模式

close 终止当前的 ftp 会话

hash 每次传输完数据缓冲区中的数据后就显示一个#号

get（mget） 从远程机传送指定文件到本地机

put（mput） 从本地机传送指定文件到远程机

open 连接远程 ftp 站点

quit 断开与远程机的连接并退出 ftp

3) telnet 登录到远程计算机上

用户结束了远程会话后，一定要确保使用 logout 命令退出远程系统。然后 telnet 报告远程会话被关闭，并返回到用户的本地机的 Shell 提示符下.

4) rlogin 命令

rlogin 是“remote login”（远程登录）的缩写。该命令与 telnet 命令很相似，允许用户启动远程系统上的交互命令会话.

5) netstat 查看网络的状况

6) finger 查询某个使用者的信息

7) ping 查询某个机器是否在工作

8) /etc/resolv.conf 文件 （2001 年上午考试 61 题）

该文件是由域名解析器（resolver，一个根据主机名解析 IP 地址的库）使用的配置文件，示例如下：

search openarch.com

nameserver 202.103.86.1

nameserver 202.103.86.2

“search domainname.com”表示当提供了一个不包括完全域名的主机名时，在该主机名后添加 domainname.com 的后缀；“nameserver”表示解析域名时使用该地址指定的主机为域名服务器。其中域名服务器是按照文件中出现的顺序来查询的

9) /etc/host.conf 文件 （2001 年上午考试 60 题）

该文件指定如何解析主机名。Linux 通过解析器库来获得主机名对应的 IP 地址。下面是一个“/etc/host.conf”的示例：

order bind,hosts

multi on

ospoof on

“order bind,hosts”指定主机名查询顺序，这里规定先使用 DNS 来解析域名，然后再查询。

10) /etc/sysconfig/network 文件

该文件用来指定服务器上的网络配置信息，下面是一个示例：

NETWORK=yes

RORWARD_IPV4=yes

HOSTNAME=deep.openarch.com

GAREWAY=0.0.0.0
GATEWAYDEV=
NETWORK=yes/no 网络是否被配置；
FORWARD_IPV4=yes/no 是否开启 IP 转发功能
HOSTNAME=hostname hostname 表示服务器的主机名
GAREWAY=gw-ip gw-ip 表示网络网关的 IP 地址
GAREWAYDEV=gw-dev gw-dw 表示网关的设备名，如：etho 等

注意：为了和老的软件相兼容，"/etc/HOSTNAME"文件应该用和 HOSTNAME=hostname 相同的主机名。

11) /etc/hosts 文件 （2001 年网设上午考试 57 题）

当机器启动时，在可以查询 DNS 以前，机器需要查询一些主机名到 IP 地址的匹配。这些匹配信息存放在/etc/hosts 文件中。在没有域名服务器情况下，系统上的所有网络程序都通过查询该文件来解析对应于某个主机名的 IP 地址。

下面是一个"/etc/hosts"文件的示例：

IP Address	Hostname	Alias
127.0.0.1	Localhost	Gate.openarch.com
208.164.186.1	gate.openarch.com	Gate

最左边一列是主机 IP 信息，中间一列是主机名。任何后面的列都是该主机的别名。一旦配置完机器的网络配置文件，应该重新启动网络以使修改生效。使用下面的命令来重新启动网络：/etc/rc.d/init.d/network

12) /etc/inetd.conf 文件 （2001 年上午考试 58 题）

众所周知，作为服务器来说，服务端口开放越多，系统安全稳定性越难以保证。所以提供特定服务的服务器应该尽可能开放提供服务必不可少的端口，而将与服务器服务无关的服务关闭，比如：一台作为 www 和 ftp 服务器的机器，应该只开放 80 和 25 端口，而将其他无关的服务如：finger auth 等服务关掉，以减少系统漏洞，而 inetd，也叫作"超级服务器"，就是监视一些网络请求的守护进程，其根据网络请求来调用相应的服务进程来处理连接请求。inetd.conf 则是 inetd 的配置文件。inetd.conf 文件告诉 inetd 监听哪些网络端口，为每个端口启动哪个服务。在任何的网络环境中使用 Linux 系统，第一件要做的事就是了解一下服务器到底要提供哪些服务。不需要的那些服务应该被禁止掉，最好卸载掉，这样黑客就少了一些攻击系统的机会。查看"/etc/inetd.conf"文件，了解一下 inetd 提供哪些服务。用加上注释的方法（在一行的开头加上#号），禁止任何不需要的服务，再给 inetd 进程发一个

13) /etc/hosts.allow 和/etc/hosts.deny 这 2 个文件允许和禁止远程主机对本地服务的访问。（2001 年上午考试 59 题）

14) route add 增加静态路由（2002 年上午考试 64 题）

```
# route add -net 192.168.1.0 netmask 255.255.255.0
```

最后要增加系统的 IP 转发功能。这个功能由/proc/sys/net/ipv4 目录下的 ip_forward 文件控制，执行如下命令打开 ip 转发功能：

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

15) ip route add 10.191.140.100 缺省路由（2002 年上午考试 65 题）

16) /etc/lilo.conf LiLo 是 linux 启动文件（2003 年上午考试 51 题）

/etc/hosts 网络主机名文件
/etc/services 网络服务端口文件
/etc/inetd.conf 网络服务文件

17）chkconfig(check config)

功能说明：检查，设置系统的各种服务。
语法：chkconfig [--add][--del][--list][系统服务] 或 chkconfig [--level <等级代号>][系统服务][on/off/reset]
参数：
add 增加所指定的系统服务，让 chkconfig 指令得以管理它，并同时在系统启动的叙述文件内增加相关数据。
del 删除所指定的系统服务，不再由 chkconfig 指令管理，并同时在系统启动的叙述文件内删除相关数据。
level<等级代号> 指定读系统服务要在哪一个执行等级中开启或关毕 。
18) enable 功能说明：启动或关闭 shell 内建指令。
19）liloconfig 功能说明：设置核心载入，开机管理程序。
20）lilo(linux loader) 功能说明：安装核心载入，开机管理程序。

Unix 下的网络命令

1) route 命令

route 命令主要用于手动配置静态路由表。例如我们要增加一条通过网关到达令一子网的路由，命令如下：

#route add net remote_net_ip gateway_ip 1

其中 add 代表要增加路由，net 表示路由到达的是一个网络而不是一台主机，1 代表远端网络需通过网关才能到达，而不是直接与它相连(直接通过网络接口相连时,该参数用 0)

2) netstat 命令

netstat 命令的功能是显示网络连接、路由表和网络接口信息，可以让用户得知目前都有哪些网络连接正在运作,起参数如下

-i 显示所有网络接口的信息，格式同“ifconfig -e”。
-n 以网络 IP 地址代替名称，显示出网络连接情形
-r 显示核心路由表，格式同“route -e”。
-t 显示 TCP 协议的连接情况。

3) traceroute 命令

traceroute 命令跟踪网络访问路由, 通过 Traceroute 我们可以知道信息从你的计算机到互联网另一端的主机是走的什么路径。当然每次数据包由某一同样的出发点（source）到达某一同样的目的地(destination)走的路径可能会不一样，但基本上来说大部分时候所走的路由是相同的. 如 traceroute hostname（对方主机名或 ip 地址）

4) Telnet 时不能用 root 登录 在默认情况下，出于安全性考虑，UNIX 系统不允许在系统操作台(console) 以外的终端用 root 登录，所以有时我们通过 Telnet 用 root 登录时，会返回 "not on system console 这样的错误,这时,我们可以通过修改/etc/default/login 文件来允许 root 通过 Telnet 登录。具体方法是，编辑 login 文件，找到下面的一行：
CONSOLE=/dev/console 将这一行注释掉，即在行首加上"#"符，存盘退出，
再次使用 Telnet 时，root 就可以登录了。

5) ifconfig 命令

ifconfig 命令用于查看和更改网络接口的地址和参数,如果要显示某台 UNIX 主机的 IP 地址,我们可以在命令行下输入： $ifconfig -a 系统会显示网络接口的名称，接口的状态(up or down)，接口的 IP 地址和掩码等信息.如果我们要更改网络接口的 IP 地址，可以在 root 权限下输入：

#ifconfig hme0 down
#ifconfig hme0 202.1.2.3 netmask 255.255.255.0 up

6) Tcp/Ip 的启动：

⑴．TCP/IP 受/etc/tcp 脚本文件的控制，在你进入多用户状态时启动，在你进入单用户状态时关闭/etc/tcp 文件操作内容：他是一个脚本文件，其功能如下：通过配置支持 TCP/IP 所必须的流设备来启动或关闭 TCP/IP，并启动或关闭与 TCP/IP 相关的 daemon.

⑵．以 ROOT 登录，使用命令行：TCP START 或 TCP STOP 手工启动或关闭 TCP/IP。该文件与 etc/rc2.d 和/etc/rc0.d 目录下的文件都有链连关系，使得/etc/tcp 在系统进入或退出多用户状态时，可以运行 START 或 STOP 选项。无论你通过 Network ，Confugration Manager 来增加还是删除一个网络接口，都会在脚本中增加或删除,ifconfig 命令，修改/etc/tcp 文件，同时导致/etc/strcf 文件也被修改。

7) Apache Web 服务器有三个主要的配置文件，它们一般位于/usr/local/apache/conf 目录。这三个文件是：httpd.conf、srm.conf 和 access.conf。这些文件是整个 Apache 的控制中心，因此需要对三个配置文件有所了解。httpd.conf 文件是主配置文件；srm.conf 允许你填加资源文件；access.conf 设置文件的访问权限。

（1）httpd.conf 是 Apache 设置文件中的主文件，httpd 程序启动时会先读取 httpd.conf。srm.conf 是数据配置文件，在这个文件中主要设置 WWW Server 读取文件的目录、目录索引时的画面、CGI 执行时的目录等等。access.conf 是负责基本的读取文件控制，限制目录所能执行的功能及访问目录的权限设(2002 年上午 56 题)

（2）srm.conf srm.conf 是服务器的资源映射文件，告诉服务器各种文件的 MIME 类型，以及如何支持这些文件

（3）access.conf 文件包含一些指令控制允许什么用户访问 Apache 目录。应该把 deny from all 作为初始化指令，然后使用 allow from 指令打开访问权限。你可以允许来自某个域、IP 地址或者 IP 段的访问。例如：

```
order deny,allow
deny from all
allow from sans.org
```

8) DirectoryIndex index.html(2002 年上午 59 题), ServerAdmin,就是管理员的邮箱啦.(2002 年上午 58 题)

(如果想增加别的类别文件，只需在这后面增加 index.htm 或 index.php 即可)

9) web 管理目录 ,ServerRoot "/../...",WEB 的根目录 DocumentRoot "/../..."(2002 年上午 57 题)

10. UserDir 命令，用来指定个人主页的位置。如果你有一个用户 test，那么它主目录是“/home/test”，当客户端输入“http://yourdomain/~test”，系统就会到对应的目录“/home/test/UserDir/”中去寻找。其中“UserDir”就是在 UserDir 命令中设置的指定目录。

命令格式: UserDir [Path] (2002 年上午 60 题)

DHCP 服务器的配置

在一个基于 TCP/IP 协议的网络中， 每台主机都有会有一个 IP 地址（如：Internet）。Internet 上的每台主机都有一个唯一的 IP 地址，根据获得 IP 址的方式不同，可以分为静态 IP，动态 IP。例如：用宽带入网，你一定会有一个固定的 IP 地址，每次连入 Internet 你的 IP 地址都一样，而用拔号上网（如用:MODEM），每次连入 Internet 时都能从 ISP 那里获得一个 IP 地址且每次所获得的可能都不同。现在以 LINUX 为例来讲述一下 DHCP 服务器的配置：

一、DHCP 服务器的工作条件

为了使 DHCP 服务器能为 Windows 平台的主机服务,必须要在 LINUX 服务器上加上一

条 255.255.255.255 的路由(因为 Windows 平台的主机都是以广播方式搜索 DHCP 服务器)为了以后每次启动时自动执行,可以在/etc/rtc.d/rc.local 中加入以下的一条命令:

route add -host 255.255.255.255 dev eth0

二.安装 DHCP 的 rpm 包，在 RED HAT LINUX 中，每项服务都以 rpm 包方式封装的，如果当前系统中没有安装 DHCP 的话，必须要添加 DHCP 的 rpm 包，可以执行以下命令：

rpm -ivh dhcp3-3.0b1plo-r.i386.rpm

配置 dhcpd.conf

dhcpd.conf 是 DHCP 服务器的配置的核心，每次启动 DHCP 服务器都有要读取该文件，在 dhcpd.conf 中对 DHCP 服务器做了很多的定义。如：IP 地址池,、租用期限，下面给出一个 dhcpd.conf 的实例：

```
default-lease-time 1800; /*定义租用期限为 1800 秒
max-lease-time 9200; /*最大租用期限为 9200 秒
option subnet-mask 255.255.255.0; /*定义子网掩码为 255.255.255.0
option broadcast-address 192.168.1.255; /*定义网络广播号为 192.168.1.255
option routers 192.168.1.254; /*定义默认路由
option domain-name-servers 192.168.1.1,192.168.1.2; ／＊定义ＤＮＳ服务器
option domain-name "ciu.net.cn"; ／*定义域名
subnet 192.168.1.0 netmask 255.255.255.0 ／*定义ＩＰ地址池
{
range 192.168.1.20 192.168.1.200;
 }
```

dhcpd.conf 可以说只需要在其中定义一个 IP 地址池就可以了，但为了加强 DHCP 服务器的功能，你可以加上一些 option 语句，利用 option 语句不仅可以定义路由，域名，还可以指定 DNS 服务器。以上的这个 dhcpd.conf 比较全面的，如果我们想将一个 IP 地址指定给一台主机应该怎么做？其实，只要在 dhcpd.conf 中加入以下语句：

```
host haagen
{
hadware ethernet 网卡号;
fixed_address 192.168.1.22;
}
```

三．为了记录 IP 地址的租用情况，必须创建一个 dhcpd.leases 文件，这个文件为空的，创建文件的过程如下：

进入/etc/dhcpd 目录下执行如下命令：

touch dhcpd.leases

四．启动与测试 DHCP 服务器启动：

方式一：为了使在每次启动 Linux 系统时自动启动 DHCP 服务器可以利用 ntsysv 将 DHCP 服务选中就可以了

方试二：手工启动，可以在/etc 目录下执行 dhcpd eth0 测试：

方式一：利用一台 Windows 98 平台的客忘掉机登录入网，利用 Winipcfg 工具查看能不能获得 IP 地址和释放 IP 地址，如果能够得获得与释放 IP 则说明 DHCP 服务器一切正常

方式二：可以在 Linux 系统中执行/etc/dhcpd -d -f 如果 DHCP 服务器配置有错的话，就会有错误提示的。

答案：（40）B、（41）D、（42）A、（43）A、（44）D。

在分布式环境中实现身份认证可以有多种方案，以下选项中最不安全的身份认证方案式__(45)__。（网络知识->网络安全->身份认证，数字签名）

(45) A.用户发送口令，由通信对方指定共享密钥
B.用户发送口令，由智能卡产生解密密钥
C.用户从 KDC 获取会话密钥
D.用户从 CA 获取数字证书

数字证书采用公钥体制进行加密和解密。每个用户有一个私钥，用它进行__(46)__；同时每个用户还有一个公钥，用于__(47)__。X.509 标准规定，数字证书由__(48)__发放，将其放入公共目录中，以供用户访问。X.509 数字证书中的签名字段是指__(49)__。如果用户 UA 从 A 地的发证机构取得了证书，用户 UB 从 B 地的发证机构取得了证书，那么__(50)__。

(46) A.解密和验证 B.解密和签名 C.加密和签名 D.加密和验证
(47) A.解密和验证 B.解密和签名 C.加密和签名 D.加密和验证
(48) A.密钥分发中心 B.证书授权中心 C.国际电信联盟 D.当地政府
(49) A.用户对自己证书的签名 B.用户对发送报文的签名
C.发证机构对用户证书的签名 D.发证机构对发送报文的签名
(50) A.UA 可使用自己的证书直接与 UB 进行安全通信
B.UA 通过一个证书链可以与 UB 进行安全通信
C.UA 和 UB 还须向对方的发证机构申请证书，才能进行安全通信
D.UA 和 UB 都要向国家发证机构申请证书，才能进行安全通信

解答：网络安全：

网络上的不安全因素可以来自网络外部，也可以来自网络内部。一般将对 Internet 构成的威胁分为故意危害和无意危害两种。

故意危害 Internet 安全的主要有 3 类人：故意破坏者又称黑客、不遵守规则者、刺探秘密者。除了信息泄露构成安全危害外，有害信息侵入也是一种不安全因素。它表现在散布不健康的图片和文字，以及不负责任的消息；也可能通过下载或游戏将病毒带入自己的计算机系统中。

防火墙是一种安装在网间连接设备上的软件，在被保护的 Intranet 和 Internet 之间竖起一道安全屏障，用以增强 Intranet 的安全性。简单他说，防火墙可以用来确定外部的哪些人可以访问 Intranet 内部的哪些服务以及哪些外部的 Internet 服务可以被内部人员访问。

防火墙技术的作用：

①集中的网络安全：防火墙能禁止存在不安全因素的访问进出网络，并抗击来自各种线路的攻击。

②安全报警：防火墙可监视网络的安全，对不安全访问产生报警信号。

⑧重新部署网络地址转换：在防火墙上完成内部私有地址到外部注册的 IP 地址的映射工作。

④监视 Internet 的使用：防火墙是审查内部人员访问 Internet 的一个最佳软件。

⑤向外发布消息：防火墙是部署 WWW 服务器和 FTP 服务器的理想软件。

防火墙的局限性

①无法防范那些绕过防火墙而从其他的途径(假如存在的话)进行的攻击。

②无法防范内部变节者或不经心的用户带来的威胁。

⑧无法防范已经进入防火墙的数据带来的威胁。

防火墙系统的主要构成

①过滤路由器：也叫分组过滤路由器，对所经过的分组的头部信息进行检查与过滤，看是否与设置的过滤规则匹配，继而决定该分组是被转发还是被丢弃。

②应用网关：即通常所说的代理服务器，它运行在 Internet 和 Intranet 之间，当收到用户对某个站点的访问请求时，如果该请求符合规定，代理服务器就代替用户去访问站点并取回所需信息，然后转发给用户。外部的访问只能看到服务器而无法获知任何内部站点的情况。

⑧电路层网关：电路层网关常用于 Intranet 连接 Internet，对分组几乎不做过滤，此时内部的用户访问 Internet 非常方便。与之配套使用的代理服务器用于 Intranet 连接 Internet。

入侵检测技术

对各种事件进行分析，从中发现违反安全策略的行为是入侵检测系统的核心功能。从技术上，入侵检测分为两类：一种基于标志（signature-based），另一种基于异常情况（anomaly-based）。

对于基于标识的检测技术来说，首先要定义违背安全策略的事件的特征，如网络数据包的某些头信息。检测主要判别这类特征是否在所收集到的数据中出现。此方法非常类似杀毒软件。而基于异常的检测技术则是先定义一组系统“正常”情况的数值，如 CPU 利用率、内存利用率、文件校验和等（这类数据可以人为定义，也可以通过观察系统、并用统计的办法得出），然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。这种检测方式的核心在于如何定义所谓的“正常”情况。

两种检测技术的方法、所得出的结论有非常大的差异。基于异常的检测技术的核心是维护一个知识库。对于已知的攻击，它可以详细、准确的报告出攻击类型，但是对未知攻击却效果有限，而且知识库必须不断更新。基于异常的检测技术则无法准确判别出攻击的手法，但它可以（至少在理论上可以）判别更广范、甚至未发觉的攻击。从总体来说，入侵检测系统可以分为两个部分：收集系统和非系统中的信息然后对收集到的数据进行分析，并采取相应措施。

加密概念，加密是通过 Intranet、Extranet 和 Internet 进行安全的信息交换的基础。从业务的角度来看，通过加密实现的安全功能包括：身份验证，使收件人确信发件人就是他或她所声明的那个人；机密性，确保只有预期的收件人能够阅读邮件；以及完整性，确保邮件在传输过程中没有被更改。从技术的角度来看，加密是利用数学方法将邮件转换为不可读格式从而达到保护数据的目的的一门科学。 对称密钥加密，一个密钥 公钥加密，两个密钥 ，单向散列算法 ，数字签名，结合使用公钥与散列 ，密钥交换，结合使用对称密钥与公钥 ，对称密钥加密一个密钥 ，对称密钥加密，也叫做共享密钥加密或机密密钥加密，使用发件人和收件人共同拥有的单个密钥。这种密钥既用于加密，也用于解密，叫做机密密钥（也称为对称密钥或会话密钥）。对称密钥加密是加密大量数据的一种行之有效的方法。

对称密钥加密有许多种算法，但所有这些算法都有一个共同的目的，可以还原的方式将明文（未加密的数据）转换为暗文。暗文使用加密密钥编码，对于没有解密密钥的任何人来说它都是没有意义的。由于对称密钥加密在加密和解密时使用相同的密钥，所以这种加密过程的安全性取决于是否有未经授权的人获得了对称密钥。这就是它为什么也叫做机密密钥加密的原因。希望使用对称密钥加密通信的双方，在交换加密数据之前必须先安全地交换密钥。衡量对称算法优劣的主要尺度是其密钥的长度。密钥越长，在找到解密数据所需的正确密钥之前必须测试的密钥数量就越多。需要测试的密钥越多，破解这种算法就越困难。有了好的加密算法和足够长的密钥，如果有人想在一段实际可行的时间内逆转转换过程，并从暗文中推导出明文，从计算的角度来讲，这种做法是行不通的。

公钥加密，两个密钥，公钥加密使用两个密钥：一个公钥 和一个私钥，这两个密钥在数学上是相关的。为了与对称密钥加密相对照，公钥加密有时也叫做不对称密钥加密。在公钥加密中，公钥可在通信双方之间公开传递，或在公用储备库中发布，但相关的私钥是保密的。只有使用私钥才能解密用公钥加密的数据。使用私钥加密的数据只能用公钥解密。与对称密钥加密相似，公钥加密也有许多种算法。然而，对称密钥和公钥算法在设计上并无相似之处。

您可以在程序内部使用一种对称算法替换另一种，而变化却不大，因为它们的工作方式是相同的。而另一方面，不同公钥算法的工作方式却完全不同，因此它们不可互换。公钥算法是复杂的数学方程式，使用十分大的数字。公钥算法的主要局限在于，这种加密形式的速度相对较低。实际上，通常仅在关键时刻才使用公钥算法，如在实体之间交换对称密钥时，或者在签署一封邮件的散列时（散列是通过应用一种单向数学函数获得的一个定长结果，对于数据而言，叫做散列算法）。将公钥加密与其它加密形式（如对称密钥加密）结合使用，可以优化性能。公钥加密提供了一种有效的方法，可用来把为大量数据执行对称加密时使用的机密密钥发送给某人。也可以将公钥加密与散列算法结合使用以生成数字签名。将公钥加密用于数字签名，数字签名是邮件、文件或其它数字编码信息的发件人将他们的身份与信息绑定在一起（即为信息提供签名）的方法。对信息进行数字签名的过程，需要将信息与由发件人掌握的秘密信息一起转换为叫做签名的标记。数字签名用于公钥环境中，它通过验证发件人确实是他或她所声明的那个人，并确认收到的邮件与发送的邮件完全相同，来帮助确保电子商务交易的安全。通常，数字签名用于以明文（如电子邮件）分发数据的情形。在这种情况下，当邮件本身的敏感性可能无法保证加密的安全性时，确保数据处于其原始格式且并非由假冒者发送，是非常重要的。常用公钥算法 下面是三种最常用的公钥算法：

RSA-适用于数字签名和密钥交换。Rivest-Shamir-Adleman (RSA) 加密算法是目前应用最广泛的公钥加密算法，特别适用于通过 Internet 传送的数据。这种算法以它的三位发明者的名字命名：Ron Rivest、Adi Shamir 和 Leonard Adleman。RSA 算法的安全性基于分解大数字时的困难（就计算机处理能力和处理时间而言）。在常用的公钥算法中，RSA 与众不同，它能够进行数字签名和密钥交换运算。

DSA-仅适用于数字签名。数字签名算法 (Digital Signature Algorithm, DSA) 由美国国家安全署 (United States National Security Agency, NSA) 发明，已经由美国国家标准与技术协会 (National Institute of Standards and Technology, NIST) 收录到联邦信息处理标准 (Federal Information Processing Standard, FIPS) 之中，作为数字签名的标准。DSA 算法的安全性源自计算离散算法的困难。这种算法仅用于数字签名运算（不适用于数据加密）。

Diffie-Hellman-仅适用于密钥交换。 Diffie-Hellman 是发明的第一个公钥算法，以其发明者 Whitfield Diffie 和 Martin Hellman 的名字命名。Diffie-Hellman 算法的安全性源自在一个有限字段中计算离散算法的困难。Diffie-Hellman 算法仅用于密钥交换。

单向散列算法 ，散列-也称为散列值 或消息摘要，是一种与基于密钥（对称密钥或公钥）的加密不同的数据转换类型。散列就是通过把一个叫做散列算法的单向数学函数应用于数据，将任意长度的一块数据转换为一个定长的、不可逆转的数字。所产生的散列值的长度应足够长，因此使找到两块具有相同散列值的数据的机会很少。发件人生成邮件的散列值并加密它，然后将它与邮件本身一起发送。而收件人同时解密邮件和散列值，并由接收到的邮件产生另外一个散列值，然后将两个散列值进行比较。如果两者相同，邮件极有可能在传输期间没有发生任何改变。

用的单向散列函数 ，面是两个最常用的散列函数：

MD5， MD5 是由 Ron Rivest 设计的可产生一个 128 位的散列值的散列算法。MD5 设计经过优化以用于 Intel 处理器。这种算法的基本原理已经泄露，这就是为什么它不太受欢迎的原因。

SHA-1 与 DSA 公钥算法相似，安全散列算法 1(SHA-1) 也是由 NSA 设计的，并由 NIST 将其收录到 FIPS 中，作为散列数据的标准。它可产生一个 160 位的散列值。SHA-1 是流行的用于创建数字签名的单向散列算法。

数字签名，结合使用公钥与散列算法 可以结合使用公钥技术与散列算法来创建数字签名。数字签名可用作数据完整性检查并提供拥有私钥的凭据。签署和验证数据（由启用 PKI

的应用程序如 Microsoft Outlook 完成）的步骤如下：发件人将一种散列算法应用于数据，并生成一个散列值。发件人使用私钥将散列值转换为数字签名。 然后，发件人将数据、签名及发件人的证书发给收件人。收件人将该散列算法应用于接收到的数据，并生成一个散列值。收件人使用发件人的公钥和新生成的散列值验证签名。对用户而言这一过程是透明的。散列算法处理数据的速度比公钥算法快得多。散列数据还缩短了要签名的数据的长度，因而加快了签名过程。当创建或验证签名时，公钥算法必须且只需转换散列值（128 或 160 位的数据）。创建签名和验证签名的详细步骤取决于所采用的公钥算法。密钥交换：结合使用对称密钥与公钥对称密钥算法非常适合于快速并安全地加密数据。但其缺点是，发件人和收件人必须在交换数据之前先交换机密密钥。结合使用加密数据的对称密钥算法与交换机密密钥的公钥算法可产生一种既快速又灵活的解决方案。基于公钥的密钥交换步骤如下：

发件人获得收件人的公钥。发件人创建一个随机机密密钥（在对称密钥加密中使用的单个密钥）。发件人使用机密密钥和对称密钥算法将明文数据转换为暗文数据。发件人使用收件人的公钥将机密密钥转换为暗文机密密钥。发件人将暗文数据和暗文机密密钥一起发给收件人。收件人使用其私钥将暗文机密密钥转换为明文。收件人使用明文机密密钥将暗文数据转换为明文数据。同样，这些步骤是由启用 PKI 的应用程序（如 Microsoft Outlook）来完成的，并且对用户来说是透明的。

公钥基本结构的概念，术语公钥基本结构（PKI）用于描述管制或操纵证书与公钥及私钥的策略、标准和软件。实际上，PKI 是指由数字证书、证书颁发机构(CA) 以及对电子交易所涉及各方的合法性进行检查和验证的其它注册机构组成的一套系统。PKI 的有关标准仍处于不断发展之中，即使这些标准已被作为电子商务的要素而广泛实施。 PKI 一般包括：证书，书颁发机构 (CA)，可更改的 CA 层次结构注册，证书登记 ，证书吊销，证书链验证 ，证书 ，公钥证书，通常简称为证书，用于在 Internet、Extranet 和 Intranet 上进行身份验证并确保数据交换的安全。证书的颁发者和签署者就是众所周知的证书颁发机构 (CA)。颁发证书的实体是证书的主体。公钥证书是以数字方式签名的声明，它将公钥的值与持有相应私钥的主体（个人、设备和服务）的身份绑定在一起。通过在证书上签名，CA 可以核实与证书上公钥相应的私钥为证书所指定的主体所拥有。可以为各种目的颁发证书，如 Web 用户身份验证、Web 服务器身份验证、使用安全/多用途 Internet 邮件扩充协议 (Secure/Multipurpose Internet Mail Extensions, S/MIME) 的安全电子邮件、IP 安全性 (IP Security)、安全套接字协议层/事务层安全性 (Secure Sockets Layer/Transaction Layer Security, SSL/TLS) 和代码签名。如果在一个组织内部使用 Windows 2000 企业证书颁发机构，证书可用于登录到 Windows 2000 域。证书还可以由一个 CA 颁发给另一个 CA，以建立证书层次结构。可以通过多个名称来识别主体，如用户主要名称（用于最终用户证书）、目录名、电子邮件名称和 DNS 域名等。证书还应包含下列信息：

证书的有效期。证书的序列号，CA 应保证该序列号是唯一的。CA 的名称以及用于签署该证书的密钥。 CA 所遵循的用来确定证书主体身份的策略的标识符。在证书中标识的密钥对（公钥及相关的私钥）的用法。证书吊销列表 (CRL) 的位置，这是一个由 CA 维护并发布的列出已被吊销的证书的文档。为确保其完整性，CRL 是用 CA 的私钥签署的。证书提供了一个在公钥和拥有相应私钥的实体之间建立关系的机制。目前最常用的证书格式通过 ITU-T X.509 版本 3 (X.509v3) 国际标准定义。RFC 2459 是 X.509v3 的一个配置文件，进一步阐明了 X.509v3 中定义的字段。Windows 2000 PKI 采用 X.509v3 标准。Windows 证书是按照 RFC 2459 中的说明编程的，但仍然叫做 X.509v3 证书。 ITU-T X.509 并非证书的唯一格式。例如，Pretty Good Privacy (PGP) 安全电子邮件依赖 PGP 所独有的一种证书。证书颁发机构，证书颁发机构 (CA) 是一个向个人、计算机或任何其它申请实体颁发证书的可信实体。CA 受理证书申请，根据该 CA 的策略验证申请人的信息，然后使用它的私

钥把其数字签名应用于证书。然后，CA 将该证书颁发给该证书的主体，作为 PKI 内部的安全凭据。由于不同的 CA 使用不同的方法验证公钥与主体之间的绑定，在选择信任该颁发机构之前，理解该 CA 的策略是非常重要的。CA 可以是远程的第三方机构，如 VeriSign。作为选择，也可以是您创建的供您所在组织使用的 CA。

答案：(45) 中密码共享最容易泄露密码，因此选项是 A，私密就好比我们平时自己用来开门的钥匙，当然是用来开锁（解密），而公钥就好比一把锁有多个钥匙，只有每个拥有钥匙的人都才可打开锁，所以是加密的。分析得 **(46) B、(47) D、(48) B、(49) C、(50) B**。

下面有关 NTFS 文件系统有点的描述中 (51) 是不正确的。要把 FAT32 分区转换为 NTFS 分区，并且保留原分区中的所有文件，不可行的方法是 (52) 。（操作系统知识）

(51) A.NTFS 可自动地修复磁盘错误　　B.NTFS 可防止未授权用户访问文件
C.NTFS 没有磁盘空间限制　　D.NTFS 支持文件压缩功能

(52) A.利用磁盘分区管理软件同时实现 FAT32 到 NTFS 的无损转换和文件拷贝
B.先把 FAT32 分区格式化为 NTFS 分区，再把盘上的文件转换为 NTFS 文件
C.先把分区中的文件拷贝出来，然后把分区格式化为 NTFS，再把文件拷贝回去
D.利用分区转换工具“Convertexe”将 FAT32 转换为 NTFS 并实现文件拷贝

解答：NTFS 是随着 Windows NT 操作系统而产生的，并随着 Windows NT4 跨入主力分区格式的行列，它的优点是安全性和稳定性极其出色，在使用中不易产生产生文件碎片，NTFS 分区对用户权限作出了非常严格的限制，每个用户都只能按着系统赋予的权限进行操作，任何试图越权的操作都将被系统禁止，同时它还提供了容错结构日志，可以将用户的操作全部记录下来，从而保护了系统的安全，在 NTFS 文件系统中，对于不同配置的硬件，实际的文件大小从 4GB 到 64GB。由于 NTFS 文件系统的开销较大，使用的最小分区应为 50MB，NTFS 支持对单个文件或者目录的压缩。这种压缩不同于 FAT 结构中，对驱动器卷的压缩，其可控性和速度都要比 FAT 的磁盘压缩要好的多，对于超过 4GB 以上的硬盘，使用 NTFS 分区，可以减少磁盘碎片的数量，大大提高硬盘的利用率；NTFS 可以支持的文件大小可以达到 64GB，远远大于 FAT32 下的 4GB；支持长文件名等等。改变卷所使用的现有文件系统将是一项非常耗时的工作，必须首先对现有数据进行备份并使用新的文件系统重新对相应卷进行格式化。然而，当您希望将 FAT 或 FAT32 卷转换为 NTFS 卷时，可以无需重新对其进行格式化，在这种情况下通过使用 Convert.exe,这种转换方式可以确保您的文件完好无损（与分区格式化方式不同）。

答案：(51) C,(52)B

在 Windows2000 操作系统中，配置 IP 地址的命令是 (53) 。若用 ping 命令来测试本机是否安装了 TCP/IP 协议，则正确的命令是 (54) 。如果要列出本机当前建立的连接，可以使用的命令是 (55) 。（操作系统知识->常见网络命令）

(53)A.winipcfg　　B. ipconfig　　C. ipcfg　　D.winipconfig
(54)A.ping 127.0.0.0　B. ping 127.0.0.1　C. ping 127.0.1.1　D.ping 127.1.1.1
(55)A.netstat-s　　B. netstat-0　　C. netstat-a　　D.netstat-r

解答：网络管理命令：

windows 下的网络命令

1）查看 DNS、IP、Mac 等

A.Win98：winipcfg

B.Win2000 以上：Ipconfig/all

ipconfig /release 和 ipconfig /renew 命令，手动释放或更新客户的 IP 配置租约

2）arp

捆绑 IP 和 MAC 地址，解决局域网内盗用 IP：

ARP －s 192.168.10.88 00－56－ff－6d－18－35

解除网卡的 IP 与 MAC 地址的绑定：

arp -d 网卡 IP

3) netstat

netstat 命令显示协议统计信息和当前的 TCP/IP 连接。netstat -a 命令将显示所有连接，而 netstat -r 显示路由表和活动连接。netstat -e 命令将显示 Ethernet 统计信息，而 netstat -s 显示每个协议的统计信息。如果使用 netstat -n，则不能将地址和端口号转换成名称。

4）tracert

Tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。Tracert 命令用 IP 生存时间 (TTL) 字段和 ICMP 错误消息来确定从一个主机到网络上其他主机的路由。数据包必须通过两个路由器（10.192.0.1 和 192.168.3.1）才能到达主机 172.36.8.99。主机的默认网关是 10.192.0.1，192.168.3.0 网络上的路由器的 IP 地址是 192.168.3.1。

C:\>tracert 172.36.8.99 –d

Tracing route to 172.36.8.99 over a maximum of 30 hops

1 2s 3s 2s 10,192.0,1

2 75 ms 83 ms 88 ms 192.168.3.1

3 73 ms 79 ms 93 ms 172.36.8.99

Trace complete.

5）pathping

pathping 命令是一个路由跟踪工具，它将 ping 和 tracert 命令的功能和这两个工具所不提供的其他信息结合起来。pathping 命令在一段时间内将数据包发送到到达最终目标的路径上的每个路由器，然后基于数据包的计算机结果从每个跃点返回。由于命令显示数据包在任何给定路由器或链接上丢失的程度，因此可以很容易地确定可能导致网络问题的路由器或链接。

答案：(53) B、(54) B、(55) C

以太网交换机根据 (56) 转发数据包。访问交换机的方式有多种，配置一台新的交换机时可以 (57) 进行访问。在键入交换机命令时可使用缩写形式，在 Switch 模式下，如果键入 con，则表示 (58)。（网络知识->网络设备->交换机配置）

(56) A.IP 地址 B.MAC 地址 C.LLC 地址 D.PORT 地址

(57) A.通过微机的串口连接交换机的控制台端口

B.通过 Telnet 程序远程访问交换机

C.通过浏览器访问指定 IP 地址的交换机

D.通过运行 SNMP 协议的网管软件访问交换机

(58) A.connect B.contrd C.configure D.confirm

解答：交换机可以通过两种方法进行配置：一种就是本地配置；另一种就是远程网络配置两种方式，但是要注意后一种配置方法只有在前一种配置成功后才可进行。交换机的本地配置方式是通过计算机与交换机的“ Console ”端口直接连接的方式进行通信的，它的连接图如下图所示：

可进行网络管理的交换机上一般都有一个“ Console ”端口（这个在前面介绍集线器时已作介绍，交换机也一样），它是专门用于对交换机进行配置和管理的。通过 Console 端口连接并配置交换机，是配置和管理交换机必须经过的步骤。虽然除此之外还有其他若干种配置和管理交换机的方式（如 Web 方式、Telnet 方式、SNMP 等），但是，这些方式必须依靠通过 Console 端口进行基本配置后才能进行。因为其他方式往往需要借助于 IP 地址、域名或设备名称才可以实现，而新购买的交换机显然不可能内置有这些参数，所以通过 Console 端口连接并配置交换机是最常用、最基本也是网络管理员必须掌握的管理和配置方式。在任何命令模式下，只需键入 ”？“ ，即显示该命令模式下所有可用到的命令及其用途，这就交换机的帮助命令。另外，还可以在一个命令和参数后面加 ”？“ ，以寻求相关的帮助，命令均支持缩写命令，也就是说，除非您有打字的癖好，否则根本没有必要键入完整的命令和关键字，只要键入的命令所包含的字符长到足以与其他命令区别就足够了。例如，可将 ”show configure “ 命令缩写为 ” sh conf “ ,可将 ” show configure “ 命令缩写为 ” sh conf “ 然后回车执行即可。以太网交换机的原理很简单，它检测从以太端口来的数据包的源和目的地的 MAC（介质访问层）地址，然后与系统内部的动态查找表进行比较，若数据包的 MAC 层地址不在查找表中，则将该地址加入查找表中，并将数据包发送给相应的目的端口。

答案：（56）B，（57）A，（58）C

在缺省配置的情况下，交换机的所有端口 (59)。连接在不同交换机上的，属于同一 VLAN 的数据帧必须通过 (60) 传输。（网络知识->网络设备->交换机配置）

（59）A.处于直通状态　　B.属于同一 VLAN
　　C.属于不同 VLAN　　D.地址都相同

（60）A.服务器　　B.路由器　　C.Backbone 链路　　D.Trunk 链路

解答：链路聚合（Trunk）是一种封装技术，它是一条点到点的链路，链路的两端可以都是交换机，也可以是交换机和路由器，还可以是主机和交换机或路由器。Trunk 的主要功能就是仅通过一条链路就可以连接多个 VLAN。在缺省配置的情况下交换机的所有端口都是属于同一 VLAN。

答案：（59）B，（60）D

以太网 100BASE-TX 标准规定的传输介质时 (61) 。（网络知识-传输介质）

（61）A.3 类 UTP　　B.5 类 UTP　　C.单模光纤　　D.多模光纤

许多网络通信需要进行组播，以下选项中不采用组播协议的应用是 (62)。在 IPv4 中把 (63) 类地址作为组播地址。（网络知识-网络协议）

（62）A.VOD　　B.Netmeeting　　C.CSCW　　D.FTP

（63）A.A　　B.B　　C.D　　D.E

将双绞线制作成交叉线（一端按 EIA/TIA 568A 线序，另一端按 EIA/TLA 568B 线序），该双绞线连接的两个设备可为 (64)。（网络知识-传输介质）

（64）A.网卡与网卡　　B.网卡与交换机
　　C.网卡与集线器　　D.交换机的以太口与下一级交换机的 UPLINK 口

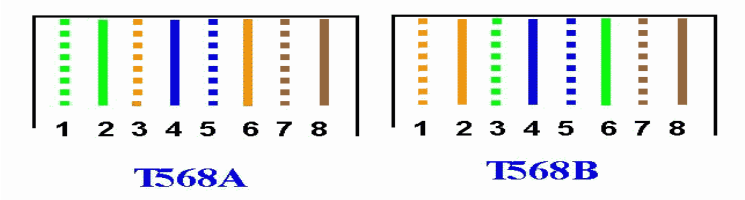
解答：

传输介质：关于连接的标准有两个：

T568A---白绿、绿色、白橙、蓝色、白蓝、橙色、白褐、褐色

T568B---白橙、橙色、白绿、蓝色、白蓝、绿色、白褐、褐色

T568A/T568B



八根线要根据标准插入到插头中

T568A/T568B

二者没有本质的区别，只是颜色上的区别

本质的问题是要保证：

1,2 线对是一个绕对

3,6 线对是一个绕对

4,5 线对是一个绕对

7,8 线对是一个绕对

大家知道网线应该是两头都要做 RJ45 头的。而两种接线的方法就可以做出两种线来——一种是平行线（也叫直连线）一种是交叉线。所谓的平行线（又叫直连线）实际上就是线的两头采用同样的做法——要么两头都用 T568A 来做，要么两头都用 T568B 来做。而交叉线就是一头 T568A 而另外一头就用 T568B——也就是两头不一样的做法——但是有一点，请遵循连线的规范。平常实际应用中是怎么使用这两种线的呢？

应用类别接线方法

计算机——计算机 交叉线

计算机——交换机 平行线

交换机——交换机 交叉线或者平行线

网卡——网卡 交叉线

交换机用 RJ45 线连接到交换机把两个交换机串起来就称做级连。级连的作用就是当一台交换机的接口数太少了的时候，将两个交换机“堆叠”起来，通过 RJ45 线来达到组成一个更多口的“大”交换机。而交换机到交换机的级连一共有三种不同的方式。

1、交换机的 UPLINK 口连接到交换机的普通口；

2、交换机的 UPLINK 口连接到交换机的 UPLINK 口；

3、交换机的普通口连接到交换机的普通口；

这三种级连的接线也是不同的：第一种情况用平行线；第二种情况用交叉线；第三种情况也用交叉线。给大家一个方便记忆的方法，那就是交换机级连中，**如果你要进行级连的两口的属性相同（要么都是 UPLINK 口，要么都是普通口），那么就一定用交叉线了**！其他情况就用平行线了。

网络传输介质：网络中传输数据、连接各网络站点的实体。网络信息还可以利用无线电系统、微波无线系统和红外技术等传输。目前常见的网络传输介质有：双绞线、同轴电缆、光纤等。一、双绞线电缆(TP)：将一对以上的双绞线封装在一个绝缘外套中，为了降低信号的干扰程度，电缆中的每一对双绞线一般是由两根绝缘铜导线相互扭绕而成，也因此把它称为双绞线。双绞线分为分 为非屏蔽双绞线(UTP)和屏蔽双绞线(STP)。

目前市面上出售的 UTP 分为 3 类，4 类，5 类和超 5 类四种：
3 类：传输速率支持 10Mbps，外层保护胶皮较薄，皮上注有“cat3”
4 类：网络中不常用
5 类（超 5 类）：传输速率支持 100Mbps 或 10Mbps，外层保护胶皮较厚，皮上注有“cat5”
超 5 类双绞线在传送信号时比普通 5 类双绞线的衰减更小，抗干扰能力更强，在 100M 网络中，受干扰程度只有普通 5 类线的 1/4，目前较少应用。
STP 分为 3 类和 5 类两种，STP 的内部与 UTP 相同，外包铝箔，抗干扰能力强、传输速率高但价格昂贵。双绞线一般用于星型网的布线连接，两端安装有 RJ-45 头(水晶头)，连接网卡与集线器，最大网线长度为 100 米，如果要加大网络的范围，在两段双绞线之间可安装中继器，最多可安装 4 个中继器，如安装 4 个中继器连 5 个网段，最大传输范围可达 500 米。
二、同轴电缆：由一根空心的外圆柱导体和一根位于中心轴线的内导线组成，内导线和圆柱导体及外界之间用绝缘材料隔开。按直径的不同，可分为粗缆和细缆两种：
粗缆：传输距离长，性能好但成本高、网络安装、维护困难，一般用于大型局域网的干线，连接时两端需终接器。

(1)粗缆与外部收发器相连。

(2)收发器与网卡之间用 AUI 电缆相连。

(3)网卡必须有 AUI 接口（15 针 D 型接口）：每段 500 米，100 个用户，4 个中继器可达 2500 米，收发器之间最小 2.5 米，收发器电缆最大 50 米。

细缆：与 BNC 网卡相连，两端装 50 欧的终端电阻。用 T 型头，T 型头之间最小 0.5 米。细缆网络每段干线长度最大为 185 米，每段干线最多接入 30 个用户。如采用 4 个中继器连接 5 个网段，网络最大距离可达 925 米。

细缆安装较容易，造价较低，但日常维护不方便，一旦一个用户出故障，便会影响其他用户的正常工作。

根据传输频带的不同，可分为基带同轴电缆和宽带同轴电缆两种类型：

基带：数字信号，信号占整个信道，同一时间内能传送一种信号。

宽带：可传送不同频率的信号。

三、光纤：是由一组光导纤维组成的用来传播光束的、细小而柔韧的传输介质。应用光学原理，由光发送机产生光束，将电信号变为光信号，再把光信号导入光纤，在另一端由光接收机接收光纤上传来的光信号，并把它变为电信号，经解码后再处理。与其它传输介质比较，光纤的电磁绝缘性能好、信号衰小、频带宽、传输速度快、传输距离大。主要用于要求传输距离较长、布线条件特殊的主干网连接。
分为单模光纤和多模光纤：
单模光纤：由激光作光源，仅有一条光通路，传输距离长，2 千米以上。
多模光纤：由二极管发光，低速短距离，2 千米以内。
在（62）中，是关于单播与组播的区别。传统的点对点单播通信，在发送方和每一接收方需要单独的数据通道。在这种通信方式下，源 IP 主机向指定的目标 IP 主机发送信息包。IP 信息包中的目标地址就是 IP 网络中惟一的主机地址。从一台主机送出的每个数据包只能传送给一个目标主机，通过路由器或交换机将这些 IP 信息包从源主机发送到目标主机。在源主机和目标主机之间的路径上的每一个路由器都维护由单播路由协议生成的单播路由信息库，并根据数据包中的 IP 目标地址在单播路由信息库中查找单播包转发路径。这种传送方式称为单播。在单播方式下，如果有另外的多个用户希望同时获得这个数据包的拷贝是不可能的。发送信息的主机必须向每个希望接收此数据包的用户发送一份单独的数据包拷贝。这种巨大的冗余会带来很大的代价，首先，会给发送数据的源主机带来沉重的负担，因为它必

须对每个要求都做出响应，这使得负担过于沉重主机的响应会大大延长。其次对路由器和交换机的性能也提出了更高的要求，管理人员被迫购买本来不必要的硬件和带宽来保证一定的服务质量。解决上述这些 IP 单播和 IP 广播问题的办法是构建一种具有组播能力的网络，允许路由器一次将数据包复制到多个通道上。采用组播方式，单台服务器能够对几十万台主机机同时发送连续数据流而无延时。组播发送方只要发送一个信息包而不是很多个，所有目的地同时收到同一信息包，更及时，更同步，可以把信息发送到任意不知名目的地，能减少网络上传输的信息包的总量。网络成本变得相当低廉，可达到从未有过的传送能力。组播应用于视频会议、视频点播、多媒体应用、数据分发、实时数据组播和游戏和仿真。

答案：（61）B，（62）D，（63）C，（64）A

以下不属于中间件技术的是（65）。（网络知识-网络新技术）

（65）A.Java RMI　　B.CORBA　　C.DCOM　　D.Java Applet

解答：计算机技术迅速发展。从硬件技术看，CPU 速度越来越高，处理能力越来越强；从软件技术看，应用程序的规模不断扩大，特别是 Internet 及 WWW 的出现，使计算机的应用范围更为广阔，许多应用程序需在网络环境的异构平台上运行。这一切都对新一代的软件开发提出了新的需求。在这种分布异构环境中，通常存在多种硬件系统平台(如 PC，工作站，小型机等)，在这些硬件平台上又存在各种各样的系统软件(如不同的操作系统、数据库、语言编译器等)，以及多种风格各异的用户界面，这些硬件系统平台还可能采用不同的网络协议和网络体系结构连接。如何把这些系统集成起来并开发新的应用是一个非常现实而困难的问题。为解决分布异构问题，人们提出了中间件(middleware)的概念。中间件是位于平台(硬件和操作系统)和应用之间的通用服务。考察当前主流的分布计算技术平台,主要有 OMG 的 CORBA、Sun 的 J2EE（J2EE 同时支持 RMI 和 IIOP）和 Microsoft DNA 2000（以 Microsoft 为首的 DCOM/COM/COM+阵营）。它们都是支持服务器端中间件技术开发的平台,但都有其各自的特点。

答案：D

分析完毕

祝广大朋友顺利通过考试！