第 1 章　过关习题

【例 1-1】分析：8 位整数补码的表示范围为−128～+127。$[-128]_{补}$=10000000，$[127]_{补}$=01111111。对于选项 C，很明显 127+1=128 超过了 8 位整数的表示范围。也可以通过计算来证明：

```
 01111111
+00000001
----------
 10000000
```

两个正数相加的结果是−128，产生错误的原因就是溢出。

答案：C

【例 1-2】 分析：程序计数器的功能是用于存放下一条指令所在单元的地址。单片机及汇编语言中常将其称作 PC(Program Counter)。

为了保证程序(在操作系统中理解为进程)能够连续地执行下去，CPU 必须具有某些手段来确定下一条指令的地址，而程序计数器正是起到这种作用，所以通常又称为指令计数器。在程序开始执行前，必须将它的起始地址，即程序的第一条指令所在的内存单元地址送入 PC，因此程序计数器(PC)的内容即是从内存提取的第一条指令的地址。当执行指令时，CPU 将自动修改 PC 的内容，即每执行一条指令 PC 增加一个量，这个量等于指令所含的字节数，以便使其保持的总是将要执行的下一条指令的地址。由于大多数指令都是按顺序来执行的，所以修改的过程通常只是简单地对 PC 加 1。

当程序转移时，转移指令执行的最终结果就是要改变 PC 的值，此 PC 值就是转去的地址，以此实现转移。有些机器中也称 PC 为指令指针 IP(Instruction Pointer)。

答案：A

【例 1-3】分析：程序计数器的功能是用于存放下一条指令所在单元的地址。

答案：C

【例 1-4】分析：为了保证程序能够连续地执行下去，CPU 必须具有某些手段来确定一条指令的地址。程序计数器的作用就是控制下一指令的位置，包括控制跳转。

答案：A

【例 1-5】分析：程序执行过程中，Cache 和主存都被分成若干个大小相等的块，每块由若干个字节组成，主存和 Cache 的数据交换是以块为单位，需要考虑二者地址的逻辑关系。

地址映像是指把主存地址空间映像到 Cache 地址空间，即按某种规则把主存的块复制到 Cache 中。

映像可分为全相联映像、直接映像和组相联映像。Cache 的地址变换和数据块的替换算法都采用硬件实现。

答案：A

【例 1-6】 分析：CPU 对 I/O 端口的编址方式主要有两种：一是独立编址方式，二是统一编址方式。独立编址方式是指系统使用一个不同于主存地址空间之外的单独的一个地址空间为外围设备及接口中的所有 I/O 端口分配 I/O 地址，在这种方式下，CPU 指令系统中有专门的用于与设备进行数据传输的输入/输出指令，对设备的访问必须使用这些专用指令进行。 统一编址方式是指 I/O 端口与主存单元使用同一个地址空间进行统一编址，在这种方式下，CPU 指令系统中无须设置专门的与设备进行数据传输的输入/输出指令，I/O 端口被当成主存单元同样对待，对主存单元进行访问和操作的指令可以同样用于对 I/O 端口的访问和操作。

答案：D

【例 1-7】分析：DMA(Direct Memory Access)技术通过硬件控制将数据块在内存和输入/输出设备间直接传送，不需要 CPU 的任何干涉，只需 CPU 在过程开始启动与过程结束时进行处理，实际操作由 DMA 硬件直接执行完成，CPU 在传送过程中可做别的事情。

答案：C

【例 1-8】 分析：总线复用方式指的是数据和地址在同一个总线上传输的方式。所谓复用传送就是指多个用户共享公用信道的一种机制，目前最常见的主要有时分多路复用、频分多路复用和码分多路复用等，优点在于各子系统的信息能有效及时地被传送，可避免信号彼此间的相互干扰和物理空间过于拥挤。

答案：C

【例 1-9】 分析：计算机系统中采用总线结构可以减少信息传输线的数量。

答案：C

【例 1-10】分析：指令系统中采用不同寻址方式的目的是缩短指令长度，扩大寻址空间，提高编程灵活性。

答案：D

【例 1-11】分析：并行的可靠度=1−(1−R)(1−R)

总可靠度=(1−(1−R)(1−R))・R・(1−(1−R)(1−R))

答案：D

【例 1-12】 分析：在三态模型中，进程有运行、就绪和阻塞三种基本状态。一个进程正在等待某一事件而暂时停止，该进程处于阻塞状态。等待的事件发生时，阻塞状态的进程被唤醒并转换为就绪状态。进程由就绪状态到运行状态是由调度程序的调度引起的，当进程的时间片用完后进入就绪状态，等待下一次的调度。

答案：A

【例 1-13】分析：文件系统一般采用一级目录结构、二级目录结构和多级目录结构。在多级目录结构的文件系统中，文件的全路径名可能较长，也会涉及多次磁盘访问，为了提高效率，操作系统提供设置工作目录的机制，每个用户都有自己的工作目录，任一目录节点都可以被设置为工作目录。一旦某个目录节点被设置成工作目录，相应的目录文件有关内容就会被调入主存，这样，对以工作目录为根的子树内任一文件的查找时间会缩短，从工作目录出发的文件路径名称为文件的相对路径名。

所以全文件名即为 D:\Program\Java-prog\f1.java；而相对路径则为从当前工作目录 Program 出发的路径名，即为 Java-prog\。

答案：(1)C　(2)A

【例 1-14】分析：在操作系统中，由文件管理系统实现文件的统一管理。文件系统采用按名存取的方式，为了实现按名存取，系统采用文件目录为每个文件设置用于描述和控制文件的数据结构，对外存中的文件进行组织和管理。

答案：C

【例 1-15】分析：软件的生命周期可以分为四个活动时期：软件分析、软件设计、编码与测试、运行与维护。其中软件设计又可以分为概要设计和详细设计两个阶段。概要设计是设计软件的结构、组成的模块、模块的层次结构、模块的调用关系以及每个模块的功能。而详细设计就是为每个模块完成的功能进行具体描述，将功能描述转换为精确的、结构化的过程描述。

答案：B

【例 1-16】分析：数据流图用来描述数据流从输入到输出的变换流程。它以图形的方式描绘数据在系统中流动和处理的过程，它只反映系统必须完成的逻辑功能，所以是一种功能模型。

数据流图仅描述了系统的“分解”，但没有对图中各成分进行说明。

数据字典就是用来定义数据流图中各个成分的含义的。数据字典有 4 类条目，包括数据流、数据项、数据存储和基本加工。

实体−关系(E-R)图在软件设计和数据库设计中经常用到，用于描述数据对象、对象的属性和对象之间的关系。

状态-迁移图通过描述系统的状态以及引起变化的事件来描述系统的行为，并指明特定事件的结构和执行的动作。

此题中要进行接口设计，显然数据流图更为合适。

答案：A

【例 1-17】分析：一般可将耦合度从弱到强分为以下七级。

- 非直接耦合：指两个模块中任一个都不依赖对方独立工作。这类耦合度最低。
- 数据耦合：指两个模块间只是通过参数表传递简单数据。
- 特征耦合：指两个模块都与同一个数据结构有关。
- 控制耦合：指两个模块间传递的信息中含有控制信息。
- 外部耦合：指若干模块都与同一个外部环境关联，例如 I/O 处理使所有 I/O 模块与特定的设备、格式和通信协议相关联。
- 公共耦合：指两个或多个模块通过引用一个公共区的数据而发生相互作用。
- 内容耦合：耦合度最高。出现内容耦合的情形包括：一个模块使用另一模块内部的控制和控制信息；一个模块直接转移到另一模块内部；等等。

一般来说，尽量使用数据耦合，少用控制耦合，限制外部耦合，完全不用内容耦合。

答案：D

【例 1-18】分析：在瀑布模型中，软件开发的各项活动严格按照线性方式进行，当前活动接受上一项活动的工作结果，实施完成所需的工作内容。当前活动的工作结果需要进行验证，如果验证通过，则该结果作为下一项活动的输入，继续进行下一项活动，否则返回修改。瀑布模型要求每个阶段都要仔细验证，但是，这种模型的线性过程太理想化，已不再适合现代的软件开发模式，几乎被业界抛弃。

快速原型模型的第一步是建造一个快速原型，实现客户或未来的用户与系统的交互，用户或客户对原型进行评价，进一步细化待开发软件的需求。快速原型通过逐步调整原型使其满足客户的要求，开发人员可以确定客户的真正需求是什么，在此基础上开发客户满意的软件产品。

V 模型是在快速应用开发模型基础上演变而来，由于将整个开发过程构造成一个“V”字形而得名。V 模型强调软件开发的协作和速度，将软件实现和验证有机地结合起来，在保证较高的软件质量情况下缩短开发周期。

螺旋模型将瀑布模型和快速原型模型结合起来，强调了其他模型所忽视的风险分析，特别适合于大型复杂的系统。螺旋模型强调风险分析，但要求许多客户接受、相信这种分析并做出相关反应是不容易的，因此，这种模型往往适合于内部的大规模软件开发。

答案：B

【例 1-19】分析：本题考查的是 PERT 图。每个任务可以有一个松弛时间，表示在不影响整个工期的前提下，完成该任务有多少余地。而松弛时间为 0 的任务是完成整个工程的关键路径。分析图中每个任务的工期可知，关键路径为 A→B→D→I→J→L，可计算出其路径长度为 20。

答案：A

【例 1-20】分析：软件产品的可靠度取决于潜在错误的数量、潜在错误的位置以及软件产品的使用方法。

答案：D

【例 1-21】分析：一定会发生的事件，就不叫风险了。

答案：B

【例 1-22】分析：即使将专家判断方法、启发式方法和机器学习方法结合起来，也不可能得到精确的估算结果。

答案：D

【例 1-23】分析：本题考查的是 PERT 图。每个任务可以有一个松弛时间，表示在不影响整个工期的前提下，完成该任务有多少余地。而松弛时间为 0 的任务是完成整个工程的关键路径。本题中关键路径是：(0)→(2)→(5)→(7)→(8)→(9)。

答案：B

【例 1-24】分析：PERT 图给出了每个任务的开始时间、结束时间和完成该任务所需要的时间，同时

还给出了任务之间的依赖关系，即哪些任务完成后才能执行另外一些任务。PERT 图的不足是不能反映任务之间的并行关系。

关键路径是松弛时间为 0 的任务完成过程所经历的路径。本题的图中没有给出松弛时间，因此关键路径是耗时最长的路径，即 A→B→E→G→H→J→K。

答案：(1)C　(2)B

【例 1-25】分析：软件复杂性度量的参数很多，如下。

- 规模，即总共的指令数，或源程序行数。
- 难度，通常由程序中出现的操作数的数目所决定的量来表示。
- 结构，通常用与程序结构有关的度量来表示。
- 智能度，即算法的难易程度。

软件复杂性主要表现在程序的复杂性。程序的复杂性主要指模块内程序的复杂性。它直接关联到软件开发费用的多少、开发周期长短和软件内部潜伏错误的多少。

答案：B

【例 1-26】分析：著作权的合理使用是指针对他人已经发表的作品，根据法律的规定，在不必征得著作权人同意的情况下，而无偿使用其作品的行为，但应指明作者姓名、作品名称，并不得侵犯著作权人的其他权利。

法定许可使用制度是指依照著作权法的规定，传播者在使用他人已经发表但没有著作权保留声明的作品时，可以不经著作权人许可，但应向其支付报酬，并尊重著作权人其他权利的制度。

法定许可与合理使用的主要区别在于：首先，合理使用无须向著作权人支付报酬，而法定许可则必须向著作权人支付报酬；其次，合理使用的范围较为广泛，我国著作权法第二十二条规定了 12 种，而法定许可的范围较窄。

答案：A

【例 1-27】分析：根据《计算机软件保护条例》第八条的规定，软件著作权人享有若干项权利，其中包括翻译权。在条例中对翻译权的定义是“将原软件从一种自然语言文字转换成另一种自然语言文字的权利”。

答案：B

【例 1-28】分析：在《反不正当竞争法》中商业秘密被定义为“不为公众所知悉的、能为权利人带来经济利益的、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”。软件中包含着技术秘密和经营秘密，具有商业秘密的特征，即使软件尚未开发完成，在软件开发中所形成的知识内容也构成商业秘密。因此，可以利用商业秘密权对软件的技术信息、经营信息提供保护。

答案：C

第 2 章　过关习题

【例 2-1】分析：总的时间= 4000 比特长的数据包的发送时间+卫星传输延迟时间。

发送 4000 比特需要 4000/64k=62.5ms。卫星传输延迟较大，大约为 270ms。因此总的时间为 62.5+270=332.5ms。

答案：D

【例 2-2】分析：总时间=线路延迟+调制延迟。

线路延迟=传输距离/传输速度。电信号在电缆上的传输速度大约是 20 万公里/秒，因此线路延迟=400/200 000 = 2ms。

调制延迟=数据帧大小/比特率=3000/4800=625ms

因此，总时间=2+625=627ms

答案：D

【例 2-3】分析：多模光纤纤芯直径较大，可为 50μm 和 61.5μm 两种，单模光纤纤芯直径较小，一般为 9～10μm，可见多模光纤比单模光纤的纤芯直径粗。

由于单模光纤纤芯直径很小，理论上只能传导一种模式的光，从而避免了模态色散，光在其中无反射地沿直线传播，因此具有较高的数据速率，传输距离较长，但成本较高。相对而言，多模光纤的传输速率较低，传输距离较短。

答案：D

【例 2-4】分析：多模光纤纤芯直径较大，有 50μm 和 62.5μm 两种，包层外径 125μm；单模光纤纤芯直径较小，一般为 9～10μm，包层外径也为 125μm，可见选项 C、D 错误。多模光纤传输的距离比较近，一般只有几公里，单模光纤中心玻璃芯很细(芯径一般为 9μm 或 10μm)，只能传输一种模式的光。因此，其模间色散很小，适用于远程通信，所以选项 A 错误。单模光纤价格比较贵，多模光纤价格便宜，所以选项 B 正确。

答案：B

【例 2-5】分析：Manchester 编码是一种双相码，用电平的跳变表示二进制位：用高电平到低电平的转换边表示“0”，用低电平到高电平的转换边表示“1”，相反表示也可。这种编码的电平转换既表示了数据，也可作为定时信号使用。由于每位中间都有一次电平跳变，因此波特率是数据传输速率的两倍，可见编码的效率仅为 50%。Manchester 编码应用在以太网中，而不是高速以太网中。

答案：D

【例 2-6】分析：曼彻斯特编码每个比特位需要两次信号变化，因此编码效率只有 50%，这意味着比特率只是波特率的一半。这种编码效率在低速的通信系统(如 10 兆以太网)中尚可以接受，但在高速通信系统中是难以接受的。

*m*B/*n*B 编码的效率计算公式为 $m/n\times100\%$。由于 $m<n$，所以 *m*B/*n*B 编码的效率并不能达到 100%，对于 4B/5B 编码和 8B/10B 编码，编码效率均为 80%，而 64B/66B 编码的编码效率则达到 96.97%。

答案：(1)B　(2)C

【例 2-7】分析：曼彻斯特编码是一种双相码。高电平到低电平的转换边表示 0，而用低电平到高电平的转换边表示 1，位中间的电平转换边既表示了数据代码，也作为定时信号使用。差分曼彻斯特编码也是一种双相码。这种编码的码元中间的电平转换边只作为定时信号，而不表示数据。数据的表示在于每一位开始处是否有电平转换：有电平转换表示 0，无电平转换表示 1。所以图中所示的比特串应为 01010011。

答案：C

【例 2-8】分析：数据传输速率 $R=B\log_2N$，其中 *B* 为码元速率，*N* 为码元的种类。本题采用二相差分相移键控(2DPSK)对信号进行调制。2DPSK 不是利用载波相位的绝对数值传送数字信息，而是用前后码元的相对载波相位值传送数字信息。载波的起始相位与前一码元载波的起始相位相同表示“0”，载波的起始相位与前一码元载波的起始相位相差π表示“1”。采用 2DPSK 调制，码元有两种状态，即 $N=2$，可以计算出数据传输速率为 $300\times\log_22=300$bps。

答案：A

【例 2-9】分析：对数字信号的调制可分为幅度键控(ASK)、移频键控(FSK)、相移键控(PSK)。

PSK：用载波的起始相位的变化表示 0 和 1，又可分为相对 PSK 和绝对 PSK。从图 2-5 中可看出，0、1 变化时，载波的相位发生变化，所以此题选 C。

答案：C

【例 2-10】分析：根据奈奎斯特定理：如果采样速率大于模拟信号最高频率的两倍，则可以用得到的样本空间恢复原来的模拟信号。可知，要是得到的样本信号不失真，采样频率必须大于 12MHz。

答案：B

【例 2-11】分析：奈奎斯特证明：当采样频率大于模拟信号最高频分量频率的两倍时，所得的离散信号可以无失真地还原回被采样的模拟信号。

答案：D

【例 2-12】分析：数据传输速率为每秒传送的位数。本题中，每秒传送 100 个字符，每个字符中的有

效数据占 7 位，因此每秒传送的有效数据为 700b，则有效数据速率为 700bps，总的数据速率为 1100bps。

答案：B

【例 2-13】分析：E1 载波在北美和日本以外的国家中使用(欧洲标准)。该载波把一个时分复用帧(其长度 T=125μs)划分为 32 个相等的时隙，每个时隙 8 位，时隙的编号为 CH0～CH31，其中时隙 CH0 用作帧同步，时隙 CH16 用来传送信令，其他 30 个时隙用作 30 个话路。E1 信道的传输速率为 8×32b/125μs =2.048Mbps。而每个话路的传输速率为 8/125μs=64kbps。

答案：(1)B (2)B

【例 2-14】分析：STM-1 为速率 155.520Mbps 的同步传输模块(Synchronous Transfer Module)，是 SDH 信号的最基本模块，称为第 1 级同步传输模块。四个 STM-1 同步复用构成 STM-4，可知 STM-4 的数据速率为 155.520×4=622.080Mbps。

答案：(1)A (2)B

【例 2-15】分析：生成多项式 $G(x)=x^4+x+1$ 对应的二进制序列码为 10011，将信息码后面补四个 0，然后与序列码 10011 进行“按位异或”运算，如下：

```
1 0 0 1 1 | 1 0 1 1 1 0 0 0 0   —— 最后4个0是补位
            1 0 0 1 1
              1 0 0 0 0
              1 0 0 1 1
                    1 1 0 0
```

答案：D

第 3 章　过关习题

【例 3-1】分析：HDLC(High-Level Data Link Control，高级数据链路控制)协议是国际标准化组织根据 IBM 公司的 SDLC 协议扩充开发而成的。它是一种面向位的数据链路控制协议。

答案：A

【例 3-2】分析：FR(Frame Relay，帧中继)向用户提供面向连接的通信服务。FR 省略了帧编号、差错控制、流量控制、应答、监视等功能，把这些功能全部交给用户终端去完成，大大节省了交换机的开销，降低了时延，提高了信息吞吐量。

答案：B

【例 3-3】分析：ATM 高层定义了如下 4 类业务。

- 固定比特率(CBR) 业务，用于模拟铜线和光纤通道，使得当前的电话系统可以平滑地转换到 B-ISDN，也适用于交互式话音和视频流。
- 变化比特率(VBR)业务，可分为：实时变化比特率业务，交换式压缩视频信号属于这一类业务；非实时变化比特率业务，多媒体电子邮件属于这一类业务。
- 不定比特率(UBR)业务，可用于传输 IP 分组。文件传输、电子邮件和 USENET 新闻是这类业务的潜在应用领域。
- 有效比特率(ABR)业务，用于突发式通信。

压缩视频信号的传送属于 VBR 业务。

答案：B

【例 3-4】分析：对于选择重发 ARQ 协议，窗口的大小有一定的限制。如果窗口过大，会出现接收窗口滑动最大距离后与旧的接收窗口重叠的现象，造成接收器误把重发的帧当做新到的帧。为了避免这种错误就要缩小窗口，当窗口的大小缩小为帧编号数的一半时就可以避免错误。所以选择重发 ARQ 协议时，窗口的最大值应为帧编号数的一半，即 $W \leqslant 2^{k-1}$ 。

答案：B

【例 3-5】分析：帧中继在第二层建立虚电路，用帧方式承载数据业务。FR 的帧层比 HDLC 操作简单，只做检错，不重传，只有拥塞控制，没有滑动窗口式的流控。帧中继协议是 LAP-D(Link Access Protocol

Channel D，D 信道链路访问协议)，它为 FR 进行信令管理提供数据链路层支持。LAP-D 与 X.25 的 LAP-B 基本相同，但简单一些，省去了控制字段。

答案：D

【例 3-6】分析：RS-232-C 采用 V.28 标准电路。V.28 的驱动器是单端信号源，所有信号共用一根公共地线，信号源产生 3～15V 的信号，负载输入阻抗为 3～7kΩ，数据传输速率为 20kbps，传输距离不大于 15m。

答案：(1)B　(2)B

【例 3-7】分析：HDLC 协议的全称是高级数据链路控制(High Level Data Link Control)协议，是一种面向比特的数据链路控制协议。HDLC 使用统一结构的帧进行同步传输，HDLC 帧由 6 个字段组成，用一特殊的位模式 01111110 作为标志以确定帧的边界。链路上所有的站都在不断地探索标志模式，一旦得到一个标志就开始接收帧；在接收的过程中如果发现另一个标志，则认为该帧结束了。

答案：(1)A　(2)B

第 4 章　过关习题

【例 4-1】分析：按照二进制指数后退算法，后退时延的取值范围与重发次数 n 形成二进制指数关系。随着重发次数 n 的增加，后退时延 t_ζ 的取值范围按 2 的指数增大。即：第一次试发时 n 的值为 0，每冲突一次 n 的值加 1，并按下式计算后退时延：

$$\begin{cases}\zeta = \text{random}[0,\ 2^n] \\ t_\zeta = \zeta_\tau\end{cases}$$

为了避免无限制的重发，要对重发次数 n 进行限制。通常当 n 增加到某一个最大值时停止发送，并向上层协议报告发送错误，等待处理。

答案：B

【例 4-2】分析：IEEE 802.11 标准定义了两种操作模式：第一种模式是 DCF(Distributed Coordination Function，分布式协调功能)，该模式没有中心控制设备，所有站点都在竞争信道；另一种模式是 PCF(Point Coordination Function，点协调功能)，该模式有基站，作为中心控制设备通过轮询机制控制决定各个站点的传输顺序。根据 IEEE 802.11 标准，DCF 是必需的而 PCF 是可选的。

CSMA/CA 协议应用于 DCF 下，目的在于解决在允许竞争的情况下信道如何分配的问题。它支持的操作方式有两种。第一种操作方式采用延时算法进行访问控制。当一个要发送数据的站点检测到信道空闲时，站点需继续监听与 IFS(Interframe Space，帧间间隔)相等的一段时间，若此时信道依然空闲，站点就可以发送帧；如果检测到信道正忙，则发送站点推迟到信道空闲时再发送数据。若冲突发生，则发生冲突的站点按照截断二进制指数退避算法延迟一段时间后，再试着重新发送数据。另一种操作方式类似于发收双方的握手过程。它是基于 MACAW(Multiple Access with Collision Avoidance for Wireless，带冲突避免的无线多路访问)，采用虚拟信道监听的方法。CSMA/CA 协议利用 IFS 机制让 PCF 和 DCF 共存在同一个通信单元内。

答案：C

【例 4-3】分析：(1)　非坚持型监听算法

当一个站准备好帧发送之前先监听信道。

①　若信道空闲，立即发送；否则转②。

②　若信道忙，则后退一个随机时间，重复①。

由于随机时延后退，从而减少了冲突的概率；然而，可能出现的问题是因为后退而使信道闲置一段时

间，这使信道的利用率降低，并增加了发送时延。

(2) 1-坚持型监听算法

当一个站准备好帧，发送之前先监听信道：

① 若信道空闲，立即发送；否则转②。

② 若信道忙，继续监听，直到信道空闲后立即发送。

1-坚持型监听算法的优缺点与前一种正好相反：有利于抢占信道，减少信道空闲时间；但是多个站同时都在监听信道时必然发生冲突。

(3) P-坚持型监听算法

P-坚持型监听算法吸取了以上两种算法的优点，但较为复杂。

① 若信道空闲，以概率 P 发送，以概率(1−P)延迟一个时间单位。一个时间单位等于网络传输时延期 τ 。

② 若信道忙，继续监听直到信道空闲，转①。

③ 若发送延迟一个时间单位 τ ，则重复①

答案：(1)A (2)B

【例 4-4】分析：基带长度为 1000m，传播速度为 200m/μs，则单程需要的传播时间为 5μs，往返需要 10μs，而数据速率为 10Mbps，则最小帧长为 10Mbps×10μs =100b。

答案： B

【例 4-5】分析：非坚持型以太网在转发数据帧之前先监听信道，如果信道空闲，则立即发送，否则后退一个随机时间。由于随机时延后退，从而减少了冲突的概率，但是后退会使信道空闲一段时间，这使得信道的利用率低，浪费了带宽。因此选项 B 是正确的，D 是错误的。

坚持型以太网在监听到信道忙的时候，会继续监听，直到信道空闲后才发送。如果多个站同时在监听信道时会发生冲突。可见，坚持型监听算法有利于抢占信道，减少发送延迟，但冲突概率高。因此，选项 A 是错误的。

P-坚持型算法吸取了坚持型和非坚持型的优点，但较为复杂，概率 P 的选择是一个困难的问题。

答案：B

【例 4-6】分析：长度字段说明数据字段的长度，其最大值为 1500。802.3 同时用长度字段指示上层协议的类型，此时长度字段的值在 1501～65 535 之间。

答案：D

【例 4-7】分析：IEEE 802.3 规定的最小帧长为 64 字节，这个帧长是指从目标地址到校验和的长度。由于前导字段和帧起始符是在物理层上加上的，所以不包括在帧长中。

答案：B

【例 4-8】分析：以太网的最小帧长是 64 字节，当数据字段过短时，填充字段就发挥作用，维持最小帧长。

答案：D

【例 4-9】分析：100Base-TX 可使用两对五类 UTP 和两对 STP，100Base-FX 可使用一对多模光纤或一对单模光纤，100Base-T4 使用四对三类 UTP，100Base-T2 使用两对三类 UTP。

答案：C

【例 4-10】分析：帧突发在千兆以太网上是一种可选功能，它使一个站(特别是服务器)一次能连续发送多个帧，当一个站点需要发送很多短帧时，该站点先试图发送第一帧，该帧可能附加了扩展位的帧。一旦第一个帧发送成功，则具有帧突发功能的站点就能够继续发送其他帧，直至帧突发的总长度达到 1500 字节为止。

答案：C

【例 4-11】分析：100Base-TX 可使用两对五类 UTP 和两对 STP。

答案：C

【例 4-12】分析：802.3 标准协议参数如表 4-3 所示。

表 4-3 802.3 标准协议参数

标准	标准颁布时间	数据率/bps	拓扑	媒体	最大电缆网段长度/m	
					半双工	全双工
10BASE5	DIX-1980, 802.3-1983	10M	总线	一根 50Ω 同轴电缆(粗缆以太网)(直径 10mm)	500	不使用
10BASE2	802.3a-1985	10M	总线	一根 50Ω RG 58 同轴电缆(细缆以太网) (直径 5mm)	185	不使用
10Broad36	802.3b-1985	10M	总线	一根 75Ω CATV 宽带电缆	1800	不使用
FOIRL	802.3d-1987	10M	星型	两根光纤	1000	>1000
1BASE5	802.3e-1987	1M	星型	两对双绞线电话电缆	250	不使用
10BASE-T	802.3i-1990	10M	星型	两对 100Ω的三类或更好的 UTP 电缆	100	100
10BASE-FL	802.3j-1993	10M	星型	两根光纤	2000	>2000
10BASE-FB	802.3j-1993	10M	星型	两根光纤	2000	不使用
10BASE-FP	802.3j-1993	10M	星型	两根光纤	1000	不使用
100BASE-TX	802.3u-1995	100M	星型	两对 100Ω的五类 UTP 电缆	100	100
100BASE-FX	802.3u-1995	100M	星型	两根光纤	412	2000
100BASE-T4	802.3u-1995	100M	星型	4 对 100Ω的三类或更好的 UTP 电缆	100	不使用
100BASE-T2	802.3y-1997	100M	星型	两对 100Ω的三类或更好的 UTP 电缆	100	100
1000BASE-LX	802.3z-1998	1G	星型	长波长激光(1300nm)使用：		
				• 62.5μm 多模光纤	316	550
				• 50μm 多模光纤	316	550
				• 10μm 单模光纤	316	5000
1000BASE-SX	802.3z-1998	1G	星型	短波长激光(850nm)使用：		
				• 62.5μm 多模光纤	275	275
				• 50μm 多模光纤	316	550
1000BASE-CX	802.3z-1998	1G	星型	特殊屏蔽双铜线电缆	25	25
1000BASE-T	802.3ab-1999	1G	星型	4 对 100Ω的五类或更好的电缆	100	100
10GBASE-SR	802.3ae-2002	10G	星型	短波长激光(850nm)	不使用	65～300
10GBASE-SW	802.3ae-2002	10G	星型	短波长激光(850nm)	不使用	65～300
10GBASE-LX4	802.3ae-2002	10G	星型	长波长激光(1300nm)，WWDM- 多模光纤 单模光纤	不使用	300 10000
10GBASE-LR	802.3ae-2002	10G	星型	长波长激光 (1300 nm)使用单模光纤	不使用	10000
10GBase-LW	802.3ae-2002	10G	星型	长波长激光(1300nm)使用单模光纤	不使用	10000
10GBase-ER	802.3ae-2002	10G	星型	特长波长激光(1550nm)使用单模光纤	不使用	40000
10GBase-EW	802.3ae-2002	10G	星型	特长波长激光(1550nm)使用单模光纤	不使用	40000

答案：D

【例 4-13】分析：交换机之间的链路包括接入链路和中继链路。接入链路只能传输单个 VLAN 的数据包。中继技术实现了在多个交换机之间进行多个 VLAN 数据包的传输。数据包在中继链路上传输的时候，交换机在数据包的头信息中加上标记来指定相应的 VLAN ID。每一个数据包指定一个唯一的 VLAN ID。

当数据包通过中继链路后，去掉标记的同时把数据包交换到相应的 VLAN 端口。

答案：A

【例 4-14】分析：如果要实现 VTP 动态修剪，一般是在 VTP 服务器上配置。因为在 VTP 服务器上，即主交换机上进行启用，在整个域中的交换机上都会启用。服务器会将相关的配置同步更新到其他的 VTP 客户机上。在透明模式下，交换机不会学习服务器广播的配置信息，因此交换机不能配置为透明模式。

答案：B

【例 4-15】分析：VTP 有三种工作模式：服务器(Server)模式、客户机(Client)模式和透明(Transparent)模式，VTP 默认模式是服务器模式。

服务器模式的交换机可以设置 VLAN 配置参数，服务器会将配置参数发给其他交换机。客户机模式的交换机不可以设置 VLAN 配置参数，只能接受服务器模式的交换机发来的 VLAN 配置参数。透明模式的交换机是相对独立的，它允许设置 VLAN 配置参数，但不向其他交换机发送自己的配置参数。当透明模式的交换机收到服务器模式的交换机发来的 VLAN 配置参数时，仅仅是简单地转发给其他交换机，并不用来设置自己的 VLAN 参数。

答案：C

【例 4-16】分析：生成树协议的工作过程简单表述如下。

(1) 唯一根网桥的推选：各个网桥互相传递 BPDU 配置信息，系统的每个网桥都能监听到 BPDU，根据网桥标识共同“选举”出具有最大优先级的根网桥。如果优先级相同，则取具有最小网桥地址的网桥作为根网桥。根网桥默认每 2 秒发出 BPDU。

(2) 在每个非根网桥选出一个根端口：根网桥向系统广播其 BPDU，对一个网桥来说，具有最小根路径开销的端口选为根端口；如果根路径开销相同，则取端口标识最小的作为根端口，同时根端口处于转发模式。一个网桥只有一个根端口，根网桥没有根端口。

(3) 在每个网段选一个指定端口：每个网桥接收到一个 BPDU 帧时，同时发出一个 BPDU 帧说明离根网桥的路径开销。在同一个网段里，具有最小的根路径开销的端口被选为指定端口。如果根路径开销相同，则取网桥标识最小的作为指定端口。如果网桥标识也相同，则取端口标识最小的为指定端口。

(4) STP 设置根端口和指定端口进入转发模式，可以转发数据帧；而落选端口则进入阻塞模式，只侦听 BPDU，不转发数据帧。各网桥周期性地交换 BPDU 信息，保证系统拓扑结构的合理性。

答案：C

【例 4-17】分析：以太网交换机端口的功能是从与其相连的 LAN 上接收或传送数据。端口的状态由生成树算法规定，包括转发、学习、监听、阻塞和禁用状态。

(1) 转发(forwarding)：端口既可以发送和监听 BPDU，也可以转发数据帧。

(2) 学习(learning)：端口学习 MAC 地址，建立地址表，但不转发数据帧。

(3) 监听(listening)：端口监听 BPDU 以确保网络中不出现环路，但不学习接收帧的地址。

(4) 阻塞(blocking)：端口仅监听 BPDU，但不转发数据帧，也不学习接收帧的 MAC 地址。

(5) 禁用(disabled)：端口不参与生成树算法，既不发送和监听 BPDU，也不转发数据帧。

答案：C

【例 4-18】分析：(1) 根网桥的选择：各个网桥互相传递 BPDU 配置信息，系统的每个网桥都能监听到 BPDU，根据网桥标识共同“选举”出具有最大优先级的根网桥。如果优先级相同，则选取具有最小网桥地址的作为根网桥。本题中没有给出优先级，因为选取 ID 最小的网桥作为根网桥。

(2) 非根网桥的根端口选择：对一个网桥来说，具有最小根路径开销的端口选为根端口；如果根路径开销相同，则取端口标识最小的作为根端口，同时根端口处于转发模式。本题中，ID 为 92 的网桥连接网段 b 的端口为根端口，其根路径的开销最小。

答案：(1)A (2)B

第 5 章　过关习题

【例 5-1】分析：IEEE 在 2009 年 9 月批准了 802.11n 高速无线局域网标准。IEEE 802.11n 使用 2.4GHz 频段和 5GHz 频段，核心是 MIMO(multiple-input multiple-output，多入多出)和 OFDM 技术，传输速度 300Mbps，最高可达 600Mbps，可向下兼容 802.11b、802.11g。

答案：A

【例 5-2】分析：Peer to Peer 网络为对等网，是点对点模式。对等网结构比较简单，不需要有线网络和接入点支持，网上各台计算机有相同的功能，无主从之分。两台插上无线网卡的 PC 即可进行连接。

答案：B

【例 5-3】分析：IEEE 802.11g 标准使用了 IEEE 802.11a 的 OFDM 调制技术，和 IEEE 802.11b 一样运行在 2.4GHz 的 ISM 频段内，理论速度可达 54Mbps。

答案：C

【例 5-4】分析：IEEE 802.11i 是 IEEE 802.11 协议标准的扩展，于 2004 年正式被 IEEE 通过，取代原来脆弱的 WEP 加密技术。IEEE 802.11i 为使用 IEEE 802.11a、IEEE 802.11b 和 IEEE 802.11g 标准的网络提供加密技术和安全认证功能，这样的网络被描述为 RSN(Robust Security Network，健壮安全的网络)。

答案：D

【例 5-5】分析：802.11 标准如下：

- IEEE 802.11，1997 年，原始标准(2Mbps，工作在 2.4GHz)。
- IEEE 802.11a，1999 年，物理层补充(54Mbps，工作在 5GHz)。
- IEEE 802.11b，1999 年，物理层补充(11Mbps，工作在 2.4GHz)。
- IEEE 802.11c，符合 802.1D 的媒体接入控制层桥接(MAC Layer Bridging)。
- IEEE 802.11d，根据各国无线电规定做的调整。
- IEEE 802.11e，对服务等级(Quality of Service, QoS)的支持。
- IEEE 802.11f，基站的互连性(Inter-Access Point Protocol，IAPP)，2006 年 2 月被 IEEE 批准撤销。
- IEEE 802.11g，2003 年，物理层补充(54Mbps，工作在 2.4GHz)。
- IEEE 802.11h，2004 年，无线覆盖半径的调整，室内(indoor)和室外(outdoor)信道(5GHz 频段)。
- IEEE 802.11i，2004 年，无线网络的安全方面的补充。

答案：D

【例 5-6】分析：2.4GHz 是工业、科学和医疗专用的免费频段，在各国通用，频率范围在 2400～2483.5MHz。902～928MHz、5725～5850MHz 是美国用于免申请的频率。868GHz 频段则用于欧洲。

答案：D

【例 5-7】分析：无线局域网标准 802.11 的 MAC 和 802.3 协议的 MAC 非常相似，都是在一个共享媒体之上支持多个用户共享资源，由发送者在发送数据前先进行网络的可用性检测。在 802.3 协议中，是由一种称为 CSMA/CD(Carrier Sense Multiple Access with Collision Detection)的协议来完成调节，这个协议解决了在 Ethernet 上的各个工作站如何在线缆上进行传输的问题，利用它检测和避免当两个或两个以上的网络设备需要进行数据传送时网络上的冲突。在 802.11 无线局域网协议中，冲突的检测存在一定的问题，这个问题称为“Near/Far”现象，这是由于要检测冲突，设备必须能够一边接收数据信号一边传送数据信号，而这在无线系统中是无法办到的。

鉴于这个差异，在 802.11 中对 CSMA/CD 进行了一些调整，采用了新的协议 CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)或者 DCF(Distributed Coordination Function)。CSMA/CA 利用 ACK 信号来避免冲突的发生，也就是说，只有当客户端收到网络上返回的 ACK 信号后才确认送出的数据已经正确到达目的地址。

答案：B

第 6 章　过关习题

【例 6-1】分析：RFC 1918 规定的 B 类私网地址范围是 172.16.0.0～172.31.255.255。

答案：B

【例 6-2】分析：IP 地址除了标识一台主机外，还有几种具有特殊意义的形式(见表 5-3)。

表 5-3　特殊的 IP 地址

特殊地址	net-id	host-id	源地址使用	目的地址使用
本网络的本台主机	全 0	全 0	可以	不可以
本网络的某台主机	全 0	host-id	不可以	可以
网络地址	net-id	全 0	可以	可以
直接广播地址	net-id	全 1	不可以	可以
受限广播地址	全 1	全 1	不可以	可以
回送地址	127	任何数	可以	可以

所以 0.0.0.0 不能作为目标地址，192.168.0.255/24 不能作为源地址。

答案：(1)A　(2)D

【例 6-3】分析：私网 IP 地址参见表 5-2。

C 类地址每个网络的最多主机数为 254 台，现有 2000 台主机，则需要 8 个网络。

有 2000 台主机则需要的主机位数为 11 位，所以子网掩码应为 11111111 11111111 11111000 00000000，即 255.255.248.0。

答案：(1)B　(2)D

【例 6-4】分析：199.34.76.64/28 就表示该 IP 地址的网络号 net-id 和子网号 subnet-id 共占用 28 位，主机号占用 32−28=4 位，所以地址数为 16。

答案：B

【例 6-5】分析：C 类地址每个网络的最多主机数为 254 台，现由 16 个 C 类网络组成，则主机位数至少为 12 位，则网络掩码为 255.255.240.0。

答案：D

【例 6-6】分析：要得到网络或子网地址，只需将 IP 地址和子网掩码按位进行“与”运算就可以得到。

答案：C

【例 6-7】分析：一个 C 类地址是由 3 个字节的网络地址和 1 个字节的主机地址组成，网络地址的最高三位必须是“110”。24 位作为网络号，8 位作为主机号。共有 2^{21}(2 097 152)个网络号，每个 C 类地址主机数少于 2^8−2(254)个。现有 2000 台主机，则至少需要 8 个 C 类网络。

CIDR 使用各种长度的“网络前缀”(network-prefix)来代替分类地址中的网络号和子网号，而不像分类地址中只使用 1 字节、2 字节和 3 字节长的网络号。CIDR 不再使用“子网”概念而使用网络前缀，使 IP 地址从三级编址(使用子网掩码)又回到两级编址，但这是一个无分类的两级编址。CIDR 使用“斜线记法”，它又称为 CIDR 记法，即在 IP 地址后面加上一斜线“/”，然后写上网络前缀所占的比特数(这个数值对应于三级编址中子网掩码中比特 1 的个数)。由于需要 2000 台主机，2^{11}=2048，所以子网号为 11 位，所以地址掩码为 C，255.255.248.0。

由于该数据报的地址为 200.9.67.33，不在 Q2 分配的 C 类网络号中，所以 Q2 不可达。而 Q1 的网络地址为 200.9.64.0/21，所以该地址可达。

答案：(1)B　(2)C　(3)A

【例 6-8】分析：回应请求/应答(Echo Request / Echo Reply)报文(类型 8/0)。回应请求/应答的目的是测试目的主机是否可以到达。在该报文格式中存在标识符和序列号，这两者用于匹配请求和应答报文。请求者向目的主机发送一个回应请求，其中包含一个任选的数据区，目的主机收到后则发回一个回应应答，其中包含一个请求中的任选数据的复件。回应请求/应答报文以 IP 数据报方式在互联网中传输，如果成功接收到应答报文的话，则说明数据传输系统 IP 与 ICMP 软件工作正常，信宿主机可以到达。在 TCP/IP 实现中，用户的 ping 命令就是利用回应请求与应答报文测试信宿主机是否可以到达。

答案：A

【例 6-9】分析：ICMP 是 IP 协议的附属协议，属于网络层协议，其报文封装在 IP 协议数据单元中进行传送，主要用于网络设备和节点之间的控制和差错报告报文的传输。

答案：(1)B　(2)A

【例 6-10】分析：传输层协议通常有多种责任。一个是创建进程间通信，UDP 使用端口数来完成这项工作。另一个责任是在传输层提供控制机制，UDP 以一个最低的级别完成这项工作，无流控制机制和接收包的应答机制。但是，UDP 在一些范围上提供了差错控制。如果 UDP 在接收包中检测到了错误，它将静静地丢弃它。

传输层同样为进程提供了一个连接机制。这个进程必须能发送数据流到传输层。而发送站传输层的责任就是与接收站建立连接，将流放入传输单元，并编号，然后一个接一个地发送。接收站传输层的责任是等待一个相同进程中的不同的数据单元的到达，检查它们，将错误单元丢弃，并且以流的形式传递到接收进程中。

答案：(1)B　(2)C　(3)B　(4)A　(5)D

【例 6-11】分析：com、org、net 这三大类域名通常称为国际域名。cn 为中国国家级域名。

答案：A

【例 6-12】分析：DNS 域名解析工作过程如下。

(1)　客户机提交域名解析请求，并将该请求发送给本地的域名服务器。

(2)　当本地的域名服务器收到请求后，就先查询本地的缓存。如果有查询的 DNS 信息记录，则直接返回查询的结果。如果没有该记录，本地的域名服务器就把请求发给根域名服务器。

(3)　根域名服务器再返回给本地域名服务器一个所查询的顶级域名服务器的地址。

(4)　本地服务器再向返回的域名服务器发送请求。

(5)　接收到该查询请求的域名服务器查询其缓存和记录，如果有相关信息则返回本地域名服务器查询结果，否则通知本地域名服务器下级的域名服务器的地址。

(6)　本地域名服务器将查询请求发送给下级的域名服务器的地址，直到获取查询结果。

(7)　本地域名服务器将返回的结果保存到缓存，并且将结果返回给客户机，完成解析过程。

答案：C

【例 6-13】分析：递归解析工作过程如图 5-9 所示。

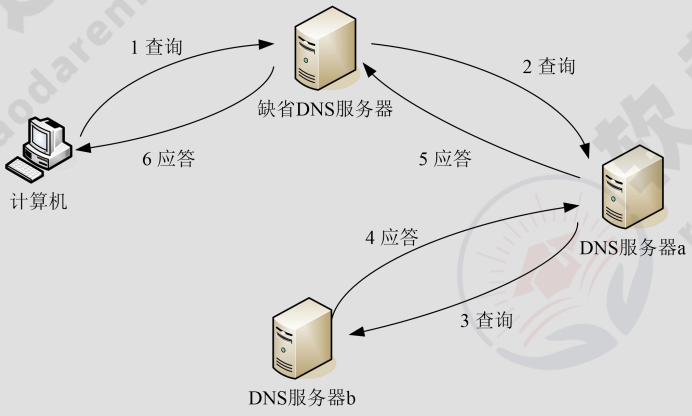

图 5-9　递归解析工作过程

答案：A

【例 6-14】分析：如果是正向解析，应该是主机名；如果是反向解析，应该是 IP 地址。而主机描述并不是主机名，所以应选择 C。

答案：C

【例 6-15】分析：ARP，即地址解析协议，实现通过 IP 地址得知其物理地址。在 TCP/IP 网络环境下，每台主机都分配了一个 32 位的 IP 地址，这种互联网地址是在网际范围标识主机的一种逻辑地址。为了让报文在物理网路上传送，必须知道对方目的主机的物理地址。这样就存在把 IP 地址变换成物理地址的地址转换问题。以以太网环境为例，为了正确地向目的主机传送报文，必须把目的主机的 32 位 IP 地址转换成为 48 位以太网的地址。这就需要在互联层有一组服务将 IP 地址转换为相应物理地址，这组协议就是 ARP 协议。采用此协议可以大大限制网络广播的数量。

答案：C

【例 6-16】分析：边界网关协议(BGP)是自治系统间的路由协议。BGP 是基于路由的方法，称为路径矢量路由。距离矢量路由不是自治系统间路由很好的候选者，因为其最小跳数的路由不一定是最合适的路由。例如，我们可能不希望数据包通过一个不安全的自治系统，即使它是最短的路线。此外，距离矢量路由是不稳定的，因为路由器只宣布到目的地的跳数，不指出到达目的地的路径。实际上，如果是通过接收路由器本身计算的最短路径，接收距离矢量通告报文的路由器可能被愚弄。链路状态路由在跨自治系统中也不是一个好的候选者，因为采用这种路由方法的互联网通常过大。要对整个互联网使用链路状态路由，就需要每个路由器有一个巨大的链路状态数据库。它也需要每个路由器用很长的时间来使用 Dijkstra 算法计算自己的路由表。

答案：(1)A　(2)B　(3)D　(4)C　(5)A

【例 6-17】分析：自治系统是由同构型的网关连接的因特网，这样的系统一般由一个网络管理中心控制。自治系统内部的网关之间执行内部网关协议。

一个互联网也可能由不同的自治系统互联而成。在这种情况下，不同的自治系统可能采用不同的路由表和不同的路由选择算法。在不同自治系统中的网关之间交换路由信息，要用外部网关协议 BGP。

答案：C

【例 6-18】分析：边界网关协议(BGP)是运行于 TCP 上的一种自治系统间路由协议。BGP 是唯一设计来处理因特网的大小的协议，也是唯一能够妥善处理好非路由主机多路连接的协议。这是通过 EGP 实现的。BGP 交互系统的主要功能是和其他的 BGP 系统交换网络可达信息。网络可达信息包括可达信息经过的自治系统(AS)清单上的信息。这些信息有效地构造了 AS 互联的图像并由此清除了路由环路，同时在 AS 级别上实施了策略决策。

BGP4 提供了一套新的机制支持无类域间路由。这些机制包括支持网络前缀的广播、取消 BGP 网络中“类”的概念。BGP4 也引入机制支持路由聚合，包括 AS 路径的聚合。这些改变为建议的超网方案提供了支持。BGP 是封装的 TCP，用的是 TCP 的 179 号端口。

答案：D

【例 6-19】分析：RIP 协议中，防止路由环路的方法有采用水平分割法、利用反向路由中毒以及设置最大度量值。

答案：A

【例 6-20】分析：运行 RIP 主动模式的路由器每隔 30 秒就发送自己完整的路由表到所有直接相邻的路由器。

答案：A

【例 6-21】分析：NBMA(非广播多路访问网络)是 OSPF(开放最短路径优先)通信协议中四种网络的一种，其他三种是广播、点对点和点对多点。X.25 和帧中继都属于 NBMA，这种模型不具备内部广播能力，

但具备多路访问能力。

答案：(1)A (2)C

【例 6-22】分析：GRP 采用复合度量来判断一个路由的好坏，复合度量由五个元素构成：带宽、延迟、负载、最大传输单元(MTU)和可靠性。默认是带宽加延迟两个元素，但可以通过人工培植来改变度量的权重，加上或去掉某个元素，达到对特定网络的设置。

答案：B

【例 6-23】分析：为了使 OSPF 能够用于规模很大的网络，OSPF 将一个自治系统再划分为若干个更小的范围。每一个区域都有一个 32b 的区域标识符(用整数或点分十进制表示)。

OSPF 使用层次结构的区域划分。在上层的区域称为主干区域(backbone area)。主干区域的标识符规定为 0.0.0.0。主干区域的作用是用来连通其他在下层的区域。存根区域不允许外部的 LSA，而完全存根区域不允许汇总的 LSA。

答案：(1)C (2)D

【例 6-24】分析：路由汇总也称路由聚合，其实现方法与超网相同，但它的主要目的是减少路由表的网络数目，减轻路由器的负担。在大型的网络中，可能包含几十万条 IP 路由，有些存储容量较小的路由器无法容纳如此庞大的路由信息，使用路由汇总可以合并几个网络地址为一个代表这几个网络的总结网络地址。

计算方法是找出 4 条路由的网络地址的共同前缀和位数，如表 5-6 所示。

表 5-6 路由汇聚过程

196.34.129.0/2:	11000100	00100010	10000	001	00000000
196.34.130.0/2:	11000100	00100010	10000	010	00000000
196.34.132.0/24:	11000100	00100010	10000	100	00000000
196.34.133.0/24:	11000100	00100010	10000	101	00000000
相同位 21:	11000100	00100010	10000	000	00000000
	(196)	(34)	(128)		(0)

答案：A

【例 6-25】分析：多协议标记交换(Multiprotocol Label Switching，MPLS，RFC3031)把第二层的链路状态信息(带宽、延迟、利用率等)集成到第三层的协议数据单元中，从而简化和改进了第三层分组的交换过程。理论上，MPLS 支持任何第三层和第三层协议。MPLS 报头的位置界于第三层和第三层之间，可称为第 2.5 层。MPLS 可以承载的报文通常是 IP 包，当然也可以直接承载以太帧、AAL5 包，甚至 ATM 信元等。

答案：B

【例 6-26】分析：FTP 使用两条 TCP 连接来完成文件传输，一条连接用于传送控制信息(命令和响应)，另一条连接用于数据发送。由于题目问的是“FTP 客户端应用进程的端口”，而客户端是通过申请一个自由端口(端口号大于 1024)来做连接准备的，那么(2)题选 D 更合适。

答案：(1)B (2)D

【例 6-27】分析：电子邮件系统是基于客户机/服务器方式，客户端也称为用户代理，提供用户界面，负责邮件发送的准备工作。服务器端也称为传输代理，负责邮件的传输，它采用端到端的传输方式。POP3(Post Office Protocol - Version 3，邮局协议版本 3)是 TCP/IP 协议簇中的一员，由 RFC 1939 定义。本协议主要用于支持使用客户端远程管理在服务器上的电子邮件。提供了 SSL 加密的 POP3 协议被称为 POP3S，其特性有以下四个方面。

- POP3 协议默认端口：110。
- POP3 协议默认传输协议：TCP。
- POP3 协议适用的构架结构：C/S。

- POP3 协议的访问模式：离线访问。

答案：(1)B (2)A

【例 6-28】分析：SMTP(简单邮件传输协议)用于主机与主机之间的电子邮件交换。SMTP 使用 TCP 连接，TCP 端口号为 25。

答案：B

第 7 章 过关习题

【例 7-1】分析：IPv6 地址的格式前缀用于表示地址类型或子网地址，用类似于 IPv4 CIDR 的方法可以表示为“IPv6 地址/前缀长度”的形式。IPv6 地址分为单播地址、组播地址和任意播地址。单播地址又包括可聚合全球单播地址、链路本地地址、站点本地地址和其他特殊单播地址。

可聚合全球单播地址在全球范围内有效，相当于 IPv4 公用地址，其格式前缀为 001。

链路本地地址的有效范围仅限于本地，其格式前缀为 1111 1110 10，用于同一链路的相邻节点间的通信，相当于 IPv4 中的自动专用 IP 地址。

站点本地地址的格式前缀为 1111 1110 11，相当于 IPv4 中的私网地址。

组播地址格式前缀为 1111 1111，此外还有标志、范围和组 ID 等字段。

任意播地址仅用作目标地址，且只能分配给路由器。一个子网内的所有路由器接口都被分配了子网-路由器任意播地址。子网-路由器任意播地址必须在子网前缀中进行预定义。子网前缀必须固定，其余位置全“0”。

答案： A

【例 7-2】分析：“0:0:0:0:0:0:0:0”表示不确定地址，不能分配给任何节点。当发送 IPv6 分组的主机还没分配地址时可以使用。“0:0:0:0:0:0:0:1”是回呼地址(或称为回环地址)，用来向自身发送 IPv6 分组，不能分配给任何物理接口。

答案：(1)A (2)B

【例 7-3】分析：链接本地地址的格式如下：

前缀(10 位)	MAC 地址(54 位)	接口 ID(64 位)
1111 1110 10	0	Interface ID

Interface ID 使用 EUI-64 地址，该地址由 MAC 地址转换而成。

答案：B

【例 7-4】分析：IPv6 地址的长度为 128 位，使用冒号分开十六进制来表示。某些 IPv6 地址中可能包含一长串 0。当出现这种情况，可将连续的 0 压缩；如果有多个连续的 0000，可用双冒号来代替。

本题中原地址为 33AB:0000:0000:CD30:0000:0000:0000:0000/60，进行压缩 0 处理后，地址变为 33AB:0:0:CD30:0:0:0:0/60；由于如果有多个连续的 0000，可用双冒号来代替，则地址可变为 33AB:0:0:CD30::/60。

答案：A

第 8 章 过关习题

【例 8-1】分析：RSA 算法密钥选取过程为：

(1) 选取两个质数，这里 p=5，q=3。

(2) 计算 $n=p\times q=15$，$z=(p-1)(q-1)=8$。

(3) 取小于 n 的整数 e，并且和 z 没有公约数。这里 $e=7$，满足条件。

(4) 找到数 d，满足 $ed-1$ 被 z 整除。

答案：B

【例 8-2】分析：IEEE 802.11i 规定使用 802.1x 认证和密钥管理方式，在数据加密方面，定义了 TKIP(Temporal Key Integrity Protocol)、CCMP(Counter-Mode/CBC-MAC Protocol)和 WRAP(Wireless Robust Authenticated Protocol)三种加密机制。其中 TKIP 采用 WEP 机制中的 RC4 作为核心加密算法，可以通过在现有的设备上升级固件和驱动程序的方法达到提高 WLAN 安全的目的。CCMP 机制基于 AES(Advanced Encryption Standard)加密算法和 CCM(Counter-Mode/CBC-MAC)认证方式，使得 WLAN 的安全程度大大提高，是实现 RSN 的强制性要求。WRAP 机制基于 AES 加密算法和 OCB(Offset Codebook)，是一种可选的加密机制。

答案：D

【例 8-3】分析：DES 是一个分组加密算法，它以 64 位为分组对数据加密。它的密钥长度是 64 位，但实际有效的密钥只是 56 位。

三重 DES 是 DES 算法扩展其密钥长度的一种方法，它使用两把密钥对报文执行三次常规的 DES 加密，在第一层、第三层中使用相同的密钥。

答案：D

【例 8-4】分析：公开密钥密码体制也叫非对称密钥加密。每个用户都有一对密钥：公开密钥和私有密钥。公钥对外公开，私钥由个人秘密保存；用其中一把密钥来加密，另一把密钥来解密。虽然解密密钥(SK)是由加密密钥(PK)决定的，但却不能根据 PK 计算出 SK。

答案：C

【例 8-5】分析：在公钥体系亦即非对称密钥体制中，每个用户都有一对密钥：公钥和密钥，公钥对外公开，私钥由个人秘密保存。因此通常采用公钥加密，私钥解密。认证技术用于辨别用户的真伪，有基于对称加密的认证方法，也有基于公钥的认证方法。在基于公钥的认证中，通信双方用对方的公钥加密，用各自的私钥解密。在签名中用私钥签名消息，公钥验证签名。

答案：(1)A (2)D

【例 8-6】分析：利用公钥加密算法的数字签名系统如图 8-9 所示。这样的签名方法是符合可靠性原则的，即：签字是可以被确认的；签字是无法被伪造的；签字是无法重复使用的；文件被签字以后是无法被篡改的；签字具有无可否认性。如果 A 方否认了，B 可以拿出 $D_A(P)$，并用 A 的公钥 E_A 解密得到 P，从而证明 P 是 A 发送的；如果 B 把消息篡改了，当 A 要求 B 出示原来的 $D_A(P)$时，B 拿不出来。

答案：(1)C (2)B

【例 8-7】分析：MD5 算法以任意长的报文作为输入，算法的输出是产生一个 128 位的报文摘要。SHA 的算法建立在 MD5 的基础上，SHA-1 是 1994 年修订的版本，该算法可以接收的输入报文小于 2^{64} 位，产生 160 位的报文摘要。

答案：(1)B (2)C

第 9【例 8-8】分析：MD5 是 MIT 的 Ron Rivest(RFC 1321)提出的。算法以任意长的报文作为输入，算法的输出是产生一个 128 位的报文摘要。SHA 的算法建立在 MD5 的基础上，SHA-1 是 1994 年修订的版本，该算法可以接收的输入报文小于 2^{64} 位，产生 160 位的报文摘要。

答案：B

【例 8-9】分析：MD5 算法以任意长的报文作为输入，算法的输出是产生一个 128 位的报文摘要。SHA 的算法建立在 MD5 的基础上，SHA-1 是 1994 年修订的版本，该算法可以接收的输入报文小于 2^{64} 位，产生 160 位的报文摘要。

答案：(1)B (2)D

【例 8-10】分析：在 Internet 上建立隧道可以在不同的协议层实现。工作在第二层的隧道协议有点对

点隧道协议(PPTP)、第二层隧道协议(L2TP)等；IPSec 是 IETF 定义的一组协议，工作在网络层，用于增强 IP 网络的安全性；安全套接字(SSL)是传输层安全协议，用于实现 Web 安全通行。

答案：C

【例 8-11】分析：HTTP 工作在传输层；安全超文本传输协议(Secure Hypertext Transfer Protocol，S-HTTP)是一种结合 HTTP 而设计的消息安全通信协议，工作在应用层。

答案：(1)B (2)C

【例 8-12】分析：PGP(Pretty Good Privacy)是一个完整的电子邮件安全软件包，包括加密、鉴别、电子签名和压缩等技术。PGP 并没有使用什么新的概念，它只是将现有的一些算法如 MD5、RSA 以及 IDEA 等综合在一起而已。PGP 提供数据加密和数字签名两种服务。

答案：C

【例 8-13】分析：客户 A 将自己的用户名以明文方式发送给认证服务器(AS)，申请初始票据。认证服务器(AS)确认 A 为合法客户后，生成一个一次性会话密钥 K_s 和一个票据 KTGS(A,K_s)，并用客户 A 的密钥 K_A 加密这两个数据包后传给客户 A，要求用户输入密码。客户 A 收到上述两个数据包后，用自己的密钥 K_A 解密获得会话密钥 K_s 和票据 K_{TGS}(A,K_s)。客户 A 将获得的票据 K_{TGS}(A,K_s)、应用服务器名 V 以及用于会话密钥加密的时间戳(用于防止重放攻击)发送给票据授予服务器(TGS)，请求会话票据。票据授予服务器 TGS 收到上述数据包后，向客户 A 返回它与服务器 V 通信的会话票据 K_{AV}，这个会话票据 K_{AV} 是用客户 A 的密钥和应用服务器 V 的密钥进行加密。客户 A 使用从票据授予服务器(TGS)获取的会话票据 K_{AV} 发送给应用服务器 V 请求登录，并且附上用 K_{AV} 加密的时间戳，以防止重放攻击。服务器 V 通过用 K_{AV} 加密的时间戳进行应答，完成认证过程。

答案：(1)B (2)C

【例 8-14】分析：Kerberos 的目标在于三个领域：认证、授权和记账审计。认证过程如下。

(1) 客户 A 将自己的用户名以明文方式发送给认证服务器(AS)，申请初始票据。

(2) 认证服务器(AS)确认 A 为合法客户后，生成一个一次性会话密钥 K_s 和一个票据 K_{TGS}(A,K_s)，并用客户 A 的密钥 K_A 加密这两个数据包后传给客户 A，要求用户输入密码。

(3) 客户 A 收到上述两个数据包后，用自己的密钥 K_A 解密获得会话密钥 K_s 和票据 K_{TGS}(A,K_s)。客户 A 将获得的票据 K_{TGS}(A,K_s)、应用服务器名 V 以及用于会话密钥加密的时间戳(用于防止重放攻击)发送给票据授予服务器(TGS)，请求会话票据。

(4) 票据授予服务器(TGS)收到上述数据包后，向客户 A 返回它与服务器 V 通信的会话票据 K_{AV}，这个会话票据 K_{AV} 是用客户 A 的密钥和应用服务器 V 的密钥进行加密的。

(5) 客户 A 使用从票据授予服务器(TGS)获取的会话票据 K_{AV} 发送给应用服务器 V 请求登录，并且附上用 K_{AV} 加密的时间戳，以防止重放攻击。

(6) 服务器 V 通过用 K_{AV} 加密的时间戳进行应答，完成认证过程。

答案：(1)A (2)D

【例 8-15】分析：Melissa 病毒是一种快速传播的能够感染那些使用 MS Word 97 和 MS Office 2000 的计算机宏病毒。即使不知道 Melissa 病毒是什么也没关系，因为前面有个 Macro，表明这是宏病毒。

答案：(1)D (2)B

【例 8-16】分析：Worm 表示蠕虫，Trojan 表示木马，Backdoor 表示后门，Macro 表示宏。

答案：A

【例 8-17】分析：【问题 1】本题考查的是 VPN 隧道技术的基本概念，这里不作详细的解析。

【问题 2】本题考查 IPSec 协议组的功能。

【问题 3】源子网 IP 地址为 ServerA 连接的内网网络地址，由图 8-12 可知为 192.168.1.0；目标子网 IP 地址应为 ServerB 连接的内网网络地址，由图 8-12 可知为 192.168.2.0。

隧道设置中的隧道终点 IP 地址应设置为服务器 ServerB 的外网地址，为 202.113.111.1。

【问题 4】题目中要求安全措施为“加密并保持完整性”。IPSec 封装安全负荷(ESP)提供了数据加密

功能和数据完整性认证。在隧道模式下，IPSec 对原来的 IP 数据报进行了封装和加密，加上了新的 IP 头，其格式如图 8-17 所示。

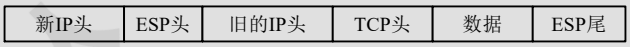

图 8-17　IP 数据报的格式(2)

答案：

【问题 1】(1)PPTP　(2)L2TP　(3)IPSec

说明：(1)和(2)答案可调换

【问题 2】(4)AH　(5)ESP　(6)ISA KMP/Oakley

【问题 3】(7)192.168.1.0　(8)192.168.2.0　(9)202.113.111.1

【问题 4】(10)B　(11)C　(12)F

【例 8-18】分析：【问题 1】隧道是建立在已连通的路由上的。ipsec 只是加密，tunnel 是建立隧道。应填接入 Internet 的对应网关地址，即(1)203.25.25.254，(2)201.18.8.254。

【问题 2】本题考查隧道本端及对端 IP 地址的设置。

【问题 3】本题考查建立 IPSec 安全关联的配置命令。

【问题 4】建立 IPSec 策略 p1，在网段 192.168.8.0/24 和网段 192.168.9.0/24 之间启用隧道 tun1。

【问题 5】从代码段 router-a(config-ipsec-prop)# esp 3des sha1 中明显看出加密算法采用 3DES，认证算法采用 SHA-1。

答案：【问题 1】(1)203.25.25.254　(2)201.18.8.254

【问题 2】(3)201.18.8.1　(4)203.25.25.1

【问题 3】(5)201.18.8.1　(6)203.25.25.1

【问题 4】建立 IPSec 策略 p1，在网段 192.168.8.0/24 和网段 192.168.9.0/24 之间启用隧道 tun1。

【问题 5】(7)3DES　(8)SHA-1

第 9 章　过关习题

【例 9-1】 分析：在采用 NTFS 格式的 Windows 2000/2003 中，应用审核策略可以对文件夹、文件以及活动目录对象进行审核，审核结果记录在安全日志中，通过安全日志就可以查看哪些组或用户对文件夹、文件或活动目录对象进行了什么级别的操作，从而发现系统可能面临的非法访问，通过采取相应的措施，将这种安全隐患减到最低。这些在 FAT32 文件系统下是不能实现的。

答案：D

【例 9-2】 分析：默认情况下，只有系统管理员用户组和系统组用户拥有访问和完全控制终端服务器的权限。远程桌面用户组的成员只具有访问权限而不具备完全控制权。

答案：B

【例 9-3】分析：l 代表是连接文件，r 代表可读，w 代表可写，x 代表可执行。

第一个 root 用户，第二个 root 用户组，4096 是文件大小，2009-04-14 17:30 是文件创建时间，profile 是文件名。

答案：C

【例 9-4】分析：cp 是文件复制命令，mv 是文件移动命令，两者的区别很明显。复制文件时源文件不动，把文件复制到目标目录中。移动文件相当于把源文件剪切掉，然后粘贴到目标目录中。

答案：B

【例 9-5】分析：install 命令的作用是安装或升级软件或备份数据，它的使用权限是所有用户。fsck 检

查与修复 Linux 档案系统，可以同时检查一个或多个 Linux 档案系统。rpm 是一个管理套件，用于管理各项软件包。

答案：B

【例 9-6】分析：ln 具有链接功能；cat 把档案串联后传到基本输出；locate 命令用于查找文件；vi 可在全屏幕方式下编辑一个或多个文件。

答案：A

【例 9-7】分析：文件或目录的访问权限分为只读 r、只写 w 和可执行 x 三种。每一文件或目录的访问权限都有三组，每组用三位表示，分别为文件属主的读、写和执行权限，与属主同组的用户的读、写和执行权限，系统中其他用户的读、写和执行权限。

答案：B

【例 9-8】分析：/proc 文件系统下的多种文件提供的系统信息，它不是针对某个特定进程的，而是能够在整个系统范围的上下文中使用，可以使用的文件随系统配置的变化而变化。

答案：D

【例 9-9】分析：/etc/shadow 是只有超级用户 root 才能读的文件，该文件包含了系统中所有用户及其口令等相关信息。

答案：C

【例 9-10】分析：出于系统安全考虑，Linux 系统中的每一个用户除了有其用户名外，还有其对应的用户口令。因此使用 useradd 命令创建新用户后，还需使用 passwd 命令为每一位新增加的用户设置口令。root 用户可以使用 passwd 命令改变系统用户的口令，系统用户也可以使用 passwd 命令改变自己的口令。

答案：B

【例 9-11】分析：IIS 6.0 组件中包括 SMTP Service、文件传输协议(FTP)服务、万维网服务、Frontpage 服务器扩展等子件，不包括 DNS。DNS 和 IIS 都是 Windows Server 2003 提供的服务。

答案：D

【例 9-12】 分析：IIS 提供多种身份验证方案。

匿名访问：如果启用了匿名访问，访问站点时，不要求提供经过身份验证的用户凭据。

集成 Windows 身份验证以 Kerberos 票证的形式通过网络向用户发送身份验证信息，并提供较高的安全级别。

Windows 域服务器的摘要式身份验证需要用户 ID 和密码，可提供中等的安全级别。此方法会将用户凭据作为 MD5 中的哈希或消息摘要在网络中进行传输，这样就无法根据哈希对原始用户名和密码进行解码。

基本身份验证需要用户 ID 和密码，提供的安全级别较低。用户凭据以明文形式在网络中发送。这种形式提供的安全级别很低，因为几乎所有协议分析程序都能读取密码。

Microsoft .NET Passport 身份验证提供了单一登录安全性，对 IIS 的请求必须在查询字符串或 Cookie 中包含有效的 .NET Passport 凭据。

答案：C

【例 9-13】分析：FTP 的数据端口号是 FTP 控制端口号−1。例如当控制端口为 21 时，数据端口就是 20。题目中，控制端口为 2222，则数据端口为 2222−1=2221。

答案：D

【例 9-14】分析：IIS 创建或设置网站，无需重新启动。

答案：A

【例 9-15】分析：主页文件的读取、写入权限都可以通过“主目录”选项卡进行配置，通过勾选来确定其文件权限。

答案：B

【例 9-16】分析：在“本地路径”右边，是网站根目录，即网站文件存放的目录，默认路径是“C:\intepub\ftproot”。如果想把网站文件存放在其他地方，可修改这个路径。

答案：B

【例 9-17】分析：虚拟主机服务是指在一台物理机器上提供多个 Web 服务。用 Apache 设置虚拟服务器通常可以采用两种方案：基于 IP 地址的虚拟主机和基于域名的虚拟主机。基于域名的虚拟主机创建比较简单，只需要配置域名服务器(即 DNS 服务器)将主机名映射到正确的 IP 地址，然后配置 Apache HTTP 服务器。

在配置信息中，DocumentRoot 是指 Apache 服务器存放网页的根目录，ServerName 是由用户指定的主机名。

答案：(1)A (2)B (3)C

【例 9-18】分析：当某个 DNS 客户机准备申请一个域名时，首先查询客户机的缓存，如果没有符合条件的记录，就产生一个查询请求并发送给本地 DNS 服务器，如果客户机在规定的时间内没有收到查询响应，会尝试其他的 DNS 服务器或再次查询。应该说是本网段内 DNS。

答案：A

【例 9-19】分析：缓存域名服务器没有域名数据库，它将向其他域名服务器进行域名查询并将查询结果保存在缓存中。缓存域名服务器可以改进网络中 DNS 服务器的性能。当 DNS 经常查询一些相同的目标时，安装缓存域名服务器可以对查询提供更快速的响应，而不需要通过主域名服务器或辅助域名服务器。缓存域名服务器因此特别适合于在局域网内部使用，其主要目的是提高域名解析的速度和节约对互联网访问的出口带宽。

答案：A

【例 9-20】分析：对于要经常访问的网站，可以通过在 Hosts 中配置域名和 IP 的映射关系，这样我们输入域名计算机就能很快解析出 IP，而不用请求网络上的 DNS 服务器。

现在有很多网站不经过用户同意就将各种各样的插件安装到你的计算机中，有些说不定就是木马或病毒。对于这些网站可以利用 Hosts 把该网站的域名映射到错误的 IP 或自己计算机的 IP，这样就不用访问了。比如不想访问 www.XXXX.com，那我们在 Hosts 写上以下内容：

```
127.0.0.1 www.XXXX.com #屏蔽的网站
0.0.0.0 www.XXXX.com #屏蔽的网站
```

这样计算机解析域名就解析到本机或错误的 IP，达到了屏蔽的目的。

答案：(1)A (2)D

【例 9-21】分析：Linux 系统中，默认安装 DHCP 服务的配置文件为/etc/dhcpd.conf。

答案：A

【例 9-22】分析：由 default-lease-time 3600 知，默认租用期为 3600 秒，换算成小时为 1 小时。

答案：A

【例 9-23】分析：POP3 的默认端口是 TCP 的 110。

答案：A

【例 9-24】 分析：邮件服务器系统由 POP3 服务、简单邮件传输协议(SMTP)服务以及电子邮件客户端三个组件组成。其中的 POP3 服务与 SMTP 服务一起使用，POP3 为用户提供邮件下载服务，而 SMTP 则用于发送邮件以及邮件在服务器之间的传递。如果路由器端口的访问控制列表设置为 denypop3，则将无法接收邮件，与题意不符。

答案：B

【例 9-25】分析：为了使 Windows 主机间的资源能够共享，Microsoft 实现了一个基于 NetBIOS 协议的共享网络文件/打印机系统，Microsoft 称之为 SMB(Server Message Block)通信协议。Samba 就是用来实现 SMB 的一种软件。Samba 服务器向 Linux 或 Windows 系统客户端提供 Windows 风格的文件和打印机共享服务，实现在 Samba 服务器上的打印机和文件系统的共享。

答案：A

【例 9-26】 分析：

【问题 1】如果启用“密码必须符合复杂性要求”策略，则密码必须符合以下最低要求。

(1) 不包含全部或部分的用户账户名。

(2) 长度至少为六个字符。

(3) 包含来自以下四个类别中三个类别的字符。

- 英文大写字母(从 A 到 Z)。
- 英文小写字母(从 a 到 z)。
- 10 个基本数字(从 0 到 9)。
- 非字母字符(例如，!、$、#、%)。

如果启用了此安全策略，而配置的用户密码不符合此配置要求时系统会提示错误。

题目中，选项 A 不符合要求 1，选项 B 不符合要求 2，选项 D 不符合要求 3。

【问题 2】

(1) 账户锁定阈值。该安全设置确定导致用户账户被锁定的登录失败尝试的次数。无法使用锁定的账户，是因为管理员进行了重新设置或该账户的锁定时间已过期。登录尝试失败的范围可设置为 0～999 之间。如果将此值设为 0，将无法锁定账户。

(2) 账户锁定时间。该安全设置确定锁定的账户在自动解锁前保持锁定状态的分钟数。有效范围为 0～99 999 分钟。如果将账户锁定时间设置为 0，那么在管理员明确将其解锁前，该账户将被锁定。

(3) 复位账户锁定计数器。该安全设置确定在登录尝试失败计数器被复位为 0(即 0 次失败登录尝试)之前，尝试登录失败之后所需的分钟数，有效范围为 1～99 999 分钟。

由“账户锁定阈值”的设置可知，3 次无效登录后，用户账户被锁定。由“账户锁定时间”可知锁定时间为 30 分钟。

【问题 3】安装活动目录的过程中，SYSVOL 文件夹必须存储在 NTFS 磁盘分区。

活动目录中域的名称解析需要 DNS 的支持，域控制器也需要登记到 DNS 服务器内，以便其他计算机通过 DNS 服务器查找到这台域控制器。

【问题 4】全局组成员来自同一域的用户账户和全局组，可以访问域林中的任何资源。

域本地组成员来自林中任何域中的用户账户、全局组和通用组以及本域中的域本地组，只能访问本地域中的资源。

通用组成员来自林中任何域中的用户账户、全局组和通用组，可以授予多个域中的访问权限。

答案：

【问题 1】(1)C

【问题 2】(2)A (3)A

【问题 3】(4)A (5)D

【问题 4】(6)B (7)C (8)A

【例 9-27】分析：

【问题 1】本题考查 Linux 系统的文件命令。chgrp 命令改变文件所属群组，vi 命令表示编辑文件，which 命令用来查找文件。

【问题 2】proc 文件系统是一个伪文件系统，它只存在于内存当中，而不占用外存空间。它以文件系统的方式为访问系统内核数据的操作提供接口。用户和应用程序可以通过 proc 得到系统的信息，并可以改变内核的某些参数。由于系统的信息如进程是动态改变的，所以用户或应用程序读取 proc 文件时，proc 文件系统是动态从系统内核读出所需信息并提交的。

【问题 3】(5)的答案可以从题目给出的程序段中找出，hda2 后面写的是 extended。

(6)中的 Shmfs 文件系统是一种内存共享模式的文件系统。

【问题 4】这是 Linux 下比较常见的关于文件系统的系统。

答案：

【问题 1】(1)B (2)C (3)D

【问题 2】(4)A

【问题 3】(5)/dev/hda2 (6)/dev/hda1

【问题 4】(7)/etc/fstab (8)moun

【例 9-28】分析：

【问题 1】配置主机网络接口命令：ifconfig。

程序/sbin/ifconfig 用来配置主机网络接口。这包括基本的配置如 IP 地址、掩码和广播地址，以及高级的选项如为点对点连接(如 PPP 连接)设置远程地址。

一个接口可以在不进行重新配置的情况下临时变为不可用和再变为可用。可以用于将服务器的网络连接临时变为不可用(当重新配置一个服务时)。使用下列命令实现本功能。

```
ifconfig interface down    关闭接口
ifconfig interface ip-address up 启动接口
```

图 9-36 中显示以太网口地址为 192.168.1.126，子网掩码为 255.255.255.128。

由于销售部的以太网接口地址为 192.168.1.126，而 192.168.1.1 不能用，因此其可用地址范围在 192.168.1.2～192.168.1.126 之间，可连接主机数为 125 台。

【问题 2】“|”，是 Linux 很有用的一个用法，俗称管道，把一个命令的输出作为下个命令的输入：

rmp -qa “-q”查找； -a all 所有；grep 正则表达匹配；所以,这个命令的含义就是“查找所有和 HTTPD 服务相关的”；即列出所有装配的软件。

(6)考查 Apache 的启动命令 service httpd start。

【问题 3】Apache 的主配置文件名是 httpd.conf，该文件所在目录为/etc/httpd/conf。

<Directory " /var/www/html/secure " >指进入此目录； AllowOverride AuthConfig 即允许该目录对 AuthConfig 属性进行覆盖；后面几句即允许指定 IP 访问，而不允许其他 IP 访问。所以语句意思为目录“/var/www/html/secure”只允许主机 192.168.1.2 访问。

【问题 4】Listen 语句的意思是允许将 Apache 绑定到指定的 IP 地址和端口，作为默认值的辅助选项。其含义为提供 Web 服务的地址是 192.168.1.126，端口是 80。

启动 Web 服务后，仅销售部的主机可以访问 Web 服务，要使研发部的主机也可以访问 Web 服务则需要增加从研发部网络到销售部网络的路由，或者将主配置文件中配置“Listen 192.168.1.126:80”修改为“Listen 80”。

答案：

【问题 1】

(1) ifconfig eth0 或 ifconfig

(2) 192.168.1.126

(3) 255.255.255.128

(4) 125 或 126

【问题 2】

(5) 确认 Apache 软件包是否已经成功安装

(6) Service httpd start

【问题 3】

(7) httpd.conf

(8) /etc/httpd/conf

(9) 目录“/var/www/html/secure”只允许主机 192.168.1.2 访问

【问题 4】

(10) 提供 Web 服务的地址是 192.168.1.126，端口是 80

将 Apache 的主配置文件中配置“Listen 192.168.1.126:80”修改为“Listen 80”，或者增加从研发部网络到销售部网络的路由

【例 9-29】 分析：

【问题 1】题中用其中一台主机作为 WWW 服务器，域名为 shangxueba.com，所以新建区域名称为 shangxueba.com，而新建主机即为新建 WWW 服务器，名称为 www，IP 地址图上已标出为 221.166.1.1。

【问题 2】由于“IP 筛选器”用以对客户端发来的 DNS 请求消息进行筛选，即本地服务器为目的端，而任意发送端为客户端。所以若要在“IP 筛选器向导”中指定 IP 通信的源地址，下拉列表框中应选择“任何 IP 地址”，指定 IP 通信的目标地址，下拉列表框中应选择“我的 IP 地址”。

同理，源端口应为“从任意端口”，而目的端口应设为“到此端口”，并且在文本框中填写 DNS 服务器的端口号 53。

【问题 3】要使规则生效，应该通过“指派”命令实现，即右击“新 IP 安全策略”，选择“指派”命令。

【问题 4】在 Windows 中运行“ipconfig /displaydns”命令以显示 DNS 解析器缓存的内容。在命令行模式中可以看到在 ipconfig /?中有一个名为/flushdns 的参数，这个就是清除 DNS 缓存信息的命令。“Record Type”=2 时，记录 IP 地址对应的域名。

答案：

【问题 1】(1)shangxueba.com (2)www (3)221.166.1.1

【问题 2】(4)任何 IP 地址 (5)我的 IP 地址 (6)选择“从任意端口”单选按钮 (7)选择“到此端口”单选按钮，文本框中输入 53

【问题 3】 右击“新 IP 安全策略”，选择“指派”命令。

【问题 4】(8) ipconfig/displaydns (9) IP 地址对应的域名(反向解析) (10) ipconfig/flushdns

【例 9-30】分析：

【问题 1】本题考查 DHCP 服务器的配置，从图中可以看出 110.115.3.1、110.115.3.2、110.115.3.3 分别已经固定给了路由器和两台服务器，所以地址范围为 110.115.3.4～110.115.3.254。

【问题 2】当客户端未能从 DHCP 服务器获得 IP 地址时，客户端会检查自己是否配置了“备用 IP 地址”。如果配置了“备用 IP 地址”，那么客户端会首先启用“备用 IP 配置”；如果没有配置“备用 IP 地址”，客户机将从 169.254.0.0/16 这个 B 类网段中选择一个作为 IP 地址，并且每隔 5 分钟就再次进行 DHCP 地址申请。

【问题 3】本题考查 DHCP 服务器的配置，打开 hosts 文件可查看记录。hosts 是静态的 IP 和域名映射的关系。

【问题 4】本题考查 FTP 服务器的配置，填写需要配置的 IP 地址。看图即可，此处还可以填写“所有未分配 IP”。

【问题 5】只有 110.115.3.10 这台主机可以访问该虚拟目录。所以命令为 ftp://110.115.3.2:2121/ 或 ftp://110.115.3.2:2121/pcn

答案：

【问题 1】(1)110.115.3.4～110.115.3.254 (2)61.202.117.193～61.202.117.252A

【问题 2】host1 不能正常访问 Internet。因为它的 IP 地址属于 169.254.0.0/16 这个 B 类网段，表明它没有从 DHCP 服务器成功获取到一个有效 IP 地址。

【问题 3】(3)hosts (4)61.202.117.253

【问题 4】(5)110.115.3.2

【问题 5】(6)ftp://110.115.3.2:2121/ 或 ftp://110.115.3.2:2121/pcn

第 10 章　过关习题

【例 10-1】分析：交换机的交换方式包括静态交换和动态交换两种。目前，交换机最常采用的交换方式是动态交换方式。动态交换方式主要有快速转发、碎片丢弃和存储转发三种模式。IP 交换是三层交换技术。

答案：B

【例 10-2】分析：交换机最常采用的交换方式是动态交换方式。动态交换方式主要有快速转发、碎片丢弃和存储转发 3 种模式。

快速转发交换模式是指交换机在接收数据帧时，一旦检测到 6 个字节，目的地址就立即进行转发操作。

碎片丢弃交换模式也被称为自由分段模式或是碎片隔离交换模式。交换机接收到数据帧时，先检测该数据帧是不是冲突碎片，如果不是冲突碎片，也不保存整个数据帧，而是接收了它的目的地址就直接进行转发操作；如果该数据帧是冲突碎片，则直接将该帧丢弃。

存储转发模式与前两种转发模式最大的不同在于：它将接收到的整个数据帧保存在缓冲区中。它把数据帧先存储起来，然后进行循环冗余码校验检查，在对错误帧进行处理后，才取出数据帧的目的地址，进行转发操作。

答案：A

【例 10-3】分析：设置交换机的 IP 地址的命令提示符为

```
Switch(config-if)#配置接口参数
```

答案：D

【例 10-4】分析：在特权模式下输入 vlan database 命令进入 VLAN 配置子模式。

```
2950# vlan database
2950(vlan)# vtp server  设置本交换机为 Server 模式
2950(vlan)# vtp pruning  启动修剪功能
```

答案：B

【例 10-5】 分析：根据交换机在 VTP 域的角色，需要对 VTP 模式进行配置。配置内容包括 VTP 域名、VTP 模式、VTP 修剪、VTP 口令等。

答案：D

【例 10-6】分析：show version 命令用于查看路由器的软硬件版本。show history 命令用于显示输入过的命令历史列表。B、C 选项中的两条命令不存在。

答案：D

【例 10-7】分析：CISCO 路由器操作系统 IOS 的基本的三种命令模式为用户模式、特权模式以及配置模式。

答案：C

【例 10-8】分析：Router(config-subif)# 命令可以设置封装类型和子接口连接的 VLAN 号。

答案：A

【例 10-9】分析：一般来说，Cisco 路由器有以下 5 种配置方式。

- 使用路由器的 Console(控制台)接口，可以将配置线缆挂接到终端，或者挂接到运行终端仿真软件的微机上。
- 使用 AUX(辅助)接口挂接 Modem，通过电话线与远方的终端相连，或者将配置线缆挂接到运行终端仿真软件的微机上。
- 通过网络中的 FTP 服务器上传、下载路由器的配置文件、路由器软件镜像等。
- 使用 Telnet 程序远程配置管理路由器。
- 使用网络中的 SNMP 网管工作站管理路由器。

但是，对于刚出厂的路由器，第一次的设置必须通过第一种方式来进行。此时终端的硬件设置如下。

- 波特率：9600。
- 数据位：8。
- 停止位：1。
- 奇偶校验：无。

答案：(1)D　(2)C

【例 10-10】分析：在路由条目前都有一个字母表示连接的情况。C 是 connected 的第一个字母，代表直连；R 表示 RIP 协议，意思是该条目由 RIP 协议计算产生。

答案：B

【例 10-11】

分析：

【问题 1】IPv6-over-IPv4 GRE 隧道技术将 IPv6 报文封装在 IPv4 报文中，可在 IPv4 的 GRE 隧道上承载 IM 数据报文。对于采用隧道技术的设备来说，在隧道的入口处，将 IPv6 的数据报文封装进 IPv4，IPv4 报文的源地址和目的地址分别是隧道入口和隧道出口的 IPv4 地址；在隧道的出口处，再将 IPv6 报文取出转发到目的节点。GRE 隧道把 IPv6 作为乘客协议，将 IPv4 作为承载协议。

【问题 2】本题主要考查路由器的接口配置。

本题中，路由器 R1 的串口 s0 与 IPv4 网络连接。对于 IPv4 网络，路由器接口 IP 地址的配置命令为 ip address *IP_address mask*。s0 的 IP 地址为 200.100.1.1，子网掩码为 255.255.255.0，因此串口 s0 的 IP 地址配置命令为 ip address 200.100.1.1 255.255.255.0。

以太网接口 E0 连接的是 IPv6 网络。为 IPv6-over-IPv4 GRE 隧道接口分配 IPv6 地址的配置命令为 ipv6 address *ipv6-address/prefix-length*，本题中应为 ipv6 address 2000:2fcc::1/64。

【问题 3】本题主要考查采用 IPv6-over-IPv4 GRE 隧道的配置命令。

【问题 4】主机 PC1 的网关地址是与 PC1 在同一个子网的路由器端口 IP 地址，也就是路由器 R1 的 E0 接口地址。

答案：

【问题 1】(1) IPv6　(2) IPv4

【问题 2】(3) 启动 IPv6 单播路由配置　(4) ip　(5) 200.100.1.1　(6) 255.255.255.0
(7) ipv6　(8) 2000:2fcc::1/64

【问题 3】(9) 设置隧道源端口为 s0　(10) 设置隧道目标地址为 200.100.1.1
(11) 将 tunnel 模式设置为 IPv6 的 GRE 隧道

【问题 4】(12) 2000:2fcc::1/64

【例 10-12】

分析：

【问题 1】本题考查 ISATAP 隧道的基本概念。

双栈主机使用 ISATAP 隧道时采用的 ISATAP 地址格式为 Prefix(64bit):0:5EFE:IPv4ADDR。0:5EFE 是 IANA 规定的格式，IPv4ADDR 是单播 IPv4 地址。

【问题 2】本题考查路由器接口地址与 OSPF 协议的基本配置操作。

由拓扑结构图可知，路由器 R1 的串口 S0 的地址为 192.1.1.1/24，以太口地址为 192.0.0.1/24。前两小题的答案很明显。

OSPF 的配置中，采用以下命令指定与路由器直接相连的网络：

```
network address wildcard-mask area area_id
```

“wildcard-mask”是通配符掩码，用于告诉路由器如何处理相应的 IP 地址位。通配符掩码中，“0”表示“检查相应的位”，“1”表示“忽略相应的位”。在大多数情况下，可以将通配符掩码理解为标准掩码的反向。对于 C 类网络，标准的子网掩码为 255.255.255.0，则通配符掩码为 0.0.0.255。

【问题 3】本题考查 ISATAP 隧道的基本配置操作。

【问题 4】使用 ISATAP 隧道完成的主机—路由器隧道，在主机的配置比较简便易行，只需要确定隧道对端路由器接口的 IPv4 地址即可，同时对于主机的要求是必须都要有 IPv4 地址。根据拓扑结构图，隧道路由器端接口为路由器 R3 的串口 S0。因此本题应填入 192.2.2.1。

配置命令为：

```
C: >netsh
netsh>interface
netsh interface> ipv6
netsh interface ipv6>isatap
netsh interface ipv6 isatap>set router 192.2.2.1
```

也可以通过一条命令完成：C:/>netsh interface ipv6 isatap set router 192.2.2.1。

答案：

【问题 1】(1)A (2)C

【问题 2】(3)192.1.1.1 (4)192.0.0.1 (5)0.0.0.255 (6)0.0.0.255

【问题 3】(7)启用 tunnel 0 (8)指定 tunnel 的源地址为 s/0 (9)tunnel 的模式为 ISATAP 隧道

【问题 4】(10)192.2.2.1

【例 10-13】

分析：

【问题 1】NAT-PT(网络地址转换协议转换)是一种纯 IPv6 节点和 IPv4 节点间的互通方式，所有包括地址、协议在内的转换工作都由网络设备来完成。支持 NAT-PT 的网关路由器应具有 IPv4 地址池，在从 IPv6 向 IPv4 域中转发包时使用，地址池中的地址是用来转换 IPv6 报文中的源地址的。此外，网关路由器需要 DNS-ALG 和 FTP-ALG 这两种常用的应用层网关的支持，在 IPv6 节点访问 IPv4 节点时发挥作用。如果没有 DNS-ALG 的支持，只能实现由 IPv6 节点发起的与 IPv4 节点之间的通信，反之则不行。如果没有 FTP-ALG 的支持，IPv4 网络中的主机将不能用 FTP 软件从 IPv6 网络中的服务器上下载文件或者上传文件，反之亦然。

【问题 2】动态 NAT-PT 的命令及功能如表 10-14 所示。

表 10-14 动态 NAT-PT 的命令及功能

命 令	功 能
Router(config)# ipv6 access-list name permit Source-ipv6-prefix-length	规定了 IPv6 单协议网络中允许被转换的 IPv6 地址范围，ipv6 access-list 命令配置了一个标准的 IPv6 ACL
Router(config)# ipv6 nat v6v4 pool natpt-pool-name start-ipv4 end-ipv4 prefix-length prefix-length	规定转换过程中使用的源 IPv4 地址池，参数 natpt-pool-name 指定这个池的名称。像 IPv4 池的前缀一样，必须指定地址池的第一个和最后一个 IPv4 地址，分别用参数 start-ipv4 和 end-ipv4 表示
Router(config)# ipv6 nat v6v4 source {list| route-map}{list-name | map-name| pool-natpt-pool-name}	配置动态 NAT-PT 映射，关键词 list 和参数 list-name 指定一个标准的 IPv6 ACL 来规定 IPv6 地址的范围，关键词 route-map 和参数 map-nam 可以作为替换，关键词 pool 和参数 natpt-pool-name 规定了源 IPv4 地址池

(3)、(4)两空为配置 E0 端口的 IP 地址，(3)为 IP 地址，即 192.17.5.1，(4)为子网掩码，即 255.255.255.0。R1(config-if)#ipv6 nat 的功能是在接口上启用 NAT-PT 机制，这个命令基于接口使用。(6)中填写 IPv6 的地址，如图可知为 2001:aaaa::1。R1(config)#ipv6 access-list ipv6 permit 2001:aaaa::1/64 any 规定了 IPv6 单协议网络中允许被转换的 IPv6 地址范围。(8)详细说明在 IPv6 域内 NAT-PT 使用的 IPv6 前缀，NAT-PT 只支持/96 的网络前缀。Router(config)# ipv6 nat v6v4 pool natpt-pool-name start-ipv4 end-ipv4 prefix-length

prefix-length 规定转换过程中使用的源 IPv4 地址池，(9)、(10)分别是起始地址和结束地址。

【问题 3】NAT 分为三种类型：静态 NAT、动态 NAT 和 NAPT-PT(网络地址端口转换协议转换)。静态模式提供一对一的 IPv6 地址和 IPv4 地址的映射。动态 NAT 也提供一对一的映射，但是使用一个 IPv4 地址池。NAPT-PT 提供多个有 NAT-PT 前缀的 IPv6 地址和一个源 IPv4 地址间的多对一动态映射。

答案：

【问题 1】(1) IPv4　　(2) IPv6

【问题 2】(3) 192.17.5.1　　(4) 255.255.255.0　　(5) 在接口上启用 NAT-PT

(6) 2001:aaaa::1　　(7) 指定 IPv6 网络中允许被转换的 IPv6 地址范围

(8) 2001：aaaa：0:0:0:1::/96　　(9) 16.23.31.10

(10) 16.23.31.20

【问题 3】(11) 静态模式　　(12) 动态模式　　(13) NAPT-PT(网络地址端口转换协议转换)

【例 10-14】分析：

【问题 1】本题考查路由的配置格式以及 RIP 协议的基本配置。(1)、(2)分别填写 IP 地址和子网掩码；而 R1(config)# router rip 是进入 RIP 协议配置子模式的指令；R1(config-router)# network 192.168.1.0 声明网络是 192.168.1.0/24。

【问题 2】要求在 R2 上使用访问控制列表禁止网络 192.168.20.0/24 上的主机访问网络 192.168.10.0/24，在 R3 上使用访问控制列表禁止网络 192.168.20.0/24 上的主机访问 10.10.10.0/24 上的 Web 服务，根据允许和禁止的先后顺序规定，可得到答案。

【问题 3】本题考试使用控制访问列表禁止和允许访问列表的顺序，应先禁止后允许访问。此外 www 服务器的端口号为 80。

答案：

【问题 1】(1)192.168.1.1　　(2)255.255.255.0　　(3)router rip　　(4)network 192.168.1.0

【问题 2】(5)e0 或 fastethernet 0/0 或 ethernet 0/0　　(6)50　(7)out

【问题 3】1. (8)tcp　　(9)www 或 80

2. 次序不可以调整。一旦调整，则所有的 IP 数据包都可以通过了，起不到禁止网络 192.168.20.0/24 上的主机访问 10.10.10.0/24 上的 Web 服务的作用。

【例 10-15】

分析：

【问题 1】IP 访问控制列表主要有两种类型，一类是标准访问控制列表(IP Standard Access List)，一类是扩展访问控制列表(IP Extended Access Lists)。

- 标准访问控制列表只对数据包中的源地址进行检查，而不考虑目的地址及端口号等过滤选项，表号为 1～99。
- 扩展访问控制列表除了检查源地址和目的地址外，还可以检查指定的协议，根据数据包头中的协议类型进行过滤；还可以检查端口号，根据端口号对数据包进行过滤。扩展访问控制列表的表号范围是 100～199，后来又进行了扩展，扩展的表号是 2000～2699。

【问题 2】此题为路由器端口配置命令，由图中的 IP 地址可以很容易推出(3)为 ethernet 0/0 (e0/0)，(4)为 ethernet 0/1 (e0/1)，(5)为 serial 0/0 (s0/0)。

【问题 3】配置命令为：

```
Router(config)#access-list list-number permit/deny source_IP_address
```

题中禁止内网用户 192.168.1.254 访问公司 Web 服务器和外网，所以 Router(config)#access-list 1 deny host 192.168.1.254，为禁止 192.168.1.254 发出的分组通过，如果不匹配，检查下一条语句；Router(config)#access-list 1 permit any 为允许其他 IP 发出的分组通过，如果不匹配，检查下一条语句；最后两句为激活 ACL 的命令。

【问题 4】此题考查扩展 ACL 的配置命令，其语法为：

```
Router(config)#access-list list-number permit/deny protocol
source_address source_wildcard_mask [protocol_information]
destination_address destination_wildcard_mask [protocol_information] [log]
```

第一句说明允许来自任意源地址到目的地址为 10.10.1.10 的 WWW 服务器的访问，后两句为激活 ACL 命令，进入 e0/0 端口，设定为从端口输出的分组。所以这组 ACL 语句的功能为允许任何主机访问公司内部的 Web 服务。

【问题 5】此题同上题，同样此题考察扩展 ACL 的配置命令，其语法为：

```
Router(config)#access-list list-number permit/deny protocol
source_address source_wildcard_mask [protocol_information]
destination_address destination_wildcard_mask [protocol_information] [log]
```

源主机地址为 192.168.1.2，目的 Web 服务器地址为 10.10.1.10，通过 Telnet 连接，所以语句应为 permit tcp host 192.168.1.2 host 10.10.1.10 eq telnet，又 Telnet 的端口号为 23，所以也可写成 permit tcp host 192.168.1.2 host 10.10.1.10 eq 23。

答案：

【问题 1】(1) 标准 ACL　　(2) 扩展 ACL

【问题 2】(3) ethernet 0/0 (e0/0)　　(4) ethernet 0/1 (e0/1)　　(5) serial 0/0 (s0/0)

【问题 3】(6) host 192.168.1.254　　(7) in

【问题 4】允许任何主机访问公司内部的 Web 服务。

【问题 5】(8) permit tcp host 192.168.1.2 host 10.10.1.10 eq telnet

注意：host x.x.x.x 可以写成 x.x.x.x 0.0.0.0，telnet 可以写成 23。

第 11 章　过关习题

【例 11-1】分析：管理站支持的设备数 N 与轮询间隔 T、单个轮询需要的时间Δ之间的关系为：$N \leqslant T/\Delta$。本题中，T=15×60，Δ=0.4，可得 $N \leqslant 2250$，因此管理站最多可支持的设备个数为 2250。

答案：C

【例 11-2】分析：SNMP 主要有五种报文：get、get-next、set、get-response 和 trap。

- get-request 操作：从代理进程处提取一个或多个参数值。
- get-next-request 操作：从代理进程处提取紧跟当前参数值的下一个参数值。
- set-request 操作：设置代理进程的一个或多个参数值。
- get-response 操作：返回一个或多个参数值。这个操作是由代理进程发出的，它是前面三种操作的响应操作。
- trap 操作：代理进程主动发出报文，通知管理进程有某些事情发生。

答案：(1)A　(2)B

【例 11-3】分析：在 SNMPv3 中，以前叫做管理站和代理的东西现在统一叫做 SNMP 实体(SNMP entity)。

答案： A

【例 11-4】分析：SNMP 的基本功能包括监视网络性能、检测分析网络差错和配置网络。只需将监测到的问题发送到网络管理工作站。

UDP 是面向无连接的，它的格式与 TCP 相比少了很多的字段，简单了很多，这也是传输数据时效率高、SNMP 采用的一个主要原因。

答案： D

【例 11-5】分析：通信规范分析最终的目标是产生通信流量，其中必要的工作是分析网络中信息流量

的分布问题。

答案：B

【例 11-6】分析：SNMP(Simple Network Management Protocol，简单网络管理协议)的前身是简单网关监控协议(SGMP)，用来对通信线路进行管理。RMON 是一组定义了监视网络通信的管理信息库的标准，是 SNMP 管理信息库的扩充，与 SNMP 配合可以提供更有效的管理性能。

答案：B

【例 11-7】分析：PC 主机的子网掩码为 255.255.255.192，所在子网可以分配的 IP 地址最多为 62。

答案：D

【例 11-8】分析：ipconfig 命令使用不同的选项表示不同的命令。ipconfig 命令用于显示各个网卡的 IP 地址、子网掩码和默认网关地址；ipconfig/all 命令用于显示所有网卡的 TCP/IP 配置信息；ipconfig/renew 用于更新网卡的 DHCP 配置。

答案：D

【例 11-9】分析：Netstat -s 按协议显示统计信息。

Netstat -r 显示 IP 路由表的内容。

Netstat -n 显示活动的 TCP 连接。

Netstat -a 显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。

答案：B

【例 11-10】分析：tracert 是路由跟踪实用命令，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。

答案：A

【例 11-11】分析：host1 是通过路由器 e0 端口连接网络的，所以探测到第一跳就应该为 e0 的 IP 地址，即 119.215.67.254。而 www.shangxueba.com 的 IP 从第二行即可得为 208.30.1.101。

答案：(1)B (2)D

【例 11-12】分析：Route 命令的语法如下：

```
Route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]
[if Interface]]
```

- -f：删除路由表中的网络路由、本地环路路由和组播路由。
- -p：与 add 命令联合使用时，一条路由被添加到注册表中，当 TCP/IP 启动时，用于初始化路由；与 print 命令联合使用时，则显示持久路由列表；对于其他命令，这个参数被忽略。
- Command：表示要运行的命令，可用的命令有 add(添加路由)、change(修改已有的路由)、delete(删除路由)和 print(打印路由)。
- Destination：说明目标地址，可以是网络地址、主机地址或默认路由。
- mask Netmask：说明了目标地址对应的子网掩码。
- Gateway：说明下一跃点的 IP 地址。
- metric Metric：说明路由度量值，通常选择度量值最小的路由。
- if Interface：说明接口的索引。

答案：(1)A (2)C

【例 11-13】分析：nslookup 是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令工具。它通常需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器，就可以用这个命令查看不同主机的 IP 地址对应的域名。

答案：A

【例 11-14】分析：nslookup 是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令工具。它通常需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器，就可以用这个命令查看不

同主机的 IP 地址对应的域名。

(1) 语法

```
nslookup [-SubCommand...] [{ComputerToFind | -Server}]
```

(2) 参数说明

- -SubCommand：将一个或多个nslookup子命令指定为命令行选项。
- ComputerToFind：如果未指定其他服务器，就使用当前默认DNS名称服务器查阅ComputerToFind的信息。要查找不在当前DNS域的计算机，在名称上附加句点。
- -Server：指定将该服务器作为DNS名称服务器使用。如果省略了-Server，将使用默认的DNS名称服务器。

答案：B

【例 11-15】分析：netstar -r 命令可以显示路由表。

route 命令可以用来修改本机的路由表。

ipconfig 命令用于显示所有网卡的 TCP/IP 配置参数，可以刷新 DHCP 和域名系统的设置。

tracert 命令用于确定到达目标的路径，并显示通路上每一个中间路由器的 IP 地址。

arp 命令用于显示和修改地址解析协议缓存表的内容，缓存表项是 IP 地址与网卡地址对。

netsh 是一个命令行脚本实用程序，可用于修改计算机的网络配置。

ping 命令通过发送 ICMP 回声请求报文来校验与另外一台计算机的连接。

答案：(1)D (2)B

【例 11-16】分析：端口或网卡有故障是不会产生大量广播包的，但故障可能降低用户的网络传输速度。

局域网会通过生成树(STP)协议阻止环路产生，不至于出现广播风暴。但如果网内没有使用支持 STP 的交换机的话(比如说只使用集线器)，则可能会产生广播风暴。

提高出口带宽与消除大量广播包无关，但可以让用户访问 Internet 时速度快一些。

ARP 欺骗程序会制造大量广播包，造成网速下降。

答案：D

第 12 章　过关习题

【例 12-1】 分析：工作区子系统是由终端设备到信息插座的整个区域，用于将用户终端设备连接到布线系统，主要包括信息插座、跳线、适配器。

答案： A

【例 12-2】分析：80/20 规则是传统网络中广泛应用的一般规则。80/20 规则是基于这样的可能性：通信流量的 80%是在某个网段中流动，只有 20%的通信流量访问其他网段。80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

答案：C

【例 12-3】分析：网络逻辑结构设计输出内容包括以下几点。

- 网络逻辑设计图。
- IP地址分配方案。
- 安全管理方案。
- 具体的软硬件、广域网连接设备和基本的网络服务。
- 招聘和培训网络员工的具体说明。
- 对软硬件费用、服务提供费用以及员工和培训费用的初步估计。

物理网络设计是逻辑网络设计的具体实现，通过对设备的具体物理分布、运行环境等的确定来确保网络的物理连接符合逻辑设计的要求。

这一阶段应得到一份网络物理结构设计文档，输出的内容包括：

- 网络物理结构图和布线方案。
- 设备和部件的详细列表清单。
- 软硬件和安装费用的估算。
- 安装日程表，详细说明服务的时间以及期限。
- 安装后的测试计划。
- 用户的培训计划。

答案：(1)A (2)B

【例 12-4】分析：层次化模型中最为经典的是三层模型。三层模型主要将网络划分为核心层、汇聚层和接入层。

- 核心层：提供不同区域或者下层的高速连接和最优传输路径。
- 汇聚层：将网络业务连接到接入层，并且实施与安全、流量负载和路由相关的策略。
- 接入层：为局域网接入广域网或者终端用户访问用户网络提供接入。

答案：B

【例 12-5】分析：FTTN 、FTTC、FTTH、FTTZ 分别是：

- FTTN(Fiber To The Node，光纤到节点)
- FTTC(Fiber To The Curb，光纤到路边)
- FTTH(Fiber To The Home，光纤到户)
- FTTZ(Fiber To The Zone，光纤到小区)

显然，FTTH 将光纤直接铺到千家万户，覆盖面是最广的。

答案：C

【例 12-6】分析：ADSL(Asymmetrical Digital Subscriber Line)是一种非对称 DSL 技术，可在现有任意双绞线上传输，误码率低。ADSL 在一对铜线上，支持上行速率 512kbps～1Mbps，下行速率 1Mbps～8Mbps，有效传输距离在 3km～5km。

甚高比特率数字用户线(VDSL)可在较短的距离上获得极高的传输速率，是各种 DSL 技术中速度最快的一种，也是一种非对称的技术。

单线路数字用户线(SDSL)技术是对称的，上行通信与下行通信具有相同的传输速率(1.5Mbps)，但 SDSL 技术还不成熟，标准也没有最终确立。

HDSL 的特点是在双绞铜线对上，采用有效的调制、数字均衡、回波抵消、信道编码等技术，均衡全部频段的线路损耗，消除噪声及串扰，使得用户环路的两对常规铜芯电缆能以 2.048Mbps 的速率全双工地进行数据传输，中继距离达 3km～5km。其为对称技术。

所以非对称技术有 ADSL 和 VDSL 两个。

答案：B

【例 12-7】分析：PPPoE 是 Point-to-Point Protocol Over Ethernet 的简称，可以使以太网的主机通过一个简单的桥接设备连到一个远端的接入集中器上。通过 PPPoE 协议，远端接入设备能够实现对每个接入用户的控制和计费。

答案：B

【例 12-8】分析：PDH 兼容方式是 SDH 实现广域网互连的方式之一，也就是说 SDH 能够向前兼容 PDH。SDH 用基本传输模块(STM-1)可以容纳 PDH 的数字信号系列，可在每个 STM-1 帧中封装 63 个 E1 信道。

答案：B

【例 12-9】分析：越是大型网络工程，越是要选择稳定的成熟的网络技术。

答案：C

【例 12-10】分析：

【问题 1】(1) 路由器和核心交换机没有冗余结构，防止单点故障，应该使用双线接入 Internet 并形成

和核心交换的冗余结构。

(2) 企业服务器不能连接在接入交换机下，以免影响桌面用户访问服务器的路径和速度。

(3) 桌面用户连接在核心交换机 2 上影响网络监控和访问控制的实施。

【问题 2】(1) MPLS 技术主要是为了提高路由器转发速率而提出的，其核心思想是利用标签交换取代复杂的路由运算和路由交换；该技术实现的核心是把 IP 数据报文封装在 MPLS 数据包中。

(2) MPLS VPN 的一些基本概念如下。

P(Provider)是核心层设备，为提供商路由器，其为不连接任何 CE 路由器的骨干网路由设备，它相当于标签交换路由器(LSR)。

PE(Provider Edge)是 Provider 的边缘设备，服务提供商骨干网的边缘路由器，它相当于标签边缘路由器(LER)。PE 路由器连接 CE 路由器和 P 路由器，是最重要的网络节点。用户的流量通过 PE 路由器流入用户网络，或者通过 PE 路由器流到 MPLS 骨干网。

CE(Customer Edge)是用户边缘设备，服务提供商所连接的用户端路由器。CE 路由器通过连接一个或多个 PE 路由器，为用户提供服务接入。CE 路由器通常是一台 IP 路由器，它与连接的 PE 路由器建立邻接关系。

【问题 3】(6)提示了查看系统安装情况，应该用 show。

光时域反射计根据光的后向散射与菲涅耳反向原理制作，利用光在光纤中传播时产生的后向散射光来获取衰减的信息，可用于测量光纤衰减、接头损耗、光纤故障点定位以及了解光纤沿长度的损耗分布情况等，是光缆施工、维护及监测中必不可少的工具。

答案：

【问题 1】(1) 所有汇聚层交换机应当分别链接到两个核心层交换机上，形成链路冗余，提高可靠性。

(2) 两个核心层交换机应该分别链接到路由器上，形成链路冗余，提高可靠性。

(3) 企业服务器应该直接连到核心层交换机上，提高访问速度。

(4) 桌面用户不应该直接链接核心层交换机，以免影响交换机性能。

【问题 2】(1) A 或 IP 数据报 (2) B 或 MPLS (3) P (4) PE (5) CE

【问题 3】(6) C 或 show (7) C 或 光时域反射计

【例 12-11】分析：

【问题 1】路由器是工作在 OSI 标准模型的第三层——网络层的数据包转发设备，它通过转发数据包来实现网络互联。路由器通常连接两个或多个由 IP 子网或点到点协议标识的逻辑端口，至少拥有 1 个物理端口。而设备①起到的作用是将此 IP 子网连接到网络中去，所以设备①应为路由器。

由于网络要求部署流控网关对 P2P 流量进行限制，以保证正常上网需求，因此设备②是流控服务器。

设备③是核心交换机，连接局域网接入交换机。

信息中心部署在图书馆；学校信息中心部署服务器，根据要求，一方面要对服务器有完善的保护措施，另一方面要对内外网分别提供不同的服务，所以应在信息中心部署防火墙，即设备④为防火墙，部署在核心交换机上。

【问题 2】常用传输介质的特性如表 12-8 所示。

表 12-8 常用传输介质的特性

传输介质	子 类	特点及应用
双绞线	三类 UTP	10Base T(10Mbps)、令牌环(16Mbps)、电话
	五类 UTP	100Base T (100Mbps)
	超五类 UTP	100Base T(100Mbps)、ATM(155Mbps)
	六类 UTP	1000Base T(1000Mbps)
	STP	外加屏蔽层，施工困难
同轴电缆	基带同轴电缆	阻抗 50Ω，细缆用于 10Base 2，粗缆用于 10Base 5

	宽带同轴电缆	阻抗 75Ω，用于 CATV
光纤	多模光纤	适合于近距离传输，价格便利
	单模光纤	较高的传输率、较长的传输距离、较高的成本

因为要求核心交换机到汇聚交换机以千兆链路聚合，同时千兆到桌面，所以将五类 UTP 排除。介质 1 连接核心交换机和接入交换机，传输距离较长，需要较高的传输率，所以使用单模光纤；介质 2 连接网络接入交换机和内部接入交换机，为短距离传输，所以使用六类 UTP；食堂到宿舍的接入交换机为近距离传输，使用多模光纤。

由于实验楼、办公楼、图书馆、学生宿舍分别有一个接入交换机，总共需要 4 个网络接入交换机。实验楼 237 个点，需要 10 个内部接入交换机；办公楼 87 个点，需要 3 个内部接入交换机；学生宿舍 422 个点，需要 18 个内部接入交换机；食堂直接用其他剩余端口，则总共需要的交换机数目为 4+10+3+18=35。

【问题 3】包转发率指基于 64 字节分组，在单位时间内交换机转发的数据总数。转发速率体现了交换引擎的转发性能。端口吞吐量反映端口的分组转发能力。交换机背板是设计值，可以大于等于交换容量(此为达到线速交换机的一个标准)。厂家在设计的时候考虑了将来模块的升级，比如模块从开始的百兆升级到支持千兆、万兆，端口密度增加等。背板带宽多指模块化交换机。它决定了各模板与交换引擎间的连接带宽的最高上限。是交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量。背板带宽标志了交换机总的数据交换能力，单位为 Gbps，也叫交换带宽。

总带宽=端口数×端口速率×2(全双工模式)，所以总带宽为 24×1000Mbps×2=48 000Mbps。

【问题 4】POE 标准供电系统的主要供电特性参数为：

(1) 电压在 44～57V 之间,典型值为 48V。

(2) 允许最大电流为 550mA,最大启动电流为 500mA。

(3) 典型工作电流为 10～350mA,超载检测电流为 350～500mA。

(4) 在空载条件下,最大需要电流为 5mA。

(5) 为 PD 设备提供 3.84～12.95W 五个等级的电功率请求,最大不超过 13W。

答案：

【问题 1】(1) A 或路由器　(2) C 或流控服务器　(3) B 或核心交换机

(4) D 或防火墙　(5) 核心交换机或设备③

【问题 2】(6) A 或单模光纤　(7) C 或 6 类双绞线　(8) B 或多模光纤　(9) 35

【问题 3】(10) 包转发率　(11) 背板带宽　(12) 48 000

【问题 4】(13)C 或 48V