(1)是指按内容访问的存储器。

(1)A.虚拟存储器 B.相联存储器 C.高速缓存（Cache) D.随机访问存储器

**【答案】B**

**【解析】本题考查计算机系统存储器方面的基础知识。**

计算机系统的存储器按所处的位置可分为内存和外存。按构成存储器的材料，可分为磁存储器、半导体存储器和光存储器。按存储器的工作方式可分为读写存储器和只读 存储器。按访问方式可分为按地址访问的存储器和按内容访问的存储器。按寻址方式可分为随机存储器、顺序存储器和直接存储器。

相联存储器是一种按内容访问的存储器。

处理机主要由处理器、存储器和总线组成。总线包括（2)。

(2)A.数据总线、地址总线、控制总线 B.并行总线、串行总线、逻辑总线

C.单工总线、双工总线、外部总线 D.逻辑总线、物理总线、内部总线

**【答案】A**

**【解析】本题考查计算机系统总线和接口方面的基础知识。**

广义地讲，任何连接两个以上电子元器件的导线都可以称为总线。通常可分为4类:

①芯片内总线。用于在集成电路芯片内部各部分的连接。

②元件级总线。用于一块电路板内各元器件的连接。

③内总线，又称系统总线。用于构成计算机各组成部分（CPU、内存和接口等）的连接。

④外总线，又称通信总线。用计算机与外设或计算机与计算机的连接或通信。

连接处理机的处理器、存储器及其他部件的总线属于内总线，按总线上所传送的内容分为数据总线、地址总线和控制总线。

计算机中常采用原码、反码、补码和移码表示数据，其中，±0编码相同的是（3）。

(3)A.原码和补码 B.反码和补码 C.补码和移码 D.原码和移码

**【答案】C**

**【解析】本题考查计算机系统数据编码基础知识。**

设机器字长为n (即采用n个二进制位表示数据），最高位是符号位，0表示正号，1表示负号。

原码表示方式下，除符号位外，n-1位表示数值的绝对值。因此，n为8时，[+0]原 = 0 0000000，[-0]原=l 0000000。

正数的反码与原码相同，负数的反码则是其绝对值按位求反。n为8时，数值0的反码表示有两种形式：[+0]反=0 0000000, [-0]反=1 1111111。

正数的补码与其原码和反码相同，负数的补码则等于其反码的末尾加1。在补码表示中，0 有唯一的编码：[+0]原= 0 0000000, [-0]原=00000000。

移码表示法是在数X上增加一个偏移量来定义的，常用于表示浮点数中的阶码。机器字长为n时，在偏移量为2n-1的情况下，只要将补码的符号位取反便可获得相应的移码表示。

某指令流水线由5段组成，第1、3、5段所需时间为△t，第2、4段所需时间分别为3△t、2△t,如下图所示，那么连续输入n条指令时的吞吐率（单位时间内执行的指令个数）TP为（4）,

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wlgcs-09-s-s-4.jpg

(4)A.http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wlgcs-09-s-s-4-2.jpg B.

C.http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wlgcs-09-s-s-4-4.jpg D.

**【答案】B**

**【解析】本题考査计算机系统流水线方面的基础知识。**

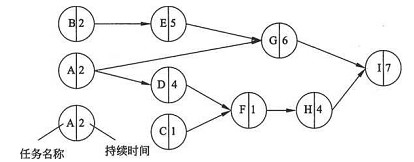
吞吐率和建立时间是使用流水线技术的两个重要指标。吞吐率是指单位时间里流水线处理机流出的结果数。对指令而言，就是单位时间里执行的指令数。流水线开始工作，须经过一定时间才能达到最大吞吐率，这就是建立时间，若m个子过程所用时间一样，

均为△t0，则建立时间T0 = m△t0。

本题目中，连续输入n条指令时，第1条指令需要的时间为(l+3+l+2+l)△t，之后，每隔3△t便完成1条指令，即流水线一旦建立好，其吞吐率为最长子过程所需时间的倒数。综合n条指令的时间为(1+3+1+2+1)△t+ (/j-1)X3△t，因此吞吐率为

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wlgcs-09-s-s-4-3.jpg

某项目主要由A〜I任务构成，其计划图（如下图所示）展示了各任务之间的前后关系以及每个任务的工期（单位：天)，该项目的关键路径是（5）。在不延误项目总工期的情况下，任务A最多可以推迟开始的时间是（6）天。



(5)A.A—G—I B.A—D—F—H—I C.B—E—G—I D.C—F—H—I

(6)A.0 B.2 C.5 D.7

**【答案】C B**

**【解析】**

(5)本题考査项目计划的关键路径和松弛时间。图中任务流A—G—I的持续时间为15; 任务流A—D—F—H—I的持续时间为18;任务流B—E—G—I的持续时间为20;任务流C—F—H—I的持续时间为13。因此关键路径为B—E—G—I,其持续时间是20。

(6)任务A处于任务流A—G—I和任务流A—D—F—H—I中，分别持续时间为15和18，因此任务A的可延迟开始时间为2。

软件风险一般包含（7)两个特性。

(7)A.救火和危机管理 B.己知风险和未知风险

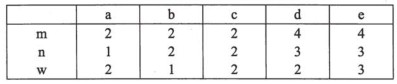
C.不确定性和损失 D.员工和预算

**【答案】C**

**【解析】本题考查软件风险的特性。**

软件风险一般包括不确定性和损失两个特性，其中不确定性是指风险可能发生，也可能不发生：损失是当风险确实发生时，会引起的不希望的后果和损失。救火和危机管理是对不适合但经常采用的软件风险管理策略。己知风险和未知风险是对软件风险进行分类的一种方式。员工和预算是在识别项目风险时需要识别的因素。

设系统中有R类资源m个，现有n个进程互斥使用。若每个进程对R资源的最大需求为w，那么当m、n、w取下表的值时，对于下表中的a~e五种情况，(8)两种情况可能会发生死锁。对于这两种情况，若将（9),则不会发生死锁。



(8)A.a和b B.b和c C.c和d D.c和e

(9)A.n加1或w加1 B.m加1或w减1

C.m减1或w加1 D.m减1或w减1

**【答案】D B**

**【解析】**

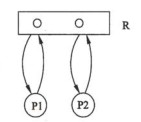
(8)本题考查对操作系统死锁方面基本知识掌握的程度。系统中同类资源分配不当会引起死锁。一般情况下，若系统中有m个单位的存储器资源，它被n个进程使用，当每个进程都要求w个单位的存储器资源，当m<nw时，可能会引起死锁。

试题（8)分析如下：

情况a: m=2, n=l, w=2,系统中有2个资源，1个进程使用，该进程最多要求2个资源，所以不会发生死锁。

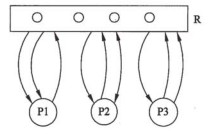
情况b: m=2, n=2, w=l,系统中有2个资源，2个进程使用，每个进程最多要求1个资源，所以不会发生死锁。

情况c: m=2, n=2, w=2,系统中有2个资源，2个进程使用，每个进程最多要求2个资源，此时，采用的分配策略是轮流地为每个进程分配，则第一轮系统先为每个进程分配1个，此时，系统中已无可供分配的资源，使得各个进程都处于等待状态导致系统发生死锁，这时进程资源图如下图所示。



情况d: m=4, n=3, w=2,系统中有4个资源，3个进程使用，每个进程最多要求2个资源，此时，采用的分配策略是轮流地为每个进程分配，则第一轮系统先为每个进程分配1个资源，此时，系统中还剩1个资源，可以使其中的一个进程得到所需资源并运行完毕，所以不会发生死锁。 .

情况e: m=4, n=3, w=3,系统中有4个资源，3个进程使用，每个进程最多要求3个资源，此时，采用的分配策略是轮流地为每个进程分配，则第一轮系统先为每个进程分配1个，第二轮系统先为一个进程分配1个，此时，系统中已无可供分配的资源，使得各个进程都处于等待状态导致系统发生死锁，这时进程资源图如下图所示。



(9) 对于c和e两种情况，若将m加1，则情况c: m=3，+ n=2, w=2,系统中有3个资源，2个进程使用，每个进程最多要求2个资源，系统先为每个进程分配1个，此时，系统中还剩1个可供分配的资源，使得其中的一个进程能得到所需资源执行完，并释放所有资源使另一个进程运行完毕；若将w减1，则情况c: m=2, n=2, w=l，系统中有2个资源，两个进程各需一个，系统为每个进程分配1个，此时，进程都能运行完，显然不会发生死锁。情况e分析同理。

关于软件著作权产生的时间，表述正确的是（10).

(10)A.自作品首次公开发表时

B.自作者有创作意图时

C.自作品得到国家著作权行政管理部门认可时

D.自作品完成创作之日

**【答案】D**

**【解析】本题考査知识产权中关于软件著作权方面的知识。**

在我国，软件著作权采用“自动保护”原则。《计算机软件保护条例》第十四条规定：“软件著作权自软件开发完成之日起产生。”即软件著作权自软件开发完成之日起自动产生，不论整体还是局部，只要具备了软件的属性即产生软件著作权，既不要求履行任何形式的登记或注册手续，也无须在复制件上加注著作权标记，也不论其是否己经发 表都依法享有软件著作权。

—般来讲，一个软件只有开发完成并固定下来才能享有软件著作权。如果一个软件一直处于开发状态中，其最终的形态并没有固定下来，则法律无法对其进行保护。因此， 条例（法律）明确规定软件著作权自软件开发完成之日起产生。当然，现在的软件开发 经常是一项系统工程，一个软件可能会有很多模块，而每一个模块能够独立完成某一项功能。自该模块开发完成后就产生了著作权。所以说，自该软件开发完成后就产生了著作权。

E载波是ITU-T建议的传输标准，其中E3信道的数据速率大约是（11) Mb/s.贝尔系统T3信道的数据速率大约是（12) Mb/s。

(11)A.64 B.34 C.8 D.2

(12)A.1.5 B.6.3 C.44 D.274

**【答案】B C**

**【解析】**

(11)E载波是ITU-T建议的数字传输标准，分为5个复用级别。在E1信道中，8位组成—个时槽，32个时槽（TS0〜TS31)组成一个帧，16个帧组成一个复帧。在E1帧中，TS0 用于帧控制，TS16用于随路信令和复帧控制，其余的30个时槽用于传送话音和数据。

E1载波的数据速率为2.048Mb/s，其中每个信道的数据速率是64Kb/s。

E2信道由4个El信道组成，数据速率为8.448Mb/s。

E3信道由16个E1信道组成，数据速率为34.368Mb/s»

(12) E4信道由4个E3信道组成，数据速率为139.264Mb/s。

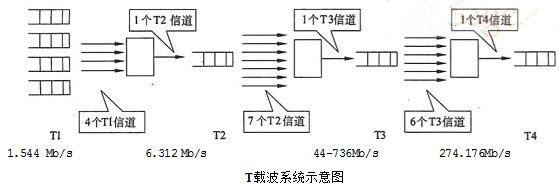
E5信道由4个E4信道组成，数据速率为565.148Mb/s。

T载波是贝尔系统的数字传输标准（如下图所示)，在北美和日本使用。T载波中话音信道的数据速率为56Kb/sd4路话音被复合在一条T1信道上，其数据速率为1.544Mb/s。

T2信道由4个T1信道组成，数据速率为6.312Mb/s。

T3信道由7个T2信道组成，数据速率为44.736Mb/s。

T4信道由6个T3信道组成，数据速率为274.176Mb/s。



RS-232-C的电气特性采用V.28标准电路，允许的数据速率是（13),传输距离不大于（14)。

(13)A.lKb/s B.20Kb/s C.100Kb/s D.IMb/s

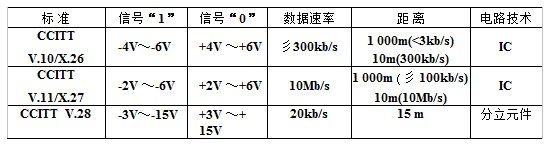
(14)A.lm B.15m C.100m D.lKm

**【答案】B B**

**【解析】**

物理层标准规定了 DTE与DCE之间接口的机械特性、电气特性、功能特性和过程特性。RS-232-C是主要的物理层接口之一，是PC的标准设备。RS-232-C的机械特性没有规定，可以采用25针、15针或9针D型连接器，RS-232-C的电气特性与CCITTV.28 标准兼容。常用的各种电气特性标准参见下表。

三种电气特性标准比较



曼彻斯特编码的特点是（15)，它的编码效率是（16)。

(15)A.在“0”比特的前沿有电平翻转，在“1”比特的前沿没有电平翻转

B.在“1”比特的前沿有电平翻转，在“0”比特的前沿没有电平翻转

C.在每个比特的前沿有电平翻转

D.在每个比特的中间有电平翻转

(16)A.50% B.60% C.80% D.100%

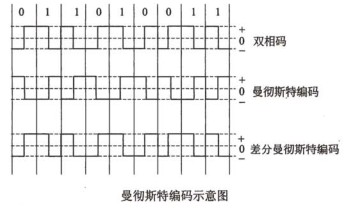
**【答案】D A**

**【解析】**

(15)曼彻斯特编码（Manchester Code)是一种双相码（或称分相码）。双相码要求每一 位中间都要有一个电平转换，因而这种代码的优点是自定时，同时双相码也有检测差错的功能，如果某一位中间缺少了电平翻转，则被认为是违例代码。在下图中，我们用髙 电平到低电平的转换边表示“0”，而低电平到髙电平的转换边表示“1”，相反的表示也是允许的。比特中间的电平转换既表示了数据代码，同时也作为定时信号使用。曼彻斯特编码用在以太网中。

差分曼彻斯特编码类似于曼彻斯特编码，它把每一比特的起始边有无电平转换作为 区分“0”和“1”的标志，这种编码用在令牌环网中。

(16)在曼彻斯特编码和差分曼彻斯特编码中，每比特中间都有一次电平跳变，因此波特率是数据速率的两倍。对于100Mb/s的高速网络，如果采用这类编码方法，就需要200M 的波特率，其硬件成本是100M波特率硬件成本的5〜10倍。作为一种变通的办法，可以使用4B/5B或8B/10B编码。



HDLC协议是一种（17),采用（18)标志作为帧定界符。

(17)A.面向比特的同步链路控制协议 B.面向字节计数的同步链路控制协议

C.面向字符的同步链路控制协议 D.异步链路控制协议

(18)A.10000001 B.01111110 C.10101010 D.10101011

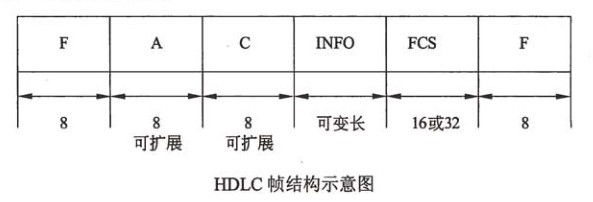
**【答案】A B**

**【解析】**

（17）数据链路控制协议分为面向字符的协议和面向比特的协议。面向字符的协议以字符作为传输的基本单位，并用10个专用字符控制传输过程。面向比特的协议以比特作为传 输的基本单位，它的传输效率高，广泛地应用于公用数据网中。

HDLC (High Level Data Link Control,高级数据链路控制）协议是ISO根据IBM公 司的SDLC (Synchronous Data Link Control)协议扩充开发而成的。美国国家标准化协会（ANSI)则根据SDLC开发出类似的协议，叫做ADCCP协议（Advanced Data Communication Control Procedure)。

(18) HDLC使用统一的帧结构进行同步传输，下图为HDLC帧的格式示意图。HDLC帧由6个字段组成，以两端的标志字段（F)作为帧的边界，在信息字段（INFO)前面的三个字段（F、A和C)叫做帧头，信息字段后面的两个字段（FCS和F)叫做帧尾，信息字段中包含了要传输的数据。



HDLC用一种特殊的比特模式01111110作为标志以确定帧的边界。同一个标志既可以作为前一帧的结束，也可以作为后一帧的开始。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。在接收帧的过程中如果发现一个标志，则认为该帧结束了。如果帧中间出现比特模式01111110时，也会被当作标志，从而破坏了帧的同步。为了避免这种错误，要使用位填充技术，即发送站的数据比特序列中一旦发现0后有5个1，则在第7位插入一个0。这样就保证了传输的数据比特序列中不会出现与帧标志相同的比特模式。接收站则进行相反的操作：在接收的比特序列中如果发现0后有5个1,则检查第7位，若第7位为0则删除之；若第7位是1且第8位是0,则认为是检测到帧尾的标志域；若第7位和第8位都是1，则认为是发送站的停止信号。

设信道带宽为3400Hz，采用PCM编码，采样周期为125us，每个样本量化为128个等级，则信道的数据速率为（19).

(19)A.10Kb/s B.16Kb/s C.56Kb/s D.64Kb/s

**【答案】C**

**【解析】**

模拟信号通过数字信道传输具有效率高、失真小的优点，而且可以开发新的通信业务。常用的数字化技术就是脉冲编码调制技术（Pulse Code Modulation, PCM),简称脉码调制。PCM主要经过3个过程：采样、量化和编码。采样过程通过周期性扫描将时间连续幅度连续的模拟信号变换为时间离散、幅度连续的采样信号，量化过程将采样信号变为时间离散、幅度离散的数字信号，编码过程将量化后的离散信号编码为二进制码组输出。

采样的频率决定了恢复的模拟信号的质量。根据尼奎斯特采样定理，为了恢复原来的模拟信号，采样频率必须大于模拟信号最高频率的二倍，即

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wlgcs_09_s_s_19.jpg

其中/为采样频率，T为采样周期，fmax为信号的最高频率。

电话线路中带通滤波器的带宽为3kHz (即300〜3300Hz)»根据Nyquist采样定理，最小采样频率应为6600 Hz，CCITT规定话音信号的采样频率为8kHz»采样后得到的样本必须通过四舍五入量化为离散值，离散值的个数决定了量化的精度。在T1系统中采用128级量化，每个样本用7位二进制数字表示，在数字信道上传输这种数字化了的话音信号的速率是7X8000=56kb/s。在E1系统中采用256级量化，每个样本用8位二进制数字表示，传输速率为64kb/s。

设数据码字为10010011，采用海明码进行校验，则必须加入（20)比特冗余位才能纠正一位错。

(20)A.2 B.3 C.4 D.5

**【答案】C**

**【解析】**

海明（Hamming)研究了用冗余数据位来检测和纠正代码差错的理论和方法。按照海明的理论，可以在数据代码上添加若干冗余位组成码字，码字之间的海明距离是一个码字变成另一个码字时必须改变的最小位数。海明用数学分析的方法说明了海明距离的几何意义，n位的码字可以用n维空间的超立方体的一个顶点来表示，两个码字之间的 海明距离就是超立方体的两个对应顶点之间的一条边，而且这是两顶点（从而两个码字) 之间的最短距离，出错的位数小于这个距离都可以被判断为就近的码字。这就是海明码纠错的原理，它用码位的增加（因而通信量的增加）来换取正确率的提高。

如果对于m位的数据，增加k位冗余为，则组成n=m+k位的纠错码。对于2m个有效码字中的每一个，都有你、n个无效但可以纠错的码字，这些可纠错的码字与有效码字的距离是1，含单个出错位。这样，对于一个有效的消息总共有n+1个可识别的码字。这n+1个码字相对于其他2m-1个有效消息的距离都大于1.这意味着2m（n+1）个有效的或者可纠错的码字。显然这个数应小于等于码字的可能的个数，即2n。于是有2m（n+1）<2n。因为n=m+k,得出m+k+1，对于给定的数据位m，上式给出了k的下界，即要纠正单个错误，k必须取的最小值。 在本题中，数据码字为10010011的m=8,由上式计算出的k的最小值应为4。

可以把所有使用DHCP协议获取IP地址的主机划分为不同的类别进行管理。下面的选项列出了划分类别的原则，其中合理的是（21)

(21)A.移动用户划分到租约期较长的类 B.固定用户划分到租约期较短的类

C.远程访问用户划分到默认路由类 D.服务器划分到租约期最短的类

**【答案】C**

**【解析】**

动态主机配置协议DHCP用于在大型网络中为客户端自动分配IP地址及有关网络参数（默认网关和DNS服务器地址等)。使用DHCP服务器便于进行网络管理，可以节省网络配置的工作量，有效地避免网络地址冲突，还能解决IP地址资源不足的问题。

DHCP租约周期是IP地址的有效期。租约周期可长可短，取决于用户的上网环境和工作性质。一般把移动用户划分到租约期较短的管理类，把固定用户划分到租约期较长的管理类，远程访问用户划分到默认路由类。对于服务器主机则要为其保留固定的IP地址，并且要把保留的IP地址与服务器主机的MAC地址进行绑定。

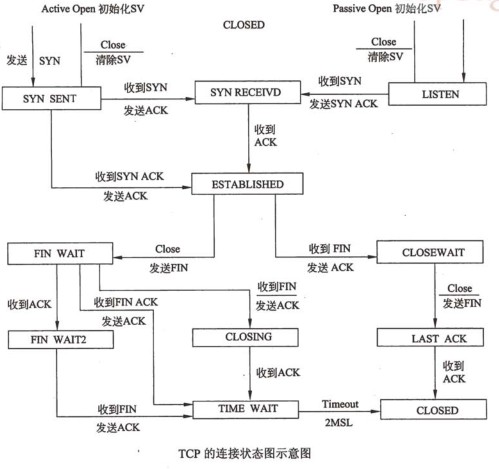
TCP协议在建立连接的过程中可能处于不同的状态，用netstat命令显示出TCP连接的状态为SYN\_SEND，则这个连接正处于（22)。

(22)A.监听对方的建立连接请求 B.已主动发出连接建立请求

C.等待对方的连接释放请求 D.收到对方的连接建立请求

**【答案】B**

**【解析】**



上图表示TCP的连接状态图。事实上，在TCP协议运行过程中，有多个连接处于不同的状态。当TCP处于SYN\_SEND状态时，表示协议实体已主动发出连接建立请求。

Tracert命令通过多次向目标发送（23)来确定到达目标的路径，在连续发送的多个IP数据包中，(24)字段都是不同的。

(23)A.ICMP地址请求报文 B.ARP请求报文

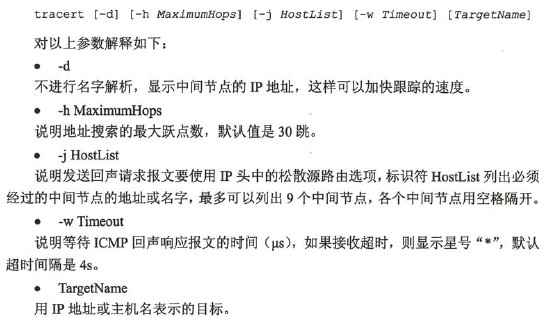
C.ICMP回声请求报文 D.ARP响应报文

(24)A.源地址 B.目标地址 C.TTL D.ToS

**【答案】C C**

**【解析】**

(23)Tracer 命令的功能是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。通过多次向目标发送ICMP回声（echo)请求报文，每次增加IP头中TTL字段的值，就可以确定到达各个路由器的时间。显示的地址是路由器接近源的这一边的端口地址。Tracert命令的语法如下：



这个诊断工具通过多次发送ICMP回声请求报文来确定到达目标的路径，每个报文中的TTL字段的值都是不同的。通路上的路由器在转发IP数据报之前先要对TTL字段减一，如果TTL为0,则路由器就向源端返回一个超时（Time Exceeded)报文，并丢弃原来要转发的报文。在tracert第一次发送的回声请求报文中置TTL=1，然后每次加1， 这样就能收到沿途各个路由器返回的超时报文，直至收到目标返回的ICMP回声响应报文。如果有的路由器不返回超时报文，那么这个路由器就是不可见的，显示列表中用星号表示之。 .

举例如下：

1. 要跟踪到达主机corp7.microsoft.com的路径，则键入：

tracert corp7.microsofl.com

2. 要跟踪到达主机corp7.microsoft.com的路径，并且不进行名字解析，只显示中间节点的IP地址，则键入：

tracert -d corp7.microsoft.com

3. 要跟踪到达主机corp7.microsoft.com的路径，并使用松散源路由，则键入：

tracert -j 10.12.0.1 10.29.3.1 10.1.44.1 corp7.microsoft.com

(24) 下图是利用命令tracert www. 163.com.cn显示的路由跟踪列表。



OSPF协议适用于4种网络。下面的选项中，属于广播多址网络（Broadcast Multi-Access) 的是（25) ，属于非广播多址网络（None Broadcast Multi-Access)的是（26)。

(25)A.Ethernet B.PPP C.Frame Relay D.RARP

(26)A.Ethernet B.PPP C.Frame Relay D.RARP

**【答案】A C**

**【解析】**

(25)OSPF定义了 4种网络：

广播多址网络（Broadcast Multi-Access)，例如 Ethernet、Token Ring 和 FDDI 等。

(26) 非广播多址网络（None Broadcast Multi-Access，NBMA)，例如 Frame Relay、 X.25 和 SMDS 等。

点到点网络（Point-to-Point)，例如 PPP、HDLC 等。

点到多点网络（Point-to-Multi-Point)，例如运行RARP协议网络。

RIPv2是增强了的RIP协议，下面关于RIPv2的描述中，错误的是（27).

(27)A.使用广播方式来传播路由更新报文

B.采用了触发更新机制来加速路由收敛

C.支持可变长子网掩码和无类别域间路由

D.使用经过散列的口令字来限制路由信息的传播

**【答案】A**

**【解析】**

RIP分为两个版本，RIPvl (RFC 1058，1988)是早期的路由协议，现在仍然广泛使用。RIPvl使用目标地址为255.255.255.255的广播来共享路由信息，默认的路由更新周期为30s，持有时间（Hold-Down Time)为180s。也就是说，RIP路由器每30s向它的所有邻居发送一次路由更新报文，如果在180s之内没有从某个邻居接收到路由更新报文，则认为该邻居已经崩溃或者其间的连接已失效。这时如果从其他邻居收到了有关同一目标的路由更新报文，则用新的路由信息替换已失效的路由表项；否则，对应的路由表项被删除。

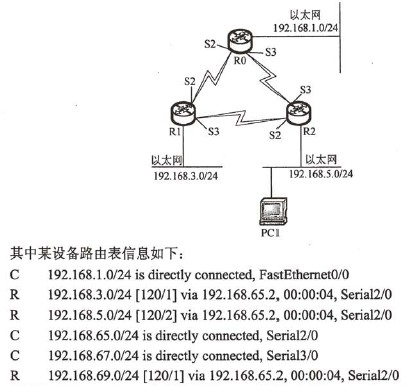
RIP以跳步计数（hopcount)来度量路由费用，显然这不是最好的度量标准。例如，若有两条到达某个网络的连接，一个连接是经过两跳的10M以太网连接，一个连接是经过一跳的64K WAN连接，则RIP选取WAN连接作为最佳路由。在RIP协议中，15跳是最大的跳数，16跳就是不可到达网络，经过16跳的任何分组将被路由器丢弃。

RIPvl是有类别的协议（class’flil protocol)，这意味着配置RIPvl时必须给定A、B 或C类IP地址和子网掩码，例如不能把子网掩码255.255.255.0用于B类网络172.16.0.0。

对于同一个目标，RIP路由表项中最多可以有6条等费用的通路，虽然默认的是4 条。RIP可以实现等费用通路的负载均衡（equal>cost load balancing),这种机制提供了链路冗余，以对付可能出现的连接失效，但是RIP不支持不等费用通路的负载均衡，这种功能出现在IGRP和EIGRP中。

RDV2是增强了的REP协议，基本上还是一个距离矢量路由协议，但是有三方面的改进。首先是它使用组播而不是广播来传播路由更新报文，并且采用了触发更新 (triggeredupdate)机制来加速路由收敛，即出现路由变化时立即向邻居发送路由更新报文，而不必等待更新周期是否到达。其次是RIPv2是一个无类别的协议（classless protocol),可以使用可变长子网掩码(VLSM),也支持无类别域间路由（CIDR)，这些功能使得网络的设计更具有伸缩性。第三个増强是RIPv2支持认证，使用经过散列的口令字来限制更新信息的传播。其他方面的特性与第一版相同，例如以跳步计数来度量路由费用，允许的最大跳步数为15等。

网络配置如下图所示：



则该设备为（28),从该设备到PCI经历的路径为（29).路由器R2接口S2 可能的IP地址为（30).

(28)A.路由器R0 B.路由器R1 C.路由器R2 D.计算机PC1

(29)A.R0—R2—PC1 B.R0—R1—R2 C.Rl—R0—PC1 D.R2—PC1

(30)A.192.168.69.2 B.192.168.65.2 C.192.168.67.2 D.192.168.5.2

**【答案】A B A**

**【解析】**

(28)采用showiproute可以査看路由表信息。题中的各条命令解释如下：

1. 192.168.1.0/24 网络通过以太口 FastEthemet0/0 直连；

2. 192.168.3.0/24网络通过串口 Serial2/0路由可达；

3. 192.168.5.0/24网络通过串口 Serial2/0路由可达；

4. 192.168.65.0/24 网络通过串 口 Serial2/0 直连：

5. 192.168.67.0/24 网络通过串 口 Serial3/0 直连；

6. 192.168.69.0/24 网络通过串 口 Serial2/0 路由可达。

依据图中拓扑信息，192.168.1.0/24网络只和路由器R0直连，故空（28)选A。

(29) 从R0到PC1所在网络192.168.5.0/24需经串口Serial2/0路由可达；串口 Seria2/0

连接的是路由器R1，故从R0到PC1经历的路径为R0—Rl—R2—PC1，空（29)选B。

(30) 从路由表中可以看出，192.168.1.0/24为R0直连；192.168.3.0/24为R1直连； 192.168.5.0/24 为 R1 直连；192.168.65.0/24 直连 R0 Serial2/0 口； 192.168.67.0/24 直连 R0SeriaB/0 P； S2 接口只可能属于 192.168.69.0/24 网络，故空（30)选 A

下列关于Windows 2003中域的描述正确的是（31)

(31)A.在网络环境中所有的计算机称为一个域

B. 同一个域中可以有多个备份域控制器

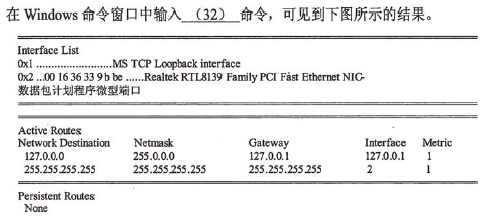
C.每个域中必须有主域控制器和备份域控制器

D.一个域中可以有多个主域控制器

**【答案】B**

**【解析】本题考查Windows域的基础知识。**

域(Domain)是一个共用“目录服务数据库”的计算机和用户的集合，用于实现集中式管理。域是逻辑分组，与网络的物理拓扑无关。 域中只能有一个主域控制器，但可以有零个或多个备份域控制器。



(32)A.ipconfig /all B.route print C.tracert –d D.nslookup

**【答案】B**

**【解析】本题考查常用网络命令。**

ipconfig/all用于显示计算机中所有网络适配器（网卡、拨号连接等）的完整TCP/IP配置信息，如IP地址、子网掩码及默认网关。route print用于查看本机路由表。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，-d指定不将IP地址解析到主机名称。nslookup用于查询域名对应的IP地址。

Linux操作系统中，建立动态路由需要用到文件（33).

(33)A./etc/hosts B./etc/hostname

C./etc/resolv.conf D./etc/gateways

**【答案】D**

**【解析】本题考查Linux常用配置文件。**

/etc/hosts是配置ip地址和其对应主机名的文件。/etc/ hostname包含了系统的主机名称，包括完全的域名。/etc/resolv.conf是DNS域名解析的配置文件。/etc/gateways是路由表文件。

Linux操作系统中，网络管理员可以通过修改（34)文件对Web服务器的端口进行配置。

(34)A./etc/inetd.conf B./etc/lilo.conf

C./etc/httpd/conf/httpd.conf D./etc/httpd/confi/access.conf

**【答案】C**

**【解析】本题考查Linux下Web服务器常用配置文件。**

/etc/inetd.conf是TCP/IP服务配置文 件，在其中可以添加或删除一个服务。/etc/lilo.conf是加载器配置文件，用于配置Linux 的引导参数。/etc/httpd/conf/httpdxonf为Web服务器主配置文件，在其中可以配置服务器所使用的端口号。/etc/httpd/confi/access.conf包含了 Web服务器中大部分同安全和用户访问相关的设置。

Linux有三个查看文件的命令，若希望能够用光标上下移动来查看文件内容，应使用(35)命令。

(35)A.cat B.more C.less D.menu

**【答案】C**

**【解析】本题考査Linux文件内容查看命令。**

使用cat、more、less都可以査看文本内容，cat 命令一次性将文件内容全部输出，more命令可以分页查看，less命令可以使用光标向上 或向下移动一行。menu命令和查看文件无关。

Windows Server 2003操作系统中，IIS 6.0不提供下列（36)服务。

(36)A. Web B.SMTP C.POP3 D.FTP

**【答案】C**

**【解析】本题考查IIS服务的基本概念。**

Windows Server 2003操作系统中，默认情况没有安装IIS服务，必须手工安装。US 是Windows下架设Web、FTP, SMTP服务器的一套整合软件。在IIS中，没有提供POP3服务。

Windows Server 2003操作系统中，(37)提供了远程桌面访问。

(37)A.FTP B.Email C.Terminal Service D.Http

**【答案】C**

**【解析】本题考查网络服务的基本概念。**

终端服务（Tenninal Service)提供了通过作为终端仿真器工作的“瘦客户端”软件远程访问服务器桌面的能力。终端服务基本由三部分技术组成，即客户端部分、协议部 分及服务器端部分。客户端和服务器通过远程桌面协议进行通信。

若在Windows “运行”窗口中键入（38)命令，可以查看和修改注册表

(38)A.CMD B.MMC C.AUTOEXE D.Regedit

**【答案】D**

**【解析】本题考查Windows的相关命令。**

CMD命令的作用是打开命令行终端。Microsoft管理控制台（MMC)集成了各种工具（包括管理单元)，可用来管理本地和远程计算机。Windows中没有AUTOEXE命令。 Regedit提供了编辑注册表的功能。

以下关于网络安全设计原则的说法，错误的是（39)。

(39)A.充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测，是设计网络安全系统的必要前提条件

B.强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽可能快地恢复网络信息中心的服务，减少损失

C.考虑安全问题解决方案时无需考虑性能价格的平衡，强调安全与保密系统的设计应与网络设计相结合

D.网络安全应以不能影响系统的正常运行和合法用户的操作活动为前提

**【答案】C**

**【解析】**

网络安全设计是保证网络安全运行的基础，基本的设计原则包括强调对信息均衡、 全面地进行保护的木桶原则、良好的信息安全系统必备的等级划分制度，网络信息安全的整体性原则、安全性评价与平衡原则等。在进行网络安全系统设计时应充分考虑现有网络结构以及性能价格的平衡，安全与保密系统的设计应与网络设计相结合。

在Windows Server 2003的DNS服务器中通过（40)操作，实现多台Web服务器构成集群并共享同一域名。

(40)A.启用循环（Round Robin)，添加每个Web服务器的主机记录

B.禁止循环（Round Robin)，启动转发器指向每个Web服务器

C.启用循环（Round Robin),启动转发器指向每个Web服务器

D.禁止循环（Round Robin),添加每个Web服务器的主机记录

**【答案】A**

**【解析】本题考查DNS的基本概念。**

DNS服务器启动循环功能可以将同一域名映射到多个主机，是分享和分配网络资源 的本地平衡机制。在Windows Server 2003的DNS服务器中，为了实现多台Web服务器构成集群并共享同一域名，需要启动DNS循环功能，添加每个Web服务器的主机记录。

廉价磁盘冗余阵列RAID利用冗余技术实现高可靠性，其中RAID1的磁盘利用率为（41)。如果利用4个盘组成RAID3阵列，则磁盘利用率为（42)。

(41)A.25% B.50% C.15% D.100%

(42)A.25% B.50% C.75% D.100%

**【答案】B C**

**【解析】本题考查廉价磁盘冗余阵列RAID的相关知识。**

RAID分为0〜7这8个不同的冗余级别，其中RAID0级无冗余校验功能；RAID1采用磁盘镜像功能，磁盘容量的利用率是50%;

Alice向Bob发送数字签名的消息M,则不正确的说法是（43)。

(43)A.Alice可以保证Bob收到消息M B.Alice不能否认发送过消息M

C.Bob不能编造或改变消息M D.Bob可以验证消息M确实来源于Alice

**【答案】A**

**【解析】本题考查数字签名的相关概念。**

数字签名设计为发送者不可否认、接收者可以验证但不能编造或篡改。所以选项B、 C和D都是正确的。选项A显然是错误的。

安全散列算法SHA-1产生的摘要的位数是（44).

(44)A.64 B.128 C.160 D.256

**【答案】C**

**【解析】本题考查安全散列算法SHA-1的基础知识。**

安全散列算法SHA-1是SHA的改进版本，此算法以最大长度不超过2M位的消息为输入，生成160位的消息摘要输出，用512为块来处理输入。

在X.509标准中，不包含在数字证书中的数据域是（45)。

(45)A.序列号 B.签名算法 C.认证机构的签名 D.私钥

**【答案】D**

**【解析】本题考查数字证书的基础知识。**

数字证书中包含用户的公钥，而用户的私钥只能被用户拥有。所以选项D是不可能包含在数字证书中的。

两个公司希望通过Internet传输大量敏感数据，从信息源到目的地之间的传输数据以密文形式出现，而且不希望由于在传输节点使用特殊的安全单元而增加开支，最合适的加密方式是（46)，使用会话密钥算法效率最高的是（47).

(46)A.链路加密 B.节点加密 C.端-端加密 D.混合加密

(47) A.RSA B.RC-5 C.MD5 D.ECC

**【答案】C B**

**【解析】**

(46)通过Internet传输数据，报文在路由器间依据路由选择算法进行转发，所经过的路径并不唯一，故采用链路加密难以实现；节点加密开支过大：混合加密结合多种方式， 也不符合题意；端-端加密在发送端与接收端之间进行加解密，是最合适的加密方式。

(47) 在传输过程中采用对称密钥比非对称密钥效率要高，故选择RC-5。

包过滤防火墙对通过防火墙的数据包进行检查，只有满足条件的数据包才能通过，对数据包的检查内容一般不包括（48)。

(48)A.源地址 B.目的地址 C.协议 D.有效载荷

**【答案】D**

**【解析】本题考查包过滤防火墙的相关知识。**

防火墙的基本功能是包过滤，能对进出防火墙的数据包包头（包括源地址、目的地址和协议）进行分析处理，但对于数据包的有效载荷一般无法分析处理。所以答案是D。

下面关于ARP木马的描述中，错误的是（49)。

(49)A.ARP木马利用ARP协议漏洞实施破坏

B.ARP木马发作时可导致网络不稳定甚至瘫痪

C.ARP木马破坏网络的物理连接

D.ARP木马把虚假的网关MAC地址发送给受害主机

**【答案】C**

**【解析】本题考査计算机病毒的相关知识。**

ARP木马的工作原理是利用ARP协议漏洞，把虚假的网关MAC地址发送给受害机，造成局域网内出现大量的ARP消息从而造成网络拥塞。但并没有破坏网络的物理连通性。所以选项C是错误的

下面几个网络管理工具的描述中，错误的是（50)。

(50)A.netstat可用于显示IP、TCP、UDP, ICMP等协议的统计数据

B.sniffer能够使网络接口处于杂收模式，从而可截获网络上传输的分组

C.winipcfg采用MS-DOS工作方式显示网络适配器和主机的有关信息

D.tracert可以发现数据包到达目标主机所经过的路由器和到达时间

**【答案】C**

**【解析】本题考查网络管理工具。**

其中，netstat可用于显示IP、TCP、UDP、ICMP等协议的统计数据；sniffer能够使用网络接口处于杂收模式，从而可截获网络上传输的分组：winipcfg在Windows中显示网络适配器和主机的有关信息；tracert可以发现数据包到达目标主机所经过的路由器和到达时间。

—个网络的地址为172.16.7.128/26，则该网络的广播地址是（51)。,

(51)A.172.16.7.255 B.172.16.7.129 C.172.16.7.191 D.172.16.7.252

**【答案】C**

**【解析】**

IP地址分为网络地址和主机地址两部分，一个网络的广播地址是将其主机地址部分置为全1。地址 172.16.7.128/26 的二进制形式为10101100.00010000.00000111.10000000, 则该网络的广播地址是10101100.00010000.00000111.10111111,即172.16.7.191。

使用CIDR技术把4个C 类网络192.24.12.0/24、192.24.13.0/24、192.24.14.0/24和192.24.15.0/24汇聚成一个超网，得到的地址是（52).

(52)A.192.24.8.0/22 B.192.24.12.0/22

C.192.24.8.0/21 D.192.24.12.0/21

**【答案】B**

**【解析】**

CIDR技术是把小的网络汇聚成大的超网。这里的4个网络地址的二进制表示如下。

192.24.12.0/24 的二进制表示为：11000000 00011000 00001100 00000000

192.24.13.0/24 的二进制表示为：11000000 00011000 00001101 00000000

192.24.14.0/24 的二进制表示为：11000000 00011000 00001110 00000000

192.24.15.0/24 的二进制表示为：11000000 00011000 00001111 00000000

可以看出，汇聚后的网络地址为11000000 00011000 00001100 00000000，即192.24. 12.0/22。

某公司网络的地址是133.10.128.0/17,被划分成16个子网，下面的选项中不属于这16个子网的地址是（53)。

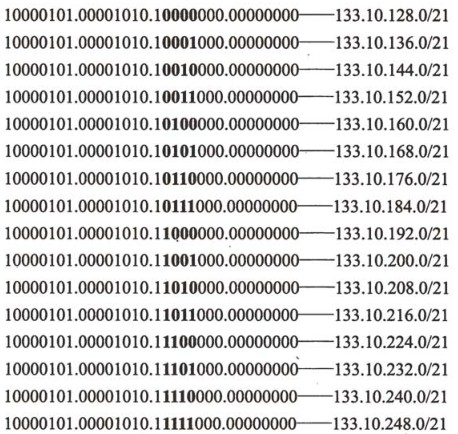
(53)A.133.10.136.0/21 B.133.10.162.0/21

C.133.10.208.0/21 D.133.10.224.0/21

**【答案】B**

**【解析】**

地址133.10.128.0/17的二进制表示为 10000101.00001010.10000000.00000000 将其划分为16个子网，则各个子网的地址为：



可以看出，以上16个网络地址的第三个字节都能被8整除，而答案B中的162不能被8整除。

以下地址中不属于网络100.10.96.0/20的主机地址是（54)。

(54)A.100.10.111.17 B.100.10.104.16

C.100.10.101.15 D.100.10.112.18

**【答案】D**

**【解析】**

地址100.10.111.17的二进制形式为:01100100.00001010.01101111.00010001

地址100.10.104.16的二进制形式为:01100100.00001010.01101000.00010000

地址100.10.101.15的二进制形式为 :01100100.00001010.01100101.00001111

地址100.10.112.18的二进制形式为:01100100.00001010.01110000.00010010

而地址 100.10.96.0/20 的二进制形式为：01100100.00001010.01100000.00000000 只有答案D不能与其匹配。

自动专用 IP 地址（Automatic Private EP Address, APIPA)是 IANA (Internet Assigned Numbers Authority)保留的一个地址块，它的地址范围是（55)。当(56)时，使用 APIPA。

(55)A.A 类地址块 10.254.0.0〜10.254.255.255

B.A 类地址块 100.254.0.0〜100.254.255.255

C.B 类地址块 168.254.0.0〜168.254.255.255

D.B 类地址块 169.254.0.0〜169.254.255.255

(56)A.通信对方要求使用APIPA地址 B.由于网络故障而找不到DHCP服务器

C.客户机配置中开启了 APIPA功能 D.DHCP服务器分配的租约到期试题

**【答案】D B**

**【解析】**

(55)自动专用IP地址（Automatic Private IP Address, APIPA)是当客户端无法从DHCP 服务器中获得IP地址时自动配置的地址。IPv4地址前缀169.254/16已经被IANA注册为APIPA专用（RFC 3927)。

(56)当网络中的DHCP服务器失效，或者由于网络故障而找不到DHCP服务器时，这个功能开始生效，使得客户端可以在一个小型局域网中运行，与其他自动或手工获得APIPA 地址的计算机进行通信。其实APIPA的主要用途是为了移动计算使用的，两个笔记本式计算机用户之间可以通过APIPA地址直接通信，而不需要其他网络连接的支持。

VLAN中继协议（VTP)用于在大型交换网络中简化VLAN的管理。按照VTP协议，交换机的运行模式分为3种：服务器、客户机和透明模式。下面关于VTP协议的描述中，错误的是（57)

(57)A.交换机在服务器模式下能创建、添加、删除和修改VLAN配置

B.一个管理域中只能有一个服务器

C.在透明模式下可以进行VLAN配置，但不能向其他交换机传播配置信息

D.交换机在客户机模式下不允许创建、修改或删除VLAN 试题

**【答案】B**

**【解析】**

VLAN中继协议（VLAN Trunking Protocol，VTP)是Cisco公司的专利协议，用于在大型交换网络中简化VLAN的管理。VTP协议在交换网络中建立了多个管理域，同一管理域中的所有交换机共享VLAN信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享VLAN信息。通过VTP协议，可以在一台交换机上配置所有的VLAN，配置信息通过VTP报文可以传播到管理域中的所有交换机。

按照VTP协议，交换机的运行模式分为3种：

1. 服务器模式（Server)。交换机在此模式下能创建、添加、删除和修改VLANS置，并从中继端口发出VTP组播帧，把配置信息分发到整个管理域中的所有交换机。一个管理域中可以有多个服务器。

2. 客户机模式（Client)。交换机在此模式下不允许创建、修改或删除VLAN,但可以监听本管理域中其他交换机的VTP组播信息，并据此修改自己的VLAN配置。

3. 透明模式（Transparent)。交换机在此模式下可以进行VLAN配置，但配置信息不会传播到其他交换机。在透明模式下，可以接收和转发VTP帧，但是并不能据此更新自己的VLAN配置，只是起到通路的作用。

VTP协议的优点有：

•提供通过一个交换机在整个管理域中配置VLAN的方法；

•提供跨不同介质类型（如ATM、FDDI和以太网）配置VLAN的方法：

• 提供跟踪和监视VLAN配置的方法；

•保持VLAN配置的一致性。

新交换机出厂时的默认配置是（58)。

(58)A.预配置为VLAN1,VTP模式为服务器 B.预配置为VLAN1,VTP模式为客户机

C.预配置为VLAN0, VTP模式为服务器 D.预配置为VLANO,VTP模式为客户机

**【答案】A**

**【解析】**

新交换机出厂时的预配置为VLAN1，VTP模式为服务器。

在生成树协议（STP) IEEE 802.1d中，根据(59)来选择交换机。

(59)A.最小的MAC地址 B.最大的MAC地址

C.最小的交换机ID D.最大的交换机ID

**【答案】C**

**【解析】**

生成树协议（Spanning Tree Protocol, STP)是交换式以太网中的重要技术，其目的是在交换机之间存在冗余连接的情况下避免网络中出现环路，实现网络的高可靠性。STP 原来是DEC公司开发的协议，EEE增强了它的功能：颁布了802.1d标准。这两种实现不兼容，Cisco交换机默认支持802.1d协议。

802.Id定义了交换机之间交换的网桥协议数据单元BPDU (如下图所示)，其中包含了交换网络的拓扑结构信息，例如交换机（或网桥）标识符BID、链路性质和根交换机标识符（Rood BID)等。

当交换网络中有多个VLAN时，一个交换机在每个VLAN中有不同的BID,每个 VLAN运行STP协议的一个实例，每个VLAN都有它自己的根交换机，各个VLAN的根交换机可以相同，也可以不同。在每个VLAN中，由STP协议确定根交换机，决定哪些端口处于转发状态，哪些端口处于阻塞状态，以免引起VLAN内部的环路。



按照802.1d定义的生成树算法，每个网桥有唯一的MAC地址和唯一的优先级，地址和优先级构成网桥的标识符BID (8字节)。根桥是作为生成树根的网桥，通常选择BID最小的网桥作为根桥。其他网桥选择到达根桥费用最小的通路作为根通路（Root Path),与根桥连接的端口称为根端口。互相连接的每个LAN都有一个指定桥，这是在 该LAN上能提供最小费用根通路的网桥。指定桥连接LAN的端口叫做指定端口。按照以上算法，直接连接两个LAN的网桥中只能有一个作为指定桥，其他都从生成树中删除掉，这就排除了两个LAN之间的任何环路。同理，以上算法也排除了多个LAN之间的环路，但保持了连通性。

由于802.1d协议的生成树算法收敛速度比较慢，可能达到30〜50s,对于某些实时应用（例如VoIP)这是不能容忍的，因此IEEE把Cisco交换机的一些扩展特性融入原来的802.1d中，颁布了收敛速度更快的快速生成树协议（Rapid Spanning Tree Protocol, RSTP) 802.lw,提供了交换机、交换机端口或整个网络的快速故障恢复功能。

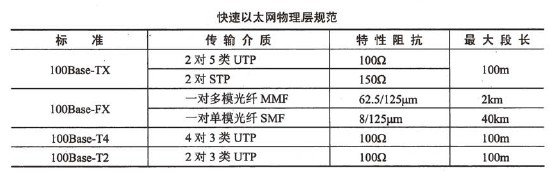
在快速以太网物理层标准中，使用两对5类无屏蔽双绞线的是（60)。

(60)A.100Base-TX B.100Base-FX C.100Base-T4 D.100Base-T2

**【答案】A**

**【解析】**

1995年,100Mb/s的快速以太网标准IEEE 802.3u正式颁布，这是基手10Base-T和lOBase-F技术、在基本布线系统不变的情况下开发的高速局域网标准。快速以太网使用的传输介质如下表所示，其中多模光纤的芯线直径为62.5um,包层直径为125um;单模光线芯线直径为8um，包层直径也是125um。



在Windows系统中，所谓“持久路由”就是（61)。要添加一条到达目标10.40.0.0/16 的持久路由，下一跃点地址为10.27.0.1，则在DOS窗口中键入命令（62).

(61)A.保存在注册表中的路由 B.在默认情况下系统自动添加的路由

C.—条默认的静态路由 D.不能被删除的路由

(62)A.route -s add 10.40.0.0 mask 255.255.0.0 10.27.0.1

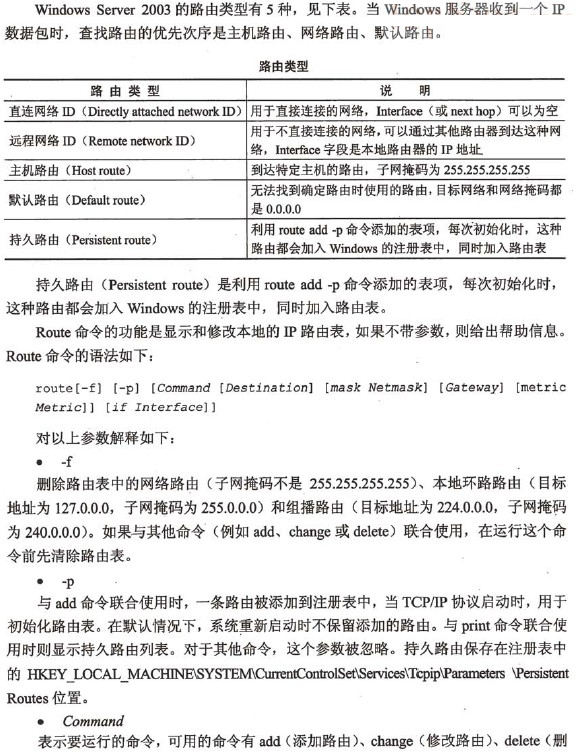
B.route -p add 10.27.0.1 10.40.0.0 mask 255.255.0.0

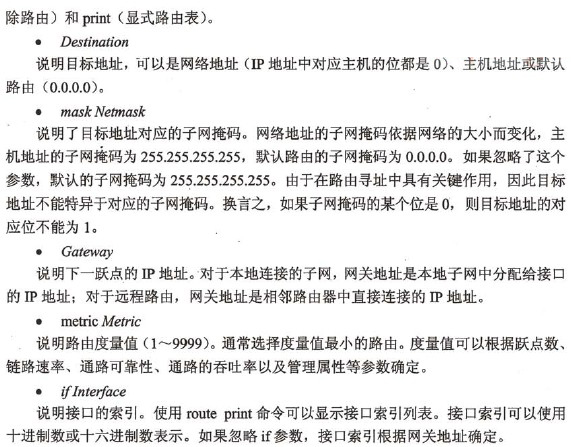
C.route -p add 10.40.0.0 mask 255.255.0.0 10.27.0.1

D.route -s add 10.27.0.1 10.40.0.0 mask 255.255.0.0

**【答案】A C**

**【解析】**





访问控制列表（ACL)分为标准和扩展两种。下面关于ACL的描述中，错误的是 (63).

(63)A.标准ACL可以根据分组中的IP源地址进行过滤

B.扩展ACL可以根据分组中的IP目标地址进行过滤

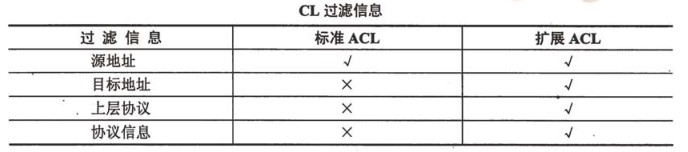
C.标准ACL可以根据分组中的IP目标地址进行过滤

D.扩展ACL可以根据不同的上层协议信息进行过滤

**【答案】C**

**【解析】**

访问控制列表（ACL)根据源地址、目标地址、源端口或目标端口等协议信息对数据包进行过滤，从而达到访问控制的目的。ACL分为标准的和扩展的两种类型。标准ACL只能根据分组中的IP源地址进行过滤，例如可以允许或拒绝来自某个源设备的所有通信。扩展ACL不但可以根据源地址或目标地址进行过滤，还可以根据不同的上层协议和协议信息进行过滤。例如，可以对PC与远程服务器的Telnet会话进行过滤。两种ACL过滤功能的区别见下表。



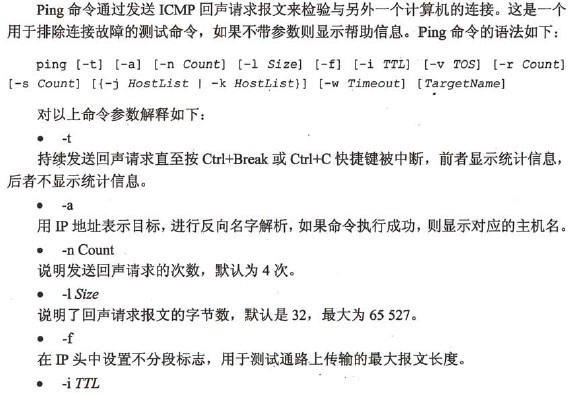
`如果要测试目标10.0.99.221的连通性并进行反向名字解析,则在DOS窗口中键入命令（64)。

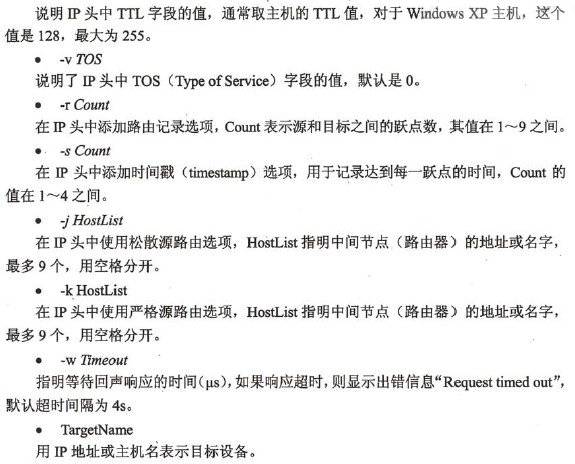
(64)A.ping -a 10.0.99.221 B.ping -n 10.0.99.221

C.ping -r 10.0.99.221 D.ping -j 10.0.99.221

**【答案】A**

**【解析】**





在IEEE 802.11标准中使用了扩频通信技术，下面选项中有关扩频通信技术说法正确的是（65)。

(65)A.扩频技术是一种带宽很宽的红外线通信技术

B.扩频技术就是用伪随机序列对代表数据的模拟信号进行调制

C.扩频通信系统的带宽随着数据速率的提高而不断扩大

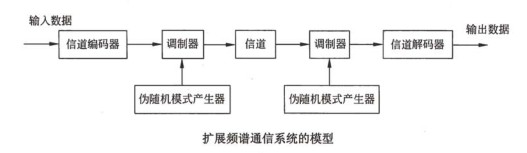
D.扩频技术就是扩大了频率许可证的使用范围

**【答案】B**

**【解析】**

扩展频谱通信技术起源于军事通信网络，其主要想法是将信号散布到更宽的带宽上以减少发生阻塞和干扰的机会。早期的扩频方式是频率跳动扩展频谱（Frequency Hopping Spread Spectrum, FHSS),更新的版本是直接序列扩展频谱（Direct Sequence Spread Spectrum, DSSS)。

下图表示了各种扩展频谱系统的共同特点。输入数据首先进入信道编码器，产生一个接近某中央频谱的较窄带宽的模拟信号。再用一个伪随机序列对这个信号进行调制。调制的结果是大大拓宽了信号的带宽，即扩展了频谱。在接收端，使用同样的伪随机序列来恢复原来的信号，最后再进入信道解码器来恢复数据。



伪随机序列由一个使用初值（称为种子seed)的算法产生。算法是确定的，因此产生的数字序列并不是统计随机的。但如果算法设计得好，得到的序列能够通过各种随机性测试，这就是被叫做伪随机序列的原因。重要的是，除非你知道算法与种子，否则预测序列是不可能的。因此，只有与发送器共享同一伪随机序列的接收器才能成功地对信号进行解码。

下面关于WLAN安全标准IEEE 802.11i的描述中，错误的是（66).

(66)A.采用了髙级加密标准AES B.定义了新的密钥交换协议TKIP

C.采用802.lx实现访问控制 D.提供的加密方式为有线等价协议WEP

**【答案】D**

**【解析】**

原来的IEEE802.il标准提供的加密方式是有线等价协议（Wired Equivalency Protocol, WEP), WEP包括共享密钥认证和数据加密两个过程。共享密钥认证使得没有 WEP密钥的用户无法访问网络，而加密则要求所有数据必须用密文传输。

认证采用了标准的询问和响应帧格式。执行过程中，AP根据RC4算法运用共享密钥对128字节的随机序列进行加密后作为询问帧发给用户，用户将收到的询问帧进行解密后以明文形式响应AP, AP将明文与原始随机序列进行比较，如果两者一致，则通过认证。

2004年6月公布的IEEE 802.11i标准是对WEP协议的改进，为无线局域网提供了全新的安全技术。802.11i定义了新的密钥交换协议（Temporal Key Integrity Protocol,TKIP)和高级加密标准（Advanced Encryption Standard, AES)。TKIP 提供了报文完整性检查，每个数据包使用不同的混合密钥（per-packet key mixing),每次建立连接时生成—个新的基本密钥（re-keying),这些手段的采用使得诸如密钥共享、碰撞攻击和重放攻击等无能为力，从而弥补了 WEP协议的安全隐患。另外，IEEE 802.11还采用802.lx实现访问控制，根据用户端的MAC地址进行认证，从而防止了非法访问。

安全审计是保障计算机系统安全的重要手段，其作用不包括（67)。

(67)A.重现入侵者的操作过程

B.发现计算机系统的滥用情况

C.根据系统运行的日志，发现潜在的安全漏洞

D.保证可信计算机系统内部信息不外泄

**【答案】D**

**【解析】**

安全审计包括识别、记录、存储、分析与安全相关行为的信息，审计记录用于检查与安全相关的活动和负责人。安全审计系统就是根据一定的安全策略记录和分析历史操作事件及数据，发现能够改进系统运行性能和系统安全的地方。安全审计的作用包括对潜在的攻击者起到震慑或瞀告的作用、检测和制止对安全系统的入侵、发现计算机的滥用情况、为系统管理员提供系统运行的日志，从而能发现系统入侵行为和潜在的漏洞及对已经发生的系统攻击行为提供有效的追纠证据。安全审计系统通常有一个统一的集中管理平台，支持集中管理，并支持对日志代理、安全审计中心、日志、数据库的集中管理，并具有事件响应机制和联动机制。

网络隔离技术的目标是确保把有害的攻击隔离，在保证可信网络内部信息不外泄的前提下，完成网络间数据的安全交换。下列隔离技术中，安全性最好的是（68).

(68)A.多重安全网关 B.防火墙 C.VLAN隔离 D.物理隔离

**【答案】D**

**【解析】**

网络隔离（NetworkIsolation)技术的目标是确保把有害的攻击隔离，在可信网络之外和保证可信网络内部信息不外泄的前提下，完成网间数据的安全交换。有多种形式的网络隔离，如物理隔离、协议隔离和VPN隔离等。无论采用什么形式的网络隔离，其实质都是数据或信息的隔离。网络隔离的重点是物理隔离。物理隔离的一个特征，就是内网与外网永不连接，内网和外网在同一时间最多只有一个同隔离设备建立非TCP/IP协议的数据连接。

下列有关网络设备选型原则中，不正确的是（69).

(69)A.所有网络设备尽可能选取同一厂家的产品，这样在设备可互连性、协议互操作性、技术支持、价格等方面都更有优势

B.在网络的层次结构中，主干设备选择可以不考虑扩展性需求

C.尽可能保留并延长用户对原有网络设备的投资，减少在资金投入上的浪费

D.选择性能价格比高、质量过硬的产品，使资金的投入产出达到最大值

**【答案】B**

**【解析】本题考查网络设备选型的基本原理。**

所有网络设备尽可能选取同一厂家的产品，这样在设备可互连性、协议互操作性、技术支持、价格等方面都更有优势。在网络的层次结构中，主干设备选择应预留一定的能力，以便将来扩展，而低端设备则够用即可。同时，应尽可能保留并延长用户对原有网络设备的投资，使资金的投入产出达到最大值，能以较低的成本、较少的人员投入来维持系统运转。网络系统应具有较高的可靠性。全系统的可靠性主要体现在网络设备的可靠性。

在层次化网络设计中，(70)不是分布层/接入层交换机的选型策略。

(70)A.提供多种固定端口数量搭配供组网选择，可堆叠、易扩展，以便由于信息点的增加而进行扩容

B.在满足技术性能要求的基础上，最好价格便宜、使用方便、即插即用、配置简单

C.具备一定的网络服务质量和控制能力以及端到端的QoS

D.具备高速的数据转发能力

**【答案】D**

**【解析】本题考查层次化网络中网络设备选型的基本原理。**

分布层/接入层交换机也称外围交换机或边缘交换机，一般都属于可堆叠，可扩充式 固定端口交换机。在大中型网络中它用来构成多层次的结构灵活的用户接入网络，在中 小型网络中它也可能用来构成网络骨干交换设备，应具备下列要求：

1)灵活性。提供多种固定端口数量搭配供组网选择，可堆叠、易扩展，以便由于 信息点的增加而进行扩容。

2)高性能。作为大型网络的二级交换设备，应支持千兆/百兆高速上连（最好支持 FEC/GEC)，以及同级设备堆叠，当然还要注意与核心交换机品牌的一致性：如果用作 小型网络的中央交换机，要求具有较髙的背板带宽和三层交换能力等。

3) 在满足技术性能要求的基础上，最好价格便宜、使用方便、即插即用、 简单。

4)具备一定的网络服务质量和控制能力以及端到端的QoS。

5) 如果用于跨地区企业分支部门通过公网进行远程上联的交换机，还应支持虚拟专网VPN标准协议。

6)支持多级别网络管理。

The Border Gateway Protocol (BGP) is an interautonomous system (71) protocol. The primary function of a BGP speaking system is to exchange network (72) information with other BGP system. This network reachability information includes information on the list of Autonomous System (ASs) that reachability information traverses. BGP-4 provides a new set of mechanisms for supporting (73) interdomain routing. These mechanisms include support for advertising an IP (74) and eliminate the concept of network class within BGP. BGP-4 also introduces mechanisms that allow aggregation of routes, including (75) of AS paths. These changes provide support for the proposed supernetting scheme.

(71)A.connecting B.resolving C.routing D.supemettting

(72)A.secubility B.reachability C.capability D.reliability

(73)A.answerless B.connectionless C.confirmless D.classless

(74)A.prefix B.suffix C.infix D.reflex

(75)A.reservation B.relation C.aggregation D.connection

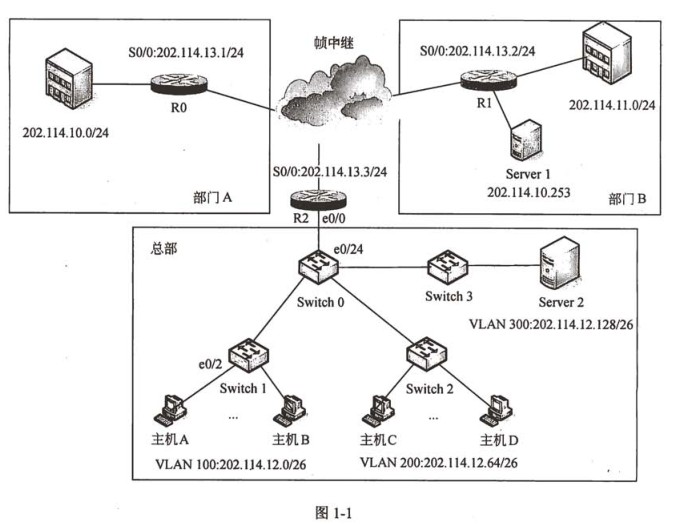
**【答案】C B D A C**

**【解析】**

边界网关协议BGP是自治系统间的路由协议。BGP发布系统的基本功能就是与其他BGP系统交换网络可到达性信息。这种网络可到达性信息包含了可到达性信息穿越的自治系统的列表。BGP-4提供了一系列新的机制来支持无类别的域间路由。这些机制包括支持发布IP前缀，从而在BGP中排除了网络类别的概念。BGP-4也引入了路由聚合机制，包括AS通路的聚合。这些改变提供了对提议的超网方案的支持。

**试题一**

某公司有1个总部和2个分部，各个部门都有自己的局域网。该公司申请了4个C 类IP地址块202.114.10.0/24〜202.114.13.0/24。公司各部门通过帧中继网络进行互联，网络拓扑结构如图1-1所示。



**【问题1】**

请根据图1-1完成R0路由器的配置：

R0 (config) #interface s0/0 (进入串口配置模式）

R0 (config-if) # ip address 202.114.13.1 (1) (设置IP地址和掩码）

R0 (config)\* # encapsulation (2) (设置串口工作模式）

(1)225.255.255.0

(2) frame-relay

本题涉及IP地址配置、VLAN以及交换机路由器配置基本命令。

从网络拓扑图可以看出，R0所在路由器S0端口掩码应为255.255.255.0，同时，由于S0端口线路工作为帧中继，因此S0端口工作模式应配置为帧中继模式。

**【问题2】**

Switch0、Switch1、Switch2和Switch3均为二层交换机。总部拥有的IP地址块为202.114.12.0/24。Switch0的端口e0/24与路由器R2的端口e0/0相连，请根据图1-1完成路由器R2及Switch0的配置。

R2 (config) tinterface fastethernet 0/0.1 R2 (config-subif) #encapsulation dotlq (3)

R2 (config-subif) #ip address 202.114.12.1 255.255.255.192 R2 (config-subif) #no shutdown R2 (config-subif) #exit

R2 (config) #interface fastethernet 0/0.2 R2 (config-subif) .encapsulation dotlq (4)

R2 (config-subif) tip address 202.114.12.65 255.255.255.192 R2 (config-subif) #no shutdown R2 (config-subif) #exit

R2 (config) #interface fastethernet 0/0.3 R2 (config-subif) #encapsulation dotlq (5)

R2 (config-subif) tip address 202.114.12.129 255.255.255.192 R2 (config-subif) #no shutdown R2 (config-subif) #exit R2 (config) #interface fastether0/0 R2 (config-if) #no shutdown

SwitchO (config) #interface f0/24

SwitchO (config-if) # switchport mode (6)

SwitchO (config-if) #switchport trunk encapsulation (7)

SwitchO (config-if) # switchport trunk allowed all Switch0(config-if) #exit

3)100

4)200

5)300

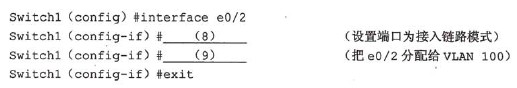
6)trunk

7)dotlq

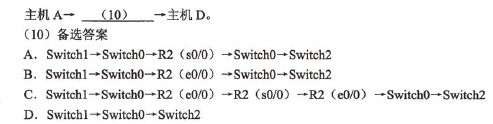
由于Switch0、Switch 1 % Switch2和Switch3均为二层交换机。根据拓扑图可以看出，在路由器R2的端口e0/0需要通过配置独臂路由实现VLAN间路由。根据VLAN的IP地址分配，路由器e0/0下的端口e0/0.1负责线路VLAN100,e0/0.2负责线路VLAN 200, e0/0.3负责线路VLAN300。同时在Switch0的f0/24端口需要配置工作模式为Trunk, 允许通过不同VLAN的数据，VLAN的封装协议为802.1q。

**【问题3】**

若主机A与Switch1 的e0/2端口相连，请完成Switch1 相应端口设置。



若主机A与主机D通信，请填写主机A与D之间的数据转发顺序。



（8）switchport mode access

（9）switchPort access vlan 100

（10）B

主机A与Switch1之间线路为接入链路，因此需要将端口设置为接入链路模式，相应命令为switchport mode access，同时主机A所处VLAN为100,因此使用switch access vlan 100设定端口VLAN 号为100。

主机A与主机D属于不同VLAN，同时由于不同VLAN间路由通过独臂路由实现，因此主机A的数据会通过路由器R2进行转发。

**【问题4】**

为了部门A中用户能够访问服务器Serverl，请在R0上配置一条特定主机路由。

R0 (config) #ip route 202.114.10.253 (11) (12)

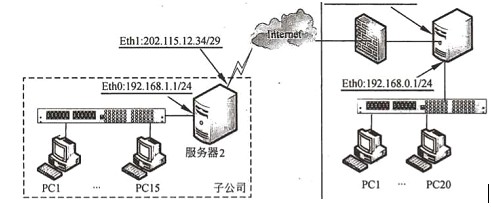
11） 255.255.255.255

12） 202.114.13.2

部门A中用户配置特定主机路由时，子网掩码需配置为255.255.255.255，同时下一条目的地址应指向路由器R1的S0/0端口，相应EP地址为202.114.13.2。

**试题二**

某公司总部服务器1的操作系统为Windows Server 2003,需安装虚拟专用网（VPN) 服务，通过Internet与子公司实现安全通信，其网络拓扑结构和相关参数如图2-1所示。



**【问题1】**

在Windows Server 2003的“路由和远程访问”中提供两种隧道协议来实现VPN服务:

（1）和L2TP, L2TP协议将数据封装在（2） 协议帧中进行传输。

1. PPTP (点对点隧道协议）

2. PPP (点对点协议）

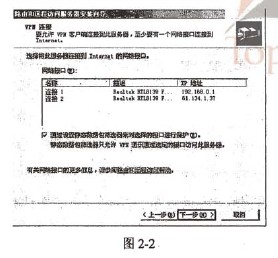
考査的是“路由和远程访问”提供的两种用于创建路由器到路由器的VPN 连接的隧道协议：点对点隧道协议（PPTP)和第二层隧道协议（L2TP)。PPTP是一种VPN隧道协议，是点对点协议（PPP)的扩展，并利用PPP的身份验证、压缩和加密机制。L2TP是一个工业标准Internet隧道协议，它先把各种网络协议封装到PPP中，再把 整个数据包装入隧道协议中。与PPTP—样，L2TP也利用PPP的身份验证和压缩机制。但与PPTP不同的是，L2TP不采用“Microsoft点对点加密（MPPE)”来加密PPP帧。L2TP依赖于加密服务的Internet协议安全性（IPSec)。

**【问题2】**

在服务器1中，利用Windows Server2003的管理工具打开“路由和远程访问”，在所列出的本地服务器上选择“配置并启用路由和远程访问”，然后选择配置“远程访问（拨号或VPN)”服务，在图2-2所示的界面中，“网络接口”应选择（3）

（3）备选答案：

A.连接1B.路由和远程访问



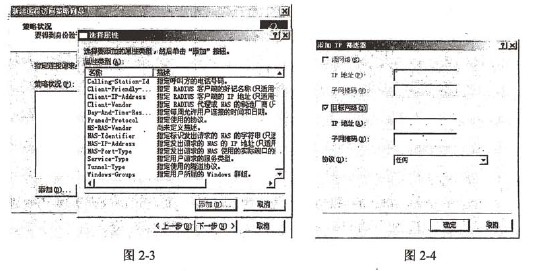
B

本题考查的是远程访问VPN服务的部署。在VPN连接页，应选择连接到Internet的网络接口，因此应选择对应的接口连接2。

**【问题3】**

为了加强远程访问管理，新建一条名为“Sublnc”的访问控制策略，允许来自子公司服务器2的VPN访问。在图2-3所示的配置界面中，应将“属性类型（A)”的名称为 （4) 的值设置为“Layer Two Tunneling Protocol”，名称为（5) 的值设置为“Virtual (VPN)”。

编辑Sublnc策略的配置文件，添加“入站IP筛选器”，在如图2-4所示的配置界面中，IP地址应填为（6)，子网掩码应填为（7)。



4) Tunnel-Type

5) NAS-Port-Vpe

6) 202.115.12.34

7) 255.255.255.255

本题考查的是远程访问策略的配置。要配置远程访问策略以控制VPN连接的身份验证和加密选项，要使用以下设置创建远程访问策略：将NAS-Port-TVpe条件设置为 “Virtual (VPN)”，并将 Tunnel-T^pe 条件设置为“Layer Two Tunneling Protocol' 在配置数据包筛选器时，要键入外部接口的IP地址。在“子网掩码”框中，键入255.255. 255,255.

**【问题4】**

子公司PCI安装Windows XP操作系统，打开“网络和Internet连接”。若要建立与公司总部服务器的VPN连接，在如图2-5所示的窗口中应该选择 (8),在图2-6所示的配置界面中填写（9) 。

(8)备选答案：

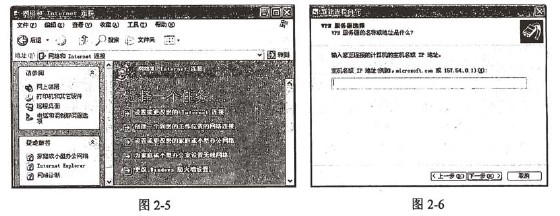
A. 设置或更改您的internet连接

B. 创建一个到您的工作位置的网络连接

C. 设置或更改您的家庭或小型办公网络

D. 为家庭或小型办公室设置无线网络

E. 更改Windows防火墙设置



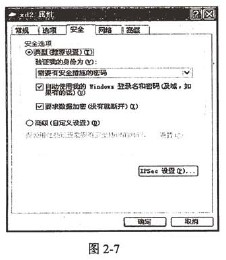
8）B

9）61.134.1.37

本题考查的是VPN客户端的配置。客户端上应新建一个“到您的工作位置的网络连接”，在VPN服务器选择时，要键入VPN服务器计算机的IP地址或主机名。

**【问题5】**

用户建立的VPN连接xd2的属性如图2-7所示，启动该VPN连接时是否需要输入用户名和密码？为什么？

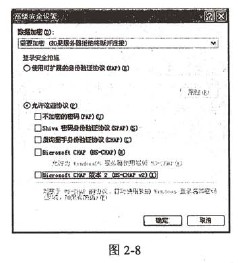


不需要。因为选中“自动使用我的Windows登录名和密码”，此时用本机Windows 登录的用户名和密码进行VPN连接。

本题考査的是VPN身份验证。该VPN连接时是不需要输入用户名和密码的，因为选中了“自动使用我的Windows登录名和密码”，此时用本机Windows登录的用户名和密码进行VPN连接。

**【问题6】**

图2-8所示的配置窗口中所列协议“不加密的密码（PAP)”和“质询握手身份验证协议（CHAP)”有何区别？



PAP使用明文身份验证。

CHAP通过使用MD5和质询-响应机制提供一种加密身份验证。

本题考查的是PPP协议定义的两种类型的认证。握手认证协议（CHAP)使用一种算法（MD-5)来计算只有认证系统和远程设备知道的值。它总是对用户ID和密码进行加密，所以该协议比PAP更安全。此协议对回放和试错法访问企图有效。可以在连接期间执行多次CHAP认证。认证系统向正在尝试连接到网络的远程设备发送一个握手信号。远程设备通过由两个设备使用的公共算法（MD-5)所算出的值进行响应。认证系统对照自己的计算结果检查该响应。当这些值匹配时，认证被认可；否则，结束连接。

不加密的密码（PAP)使用双向握手为同级系统提供鉴别其身份的简单方法，也就是普通的口令认证，要求将密钥信息在通信信道中明文传输。在建立链接时进行握手。 在建立链接之后，远程设备将一个用户ID/密码对发送到认证系统。根据用户ID/密码对的正确与否，认证系统继续连接或结束连接。

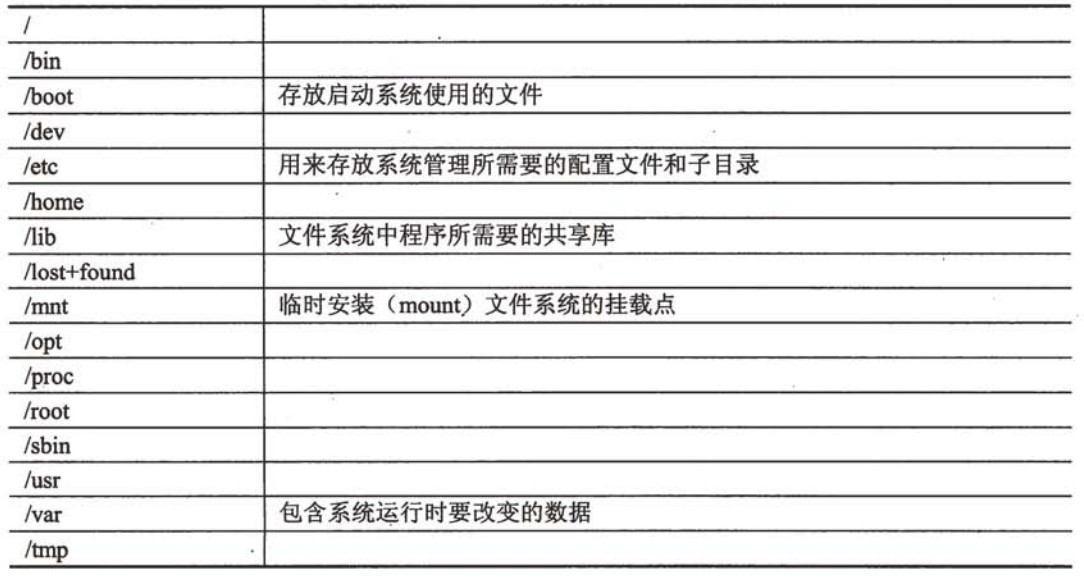
**试题三**

Linux系统采用了树型多级目录来管理文件，树型结构的最上层是根目录，其他的所有目录都是从根目录生成的。

通过Sapba可以实现基于Linux操作系统的服务器和基于Windows操作系统的客户机之间的文件、目录及共享打印服务。

**【问题1】**

Linux在安装时会创建一些默认的目录，如下表所示：



依据上述表格，在空（1)〜（6)中填写恰当的内容（其中空（1）在候选答案中选择)。

①对于多分区的Linux系统，文件目录树的数目是（1）。

@ Linux系统的根目录是（2）,默认的用户主目录在（3）目录下，系统的设备文件（如打印驱动）存放在（4）目录中,（5）目录中的内容关机后不能被保存。

③如果在工作期间突然停电，或者没有正常关机，在重新启动机器时，系统将要复查文件系统，系统将找到的无法确定位置的文件放到目录(6)中。

(1)备选答案：

A. 1B.分区的数目C.大于1

1. A

2. /

3. /home

4. /dev

5. /proc

6. /lost+found

Linux系统中每个分区都是一个文件系统，Linux将这些分属不同分区、单独的文件系统按一定的方式形成一个系统的总目录层次结构，即一个目录树。

Linux使用树型目录结构管理文件和目录。树型结构由一个根目录（root)和根目录下的子目录构成，每一个目录内可以包含下一级目录、文件、指向其他文件系统的符号 链接、表示设备的设备名（如/dev/had)。

Linux系统主要的目录项包括：



**【问题2】**

默认情况下，系统将创建的普通文件的权限设置为-rw-r-r-，即文件所有者对文件（7),同组用户对文件（8),其他用户对文件（9).文件的所有者或者超级用户，采用（10)命令可以改变文件的访问权限。

7）可读、可写

8）仅可读 .

9） 仅可读

10） chmod

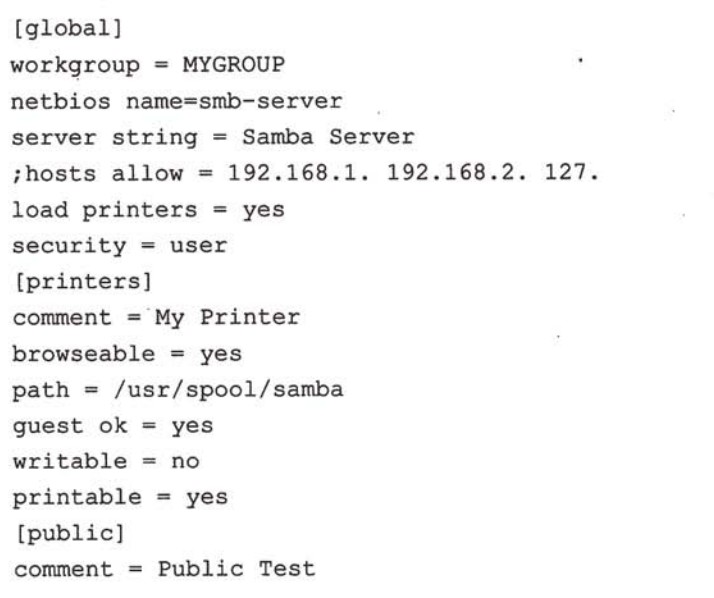
Linux文件的访问权限有4种：读（r)、写（w)、执行（x)和无权(-)。对于目录来说，执行权限允许用户进入该目录。对每个文件可以指定三种存取控制权限：文件所有者对文件所拥有的存取权限，文件所有者所在组对文件所拥有的存取权限，其他任意用户对文件所拥有的存取权限。根用户（root)具有对一切目录和文件的控制权限并可以指定对任何一个文件和目录的存取权限，一般用户只能对自己建立的文件和目录制定存取权限。默认情况下，系统将创建的普通文件的权限设置为-rw-r-r--，即文件所有者对该文件可读可写（rw)，而同组用户和其他用户都只可读：同样，在默认配置中，将每—个用户所有者目录的权限都设置为drwx------， 即只有文件所有者对该目录可读、写和可查询，也意味着用户不能读其他用户目录中的内容。

chmod (change mode的简写）命令用于改变文件或目录的访问权限。只有文件所有者或超级用户root才有权用chmod改变文件或目录的访问权限。

**【问题3】**

Linux系统中Samba的主要配置文件是/etc/samba/smb.conf。请根据以下的smb.conf 配置文件，在空（11)〜（15)中填写恰当的内容。

Linux服务器启动Samba服务后，在客户机的“网络邻居”中显示提供共享服务的Linux主机名为（11)，其共享的服务有（12),能够访问Samba共享服务的客户的地址范围（13)；能够通过Samba服务读写/home/samba中内容的用户是（14)： 该Samba服务器的安全级别是（15)





11）smb-server

12）printers或My Printer

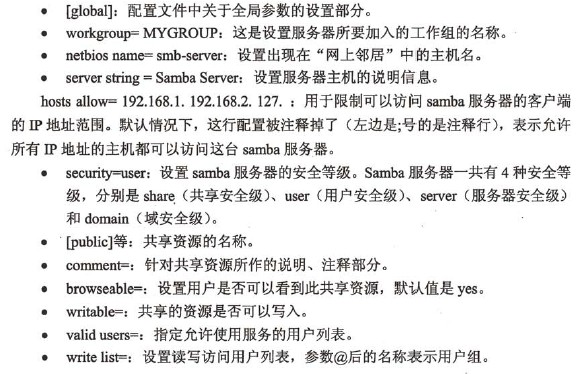
13）无限制（因为hosts allow被分号注释掉了）

14）Linux系统的test组中用户（仅回答test用户不给分）

15）用户安全级

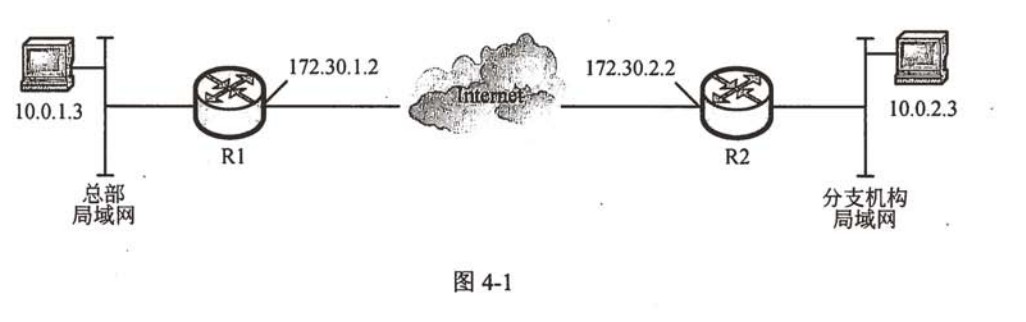
Samba是一个基于SMB (Server Message Block)协议的功能强大的软件工具，可以实现基于Linux操作系统的文件/目录及打印机共享服务。SMB是一种客户端/服务器协议，SMB客户端使用TCP/IP、NetBEUI或IPX/SPX与服务器连接。当工作在TCP/IP网络上时，通过NetBIOS nameserver使网络中Linux系统用户的机器可以在Windows系统 的网络邻居上被看到。

Samba安装完成后，通过配置/etc/samba/smb.conf文件，才能使其有效工作，该配置文件的部分重要参数说明如下。



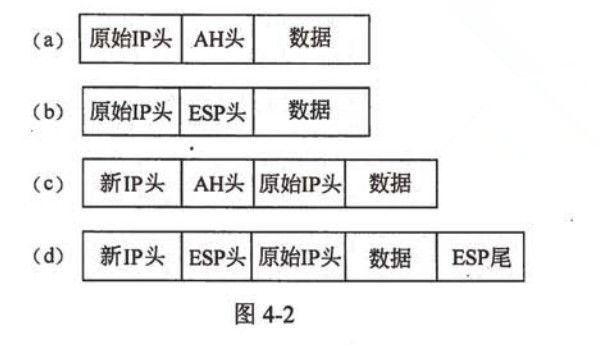
**试题四**

某公司总部和分支机构的网络配置如图4-1所示。在路由器R1和R2上配置IPSec 安全策略，实现分支机构和总部的安全通信。



**【问题1】**

图4-2中（a)、（b)、（c)、(d)为不同类型IPSec数据包的示意图，其中(1)和(2) 工作在隧道模式；(3)和(4)支持报文加密。



（1）(2) c、d (顺序可交换）

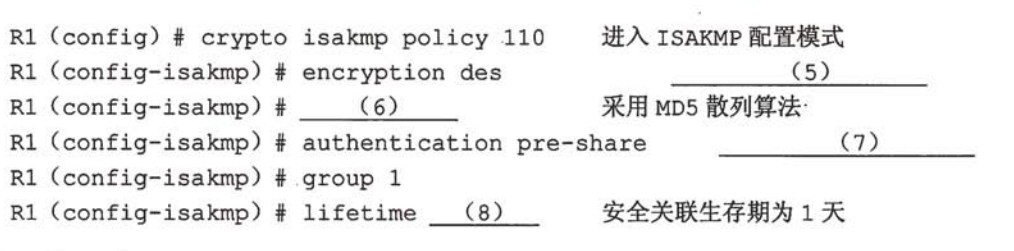
（3）（4) b、d (顺序可交换）

考查IPSec的基本概念，IPSec支持认证头（AH)协议和封装安全有效载荷（ESP)协议，其中认证头协议仅支持认证，不支持加密；封装安全有效载荷协议既支持认证又支持加密。IPSec有两种工作模式，分别是传输模式和隧道模式，工作在传输模式时，AH或ESP被插入到IP头和有效载荷之间：工作在隧道模式时，在AH或ESP前面会生成一个新的IP头。从图4-2中可以看出，（a)、（c)支持的是AH协议，（b)、 (d)支持的是ESP协议，（a)、(b)工作在传输模式，（c)、(d)工作在隧道模式。所以

(1)、（2)答案为c和d; (3)、（4)答案为b和d。

**【问题2】**

下面的命令在路由器R1中建立IKE策略，请补充完成命令或说明命令的含义。



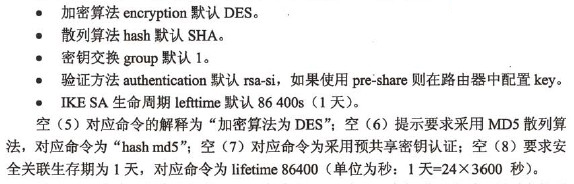
1. 加密算法为DES

2. hash md5

3. 认证采用预共享密钥

4. 86400

考查IKE策略的建立步骤和命令。配置IKE的策略配置主要包含以下方面：



**【问题3】**

R2与R1之间采用预共享密钥“12345678”建立IPSec安全关联，请完成下面配置命令。

R1 (config) # crypt isakmp key 12345678 address (9)

R2 (config) # crypt isakmp key 12345678 address (10)

(9) 172.30.2.2

(10) 172.30.1.2

考查预共享密钥的设置，在路由器R1与R2之间需要分别配置对方的预共享密钥，路由器R1与R2的对方分别是R2和R1,所以（9)、(10)分别是R2和R1的IP地址172.30.2.2 和172.30.1.2。

**【问题4】**

完成以下ACL配置，实现总部主机10.0.1.3和分支机构主机10.0.2.3的通信。

R1 (config) # access-list 110 permit ip host (11) host (12)

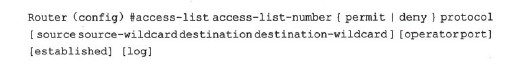
R2 (config) # access-list 110 permit ip host (13) host 10.0.1.3

（11） 10.0.1.3

（12） 10.0.2.3

（13） 10.0.2.3

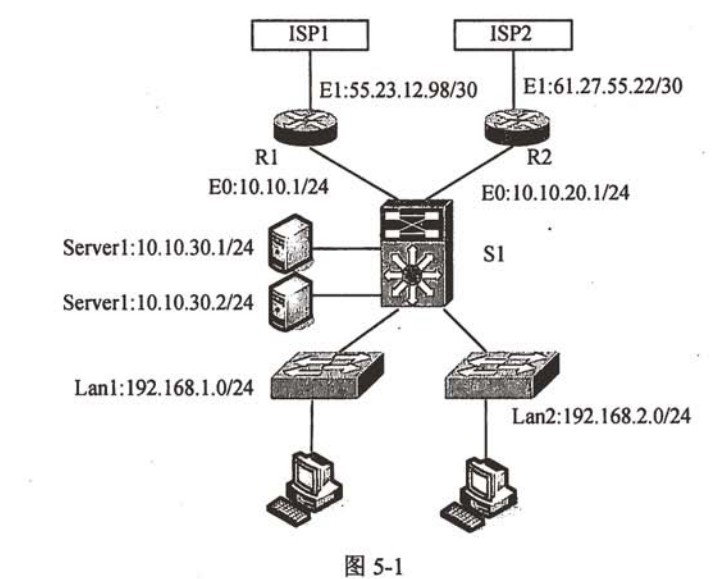
考查ACL配置，为了实现10.0.1.3和10.0.2.3的通信，需要分别在路由器R1和R2上作相应的AC1配置，R1的配置为允许10.0.1.3到10.0.2.3的IP包，R2的配置为允许10.0.2.3到10.0:1.3的IP包。根据扩展ACL配置命令语法：



空（11)为源主机IP地址10.0.1.3，空（12)为目标主机IP地址10.0.2.3,空（13) 为源主机IP地址10.0.2.3。

**试题五**

某单位采用双出口网络，其网络拓扑结构如图5-1所示。



该单位根据实际需要，配置网络出口实现如下功能：

1. 单位网内用户访问IP地址158.124.0.0/15和158.153.208.0/20时，出口经ISP2;

2. 单位网内用户访问其他IP地址时，出口经ISP1;

3. 服务器通过ISP2线路为外部提供服务。

**【问题1】**

在该单位的三层交换机S1上，根据上述要求完成静态路由配置。



(1) 0.0.0.0 0.0.0.0 10.10.10.1

(2) 255.254.0.0

(3) 10.10.20.1

(4) 255.255.240.0

(5) 10.10.20.1

考查的是路由器静态路由的设置方法。根据题目要求，该网络内用户访问IP地址158.124.0.0/15 和158.153.208.0/20 时，出口经ISP2,由图 5-1 可知，其端口地址为10.10.20.1/24，网内用户访问其他IP地址时，出口经ISP1,由图5-1可知，其端口地址为10.10.10.1/24。所以，在该单位的三层交换机S1上，静态路由配置如下：

ip route 0.0.0.0 0.0.0.0 10.10.10.1

ip route 158.124.0.0 255.254.0.0 10.10.20.1

ip route 158.153.208.0 255.255.240.0 10.10.20.1

**【问题2】**

1. 根据上述要求，在三层交换机S1上配置了两组ACL,请根据题目要求完成以下配置。

access -list 10 permit ip host 10.10.30.1 any

access -list 10 permit ip host (6) any

access -list 12 permit ip any 158.124.0.0 (7)

access -list 12 permit ip any 158.153.208.0 (8)

access -list 12 deny ip any any

2.完成以下策略路由的配置。

route-map test permit 10

（9） ip address 10

（10） ip next-hop (11)

(6)10.30.2

(7) 0.1.255.255

(8) 0.0.15.255

(9) match

(10) set

(11) 10.10.20.1

考査的是ACL设置及策略路由配置问题。根据题目要求可知，服务器通过ISP2线路为外部提供服务，另外单位网内用户访问IP地址158.124.0.0/15和158.153. 208.0/20 时，出口经ISP2。

access -list 10结合策略路由，保证服务器通过ISP2线路为外部提供服务，所以access -list 10内容如下：

access -list 10 permit ip host 10.10.30.1 any

access -list 10 permit ip host 10.10.30.2 any

对应的策略路由为：

route-map test permit 10

match ip address 10

access -list 12 配置网内用户访问 IP 地址 158.124.0.0/15 和 158.153.208.0/20 时，出口经ISP2,所以配置如下：

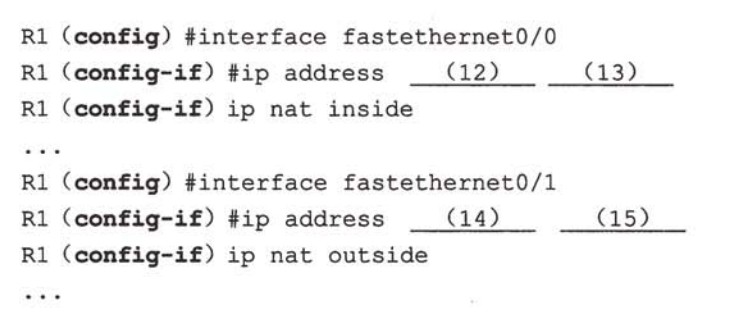
access -list 12 permit ip any 158.124.0.0 0.1.255.255

access -list 12 permit ip any 158•153•208•0 0.0.15.255

access -list 12 deny ip any any

**【问题3】**

以下是路由器R1的部分配置。请完成配置命令。



（12）10.10.10.1

（13） 255.255.255.0

（14）55.23.12.98

（15）255.255.255.252

考查的是路由器的配置问题。由图5-1可知，路由器R1的内网IP为10. 10.10.1/24，外网IP地址为55.23.12.98/30，所以其地址配置如下：

