以下关于CPU的叙述中，错误的是(1) 。

(1)A.CPU产生每条指令的操作信号并将操作信号送往相应的部件进行控制

B.程序计数器PC除了存放指令地址，也可以临时存储算术/逻辑运算结果

C.CPU中的控制器决定计算机运行过程的自动化

D.指令译码器是CPU控制器中的部件

**【答案】B**

**【解析】本题考查计算机硬件组成基础知识。**

CPU是计算机的控制中心，主要由运算器、控制器、寄存器组和内部总线等部件组成。控制器由程序计数器、指令寄存器、指令译码器、时序产生器和操作控制器组成，它是发布命令的“决策机构”，即完成协调和指挥整个计算机系统的操作。它的主要功能：从内存中取出一条指令，并指出下一条指令在内存中的位置；对指令进行译码或测试，并产生相应的操作控制信号，以便启动规定的动作；指挥并控制CPU、内存和输入输出设备之间数据的流动。

程序计数器(PC)是专用寄存器，具有寄存信息和计数两种功能，又称为指令计数器，在程序开始执行前，将程序的起始地址送入PC，该地址在程序加载到内存时确定，因此PC的初始内容即是程序第一条指令的地址。执行指令时，CPU将自动修改PC的内容，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执行的，因此修改的过程通常只是简单地对PC加1。当遇到转移指令时，后继指令的地址根据当前指令的地址加上一个向前或向后转移的位移量得到，或者根据转移指令给出的直接转移的地址得到。

以下关于 CISC (Complex Instruction Set Computer.复杂指令集计算机）和RISC (Reduced Instruction Set Computer,精简指令集计算机）的叙述中，错误的是(2)。

(2)A.在CISC中，其复杂指令都采用硬布线逻辑来执行

B.采用CISC技术的CPU，其芯片设计复杂度更高

C.在RISC中，更适合采用硬布线逻辑执行指令

D.采用RISC技术，指令系统中的指令种类和寻址方式更少

**【答案】A**

**【解析】本题考查指令系统和计算机体系结构基础知识。**

CISC (Complex Instruction Set Computer,复杂指令集计算机）的基本思想是：进一步增强原有指令的功能，用更为复杂的新指令取代原先由软件子程序完成的功能，实现软件功能的硬件化，导致机器的指令系统越来越庞大而复杂。CISC计算机一般所含的令数目至少300条以上，有的甚至超过500条。

RISC (Reduced Instruction Set Computer,精简指令集计算机）的基本思想是：通过减少指令总数和简化指令功能，降低硬件设计的复杂度，使指令能单周期执行，并通过优化编译提高指令的执行速度，采用硬布线控制逻辑优化编译程序。在20世纪70年代末开始兴起，导致机器的指令系统进一步精炼而简单。

以下关于校验码的叙述中，正确的是(3)。

(3)A.海明码利用多组数位的奇偶性来检错和纠错

B.海明码的码距必须大于等于1

C.循环冗余校验码具有很强的检错和纠错能力

D.循环冗余校验码的码距必定为1

**【答案】A**

**【解析】本题考查校验码的基础知识。**

一个编码系统中任意两个合法编码（码字）之间不同的二进数位数称为这两个码字的码距，而整个编码系统中任意两个码字的最小距离就是该编码系统的码距。为了使一个系统能检查和纠正一个差错，码间最小距离必须至少是3。

海明码是一种可以纠正一位差错的编码，是利用奇偶性来检错和纠错的校验方法。海明码的基本意思是给传输的数据增加r个校验位，从而增加两个合法消息（合法码字) 的不同位的个数（海明距离）。假设要传输的信息有m位，则经海明编码的码字就有n=m+r位。

循环冗余校验码（CRC)编码方法是在k位信息码后再拼接r位的校验码，形成长度为n位的编码，其特点是检错能力极强且开销小，易于用编码器及检测电路实现。

在数据通信与网络中，通常k相当大，由一千甚至数千数据位构成一帧，而后采用CRC码产生r位的校验位。它只能检测出错误，而不能纠正错误。一般取r=16,标准的16位生成多项式有 CRC-16=x16+x15+ x2+1 和CRC-CCITT=x16+ x12+ x5+1。一般情况下，r位生成多项式产生的CRC码可检测出所有的双错、奇数位错和突发长度小于等于r的突发错。用于纠错目的的循环码的译码算法比较复杂。

以下关于Cache的叙述中，正确的是(4)。

(4)A.在容量确定的情况下，替换算法的时间复杂度是影响Cache命中率的关键因素

B.Cache的设计思想是在合理成本下提高命中率

C.Cache的设计目标是容量尽可能与主存容量相等

D.CPU中的Cache容量应大于CPU之外的Cache容量

**【答案】B**

**【解析】本题考查高速缓存基础知识。**

Cache是一个高速小容量的临时存储器，可以用高速的静态存储器(SRAM)芯片实现，可以集成到CPU芯片内部，或者设置在CPU与内存之间，用于存储CPU最经常访问的指令或者操作数据。Cache的出现是基于两种因素：首先是由于CPU的速度和性能提高很快而主存速度较低且价格高，其次是程序执行的局部性特点。因此，才将速度比较快而容量有限的SRAM构成Cache，目的在于尽可能发挥CPU的高速度。很显然，要尽可能发挥CPU的高速度，就必须用硬件实现其全部功能。

面向对象开发方法的基本思想是尽可能按照人类认识客观世界的方法来分析和解决问题，(5)方法不属于面向对象方法。

(5)A.Booch B.Coad C.OMT D.Jackson

**【答案】D**

**【解析】本题考查面向对象开发方法。**

面向对象开发方法有Booch方法、Coad方法和OMT方法。Jackson方法是一种面向数据结构的开发方法。

确定构建软件系统所需要的人数时，无需考虑(6)。

(6)A.系统的市场前景 B.系统的规模 C.系统的技术复杂性 D.项目计划

**【答案】A**

**【解析】本题考查项目管理内容。**

在对软件开发资源进行规划时，为了确定构建软件系统所需的人数，需要考虑软件系统的规模、系统的技术复杂性、项目计划和开发人员的技术背景等方面，而与系统是否有市场前景无关。

一个项目为了修正一个错误而进行了变更。但这个错误被修正后，却引起以前可以正确运行的代码出错。(7)最可能发现这一问题。

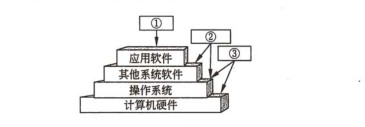
(7)A.单元测试 B.接受测试 C.回归测试 D.安装测试

**【答案】C**

**【解析】本题考查软件测试知识。**

回归测试是在软件发生变更之后进行的测试，以发现在变更时可能引起的其他错误。

操作系统是裸机上的第一层软件，其他系统软件(如(8)等)和应用软件都是建立在操作系统基础上的。下图①②③分别表示（9）。



(8)A.编译程序、财务软件和数据库管理系统软件

B.汇编程序、编译程序和Java解释器

C.编译程序、数据库管理系统软件和汽车防盗程序

D.语言处理程序、办公管理软件和气象预报软件

(9)A.应用软件开发者、最终用户和系统软件开发者

B.应用软件开发者、系统软件开发者和最终用户

C.最终用户、系统软件开发者和应用软件开发者

D.最终用户、应用软件开发者和系统软件开发者

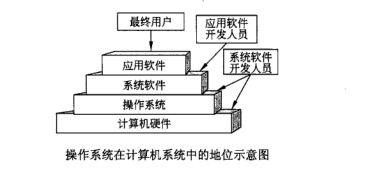
**【答案】B D**

**【解析】**

本题考查操作系统基本概念。

财务软件、汽车防盜程序、办公管理软件和气象预报软件都属于应用软件，而选项A、C和D中含有这些软件。选项B中汇编程序、编译程序和数据库管理系统软件都属于系统软件。

计算机系统由硬件和软件两部分组成。通常把未配置软件的计算机称为裸机，直接使用裸机不仅不方便，而且将严重降低工作效率和机器的利用率。操作系统（Operating System)的目的是为了填补人与机器之间的鸿沟，即建立用户与计算机之间的接口而为裸机配置的一种系统软件。由下图可以看出，操作系统是裸机上的窠一层软件，是对硬 件系统功能的首次扩充。它在计算机系统中占据重要而特殊的地位，所有其他软件，如编辑程序、汇编程序、编译程序和数据库管理系统等系统软件，以及大量的应用软件都 是建立在操作系统基础上的，并得到它的支持和取得它的服务。从用户角度看，当计算机配置了操作系统后，用户不再直接使用计算机系统硬件，而是利用操作系统所提供的 命令和服务去操纵计算机，操作系统已成为现代计算机系统中必不可少的最重要系统软件，因此把操作系统看作是用户与计算机之间的接口。因此，操作系统紧贴系统硬件之上，所有其他软件之下（是其他软件的共同环境)。



软件权利人与被许可方签订一份软件使用许可合同。若在该合同约定的时间和地域范围内，软件权利人不得再许可任何第三人以此相同的方法使用该项软件，但软件权利人可以自己使用，则该项许可使用是(10)。

(10)A.独家许可使用 B.独占许可使用 C.普通许可使用 D.部分许可使用

**【答案】A**

**【解析】**

软件许可一般有独占许可使用、独家许可使用和普通许可使用三种形式。独占许可使用，许可的是专有使用权，实施独占许可使用后，软件著作权人不得将软件使用权授予第三方，软件著作权人自己不能使用该软件；独家许可使用，许可的是专有使用权，实施独家许可使用后，软件著作权人不得将软件使用权授予第三方，软件著作权人自己可以使用该软件；普通许可使用，许可的是非专有使用权，实施普通许可使用后，软件著作权人可以将软件使用权授予第三方，软件著作权人自己可以使用该软件。

E1载波的基本帧由32个子信道组成，其中30个子信道用于传送话音数据，2个子信道(11)用于传送控制信令，该基本帧的传送时间为(12)。

(11)A.CH0和CH2 B.CH1和CH15 C.CH15和CH16 D.CH0和CH16

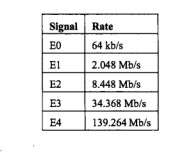
(12)A.100ms B.200μs C.125μs D.150μs

**【答案】D C**

**【解析】**

El载波的基本巾贞划分为32个子信道（E0)，每个子信道含8位数据，子信道CH0 (或TS0)用于组帧，使得接收方可以检测帧的开起点。另一个子信道CH16(或TS16) 用于承载控制呼叫的信令(例如CAS信令)。其余30个子信道用于承载PCM编码的话音数据。E1帧每秒发送8000次，发送时间为125啤，其数据速率为8×32×8000= 2.048Mb/s。

基于E0的准同步数字系列PDH (Plesiocnronous Digital Hierarchy)以4个低级信道组成更高一级的信道，如下图所示。实际使用的是E1和E3信道。



4B/5B编码是一种两级编码方案，首先要把数据变成(13)编码,再把4位分为一组的代码变换成5单位的代码。这种编码的效率是(14) 。

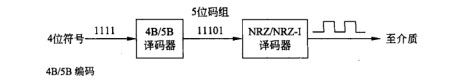
(13)A.NRZ-I B.AMI C.QAM D.PCM

(14)A.0.4 B.0.5 C.0.8 D.1.0

**【答案】A C**

**【解析】**

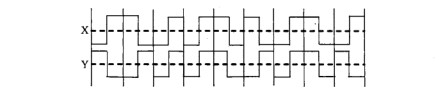
采用4B/5B编码能够提高编码的效率，降低电路成本。这种编码方法的原理如下图所示。



这实际上是一种两级编码方案。系统中使用不归零码（NRZ)，在发送到传输介质时要变成见1就翻不归零码（NRZ-I)。NRZ-I代码序列中1的个数越多，越能提供同步信息，如果遇到长串的“0”，则不能提供同步信息，所以在发送到介质上之前还需经过一次4B/5B编码。发送器扫描要发送的位序列，4位分为一组，然后按照对应规则变换成5位二进制代码。

5位二进制代码的状态共有32种，其中1的个数都不少于2个，这样就保证了传输的代码能提供足够多的同步信息。另外，还有5B/6B、8B/10B等编码方法，其原理是类似的。

下图表示了某个数据的两种编码，这两种编码分别是（15），该数据是（16）。



(15)A.X为差分曼彻斯特码，Y为曼彻斯特码

B.X为差分曼彻斯特码，Y为双极性码 .

C.X为曼彻斯特码，Y为差分曼彻斯特码

D.X为曼彻斯特码，Y为不归零码

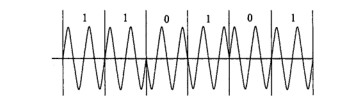
(16)A.010011110 B.010011010 C.011011010 D.010010010

**【答案】C B**

**【解析】**

首先可以断定图中所示是两种双相码，然后按照曼彻斯特编码的特点（以正负或负正脉冲来区别“1”和“0”）和差分曼彻斯特编码的特点（以位前沿是否有电平跳变来区别“1”和“0”）可以断定，X为曼彻斯特编码，Y为差分曼彻斯特编码，表示的数据是010011010。

下图所示的调制方式是(17),若载波频率为2400Hz，则码元速率为(18)。



(17)A.FSK B.2DPSK C.ASK D.QAM

(18)A.100 Baud B.200 Baud C.1200 Baud D.2400 Baud

**【答案】B C**

**【解析】**

根据波形可以看出，这是一种差分编码，所以应选2DPSK。另外，每一位包含两个周期，如果载波频率为2400Hz，则码元速率就是1200波特。

在相隔2000km的两地间通过电缆以4800b/s的速率传送3000比特长的数据包，从开始发送到接收完数据需要的时间是(19),如果用50Kb/s的卫星信道传送，则需要的时间是(20)。

(19)A.480ms B.645ms C.630ms D.635ms

(20)A.70ms B.330ms C.500ms D.600ms

**【答案】D B**

**【解析】**

一个数据包从开始发送到接收完成的时间包含发送时间tf和传播延迟时间tp两部分，可以计算如下：

对电缆信道：tp=2000km/(200km/ms)= 10ms, tf=3000b/4800b/s=625ms, tp+tf=635ms.

对卫星信道：tp=270ins, tf=3000b/50kb/s=60ms, tp+tf=270ms+60ms:=330ms.

对于选择重发ARQ协议，如果帧编号字段为k位，则窗口大小为(21)。

(21)A.W≤2k-1 B.W≤2k-1 C.W=2k D.W<2k-1

**【答案】B**

**【解析】**

如果顿编号字段为k位，对于选择重发ARQ协议，发送窗口大小为W≤2k-1 ;对于后退N帧ARQ协议，则窗口大小为W≤2k-1。

RIPv2对RIPv1协议有三方面的改进。下面的选项中，RIPv2的特点不包括(22)。

在RIPv2中，可以采用水平分割法来消除路由循环，这种方法是指(23)。

(22)A.使用组播而不是广播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.使用经过散列的口令来限制路由信息的传播

D.支持动态网络地址变换来使用私网地址

(23)A.不能向自己的邻居发送路由信息

B.不要把一条路由信息发送给该信息的来源

C.路由信息只能发送给左右两边的路由器

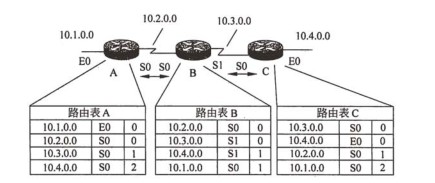
D.路由信息必须用组播而不是广播方式发送

**【答案】D B**

**【解析】**

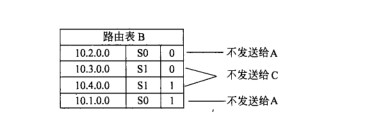
RIPv2是增强了的RIP协议，定义在RFC 1721和RFC 1722 (1994)中。RIPv2基本上还是一个距离矢量路由协议，但是有三方面的改进。首先，使用组播而不是广播来传播路由更新报文，并且采用了触发更新（triggered update)机制加速路由收敛，即出现路由变化时立即向邻居发送路由更新报文，而不必等待更新周期是否到达。其次，RIPv2是一个无类别的协议（classless protocol)，可以使用可变长子网掩码CVLSM),也支持无类别域间路由（CIDR)，这些功能使得网络的设计更具伸缩性。第三个增强是RIPv2支持认证，使用经过散列的口令字来限制路由更新信息的传播。其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。

距离矢量算法要求相邻路由器之间周期性地交换路由表，并通过逐步交换把路由信息扩散到网络中所有的路由器。这种逐步交换过程如果不加以限制，将会形成路由环路 (Routing Loops),使得各个路由器无法就网络的可到达性取得一致。



例如在上图中，路由器A、B、C的路由表已经收敛，每个路由表的后两项是通过交换路由信息学习到的。如果在某一时刻，网络10.4.0.0发生故障，C检测到故障，并通过接口 S0把故障通知B。然而，如果B在收到C的故障通知前将其路由表发送到C，C则会认为通过B可以访问10.4.0.0，并据此将路由表中第二条记录修改为（10.4.0.0, S0, 2)。这样一来，路由器A、B、C都认为通过其他的路由器存在一条通往10.4.0.0的路径，结果导致目标地址为10.4.0.0的数据包在三个路由器之间来回传通，从而形成路由环路。

解决路由环路问题可以采用水平分割法（SplitHorizon)。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源。可以对上图中B的路由表项加上一些注释，如下图所示，可以看出，每条路由信息都不会通过其来源接口向回发送，这样就可以避免环路的产生。



简单的水平分割方案是：“不能把从邻居学习到的路由发送给那个邻居”，带有反向毒化的水平分割方案(Split Horizon with Poisoned Reverse)是：“把从邻居学习到的路由 费用设置为无限大，并立即发送给那个邻居”。采用反向毒化的方案更安全一些，它可以立即中断环路。相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成过程。

另外，前面提到的触发更新技术也能加快路由收敛，如果触发更新足够及时——路由器C在接收B的更新报文之前把网络10.4.0.0的故障告诉B，则可以防止环路的形成。

为了限制路由信息传播的范围，OSPF协议把网络划分成4种区域(Area)，其中(24) 的作用是连接各个区域的传输网络，(25)不接受本地自治系统以外的路由信息。

(24)A.不完全存根区域 B.标准区域 C.主干区域 D.存根区域

(25)A.不完全存根区域 B.标准区域 C.主干区域 D.存根区域

**【答案】C D**

**【解析】**

每个OSPF区域被指定了一个32位的区域标识符，可以用点分十进制表示，例如主干区域的标识符可表示为0.0.0.0。OSPF的区域分为以下5种，不同类型的区域对由自治系统外部传入的路由信息的处理方式不同。

•标准区域：标准区域可以接收任何链路更新信息和路由汇总信息。

•主干区域：主干区域是连接各个区域的传输网络，其他区域都通过主干区域交换路由信息。主干区域拥有标准区域的所有性质。

•存根区域：不接受本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由0.0.0.0。

•完全存根区域：不接受自治系统以外的路由信息，也不接受自治系统内其他区域的路由汇总信息，发送到本地区域外的报文使用默认路由0.0.0.0。完全存根区域是Cisco定义的，是非标准的。

•不完全存根区域（NSSA):类似于存根区域，但是允许接收以类型7的链路状态公告发送的外部路由信息。

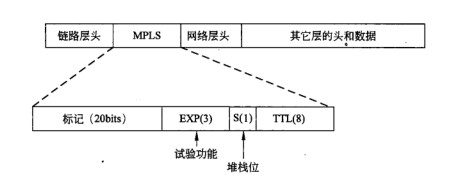
MPLS根据标记对分组进行交换，其标记中包含(26)。

(26)A.MAC地址 B.IP地址 C.VLAN编号 D.分组长度

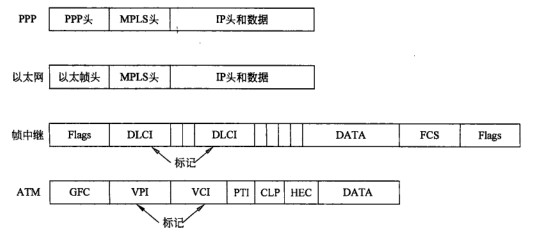
**【答案】B**

**【解析】**

第三层交换是指利用第二层交换的高带宽和低延迟优势尽快地传送网络层分组的技术。交换与路由不同，前者用硬件实现，速度快，而后者由软件实现，速度慢。三层交换机的工作原理可以概括为：一次路由，多次交换。就是说，当三层交换机第一次收到一个数据包时必须通过路由功能寻找转发端口，同时记住MAC层的目标地址和源地址，以及其他有关信息，当再次收到目标地址和源地址相同的帧时就可以直接进行交换，不再调用路由功能。所以三层交换机不但具有路由功能，而且比通常的路由器转发得更快。

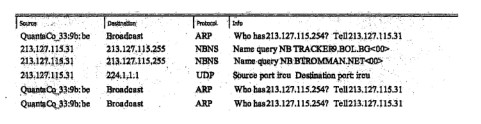


IETF 开发的多协议标记交换 MPLS (Multiprotocol Label Switching, RFC3031)把第二层的链路状态信息（带宽、延迟和利用率等）集成到第三层的协议数据单元中，从而简化和改进了第三层分组的交换过程。理论上，MPLS支持任何第二层和第三层协议。MPLS包头的位置界于第二层和第三层之间，可称为第2.5层，标准格式如上图所示。MPLS承载的报文通常是IP包，当然也可以是以太帧、AAL5包、甚至ATM信元等。可以承载MPLS的第二层协议可以是PPP、以太帧、ATM和帧中继等，参见下图。



当分组进入MPLS网络时，标记边缘路由器（Label Edge Router，LER)就为其加上一个标记，这种标记不仅包含了路由表项中的信息（目标地址、带宽和延迟等)，而且还引用了IP头中的源地址字段、传输层端口号和服务质量等。这种分类一旦建立，分组就被指定到对应的标记交换通路（Label Switch Path，LSP)中，标记交换路由器（Label Switch Router, LSR)将根据标记来处置分组，不再经过第三层转发，从而加快了网络的传输速度。

某PC不能接入Internet，此时采用抓包工具捕获的以太网接口发出的信息如下：



则该PC的IP地址为(27)，默认网关的IP地址为(28) 。该PC不能接入Internet的原因可能是(29)。

(27)A.213.127.115.31 B.213.127.115.255

C.213.127.115.254 D.224.1.1.1

(28)A.213.127.115.31 B.213.127.115.255

C.213.127.115.254 D.224.1.1.1

(29)A.DNS解析错误 B.TCP/IP协议安装错误

C.不能正常连接到网关 D.DHCP服务器工作不正常

**【答案】A C C**

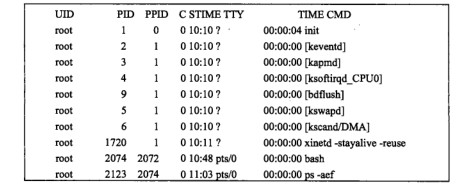
**【解析】**

采用抓包工具捕获的信息由源、目的、采用的协议以及数据报文中包含的信息组成。源字段中分别包含了该PC的MAC地址(QuantaCo\_33:9b:be)和IP地址(213.127.115.31)， 其发出的信息表明主机不停地广播ARP报文，寻找网关213.127.115.254。

由此，（27)、（28)选项中A为主机地址，B选项213.127.115.255为广播地址，C选项213.127.115.254为网关地址，D选项224.1.1.1为组播地址。故(27)题选A, (28) 题选C。

由主机不停地广播ARP报文寻找网关可以判断该PC不能接入Internet的原因是不能正常连接到网关，故（29)题选C。

在Linux系统中，采用（30)命令査看进程输出的信息,得到下图所示的结果。系统启动时最先运行的进程是(31),下列关于进程xinetd的说法中正确的是(32)。



(30)A.ps-all B.ps-aef C.ls-a D.ls-la

(31)A.0 B.null C.init D.bash

(32)A.xinetd是网络服务的守护进程 B.xinetd是定时任务的守护进程

C.xinetd进程负责配置网络接口 D.xinetd进程负责启动网卡

**【答案】B C A**

**【解析】**

Linux系统中用Is命令查看目录信息；用ps命令查看进程信息的命令。ps命令的几个主要参数和含义解释如下：

•-A：将关于所有进程（除了会话导带和与终端无关的进程）的信息写到标准输出。

•-D：将关于所有进程（除会话导带）的信息写到标准输出。

•-E：将除内核进程以外所有进程的信息写到标准输出。

•-F：生成二个完整列表。

在ps命令显示的进程信息中，PID是该进程的ID, Linux进程的ID—般是根据创建的先后顺序递增的。从图中可知，init进程的PID是1，它在系统启动时第一个动态创建。

xinetd是一个守护（daemon)进程，Linux把一些网络相关服务（如FTP、HTTP等）的监听端口全部由xinetd集中监听,当收到相应的客户端请求之后，xinetd进程就临时启动相应服务并把相应端口移交给相应服务，客户端断开之后，相应的服务进程结束，xinetd继续监听。

Linux操作系统中，网绐管理员可以通过修改（33)文件对Web服务器端口进行配置。

(33)A.inetd.conf B.lilo.conf C.httpd.conf D.resolv.confvv

**【答案】C**

**【解析】本题考查Linux中Web服务器端口配置相关知识。**

在Linux系统中，很多服务的配置数据都保存在相应的配置文件中（文件名一般为server-name.conf)。

inetxonf是/usr/sbin/inetd的初始化文件，告诉/usr/sbin/inetd所需要监听的inet服务及有关信息，主要的信息有服务名称、协议（tcp或udp)、标志（wait或nowait)、属主、真实服务程序全路径、真实服务程序名称及参数。lilo.conf是Linux中多引导程序lilo的配置文件：resolv.conf是DNS域名解析服务的配置文件。

httpd.conf是Linux中Apache Web服务的配置文件，其中的Listen选项用于配置服务的IP地址和端口号。例如,Listen192.168.1.1:8080指定Web服务的IP地址为192.168. 1.1，端口号为8080。

在Linux操作系统中，存放用户账号加密口令的文件是(34)。

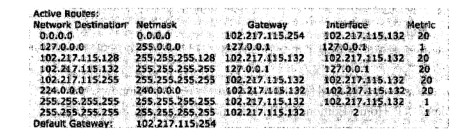
(34)A./etc/sam B./etc/shadow C./etc/group D./etc/security

**【答案】B**

**【解析】本题考查Linux用户账号密码的相关知识。**

在Linux操作系统中,存放用户账号和密码的文件有两个:/etc/passwd和/etc/shadow。/etc/shadow文件是/etc/passwd的影子文件，和/etc/passwd应该是对应互补的。shadow内容包括用户及被加密的密码以及其他/etc/passwd不能包括的信息，比如用户的有效期限等。

在Windows中运行(35)命令后得到如下图所示的结果。如果要将目标地址为102.217.112.0/24的分组经102.217.115.1发出，需增加一条路由，正确的命令为(36)



(35)ipconfig /renew B.ping C.nslookup D.route print

(36)A.route add 102.217.112.0 mask 255.255.255.0 102.217.115.1

B.route add 102.217.112.0 255.255.255.0 102.217.115.1

C.add route 102.217.112.0 255.255.255.0 102.217.115.1

D.add route 102.217.112.0 mask 255.255.255.0 102.217.115.1

**【答案】D A**

**【解析】**

Route在本地IP路由表中显示和修改条目。其语法为：

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/xt-09-s-x-35-2.jpg

其中，命令参数print用以显示主机路由信息，add用以添加路由，change用以更改现存路由，delete用以删除路由。

空（35)的选项中ipconfig/renew用于命令重新自动获取IP地址；ping命令通过向对方主机发送“网际消息控制协议（ICMP)”回响请求消息来验证与对方计算机的连接，是用于检测网络连接性、可到达性的TCP/IP命令；nslookup最简单的用法就是查询域名对应的IP地址，包括A记录和CNAME记录；route print用以显示主机路由信息。故正确答案为D。

Route命令参数add用以添加路由，例如要添加目标为10.41.0.0,子网掩码为255.255.0.0，下一个跃点地址为10.27.0.1，跃点数为7的路由,正确的命令为：

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/xt-09-s-x-35-3.jpg

故空(36)选择A。

下列关于Microsoft管理控制台（MMC)的说法中，错误的是(37)。

(37)A.MMC集成了用来管理网络、计算机、服务及其他系统组件的管理工具

B.MMC创建、保存并打开管理工具单元

C.MMC可以运行在Windows XP和Windows 2000操作系统上

D.MMC是用来管理硬件、软件和Windows系统的网络组件

**【答案】D**

**【解析】**

Microsoft管理控制台集成了用来管理网络、计算机、服务及其他系统组件的管理工具。可以使用MMC创建、保存并打开管理工具单元，这些管理工具用来管理硬件、软件和Windows系统的网络组件。MMC可以运行在各种Windows 9x/NT操作系统上， 以及Windows XP Home Edition/XP Professional 和 Windows Server 2003 家族的操作系统上。

MMC不执行管理功能，但集成管理工具。可以添加到控制台的主要工具类型称为管理单元，其他可添加的项目包括ActiveX控件、网页的链接、文件夹、任务板视图和任务。

但是，MMC不是管理硬件、软件和Windows系统的网络组件，故(37)题选择D。

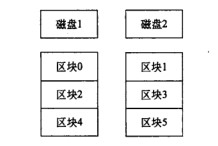
RAID技术中，磁盘容量利用率最高的是(38)。

(38)A.RAID 0 B.RAID 1 C.RAID 3 D.RAID 5

**【答案】A**

**【解析】**

RAID 0需要两个以上硬盘驱动器，每个磁盘划分为不同的区块，如下图所示。



数据按区块Al、A2、A3、A4、…的顺序存储，数据访问采用交叉存取、并行传输的方式。将数据分布在不同驱动器上可以提高传输速度，平衡驱动器的负载。这种系统没有镜像盘，也没有差错控制措施，磁盘容量利用率在RAID技术中最高。

xDSL技术中，能提供上下行信道非对称传输的是(39)。

(39)A.ADSL 和 HDSL B.ADSL 和 VDSL C.SDSL 和 VDSL D.SDSL 和 HDSL

**【答案】B**

**【解析】**

数字用户线路（Digital Subscriber Line，DSL)允许用户在传统电话线上提供高速的数据传输，用户计算机借助于DSL调制解调器连接到电话线上，通过DSL连接访问互联网络或者企业网络。

DSL技术存在多种类型，以下是常见的技术类型：

ADSL：非对称DSL，用户的上下行流量不对称，一般具有三个信道，分别为1.544〜9Mb/s的高速下行信道，16〜640Kb/s的双工信道，64Kb/s的语音信道。

SDSL：对称DSL，用户的上下行流量对等，最高可以达到1.544Mb/s。

HDSL：高比特率DSL，是在两个线对上提供1.544Mb/s或在三个线对上提供2.048Mb/s对称通信的技术，其最大特点是可以运行在低质量线路上，最大距离为3700〜4600m。

VDSL：甚高比特率DSL，一种快速非对称DSL业务，可以在一对电话线上提供数据和语音业务。

若FTP服务器开启了匿名访问功能，匿名登录时需要输入的用户名是(40)。

(40)A.root B.user C.guest D.anonymous

**【答案】D**

**【解析】**

FTP服务器采用用户名anonymous进行匿名登录。

在Kerberos系统中，使用一次性密钥和(41)来防止重放攻击。

(41)A.时间戳 B.数字签名 C.序列号 D.数字证书

**【答案】A**

**【解析】本题考查Kerberos系统安全相关知识。**

一次性密钥、序列号和时间戳都是对付重放攻击的有效手段，Kerberos系统采用一次性密钥和时间戳来防止重放攻击。

在下面4种病毒中，(42)可以远程控制网络中的计算机。

(42)A.worm.Sasser.f B.Win32.CIH C.Trojan.qq3344 D.Macro.Melissa

**【答案】C**

**【解析】本题考查病毒相关知识。**

以上4种病毒中，worm是婦虫病毒，Win32.CIH是CIH病毒，Macro.Melissa是宏病毒，这三种病毒都属于单机病毒；而Trojan.qq3344是一种特洛伊木马，通过网络实现对计算机的远程攻击。

将ACL应用到路由器接口的命令是（43) 。

(43)A.Router(config-if)#ip access-group 10 out

B.Router(config-if)#apply access-list 10 out

C.Router(config-if)#fixup access-list 10 out

D.Router(config-if)#route access-group 10 out

**【答案】A**

**【解析】本题考查路由器配置命令，属于记忆题。**

某网站向CA申请了数字证书，用户通过(44)来验证网站的真伪。在用户与网站进行安全通信时，用户可以通过(45)进行加密和验证，该网站通过(46)进行解密和签名。

(44)A.CA的签名 B.证书中的公钥 C.网站的私钥 D.用户的公钥

(45)A.CA的签名 B.证书中的公钥 C.网站的私钥 D.用户的公钥 (46)A.CA的签名 B.证书中的公钥 C.网站的私钥 D.用户的公钥

**【答案】A B C**

**【解析】本题考查数字证书相关知识点。**

数字证书是由权威机构CA证书擇权（Certificate Authority)中心发行的，能提供在Internet上进行身份验证的一种权威性电子文档，人们可以在因特网交往中用它来证明自己的身份和识别对方的身份。

数字证书包含版本、序列号、签名算法标识符、签发人姓名、有效期、主体名和主体公钥信息等并附有CA的签名，用户获取网站的数字证书后通过验证CA的签名来确认数字证书的有效性，从而验证网站的真伪。

在用户与网站进行安全通信时，用户发送数据时使用网站的公钥（从数字证书中获得）加密，收到数据时使用网站的公钥验证网站的数字签名；网站利用自身的私钥对发送的消息签名和对收到的消息解密。

IPSec的加密和认证过程中所使用的密钥由(47)机制来生成和分发。

(47)A.ESP B.IKE C.TGS D.AH

**【答案】B**

**【解析】本题考查IPSec相关知识。**

IPSec密钥管理利用IKE (Internet密钥交换协议)机制实现，IKE解决了在不安全的网络环境(如Internet)中安全地建立或更新共享密钥的问题。

SSL协议使用的默认端口是(48)。

(48)A.80 B.445 C.8080 D.443

**【答案】D**

**【解析】本题属于记忆题。**

80端口是Web服务默认端口：8080端口一般用于局域网内部提供Web服务；445端口和139端口一样，用于局域网中共享文件夹或共享打印机。

某用户分配的网络地址为192.24.0.0〜192.24.7.0,这个地址块可以用(49)表示, 其中可以分配(50)个主机地址。

(49)A.192.24.0.0/20 B.192.24.0.0/21

C.192.24.0.0/16 D.192.24.0.0/24

(50)A.2032 B.2048 C.2000 D.2056

**【答案】B A**

**【解析】**

192.24.0.0 的二进制表示为：11000000 00011000 00000000 00000000

192.24.7.0 的二进制表示为：11000000 00011000 00000111 00000000

汇聚后的网络地址为11000000 00011000 00000000 00000000，即192.24.0.0/21。可以分配的主机地址为8×(28-2) =2032.

使用CIDR 技术把4个C 类网络220.117.12.0/24、220.117.13.0/24、220.117.14.0/24和220.117.15.0/24汇聚成一个超网，得到的地址是(51)。

(51)A.220.117.8.0/22 B.220.117.12.0/22

C.220.117.8.0/21 D.220.117.12.0/21

**【答案】B**

**【解析】**

CIDR技术是把小的网络汇聚成大的超网。这里4个网络地址的二进制表示如下：

220.117.12.0/24的二进制表示为11011100 01110101 00001100 00000000

220.117.13.0/24的二进制表示为11011100 01110101 00001101 00000000

220.117.14.0/24的二进制表示为11011100 01110101 00001110 00000000

220.117.15.0/24的二进制表示为11011100 01110101 00001111 00000000

可以看出，汇聚后的网络地址为11011100 0111010100001100 00000000,即220.117.12.0/22。

某公司网络的地址是200.16.192.0/18,划分成16个子网，下面的选项中，不属于这16个子网地址的是(52)。

(52)A.200.16.236.0/22 B.200.16.224.0/22

C.200.16.208.0/22 D.200.16.254.0/22

**【答案】D**

**【解析】**

地址200.16.192.0/18的二进制表示为11001000.00010000.11000000.00000000,将其划分为16个子网，则各个子网的地址为：

11001000.00010000.11000000.00000000——200.16.192.0/22

11001000.00010000.11000100.00000000——200.16.196.0/22

11001000.00010000.11001000.00000000——200.16.200.0/22

11001000.00010000.11001100.00000000——200.16.204.0/22

11001000.00010000.11010000.00000000——200.16.208.0/22

11001000.00010000.11010100.00000000——200.16.212.0/22

11001000.00010000.11011000.00000000——200.16.216.0/22

11001000.00010000.11011100.00000000——200.16.220.0/22

11001000.00010000.11100000.00000000——200.16.224.0/22

11001000.00010000.11100100.00000000——200.16.228.0/22

11001000.00010000.11101000.00000000——200.16.232.0/22

11001000.00010000.11101100.00000000——200.16.236.0/22

11001000.00010000.11110000.00000000——200.16.240.0/22

11001000.00010000.11110100.00000000——200.16.244.0/22

11001000.00010000.11111000.00000000——200.16.248.0/22

11001000.00010000.11111100.00000000——200.16.252.0/22

可以看出，以上16个网络地址的第三个字节都能被4整除，而答案D中的254不能被4整除。

IPv6 地址 12AB:0000:0000:CD30:0000:0000:0000:0000/60 可以表示成各种简写形式，下面的选项中，写法正确的是(53)。

(53)A.12AB:0:0:CD30::/60 B.12AB:0:0:CD3/60

C.12AB::CD30/60 D.12AB::CD3/60

**【答案】A**

**【解析】**

IPv6地址采用冒号分隔的十六进制数表示，例如下面是一个IPv6地址

8000:0000:0000:0000:0123:4567:89AB:CDEF

为了便于书写，规定了一些简化写法。首先，每个字段前面的0可以省去，例如0123 可以简写为123;其次，一个或多个全0字段0000可以用一对冒号代替。例如以上地址可简写为：

8000::123:4567:89AB:CDEF.

IPv6地址的格式前缀(Format Prefix, FP)用于表示地址类型或子网地址，用类似于IPv4 CIDR的方法可表示为“IPv6地址/前缀长度”的形式。例如，60位的地址前缀 12AB00000000CD3有下列几种合法的表示形式：

12AB:0000:0000:CD30:0000:0000:0000:0000/60 12AB::CD30:0:0:0:0/60 12AB:0:0:CD30: :/60

下面的表示形式是不合法的：

12AB:0:0:CD3/60 (在16位的字段中可以省掉前面的0，不能省掉后面的0)

12AB: :CD30/60 (可展开为 12AB: 0000 : 0000 : 0000 : 0000 : 0000 : 0000 :CD30)

12AB: :CD3/60 (可展开为 12AB: 0000 : 0000 : 0000 : 0000 : 0000 : 0000 : 0CD3)

一般来说，结点地址与其子网前缀组合起来可采用紧缩形式表示，例如结点地址

12AB:0:0:CD30:123:4567:89AB:CDEF

若其子网号为12AB:0:0:CD30::/60，则等价的写法是

12AB:0:0:CD30:123:4567:89AB:CDEF/60

IPv6协议数据单元由一个固定头部和若干个扩展头部以及上层协议提供的负载组成，其中用于表示松散源路由功能的扩展头是(54)。如果有多个扩展头部，第一个扩展头部为(55)。

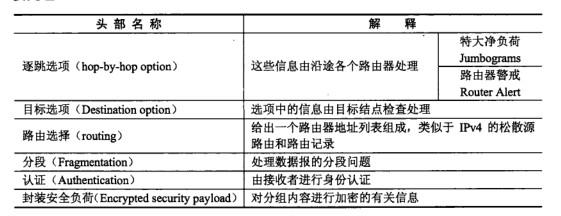
(54)A.目标头部 B.路由选择头部 C.分段头部 D.安全封装负荷头部

(55)A.逐跳头部 B.路由选择头部 C.分段头部 D.认证头部

**【答案】B A**

**【解析】**

IPv6有6种扩展头部，如下表所示，这6种扩展头部都是任选的。扩展头部的作用是保留IPv4某些字段的功能，但只是由特定的网络设备来检查处理，而不是每个设备都要处理。



如果一个IPv6分组包含多个扩展头，建议采用下面的封装顺序：

(1)IPv6 头部。

(2)逐跳选项头。

(3)目标选项头（IPv6头部目标地址字段中指明的第一个目标结点要紅理的信息， 以及路由选择头中列出的后续目标结点要处理的信息）。

(4)路由选择头。

(5)分段头。

(6)认证头。

(7)封装安全负荷头。

(8)目标选项头（最后的目标结点要处理的信息)。

(9)上层协议头部。

下面关于帧中继网络的描述中，错误的是(56)。

(56)A.用户的数据速率可以在一定的范围内变化

B.既可以适应流式业务，又可以适应突发式业务

C.帧中继网可以提供永久虚电路和交换虚电路

D.帧中继虚电路建立在HDLC协议之上

**【答案】D**

**【解析】**

帧中继（FR)在第二层建立虚电路，用帧方式承载数据业务，因而第三层被简化掉了。在用户平面，FR帧比HDLC帧操作简单，只检查错误，不再重传，没有滑动窗口式的流量控制机制，只有拥塞控制。

FR的虚电路分为永久虚电路(Permanent Virtual Circuit，.PVC)和交换虚电路（Switch Virtual Circuit, SVC)。PVC是在两个端用户乏间建立的固定逻辑连接，为用户提供约定的服务。帧中继交换设备根据预先配置的\_电路表把数据帧从一段链路交换到另外一段链路，最终传送到接收用户^ SVC是通过ISDN信令协议（Q931/Q933)临时建立的逻辑信道，它以呼叫的形式建立和释放连接。很多帧中继网络只提供PVC业务，不提供SVC业务。

帧中继网为用户提供约定信息速率(CIR)和扩展的信息速率（EIR)，以及约定突发量（Be)和超突发量（Be)，这些参数之间有如下关系：

Be = Tc × CIR

Be = Tc × EIR

其中，Tc为数据速率测量时间。网络应该保证用户以等于或低于cm的速率传送数据。对于超过CIR的Be部分，在正常情况下能可靠地传送，但若出现网络拥塞，则会被优先丢弃。对于Be部分的数据，网络将尽量传送，但不保证传送成功。对于超过Bc+Be的部分，网络拒绝接收。这是在保证用户正常通信的前提下防止网络拥塞的主要手段，对各种数据通信业务有很强的适应能力.

帧中继网中，用户的信息速率可以在一定的范围内变化，从而既可以适应流式业务，又可以适应突发式业务。

SNMP MIB中被管对象的Access属性不包括（57)。

(57)A.只读 B.只写 C.可读写 D.可执行

**【答案】D**

**【解析】**

SNMP MIB中被管对象的Access包括读、写、可读写属性，但不包括可执行。

汇聚层交换机应该实现多种功能，下面选项中，不属于汇聚层功能的是（58)。

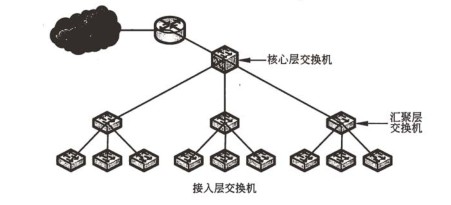
(58)A.VLAN间的路由选择 B.用户访问控制

C.分组过滤 D.组播管理

**【答案】B**

**【解析】**

网络的分层结构把复杂的大型网络分解为多个容易管理的小型网络，每一层交换设备分别实现不同的特定任务。分层的网络设计如下图所示。



•接入层交换机：接入层是工作站连接网络的入口，实现用户的访问控制，这一层的交换机应该以低成本提供高密度的接入端口。例如，Cisco Catalyst 2950系列可以提供12或24个快速以太网端口，适合中小型企业网络使用。

•汇聚层交换机：汇聚层将网络划分为多个广播/组播域，可以实现VLAN间的路由选择，并通过访问控制列表实现分组过滤。这一层交换机的端口数量和交换速率不要求很髙，但应提供第三层交换功能。例如，Cisco Catalyst 3550系列交换机具有多个10M/100M端口和两个内置的千兆以太网端口，可以支持多种GBIC 收发器，同时提供先进的服务质量（QoS)和速度限制，以及安全访问控制列表、组播管理和高性能的BP路由。

•核心层交换机：核心层应采用可扩展的高性能交换机组成园区网的主干线路，提供链路冗余、路由冗余、VLAN中继和负载均衡等功能，并且与汇聚层交换机具有兼容的技术，支持相同协议。例如，Cisco Catalyst 6500系列交换机就是一种适合部署到核心网络的交换机。

交换机命令Switch >enable的作用是（59)。

(59)A.配置访问口令 B.进入配置模式 C.进入特权模式 D.显示当前模式

**【答案】C**

**【解析】**

交换机的命令状态如下：

Switch >：交换机处于用户命令状态，这时用户可以看交换机的连接状态，访问其他网络和主机，但不能看到和更改交换机配置的内容。

Switch #：在Switch >提示符下输入enable,交换机进入特权命令状态，这时不但可以执行所有的用户命令，还可以看到和更改交换机的配置内容。

Switch (config)#：在Switch #提示符下输入configure terminal,这时交换机处于全局配置状态，可以配置交换机的全局参数。

Switch (config-if)#：交换机处于局部配置状态，这时可以配置交换机当前端口的参数。

IEEE 802.1q协议的作用是（60)。

(60)A.生成树协议 B.以太网流量控制

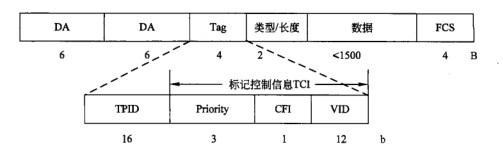
C.生成VLAN标记 D.基于端口的认证

**【答案】C**

**【解析】**

在划分成VLAN的局域网中，每个数据包都被加上一个有关VALN属性的帧标记，交换机之间根据帧标记来转发数据包。一个VLAN可以跨越多个交换机，带有VLAN标记的数据包在交换机之间的中继链路上传播，在进入PC时恢复原来的巾贞格式。

VLAN帧标记有两种格式：一种是交换机间链路协议(Inter-Switch Link, ISL)，这是Cisco公司的专利协议，适用于Cisco的Catalyst系列交换机；另一种是IEEE 802.1q协议，是在原来的以太帧中增加了4个字节的标记（Tag)字段，如下图所示，其中标记控制信息（Tag Control Information, TCI )包含Priority、CFI和VID三部分，各个字段的含义参见下图。



802.1q并没有定义优先级的含义，提供这种功能的是802.1p协议。另外，802.1p协议还提供了组播过滤机制，以配合IP组播功能，使得IP组播流量不会被交换机广播扩散。许多高档交换机都把实现802.1p和802.1q作为重要的性能指标。

CSMA/CD协议可以利用多种监听算法来减小发送冲突的概率，下面关于各种监听算法的描述中，正确的是（61)。

(61)A.非坚持型监听算法有利于减少网络空闲时间

B.1-坚持型监听算法有利于减少冲突的概率

C.P-坚持型监听算法无法减少网络的空闲时间

D.坚持型监听算法能够及时抢占信道

**【答案】D**

**【解析】**

CSMA/CD协议定义的监听算法有以下三种：

（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，而且增加了发送时延。

（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。

这种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。这种算法汲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T。

②若信道忙，继续监听直到信道空闲，转①。

③如果发送延迟一个时间单位T，则重复①。

困难的问题是决定概率P的值，P的取值应在重负载下能使网络有效地工作。为了说明P的取值对网络性能的影响，假设有n个站正在等待发送，与此同时，有一个站正在发送。当这个站发送停止时，实际要发送的站数等于nP。若nP大于1，则必有多个站同时发送，这必然会发生冲突，nP必须小于1。然而若P值太小，发送站就要等待较长的时间，在轻负载的情况下，这意味着较大的发送时延。

在Windows的DOS窗口中键入命令

C:\> nslookup

set type=ptr

> 211.151.91.165

这个命令序列的作用是(62)。

(62)A.査询211.151.91.165的邮件服务器信息

B.查询211.151.91.165到域名的映射

C.查询211.151.91.165的资源记录类型

D.显示211.151.91.165中各种可用的信息资源记录

**【答案】B**

**【解析】**

Nslookup显示可用来诊断域名系统（DNS)基础结构的信息。只有在已安装TCP/IP 协议的情况下才可以使用Nslookup命令行工具。Nslookup有两种模式:交互式和非交互式。语法为：

nslookup [-option] [hostname] [server]

在交互模式下，部分查询类型和查询的内容如下：

set type=mx：査询邮件交换记录；

set type=soa：査询SOA (Start of Authority)记录；

set type=CNAME：査询别名记录；

set type=NS：査询名字服务器记录；

set type=PTR：查询反向记录（从IP地址解释域名）

在Windows的命令窗口中键入命令arp -s 10.0.0.80 00-AA-00-4F-2A-9C,这个命令的作用是（63)。

(63)A.在ARP表中添加一个动态表项 B.在ARP表中添加一个静态表项

C.在ARP表中删除一个表项 D.在ARP表中修改一个表项

**【答案】B**

**【解析】**

Arp命令用于显示和修改地址解析协议（ARP)缓存表的内容，缓存表项是IP地址与网卡地址对。计算机上安装的每个网卡各有一个缓存表。如果使用不含参数的arp命令，则显示帮助信息。Arp命令的语法如下：

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/xt-09-s-x-63-1.jpg

对以上命令参数解释如下：

-a [InetAddr] [-N IfaceAddr]:显示所有接口的ARP缓存表。如果要显示特定IP地址的ARP表项，则使用参数InetAddr;如果要显示指定接口的ARP缓存表，则使用参数-N IfaceAddr。这里，N必须大写。InetAddr和IfaceAddr都是IP地址。

-g [InetAddr] [-N IfaceAddr]：与参数-a 相同。

-d InetAddr [IfaceAddr]-.删除由InetAddr指示的ARP缓存表项。要删除特定接口的ARP缓存表项，使用参数IfaceAddr指明接口的IP地址。要删除所有ARP缓存表项，使用通配符代替参数InetAddr。

-s InetAddr EtherAddr [ IfaceAddr]：添加一个静态的 ARP 表项，把 IP 地址InetAddr 解析为物理地址EtherAddr。参数IfaceAddr指定了接口的IP地址。

用参数-s添加的ARP表项是静态的，不会由于超时而被删除。如果TCP/IP协议停止运行，ARP表项都被删除。为了生成一个固定的静态表项，可以在批文件中加入适当的ARP命令，并在机器启动时运行批文件。

要添加一个静态表项，把IP地址10.0.0.80解析为物理地址00-AA-0(MF-2A-9C，则输入：

arp -s 10.0.0.80 00—AA—00-4F-2A-9C

下图是使用arp命令添加一个静态表项的例子。



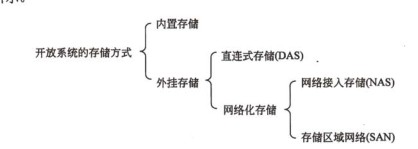
开放系统的数据存储有多种方式，属于网络化存储的是（64) 。

(64)A.内置式存储和DAS B.DAS和NAS C.DAS和SAN D.NAS和SAN

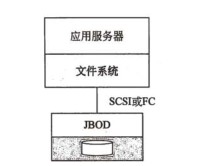
**【答案】D**

**【解析】**

基于Windows、Linux和UNIX等操作系统的服务器称为开放系统。开放系统的数据存储方式分为内置存储和外挂存储两种，而外挂存储又根据连接的方式分为直连式存储和网络化存储，目前应用的网络化存储方式有两种，即网络接入存储和存储区域网络，如下图所示。



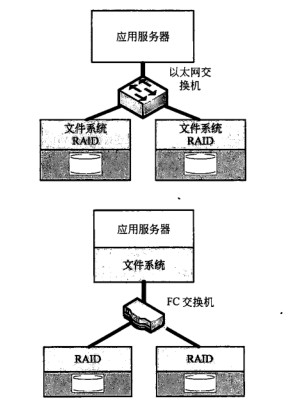
开放系统的直连式存储(Direct-Attached Storage, DAS)如下图所示，即在服务器上外挂了一组大容量硬盘，存储设备与服务器主机之间采用SCSI通道连接，带宽为10MB/S、 20MB/S、40MB/S和80MB/S等。DAS已经有近40年的使用历史，目前正在让位于日渐兴盛的网络化存储。



网络接入存储（Network Attached Storage, NAS)是将存储设备连接到现有的网络上，来提供数据存储和文件访问服务的设备。NAS服务器是在专用主机上安装简化了的操作系统的文件服务器。NAS服务器内置了与网络连接所需要的协议，可以直接联网，具有权限的用户都可以通过网络来访问NAS服务器中的文件。NAS服务器直接连接磁盘阵列，它具备磁盘阵列的所有特征：高容量、高效能、高可靠性。典型的NAS都连接到普通的以太网上，提供预先配置好的磁盘容量和存储管理软件，成为完备的网络存储解决方案，如下图所示。

存储区域网络（Storage Area Network, SAN)是一种连接存储设备和存储管理子系统的专用网络，专门提供数据存储和管理功能。SAN可以被看作是负责数据传输的后端网络，而前端网络（或称为数据网络）则负责正常的TCP/IP传输。也可以把SAN看作是通过特定互连方式连接的若干台存储服务器组成的单独的数据网络，提供企业级的数数

据存储服务，其拓扑结构如下图所示。



IEEE 802.11采用了类似于802.3 CSMA/CD协议的CSMA/CA协议，之所以不采用CSMA/CD协议的原因是(65)。

(65)A.CSMA/CA协议的效率更高 B.CSMA/CD协议的开销更大

C.为了解决隐蔽终端问题 D.为了引进其他业务

**【答案】C**

**【解析】**

CSMA/CA类似于802.3的CSMA/CD协议，这种访问控制机制叫做载波监听多路访问/冲突避免协议。在无线网中进行冲突检测有时是困难的，例如两个站由于距离过大或者中间障碍物的分隔从而检测不到冲突，但是位于它们之间的第三个站可能会检测到冲突，这就是所谓隐蔽终端问题。采用冲突避免的办法可以解决隐蔽终端的问题。802.11定义了一个巾贞间隔（Inter Frame Spacing, IFS)时间。另外还有一个后退计数器，它的初始值是随机设置的，递减计数直到'0。基本的操作过程是：

①如果一个站有数据要发送并且监听到信道忙，则产生一个随机数设置自己的后退计数器并坚持监听。

②听到信道空闲后等待IFS时间，然后开始计数。最先计数完的站可以开始发送。

③其他站在听到有新的站开始发送后暂停计数，在新的站发送完成后再等待一个IFS时间继续计数，直到计数完成开始发送。

分析这个算法发现，两次IFS之间的间隔是各个站竞争发送到时间。这个算法对参与竞争的站是公平的，基本上挺按先来先服务的顺序获得发送的机会。

建筑物综合布线系统中的工作区子系统是指（66)。

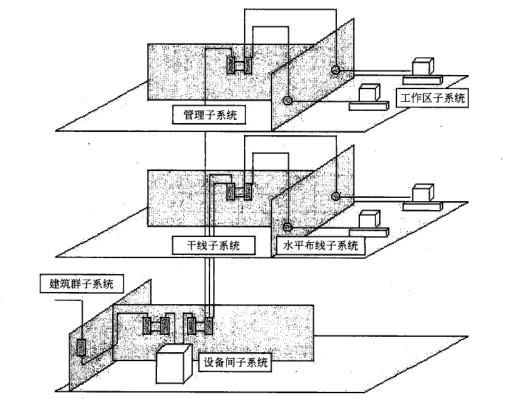
(66)A.由终端到信息插座之间的连线系统 B.楼层接线间的配线架和线缆系统

C.各楼层设备之间的互连系统 D.连接各个建筑物的通信系统

**【答案】A**

**【解析】**

建筑物综合布线系统分为6个子系统：工作区子系统、7JC平布线子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统，如下图所示。



工作区子系统是由终端设备到信息插座的整个区域。一个独立的需要安装终端设备的区域划分为一个工作区，工作区应支持电话、数据终端、计算机、电视机、监视器，以及传感器等多种终端设备。

各个楼层接线间的配线架到工作区信息插座之间所安装的线缆属于水平子系统。水平布线子系统的作用是将干线子系统线路延伸到用户工作区。

管理子系统设置在楼层的接线间内，由各种交连设备（双绞线跳线架、光纤跳线架) 以及集线器和交换机等交换设备组成，交连方式取决于网络拓扑结构和工作区设备的要求。

干线子系统是建筑物的主干线缆，实现各楼层设备间子系统之间的互连。干线子系统通常由垂直的大对数铜缆或光缆组成，一头端接于设备间的主配线架上，另一头端接在楼层接线间的管理配线架上。

建筑物的设备间是网络管理人员值班的场所，设备间子系统由建筑物的进户线、交换设备、电话、计算机、适配器以及保安设施组成，实现中央主配线架与各种不同设备 (如PBX，网络设备和监控设备等）之间的连接。

建筑群子系统也叫园区子系统，它是连接各个建筑物的通信系统。

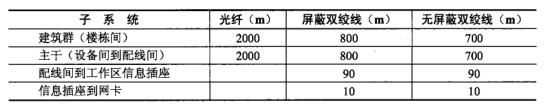
EIA/TIA-568标准规定，在综合布线时，如果信息插座到网卡之间使用无屏蔽双绞，布线距离最大为（67) m。

(67)A.10 B.30 C.50 D.100

**【答案】A**

**【解析】**

在进行结构化布线系统设计时，要考虑线缆长度的限制，下表是EIA/TIA-568标准提出的布线距离最大值。



网络安全体系设计可从物理线路安全、网络安全、系统安全、应用安全等方面来进行，其中，数据库容灾属于（68)。

(68)A.物理线路安全和网络安全 B.应用安全和网络安全

C.系统安全和网络安全 D.系统安全和应用安全

**【答案】D**

**【解析】**

网络安全体系设计是逻辑设计工作的重要内容之一，数据库容灾属于系统安全和应用安全考虑范畴。

下列关于网络核心层的描述中，正确的是（69)。

(69)A.为了保障安全性，应该对分组进行尽可能多的处理

B.将数据分组从一个区域高速地转发到另一个区域

C.由多台二、三层交换机组成

D.提供多条路径来缓解通信瓶颈

**【答案】B**

**【解析】**

三层模型主要将网络划分为核心层、汇聚层和接入层，每一层都有着特定的作用。核心层提供不同区域或者下层的高速连接和最优传送路径；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网络提供接入。其中核心层是互连网络的高速骨干，由于其重要性，因此在设计中应该采用冗余组件设计，使其具备高可靠性，能快速适应变化。

在设计核心层设备的功能时，应尽量避免使用数据包过滤、策略路由等降低数据包转发处理的特性，以优化核心层获得低延迟和良好的可管理性。

核心层应具有有限的和一致的范围，如果核心层覆盖的范围过大，连接的设备过多，必然引起网络的复杂度加大，导致网络管理性降低；同时，如果核心层覆盖的范围不一致，必然导致大量处理不一致情况的功能都在核心层网络设备中实现，会降低核心网络设备的性能。

对于那些需要连接因特网和外部网络的网络工程来说，核心层应包括一条或多条连接到外部网络的连接，这样可以实现外部连接的可管理性和高效性。

网络系统设计过程中，物理网络设计阶段的任务是（70)。

(70)A.依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境

B.分析现有网络和新网络的各类资源分布，掌握网络所处的状态

C.根据需求规范和通信规范，实施资源分配和安全规划

D.理解网络应该具有的功能和性能，最终设计出符合用户需求的网络

**【答案】A**

**【解析】**

网络的生命周期至少包括网络系统的构思计划、分析设计、实时运行和维护的过程。对于大多数网络系统来说，由于应用的不断发展，这些网络系统需要进行不断重复设计、 实施、维护的过程。其中：

网络逻辑结构设计是体现网络设计核心思想的关键阶段，在这一阶段根据需求规范和通信规范选择一种比较适宜的网络逻缉结构，并基于该逻辑结构实施后续的资源分配规划、安全规划等内容。

物理网络设计是对逻辑网络设计的物理实现，通过对设备的具体物理分布、运行环境等的确定，确保网络的物理连接符合逻辑连接的要求。在这一阶段，网络设计者需要确定具体的软硬件、连接设备、布线和服务。

现有网络体系分析的工作目的是描述资源分布，以便于在升级时尽量保护已有投资，通过该工作可以使网络设计者掌握网络现在所处的状态和情况。

需求分析阶段有助于设计者更好地理解网络应该具有什么功能和性能，最终设计出符合用户需求的网络，它为网络设计提供依据。

Routing protocols use different techniques for assigning (71) to individual networks. Further, each routing protocol forms a metric aggregation in a different way. Most routing protocols can use multiple paths if the paths have an equal (72) . Some routing protocols can even use multiple paths when paths have an unequal cost In either case, load (73) can improve overall allocation of network bandwidth. When multiple paths are used, there are several ways to distribute the packets. The two most common mechanisms are per-packet load balancing and per-destination load balancing. Per-packet load balancing distributes the (74) across the possible routes in a manner proportional to the route metrics. Per-destination load balancing distributes packets across the possible routes based on (75).

(71)A.calls B.metrics C.links D.destinations

(72)A.user B.distance C.entity D.cost

(73)A.bracketing B.balancing C.downloading D.transmitting

(74)A.destinations B.resources C.packets D.sources

(75)A.destinations B.resources C.packets D.Sources

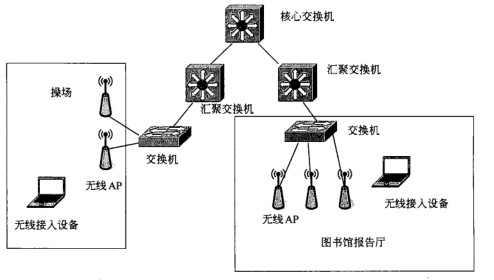
**【答案】B D B C A**

**【解析】**

各种路由协议使用不同的技术来为网络赋予度量值。进一步说，每一种路由协议都形成了不同的度量汇聚模式。大部分路由协议在各个通路具有相等费用时可以使用多个通路。某些路由协议甚至在各个通路费用不相等时也可以使用多个通路。在上述任何一种情况下，负载均衡都可以改进网络带宽的全局分配。当使用多个通路时，可以使用多种方法来分配分组。两种最通常的机制是按分组进行负载均衡和按目标进行负载均衡。按分组进行负载均衡是指按照路由度量的比例向各个可能的路由上分配分组。按目标进行负载均衡是指根据目标向各个可能的路由上分配分组。

**试题一**

某校园网中的无线网络拓扑结构如下图所示。



该网络中无线网络的部分需求如下：

1.学校操场要求部署AP，该操场区域不能提供外接电源。

2.学校图书馆报告厅要求高带宽、多接入点。

3.无线网络接入要求有必要的安全性。

**【问题1】**

根据学校无线网络的需求和拓扑图可以判断，连接学校操场无线AP的是（1）交换机，它可以通过交换机的（2）口为AP提供直流电。

(1)PoE (或答802.3af也给全分）

(2)以太（或 Ethernet)

本题考查无线网络的部署问题。

本问题考查POE知识。根据题目要求，学校操场要求部署AP，该操场区域不能提供外接电源，所以应采用POE技术供电。

POE (Power Over Ethernet)指的是在现有的以太网Cat.5布线基础架构不做任何改动的情况下，在为一些基于IP的终端（如IP电话机、无线局域网接入点AP、网络摄像机等）传输数据信号的同时，还能为此类设备提供直流供电的技术。POE技术能在确保现有结构化布线安全的同时现有网络的正常运作，最大限度地降低成本。

POE也被称为基于局域网的供电系统(Power over LAN，POL)或有源以太网（Active Ethernet),有时也被简称为以太网供电，这是利用现存标准以太网传输电缆的同时传送数据和电功率的最新标准规范，并保持了与现存以太网系统和用户的兼容性。IEEE802.3af标准是基于以太网供电系统POE的新标准，它在IEEE 802.3的基础上增加了通过网线直接供电的相关标准，是现有以太网标准的扩展，也是第一个关于电源分配的国际标准。

**【问题2】**

1.根据需求在图书馆报告厅安装无线AP。如果采用符合IEEE 802.11b规范的AP，理论上最高可以提供（3)Mb/s的传输速率；如果釆用符合IEEE 802.llg规范的AP，理论上最高可以提供（4)Mb/s的传输速率。如果采用符合（5)规范的AP，由于将MMO技术和（6)调制技术结合在一起，理论上最高可以提供600Mbps的传输速率。

(5)备选答案

A.IEEE 802.11a B. IEEE 802.11e

C.IEEE 802.11i D. IEEE 802.11n

(6)备选答案

A. BFSK B. QAM C. OFDM D. MFSK

2.图书馆报告厅需要部署10台无线AP，在配置过程中发现信号相互干扰严重，这时应调整无线AP的(7)设置，用户在该报告厅内应选择(8),接入不同的无线AP。

(7)〜（8)备选答案

A.频道 B.功率 C.加密模式 D.操作模式E.SSID

(3)11

(4)54

(5)D

(6)C

(7)A

(8)E

本问题考查802.11的标准规范问题。

802.11是IEEE最初制定的一个无线局域网标准，主要用于解决办公室局域网和校园网中用户与用户终端的无线接入，业务主要限于数据存取，速率最高只能达到2Mbps。由于它在速率和传输距离上都不能满足人们的需要，因此IEEE小组又相继推出了多个新标准，主要如下：

IEEE 802.11a (Wi-Fi5)标准是得到广泛应用的802.11b标准的后续标准，工作在5GHzU-NII频带，物理层速率可达54Mbps，传输层可达.25Mbps;可提供25Mbps的无线ATM接口和10Mbps的以太网无线帧结构接口，以及TDD/TDMA的空中接口；支持语音、数据、图像业务；一个扇区可接入多个用户，每个用户可带多个用户终端。

IEEE802.11b是无线局域网的一个标准。其载波的频率为2.4GHz,传送速度为llMbit/s。IEEE 802.11b在2.4-GHz-ISM频段共有14个频宽为22MHz的频道可供使用。IEEE802.11b的后继标准是IEEE 802.11g,其传送速度为54Mb/s。

IEEE 802.11n是2004年1月IEEE宣布组成的一个新的单位来发展新的802.11标准，它增加了 MIMO (multiple-input multiple-output)的标准。利用MIMO使用多个发射和接收天线来允许更高的资料传输率。IEEE 802.1 In将MIMO技术与OFDM调制技术结合在一起，理论上最髙可以提供600Mbps的传输速率。

无线AP —般在某个频段工作。当在某个区域有多个无线AP，且使用同一频道时，可能出现信号相互干扰严重的问题。在某个频段下，实际有多个频道，可以通过手动方式修改无线AP所使用的频道，或在无线AP上安装一个5GHz的组件。5GHz可以使用的频段有23个，且几乎没有其他人在使用，这样可以解决信号相互干扰的问题。另外，在无线AP中，SSID (Service Set Identifier)用来区分不同的网络，最多可以有32个字符，无线网卡设置不同的SS1D就可以进入不同网络，SSID通常由AP广播出来，用户选择不同的SSID,接入不同的无线AP。

**【问题3】**

若在学校内一个专项实验室配置无线AP,为了保证只允许实验室的PC机接入该无线AP,可以在该无线AP上设置不广播（9),对客户端的（10) 地址进行过滤，同时为保证安全性，应采用加密措施。无线网络加密主要有三种方式：(11)、WPA/WPA2、WPA-PSKAVPA2-PSK。在这三种模式中，安全性最好的是（12),其加密过程采用了TKIP和(13) 算法。

(13)备选答案

A. AES B. DES C. IDEA D. RSA

(9)SSID

(10)MAC (或物理地址）

(11)WEP (或有线等效加密）

(12)WPA-PSK/WPA2-PSK或WPA/WPA2

(13)A

本问题考査配置无线AP安全的问题。

解决无线AP安全，首先要通过SSID和MAC地址过滤防止非法链接。

SSID用来区分无线访问节点所使用的初始化字符串，客户端要通过SSID来完成链接的初始化。该校验器由制造商进行设定，同一厂商产品使用同样的默认值。如果使用厂家的初始化字符串，那么就可能被非授权链接。因此，在配置无线网络时，应更改SSID初始化字符串，使其难于猜测，并在条件许可的情况下限制SSID广播，以此来杜绝非法链接。

在无线AP中，可以设置MAC地址过滤，这样只用指定的MAC地址才能登录无线AP,从而保证杜绝非法链接。

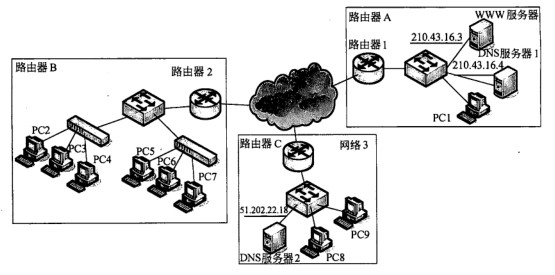
为保证无线网络的安全性，还应采用加密措施。无线网络加密主要有三种方式：WEP、WPA/WPA2 和 WPA-PSK/WPA2-PSK。

无线网络最初采用的安全机制是WEP (有线等效私密），但是后来发现WEP是很不安全的，802.11组织开始着手制定新的安全标准，也就是后来的802.11i协议。但是标准的制定到最后的发布需要较长的时间，而且考虑到消费者不会为了网络的安全性而放弃原来的无线设备，因此Wi-Fi联盟在标准推出之前，在802.11i草案的基础上制定了一种称为WPA( Wi-Fi Protected Access)的安全机制，它使用TKJP(临时密钥完整性协议)，使用的加密算法还是WEP中使用的加密算法RC4,所以不需要修改原来无线设备的硬件，WPA针对WEP中存在的问题：IV过短、密钥管理过于简单、对消息完整性没有有效的保护，通过软件升级的方法提髙了网络的安全性。

在802.11i颁布之后，Wi-Fi联盟推出了 WPA-PSK/WPA2-PSK，它支持AES (高级加密算法)，因此需要新的硬件支持，使用qcMP (计数器模式密码块链消息完整码协议)，其安全性最好。

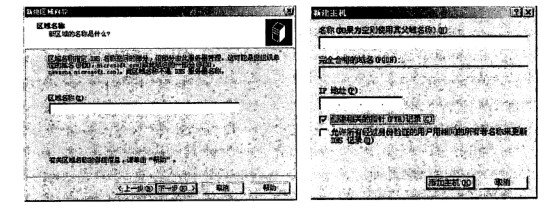
**试题二**

网络拓扑结构如下图所示。



**【问题1】**

网络A的WWW服务器上建立了一个Web站点，对应的域名是www.abc.edu。DNS 服务器1上安装Windows Server 2003操作系统并启用DNS服务。为了解析WWW服务器的域名，在左下图所示的对话框中，新建一个区域的名称是（1);在右下图所示的对话框中，添加的对应的主机“名称”为(2)。



(1)abc.edu

(2)www

由网络A的WWW服务器对应的域名是www.abc.edu，故在DNS服务器上新建的区域的名称是abc.edu，主机名称为www。

**【问题2】**

在DNS系统中反向查询（Reverse Query)的功能是(3)。为了实现网络A中WWW服务器的反向查询，在左下图和右下图中进行配置，其中网络ID应填写为(4), 主机名应填写为(5)。

(3)用IP地址查询对应的域名

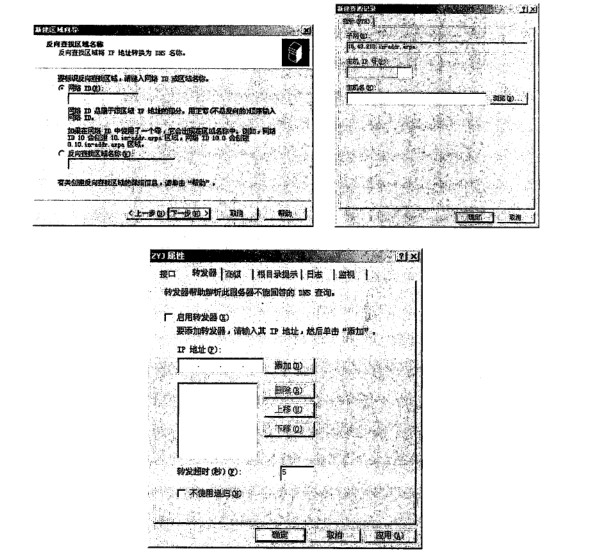
(4)210.43.16.3

(5)www.abc.edu

在DNS系统中可利用反向查询功能来依据IP地址查询对应的域名Windows Server 2003操作系统中配置DNS反向查询时IP地址倒写，且只取前3个字节，故(4)应填入“210.43.16”，对应的主机名为www.abc.edu。

**【问题3】**

DNS服务器1负责本网络区域的域名解析，对于非本网络的域名，可以通过设置“转发器”，将自己无法解析的名称转到网络C中的DNS服务器2进行解析。设置步骤：首先在“DNS管理器”中选中DNS服务器，单击鼠标右键，选择“属性”对话框中的“转发器”选项卡，在弹出的如下图所示的对话框中应如何配置？



选中“启用转发器”复选框，在IP地址栏输入“51.202.22.18”，单击“添加”按钮，然后单击“确定”按钮关闭对话框。

转发器的功能是将自己无法解析的名称转到另一个DNS服务器进行转发，配置转发服务器时需要指定转发服务器的IP地址。故在图中应选中“启用转发器”复选框，并在IP地址栏输入DNS服务器2的IP地址，即“51.202.22.18”。

**【问题4】**

网络C的Windows Server 2003服务器上配置了 DNS服务，在该服务器上两次使用nslookup www.sohu.com命令得到的结果如下图所示，由结果可知，该DNS服务器（6)。

(6)备选答案：

A.启用了循环功能 B.停用了循环功能 C.停用了递归功能 D.启用了递归功能

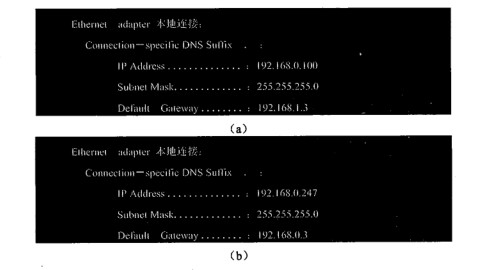


（6）A

从DNS服务器上两次使用nslookup得到的结果可以看出，该DNS服务器启用了循环功能。

**【问题5】**

在网络B中，除PC5计算机以外，其他的计算机都能访问网络A的WWW服务器，而PC5计算机与网络B内部的其他PC都是连通的。分别在PC5和PC6上执行命令ipconfig,结果信息如下图（a)和（b)所示：



请问PC5的故障原因是什么？如何解决？

PC5的默认网关配置错误。

将默认网关IP地址修改为“192.168.0.3”。

PC5和PC6Intemet协议属性参数中网关地址不同，故PC5的默认网关配置错误。将其默认网关IP地址修改为“192.168.0.3”即可。

**试题三**

在大型网络中，通常采用DHCP完成基本网络配置会更有效率。

**【问题1】**

在Linux系统中，DHCP服务默认的配置文件为（1）。

(1)备选答案：

A. /etc/dhcpd.conf B. /etc/dhcpd.config C./etc/dhcp.conf D. /etc/dhcp.config

(1)A

在Linux系统中，DHCP服务默认的配置文件为/etc/dhcpd.conf。

**【问题2】**

管理员可以在命令行通过（2)命令启动DHCP服务；通过（3)命令停止DHCP服务。

(2)、(3)备选答案：

A. service dhcpd start B. service dhcpd up

C.service dhcpd stop D. service dhcpd down

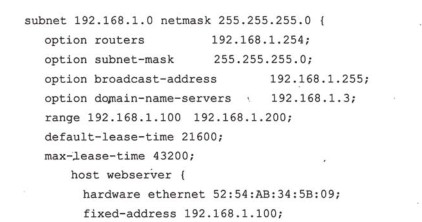
(2)A

(3)C

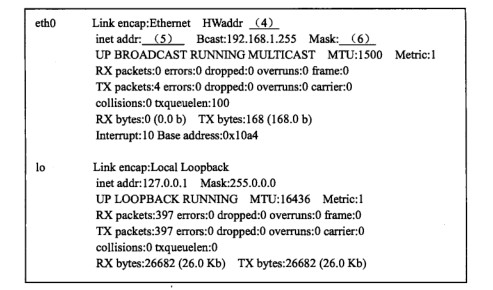
在Linux系统中，可以在命令行下通过service dhcpd start和service dhcpd stop进行DHCP服务的启动和停止。

**【问题3】**

在Linux系统中配置DHCP服务器，该服务器配置文件的部分内容如下：



在主机Webserver上运行ifconfig命令时显示如下，根据DHCP配置，填写空格中缺少的内容。



该网段的网关IP地址为（7),域名服务器IP地址为（8) 。

(4)52:54:AB:34:5B:09

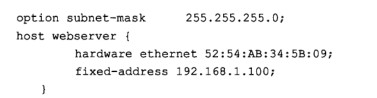
(5) 192.168.1.100

(6)255.255.255.0

(7)192.168.1.254

(8)192.168.1.3

问题（4)〜（6)是Webserver的MAC地址、IP地址和网络掩码。在/etc/dhcpd.conf 中有如下相关内容：、



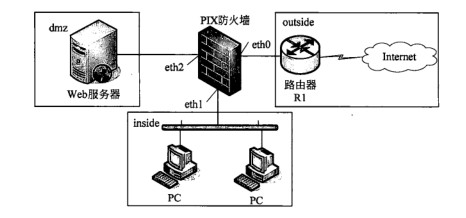
因此可以知道Webserver 的MAC地址是 52:54:AB:34:5B:09, IP 地址是192.168.1.100, 网路掩码为255.255.255.0。

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

因此该网段的网关IP地址为192.168.1.254, DNS为192.168.1.3。

**试题四**

某公司通过PIX防火墙接入Internet,网络拓扑如下图所示。



在防火墙上利用show命令查询当前配置信息如下:

PIX# show config ?

nameif eth0 outside security 0

nameif eth1 inside security 100

nameif eth2 dmz security 40

fixup protocol ftp 21 （1）

fixup protocol http 80 ?

ip address outside 61.144.51.42 255.255.255.248

ip address inside 192.168.0.1 255.255.255.0

ip address dmz 10.10.0.1 255.255.255.0 ?

global(outside) 1 61.144.51.46

nat(inside) 1 0.0.0.0 0.0.0.0

route outside 0.0.0.0 0.0.0.0 61.144.51.45 1 （2）

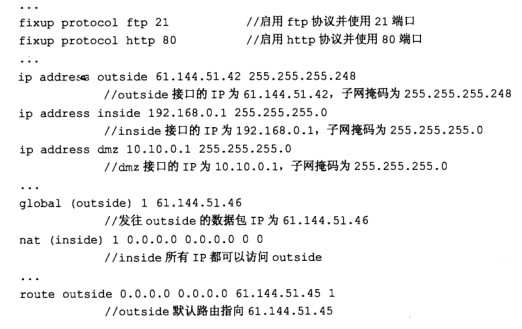
**【问题1】**

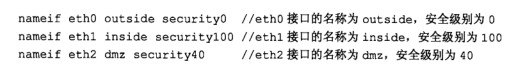
解释（1)、(2)处画线语句的含义。

(1)启用ftp服务

(2)设置eth0口的默认路由，指向61.144.51.45,且跳步数为1

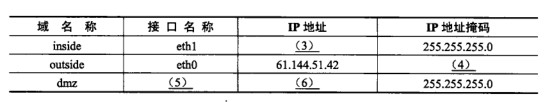
使用show config命令得到的配置信息解释如下：





**【问题2】**

根据配置信息，填写下表。



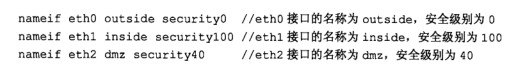
(3) 192.168.0.1

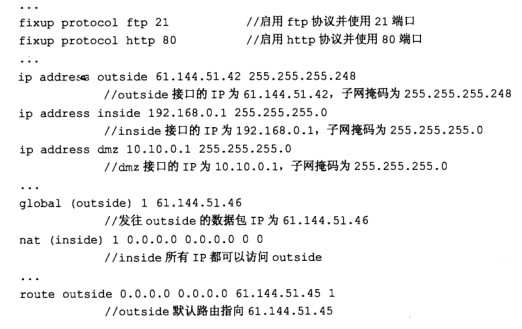
(4)255.255.255.248

(5)eth2

(6)10.10.0.1

使用show config命令得到的配置信息解释如下：



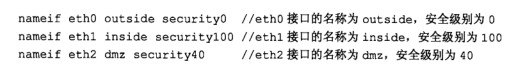


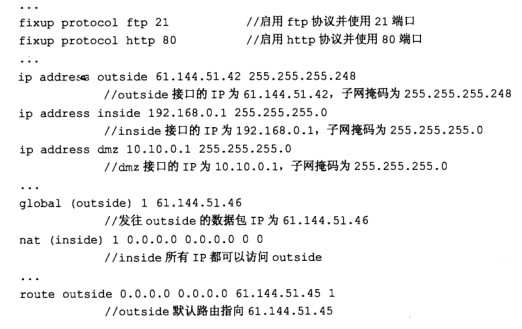
**【问题3】**

根据所显示的配置信息，由inside域发往Internet的IP分组，在到达路由器R1时的源IP地址是（7)。

(7)61.144.51.46

使用show config命令得到的配置信息解释如下：





**【问题4】**

如果需要在dmz域的服务器（IP地址为10.10.0.100)对Internet用户提供Web服务(对外公开IP地址为61.144.51.43)，请补充完成下列配置命令。

PIX(config)#static (dmz, outside) (8) (9)

PIX(config)#conduit permit tcp host (10) eq www any

(8)61.144.51.43

(9)10.10.0.100

(10)61.144.51.43

static命令的语法如下：

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/xt-09-x-x-4-7.jpg

根据static命令的语法，空（8)应该填对outside公开的IP地址61.144.51.43,空（9) 应该填dmz域服务器的IP地址10.10.0.100。

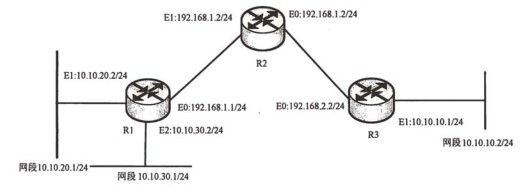
conduit命令用来设置允许数据从低安全级别的接口流向具有较高安全级别的接口。 conduit命令的语法如下：

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/xt-09-x-x-4-8.jpg

根据conduit命令的语法，空（10)应该填Web服务对外公开的IP地址61.144.51.43。

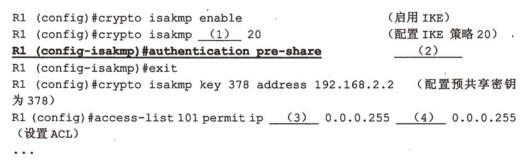
**试题五**

某单位网络拓扑结构如下图所示，要求配置IPSec VPN使10.10.20.1/24网段能够连通10.10.10.2/24 网段，但10.10.30.1/24 网段不能连通10.10.10.2/24网段。



**【问题1】**

根据网络拓扑和要求，解释并完成路由器R1上的部分配置。



(1)Policy

(2)在IKE协商过程中使用预共享密钥认证方式

(3)10.10.20.0

(4)10.10.10.0

本题目考查IPSec VPN的配置问题。



**【问题2】**

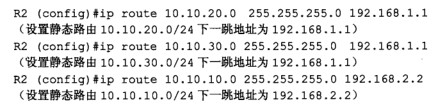
根据网络拓扑和要求，完成路由器R2上的静态路由配置。

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/xt-09-x-x-5-5.jpg

(5)10.10.20.0

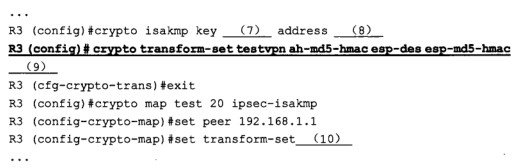
(6)192.168.1.1

分析：



**【问题3】**

根据网络拓扑和R1的配置，解释并完成路由器R3的部分配置。



(7)378

(8)192.168.1.1

(9)设置名为testvpn的VPN，采用MD5认证、DES进行数据加密

(10)testvpn

根据R1配置和拓扑结构可知，R3路由器配置IPSec VPN对端连接地址192.168.1.1，其预共享密钥为378。

