在输入输出控制方法中，采用 （1) 可以使得设备与主存间的数据块传送无需CPU干预。

(1)A.程序控制输入输出 B.中断 C.DMA D.总线控制

**【答案】C**

**【解析】本题考查CPU中相关寄存器的基础知识。**

计算机中主机与外设间进行数据传输的输入输出控制方法有程序控制方式、中断方式、DMA等。

在程序控制方式下，由CPU执行程序控制数据的输入输出过程。

在中断方式下，外设准备好输入数据或接收数据时向CPU发出中断请求信号，CPU 若决定响应该请求，则暂停正在执行的任务，转而执行中断服务程序进行数据的输入输出处理，之后再回去执行原来被中断的任务。

在DMA方式下，CPU只需向DMA控制器下达指令，让DMA控制器来处理数据的传送，数据传送完毕再把信息反馈给CPU，这样就很大程度上减轻了CPU的负担，可以大大节省系统资源。

若某计算机采用8位整数补码表示数据，则运算（2）将产生溢出。

(2)A.-127+1 B.-127-1 C.127+1 D.127-1

**【答案】C**

**【解析】本题考查计算机中的数据表示和运算的基础知识。**

采用8位补码表示整型数据时，可表示的数据范围为-128〜127,因此进行127+1的运算会产生溢出。

编写汇编语言程序时，下列寄存器中程序员可访问的是（3)。

(3)A.程序计数器（PC) B.指令寄存器(IR)

C.存储器数据寄存器（MDR) D.存储器地址寄存器（MAR)

**【答案】A**

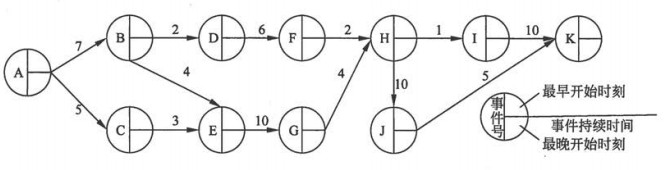
**【解析】本题考查CPU中相关寄存器的基础知识。**

指令寄存器（IR)用于暂存从内存取出的、正在运行的指令，这是由系统使用的寄存器，程序员不能访问.

存储器数据寄存器（MDR)和存储器地址寄存器（MAR)用于对内存单元访问时的数据和地址暂存，也是由系统使用的，程序员不能访问。

程序计数器（PC)用于存储指令的地址，CPU根据该寄存器的内容从内存读取待执行的指令，程序员可以访问该寄存器。

使用PERT图进行进度安排，不能清晰地描述（4)，但可以给出哪些任务完成后才能开始另一些任务。下面的PERT图所示工程从A到K的关键路径是（5)(图中省略了任务的开始和结束时细)。



(4)A.每个任务从何时开始 B.每个任务到何时结束

C.各任务之间的并行情况 D.各任务之间的依赖关系

(5)A.ABEGHIK B.ABEGHJK C.ACEGHIK D.ACEGHJK

**【答案】C B**

**【解析】本题考查软件项目管理的基础知识。**

软件项目计划的一个重要内容是安排进度，常用的方法有Gantt图和PERT图。Gantt 图用水平条状图描述，它以日历为基准描述项目任务，可以清楚地表示任务的持续时间和任务之间的并行，但是不能清晰地描述各个任务之间的依赖关系。PERT图是一种网络模型，描述一个项目的各任务之间的关系。可以明确表达任务之间的依赖关系，即哪些任务完成后才能开始另一些任务，以及如期完成整个工程的关键路径，但是不能清晰地描述各个任务之间的并行关系。

图中任务流ABEGHIK的持续时间是36, ABEGHJK的持续时间是40, ACEGHIK的持续时间是33, ACEGHJK的持续时间为37。所以项目关键路径长度为40。

某项目组拟开发一个大规模系统，且具备了相关领域及类似规模系统的开发经验。下列过程模型中，(6)最合适开发此项目。

(6)A.原型模型 B.瀑布模型 C.V模型 D.螺旋模型

**【答案】B**

**【解析】本题考查软件开发生命周期模型的基本知识。**

常见的软件生存周期模型有瀑布模型、演化模型、螺旋模型、喷泉模型等。瀑布模型是将软件生存周期各个活动规定为依线性顺序连接的若干阶段的模型，适合于软件需求很明确的软件项目。V模型是瀑布模型的一种演变模型，将测试和分析与设计关联进行，加强分析与设计的验证。原型模型是一种演化模型，通过快速构建可运行的原型系统，然后根据运行过程中获取的用户反馈进行改进。演化模型特别适用于对软件需求缺乏准确认识的情况。螺旋模型将瀑布模型和演化模型结合起来，加入了两种模型均忽略的风险分析。

本题中项目组具备了所开发系统的相关领域及类似规模系统的开发经验，即需求明确，瀑布模型最适合开发此项目。

软件复杂性度量的参数不包括（7)。

(7)A.软件的规模 B.开发小组的规模 C.软件的难度 D.软件的结构

**【答案】B**

**【解析】**

软件复杂性度量是软件度量的一个重要分支。软件复杂性度量的参数有很多，主要包括：（1)规模，即指令数或者源程序行数；（2)难度，通常由程序中出现的操作数所决定的量来表示；结构，通常用与程序结构有关的度量来表示；（3)智能度，即算法的难易程度。

在操作系统文件管理中，通常采用（8)来组织和管理外存中的信息。

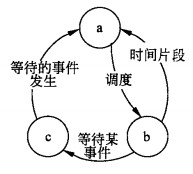
(8)A.字处理程序 B.设备驱动程序 C.文件目录 D.语言翻译程序

**【答案】C**

**【解析】本题考査的是操作系统文件管理方面的基础知识。**

存放在磁盘空间上的各类文件必须进行编目，操作系统才能实现文件的管理，这与图书馆中的藏书需要编目录、一本书需要分章节是类似的。用户总是希望能“按名存取”文件中的信息。为此，文件系统必须为每一个文件建立目录项，即为每个文件设置用于描述和控制文件的数据结构，记载该文件的基本信息，如文件名、文件存放的位置、文件的物理结构等。这个数据结构称为文件控制块FCB，文件控制块的有序集合称为文件目录。

假设系统中进程的三态模型如下图所示，图中的a、b和c的状态分别为（9)。



(9)A.就绪、运行、阻塞 B.运行、阻塞、就绪

C.就绪、阻塞、运行 D.阻塞、就绪、运行

**【答案】A**

**【解析】**

进程具有三种基本状态：运行态、就绪态和阻塞态。处于这三种状态的进程在一定条件下，其状态可以转换。当CPU空闲时，系统将根据某种调度算法选择处于就绪态的一个进程进入运行态；而当CPU的一个时间片用完时，当前处于运行态的进程就进入了就绪态；进程从运行到阻塞状态通常是由于进程释放CPU,等待系统分配资源或等待某些事件的发生，如：执行了P操作，系统暂时不能满足其对某资源的请求，或等待用户的输入信息等；当进程正在等待的事件发生时，进程从阻塞到就绪状态，如I/O完成。

利用（10)可以对软件的技术信息、经营信息提供保护。

(10)A.著作权 B.专利权 C.商业秘密权 D.商标权

**【答案】C**

**【解析】本题考查知识产权方面的基础知识，涉及软件商业秘密权的相关概念。**

著作权从软件作品性的角度保护其表现形式，源代码（程序)、目标代码（程序)、软件文档是计算机软件的基本表达方式（表现形式)，受著作权保护；专利权从软件功能性的角度保护软件的思想内涵，即软件的技术构思、程序的逻辑和算法等的思想内涵，当计算机软件同硬件设备是一个整体，涉及计算机程序的发明专利，可以申请方法专利，取得专利权保护。商标权是为商业化的软件从商品、商誉的角度为软件提供保护，利用商标权可以禁止他人使用相同或者近似的商标、生产（制作）或销售假冒软件产品。商标权受保护的力度大于其他知识产权，对软件的侵权行为更容易受到行政查处。而商业秘密权是商业秘密的合法控制人采取了保密措施，依法对其经营信息和技术信息享有的专有使用权，我国《反不正当竞争法》中对商业秘密的定义为“不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利人釆取保密措施的技术信息和经营信息”。软件技术秘密是指软件中适用的技术情报、数据或知识等，包括程序、设计方法、技术方案、功能规划、开发情况、测试结果及使用方法的文字资料和图表，如程序设计说明书、流程图、用户手册等。软件经营秘密指具有软件秘密性质的经营管理方法以及与经营管理方法密切相关的信息和情报，其中包括管理方法、经营方法、产销策略、客户情报（客户名单、客户需求)，以及对软件市场的分析、预测报告和未来的发展规划、招投标中的标底及标书内容等。

光纤分为单模光纤和多模光纤，这两种光纤的区别是（11)。

(11)A.单模光纤的数据速率比多模光纤低

B.多模光纤比单模光纤传输距离更远

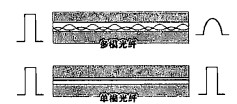
C.单模光纤比多模光纤的价格更便宜

D.多模光纤比单模光纤的纤芯直径粗

**【答案】D**

**【解析】本题考查有关光纤传输介质的基础知识。**

光波在光导纤维中以多种模式传播，不同的传播模式有不同的电磁场分布和不同的传播路径，这样的光纤叫多模光纤（Multi Mode Fiber)。光波在光纤中以什么模式传播， 这与芯线的直径、芯线和包层的相对折射率，以及工作波长有关。如果芯线的直径小到光波波长大小，则光纤就成为波导，光在其中无反射地沿直线传播，这种光纤叫单模光纤（Single Mode Fiber)，如下图所示。



单模光纤采用激光二极管作为光源，波长分为1310nm和1550nm两种。单模光纤的纤芯直径为8.3um，包层外径为125um，可表示为8.3/125um。单模光纤只能传导一种模式的光，色散很小，适用于远程通信。如果希望支持万兆传输，而且距离较远，应考虑采用单模光缆。

多模光纤采用LED作为光源，波长分为850nm和1300nm两种。多模光纤的纤芯较粗，有50um和62.5um两种，包层外径125um，分别表示为50/125um和62.5/125um。多模光纤可传输多种模式的光，但模间色散较大，这就限制了传输信号的频率，而且随着距离的增加，限制会更加严重。多模光纤传输的距离比较近，一般只有几公里。但是多模光纤要比单模光纤价格便宜，如果对传输距离或数据速率要求不高，则可选择多模光缆。

下面关于交换机的说法中，正确的是（12)。

(12)A.以太网交换机可以连接运行不同网络层协议的网络

B.从工作原理上讲，以太网交换机是一种多端口网桥

C.集线器是一种特殊的交换机

D.通过交换机连接的一组工作站形成一个冲突域

**【答案】B**

**【解析】本题考查网络交换设备的基础知识。**

集线器也是一神物理层设备，虽然它还有检测冲突的作用，但这些操作都属于物理层功能的范围。

网桥是一种数据链路层设备，它处理的对象是数据链路层的协议数据单元---帧，其处理功能包括检查帧的格式、进行差错校验、识别目标地址、选择路由并实现帧的转发等。更准确地说，网桥包含了物理层和数据链路层两个功能层次，所以在以太网中， 网桥也能起到延长传输距离的作用。

现代以太网中，更多地使用交换机代替网桥，只有在简单的小型网络中才用微机软件实现网桥的功能。以太网交换机也是一种数据链路层设备，除传统网桥的功能之外，交换机把共享介质变成了专用链路，使得网络的有效数据速率大大提高。

虽然交换机与集线器在外部结构上相似，连接的网络拓扑结构相同，但它们是不同的设备。通过集线器连接的一组工作站形成一个冲突域，其中只能有一个设备发送数据，其他设备只能接收数据或处于等待状态。用交换机连接的一组工作站可以多个设备同时发送数据，只要目标站不冲突就可以了。用集线器连接的工作站和用交换机逹接的工作站都处于同一广播域中，即网上的所有工作站都能收到广播信息。

路由器通过光纤连接广域网的是（13)。

(13)A.SFP端口 B.同步串行口 C.Console 端口 D.AUX 端口

**【答案】A**

**【解析】本题考查交换设备端口的基础知识。**

路由器与广域网连接的端口称为WAN端口，路由器与局域网连接的端口称为LAN 口。常见的网络端口有以下几种：

• RJ-45端口：这种端口通过双绞线连接以太网。10Base-T的RJ-45端口标识为 “ETH”，而100Base-TX 的RJ-45 端口标识为“10/100bTX”。

•高速同步串口（Synchronous Serial Port)：在路由器与广域网的连接中，应用最多的是高速同步串行口，这种端口用于连接DDN、帧中继、X.25和PSTN等网络。

• ISDN BRI端口：ISDN BRI端口通过ISDN线路实现路由器与Internet或其他网络的远程连接。ISDN BRI端口采用RJ45标准，与ISDN NT1的连接使用 RJ-45-to-RJ-45 直通线。

•异步串口（ASYNC):异步串口主要应用于与Modem或Modem池的连接，以实现远程计算机通过PSTN拨号接入。异步端口的速率不是很高，也不要求同步传输。 .

• Console端口：Console端口通过专用电缆连接至计算机串行口，利用终端仿真程序对路由器进行本地配置。路由器的Console端口为RJ-45端口。

• AUX端口：对路由器进行远程配置时要使用“AUX”端口（Auxiliary Port)。AUX 端口在外观上与RJ45端口一样，只是内部电路不同，实现的功能也不一样。通过AUX端口与Modem进行连接必须借助RJ45 to DB9或RJ45 to DB25适配器进行转换。AUX端口支持硬件流控。

•光纤端口：SC端口（SubscriberConnector)是一种光纤端口，可提供千兆数据传输速率，通常用于连接服务器的光纤网卡。光纤端口一般是两个，一发一收，光纤跳线也必须是两根。

• GBIC端口：GBIC插#用于安装吉比特端口转换器（Giga Bit-rate Interface Converter, GBIC)。GBIC模块是将千兆位电信号转换为光信号的热插拔器件，分为用于级连的GBIC模块和用于堆叠的GBIC模块。

• SFP 端口：小型机架可插拔设备SFP (Small Form-factor Pluggable)是GBIC 的升级版本，其功能基本和GBIC—样，但体积减少一半。

下面关于Manchester编码的叙述中，错误的是（14)。

(14)A.Manchester编码是一种双相码

B.Manchester编码提供了比特同步信息

C.Manchester编码的效率为50%

D.Manchester编码应用在高速以太网中

**【答案】D**

**【解析】本题考查数据编码的基础知识。**

Manchester编码是一种双相码，即码元取正负两个不同的电平，或者说由正负两个不同的码元表示一个比特，这样编码的效率为50%，但是由于每个比特中间都有电平跳变，因而提供了丰富的同步信息。这种编码用在数据速率不太高的以太网中。

差分Manchester编码也是一种双相码，但是区分“0”和“1”的方法不同。Manchester 编码正变负表示“0”，负变正表示“1”，而差分Manchester编码是“0”比特前沿有跳变，“1”比特前沿没有跳变。这种编码用在令牌环网中。

在Manchester和差分Manchester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，如果釆用这类编码方法，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。

设信道釆用2DPSK调制，码元速率为300波特，则最大数据速率为（15) b/s,

(15)A.300 B.600 C.900 D.1200

**【答案】A**

**【解析】本题考查数字调制的基础知识。**

2DPSK是一种差分相位调制技术，利用前后码元之间的相位变化来表示二进制数据，例如传送“1”时载波相位相对于前一码元的相移为71，传送“0”时载波相位相对于前一码元的相移为0。在这种调制方案中，每一码元代表一个比特，由于码元速率为300波特，所以最大数据速率为300b/s。

假设模拟信号的最高频率为6MHz，采样频率必须大于（16)时，才能使得到的样本信号不失真。

(16)A.6MHz B.12MHz C.18MHz D.20MHz

**【答案】B**

**【解析】本题考查脉冲编码调制的基础知识。**

用数字脉冲表示模拟数据的编码方法叫做脉冲编码调制（PCM)。这里要经过采样、量化和编码3个处理步骤：

•采样定理：f≥2fmax(即采样频率要大于2倍的模拟信号频率）。

• •量化等级：根据编码的长度n确定量化等级N,n= log2N。

•数字编码：把量化后的样本值变成对应的二进制代码。

由于模拟信号的频率为6MHz，而采样频率必须大于模拟信号频率的2倍，所以应为12MHz。

在异步通信中，每个字符包含1位起始位、7位数据位、1位奇偶位和2位终止位，每秒钟传送100个字符，则有效数据速率为（17)。

(17)A.500b/s B.700b/s C.770b/s D.1100b/s

**【答案】B**

**【解析】本题考查异步通信的基础知识。**

所谓异步通信就是把一个字符作为同步的单位，字符之间插入同步信息。通常一个字符为7b，加上起始位、奇偶位和2b终止位，共11b，可计算如下：

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wl_10_x_s_17_1.jpg

通过ADSL访问Internet,在用户端通过(18)和ADSL Modem连接PC,在ISP 端通过（19)设备连接因特网。

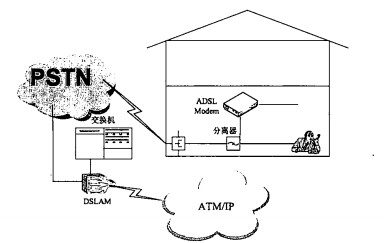
(18)A.分离器 B.电话交换机 C.DSLAM D.IP路由器

(19)A.分离器 B.电话交换机 C.DSLAM D.IP路由器

**【答案】A C**

**【解析】本题考查ADSL接入知识。**

ADSL接入方式分为虚拟拨号和准专线两种。采用虚拟拨号的用户需要安装PPPoE(PPP over Ethernet)或PPPoA (PPP over ATM)客户端软件，以及类似于Modem的拨号程序，输入用户名称和用户密码即可连接到宽带接入站点。采用准专线方式的用户使用电信部门静态或动态分配的IP地址，开机即可接入Internet。



上图表示家庭个人应用的连接线路，PC通过ADSL Modem→分离器→入户接线盒→电话线→DSL接入复用器（DSL Access Multiplexer，DSLAM)连接ATM或IP网络， 而话音线路通过分离器→入户接线盒→电话线→DSL接入复用器接入电话交换机。

IPv4协议头中标识符字段的作用是（20)。

(20)A.指明封装的上层协议 B.表示松散源路由

C.用于分段和重装配 D.表示提供的服务类型

**【答案】C**

**【解析】本题考查IP协议的基础知识。**

IP协议的标识符由主机指定，当源主机对数据分段时，对同一上层协议数据单元划分出的各个数据报指定同样的标识符，目标主机使用这个字段进行重装配。

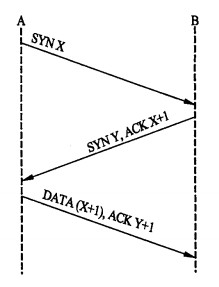
当TCP实体要建立连接时，其段头中的（21)标志置1。

(21)A.SYN B.FIN C.RST D.URG

**【答案】A**

**【解析】本题考查TCP协议的基础知识。**

TCP用三次握手过程建立连接，首先是发起方发送一个SYN标志置位的段，其中的发送顺序号为某个值尤称为初始顺序号（Initial Sequence Number, ISN)，接收方以SYN和ACK标志置位的段响应，其中的应答顺序号应为X+1 (表示期望从第X+1个字节处开始接收数据)，发送顺序号为某个值F (接收端指定的ISN)。这个段到达发起端后，发起端以ACK标志置位，应答顺序号为7+1的段回答，连接就正式建立了，连接建立的同时发起方还可以发送数据，参见下图。



UDP协议在IP层之上提供了（22)能力。

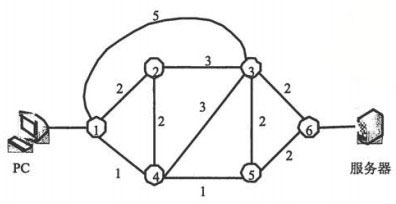
(22)A.连接管理 B.差错校验和重传 C.流量控制 D.端口寻址

**【答案】D**

**【解析】本题考查UDP协议的基础知识。**

用户数据报协议UDP提供无连接的传输服务，由于协议开销少而在很多场合相当实用，特别是网络管理方面，大都使用UDP协议。UDP运行在IP协议层之上，由于它不提供连接，所以只是在IP协议之上加上端口寻址能力。

网络由6个路由器互连而成，路由器之间的链路费用如下图所示，从PC到服务器的最短路径是（23),通路费用是（24)。



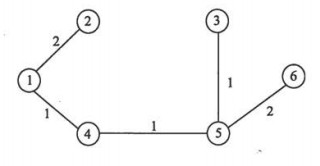
(23)A.1→3→6 B.1→4→5→6 C.1→4→3→6 D.1→2→4→5→6

(24)A.4 B.5 C.2 D.6

**【答案】B A**

**【解析】本题考查最短通路算法的基础知识。**

最短通路更一般的说法是最小费用通路，最小费用通路问题可归结为加权图中的最短通路。通常在实际网络中使用的最短通路算法有Dijkstra算法和Bellman-Ford算法。对本题中的网络采用Dijkstra算法，计算得到下图所示的最小生成树，可见从PC到服务器的最短路径是1→4→5→6，通路费用是4。



RIPv1不支持CIDR,对于运行RIPv1协议的路由器，不能设置的网络地址是（25).

(25)A.10.16.0.0/8 B.172.16.0.0/16

C.172.22.0.0/18 D.192.168.1.0/24

**【答案】C**

**【解析】本题考查路由协议的基础知识。**

路由信息协议RIP的原型最早出现在UNIX Berkley 4.3 BSD中，用于在早期的ARPAnet中计算最佳路由。RIP路由器把自己的路由表广播出去，每个路由器根据邻居发来的路由信息，使用Bellman-Ford的距离矢量路由算法更新自己的路由表。RIP适用于小型网络，因为它允许的跳步数不超过15步。

RIPv1是有类别的协议（classful protocol)，这意味着配置RIPv1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255.255.192.0用于B类网络172.22.0.0。

RIPv2相对RIPv1主要有三方面的改进，其中不包括（26)。

(26)A.使用组播来传播路由更新报文 B.采用了分层的网络结构

C.采用了触发更新机制来加速路由收敛 D.支持可变长子网掩码和路由汇聚

**【答案】B**

**【解析】本题考查路由协议的基础知识。**

RIPv2 (RFC 1721，1722, 1994)是增强了的RIP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，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（triggered update)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，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具有更大的伸缩性。第三，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。

IGRP和EIGRP是Cisco公司开发的路由协议，它们采用的路由度量方法是（27)。

(27)A.以跳步计数表示通路费用

B.链路费用与带宽成反比

C.根据链路负载动态计算通路费用

D.根据带宽、延迟等多种因素来计算通路费用

**【答案】D**

**【解析】本题考查路由协议的基础知识。**

IGRP是Cisco公司开发的路由协议。IGRP不使用跳步数作为路由度量，虽然在一般情况下可以简化为跳步数。IGRP的路由度量因素包括带宽、延迟、可靠性、负载和 MTU,其中前两者是默认的，但是可以通过配置加入其他参数。可靠性和负载划分为1〜 255级，可靠性1是最低的，可靠性255是最高的，负载1使用最少，负载255是百分之百利用的。MTU指最大帧长度，在实际运行中，它是一个常数值，通常采用一条通路中最小的MTU值。这些因素综合起来作为路由费用的度量，使得IGRP可以选择更好的路由。相对于RIP的跳步计数，IGRP协议的路由选择更加合理。

与IGRP —样，EIGRP采用的路由度量（metric)包括带宽、延迟、可靠性、负载等因素，计算方法如下：

metric=[K1X带宽 + (K2X带宽）/ (256-负载）+K3X延迟]+[K5/ (可靠性+K4)]

默认的K值如下：

K1=1 K2=0 K3=1 K4=0 K5=0

当K5为0时，最后的乘数因子被忽略。这样就得到简化的计算公式：

metric=带宽+延迟

计算结果是一个32位的数，是通路中各个链路段延迟之和加上带宽，其中带宽经过了规格化：10的7次方除以源和目标之间最小的带宽乘以256。如果一条路由中各个链路段的传输介质相同，则度量值简化为跳步数。

在进行域名解析的过程中，由（28)获取的解析结果耗时最短。

(28)A.主域名服务器 B.辅域名服务器 C.缓存域名服务器 D.转发域名服务器

**【答案】C**

**【解析】本题考查DNS服务器的解析机制。**

通常由主域名服务器、辅域名服务器、缓存域名服务器、转发域名服务器进行域名解析。主域名服务器负责维护这个区域的所有域名信息，需要从域管理员构造的本地磁盘文件中加载域信息进行解析。辅助域名服务器作为主域名服务器的备份服务器提供域名解析服务。辅助域名服务器从主域名服务器获得授权，有一个所有域信息的完整拷贝，解析时需要访问本地存储文件。缓存域名服务器可运行域名服务器软件，但是没有域名数据库，它从某个远程服务器取得每次域名服务器查询的回答，一旦取得一个答案，就将它放在高速缓存中，以后查询相同的信息时就用它予以回答。转发域名服务器负责所有非本地域名的本地查询，转发域名服务器接到查询请求时，在其缓存中查找，如找不到就把请求依次转发到指定的域名服务器，直到查询到结果为止，否则返回无法映射的结果。

从上述服务器的查询机制中可以看出，缓存域名服务器通过高速缓存的存取进行域名解析，因此获取的解析结果耗时最短。

ftp命令中用来设置客户端当前工作目录的命令是（29)。

(29)A.get B.list C.lcd D.!list

**【答案】C**

**【解析】本题考查考生对ftp命令的掌握程度。**

get或recv的功能是下载远程主机的一个文件到自己的计算机上。

list显示远程计算机上的目录文件和子目录列表。

lcd命令的功能是更改本地计算机上的工作目录。默认情况下，工作目录是启动ftp的目录。

! list命令的功能是从ftp命令行提示符临时退出到Windows命令行提示符下，然后运行list命令。

HTTP协议中，用于读取一个网页的操作方法为（30)。

(30)A.READ B.GET C.HEAD D.POST

**【答案】B**

**【解析】本题考查对HTTP命令的掌握程度。**

GET是HTTP协议提供的少数操作方法中的一种，其含义是读一个网页。

HEAD命令用于读取网页头信息。

POST命令用于把消息加到指定的网页上。不存在READ命令。

在Linux系统中可用Is -a1命令列出文件列表，(31)列出的是一个符号连接文件。(31)A.drwxr-xr-x 2 root root 220 2009-04-14 17:30 doc

B.-rw-r—r— 1 root root 1050 2009-04-14 17:30 doc1

C.lrwxrwxrwx 1 root root 4096 2009-04-14 17:30 profile

D.drwxrwxrwx 4 root root 4096 2009-04-14 17:30 protocols

**【答案】C**

**【解析】本题考查Linux系统下文件属性的基本概念。**

其中符号连接文件的属性用1表示。

Linux系统中，下列关于文件管理命令cp与mv说法正确的是（32)。

(32)A.没有区别 B.mv操作不增加文件个数

C.cp操作不增加文件个数 D.mv操作不删除原有文件 .

**【答案】B**

**【解析】本题考查Linux系统下文件操作命令cp和mv的基本概念。**

其中mv命令是移动文件，不增加文件个数。

Linux系统中，默认安装DHCP服务的配置文件为（33)。

(33)A./etc/dhcpd.conf B./etc/dhcp.conf

C./etc/dhcpd.config D./etc/dhcp.config

**【答案】A**

**【解析】本题考査Linux系统下DHCP服务的配置文件存放位置。**

默认情况下，远程桌面用户组（Remote Desktop Users)成员对终端服务器(34)。

(34)A.具有完全控制权 B.具有用户访问权和来宾访问权

C.仅具有来宾访问权 D.仅具有用户访问权

**【答案】B**

**【解析】本题考査Windows操作系统中远程桌面组用户的默认权限。**

默认情况下，远程桌面用户组成员具有用户访问权和来宾访问权。

Windows Server 2003采用了活动目录（Active Directory)对网络资源进行管理，活动目录需安装在(35)分区:

(35)A.FAT 16 B.FAT32 C.ext2 D.NTFS

**【答案】D**

**【解析】本题考查Windows操作系统活动目录的基本概念。**

活动目录必须安装在NTFS分区。

Linux系统中，（36)服务的作用与Windows的共享文件服务作用相似，提供基于网络的共享文件/打印服务。

(36)A.Samba B.Ftp C.SMTP D.Telnet

**【答案】A**

**【解析】本题考查Linux系统中SAMBA服务的基本概念。**

以下关于DHCP协议的描述中，错误的是（37)。

(37)A.DHCP客户机可以从外网段获取IP地址

B.DHCP客户机只能收到一个dhcpoffer

C.DHCP不会同时租借相同的IP地址给两台主机

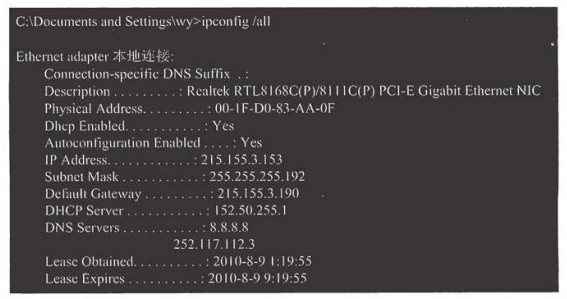
D.DHCP分配的IP地址默认租约期为8天

**【答案】B**

**【解析】本题考查考生对DHCP协议的掌握程度。**

借助中继代理，DHCP客户机可以从外网段获取IP地址；DHCP不会同时租借相同的IP地址给两台主机；默认情况下DHCP分配的IP地址租约期为8天；DHCP客户机可以收到多个dhcpoffer,通常从中选择最先到达的作为本机的IP地址。

在某台PC上运行ipconfig /all命令后得到如下结果，下列说法中错误的是（38)。



(38)A.该PC的IP地址的租约期为8小时

B.该PC访问Web网站时最先査询的DNS服务器为8.8.8.8

C.接口215.155.3.190 和152.50.255.1 之间使用了DHCP 中继代理

D.DHCP服务器152.50.255.1可供分配的IP地址数只能为61

**【答案】D**

**【解析】本题考查考生对本机配置信息的掌握程度。**

IP地址的发放时间为2010-8-9 1:19:55,释放时间为2010-8-9 9:19:55，由此可知该PC的IP地址的租约期为8小时，选项A说法正确。

首选DNS服务器地址为8.8.8.8，由此可知该PC访问Web网站时最先查询的DNS服务器为8.8.8.8,故选项B说法正确。

DHCP服务器地址为152.50.255.1，本机地址为215.155.3.155，和DHCP服务器不属同一网段，因此接口215.155.3.190和152.50.255.1之间使用了 DHCP中继代理，选项C说法正确。

DHCP服务器215.155.3.153/26可供分配的IP地址数为61，但其地址池可以分配多个网段，选项D说法不正确。

在Windows系统中需要重新从DHCP服务器获取IP地址时，可以使用（39) 命令。(39)A.ifconfig -a B.ipconfig C.ipconfig/all D.ipconfig/renew

**【答案】D**

**【解析】本题考查考生对ipconfig命令的运用。**

ipconfig是最常用的Windows实用程序，可以显示所有网卡的TCP/IP配置参数，刷新动态主机配置协议（DHCP)和域名系统（DNS)的设置。

ipconfig/all用于显示所有网卡的TCP/IP配置信息。如果没有该参数，则只显示各个网卡的IP地址、子网掩码和默认网关地址。

ipconfig /renew用于更新网卡的DHCP配置，如果使用标识符Adapter说明了网卡的名字，则只更新指定网卡的配置，否则就更新所有网卡的配置。

IIS 6.0将多个协议结合起来组成一个组件，其中不包括（40)。

(40)A.POP3 B.SMTP C.FTP D.DNS

**【答案】D**

**【解析】本题考查考生对IIS 6.0组件的了解程度。**

可以利用因特网信息服务器（Internet Information Server, IIS)来构建WWW服务器、FTP服务器、SMTP服务器和POP3服务器等。IIS服务将HTTP协议、FTP协议与Windows Server 2000出色的管理功能和安全特性结合起来，提供了一个功能全面的软件包，面向不同的应用领域给出了 Intemet/Intranet服务器解决方案。

按照RSA算法，若选两奇数p=5, q=3,公钥e=7,则私钥d为（41)。

(41)A.6 B.7 C.8 D.9

**【答案】B**

**【解析】本题考查RSA的算法知识。**

RSA是一种公钥加密算法，它按照下面的要求选择公钥和密钥：

1) 选择两个大素数p和9 (大于10100)

2) 令 n=p\*q 和 z=(p-1)\*(q-1)

3) 选择d与z互质

4) 选择e，使 e\*d=1(mod z)

从题中举例数据p=5、q=3、e=7可得：

n=5\*3=15;

z=(5-1)\*(3-1)=8；

7\*d=1(mod 8)；

将题中4个选项代入上式可知，只有d=7满足要求。

在SNMP中，管理进程杳询代理中一个或多个变量的值所用报文名称为（42), 该报文的缺省目标端口是（43)。

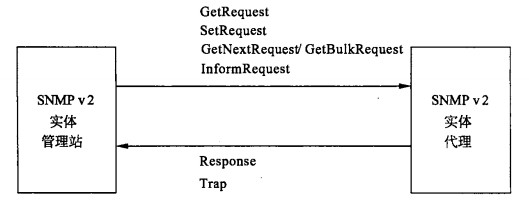
(42)A.get-request B.set-request C.get-response D.trap

(43)A.160 B.161 C.162 D.163

**【答案】A B**

**【解析】本题考查网络管理协议SNMP的基础知识。**

在SNMP管理中，管理站和代理之间交换的管理信息构成了SNMP报文。SNMP报文包括GetRequest、GetNextRequest、GetBulkRequest ( SNMPv2 )、SetRequest、InformRequest (SNMPv2)和Trap、Response,如下图所示。



其中选项（A) get-request可用于管理进程查询代理中一个或多个变量的值。

根据SNMP协议规定（RFC1157)，管理站发送报文的协议为UDP，目的端口为161，代理发送的Trap报文的目的端口为162。所以get-request报文的缺省目的端口是161。

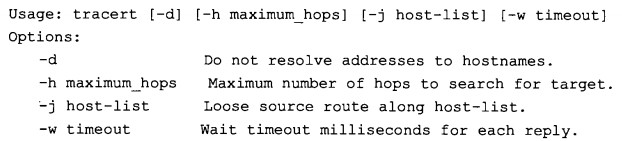
Windows系统中，路由跟踪命令是（44)。

(44)A.tracert B.traceroute C.routetrace D.trace

**【答案】A**

**【解析】本题考査Windows系统中的网络操作命令。**

查询Windows帮助可得以下信息：



报文摘要算法MD5的输出是(45)位，SHA-1的输出是(46)位。

(45)A.56 B.128 C.160 D.168

(46)A.56 B.128 C.160 D.168

**【答案】B C**

**【解析】本题考查网络安全中报文摘要算法的相关知识。**

MD5以512位分组来处理输入的信息，且每一分组又被划分为16个32位子分组，经过了一系列的处理后，算法的输出由4个32位分组组成，将这4个32位分组级联后将生成一个128位散列值。

SHA (安全散列算法）是美国国家安全局设计、美国国家标准与技术研究院（NIST) 发布的一系列密码散列函数。其中SHA-1会从一个最大264位元的信息中产生一串160 位元的摘要。

下列隧道协议中工作在网络层的是（47)。

(47)A.SSL B.L2TP C.IPSec D.PPTP

**【答案】C**

**【解析】本题考查隧道协议的综合知识。**

隧道技术是VPN的基本技术，它在公用网建立一条数据通道（隧道)，让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。

第二层隧道协议是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。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有L2F、PPTP、L2TP等。L2TP协议是目前IETF的标准，由IETF融合PPTP与L2F而形成。

第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有VTP、IPSec (IP Security)等。IPSec由一组RFC文档组成，定义了一个系统来提供安全协议选择、安全算法、确定服务所使用密钥等服务，从而在IP层（网络层）提供安全保障。

IEEE 802.11i所采用的加密算法为（48)。

(48)A.DES B.3DES C.IDEA D.AES

**【答案】D**

**【解析】本题考查加密算法的应用。**

IEEE 802.11i是IEEE为了弥补802.11脆弱的安全加密功能（WEP)而制定的修正案，于2004年7月完成。其中定义了基于AES的全新加密协议CCMP (CTR with CBC-MAC Protocol)。

公钥体系中，私钥用于（49),公钥用于（50)。

(49)A.解密和签名 B.加密和签名 C.解密和认证 D.加密和认证

(50)A.解密和签名 B.加密和签名 C.解密和认证 D.加密和认证

**【答案】A D**

**【解析】本题考查公钥体系的理解和应用。**

1976年斯坦福大学的Diffie和Heilman提出了使用不同的密钥进行加密和解密的公钥加密算法。设P为明文，C为密文，E为公钥控制的加密算法，D为私钥控制的解密算法，这些参数满足下列3个条件：

(1) D (E (P)) =P

(2) 不能由E导出D

(3) 选择明文攻击（选择任意明文-密文对以确定未知的密钥）不能破解E

加密时计算C=E (P),解密时计算P=D (C)。加密和解密是互逆的。用公钥加密、私钥解密，可实现保密通信；用私钥加密、公钥解密，可实现数字签名。

网络 172.21.136.0/24 和 172.21.143.0/24 汇聚后的地址是（51)。

(51)A.172.21.136.0/21 B.172.21.136.0/20

C.172.21.136.0/22 D.172.21.128.0/21

**【答案】A**

**【解析】本题考查IP地址计算的基础知识。**

网络 172.21.136.0/24 的二进制表示为：10101100 00010101 10001000 00000000

网络 192.21.143.0/24 的二进制表示为：10101100 00010101 10001111 00000000

所以汇聚后的地址是：10101100 00010101 10001000 00000000

即172.21.136.0/21。

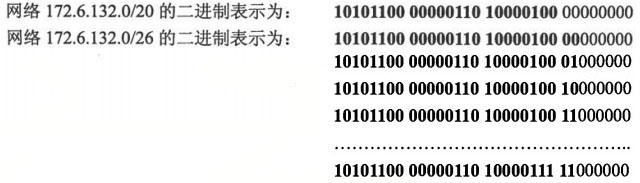
如果子网172.6.32.0/20再划分为172.6.32.0/26,则下面的结论中正确的是（52)。

(52)A.划分为1024个子网 B.每个子网有64台主机

C.每个子网有62台主机 D.划分为2044个子网

**【答案】C**

**【解析】本题考查IP地址计算的基础知识。**



共分成了16个子网，每个子网的主机地址部分有6位。除去全0和全1，有62个主机地址。

下面给出的网络地址中，属于私网地址的是（53)。

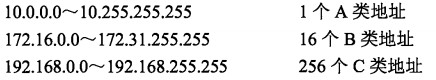
(53)A.119.12.73.214 B.192.32.146.23

C.172.34.221.18 D.10.215.34.124

**【答案】D**

**【解析】本题考查IP地址的基础知识。**

私网地址不能在公网上出现，只能用在内部网络中，所有的路由器都不转发目标地址为私网地址的数据报。下面的地址都是私网地址：



IP 地址 172.17.16.255/23 是一个（54),

(54)A.网络地址 B.主机地址 C.定向广播地址 D.不定向广播地址

**【答案】B**

**【解析】本题考查IP地址的基础知识。**

IP 地址172.17.16.255/23 的二进制表示为:10101100 00010001 00010000 11111111

所以应该是主机地址。

给定一个C类网络192.168.1.0/24,要在其中划分出3个60台主机的网段和2个30 台主机的网段，则采用的子网掩码应该分别为（55)。

(55)A.255.255.255.128 和255.255.255.224

B.255.255.255.128和255.255.255.240

C.255.255.255.192 和255.255.255.224

D.255.255.255.192 和255.255.255.240

**【答案】C**

**【解析】本题考查IP地址计算的基础知识。**

要在网络192.168.1.0/24中划分出3个60台主机的网段和2个30台主机的网段，首先可采用子网掩码255.255.255.192，得到3个子网：



然后采用子网掩码和255.255.255.224，得到两个子网：

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wl_10_x_s_55_2.jpg

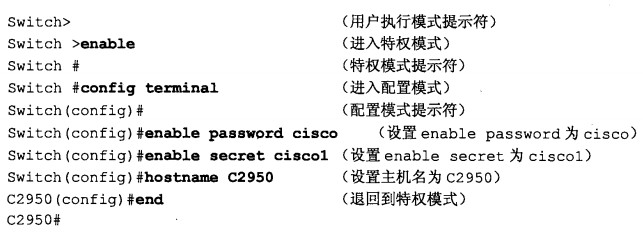
在交换机上同时配置了使能口令（enable password)和使能密码（enable secret),起作用的是（56)。

(56)A.使能口令 B.使能密码 C.两者都不能 D.两者都可以

**【答案】B**

**【解析】本题考查交换机的配置命令。**

在交换机中可以配置使能口令和使能密码，两者的区别是使能口令以明文显示，而使能密码以密文显示。一般只需配置一个就可以了，当两者同时配置时，后者生效，参见下面的例子。



以下的命令中，可以为交换机配置默认网关地址的是（57)。

(57)A.2950(config)# default-gateway 192.168.1.254

B.2950(config-if)# default-gateway 192.168.1.254

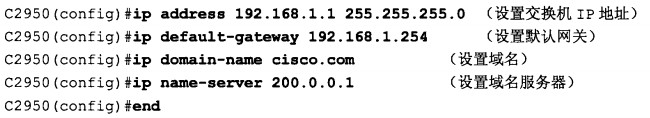
C.2950(config)#ip default-gateway 192.168.1.254

D.2950(config-if)#ip default-gateway 192.168.1.254

**【答案】C**

**【解析】本题考查交换机的配置命令。**

在全局配置模式下可以设置交换机的IP地址、默认网关、域名等信息，这些信息是用来管理交换机的，与连接在交换机上的计算机或其他设备无关，参见下面的例子。

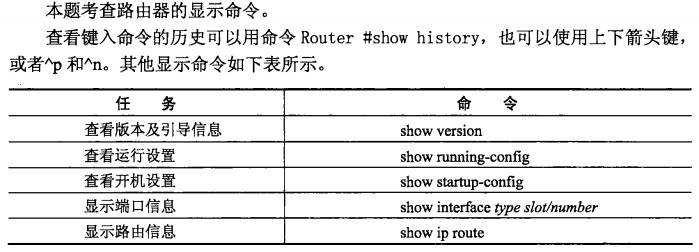


在路由器配置过程中，要查看用户输入的最后几条命令，应该键入（58)。

(58)A.show version B.show commands C.show previous D.show history

**【答案】D**

**【解析】**



在交换机之间的链路中，能够传送多个VLAN数据包的是（59)。

(59)A.中继连接 B.接入链路 C.控制连接 D.分支链路

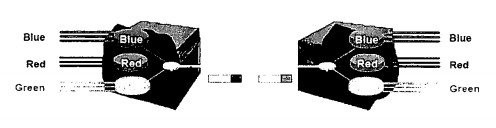
**【答案】A**

**【解析】本题考査VLAN的基础知识。**

在划分成VLAN的交换局域网中，交换机端口之间的连接分为两种：接入链路连接 (Access-Link Connection)和中继连接(Trunk Connection)。接入链路只能连接具有标准以太网卡的设备，只能解释以太帧，也只能传送属于单个VLAN的数据包。任何连接到接入链路的设备都属于同一广播域。

中继连接能够传送多个VLAN的数据包。为了支持中继连接，应该修改原来的以太网数据包，在其中加入VLAN标记，以区分属于不同VLAN的广播域。例如，VLAN1中的设备发出一个广播包，这个广播包在交换网络中传送，所有的交换机都必须识别VLAN1的标识符，以便把该数据包转发到属于VLAN1的端口去。

中继链路是在一条物理连接上生成多个逻辑连接，每个逻辑连接属于一个VLAN。在进入中继端口时，交换机在数据包中加入VLAN标记。这样，在中继链路另一端的交换机不仅根据目标地址进行转发，而且要根据数据包所属的VLAN进行转发决策。下图用不同的颜色表示不同VLAN的帧，这些帧共享一条中继链路。



为了与接入链路设备兼容，在数据包进入接入链路连接的设备时，交换机要删除VLAN标记，恢复原来的帧结构。添加和删除VLAN标记的过程是由交换机中的专用硬件自动实现的。从用户角度看，数据源产生标准的以太帧，目标接收的也是标准的以太帧，VLAN标记对用户是透明的。

通常的PC网卡不支持中继连接，但是也有的网卡支持中继连接。如果一个服务器要接受多个VLAN的访问，并直接连接在交换机上，则应该在服务器中插入支持中继连接的网卡，这种配置比通过路由器转发效率高。

要实现VTP动态修剪，在VTP域中的所有交换机都必须配置成（60)。

(60)A.服务器 B.服务器或客户机 C.透明模式 D.客户机

**【答案】A**

**【解析】本题考查VTP协议的基础知识。**

VLAN 中继协议（VLAN Trunking Protocol, VTP)是Cisco 公司的专利协议。VTP 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VLAN 配置，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)：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)：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。

能进入VLAN配置状态的交换机命令是（61)。

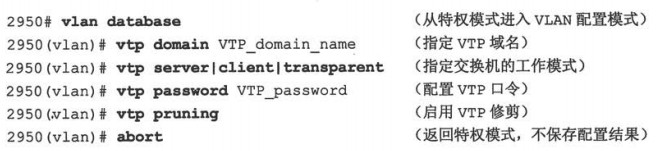
(61)A.2950(config)# vtp pruning B.2950# vlan database

C.2950(config)# vtp server D.2950(config)# vtp mode

**【答案】B**

**【解析】本题考查交换机的配置命令。**

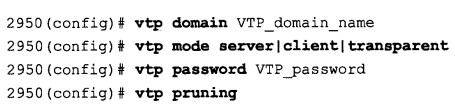
根据IOS版本的不同，2950可以用两种方式配置。在老版本中是从特权模式 (Privilege EXEC)开始配置的，使用下面的命令：



或者

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wl_10_x_s_61_2.jpg

如果使用的是IOS12.1(11)EA1以后的新版本，则从全局配置模式开始：



以太网协议可以采用非坚持型、坚持型和P坚持型3种监听算法。下面关于这3种算法的描述中，正确的是（62) 。

(62)A.坚持型监听算法的冲突概率低，但可能引入过多的信道延迟

B.非坚持型监听算法的冲突概率低，但可能浪费信道带宽

C.P坚持型监听算法实现简单，而且可以达到最好性能

D.非坚持型监听算法可以及时抢占信道，减少发送延迟

**【答案】B**

**【解析】本题考查以太网协议的基础知识。**

以太网监听算法有如下3种：

①非坚持型监听算法：若信道忙，则放弃监听，后退一段随机时间后再试图重新发送。这种方法重新冲突的概率低，但可能引入过多的信道延迟，浪费信道的带宽。

②坚持型监听算法：若信道忙，则继续监听，直到信道空闲就可发送。这种方法发生冲突的概率高，但可以减少发送延迟。

③P坚持型监听算法：若信道忙，则以概率P继续监听，或以概率1-P放弃监听并后退一段随机时间，再试图重新发送。这种方法具有以上两种方法的优点，但是算法复杂，P值的大小对网络的性能有较大影响。

以太网帧格式如下图所示，其中的“长度”字段的作用是（63)。

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wl_10_x_s_63_1.jpg

(63)A.表示数据字段的长度

B.表示封装的上层协议的类型

C.表示整个帧的长度

D.既可以表示数据字段长度也可以表示上层协议的类型

**【答案】D**

**【解析】**

本题考查以太网协议的基础知识。最早采用CSMA/CD协议的网络是Xerox公司的以太网。1981年，DEC、Intel和Xerox三家公司制定了DIX以太网标准，使这一技术得到越来越广泛的应用。IEEE 802委员制定局域网标准时参考了以太网标准，并增加了几种新的传输介质。

早期的802.3帧格式与DIX以太网不同，DIX以太网用类型字段指示所封装的上层协议，而IEEE 802.3为了通过LLC实现向上复用，用长度字段取代了类型字段。实际上，这两种格式可以并存，两个字节可表示的数字值范围是0〜65 535,长度字段的最大值是1500,因此1501〜65 535之间的值都可以用来标识协议类型。事实上，这个字段的1536〜65 535 (0x0600〜OxFFFF)之间的值都被保留作为类型值，而0〜1500则被用作长度的值。许多高层协议（例如TCP/IP、IPX、DECnet4)使用DIX以太网帧格式，而 IEEE 802.3/LLC 在AppleTalk-2 和 NetBIOS 中得到应用。

IEEE802.3x工作组为了支持全双工操作，开发了流量控制算法，这使得帧格式出现了一些变化，新的MAC协议使用类型字段来区分MAC控制帧和其他类型的帧。IEEE 802.3x在1997年2月成为正式标准，使得原来的“以太网使用类型字段而IEEE 802.3 使用长度字段”的差别消失。

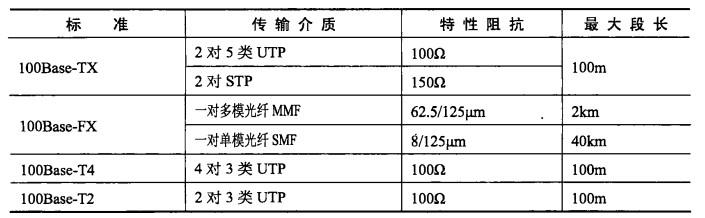
下面列出的4种快速以太网物理层标准中，使用两对5类无屏蔽双绞线作为传输介质的是（64)。

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

**【答案】C**

**【解析】本题考查快速以太网的基础知识。**

1995年100Mb/s的快速以太网标准IEEE 802.3u正式颁布，这是基于10Base-T和10Base-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。



用于工业、科学和医疗方面的免许可证的微波频段有多个，其中世界各国通用的ISM 频段是（65)。

(65)A.902〜928MHz B.868〜915MHz C.5725〜5850MHz D.2400〜2483.5MHz

**【答案】D**

**【解析】本题考査无线通信的基础知识。**

世界各国都划出一些无线频段，用于工业、科学研究和微波医疗方面。应用这些频段无需许可证，只要低于一定的发射功率（一般为1w)即可自由使用。美国有3个ISM 频段（902〜928MHz、2400〜2483.5MHz、5725〜5850MHz)，2.4GHz 为各国共同的ISM 频段。频谱越高，潜在的带宽也越大。另外，还要考虑可能出现的干扰。有些设备（例如无绳电话、无线麦克、业余电台等）的工作频率为900MHz。还有些设备运行在2.4GHz 上，典型的例子就是微波炉，它使用久了会泄露更多的射线。目前看来，在5.8GHz频带上还没有什么竞争。但是频谱越高，设备的价格就越贵。

2009年发布的（66)标准可以将WLAN的传输速率由54Mb/s提高到300〜600Mb/S。

(66)A.IEEE 802.11n B.IEEE 802.11a C.IEEE 802.11b D.IEEE 802.11g

**【答案】A**

**【解析】本题考査WLAN的基础知识。**

自从1997年IEEE 802.11标准实施以来，先后有二十多个标准出台，其中802.11a、802.11b和802.11g采用了不同的通信技术，使得数据传输速率不断提升，但是与有线网络相比仍然存在一定差距。随着2009年9月11日IEEE802.11n标准的正式发布，这一差距正在缩小，有望使得一些杀手级的应用能够在WLAN平台上畅行无阻。

802.11n可以将WLAN的传输速率由目前802.11a/802.11g的54Mb/s提高到 300Mb/s,甚至600Mb/s。这个成就主要得益于MIMO与OFDM技术的结合。应用先进的无线通信技术，不但提高了传输速率，也极大地提升了传输质量。

网络系统生命周期可以划分为5个阶段，实施这5个阶段的合理顺序是（67)。

(67)A.需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段

B.需求规范、逻辑网络设计、通信规范、物理网络设计、实施阶段

C.通信规范、物理网络设计、需求规范、逻辑网络设计、实施阶段

D.通信规范、需求规范、逻辑网络设计、物理网络设计、实施阶段

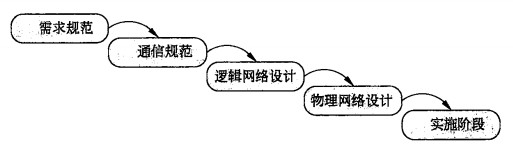
**【答案】A**

**【解析】本题考查网络规划和设计方面的基础知识。**

一个网络系统从构思开始，到最后被淘汰的过程称为网络生命周期。一般来说，网络生命周期至少应包括网络系统的构思和计划、分析和设计、运行和维护的全过程。网络系统的生命周期与软件工程中的软件生命周期类似，首先它是一个循环迭代的过程，每次循环迭代的动力都来自网络应用需求的变更。其次，每次循环过程中，都存在需求分析、规划设计、实施调试和运营维护等多个阶段。一般来说，网络规模越大，则可能经历的循环周期也越长。

每一个迭代周期都是网络重构的过程，不同的网络设计方法，对迭代周期的划分方式是不同的，拥有不同的网络文档模板，但是实施后的效果都满足了用户的网络需求。常见的迭代周期构成可分为如下5个阶段：需求规范阶段、通信规范阶段、逻辑网络设计阶段、物理网络设计阶段及实施阶段。

在这5个阶段中，每个阶段都是一个工作环节，每个环节完毕后才能进入下一个环节，类似于软件工程中的“瀑布模型”，形成了特定的工作流程。如下图所示。



按照这种流程构建网络，在下一个阶段开始之前，前一阶段的工作已经完成，一般情况下，不允许返回到前面的阶段。

大型局域网通常划分为核心层、汇聚层和接入层，以下关于各个网络层次的描述中，不正确的是（68)。

(68)A.核心层承担访问控制列表检查 B.汇聚层定义了网络的访问策略

C.接入层提供局域网络接入功能 D.接入层可以使用集线器代替交换机

**【答案】A**

**【解析】本题考査局域网体系结构的基础知识。**

大型局域网的层次结构是将局域网络划分成不同的功能层次，例如划分成核心层、 汇聚层和接入层，通过与核心设备互连的路由器接入广域网。

在三层模型中，核心层提供不同区域之间的髙速连接和最优传输路径，汇聚层提供网络业务接入，并实现与安全、流量和路由相关的控制策略，接入层为终端用户提供接入服务。

网络系统设计过程中，逻辑网络设计阶段的任务是（69) 。

(69)A.依据逻辑网络设计的要求，确定设备的物理分布和运行环境

B.分析现有网络和新网络的资源分布，掌握网络的运行状态

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，设计出符合用户需求的网络

**【答案】C**

**【解析】本题考查网络规划和设计的基础知识。**

网络逻辑设计阶段要根据网络用户的分类和分布，选择特定的技术，形成特定的网络结构。网络逻辑结构大致描述了设备的互联及分布情况，但是并不涉及具体的物理位置和运行环境。逻辑设计过程主要由确定逻辑设计目标、网络服务评价、技术选项评价及进行技术决策4个步骤组成。

逻辑网络设计工作主要包括网络结构的设计、物理层技术选择、局域网技术选择与应用、广域网技术选择与应用、地址设计和命名模型、路由选择协议、网络管理和网络安全等内容。

利用SDH实现广域网互联，如果用户需要的数据传输速率较小，可以用准同步数 字系列（PDH)兼容的传输方式在每个STM-1帧中封装（70)个E1信道。

(70)A.4 B.63 C.255 D.1023

**【答案】B**

**【解析】本题考查SDH接入的基础知识。**

同步数字系列（Synchronous Digital Hierarchy, SDH)是一种将复接、线路传输及交换功能融为一体的物理传输网络。SDH不是一种协议，也不是一种传输介质，而是一种传输技术。SDH网络主要使用光纤通信技术，但也可以使用微波和卫星传送。SDH 可以对网络实现有效的管理、提供实时业务监控、动态网络维护、不同厂商设备间的互 通等多项功能，能大大提高网络资源利用率，降低网络管理及维护的费用，是运营商主要的基础设施网络。

SDH采用的信息结构等级称为同步传送模块STM-N (N=1，4，16, 64等），最基本的模块为STM-1 (155.520Mb/s), 4 个STM-1 同步复用构成 STM-4 (622.080Mb/s), 16 个STM-1 同步复用构成STM-16 (2488.320Mb/s)„

如果用户需要的数据传输速率较小，则SDH还可以提供准同步数字系列 (Plesiochronous Digital Hierarchy, PDH)兼容的传输方式。这种方式在STM-1中封装了 63个E1信道，可以同时向63个用户提供2Mb/s的接入速率。PDH兼容方式提供两种接口，一是传统的E1接口，例如路由器上的G703转V.35接口；另一种是封装了多个E1信道的CPOS (Channel P0S)接口；路由器通过一个CP0S接口接入SDH网络，并通过封装的多个E1信道连接多个远程站点。

The metric assigned to each network depends on the type of protocol. Some simple protocol, like RIP, treats each network as equals. The (71) of passing through each network is the same; it is one (72) count. So if a packet passes through 10 network to reach the destination, the total cost is 10 hop counts. Other protocols, such as OSPF, allow the administrator to assign a cost for passing through a network based on the type of service required. A (73) through a network can have different costs (metrics). For example, if maximum (74) is the desired type of service, a satellite link has a lower metric than a fiber-optic line. On the other hand, if minimum (75) is the desired type of service, a fiber-optic line has a lower metric than a satellite line. OSPF allow each router to have several routing table based on the required type of service.

(71)A.number B.connection C.diagram D.cost

(72)A.process B.hop C.route D.flow

(73)A.flow B.window C.route D.cost

(74)A.packet B.throughput C.error D.number

(75)A.delay B.stream C.packet D.cost

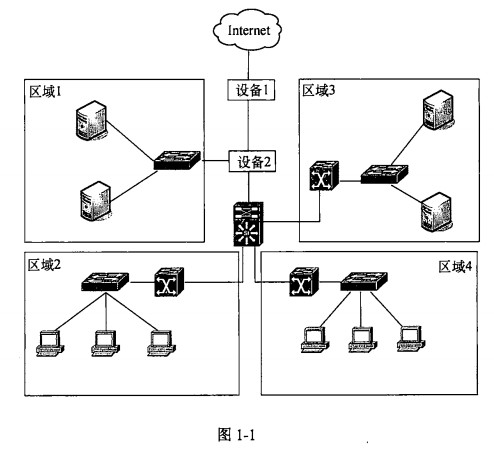
**【答案】D B C B A**

**【解析】**

赋予每一个网络的路由度量依赖于协议的类型。对于像RIP这样的简单协议，可以认为每个网络都是相同的，因而通过每一个网络的费用也都是相同的，其费用为1。所以，如果一个分组经过10个网络到达目标，则总的费用就是10跳。其他的协议，例如OSPF,允许网络管理员根据要求的服务类型赋予所通过的网络一个度量值。通过一个网络的路由可以具有不同的费用。例如，若期望的服务类型为最大吞吐率，则卫星链路比光纤线路的费用低。而如果期望的服务类型为最小延迟，则光纤线路比卫星线路的费用低。OSPF协议允许每一个路由器根据需要的服务类型设置几个不同的路由表。

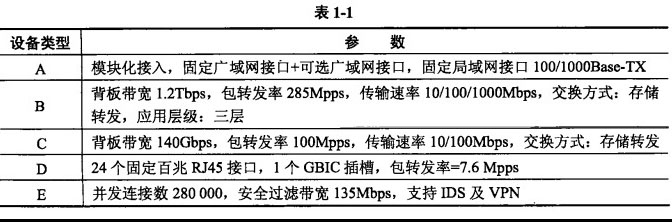
**试题一**

某企业网拓扑结构如图1-1所示。



**【问题1】**

企业根据网络需求购置了如下设备，其基本参数如表1-1所示。



根据网络需求、拓扑图和设备参数类型，图1-1中设备1应选择类型为（1）的设备，设备2应选择类型为（2）的设备。

（1）A

（2）E

主要考查对网络设备选型的了解和应用。从拓扑结构可以看出，设备1是路由设备，设备2是防火墙设备。

**【问题2】**

该网络采用核心层、汇聚层、接入层的三层架构，所有计算机都采用静态IP地址。为了防止恶意用户盗用IP地址，网管员可采用 （3） 的策略来防止IP地址盗用，该策略应在三层架构中的 （4） 层实施。 企业架设Web服务器对外进行公司及产品宣传，同时企业内部需架设数据库服务器存放商业机密数据，则Web服务器应放置在图1-1中的区域 （5） ，数据库服务器应放置在区域 （6） 。

（3）MAC地址与IP地址绑定

（4）接入层

（5）1

（6）3

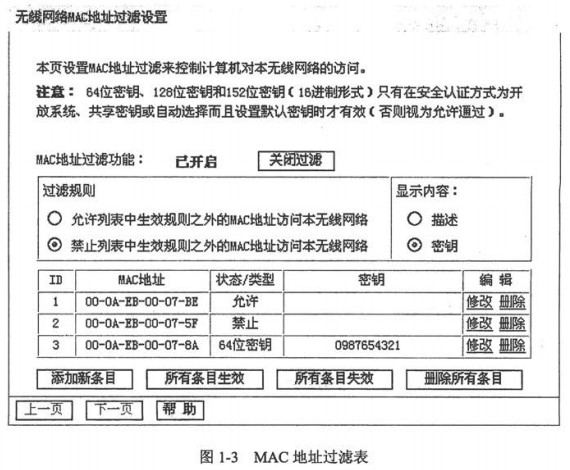
主要考查网络拓扑的三层结构基本概念及网络设备的放置位置。为了防止用户恶意盗用IP地址，网络管理人员可采用IP地址与MAC地址绑定的策略，同时该策略的实施应该在接入层实施。

从拓扑结构可以看出，区域1数据可供外部访问，而区域3是企业内部区，因此Web服务器可放置在区域1，而数据库应放置在区域3。

**【问题3】**

若网络管理员决定在企业内部增加WLAN接入功能，无线路由器基本参数设置如图1-2所示。





网络管理员决定在无线AP上开启MAC地址过滤功能，若该AP的MAC地址过滤表如图1-3所示，则下面说法正确的是（7）。

A．MAC地址为“00-OA-EB-00-07-5F”的主机可以访问AP

B．MAC地址为“00-OA-EB-00-07-8A”的主机可以使用64位WEP密钥“1234567890”来访问AP

C．MAC地址为“00-OA-EB-00-07-8A”的主机可以使用64位WEP密钥“0987654321”来访问AP

D．其它主机均可以访问本无线网络AP

若将MAC地址过滤规则设为“允许列表中生效规则之外的MAC地址访问本无线网络”，则下面说法正确的是 （8）。

A．MAC地址为“00-OA-EB-00-07-5F”的主机可以访问AP

B．MAC地址为“00-OC-EC-00-08-5F”的主机可以访问AP，不需要输入WEP密码

C．MAC地址为“00-OC-EC-00-08-5F”的主机可以访问AP，需使用64位WEP密码 “0123456789”

D．MAC地址为“00-OA-EB-00-07-8A”的主机可以访问AP，不需要输入WEP密码

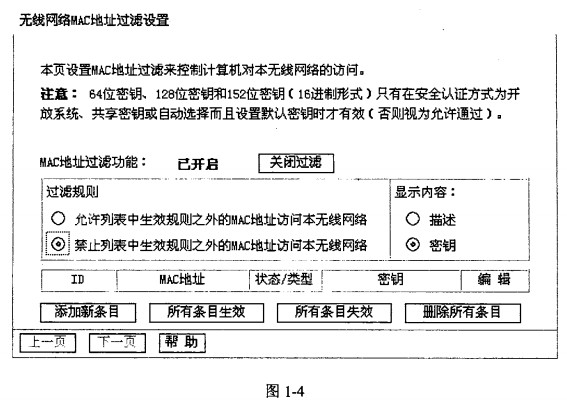
(7) C. MAC地址为“00-0A-EB-00-07-8A”的主机可以使用64位WEP密钥“0987654321” 来访问AP。

(8) C. MAC地址为“00-0C-EC-00-08-5F”的主机可以访问AP，需使用64位WEP 密码“1234567890”。

主要考查WLAN的基本安全设置，从图中可以看出，MAC地址为“00-0A-EB-00-07-8A”的主机可以使用64位WEP密钥“0987654321 ”来访问AP。而MAC 地址为“00-0C-EC-00-08-5F”的主机可以访问AP，需使用64位WEP密码“0123456789”。

**【问题4】**

若MAC地址过滤规则如图1-4所示，MAC地址为“00-OA-EB-00-07-5F”的主机能访问该AP吗？请说明原因。



（9）不能。MAC地址过滤功能已开启，并设置过滤规则为“禁止列表中生效规则之外的MAC地址访问本无线网络”。由于MAC地址为“00-OA-EB-00-07-5F”的主机在列表中没有任何说明，因此自然是不能访问AP的。

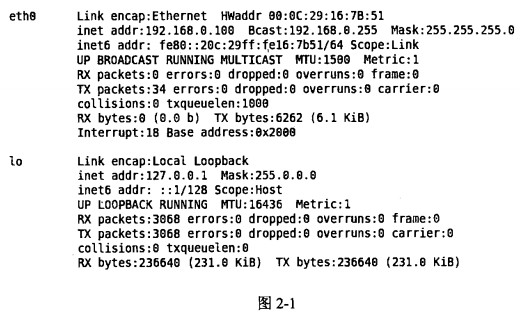
主要考査WLAN中的MAC地址过滤规则的使用方法，由于过滤规则为“禁止列表中生效规则之外的MAC地址访问本无线网络”，过滤列表中又没有任何生效的条目，所以任何主机都不能访问该无线网络。

**试题二**

在Linux操作系统中，TCP/IP网络可通过若干文本文件及命令进行配置。

**【问题1】**

在Linux操作系统下，可通过命令 （1） 获得如图2-1所示的网络配置参数。



（1）备选答案： A．netconf B．ifconf C．netconfig D．ifconfig

（1）D

主要考查对ifconfig命令的了解程度。

**【问题2】**

在Linux操作系统下，可通过命令 （2）显示路由信息。若主机所在网络的网关IP地址为192.168.0.254,则可使用命令 （3）add default （4）192.168.0.254添加网关为默认路由。

（2）备选答案： A．netstat -nr B．Is route C．Ifconfig D．netconfig

（3）备选答案： A．route B．netstat C．ifconf D．ifconfig

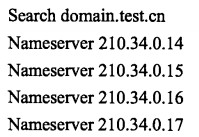
（4）备选答案： A．gateway B．gw C．gate D．g

（2）A（3）A（4）B

主要考査路由信息的查看命令和默认路由的添加命令。在Linux操作系统下，可通过netstat -nr显示路由信息。可以使用route命令对路由表进行操作。

**【问题3】**

在Linux系统中，DNS查询文件内容如下所示，该文件的默认存储位置为 （5），当用户做DNS查询时，首选DNS服务器的IP地址为 （6）。



（5）备选答案： A．/etc/inet.conf B．/etc/resolv.conf C．/etc/inetd.conf D．/etc/net.conf

（6）备选答案： A．210.34.0.14 B．210.34.0.15 C．210.34.0.16 D．210.34.0.17

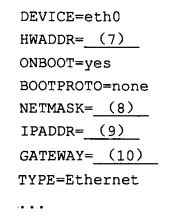
（5）B

（6）A

主要考査DNS的配置，其中DNS査询文件默认存储位置为/etc/resolv.conf，从该文件可以看出，首选DNS服务器为210.34.0.14。

**【问题4】**

文件/etc/sysconfig/network-scripts/eth0用于存储网络配置信息，请根据图2-1填写下面的空缺信息，完成主机的配置。



（7）00:0C:29:16:7B:51

（8）255.255.255.0

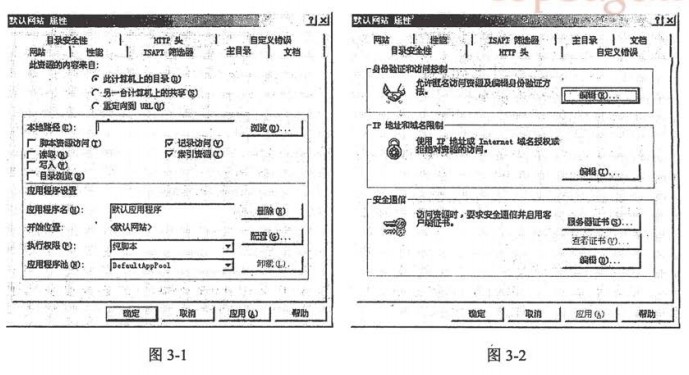
（9）192.168.0.100

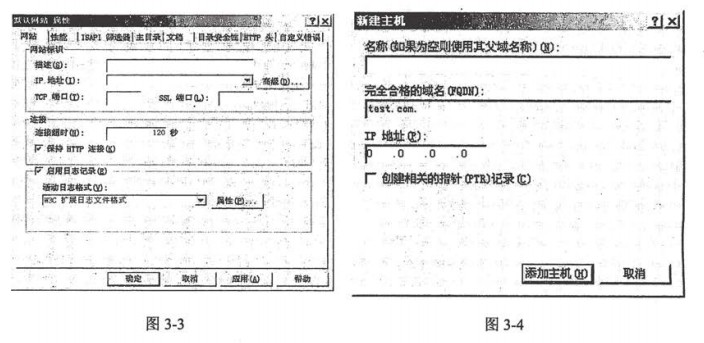
（10）192.168.0.254（该网关并不在图上）

考查对文本方式下网络配置的掌握程度。HWADDR是MAC地址信息，NETMASK 是网络掩码信息，IPADDR为IP地址，GATEWAY为网关IP地址。

**试题三**

某公司采用Windows Server 2003操作系统构建了一个企业网站，要求用户输入https://www.test.com访问该网站。该服务器同时又配置了FTP服务，域名为ftp.test.com。在IIS6.0安装完成后，网站的属性窗口“主目录”选项卡、“目录安全性”以及“网站”选项卡分别如图3-1、图3-2和图3-3所示。





Web服务器安装完成后，需要在DNS服务器中添加记录，为Web服务器建立的正向搜索区域记录如图3-4所示。

**【问题1】**

为了让用户能够查看网站文件夹中的内容，在图3-1中应勾选 （1） 。

（1）目录浏览

在“主目录”选项卡中，有“脚本资源访问”、“读取”、“写入”、“目录浏览”、“记录访问”、“索引资源”等选项，其中“脚本资源访问”选项允许用户读取网站的脚本原文件，“读取”选项允许用户访问.网站资源，“写入”选项允许的权限实际上是对HTTP PUT指令的处理，对于普通网站，一般情况下这个权限是不打开的。“目录浏览”则允许用户能够查看网站文件夹中的内容，故正确答案为勾选“目录浏览”。

**【问题2】**

为了配置安全的Web网站，在图3-2中需点击安全通信中的“服务器证书”按钮来获取服务器证书。获取服务器证书共有以下4个步骤，正确的排序为 （2）。

A．生成证书请求文件

B．在IIS服务器上导入并安装证书

C．从CA导出证书文件

D．CA颁发证书

（2）ADCB

服务器证书的获取过程通常是先在本地生成证书文件，提交后由CA颁发证书，收到证书文件后从CA导出文件，最后在IIS服务器上导入并安装证书。

**【问题3】**

默认情况下，图3-3中“SSL端口”应填入 （3）。

（3）443

SSL的默认端口为443。

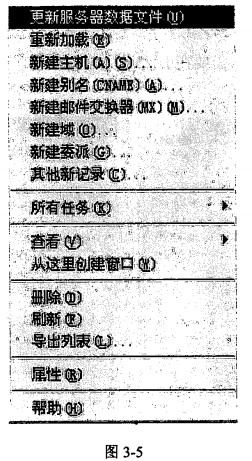
**【问题4】**

在图3-4中，“名称”栏中应输入 （4）。

（4）备选答案：

A．https.www B．www C．https D．index

在如图3-5所示的下拉菜单中点击 （5）可为ftp.test.com建立正向搜索区域记录。



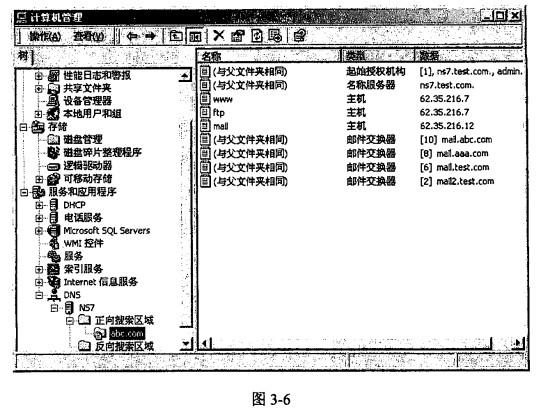
（4）B

（5）“新建主机（A）”

DNS记录中，www.test.com的主机名为www,故“名称”栏中应输入www,选B。采用“新建主机”或“新建别名”均能为ftp.test.com建立正向搜索区域记录。

**【问题5】**

该DNS服务器配置的记录如图3-6所示。



邮件交换器中优先级别最高的是（6） ；

A．[10]mail.abc.com

B．[8]mail.aaa.com

C．[6]mail.test.com

D．[2]mail2.test.com

在客户端可以通过 （7） 来测试到Web网站的连通性。

A．ping 62.35.216.12

B．ping 62.35.216.7

C．ping mail.test.com

D．ping ns7.test.com

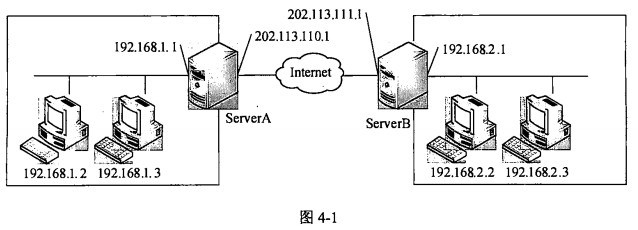
（6）D

（7）B

邮件交换器中优先级别最高的是[2]mail2.test.com。从图3-6中可以看出，62.35.216.7 同时配置了Web和ftp服务，故可采用ping 62.35.216.7命令来测试到Web网站的连通性。

**试题四**

某企业在公司总部和分部之间采用两台Windows Server 2003服务器部署企业IPSec VPN，将总部和分部的两个子网通过Internet互联，如图4-1所示。



**【问题1】**

隧道技术是VPN的基本技术，隧道是由隧道协议形成的，常见隧道协议有IPSec，PPTP 和L2TP，其中（1） 和 （2） 属于第二层隧道协议， （3） 属于第三层隧道协议。

（1）PPTP

（2）L2TP [说明]（1）和（2）答案可调换

（3）IPSec

本问题考查VPN隧道技术的基本概念。

隧道技术是VPN的基本技术，它在公用网建立一条数据通道（隧道)，让数据包通过这条隧道传输。隧道是由隧道协议形成的，分为第二、三层隧道协议。第二层隧道协议是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。这种双层封装方法形成的数据包靠第二层协议进行传输。第二层隧道协议有L2F、PPTP、L2TP等。L2TP协议是目前IETF的标准，由IETF融合PPTP与L2F而形成。第三层隧道协议是把各种网络协议直接装入隧道协议中，形成的数据包依靠第三层协议进行传输。第三层隧道协议有VTP、IPSec等。

**【问题2】**

IPSec安全体系结构包括AH, ESP和ISA KMP/Oakley等协议。其中， （4）为IP包提供信息源验证和报文完整性验证，但不支持加密服务； （5）提供加密服务；（6）提供密钥管理服务。

（4）AH

（5）ESP

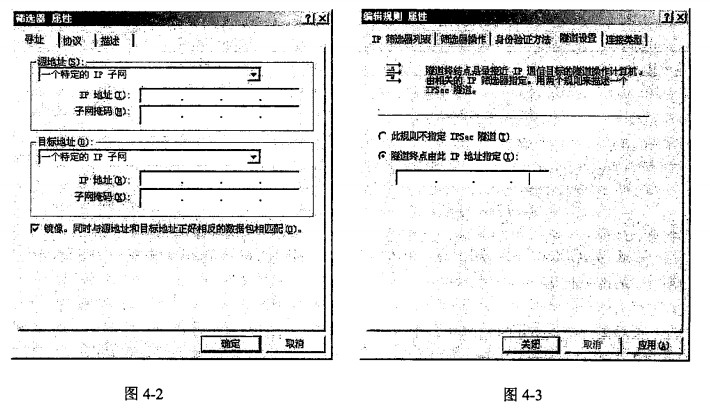
（6）ISA KMP/Oakley

本问题考査IPSec的基本概念。

IPSec安全体系结构包括AH、ESP和ISAKMP/Oakley等协议。IPSec认证头提供了数据完整性和数据源认证，但是不提供保密服务。AH包含了对称密钥的散列函数，使得第三方无法修改传输中的数据。IPSec封装安全负荷（ESP)提供了数据加密功能。ESP 利用对称密钥对IP数据（例如TCP包）进行加密。IPSec传送认证或加密的数据之前，必须就协议、加密算法和使用的密钥进行协商。密钥交换协议IKE提供这个功能，并且在密钥交换之前还要对远程系统进行初始的认证。IKE实际上是3个协议ISAKMP (Internet Security Association and Key Management Protocol)、Oakley 和SKEME( Versatile Secure Key Exchange Mechanism for Internet protocol)的混合体。

**【问题3】**

设置ServerA和ServerB之间通信的筛选器属性界面如图4-2所示，在ServerA的IPSec安全策略配置过程中，当源地址和目标地址均设置为“一个特定的IP子网”时，源子网IP地址应设为（7），目标子网IP地址应设为 （8） 。图4-3所示的隧道设置中的隧道终点IP地址应设为 （9）。



（7）192.168.1.0

（8）192.168.2.0

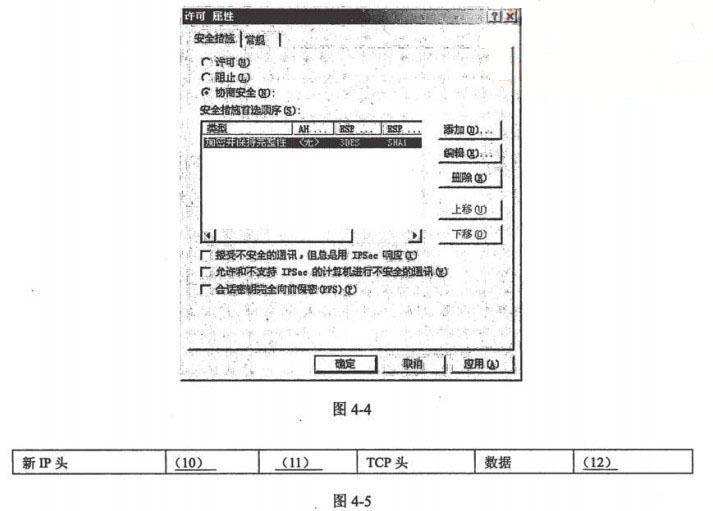
（9）202.113.111.1

本问题考查Windows中IPSec的配置。

在ServerA上配置IPSec的过程中，筛选器的源子网地址应该是ServerA连接的内部子网192.168.1.1/32，目标子网地址应该是ServerB连接的内部子网192.168.1.2/32,在 图4-2中用源IP地址1921.68.1.0代表源子网，目标IP地址192.168.2.0代表目标子网。 图4-3中的隧道终点IP地址应设为ServerB的入口地址202.113.111.1。

**【问题4】**

在ServerA的IPSec安全策略配置过程中，ServerA和ServerB-之间通信的IPSec筛选器“许可”属性设置为“协商安全”，并且安全措施为“加密并保持完整性”，如图4-4所示。根据上述安全策略填写图4-5中的空格，表示完整的IPSec数据包格式。



（10）-（12）备选答案： A．AH头 B．ESP头 C．旧IP头 D．新TCP头 E．AH尾 F．ESP尾 G．旧IP尾 H．新TCP尾

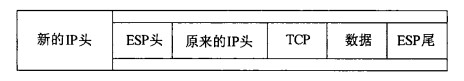
（10）B

（11）C

（12）F

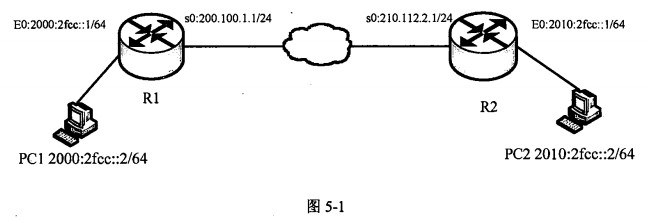
本问题考查IPSec的综合知识。

在ServerA的IPSec安全策略配置过程中，ServerA和ServerB之间通信的IPSec筛 选器“许可”属性设置为“协商安全”，并且安全措施为“加密并保持完整性”，而支持“加密并保持完整性”提示了 ServerA和ServerB之间的IPSec通信只能采用ESP协议。而公司总部和分部之间的VPN采用隧道模式通信，所以IPSec数据包的格式就是ESP 的隧道模式，该模式的数据包可以表示为下图。



**试题五**

某单位的两个分支机构各有1台采用IM的主机，计划采用IPv6-over-IPv4 GRE隧道技术实现两个分支机构的IM主机通信，其网络拓扑结构如图5-1所示。



**【问题1】**

使用IPv6-over-IPv4 GRE隧道技术，可在IPv4的GRE隧道上承载IM数据报文。此时（1）作为乘客协议，（2）作为承载协议。

（1）IPv6

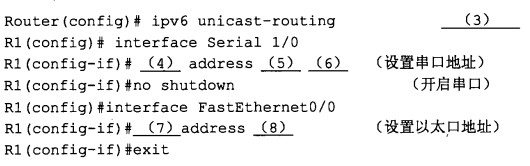
（2）IPv4

本问题考查IPv6-over-IPv4GRE隧道的基本概念。

IPv6-over-IPv4隧道是将IPv6报文封装在IPv4报文中，让IPv6数据包穿过IPv4网络进行通信。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。險道技术只要求在隧道的入口和出口处进行修改，对其他部分没有要求，容易实现。但是，隧道技术不能实现IPv4主机与IPv6 主机的直接通信。使用标准的GRE隧道技术，可在IPv4的GRE隧道上承载IPv6数据报文。GRE隧道是两点之间的连路，每条连路都是一条单独的隧道。GRE隧道把IPv6作为乘客协议，将GRE作为承载协议。所配置的IPv6地址是在Tunnel接口上配置的，而所配置的IPv4 地址是Tunnel的源地址和目的地址（隧道的起点和终点）。

**【问题2】**

根据网络拓扑和需求说明，完成（或解释）路由器R1的配置。



（3）启动IPv6单播路由配置

（4）ip

（5）200.100.1.1

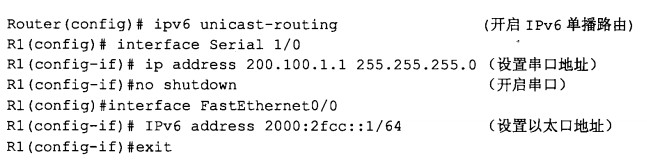
（6）255.255.255.0

（7）ipv6

（8）2000:2fcc::1/64

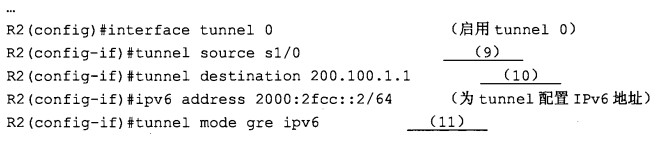
本问题考查路由器接口地址的基本配置操作。

根据题目的拓扑结构图可知，路由器R1的S0口地址为：200.100.1.1/24; E0 口地址为：2000:2fcc::l/64,所以配置命令如下。

b

**【问题3】**

根据网络拓扑和需求说明，解释路由器R2的GRE隧道配置。



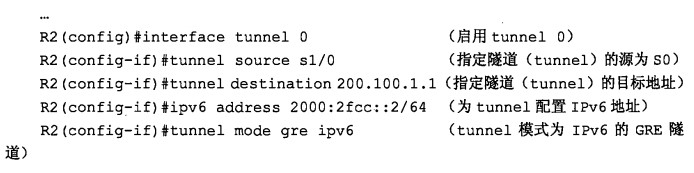
（9）设置隧道源端口为s1/0

（10）设置隧道目标地址为200.100.1.1

（11）设置IPv6隧道封装模式为GRE

本问题考查GRE隧道基本配置操作。

根据网络拓扑和需求说明，路由器R2的GRE隧道配置如下：



**【问题4】**

IPv6主机PC1的IP地址为2000:2fcc::2/64,在这种配置环境下，其网关地址应为 （12）。

（12）2000:2fcc::1/64

本问题考查使用IPv6-over-IPv4 GRE隧道时，使用IPv6的PC上的基本配置操作。IPv6主机PC1的IP地址为2000:2fcc::2/64,根据网络拓扑图可知，其网关地址应为路由器R1 的E0口地址2000:2fcc:: 1/64。