计算机指令一般包括操作码和地址码两部分，为分析执行一条指令，其(1)。

(1)A.操作码应存入指令寄存器（IR)，地址码应存入程序计数器（PC)

B.操作码应存入程序计数器（PC)，地址码应存入指令寄存器（IR)

C.操作码和地址码都应存入指令寄存器（IR)

D.操作码和地址码都应存入程序计数器（PC)

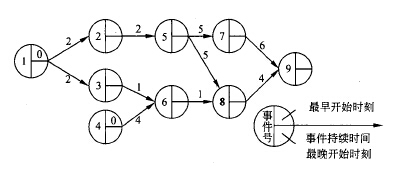
**【答案】C**

**【解析】本题考查指令系统基础知识。**

程序被加载到内存后开始运行，当CPU执行一条指令时，先把它从内存储器取到缓冲寄存器DR中，再送入IR暂存，指令译码器根据IR的内容产生各种微操作指令，控制其他的组成部件工作，完成所需的功能。

程序计数器（PC)具有寄存信息和计数两种功能，又称为指令计数器。程序的执行分两种情况，一是顺序执行，二是转移执行。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来执行的，所以修改的过程通常只是简单的对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地址得到。

进度安排的常用图形描述方法有Gantt图和PERT图。Gantt图不能清晰地描述(2)； PERT图可以给出哪些任务完成后才能开始另一些任务。下图所示的PERT图中，事件6的最晚开始时刻是（3）。



(2)A.每个任务从何时开始 B.每个任务到何时结束

C.每个任务的进展情况 D.各任务之间的依赖关系

(3)A.0 B.3 C.10 D.11

**【答案】D C**

**【解析】本题考查软件项目计划知识。**

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。

图中任务流1→2→5→7→9的持续时间是15，1→2→5→8→9的持续时间是13，1→3→6→8→9的持续时间是8, 4→6→8→9的持续时间为9。所以项目关键路径长度为15。事件6在非关键路径上，其后的任务需要时间为5,所以最晚开始时间=15-5=10。

使用白盒测试方法时，应根据（4）和指定的覆盖标准确定测试数据。

(4)A.程序的内部逻辑 B.程序结构的复杂性

C.使用说明书 D.程序的功能

**【答案】A**

**【解析】本题考查软件测试方法中白盒测试的基础知识。**

白盒测试也称为结构测试，根据程序的内部结构和逻辑来设计测试用例，对程序的执行路径和过程进行测试，检查是否满足设计的需要。白盒测试常用的技术涉及不同覆盖标准，在测试时需根据指定的覆盖标准确定测试数据。

若某整数的16位补码为FFFFH (H表示十六进制），则该数的十进制值为（5)。

(5)A.0 B.-1 C.216-1 D.-216+1

**【答案】B**

**【解析】本题考查数据表示基础知识。**

根据补码定义，数值X的补码记作[X]补，如果机器字长为n,则最高位为符号位，0表示正号，1表示负号，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。

16位补码能表示的数据范围为[-215, 215, -1]。对于整数(216-1)和(-216+1), 数据表示需要16位，再加一个符号位，共17位，因此不在其16位补码能表示的数据范围之内。

在补码表示中，0有唯一的编码：[+0]补=0 000000000000000， [-0] 补= 0000000000000000,即0000H。

[-1]原=1 00000000000000 , [-1]反=1111111111111110,因此-1 的补码为[-1]补 =111111111111111 =FFFF。

若在系统中有若干个互斥资源R, 6个并发进程，每个进程都需要2个资源R，那么使系统不发生死锁的资源R的最少数目为（6)。

(6)A. 6 B.7 C.9 D.12

**【答案】B**

**【解析】**

对于选项A，操作系统为每个进程分配1个资源R后，若这6个进程再分别请求1个资源R时系统已无可供分配的资源R，则这6个进程由于请求的资源R得不到满足而死锁。对于选项B,操作系统为每个进程分配1个资源R后，系统还有1个可供分配的资源R，能满足其中的1个进程的资源R要求并运行完毕释放占有的资源R，从而使其他进程也能得到所需的资源R并运行完毕。

软件设计时需要遵循抽象、模块化、信息隐蔽和模块独立原则。在划分软件系统模块时，应尽量做到（7)。

(7)A.高内聚高耦合 B.高内聚低耦合 C.低内聚高耦合 D.低内聚低耦合

**【答案】B**

**【解析】本题考查软件设计原则的基础知识。**

软件设计时需要遵循抽象、模块化、信息隐蔽和模块独立原则。耦合性和内聚性是模块独立性的两个定性标准，在划分软件系统模块时，尽量做到高内聚、低耦合，提高模块的独立性。

程序的三种基本控制结构是（8)。

(8)A.过程、子程序和分程序 B.顺序、选择和重复

C.递归、堆栈和队列 D.调用、返回和跳转

**【答案】B**

**【解析】本题考查软件程序设计的基础知识。.**

程序的三种基本控制结构是顺序结构、选择结构和重复结构。

栈是一种按“后进先出”原则进行插入和删除操作的数据结构，因此，(9)必须用栈。

(9)A.实现函数或过程的递归调用及返回处理时

B.将一个元素序列进行逆置

C.链表结点的申请和释放

D.可执行程序的装入和卸载

**【答案】A**

**【解析】本题考查数据结构基础知识。**

桟是一种后进先出的数据结构。将一个元素序列逆置时，可以使用栈也可以不用。 链表结点的申请和释放次序与应用要求相关，不存在“先申请后释放”的操作要求。可执行程序的装入与卸载，也不存在“后进先出”的操作要求。对于函数的递归调用与返回，一定是后被调用执行的先返回。

两个以上的申请人分别就相同内容的计算机程序的发明创造，先后向国务院专利行政部门提出申请，(10)可以获得专利申请权。

(10)A.所有申请人均 B.先申请人 C.先使用人 D.先发明人

**【答案】B**

**【解析】本题考查知识产权基本知识，即专利管理部门授予专利权的基本原则。**

我国授予专利权采用先申请原则，即两个以上的申请人分别就同一项发明创造申请专利权的，专利权授予最先申请的人。如果两个以上申请人在同一日分别就同样的发明创造申请专利的，应当在收到专利行政管理部门的通知后自行协商确定申请人。如果协商不成，专利局将驳回所有申请人的申请，即所有申请人均不能取得专利权。所以，先申请人可以获得专利申请权。

第三层交换根据（11）对数据包进行转发。

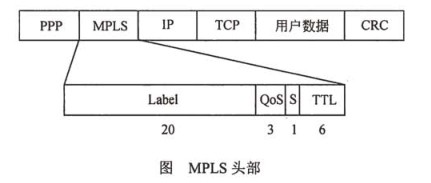
(11)A.MAC地址 B.IP地址 C.端口号 D.应用协议

**【答案】B**

**【解析】**

第三层交换是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。也就是说，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直接进行交换了，不再调用路由功能。所以三层交换机是按照IP地址选择路由，但是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, RFC 3031)简化和改进了第3层分组的交换过程。理论上，MPLS支持任何第2层和第3层协议。MPLS 包头的位置界于第2层和第3层之间，可称为第2.5层协议，标准格式如下图所示。



当带有MPLS标记的分组到达路由器时，标记被作为虚电路表的索引用来选择转发路径，同时路由器还可能加入新的标记。为了在另外一端能够区分，标记在每一跳步中必须重新映像，就像在虚电路网络中随着分组在子网之间转发不断改变连接标识一样。

按照IEEE 802.1d协议，当交换机端口处于（12)状态时，既可以学习MAC帧中的源地址，又可以把接收到的MAC帧转发到适当的端口。

(12)A.阻塞（blocking) B.学习（learning)

C.转发（forwarding) D.监听（listening)

**【答案】C**

**【解析】**

按照IEEE 802.Id协议，所有网桥可能处于下列5种状态之一：

•阻塞（blocking): MAC端口不参与帧转发，也不能学习接收帧的MAC地址，仅监听进入的BPDU。

•监听（listening):网桥能够识别根网桥，并且可以区分根端口、指定端口和非指定端口，但不能学习接收帧的地址。 '

•学习（learning): MAC端口能够学习接收帧的MAC地址，但还不能进行转发。

•转发（forwarding): MAC端口可以学习接收帧的源地址，并且可以根据目标地址将其转发到适当的端口。

•禁用（disabled): MAC端口不参与生成树算法。

以下关于帧中继网的叙述中，错误的是（13)。

(13)A.帧中继提供面向连接的网络服务

B.帧在传输过程中要进行流量控制

C.既可以按需提供带宽，也可以适应突发式业务

D.帧长可变，可以承载各种局域网的数据帧

**【答案】B**

**【解析】**

帧中继在第二层建立虚电路，因而第三层被简化掉了。同时，帧中继的第二层比HDLC操作简单，只进行检错而不再重传，没有滑动窗口式的流控，只有拥塞控制。

帧中继网络提供虚电路业务。虚电路是端到端的连接，不同的数据链路连接标识符 (DLCI)代表不同的虚电路。虚电路分为永久虚电路（PVC)和交换虚电路（SVC)。PVC 是在两个端用户之间建立的固定逻辑连接，为用户提供约定的服务。SVC是临时建立的虚电路，通过ISDN信令来建立和释放连接。

在帧中继的虚电路上可以提供不同的服务质量，网络应该保证用户以等于或低于约定数据速率CIR的速率正常传送数据。对于超过CIR的部分，一般也能可靠地传送，但是若出现网络拥塞，则会被优先丢弃。

在帧中继网上，用户的数据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，这使得帧中继成为远程传输的理想形式。

在地面上相隔2000km的两地之间通过卫星信道传送4000比特长的数据包，如果数据速率为64kb/s，则从开始发送到接收完成需要的时间是（14)。

(14)A.48ms B.640ms C.322.5ms D.332.5ms

**【答案】D**

**【解析】**

卫星信道的传输延迟为270ms，4000比特数据包发送时间为4000b / 64kb/s=62.5ms, 二者相加270+62.5=332.5ms。

同步数字系列（SDH)是光纤信道的复用标准，其中最常用的STM-1(OC-3)的数据速率是（15) ， STM-4(OC-12)的数据速率是（16)。

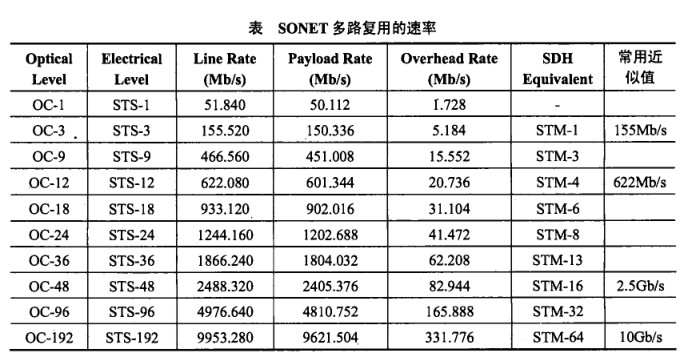
(15)A.155.520 Mb/s B.622.080 Mb/s C.2488.320 Mb/s D.10Gb/s

(16)A.155.520 Mb/s B.622.080 Mb/s C.2488.320 Mb/s D.10Gb/s

**【答案】A B**

**【解析】**

同步数字系列 SDH (Synchronous Digital Hierarchy)中最常用的是 STM-1(155.520 Mb/s)、STM-4(622.080 Mb/s), STM-16 (2488.320 Mb/s)和 STM-64 (10Gb/s)，参见下表。

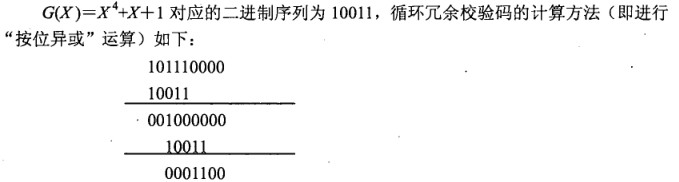


采用CRC进行差错校验，生成多项式为G(X) =X4+X+1，信息码字为10111，则计算出的CRC校验码是（17）。

(17)A.0000 B.0100 C.0010 D.1100

**【答案】D**

**【解析】**



数字用户线（DSL)是基于普通电话线的宽带接入技术，可以在铜质双绞线上同时传送数据和话音信号。下列选项中，数据速率最高的DSL标准是（18）.

(18)A.ADSL B.VDSL C.HDSL D.RADSL

**【答案】B**

**【解析】**

数字用户线（Digital Subscriber Line, DSL)是基于普通电话线的宽带接入技术，可以在一对铜质双绞线上同时传送数据和话音信号。DSL有多种模式，统称为xDSL。

根据上、下行传输速率是否相同，可以把DSL划分为对称和不对称两种传输模式。对称DSL的上、下行传输速率相同，用于代替传统的T1/E1接入线路。

高数据速率用户数字线（High-data-rate DSL, HDSL)采用两对双绞线提供全双工数据传输，支持nX64kb/s(n=l，2, 3,…）的各种速率，最高可达1.544Mb/s或2.048Mb/s, 传输距离可达3〜5km。HDSL在视频会议、远程教学、移动电话基站连接等方面得到了广泛应用。

速率自适应用户数字线（Rate Adaptive DSL, RADSL)支持同步和非同步传输方式，下行速率为640Kb/s〜12Mb/s，上行速率为128Kb/s〜1Mb/s，也支持数据和语音同时传输。RADSL具有速率自适应的特点，可以根据双绞线的质量和传输距离动态调整用户访问速率。RADSL允许通信双方的Modem寻找流量最小的频道来传送数据，以保证一定的数据速率。RADSL特别适用于线路质量千差万别的农村、山区等地区使用。

甚高比特率数字用户线（VeryHighBit-rateDSL, VDSL)可在较短的距离上获得极高的传输速率，是各种DSL中速度最快的一种。在一对铜质双绞线上，VDSL的下行速率可以扩展到52Mb/s，同时支持1.5〜2.3Mb/s的上行速率，但传输距离只有300〜1000m。 当下行速率降至13Mb/s时，传送距离可达到1.5km以上，此时上行速率为1.6〜2.3Mb/s 左右。传输距离的缩短，会使码间干扰大大减少，数字信号处理过稈就大为简化，所以其设备成本要比ADSL低。

ADSL (Asymmetrical Digital Subscriber Line)是一种非对称DSL 技术，在一对铜线上可提供512Kb/s〜1Mb/s的上行速率和1〜8Mb/s的下行速率，有效传输距离为3〜5km左右。ADSL在进行数据传输的同时还可以使用第三个信道提供4KHz的语音传输。现在比较成熟的ADSL标准有两种，即G.DMT和Giite。G.DMT是全速率的ADSL标准，支持8Mb/s的下行速率及1.5Mb/s的上行速率，但G.DMT要求用户端安装POTS分离器，技术复杂而且价格昂贵。G.Lite标准速率较低，下行速率为1.5Mb/s，上行速率为512Kb/s，但省去了 POTS分离器，成本较低且便于安装。G.DMT较适用于小型办公室 (SOHO)应用，而GLite则更适用于普通家庭应用。

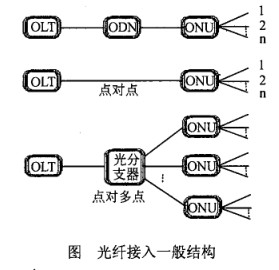
下列FTTx组网方案中，光纤覆盖面最广的是 （19）.

(19)A.FTTN B.FTTC C.FTTH D.FTTZ

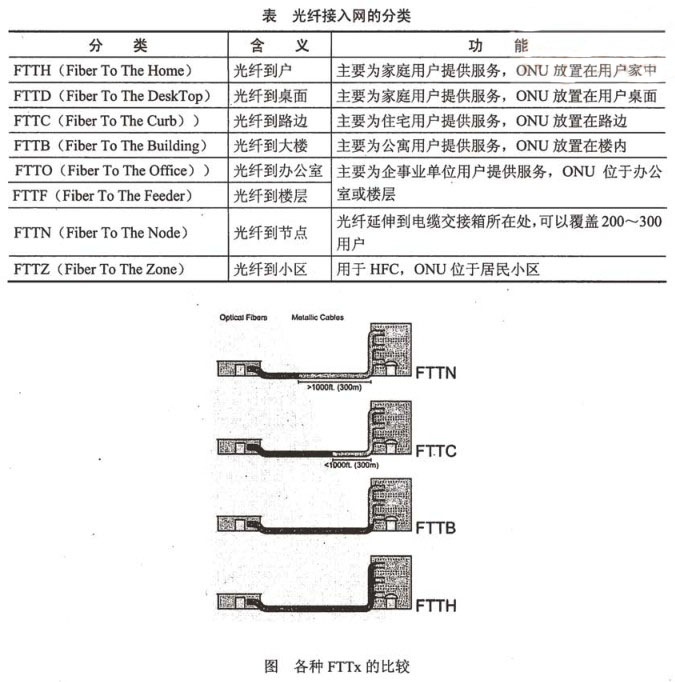
**【答案】C**

**【解析】**

光纤接入网（Optical Access Network, OAN)又称光纤用户环路（Fiber in the loop, FITL),其结构如下图所示。



在交换局中设有光纤线路终端设备（Optical Line Terminal，OLT)，在用户侧安装光纤网络单元（Optical Network Unit, ONU), OLT和ONU之间则是光纤配线网（Optical DistrabutionNetwork, ODN)。ODN可釆用多种拓扑结构，例如点对点或点到多点方式。在点对多点的连接方式中，从OLT出来的光纤信号通过光分路器或星型耦合器传送到多个ONU上，这种方式被称为双星结构。ONU采用星型拓扑连接多个用户，传输介质可以是同轴电缆或双绞铜线。根据ONU所在位置以及ONU与用户的距离，FITL可分为多种形式，统称为FTTx (Fiber-to-the-x),如下表所示。



上图表示光纤与用户终端之间距离的变化情况，左边是电信中心局，与光纤连接；右边是连接电信网络的用户住所，其中的虚线方框表示同一建筑物内的用户家庭或办公室，与铜缆相连。可以看出，对于FTTN，光纤网离用户终端最远，而在FTTH中，光纤可以直接连接到用户桌面。FTTH比FTTN建设成本高，光纤覆盖面更广，用户可以获得更高的带宽，因此在高端用户小区建设方面具有一定的优势。然而，FTTN可以有效降低光纤接入的成本，运营维护比较方便，是普通居民社区的理想接入方案。

网络地址和端口翻译（NAPT)用于（20),这样做的好处是（21)。

(20)A.把内部的大地址空间映射到外部的小地址空间

B.把外部的大地址空间映射到内部的小地址空间

C.把内部的所有地址映射到一个外部地址

D.把外部的所有地址映射到一个内部地址

(21)A.可以快速访问外部主机 B.限制了内部对外部主机的访问

C.增强了访问外部资源的能力 D.隐藏了内部网络的IP配置

**【答案】C D**

**【解析】**

网络地址翻译（Network Address Translation, NAT)技术主要解决IP地址短缺问题，最初提出的建议是在子网内部使用局部地址，而在子网外部使用少量的全局地址，通过路由器进行内部和外部地址的转换。局部地址是在子网内部独立编址的，可以与外部地址重叠。这种想法的基础是假定在任何时候子网中只有少数计算机需要与外部通信，可以让这些计算机共享少量的全局IP地址。后来根据这种技术又开发出其他一些应用。

首先是动态地址翻译(Dynamic Address Translation)技术。所谓存根域(Stub Domain) 是内部网络的抽象，任何时候存根域内只有一部分主机要与外界通信，所以整个存根域只需共享少量的全局IP地址。存根域有一个边界路由器，由它来处理域内与外部的通信。我们假定：

•m：内部地址数。

•n：全局地址数（NAT地址)。

当m≥1并且m≥n时，可以把大的地址空间映像到小的地址空间。所有NAT地址放在一个缓冲区中，并在存根域的边界路由器中建立一个内部地址和全局地址的动态映像 表，用以把内部地址翻译成全局地址。动态地址翻译的好处是节约了全局IP地址，而且不需要改变子网内部的配置。

另外一种特殊的NAT应用是m:1翻译，这种技术也叫做地址伪装（Masquerading)， 因为用一个全局地址就可以把子网中所有主机的IP地址隐藏起来。如果子网屮有多 个主机要同时通信，那么还要对端口号进行翻译，所以这种技术经常被称为网络地址和端口翻译（Network Address Port Translation, NAPT)。在很多NAPT 实现中专门保留一部分端口号给地址伪装使用，叫做伪装端口号。这种方法有如下特点：

•出口分组的源地址被路由器的外部IP地址代替，出口分组的源端口号被一个未使用的伪装端口号代替。

•如果进来的分组的目标地址是本地路由器的IP地址，而目标端口号是路由器的伪装端口号，则NAT路由器就检查是否为伪装会话，并试图通过伪装表对IP地址和端口号进行翻译。

伪装技术吋以作为一种安全手段使用，借以限制外部对内部主机的访问。另外还可以用这种技术实现虚拟主机和虚拟路由，以便达到负载均衡和提高可靠性的目的。

边界网关协议BGP的报文（22)传送。一个外部路由器通过发送（23)报文与另一个外部路由器建立邻居关系，如果得到应答，才能周期性地交换路由信息。

(22)A.通过TCP连接 B.封装在UDP数据报中

C.通过局域网 D.封装在ICMP包中

(23)A.Update B.Keepalive C.Open D.通告

**【答案】A C**

**【解析】**

通用的外部网关协议是边界网关协议（Border Gateway Protocol，BGP)第4版。运行这个协议的网关向对等实体（Peer)发布可以到达的AS列表。通过交换路由信息，网关可以建立所有AS的互连结构图，并根据路由决策算法对环路进行修剪。

BGP4发布的路由信息是可到达网络的IP地址前缀，并支持CIDR技术，通过路由汇聚功能形成超级网络，以简化路由表，并提高转发速度。

BGP4报文通过TCP连接传送，其报文类型有建立邻居关系的OPEN报文，对OPEN请求进行应答的KEEPALIVE报文，发送路由更新信息的UPDATE报文，以及通告路由错误的NOTIFICATION报文。

BGP的有限状态机如下图所示，共有13个BGP事件，引起BGP协议机在6个状态之间转换。

在IPv6中，地址类型是由格式前缀来区分的。IPv6可聚合全球单播地址的格式前缀是（24)。

(24)A.001 B.1111 1110 10 C.1111 1110 11 D.1111 1111

**【答案】A**

**【解析】**

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。例如结点地址如下：

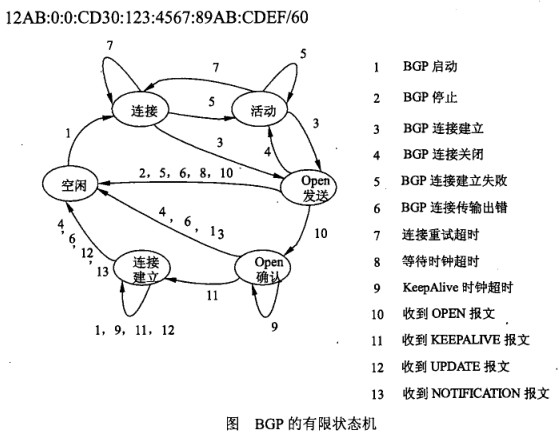
12AB:0:0:CD30:123:4567:89AB:CDEF

若其子网号为

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

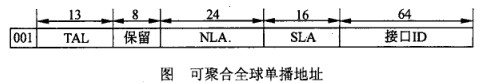
则等价的写法是

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



IPv6单播地址包括可聚合全球单播地址、链路本地地址、站点本地地址和其他特殊单播地址。

①可聚合全球单播地址：这种地址在全球范围内有效，相当于IPv4公用地址。全球地址的设计有助于构架一个基于层次的路由基础设施。可聚合全球单播地址结构如下图所示。



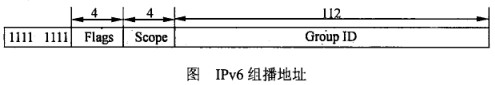
可聚合全球单播地址格式前缀为001，随后的顶级聚合体TLA (Top Level Aggregator)、下级聚合体NLA(Next Level Aggregator)以及站点级聚合体SLA( Site Level Aggregator)构成了自顶向下的3级路由层次结构。TLA是远程服务供应商的骨干网接入点，TLA向地区互联网注册机构RIR (ARIN、RIPE NCC、APNIC等）申请IPv6地址块，TLA之下就是商业地址分配范围。NLA是一般的ISP，它们把从TLA申请的地址分配给SLA，各个站点级聚合体再为机构用户或个人用户分配地址。分层结构的最底层是主机接口，通常是在主机的48位MAC地址前面填充OxFFFE构成的接口ID。

②本地单播地址：这种地址的有效范围仅限于本地，又分为两类：

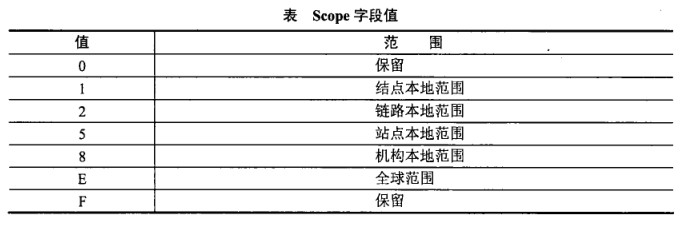
•链路本地地址：其格式前缀为1111 1110 10,用于同一链路的相邻结点间的通信。链路本地地址相当于IPv4中的自动专用IP地址（APIPA)，可用于邻居发现，并且总是自动配置的，包含链路本地地址的分组不会被路由器转发。

•站点本地地址：其格式前缀为1111 1110 11，相当于IPv4中的私网地址。如果企业内部网没有连接到Internet上，则可以使用这种地址。站点本地地址不能被其他站点访问，包含这种地址的分组也不会被路由器转发到站点之外。

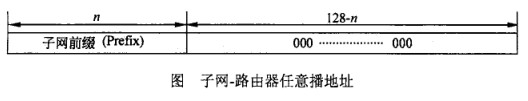
③组播地址：IPv6组播可以将数据报传输给组内所有成员。IPv6组播地址格式前缀为1111 1111，此外还包括标志（Flags)、范围和组ID等字段，如下图所示。



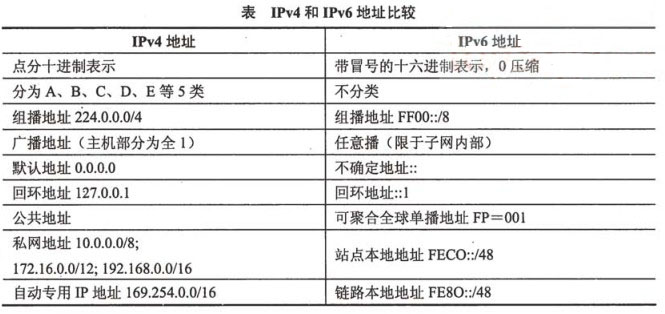
Flags可表示为000T，T=0表示被IANA永久分配的组播地址；T=1表示临时的组播地址。Scope是组播范围字段，下表列出了在RFC 2373中定义的Scope的值。Group ID标识了一个给定范围内的组播组。永久分配的组播组ID与范围字段无关，临时分配的组播组ID在特定的范围内有效。



④任意播地址：任意播地址仅用做目标地址，且只能分配给路由器。任意播地址是在单播地址空间中分配的。一个子网内的所有路由器接口都被分配了子网-路由器任意播地址。子网-路由器任意播地址必须在子网前缀中进行预定义。为构造一个子网-路由器任意播地址，子网前缀必须固定，其余位置全“0”，见下图。



下表是对IPv4与IPv6地址的比较。



在IPv6的单播地址中有两种特殊地址，其中地址0:0:0:0:0:0:0:0表示（25),地址 0:0:0:0:0:0:0:1 表示（26)。

(25)A.不确定地址，不能分配给任何结点

B.回环地址，结点用这种地址向自身发送IPv6分组

C.不确定地址，可以分配给任何结点

D.回环地址，用于测试远程结点的连通性

(26)A.不确定地址，不能分配给任何结点

B.回环地址，结点用这种地址向自身发送IPv6分组

C.不确定地址，可以分配给任何结点

D.回环地址，用于测试远程结点的连通性

**【答案】A B**

**【解析】**

IPv6地址有单播地址、任意播地址和组播地址三种类型：

（1）单播（Unicast)地址

单播地址是单个网络接口的标识符。对于有多个接口的结点，其中任何一个单播地址都可以用作该结点的标识符。但是为了满足负载平衡的需要，在RFC 2373中规定， 只要在实现中多个接口看起来形同一个接口就允许这些接口使用同一地址。IPv6的单播地址是用一定长度的格式前缀汇聚的地址，类似于IPv4中的CIDR地址。单播地址中有 下列两种特殊地址：

•不确定地址：地址0:0:0:0:0:0:0:0称为不确定地址，不能分配给任何结点。不确定地址可以在初始化主机时使用，在主机未取得地址之前，它发送的IPv6分组中的源地址字段可以使用这个地址。这种地址不能用作目标地址，也不能用在IPv6路由头中。

•回环地址：地址0:0:0:0:0:0:0:1称为回环地址，结点用这种地址向自身发送IPv6 分组。这种地址不能分配给任何物理接口。

（2）任意播（AnyCast)地址

这种地址表示i组接口（可属于不同结点的）的标识符。发往任意播地址的分组被送给该地址标识的接口之一，通常是路由距离最近的接口。对IPv6任意播地址存在下列 限制：

•任意播地址不能用作源地址，而只能作为目标地址。

•任意播地址不能指定给IPv6主机，只能指定给IPv6路由器。

组播(Multicast)地址

组播地址是一组接口（一般属于不同结点）的标识符，发往组播地址的分组被传送给该地址标识的所有接口。IPv6中没有广播地址，它的功能已被组播地址所代替。

在IPv6地址中，任何全“0”和全“1”字段都是合法的，除非特别排除的之外。特别是前缀可以包含“0”值字段，也可以用“0”作为终结字段。一个接口可以被赋予任何类型的多个地址（单播、任意播、组播）或地址范围。

Telnet采用客户端/服务器工作方式，采用（27)格式实现客户端和服务器的数据传输。

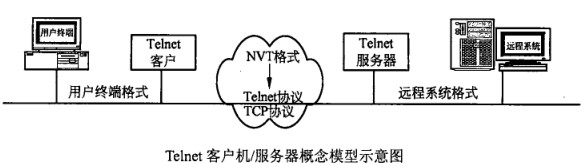
(27)A.NTL B.NVT C.base -64 D.RFC 822

**【答案】B**

**【解析】本试题考査Telnet文件传输格式。**

Telnet采用客户机/服务器工作方式。用户终端运行Telnet客户程序,远程主机运行Telnet服务器程序。Telnet定义了网络虚拟终端NVT (Network Virtual Terminal)。NVT代码包括标准的7单位ASCII字符集和Telnet命令集。这些字符和命令提供了本地终端和远程主机之间的网络接口。

客户机与服务器程序之间执行Telnet NYT协议，而在两端则分别执行各自的操作系统功能，如下图所示。



以下关于DNS服务器的叙述中，错误的是（28)。

(28)A.用户只能使用本网段内DNS服务器进行域名解析

B.主域名服务器负责维护这个区域的所有域名信息

C.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

D.转发域名服务器负责非本地域名的查询

**【答案】A**

**【解析】本试题考查DNS的几种服务器形式。**

主域名服务器（primary name server)负责维护这个区域的所有域名信息，是特定域所有信息的权威性信息源。当主域名服务器关闭、出现故障或负载过重时，辅域名服务器（secondary name server)作为备份服务器提供域名解析服务。辅助服务器从主域名服务器获得授权，并定期向主服务器询问是否有新数据，如果有则调入并更新域名解析数据，以达到与主域名服务器同步的目的。缓存域名服务器（caching-only server)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予以回答。转发域名服务器（forwarding server)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。

用户可以通过中继代理使用外网段内DNS服务器进行域名解析，故选A。

以下域名服务器中，没有域名数据库的是（29)。

(29)A.缓存域名服务器 B.主域名服务器

C.辅域名服务器 D.转发域名服务器

**【答案】A**

**【解析】本试题考查DNS的域名数据库。**

缓存域名服务器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 时就予以回答。因此缓存域名服务器没有域名数据库。故选A。

通过“Internet信息服务（IIS)管理器”管理单元可以配置FTP服务，若将控制端口设置为2222,则数据端口自动设置为（30)。

(30)A.20 B.80 C.543 D.2221

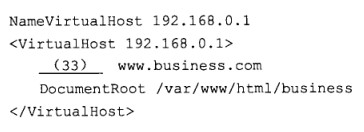
**【答案】D**

**【解析】**

客户端向服务器的FTP端口发送连接请求，服务器接受连接，建立一条命令链路。当需要传送数据时，服务器从另一端口向客户端的空闲端口发送连接请求，建立一条数据链路来传送数据。默认情况下控制端口为21，数据端口为20,但数据端口和控制端口都可以人为设置。若将控制端口重新设置，则数据端口自动设置为数据端口-1。

因此，若将控制端口设置为2222,则数据端口自动设置为2221，正确答案为D。

在一台Apache服务器上通过虚拟主机可以实现多个Web站点。虚拟主机可以是基于(31)的虚拟主机，也可以是基于名字的虚拟主机。若某公司创建名字为www.business.com的虚拟主机，则需要在（32)服务器中添加地址记录。在Linux中该地址记录的配置信息如下，请补充完整。



(31)A.IP B.TCP C.UDP D.HTTP

(32)A.SNMP B.DNS C.SMTP D.FTP

(33)A.WebName B.HostName C.ServerName D.WWW

**【答案】A B C**

**【解析】本题考查APACHE虚拟主机方面的相关知识。**

Apache服务器可提供基于IP的虚拟主机或者基于名字的虚拟主机，服务器构建好之后，需要在DNS记录中添加对应的地址记录，从而其他用户可通过域名进行访问， ServerName选项用于设置服务器用于辨识自己的主机信息。

ATM高层定义了4类业务，压缩视频信号的传送属于（34)类业务。

(34)A.CBR B.VBR C.UBR D.ABR

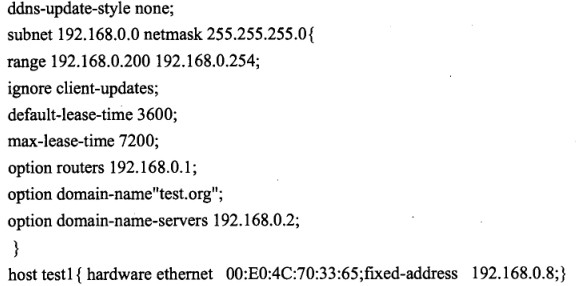
**【答案】B**

**【解析】本试题考查ATM的业务类别知识。**

ATM高层与业务相关，ATM4.0规定的用户业务分为4类。其中CBR (Constant Bit Rate)采用固定比特率业务适合于交互式话音和视频流。VBR (Variable Bit Rate)可变比特率业务适合交互式压缩视频信号（MPEG)。ABR (Available Bit Rate)釆用有效比特率业务，用于突发式通信。UBR (Unspecified Bit Rate) 为不定比特率，可用于传送IP分组，包括文件传输，电子邮件和USENET新闻是这类业务潜在的应用领域。

故压缩视频信号的传送属于VBR类业务，选B。

某Linux DHCP服务器dhcpdconf的配置文件如下：



客户端IP地址的默认租用期为（35)小时。

(35)A.1 B.2 C.60 D.120

**【答案】A**

**【解析】本试题考查Linux DHCP服务器的配置。**

配置文件中default-lease-time 3600表明客户端IP地址的默认租用期为3600秒，即1小时；max-lease-time 7200表明客户端IP地址的最大租用期为7200秒，即2小时。故选A。

DHCP客户端不能从DHCP服务器获得（36)。

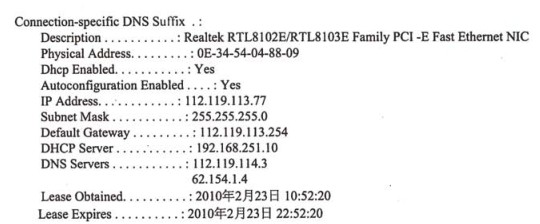
(36)A.DHCP服务器的IP地址 B.Web服务器的IP地址

C.DNS服务器的IP地址 D.默认网关的IP地址

**【答案】B**

**【解析】本试题考查DHCP服务器的配置。**

DHCP客户端不能从DHCP服务器获得DHCP服务器的IP地址、DNS服务器的IP地址、默认网关的IP地址等，从下图中即可看出。



但是，不能获得Web服务器的IP地址。故选B。

配置POP3服务器时，邮件服务器的属性对话框如下图所示，其中默认情况下“服务器端口”文本框应填入（37)。



(37)A.21 B.25 C.80 D.110

**【答案】D**

**【解析】本试题考査POP3服务器的配置。**

POP3服务器默认端口为110, 故“服务器端口”文本框应填入110,选D。

在Windows的DOS窗口中键入命令

C:\> nslookup

set type=ns

>202.30.192.2

这个命令序列的作用是（38)。

(38)A.查询202.30.192.2的邮件服务器信息

B.查询202.30.192.2到域名的映射

C.查询202.30.192.2的区域授权服务器

D.显示202.30.192.2中各种可用的信息资源记录

**【答案】C**

**【解析】本试题考查nslookup命令。**

Nslookup命令用于显示DNS查询信息，诊断和排除DNS 故障。Nslookup有交互式和非交互式两种工作方式，交互模式下，可以用set命令设置 选项，满足指定的查询需要。DNS服务器中主要的资源记录有A (域名到IP地址的映射)、PTR (IP地址到域名的映射)、MX (邮件服务器及其优先级)、CNAM (别名）和 NS (区域的授权服务器）等类型。故选C。

HTTPS采用（39)协议实现安全网站访问。

(39)A.SSL B.IPSec C.PGP D.SET

**【答案】A**

**【解析】本题考查网络安全方面关于安全协议的基础知识。**

IPSec (IP Security)是IETF定义的一组协议，用于增强IP网络的安全性。IPSec 是在网络层建立安全隧道，适用于建立固定的虚拟专用网。

PGP (Pretty Good Privacy)是 Philip R. Zimmermann 在1991年开发的电子邮件加密软件包，如今PGP已经成为使用最广泛的电子邮件加密软件。

SET (Secure Electronic Transaction)是一个安全协议和报文格式的集合，它融合了Netscape的SSL、Microsoft 的STT (Secure Transaction Technology)、Terisa 的S-HTTP、以及PKI技术，通过数字证书和数字签名机制，使得客户可以与供应商进行安全的电子交易。

SSL (Secure Socket Layer)是Netscape于1994年开发的传输层安全协议，用于实现Web安全通信。SSL/TLS在Web安全通信中被称为HTTPS。所以答案是A。

杀毒软件报告发现病毒Macro.Melissa，由该病毒名称可以推断出病毒类型是(40)， 这类病毒主要感染目标是（41)。

(40)A.文件型 B.引导型 C.目录型 D.宏病毒

(41)A.EXE或COM可执行文件 B.Word或Excel文件

C.DLL系统文件 D.磁盘引导区

**【答案】D B**

**【解析】本题考查计算机病毒方面的基础知识。**

计算机病毒的分类方法有许多种，按照最通用的区分方式，即根据其感染的途径以及采用的技术区分，计算机病毒可分为文件型计算机病毒、引导型计算机病毒、宏病毒和目录型计算机病毒。

文件型计算机病毒感染可执行文件（包括EXE和COM文件）。

引导型计算机病毒影响软盘或硬盘的引导扇区。

目录型计算机病毒能够修改硬盘上存储的所有文件的地址。

宏病毒感染的对象是使用某些程序创建的文本文档、数据库、电子表格等文件，从文件名可以看出Macro.Melissa是一种宏病毒。

以下ACL语句中，含义为“允许172.168.0.0/24网段所有PC访问10.1.0.10中的FTP服务”的是（42)。

(42)A.access-list 101 deny tcp 172.168.0.0 0.0.0.255 host 10.1.0.10 eq ftp

B.access-list 101 permit tcp 172.168.0.0 0.0.0.255 host 10.1.0.10 eq ftp

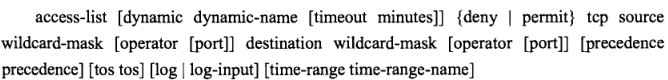
C.access-list 101 deny tcp host 10.1.0.10 172.168.0.0 0.0.0.255 eq ftp

D.access-list 101 permit tcp host 10.1.0.10 172.168.0.0 0.0.0.255 eq ftp

**【答案】B**

**【解析】本题考查防火墙方面ACL配置的基础知识。**

题中四个选项给出的是4条扩展ACL语句，扩展ACL语句的语法如下：



在 ACL 语句中，“172.168.0.0/24 网段”表示为 172.168.0.0 0.0.0.255，目标主机10.1.0.10表示为host 10.1.0.10,并且源地址位于目标地址之前。所以，正确的ACL语句应该是选项B。

以下关于加密算法的叙述中，正确的是（43)。

(43)A.DES算法采用128位的密钥进行加密

B.DES算法采用两个不同的密钥进行加密

C.三重DES算法采用3个不同的密钥进行加密

D.三重DES算法采用2个不同的密钥进行加密

**【答案】D**

**【解析】本题考查网络安全方面加密算法的基础知识。**

DES (Data Encryption Standard)明文被分成64位的块进行变换运算，变换由56位的密钥的不同排列形式控制，最后产生64位的密文块。

三重DES (Triple-DES)是DES的改进算法，它使用两把密钥对报文作三次DES加密，第一层和第三层中使用相同的密钥，产生一个有效长度为112位的密钥。所以正确答案是D。

IIS服务支持的身份验证方法中，需要利用明文在网络上传递用户名和密码的是(44)。

(44)A..NET Passport身份验证 B.集成Windows身份验证

C.基本身份验证 D.摘要式身份验证

**【答案】C**

**【解析】本题考查Windows IIS服务中身份认证的基础知识。**

Windows IIS服务支持的身份认证方式有四种：.NET Passport身份验证、集成 Windows身份验证、摘要式身份验证和基本身份验证。

集成Windows身份验证以Kerberos票证的形式通过网络向用户发送身份验证信息，并提供较高的安全级别。Windows集成身份验证使用Kerberos版本5和NTLM身份验

证。

摘要式身份验证，将用户凭据作为MD5哈希或消息摘要在网络中进行传输，这样就无法根据哈希对原始用户名和密码进行解码。

.NET Passport身份验证，对IIS的请求必须在查询字符串或Cookie中包含有效的.NET Passport凭据，提供了单一登录安全性，为用户提供对Internet上各种服务的访问权限。

基本身份验证：用户凭据以明文形式在网络中发送。这种形式提供的安全级别很低，因为几乎所有协议分析程序都能读取密码。所以答案是C。

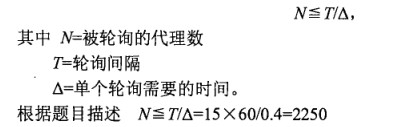
某局域网采用SNMP进行网络管理，所有被管设备在15分钟内轮询一次，网络没有明显拥塞，单个轮询时间为0.4s，则该管理站最多可支持（45)个设备。

(45)A.18000 B.3600 C.2250 D.90000

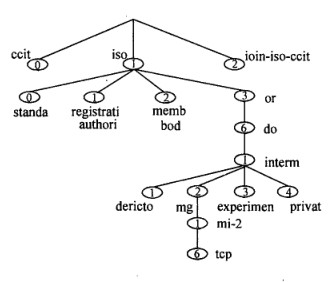
**【答案】C**

**【解析】本题考查SNMP的基础知识。**

SNMP在进行网络管理时釆用轮询机制，通常轮询频率与网络的规模和代理的多少有关。而网络管理性能还取决于管理站的处理速度、子网数据速率、网络拥塞程度等众多的因素。管理站轮询一般只是釆用get请求/响应这种简单形式，而管理站主要操作用来轮询，测算管理站最多可支持设备釆用如下不等式：



下图是被管理对象的树结构，其中private子树是为私有企业管理信息准备的，目前 这个子树只有一个子结点enterprises(1)。某私有企业向Internet编码机构申请到一个代码920,该企业为它生产的路由器赋予的代码为3,则该路由器的对象标识符是（46)。



(46)A.1.3.6.1.4.920.3 B.3.920.4.1.6.3.1

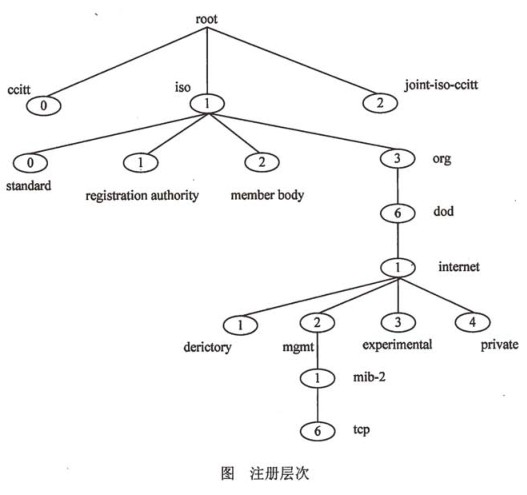
C.1.3.6.1.4.1.920.3 D.3.920.1.4.1.6.3.1

**【答案】C**

**【解析】本题考查SNMP中管理对象树结构的基础知识。**

SNMP环境中的所有被管理对象组织成树型结构，如下图所示。这种层次树结构有3个作用：

①表示管理和控制关系。从下图可知，上层的中间结点是某些组织机构的名字， 说明这些机构负责它下面的子树的管理。有些中间结点虽然不是组织机构名，但己委托给某个组织机构代管，例如org(3)由ISO代管，而intemet( 1)由IAB( Internet Architecture Board)代管等。树根没有名字，默认为抽象语法表示ASN.1。



②提供了结构化的信息组织技术。从上图可看出，下层的中间结点代表的子树是与每个网络资源或网络协议相关的信息集合。例如，有关IP协议的管理信息都放置在ip(4) 子树中。这样，沿着树层次访问相关信息很方便。

③提供了对象命名机制。树中每个结点都有一个分层的编号。叶子结点代表实际的管理对象，从树根到树叶的编号串联起来，用圆点隔开，就形成了管理对象的全局标 识。例如internet 的标识符是1.3.6.1，或者写为{iso(1) org(3) dod(6) 1}。

internet下面的4个结点需要解释。directory 1是OSI的目录服务（X.500)。mgmt 2 包括由IAB批准的所有管理对象，而mib-2是mgmt 2的第一个孩子结点。experimental 3 子树用来标识在互联网上实验的所有管理对象。最后，private 4子树是为私有企业管理信息准备的，目前这个子树只有一个孩子结点enterprises 1。

根据题目描述，某私有企业向Internet编码机构申请到一个代码920,该企业为它生产的路由器赋予的代码为3。这样，该路由器的对象标识符就是1.3.6.1.4.1.920.3。

使用Windows提供的网络管理命令（47)可以查看本机的路由表，(48)可以修改本机的路由表。

(47)A.tracert B.arp C.ipconfig D.netstat

(48)A.ping B.route C.netsh D.nbtstat

**【答案】D B**

**【解析】本题考查网络管理命令的使用。**

tracert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。

arp命令用来显示和修改arp缓存中的值。

ipconfig命令可用于显示当前的TCP/IP配置的设置值。

netstat是Windows提供的网络管理命令，是一个监控TCP/IP网络的非常有用的工具，它可以显示路由表、实际的网络连接以及每一个网络接口设备的状态信息。netstat 常用的参数如下：

•netstat-s：能够按照各个协议分别显示其统计数据。

•netstat-e：用于显示关于以太网的统计数据。它列出的项目包括传送的数据报的总字节数、错误数、删除数、数据报的数量和广播的数量。

•netstat-r:可以显示关于路由表的信息，类似于后面所讲使用route print命令时 看到的信息。除了显示有效路由外，还显示当前有效的连接。

•netstat -a:显示一个所有的有效连接信息列表，包括已建立的连接 (ESTABLISHED),也包括监听连接请求（LISTENING)的那些连接。

•netstat-n：显示所有已建立的有效连接。

ping命令是Windows系列自带的一个可执行命令。利用它可以检查网络是否能够 连通。

route用于显示本地IP路由表或修改本地路由表。

netsh是Windows系统本身提供的功能强大的网络配置命令行工具。可以导入、导出配置脚本，还可以对wins、route, ras等网络服务的配置进行操作。

nbtstat命令可以显示基于TCP/IP的NetBIOS (NetBT)协议统计资料、本地计算机和远程计算机的NetBIOS名称表和NetBIOS名称缓存。

某局域网访问Internet速度很慢，经检测发现局域网内有大量的广播包，采用（49)方法不可能有效地解决该网络问题。

(49)A.在局域网内查杀ARP病毒和蠕虫病毒

B.检查局域网内交换机端口和主机网卡是否有故障

C.检查局域网内是否有环路出现

D.提高出口带宽速度.

**【答案】D**

**【解析】本题考查网络故障排查的基础知识。**

局域网访问Internet速度很慢的原因可能是由于出口带宽速度不够或网络内部出现问题造成的。根据题目描述，发现局域网内有大量的广播包，造成这种情况的原因可能是有以下几种：

• ARP病毒和蠕虫病毒攻击。

•局域网内交换机端口和主机网卡出现故障。

•局域网内出现环路。

下列IP地址中，属于私网地址的是（50)。

(50)A.100.1.32.7 B.192.178.32.2

C.172.17.32.15 D.172.35.32.244

**【答案】C**

**【解析】**

有一些特殊的IP地址必须记住：

•网络地址：主机地址全为0地址称为网络地址，例如129.45.0.0就是指一个B类网络地址。

•广播地址：主机地址为全1的地址称为广播地址，例如129.45.255.255就是一个B类广播地址，网络129.45.0.0中的主机都可以接收这个数据报。

•本地回路地址：网络地址127保留给诊断用，例如127.0:0.1用于回路测试。

•本地网络地址：网络地址的第一个字节全为0时表示本地网络。

•私网地址：这种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：

■ 10.0.0.0 〜10.255.255.255 1 个A类地址

■172.16.0.0〜172.31.255.255 16 个B 类地址

■192.168.0.0〜192.168.255.255 256 个C 类地址

网络200.105.140.0/20中可分配的主机地址数是（51)。

(51)A.1022 B.2046 C.4094 D.8192

**【答案】C**

**【解析】**

由于地址200.105.140.0/20中的子网掩码有20位，留给主机的地址只有12位，所以212-2=4094。

下列地址中，属于154.100.80.128/26的可用主机地址是（52)。

(52)A.154.100.80.128 B.154.100.80.190

C.154.100.80.192 D.154.100.80.254

**【答案】B**

**【解析】**

网络154.100.80.128/26中的主机地址都采用154.100.80.10xxxxxx形式，显然154.100.80.192和154.100.80.254都超出了地址范围,154.100.80.128是子网地址，只有154.100.80.190属于规定的子网。

无类别域间路由（CIDR)技术有效地解决了路由缩放问题。使用CIDR技术把4个网络

C1： 192.24.0.0/21

C2： 192.24.16.0/20

C3： 192.24.8.0/22

C4： 192.24.34.0/23

汇聚成一条路由信息，得到的网络地址是（53)。

(53)A.192.24.0.0/13 B.192.24.0.0/24

C.192.24.0.0/18 D.192.24.8.0/20

**【答案】C**

**【解析】**

网络C1:192.24.0.0/21 的二进制表示为：11000000 00011000 00000000 00000000

网络C2:192.24.16.0/20 的二进制表示为：11000000 00011000 00010000 00000000

网络C3:192.24.8.0/22的二进制表示为： 11000000 00011000 00001000 00000000

网络C4:192.24.34.0/23的二进制表示为： 11000000 00011000 00100010 00000000

地址192.24.0.0/18 二进制表示为：10101100 00011000 00000000 00000000

所以C是正确答案。

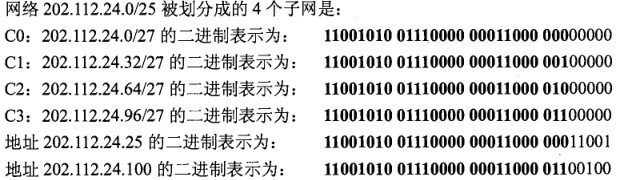
网络202.112.24.0/25被划分为4个子网，由小到大分别命名为C0、C1、C2和C3, 子网， 则主机地址202.112.24.25应该属于（54)子网，主机地址202.112.24.100应该属于(55)子网。

(54)A.C0 B.C1 C.C2 D.C3

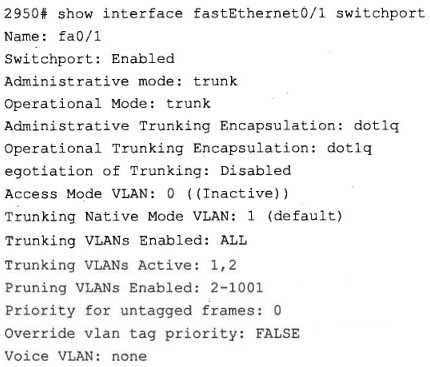
(55)A.C0 B.C1 C.C2 D.C3

**【答案】A D**

**【解析】**



交换机命令show interfaces type 0/port\_# switchport|trunk用于显示中继连接的配置情况，下面是显示例子：



在这个例子中，端口fa0/1的链路模式被设置为（56)状态，默认的VLAN是（57)。

(56)A.Desirable B.No-Negotiate C.Auto negotiate D.trunk

(57)A.VLAN0 B.VLAN1 C.VLAN2 D.VLAN3

**【答案】D B**

**【解析】**

由Administrative mode: trunk 和Operational Mode: trunk 可看出，端口fa0/1的链路模式被设置为trunk状态，由Trunking Native Mode VLAN: 1 (default)可看出，默认的VLAN 是VLAN 1。

按照Cisco公司的VLAN中继协议（VTP)，当交换机处于（58)模式时可以改变VLAN配置，并把配置信息分发到管理域中的所有交换机。

(58)A.客户机（Client) B.传输（Transmission)

C.服务器（Server) D.透明（Transparent)

**【答案】C**

**【解析】**

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VLANS 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桢，但是并不能据此更新自己的VLAN配置，只是起到通路的作用。

交换机命令switch(config)# vtp pruning的作用是（59)。

(59)A.指定交换机的工作模式 B.启用VTP静态修剪

C.指定VTP域名 D.启用VTP动态修剪

**【答案】D**

**【解析】**

在默认情况下，所有交换机通过中继链路连接在一起，如果VLAN中的任何设备发出一个广播包、组播包，或者一个未知的单播数据包，交换机都会将其洪泛到所有与源VLAN端口相关的各个输出端口上，包括中继端口。在很多情况下，这种洪泛转发是必要的，特别是在VLAN跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源VLAN的活动端口，则这种洪泛发送的数据包是无用的。

虽然单个广播包尚不足以引起太大的问题，但是如果这是PC-A发出的10Mb/s的组播视频流，那么中继链路的吞吐率就会遇到严重的挑战。

为了解决这个问题，可以使用静态或动态修剪方法。所谓静态修剪，就是手工剪掉中继链路上不活动的VLAN。但是，手工修剪方式容易出错。

VTP动态修剪允许交换机从中继连接上动态地剪掉不活动的VLAN，使得所有共享的VLAN都是活动的。例如，交换机A告诉交换机B，它有两个活动的VLAN1和VLAN2，而交换机B告诉交换机A，它只有一个活动的VLAN1，于是，它们就共享这样的事实: VLAN 2在它们之间的中继链路上是不活动的，应该从中继链路的配置中剪掉。

这样做的好处是显而易见的，如果以后在交换机B上添加了VLAN2的成员，交换机B就会通知交换机A，它有了一个新的活动的VLAN2,于是，两个交换机动态地把VLAN2添加到它们之间的中继链路配置中，如下图所示。

VTP动态修剪的缺点是它要求在VTP域中的所有交换机都必须配置成服务器。由于交换机在服务器模式下工作时可以改变VLAN配置，也可以接受VLAN配置的改变， 所以当多个管理员在多个服务器上同时配置VLAN时将会出现灾难性的后果。

交换机命令switch(config)# vtp pruning的作用是启用VTP动态修剪。

IEEE 802.3规定的最小帧长为64字节，这个帧长是指（60)。

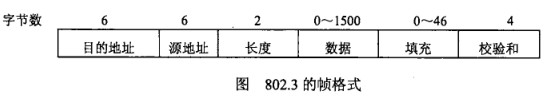
(60)A.从前导字段到校验和的长度 B.从目标地址到校验和的长度

C.从帧起始符到校验和的长度 D.数据字段的长度

**【答案】B**

**【解析】**

IEEE 802.3规定的最小帧长为64字节，这个帧长是指从目标地址到校验和的长度, 如下图所示。



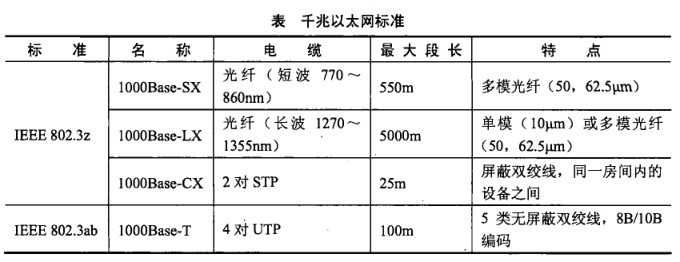
千兆以太网标准802.3z定义了一种帧突发方式（frame bursting),这种方式是指(61)。(61)A.一个站可以突然发送一个帧 B.一个站可以不经过竞争就启动发送过程

C.一个站可以连续发送多个帧 D.一个站可以随机地发送紧急数据

**【答案】C**

**【解析】**

1998年6月公布的IEEE 802.3z和1999年6月公布的IEEE 802.3ab已经成为千兆以太网的正式标准。它规定了四种传输介质，如下表所示。



实现千兆数据速率需要采用新的数据处理技术。首先是最小帧长需要扩展，以便在半双工的情况下增加跨距。另外802.3z还定义了一种帧突发方式（frame bursting),使 得一个站可以连续发送多个帧。最后物理层编码也采用了与10Mb/s不同的编码方法， 即4b/5b或8b/9b编码法。

千兆以太网标准可用于已安装的综合布线基础之上，以保护用户的投资。

IEEE 802.11 标准定义的 Peer to Peer 网络是（62)。

(62)A.—种需要AP支持的无线网络

B.一种不需要有线网络和接入点支持的点对点网络

C.一种采用特殊协议的有线网络

D.一种髙速骨干数据网络

**【答案】B**

**【解析】**

IEEE 802.11标准定义了两种无线网络拓扑结构，一种是基础设施网络(Infrastructure Networking),另一种是特殊网络（Ad Hoc Networking)。在基础设施网络中，无线终端通过接入点（Access Point, AP)访问骨干网设备，或者互相访问。接入点如同一个网桥，它负责在802.11和802.3 MAC之间进行转换。

Ad hoc网络是一种点对点网络，不需要有线网络和接入点的支持，以无线网卡连接 的终端设备之间可以直接通信。这种拓扑结构适合在固定或移动情况下快速部署网络。802.11支持单跳的Ad hoc网络，当一个无线终端接入时首先寻找来自AP或其他终端的信标信号，如果找到了信标，则AP或其他终端就宣布新的终端加入了网络。如果没有检测到信标，该终端就自行宣布存在于网络之中。

IEEE 802. 11g标准支持的最高数据速率可达（63) Mb/s。

(63)A.5 B.11 C.54 D.100

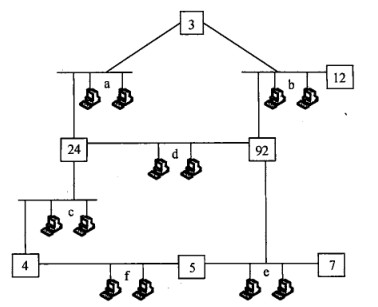
**【答案】C**

**【解析】**

IEEE公布的无线局域网正式标准如下表所示。



下图表示一个局域网的互连拓扑，方框中的数字是网桥ID,用字母来区分不同的网段。按照IEEE802.1d协议，ID为（64)的网桥被选为根网桥,如果所有网段的传输费用为1，则ID为92的网桥连接网段（65)的端口为根端口。



(64)A.3 B.7 C.92 D.12

(65)A.a B.b C.d D.e

**【答案】A B**

**【解析】**

按照IEEE 802.1d协议定义的生成树算法，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ID, ID最小的网桥被选举为根网桥。其他网桥的连接根网桥的费用最小的端口成为根端口。

建筑物综合布线系统中的干线子系统是（66),水平子系统是（67)。

(66)A.各个楼层接线间配线架到工作区信息插座之间所安装的线缆

B.由终端到信息插座之间的连线系统

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

(67)A.各个楼层接线间配线架到工作区信息插座之间所安装的线缆

B.由终端到信息插座之间的连线系统

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】C A**

**【解析】**

结构化布线系统分为6个子系统：

①工作区子系统（WorkLocation):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。

②水平子系统（Horizontal):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。水平子系统的作用是将干线子系统线路延伸到用户工作区。

③管理子系统（Administration):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。交连设备通过水平布线子系统连接到各个工作区的信息插座，集线器或交换机与交连设备之间通过短线缆（跳线）互连，通过跳线的调整，可以对工作区的信息插座和交换机端口之间进行连接切换。

④干线子系统（Backbone):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。

⑤设备间子系统（Equipment):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。

⑥建筑群子系统（Campus):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。大楼之间的布线方法有3种。一种是地下管道敷设方式，管道内敷设的铜缆或光缆应遵循电话管道和入孔的各种规定，安装时至少应预留1〜2个备用管孔，以备扩充之用。第二种是直埋法，要在同一个沟内埋入通信和监控电缆，并应设立明显的地面标志。最后是架空明线，这种方法需要经常维护。

假设生产管理网络系统采用B/S工作方式，经常上网的用户数为150个，每用户每分钟产生8个事务处理任务，平均事务章大小为0.05MB，则这个系统需要的信息传输速率为(68)。

(68)A.4 Mb/s B.6 Mb/s C.8 Mb/s D.12 Mb/s

**【答案】C**

**【解析】**

可以根据下面的公式计算出应用需要的传输信息速率：

总信息传输速率=平均事务量大小X每字节位数X每个会话事务数X平均用户数/平均会话时长

根据这个公式，结算结果为：0.05X8X8X150/ 60=8Mb/s

网络设计过程包括逻辑网络设计和物理网络设计两个阶段，每个阶段都要产生相应的文档。以下选项中，(69)属于逻辑网络设计文档，(70)属于物理网络设计文档。

(69)A.网络IP地址分配方案 B.设备列表清单

C.集中访谈的信息资料 D.网络内部的通信流量分布

(70)A.网络IP地址分配方案 B.设备列表清单

C.集中访谈的信息资料 D.网络内部的通信流量

**【答案】A B**

**【解析】**

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于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五个阶段：需求规范、通信规范、逻辑网络设计、物理网络设计、实施阶段。

在5个阶段中，每个阶段都声一个工作环节，每个环节完毕后才能进入到下一个环节，类似于软件工程中的“瀑布模型”，形成了特定的工作流程。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。

集中访谈和收集信息资料属于需求分析阶段，网络内部通信流量分析属于通信规范阶段，网络IP地址分配方案的制定属于逻辑网辂设计阶段，建立设备列表属于物理网络设计阶段。

Although a given waveform may contain frequencies over a very broad range, as a practical matter any transmission system will be able to accommodate only a limited band of (71) . This, in turn, limits the data rate that can be carried on the transmission (72). A square wave has an infinite number of frequency components and hence an infinite (73). However, the peak amplitude of the Mi frequency component, kf，is only 1/k, so most of the (74) in this waveform is in the first few frequency components. In general, any digital waveform will have (75) bandwidth. If we attempt to transmit this waveform as a signal over any medium, the transmission system will limit the bandwidth that can be transmitteD.

(71)A.frequencies B.connections C.diagrams D.resources

(72)A.procedure B.function C.route D.medium

(73)A.source B.bandwidth C.energy D.cost

(74)A.frequency B.energy C.amplitude D.phase

(75)A.small B.limited C.infinite D.finite

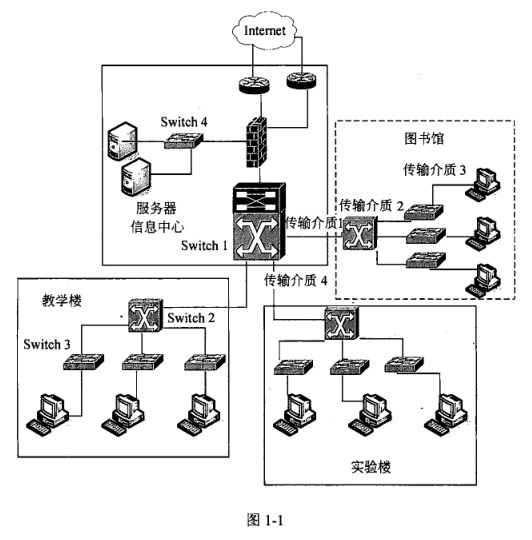
**【答案】A D B B C**

**【解析】**

虽然一个给定的波形包含了很宽的频率范围，但是任何实际的传输系统只能够通过有限的频带。这样，就限制了传输介质可以承载的数据速率。一个方波包含了无限多的频率成分，因而也具有无限的带宽。然而，第k个频率成分的峰值幅度kf只是1/k，所以波形的大部分能量只是包含在前面的少数频率成分中。一般来说，任何数字波形都有无限带宽。如果我们试图在某种介质上传输这种波形信号，则传输系统实际上会限制可以发送的带宽。

**试题一**

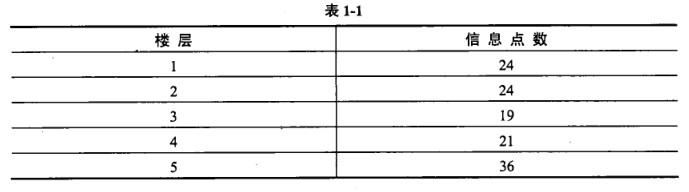
某校园网拓扑结构如图1-1所示。



该网络中的部分需求如下：

1.信息中心距图书馆2千米，距教学楼300米，距实验楼200米。

2.图书馆的汇聚交换机置于图书馆主机房内，楼层设备间共2个，分别位于二层和四层，距图书馆主机房距离均大于200米，其中，二层设备间负责一、二层的计算机接 入，四层设备间负责三、四、五层的计算机接入，各层信息点数如表1-1所示。



3.所有计算机采用静态IP地址。

4.学校网络要求千兆干线，百兆到桌面。

5.信息中心有两条百兆出口线路，在防火墙上根据外网IP设置出口策略，分别从两个出口访问Internet。

6.信息中心共有多台服务器，通过交换机接入防火墙。

7.信息中心提供的信息服务包括Web、FTP、数据库、流媒体等，数据流量较大，要求千兆接入。

**【问题1】**

根据网络的需求和拓扑图，在满足网络功能的前提下，本着最节约成本的布线方式， 传输介质1应采用 （1)，传输介质2应采用（2),传输介质3应采用（3), 传输介质4应采用 （4)。

(1)〜（4)备选答案：

A.单模光纤

B.多模光纤

C.基带同轴电缆

D.宽带同轴电缆

E. 1类双绞线

F. 5类双绞线

(1) A或单模光纤

(2) B或多模光纤

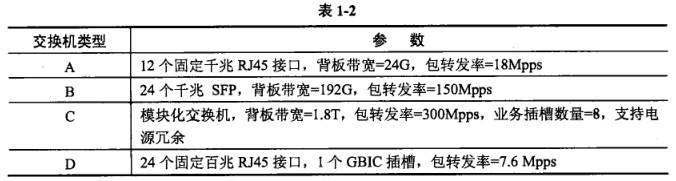
(3) F或5类双绞线

(4) B或多模光纤

本问题考查网络传输介质的选用知识。根据网络的需求和拓扑图，传输介质1连接信息中心核心交换机和图书馆汇聚交换机，两地之间距离2千米，且网络要求千兆干线，所以应该采用单模光纤。传输介质2连接图书馆汇聚交换机和图书馆接入交换机，两地之间距离大于200米，所以应该采用多模光纤。传输介质3连接图书馆接入交换机和接A PC,网络要求百兆到桌面，根据拓扑结构，在选项中应选择5类双绞线。传输介质4 连接信息中心核心交换机和实验楼汇聚交换机，两地之间距离200米，所以应该采用多模光纤。

**【问题2】**

学校根据网络需求选择了四种类型的交换机，其基本参数如表1-2所示。



根据网络需求、拓扑图和交换机参数类型，在图1-1中，Switch 1应采用（5)类型交换机，Switch 2应采用 （6)类型交换机，Switch3应采用 （7)类型交换机， Switch 4应采用 （8)类型交换机。

根据需求描述和所选交换机类型，图书馆二层设备间最少需要交换机 （9)台， 图书馆四层设备间最少需要交换机 （10)台。

(5) C

(6) B

(7) D

(8) A

(9) 2

(10) 4

本问题考査交换机设备选型问题。

根据交换机参数类型判断，A类交换机是12 口千兆RJ45端口交换机，适合做千兆设备接入、B类交换机是24口光纤接口交换机，背板速度较髙，可以作为小型汇聚交换机、C类交换机背板带宽和包转发率高，且为模块化设计，一般用于核心交换机使用，D类交换机是标准百兆的接入交换机。

根据网络需求、拓扑图和交换机参数类型判断，在图1-1中，Switch 1是核心交换机，所以应采用A类型交换机（核心交换机)，Switch 2是教学楼汇聚交换机，应采用B类型交换机（汇聚交换机)，Switch 3是教学楼接入交换机，应采用C类型交换机（百兆接入交换机)，Switch4是信息中心服务器接入交换机，因为信息中心数据流量较大，要求千兆接入，应采用A类型交换机（千兆接入交换机)。

根据需求描述，图书馆二层设备间负责一、二层的计算机接入（共48个接入点），四层设备间负责三、四、五层的计算机接入（共76个接入点）。根据拓扑结构，图书馆接入交换机应采用GBIC插槽，使用多模光纤上联到图书馆汇聚交换机，再根据所选交换机类型参数（24个固定百兆RJ45接口，1个GBIC插槽）判断，图书馆二层设备间最少需要接入交换机2台，图书馆四层设备间最少需要接入交换机4台。

**【问题3】**

该网络采用核心层、汇聚层、接入层的三层架构。根据层次化网络设计的原则，数据包过滤、协议转换应在（11)层完成;(12)层提供高速骨干线路:MAC层过滤和IP地址绑定在（13)层完成。

(11)汇聚层

(12)核心层

(13)接入层

本问题考查层次化网络中各分层的功能的基本概念。

层次化网络模型中一般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；核心层提供高速干线和不同区域的最优传送路径；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，数据包过滤、协议转换都在汇聚层完成；接入层为局域网璋入广域网或者终端用户访问网络提供接入，MAC层过滤和IP地址绑定都在接入层完成。

**【问题4】**

根据该网络的需求，防火墙至少需要（14)个百兆接口和（15)个千兆接口。

(14) 2

(15) 2

本问题考查防火墙设备接口的基本概念。

根据网络拓扑和题目需求描述可知，信息中心有两条百兆出口线路，在防火墙上根据外网IP设置出口策略，分别从两个出口访问Internet，所以防火墙需要2个百兆接口。再根据需求描述可知，内部网络干线为千兆、服务器需要千兆接入，所以防火墙还需要2个千兆接口。

**试题二**

在Linux服务器中，inetd/xinetd是Linux系统中一个重要服务。

**【问题1】**

下面选项中（1) 是xinetd的功能。

(1)备选答案：

A.网络服务的守护进程 B.定时任务的守护进程

C.负责配置网络接口 D.负责启动网卡

Xinetd是一个守护程序，主要用于管理网络服务，因此本题选择A。

**【问题2】**

默认情况下，xinetd配置百录信息为：

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wl_10_s_x_2_1.jpg

则下列说法错误的是（2)。 .

(2) 备选答案：

A. root用户拥有可执行权限

B. 除root用户外，其他用户不拥有执行权限

C. root用户拥有可写权限

D. 除root用户外，其他用户不拥有写权限

本问题考查Linux下文件权限的基础知识，从目录权限信息可知，应选择B。

**【问题3】**

在Linux系统中，inetd服务的默认配置文件为（3)。

(3) 备选答案：

A. /etc/inet.conf B. /etc/inetd.config

C. /etc/inetd.confD. /etc/inet.config

在Linux系统中，默认情况下，xinetd所管理服务的配置文件存放在（4)。

(4) 备选答案：

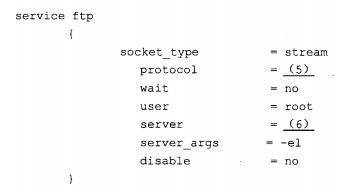
A. /etc/xinetd/ B. /etc/xinetd.d/

C. /usr/etc/xinetd/ D. /usr/etc/xinetd.d/

本问题考查inetd和xinetd的默认配置文件存储位置，默认情况下inetd配置文件存储etc/inetd.conf，xinetd 存储目录为/etc/xinetd.d/，因此（3)选择C，(4)选择B。

**【问题4】**

某Linux服务器上通过xinetd来对各种网络服务进行管理，该服务器上提供ftp服务，ftp服务器程序文件为/usr/bin/ftpd，ftp服务器的配置文件/etc/xinetd.d/ftp内容如下所示，目前该服务器属于开启状态：



请完善该配置文件。

(5) 备选答案：

A. TCP B. UDP

C. IP D. HTTP

(6) 备选答案：

A. /usr/bin/ftpd B. ftpd

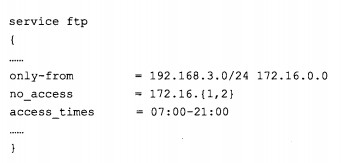
C. ftp D. /bin/ftpd

本问题考查xinetd对网络服务的配置选项基本知识，从题干可知，该服务为ftp服务，服务器程序为/usr/bin/ftpd，由于ftp是基于tcp协议的，因此（5)应选择A，(6) 需要填写服务器程序路径，因此应选择A。

**【问题5】**

xinetd可使用only\_ftom、no\_access以及access\_time等参数对用户进行访问控制。

若服务器上ftp服务的配置信息如下所示：



则下列说法中错误的是（7)。

(7)备选答案：

A. 允许192.168.3.0/24中的主机访问该ftp服务器

B. 172.16.3.0/24网络中的主机可以访问该ftp服务器

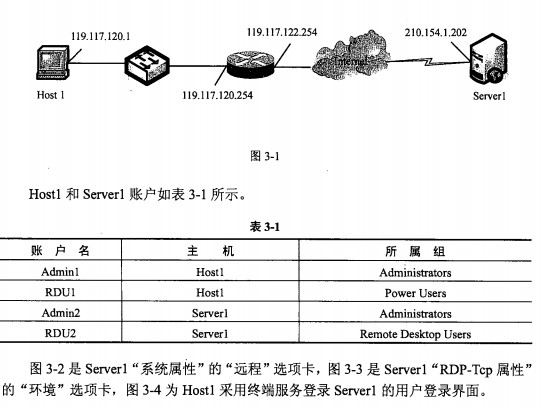
C. IP地址为172.16.X.X的主机可以连接到此主机，但地址属于172.16.1.x、172.16.2.x的则不能连接

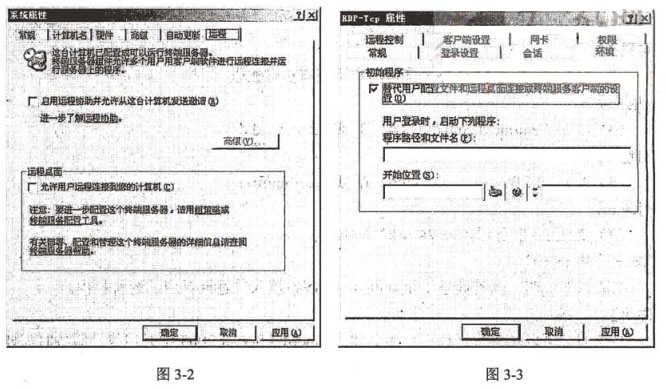
D. ftp服务器可以24小时提供服务

本问题考查xinetd对网络服务的访问权限基本知识，从配置中可以发现，ftp服务不提供24小时访问，因此（7)应选择D。

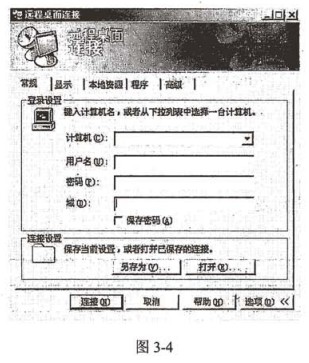
**试题三**

终端服务可以使客户远程操作服务器，Windows Server 2003中开启终端服务时需要 分别安装终端服务的服务器端和客户端，图3-1为客户机Host1连接终端服务器Served的网络拓扑示意图。





此外，在Serverl中为了通过日志了解每个用户的行踪，把“D:\tom\note.bat”设置成用户的登录脚本，通过脚本中的配置来记录日志。



**【问题1】**

默认情况下，RDU2对终端服务具有（1)和（2)权限。 (1)、(2)备选答案：

A.完全控制 B.用户访问 C.来宾访问 D.特别权限

(1) B或用户访问 （2) C或来宾访问 （（1)、(2)答案可互换）

默认情况下只有系统管理员组用户（Administrators)和系统组用户（SYSTEM)拥有访问和完全控制终端服务器的权限，另外远程桌面用户组（Remote Desktop Users)的成员只拥有访问权限而不具备完全控制权。

依据表3-1，RDU2属于远程桌面用户组，故其拥有用户访问和来宾访问的权限。

**【问题2】**

将RDU2设置为Server1的终端服务用户后，在Host1中登录Server1时，图3-4中“计算机”栏应填入（3)；“用户名”栏应填入（4)。

此时发现Host1不能远程登录终端服务器，可能原因是（5) 。

(3) 210.154.1.202 (4) RDU2

(5) 图3-2中没有勾选“允许用户远程连接到您的计算机”复选框

客户机登录终端服务的服务器时，“计算机”栏应填入终端服务器的IP地址；“用户名”'栏应填入终端服务用户，故（3)处应填入210.154.1.202，(4)处应填入RDU2。除此之外，要登录服务器，服务器中必须允许用户远程连接。

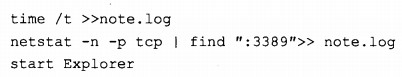
**【问题3】**

在图3-3 “程序路径和文件名”栏中应输入（6)。

(6)处应填入的是日志文件存放的目录，即D:\tom\note.bat。

**【问题4】**

note.bat脚本文件如下：



第一行代码用于记录用户登录的时间，“time/t”的意思是返回系统时间，使用符号“》”把这个时间记入“note.log”作为日志的时间字段。请解释下面命令的含义。

netstat -n -p tcp | find":3389"» note.log

将通过3389端口访问主机的TCP协议状态信息写入note.log文件中，或将远程访问主机的信息记录在日志文件note.log中。

netstat -n -p tcp | fmd":3389"» note.log的目的是将远程访问主机的信息记录在日志文件note.log中，记录3389端口的TCP协议状态。

**试题四**

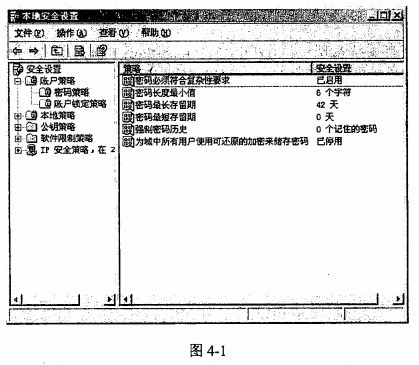
在Windows Server2003系统中，用户分为本地用户和域用户，本地用户的安全策略用“本地安全策略”设置，域用户的安全策略通过活动目录管理。

**【问题1】**

在“本地安全设置”中启用了“密码必须符合复杂性要求”功能，如图4-1所示，则用户“ABC”可以采用的密码是（1) 。

(1)备选答案：

A. ABC007 B. deE#3 C. Testl23 D. adsjfs



（1）C

“本地安全设置”中启用了 “密码必须符合复杂性要求”功能，启用该策略，则密码必须符合以下最低要求：

(1) 不得明显包含用户账户名或用户全名的一部分。

(2) 长度至少为六个字符。

(3) 包含来自以下四个类别中的三个字符：

①英文大写字母（从A到Z)。

②英文小写字母（从a到z)。

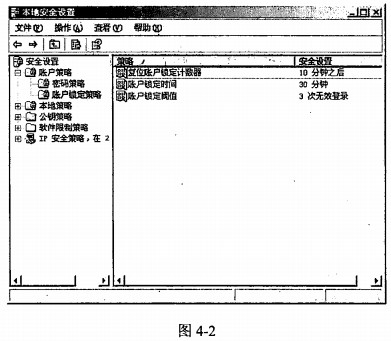
③10个基本数字（从0到9)。

④非字母字符（例如，！、$、#、％)。

备选答案中选项A不满足上述要求1,选项B不满足要求（2),选项D不满足要求(3),同时满足要求（1)、（2)和（3)的密码只有选项C。

**【问题2】**

在“本地安全设置”中，用户账户锁定策略如图4-2所示，当3次无效登录后，用户账户被锁定的实际时间是（2) 。如果“账户锁定时间”设置为0,其含义为（3)。



(2) 备选答案：

A. 30分钟 B. 10分钟 C. 0分钟 D.永久锁定

(3) 备选答案：

A. 账户将一直被锁定，直到管理员明确解除对它的锁定

B. 账户将被永久锁定，无法使用

C. 账户锁定时间无效

D. 账户锁定时间由锁定计数器复位时间决定

（2）A

（3）A

在“本地安全设置”中，用户账户锁定策略中各项设置的含义如下：

(1) 复位账户锁定计数器

此安全设置确定在某次登录尝试失败之后将登录尝试失败计数器重置为0次错误登录尝试之前需要的时间。

(2) 账户锁定时间

此安全设置确定锁定账户在自动解锁之前保持锁定的分钟数。可用范围从0到99 999分钟。如果将账户锁定时间设置为0,账户将一直被锁定直到管理员明确解除对它的锁定。

(3) 账户锁定阈值

此安全设置确定导致用户账户被锁定的登录尝试失败的次数。在管理员重置锁定账户或账户锁定时间期满之前，无法使用该锁定账户。可以将登录尝试失败次数设置为介于0和999之间的值。如果将值设置为0,则永远不会锁定账户。

从图4-2可知，用户3次登录失败后账户将会被锁定，实际锁定时间是30分钟，如果设置账户锁定时间为0,账户将一直被锁定直到管理员明确解除对它的锁定。

**【问题3】**

在Windows Server 2003中活动目录必须安装在（4)分区上，并且需要有（5) 服务的支持。'

(4) 备选答案：

A. NTFS B. FAT32 C. FAT 16 D. ext2

(5) 备选答案：

A. Web B. DHCP C. IIS D. DNS

(4) A

(5) D

安装活动目录的必备条件包括一个NTFS磁盘分区和一个DNS服务器。

安装活动目录过程中，SYSVOL文件夹必须存储在NTFS磁盘分区。SYSVOL文件夹存储着与组策略等有关的数据。

活动目录与DNS是紧密集成的，活动目录中域的名称的解析需要DNS的支持。而域控制器也需要登记到DNS服务器内，以便其他计算机通过.DNS服务器查找到这台域控制器。

**【问题4】**

在Windows Server 2003的活动目录中，用户分为全局组（Global Groups)、域本地组（Domain Local Groups)和通用组（Universal Groups)。全局组的访问权限是（6)， 域本地组的访问权限是（7),通用组的访问权限是（8)。

(6)〜（8)备选答案：

A.可以授予多个域中的访问权限

B. 可以访问域林中的任何资源

C. 只能访问本地域中的资源

(6) B

(7) C

(8) A

在Windows Server 2003的活动目录中，用户分为全局组（Global Groups)、域本地组（Domain Local Groups)和通用组（Universal Groups)。

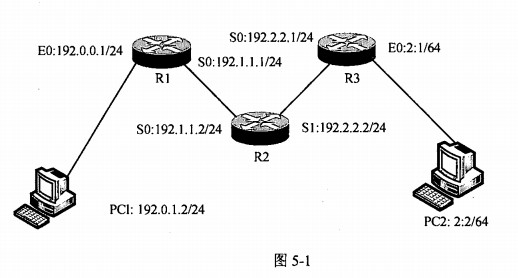
全局组成员来自于同一域的用户账户和全局组，可以访问域林中的任何资源。

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

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

**试题五**

某单位网络内部部署有IPv4主机和IPv6主机，该单位计划采用ISATAP隧道技术实现两类主机的通信，其网络拓扑结构如图5-1所示，路由器R1、R2、R3通过串口经IPv4网络连接，路由器R1连接IPv4网络，路由器R3连接IPv6网段。通过ISATAP隧道将IPv6的数据包封装到IPv4的数据包中，实现PC1和PC2的数据传输。



**【问题1】**

双栈主机使用ISATAP隧道时，IPv6报文的目的地址和隧道接口的IPv6地址都要采 用特殊的ISATAP地址。在ISATAP地址中，前64位是向ISATAP路由器发送请求得到的，后64位中由两部分构成，其中前32位是（1)，后32位是（2)。

(1) 备选答案：

A. 0:5EFE

B. 5EFE:0

C. FFFF:FFFF

D. 0:0

(2) 备选答案：

A. IPv4广播地址

B. IPv4组播地址

C. IPv4单播地址

(1) A或0:5EFE

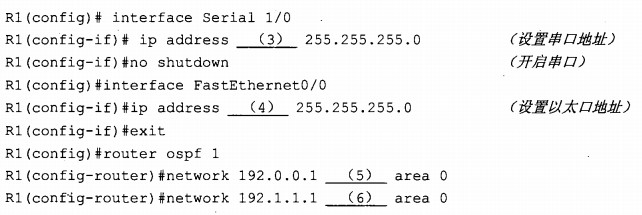
(2) C或IPv4单播地址

本问题考查ISATAP隧道的基本概念。

双栈主机使用ISATAP隧道时，IPv6报文的目的地址和隧道接口的IPv6地址都要采用特殊的地址：ISATAP地址。ISATAP 地址格式为：Prefix (64bit) :0:5EFE:IPv4ADDR, 其中，0:5EFE是IANA规定的格式，IPv4ADDR是单播IPv4地址，它嵌入到IPv6地址的低32位。ISATAP地址的前64位是通过向ISATAP路由器发送请求得到的，如果需要和其他网络的ISATAP客户机或者IPv6网络通信，必须通过ISATAP路由器拿到全球单播地址前缀（2001:，2002:，3ffe:开头），通过路由器与其他IPv6主机和网络通信。

**【问题2】**

根据网络拓扑和需求说明，完成路由器R1的配置。



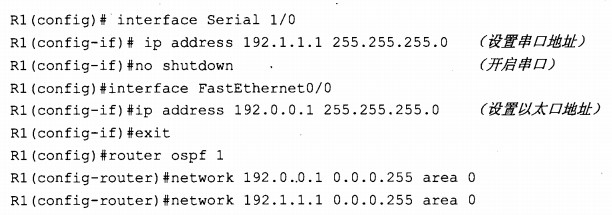
(3) 192.1.1.1

(4) 192.0.0.1

(5) 0.0.0.255

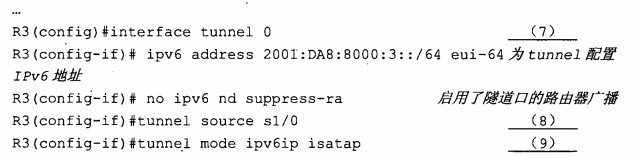
(6) 0.0.0.255

本问题考查路由器接口地址及OSPF的基本配置操作。根据拓扑结构图可知，路由器R1的E0口地址为：192.0.0.1/24; S0 口地址为：192.1.1.1/24，所以配置命令如下：



**【问题3】**

根据网络拓扑和需求说明，解释路由器R3的ISATAP隧道配置。

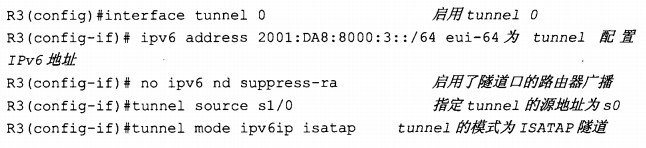


(7) 启用tunnel 0

(8)指定tunnel的源地址为s0

(9) tunnel的模式为ISATAP隧道

本问题考查ISATAP隧道基本配置操作。



**【问题4】**

实现ISATAP,需要在PCI进行配置，请完成下面的命令。

http://www.rkpass.cn:8080/ruankao_work_version_0103/userfile/image/wl_10_s_x_5_4.jpg

(10) 192.2.2.1

本问题考查使用ISATAP隧道时，PC上的基本配置操作。

.实现ISATAP，需要在PC上进行配置，本题中PC1启用双栈，根据拓扑结构图，PC1的IPv6路由应指定R3的S0口地址，所以配置操作如下：

C:\> netsh interface Ipv6 isatap set router 192.2.2.1