位于 CPU 与主存之间的高速缓冲存储器（Cache)用于存放部分主存数据的拷贝， 主存地址与 Cache 地址之间的转换工作由（1）完成。

(1)A.硬件　　B.软件　　C.用户　　D.程序员

【答案】A

【解析】本题考查高速缓冲存储器（Cache)的工作特点。

提供“高速缓存”的目的是为了让数据存取的速度适应 CPU 的处理速度，其基于的原理是内存中“程序执行与数据访问的局域性行为”，即一定程序执行时间和空间内，被访问的代码集中于一部分。为了充分发挥高速缓存的作用，不仅依靠“暂存刚刚访问过的数据”，还要使用硬件实现的指令预测与数据预取技术,即尽可能把将要使用的数据预先从内存中取到高速缓存中。

一般而言，主存使用 DRAM 技术，而 Cache 使用昂贵但较快速的 SRAM 技术。

目前微计算机上使用的 AMD 或 Intel 微处理器都在芯片内部集成了大小不等的数据高速缓存和指令高速缓存，通称为 L1 高速缓存（L1 Cache,即第一级片上高速缓冲存储器)；而比 U 容量更大的 L2 高速缓存曾经被放在 CPU 外部（主板或者 CPU 接口卡上)， 但是现在已经成为 CPU 内部的标准组件；更昂贵的顶级家用和工作站 CPU 甚至会配备比 L2 高速缓存还要大的 L3 高速缓存。

内存单元按字节编址，地址 0000A000H～0000BFFFH 共有（2）个存储单元。

(2)A.8192K　　B.1024K　　C.13K　　D.8K

【答案】D

【解析】本题考查存储器的地址计算知识。

每个地址编号为一个存储单元(容量为 1 个字节),地址区间 0000A000H～0000BFFFH 共有 1FFF+1 个地址编号（即 213)，1K=1024,因此该地址区间的存储单元数为也就是 8K。

相联存储器按（3）访问。

(3)A.地址　　B.先入后出的方式　　C.内容　　D.先入先出的方式

【答案】C

【解析】本题考查相联存储器的概念。

相联存储器是一种按内容访问的存储器。其工作原理就是把数据或数据的某一部分作为

关键字，将该关键字与存储器中的每一单元进行比较，找出存储器中所有与关键字相同的数据字。

相联存储器可用在高速缓冲存储器中，在虚拟存储器中用来作段表、页表或快表存储器，还常用在数据库和知识库中。

若 CPU 要执行的指令为：MOV R1, #45 (即将数值 45 传送到寄存器 R1 中)，则该指令中采用的寻址方式为（4）。

(4)A.直接寻址和立即寻址　　B.寄存器寻址和立即寻址

C.相对寻址和直接寻址　　D.寄存器间接寻址和直接寻址

【答案】B

【解析】本题考查指令系统基础知识。

指令中的寻址方式就是如何对指令中的地址字段进行解释，以获得操作数的方法或获得程序转移地址的方法。

常用的寻址方式有：

•立即寻址。操作数就包含在指令中。

•直接寻址。操作数存放在内存单元中，指令中直接给出操作数所在存储单元的地址。

•寄存器寻址。操作数存放在某一寄存器中，指令中给出存放操作数的寄存器名。

•寄存器间接寻址。操作数存放在内存单元中，操作数所在存储单元的地址在某个寄存器中。

•间接寻址。指令中给出操作数地址的地址。

•相对寻址。指令地址码给出的是一个偏移量（可正可负），操作数地址等于本条指令的地址加上该偏移量。

•变址寻址。操作数地址等于变址寄存器的内容加偏移量。

题目给出的指令中，R1 是寄存器，属于寄存器寻址方式，45 是立即数，属于立即寻址方式。

数据流图(DFD)对系统的功能和功能之间的数据流进行建模，其中顶层数据流图描述了系统的（5)。

(5)A.处理过程　　B.输入与输出　　C.数据存储　　D.数据实体

【答案】B

【解析】本题考查数据流图的基本概念。

数据流图从数据传递和加工的角度，以图形的方式刻画数据流从输入到输出的移动变换

过程，其基础是功能分解。对于复杂一些的实际问题，在数据流图中常常出现许多加工，这样看起来不直观，也不易理解，因此用分层的数据流图来建模。按照系统的层次结构进行逐步分解，并以分层的数据流图反映这种结构关系。

在分层的数据流图中，各层数据流图之间应保持“平衡”关系，即输入和输出数据流在各层应该是一致的。

以下关于类继承的说法中，错误的是（6）。

(6)A.通过类继承，在程序中可以复用基类的代码

B.在继承类中可以增加新代码

C.在继承类中不能定义与被继承类（基类）中的方法同名的方法

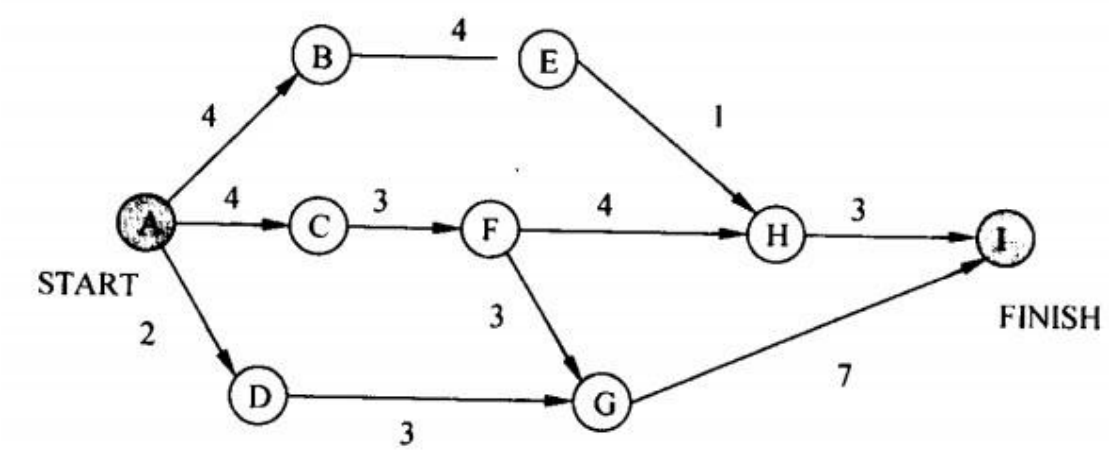
D.在继承类中可以覆盖被继承类（基类）中的方法

【答案】C

【解析】本题考查面向对象的基本知识。

继承是面向对象技术的核心概念之一，它是父类和子类之间共享数据和方法的机制，是类之间的一种关系。在定义和实现一个类的时候，可以在一个已经存在的类的基础上来进行，把这个已经存在的类所定义的内容作为自己的内容，并加入若干新的内容，也可以定义和被继承类相同方法名称的方法，构成方法的重载或覆盖。

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示活动，边上的值表示完成活动所需要的时间，则（7）在关键路径上。



(7)A.B　　B.C　　C.D　　D.H

【答案】B

【解析】本题考查项目管理及工具技术。

根据关键路径法，计算出关键路径为 A—C—F—G—I,关键路径长度为 17。因此里程碑 C 在关键路径上，而里程碑 B、D 和 H 不在关键路径上。

软件开发的增量模型（8）。

(8)A.最适用于需求被清晰定义的情况　B.是一种能够快速构造可运行产品的好方法

C.最适合于大规模团队开发的项目　D.是一种不适用于商业产品的创新模型

【答案】B

【解析】本题考查软件开发过程模型。

增量模型是一种阶段化的软件开发过程模型。在该过程模型中，客户提出系统需求，并指出哪些需求是最重要的。开发团队把软件产品作为一系列的增量构件来设计、编码、集成和测试。每个构件由多个相互作用的模块构成，并且能完成特定的功能。其优点包括：能在较短时间内向用户提交可完成一些有用的工作产品；逐步增加产品的功能，使用户有较充裕的时间学习和适应新产品；项目失败的风险较低；优先级最高的服务首先交付，然后依次将其他构件集成进来，这意味着最重要的服务将接受最多的测试。因此增量模式是一种能够快速构造可运行产品的方法，也适用于今天竞争激烈，需要快速发布产品的市场环境。

假设某软件公司与客户签订合同开发一个软件系统，系统的功能有较清晰的定义， 且客户对交付时间有严格要求，则该系统的开发最适宜采用（9）。

(9)A.瀑布模型　B.原型模型　C.V 模型　D.螺旋模型

【答案】A

【解析】本题考查软件过程模型。

软件过程是软件生存周期中的一系列相关活动,即用于开发和维护软件及相关产品的一系列活动。瀑布模型从一种非常高层的角度描述了软件开发过程中进行的活动，并且提出了要求开发人员经过的事件序列。该模型适用于项目开始时需求已确定的情况。V 模型是瀑布模型的变种，它说明测试活动是如何与分析和设计相联系的。原型模型允许开发人员快速地构造整个系统或系统的一部分以理解或澄清问题。原型的用途是获知用户的真正需求，因此原型模型可以有效地引发系统需求。螺旋模型把开发活动和风险管理结合起来，以将风险减到最小并控制风险。本题中系统功能有较清晰定义意味着需求较确定，且对交付时间有严格要求，因此最适宜用瀑布模型。

中国企业M与美国公司L进行技术合作，合同约定M使用一项在有效期内的美国专利，但该项美国专利未在中国和其他国家提出申请。对于M销售依照该专利生产的产品，以下叙述正确的是 （10）。

(10)A.在中国销售，M需要向L支付专利许可使用费

B.返销美国，M不需要向L支付专利许可使用费

C.在其他国家销售，M需要向L支付专利许可使用费

D.在中国销售，M不需要向L支付专利许可使用费

【答案】D

【解析】本题考查知识产权知识，涉及专利权的相关概念。

知识产权受地域限制，只有在一定地域内知识产权才具有独占性。也就是说，各国依照其本国法律授予的知识产权，只能在其本国领域内受其法律保护，而其他国家对这种权利没有保护的义务，任何人均可在自己的国家内自由使用外国人的知识产品，既无需取得权利人的同意（授权），也不必向权利人支付报酬。例如，中国专利局授予的专利权或中国商标局核准的商标专用权，只能在中国领域内受保护，在其他国家则不给予保护。外国人在我国领域外使用中国专利局授权的发明专利不侵犯我国专利权，如美国人在美国使用我国专利局授权的发明专利不侵犯我国专利权。

通过缔结有关知识产权的国际公约或双边互惠协定的形式，某一国家的国民（自然 人或法人）的知识产权在其他国家（缔约国）也能取得权益。参加知识产权国际公约的国家（或者签订双边互惠协定的国家）会相互给予成员国国民的知识产权保护。所以，我国公民、法人完成的发明创造要想在外国受保护，必须在外国申请专利。商标要想在外国受保护，必须在外国申请商标注册。著作权虽然自动产生，但它受地域限制，我国法律对外国人的作品并不是都给予保护，只保护共同参加国际条约国家的公民作品。同样，参加公约的其他成员国也按照公约规定，对我国公民和法人的作品给予保护。虽然众多知识产权国际条约等的订立使地域性有时会变得模糊，但地域性的特征不但是知识 产权最“古老”的特征，也是最基础的特征之一。目前知识产权的地域性仍然存在，是否授予权利、如何保护权利仍须由各缔约国按照其国内法来决定。

本题涉及的依照该专利生产的产品在中国或其他国家销售，中国M企业不需要向美国L公司支付这件美国专利的许可使用费。这是因为L公司未在中国及其他国家申请该专利，不受中国及其他国家专利法的保护，因此依照该专利生产的产品在中国及其他国家销售，M企

业不需要向 L 公司支付这件专利的许可使用费。如果返销美国，需要向 L 公司支付这件专利的许可使用费。这是因为这件专利已在美国获得批准，因而受到美国专利法的保护，M 企业依照该专利生产的产品要在美国销售，则需要向 L 公司支付这件专利的许可使用费。

网络中存在各种交换设备，下面的说法中错误的是（11）。

(11)A.以太网交换机根据 MAC 地址进行交换

B.帧中继交换机只能根据虚电路号 DLCI 进行交换

C.三层交换机只能根据第三层协议进行交换

D.ATM 交换机根据虚电路标识进行信元交换

【答案】C

【解析】

以太网交换机根据数据链路层 MAC 地址进行帧交换;帧中继网和 ATM 网都是面向连接的通信网，交换机根据预先建立的虚电路标识进行交换。帧中继的虚电路号是 DLCI，进行交换的协议数据单元为“帧”；而 ATM 网的虚电路号为 VPI 和 VCI，进行交换的协议数据单元为“信元”。

三层交换机是指因特网中使用的高档交换机，这种设备把 MAC 交换的高带宽和低延迟优势与网络层分组路由技术结合起来，其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，同时记住目标 MAC 地址和源 MAC 地址，以及其他相关信息，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。所以三层交换机不但具有路由功能，而且比通常的路由器转发得更快。

通过以太网交换机连接的一组工作站（12）。

(12)A.组成一个冲突域，但不是一个广播域　B.组成一个广播域，但不是一个冲突域

C.既是一个冲突域，又是一个广播域　　D.既不是冲突域，也不是广播域

【答案】B

【解析】

在网络互联设备中，集线器（Hub)工作于第二层，它把从一个端口接收的数据包分发到其他所有端口。任何时刻集线器只允许一个端口发送数据，所以其连接的各个设备构成一个冲突域，同时也是一个广播域。以太网交换机可以识别数据帧中的地址字段， 根据目标地

址进行转发，所以这种设备可以允许多个端口同时接收数据。可以说，以太网交换机的所有端口不是一个冲突域，而是一个广播域。

E1 载波的数据速率是（13） Mb/s，T1 载波的数据速率是（14） Mb/s。

(13)A.1.544　　B.2.048　　C.6.312　　D.8.448

(14)A.1.544　　B.2.048　　C.6.312　　D.8.448

【答案】B　A

【解析】

E1 载波的数据速率是 2.048Mb/s，T1 载波的数据速率是 1.544Mb/s。

设信道带宽为 3400Hz,采用 PCM 编码，采样周期为 125us，每个样本量化为 256 个等级，则信道的数据速率为（15）。

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

【答案】D

【解析】

采用 PCM 编码，数据速率与采样周期和量化等级有关。根据题意，每秒采样 8000 次，每个样本提供 8 位数据，所以数据速率 R=8X8000=64Kb/s。考虑到信道带宽为 3400Hz,根据理论分析（奈奎斯特定理和香农定理）和实际情况（有关国际标准），这样的信道是可以提供这个数据速率的。

曼彻斯特编码的效率是（16） %，4B/5B 编码的效率是（17） %。

(16)A.40　　B.50　　C.80　　D.100

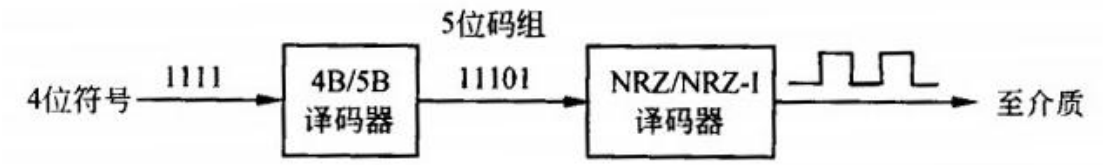
(17)A.40　　B.50　　C.80　　D.100

【答案】B　C

【解析】

在曼彻斯特编码和差分曼彻斯特编码中，每位中间都有一次电平跳变，因此波特率是数据速率的两倍，编码效率为 50%。对于高速网络，如果采用这种编码方法，就需要很高的波特率，其硬件成本则大幅度提高。

为了提高编码的效率，降低电路成本，可以采用 4B/5B 编码。这种编码方法的原理表示如下图所示。



这实际上是一种两级编码方案。在传输介质上传送的是“见 1 就翻不归零码” (NRZ-I),这种编码的效率是 100%，即一个脉冲代表一位。NRZ-I 代码序列中“1”的个数越多，越能提供同步定时信息，但如果遇到长串的“0”，则不能提供同步信息，所以在此之前还需经过一次 4B/5B 编码转换。发送器扫描要发送的位序列，4 位分为一组，然后按照下表的对应规则变换成 5 位的代码。

4B/5B 编码规则表

十六进制数	4 位二进制数	4B/5B 码	十六进制数	4 位二进制数	4B/5B 码
0	0000	11110	8	1000	10010
1	0001	01001	9	1001	10011
2	0010	10100	A	1010	10110
3	0011	10101	B	1011	10111
4	0100	01010	C	1100	11010
5	0101	01011	D	1101	11011
6	0110	01110	E	1110	11100
7	0111	01111	F	1111	11101

5 位二进制代码共有 32 种状态，在 4B/5B 编码规则表中选用的 5 位代码中 1 的个数都不小于 2 个，这就保证了在介质上传输的代码能提供足够多的同步信息。由于 5 个位实际上表示的是 4 位原始数据，因此其编码效率为 80%。

另外还有 5B/6B、8B/10B 等编码方法，其原理是类似的。

ARP 协议的作用是（18)，它的协议数据单元封装在（19)中传送。ARP 请求是采用（20)方式发送的。

(18)A.由 MAC 地址求 IP 地址　　B.由 IP 地址求 MAC 地址

C.由 IP 地址查域名　　D.由域名查 IP 地址

(19)A.IP 分组　　B.以太帧　　C.TCP 段　　D.UDP 报文

(20)A.单播　　B.组播　　C.广播　　D.点播

【答案】B　B　C

【解析】

IP 地址是分配给主机的逻辑地址，在因特网中表示唯一的主机。另外，各个局域网（称为子网）中的主机都有一个子网内部唯一的地址，这种地址是在子网建立时一次性指定的，

甚至可能是与网络硬件相关的，称这个地址为主机的物理地址或硬件地址。

从网络互连的角度看，逻辑地址在整个互连网络中有效，而物理地址只是在子网内部有效；逻辑地址由 Internet 层使用，而物理地址由子网访问子层（即数据链路层） 使用。

由于有两种主机地址，因而需要一种映像关系能把这两种地址对应起来。在 Internet 中用地址分解协议（Address Resolution Protocol, ARP)来实现逻辑地址到物理地址映像。ARP 分组的格式如下图所示，各字段的含义解释如下：

•硬件类型：网络接口硬件的类型，对以太网此值为 1。

•协议类型：发送方使用的协议，0800H 表示 IP 协议。

•硬件地址长度：对以太网，地址长度为 6 字节。

•协议地址长度：对 IP 协议，地址长度为 4 字节。

•操作类型：

- 1——ARP 请求；
- 2——ARP 响应；
- 3——RARP 请求；
- 4——RARP 响应。

硬件类型		协议类型
硬件地址长度	协议地址长度	操作类型
发送结点硬件地址		
发送结点协议地址		
目标结点硬件地址		
目标结点协议地址		

通常 Internet 应用程序把要发送的报文交给 IP 协议，IP 当然知道接收方的逻辑地址(否则就不能通信了)，但不一定知道接收方的物理地址。在把 IP 分组向下传送给本地数据链路实体之前可以用两种方法得到目标物理地址：

（1）查本地内存中的 ARP 地址映像表，其逻辑结构如下表所示。可以看出这是 IP 地址和以太网地址的对照表。

（2）如果 ARP 表查不到，就广播一个 ARP 请求分组，这种分组经过路由器进一步转发，可以到达所有连网的主机。收到该分组的主机一方面可以用分组中的两个源地址更新自己的 ARP 地址映像表，一方面用自己的 IP 地址与目标结点协议地址字段比较，若相符则发回一

个 ARP 响应分组，向发送方报告自己的硬件地址；若不相符，则不予回答。

ARP 地址映像表

IP 地址	以太网地址
130.130.87.1	08 00 39 00 29 D4
129.129.52.3	08 00 5A 21 17 22
192.192.30.5	08 00 10 99 A1 44

RIP 是一种基于（21)算法的路由协议，一个通路上最大跳数是（22)，更新路由表的原则是到各个目标网络的（23)。

(21)A.链路状态　　B.距离矢量　　C.固定路由　　D.集中式路由

(22)A.7　　B.15　　C.31　　D.255

(23)A.距离最短　　B.时延最小　　C.流量最小　　D.路径最空闲

【答案】B　B　A

【解析】

RIP 协议采用 Bellman-Ford 的距离矢量路由算法,用于在 TCP/IP 的网络中计算最佳路由。RIP 以跳步计数（hop count)来度量路由费用，跳步数最小被认为是距离最短。RIP 适用于小型网络，允许的跳步数不超过 15 跳，16 跳是不可到达网络，经过 16 跳的任何分组将被路由器丢弃。

OSPF 协议使用（24）报文来保持与其邻居的连接。下面关于 OSPF 拓扑数据库的描述中，正确的是（25）。

(24)A.Hello　　B.Keepalive　　C.SPF　　D.LSU

(25)A.每一个路由器都包含了拓扑数据库的所有选项

B.在同一区域中的所有路由器包含同样的拓扑数据库

C.使用 Dijkstra 算法来生成拓扑数据库

D.使用 LSA 分组来更新和维护拓扑数据库

【答案】A　D

【解析】

OSPF 是一种链路状态协议，用于在自治系统内部的路由器之间交换路由信息。OSPF 路由器根据收集到的链路状态信息构造网络拓扑结构图，使用 Dijkstra 最短通路优先算法(SPF)计算到达各个目标的最佳路由。

下表列出了 OSPF 协议的 5 种报文，这些报文通过 TCP 连接传送。OSPF 路由器启动后以固定的时间间隔泛洪传播 Hello 报文，采用目标地址 224.0.0.5 代表所有的 OSPF 路由器。在点对点网络上每 10s 发送一次，在 NBMA 网络中每 30s 发送一次。管理 Hello 报文交换的规则称为 Hello 协议。Hello 协议用于发现邻居，建立毗邻关系，还用于选举区域内的指定路由器 DR 和备份指定路由器 BDR。

OSPF 的 5 种报文类型表

类型	报 文 类 型	功 能 描 述
1	Hello	用于发现相邻的路由器
2	数据库描述 DBD(DataBase Description)	表示发送者的链路状态数据库内容
3	链路状态请求 LSR(Link-State Request)	向对方请求链路状态信息
4	链路状态更新 LSU(Link-State Update)	向邻居路由器发送链路状态通告
5	链路状态应答 LSAck(Link-State Acknowledgement)	对链路状态更新报文的应答

OSPF 路由器之间通过链路状态公告（Link State Advertisment，LSA)交换网络拓扑信息。LSA 中包含连接的接口、链路的度量值（Metric)等信息。

在多区域网络中，OSPF 路由器可以按不同的功能划分为以下 4 种：

①内部路由器。所有接口在同一区域内的路由器，只维护一个链路状态数据库。

②主干路由器。具有连接主干区域接口的路由器。

③区域边界路由器（ABR)。连接多个区域的路由器，一般作为一个区域的出口。ABR 为每一个连接的区域建立一个链路状态数据库，负责将所连接区域的路由摘要信息发送到主干区域，而主干区域上的 ABR 则负责将这些信息发送给各个区域。

④自治系统边界路由器（ASBR)。至少拥有一个连接外部自治系统接口的路由器，负责将外部非 OSPF 网络的路由信息传入 OSPF 网络。

在正常情况下，区域内的路由器与本区域的 DR 和 BDR 通过互相发送数据库描述报文（DBD)交换链路状态信息。路由器把收到的链路状态信息与自己的链路状态数据库进行比较，如果发现接收到了不在本地数据库中的链路信息，则向其邻居发送链路状态请求报文 LSR，要求传送有关该链路的完整更新信息。接收到 LSR 的路由器用链路状态更新 LSU 报文响应，其中包含了有关的链路状态通告 LSA。LSAck 用于对 LSU 进行确认。

根据以上说明，并不是每个路由器都包含了拓扑数据库的所有选项，在同一区域中的路由器包含的拓扑数据库也不一定完全相同。

TCP 协议使用（26）次握手机制建立连接，当请求方发出 SYN 连接请求后，等待对方回答（27），这样可以防止建立错误的连接。

(26)A.1　　B.2　　C.3　　D.4

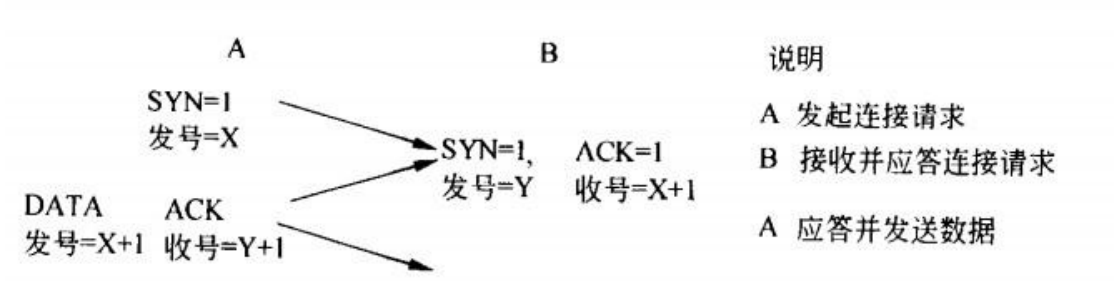
(27)A.SYN，ACK　　B.FIN，ACK　　C.PSH，ACK　　D.RST，ACK

【答案】C　A

【解析】

TCP 建立和释放连接的过程采用三次握手协议。这种协议的目的是连接两端都要声明自己的连接端点标识，并回答对方的连接端点标识，以确保不出现错误的连接。

同步标志 SYN 用于连接建立阶段。建立连接的过程如下：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 X，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 Y（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 Y+1 的段回答，连接就正式建立了。可见，所谓初始顺序号是收发双方对连接的标识，也与字节流的位置有关，参见下图。



采用 DHCP 分配 IP 地址无法做到（28），当客户机发送 dhcpdiscover 报文时采用(29)方式发送。

(28)A.合理分配 IP 地址资源　　B.减少网管员工作量

C.减少 IP 地址分配出错可能　　D.提高域名解析速度

(29)A.广播　　B.任意播　　C.组播　　D.单播

【答案】D　A

【解析】本题考查考生对 DHCP 协议及其工作过程的掌握程度。

采用 DHCP 协议可以自动分配 IP 地址，便于网络管理员依据上网实际用户数合理、动态地分配地址资源，从而达到减轻工作量的目的。由于 IP 地址资源的分配是由服务器依据地址池进行分配的，减少了分配地址出错的可能，但地址的分配和域名解析不存在直接的联系，无法做到提高域名解析速度。

通过 DHCP 服务器分配 IP 地址的工作流程为：寻找 DHCP 服务器、提供 IP 租用、接受 IP 租约及租约确认 4 步，分别对应的报文为 Dhcpdiscover、Dhcpoffer、Dhcprequest 和 Dhcpack。当客户端发送 dhcpdiscover 报文时尚不清楚提供服务的 DHCP 服务器，只能采用广播方式发送。

客户端登录 FTP 服务器后使用 (30)命令来上传文件。

(30)A.get　　B.!dir　　C.put　　D.bye

【答案】C

【解析】本题考查 FTP 服务器相关命令。

部分命令及功能如下：

put：put 或 send 的功能是把本地计算机的一个文件上传到远程主机上。

get：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。

!dir：显示远程计算机上的目录文件和子目录列表。

bye：结束 FTP 服务。

SMTP 传输的邮件报文采用(31)格式表示。

(31)A.ASCII　　B.ZIP　　C.PNP　　D.HTML

【答案】A

【解析】本题考查 SMTP 协议及相关服务。

SMTP 传输的邮件报文需采用 ASCII 进行编码。

在下列选项中，属于 IIS 6.0 提供的服务组件是(32)。

(32)A.Samba　　B.FTP　　C.DHCP　　D.DNS

【答案】B

【解析】本题考查 IIS6.0 组件及相关服务。

IIS 6.0 提供了更为方便的安装/管理功能和增强的应用环境、基于标准的分布协议、改进的性能表现和扩展性，以及更好的稳定性和易用性。其服务组件包括：

①WWW 服务。WWW 是图形最为丰富的 Internet 服务。Web 具有很强的链接能力，支持协作和工作流程，可以给分布在世界各地的用户提供商业应用程序。

②FTP 服务。文件传输协议是在 Internet 中两个远程计算机之间传送文件的协议。该协议

允许用户使用 FTP 命令对远程计算机中的文件系统进行操作。

③SMTP 服务。简单邮件传输协议在客户端应用程序和远程计算机的邮件服务器之间传送邮件信息。

④POP3 服务。POP3 的功能是邮件的存储和管理，能为用户提供账号、密码和身份验证功能，与 SMTP 服务配合，提供完整的邮件服务。

与 route print 具有相同功能的命令是（33）。

(33)A.ping　　B.arp -a　　C.netstat -r　　D.tracert -d

【答案】C

【解析】本题考查网络管理命令的使用及其作用。

route print 用于显示路由表项，比如要显示整个路由器的内容，则输入“route print”；要显示路由表中以“10.”开头的表项，则输入“routeprint 10.*”。

Netstat 命令用于显示 TCP 连接、计算机正在监听的端口、以太网统计信息、IP 路由表、IPv4 统计信息（包括 IP、ICMP、TCP 和 UDP 等协议）和 IPv6 统计信息（包括 IPv6、 ICMPv6、TCP over IPv6 和 UDP over IPv6 等协议）等。Netstat-r 显示 IP 路由表的内容，其作用等价于路由打印命令 route print。

下面的 Linux 命令中，能关闭系统的命令是（34）。

(34)A.kill　　B.shutdown　　C.exit　　D.logout

【答案】B

【解析】本题考查 Linux 基本操作方面的知识。

题中的 4 个选项中，kill 用于发送 SIGKILL 信号，可以用于杀死进程；shutdown 用于关闭系统；exit 是一个系统调用，用于退出进程，也是一个命令，可以关闭控制台程序；logout 用于注销用户。

在 Linux 中，DNS 服务器的配置文件是（35）。

(35)A./etc/hostname　　B./etc/host.conf

C./etc/resolv.conf　　D./etc/httpd.conf

【答案】C

【解析】本题考查 DNS 服务器配置方面的知识。

DNS 服务器的配置文件是/etc/resolv.conf，Web 服务器的配置文件是/etc/httpd.conf。

在Linux中，可以利用(36)命令来终止某个进程。

(36)A.kill　　B.dead　　C.quit　　D.exit

【答案】A

【解析】本题考查Linux基本操作方面的知识。

kill可以用于终止进程；dead不是一个有效命令；quit和exit可以用于关闭控制台程序。

DNS服务器中提供了多种资源记录，其中(37)定义了区域的邮件服务器及其优先级。

(37)A.SOA　　B.NS　　C.PTR　　D.MX

【答案】D

【解析】本题考查DNS服务器中提供的资源记录。

资源记录分为许多不同的类型，常用的有：

•SOA (Start Of Authoritative)：开始授权记录是区域文件的第一条记录，指明区域的主服务器，指明区域管理员的邮件地址，并给出区域复制的有关信息。

•生命期（TTL):资源记录在其他名字服务器缓存中保存的最少有效时间（秒）。

•A (Address)：地址记录表示主机名到IP地址的映像。

•PTR (Pointer)：指针记录是IP地址到主机名的映射。

•NS (Name Server)：给出区域的授权服务器。

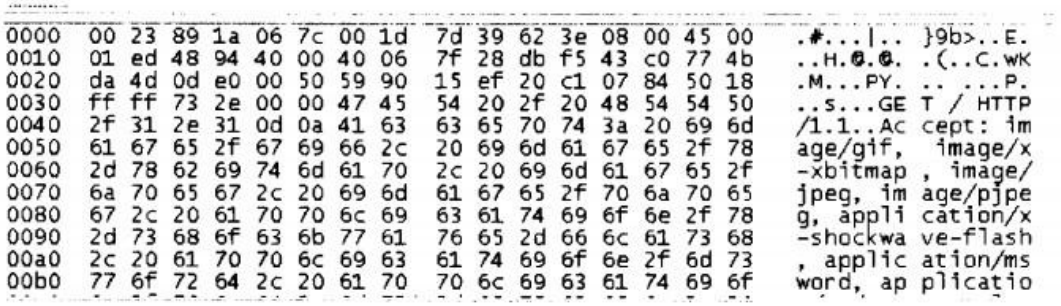
MX (Mail exchanger)：定义了区域的邮件服务器及其优先级（搜索顺序）。

CNAME：为正式主机名（canonical name)定义了一个别名（alias)。

某用户正在Internet浏览网页，在Windows命令窗口中输入(38)命令后得到下图所示的结果。

```
C:\Documents and Settings\User>
Interface: 219.245.67.192 --- 0x2
  Internet Address      Physical Address      Type
  219.245.67.254        10-2B-89-2A-16-7D     dynamic
```

若采用抓包器抓获某一报文的以太帧如下图所示，该报文是（39）。



```
0000  00 23 89 1a 06 7c 00 1d  7d 39 62 3e 08 00 45 00   .#...|.. }9b>..E.
0010  01 ed 48 94 40 00 40 06  7f 28 db f5 43 c0 77 4b   ..H.@.@. .(..C.wK
0020  da 4d 0d e0 00 50 59 90  15 ef 20 c1 07 84 50 18   .M...PY. .. ...P.
0030  ff ff 73 2e 00 00 47 45  54 20 2f 20 48 54 54 50   ..s...GE T / HTTP
0040  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 69 6d   /1.1..Ac cept: im
0050  61 67 65 2f 67 69 66 2c  20 69 6d 61 67 65 2f 78   age/gif,  image/x
0060  2d 78 62 69 74 6d 61 70  2c 20 69 6d 61 67 65 2f   -xbitmap , image/
0070  6a 70 65 67 2c 20 69 6d  61 67 65 2f 70 6a 70 65   jpeg, im age/pjpe
0080  67 2c 20 61 70 70 6c 69  63 61 74 69 6f 6e 2f 78   g, appli cation/x
0090  2d 73 68 6f 63 6b 77 61  76 65 2d 66 6c 61 73 68   -shockwa ve-flash
00a0  2c 20 61 70 70 6c 69 63  61 74 69 6f 6e 2f 6d 73   , applic ation/ms
00b0  77 6f 72 64 2c 20 61 70  70 6c 69 63 61 74 69 6f   word, ap plicatio
```

(38)A.arp -a　　B.ipconfig /all　　C.route　　D.nslookup

(39)A.由本机发出的 Web 页面请求报文

B.由 Internet 返回的 Web 响应报文

C.由本机发出的查找网关 MAC 地址的 ARP 报文

D.由 Internet 返回的 ARP 响应报文

【答案】A　　A

【解析】本题考查对实际的网络管理与分析工具的使用情况。

图中显示的是 IP 地址与物理地址的映射表，实现这一功能的协议是 ARP，命令为 arp -a。从结果图中可以从两个方面得出报文的信息：首先从图中右侧的文字信息 GET 和 HTTP 1.0 中可以看出，是由客户端发送的 HTTP 请求报文，因此是由本机发出的 Web 页面请求报文。此外，从捕获的以太帧中，目的 MAC 为网关、源 IP 为本地 PC 也能判断出相同结果。

在 Windows 系统中，默认权限最低的用户组是（40）。

(40)A.everyone　　B.administrators　　C.power users　　D.users

【答案】A

【解析】本题考查 Windows 用户权限方面的知识。

在以上 4 个选项中，用户组默认权限由高到低的顺序是 administrators—power users— users—everyone。

IIS6.0 支持的身份验证安全机制有 4 种验证方法，其中安全级别最高的验证方法是(41)。

(41)A.匿名身份验证　　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】B

【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.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。

①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。

②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。

③.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。

④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。

以下关于钓鱼网站的说法中，错误的是(42)。

(42)A.钓鱼网站仿冒真实网站的 URL 地址

B.钓鱼网站是一种网络游戏

C.钓鱼网站用于窃取访问者的机密信息

D.钓鱼网站可以通过 Email 传播网址

【答案】B

【解析】本题考查网络安全方面的知识。

钓鱼网站是指一类仿冒真实网站的 URL 地址，通过 E-mail 传播网址，目的是窃取用户账号、密码等机密信息的网站。

支持安全 Web 服务的协议是(43)。

(43)A.HTTPS　　B.WINS　　C.SOAP　　D.HTTP

【答案】A

【解析】本题考查网络安全方面的知识。

Web 服务的标准协议是 HTTP 协议，HTTPS 对 HTTP 协议增加了一些安全特性。WINS 是 Windows 系统的一种协议。SOAP 是基于 HTTP 和 XML，用于 Web Service 的简单对象访问协议。

甲和乙要进行通信，甲对发送的消息附加了数字签名，乙收到该消息后利用(44) 验证该消息的真实性。

(44)A.甲的公钥　　B.甲的私钥　　C.乙的公钥　　D.乙的私钥

【答案】A

【解析】本题考查数字签名的概念。

数字签名（Digital Signature)技术是不对称加密算法的典型应用：数据源发送方使用自己的私钥对数据校验和（或）其他与数据内容有关的变量进行加密处理，完成对数 据的合法“签名”，数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名主要的功能是保证信息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

下列算法中，(45)属于摘要算法。

(45)A.DES　　B.MD5　　C.Diffie-Hellman　　D.AES

【答案】B

【解析】本题考查安全算法方面的知识。

题中的 4 个选项中，DES 是一种经典的数据加密算法，AES 是高级加密算法，Diffie-Hellman 是一种密钥交换算法，MD5 和 SHA 属于报文摘要算法。

网络的可用性是指(46)。

(46)A.网络通信能力的大小　　B.用户用于网络维修的时间

C.网络的可靠性　　D.用户可利用网络时间的百分比

【答案】D

【解析】

可用性是指网络系统、网络元素或网络应用对用户可利用的时间的百分比。有些应用对可用性很敏感，例如，飞机订票系统若宕机一小时，就可能减少几十万元的票款；而股票交

易系统如果中断运行一分钟，就可能造成几千万元的损失。实际上，可用性是网络元素可靠性的表现，而可靠性是指网络元素在具体条件下完成特定功能的概率。如果用平均无故障时间（Mean Time Between Failure, MTBF)来度量网络元素的故障率，则可用性 A 可表示为 MTBF 的函数：

$$A = \frac{MTBF}{MTBF + MTTR}$$

其中 MTTR (Mean Time To Repair)为发生失效后的平均维修时间。由于网络系统由许多网络元素组成，因此系统的可靠性不但与各个元素的可靠性有关，而且还与网络元素的组织形式有关。根据可靠性理论，由元素串并联组成的系统的可用性与网络元素的可用性之间的关系如下图所示。

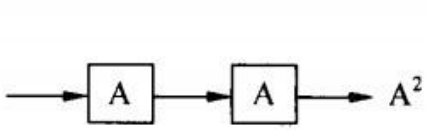


图 a 串联

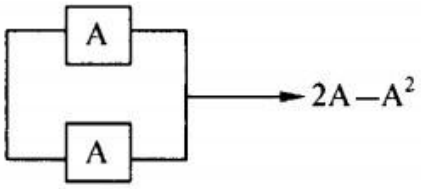


图 b 并联

从图 a 可以看出，若两个元素串联，则可用性减少。例如，两个 Modem 串联在链路的两端，若单个 Modem 的可用性 A=0.98,并假定链路其他部分的可用性为 1，则整个链路的可用性 A=0.98x0.98=0.9604。从图 b 可以看出，若两个元素并联，则可用性增加。例如，终端通过两条链路连接到主机，若一条链路失效，另外一条链路自动备份。假定单个链路的可用性 A=0.98,则双链路的可用性 A=2x0.98 - 0.98x0.98= 1.96 - 0.9604=0.9996。

网络管理的 5 大功能域是（47)。

(47)A.配置管理、故障管理、计费管理、性能管理和安全管理

B.配置管理、故障管理、计费管理、带宽管理和安全管理

C.配置管理、故障管理、成本管理、性能管理和安全管理

D.配置管理、用户管理、计费管理、性能管理和安全管理

【答案】A

【解析】

网络管理有 5 大功能域：故障管理（Fault Management),配置管理（Configuration Management)、计费管理（Accounting Management)、性能管理（Performance Management)

和安全管理（Security Management)，简写为F-CAPS。

SNMPv2提供了3种访问管理信息的方法，这3种方法不包括（48)。

(48)A.管理站向代理发出通信请求　　B.代理向管理站发出通信请求

C.管理站与管理站之间的通信　　D.代理向管理站发送陷入报文

【答案】B

【解析】

SNMPv2提供了3种访问管理信息的方法：

•管理站和代理之间的请求/响应通信，这种方法与SNMPv1是一样的。

•管理站和管理站之间的请求/响应通信，这种方法是SNMPv2特有的，可以由一个管理站把有关管理信息告诉另外一个管理站。

•代理系统到管理站的非确认通信，即由代理向管理站发送陷入报文，报告出现的异常情况。SNMPv1中也有对应的通信方式。

嗅探器改变了网络接口的工作模式，使得网络接口（49)。

(49)A.只能够响应发送给本地的分组　　B.只能够响应本网段的广播分组

C.能够响应流经网络接口的所有分组　　D.能够响应所有组播信息

【答案】C

【解析】

由于以太网采用广播通信方式,因此在网络中传送的分组可以出现在同一冲突域中的所有端口上。在常规状态下，网卡控制程序只接收发送给自己的数据包和广播包，对目标地址不是自己的数据包则丢弃之。如果把网卡配置成混杂模式（Promiscuous Mode)，它就能接收所有分组，无论是否是发送给自己的。

混杂模式通信被广泛地使用在恶意软件中，最初是为了获取根用户权限（Root Compromise),继而进行ARP欺骗（ARP Spoofing)。凡是进行ARP欺骗的计算机必定 把网卡设置成了混杂模式，所以检测那些滥用混杂模式的计算机是很重要的。

嗅探器（Sniffer)就是采用混杂模式工作的协议分析器，可以用纯软件实现，运行在普通的计算机上，也可以做成硬件，用独立设备实现高效率的网络监控。“Sniffer Network Analyzer” 是美国网络联盟公司（Network Associates INC，NAI)的注册商标，然而许多采用类似技术的网络协议分析产品也可以叫做嗅探器。NAI是电子商务和网络安全解决方案

的主要供应商，它的产品除了 Sniffer Pro 之外，还有著名的防毒软件 McAfee。

ICMP 协议的功能包括 (50),当网络通信出现拥塞时，路由器发出 ICMP(51)报文。

(50)A.传递路由信息　　B.报告通信故障　　C.分配网络地址　　D.管理用户连接

(51)A.回声请求　　B.掩码请求　　C.源抑制　　D.路由重定向

【答案】B　C

【解析】

ICMP (Internet control Message Protocol)与 IP 协议同属于网络层，用于传送有关通信问题的消息，例如数据报不能到达目标站，路由器没有足够的缓存空间，或者路由器向发送主机提供最短通路信息等。ICMP 报文封装在 IP 数据报中传送，报文格式如下图所示。其中的类型字段表示 ICMP 报文的类型，代码字段可表示报文的少量参数，当参数较多时写入 32 位的参数字段，ICMP 报文携带的信息包含在可变长的信息字段中，校验和字段是关于整个 ICMP 报文的校验和。

下面解释常见的 ICMP 报文的含义。

①目标不可到达（类型 3):如果路由器判断出不能把 IP 数据报送达目标主机，则向源主机返回这种报文。另一种情况是目标主机找不到有关的用户协议或上层服务访问点，也会返回这种报文。出现这种情况的原因可能是 IP 头中的字段不正确；或是数据报中说明的源路由无效；也可能是路由器必须把数据报分段，但 IP 头中的 D 标志已置位。

②超时（类型 11):路由器发现 IP 数据报的生存期已超时，或者目标主机在一定时间内无法完成重装配，则向源端返回这种报文。

③源抑制（类型 4):这种报文提供了一种流量控制的初等方式。如果路由器或目标主机缓冲资源耗尽而必须丢弃数据报，则每丢弃一个数据报就向源主机发回一个源抑制报文，这时源主机必须减小发送速度。另外一种情况是系统的缓冲区已用完，并预感到行将发生拥塞，则发出源抑制报文。但是与前一种情况不同，涉及的数据报尚能提交给目标主机。

④参数问题（类型 12):如果路由器或主机判断出 IP 头中的字段或语义出错，则返回这种报文，报文头中包含一个指向出错字段的指针。

⑤路由重定向(类型 5):路由器向直接相连的主机发出这种报文，告诉主机一个更短的路径。例如，路由器 R1 收到本地网络上的主机发来的数据报，R1 检查它的路由表，发现要把数据报发往网络 X，必须先转发给路由器 R2,而 R2 又与源主机在同一网络中。于是 R1 向源主机发出路由重定向报文，把 R2 的地址告诉它。

⑥回声（请求/响应，类型 8/0):用于测试两个结点之间的通信线路是否畅通。收到回声请求的结点必须发出回声响应报文。该报文中的标识符和序列号用于匹配请求和响应报文。当连续发出回声请求时，序列号连续递增。常用的 PING 工具就是这样工作的。

⑦时间戳（请求/响应，类型 13/14):用于测试两个结点之间的通信延迟时间。请求方发出本地的发送时间，响应方返回自己的接收时间和发送时间。这种应答过程如果结合强制路由的数据报实现，则可以测量出指定线路上的通信延迟。

⑧地址掩码（请求/响应，类型 17/18):主机可以利用这种报文获得它所在的 LAN 的子网掩码。首先主机广播地址掩码请求报文，同一 LAN 上的路由器以地址掩码响应报文回答，告诉请求方需要的子网掩码。了解子网掩码可以判断出数据报的目标结点与源结点是否在同一 LAN 中。

IP 地址分为公网地址和私网地址，以下地址中属于私网地址的是(52)。

(52)A.10.216.33.124　　B.127.0.0.1　　C.172.34.21.15　　D.192.32.146.23

【答案】A

【解析】

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：

•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

如果子网 172.6.32.0/20 被划分为子网 172.6.32.0/26,则下面的结论中正确的是(53)。

(53)A.被划分为 62 个子网　　B.每个子网有 64 个主机地址

C.被划分为 32 个子网　　D.每个子网有 62 个主机地址

【答案】D

【解析】

子网 172.6.32.0/20 被划分为子网 172.6.32.0/26，网络掩码增加了 6 位，被划分成了 64 个子网，每个子网的主机 ID 部分为 6 位，可以提供主机地址个数为 62。

地址 192.168.37.192/25 是(54),地址 172.17.17.255/23 是(55)。

(54)A.网络地址　　B.组播地址　　C.主机地址　　D.定向广播地址

(55) A.网络地址　　B.组播地址　　C.主机地址　　D.定向广播地址

【答案】C　D

【解析】

地址 192.168.37.192/25 的二进制展开形式为（黑体部分为网络 ID)：

11000000 10101000 00100101 11000000,可见这是一个主机地址。

地址 172.17.17.255/23 的二进制展开形式为（黑体部分为网络 ID)：

10101100 00010001 00010001 11111111，可见这是一个广播地址。

某公司有 2000 台主机，则必须给它分配(56)个 C 类网络。为了使该公司的网络地址在路由表中只占一行，给它指定的子网掩码必须是(57)。

(56)A.2　　B.8　　C.16　　D.24

(57)A.255.192.0.0　　B.255.240.0.0

C.255.255.240.0　　D.255.255.248.0

【答案】B　D

【解析】

每个 C 类网络可提供 254 个主机地址，2000 台主机大约需要 8 个 C 类网络，这些子网合成一个超网，其网络掩码应为 255.25.5.248.0。

以下给出的地址中，属于子网 172.112.15.19/28 的主机地址是(58)。

(58)A.172.112.15.17　　B.172.112.15.14

C.172.112.15.16　　D.172.112.15.31

【答案】A

【解析】

子网 172.112.15.19/28 的二进制形式为 10101100 01110000 00001111 00010011。

4 个选项的展开形式分别为：

选项 A: 172.112.15.17： 10101100 01110000 0000111100010001 选项 B: 172.112.15.14：10101100 01110000 00001111 00001110

选项 C: 172.112.15.16： 10101100 01110000 00001111 00010000 选项 D: 172.112.15.31：10101100 01110000 00001111 00011111

可以看出，选项 A 属于该子网的主机地址，选项 C 是子网地址，而选项 D 是该子网的广播地址。

IPv6 地址分为 3 种类型，它们是（59）。

(59)A. A 类地址、B 类地址、C 类地址　　B. 单播地址、组播地址、任意播地址

C. 单播地址、组播地址、广播地址　　D. 公共地址、站点地址、接口地址

【答案】B

【解析】

IPv6 地址是一个或一组接口的标识符。IPv6 地址被分配到接口，而不是分配给结点。IPv6 地址有 3 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。

这种地址表示一组接口（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。

③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。

FTP 默认的控制连接端口是（60)。

(60)A.20　　B.21　　C.23　　D.25

【答案】B

【解析】

FTP 默认的控制连接端口是 21，数据连接的端口号是 20。

路由器命令 “Router(config)# access-list 1 deny 192.168.1.1 ” 的含义是（61)。

(61)A.不允许源地址为 192.168.1.1 的分组通过

B.允许源地址为 192.168.1.1 的分组通过

C.不允许目标地址为 192.168.1.1 的分组通过

D.允许目标地址为 192.168.1.1 的分组通过

【答案】A

【解析】

标准 ACL 语句只能根据数据包中的源地址进行过滤，可以允许（permit)或阻止 (deny)数据包通过。配置标准 ACL 的路由器命令格式如下：

```
Router(config)# access-list ACL_#  permit|deny source_IP_address
[wildcard_mask] [log]
```

标准 ACL 的编号为 1～99 和 1300～1999,编号之后是路由器实施的动作。匹配条件仅考虑分组的源地址，后随一个任选的通配符掩码。如果忽略了通配符掩码，则默认为 0.0.0.0，即要求整个地址全部匹配。最后的任选 log 参数使得匹配的分组在路由器控制台端口打印输出，但是不会在远程连接的路由器上输出。

路由器命令“ Router(config)# access-list 1 deny 192_168.1_1”的含义是阻止源

地址为192.168.1.1的分组通过。

局域网冲突时槽的计算方法如下。假设tPHY表示工作站的物理层时延，C表示光速，S表示网段长度，tR表示中继器的时延，在局域网最大配置的情况下，冲突时槽等于 (62)。

(62)A.S/0.7C+2tPHY+8tR　　B.2S/0.7C+2tPHY+8tR

C.2S/0.7C+tPHY+8tR　　D.2S/0.7C+2tPHY+4tR

【答案】B

【解析】

IEEE 802.3标准规定的冲突时槽计算方法适用于由4个中继器连接的、5个网段组成的最大配置，整个网络长度达到2500m，其公式为2S/0.7C+2tPHY+8tR。其中2S表示 整个网络长度2倍，即来回传输一圈的距离。0.7C表示光速的0.7倍，2S/0.7C表示来回 传输的时延。2tPHY表示网络两端相距最远的两个网站的物理层时延，而8tR表示来回传输时经过各个中继器的时延。

在局域网标准中，100BASE-T规定从收发器到集线器的距离不超过（63)米。

(63)A.100　　B.185　　C.300　　D.1000

【答案】A

【解析】

在局域网标准中，100BASE-T规定从收发器到集线器的距离不超过100米。

IEEE 802.11 在 MAC 层采用了（64)协议。

(64)A.CSMA/CD　　B.CSMA/CA　　C.DQDB　　D.令牌传递

【答案】B

【解析】

IEEE 802.11在MAC层采用了CSMA/CA协议，即载波监听多路访问/冲突避免协议。其所以不使用CSMA/CD是因为在无线传输的情况下会出现隐蔽终端的问题，使得冲突检测不可行。

在无线局域网中，AP的作用是（65)。新标准IEEE 802.11n提供的最高数据速率可达到（66)。

(65)A.无线接入　　B.用户认证　　C.路由选择　　D.业务管理

(66)A.54Mb/s　　B.100Mb/s　　C.200Mb/s　　D.300Mb/s

【答案】A　　D

【解析】

在无线局域网中，AP 的作用是无线接入，但通常使用的无线路由器则增加了路由等更加复杂的功能。新标准 IEEE 802.11n 提供的最高数据速率可达到 300Mb/s，这也是目前市售的无线接入设备提供的最高数据速率。

IEEE 802.16 工作组提出的无线接入系统空中接口标准是（67）。

(67)A.GPRS　　B.UMB　　C.LTE　　D.WiMAX

【答案】D

【解析】

IEEE 802.16 工作组提出的无线接入系统空中接口标准是一种无线城域网技术\许多网络运营商都加入了支持这个标准的行列。WiMAX (World Interoperability for Microwave Access)论坛是由 Intel 等芯片制造商于 2001 年发起成立的财团，其任务是对 IEEE 802.16 产品进行一致性认证，促进标准的互操作性，其成员囊括了超过 500 家通信行业的运营商和组件/设备制造商。

目前已推出的比较成熟的标准有两个：一个是 2004 年颁布的 IEEE 802.16d，这个标准支持无线固定接入，也叫做固定 WiMAX;另一个是 2005 年颁布的 IEEE802.16e，是在前一标准的基础上增加了对移动性的支持，所以也称为移动 WiMAX。

WiMAX 技术主要有两个应用领域：一个是作为蜂窝网络、Wi-Fi 热点和 Wi-Fi Mesh 的回程链路；另一个是作为最后一公里的无线宽带接入链路。

在无线宽带接入方面，WiMAX 比 Wi-Fi 的覆盖范围更大，数据速率更高。同时，WiMax 较之 Wi-Fi 具有更好的可扩展性和安全性，从而能够实现电信级的多媒体通信服务。高带宽可以补偿 IP 网络的缺陷，从而使 VoIP 的服务质量大大提高。

移动 WiMAX (IEEE 802.16e)向下兼容 IEEE 802.16d,在移动性方面定位的目标速率为车速，可以支持 120km/h 的移动速率。当移动速度较高时，由于多谱勒频移造成系统性能下降，因此必须在移动速率、带宽和覆盖范围之间进行权衡折衷。3G 技术强调地域上的全覆盖和高速的移动性，强调“无所不在”的服务，而 IEEE 802.16 则牺牲了全覆盖，仅保证在一定区域内实现连续覆盖，从而换取了数据传输速率的提高。

安全电子邮件使用（68)协议。

(68)A.PGP　　B.HTTPS　　C.MIME　　D.DES

【答案】A

【解析】

PGP (Pretty Good Privacy)是 Philip R. Zimmermann 在 1991 年开发的电子邮件加密软件包。现在 PGP 已经成为使用最广泛的电子邮件加密软件。PGP 提供两种服务：数据加密和数字签名。数据加密机制可以应用于本地存储的文件，也可以应用于网络上传输的电子邮件。数字签名机制用于数据源身份认证和报文完整性验证。PGP 使用 RSA 公钥证书进行身份认证，使用 IDEA (128 位密钥）进行数据加密，使用 MD5 进行数据完整性验证。

PGP 进行身份认证的过程叫做公钥指纹（Public-Key Fingerprint)。所谓指纹，就是对密钥进行 MD5 变换后所得到的字符串。假如 Alice 能够识别 Bob 的声音，则 Alice 可以设法得到 Bob 的公钥，并生成公钥指纹，通过电话验证他得到的公钥指纹是否与 Bob 的公钥指纹一致，以证明 Bob 公钥的真实性。

建筑物综合布线系统中的园区子系统是指（69)。

(69)A.由终端到信息插座之间的连线系统　　B.楼层接线间到工作区的线缆系统

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】D

【解析】

结构化综合布线系统（Structure Cabling System)是基于现代计算机技术的通信物理平台，集成了语音、数据、图像和视频的传输功能，消除了原有通信线路在传输介质上的差别。

结构化布线系统分为 6 个子系统：工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统。

(1)工作区子系统（Work Location)。

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。

(2)水平布线子系统（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，交连方式取决于网络拓扑结构和工作区设备的要求。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互连，这些短线被称为跳线。通过跳线的调整，可以在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三种：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。最后一种是架空明线，这种方法需要经常维护。

下面有关 RMON 的论述中，错误的是（70)。

(70)A.RMON 的管理信息库提供整个子网的管理信息

B.RMON 的管理信息库属于 MIB-2 的一部分

C.RMON 监视器可以对每个分组进行统计和分析

D.RMON 监视器不包含 MIB-2 的功能

【答案】D

【解析】

通常用于监视整个网络通信情况的设备叫做网络监视器（Monitor)或网络分析器(Analyzer)、探测器（Probe)等。监视器观察LAN上出现的每个分组，并进行统计和总结，给管理人员提供重要的管理信息。监视器还能存储部分分组，供以后分析用。监视器也根据分组类型进行过滤并捕获特殊的分组。通常是每个子网配置一个监视器，并且与中央管理站通信，因此叫做远程监视器。

RMON定义了远程网络监视的管理信息库（属于MIB-2的一部分)，以及SNMP管理站与远程监视器之间的接口。一般地说，RMON的目标就是监视子网范围内的通信，从而减少管理站和被管理系统之间的通信负担。

The TCP protocol is a (71) layer protocol. Each connection connects two TCPs that may be just one physical network apart or located on opposite sides of the globe. In other words, each connection creates a (72) with a length that may be totally different from another path created by another connection. This means that TCP cannot use the same retransmission time for all connections. Selecting a fixed retransmission time for all connections can result in serious consequences. If the retransmission time does not allow enough time for a (73) to reach the destination and an acknowledgment to reach the source, it can result in retransmission of segment that are still on the way. Conversely, if the retransmission time is longer than necessary for a short path, it may result in delay for the application programs. Even for one single connection, the retransmission time should not be fixed. A connection may be able to send segments and receive (74) faster during nontraffic period than during congested periods. TCP uses the dynamic retransmission time, a transmission time is different for each connection and which may be changed during the same connection. Retransmission time can be made (75) by basing it on the round-trip time (RTT). Several formulas are used for this purpose.

(71)A.physical	B.network	C.transport	D.application
(72)A.path	B.window	C.response	D.process
(73)A.process	B.segment	C.program	D.user
(74)A.connections	B.requests	C.acknowledgents	D.datagrams

(75)A.error　　B.short　　C.fixed　　D.dynamic

【答案】C　A　B　C　D

【解析】

TCP 是一种传输层协议。每一个连接都连接了两个 TCP 实体，这两个 TCP 实体可能存在于同一个物理网络中，也可能是分居于地球的两边。换言之，每一个连接都产生了一条通路，其长度与另外一个连接产生的通路完全不同。这就意味着，TCP 不能对所有的连接使用同样的重传时间。对所有的连接选择一个固定的重传时间可能产生严重的后果。如果重传时间不足以使一个段到达目标，或者不足以使一个应答到达源站，这就可能对尚在路途中的段产生重传。反之，如果重传时间比一条短通路所需要的时间长， 则可能对应用程序产生延迟。即使对单个连接，重传时间也不应该固定。一个连接应该能够在非峰值时段比拥堵时段更快地发送数据段和接收应答。TCP 使用了动态重传时间，重传时间对每一个连接是不同的，在同一个连接持续期间也是可以改变的。重传时间可以动态地根据环回时间 (RTT)而改变。为此建立了几个有用的公式。

试题一

某公司计划部署园区网络，其建筑物分布如图 1-1 所示。

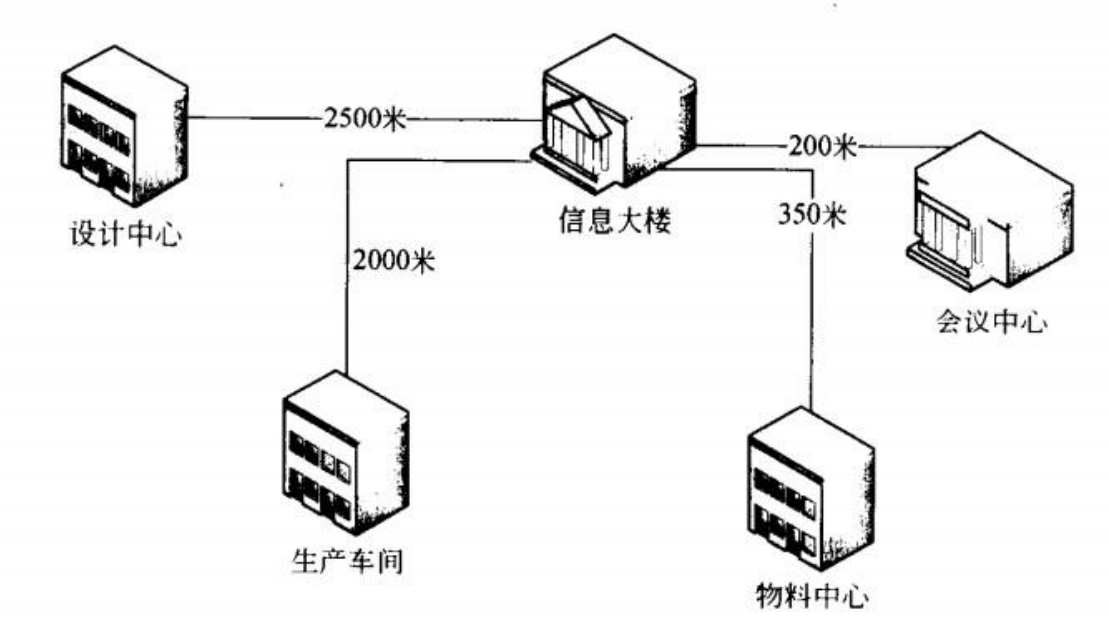


图 1-1

根据需求分析结果，网络规划要求如下：

网络中心机房在信息大楼。

设计中心由于业务需求，要求千兆到桌面；同时要求设计中心汇聚交换机到核心交换机以千兆链路聚合。

会议中心采用 PoE 无线网络部署。

【问题 1】

根据公司网络需求分析，设计人员设计的网络拓扑结构如图 1-2 所示。

1.根据网络需求描述和网络拓扑结构，图 1-2 中介质 1 应选用（1);介质 2 应 选用（2)；介质 3 应选用（3)。

问题（1)～（3)备选答案：（注：每项只能选择一次）

A.单模光纤

B.多模光纤

C.6 类双绞线

D.同轴电缆

2.在该网络中，应至少选用单模 SFP（4)个，多模 SFP（5)个。

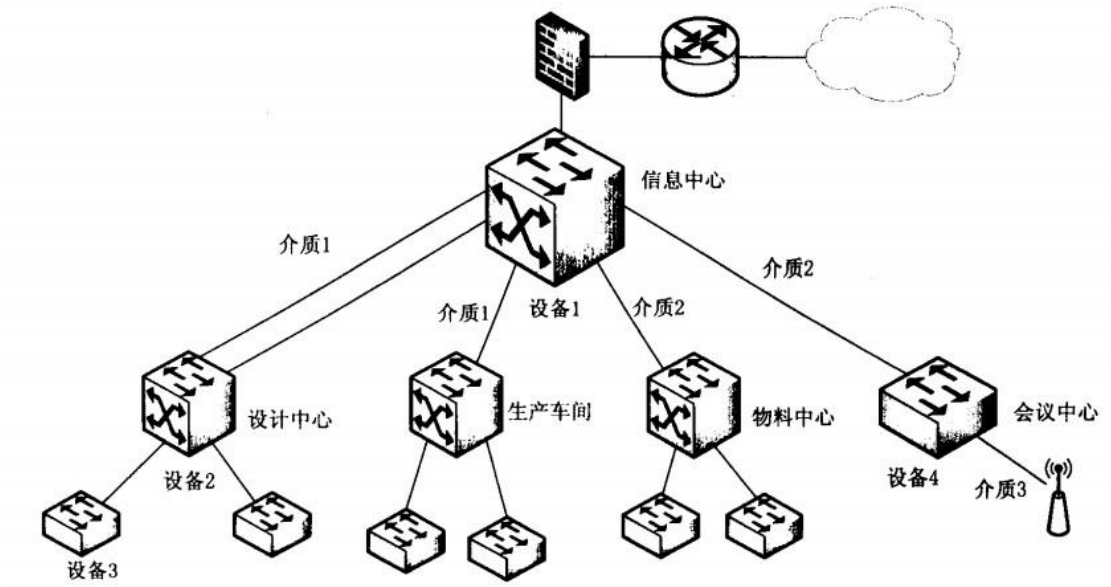


图 1-2

（1）A.单模光纤

（2）B.多模光纤

（3）C. 6 类双绞线

（4）6

（5）4

根据题目说明和建筑物分布图可知，网络中心机房在信息大楼；信息大楼距离设计中心 2500 米；信息大楼距离生产车间 2000 米；信息大楼距离物料中心 350 米；信息大楼距离会议中心 200 米。

由于距离的问题，介质 1（信息大楼至设计中心和生产车间）只能选择单模光纤，介质 2（信息大楼至会议中心和物料中心)可以选择单模光纤和多模光纤，但是题目要求选项只能单选，所以此处只能选择多模光纤；介质 3（会议中心交换机至 AP)由于会议中心采用 PoE 无线网络部署，因此此处只能选择 6 类双绞线。

另外，设计中心汇聚交换机到核心交换机以千兆链路聚合，所以信息大楼至设计中心为双路光纤，这样可以判断在该网络中，应至少选用单模 SFP6 个，多模 SFP4 个。

【问题 2】

该网络部分设备如下表所示：

名称	主要技术指标
设备 A	交换容量≥1Tbps；包转发率≥750Mpps；业务插槽数≥6；双引擎，冗余电源；配置接口≥12 口千兆光口，≥24 口千兆电口
设备 B	交换容量≥190Gbps；包转发率≥40Mpps；接口为 24 个 10/100/1000M 电口；至少有 2 个 1000M SFP 光口；支持 802.1x 认证，MAC 认证和 Web 认证
设备 C	交换容量≥70Gbps；包转发率≥40Mpps；接口为 24 个 10/100/1000M 电口，2 个 1G SFP；可管理 AP 数目≥16；支持高级加密标准(AES)、临时密钥交换协议（TKIP）以及有线对等加密（WEP）、支持 WPA 及 WPA2 加密算法；防止 ARP 欺骗攻击
设备 D	交换容量≥268Gbps；包转发率≥150Mpps；接口为 24 个 10/100/1000Base-T 以太网端口，4 个 1/10G SFP

根据题目说明和网络拓扑图，在图 1-2 中，设备 1 应选用（6），设备 2 应选用（7），设备 3 应选用(8)，设备 4 应选用（9）。

(6)设备 A

(7)设备 D

(8)设备 B

(9)设备 C

根据设备表可知，设备 A 属于核心交换设备；设备 B 属于接入交换设备；设备 C 属于无线管理设备；设备 D 属于汇聚交换设备。再根据网络拓扑图，在图 1-2 中，设备 1 应选用核心交换设备（设备 A），设备 2 应选用汇聚交换设备（设备 D），设备 3 应选用接入交换设备（设备 B），设备 4 应选用无线管理设备（设备 C）。

【问题 3】

该网络在进行地址分配时，其 VLAN 分配如下表所示：

设备	端口连接设备		IP	网关	VLAN ID
	设备名称	接口号			
生产车间汇聚交换机	核心交换机	g2/1			TRUNK
	接入交换机 A	f1/2	192.168.99.0/24	192.168.99.254	VLAN 99
	接入交换机 B	f1/3	192.168.100.0/24	192.168.100.254	VLAN 100
	管理地址		192.168.1.11/24	192.168.1.254	VLAN 1

根据上表，完成下列生产车间汇聚交换机的配置：

```
Switch(config)#interface vlan 99
Switch(config-if)#ip address 192.168.99.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#interface vlan 100
Switch(config-if)#ip address __(10)__ __(11)__
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#interface f1/2
Switch(config-if)#switchport mode __(12)__
Switch(config-if)#switchport access vlan __(13)__
Switch(config-if)#exit

Switch(config)#interface g2/1
Switch(config-if)#switchport mode __(14)__
Switch(config-if)#exit
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway __(15)__
…
```

(10) 192.168.100.254

(11) 255.255.255.0

(12) access

(13) 99

(14) trunk

(15) 192.168.1.254

本题考查的是 VLAN 分配应用的基础知识。根据 VLAN 分配表，生产车间汇聚交换机的配置应如下：

```
Switch(config)#interface vlan 99
Switch(config-if)#ip address 192.168.99.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#interface vlan 100
Switch(config-if)#ip address 192.168.100.254  255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit

Switch(config)#interface f1/2
Switch(config-if)#switchport mode  access
Switch(config-if)#switchport access vlan 99
Switch(config-if)#exit

Switch(config)#interface g2/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.1.254 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.1.254
…
```

试题二

阅读以下说明，回答问题 1 至问题 3,将解答填入答题纸对应的解答栏内。

【问题 1】

Linux 服务器中 DHCP 服务程序/usr/sbin/dhcpd 对应的配置文件名称是（1),该文件的缺省目录是（2)。

(1) dhcpd.conf

(2) /etc

本题考查 Linux 系统中 DHCP 服务的相关配置。

DHCP 是 Dynamic Host Configuratioq Protocol（动态主机配置协议）的缩写。在常见的小型网络中，IP 地址的分配一般都采用静态方式，但在大中型网络中，为每一台计算机分配一个静态 IP 地址的方式会加重网管人员的负担，并且容易导致 IP 地址分配错误。因此，在大中型网络中使用 DHCP 服务是非常有效率的。

Linux 下默认安装 DHCP 服务的配置文件为/etc/dhcpd.conf，DHCP 配置通常包括三部分：parameters、declarations、option。

parameters 用于说明 DHCP 服务工作的网络配置参数，如下表所示。

参　数	参 数 含 义
ddns-update-style	配置 DHCP-DNS 更新模式。更新模式包括 none、interim 和 ad-hoc
default-lease-time	指定缺省的 IP 地址租赁时间，单位是秒
max-lease-time	指定最大租赁时间长度，单位是秒
hardware	指定网卡接口类型和 MAC 地址
server-name	DHCP 服务器名称
get-lease-hostnames flag	检查客户端使用的 IP 地址
fixed-address ip	分配给客户端一个固定的地址
authritative	拒绝不正确的 IP 地址请求

declarations 用来描述网络布局、提供 DHCP 客户的 IP 地址分配策略等，如下表所示。

声　明	参 数 含 义
shared-network	用来设置是否一些 IP 子网共享同一物理网络
subnet	描述一个 IP 地址是否属于该子网
range	提供动态分配 IP 的范围
host	用于定义保留主机
group	为一组参数提供声明
Allow unknown-clients; deny unknown-client	是否动态分配 IP 给未知的使用者
allow bootp;deny bootp	是否响应 BOOTP 查询
Allow booting;deny booting	是否响应 TFTP 查询，主要用于无盘工作站
filename	启动文件的名称，主要用于无盘工作站
next-server	设置 TFTP 服务器的地址，主要用于无盘工作站

option（选项）用来配置 DHCP 可选参数，用 option 关键字作为开始，如下表所示。

选　项	解　释
subnet-mask	为客户端设定子网掩码
domain-name	为客户端指明 DNS 名字
domain-name-servers	为客户端指明 DNS 服务器 IP 地址
host-name	为客户端指定主机名称
routers	为客户端设定默认网关
broadcast-address	为客户端设定广播地址
ntp-server	为客户端设定网络时间服务器 IP 地址
time－offset	为客户端设定和格林威治时间的偏移时间，单位是秒

Linux 下默认安装 DHCP 服务的配置文件为/etc/dhcpd.conf，所以 DHCP 服务对应的配置文件名称是 dhcpd.conf，缺省目录是/etc。

【问题 2】

某网络采用 Linux DHCP 服务器为主机提供服务，查看某主机的网络连接详细信息如图 2-1 所示。

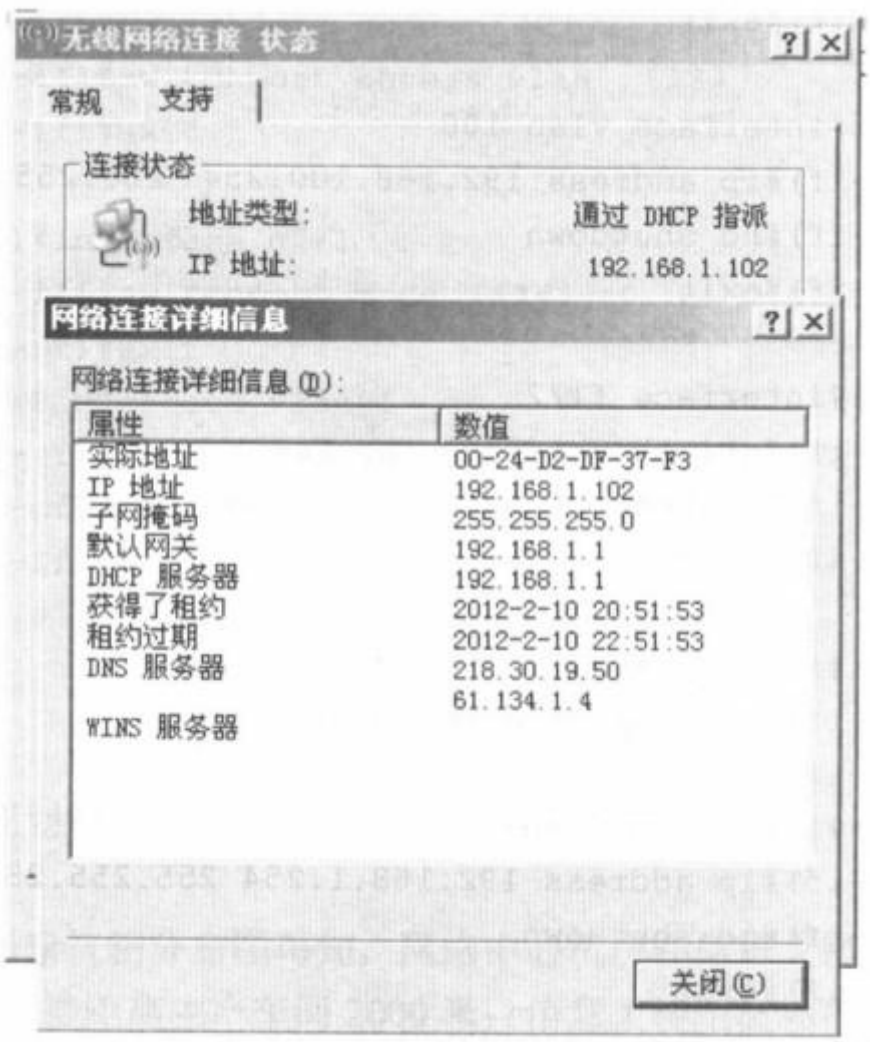


图 2-1

请根据图 2-1 中补充完成 Linux DHCP 服务器中 DHCP 配置文件的相关配置项。

```
…
subnet 192.168.1.0  netmask 255.255.255.0 {
range 192.168.1.10 192.168.1.200;
default-lease-time  (3)  ;
max-lease-time  14400;
option subnet-mask  (4)  ;
option routers  (5)  ;
option domain-name "myuniversity.edu.cn";
option broadcast-address  (6);
option domain-name-servers  (7)  ,  (8)  ;
}
```

(3)7200

(4)255.255.255.0

(5)192.168.1.1

(6)192.168.1.255

(7)218.30.19.50

(8)61.134.1.4

本题考查 Linux 系统中 DHCP 服务的相关配置。

DHCP 是 Dynamic Host Configuratioq Protocol(动态主机配置协议）的缩写。在常见的小型网络中，IP 地址的分配一般都采用静态方式，但在大中型网络中，为每一台计算机分配一个静态 IP 地址的方式会加重网管人员的负担，并且容易导致 IP 地址分配错误。因此，在大中型网络中使用 DHCP 服务是非常有效率的。

Linux 下默认安装 DHCP 服务的配置文件为/etc/dhcpd.conf，DHCP 配置通常包括三部分：parameters、declarations、option。

parameters 用于说明 DHCP 服务工作的网络配置参数，如下表所示。

参　数	参 数 含 义
ddns-update-style	配置 DHCP-DNS 更新模式。更新模式包括 none、interim 和 ad-hoc
default-lease-time	指定缺省的 IP 地址租赁时间，单位是秒
max-lease-time	指定最大租赁时间长度，单位是秒
hardware	指定网卡接口类型和 MAC 地址
server-name	DHCP 服务器名称
get-lease-hostnames flag	检查客户端使用的 IP 地址
fixed-address ip	分配给客户端一个固定的地址
authritative	拒绝不正确的 IP 地址请求

declarations 用来描述网络布局、提供 DHCP 客户的 IP 地址分配策略等，如下表所示。

声　明	参 数 含 义
shared-network	用来设置是否一些 IP 子网共享同一物理网络
subnet	描述一个 IP 地址是否属于该子网
range	提供动态分配 IP 的范围
host	用于定义保留主机
group	为一组参数提供声明
Allow unknown-clients; deny unknown-client	是否动态分配 IP 给未知的使用者
allow bootp;deny bootp	是否响应 BOOTP 查询
Allow booting;deny booting	是否响应 TFTP 查询，主要用于无盘工作站
filename	启动文件的名称，主要用于无盘工作站
next-server	设置 TFTP 服务器的地址，主要用于无盘工作站

option（选项）用来配置 DHCP 可选参数，用 option 关键字作为开始，如下表所示。

选　项	解　释
subnet-mask	为客户端设定子网掩码
domain-name	为客户端指明 DNS 名字
domain-name-servers	为客户端指明 DNS 服务器 IP 地址
host-name	为客户端指定主机名称
routers	为客户端设定默认网关
broadcast-address	为客户端设定广播地址
ntp-server	为客户端设定网络时间服务器 IP 地址
time－offset	为客户端设定和格林威治时间的偏移时间，单位是秒

由图 2-1 可知，default-lease-time 为租约过期时间减去获取租约时间，等于 2 小时，合计 7200 秒。

【问题 3】

如果要确保 IP 地址 192.168.1.102 分配给图 2-1 中的 PC，需要在 DHCP 配置文件中补充以下语句。

(9)　pc1{hardware ethernet　(10)　; fixed-address　(11)　;}

（9）host

（10）00:24:D2:DF:37:F3

（11）192.168.1.102

本题考查 Linux 系统中 DHCP 服务的相关配置。

DHCP 是 Dynamic Host Configuratioq Protocol（动态主机配置协议）的缩写。在常见的小型网络中，IP 地址的分配一般都采用静态方式，但在大中型网络中，为每一台计算机分配一个静态 IP 地址的方式会加重网管人员的负担，并且容易导致 IP 地址分配错误。因此，在大中型网络中使用 DHCP 服务是非常有效率的。

Linux 下默认安装 DHCP 服务的配置文件为/etc/dhcpd.conf，DHCP 配置通常包括三部分：parameters、declarations、option。

parameters 用于说明 DHCP 服务工作的网络配置参数，如下表所示。

参　数	参 数 含 义
ddns-update-style	配置 DHCP-DNS 更新模式。更新模式包括 none、interim 和 ad-hoc
default-lease-time	指定缺省的 IP 地址租赁时间，单位是秒
max-lease-time	指定最大租赁时间长度，单位是秒
hardware	指定网卡接口类型和 MAC 地址
server-name	DHCP 服务器名称
get-lease-hostnames flag	检查客户端使用的 IP 地址
fixed-address ip	分配给客户端一个固定的地址
authritative	拒绝不正确的 IP 地址请求

declarations 用来描述网络布局、提供 DHCP 客户的 IP 地址分配策略等，如下表所示。

声　明	参 数 含 义
shared-network	用来设置是否一些 IP 子网共享同一物理网络
subnet	描述一个 IP 地址是否属于该子网
range	提供动态分配 IP 的范围
host	用于定义保留主机
group	为一组参数提供声明
Allow unknown-clients; deny unknown-client	是否动态分配 IP 给未知的使用者
allow bootp;deny bootp	是否响应 BOOTP 查询
Allow booting;deny booting	是否响应 TFTP 查询，主要用于无盘工作站
filename	启动文件的名称，主要用于无盘工作站
next-server	设置 TFTP 服务器的地址，主要用于无盘工作站

option（选项）用来配置 DHCP 可选参数，用 option 关键字作为开始，如下表所示。

选　项	解　释
subnet-mask	为客户端设定子网掩码
domain-name	为客户端指明 DNS 名字
domain-name-servers	为客户端指明 DNS 服务器 IP 地址
host-name	为客户端指定主机名称
routers	为客户端设定默认网关
broadcast-address	为客户端设定广播地址
ntp-server	为客户端设定网络时间服务器 IP 地址
time－offset	为客户端设定和格林威治时间的偏移时间，单位是秒

host 语句用于保留主机的设置，参数是保留主机的 MAC 地址和对应分配的 IP 地址。

试题三

网络拓扑结构如图 3-1 所示，其中 Web 服务器 WebServer1 和 WebServer2 对应同一域名 www.abc.com，DNS 服务器采用 Windows Server 2003 操作系统。

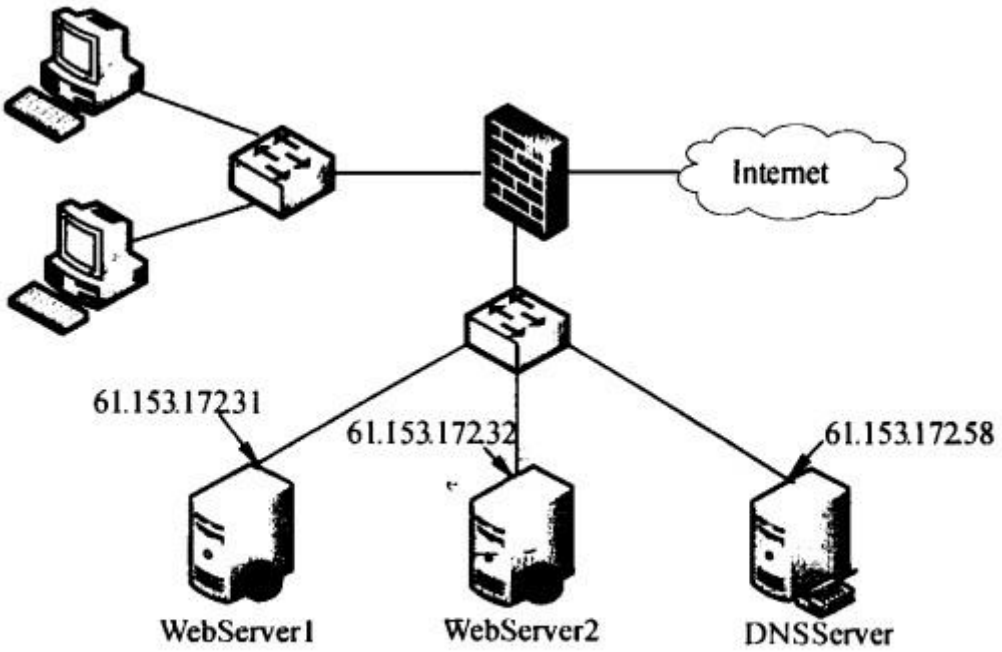


图 3-1

【问题 1】

客户端向 DNS 服务器发出解析请求后，没有得到解析结果，则（1）进行解析。

(1)备选答案：

A.查找本地缓存　B.使用 NetBIOS 名字解析

C.查找根域名服务器 D.查找转发域名服务器

（1）B.使用 NetBIOS 名字解析

DNS 主机名解析的查找顺序是：先查找客户端解析程序缓存；如果没有成功，则向 DNS 服务器发出解析请求；如果还没有成功，则尝试使用 NetBIOS 名字解析方法取得结果。

【问题 2】

在图 3-1 中，两台 Web 服务器采用同一域名的主要目的是什么？

对 Web 服务实现负载均衡或防止单点失效

两台 Web 服务器采用同一域名有两个好处：首先，对同一域名进行解析时可以由 DNS 服务器采用某种策略均衡到两台 Web 服务器上，对 Web 服务实现负载均衡；其次，当某一台服务器产生故障时可以由另一台提供服务，可防止单点失效。

【问题 3】

DNS 服务器为 WebServer1 配置域名记录时，在图 3-2 所示的对话框中，添加的主机“名称”为（2），“IP 地址”是(3)。

采用同样的方法为 WebServer2 配置域名记录。

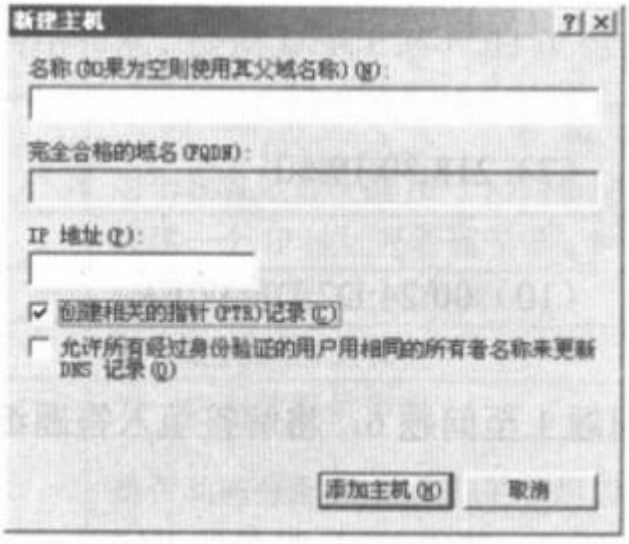


图 3-2

（2）www

（3）61.153. 172.31

DNS 服务器为 WebServer1 配置域名记录时，添加的主机“名称”栏对应的是主机名，即 WWW，“IP 地址”栏应填入提供 Web 服务的 IP 地址，即 61.153.172.31。

【问题 4】

在 DNS 系统中，反向查询（Reverse Query)的功能是（4)。若不希望对域名 www.abc.com 进行反向查询，在图 3-2 所示的窗体中应如何操作？

（4）用 IP 地址查询对应的域名

去掉“创建相关的指针（PTR)记录”

在 DNS 系统中，反向查询的功能是用 IP 地址查询对应的域名。若新建一条 DNS 记录时希望同时创建它的反句查询记录，需勾选“创建相关的指针（PTR)记录”。若不希望对域名 www.abc.com 进行反向查询，需“创建相关的指针（PTR)记录”。

【问题 5】

在图 3-3 中所示的 DNS 服务器属性窗口中应如何配置，才使得两次使用 nslookup www.abc.com 命令得到如图 3-4 所示结果？

图 3-3

```
C:\Documents and Settings\asd>nslookup www.abc.com
Server:  ns.abc.com
Address:  61.153.172.58
Non-authoritative:
Name:  www.abc.com
Addresses:61.153.172.31,61.153.172.32

C:\Documents and Settings\asd>nslookup www.abc.com
Server:  ns.abc.com
Address:  61.153.172.58
Non-authoritative:
Name:  www.abc.com
Addresses:61.153.172.32,61.153.172.31
```

图 3-4

勾选“启用循环”

从结果图中可以看出，在解析 www.abc.com 时，循环对应到了 61.153.172.31 和 61.153.172.32 两个主机，故在 DNS 服务器中应该配置循环功能。

【问题 6】

要测试 DNS 服务器是否正常工作，在客户端可以采用的命令是（5)或（6)。

(5)、(6)备选答案：

A. ipconfig B. nslookup C. ping D. netstat

(5) B. Nslookup

(6) C. ping

注意：(5)、(6)答案可以互换

测试 DNS 服务器是否正常工作，可以采用两种方式：第一种通过 ping 域名来测试；第二种采用 nslookup 来查看提供服务的 DNS 服务器。

试题四

某企业在部门 A 和部门 B 分别搭建了局域网，两局域网通过两台 Windows Server 2003 服务器连通，如图 4-1 所示，要求采用 IPSec 安全机制，使得部门 A 的主机 PC1 可以安全访问部门 B 的服务器 S1。

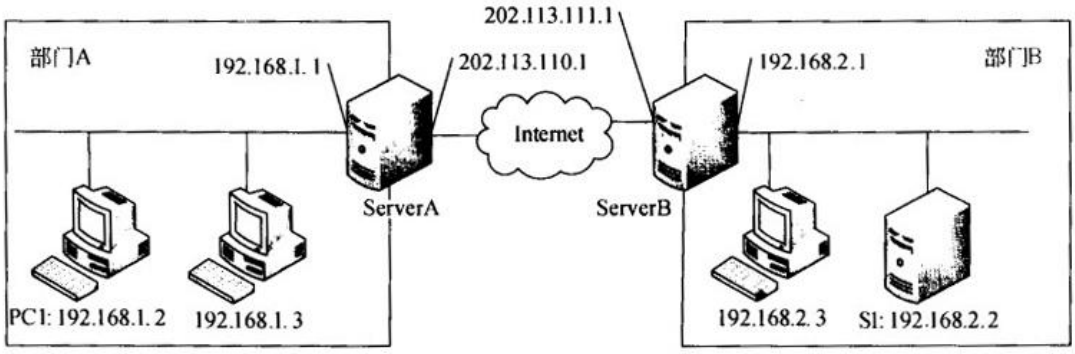


图 4-1

【问题 1】

IPSec 工作在 TCMP 协议栈的（1)层，为 TCP/IP 通信提供访问控制、数据完整性、数据源验证、抗重放攻击、机密性等多种安全服务。IPSec 包括 AH、ESP 和 ISAKMP/Oakley 等协议，其中，(2)为 IP 包提供信息源和报文完整性验证，但不支持加密服务；(3)提供加密服务。

(1) IP （网络）

(2) AH

(3) ESP

IPsec (IP Security)是 IETF 定义的一组协议，用于增强 IP 网络的安全性。其功能可以划分为下面三类：

•认证头（AuthenticationHeader，AH)：用于数据完整性认证和数据源认证。

•封装安全负荷（Encapsulating Security Payload，ESP)：提供数据保密性和数据完整性认证。ESP 也包括了防止重放攻击的顺序号。

• Internet 密钥交换协议（Internet Key Exchange，IKE)：用于生成和分发在 ESP 和 AH 中使用的密钥。IKE 也对远程系统进行初始认证。

因此，IPSec 工作在 TCP/IP 协议栈的 IP 层，AH 为 IP 包提供信息源和报文完整性验证，但不支持加密服务，ESP 提供加密服务。

【问题 2】

IPSec 支持传输和隧道两种工作模式,如果要实现 PC1 和 S1 之间端到端的安全通信，则应该采用（4)模式。

(4) 传输

IPSec 支持传输和隧道两种工作模式，其中传输模式一般用于主机到主机之间端到端的安全通信，隧道模式用于网关到网关之间的安全通信。

【问题 3】

如果 IPSec 采用传输模式,则需要在 PC1 和(5)上配置 IPSec 安全策略。在 PC1 的 IPSec 筛选器属性窗口页中（见图 4-2)，源 IP 地址应设为（6),目标 IP 地址应设为（7)。

(5) S1 或 192.168.2.2

(6) 192.168.1.2

(7) 192.168.2.2

如果 IPSec 采用传输模式，则需要在通信的两个端点 PC1 和 S1 上配置 IPSec 安全策略。在 PC1 的 IPSec 筛选器属性窗口页中，源 IP 地址应设为 PC1 自身的 IP 地址 192.168.1.2，目标 IP 地址应设为 S1 的 IP 地址 192.168.2.2。

【问题 4】

如果要保护部门 A 和部门 B 之间所有的通信安全，则应该采用隧道模式，此时需要在 ServerA 和(8)上配置 IPSec 安全策略。

在 ServerA 的 IPSec 筛选器属性窗口页中（见图 4-3)，源 IP 子网的 IP 地址应设为(9),目标子网 IP 地址应设为(10),源地址和目标地址的子网掩码均设为 255.255.255.0。ServerA 的 IPSec 规则设置中（见图 4-4)，指定的隧道端点 IP 地址应设为（11)。

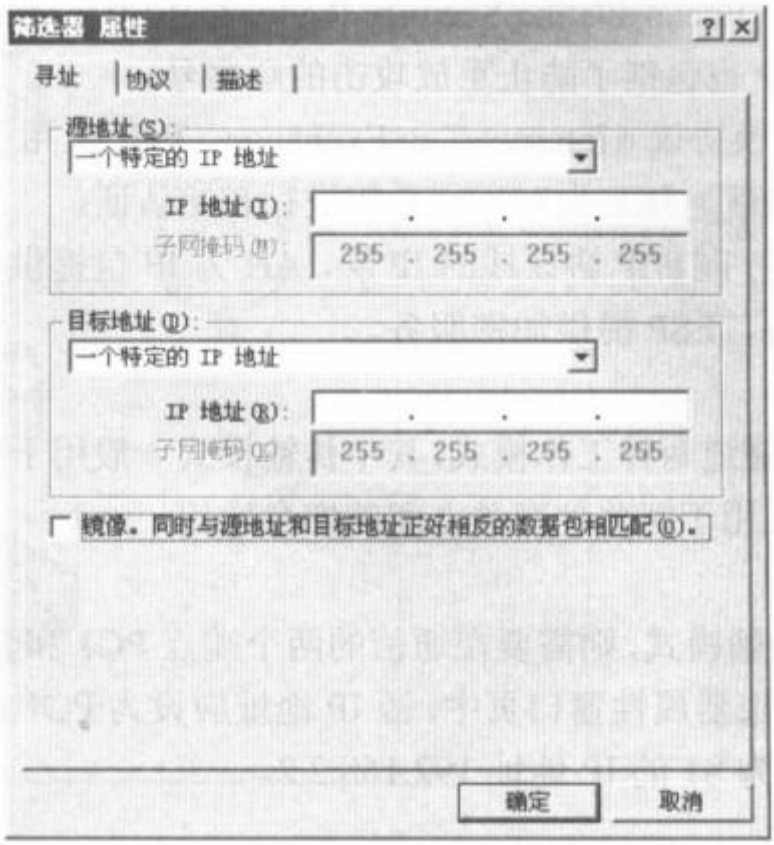


图 4-2

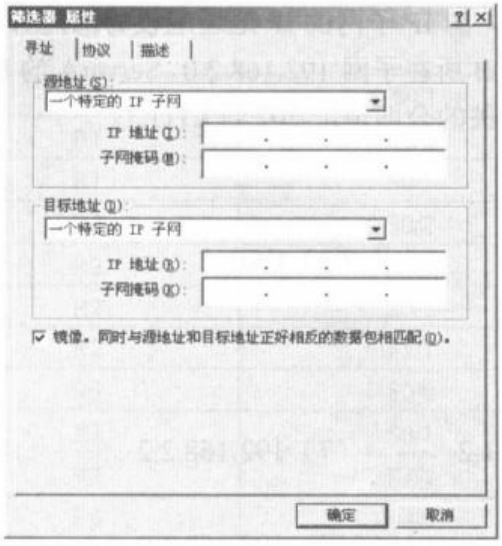


图 4-3

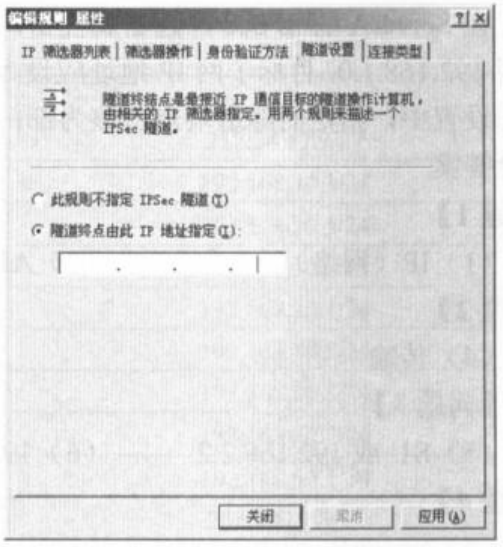


图 4-4

(8) ServerB 或 202.113.111.1

(9) 192.168.1.0

(10) 192.168.2.0

(11) 202.113.111.1

如果要保护部门 A 和部门 B 之间所有的通信安全，应该采用隧道模式，此时需要在部门 A 和部门 B 的网关 ServerA 和 ServerB 上配置 IPSec 安全策略。

在 ServerA 的 IPSec 筛选器属性窗口页中，源 IP 子网的 IP 地址应设为部门 A 所在子网 192.168.1.0,目标子网 IP 地址应设为部门 B 所在子网 192.168.2.0。ServerA 的 IPSec 规则设置中，指定的隧道端点应该为部门 B 网关的公网地址 202.113.111.1。

试题五

某公司总部内采用 RIP 协议，网络拓扑结构如图 5-1 所示。根据业务需求，公司总部的 192.168.40.0/24 网段与分公司 192.168.100.0/24 网段通过 VPN 实现互联。

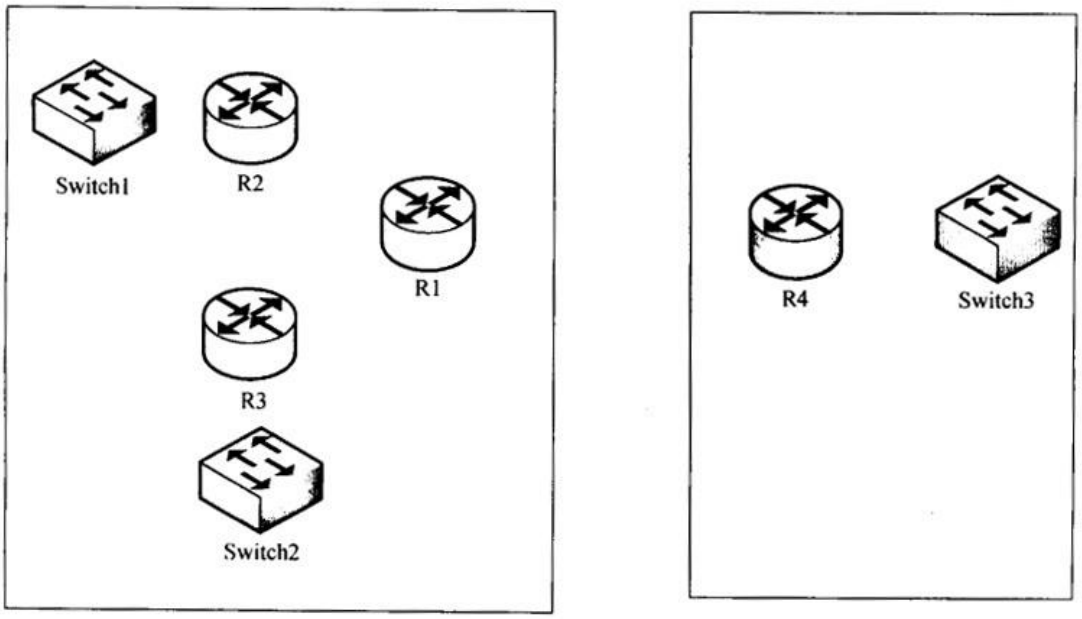


图 5-1

在网络拓扑图中的路由器各接口地址如表 5-1 所示。

表 5-1

名称	接口	IP
R1	S0/0	212.34.17.9/27
R1	S0/1	192.168.10.1/24
R1	S0/2	192.168.20.1/24
R2	S0/0	192.168.10.2/24
R2	S0/1	192.168.30.1/24
R2	F1/1	192.168.40.1/24
R3	S0/0	192.168.20.2/24
R3	S0/1	192.168.30.2/24
R3	F1/1	192.168.50.1/24
R4	S0/0	202.100.2.3/27
R4	F1/1	192.168.100.1/24

【问题 1】

根据网络拓扑和需求说明，完成路由器 R2 的配置:

```
R2#config t
R2 (config)#interface serial 0/0
R2 (config-if)#ip address  (1)   (2)
R2 (config-if)#no shutdown
R2(config-if)#exit
R2 (config)#ip routing
R2 (config)#router (3)                    ;(进入 RIP 协议配置子模式
R2 (config-router)#network (4)
R2 (config-router)#network (5)
R2 (config-router)#network (6)
R2 (config-router)#version 2              ;(设置 RIP 协议版本 2)
R2(config-router)#exit
```

(1) 192.168.10.2

(2) 255.255.255.0

(3) RIP

(4) 192.168.10.0

(5) 192.168.40.0

(6) 192.168.30.0

注意：(4)、(5)、(6)可以互换。

根据题目说明和路由器各接口地址表可知，在公司总部路由器 R2 的 RIP 配置应如下:

```
R2#config t
R2 (config)#interface serial 0/0
R2 (config-if)#ip address  192.168.10.2  255.255.255.0
R2 (config-if)#no shutdown
R2(config-if)#exit
R2 (config)#ip routing
R2 (config)#router RIP                        ;(进入 RIP 协议配置子模式)
R2 (config-router)#network 192.168.10.0       ;(声明网络 192.168.10.0/24)
R2 (config-router)#network 192.168.40.0       ;(声明网络 192.168.10.0/24)
R2 (config-router)#network 192.168.30.0       ;(声明网络 192.168.10.0/24)
R2 (config-router)#version 2                  ;(设置 RIP 协议版本 2)
R2(config-router)#exit
```

```
R1(config)# interface serial 0/0
R1(config-if)# ip address 212.34.17.9 255.255.255.224
R1(config-if)# no shutdown
R1(config)#ip route 192.168.100.0 0.0.0.255 202.100.2.3
                                          ; 配置静态路由（指向 VPN 的对端）
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#authentication pre-share  ; 定义预共享密钥
R1(config-isakmp)#encryption 3des           ; 加密使用 3DES 算法
R1(config-isakmp)#hash md5                  ; 定义 MD5 算法
R1(config)#crypto isakmp key test123 address 202.100.2.3
                                          ; 设置密钥为 test123 和对端地址
R1(config)#crypto isakmp transform-set link ah-md5-h esp-3des
                                          ; 指定 VPN 的加密和认证算法
R1(config)#accress-list 300 permit ip 192.168.100.0 0.0.0.255
                                          ; 配置 ACL
R1(config)#crypto map vpntest 1 ipsec-isakmp
                                          ;创建 crypto map 名字为 vpntest

R1(config-crypto-map)#set peer 202.100.2.3  ; 指定链路对端 IP 地址
R1(config-crypto-map)#set transfrom-set link ; 指定传输模式 link
R1(config-crypto-map)#match address 300     ; 指定应用访控列表
R1(config)# interface serial 0/0
R1(config)#crypto map vpntest               ; 应用到接口
```

【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。

```
R1(config)# interface serial 0/0
R1(config-if)# ip address (7) (8)
R1(config-if)# no shutdown
R1(config)#ip route 192.168.100.0 0.0.0.255 202.100.2.3; (9)
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#authentication pre-share              ; (10)
R1(config-isakmp)#encryption 3des       ; 加密使用 3DES 算法
R1(config-isakmp)#hash md5              ; 定义 MD5 算法
R1(config)#crypto isakmp key test123 address (11)
                                        ; 设置密钥为 test123 和对端地址
R1(config)#crypto isakmp transform-set link ah-md5-h esp-3des
                                        ; 指定 VPN 的加密和认证算法
R1(config)#accress-list 300 permit ip 192.168.100.0 0.0.0.255
                                        ; 配置 ACL
R1(config)#crypto map vpntest 1 ipsec-isakmp
                                        ; 创建 crypto map 名字为 vpntest
```

```
R1(config-crypto-map)#set peer 202.100.2.3          ; 指定链路对端 IP 地址
R1(config-crypto-map)#set transfrom-set link        ; 指定传输模式 link
R1(config-crypto-map)#match address 300             ; 指定应用访控列表
R1(config)# interface serial 0/0
R1(config)#crypto map (12)                          ; 应用到接口
```

(7) 212.34.17.9

(8) 255.255.255.224

(9) 配置静态路由（指向 VPN 的对端）

(10)定义预共享密钥

(11) 202.100.2.3

(12) vpntest

本题考查的是 vpn 配置的基础知识。根据题目说明，公司总部的 192.168.40.0/24 网段与分公司 192.168.100.0/24 网段通过 VPN 实现互联，所以路由器 VPN 配置如下：

```
R2#config t
R2 (config)#interface serial 0/0
R2 (config-if)#ip address  192.168.10.2  255.255.255.0
R2 (config-if)#no shutdown
R2(config-if)#exit
R2 (config)#ip routing
R2 (config)#router RIP                              ;(进入 RIP 协议配置子模式)
R2 (config-router)#network 192.168.10.0             ;(声明网络 192.168.10.0/24)
R2 (config-router)#network 192.168.40.0             ;(声明网络 192.168.10.0/24)
R2 (config-router)#network 192.168.30.0             ;(声明网络 192.168.10.0/24)
R2 (config-router)#version 2                        ;(设置 RIP 协议版本 2)
R2(config-router)#exit
```

```
R1(config)# interface serial 0/0
R1(config-if)# ip address 212.34.17.9 255.255.255.224
R1(config-if)# no shutdown
R1(config)#ip route 192.168.100.0 0.0.0.255 202.100.2.3
                                          ; 配置静态路由（指向 VPN 的对端）
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#authentication pre-share  ; 定义预共享密钥
R1(config-isakmp)#encryption 3des           ; 加密使用 3DES 算法
R1(config-isakmp)#hash md5                  ; 定义 MD5 算法
R1(config)#crypto isakmp key test123 address 202.100.2.3
                                          ; 设置密钥为 test123 和对端地址
R1(config)#crypto isakmp transform-set link ah-md5-h esp-3des
                                          ; 指定 VPN 的加密和认证算法
R1(config)#accress-list 300 permit ip 192.168.100.0 0.0.0.255
                                          ; 配置 ACL
R1(config)#crypto map vpntest 1 ipsec-isakmp
                                          ;创建 crypto map 名字为 vpntest

R1(config-crypto-map)#set peer 202.100.2.3  ; 指定链路对端 IP 地址
R1(config-crypto-map)#set transfrom-set link ; 指定传输模式 link
R1(config-crypto-map)#match address 300     ; 指定应用访控列表
R1(config)# interface serial 0/0
R1(config)#crypto map vpntest               ; 应用到接口
```