在 CPU 中用于跟踪指令地址的寄存器是（1）。

(1)A.地址寄存器(MAR)　　B.数据寄存器（MDR)

C.程序计数器(PC)　　D.指令寄存器（IR)

【答案】C

【解析】本题考查寄存器的基本知识。

CPU 中通常设置一些寄存器，用于暂时存储程序运行过程中的相关信息。其中，通用寄存器常用于暂存运算器需要的数据或运算结果，地址寄存器和数据寄存器用于访问内存时的地址和数据暂存，指令寄存器用于暂存正在执行的指令，程序计数器中存放待执行的指令的地址。

指令系统中采用不同寻址方式的目的是(2).

(2)A.提高从内存获取数据的速度　　B.提高从外存获取数据沾速度

C.降低操作码的译码难度　　D.扩大寻址空间并提高编程灵活性

【答案】D

【解析】本题考查指令系统的基本概念。

寻址方式是指寻找操作数或操作数地址的方式。指令系统中采用不同寻址方式的目的是为了在效率和方便性上找一个平衡。立即数寻址和寄存器寻址在效率上是最快的，但是寄存器数目少，不可能将操作数都存入其中等待使用，立即数的使用场合也非常有限，这样就需要将数据保存在内存中，然后使用直接寻址、寄存器间接寻址、寄存器相对寻址、基址加变址寻址、相对基址加变址寻址这些寻址方式将内存中的数据移入寄存器中。

在计算机系统中采用总线结构，便于实现系统的积木化构造，同时可以(3).

(3)A.提高数据传输速度　　B.提高数据传输量

C.减少信息传输线的数量　　D.减少指令系统的复杂性

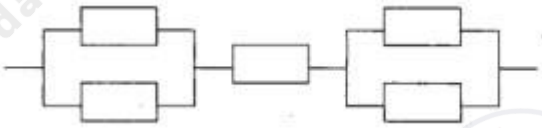
【答案】C

【解析】本题考查计算机系统的基础知识。

总线是连接计算机有关部件的一组信号线，是计算机中用来传送信息代码的公共通道。采用总线结构主要有以下优点：简化系统结构，便于系统设计制造；大大减少了连线数目，便于布线，减小体积，提高系统的可靠性；便于接口设计，所有与总线连接的设备均采用类似的接口；便于系统的扩充、更新与灵活配置，易于实现系统的模块化；便于设备的软件设

计，所有接口的软件就是对不同的口地址进行操作；便于故障诊断和维修，同时也降低了成本。

某计算机系统由下图所示的部件构成，假定每个部件的千小时可靠度都为 R，则该系统的千小时可靠度为(4)。



(4)A. R+2R/4　　B. R+R2/4　　C. R(1-(1-R)2)　　D. R(1-(1-R)2)2

【答案】D

【解析】本题考查系统可靠性方面的基础知识。

由子系统构成串联系统时，其中任何一个子系统失效就足以使系统失效，其可靠度等于各子系统可靠度的乘积；构成并联系统时，只要有一个子系统正常工作，系统就能正常工作。每个子系统的可靠性分别以 R1，R2，…，RN 表示,则整个系统用串联方式构造时的可靠度为 R=R1×R2…×…RN，整个系统用串联方式构造时的可靠度为 R=1-（1-R1)(1-R2)…(1-RN)．因此，本系统的可靠度为 R(1-(1-R)2)2

软件产品的可靠性并不取决于(5)。

(5)A. 潜在错误的数量　　B. 潜在错误的位置

C. 软件产品的使用方式　　D. 软件产品的开发方式

【答案】D

【解析】本题考查软件质量管理。

软件可靠性指的是一个系统对于给定的时间间隔内、在给定条件下无失效运作的概率。根据定义，软件可靠性与软件的潜在错误的数量、位置有关，与软件产品的使用方式有关，而软件产品的开发方式不决定软件产品的可靠性。

模块 A 直接访问模块 B 的内部数据，则模块 A 和模块 B 的耦合类型为(6)。

(6)A. 数据耦合　　B. 标记耦合　　C. 公共耦合　　D. 内容耦合

【答案】D

【解析】本题考查软件的分析与设计方法。

模块独立性是创建良好设计的一个重要原则，一般采用模块间的耦合和模块的内聚两个准则来进行度量。耦合是模块之间的相对独立性的度量，模块之间的连接越紧密，联系越多，耦合性就越高，而其模块独立性就越弱。一般来说，模块之间的耦合有 7 种类型，根据耦合性从低到高为非直接耦合、数据耦合、标记耦合、控制耦合、外部耦合、公共耦合和内容耦合。如果一个模块访问另一个模块时，彼此之间是通过数据参数（不是控制参数、公共数据结构或外部变量）来交换输入、输出信息的，则称这种耦合为数据耦合；如果一组模块通过数据结构本身传递，则称这种耦合为标记耦合；若一组模块都访问同一个公共数据环境，则它们之间的耦合就称为公共耦合；若一个模块直接访问另一个模块的内部数据、一个模块不通过正常入口转到另一个模块内部、两个模块有一部分程序代码重叠或者一个模块有多个入口，上述几个情形之一发生则两个模块之间就发生了内容耦合。

下列关于风险的叙述不正确的是：风险是指(7)

(7)A.可能发生的事件　　B.一定会发生的事件

C.会带来损失的事件　　D.可能对其进行干预，以减少损失的事件

【答案】B

【解析】本题考查风险分析和风险控制技术。

风险是一种具有负面后果的、人们不希望发生的事件。通常认为风险具有以下特点：风险是可能发生的事件，其发生的可能性用风险概率来描述；风险是会给项目带来损失的时间；可能对风险进行干预，以期减少损失。针对每一种风险，应弄清可能减少造成损失或避免损失的程度。对风险加以控制，采取一些有效的措施来降低风险或是消除风险。

下列关于项目估算方法的叙述不正确的是(8)。

(8)A.专家判断方法受到专家经验和主观性影响

B.启发式方法（如 COCOMO 模型）的参数难以确定

C.机器学习方法难以描述训练数据的特征和确定其相似性

D.结合上述三种方法可以得到精确的估算结果

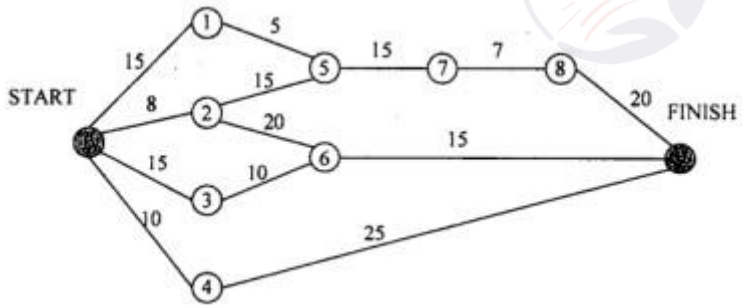
【答案】D

【解析】本题考查项目管理及工具技术。

项目估算是项目计划和管理的一个至关重要的方面。成本超出某个限度可能导致客户取消项目，而过低的成本估算可能会迫使开发小组投入大量的时间却没有相应的经济回报。目

前常用的项目估算方法有专家判断方法，该方法受到专家经验和主观性等方面的影响；算法方法，根据某个计算模型来估算项目开发成本，如启发式方法 COCOMO 模型，但这些模型中的参数难以确定；机器学习方法，如根据过去的项目开发数据，建立分类模型，预测新项目的开发成本，但这类方法中难以定义训练数据的特征以及定义数据对象之间的相似性。即使结合多种方法，上述问题仍然存在，因此并不能得到精确地估算结果。

下图是一个软件项目的活动图，其中顶点表示项目里程碑，边表示包含的活动，边上的权重表示活动的持续时间，则里程碑(9)在关键路径上。



(9)A. 1　　B. 2　　C. 3　　D. 4

【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 0—2—5—-8—9,关键路径长度为 65。因此里程碑 2 在关键路径上，而里程碑 1、3 和 4 不在关键路径上。

下列关于软件著作权中翻译权的叙述不正确的是：翻译权是指(10)的权利

(10)A. 将原软件从一种自然语言文字转换成另一种自然语言文字

B. 将原软件从一种程序设计语言转换成另一种程序设计语言

C. 软件著作权人对其软件享有的以其他各种语言文字形式再表现

D. 对软件的操作界面或者程序中涉及的语言文字翻译成另一种语言文字试题

【答案】B

【解析】

软件著作权中翻译权是指以不同于原软件作品的一种程序语言转换该作品原使用的程序语言，而重现软件作品内容的创作的产品权利。简单地说，也就是指将原软件从一种程序

语言转换成另一种程序语言的权利。

10Base-T 以太网使用曼彻斯特编码，其编码效率为（11）%，在快速以太网中使用 4B/5B 编码，其编码效率为（12）%。

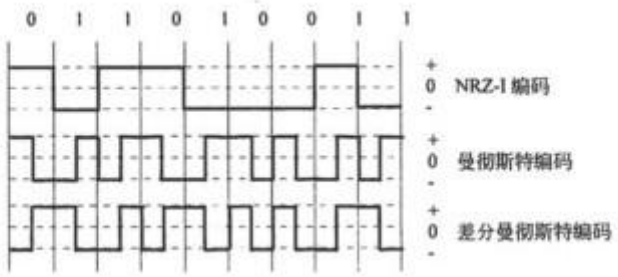
(11)A. 30　　B. 50　　C. 80　　D. 90

(12)A. 30　　B. 50　　C. 80　　D. 90

【答案】B　C

【解析】

曼彻斯特编码和差分曼彻斯特编码都是双相码，即码元取正负两个不同的电平，或者说由正负两个不同的码元表示一个比特，如下图所示。这种编码的效率就是 50%，但是由于每个比特中间都有电平跳变，因而提供了丰富的同步信息。这两种编码使用在数据速率不太高的以太网中。



为了提高编码的效率，降低电路成本，可以采用 4B/5B 编码，其原理如下图所示。这实际上是一种两级编码方案。系统中使用不归零码(NRZ)，在发送到传输介质之前要变成见 1 就翻不归零码(NRZ-I) 。NRZ-I 代码序列中 1 的个数越多，越能提供同步定时信息，但如果遇到长串的 0，则不能提供同步信息。所以在发送到介质上之前还需经过一次 4B/5B 编码，发送器扫描要送的比特序列，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。

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 位二进制代码的状态共有 32 种，在上表选用的 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。另外，还有 8B/10B 等编码方法，其原理是类似的。这两种编码的效率是 80%。

在相隔 400km 的两地间通过电缆以 4800b/s 的速率传送 3000 比特长的数据包，从开始发送到接收完数据需要的时间是(13)。

(13)A. 480ms　　B. 607ms　　C. 612ms　　D. 627ms

【答案】D

【解析】

一个数据包从开始发送到接收完成的时间包含两部分:发送时间 tf 和传播延迟时间 tp，根据题目要求可以计算如下。

对电缆信道：tp=400km/(200km/ms)=2ms,tf=3000bit/4800b/s=625ms,tp+tf=627ms.

假设模拟信号的最高频率为 10MHz，采样频率必须大于(14)时,才能使得到的样本信号不失真。

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

【答案】D

【解析】

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

采样的频率决定了恢复的模拟信号的质量。根据尼奎斯特采样定理，为了恢复原来的模拟信号，采样频率必须大于模拟信号最高频率的二倍，即 f=1/T≥2fmax.

其中 f 为采样频率，T 为采样周期,fmax 为信号的最高频率。

根据题意，对于最高频率为 10MHz 的模拟信号，采样频率必须大于 20MHz。

数据链路协议 HDLC 是一种(15).

(15)A. 面向比特的同步链路控制协议　　B. 面向字节计数的同步链路控制协议

C. 面向字符的同步链路控制协议　　D. 异步链路控制协议

【答案】A

【解析】

数据链路控制协议可分为两大类：面向字符的协议和面向比特的协议。面向字符的协议以字符作为传输的基本单位，并用 10 个专用字符（例如 STX、ETX、ACK、NAK 等）控制传输过程，这类协议发展较早，至今仍在使用。面向比特的协议以比特作为传输的基本单位，它的传输效率高，广泛应用于公用数据网中。

HDLC 协议的全称是高级数据链路控制协议（High Level Data Link Control),在数据链路两端的对等实体之间实现同步控制传输。

快速以太网标准 100Base-TX 规定的传输介质是(16)。

(16)A.2 类 UTP　　B.3 类 UTP　　C.5 类 UTP　　D.光纤

【答案】C

【解析】

1995 年 100Mb/s 的快速以太网标准 IEEE 802.3u 正式颁布。快速以太网使用的传输介质如下表所示，其中多模光纤的芯线直径为 62.5μm，包层直径为 125μm，单模光线芯线直径为 8μm，包层直径也是 125μm。

标　准	传输介质	特性阻抗	最大段长
100BASE-TX	2 对 5 类 UTP	100Ω	100m
	2 对 STP	150Ω	
100BASE-FX	一对多模光纤 MMF	62.5/125μm	2km
	一对单模光纤 SMF	8/125μm	40km
100BASE-T4	4 对 3 类 UTP	100Ω	100m
100BASE-T2	2 对 3 类 UTP	100Ω	100m

以太网交换机的交换方式有三种，这三种交换方式不包括(17)。

(17)A.存储转发式交换　　B.IP 交换

C.直通式交换　　D.碎片过滤式交换

【答案】B

【解析】

以太网交换机的交换方式分为存储转发式交换、直通式交换和碎片过滤式交换三类。

①存储转发式交换（Store and Forward)：交换机对输入的数据包先进行缓存、验证、

碎片过滤，然后再进行转发。这种交换方式延时大，但是可以提供差错校验，并支持不同速度的输入/输出端口间的交换（非对称交换），是交换机的主流工作方式。

②直通式交换（Cut-through）：直通式交换类似于采用交叉矩阵的电话交换机，它在输入端口扫描到目标地址后立即开始转发。这种交换方式的优点是延迟小、交换速度快。其缺点是没有检错能力；不能实现非对称交换；并且当交换机的端口增加时，交换矩阵实现起来比较困难。

③碎片过滤式交换（Fragment Free）：这是介于直通式和存储转发式之间的一种解决方案。交换机在开始转发前先检查数据包的长度是否够 64 个字节，如果小于 64 字节，说明是冲突碎片，则丢弃之；如果大于等于 64 字节，则转发该包。这种转发方式的处理速度介于前两者之间，被广泛应用于中低档交换机中。

Cisco 路由器操作系统 IOS 有三种命令模式，其中不包括（18）。

(18)A.用户模式　　B.特权模式　　C.远程连接模式　　D.配置模式

【答案】C

【解析】

Cisco 操作系统 IOS 有三种命令模式：

® router〉

路由器处于用户模式，这时用户可以查看路由器的连接状态，访问其他网络和主机，但不能看到和更改路由器配置的内容。

© router#

在 router>提示符下键入 enable,路由器进入特权模式 router#，这时不但可以执行所有的用户命令，还可以看到和更改路由器的配置内容。

③ router(config)#

在 router#提示符下键入 configure terminal,出现提示符 router(config)#，这时路由器处于全局配置状态，可以配置路由器的全局参数。如果输入某个端口标识，则可以进入局部配置状态。

router(config-if)#;

router(config-line)#;

router (config-router) #;...

这时可以配置路由器的局部参数。

通过 CATV 电缆访问因特网，在用户端必须安装的设备是（19）。

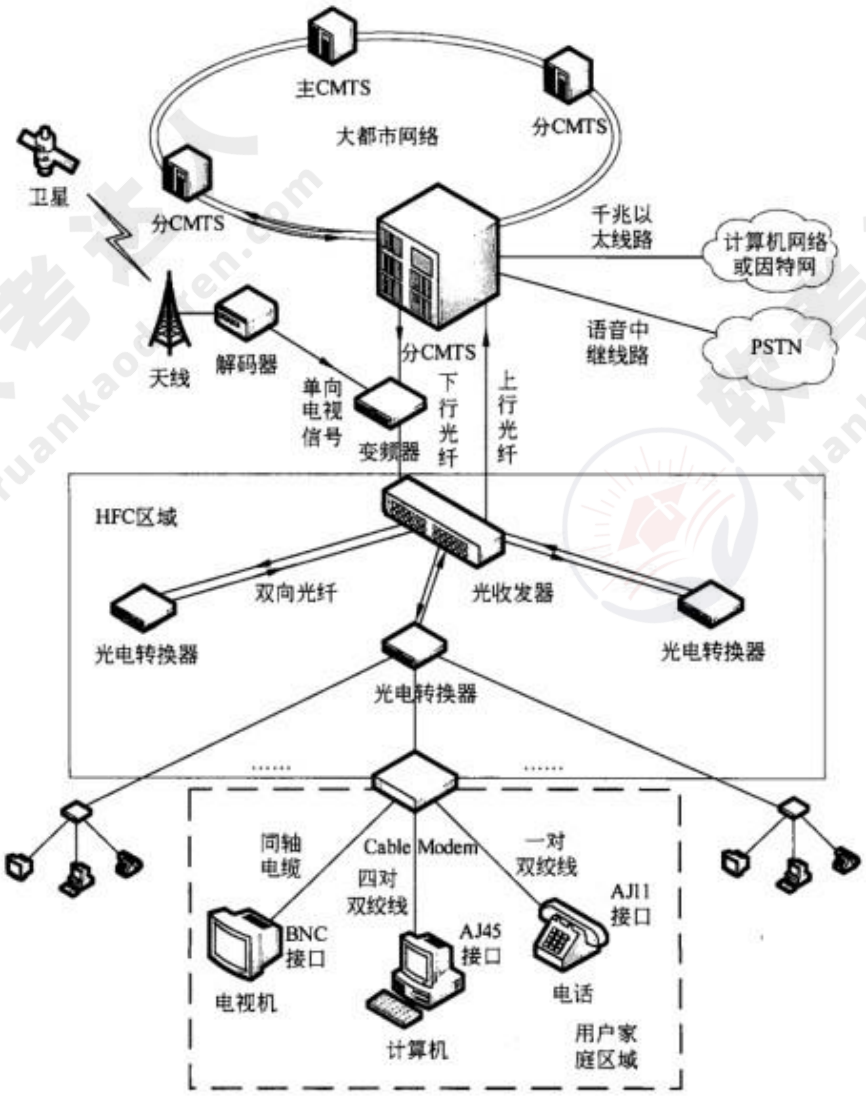
(19)A. ADSL Modem　　B. Cable Modem　　C. 无线路由器　　D. 以太网交换机

【答案】B

【解析】

对传统的 CATV 网络进行改造就可以实现双向的数字传输业务，通过线缆调制解调器不需要拨号就能实现远程站点访问。可以采用一根上行、一根下行的双缆方式，也可以采用高频下行、低频上行的单缆方式。运营商通常采用混合光纤/铜缆（Hybrid Fiber/Coax, HFC）系统将 CATV 网络和运营商的高速光纤网络连接在一起。运营商一端的线缆调制解调器终接设备（CMTS）向大量的线缆调制解调器（CableModem，CM）提供高速连接。多数运营商借助于通用宽带路由器来实现 CMTS 功能，如下图所示。 CMTS 的以太端口与以太网连接，同时通过中继线路连接 PSTN 网络，并将双向的计算机网络和语音信号调制，形成上行和下行的模拟信号，而单向的有线电视信号以频分复用方式进入下行信号中。在 HFC 区域，借助于光收发器、光电转换器等设备完成信号的中继传输。

客户端与 CM 相连，并分解出有线电视、计算机网络和电话信号。典型的 CATV 系统提供 25～50Mb/s 的下行带宽和 2～3Mb/s 的上行带宽。



在互联网中可以采用不同的路由选择算法，所谓松散源路由是指 IP 分组（20）。

(20)A. 必须经过源站指定的路由器　　B. 只能经过源站指定的路由器

C. 必须经过目标站指定的路由器　　D. 只能经过目标站指定的路由器

【答案】A

【解析】

在互联网中可以由源端指明到达目标的路由，这个功能是通过 IP 分组头中的选项实现的。所谓松散源路由是指传输的 IP 分组必须经过源端指定的路由器，但是也可能要经过源端没有指明的路由器；与此相反，所谓严格源路由则是指，传输的 IP 分组只能经过源端指定的路由器，而不能经过源端没有指定的路由器。

下面关于边界网关协议 BGP4 的描述中，不正确的是（21）。

(21)A.BGP4 网关向对等实体（Peer)发布可以到达的 AS 列表

B.BGP4 网关采用逐跳路由（hop-by-hop)模式发布路由信息

C.BGP4 可以通过路由汇聚功能形成超级网络（Supemet)

D.BGP4 报文直接封装在 IP 数据报中传送

【答案】D

【解析】

现在通用的外部网关协议叫做 BGP (Border Gateway Protocol)。 BGP4 广泛地应用于不同 ISP 的网络（AS)之间，成为事实上的 Internet 外部路由协议标准。BGP4 是一种动态路由发现协议，支持无类别域间路由 CIDR。BGP 的主要功能是控制路由策略，例如是否愿意转发过路的分组等。BGP 的 4 种报文类型见下表，这些报文通过 TCP (179 端口）连接传送。

报 文 类 型	功 能 描 述
打开（Open）	建立邻居关系
更新（Update）	发送新的路由信息
保持活动状态（Keepalive）	对 Open 的应答/周期性地确认邻居关系
通告（Notification）	报告检测到的错误

RIP 协议中可以使用多种方法防止路由循环，在以下选项中不属于这些方法的是(22)。

(22)A.垂直翻转　　B.水平分割　　C.反向路由中毒　　D.设置最大度量值

【答案】A

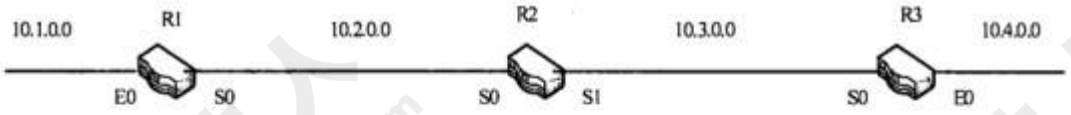
【解析】

路由信息协议 RIP 采用距离矢量路由算法计算最佳路由。RIP 以跳步计数(hop count)作为路由费用的度量，允许的最大跳步数不超过 15 步。

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

例如在下图中，路由器 R1、R2、R3 的路由表已经收敛，每个路由表的后两项是通过交换路由信息而学习到的。如果在某一时刻，网络 10.4.0.0 发生故障，R3 检测到故障，并通过接口 S0 把故障通知 R2。如果 R2 在收到 R3 的故障通知前将其路由表发送到 R3，则 R3 会认为通过 R2 可以访问 10.4.0.0,并据此将路由表中第二条记录修改为（10.4.0.0, S0, 2)。这样一来，路由器 R1、R2、R3 都认为通过其他的路由器存在一条通往 10.4.0.0 的路径，结果导致目标地址为 10.4.0.0 的数据包在三个路由器之间来回传递，从而形成路由环路，

直至达到最大跳步数时才能终止循环传送过程。



R1路由表		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

R2路由表		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

R3路由表		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

解决路由环路问题可以采用水平分割法（SplitHorizon)。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源。可以对上图 R2 的路由表项将加上一些注释，如下图所示，可以看出，每一条路由信息都不会通过其来源接口向回发送，这样就可以避免环路的产生。简单的水平分割方案是“不能把从邻居学习到的路由发送给那个邻居”，带有反向毒化的水平分割方案（Split Horizon with Poisoned Reverse)是“把从邻居学习到的路由费用设置为无限大，并立即发送给那个邻居”。采用反向毒化的方案更安全一些，它可以奋即中断环路。相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成过程。

R2路由表			
10.2.0.0	S0	0	不发送给R1
10.3.0.0	S1	0	不发送给R3
10.4.0.0	S1	1	不发送给R3
10.1.0.0	S0	1	不发送给R1

另外，前面提到的触发更新技术也能加快路由收敛，如果触发更新足够及时——路由器 R3 在接收 R2 的更新报文之前把网络 10.4.0.0 的故障告诉 R2,则也可以防止环路的形成。

RIP 协议默认的路由更新周期是(23)秒。

(23)A.30　　B.60　　C.90　　D.100

【答案】A

【解析】

RIPv1 (RFC 1058，1988)是早期的路由协议，使用本地广播地址 255.255.255.255 发布路由信息，默认的路由更新周期为 30 秒，持有时间（Hold-Down Time)为 180 秒。也就是

说，RIP 路由器每 30 秒向所有邻居发送一次路由更新报文，如果在 180 秒之内没有从某个邻居接收到路由更新报文，则认为该邻居已经不存在了。这时如果从其他邻居收到了有关同一目标的路由更新报文，则用新的路由信息替换已失效的路由表项，否则，对应的路由表项被删除。

RIPv1 是有类别的协议（classfiil protocol),这意味着配置 RIPv1 时必须使用 A、B 或 C 类 IP 地址和子网掩码,例如不能把子网掩码 255.255.255.0 用于 B 类网络 172.16.0.0。对于同一目标，RIP 路由表项中最多可以有 6 条等费用的通路，虽然默认是 4 条。RIP 可以实现等费用通路的负载均衡（equal-cost load balancing)，这种机制提供了链路冗余功能，以对付可能出现的连接失效，但是 RIP 不支持不等费用通路的负载均衡，这种功能出现在后来的 IGRP 和 EIGRP 中。

RIPv2 是增强了 RIP 协议，定义在 RFC 1721 和 RFC 1722 (1994)中。RIPv2 基本上还是一个距离矢量路由协议，但是有三方面的改进。首先是它使用组播而不是广播来传播路由更新报文，并且采用了触发更新（triggered update)机制来加速路由收敛，即出现路由变化时立即向邻居发送路由更新报文，而不必等待更新周期是否到达。其次是 RIPv2 是一个无类别的协议(classless protocol),可以使用可变长子网掩码(VLSM)，也支持无类别域间路由（CIDR)，这些功能使得网络的设计更具伸缩性。第三个增强是 RIPv2 支持认证，使用经过散列的口令字来限制路由更新信息的传播。其他方面的特性与第一版相同，例如以跳步计数来度量路由费用，允许的最大跳步数为 15 等.

OSPF 协议适用于 4 种网络。下面的选项中，属于广播多址网络的是（24），属于非广播多址网络的是（25）。

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

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

【答案】A　C

【解析】

OSPF (RFC 2328，1998)是一种链路状态协议，用于在自治内部的路由器之间交换路由信息。OSPF 具有支持大型网络、占用网络资源少、路由收敛快等优点，在目前的网络配置中占有重要的地位。

距离矢量协议发布自己的路由表，交换的路由信息量很大。链路状态协议与之不同，它是从各个路由器收集链路状态信息，构造网络拓扑结构图，使用 Dijkstra 的最短通路优先

算法（Shortest Path First，SPF)计算到达各个目标的最佳路由。

网络的物理连接和拓扑结构不同，交换路由信息的方式就不同。OSPF 将路由器连接的物理网络划分为 4 种类型：

①点对点网络：例如一对路由器用 64Kb 的串行线路连接，就属于点对点网络，在这种网络中，两个路由器可以直接交换路由信息。

②广播多址网络：以太网（Ethernet)或者其他具有共享介质的局域网都属于这种网络。在这种网络中，一条路由信息可以广播给所有的路由器。

③非广播多址网络（non-broadcast multi-access，NBMA)：例如 X.25 分组交换网或帧中继网络就属于这种网络，在这种网络中可以通过组播方式发布路由信息。

④点到多点网络：可以把非广播网络当作多条点对点网络来使用，从而把一条路由信息发送到不同的目标，RARP 协议就是以这种方式工作的。

MPLS（多协议标记交换）根据标记对分组进行交换，MPLS 包头的位置应插入在（26）

(26)A.以太帧头的前面　　B.以太帧头与 IP 头之间

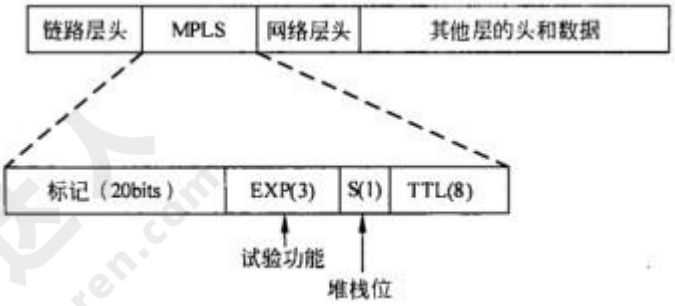
C.IP 头与 TCP 头之间　　D.应用数据与 TCP 头之间

【答案】B

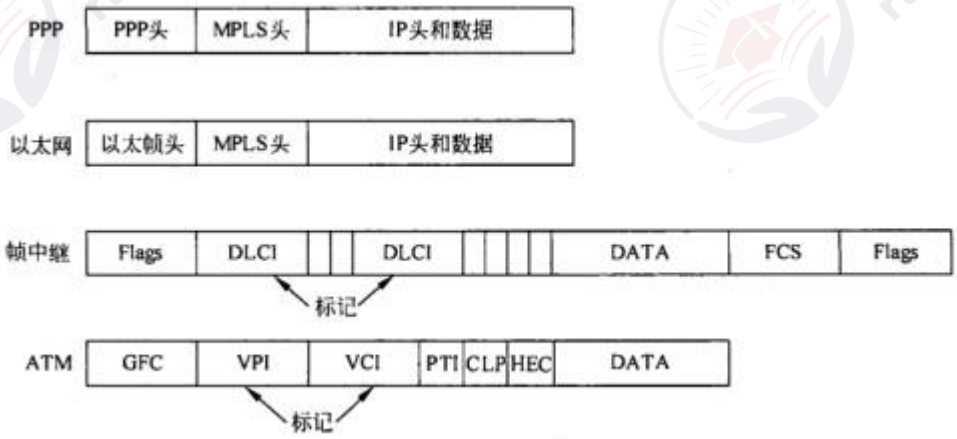
【解析】

所谓第三层交换是指利用第二层交换的高带宽和低延迟优势尽快地传送网络层分组的技术。交换与路由不同，前者用硬件实现，速度快。而后者由软件实现，速度慢。三层交换机的工作原理可以概括为：一次路由，多次交换。就是说，当三层交换机第一次收到一个数据包时必须通过路由功能寻找转发端口，同时记住目标 MAC 地址和源 MAC 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。所以三层交换机不但具有路由功能，而且比通常的路由器转发得更快。

ETF 开发的多协议标记交换(Multi-protocol Label Switching，MPLS，RFC3031)把第 2 层的链路状态信息（带宽、延迟、利用率等）集成到第 3 层的协议数据单元中，从而简化和改进了第 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，标准格式如下图所示。



MPLS 可以承载的报文通常是 IP 包，当然也可以直接承载以太帧、AAL5 包，甚至 ATM 信元等。可以承载 MPLS 的第 2 层协议可以是 PPP、以太帧、ATM 和帧中继等，如下图所示。



IGRP 协议的路由度量包括多种因素，但是在一般情况下可以简化为（27）。

(27)A.可靠性　　B.带宽　　C.跳步数　　D.MTU

【答案】C

【解析】

IGRP 是 Cisco 公司开发的路由协议。它也是一个距离矢量协议，但是与 RIP 相比，它有下列优点：

①使用了带宽和延迟等参数作为路由度量标准；

②利用触发更新来加快路由收敛；

③支持不等费用通路的负载均衡；

④最大跳步数扩充到 255,可以支持更大的网络。

IGRP 不使用跳步数作为路由度量，虽然在一般情况下可以简化为跳步数。IGRP 的路由度量因素包括带宽、延迟、可靠性、负载和 MTU，其中前两者是默认的，但是可以通过配置加入其他参数。可靠性和负载划分为 1～255 级，可靠性 1 是最低的，可靠性 255 是最高的，负

载 1 使用最少，负载 255 是百分之百利用的。MTU 指最大帧长度，在实际运行中，它是一个常数值，通常采用一条通路中最小的 MTU 值。这些因素综合起来作为路由费用的度量，使得 IGRP 可以选择更好的路由。相对于 RIP 的跳步计数，IGRP 协议的路由选择更加合理。IGRP 的路由更新周期是 90 秒，持有时间是 280 秒，为了加速收敛，采用了触发更新技术。

采用 Windows Server 2003 创建一个 Web 站点，主目录中添加主页文件 index.asp 后，在客户机的浏览器地址栏内输入该网站的域名后不能正常访问，则不可能的原因是（28）。

(28)A.Web 站点配置完成后没有重新启动

B.DNS 服务器不能进行正确的域名解析

C.没有将 index.asp 添加到该 Web 站点的默认启动文档中

D.没有指定该 Web 站点的服务端口

【答案】D

【解析】本试题考查 Windows Server2003 Web 服务器的配置。

采用 Windows Server 2003 创建一个 Web 站点时，通常是先安装 IIS 建立网站，然后对网站进行配置，重新启动系统生效。若 Web 站点配置完成后没有重新启动，或 DNS 服务器不能进行正确的域名解析，以及没有将 index.asp 添加到该 Web 站点的默认启动文档中都可能导致站点无法正常访问。若没有配置站点的服务端口系统会默认为 80，故正确答案为 D。

DNS 服务器在名称解析过程中正确的查询顺序为（29）。

(29)A.本地缓存记录一区域记录一转发域名服务器一根域名服务器

B.区域记录一本地缓存记录一转发域名服务器一根域名服务器

C.本地缓存记录一区域记录一根域名服务器一转发域名服务器

D.区域记录一本地缓存记录一根域名服务器一转发域名服务器

【答案】A

【解析】

DNS 服务器在名称解析过程中，首先查询本地缓存，若缓存中没有被查域名的记录，则在本区域主域名服务器中进行查找，紧接着查询转发域名服务器，最后是根域名服务 器，因此，正确的查询顺序为：本地缓存记录—区域记录一转发域名服务器一根域名服务器。

DNS 服务器进行域名解析时，若采用递归方法，发送的域名请求为（30）。

(30)A.1 条　　B.2 条　　C.3 条　　D.多条

【答案】A

【解析】

DNS 服务器进行域名解析时，若采用递归方法，发出 1 条请求后，类似于程序递归的思想，最终只有一条结果返回。若采用迭代方法，每次返回的是上一级查到的可提供解析的地址，因此会有多条域名请求发出。

若 DNS 资源记录中记录类型（record-type)为 A，则记录的值为（31).

(31)A.名字服务器　　B.主机描述　　C.IP 地址　　D.别名

【答案】C

【解析】

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)、CNAME（别名）和 NS（区域的授权服务器）等类型。通过 A 记录可以由域名查地址，也可以由地址查域名。

FTP 客户上传文件时，通过服务器 20 端口建立的连接是（32)，客户端应用进程的端口可以为（33) 。

(32)A.建立在 TCP 之上的控制连接　　B.建立在 TCP 之上的数据连接

C.建立在 UDP 之上的控制连接　　D.建立在 UDP 之上的数据连接

(33)A.20　　B.21　　C.80　　D.4155

【答案】B　D

【解析】

FTP 客户机与服务器之间建立两条 TCP 连接，一条用于传送控制信息（端口号为 21)，另一条用于传送文件内容（端口号为 20)。客户端应用进程的端口应该为高端（端口号大于 1024)。

在 Linux 系统中，命令（34)用于管理各项软件包。

(34)A.install　　B.rpm　　C.fsck　　D.msi

【答案】B

【解析】本题考查 linux 系统下 rpm 命令的基本概念。

RPM 全称为 Redhat Package Manager,它是许多流行的 Linux 发行版的软件包管理工具。

Linux 系统中，为某一个文件在另外一个位置建立一个文件链接的命令为（35），

(35)A. ln　　B. copy　　C. locate　　D. cat

【答案】A

【解析】本题考查 Linux 系统下文件操作命令 In 的基本概念。

In 命令在两个文件之间创建链接。

默认情况下，Linux 系统中用户登录密码信息存放在（36）文件中。

(36)A. /etc/group　　B. /etc/userinfo　　C. /etc/shadow　　D. /etc/profie

【答案】C

【解析】本题考查 Linux 系统下 shadow 文件的基本概念。

Shadow 文件用于存储 Linux 系统中用户账号密码配置文件。

若要显示 IP 路由表的内容，可以使用命令(37)，

(37)A. Netstat －s　　B. Netstat －r　　C. Netstat －n　　D. Netstat －a

【答案】B

【解析】本题考查常用网络命令。

Netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议相关的信息，其中参数 r 用于打印当前系统的路由信息。

下列命令中，不能查看网关 IP 地址的是（38）。

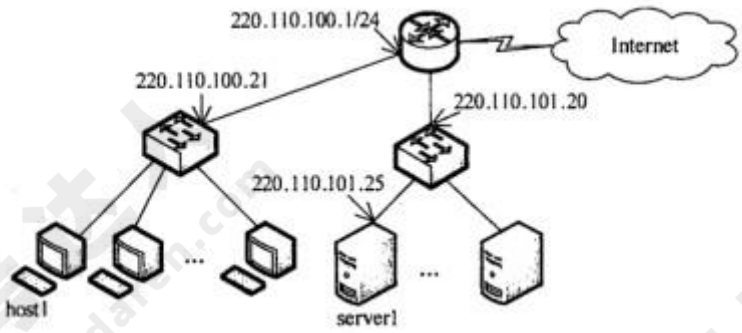
(38)A. Nslookup　　B. Tracert　　C. Netstat　　D. Route print

【答案】A

【解析】本题考查常用网络命令。

Tracert、Netstat 及 Route print 均可以获得网关 IP 地址信息。

某网络拓扑如下图所示，在主机 host1 上设置默认路由的命令为（39）；在主机 host1 上增加一条到服务器 server1 主机路由的命令为（40）。



(39)A. route add 220.110.101.25 mask 255.255.255.255 220.110.100.1

B. route add 220.110.100.1 0.0.0.0 mask 0.0.0.0

C. route add 0.0.0.0 mask 0.0.0.0 220.110.100.1

D. add route 220.110.100.1 0.0.0.0 mask 0.0.0.0

(40)A. add route 220.110.100.1 220.110.101.25. mask 255.255.255.0

B. route add 220.110.101.25. mask 255.255.255.0 220.110.100.1

C. route add 220.110.101.25. mask 255.255.255.255 220.110.100.1

D. add route 220.110.100.1 220.110.101.25. mask 255.255.255.255

【答案】C C

【解析】

Route 命令的功能是显示和修改本地的 IP 路由表，其语法如下：

route [-f] [-p] [Command [Destination] [mask Netmask] [Gateway] [metric Metric]] [if Interface]]

例如，若要对网关地址 220.110.100.1 要添加一条默认路由，则命令为：

route add 0.0.0.0 mask 0.0.0.0 220.110.100.1

在主机 host1 上增加一条到服务器 server1 主机路由，需要指定 server1 的 IP 地址，掩码为 255.255.255.255，下一跳为 host1 所在网络的网关，即 route add 220.110.101.25. mask 255.255.255.255 220.110.100.1。

在 SNMPv3 中，把管理站（Manager)和代理（Agent)统一叫做 (41)。

(41)A. SNMP 实体 B. SNMP 引擎 C. 命令响应器 D. 命令生成器

【答案】A

【解析】本题考查 SNMP 协议的基础知识。

按照 SNMP 协议的体系结构，网络管理系统由管理站（Manager)和代理（Agent) 两种功

能实体组成。

在 SNMPv3 中管理站（Manager)和代理（Agent)两种功能实体统一叫做 SNMP 实体（SNMP entity)。实体是体系结构的一种实现，由一个或多个 SNMP 引擎（SNMP engine)和一个或者多个 SNMP 应用（SNMP Application)组成。

SNMPv3 的应用程序分为命令生成器、命令响应器、通知发送器、通知接收器和代理转发器 5 种。

下列选项中，同属于报文摘要算法的是（42)。

(42)A. DES 和 MD5　　B. MD5 和 SHA-1　　C. RSA 和 SHA-1　　D. DES 和 RSA

【答案】B

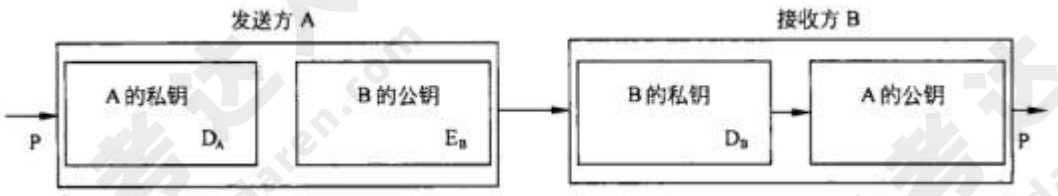
【解析】本题考查安全算法相关常识。

数据加密的基本过程就是对原来为明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码，通常称为“密文”，从而使其只能在输入相应的密钥之后才能显示 出本来内容，通过这样的途径来达到保护数据不被非法人窃取、阅读的目的。

常见加密算法有：DESCData Encryption Standard)、3DES(Triple DES)、RC2 和 RC4、IDEA (International Data Encryption Algorithm)、RSA.

报文摘要算法主要应用在“数字签名”领域，作为 明文的摘要算法。著名的摘要算法有 RSA 公司的 MD5 算法和 SHA1 算法及其大量的变体。

下图所示为一种数字签名方案，网上传送的报文是（43)，防止 A 抵赖的证据是（44)。



(43)A. P　　B. DA(P)　　C. EB(DA(P))　　D. DA

(44)A. P　　B. DA(P)　　C. EB(DA(P))　　D. DA

【答案】C　B

【解析】本题考查数字签名的实现过程。

题图中所示为一种利用公钥加密算法实现的数字签名方案，发送方 A 要发送给接收方 B 的报文 P 经过 A 的私钥签名和 B 的公钥加密后形成报文 EB(DA(P))发送给 B，B 利用自己的

私钥 DB 和 A 的公钥 EA 对消息 EB(DA(P))进行解密和认证后得到报文 P，并且保存经过 A 签名的消息 DA(P)乍为防止 A 抵赖的证据。

下面关于域本地组的说法中，正确的是（45）。

(45)A.成员可来自森林中的任何域，仅可访问本地域内的资源

B.成员可来自森林中的任何域，可访问任何域中的资源

C.成员仅可来自本地域，仅可访问本地域内的资源

D.成员仅可来自本地域，可访问任何域中的资源

【答案】A

【解析】本题考查 Windows Server 2003 活动目录中用户组的概念。

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)。其中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；域本地组成员来自森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 用组成员来自森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。

在 Kerberos 认证系统中，用户首先向（46）申请初始票据，然后从（47)获得会话密钥。

(46)A.域名服务器 DNS　　B.认证服务器 AS

C.票据授予服务器 TGS　　D.认证中心 CA

(47)A.域名服务器 DNS　　B.认证服务器 AS

C.票据授予服务器 TGS　　D.认证中心 CA

【答案】B　C

【解析】本题考查 Kerberos 认证系统的基础知识。

Kerberos 认证系统的认证过程如下图所示。

①用户向认证服务器 AS 申请初始票据；

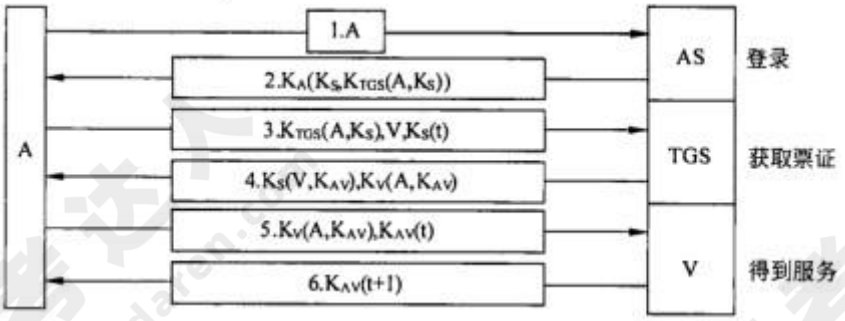
②认证服务器 AS 向用户发放票据授予票据（TGT)；

③用户向 TGS 请求会话票据；

④TGS 验证用户身份后发放给用户会话票据 Kav；

⑤用户向应用服务器请求登录；

⑥应用服务器向用户验证时间戳。



HTTPS 的安全机制工作在（48），而 S-HTTP 的安全机制工作在 （49）

(48)A. 网络层　　B. 传输层　　C. 应用层　　D. 物理层

(49)A. 网络层　　B. 传输层　　C. 应用层　　D. 物理层

【答案】B　C

【解析】本题考查安全协议的概念。

安全的超文本传输协议（Secure HTTP，S-HTTP)是一个面向报文的安全通信协议，是 HTTP 协议的扩展，位于应用层。

SSL/TLS 位于传输层，SSI7TLS 在 Web 安全通信中被称为 HTTPS。

下面病毒中，属于蠕虫病毒的是（50）。

(50)A. Worm. Sasser 病毒　　B. Trojan. QQPSW 病毒

C. Backdoor. IRCBot 病毒　　D. Macro. Melissa 病毒

【答案】A

【解析】本题考查计算机病毒的基础知识。

病毒文件名称一般分为三部分，第一部分表示病毒的类型，如 Worm 表示蠕虫病毒，Trojan 表示特洛伊木马，Backdoor 表示后门病毒，Macro 表示宏病毒等。

互联网规定的 B 类私网 IP 地址为（51）.

(51)A. 172. 16. 0. 0/16　　B. 172. 16. 0. 0/12

C. 172. 15. 0. 0/16　　D. 172. 15. 0. 0/12

【答案】B

【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

如果一个公司有 2000 台主机，则必须给它分配（52）个 C 类网络。为了使该公司网络在路由表中只占一行，指定给它的子网掩码应该是（53）.

(52)A.2　　B.8　　C.16　　D.24

(53)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】

无类别的域间路由（Classless Inter-Domain Routing，CIDR)技术解决路由缩放问题。所谓路由缩放有两层含义：其一是对于大多数中等规模的组织没有适合的地址空间，这样的组织一般拥有几千台主机，C 类网络太小，只有 254 个地址，B 类网络太大，有 65 000 多个地址，A 类网络就更不用说了，况且 A 类和 B 类地址也快分配完了；其二是路由表增长太快，如果所有的 C 类网络号都在路由表中占一行，这样的路由表就太大了，其查找速度无法达到满意的程度。CIDR 技术就是解决这两个问题的，它可以把若干个 C 类 网络分配给一个用户，并且在路由表中只占一行，这是一种将大块的地址空间合并为少量路由信息的策略。由于一个 C 类网络可以提供 254 个主机地址，所以 2000 个地址需要 8 个 C 类网络。 把 8 个 C 类网络汇聚成一个超网地址，使用的网络掩码为 255.255.248.0。

ISP 分配给某公司的地址块为 199.34.76.64/28,则该公司得到的地址数是（54）。

(54)A.8　　B.16　　C.32　　D.64

【答案】B

【解析】

地址块 199.34.76.64/28 的二进制形式如下：

11000111.00100010.01001100.01000000

11111111.1111 1111.1111 1111.11110000

由于网络掩码占用了 28 位，只有 4 位留给主机地址，所以只有 16 个地址（包括全 0 和全 1 地址）。

由 16 个 C 类网络组成一个超网（supernet),其网络掩码（mask)应为（55)。

(55)A. 255. 255. 240. 16　　B. 255. 255. 16. 0

C. 255. 255. 248. 0　　D. 255. 255. 240. 0

【答案】D

【解析】

16 个 C 类网络组成一个超网，其网络掩码(mask)应为 255. 255. 240. 0。

设 IP 地址为 18. 250. 31. 14，子网掩码为 255. 240. 0. 0,则子网地址是（56)。

(56)A. 18. 0. 0. 14　　B. 18. 31. 0. 14　　C. 18. 240. 0. 0　　D. 18. 9. 0. 14

【答案】C

【解析】

IP 地址 18. 250. 31. 14/255. 240. 0. 0 的二进制形式为：

00010010. 11111010. 00011111. 00001110

11111111. 11110000. 00000000. 00000000

则子网地址是 00010010. 11110000. 00000000. 00000000,即 18. 240. 0. 0。

IPv6 的“链路本地地址”是将主机的（57)附加在地址前缀 1111 1110 10 之后产生的。

(57)A. IPv4 地址　　B. MAC 地址　　C. 主机名　　D. 任意字符串

【答案】B

【解析】

IPv6 中的链路本地地址是将主机网卡的 MAC 地址附加在链路本地地址前缀 1111 1110 10 之后形成的。链路本地地址用于同一链路相连的结点间通信。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。

如果要设置交换机的 IP 地址，则命令行提示符应该是（58)。

(58)A. Switch>　　B. Switch#　　C. Switch(config) #　　D. Switch(config-if)#

【答案】C

【解析】

如果要设置交换机的IP地址，应进入全局配置模式，其命令行提示符为Switch(config)#。Switch(config-if)#为端口配置模式，Switch#为特权模式，Switch>为用户模式。

路由器命令“Router(config-subif)# encapsulation dotlq 1”的作用是(59)。

(59)A.设置封装类型和子接口连接的VLAN号　　B.进入VLAN配置模式

C.配置VTP口号　　D.指定路由器的工作模式

【答案】A

【解析】

路由器命令“Router(config-subif)# encapsulation dotlq 1”的作用是设置封装类型为802.1q,子接口连接的虚拟局域网编号为VLAN 1。

若路由器显示的路由信息如下，则最后一行路由信息是怎样得到的？(60)。

```
R3#show ip route
Gateway of last resort is not set
192.168.0.0/24 is subnetted, 6 subnets
C 192.168.1.0 is directly connected, Ethernet0
C 192.168.65.0 is directly connected, Serial0
C 192.168.67.0 is directly connected, Serial 1
R 192.168.69.0 [120/1] via 192.168.67.2, 00:00:15, Serial1
[120/1] via 192.168.65.2, 00:00:24, Serial0
R 192.168.5.0 [120/1] via 192.168.67.2, 00:00:15,Serial1
R 192.168.3.0 [120/1] via 192.168.65.2, 00:00:24, Serial0
```

(60)A.串行口直接连接的　　B.由路由协议发现的

C.操作员手工配置的　　D.以太网端口直连的

【答案】B

【解析】

对路由表中的最后一项 R 192.168.3.0 [120/1] via 192.168.65.2, 00:00:24, Serial0

解释如下：

①R——表示该路由是由 RIP 协议获取的，C 代表直接相连的网段；

②192.168.3.0 表示目标网段；

③[120/1]——120 表示 RIP 的管理距离（默认值），1 是该路由的度量值（跳数）；

④Via 经由的意思；

⑤192.168.65.2——表示从当前路由器出发到达目标的下一跳点的 IP 地址；

⑥00:00:24——表示该条路由产生的时间；

⑦Serial0——表示该路由的输出端口。

按照 802.1d 生成树协议(STP),在交换机互连的局网中,(61)的交换机被选为根交换机。

(61)A.MAC 地址最小的　　B.MAC 地址最大的

C.ID 最小的　　D.ID 最大的

【答案】C

【解析】

按照 802.1d 生成树协议（STP),在交换机互连的局域网中，ID 最小的交换机被选为根交换机。网桥或交换机 ID 由优先级和 MAC 地址两部分组成。

以太网中采用了二进制指数后退算法，这个算法的特点是（62)。

(62)A.网络负载越轻，可能后退的时间越长

B.网络负载越重，可能后退的时间越长

C.使得网络既可以适用于突发性业务，也可以适用于流式业务

D.可以动态地提高网站发送的优先级

【答案】B

【解析】

在检测到冲突时，为减少再一次冲突的概率，按照下面的二进制指数后退算法计算后退时间：随着重发次数 n 的增加，后退时延 t § 按 2 的指数增大。即：第一次试发送时 n 值为 0，每冲突一次 n 的值增加 1，并按下式计算后退时延

$$\begin{cases} \xi=\text{random}[0,2^n] \\ t_\xi=\xi\tau \end{cases}$$

中 r(网络最大传播时延的 2 倍）是一个很重要的参数，表示网络上检测冲突的最长时间。

上面第一式表示在区间[0, 2n]中取一均匀分布的随机整数§第二式的作用是计算出随机后退时延。按照这种方法，网络负载越重，可能后退的时间越长。

为了避免无限制的重发，要对重发次数 n 行限制，当 n 增加到某一最大值（例如 16)时停止发送，并向上层协议报告发现的错误。

以太网帧格式如下图所示，其中“填充”字段的作用是（63）。

前导字段	帧起始符	目的地址	源地址	长度	数据	填充	校验和

(63)A.可用于表示任选参数　　B.表示封装的上层协议

C.表示控制帧的类型　　D.维持 64 字节的最小帧长

【答案】D

【解析】

以太网规定了最小帧长，以避免在发送的过程中检测不到冲突。如果帧中包含的数据较少，则要填充冗余字节，以便补充到 64 字节的最小帧长。

IEEE802.11 采用了 CSMA/CA 协议，下面关于这个协议的描述中错误的是（64)。

(64)A.各个发送站在两次帧间隔（IFS)之间进行竞争发送

B.每一个发送站维持一个后退计数器并监听网络上的通信

C.各个发送站按业务的优先级获得不同的发送机会

D.CSMA/CA 协议适用于突发性业务

【答案】C

【解析】

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

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

②听到信道空闲后等待一个 IFS 时间，然后开始计数。最先计数完的站开始发送。

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

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

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

(65)A.扩频技术是一种带宽很宽的红外线通信技术

B.扩频技术就是用伪随机序列对代表数据的模拟信号进行调制

C.扩频通信系统的带宽随着数据速率的提高而不断扩大

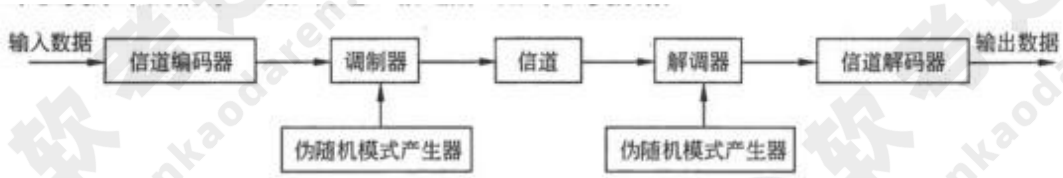
D.扩频技术扩大了频率许可证的使用范围

【答案】B

【解析】

IEEE 802.11 WLAN 中使用扩展频谱通信技术，这种技术的特点是将信号散布到更宽的频带上以减少发生阻塞和干扰的机会。有两种扩频方式，一种是频率跳动扩频(Frequency Hopping Spread Spectrum, FHSS)，另外一种是直接序列扩频（Direct SequenceSpread Spectrum，DSSS ）。

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



伪随机序列由一个使用初值（称为种子）的算法产生。算法是确定的，因此产生的数字序列并不是统计随机的。但如果算法设计得好，得到的序列还是能够通过各种随机性测试的，这就是被叫做伪随机序列的原因。除非你知道算法与种子，否则预测序列是不可能的。因此只有与发送器共享一个伪随机序列的接收器才能对信号进行解码。

Wi-Fi 联盟制定的安全认证方案 WPA (Wi-Fi Protected Access)是(66)标准的子集。

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

【答案】D

【解析】

Wi-Fi (Wireless Fidelity)是无线通信技术的商标，由 Wi-Fi 联盟（Wi-Fi Alliance)所持有，使用在经过认证的 IEEE 802.11 产品上，其目的是改善基于 IEEE 802.11 标准的网络产品之间的兼容性.

无线网络中的安全问题从暴露到最终解决经历了相当长的时间。这期间，Wi-Fi 联盟 的厂商们迫不及待地以 802.11i 草案的一个子集为蓝图制定了称为 WPA (Wi-Fi Protected Access)的安全认证方案，以便在市场上及时推出新的无线网络产品。

在 WPA 的设计中包含了认证、加密和数据完整性校验三个组成部分。首先是 WPA 使用了 802.1X 协议对用户的 MAC 地址进行认证；其次是 WEP 增大了密钥和初始向量的长度，以 128 比特的密钥和 48 位的初始向量（IV)用于 RC4 加密。WPA 还采用了可以动态改密钥的临时密钥完整性协议（Temporary Key Integrity Protocol，TKJP),以更频繁地变换密钥来减少安全风险。最后，WPA 强化了数据完整性保护。在 IEEE 802.11 标准中定义的 WEP 协议使用的循环冗余校验方法具有先天性缺陷，在不知道 WEP 密钥的情况下，要篡改分组和对应的 CRC 也是可能的。WPA 使用报文完整性编码来检测伪造的数据包，并且在报文认证码中包含有帧计数器，还可以防止重放攻击。

IEEE 802.11i 标准正式发布后，Wi-Fi 联盟就按照新的安全标准对无线产品进行认证，并且把这种认证方案称为 WPA2。

为了确定一个网络是否可以连通，主机应该发送 ICMP (67)报文。

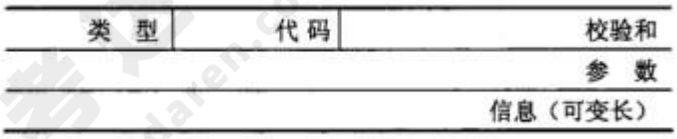
(67)A. 回声请求　B. 路由重定向　C. 时间戳请求　D. 地址掩码请求

【答案】A

【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，因而不保证可靠的提交。

ICMP 报文的格式如下所示。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 ICMP 各类报文的含义。

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。

在域名系统中，根域下面是顶级域（TLD)。在下面的选项中（68)属于全世界通用的顶级域。

(68)A.org　　B.cn　　C.microsoft　　D.mil

【答案】A

【解析】

域名系统 DNS 的逻辑结构是一个分层的域名树，Internet 网络信息中心（Internet Network Information Center, InterNIC)管理着域名树的根，称为根域。根域没有名称，用圆点表示，是域名空间的最高级别。在 DNS 的名称中，有时在末尾附加一个就是表示根域，但经常是省略的。DNS 服务器可以自动补上结尾的圆点，也可以处理结尾带圆点的域名。根域下面是顶级域（Top-Level Domains，TLD),分为国家顶级域（country code Top Level Domain, ccTLD)和通用顶级域（generic Top Level Domain，gTLD)。国家顶级域名包含 243 个国家和地区代码，例如 cn 代表中国，uk 代表英国等。最初的通用顶级域有 7 个，如下表所示，这些顶级域名原来主要供美国使用，随着 Internet 的发展，com、org 和 net 成为全世界通用的顶级域名，这就是所谓的国际域名，而 edu、gov 和 mil 则限于美国使用。

com	商业机构等盈利性组织
edu	教育机构、学术组织、国家科研中心等
gov	美国非军事性的政府机关
mil	美国的军事组织
net	网络信息中心(NIC)和网络操作中心(BIC)等
org	非盈利性组织，例如技术支持小组，计算机用户小组等
int	国际组织

负责互联网域名注册的服务商 ICANN 在 2000 年 11 月决定，从 2001 年开始使用 7 个新的国际顶级域名：biz（商业机构)、info（网络公司)、name（个人网站)、pro（医生和律师等职业人员)、aero（航空运输业专用)、coop（商业合作社专用）和 museum（博物馆专用)，其中前 4 个是非限制性域名，后 3 个限于专门的行业使用，受有关行业组织的管理。

2008 年 6 月，ICANN 在巴黎年会上通过了个性化域名方案，可以用公司名字为结尾的域名，例如 ibm、hp、qq 等。可以认为，这些域名的所有者在某种意义上就是一个域名注册机构，今后将会有无穷多的国际域名。

顶级域下面是二级域，这是正式注册给组织和个人的唯一名称，例如 www.micosoft.com 中的 micotsoft 就是微软注册的域名。

在二级域之下，组织机构还可以划分子域，使其各个分支部门都获得一个专用的名称标识，例如 www.sales.micosoft.com 中的 sales 是微软销售部门的子域名称。划分子域的工作可以一直延续下去，直到满足组织机构的管理需要为止。但是标准规定，一个域 名的长度通常不超过 63 个字符，最多不能超过 255 个字符。

DNS 标准还规定，域名中只能使用'ASCII 字符集的有限子集，包括 26 个英文字母（不区分大小写）和 10 个数字，以及连字符"-"并且连字符不能作为子域名的第一个和最后一个字母。后来的标准对字符集有所扩大。

在网络设计阶段进行通信流量分析时可以采用简单的 80/20 规则，下面关于这种规则的说明中，正确的是（69）。

(69)A.这种设计思路可以最大限度地满足用户的远程联网需求

B.这个规则可以随时控制网络的运行状态

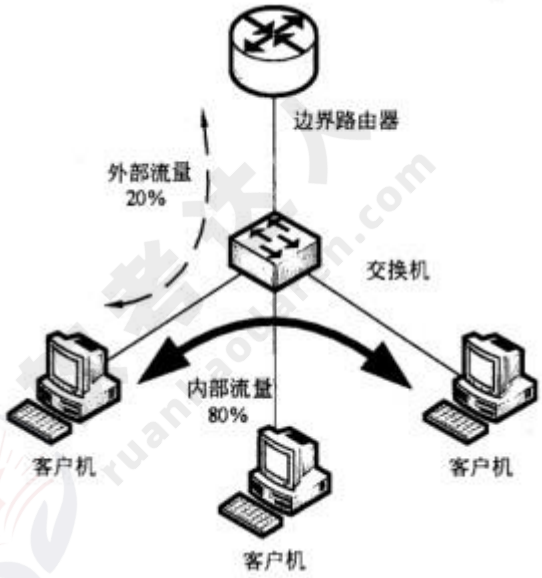
C.这个规则适用于内部交流较多而外部访问较少的网络

D.这个规则适用的网络允许存在具有特殊应用的网段

【答案】C

【解析】

在网络规划过程中，需要根据业务需求和应用需求来计算各个信息流量的大小，并根据通信模式、通信边界的分析，确定不同信息流在网络的不同区域和区域边界上的分布情况。对于较为简单的网络，不需要进行复杂的通信流量分析，仅采用一些简单的方法就可以确定通信流量，例如 80/20 规则等。但是对于复杂的网络，仍必须进行复杂的通信流量分布分析。根据 80/20 规则如下图所示，对一个网段内部的通信流量并不进行严格的计算，仅仅是根据用户和应用需求进行统计，产生网段内总的通信流量，并认为总量的 80%是在网段内部，而 20%是对网段外部的流量.



80/20 规则是一种设计思路，通过这种方式可以限制用户的不合理需求，是最优化地使用网络骨干和使用昂贵的广域网连接的一种行之有效的方法。例如，如果核心交换机容量为100Mb/s，局域网至外部的带宽应限制在 20Mb/s 以内。

80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

随着互联网络的发展，出现了另外一种通信情况，即网段内部用户之间相互访问较少，大多数通信都是对网段外部资源的访问。例如小区内计算机用户形成的局域网络，大型公司用于实现远程协同工作的工作组网络等。对于这种情况，可以采用 20/80 规则。

根据 20/80 规则，要根据用户和应用需求的统计数据产生网段内的通信总量大小，并认为总量的 20%是在网段内部的流量，而 80%是网段外部的流量。

根据用户需求选择正确的网络技术是保证网络建设成功的关键，在选择网络技术时应考虑多种因素。下面的各种考虑中，不正确的是（70）。

(70) A. 选择的网络技术必须保证足够的带宽，使得用户能够快速地访问应用系统

B. 选择网络技术时不仅要考虑当前的需求，而且要考虑未来的发展.

C. 越是大型网络工程，越是要选择具有前瞻性的新的网络技术

D. 选择网络技术要考虑投入产出比，通过投入产出分析确定使用何种技术

【答案】C

【解析】

根据用户需求选择网络技术时应考虑如下因素：

(1)通信带宽

所选择的网络技术必须保证足够的带宽，能够保证用户快速地访问应用系统。在进行选择时，不仅局限于现有的应用需求，还要适当考虑将来的带宽增长需求。

(2)技术成熟性

所选择的网络技术必须是成熟稳定的技术，有些新的网络技术在尚没有大规模投入使用时，还存在着较多不确定因素，这将会对网络建设带来很多无法估量的损失。对于大型网络工程来说，项目本身不能成为新技术的试验田。使用较为成熟、拥有较多案例的技术是明智的选择。

(3)可扩充性

网络设计的设计依据是详细的需求分析，但是在选择网络技术时，不能仅考虑当前的需求而忽视未来的发展。在大多数情况下，设计人员都会在网络带宽、数据吞吐量、用户并发数等方面的设计中预留一定的冗余量。一般来说，这个冗余量值在70%～80%之间。

(4)高投资产出

选择网络技术的关键是投入产出比，尤其是一些借助于网络来实现营运的工程项目，只有通过投入产出分析，才能最后决定使用何种技术。

Border Gateway Protocol (BGP) is inter-autonomous system (71) protocol. BGP is based on a routing method called path vector routing. Distance vector routing is not a good candidate for inter-autonomous system routing because there are occasions on which the route with the smallest (72) count is not the preferred route. For example, we may not want a packet through an autonomous system that is not secure even though it is the shortest route. Also, distance vector routing is unstable due to the fact that the routers announce only the number of hop counts to the destination without actually defining the path that leads to that (73) .A router that receives a distance vector advertisement packet may be fooled if the shortest path is actually calculated through the receiving router itself. Link (74) routing is also not a good candidate for inter-autonomous system routingbecause an internet is usually too big for this routing methoD. To use link state routing for the whole internet would require each router to have a huge link state database. It would also take a long

time for each router to calculate its routing (75) using the Dijkstra algorism.

(71)A.routing B.switching C.transmitting D.receiving

(72)A.path B.hop C.route D.packet

(73)A.connection B.window C.source D.destination

(74)A.status B.search C.state D.research

(75)A.table B.state C.mertric D.cost

【答案】A B D C A

【解析】

边界网关协议（BGP)是自治系统之间的路由协议。BGP 基于一种叫做通路矢量路由的路由算法。距离矢量路由算法对于自治系统之间的路由选择不是一种好方法，因为会出现一种情况，最小跳步数路由并不是所期望的路由。例如，我们不希望分组通过一个不安全的自治系统，虽然它是最短路由。同时，距离矢量路由不合适还由于下面的事实，路由器只宣布到达目标的跳步数，而没有实际定义到达那个目标的通路。如果要计算的最短通路实际上通过接收路由器本身，则接收到距离矢量公告分组的路由器就被欺骗了。对于自治系统间的路由，链路状态算法也不是好的选项，因为互联网对于这种路由方法是太大了.把链路状态算法用于整个互联网，则要求每一个路由器维护一个巨大的链路状态数据库。这就要求每一个路由器花费很长时间根据 Dijkstra 算法计算它的路由表。

试题一

某企业欲构建局域网，考虑到企业的很多业务依托于网络，要求企业内部用户能够高速的访问企业服务器，并且对网络的可靠性要求很高。因此，在网络的设计中，要考虑网络的冗余性，不能因为单点故障引起整个网络的瘫痪。

某网络公司根据企业需求，将网络拓扑结构设计为双核心来进行负载均衡，当其中一个核心交换机出现故障时，数据能够转换到另一台交换机上，起到冗余备份的作用。该公司给出的网络拓扑如图 1-1 所示。

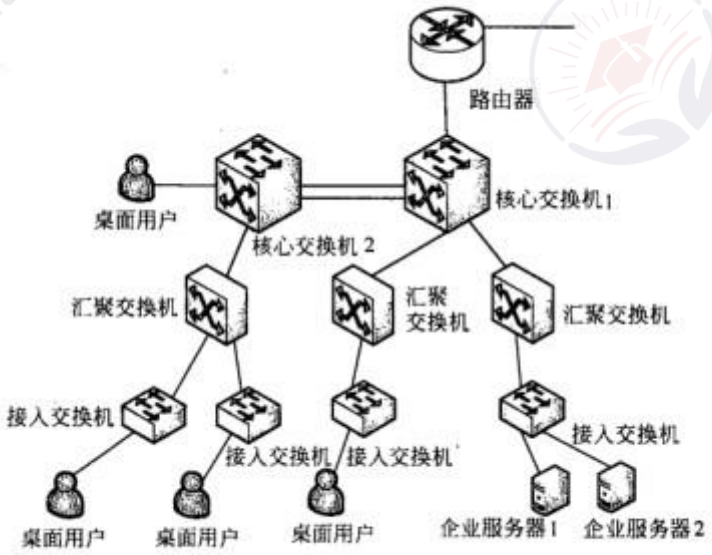


图 1-1

【问题 1】

在该网络拓扑图中，请根据用户需求和设计要求，指出至少三个不合理之处，并简要说明理由。

1. 汇聚交换机应该分别链路连接到 2 个核心交换机，形成链路冗余，保证网络的可靠性。

2. 2 个核心交换机都应直接上连到路由器上，保证网络的可靠性。

3. 服务器应该连接到核心交换机，保证高速访问。

4. 桌面用户不应直接接入到核心交换机上，影响核心交换机性能。

本题考查网络规划及网络故障排除的基本知识。

本问题考查双核心网络结构的基本知识。双核心网络结构主要由两台核心交换设备构建局域网核心，该网络一般也是通过与核心交换机互连的路由设备接入广域网，并且路由器与两台

核心交换设备之间都存在物理链路。

双核心结构一般有如下特点：

•核心交换设备在实现上多采用三层交换机或多层交换机；

•网络内各 VLAN 之间访问需要经过两台核心交换设备中的一台；

•网络中除核心交换设备之外，不存在其他的具备路由功能的设备；

•核心交换设备之间运行特定的网关保护或负载均衡协议，例如 HSRP、VRRP、GLBP 等；

•核心交换设备与各 VLAN 设备间可以采用 10M/100M/1000M 以太网连接；

•网络拓扑结构可靠；

•路由层面可以时间无缝热切换；

•部门局域网络访问核心局域网以及相互之间多条路径选择可靠性更高；

•在核心交换设备端口富余的前提下，部门网络接入较为方便；

•设备投资比单核心高；

•对核心路由设备的端口密度要求较高；

•核心交换设备和桌面计算机之间，存在接入交换设备，接入交换设备同时和双核心存在物理连接；

•所有服务器都直接同时连接至两台核心交换机，借助于网关保护协议，实现桌面用户对服务器的高速访问。

根据双核心结构的特点和题目要求及拓扑结构图可以判断，该网络拓扑图中的不合理之处有：

①汇聚交换机应该分别链路连接到 2 个核心交换机，形成链路冗余，保证网络的可靠性。

②2 个核心交换机都应直接上联到路由器上，保证网络的可靠性。

③服务器应该连接到核心交换机，保证高速访问。

④桌面用户不应直接接入到核心交换机上，影响核心交换机性能。

【问题 2】

该企业有部分分支机构地处其他省市，计划采用 MPLS VPN 进行网络互连，请根据 MPLS VPN 的技术原理回答以下问题：

1.MPLS 技术主要是为了提高路由器转发速率而提出的，其核心思想是利用标签交换取代复杂的路由运算和路由交换；该技术实现的核心就是把（1)封装在（2)数据包。

(1)、(2)备选答案：

A. IP 数据报。B. MPLS 。C. TCP 。D. GRE。

2.MPLS VPN 承载平台上的设备主要由各类路由器组成，其中(3)是 MPLS 核心网中的路由器，

这些路由器只负责依据 MPLS 标签完成数据包的高速转发，(4) 是 MPLS 核心网上的边缘路由器，负责待传送数据包的 MPLS 标签的生成和弹出，还将发起根据路由建立交换标签的动作。(5)是直接与电信运营商相连的用户端路由器，该设备上不存在任何带有标签的数据包。

(3)～(5)备选答案：

A. PE 路由器。B. CE 路由器。C. P 路由器。

(1) A. IP 数据报。(2) B. MPLS。(3)P 路由器。(4)PE 路由器。(5)CE 路由器。

本问题考查 MPLS 技术的基本知识。

MPLS (Multi-protocol Label Switching)是多协议标签交换的简称，它用短而定长的标签来封装分组。MPLS 从各种链路层（如 PPP、ATM、帧中继、以太网等）得到链路层服务，又为网络层提供面向连接的服务。MPLS 能从 IP 路由协议和控制协议中得到支持，同时还支持基于策略的约束路由，路由功能强大、灵活，可以满足各种新应用对网络的要求。

MPLS 技术主要是为了提高路由器转发速度而提出的，其核心思想是利用标签交换取代复杂的路由运算和路由交换；该技术实现的核心就是在 IP 数据包之外封装一个 32 比特的 MPLS 包头，MPLS 体系中的各个路由设备将根据 MPLS 包头中的标签进行转发，而不是传统方式下根据 IP 包头中的目标地址来转发；由于 MPLS 标签栈可以无限嵌套，从而提供无限的业务支持能力，而 MPLS VPN 就是一个典型的标签嵌套应用。

MPLS VPN 承载平台上的设备主要由各类路由器组成，这些路由器在 MPLS VPN 平台中的角色各不相同，分别被称为 P 设备、PE 设备、CE 设备；P (Provider Router)路由器是 MPLS 核心网中的路由器，这些路由器只负责依据 MPLS 标签完成数据包的高速转发；PE (Provider Edge Router)路由器是 MPLS 核心网上的边缘路由器，与用户的 CE 路由器互连，PE 设备负责待传送数据包的 MPLS 标签的生成和弹出，负责将数据包按标签发送给 P 路由器或接收来自 P 路由器的含标签数据包，PE 路由器还将发起根据路 由建立交换标签的动作；CE (Custom Edge)路由器是直接与电信运营商相连的用户端路由器，该设备上不存在任何带有标签的数据包，CE 路由器将用户网络的信息发送给 PE 路由器，以便于在 MPLS 平台上进行路由信息的处理。

【问题 3】

企业网络运行过程中会碰到各种故障。一方面，网络管理人员可以利用网络设备及系统

本身提供的集成命令对网络进行故障排除，例如利用(6)命令查看系统的安装情况与网络的正常运行状况。另一方面，利用专用故障排除工具可以快速的定位故障点，例如利用(7) 可以精确地测量光纤的长度、定位光纤的断点。

(6)备选答案：

A. ping B. debug C. show D. tracert

(7)备选答案：

A.数字万用表 B.时域反射计

C.光时域反射计 D.网络分析仪

(6)C 或 show. (7) C 或光时域反射计.

本问题考查网络故障排除的基本知识。

利用网络设备及系统提供的集成命令可以监视网络并排除故障。一些常用的诊断命令有：

show 可以用于监测系统的安装情况与网络的正常运行状况，也可以用于对故障区域的定位。

debug 命令帮助分离协议和配置问题。

ping 命令用于检测网络上不同设备之间的连通性。

trace 命令可以用于确定数据包在从一个设备到另一设备直至目的地的过程中所经过的路径。

专用故障排除工具：

典型的排除网络故障的专用工具如下：

（1）欧姆表、数字万用表及电缆测试器

欧姆表、数字万用表属于电缆检测工具中比较低档的一类。这类设备能够测量诸如交直流电压、电流、电阻、电容以及电缆连续性之类的参数。利用这些参数可以检测电缆的物理连通性。

（2）时域反射计与光时域反射计

电缆检测工具中比较高¥当的是时域反射计（TDR)。这种设备能够快速的定位金属电缆中的断路、短路、压接、扭结、阻抗不匹配及其他问题。

对于光纤的测试则需要使用光时域反射计（OTDR)。OTDR 可以精确地测量光纤的长度、定位光纤的断裂处、测量光纤的信号衰减、测量接头或连接器造成的损耗。

(3)断接盒、智能测试盘和位/数据块错误测试器

断接盒、智能测试盘和位/数据块错误测试器（BERT/BLERT)是用于测量 PC、打印机、调制解调器、信道服务：设备/数字服务设备（CSU/DSU)以及其他外围接口数字信号的数字接口测试工具。

(4)网络监测器

网络监测器能够持续不断地跟踪数据包在网络上的传输，能够提供任何时刻网络活动的精确描述或者一段时间内网络活动的历史记录。

(5)网络分析仪

网络分析仪（network analyzer)，也称为协议分析仪（protocol analyzer)，它能够对不同协议层的通信数据进行解码，详细表示哪个层被调用（物理层、数据链路层等)，以及每个字节或者字节内容起什么作用。

试题二

Linux 系统有其独特的文件系统 ext2,文件系统包括了文件的组织结构、处理文件的数据结构及操作文件的方法。可通过命令获取系统及磁盘分区状态信息，并能对其进行管理。

【问题 1】

以下命令中，改变文件或所属群组的命令是（1),编辑文件的命令是（2)，查找文件的命令是（3）。

(1)～(3)备选答案：

A. chmod B. chgrp C. vi D. which

(1)B 或 chgrp (2) C 或 vi (3) D 或 which

本问题主要考查对常用文件操作命令的了解程度。

【问题 2】

Linux 系统中，用户和应用程序可以通过（4)文件系统得到系统的信息，并可以改变内核的某些参数，该文件系统只存在于内存中。

(4)备选答案：

A. /proc B. ntfs C. /tmp D. /etc/profile

（4） A 或 /proc

本问题主要考查 Linux 系统中/proc 文件系统的基本概念。

【问题 3】

在 Linux 中，分区分为主分区、扩展分区和逻辑分区，使用 fdisk-l 命令获得分区信息如下所示：

```
Disk /dev/hda:240 heads, 63 sectors, 1940 cylinders
Units = cylinders of 15120 * 512 bytes
Device Boot      Start  End      Blocks         Id         System
                                  —  -
```

```
/dev/hda    1       286     2162128+    c       Win95 FAT32 (LBA)
/dev/hda2 * 288     1940    12496680    5       Extended
/dev/hda5   288     289     15088+      83      Linux
/dev/hda6   290     844     4195768+    83      Linux
/dev/hda7   845     983     1050808+    82      Linux swap
/dev/hda8   984     1816    6297448+    83      Linux
/dev/hda9   1817    1940    937408+     83      Linux
```

其中属于扩展分区的是（5）

使用 df-T 命令获得信息部分如下：

```
Filesystem   Type    1K Blocks   Used    Available   Use%    Mounted on
/dev/hda6    reiserfs 4195632    2015020 2180612     49%     /
/dev/hda5    ext2    14607       3778    10075       8%      /boot
/dev/hda9    reiserfs 937372     202368  735004      22%     /home
/dev/hda8    reiserfs 6297248    3882504 2414744     62%     /opt
Shmfs    shm         256220      0       256220      0%      /dev/shm
/dev/hda1    vfat    2159992     1854192 305800      86%     /windows/C
```

其中，不属于 Linux 系统分区的是（6）.

（5）/dev/hda2 （6） /dev/hda1

本问题主要考查 Linux 系统分区的基础知识。

【问题 4】

在 Linux 系统中，对于（7）文件中列出的 Linux 分区，系统启动时会自动挂载。此外，超级用户可通过（8）命令将分区加载到指定目录，从而该分区才在 Linux 系统中可用。

（7）/etc/fstab （8） mount

本问题考查对 Linux 系统中/etc/fstab 配置文件及分区加载命令的熟悉程度。

试题三

某网络拓扑结构如图 3-1 所示，网络 1 和网络 2 的主机均由 DHCP_Server 分配 IP 地址。FTP_Server 的操作系统为 Windows Server 2003，Web_Server 的域名为 www.softexamtest.com。

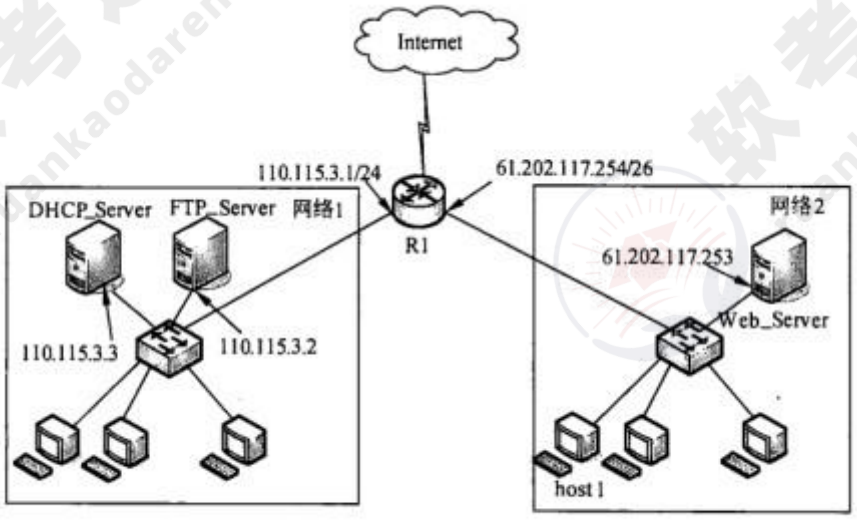


图 3-1

【问题 1】

DHCP_Server 服务器必须包含的 IP 地址范围为（1)和（2).

（1）110.115.3.4 ～110.115.3.254

（2） 61.202.117.193～61.202.117.252（（1)、(2）可互换）

DHCP_Server 服务器需为网络 1 和网络 2 的主机分配 IP 地址。由网络 1 和网络 2 的网关分别为 110.115.3.1/24 与 61.202.117.254/26 可知，网络 1 包含的可用的 IP 地址范围为 110.115.3.1 ～ 110.115.3.254，网络 2 可用的 IP 地址范围为 61.202.117.193 ～ 61.202.117.254，除去网络 1 和网络 2 中已用的服务器和路由器接口地址，能分配的地址区间为 110.115.3.4～110.115.3.254 和 61.202.117.193～61.202.117.252。

【问题 2】

若在 host1 上运行 ipconfig 命令，获得如图 3-2 所示结果，host1 能正常访问 Internet 吗？说明原因。

不能。由于该主机地址是自动专用 IP 地址（APIPA),即当客户机无法从 DHCP 服务器中获得 IP 地址时自动配置的地址。

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

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

host1 的 IP 地址为 169.254.150.219，故不能正常访问 Internet。

【问题 3】

若 host1 成功获取 IP 地址后，在访问 http://www.abc.com 网站时，总是访问到 www.softexamtest.com，而同一网段内的其他客户端访问该网站正常。在 host1 C:\WINDOWS\system32\drivers\etc 目录下打开（3）文件，发现其中有如下两条记录：

```
127.0.0.1       localhost
   (4)          www.abc.com
```

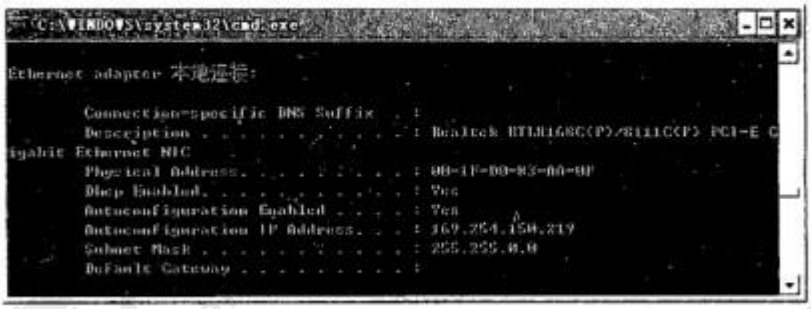


图 3-2

在清除第 2 条记录后关闭文件，重启系统后 host1 访问 http://www.abc.com 网站正常，请填充空（4)处空缺内容。

(3)hosts （4）61.202.117.253

host11 访问 http://www.abc.com 网站时总是访问到 www.softexamtest.com，而同一网段内的其他客户端访问该网站正常。可知在 host1 本地 hosts 文件中应该存在一条 DNS 记录，把域名 www.abc.com 映射到 www.softexamtest.com 所对应的 IP 地址，故解决该故障的方法是打开 host1 的 hosts 文件，清除该记录，重启系统。

hosts 文件中记录的格式为：IP 地址域名，故空（3)处应填入 hosts,空（4)处 应填入 61.202.117.253。

【问题 4】

在配置 FTP_server 时，图 3-3 中“IP 地址”文本框中应填入（5)

图 3-3

(5)110.115.3.2

“IP 地址”文本框中应填入的是该 FTP 站点对应的 IP 地址，故空(5)处应填入 110.115.3.2。

【问题 5】

若 FTP 配置虚拟目录为 pen，虚拟目录配置如图 3-4 与图 3-5 所示。

图 3-4

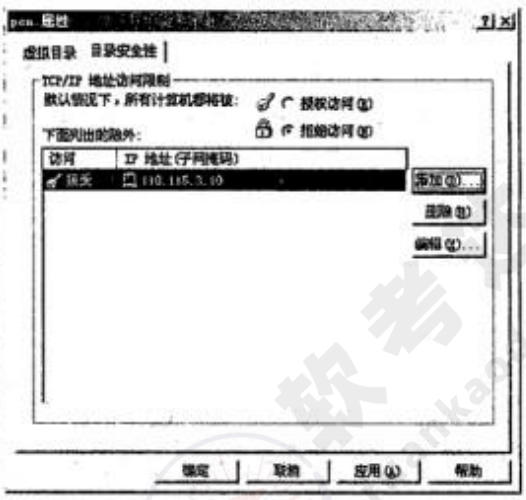


图 3-5

根据以上配置，哪些主机可访问该虚拟目录？访问该虚拟目录的命令是（6）。

只有 110.115.3.10 可访问该虚拟目录。

(6)ftp://110.115.3.2:2121 或 ftp://110.115.3.2:2121/pen

图中显示除了添加上的 IP 地址可以访问虚拟目录 pen,其他均拒绝访问，故具有访问权限的只有主机 110.115.3.10。由配置方式的不同，采用带虚拟目录名和不带虚拟目录名两种方式均可访问该站点，再加上配置图中已经指明 TCP 的端口号为 2121，故访问该虚拟目录的命令为 ftp://110.115.3.2:2121 或 ftp://110.115.3.2:2121/pen 均可。

试题四

某公司两分支机构之间的网络配置如图 4-1 所示，为保护通信安全，在路由器 router-a 和 router-b 上配置 IPSec 安全策略，对 192.168.8.0/24 网段和 192.168.9.0/24 网段之间的数据进行加密处理。

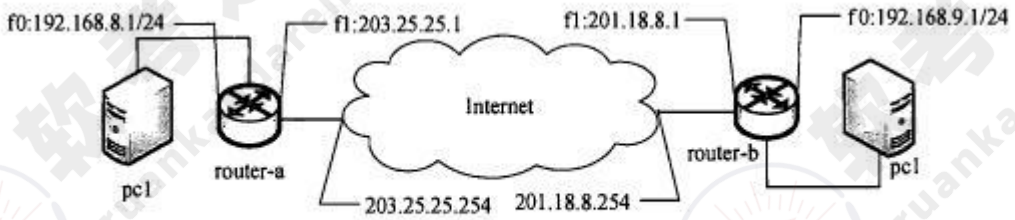


图 4-1

【问题 1】

为建立两分支机构之间的通信，请完成下面的路由配置命令。

```
router-a (config) #ip route  0.0.0.0  0.0.0.0  (1)
router-b (config) #ip route  0.0.0.0  0.0.0.0  (2)
```

(1) 203.25.25.254 (2) 201.18.8.254

本题考查考生在路由器上配置 IPSec 安全策略的实际操作能力。

本问题考查如何在两个路由器上配置默认路由，从图 4-1 中可以得到 router-a 的默认路由是 203.25.25.254，router-b 的默认路由是 201.18.8.254。

【问题 2】

下面的命令是在路由器 router-a 中配置 IPSec 随道。请完成下面的隧道配置命令。

```
router-a(config)# crypto tunnel tun1          (设置 IPSec 隧道名称为 tun1)
router-a(config-tunnel)# peer address (3)     (设置隧道对端 IP 地址)
router-a(config-tunnel)# local address (4)    (设置隧道本端 IP 地址)
router-a(config-tunnel)# set auto-up          (设置为自动协商)
router-a(config-tunnel)# exit                 (退出隧道设置)
```

(3)201.18.8.1 (4) 203.25.25.1

本问题考查如何在 router-a 上配置 IPSec 隧道，对端 IP 地址应该是 router-b 的 f1 口地址 201.18.8.1，本地地址是 router-b 的 f1 口地址 203.25.25.1。

【问题 3】

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

```
router-a(config)# crypt  ike key 12345678 address __(5)__
router-b(config)# crypt  ike key 12345678 address __(6)__
```

(5)201.18.8.1 (6) 203.25.25.1

本问题考查如何在 router-a 与 router-b 之间预设共享密钥，address 后面是对端的 id，默认是对端的 IP 地址。

【问题 4】

下面的命令在路由器 router-a 中配置了相应的 IPSec 策略，请说明该策略的含义。

```
router-a(config)# crypto policy p1
router-a(config-policy)# flow 192.168.8.0 255.255.255.0 192.168.9.0
255.255.255.0
ip tunnel tun1
router-a(config-policy)#exit
```

从 192.168.8.0/24 子网到 192.168.9.0/24 子网的所有 IP 报文经由 IPSec 隧道到达。

本问题考查如何配置相应的 IPSec 策略，该策略说明从 192.168.8.0/24 子网到 192.168.9.0/24 子网的所有 IP 报文经由 IPSec 隧道到达。

【问题 5】

下面的命令在路由器 router-a 中配置了相应的 IPSec 提议，该提议表明：IPSec 采用 ESP 报文，加密算法采用（7),认证算法采用（8)。

```
router-a(config)# crypto ipsec proposal secp1
router-a(config-ipsec-prop)# esp 3des sha1
router-a(config-ipsec-prop)# exit
```

(7)3DES (8) SHA-1

本问题考查如何配置 IPSec 提议，提议表明 IPSec 采用 ESP 报文，加密算法采用 3DES,认证算法采用 SHA-U

试题五

某单位网络的拓扑结构示意图如图 5-1 所示。该网络采用 RIP 协议，要求在 R2 上使用访问控制列表禁止网络 192.168.20.0/24 上的主机访问网络 192.168.10.0/24,在 R3 上使用访问控制列表禁止网络 192.168.20.0/24 上的主机访问 10.10.10.0/24 上的 Web 服务,但允许其访问其他服务器。

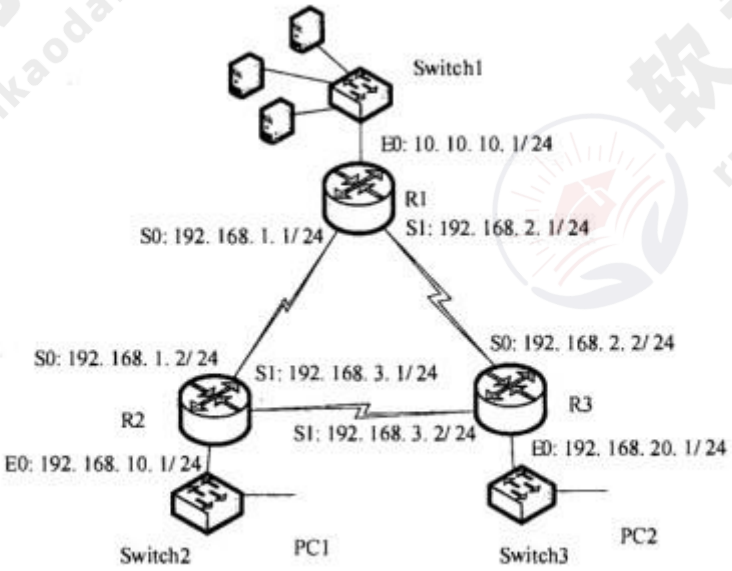


图 5-1

【问题 1】

下面是路由器 R1 的部分配置，请根据题目要求，完成下列配置。

```
……
R1(config)# interface Serial0
R1(config-if)# ip address ___(1)___ ___(2)___
R1 (config)#ip routing
R1 (config)#__(3)___                          (进入 RIP 协议配置子模式)
R1 (config-router)#__(4)___                   (声明网络 192.168.1.0/24)
……
```

(1) 192.168.1.1 (2) 255.255.255.0 (3) router rip (4)network 192.168.1.0

本问题考查路由器的 RIP 协议的配置及路由器接口地址的基本配置操作。根据题目拓扑结构图可知，路由器 R1 的 S0 口地址为 192.168.1.1/24;所以其配置如下：

```
……
R1(config)# interface Serial0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1 (config)#ip routing
R1 (config)# router rip                          (进入 RIP 协议配置子模式)
R1 (config-router)# network 192.168.1.0          (声明网络 192.168.1.0/24)
……
```

【问题 2】

下面是路由器 R2 的部分配置，请根据题目要求，完成下列配置。

```
R2# config t
R2(config)# access-list 50 deny 192.168.20.0  0.0.0.255
R2(config)# access-list 50 permit  any
R2(config)# interface  (5)
R2(config-if)# ip access-group  (6)  (7)
```

(5) fastethemet 0/0 (或 ethemet0/0) (6) 50 (7) out

本问题考查标准 ACL 的基本配置。根据题目要求，要求在 R2 上使用访问控制列表 禁止网络 192.168.20.0/24 上的主机访问网络 192.168.10.0/24。根据题目拓扑结构图可知，该 ACL 应该配置在 R2 的 E0 口上，方向为 out。所以配置命令如下：

```
R2# config t
R2(config)# access-list 50 deny 192.168.20.0  0.0.0.255
                          (创建 ACL50 拒绝源 192.168.20.0/24 数据)
R2(config)# access-list 50 permit  any
R2(config)# interface fastethernet 0/0          (进入端口 E0 配置模式)
R2(config-if)# ip access-group 50  out          (激活 ACL  50)
```

【问题 3】

1. 下面是路由器 R3 的部分配置，请根据题目要求，完成下列配置。

R3 (config) # access-list 110 deny (8) 192.168.20.0 0.0.0.255 10.10.10.00.0.0.255 eg (9)

R3 (config)# access-list 110 permit ip any any

2. 上述两条语句次序是否可以调整？简单说明理由。

1. (8) tcp (9) www 或 80

2. 不可以调整次序，acl 执行顺序是自上而下，一旦次序调整后，原第一条规则失效。

本问题考查扩展 ACL 的基本配置。

1.根据题目要求，在 R3 上使用访问控制列表禁止网络 192.168.20.0/24 上的主机访问 10.10.10.0/24 上的 Web 服务，但允许其访问其他服务器。对于 TCP 和 UDP 协议，扩展 ACL 配置命令的格式如下：

```
Router(config)# access-list 100-199|2000-2699 permit|deny tcp|udp
source_address source_wildcard_mask [operator source_port_#]

destination_address destination_wildcard_mask [operator destination_port_#]
[established] [log]
```

所以，路由器 R3 配置如下：

```
……
    R3(config)# access-list 110 deny tcp 192.168.20.0 0.0.0.255 10.10.10.0
0.0.0.255 eq www _
    R3(config)# access-list 110 permit ip any any
```

2.上述两条语句次序不可以调整。因为路由器对-CL 语句的处理规则如下：

• 一旦发现匹配的语句，就不再处理列表中的其 4 语句，所以语句的排列顺序非常重要；

•如果整个列表中没有匹配的语句，则分组被丢弃。

在本例中，如果次序调整，则语句 access-list 110 permit ip any any 将放行所有数据，包括网络 192.168.20.0/24 上的主机访问 10.10.10.0/24 上的 Web 服务，这样语句 access-list 110 deny tcp 192.168.20.0 0.0.0.255 10.10.10.0 0.0.0.255 eq www 将失去作用。