在 CPU 中，(1)不仅要保证指令的正确执行，还要能够处理异常事件。

(1)A.运算器　　B.控制器　　C.寄存器组　　D.内部总线

【答案】B

【解析】本题考查计算机系统硬件方面的基础知识。

计算机中的 CPU 是硬件系统的核心，用于数据的加工处理，能完成各种算术、逻辑运算及控制功能。其中，控制器的作用是控制整个计算机的各个部件有条不紊地工作，它的基本功能就是从内存取指令和执行指令。

计算机中主存储器主要由存储体、控制线路、地址寄存器、数据寄存器和（2）组成。

(2)A.地址译码电路　　B.地址和数据总线　　C.微操作形成部件　　D.指令译码器

【答案】A

【解析】本题考查存储系统基础知识。

主存储器简称为主存、内存，设在主机内或主机板上，用来存放机器当前运行所需要的程序和数据，以便向 CPU 提供信息。相对于外存，其特点是容量小速度快。

主存储器主要由存储体、控制线路、地址寄存器、数据寄存器和地址译码电路等部分组成。

以下关于数的定点表示和浮点表示的叙述中，不正确的是（3）。

(3)A.定点表示法表示的数（称为定点数）常分为定点整数和定点小数两种

B.定点表示法中，小数点需要占用一个存储位

C.浮点表示法用阶码和尾数来表示数，称为浮点数

D.在总位数相同的情况下，浮点表示法可以表示更大的数

【答案】B

【解析】

本题考查数据表示基础知识。

各种数据在计算机中表示的形式称为机器数，其特点是采用二进制计数制，数的符号用0、1表示，小数点则隐含表示而不占位置。机器数对应的实际数值称为数的真值。

为了便于运算，带符号的机器数可采用原码、反码、补码和移码等不同的编码方法。

所谓定点数，就是表示数据时小数点的位置固定不变。小数点的位置通常有两种约定方式：定点整数（纯整数，小数点在最低有效数值位之后）和定点小数（纯小数，小数点在最高有效数值位之前）。

当机器字长为n时，定点数的补码和移码可表示2^n个数，而其原码和反码只能表示2^n－1个数（0表示占用了两个编码），因此，定点数所能表示的数值范围比较小，运算中很容易因结果超出范围而溢出。

数的浮点表示形式为：$N=2^E\times F$，其中E称为阶码，F为尾数。阶码通常为带符号的纯整数，尾数为带符号的纯小数。浮点数的表示格式如下：

阶符	阶码	数符	尾数

很明显，一个数的浮点表示不是唯一的。当小数点的位置改变时，阶码也相应改变，因此可以用多种浮点形式表示同一个数。

浮点数所能表示的数值范围主要由阶码决定，所表示数值的精度则由尾数决定

X、Y为逻辑变量，与逻辑表达式$X+\bar{X}Y$等价的是__（4）__。

(4) A. $X+\bar{Y}$　　B. $\bar{X}+\bar{Y}$　　C. $\bar{X}+Y$　　D. $X+Y$

【答案】D

【解析】本题考查逻辑运算基础知识。

题中各逻辑式的真值表如下所示。

X	Y	$X+\bar{X}Y$	$X+\bar{Y}$	$\bar{X}+\bar{Y}$	$\bar{X}+Y$	$X+Y$
0	0	0	1	1	1	0
0	1	1	0	1	1	1
1	0	1	1	1	0	1
1	1	1	1	0	1	1

在软件设计阶段，划分模块的原则是，一个模块的__（5）__。

(5) A. 作用范围应该在其控制范围之内　　B. 控制范围应该在作用范围之内

C. 作用范围与控制范围互不包含　　D. 作用范围与控制范围不受任何限制

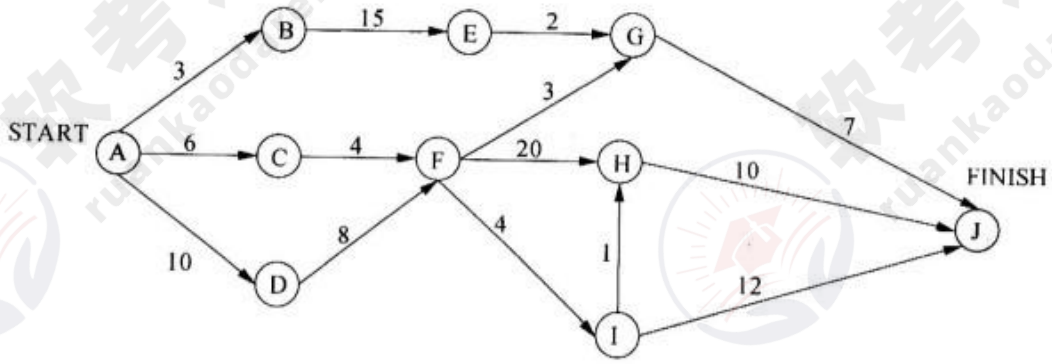
【答案】A

【解析】

模块的作用范围定义为受该模块内一个判定影响的模块集合，模块的控制范围为模块本

身以及所有直接或间接从属于该模块的模块集合。其作用范围应该在控制范围之内。

下图是一个软件项目的活动图，其中顶点表示项目里程碑，连接顶点的边表示包含的活动，则里程碑（6）在关键路径上，活动 FG 的松弛时间为（7）。



(6) A. B　　B. C　　C. D　　D. I

(7) A. 19　　B. 20　　C. 21　　D. 24

【答案】C　B

【解析】

该活动图的关键路径为 ADFHJ 关键路径长度为 48 天，因此里程碑 D 在关键路径上，B、C 和 I 步骤关键路径上。活动 FG 的最早开始时间为第 19 天，最晚开始时间为第 39 天，因此松弛时间为 20 天。

设文件索引节点中有 8 个地址项，每个地址项大小为 4 字节，其中 5 个地址项为直接地址索引，2 个地址项是一级间接地址索引，1 个地址项是二级间接地址索引，磁盘索引块和磁盘数据块大小均为 1KB 字节。若要访问文件的逻辑块号分别为 5 和 518,则系统应分别采用（8）。

(8) A. 直接地址索引和一级间接地址索引

B. 直接地址索引和二级间接地址索引

C. 一级间接地址索引和二级间接地址索引

D. 一级间接地址索引和一级间接地址索引

【答案】C

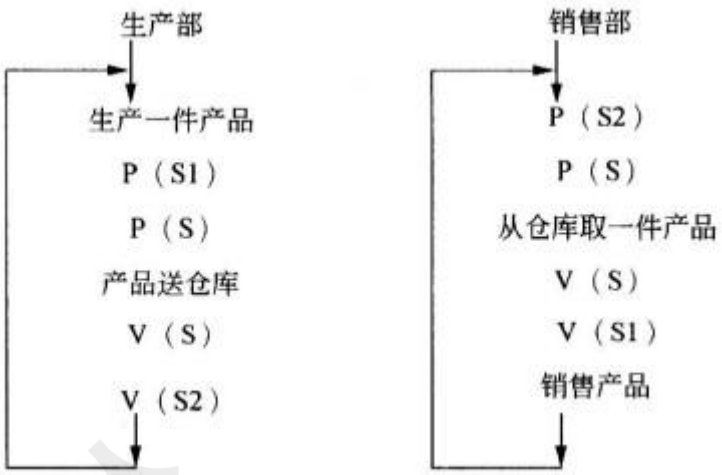
【解析】本题考查操作系统文件管理方面的基础知识。

根据题意，磁盘索引块为 1KB 字节，每个地址项大小为 4 字节，故每个磁盘索引块可存

放 1024/4=256 个物理块地址。又因为文件索引节点中有 8 个地址项，其中 5 个地址项为直接地址索引，这意味着逻辑块号为 0～4 的为直接地址索引；2 个地址项是一级间接地址索引，这意味着第一个地址项指出的物理块中存放逻辑块号为 5～260 的物理块号，第一个地址项指出的物理块中存放逻辑块号为 261～516 的物理块号；1 个地址项是二级间接地址索引，该地址项指出的物理块存放了 256 个间接索引表的地址，这 256 个间接索引表存放逻辑块号为 517～66052 的物理块号。

经上分析不难得出，若要访问文件的逻辑块号分别为 5 和 518,则系统应分别采用一级间接地址索引和二级间接地址索引。

某企业有生产部和销售部，生产部负责生产产品并送入仓库，销售部从仓库取出产品销售。假设仓库可存放 n 件产品。用 PV 操作实现他们之间的同步过程如下图所示。



图中信号量 S1 和 S2 为同步信号量，初值分别为 n 和 0；S 是一个互斥信号量，初值为（9）。

(9)A. 0　　B. 1　　C. n　　D. -1

【答案】B

【解析】本题考查 PV 操作方面的基本知识。

根据题意，可以通过设置三个信号量 S、S1、S2,其中，S 是一个互斥信号量，初值为 1，因为仓库是一个互斥资源，所以将产品送仓库时需要执行进行 P (S)操作，当产品放入仓库后需要执行 V (S)操作。

M 软件公司的软件产品注册商标为 M，为确保公司在市场竞争中占据优势，对员工进行了保密约束。此情形下该公司不享有（10）。

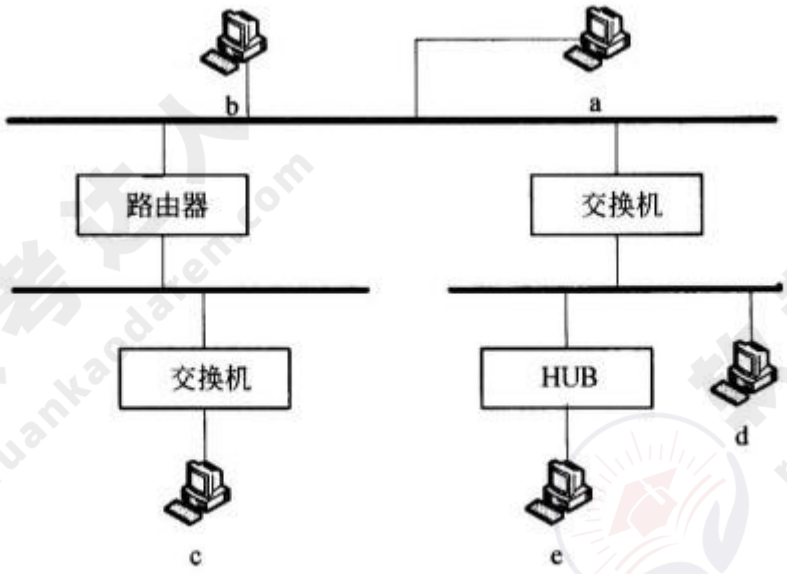
(10)A. 商业秘密权　　B. 著作权　　C. 专利权　　D. 商标权

【答案】C

【解析】本题考查知识产权基础知识。

关于软件著作权的取得，《计算机软件保护条例》规定：“软件著作权自软件开发完成之日起产生，即软件著作权自软件开发完成之日起自动产生，不论整体还是局部，只要具备了软件的属性即产生软件著作权，既不要求履行任何形式的登记或注册手续，也无须在复制件上加注著作权标记，也不论其是否已经发表都依法享有软件著作权。软件开发经常是一项系统工程，一个软件可能会有很多模块， 而每一个模块能够独立完成某一项功能。自该模块开发完成后就产生了著作权。软件公司享有商业秘密权。因为一项商业秘密受到法律保护的依据，必须具备构成商业秘密的三个条件，即不为公众所知悉、具有实用性、采取了保密措施。商业秘密权保护软件是以软件中是否包含着“商业秘密”为必要条件的。该软件公司组织开发的应用软件具有商业秘密的特征，即包含着他人不能知道到的技术秘密；具有实用性，能为软件公司带来经济效益；对职工进行了保密的约束，在客观上已经采取相应的保密措施。所以软件公司享有商业秘密权。商标权、专利权不能自动取得，申请人必须履行商标法、专利法规定的申请手续，向国家行政部门提交必要的申请文件，申请获准后即可取得相应权利。获准注册的商标通常称为注册商标。

下面的地址中，属于全局广播地址的是（11）。在下面的网络中，IP 全局广播分组不能通过的通路是（12）。



(11)A. 172. 17. 255. 255　　B. 0. 255. 255. 255

C. 255. 255. 255. 255　　D. 10. 255. 255. 255

(12)A. a 和 b 之间的通路　　B. a 和 c 之间的通路

C. b 和 d 之间的通路　　D. b 和 e 之间的通路

【答案】C　B

【解析】

IP 地址可以划分为“网络地址”和“主机地址”两部分。主机地址部分全为“0” 地址称为网络地址，例如 129. 45. 0. 0 就是指一个 B 类网络地址。主机地址部分全为“1” 的地址称为广播地址，例如 129. 45. 255. 255 就是一个 B 类广播地址，这种地址也称为定向广播地址，意味着网络 129. 45. 0. 0 中的主机都可以接收这个数据报。所有字节为全“1” 的地址 255. 255. 255. 255 是全局广播地址，理论上，以这种地址为目标地址的全局广播分组可以传播到任何网络中去，但是为了避免不必要的通信干扰，一般路由器都会阻止这种分组进入本地网络，所以全局广播分组一般不能通过路由器进行扩散，也就是说，路由器可以把整个互联网络分成互相区分的许多子网。

下面用于表示帧中继虚电路标识符的是（13）。

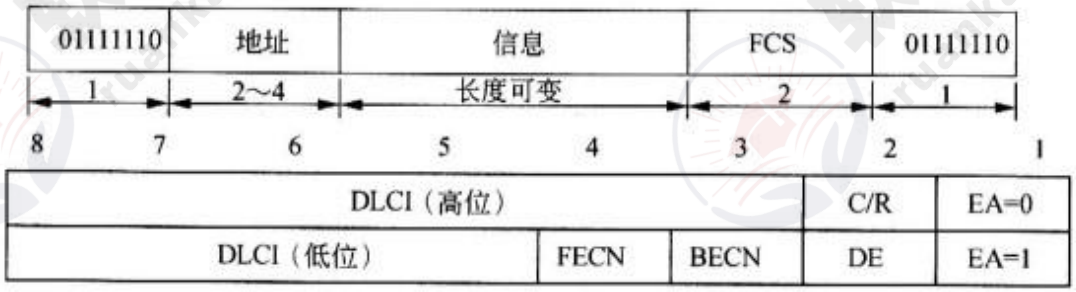
(13)A. CIR　　B. LMI　　C. DLCI　　D. VPI

【答案】C

【解析】

帧中继协议 LAP-D(Q. 921)的帧格式如下图所示。帖头和帧尾都是编码为“01111110” 的

帧标志字段，信息字段长度可变，1600 是默认的最大长度。帧效验序列 FCS 与 HDLC 的相同。EA 为地址扩展比特，EA 为 0 时表示地址向后扩展一个字节，EA 为 1 时表示最后一个字节。C/R 是命令/响应比特，协议本身不使用这个比特，用户可以用这个比特区分不同的帧。FECN 是向前拥塞比特，若网络置该位为 1，则表示在帧的传送方向上出现了拥塞，BECN 是向后拥塞比特，若网络置该位为 1，则表示在与帧传送相反的方向上出现了拥塞。DE 是优先丢弃比特，当网络发生拥塞时，DE 置位的帧被优先丢弃。最后，DLCI 表示数据链路连接标识符。



下面关于 RS-232-C 标准的描述中，正确的是（14）。

(14)A. 可以实现长距离远程通信　　B. 可以使用 9 针或 25 针 D 型连接器

C. 必须采用 24 根线的电缆进行连接　　D. 通常用于连接并行打印机

【答案】B

【解析】

RS-232-C 是美国电子工业协会制定的串行接口标准，其机械特性规定可以使用 9 针或 25 针的 D 型连接器。功能特性采用 V.24 建议，如果只采用主通道进行双工通信，仅需少数几根线（例如 3 根或 9 根）就可以了。由于驱动器允许有 2500pF 的电容负载，所以通信距离会受到限制，例如采用 150pF/m 的电缆时，最大通信距离为 15m。另外，由于这个标准采用单端信号传送，共地噪声和共模干扰也限制了信号传送的距离，一般状况下，通信距离不超过 20m。

设信道带宽为 4000Hz，采用 PCM 编码，采样周期为 125 供，每个样本量化为 128 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】C

【解析】

PCM 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。采样的频率决定了可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。所以对带宽为 4000Hz 的信号的采样频率必须大于 8000Hz，即 125 押。量化为 128 个等级，即用 7 位二进制编码来表示一个采样值，这样，7X8000=56Kb/s。

在异步通信中，每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 1 位终止位，每秒钟传送 200 个字符，采用 DPSK 调制，则码元速率为（16），有效数据速率为（17）。

(16)A. 200 波特　　B. 500 波特　　C. 1000 波特　　D. 2000 波特

(17)A. 200b/s　　B. 1000b/s　　C. 1400b/s　　D. 2000b/s

【答案】D　C

【解析】

由于每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 1 位终止位，总共 10 位，每秒钟传送 200 个字符，即波特率为 10X200=2000 波特。而有效数据速率为 7X200=1400b/s„

以下关于 ICMP 协议的说法中，正确的是（18）。

(18)A. 由 MAC 地址求对应的 IP 地址

B. 在公网 IP 地址与私网 IP 地址之间进行转换

C. 向源主机发送传输错误警告

D. 向主机分配动态 IP 地址

【答案】C

【解析】

在 TCP/IP 协议簇中，ICMP 协议的作用是提供网络层通信过程的差错控制和告警、以及网络邻居发现等功能，例如向源主机发送目标不可到达警告、获取默认路由器的地址等。

以下关于 RARP 协议的说法中，正确的是（19）。

(19)A. RARP 协议根据主机 IP 地址查询对应的 MAC 地址

B. RARP 协议用于对 IP 协议进行差错控制

C. RARP 协议根据 MAC 地址求主机对应的 IP 地址

D. RARP 协议根据交换的路由信息动态改变路由表

【答案】C

【解析】

ARP 协议根据目标的 IP 地址获取目标的 MAC 地址，而 RARP 协议根据本地主机的 MAC 地址请求对应的 IP 地址，这个协议主要用在无盘工作站中。

所谓“代理 ARP”是指由（20）假装目标主机回答源主机的 ARP 请求。

(20) A. 离源主机最近的交换机　　B. 离源主机最近的路由器

C. 离目标主机最近的交换机　　D. 离目标主机最近的路由器

【答案】B

【解析】

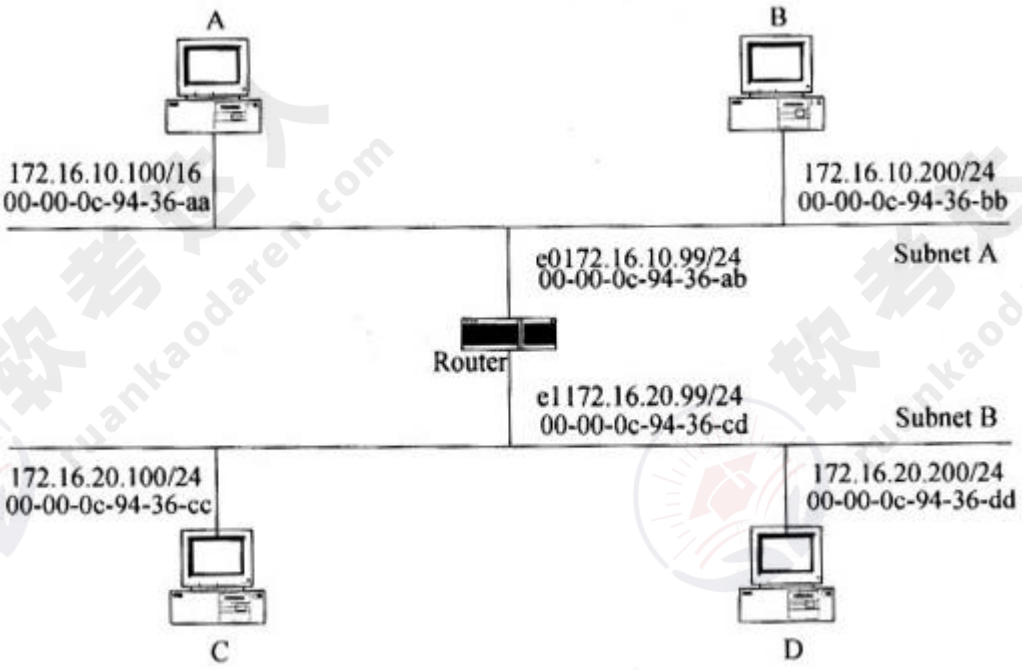
当两个主机通过 Internet 通信时，如果发送方主机不知道目标主机的 MAC 地址，就要广播一个 ARP 请求分组，这种分组的作用是由目标主机的 IP 地址求对应的 MAC 地址。收到这种请求分组的主机用自己的 IP 地址与目标结点协议地址字段比较，若相符则发回一个 ARP 响应分组，向发送方报告自己的硬件地址，若不相符则不予回答。

代理 ARP 如下图所示，设子网 A 上的主机 A (172.16.10.100)需要与子网 B 上的主机 D (172.16.20.200)通信。当主机 A 需要与它直接连接的设备通信时，它就向目标发送一个 ARP 请求。

主机 A 在子网 A 上广播的 ARP 请求分组是：

发送者的 MAC 地址	发送者的 IP 地址	目标的 MAC 地址	目标的 IP 地址
00-00-0c-94-36-aa	172.16.10.100	00-00-00-00-00-00	172.16.20.200

这个请求的含义是要求主机 D (172.16.20.200)回答它的 MAC 地址。ARP 请求分组被包装在以太帧中，其源地址是 A 的 MAC 地址，而目标地址是广播地址 (FFFF.FFFF.FFFF)。由于路由器不转发广播帧，所以这个 ARP 请求只能在子网 A 中传播，而到不了主机 D。



如果路由器知道目标地址(172.16.20.200)在另外一个子网中，它就以自己的 MAC 地址回答主机 A，路由器发送的应答分组是：

发送者的 MAC 地址	发送者的 IP 地址	目标的 MAC 地址	目标的 IP 地址
00-00-0c-94-36-ab	172.16.20.200	00-00-0c-94-36-aa	172.16.10.100

这个应答分组包装在以太帧中，以路由器的 MAC 地址为源地址，以主机 A 的 MAC 地址为目标地址，ARP 应答帧是单播传送的。在接收到 ARP 应答后，主机 A 就更新它的 ARP 表：

IP Address	MAC Address
172.16.20.200	00-00-0c-94-36-ab

此后主机 A 就把所有发送给主机 D (172.16.20.200)的分组发送给 MAC 地址为 00-00-0c-94-36-ab 的主机，这就是路由器的网卡地址。

通过这种方式，子网 A 中的 ARP 映像表都把路由器的 MAC 地址当作子网 B 中主机的 MAC 地址。例如主机 A 的 ARP 映像表如下所示：

IP Address	MAC Address
172.16.20.200	00-00-0c-94-36-ab
172.16.20.100	00-00-0c-94-36-ab
172.16.10.99	00-00-0c-94-36-ab
172.16.10.200	00-00-0c-94-36-bb

多个 IP 地址被映像到一个 MAC 地址这一事实正是代理 ARP 的标志。

在距离矢量路由协议中，每一个路由器接收的路由信息来源于（21）。

(21)A.网络中的每一个路由器　　B.它的邻居路由器

C.主机中存储的一个路由总表　　D.距离不超过两个跳步的其他路由器

【答案】B

【解析】

ARPAnet 最初采用了距离矢量路由协议 RIP，RIPv1 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，则认为该邻居不存在了。收到邻居发来的距离矢量后，路由器采用 Ford-Fulkerson 算法重新计算路由表。

在 BGP4 协议中，(22)报文建立两个路由器之间的邻居关系，(23)报文给出了新的路由信息。

(22)A.打开（open）　B.更新　C.保持活动（keepalive）　D.通告

(23)A.打开（open）　B.更新　C.保持活动（keepalive）　D.通告

【答案】A　B

【解析】

外部网关协议 BGP4 广泛地应用于不同 ISP 的网络之间，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 种报文表示在下表中。

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

在 BGP 中用上述 4 种报文可实现以下 3 个功能过程：

•建立邻居关系。建立邻居关系的过程是由一个路由器发送 Open 报文，另一个路由器若愿意接受请求则以 Keepalive 报文应答。Open 报文中包含发送者的 IP 地址及其所属自治系统的标识，另外还有一个保持时间参数，即定期交换信息的时间间隔。接收者把 Open 报文中的保持时间与自己的保持时间计数器比较，选取其中的较小者，这就是一次交换信息保持有效的最长时间。建立邻居关系的一对路由器以选定的周期交换路由信息。

•邻居可到达性。这个过程维护邻居关系的有效性，通过周期性地互相发送 Keepalive 报文，

双方都知道对方的活劫状态。

•网络可到达性。每个路由器维护一个数据库，记录着它可到达的所有子网。当情况有变化时用更新报文把最新消息及时地传送给其他 BGP 路由器。Update 报文包含两类信息：一类是要作废的路由器列表，另一类是新增路由的属性信息。

在 OSPF 协议中，链路状态算法用于（24）。

(24)A.生成链路状态数据库　　B.计算路由表

C.产生链路状态公告　　D.计算发送路由信息的组播树

【答案】B

【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 路由器发布链路状态公告，报告本地网络各个链路的状态信息。路由器收到的链路状态信息保存在本地的链路状态数据库中，这些数据可用于构造网络拓扑结构图。路由器使用 Dijkstra 的最短通路优先算法（Shortest Path first，SPF)根据网络拓扑结构图计算到达各个目标的最佳路由，生成新的路由表。

以下关于两种路由协议的叙述中，错误的是（25）.

(25)A.链路状态协议在网络拓扑发生变化时发布路由信息

B.距离矢量协议是周期性地发布路由信息

C.链路状态协议的所有路由器都发布路由信息

D.距离矢量协议是广播路由信息

【答案】C

【解析】

链路状态协议与距离矢量协议发布路由信息的时机不同，链路状态协议是在网络拓扑发生变化时才发布路由信息；而距离矢量协议是周期性地发布路由信息。链路状态协议使用了分层的网络结构，在广播网络或 NBMA 网络构成的区域中，OSPF 协议要选举一个指定路由器（DR)，由 DR 代表这个网络向外界发布路由信息，从而减小了链路状态公告的传播范围，同时也减小了网络拓扑变化时影响所有路由器的可能性；与之相反，距离矢量网络是扁平结构，所有路由器都在发布路由信息，并且网络某一部分出现的变化会影响到网络中的所有路由器。链路状态协议使用组播来共享路由信息，并且发布的是增量式的更新消息，这使得网络带宽

的利用率和资源消耗率得到改善；而距离矢量协议 RIP 是每隔 30 秒向所有邻居广播路由更新报文。链路状态协议支持无类别域间路由和路由汇聚功能，通过 CIDR 技术使得发布的路由信息减少，也使得链路状态数据库减小，从而减少了所需要的 CPU 周期，也减少了路由器中的存储需求;距离矢量协议 RIPv1 是有类别的协议，不支持 CIDR 技术。链路状态协议使用 SPF 算法计算最短通路，不会在路由表中出现环路，而这是距离矢量路由协议难以处理问题，必须采用水平分割、反向路由毒化或触发更新等特别方法来加快路由收敛，防止路由环路的形成。

下面的 D 类地址中，可用于本地子网作为组播地址分配的是（26）。一个组播组包含 4 个成员，当组播服务器发送信息时需要发出（27）个分组。

(26)A. 224.0.0.1　　B. 224.0.1.1　　C. 234.0.0.1　　D. 239.0.1.1

(27)A. 1　　B. 2　　C. 3　　D. 4

【答案】D　　A

【解析】

组播技术用于向一组目标发送同样的分组，每一个组播组被指定了一个 D 类地址作为组标识符，组播源利用组地址作为目标地址来发送分组。组播成员向网络发出通知，声明它期望加入的组的地址。IGMP 协议用于支持接收者加入或离开组播组。一旦有接收者加入了一个组，就要为这个组在网络中构建一个组播分布树，用于生成和维护组播 树的协议有许多种，例如独立组播协议 PIM 等。在 IP 组播模式下，组播源无须知道所有的组成员，组播树的构建是由接收者驱动的，是由最接近接收者的网络结点完成的， 这样建立的组播树可以扩展到很大的范围。有人形容 IP 组播模型是：你在一端注入一个分组，网络正好可以把这个分组提交给所有需要的接收者。

IPv4 的 D 类地址是组播地址，用作一个组的标识符，其地址范围是 224.0.0.0～239.255.255.255o 按照约定，D 类地址被划分为 3 类：

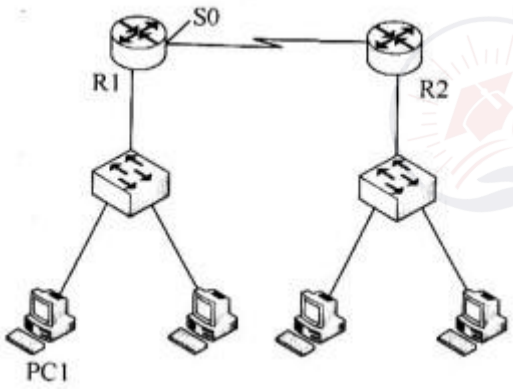
•224.0.0.0～224.0.0.255:保留地址，用于路由协议或其他下层拓扑发现协议以及维护管理协议等，例如 224.0.0.1 代表本地子网中的所有主机，224.0.0.2 代表本地子网中的所有路由器，224.0.0.5 代表所有 OSPF 路由器，224.0.0.9 代表所有 RIP2 路由器，224.0.0.12 代表 DHCP 服务器或中继代理，224.0.0.13 代表所有支 持 PIM 的路由器等。

•224.0.1.0～238.255.255.255:用于全球范围的组播地址分配，可以把这个范围的 D 类地址

动态地分配给一个组播组，当一个组播会话停止时，其地址被回收，以后还可以分配给新出现的组播组。

•239.0.0.0～239.255.255.255:在管理权限范围内使用的组播地址，限制了组播的范围，可以在本地子网中作为组播地址使用。

某网络拓扑结构如下图所示。



在路由器 R2 上采用命令（28）得到如下所示结果。

```
Router>
…
R    192.168.0.0/24 [120/1] via 202.117.112.1, 00:00:11, Serial2/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
  202.117.112.0/30 is subnetted, 1 subnets
C    202.117.112.0 is directly connected, Serial2/0
Router>
```

则 PC1 可能的 IP 地址为（29），路由器 R1 的 S0 口的 IP 地址为（30），路由器 R1 和 R2 之间采用的路由协议为（31）。

(28)A. netstat -r　　B. show ip route　　C. ip routing　　D. route print

(29)A. 192.168.0.1　　B. 192.168.1.1　　C. 202.117.112.1　　D. 202.117.112.2

(30)A. 192.168.0.1　　B. 192.168.1.1　　C. 202.117.112.1　　D. 202.117.112.2

(31)A. OSPF　　B. RIP　　C. BGP　　D. TGRP

【答案】B　A　D　B

【解析】本题考查路由器配置、路由相关基础知识。

在路由器上查看路由的命令为 show ip route。

由题干显示的 R2 路由信息可知，网络 192.168.1.0/24 直连快速以太口 0/0，网络

202.117.112.0/30 直连串口 2/0,网络 192.168.0.0/24 经串口 2 路由可达。由此可判断 PC1 所在网络为 192.168.0.0/24，路由器 R1 的 S0 口和 202.117.112.1 在一个子网，故 PC1 可能的 IP 地址为 192.168.0.1,路由器 R1 的 S0 口的 IP 地址为 202.117.112.2。

又由网络 192.168.0.0/24 经串口 2 路由采用协议的标志为“R”可知，路由器 R1 和 R2 之间采用的路由协议为 RIP。

DNS 服务器中提供了多种资源记录，其中（32）定义了区域的授权服务器。

(32)A. SOA　　B. NS　　C. PTR　　D. MX

【答案】B

【解析】本题考查 DNS 服务器资源记录相关基础知识。

资源记录分为许多不同的类型，常用的是（参见下表）：

• 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

•序列号：当区域文件改变时，序列号要增加，辅助服务器把自己的序列号与主服务器的序列号比较，以确定是否需要更新数据

•刷新间隔：辅助服务器更新数据的时间间隔（秒）

•重试间隔：当辅助服务器不能连接主服务器进行更新时，必须每隔一定时间间隔(秒）重新试图连接

•有效期：如果辅助服务器不能更新自己的区域文件，超过有效期（秒）后就不再提供查询服务

•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 (Mailexchanger)：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)

记 录 类 型	说　明	示　例
开始授权（SOA）	指明区域主服务器（primary nameserver） 指明区域管理员的邮件地址，及区域复制信息： 序列号 刷新间隔 重试间隔 有效期 TTL	区域 microsoft.com 的主服务器为 ns1.microsoft.com 2003080800　;serial number 172800　;refresh=2d 900　;retry=15m 1209600　;expire=2w 3600　;default TTL=1h
地址（A）	最常用的资源记录 把主机名解析为 IP 地址	compuer1.microsoft.com 被解析为 10.1.1.4
指针（PTR）	用于反向查询的资源记录 把 IP 地址解析为主机名	10.1.1.4 被解析为 compuer1.microsoft.com
名字服务器（NS）	为一个域指定了授权服务器 该域的所有子域也被委派给这个服务器	域 microsoft.com 的授权服务器为 ns2.microsoft.com
邮件服务器（MX）	指明区域的 SMTP 服务器	区域 microsoft.com 的邮件服务器为 mail.microsoft.com
别名（CNAME）	指定主机的别名 把主机名解析为另一个主机名	www.microsoft.com 的别名为 webserver12.microsoft.com

某主机本地连接属性如下图所示，下列说法中错误的是（33）。

(33) A. IP 地址是采用 DHCP 服务自动分配的

B. DHCP 服务器的网卡物理地址为 00-1D-7D-39-62-3E

C. DNS 服务器地址可手动设置

D. 主机使用该地址的最大租约期为 7 天

【答案】B

【解析】本题考查 DHCP 服务器配置相关知识。

从该主机的本地连接属性可以看出：该主机的 MAC 地址为 00-1D-7D-39-62-3E，IP 地址是采用 DHCP 服务自动分配的，租约期为 7 天。在选用 DHCP 自动分配 IP 地址时，可以手工设置 DNS 服务器地址。

Linux 系统中，DHCP 服务的主配置文件是（34），保存客户端租约信息的文件是（35）。

(34)A. dhcpd. leases　　B. dhcpd. conf　　C. xinetd. conf　　D. lease. conf

(35)A. dhcpd. leases　　B. dhcpd. conf　　C. xinetd. conf　　D. lease. conf

【答案】B　A

【解析】本题考查 Linux 系统 K DHCP 服务器配置的基础知识。

在 Linux 系统中，DHCP 服务由 dhcpd 提供，dhcpd 的配置文件是/etc/dhcpd. conf，dhcpd 中用于保存客广端租约信息的文件是/var/lib/dhcp/dhcpd. leases。

在 Windows Server 2003 操作系统中，WWW 服务包含在（36）组件下。

(36)A. DNS　　B. DHCP　　C. FTP　　D. IIS

【答案】D

【解析】本题考查在 Windows Server 2003 操作系统下有关网络服务组件的基础知识。

在 Windows Server 2003 操作系统下，虽然也包含 DNS、DHCP 服务，但 WWW、FTP 是包含在 IIS (Internet Information Services)服务下的。

DNS 正向搜索区的功能是将域名解析为 IP 地址，Windows XP 系统中用于测试该功能的命令是（37）。

(37)A. nslookup　　B. arp　　C. netstat　　D. query

【答案】A

【解析】本题考查在 Windows XP 操作系统下，常用的网络有关测试命令使用基础知识。

query：显示与终端服务器上运行的进程、用户会话等有关信息。 netstat：可以使用户了解到自己的主机是怎样与 Internet 相连接的，这有助于用户了解网络的整体使用情况。它可以显示当前正在活动的网络连接的详细信息，如网络连接、路由表和网络接口等信息，也可以让用户得知目前总共有哪些网络连接正在运行。

arp：显示和修改地址解析协议缓存中的项目，ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。

nslookup：显示可用来诊断域名系统（DNS)基础结构的信息。

在 Windows 环境下，DHCP 客户端可以使用（38）命令重新获得 IP 地址，这时客户机向 DHCP 服务器发送一个 Dhcpdiscover 数据包来请求重新租用 IP 地址。

(38)A. ipconfig/renew　　B. ipconfig/reload

C. ipconfig/release　　D. ipconfig/reset

【答案】A

【解析】本题考查在 Windows 操作系统下，DHCP 网络服务启动后，手动获取 IP 地址的知识。

ipconfig 命令的参数/renew:重新获得 IP 地址，符合本题的要求。

ipconfig 命令的参数/release:所有接口的租用 IP 地址便重新交付给 DHCP 服务器（归还 IP 地址）。

/reload 和/reset 是两个干扰项，ipconfig 不支持这两个参数。

匿名 FTP 访问通常使用（39）作为用户名。

(39)A. guest　　B. ip 地址　　C. administrator　　D. anonymous

【答案】D

【解析】本题考查有关 FTP 服务的管理基础知识，匿名用户的用户名称。

一般情况下，匿名用户的英语名称就是 anonymous，guest 是来宾用户，administrator 是超级用户，ip 地址是干扰项，不能使用 ip 地址作为 FTP 访问用户名。

下列不属于电子邮件协议的是（40）。

(40)A. POP3　　B. SMTP　　C. SNMP　　D. IMAP4

【答案】C

【解析】本题考查常用的电子邮件有关协议的基础知识。

在 TCP/IP 协议簇中，包含了常用的电子邮件协议 SMTP、POP3、IMAP4,而 SNMP 是简单网络管理协议（Simple Network Management Protocol)。

下列安全协议中，与 TLS 功能相似的协议是（41)。

(41)A. PGP　　B. SSL　　C. HTTPS　　D. IPSec

【答案】B

【解析】本题考查安全协议方面的基础知识。

SSL（Secure Socket Layer,安全套接层）是 Netscape 于 1994 年开发的传输层安全协议，用于实现 Web 安全通信。1996 年发布的 SSL 3.0 协议草案已经成为一个事实上的 Web 安全标准。

TLS（Transport Layer Security,传输层安全协议）是 IETF 制定的协议，它建立在 SSL3.0 协议规范之上，是 SSL3.0 的后续版本。

用户 B 收到用户 A 带数字签名的消息 M,为了验证 M 的真实性,首先需要从 CA 获取用户 A 的数字证书，并利用（42）验证该证书的真伪，然后利用（43）验证 M 的真实性。

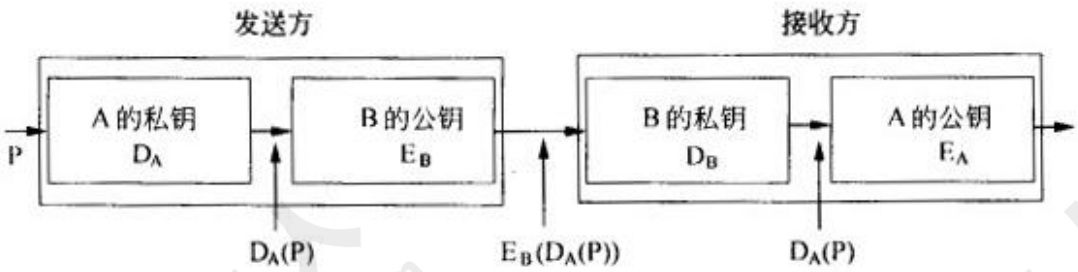
(42)A.CA 的公钥　　B.B 的私钥　　C.A 的公钥　　D.B 的公钥

(43)A.CA 的公钥　　B.B 的私钥　　C.A 的公钥　　D.B 的公钥

【答案】A　C

【解析】本题考查数字签名和数字证书方面的知识。

基于公钥的数字签名系统如下图所示：A 为了向 B 发送消息 P，A 用自己的私钥对 P 签名后再用 B 的公钥对签名后的数据加密,B 收到消息后先用 B 的私钥解密后在用 A 的公钥认证 A 的签名以及消息的真伪。



用户 B 收到用户 A 带数字签名的消息 M，为了验证 M 的真实性，首先需要从 CA 获取用户 A 的数字证书，验证证书的真伪需要用 CA 的公钥验证 CA 的签名，验证 M 的真实性需要用用户 A 的公钥验证用户 A 的签名。

3DES 是一种（44）算法。

(44)A.共享密钥　　B.公开密钥　　C.报文摘要　　D.访问控制

【答案】A

【解析】本题考查加密方面的基础知识。

3DES 是 DES 的改进算法，它使用两把密钥对报文作三次 DES 加密，效果相当于将 DES 密钥的长度加倍了，克服了 DES 密钥长度较短的缺点。

3DES 跟 DES一样，是一种共享密钥加密算法。

IPSec 中安全关联（Security Associations)三元组是（45)。

(45)A.<安全参数索引 SPI，目标 IP 地址，安全协议>

B.<安全参数索引 SPI，源 IP 地址，数字证书>

C.<安全参数索引 SPI,目标 IP 地址，数字证书>

D.<安全参数索引 SPI,源 IP 地址，安全协议>

【答案】A

【解析】本题考查 IPSec 方面的基础知识。

安全关联(Security Association,简称 SA)是 IPsec 的基础，是两个应用 IPsec 系统(主机、路由器)间的一个单向逻辑连接，是安全策略的具体化和实例化，它提供了保护通信的具体细节。一个 SA 由一个三元组唯一标识，该三元组是：一个安全参数索引（SPI)、一个 IP 目的地址和一个安全协议（AH 或 ESP)标识符。

在 SNMP 协议中，当代理收到一个 GET 请求时，如果有一个值不可或不能提供，则返回（46)。

(46)A.该实例的下个值　　B.该实例的上个值　　C.空值　　D.错误信息

【答案】A

【解析】本题考查 SNMP 协议中检索简单对象的相关基础知识。

在 SNMP 协议中检索简单对象时，当代理收到一个 GET 请求时：如果能检索到所有的对象实例，则返回请求的每个值；如果有一个值不可或者不能提供，则返回该实例的下一个值。

SNMP 网络管理中，一个代理可以由（47）管理站管理。

(47)A.0 个　　B.1 个　　C.2 个　　D.多个

【答案】D

【解析】本题考查 SNMP 协议体系架构中的相关基础知识。

SNMP 要求所有的代理设备和管理站都必须实现 TCP/IP 协议。对于不支持 TCP/IP 的设备不能直接用 SNMP 进行管理。为此提出了委托代理的概念。一个委托代理设备可以管理若

干台非 TCP/IP 设备，并代表这些设备接收管理站的查询，同时与某些管理站建立团体关系。

在 Windows 命令行下执行（48）命令出现下图的效果。

```
Tracing route to microsoft [157.54.1.196] over a maximum of 30 hops:
0  172.16.87.35
1  172.16.87.218
2  192.168.52.1
3  192.168.80.1
4  157.54.247.14
5  157.54.1.196

Computing statistics for 125 seconds...Source to Here   This
Node/Link

Hop   RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
0                                              172.16.87.35
                                 0/ 100 =  0%   |
1    41ms      0/ 100 =  0%      0/ 100 =  0%  172.16.87.218
                                13/ 100 = 13%   |
2    22ms     16/ 100 = 16%      3/ 100 =  3%  192.168.52.1
                                 0/ 100 =  0%   |
3    24ms     13/ 100 = 13%      0/ 100 =  0%  192.168.80.1
                                 0/ 100 =  0%   |
4    21ms     14/ 100 = 14%      1/ 100 =  1%  157.54.247.14
                                 0/ 100 =  0%   |
5    24ms     13/ 100 = 13%      0/ 100 =  0%  157.54.1.196

Trace complete.
```

(48)A. pathping -n Microsoft　　B. tracert -d microsoft

C. nslookup microsoft　　D. arp -a

【答案】A

【解析】本题考查网络管理命令的使用。

pathping 是一个基于 TCP/IP 的命令行工具，它可以反映出数据也从源主机到目标主机所经过的路径、网络延时以及丢包率，帮助我们解决网络问题。它使用 ICMP 回应信息来分析网络连通情况。pathping 发送回应信息到源地址与目标地址之间的所有路由器。

-n 参数可以阻止 pathping 试图将中间路由器的 IP 地址解析为各自的名称。这有可能加快 pathping 的结果显示。

tracert 是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。

nslookup 是一个用于查询 Internet 域名信息或诊断 DNS 服务器问题的工具。

arp 命令用来显示和修改 aip 缓存中的值。

在 Windows 系统中监听发送给 NT 主机的陷入报文的程序是（49）。

(49)A. snmp.exe　　B. mspaint.com　　C. notepad.exe　　D. snmptrap.exe

【答案】D

【解析】本题考查 Windows SNMP 服务的基本概念。

Windows NT 的 SNMP 的服务包括两个应用程序。一个是 SNMP 代理服务程序 snmp.exe,另一个是 SNMP 陷入服务程序 snmptrap.exe。snmp.exe 接收 SNMP 请求报文，根据要求发送响应报文，能对 SNMP 报文进行语法分析，ASN.1 和 BER 编码/译码，也能发送陷入报文，并处理 WinSockAPl 的接口。snmptrap.exe 监听发送给 NT 主机的陷入报文，然后把其中的数据传送给 SNMP 管理 API。

Windows Server 2003 中配置 SNMP 服务时,必须以（50)身份登录才能完成 SNMP 服务的配置功能。

(50)A.Guest　　B.普通用户　　C.Administrators 组成员　　D.Users 组成员

【答案】C

【解析】本题考查 Windows2003 中有关 SNMP 服务配置的操作权限。

Windows Server 2003 中配置 SNMP 服务时，必须以管理员身份或者 Administrators 组成员身份登录才能完成 SNMP 服务的配置功能。一般用户或者普通用户不能完成 SNMP 配置服务。

有一种 NAT 技术叫做“地址伪装”(Masquerading)，下面关于地址伪装的描述中正确的是（51)。

(51)A.把多个内部地址翻译成一个外部地址和多个端口号

B.把多个外部地址翻译成一个内部地址和一个端口号

C.把一个内部地址翻译成多个外部地址和多个端口号

D.把一个外部地址翻译成多个内部地址和一个端口号

【答案】A

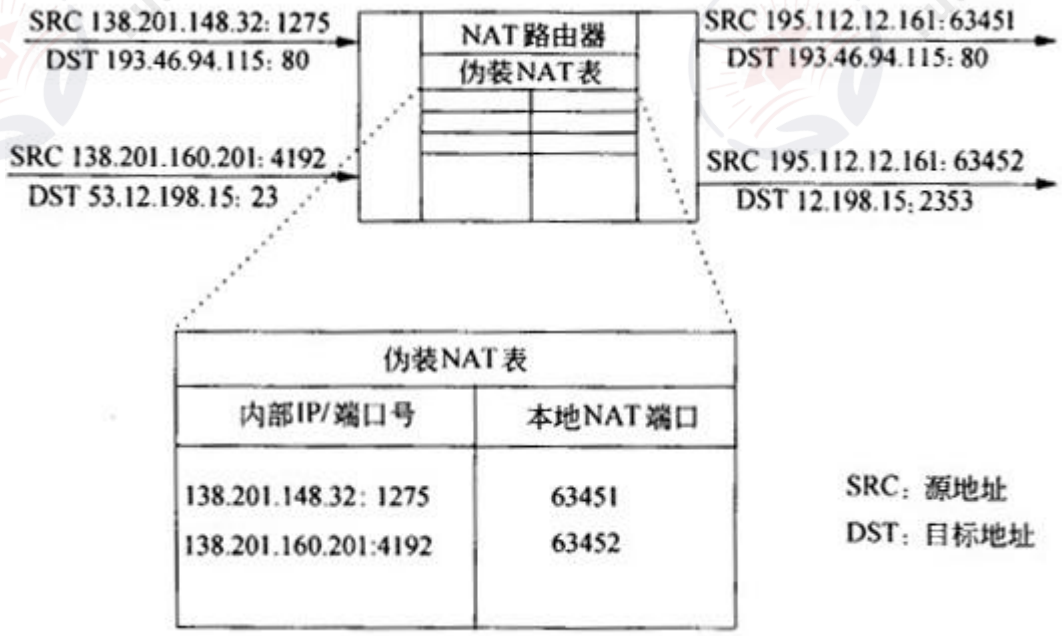
【解析】

有一种特殊的 NAT 应用是 m:1 翻译,即把 m 个内部地址翻译成 1 个外部地址和多个端口号。这种技术也叫做伪装（Masquerading)，因为用一个路由器的 IP 地址可以把 子网中所有主机的 IP 地址都隐蔽起来。如果子网中有多个主机同时都要通信，那么还要对接口号进行翻译，所以这种技术更经常被称为网络地址和端口翻译(Network Address Port Translation, NAPT)。在很多 NAPT 实现中专门保留一部分端口号给伪装使用，叫做伪装端口号。下图中的 NAT 路由器中有一个伪装表，通过这个表对端口号进行翻译，从而隐藏了内部网络 138.201.0.0 中的所有主机。可以看出，这种方法有如下特点：

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

•如果进来的分组的目标地址是本地路由器的 IP 地址，而目标端口号是路由器的伪装端口号，则 NAT 路由器就检查该分组是否为当前的一个伪装会话，并试图通过伪装表对 IP 地址和端口号进行翻译。

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



有一种特殊的 IP 地址叫做自动专用 IP 地址（APIPA），这种地址的用途是（52），以下地址中属于自动专用 IP 地址的是（53）。

(52)A. 指定给特殊的专用服务器　　B. 作为默认网关的访问地址

C. DHCP 服务器的专用地址　　D. 无法获得动态地址时作为临时的主机地址

(53)A. 224.0.0.1　　B. 127.0.0.1　　C. 169.254.1.15　　D. 192.168.0.1

【答案】D　　C

【解析】

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。IANA（Internet Assigned Numbers Authority）为 APIPA 保留了一个 B 类地址块 169.254.0.0～169.254.255.255。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。

把网络 10.1.0.0/16 进一步划分为子网 10.1.0.0/18,则原网络被划分为（54）个子网。

(54)A.2　　B.3　　C.4　　D.6

【答案】C

【解析】

把子网掩码增加两位，即把原来的网络划分成了 4 个子网。

IP 地址 202.117.17.255/22 是什么地址？ (55)。

(55)A.网络地址　　B.全局广播地址　　C.主机地址　　D.定向广播地址

【答案】C

【解析】

IP 地址 202.117.17.255/22 的二进制形式是 11001010.01110101.00010001.11111111，其中黑体部分是 22 位网络号，其余的主机地址部分是 01.11111111，可见这是一个主机地址。

对下面 4 条路由：202.115.129.0/24、202.115.130.0/24、202.115.132.0/24 和 202.115.133.0/24 进行路由汇聚，能覆盖这 4 条路由的地址是（56）。

(56)A.202.115.128.0/21　　B.202.115.128.0/22

C.202.115.130.0/22　　D.202.115.132.0/23

【答案】A

【解析】

地址 202.115.129.0/24 的二进制形式为：11001010 01110011 10000001 00000000。
地址 202.115.130.0/24 的二进制形式为：11001010 01110011 10000010 00000000。
地址 202.115.132.0/24 的二进制形式为：11001010 01110011 10000100 00000000。
地址 202.115.133.0/24 的二进制形式为：11001010 01110011 10000101 00000000。
地址 202.115.128.0/21 的二进制形式为：11001010 01110011 10000000 00000000。
所以能覆盖这 4 条路由的地址是 202.115.128.0/21。

可以用于表示地址块 220.17.0.0～220.17.7.0 的网络地址是（57），这个地址块中可以

分配（58）个主机地址。

(57)A. 220.17.0.0/20　　B. 220.17.0.0/21

C. 220.17.0.0/16　　D. 220.17.0.0/24

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

【答案】B　A

【解析】

8 个地址块的二进制形式是：

220.17.0.0　11011100.00010001.00000000.00000000

220.17.1.0　11011100.00010001.00000001.00000000

220.17.2.0　11011100.00010001.00000010.00000000

220.17.3.0　11011100.00010001.00000011.00000000

220.17.4.0　11011100.00010001.00000100.00000000

220.17.5.0　11011100.00010001.00000101.00000000

220.17.6.0　11011100.00010001.00000110.00000000

220.17.7.0　11011100.00010001.00000111.00000000

地址 220.17.0.0　11011100.00010001.00000000.00000000

可以覆盖这 8 个地址块，每个地址块可以分配 254 个主机地址，共可以分配 254×8=2032 个主机地址。

下面关于 IPv6 的描述中，最准确的是（59）。

(59)A. IPv6 可以允许全局 IP 地址重复使用　B. IPv6 解决了全局 IP 地址不足的问题

C. IPv6 的出现使得卫星联网得以实现　D. IPv6 的设计目标之一是支持光纤通信

【答案】B

【解析】

IPv6 解决了全局 IP 地址不足的问题，但是全局地址不能重复使用。IPv6 可以实现卫星联网，也支持光纤通信，但这些功能在 IPv4 中也是支持的。

下面哪个字段的信息出现在 TCP 头部而不出现在 UDP 头部？（60）。

(60)A. 目标端口号　　B. 顺序号　　C. 源端口号　　D. 校验和

【答案】B

【解析】

UDP 是无连接的协议，不需要用顺序号来进行流量和差错控制。UDP 和 TCP 都用端口号来提供向上的多路复用功能，校验和则用于检验协议头出现的差错。

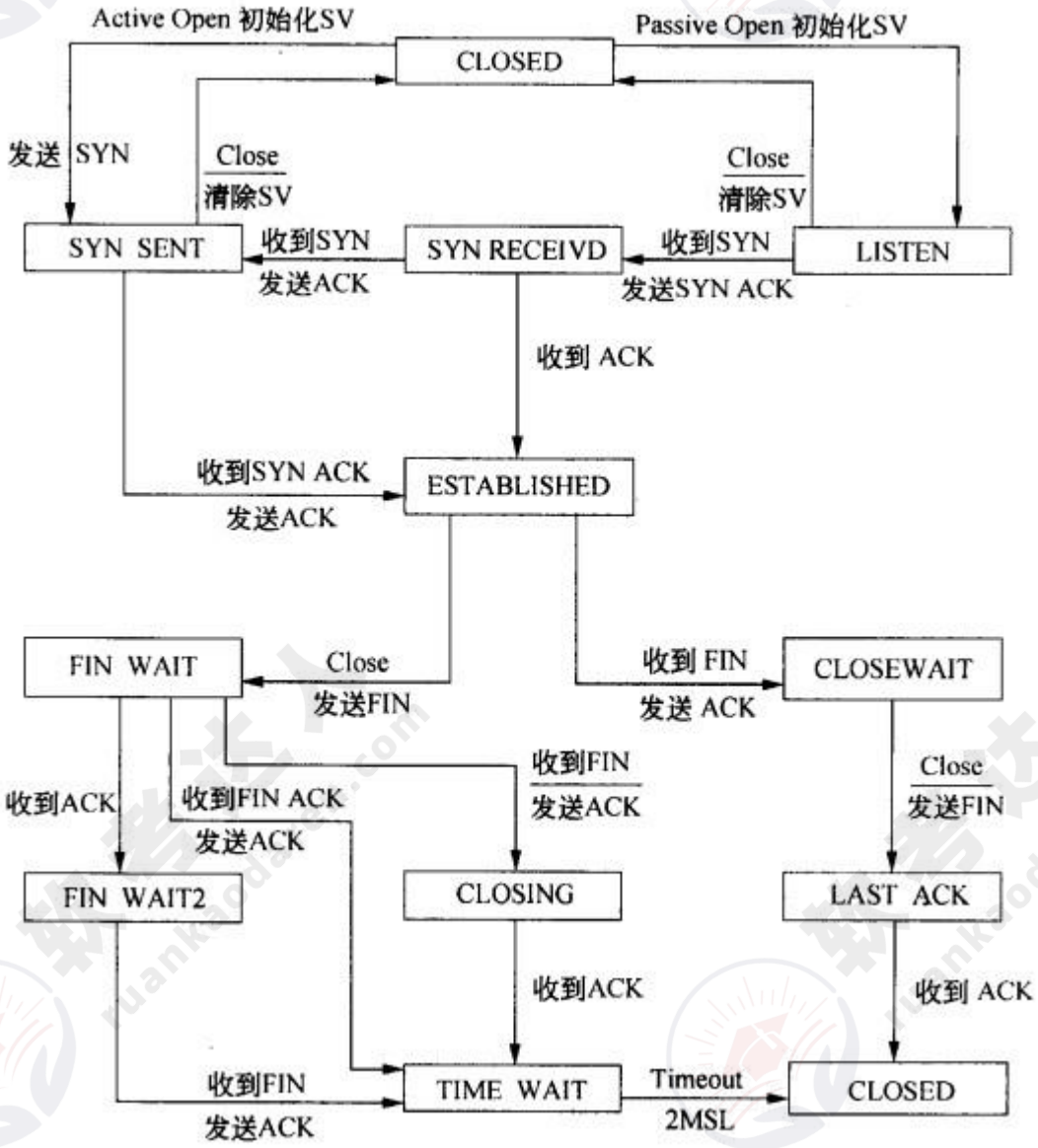
当一个 TCP 连接处于什么状态时等待应用程序关闭端口？(61)。

(61)A. CLOSED　　B. ESTABLISHED　　C. CLOSE-WAIT　　D. LAST-ACK

【答案】C

【解析】

TCP 建立和释放连接的过程采用三次握手协议。这种协议的实际目的是连接两端都 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。连接可能是主动建立的，也可能是被动建立的。在连接建立、存在和释放的各个阶段形成了不同的连接状态，表示在下图中，其中发送和应答的各种信号都是 TCP 段头中的标志。由图可以看出，TCP 连接处于 CLOSE WAIT 状态时等待应用程序关闭端口。



一个运行 CSMA/CD 协议的以太网，数据速率为 1Gb/s，网段长 1km，信号速率为 200,000km/sec,则最小帧长是（62）比特。

(62)A. 1000　　B. 2000　　C. 10000　　D. 200000

【答案】C

【解析】

网段长 1km，意味着最远两个结点之间的时延为 τ=5μs，则最小帧长=1Gb/s×2τ=10000 比特。

以太网帧结构中“填充”字段的作用是（63)。

(63)A. 承载任选的路由信息　　B. 用于捎带应答

C. 发送紧急数据　　D. 保持最小帧长

【答案】D

【解析】

以太网帧结构中“填充”字段的作用是保持最小帧长，便于检测冲突。如果满足了最小帧长的限制，则在最远的两个站之间出现的发送冲突都会在发送期间检测到。

关于无线网络中使用的扩频技术，下面描述中错误的是（64)。

(64)A. 用不同的频率传播信号扩大了通信的范围

B. 扩频通信减少了干扰并有利于通信保密

C. 每一个信号比特可以用 N 个码片比特来传输

D. 信号散布到更宽的频带上降低了信道阻塞的概率

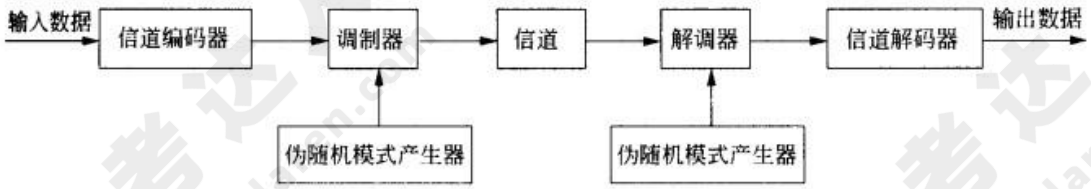
【答案】A

【解析】

扩展频谱通信技术起源于军事通信网络，其主要想法是将信号散布到更宽的带宽上以减少发生阻塞和干扰的机会。早期的扩频方式是频率跳动扩展频谱 (Frequency-Hopping Spread Spectrum, FHSS)，更新的版本是直接序列扩展频谱（Direct Sequence Spread Spectrum, DSSS)，这两种技术在 IEEE802.il 定义的 WLAN 中都有应用。

下图表示了各种扩展频谱通信系统的共同特点。输入数据首先进入信道编码器，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 seed)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，这就是被叫做伪随机序列的原因。重要的是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成功地对信号进行解码。

物联网中使用的无线传感网络技术是（65）。

(65)A.802.15.1 蓝牙个域网　　B.802.11n 无线局域网

C.802.15.4ZigBee 微微网　　D.802.16m 无线城域网

【答案】C

【解析】

IEEE802.15 工作组负责制定无线个人网（WPAN)的技术规范。这是一种小范围的无线通信系统，覆盖半径仅 10 米左右，可用来代替电脑、手机、PDA、数码相机等智能设备的通信电缆，或者构成无线传感器网络和智能家庭网络等。WPAN 并不是一种与无线局域网（WLAN)竞争的技术，WLAN 可替代有线局域网，而 WPAN 无须基础网络连接的支持，只能提供少量小型设备之间的低速率连接。

IEEE 802.15 工作组划分成四个任务组，分别制定适合不同应用环境的技术标准。802.15.1 采用了蓝牙技术规范，这是最早实现的面向低速率应用的 WPAN 标准，主要开发工作由蓝牙专业组（SIG)来做，其研究成果由 IEEE LAN/MAN 标准委员会颁布为正式标准。802.15.2 对蓝牙网络与 802.11b 网络之间的共存提出了建议。这两种网络都采用了免. 许可证的 2.4GHz 频段，它们之间会产生通信干扰，要在共享环境中协同工作，必须采用 802.15.2 提出的交替无线介质访问（AWMA)和分组通信仲裁（PTA)方案。

802.15.3 把目标瞄准了低复杂性、低价格、低功耗的消费类电子设备，为其提供至少 20Mb/s 的高速无线连接。2003 年 8 月批准的 IEEE 802.15.3 采用 64-QAM 调制，数据 速率高达 55 Mb/s，适合于短时间内传送大量的多媒体文件。在人手可及的范围内，多个电子设备可以组成一个

无线 Ad Hoc 网络，802.15 把这种网络叫做 piconet，通常翻译为微微网。802.15.3 给出的 piconet 网络模型的特点是，各个电子设备（DEV)可以独立地互相通信，其中一个设备可以作为通信控制的协调器 PNC,负责网络定时和向 DEV 发放令牌，获得令牌的 DEV 才可以发送通信请求。PNC 还具有管理 QoS 需求和调节电源功耗的功能。IEEE 802.15.3 定义了微微网的介质访问控制协议和物理层技术规范，适合于多媒体文件传输的需求。

与 802_15.3 相反，802.15.4 则瞄准了速率更低距离更近的无线个人网。802.15.4 标准适合于固定的、手持的、或移动的电子设备，这些设备的特点是使用电池供电，电池寿命可以长达几年时间，通信速率可以低至 9.6Kb/s，从而实现低成本的无线通信。802.15.4 标准的研发工作主要由 ZigBee 联盟来做。所谓 ZigBee 是指蜜蜂跳的“之”字形舞蹈，蜜蜂用跳舞来传递信息，告诉同伴蜜源的位置。“ZigBee”形象地表达了通过 M 络结点之间互相传递，将信息从一个结点传输到远处另外一个结点的通信方式。

正在发展的第四代无线通信技术推出了多个标准，下面的选项中不属于 4G 标准的是(66)。

(66)A.LTE　　B.WiMAXII　　C.WCDMA　　D.UMB

【答案】C

【解析】

候选的 4G 标准有 3 个：即 UMB (ultramobile broadband)、LTE (long-term evolution) 和 WiMAXII (IEEE 802.16m)。

超级移动宽带 UMB 是由高通公司为首的 3GPP2 组织推出的 CDMA-2000 的升级版。UMB 的最高下载速率可达到 288Mb/s,最高上传速率可达到 75Mb/s，支持的终端移动速率超过 300km/h。

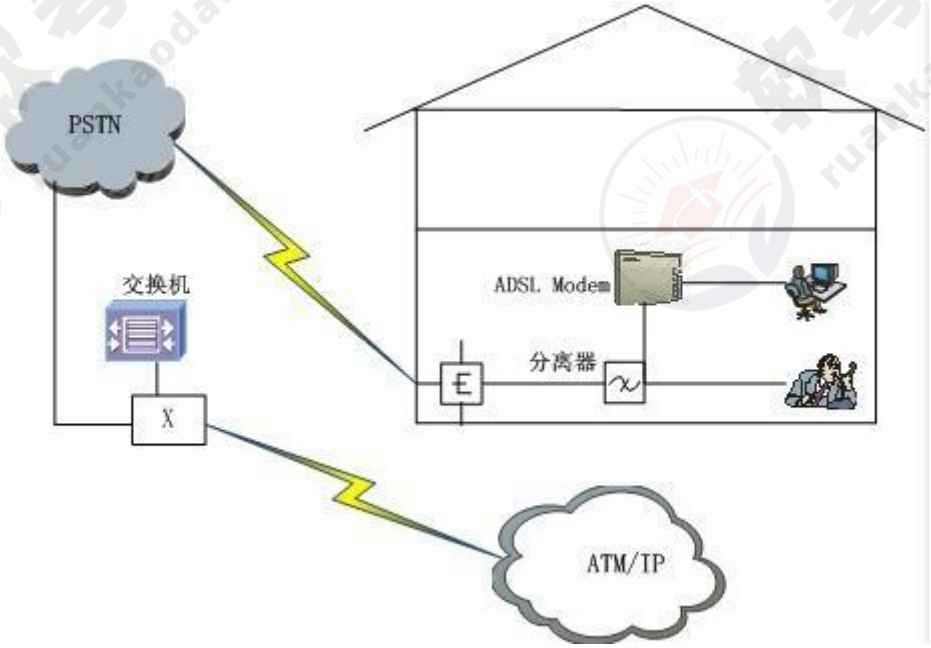
长期演进 LTE (Long Term Evolution)是沿着 GSM—W-CDMA4G 路线发展的技术，是由以欧洲电信为首的 3GPP 组织启动的新技术研发项目。同 UMB—样，LTE 也采用了 OFDM/OFDMA 作为物理层的核心技术。

2006 年 12 月批准的 802.16m 是向 IMT-Advanced 迈进的研究项目。为了达到 4G 的技术要求，IEEE802.16m 的下行峰值速率在低速移动、热点覆盖条件下可以达到 1Gb/s，在高速移动、广域覆盖条件下可以达到 100Mb/s。为了向前兼容，802.16m 准备对 802.16e 采用的 OFDMA 调制方式进行增补，进一步提高系统吞吐量和传输速率。

UMB、LTE 和移动 WiMAX 虽然各有差别，但是它们的共同之处是都采用 OFDM 和 MIMO 技

术来提供更高的频谱利用率。在未来的发展过程中，哪一种技术将会胜出，哪一种技术将会被淘汰，尚很难预料。

下面是家庭用户安装 ADSL 宽带网络时的拓扑结构图，图中左下角的 X 是(67)设备，为了建立虚拟拨号线路，在用户终端上应安装（68)协议。



(67)A. DSLAM　　B. HUB　　C. ADSL Modem　　D. IP Router

(68)A. ARP　　B. HTTP　　C. PPTP　　D. PPPoE

【答案】A　　D

【解析】

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

ADSL 需要的接入设备包括局端接入设备 DSLAM 和用户端设备 ATU-R，以及用户线路和管理服务器。DSLAM 作为 ADSL 的局端收发设备由运营商提供，实现用户接入和集中复用功能，

同时提供不对称的流量控制机制。用户端设备 ATU-R 就是 ADSL Modem，可以实现 POTS 语音与数据的分离，完成用户端 ADSL 数据的接收和发送。ADSL 采用双绞线作为传输介质，无需对现有的用户线路进行改造就可直接使用。管理服务器主要是宽带接入服务器（BRAS），能够提供 ADSL 用户接入的终结、认证、计费、管理等基本业务，此外还可以提供防火墙、安全控制、NAT 转换、带宽管理、流量控制等网络业务管理功能。ADSL 采用的调制技术有 3 种：

•QAM (Quadrature Amplitude Modulation)

•CAP (Carrierless Amplitude-Phase modulation)

•DMT (Discrete Multitone)

离散多音(DMT)调制技术的传输质量较佳，被广泛采用。DMT 在铜质电话线上将从直流到 1MHz 的频带划分成 256 个子信道，每个子信道带宽 4.3kHz。频率最低的信道（0～4.3KHZ)用来传输模拟电话信号，其余频带在低频部分传输上行信号，高频部分传输下行信号。ADSL Modem 独立地分析每个信道的信噪比，以确定该信道可适用的数据速率。当某一信道的信噪比恶化时，Modem 自动降低该信道的数据速率，以保证传输的正确性。如果一个信道的信噪比极其恶化，甚至可能将其关闭。上、下行信号的分割有两种办法：频率分割法（FDM)和回波抵消法（EC)，现在市场上的 ADSL 产品绝大多数采用频分法。

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

网络系统设计过程中，物理网络设计阶段的任务是（69）。

(69)A.依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境

B.分析现有网络和新网络的各类资源分布，掌握网络的状态

C.根据需求规范和通信规范，实施资源分配和安全规划

D.理解网络应该具有的功能和性能，最终设计出符合用户需求的网络

【答案】A

【解析】

物理网络是逻辑网络的具体实现，通过对设备的具体物理分布、运行环境等的确定来确

保网络的物理连接符合逻辑设计的要求。在这一阶段，网络设计者需要确定具体的软硬件、连接设备、布线和服务的部署方案。

下列关于网络核心层的描述中，正确的是（70）。

(70)A.为了保障安全性，应该对分组进行尽可能多的处理

B.将数据分组从一个区域高速地转发到另一个区域

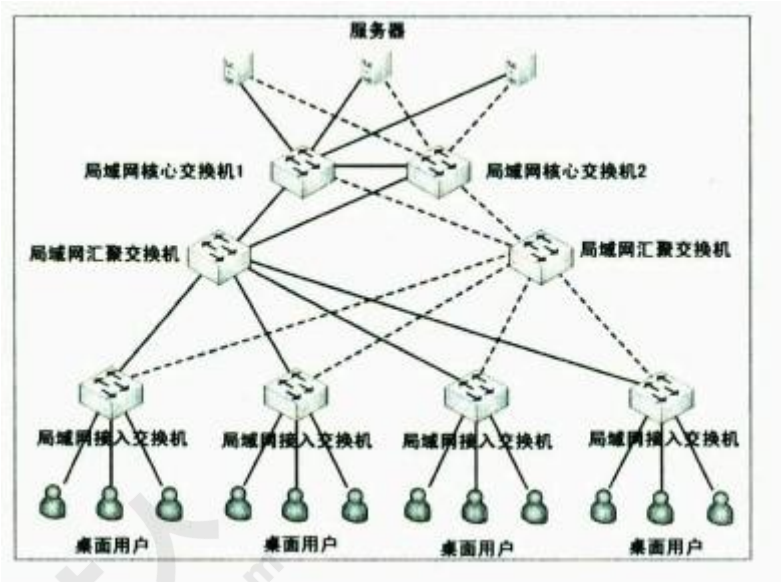
C.由多台二、三层交换机组成

D.提供多条路径来缓解通信瓶颈

【答案】B

【解析】

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



层次结构的特点如下：

•网络功能划分清晰，有利发挥联网设备的最大效率；

•网络拓扑结构使得故障定位可分级进行，便于维护；

•便于网络拓扑的后续扩展。

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

核心层是互连网络的高速主干网，在设计中应增加冗余组件，使其具备高可靠性，能快速适应通信流量的变化。

在设计核心层设备的功能时应避免使用数据包过滤、策略路由等降低转发速率的功能特性，使得核心层具有高速率、低延迟和良好的可管理性。

核心层设备覆盖的地理范围不宜过大，连接的设备不宜过多，否则会使得网络的复杂度增大，导致网络性能降低。

核心层应包括一条或多条连接外部网络的专用链路，使得可以高效地访问互联网。

汇聚层是核心层与接入层之间的分界点，应实现资源访问控制和流量控制等功能。汇聚层应该对核心层隐藏接入层的详细信息，不管划分了多少个子网，汇聚层向核心路由器发布路由通告时，只通告各个子网汇聚后的超网地址。

如果局域网中运行了以太网和弹性分组环等不同类型的子网，或者运行了不同路由算法的区域网络，可以通过汇聚层设备完成路由汇总和协议转换功能。

接入层提供网络接入服务，并解决本地网段内用户之间互相访问的需求，要提供足够的带宽，使得本地用户之间可以高速访问；

接入层还应提供一部分管理功能，例如 MAC 地址认证、用户认证、计费管理等；

接入层要负责收集用户信息（例如用户 IP 地址、MAC 地址、访问日志等），作为计费和排错的依据。

Let us now see how randomization is done when a collision occurs. After a （71）, time is divided into discrete slots whose length is equal to the worst-case round-trip propagation time on the ether(2τ). To accommodate the longest path allowed by Ethernet, the slot time has been set to 512 bit times, or 51.2μsec.

After the first collision, each station waits either 0 or 1 （72）times before trying again. If two stations collide and each one picks the same random number, they will collide again. After the second collision, each one picks either 0, 1, 2, or 3 at random and waits that number of slot times. If a third collision occurs (the probability of this happening is 0.25), then the next time the number of slots to wait is chosen at （73） from the interval 0 to 2^3-1.

In general, after i collisions, a random number between 0 and 2^i-1 is chosen, and that number of slots is skippeD. However, after ten collisions have been reached, the randomization （74）is frozen at a maximum of 1023 slots. After 16 collisions, the controller throws in the towel and reports failure back to the computer. Further recovery is up to （75） layers.

(71)A. datagram	B. collision	C. connection	D. service
(72)A. slot	B. switch	C. process	D. fire
(73)A. rest	B. ramdom	C. once	D. odds
(74)A. unicast	B. multicast	C. broadcast	D. interval

(75)A. local　　B. next　　C. higher　　D. lower

【答案】B　A　B　D　C

【解析】

现在让我们看看当冲突发生时，随机性操作是如何体现的。出现冲突时，时间被划分为离散的时槽，其长度等于最坏情况下以太网的周转传播时间（2t），为了适应以太网中的最长通路，时槽被设为 512 比特的发送时间，即 51.2 微秒。

第一次冲突后，每个站在再次试图发送前等待 0 或 1 个时槽。如果两个站出现了冲突，并且每个站都选用了同样的随机数，那么就会再一次发生冲突。第二次发生冲突后，每个站随机地选取数字 0、1、2 或者 3,并等待相应的时槽数如果发生了第三次冲突（这种情况出现的概率为 0.25），则下一次等待的时槽数目就随机地在 0～23-1 中选取。

一般情况下，第 i 次冲突后，随机数在 0 到 2i-1 之间选取，相应的时槽数被跳过。然而，达到 10 次冲突后，随机数被固定在最大 1023 个时槽之内。16 次冲突后，控制器放弃发送，向计算机发出故障报告。进一步的恢复措施由上层协议实施。

试题一

某学校有三个校区，校区之间最远距离达到 61km，学校现在需要建设校园网，具体要求如下：校园网通过多运营商接入互联网，主干网采用千兆以太网将三个校区的中心节点连起来，每个中心节点都有财务、人事和教务三类应用。按应用将全网划分为 3 个 VLAN，三个中心都必须支持 3 个 VLAN 的数据转发。路由器用光纤连到校区 1 的中心节点上，距离不超过 500 米，网络结构如图 1-1 所示。

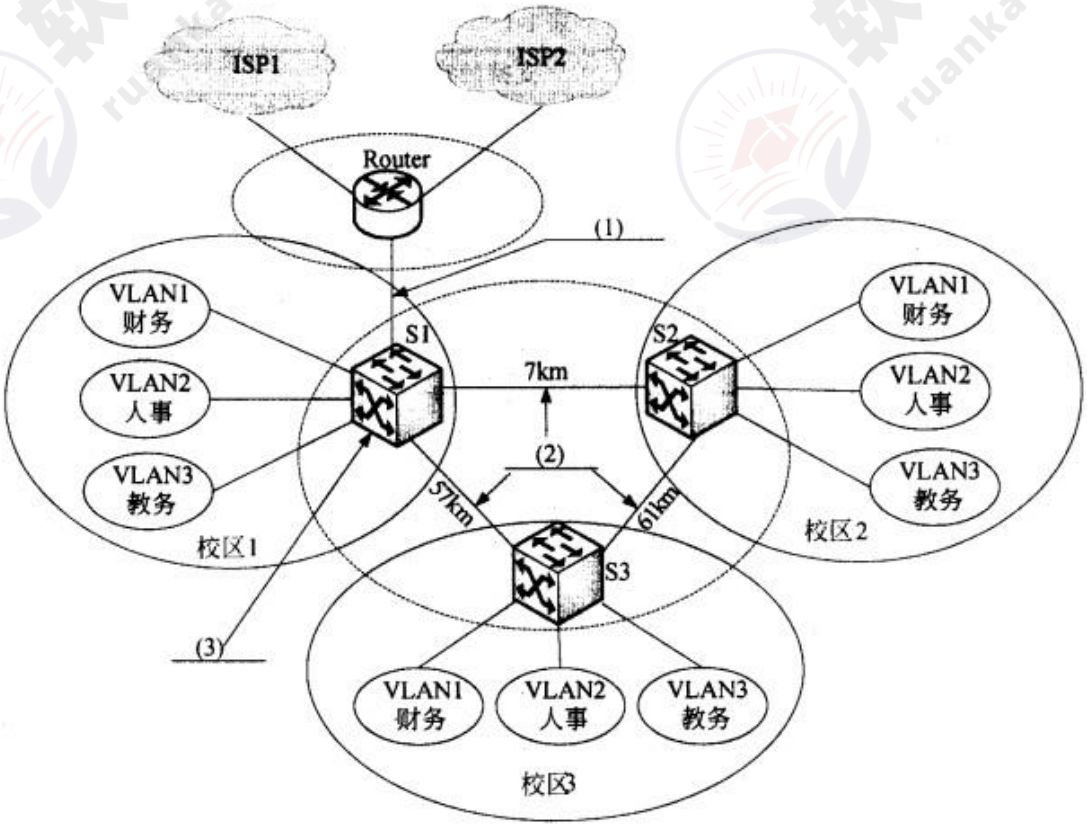


图 1-1

【问题 1】

根据题意和图 1-1，从经济性和实用性出发填写网络拓扑图中所用的传输介质和设备。

空（1)～（3)备选答案：

A. 3 类 UTP

B. 5 类 UTP

C. 6 类 UTP

D. 单模光纤

E. 多模光纤

F.千兆以太网交换机

G.百兆以太网交换机

H.万兆以太网交换机

(1) E (2) D (3) F

本问题考查网络传输介质以及网络设备的选用知识。根据网络的需求和拓扑图，传输介质 1 连接出口路由器和网络中心节点交换机，两台设备之间距离不超过 500 米,且网络要求用光纤连接，又因为题目要求经济性，所以应该采用多模光纤。传输介质 2 连接三个校区的中心交换机，三个中心之间距离最小 7km，所以应该采用单模光纤。网络设备 3 连接出口路由器和其他两个校区的节点交换机，网络要求主干网采用千兆以太网，本着经济性并满足要求的目的，应该采用千兆以太网交换机。

【问题 2】

如果校园网中办公室用户没有移动办公的需求，采用基于（4)的 VLAN 划分方法比较合理；如果有的用户需要移动办公，采用基于 （5）的 VLAN 划分方法比较合适。

(4)交换机端口

(5) MAC 地址

本问题考查交换机 VLAN 划分知识。

VLAN 的划分方法有基于端口划分、基于 MAC 地址划分等。

基于端口的 VLAN，简单的讲就是交换机的一个端口就是一个虚拟局域网，凡是连接在这个端口上的主机属于同个虚拟局域网之中。基于端口的 VLAN 的优点为：由于一个端口就是一个独立的局域网。所以，当数据在网络中传输的时候，交换机就不会把数据包转发给其他的端口，如果用户需要将数据发送到其他的虚拟局域网中，就需要先由交换机发往路由器再由路由器发往其他端口；同时以端口为中心的 VLAN 中完全由用户自由支配端口，无形之中就更利于管理。但是以端口为中心的 VLAN，当用户位置改变时，往往也伴随着用户位置的改变而对网线也要进行迁移。如果不会经常移动客户机的话，可以采用这种方式。从目前来看，这种根据端口来划分 VLAN 的方式仍然是最常用的一种方式。

基于 MAC 地址划分 VLAN 的方法。这种划分 VLAN 的方法是根据每个主机的 MAC 地址来划分，

即对每个 MAC 地址的主机都配置它属于哪个组。这种划分 VLAN 方法的最大优点就是当用户物理位置移动时，即从一个交换机换到其他的交换机时，VLAN 不用重新配置，所以，可以认为这种根据 MAC 地址的划分方法是基于用户的 VLAN，这种方法的缺点是初始化时，所有的用户都必须进行配置，如果有几百个甚至上千个用户的话，配置是非常累的。而且这种划分的方法也导致了交换机执行效率的降低，因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员，这样就无法限制广播包了。

根据需求描述，没有移动办公需求的可考虑采用基于端口的 VLAN 划分方法；有移动办公需求的可考虑采用基于 MAC 的 VLAN 划分方法。

【问题 3】

图 1-1 中所示的交换机和路由器之间互连的端口类型全部为标准的 GBIC 端口，表 1-1 列出了互联所用的光模块的参数指标，请根据组网需求从表 1-1 中选择合适的光模块类型满足合理的建网成本，Router 和 S1 之间用（6)互联，S1 和 S2 之间用（7)互联，S1 和 S3 之间（8)用互联，S2 和 S3 之间用（9)互联。

表 1-1

光模块类型	支持的参数指标			
	标　准	波　长	光纤类型	备　注
模块 1	1000BaseSX	850nm	62.5/125μm 50/125μm	多模，价格便宜
模块 2	1000BaseLX/1000BaseLH	1310nm	62.5/125μm 50/125μm 9/125μm	单模，价格稍高
模块 3	1000BaseZX	1550nm	9/125μm	单模，价格昂贵

(6)模块 1

(7)模块 2

(8)模块 3

(9)模块 3

本问题考查网络设备配置的光模块的相关知识。

根据网络拓扑和题目需求描述可知，考虑建网成本和实际联网网络介质可知选择满足需求的光纤模块即可。Router 和 S1 之间传输介质为多模光纤，因此采用多模光模块。S1 和 S2 之间距离 7km，采用波长为 1310nm 的可传输 10km 的单模光模块即可。S1 和 S3 以及 S2 和 S3 之间距离大于 50KM，只能采用波长为 1550xmi 的远距离传输的单模光模块。

【问题 4】

如果将 Router 和 S1 之间互连的模块与 S1 和 S2 之间的模块互换，Router 和 S1 以及 S1 和 S2 之间的网络是否能否联通？并请解释原因。

Router 与 S1 通，S1 与 S2 不通，因为模块 2 的传输介质兼容多模光纤，模块 1 的传输介质不兼容单模光纤。

本问题考查实际组网工程中光模块的使用知识。

因为波长为 1310nm 的光波可以在 62.5/125um、50/125um 以及 9/125um 的传输介质中传输，也就是说可以在多模光纤中传输，因此 Router 与 S1 之间仍然可以通信；但是波长为 850nm 的光波不能在 9/125|jm 的单模光纤中传输，因此 S1 与 S2 之间不能通信。

【问题 5】

若 VLAN3 的网络用户因为业务需要只允许从 ISP1 出口访问 Internet，在路由器上需进行基于（10)的策略路由配置。其他 VLAN 用户访问 Internet 资源时，若访问的是 ISP1 上的网络资源，则从 ISP1 出口；若访问的是其他网络资源，则从 ISP2 出口，那么在路由器上需进行基于（11)的策略路由配置。

(10)源地址

(11)目的地址

本问题考查路由器有关策略路由的相关配置知识。

传统的路由只能根据目的地址进行报文转发，策略路由相对来说就比较灵活了，可以根据源地址、目的地址、协议类型、报文大小等进行路由转发。在进行路由转发的时候，路由器根据已经设定的策略对数据包进行匹配，如果匹配到一条策略，就用该策略进行转发，如果没有匹配到，就根据路由表中的路由进行转发。策略路由主要应用在路由表复杂或者需要对路由进行控制的情况下，特别是当网络出口有两条及以上，需要对不同服务和应用或者不同客户端的路由进行控制时。对于网络用户访问网络资源时的不同需求，如一部分用户仅需访问某个 ISP，可考虑根据源地址进行路由转发；另一部分用户的网络访问根据目的 IP 有所不同时可考虑采用基于目的地址的策略路由。

试题二

某公司搭建了一个小型局域网，网络中配置一台 Linux 服务器作为公司内部文件服务器和 Internet 接入服务器，该网络结构如图 2-1 所示。

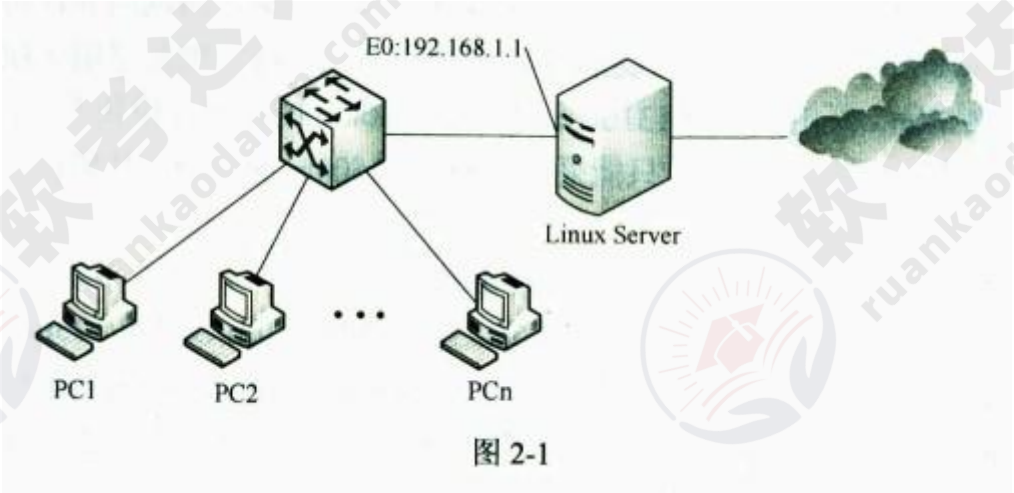


图 2-1

【问题 1】

Linux 的文件传输服务是通过 vsftpd 提供的，该服务使用的应用层协议是（1)协议，传输层协议是（2）协议，默认的传输层端口号为（3）。

vsftpd 服务可以通过命令行启动或停止，启动该服务的命令是(4)，停止该服务的命令是(5)。

(1) FTP

(2) TCP

(3) 21

(4) service vsftpd start

(5) service vsftpd stop

Linux 的文件传输服务是通过 vsftpd 提供的，该服务使用的应用层协议是文件传输协议（FTP)，文件传输协议 FTP 采用的传输层协议是有连接的、可靠的 TCP 协议，FTP 协议默认的传输层端口号为 21，FTP 服务默认值该端口上提供服务。

Linux 中的所有服务都可以通过 service 命令从命令行启动或停止，命令的格式是：service 服务程序名称 start/stop。

vsftpd 服务可以通过命令行启动或停止，启动该服务的命令是 service vsftpd start，停止该服务的命令是 service vsftpd stop。

【问题 2】

vsftpd 程序主配置文件的文件名是 （6）。若当前配置内容如下所示，请给出对应配置项和配置值的含义。

```
...
listen_address=192.168.1.1
#listen_port=21
#max_per_ip=10
#max_clients=1000
anonymous_enable=YES          （7）
local_enable=YES              （8）
write_enable=YES              （9）
userlist_enable=YES           （10）
...
```

(6) vsftpd.conf

(7) 允许匿名用户访问

(8) 允许本地用户访问

(9) 允许用户上传文件

(10) 禁止用户列表文件中的用户访问

vsftpd 程序主配置文件的文件名是 vsftpd.conf，该文件缺省安装于/etc/vsflpd 目录中。该配置文件中所有参数的配置形式均为“参数=值”的方式，关键字对大小写敏感，以“#”开始的是注释行，注释行在执行时被忽略。

vsftpdxonf 配置文件中的配置项非常多，下面仅对题目中出现的配置项做出解释， 其余配置项和相关含义请参看联机手册。

listen_address=192.168.1.1
指定服务监听的 IP 地址，如果没有该配置项则默认//监听本机的所有 IP 地址
listen_port=21
指定服务监听的端口号，默认值是 21
max_per_ip=10
指定每一给定 IP 地址的客户端的最大连接数
max_clients=1000
指定服务器可以同时提供服务的客户端数量
anonymous_enable=YES
允许匿名用户登录
local_enable=YES
允许 Linux 系统中的本地用户登录
write_enable=YES
允许用户上传文件
userlist_enable=YES

userlist 文件有效，此时默认禁止 userlist 文件中的用户登录，如果要允许 userlist 文件中的用户登录，需要增加另一配置项 userlist_deny=NO。

【问题 3】

为了使因特网上的用户也可以访问 vsftpd 提供的文件传输服务，可以通过简单的修改上述主配置文件实现，修改的方法是（11）。

(11) 注释或删除 “listen—address= 192.168.1.1” 配置项

因为配置文件 vsftpdxonf 中有配置项 listen_address=192.168.1.1,即 FTP 服务仅仅在内网所在地址上监听，因特网上的用户无法访问，为了使因特网上的用户也可以访问 vsftpd 提供的文件传输服务，只需注释该配置项即可。

【问题 4】

由于 Linux 服务器的配置较低，希望限制同时使用 FTP 服务的并发用户数为 10,每个用户使用 FTP 服务时可以建立的连接数为 5,可以通过简单的修改上述主配置文件实现，修改的方法是 （12）。

(12) 改“ #max_per—ip=10’’ 为“ max_per_ip=5 ”，改“ #max—clients=1000 ”为“ max_clients= 10”

试题三

某单位网络拓扑结构如图 3-1，该单位 Router 以太网接口 E0 接内部交换机 S1，S0 接口连接到电信 ISP 的路由器；交换机 S1 连接内部的 WEB 服务器、DHCP 服务器、DNS 服务器和部分客户机，服务器均安装 Windows Server 2003,办公室的代理服务器（Windows XP 系统）安装了两块网卡，分别连接交换机 S1、S2,交换机 S1、S2 的端口均在 VLAN1 中。

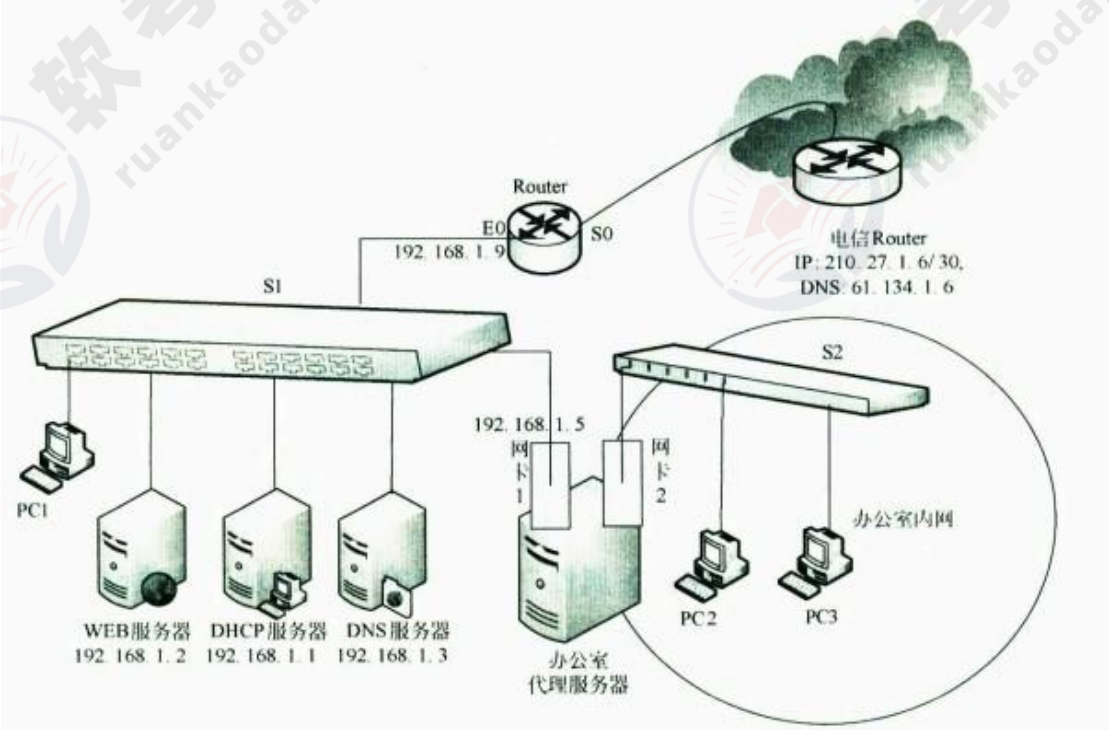


图 3-1

【问题 1】

根据图 3-1，该单位 Router S0 接口的 IP 地址应设置为（1）：在 S0 接口与电信 ISP 路由器接口构成的子网中，广播地址为（2）。

考查 IP 地址根据子网掩码的配置分配，根据 ip 信息 210.27.1.6/30,可知：该子网的子网掩码是 255.255.255.252,该子网是 210.27.1.4,广播地址为 210.27.1.7,因为 210.27.1.6 已用，故 Router S0 接口的 IP 地址只能设置为 210.27.1.5。

所以(1)的正确答案 210.27.1.5，(2)的正确答案 210.27.1.7。

【问题 2】

办公室代理服务器的网卡 1 为静态地址，在网卡 1 上启用 Windows XP 内置的“Internet

连接共享”功能，实现办公室内网的共享代理服务；那么通过该共享功能自动分配给网卡 2 的 IP 地址是（3）。

根据图上的设计，通过网卡 2 实现办公室内网的共享代理服务，在 Windows XP 内置的“Internet 连接共享”功能中，自动分配给代理网卡网卡 2 的 IP 地址是 192.168.0.1。

【问题 3】

在 DHCP 服务的安装过程中，租约期限一般默认为(4)天。

在 Windows 2003 Server 的网络组件 DHCP 服务的安装过程中，按照操作系统的设置，租约期限一般默认为 8 天。

【问题 4】

该单位路由器 Router 的 E0 口设置为 192.168.1.9/24,若在 DHCP 服务器上配置、启动、激活 DHCP 服务后，查看 DHCP 地址池的结果如图 3-2 所示。

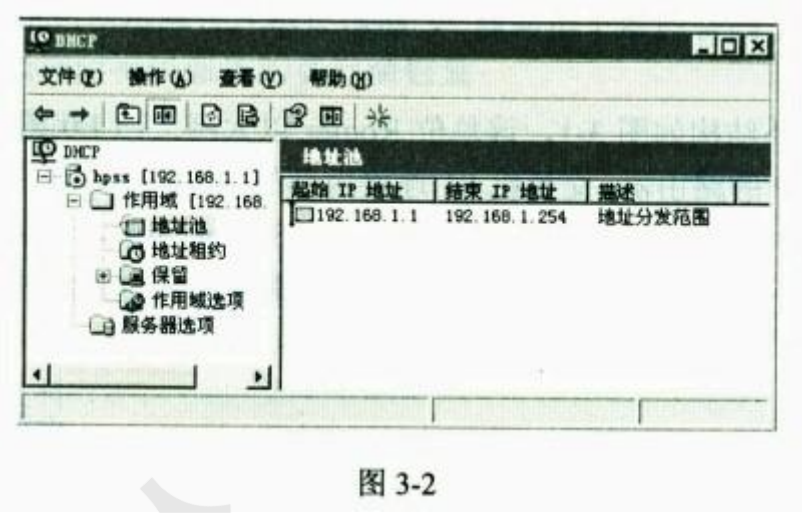


图 3-2

为了满足图 3-1 的功能，在 DHCP 服务器地址池配置操作中还应该增加什么操作？

进行“添加排除” IP 地址的操作

该题考查 DHCP 服务器的配置，结合图 3-1 和图 3-2,可看到图 3-2 中 DHCP 的 IP 地址池范围设置了 192.168.1.1 到 254,但是在该子网中，已经把 192.168.1.1、192.168.1.2、192.168.1.3、192.168.1.5、192.168.1.9 静态分配给了其他设备，所以还要进行“添加排除 IP 地址的操作”，要把上述 5 个已用了的 IP 排除掉。

【问题 5】

假如在图 3-1 中移除 DHCP 服务器，改由单位 Router 来提供 DHCP 服务，在 Router 上配置 DHCP 服务时用到了如下命令，请在下划线处将命令行补充完整。

```
Router(config)# ip__（5）__ hkhk  //配置 DHCP 地址池名为 hkhk
Router(dhcp-config)#__（6）__ 192.168.1.0  255.255.255.0
Router(dhcp-config)#__（7）__192.168.1.9
```

(5) dhcp pool

(6) network

(7) default-router

该题考查对路由器 DHCP 功能的配置操作，CISCO 路由器的配置命令序列如下：

```
Router(config)# ip__dhcp pool__ hkhk
Router(dhcp-config)#__network__ 192.168.1.0  255.255.255.0
Router(dhcp-config)#__default-router__ 192.168.1.9
```

【问题 6】

在网站的属性窗口中，若“QQQ 属性”选项卡的“IP 地址”选项设置为“全部未分配”，如图 3-3 所示，则说明 （8） 。

空（8)备选答案：

A. 网站的 IP 地址为 192.168.1.1，可以正常访问

B. 网站的 IP 地址为 192.168.1.2，可以正常访问

C.网站的 IP 地址未分配，无法正常访问

图 3-3

在图 3-4 的 WEB 服务主目录选项卡上，至少要设置对主目录的（9)权限,才能访问该 WEB 服务器。

空（9)备选答案：

A.读取 B.写入 C.目录浏览 D.记录访问

图 3-4

(8) B

(9) A

该题空（8)考查对 WEB 网站服务器配置的操作，如图 3-3 所示，“IP 地址”选项中的“(全部未分配)”的意思是对配置过 WEB 服务的任何地址都可以 WEB 访问，结合图 3-1，知道 WEB 服务器的 IP 是 192.168.1.2，所以该题（8)的答案是“网站的 IP 地 址为 192.168.1.2，可以正常访问”。

该题(9)考查对 WEB 服务器配置中权限有关的设置，要设置对 WEB 主目录的“读取”权限’才能正常访问该 WEB 服务器。

【问题 7】

按系统默认的方式配置了 KZ 和 QQQ 两个网站（如图 3-5 所示），此时两个网站均处于停止状态，若要使这两个网站能同时工作，请给出三种可行的解决办法。

方法一：（10）；

方法二：（11）；

方法三：（12）。

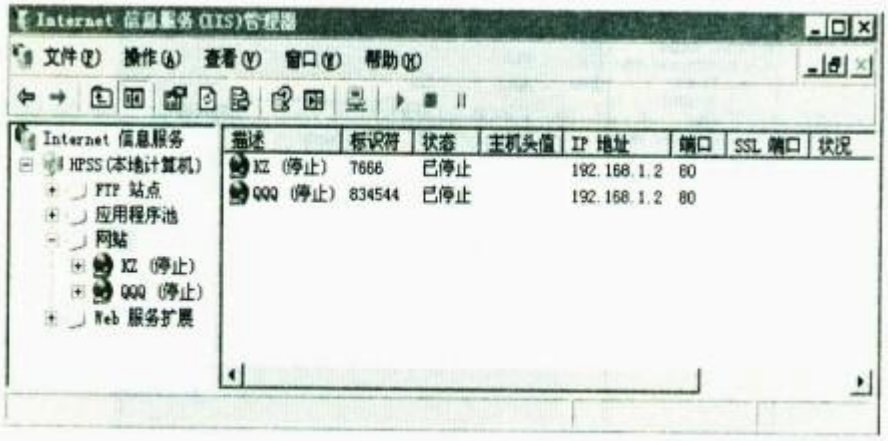


图 3-5

(10)给 KZ 和 QQQ 指定不同的 IP 地址

(11) 给 KZ 和 QQQ 指定不同的主机头值

(12)给 KZ 和 QQQ 指定不同的端口号

(10) ~ (12)位置可互换

该题考查对 WEB 网站服务器配置操作时，当在一台服务器上配置多个 WEB 服务时，应该怎么避免冲突。常用的方法是：

方法一：给 KZ 和 QQQ 两个服务器指定不同的地址；

方法二：给 KZ 和 QQQ 两个服务器指定不同的主机头值；

方法三：给 KZ 和 QQQ 两个服务器指定不同的端口号。

试题四

某单位网络结构如图 4-1 所示，其中维护部通过 DDN 专线远程与总部互通。

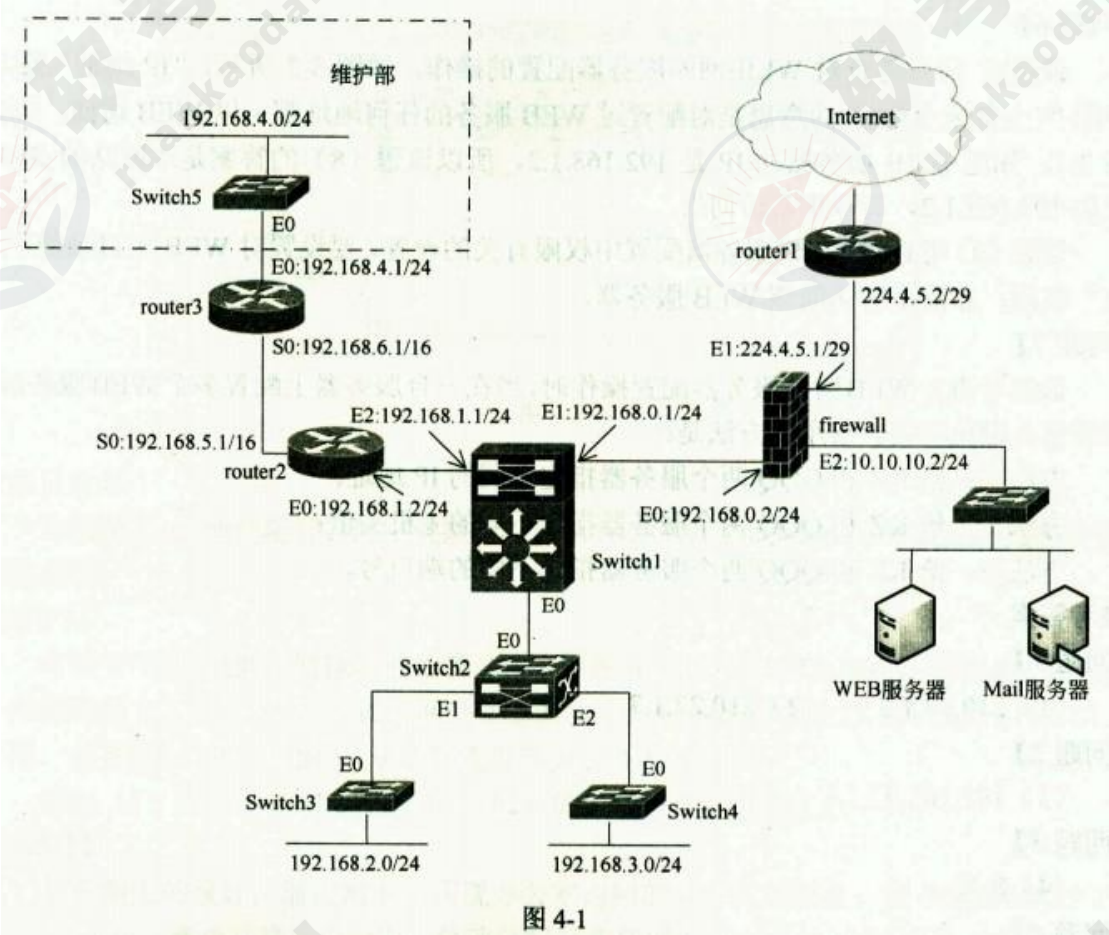


图 4-1

【问题 1】

核心交换机 Switch1 的部分配置如下，请根据说明和网络拓扑图完成下列配置。

```
……
Switch1(config)#interface vlan 1
Switch1(config-if)#ip address 192.168.0.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 2
Switch1(config-if)#ip address 192.168.1.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 3
Switch1(config-if)#ip address 192.168.2.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 4
Switch1(config-if)#ip address 192.168.3.1 255.255.255.0
Switch1(config-if)#no shutdown
……
Switch1(config-router)#ip route 0.0.0.0 0.0.0.0 ____(1)____
Switch1(config)#ip route ____(2)____ 255.255.255.0 ____(3)____
```

(1) 192.168.0.2

(2) 192.168.4.0

(3) 192.168.1.2

本题考查三层交换机路由的配置。根据题目说明和拓扑图可知，核心交换机的默认路由应该指向防火墙 E0 口，但是由于 DDN 通讯的要求，192.168.4.0 网段地址的路由应指向 route2 的 E0 口，所以交换机 Switch1 配置如下：

```
……
Switch1(config)#interface vlan 1
Switch1(config-if)#ip address 192.168.0.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 2
Switch1(config-if)#ip address 192.168.1.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 3
Switch1(config-if)#ip address 192.168.2.1 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config)#interface vlan 4
Switch1(config-if)#ip address 192.168.3.1 255.255.255.0
Switch1(config-if)#no shutdown
……
Switch1(config-router)#ip route 0.0.0.0 0.0.0.0 192.168.0.2
Switch1(config)#ip route 192.168.4.0 255.255.255.0 192.168.1.2
……
```

【问题 2】

根据网络拓扑和需求说明，完成汇聚交换机 Switch2 的部分配置。

```
Switch2(config)#interface fastEthernet 0/0
Switch2(config-if)#switchport mode ___(4)___
Switch2(config-if)#no shutdown

Switch2(config)#interface fastEthernet 0/1
Switch2(config-if)#switchport mode ___(5)___
Switch2(config-if)#switchport access ___(6)___
Switch2(config-if)#no shutdown
…
```

(4) trunk

(5) access

(6) vlan3

本题考查交换机 vlan 的配置方法。根据题目说明和拓扑结构图，Switch2 的 E0 口上行连接核心交换机，所以该接口为 trunk 口，Switch2 的 E1 口连接 Switch3 的 E0 口，而 Switch3

的网段为 192.169.2.0,根据问题 1 可知，其 vlan 号为 vlan3,所以 Switch2 的配置如下：

```
Switch2(config)#interface fastEthernet 0/0
Switch2(config-if)#switchport mode trunk
Switch2(config-if)#no shutdown

Switch2(config)#interface fastEthernet 0/1
Switch2(config-if)#switchport mode access
Switch2(config-if)#switchport access vlan3
Switch2(config-if)#no shutdown
…
```

【问题 3】

根据网络拓扑和需求说明，完成（或解释）路由器 router2 的部分配置。

```
……
R2(config-if) # interface ethernet0
R2(config-if) # ip address ___(7)___ ___(8)___
R2(config-if) # no shutdown
R2(config-if) # interface Serial0
R2(config-if) # ip address ___(9)___ ___(10)___
R21(config-if) # no shutdown
…
R2(config) # ip route 0.0.0.0 0.0.0.0 ___(11)___
R2(config) # ip route ___(12)___ 255.255.255.0 ___(13)___
R2(config) # snmp-server community publicr ro          //___(14)___
R2(config) # snmp-server community publicw rw          //___(15)___
……
```

(7) 192.168.1.2

(8) 255.255.255.0

(9) 192.168.5.1

(10) 255.255.0.0

(11) 192.168.1.1

(12) 192.168.4.0

(13) 192.168.6.1

(14) 设置 snmp-server 的只读团体名为 publicr

(15) 设置 snmp-server 的读写团体名为 publicw

本题考查路由器的配置。根据题目说明和拓扑图可知 R2 的各个接口地址，R2 的默认路由应该指向核心交换机 E2 口，但是由于 DDN 通讯的要求，192.168.4.0 网段地址的路由应指向 route3 的 s0 口，所以路由器 R2 配置如下：

```
R2(config-if) # interface ethernet0
R2(config-if) # ip address 192.168.1.2 255.255.255.0
R2(config-if) # no shutdown
R2(config-if) # interface Serial0
R2(config-if) # ip address 192.168.5.1 255.255.0.0
R21(config-if) # no shutdown
…
R2(config) # ip route 0.0.0.0 0.0.0.0 192.168.1.1
R2(config) # ip route 192.168.4.0 255.255.255.0 192.168.6.1
R2(config) # snmp-server community publicr ro     //设置 snmp-server 的只读团体名为 publicr
R2(config) # snmp-server community publicw rw    //设置 snmp-server 的读写团体名为 publicw
```

【问题 4】

按照图 4-1 所示，设置防火墙各接口 IP 地址，并根据配置说明，完成下面的命令。

```
PIX(config)#interface ethernet0 auto
PIX(config)#interface ethernet1 100full
PIX(config)#interface ethernet2 100full
PIX(config)#ip address outside  (16)   (17)        //设置外网接口 IP
PIX(config)#ip address inside 192.168.0.2 255.255.255.0 //设置内网接口 IP
PIX(config)#ip address dmz  (18)  255.255.255.0     //设置 DMZ 接口 IP
PIX(config)#global (outside) 1 224.4.5.1-224.4.5.6  //指定公网地址范围，定义地址池
PIX(config)#  (19)                                  //表示内网的所有主机都可以访问外网
PIX(config)#route outside 0 0  (20)          //设置默认路由
```

(16) 224.4.5.1

(17) 255.255.255.248

(18) 10.10.10.2

(19) nat (inside) 1 0 0 或 nat (inside) 1 0.0.0.0 0.0.0.0

(20) 224.4.5.2

本题考查防火墙的配置方法。根据题目说明和拓扑结构图可知防火墙各接口 ip 地址，其默认路由应指向 route1 的接口，所以防火墙的配置如下：

```
PIX(config)#interface ethernet0 auto
PIX(config)#interface ethernet1 100full
PIX(config)#interface ethernet2 100full
PIX(config)#ip address outside 224.4.5.1 255.255.255.248    //设置外网接口IP
PIX(config)#ip address inside 192.168.0.2 255.255.255.0     //设置内网接口IP
PIX(config)#ip address dmz 10.10.10.2 255.255.255.0     //设置DMZ接口IP
PIX(config)#global (outside) 1 224.4.5.1-224.4.5.6 //指定公网地址范围，定义地址池
PIX(config)# nat (inside) 1 0.0.0.0  0.0.0.0         //表示内网的所有主机都可以访问外网
PIX(config)#route outside 0 0 224.4.5.2          //设置默认路由
```