常用的虚拟存储器由（1）两级存储器组成。

(1)A.主存－辅存　　B.主存-网盘　　C.Cache-主存　　D.Cache-硬盘

【答案】A

【解析】本题考查计算机系统存储系统基础知识。

在具有层次结构存储器的计算机中，虚拟存储器是为用户提供一个比主存储器大得多的可随机访问的地址空间的技术。虚拟存储技术使辅助存储器和主存储器密切配合，对用户来说，好像计算机具有一个容量比实际主存大得多的主存可供使用，因此称为虚拟存储器。虚拟存储器的地址称为虚地址或逻辑地址。

中断向量可提供（2）。

(2)A.I/O 设备的端口地址　　B.所传送数据的起始地址

C.中断服务程序的入口地址　　D.主程序的断点地址

【答案】C

【解析】本题考查计算机系统基础知识。

计算机在执行程序过程中，当遇到急需处理的事件时，暂停当前正在运行的程序，转去执行有关服务程序，处理完后自动返回原程序，这个过程称为中断。中断是一种非常重要的技术，输入输出设备和主机交换数据、分时操作、实时系统、计算机网络和分布式计算机系统中都要用到这种技术。为了提高响应中断的速度，通常把所有中断服务程序的入口地址（或称为中断向量）汇集为中断向量表。

为了便于实现多级中断，使用（3）来保护断点和现场最有效。

(3)A.ROM　　B.中断向量表　　C.通用寄存器　　D.堆栈

【答案】D

【解析】本题考查计算机系统基础知识。

当系统中有多个中断请求时，中断系统按优先级进行排队。若在处理低级中断过程中又有高级中断申请中断，则高级中断可以打断低级中断处理，转去处理高级中断，等处理完高级中断后再返回去处理原来的低级中断，称为中断嵌套。实现中断嵌套用后进先出的栈来保护断点和现场最有效。

DMA 工作方式下，在（4）之间建立了直接的数据通路。

(4)A.CPU 与外设　　B.CPU 与主存　　C.主存与外设　　D.外设与外设

【答案】C

【解析】本题考查计算机系统基础知识。

计算机系统中主机与外设间的输入输出控制方式有多种，在 DMA 方式下，输入输出设备与内存储器直接相连，数据传送由 DMA 控制器而不是主机 CPU 控制。CPU 除了传送开始和终了时进行必要的处理外，不参与数据传送的过程。

地址编号从 80000H 到 BFFFFH 且按字节编址的内存容量为（5）KB,若用 16KX4bit 的存储芯片够成该内存，共需（6）片。

(5)A.128　　B.256　　C.512　　D.1024

(6)A.8　　B.16　　C.32　　D.64

【答案】B　C

【解析】本题考查计算机系统基础知识。

从 80000H 到 BFFFFH 的编址单元共 3FFFF（即 218)个，按字节编址的话，对应的容量为 28KB, HP 256KB，若用 16KX4bit 的芯片构成该内存，构成一个 16KB 存储器需要 2 片，256+16=16,共需要 32 片。

王某是一名软件设计师，按公司规定编写软件文档，并上交公司存档。这些软件文档属于职务作品，且（7）。

(7)A.其著作权由公司享有

B.其著作权由软件设计师享有

C.除其署名权以外，著作权的其他权利由软件设计师享有

D.其著作权由公司和软件设计师共同享有

【答案】A

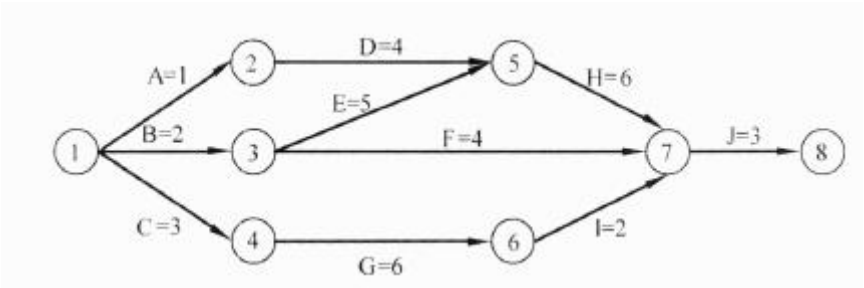
【解析】本题考查知识产权知识。

公民为完成法人或者其他组织工作任务所创作的作品是职务作品。职务作品可以是作品分类中的任何一种形式，如文字作品、电影作品、计算机软件等。职务作品的著作权归属分两种情形：

一般职务作品的著作权由作者享有。所谓一般职务作品是指虽是为完成工作任务而为，但非经法人或其他组织主持，不代表其意志创作，也不由其承担责任的职务作品。对于一般

职务作品，法人或其他组织享有在其业务范围内优先使用的权利，期限为两年。优先使用权是专有的，未经单位同意，作者不得许可第三人以与法人或其他组织使用的相同方式使用该作品。在作品完成两年内，如单位在其业务范围内不使用，作者可以要求单位同意由第三人以与法人或其他组织使用的相同方式使用，所获报酬，由作者与单位按约定的比例分配。特殊的职务作品，除署名权以外，著作权的其他权利由法人或者其他组织（单位） 享有。所谓特殊职务作品是指著作权法第 16 条第 2 款规定的两种情况：一是主要利用法人或者其他组织的物质技术条件创作，并由法人或者其他组织承担责任的工程设计、产品设计图、计算机软件、地图等科学技术作品；二是法律、法规规定或合同约定著作权由单位享有的职务作品。

在进行进度安排时，PERT 图不能清晰地描述（8），但可以给出哪些任务完成后才能开始另一些任务，某项目 X 包含 A、B.....J，其 PERT 如下图所示（A=1 表示任务 A 的持续时间是 1 天），则项目 X 的关键路径是（9）。



(8)A.每个任务从何时开始　　B.每个任务到何时结束

C.各任务之间的并行情况　　D.各任务之间的依赖关系

(9)A.A-D-H-J　　B.B-E-H-J　　C.B-F-J　　D.C-G-I-J

【答案】C　B

【解析】本题考查项目管理及工具技术。

PERT 图可以清晰地表示各任务的开始时间和结束时间以及各任务之间的依赖关系，但是无法很好地表示各任务之间的并行情况。

根据关键路径法，计算出题图中的关键路径为 B-E-H-J，关键路径长度为 16。

假设某分时系统采用简单时间片轮转法，当系统中的用户数为 n,时间片为 q 时，系统对每个用户的响应时间 T=（10）。

(10)A.n　　B.q　　C.nXq　　D.n+q

【答案】C

【解析】

在分时系统中是将把 CPU 的时间分成很短的时间片轮流地分配给各个终端用户，当系统中的用户数为 n、时间片为 q 时，那么系统对每个用户的响应时间等于 nXq。

各种联网设备的功能不同，路由器的主要功能是（11）。

(11)A.根据路由表进行分组转发　　B.负责网络访问层的安全

C.分配 VLAN 成员　　D.扩大局域网覆盖范围

【答案】A

【解析】

网络互连设备可以根据它们工作的协议层进行分类；中继器工作于物理层；网桥和交换机工作于数据链路层；路由器工作于网络层；而网关则工作于网络层以上的协议层。

路由器根据分组中“目标网络”字段在路由表中选择匹配项，以便把分组转发到目标网络中去。通过路由器连接的局域网分属不同的子网，通过路由器互联扩大了网络的覆盖范围，但不是扩大了局域网的覆盖范围。通过在路由器中设置过滤规则可以提供网络层安全访问功能，但这不是路由器最基本、最主要的功能。而配置 VLAN 属于交换机的基本功能。

假设模拟信号的频率范围为 3~9MHz，采样频率必须大于（12）时，才能使得到的样本信号不失真。

(12)A.6MHz　　B.12MHz　　C.18MHz　　D.20MHz

【答案】C

【解析】

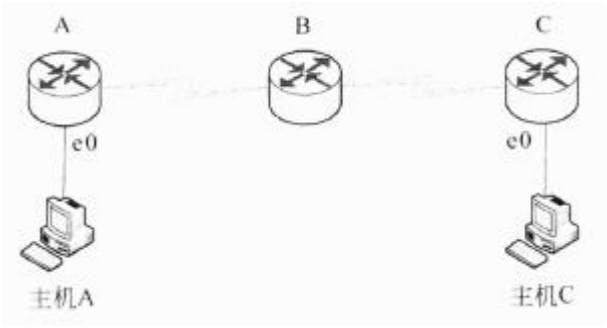
根据脉冲编码调制方案，采样的频率决定了恢复的模拟信号的质量。尼奎斯特采样定理说明，为了恢复原来的模拟信号，采样频率必须大于模拟信号最高频率的二倍，即

$$f=\frac{1}{T}\geqslant 2f_{\max}$$

其中 f 为采样频率，T 为采样周期，fmax 为信号的最高频率。本题中信号最高频率为 9MHz，所以采样频率必须大于 18MHz。

如下图所示，若路由器 C 的 e0 端口状态为 down,则当主机 A 向主机 C 发送数据时，路

由器 C 发送（13）。



(13)A.ICMP 回声请求报文　　B.ICMP 参数问题报文

C.ICMP 目标不可到达报文　　D.ICMP 源抑制报文

【答案】C

【解析】

ICMP (Internet control Message Protocol)属于网络层协议，主要用于传送有关通信故障方面的消息，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 报文有许多种，封装在 IP 数据报中传送。常见的 ICMP 报文的含义如下。

•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。

•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。

•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。

•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。

•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。

•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。

•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。

•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。

当一个主机要获取通信目标的 MAC 地址时，(14).

(14)A.单播 ARP 请求到默认网关　　B.广播发送 ARP 请求

C.与对方主机建立 TCP 连接　　D.转发 IP 数据报到邻居结点

【答案】B

【解析】

在 Internet 中用地址分解协议（Address Resolution Protocol, ARP)来实现逻辑地址到物理地址映像，通常这种地址是与网络硬件相关的。

图　ARP/RARP 分组格式

由于有两种主机地址，因而需要一种映像关系把这两种地址对应起来。ARP 分组的格式如上图所示。

通常 Internet 应用程序把要发送的报文交给 IP 协议，IP 层实体当然知道接收方的逻辑地址，但不一定知道接收方的物理地址。在把 IP 分组向下传送给本地数据链路层实体之前可

以用两种方法得到目标物理地址：

①查本地内存中的ARP地址映像表，这是本地主机已知的IP地址和MAC地址的对照表，可以由IP地址查找对应的MAC地址。

②如果ARP表查不到，就广播一个ARP请求分组，这种分组可以到达同一子网中的所有主机和路由器。它的含义是：“如果你的IP地址是这个分组中的目标结点协议地址，请回答你的物理地址是什么”。

③收到该分组的主机一方面可以用分组中的两个源地址更新自己的ARP地址映像表，一方面用自己的IP地址与目标结点协议地址字段比较，若相符则发回一个ARP响应分组，向发送方报告自己的MAC地址，若不相符则不予回答。

④如果路由器知道所询问的主机的IP地址，则代表主机回答由以上询问，并把自己的MAC地址告诉发送方，后续源和目标之间的通信都是通过路由器从中转发。

路由器出厂时，默认的串口封装协议是(15)。

(15)A.HDLC　　B.WAP　　C.MPLS　　D.L2TP

【答案】A

【解析】

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

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

• AUI端口：这种端口采用D型15针连接器，用在令牌环网或总线型以太网中。 路由器经AUI端口通过粗同轴电缆收发器连接10Base-5网络，也可以通过外接的AUI-to-RJ-45适配器连接10Base-T以太网。

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

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

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

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

• AUX 端口：对路由器进行远程配置时要使用“AUX”端口（Auxiliary Prot)。AUX 端口在外观上与 RJ-45 端口一样，只是内部电路不同，实现的功能也不一样。通过 AUX 端口与 Modem 进行连接必须借助 RJ-45 to DB9 或 RJ-45 to DB25 适配器进行转换。AUX 端口支持硬件流控。

在异步通信中，每个字符包含 1 位起始位，7 位数据位，1 位奇偶位和 2 位终止位，每秒传送 100 个字符，则有效数据速率为（16）。

(16)A.100b/s　　B.500b/s　　C.700b/s　　D.1000b/s

【答案】C

【解析】

异步通信方案是把字符作为同步的单位，字符之间插入少量的同步信息。面向字符的同步协议依赖于具体的字符编码，不同字符编码的系统之间不能通信。按照本题意说明，每秒传送 100 个字符，每个字符中的有效信息占 7/11，所以有效数据速率为 11X100X7/11= 700b/S。

下列选项中，不采用虚电路通信的网络是(17)网。

(17)A.X.25　　B.帧中继　　C.ATM　　D.IP

【答案】D

【解析】

X.25 网络是早期的公用数据网，在网络层通过虚电路提供面向连接的服务。帧中继是对 X.25 网络的改进，在数据链路层建立虚电路连接，同时也简化了差错控制功能，以适应高速光纤通信的需要。ATM 是为综合业务数字网开发的传输技术，在网络层建立虚电路连接，以 53 字节的信元为传输的单位。以上三种网络都是电信部门开发的网络通信技术，继承了早期电话网络面向连接的通信模式。IP 协议是在因特网中使用的网络层协议，当初设计时为了适应军事通信的需要，采用了无连接的通信方案。在 IP 网络中，每个数据报都是独立传送的，所有的协议数据单元到达目标后需要进行纠错和重新排序，才能提交给上层实体。

在网络层采用分层编址方案的好处是(18)。

(18)A.减少了路由表的长度　　B.自动协商数据速率

C.更有效地使用 MAC 地址　　D.可以采用更复杂的路由选择算法

【答案】A

【解析】

在网络层采用分层的编址方案可以把网络分成大小不等的多级网络，即大网络中包含小网络。不同层级的网络路由器提供的路由信息的繁简程度不同。这样，上一级网络路由器的路由表就可以得到简化，只有子网内部的路由器才指向具体的目标主机。

在交换网络中，VTP 协议作用是什么？(19)。

(19)A.选举根网桥　　B.将 VLAN 信息传播到整个网络

C.建立端到端连接　　D.选择最佳路由

【答案】B

【解析】

VLAN 中继协议（VLAN Trunking Protocol，VTP)是 Cisco 公司的专利协议。VTP 在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文可以传播到管理域中的所有交换机。

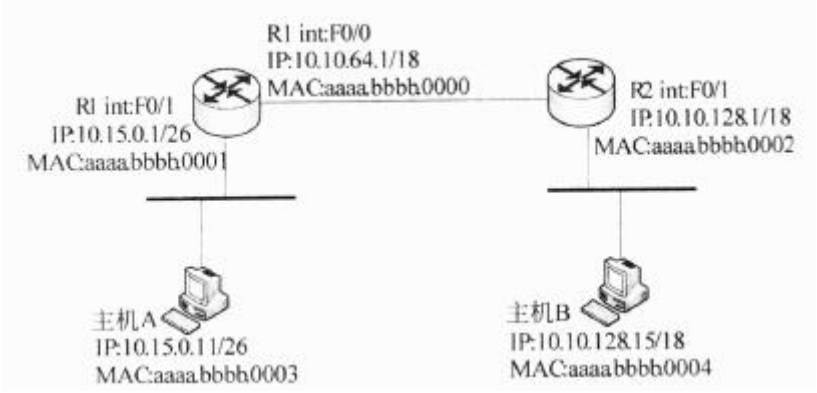
按照 VTP 协议，交换机的运行模式分为 3 种：

①服务器模式（Server)：交换机在此模式下能创建、添加、删除和修改 VLAN 配置，并从中继端口发出 VTP 组播帧，把配置信息分发到整个管理域中的所有交换机。一个管理域中可以有多个服务器。

②客户机模式（Client)：在此模式下不允许创建、修改或删除 VLAN,但可以监听本管理域中其他交换机的 VTP 组播信息，并据此修改自己的 VLAN 配置。

③透明模式（Transparent)：在此模式下可以进行 VLAN 配置，但配置信息不会传播到其他交换机。在透明模式下，可以接收和转发 VTP 巾贞，但是并不能据此更新自己的 VLAN 配置，只是起到通路的作用。

参见下图，主机 A ping 主机 B，当数据帧到达主机 B 时，其中包含的源 MAC 地址和源 IP 地址是(20)。



(20)A. aaaa. bbbb. 0003 和 10. 15. 0. 11　　B. aaaa. bbbb. 0002 和 10. 10. 128. 1

C. aaaa. bbbb. 0002 和 10. 15. 0. 11　　D. aaaa. bbbb. 0000 和 10. 10. 64. 1

【答案】C

【解析】

主机 A 发出的 ping 报文经过路由器 R1 和 R2 转发，到达主机 B 时，根据 ARP 协议代理机制，其中包含的源 MAC 地址是 R2 的 MAC 地址——aaaa. bbbb. 0002。当然，源 IP 地址还是主机 A 的 IP 地址 10. 15. 0. 11。

下面描述中，不属于链路状态协议特点的是(21)。

(21)A. 提供了整个网络的拓扑视图　　B. 计算到达的各个目标最短通路

C. 邻居之间互相交换路由表　　D. 具有事件触发的路由更新功能

【答案】C

【解析】

执行链路状态路由协议的路由器只保留自己知道的部分网络的拓扑信息，但是所有路由器保存的路由信息的总和则可以提供整个网络的拓扑结构视图。各个链路状态路由器根据自己的路由表计算到达目标的最短通路。链路状态路由协议在网络拓扑结构改变时触发路由更新功能。执行链路状态协议的路由器通过 Hello 协议来发现邻居，并在其邻居中选择需要交换链路状态信息的路由器，与之建立毗邻关系（Adjacency)。并不是每一对邻居都需要交换路由信息，因而也不是每一对邻居都要建立毗邻关系。在一个广播网络或 NBMA 网络中要选举一个指定路由器（Designated Router, DR),其他的路由器都与 DR 建立毗邻关系，把自己掌握的链路状态信息提交给 DR，由 DR 代表这个网络向外界发布。

关于网桥和交换机，下面的描述中正确的是(22)。

(22)A.网桥端口数少，因此比交换机转发更快

B.网桥转发广播帧，而交接机不转发广播帧

C.交换机是一种多端口网桥

D.交换机端口多，因此扩大了冲突域大小

【答案】C

【解析】

网桥和交换机都是第二层转发设备，即都是根据数据链路层地址转发（包括广播）数据包。二者的区别是网桥的端口数较少，一般是用主机插入多个网卡来连接多个子网，并通过软件来实现分组过滤功能。而交换机通常是采用专门的硬件实现，端口数较多。由于采用了专用硬件，因此交换机转发速度更快。无论网桥或交换机，一个端口就是一个冲突域。

使用路由器对局域网进行分段的好处是(23)。

(23)A.广播帧不会通过路由进行转发　　B.通过路由器转发减少了通信延迟

C.路由器的价格便宜，比使用交换机更经济　D.可以开发新的应用

【答案】A

【解析】

路由器是第三层设备，它不转发第二层广播帧。所以使用路由器对局域网进行分段的好处是可以隔离第二层广播风暴，减少了冲突域的范围。

OSPF 网络可以划分为多个区域（area），下面关于区域的描述中错误的是(24)。

(24)A.区域可以被赋予 0~65535 中的任何编号

B.单域 OSPF 网络必须配置成区域 1

C.区域 0 被称为主干网

D.分层的 OSPF 网络必须划分为多个区域

【答案】B

【解析】

OSPF 网络可以划分为多个区域（area),每个 OSPF 区域被指定了一个 32 位的区域标识符，可以用点分十进制表示，例如主干区域的标识符可表示为 0.0.0.0。单域 OSPF 网络就是只有主干区域的网络（配置成区域 0)。分层的 OSPF 网络必须划分为多个区域。OSPF 的区域分为以下 5 种，不同类型的区域对由自治系统外部传入的路由信息的处理方式不同：

•标准区域：可以接收任何链路更新信息和路由汇总信息。

.主干区域：是连接各个区域的传输网络，其他区域都通过主干区域交换路由信息。主干区域拥有标准区域的所有性质。

•存根区域：不接收本地自治系统以外的路由信息，对自治系统以外的目标采用默认路由0.0.0.0。

•完全存根区域：不接收自治系统以外的路由信息，也不接收自治系统内其他另域的路由汇总信息，发送到本地区域外的报文使用默认路由0.0.0.0。完全存根区域是Cisco定义的，是非标准的。

•不完全存根区域（NSSA):类似于存根区域，但是允许接收以类型7的链路状态公告发送的外部路由信息。

与RIPv1相比，RIPv2的改进是(25)。

(25)A.采用了可变长子网掩码　　B.使用SPF算法计算最短路由

C.广播发布路由更新信息　　D.采用了更复杂的路由度量算法

【答案】A

【解析】

RIP分为两个版本。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。RIP以跳步计数（hop count)来度量路由费用，显然这不是最好的度量标准。例如，若有两条到达同一目标的连接，一条是经过两跳的10MB以太网连接，另一条是经过一跳的64KBWAN连接，则RIP会选取WAN连接作为最佳路由。在RIP协议中，15跳是最大跳数，16跳是不可到达网络，经过16跳的任何分组将被路由器丢弃。

RIPv1是有类别的协议，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。

RIPv2是增强了的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。

把网络 117.15.32.0/23 划分为 117.15.32.0/27，则得到的子网是多少个？(26) 每个子网中可使用的主机地址是多少个？(27)。

(26)A.4　　B.8　　C.16　　D.32

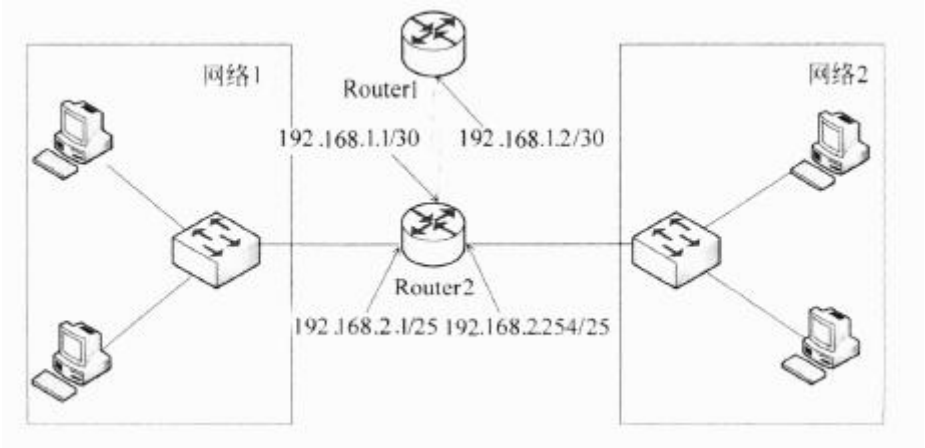
(27)A.30　　B.31　　C.32　　D.34

【答案】C　A

【解析】

把网络 117.15.32.0/23 划分为 117.15.32.0/27，则子网掩码扩大了 4 位，所以得到的子网是 16 个。由于子网掩码为 27 位，所以主机地址只占 5 位，每个子网中可使用的主机地址是 30 个。

网络配置如下图所示，为路由器 Router1 配置访问网络 1 和网络 2 的命令是(28)。路由配置完成后，在 Router1 的(29)可以查看路由，查看路由采用的命令是(30)。



(28)A.ip route 192.168.2.0 255.255.255.0192.168.1.1

B.ip route 192.168.2.0255.255.255.128192.168.1.2

C. ip route 192.168.1.0255.255.255.0192.168.1.1

D.ip route 192.168.2.128 255.255.255.128192.168.1.2

(29)A.仅 Router1#模式下　　B.Router1>或 Router1#模式下

C.Router1(config)#模式下　　D.Router1(config-if)#模式下

(30)A.config/all　　B.route display　　C.show ip route　　D.show route

【答案】A　B　C

【解析】本试题考查路由器配置及相关命令、模式。

在路由器 Router1 上配置一条记录即可访问网络 1 和网络 2,网络 1 和网络 2 汇聚后的地址为 192.168.2.0/24,下一跳地址为 192.168.1.1,故配置命令为 ip route192.168.2.0 255.255.255.0 192.168.1.1

路由器中，Router1>或 Router1#模式下均可查看路由，查看的命令为 show ip route。

有多种方案可以在一台服务器中安装 windows 和 Linux 两种网络操作系统,其中可以同时运行 windows 和 Linux 系统的方案是__(31)__。

(31)A.GRUB 引导程序　　B.LILO 多引导程序

C.VMare 虚拟机　　D.windows 多引导程序

【答案】C

【解析】本题考查网络操作系统安装和引导的基础知识。

在一台服务器中安装 Windows 和 Linux 两种网络操作系统，可以有多种方案，选项 A、B、C 和 D 都是可行方案。但 A、B 和 D 三个选项使用的都是多引导程序,每次运行只能从 Windows 和 Linux 两个系统中选择一个运行,如果需要同时运行 Windows 和 Linux 系统则只能选用虚拟机方案。

Linux 系统中的文件操作命令 grep 用于__(32)__。

(32)A.列出文件的属性信息　　B.在指定路径查找文件

C.复制文件　　D.在指定文件中查找指定字符串

【答案】D

【解析】

本题考查 Linux 系统下的常用命令。

linux 系统中常用的文件操作命令有 Is、find、cp、grep 等。

Is 命令将每个由 Directory 参数指定的目录或者每个由 File 参数指定的名称写到标准输出，以及所要求的和标志一起的其他信息。如果不指定 File 或 Directory 参数，Is 命令显示当

前目录的内容。

find 将文件系统内符合 expression 的文件列出来。可以指定文件的名称、类别、时间、大小、权限等不同信息的组合，只有完全相符的文件才会被列出来。

cp 命令的功能是将给出的文件或目录拷贝到另一文件或目录中。

grep (global search regular expression(RE) and print out the line,全面搜索正则表达式并把行打印出来）是一种强大的文本搜索工具，它能使用正则表达式搜索文本，并把匹配的行打印出来。

在某台主机上无法访问域名为 www.bbb.cn 的网站，而局域网中的其他主机可以访问，在该主机上执行 ping 命令时有如下所示的信息：

```
C:\>ping www.bbb.cn
Pinging www.bbb.cn [202.112.0.36] with 32 bytes of data:
Reply from 202.112.0.36: Destination net unreachable.
Reply from 202.112.0.36: Destination net unreachable.
Reply from 202.112.0.36: Destination net unreachable.
Reply from 202.112.0.36: Destination net unreachable.
Ping statistics for 202.112.0.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

分析以上信息，可能造成该现象的原因是(33)。

(33)A.该计算机设置的 DNS 服务器工作不正常

B.该计算机的 TCP/IP 协议工作不正常

C.该计算机连接的网络中相关的网络设备配置了拦截的 ACL 规则

D.该计算机网关地址设置错误

【答案】C

【解析】本题考查 Internet 的综合运用。

采用 Pingwww.bbb.com 命令得到目的 IP 地址不可达的结果，首先可排除 DNS 服务器不正常这一选项；如果 TCP/IP 协议工作不正常，或计算机网关地址设置错误，也都不可能得到域名的正确解析，因此只可能是在防火墙或相关设备上进行了规则设置。

近年来，我国出现的各类病毒中，(34)病毒通过木马形式感染智能手机。

(34)A.欢乐时光　　B.熊猫烧香　　C.X卧底　　D.CIH

【答案】C

【解析】本题考查病毒及其危害。

欢乐时光及熊猫烧香均为蠕虫病毒，CIH则为系统病毒，这3者均以感染台式机或服务器为主，且产生较早；X卧底则是新近产生的、通过木马形式传播、目标为智能手机的病毒。

某DHCP服务器设置的IP地址池从192.168.1.100到192.168.1.200，此时该网段下某台安装Windows系统的工作站启动后，获得的IP地址是169.254.220.188，导致这一现象最可能的原因是（35）。

(35)A.DHCP服务器设置的租约期太长

B.DHCP服务器提供了保留的IP地址

C.网段内还有其他的DHCP服务器，工作站从其他的服务器上获得的地址

D.DHCP服务器没有工作

【答案】D

【解析】本题考查DHCP服务器及DHCP协议的工作原理。

Windows系统中，获得的IP地址是169.254.220.188,表明DHCP服务器没有工作，系统给客户机自行分配了一个169段的地址。

下列关于DHCP的说法中，错误的是（36）。

(36)A.Windows操作系统中，默认的租约期是8天

B.客户机通常选择最近的DHCP服务器提供的地址

C.客户机可以跨网段申请DHCP服务器提供的IP地址

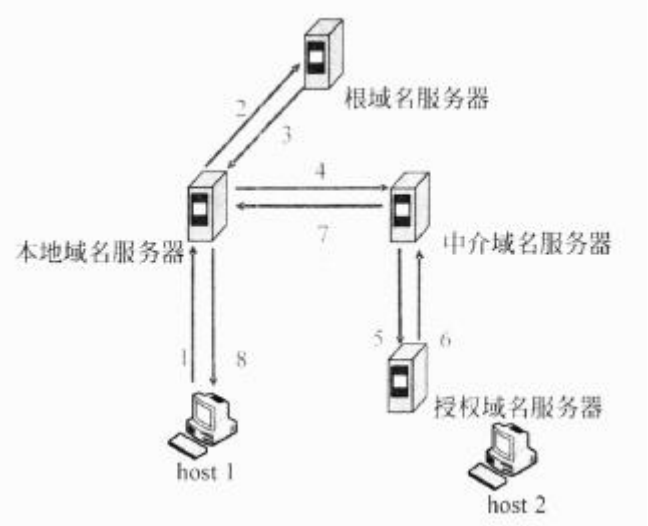
D.客户机一直使用DHCP服务器分配给它的IP地址，直到租约期结束才开始请求更新租约

【答案】D

【解析】本题考查DHCP协议及服务器的配置。

Windows操作系统中，DHCP提供的IP地址的默认租约期是8天；在有多个DHCP服务器响应时，客户机通常选择最先响应的DHCP服务器提供的地址；客户机可以通过中继代理跨网段申请DHCP服务器提供的IP地址；客户机一直使用DHCP服务器分配给它的IP地址，在租约期50%时开始请求更新租约。

主机 host1 对 host2 进行域名查询的过程如下图所示，下列说法中正确的是（37）。



(37)A.根域名服务器采用迭代查询，中介域名服务器采用递归查询

B.根域名服务器采用递归查询，中介域名服务器采用迭代查询

C.根域名服务器和中介域名服务器采用迭代查询

D.根域名服务器和中介域名服务器采用递归查询

【答案】A

【解析】本试题考查域名服务器进行域名解析时的查询方法。

DNS 客户端都配置了一个或多个 DNS 服务器的地址，无论是静态或动态配置的，这些 DNS 服务器都是用户所在域的授权服务器，而用户主机则是该域的成员。当用户在浏览器地址栏输入一个域名时，客户端就可以向本地的 DNS 服务器发出查询请求。查询过程分为两种查询方式：

①递归查询：当用户发出查询请求时，本地服务器要进行递归查询。这种查询方式要求服务器彻底地进行名字解析，并返回最后的结果——IP 地址或错误信息。如果查询请求在本地服务器中不能完成，那么服务器就根据它的配置向域名树中的上级服务器进行查询，在最坏的情况下可能要查询到根服务器。每次查询返回的结果如果是其他名字服务器的 IP 地址，则本地服务器要把查询请求发送给这些服务器做进一步的查询。

②迭代查询：服务器与服务器之间的查询采用迭代的方式进行，发出查询请求的服务器得到的响应可能不是目标的 IP 地址，而是其他服务器的引用（名字和地址），那么本地服务器就要访问被引用的服务器，做进一步的查询。如此反复多次，每次都更接近目标的授权服务器，直至得到最后的结果——目标的 IP 地址或错误信息。

因此，根域名服务器采用迭代查询，中介域名服务器采用递归查询。

网络拓扑设计对网络的影响主要表现在（38）。

①网络性能 ②系统可靠性 ③出口带宽 ④网络协议

(38)A.①、② B.①、②、③ C.③、④ D.①、② 、④

【答案】D

【解析】本试题考查网络规划与设计，以及网络拓扑结构等知识。

网络拓扑结构不同，对网络的性能、系统可靠性、网络协议的选择均会造成影响；出口带宽与 ISP 提供的容量有关，与内部网络结构的设计无关。

如果一台 cisco PIX 防火墙有如下的配置：

```
PIX(config)#nameif ethernet0 f1 security0
PIX(config)#nameif ethernet1 f2 security100
PIX(config)#nameif ethernet2 f3 security50
```

那么，以下说法中正确的是（39）。

(39)A.端口 f1 作为外部网络接口，f2 连接 DMZ 区域，f3 作为内部网络接口

B.端口 f1 作为内部网络接口，f2 连接 DMZ 区域，f3 作为外部网络接口

C.端口 f1 作为外部网络接口，f2 作为内部网络接口，f3 连接 DMZ 区域

D.端口 f1 作为内部网络接口，f2 作为内部网络接口，f3 连接 DMZ 区域

【答案】C

【解析】本题考查 cisco PIX 防火墙的安全级别设置。

cisco PIX 防火墙中，给定的数字越大说明安全级别越高。在网络中，外部网络安全级别最低，其次是 DMZ 区，内部网络接口最高。

在接收邮件时，客户端代理软件与 POP3 服务器通过建立（40）连接来传送报文。

(40)A.UDP B.TCP C.P2P D.DHCP

【答案】B

【解析】本题考查电子邮件及相关应用。

在接收邮件时，客户端代理软件与 POP3 服务器通过建立 TCP 连接来传送报文。

利用三重 DES 进行加密，以下说法正确的是（41）。

(41)A.三重 DES 的密钥长度是 56 位

B.三重 DES 使用三个不同的密钥进行三次加密

C.三重 DES 的安全性高于 DES

D.三重 DES 的加密速度比 DES 加密速度快

【答案】C

【解析】本题考查三重 DES 的知识。

三重 DES 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。本来，应该使用三个不同的密钥进行三次加密，这样就可以把密钥的长度加长到 3x56=168 位。但许多密码设计者认为 168 位的密钥已经超过实际需要了，所以便在第一层和第三层中使用相同的密钥，产生一个有效长度为 112 位的密钥。之所以没有直接采用两重 DES，是因为第二层 DES 不是十分安全，它对一种称为“中间可遇”的密码分析攻击极为脆弱，所以最终还是采用了利用两个密钥进行三重 DES 加密操作。这种方法的缺点是要花费原来三倍的时间，但从另一方面来看，三重 DES 的 112 位密钥长度是很“强壮”的加密方式了。

利用报文摘要算法生成报文摘要的目的是（42）。

(42)A.验证通信对方的身份，防止假冒　　B.对传输数据进行加密，防止数据被窃听

C.防止发送方否认发送过的数据　　D.防止发送的报文被篡改

【答案】D

【解析】本题考查报文摘要的知识。

报文摘要是指单向哈希函数算法将任意长度的输入报文经计算得出固定位的输出。报文摘要是用来保证数据完整性的。传输的数据一旦被修改那么计算出的摘要就不同，只要对比两次摘要就可确定数据是否被修改过。

(43)是支持电子邮件加密服务的协议。

(43)A.PGP　　B.PKI　　C.SET　　D.Kerberos

【答案】A

【解析】本题考查电子邮件加密服务的知识。

PKI 即公钥基础设施，是一种遵循既定标准的密钥管理平台，它能够为所有网络应用提

供加密和数字签名等密码服务及所必需的密钥和证书管理体系。

SET 即安全电子交易协议，是美国 Visa 和 MasterCard 两大信用卡组织等联合于 1997 年 5 月 31 日推出的用于电子商务的行业规范，其实质是一种应用在 Internet 上、以信用卡为基础的电子付款系统规范，目的是为了保证网络交易的安全。

Kerberos 是一种网络认证协议，其设计目标是通过密钥系统为客户机服务器应用程序提供强大的认证服务。

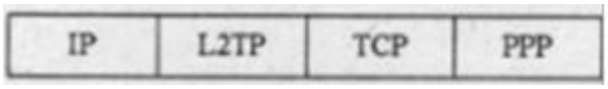
PGP 是一个基于 RSA 公匙加密体系的邮件加密软件。可以用它对邮件保密以防止非授权者阅读，它还能对邮件加上数字签名从而使收信人可以确认邮件的发送者，并能确信邮件没有被篡改。

下面能正确表示 L2TP 数据包封装格式的(44)。

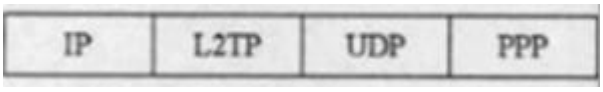
(44)A.

B.

C.



D.



【答案】B

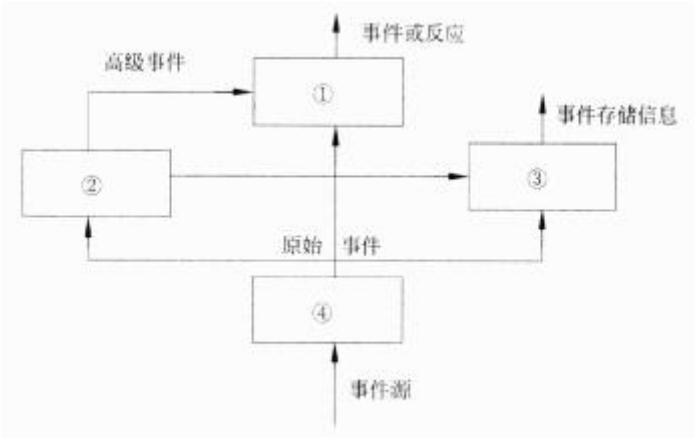
【解析】本题考查 L2TP 数据包的基本知识。

第 2 层隧道协议（Layer 2 Tunneling Protocol, L2TP)用于把各种拨号服务集成到 ISP 的服务提供点。L2TP 扩展了 PPP 模型，允许第二层连接端点和 PPP 会话端点驻在由分组交换网连接的不同的设备中。

L2TP 报文分为控制报文和数据报文。控制报文用于建立、维护和释放隧道和呼叫。数据报文用于封装 PPP 帧，以便在隧道中传送。控制报文使用了可靠的控制信道以保证提交，数据报文被丢失后不再重传。

在 IP 网上使用 UDP 和一系列的 L2TP 消息对隧道进行维护，同时使用 UDP 将 L2TP 封装的 PPP 帧通过隧道发送。可以对封装的 PPP 帧中的负载数据进行加密或压缩。下图为一个 L2TP 数据包格式。

下图为DARPA提出的公共入侵检测框架示意图，该系统由4个模块组成，其中模块①-④对应的正确名称为(45)。



(45)A.事件产生器、事件数据库、事件分析器、响应单元

B.事件分析器、事件产生器、响应单元、事件数据库

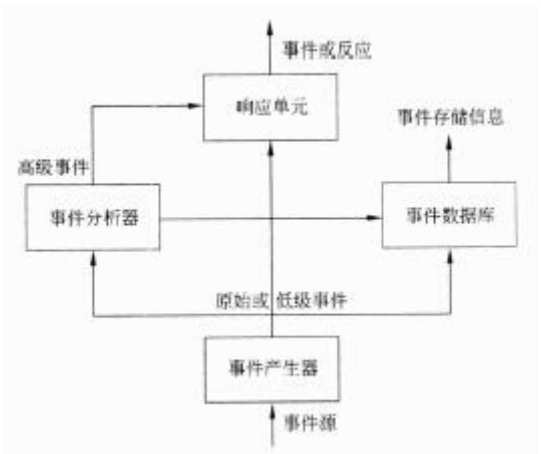
C.事件数据库、响应单元、事件产生器、事件分析器

D.响应单元、事件分析器、事件数据库、事件产生器

【答案】D

【解析】本题考查入侵检测的知识。

美国国防部高级研究计划局（DARPA)提出的公共入侵检测框架（Common Intrusion Detection Framework, CIDF)由4 个模块组成（如下图所示)。



①事件产生器（Event generators, E-boxes)。负责数据的采集，并将收集到的原始数据转

换为事件，向系统的其他模块提供与事件有关的信息。

②事件分析器（EventAnalyzers，A-boxes)。接收事件信息并对其进行分析，判断是否为入侵行为或异常现象。

③事件数据库（EventDataBases，D-boxes)。存放有关事件的各种中间结果和最终数据的地方，可以是面向对象的数据库，也可以是一个文本文件。

④响应单元（Response units，R-boxes)。根据报警信息做出各种反应，强烈的反应就是断开连接、改变文件属性等，简单的反应就是发出系统提示，引起操作人员注意。

在 Windows Server 2003 中，创建用户组时，可选择的组类型中，仅用于分发电子邮件且没有启用安全性的是(46).

(46)A.安全组　　B.本地组　　C.全局组　　D.通信组

【答案】D

【解析】

在 Windows Server 2003 中创建域组时，在“组类型”选项区域中可选择组的类型：安全组。可以显示在随机访问控制列表（DACL)中的组，该列表用于定义对资源和对象的权限。“安全组”也可用作电子邮件实体，给这种组发送电子邮件的同时也会将该邮件发给组中的所有成员。

通信组。仅用于分发电子邮件并且没有启用安全性的组。不能将“通信组”显示在用于定义资源和对象权限的随机访问控制列表(DACL)中。“通信组”只能与电子邮件应用程序（例如，Microsoft Exchange）一起使用，以便将电子邮件发送到用户集合。如果因为安全目的并不需要组，可以选择创建“通信组”而不要创建“安全组”。

在 Window Server 2003 中，与 Window Server 2000 终端服务对应的是(47)

(47)A.远程协助　　B.管理远程桌面

C.远程管理的 Web 界面　　D.远程安装服务

【答案】B

【解析】本题考查 Window Server 2003 中有关终端服务的新特性。

Windows Server 2003 终端服务添加了管理远程桌面，它实际上是所有服务器版本的远程管理模式，无需像 Windows 2000 那样一定要 Windows 2000 Server CD 才能安装它，只需进入远程选项卡，就可以在所有服务器版本中打开远程桌面。

网络管理系统由网络管理站，网管代理，网络管理协议和管理信息库 4 个要素组成，当网管代理向管理站发送事件报告时，使用的操作是(48)。

(48)A.get　　B.get-next　　C.trap　　D.set

【答案】C

【解析】本题考查网络管理中 SNMP 协议支持的服务原语。

Get 检索数据，Set 改变数据，GetNext 提供扫描 MIB 树和连续检索数据的方法，Trap 则提供从代理进程到管理站的异步报告机制。

在 MIB-2 中，IP 组对象 ipInReceives 为接收的 IP 数据报总数，其数据类型为（49）类型。

(49)A.整数　　B.计数器　　C.序列　　D.计量器

【答案】B

【解析】本题考查 SNMP 协议中 MIB-2 的功能组对象的数据类型。

在 MIB-2 中，IP 组对象 ipInReceives 为接收的 IP 数据报总数，其数据类型为计数器类型（Counter)。

在 TCP/IP 协议分组结构中，SNMP 是在（50）协议之上的异步请求/响应协议。

(50)A.TCP　　B.UDP　　C.HTTP　　D.P2P

【答案】B

【解析】本题考查 SNMP 协议体系结构。

SNMP 定义为应用层协议，它依赖于 UDP 数据报服务。SNMP 实体向管理应用程序提供服务，它的作用是把管理应用程序的服务调用变成对应的 SNMP 协议数据单元，并利用 UDP 数据报发送出去。

一台电脑的本地连接设置如下图所示，结果发现不能 ping 通任何远程设备，该故障的原因是什么？（51)。

(51)A.默认网关的地址不属于主机所在的子网

B.该主机的地址是一个广播地址

C.默认网关的地址是该子网中的广播地址

D.该主机的地址是一个无效的组播地址

【答案】C

【解析】

在这个配置中，子网掩码是 255.255.255.248,而默认网关的地址 220.15.17.7 广播地址，这种配置是无效的。

如果指定子网掩码为 255.255.254.0，则地址（52）可以被赋予一个主机。

(52)A.112.10.4.0　　B.186.55.3.0　　C.117.30.3.255　　D.17.34.36.0

【答案】B

【解析】

如果指定子网掩码为 255.255.254.0，则 IP 地址的最后 9 位为主机地址，所以这 9 位不能为全 0 或全 1，由于

112.10.4.0 的二进制形式是：　01110000.00001010.00000100.00000000
186.55.3.0 的二进制形式是：　10111010.00110111.0000001 1.00000000
117.30.3.255 的二进制形式是：　01110101.00011110.0000001 1.11111111
17.34.36.0 的二进制形式是：　00010001.00100010.00100100.00000000

所以只有地址 B 可以被赋予一个主机

某个网络中包含 320 台主机，采用什么子网掩码可以把这些主机置于同一个子网中而且不浪费地址？（53）。

(53)A. 255.255.255.0　　B. 255.255.254.0

C. 255.255.252.0　　D. 255.255.248.0

【答案】B

【解析】

320 台主机要至少要占用 9 位子网掩码，所以只有 B 是正确答案。

如果 DHCP 服务器分配的默认网关地址是 192.168.5.33/28，则主机的有效地址应该是（54）。

(54)A. 192.168.5.55　　B. 192.168.5.47

C. 192.168.5.40　　D. 192.168.5.32

【答案】C

【解析】

网关地址 192.168.5.33/28 的二进制形式是：11000000.10101000.00000101.00100001

A．192.168.5.55 的二进制形式是：

11000000.10101000.00000101.00110111

B．192.168.5.47 的二进制形式是：

11000000.10101000.00000101.00101111

C．192.168.5.40 的二进制形式是：

11000000.10101000.00000101.00101000

D．192.168.5.32 的二进制形式是：

可见答案 C 与网关地址属于同一个子网。答案 B 是同一子网中的广播地址，答案 D 是同一子网的网络地址。

4 条路由：124.23.129.0/24,124.23.130.0/24,124.23.132.0/24 和 124.23.133.0/24 经过汇聚后得到的网络地址是(55)

(55)A. 124.23.128.0/21　　B. 124.23.128.0/22

C. 124.23.130.0/22　　D. 124.33.128.0/23

【答案】A

【解析】

地址 124.23.129.0/24 的二进制展开形式为：01111100.00010111.10000001.00000000
地址 124.23.130.0/24 的二进制展开形式为：01111100.00010111.10000010.00000000
地址 124.23.132.0/24 的二进制展开形式为：01111100.00010111.10000100.00000000
地址 124.23.133.0/24 的二进制展开形式为：01111100.00010111.10000101.00000000
所以提供 21 位子网掩码的地址 124.23.128.0/21 可以作为汇聚后的网络地址。

下面哪一个 IP 地址属于 CIDR 地址块 120.64.4.0/22？(56)

(56)A.120.64.8.32　　B.120.64.7.64

C.120.64.12.128　　D.120.64.3.255

【答案】B

【解析】

地址块 120.64.4.0/22 的二进制形式为：　01111000.01000000.00000100.00000000
A 地址 120.64.8.32 的二进制形式为：　01111000.01000000.00001000.00100000
B 地址 120.64.7.64 的二进制形式为：　01111000.01000000.00000111.01000000
C 地址 120.64.12.128 的二进制形式为：　01111000.01000000.00001100.10000000
D 地址 120.64.3.255 的二进制形式为：　01111000.01000000.00000011.11111111
所以只有 B 答案是正确的。

两个主机通过电缆直接相连，主机 A 的 IP 地址为 220.17.33.24/28，而主机 B 的 IP 地址为 220.17.33.100/28，两个主机互相 Ping 不能，这时应该(57)

(57)A.改变主机 A 的地址为 220.17.33.15

B.改变主机 B 的地址为 220.17.33.111

C.改变子网掩码为 26

D.改变子网掩码为 25

【答案】D

【解析】

主机 A 地址 220.17.33.24/28 的二进制形式是:11011100.00010001.00100001.00011000
主机 B 地址 220.17.33.100/28 的二进制形式是：11011100.00010001. 00100001. 01100100
可见两个主机地址被子网掩码覆盖的部分不同，不在一个子网中，所以互相 Ping 不通。纠正的方法是缩短子网掩码到 25 位，使两个地址处于同一子网中。

下面哪个地址可以应用于公共互联网中？(58)

(58)A.10.172.12.56　　B.172.64.12.23

C.192.168.22.78　　D.172.16.33.124

【答案】B

【解析】

公共互联网中的地址不能是规定的私网地址，地址 10.172.12.56 是 A 类私网地址，地址 192.168.22.78 是 C 类私网地址，地址 172.16.33.124 是 B 类私网地址，都不能应用于互联网中。

下面关于 IPv6 单播地址的描述中，正确的是（59）。

(59)A.全球单播地址的格式前缀为 2000::/3

B.链路本地地址的格式前缀为 FE00::/12

C.站点本地地址的格式前缀为 FE00::/10

D.任何端口只能有唯一的全局地址

【答案】A

【解析】

IPv6 地址是一个或一组接口的标识符。IPv6 地址被分配到接口，而不是分配给结点。IPv6 地址的格式前缀（Format Prefix, FP)用于表示地址类型或子网地址，可表示为“IPv6 地址/前缀长度”的形式。IPv6 地址的具体类型是由格式前缀来区分的，这些前缀的初始分配如下表所示。

表　IPv6 地址的初始分配

分配	前缀(二进制)	占地址空间的比例
保留	0000 0000	1/256
未分配	0000 000	11/256
可聚合全球单播地址	001	1/8
链路本地单播地址	1111 1110 10	1/1024
站点本地单播地址	1111 1110 11	1/1024
组播地址	1111 1111	1/256

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

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

②本地单播地址：这种地址的有效范围仅限于本地，又分为两类：

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

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

在 Wi-Fi 安全协议中，WPA 与 WEP 相比，采用了（60）。

(60)A.较短的初始化向量　　B.更强的加密算法

C.共享密钥认证方案　　D.临时密钥以减少安全风险

【答案】D

【解析】

有线等效保密（Wired Equivalent Privacy, WEP)是 IEEE 802.11 标准的一部分，其设计目的是提供与有线局域网等价的机密性。WEP 使用 RC4 协议进行加密，并使用 CRC-32 校验保证数据的正确性。最初的 WEP 标准使用 24 比特的初始向量，加上 40 比特的字符串，构成 64 比特的 WEP 密钥。后来也允许使用 104 比特的字符串，加上 24 比特的初始向量，构成 128 比特的 WEP 密钥。WEP 存在一些安全缺陷，包括初始向量 IV 雷同的可能性，以及编造的数据包等。利用 RC4 加解密原理和初始向量的特点，通过网络偷听，不要很长时间就可以把 RC4 密钥破解出来。

Wi-Fi 联盟为了改善 WLAN 的安全性,根据 802.11i 草案制定了 WPA(Wi-Fi Protected Access)安全认证方案。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变密钥的临时密钥完整性协议 TK1P，以更频繁地变换密钥来降低安全风险。最后，WPA 强化了数据完整性保护，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。

在 IEEE 802.1 1i 后，Wi-Ft 联盟就按照新的安全标准对无线产品进行认证，并且这种认证方案称为 WPA2。

生成树协议 STP 使用了哪两个参数来选举根网桥？（61）。

(61)A.网桥优先级和 IP 地址　　B.链路速率和 IP 地址

C.链路速率和 MAC 地址　　D.网桥优先级和 MAC 地址

【答案】D

【解析】

在通过网桥互联的局域网中，每一个网桥有唯一的 MAC 地址和唯一的优先级，地址和优先级构成网桥的标识符。按照生成树算法，通常选择标识符最小的网桥作为生成树的根网桥。

关于 VLAN，下面的描述中正确的是（62）。

(62)A.一个新的交换机没有配置 VLAN　　B.通过配置 VLAN 减少了冲突域的数量

C.一个 VLAN 不能跨越多个交换机　　D.各个 VLAN 属于不同的广播域

【答案】D

【解析】

虚拟局域网（Virtual Local Area Network, VLAN)是根据管理功能、组织机构或应用类型对交换局域网进行分段而形成的逻辑网络。虚拟局域网与物理局域网具有同样的属性，然而其中的工作站可以不属于同一物理网段。每一个 VLAN 是一个逻辑网络，发往 VLAN 之外的分组必须通过路由器进行转发。任何交换端口都可以分配给某个 VLAN，属于同一个 VLAN 的所有端口构成一个广播域，各个 VLAN 属于不同的广播域。

新交换机出厂时被预配置了 VLAN1,交换机本身的通信（VTP 报文、CDT 组播、以及交换机发出其他报文）都发生在 VLAN 1 中。VLAN 1 被称为管理 VLAN，当然也可以用其他的 VLAN 作为管理 VLAN。为了安全起见，网络中所有交换机的默认配置都必须改变，这样，不同 VLAN 之间的访问都要经第三层设备转发，通过访问控制列表可以过滤不必要的通信。

下面哪个协议用于承载多个 VLAN 信息？（63）。

(63)A.802.3　　B.802.1q　　C.802.1x　　D.802.11

【答案】B

【解析】

在划分成 VLAN 的交换局域网中，交换机端口之间的连接分为两种：接入链路和中继链路。接入链路只能连接具有标准以太网卡的设备，只能传送属于单个 VLAN 的数据包。中继链路则能够传送多个 VLAN 的数据包。

为了支持中继连接，应该修改原来的以太网数据包，在其中加入 VLAN 标记，以区分属于不

同 VLAN 的广播域。

VLAN 帧标记有两种格式。一种是 IEEE 制定的 802.1q 协议，在原来的以太帧中增加了 4 个字节的标记(Tag)字段，如图 3 所示，其中标记控制信息(Tag Control Information, TCI)包含 Priority、CFI 和 VID 三部分。

图 3　802.1q 帧格式

另一个是 Cisco 公司的交换机间链路协议（Inter-Switch Link, ISL),适用于 Cisco 的 Catalyst 系列交换机。ISL 协议在每个帧的头部增加 26 字节的帧标记，在帧尾附加 4 字节的 CRC 校验码。

以太网协议中使用物理地址作用是什么？（64）。

(64)A.用于不同子网中的主机进行通信　　B.作为第二层设备的唯一标识

C.用于区别第二层第三层的协议数据单元　　`D.保存主机可检测未知的远程设备

【答案】B

【解析】

以太网协议中的物理地址是作为第二层设备的唯一标识，通常称为 MAC 地址，每一个网卡都具有其唯一的 MAC 地址。

下面的光纤以太网标准中，支持 1000m 以上传输距离的是（65）。

(65)A.1000BASE-FX　　B.1000BASE-CX　　C.1000BASE-SX　　D.1000BASE-LX

【答案】D

【解析】

千兆以太网通常作为主干网提供无阻塞的数据传输服务。1998 年 6 月公布的 IEEE 802.3z 和 1999 年 6 月公布的 IEEE 802.3ab 已经成为千兆以太网的正式标准。它规定了四种传输介质，如下表所示。

表　千兆以太网标准

标准	名称	电缆	最大段长	特点
IEEE802.3z	1000Base-SX	光纤（短波 770～860nm）	550m	多模光纤（50，62.5μm）
	1000Base-LX	光纤（长波 1270～1355nm）	**5000m**	单模（10μm）或多模光纤（50，62.5μm）
	1000Base-CX	2 对 STP	25m	屏蔽双绞线，同一房间内的设备之间
IEEE 802.3ab	1000Base-T	4 对 UTP	100m	5 类无屏蔽双绞线，8B/10B 编码

IEEE 802.11 采用了 CSMA/CA 协议，采用这个协议的原因是（66）。

(66)A.这个协议比 CSMA/CD 更安全　　B.这种协议可以开放更多业务

C.这种协议可能解决隐蔽站的问题　　D.这个协议比其它协议更有效率

【答案】C

【解析】

802.11 MAC 子层的功能是提供访问控制机制，定义了 3 种访问控制机制:CSMA/CA 支持竞争访问，RTS/CTS 和点协调功能支持无竞争的访问。

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，例如两个站由子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。

配置路由器默认路由的命令是（67）。

(67)A.ip route 220.117.15.0255.255.255.00.0.0.0

B.ip route 220.117.15.0255.255.255.0220.117.15.1

C.ip route 0.0.0.0255.255.255.0220.117.15.1

D.ip route 0.0.0.00.0.0.0220.117.15.1

【答案】D

【解析】

默认路由（Default Route)是在路由器无法找到通往目标的路径时使用的转发通路。一般来说，当路由器收到了一个分组，其目标地址在路由表中找不到时，该分组就被丢弃。这与交换机对未知分组进行泛洪（flooding)发送是不同的。在路由表中设置的默认路由是用

来转发未知分组的通路。配置默认路由可以把以上命令中的目标网络号和子网掩码表示为“0.0.0.0 0.0.0.0”，其含义是“所有网络的所有主机”。

路由表如下图所示，如果一个分组的目标地址是220.117.5.65，则会发送给那个端口？（68）。

Network	interface	next-hop
220.117.1.0/24	e0	directly connected
220.117.2.0/24	e0	directly connected
220.117.3.0/25	s0	directly connected
220.117.4.0/24	s1	directly connected
220.117.5.0/24	e0	220.117.1.2
220.117.5.64/28	e1	220.117.2.2
220.117.5.64/29	s0	220.117.3.3
220.117.5.64/27	s1	220.117.4.4

(68)A.220.117.1.2　　B.220.117.2.2　　C.220.117.3.3　　D.220.117.4.4

【答案】C

【解析】

如果一个分组的目标地址是220.117.5.65，按照最长匹配原则，与之匹配的是220.117.5.64/29,所以该分组会被发送给端口220.117.3.3。

一家连锁店需要设计一种编址方案来支持全国各个门店销售网络，门店有300家左右，每个门店一个子网，每个子网终端最多50台电脑，该连锁店从ISP处得到一个B类地址，应该采用的子网掩码是（69）。

(69)A.255.255.255.128　　B.255.255.252.0

C.255.255.248.0　　D.255.255.255.224

【答案】A

【解析】

每个子网有50台终端，至少要占用6位地址码。300家门店需要占用9位地址码。对于B类网络，用第三字节的8位和第四字节的1位来区分不同的门店子网，用第四字节的7位作为子网内的主机地址，是一种合适的编址方案。

网络系统设计过程中，物理网络设计阶段的任务是（70）。

(70)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，掌握网络所处的状态

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。

Traditional IP packet forwarding analyzes the（71）IP address contained in then network layee header of each packet as the packet rravels from its sourse to its final destination. A router analyzes the destination IP address independently at each hop in the network. Dynamic（72)protocols or staitic configuration builds the database needed to analyze the destination IP address(the routing table). The process of implementing traditional IP routing also is called hop-by-hop destination-based (73) routing. Although successful,and obviously widely deployed,certain restrictions,which have been realized for some time,exist for this method of packet forwarding that diminish its（74）.New techniques are therefore required to address and expand the functionality of an IP-based network infrastructure. This first chapter concertrates on idenfifying these restrictions.and presents a new architecture,known as multiprotocl（ 75 ） switching,that provides solutions to some of this restrictions.

(71)A.datagram	B.destination	C.connection	D.service
(72)A.routing	B.forwarding	C.transmission	D.managerment
(73)A.anycast	B.multicast	C.broadcast	D.unicast
(74)A.reliability	B.fexibility	C.stability	D.capability
(75)A.cost	B.cast	C.mark	D.label

【答案】B　A　D　B　D

【解析】

传统的 ip 分组转发机制是在分组从源端到达最终目标的旅行过程中，分析包含在每个

分组网络层头部的目标 ip 地址字段。在网络的每一跳步中，路由器独立地分析 y 标 ip 地址字段。动态路由协议或者静态配置都建立了用于分析目标 ip 地址字段的数据库（路由表)。实现传统 ip 路由的过程也被叫做逐跳的基于目标的单播路由。虽然这种分组转发技术已经取得了成功并被广泛地部署在网络中，然而人们早已认识到，还存在一些约束条件降低了它的灵活性。因而需要一种新技术来改进和扩展基于 ip 的网络架构功能。这一章集中于识别这些约束条件，并提出一种新的体系结构，这就是多协议标记交换技术，它提供了克服这些约束条件的解决方案。

试题一

【说明】

某学校计划部署园区网络，本部与分校区地理分布如图 1-1 所示。

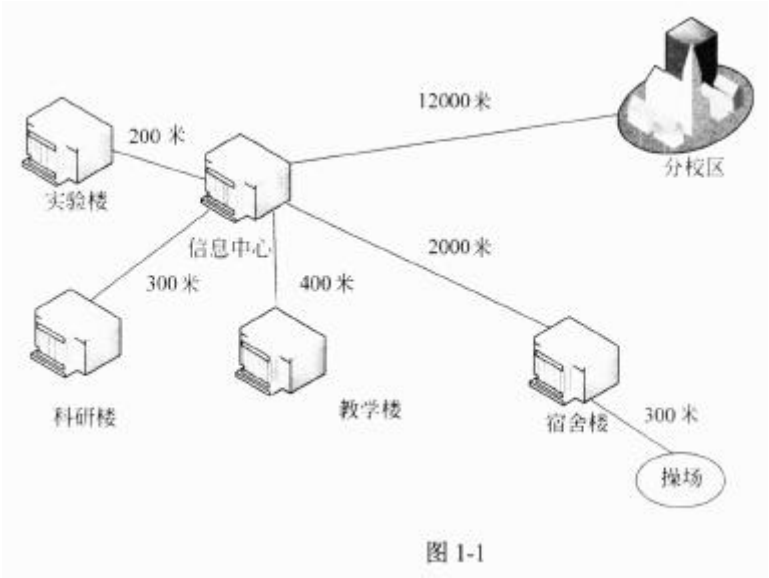


图 1-1

根据需求分析结果，网络部分要求如下：

1．网络中心机房在信息中心。

2．要求汇聚交换机到核心交换机以千兆链路聚合。

3．核心交换机要求电源、引擎双冗余。

4．信息中心与分校区实现互通。

【问题 1】

网络分析与设计过程一般采用五个阶段：需求分析、通信规范分析、逻辑网络设计、物理网络设计与网络实施。其中，确定新网络所需的通信量和通信模式属于（1）阶段；确定 IP 地址分配方案属于（2）阶段；明确网络物理结构和布线方案属于（3）阶段；确定网络投资规模属于（4）阶段。

（1）通信规范分析

（2）逻辑设计

（3）物理网络设计

（4）需求分析

本问题考查网络规划周期的基本知识。

网络规划一般采用五阶段周期，将网络建设划分为需求分析、通信规范分析、逻辑网络设计、物理网络设计、实施五个阶段。其中，需求分析应完成业务需求、用户需求、应用需求、计算机平台需求、网络通信需求等各项分析，其中网络投资规模属于需求分析要完成的工作。现有的网络体系分析，即通信规范分析应完成现有网络的拓扑结构分析、容量分析，以及新网络所需的通信量和通信模式等分析。

逻辑网络设计是体现网络设计核心思想的关键阶段，在这一阶段根据需求规范和通信规范选择一种比较适宜的网络逻辑结构，并实施后续的资源分配规划、安全规划等内容。其中，IP地址分配方案就属于这一阶段的工作。

物理网络设计是逻辑网络设计的具体实现，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。

实施阶段就是根据以上的工作完成网络的安装和维护。

【问题 2】

根据需求分析，规划网络拓扑如图 1-2 所示。

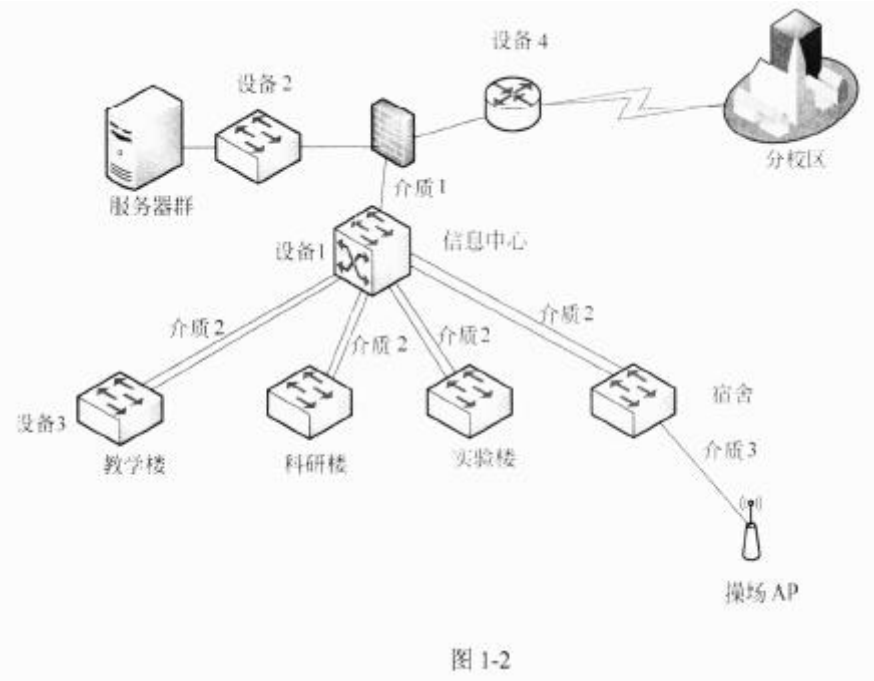


图 1-2

1. 核心交换机配置如表 1-1 所示，确定核心交换机所需配备的模块最低数量。

设备大类	模块描述	数量
核心交换机	以太网交换机主机	1
	交换路由引擎	（5）
	交流电源模块，1400W	（6）
	24 端口千兆以太网电接口板（RJ45）	1
	12 端口千兆以太网光接口板（SFP，LC）	（7）
	SFP-GE 模块（1310nm，LC）	（8）

2．根据网络需求描述、网络拓扑结构、核心交换机设备表，图 1-2 中的介质 1 应选用（9）；介质 2 应选用（10）；介质 3 应选用（11）。

问题（9）～（11）备选答案：（注：每项只能选择一次）

A．单模光纤 B．多模光纤 C．6 类双绞线 D．同轴电缆

3．为了网络的安全运行，该网络部署了 IDS 设备。在图 1-2 中的设备 1、2、3、4 上，适合部署 IDS 设备的是（12）及（13） 。

（5）2

（6）2

（7）1

（8）8

（9）C

（10）A

（11）B

（12）设备 1

（13）设备 2

（(12)、(13）答案可互换）

本问题考查网络设备选型、部署及介质选择知识。

根据题 H 描述可知，核心交换机要求电源、引擎双冗余，而且要求汇聚交换机到核心交换机以千兆链路聚合。所以核心交换机的交换路由引擎及交流电源模块最低数量为 2 个。根据拓扑结构图，核心交换机下共有 4 个汇聚交换机，而汇聚交换机到核心交换机以千兆链路聚合，所以光模块-SFP-GE-单模模块最少需要 8 个，12 端口千兆/百兆以太网光接口模块最少需要

1 个。

根据网络需求描述、网络拓扑结构、核心交换机设备表，由于备选答案每项只能选择一次，故先判断介质 2 必须选择单模光纤，介质 3 只能选择多模光纤，所以介质 1 只能选择 6 类双绞线。

入侵检测系统是一个监听设备，无须跨接在任何链路上，不产生任何网络流量便可以工作。因此，部署 IDS 的唯一的要求是，应当挂接在所关注流量必须流经的链路上。在这里，“所关注流量”指的是来自高危网络区域的访问流量，以及需要统计、监视的网络报文。目前的网络都是交换式的拓扑结构，因此一般选择在尽可能靠近攻击源，或者尽可能接近受保护资源的地方，这些位置通常是：服务器区域的交换机上、Internet 接入路由器之后的第一台交换机上、重点保护网段的局域网交换机上。所以，在图 2-1 中的设备 1、2、3、4 中，适合部署 IDS 设备 1 和设备 2 。

【问题 3】

该校园根据需要部署了两处无线网络。一处位于学校操场；一处位于科研楼。其中操场的无线 AP 只进行用户认证，科研楼的无线 AP 中允许指定的终端接入。

1、无线 AP 分为 FIT AP 和 FAT AP 两种。为了便于集中管理，学校的无线网络采用了无线网络控制器。所以该学校的无线 AP 为（14）AP。天线通常分为全向天线和定向天线，为保证操场的无线覆盖范围，此时应配备（15）天线。

2、为了保证科研楼的无线 AP 的安全性，根据需求描述，一方面需要进行用户认证，另一方面还需要多接入终端的（16）进行过滤，同时保证信息传输的安全性，应采用加密措施。无线网络加密主要有 WEP、WPA 和 WPA2 三种方式目前安全性最好的是（17）。

（14）FIT AP

（15）全向

（16）MAC（或物理）

（17）WPA2

本题考查无线网络的基础知识。

无线 AP 分为 FIT AP 和 FAT AP 两种，FAT AP 是与 FIT AP 相对来讲的，FAT AP 将 WLAN 的实体层、加密、用户认证、网路管理等功能集于一身；而 FIT AP 是一个只有射频和通信功能的 AP，功能单一，不能独立工作。FAT AP 无线网路解决方案可由 FAT AP 直接在有线网的基

础上构成，所有 AP 都单独进行配置，且难于集中管理；而 FITAP 无线网路解决方案则是由无线网路控制器和 FIT AP 在有线网的基础上构成，且 FIT AP 上 “零配置”，所有配置都集中到无线网路控制器上。易于集中管理。所以该学校的无线 AP 为 FITAP。天线通常分为全向天线和定向天线，为保证操场的无线覆盖范围，此时应配备全向天线。

根据需求描述，科研楼的无线 AP 中允许指定的终端接入，所以为了保证科研楼的无线 AP 的安全性，一方面需要进行用户认证，另一方面还需要对接入终端的 MAC 地址进行过滤，同时为保证信息传输的安全性，应采用加密措施。无线网络加密主要有 WEP、WPA 和 WPA2 三种方式。目前，安全性最好的是 WPA2。

【问题 4】

学校计划采用VPN方式实现分校区与本部的互通VPN的隧道协议主要有三种:PPTP,L2TP和 IPSec，其中（18）和（19）协议工作在 OSI 模型的第二层，又称为二层隧道协议；（20）是第三层隧道协议。

（18）PPTP

（19）L2TP（(18)、(19）答案可互换）

（20）IPSee

本问题考查 VPN 的基础知识。

VPN 的隧道协议主要有三种：PPTP，L2TP 和 IPSec，其中 PPTP 和 L2TP 协议工作在 OSI 模型的第二层，又称为二层隧道协议；而 IPSec 是第三层隧道协议。

试题二

【说明】

某公司搭建了一个小型局域网，网络内有200台PC机，网络中配置一台Linux服务器作为Internet接入服务器，Linux服务器E0网卡的IP地址为192.168.1.1，E1 网卡IP地址为 202.100.20.30，该网络结构如图2-1所示。

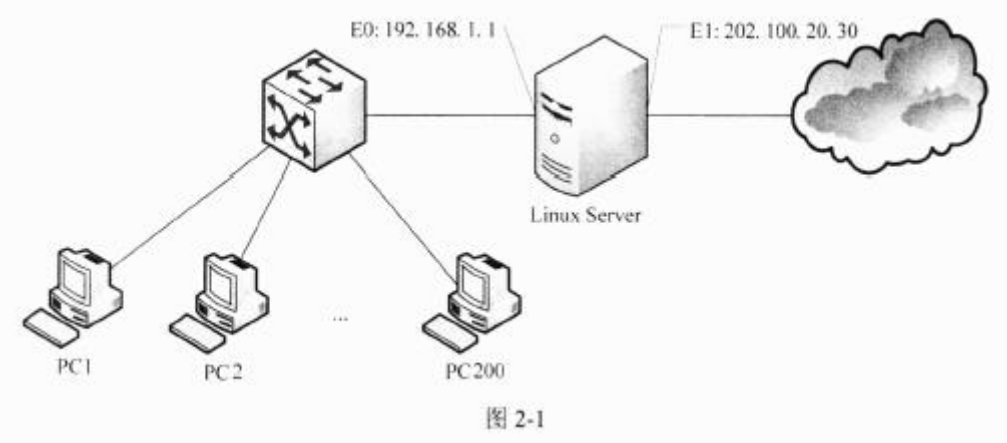


图 2-1

为了方便局域网IP地址管理，决定在Linux Server中配置DHCP服务要求DHCP服务的配置满足几个条件：

1．考虑今后扩展需求，当前只能使用从192.168.1.1到192.168.1.201的IP地址；

2．PC100（MAC 地址为00:A0:78:8E:9E:AA）作为内部文件服务器，需要使用固定IP地址192.168.1.100；

3．在Linux Server上配置DNS服务；

【问题1】

根据题目要求补充完成DHCP服务器配置文件dhcpd.conf的配置项。

```
default-lease-time 1200;
max-lease-time 9200;
option subnet-mask 255.255.255.0;
option broadcast-address    (1)    ;
option routers    (2)    ;
option domain-name-servers    (3)    ;
subnet    (4)    netmask    (5)
{
range    (6)    (7)    ;
}
host fixed{
hardware ethernet    (8)    ;
fixed-address    (9)    ;
}
```

（1）192.168.1.255

（2）192.168.1.1

（3）192.168.1.1

（4）192.168.1.0

（5）255.255.255.0

（6）192.168.1.2

（7）192.168.1.201

（8）00:A0:78:8E:9E:AA

（9）192.168.1.100

本题主要考查考生对 Linux 系统中 DHCP 服务 dhcpd 配置等相关知识点的掌握情况。

Linux 的 DHCP 服务是通过 dhcpd 提供的，该服务通过配置文件 dhcpd.conf 对服务参数等进行设置，相应的命令和解释如下：

default-lease-time 1200;//设置默认租期，单位为秒，DHCP 客户端请求 IP 地址时如果没有带租约参数，则 DHCP 服务器为客户端设置租期为默认租期。

max-lease-time 9200; //设置客户端最长租期，单位为秒，DHCP 客户端请求 IP 地址时如果请求租约超过该最长租期，则 DHCP 服务器为客户端设置租期为该租期。

```
option subnet-mask 255.255.255.0; //设置子网掩码
option broadcast-address   （1）  ;//设置子网广播地址
option routers   （2）  ; //设置网关地址
option domain-name-servers   （3）  ; //设置 DNS 服务器地址
subnet   netmask    //设置一个子网
range    //起始 IP 终止 IP 提供动态分配 IP 的范围
host     //参考特别的主机
hardware ethernet //指定 MAC 地址
fixed-address    //保留的 IP 地址
```

【问题 2】

依据 DHCP 协议约定和问题 1 中的配置，DHCP 客户端 PC1 从获取 IP 地址后经过（10）分钟需要到 DHCP 服务器申请租用更新。此时 PC1 发送到 DHCP 服务器的消息是（11），如果 DHCP 服务器同意租约更新，响应的消息是（12），如果 DHCP 服务器不同意租约更新，响应的消息是（13）。

（10）10

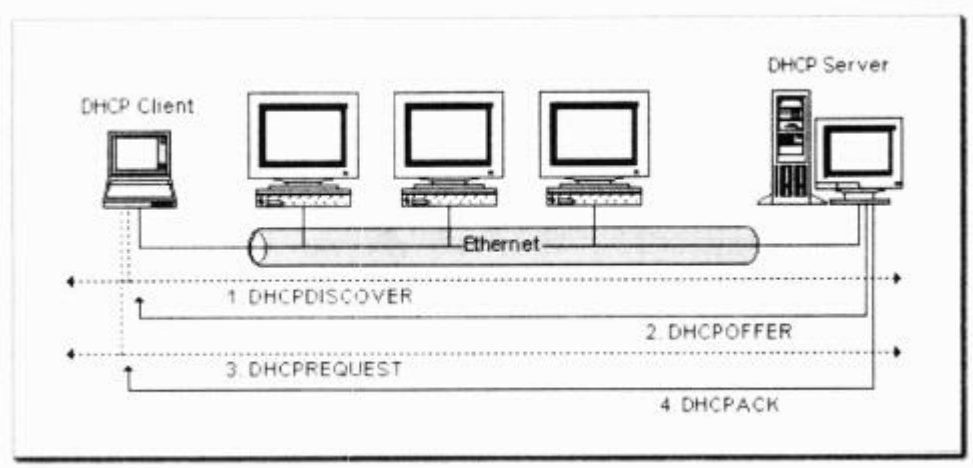
（11）DHCPREQUEST

（12）DHCPACK

（13）DHCPNACK

依据 DHCP 协议约定，DHCP 客户端从获取 IP 地址后到租约时间的 50%需要到 DHCP 服务器申请租约更新，从问题 1 中的配置可以得出默认租约是 1200 秒（20 分钟），所以 DHCP 客户端 PC1 从获取 IP 地址后经过 10 分钟需要到 DHCP 服务器申请租约更新。

DHCP 客户端和服务器交互的消息序列如下图所示。



从图中可知，此时 PC1 发送到 DHCP 服务器的消息是 DHCPREQUEST，如果 DHCP 服务器同意租约更新，响应的消息是 DHCPACK，如果 DHCP 服务器不同意租约更新，响应的消息是 DHCPNAK。

【问题 3】

在 DHCP 客户端还可以通过 Windows 命令（14）来立即释放申请到的 IP 地址，通过命令（15）来立即重新申请租约。

（14）ipconfig/release

（15）ipconfig/renew

在 DHCP 客户端，ifconfig 可以用于网络接口配置相关操作，带上参数也可以用于发送 DHCP 协议消息，可以通过命令 ipconfig/release 来立即释放申请到的 IP 地址，通过命令 ipconfig/renew 来立即重新申请租约。

试题三

【说明】

某学校的图书馆电子阅读室已经连接为局域网（局域网段 192.168.1.0/24）在原有接入校园网的基础上又租用了一条电信的 ADSL 宽带接入来满足用户的上网需求。其中校园网网段为 210.27.176.0 ～ 210.27.191.255 ，DNS 为 210.27.176.3，子网按照 C 类网络划分，每个子网的网关都为 210.27.xxx.1。ADSL 宽带的网络地址由电信自动分配。具体网络结构如图 3-1 所示。

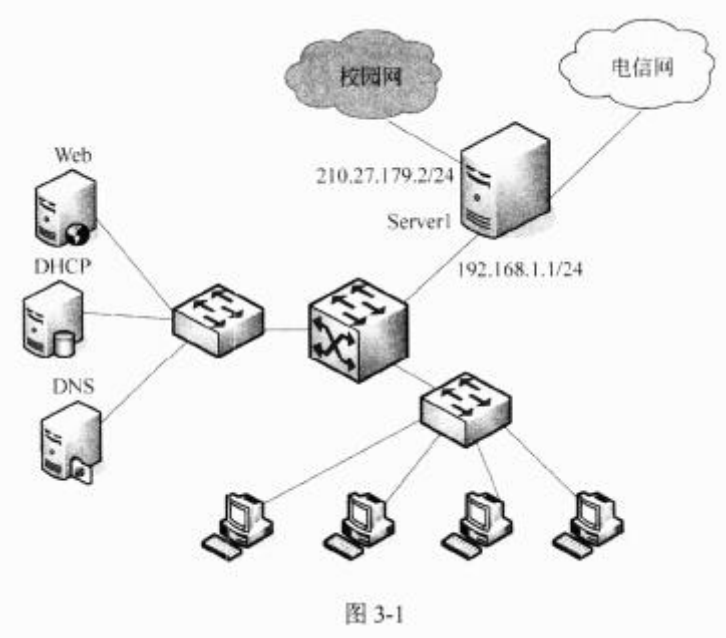


图 3-1

【问题 1】

如图 3-1 所示，在该电子阅览室的出口利用了一台安装 Windows Server 2003 的服务器实现客户端既能访问到本校和本馆内的电子资源，又能通过 ADSL 访问外部资源。现计划在 Server 上安装 3 块网卡来实现这个功能，三块网卡首先需要在如图 3-2 所示的界面上配置 IP 地址等信息。按照题目要求选择（1）～（6）中的正确选项。

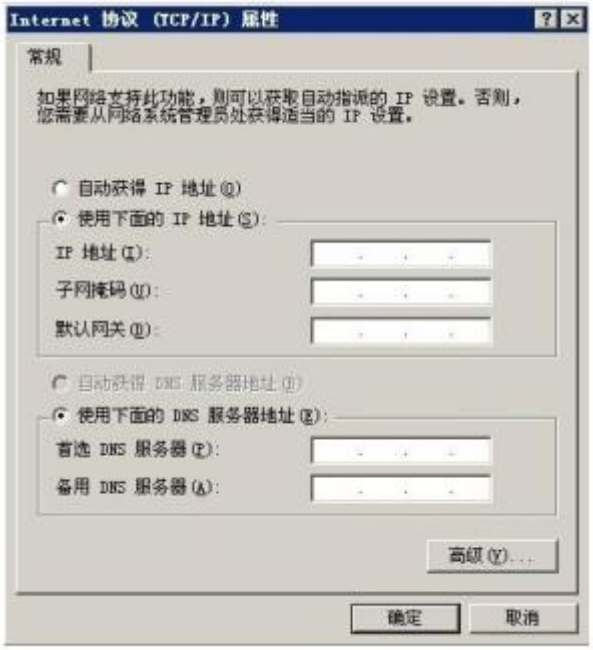


图 3-2

网卡 1：连接电子阅览室内网，IP 地址：192.168.1.1，子网掩码 255.255.255.0。

网关：（1），DNS：（2）。

网卡 2：连接 ADSL 电信网，IP 地址：（3），DNS：（4）。

网卡 3：连接校园网，IP 地址：（5），子网掩码：255.255.255.0，

网关：（6），DNS：210.27.176.3。

空（1）～（6）备选答案：

A. 192.168.1.1 B. 自动获取 C. 192.168.1.2

D. 不确定，保持为空 E. 210.27.179.2 F. 210.27.179.1

G. 255.255.255.0

（1）D

（2）D

（3）B

（4）B

（5）E

（6）F

本问题考查网络地址规划方面的知识。根据电子阅览室的网络拓扑图以及题目给出的提示，

连接电子阅览室内网的网段为 192.168.1.0/24,只有一个网段不需要跨网段访问，所以网关以及 DNS 皆可不用指定，保持为空即可；通过 ADSL 宽带接入到电信网的网卡一般利用 PPPoE 协议接入，接入网卡的 IP 地址和 DNS 都采用动态获取方式获得；接入到校园网的网卡地址题目中已经明确给出利用静态分配的方式，符合题目要求的 IP 地址选项只能是 210.27.179.2，而网关地址只能是 210.27.179. 1.

【问题 2】

在 Server1 上开启路由和远程访问服务出现如图 3-3 所示的窗口，在继续配置“网络接口”时，出现如图 3-4 所示的对话框,应该选择“(7)”,然后输入 ADSL 帐号和密码完成连接建立过程。

图 3-3

图 3-4

为了使客户机自动区分电子阅览室内网、校园网和 ADSL 电信网还需新建一个批处理文件 route.bat，并把路由功能加入到服务器中，route.bat 文件内容如下所示，完成相关配置。

```
cd\
route delete    (8)     //删除默认路由
route add       (9)     mask 255.255.255.0 192.168.1.1   //定义内网路由
route add       (10)    mask 255.255.255.0 210.27.179.1
//定义校园网一个网段路由
……  //依次定义校园网其他各网段路由
```

（7）使用以太网上的 PPP（PPPoE）连接

（8）0.0.0.0

（9）192.168.1.0

（10）210.27.176.0

本问题考查 Windows Server 2003 的路由与远程服务相关知识。

在 Server1 上开启路由和远程访问服务，题目明确要求“新建请求拨号接口”，而根据题意拨号接口采用的是 ADSL 方式接入电信网，ADSL 接入方式一般采用的是 PPPoE 协议，因此在图 3-4 的连接类型中只能选择“使用以太网上的 PPP (PPPoE)连接”这个选项。

同时为了使客户机自动区分电子阅览室内网、校园网和 ADSL 电信网，在该题目中还需在 Server1 上新建一个批处理文件 route.bat，并把路由功能加入到服务器中，即把 Server1 当作路由器来使用，只是使用的命令是 windows 支持的配置命令。具体来说 route.bat 文件的内容解释如下：

```
cd\
route delete   0.0.0.0   //删除默认路由
route add   192.168.1.0   mask 255.255.255.0 192.168.1.1   //定义内网路由
route add   210.27.176.0   mask 255.255.255.0 210.27.179.1 //定义校园网一个网段路由
route add   210.27.177.0   mask 255.255.255.0 210.27.179.1
… …
route add   210.27.191.0   mask 255.255.255.0 210.27.179.1
//依次定义校园网其他各网段路由
```

【问题 3】

因为电子阅览室的 DHCP 服务器设备老化需要更换，原有的 DHCP 服务器内容需要转移到新的服务器设备上，这时采用导入导出方式进行配置的迁移，采用的步骤如下：

1.在原有的 DHCP 服务器命令行模式下输入“netsh dhcp server export c:\dhcpbackup.txt”命令，将该文件拷贝到新服务器的相同位置。

2．在新的服务器上安装好 DHCP 服务后，在命令行模式下输入“（11）”命令，即可完成 DHCP 服务器的迁移。

3．在迁移操作时，一定要使用系统（12）组的有效账户。

（11）netsh dhcp server import c:\dhcpbackup.txt

（12）Administrators 或系统管理员

本问题考查 Windows Server 2003 DHCP 服务器迁移的相关知识。

当需要更换 Windows Server 2003 DHCP 服务器设备时，原有的 DHCP 服务器内容需要转移到新的服务器设备上，这时可以使用导入导出 DHCP 数据库的方式，实现 DHCP 服务器从一台服务器设备转移到另一台服务器设备上。具体操作是在原有的 DHCP 服务器命令行模式下输入“netsh dhcp server export c:\dhcpbackup.txt”命令，开始执行本服务器 DHCP 数据库的导出，导出目录和文件名为“c:\dhcpbackup.txt”；接着将该文件复制到新服务器的相同位置，打开新的服务器的命令行界面，输入“netsh dhcp server import c:\dhcpbackup.txt”

命令，将复制的 DHCP 数据库文件导入本机中。不过要注意的是在迁移操作中，一定要使用系统管理员组的有效账户，如果新服务器要升级为域控制器，尽量先做迁移后再做域身份的升级。

【问题 4】

1．若电子阅览室的客户机访问 Web 服务器时，出现“HTTP 错误 401.1-未经授权；访问由于凭据无效被拒绝。”现象，则需要在控制面板管理工具计算机管理本地用户和组，将（13）帐号启用来解决此问题。

2．若出现“HTTP 错误 401.2-未经授权；访问由于配置被拒绝。”的现象，造成错误的原因是身份验证设置问题，一般应将其设置为（14）身份认证

空（13）、（14）备选答案：

A．IUSR_计算机名 B．Administrator C．Guest D．匿名

（13）A

（14）D

本问题考查 WEB 访问中的故障排查的相关知识。

(1)错误现象一：HTTP 错误 401.1-未经授权：访问由于凭据无效被拒绝。

原因分析：由于用户匿名访问使用的账号是 IUSRJI1 器名，因此如果此账号被禁用，将造成用户无法访问。

解决办法：控制面板一管理工具一计算机管理一本地用户和组，将 IUSR 机器名账号启用。

(2)错误现象二： HTTP 错误 401.2-未经授权：访问由于服务器配置被拒绝。

原因分析：

IIS 支持以下几种 Web 身份验证方法：

(1)匿名身份验证

IIS 创建 IUSRJ+算机名称账户（其中计算机名称是正在运行 IIS 的服务器的名称），用来在匿名用^请求 Web 内容时对他们进行身份验证。此账户授予用户本地登录权限。你可以将匿名用户访问重置为使用任何有效的 Windows 账户。

(2)基本身份验证

使用基本身份验证可限制对 NTFS 格式 Web 服务器上的文件的访问。使用基本身份验证，用户必须输入凭据，而且访问是基于用户 ID 的。用户 ID 和密码都以明文形式在网络间进行发

送。

(3) Windows 集成身份验证

Windows 集成身份验证比基本身份验证安全，而且在用户具有 Windows 域账户的内部网环境中能很好地发挥作用。在集成的 Windows 身份验证中，浏览器尝试使用当前用户在域登录过程中使用的凭据，如果尝试失败，就会提示该用户输入用户名和密码。如果你使用集成的 Windows 身份验证，则用户的密码将不传送到服务器。如果该用户作为域用户登录到本地计算机，则他在访问此域中的网络计算机时不必再次进行身份验证。

(4)摘要身份验证

摘要身份验证克服了基本身份验证的许多缺点。在使用摘要身份验证时，密码不是以明文形式发送的。另外，你可以通过代理服务器使用摘要身份验证。摘要身份验证使用一种挑战/响应机制（集成 Windows 身份验证使用的机制），其中的密码是以加密形式发送的。

(5) .NET Passport 身份验证

Microsoft .NET Passport 是一项用户身份验证服务，它允许单一签入安全性，可使用户在访问启用了 .NET Passport 的 Web 站点和服务时更加安全。启用了 .NET Passport 的站点会依靠.NET Passport 中央服务器来对用户进行身份验证。但是，该中心服务器不会授权或拒绝特定用户访问各个启用了 .NETPassport 的站点。

解决方法：

根据需要配置不同的身份认证（一般为匿名身份认证，这是大多数站点使用的认证方法）。认证选项在 IIS 的属性一安全性一身份验证和访问控制下配置。

试题四

【说明】

某企业网络结构如图 4-1 所示

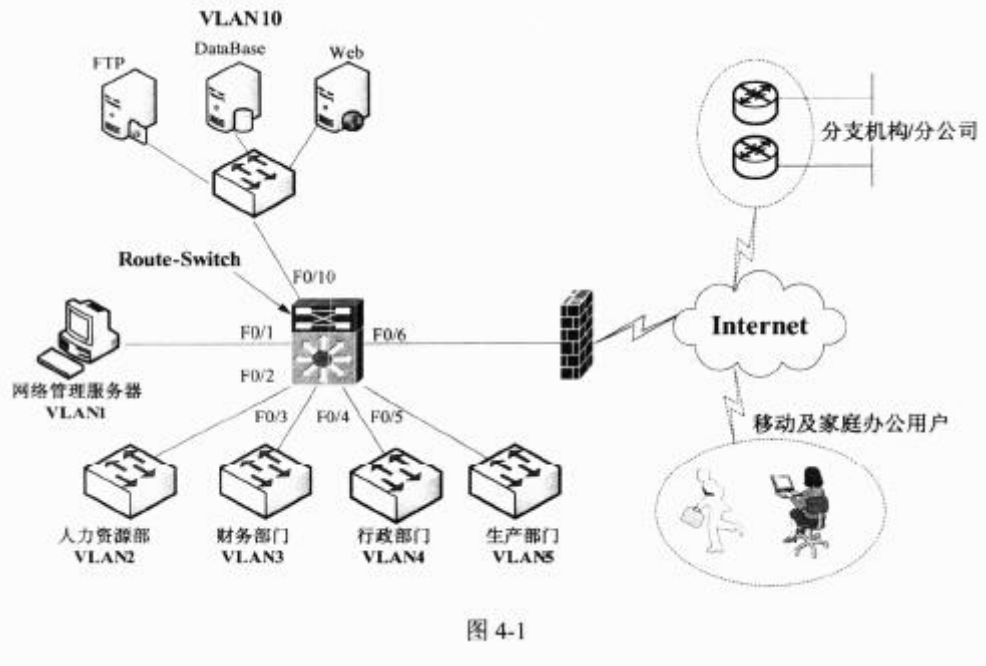


图 4-1

按照网络拓扑结构为该企业网络进行 IP 地址和 VLAN 规划，具体规划入表 4-1 所示。

表 4-1 网络规划地址表

VLAN	IP 地址分配	服务器	IP 地址分配
VLAN1（管理 VLAN）	192.168.100.0/24	网络管理服务器	192.168.100.10
VLAN2（人力资源部）	192.168.2.0/24	FTP 服务器	192.168.10.10
VLAN3（财务部门）	192.168.3.0/24	DataBase 服务器	192.168.10.20
VLAN4（行政部门）	192.168.4.0/24	Web 服务器	192.168.10.30
VLAN5（生产部门）	192.168.5.0/24		
VLAN10（内网服务器）	192.168.10.1/24		

【问题 1】

访问控制列表 ACL 可以通过编号或（1）来引用；ACL 分为两种类型，其中（2）ACL 只能根据源地址进行过滤，（3）ACL 使用源地址、目标地址、上层协议及协议信息进行过滤。

（1）名字

（2）标准

（3）扩展

本问题考查核心访问控制列表的基本知识。

访问控制列表（ACL)是最常用的网络流量限制技术，通过该技术可以为路由器或者交换机的接口配置一些控制命令，用来控制接口的进出数据包。配置 ACL 主要有两步，首先要指定访问控制条件，需要创建列表编号或者名称；然后在指定的列表编号或者名称内添加流量筛选条件，并指定是允许还是拒绝。

访问控制列表根据筛选条件不同，一般可以分为两种标准访问控制列表和扩展访问控制列表。其中标准访问控制列表只可以限定源地址的流量，通常使用 1～99 的列表编号。而扩展访问控制列表可以针对源地址、目标地址、传输层协议、源端口、目标端口等进行流量控制，通常使用 100～199 的列表编号。

【问题 2】

在网络使用中，该企业要求所有部门都可以访问 FTP 和 Web 服务器，只有财务部可以访问 DataBase 服务器；同时，网络管理员可以访问所有网络资源，禁止非网络管理员访问交换设备。根据需求，完成核心交换机 Route-Switch 以下配置命令。

```
Route-Switch(config)#access-list 101 permit ip host 192.168.100.10 any
Route-Switch(config)#access-list 101 permit tcp any host 192.168.10.10
eq ftp
Route-Switch(config)#access-list 101 _____(4)_____ eq www
//允许所有主机访问 Web 服务器
Route-Switch(config)#access-list 101 _____(5)_____
//允许财务部访问 DataBase 服务器
Route-Switch(config)#access-list 101 deny any any
Route-Switch(config)# int VLAN 10
Route-Switch(config-if)#ip access-group 101 in //在 VLAN10 的入方向应用 acl
101
Route-Switch(config)#access-list 102 deny any any
Route-Switch(config)# int VLAN 1
Route-Switch(config-if)#_____(6)_____
//禁止非网管员用户访问网络设备和网管服务器等
```

（4）permit tcp any host 192.168.10.30

（5）permit tcp 192.168.3.0 0.0.0.255 host192.168.10.20

（6）ip access-group 102 in

本问题考查核心交换机 Route-Switch 扩展访问控制列表的配置知识，主要用来配置各个 VLAN 主机对内网服务器的访问权限。

```
    Route-Switch(config)#access-list 101 permit ip host 192.168.100.10 any
    //允许网管服务器访问内网的所有主机
    Route-Switch(config)#access-list 101 permit tcp any host 192.168.10.10
eq ftp
    //允许所有主机访问 FTP 服务器 192.168.10.10 的 FTP 端口
    Route-Switch(config)#access-list 101 permit tcp any host 192.168.10.30
eq www
    //允许所有主机访问 Web 服务器 192.168.10.30 的 WWW 服务端口
    Route-Switch(config)#access-list 101 permit tcp 192.168.3.0 0.0.0.255 host
192.168.10.20
    //允许财务部网络 192.168.3.0/24 访问 DataBase 服务器
    Route-Switch(config)#access-list 101 deny any any
    Route-Switch(config)# int VLAN 10
    Route-Switch(config-if)#ip access-group 101 in
   //在 VLAN10 的入方向应用 acl 101
   Route-Switch(config)#access-list 102 deny any any
   Route-Switch(config)# int VLAN 1
   Route-Switch(config-if)# ip access-group 102 in
   //禁止非网管员用户访问网络设备和网管服务器等
   …
```

【问题 3】

企业员工访问互联网时，为了财务部的安全，必须限制财务部门的互联网访问请求；要求员工只能在周一至周五 08:00—18:00 和周末 08:00—12:00 这两个时间段访问互联网，根据要求完成（或解释）核心交换机 Route-Switch 的部分配置命令。

```
    Route-Switch(config)#time-range telnettime //定义时间范围
    Route-Switch(config-time-range)#periodic weekday ____(7)____
    //定制周期性执行时间为工作日的 08:00—18:00
    Route-Switch(config-time-range)#periodic weekend 08:00 to 12:00
    //____(8)____
    Route-Switch(config-time-range)#exit
    Route-Switch(config)#access-list 104 deny ip 192.168.3.0 0.0.0.255 any
    //____(9)____
    Route-Switch(config)#access-list 104 permit ip any any time-range
telnettime
    //应用访问控制时间，定义流量筛选条件
    Route-Switch(config)# int f0/6
    Route-Switch(config-if)#_____(10)_____
    //在接口 F0/6 的出方向应用 acl104 规则
```

（7）08:00 to18:00

（8）定制周期性执行检查周末的 8:00——12：00

（9）禁止财务部访问互联网

（10）ip access-group 104 out

本问题考查核心交换机 Route-Switch 定时访问控制列表的配置知识，主要用来设置互联网的访问权限。

```
Route-Switch(config)#time-range telnettime  //定义时间范围
Route-Switch(config-time-range)#periodic weekday 08:00 to 18:00
//定制周期性执行时间为工作日的 08:00—18:00
Route-Switch(config-time-range)#periodic weekend 08:00 to 12:00
//定制周期性执行时间为周末的 08:00—18:00
Route-Switch(config-time-range)#exit
Route-Switch(config)#access-list 104 deny ip 192.168.3.0 0.0.0.255 any
//禁止财务部访问互联网
Route-Switch(config)#access-list  104  permit  ip  any  any  time-range
telnettime
//应用访问控制时间，定义流量筛选条件
Route-Switch(config)# int f0/6
Route-Switch(config-if)# ip access-group 104 out
//在接口 F0/6 的出方向应用 acl104 规则
```

【问题 4】

随着企业的不断扩大，企业新建了很多分支机构，为了满足各地新建分支机构和移动办公人员使用企业网络的需求，比较经济快捷的做法是选择 VPN 技术来实现这种需求。该技术根据连接主体的不同，针对移动办公用户和家庭用户可以采用的连接方式为（11）连接方式，针对分支机构长期性的使用可以采用（12）连接方式。

（11）远程访问的 VPN

（12）站点到站点的 VPN

本问题考查 VPN，即虚拟专用网的基础知识。

VPN 技术用于实现局域网络之间通过 Internet 公共网络安全地传递数据。VPN 技术根据两端的连接主体不同，可以分为远程访问的 VPN 和站点到站点的 VPN。

远程访问的 VPN 适用于建立临时性的 VPN 连接，家庭和移动办公用户使用的比较多。只需要企业网络中配置有软件或者硬件形式的 VPN 设备，家庭和移动办公用户就可以通过自己的客户端直接建立 VPN 连接请求。

站点到站点的 VPN 连接可以建立长期的 VPN 连接，适合公司总部和子公司之间长期进行数据传输。需要两端网络中都有配置好的 VPN 软件程序或硬件设备，并且有匹配的认证加密配置。