假设系统中有n个进程共享3台打印机，任一进程在任一时刻最多只能使用1台打印机。若用PV操作控制n个进程使用打印机，则相应信号量S的取值范围为（1）；若信号量S的值为-3，则系统中有（2）个进程等待使用打印机。

(1)A.0，-1，…，-(n-1)　　B.3，2，1，0，-1，…，-(n-3)

C.1，0，-1，•••,-(n-1)　　D.2，1，0，-1，•••,-(n-2)

(2)A.0　　B.1　　C.2　　D.3

【答案】B　D

【解析】本题考查操作系统进程管理方面的基础知识。

根据题意假设系统中有n个进程共享3台打印机，意味着每次只允许3个进程进入互斥段，那么信号量的初值应为3。可见，根据排除法只有选项B中含有3。

信号量S的物理意义为：当S≥0时，表示资源的可用数；当S<0时，其绝对值表示等待资源的进程数。

CRM是一套先进的管理思想及技术手段，它通过将（3）进行有效的整合，最终为企业涉及到的各个领域提供了集成环境。CRM系统的四个主要模块包括（4）。

(3)A.员工资源、客户资源与管理技术　　B.销售资源、信息资源与商业智能

C.销售管理、市场管理与服务管理　　D.人力资源、业务流程与专业技术

(4)A.电子商务支持、呼叫中心、移动设备支持、数据分析

B.信息分析、网络应用支持、客户信息仓库、工作流集成

C.销售自动化、营销自动化、客户服务与支持、商业智能

D.销售管理、市场管理、服务管理、现场服务管理

【答案】D　C

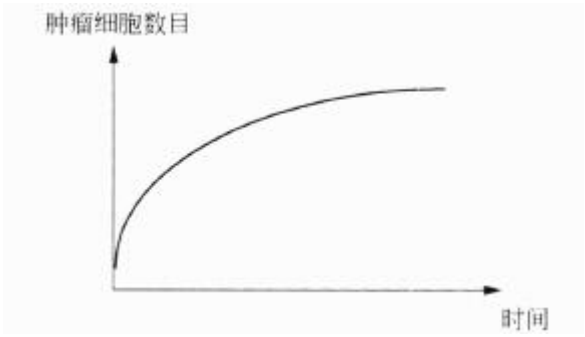
【解析】本题考杏企业信息化的基本知识。

CRM是一套先进的管理思想及技术手段，它通过将人力资源、业务流程与专业技术进行有效的整合，最终为企业涉及到客户或者消费者的各个领域提供了完美的集成，使得企业可以更低成本、更高效率地满足客户的需求，并与客户建立起基于学习，生关系基础上的一对一营销模式，从而让企业可以最大程度提高客户满意度和忠诚度。CRM系统的主要模块包括销售自动化、营销自动化、客户服务与支持、商业智能。

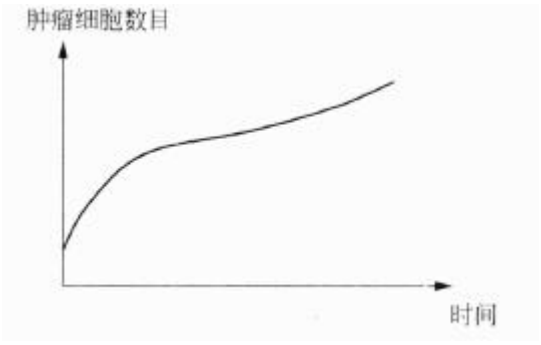
研究表明，肿瘤的生长有以下规律：当肿瘤细胞数目超过1011时才是临床可观察的;在

肿瘤生长初期，几乎每隔一定时间就会观测到肿瘤细胞数量翻一番；在肿瘤生长后期，肿瘤细胞的数目趋向某个稳定值。为此，图(5)反映了肿瘤的生长趋势。

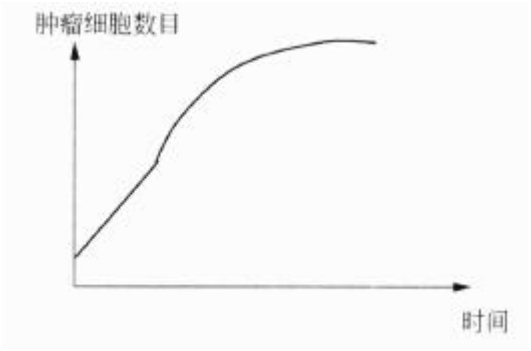
(5)A.



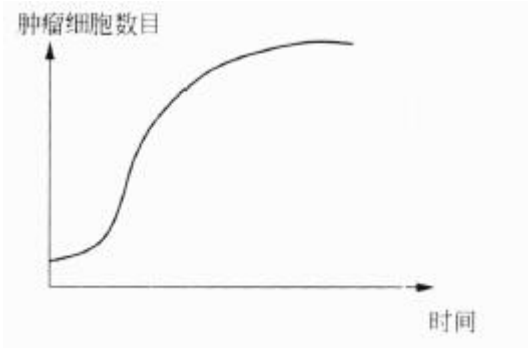
B.



C.



D.



【答案】D

【解析】本题考查应用数学基础知识。

用函数曲线来表示事物随时间变化的规律十分常见。可以用函数 f(t)表示肿瘤细胞数量随时间变化的函数。那么，当肿瘤细胞数目超过 1011 时才是临床可观察的，可以表示为

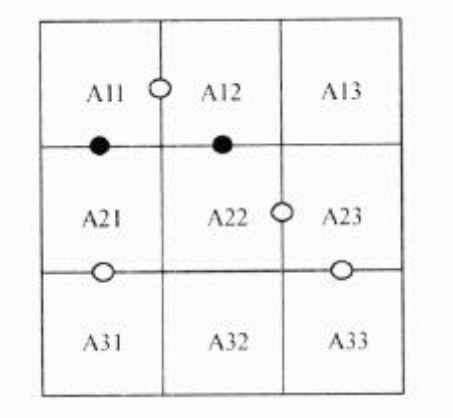
f(0)=1011。在肿瘤生长初期，几乎每隔一定时间就会观测到肿瘤细胞数量翻一番，可以表示为 t<t0 时，f(t+c)=2f(t)。符合这种规律的函数是指数函数：f(t)=at，其曲线段呈凹形上升态。在肿瘤生长后期，肿瘤细胞的数目趋向某个稳定值，表示当 P.T 时，f(t)逐渐逼近某个常数，即函数曲线从下往上逐渐靠近直线 y=L。

九个项目 A11,A12,A13,A21,A22,A23,A31,A32,A33 的成本从 1 百万，2 百万，……，到 9 百万各不相同，但并不顺序对应。已知 A11 与 A21、A12 与 A22 的成本都有一倍关系，A11 与 A12、A21 与 A31、A22 与 A23、A23 与 A33 的成本都相差 1 百万。由此可以推断，项目 A22 的成本是(6)百万。

(6)A.2　　B.4　　C.6　　D.8

【答案】C

【解析】本题考查应用数学基础知识。



九个项目 Aij(i=1,2,3；j=1,2,3)的成本值（单位为百万，从 1 到 9 各不相同)

将分别填入 i 行 j 列对应的格中。格间的黑点表示相邻格有一倍关系，白点表示相邻格相差 1。

已知 A22 与 A12 的值有一倍关系，那就只可能是 1-2，2-4，3-6 或 4-8,因此 A22 的值只可能是 1，2,3,4,6,8。

如果 A22=1，则 A23=A12=2，出现相同值，不符合题意。

如果 A22=2，则 A12 只能是 4(A12=1 将导致 A11=A22=2 矛盾)，A23 只能为 3:A23=1 将导致 A33=A22=2 矛盾)，A33 出现矛盾。

如果 A22=3，则 A12=6，A11=5 或 7，不可能与 A21 有一倍关系。

如果 A22=4,则 A12=2 或 8。A12=8 将导致 A11=7 或 9,不可能与 A21 有成倍关系。因此 A12=2，

A23 只能是 5(A23=3 将导致 A33 矛盾)，A33=6,而 A11=1 或 3 都将导致 A21 矛盾。

如果 A22=8，则 A12=4,A23 只能是 7(A23=9 将导致 A33=8 矛盾)，A33 只能是 6,A11 只能是 3(A11=5 将导致 A21 矛盾)，A21=6 矛盾。

因此，A22 只可能为 6。

实际上，当 A22=6 时，A12=3,A23 只能为 7(A23=5 将最终导致矛盾)，A33=8。此时，A11、A21、A31 可能分别是 2、4、5，也可能是 4、2、1。

以下关于软件生存周期模型的叙述，正确的是（7）。

(7)A.在瀑布模型中，前一个阶段的错误和疏漏会隐蔽地带到后一个阶段

B.在任何情况下使用演化模型，都能在一定周期内由原型演化到最终产品

C.软件生存周期模型的主要目标是为了加快软件开发的速度

D.当一个软件系统的生存周期结束之后，它就进入到一个新的生存周期模型

【答案】A

【解析】

软件产品从形成概念开始，经过开发、使用和维护，直到最后退役的全过程成为软件生存周期。一个完整的软件生存周期是以需求为出发点，从提出软件开发计划的那一刻开始，直到软件在实际应用中完全报废为止。软件生存周期的提出了是为了更好地管理、维护和升级软件，其中更大的意义在于管理软件开发的步骤和方法。

软件生存周期模型又称软件开发模型（softwaredevelopmodel)或软件过程模型(softwareprocessmodel),它是从某个特定角度提出的软件过程的简化描述。软件生存周期模型主要有瀑布模型、演化模型、原型模型、螺旋模型喷泉模型和基于可重用构件的模型等。瀑布模型是最早使用的软件生存周期模型之一。瀑布模型的特点是因果关系紧密相连，前一个阶段工作的结果是后一个阶段工作的输入。或者说，每一个阶段都逛建立在前一个阶段的正确结果之上，前一个阶段的错误和疏漏会隐蔽地带入后一个阶段。这种错误有时甚至可能是灾难性的，因此每一个阶段工作完成后，都要进行审查和确认。

演化模型主要针对事先不能完整定义需求的软件开发,是在快速开发一个原型的基础上,根据用户在调用原型的过程中提出的反馈意见和建议,对原型进行改进,获得原型的新版本,重复这--过程，直到演化成最终的软件产品。演化模型的主要优点是，任何功能一经开发就能进入测试，以便验证是杏符合产品需求，可以帮助引导出高质量的产品要求。其主要缺点是，如果不控制地让用户接触开发中尚未稳定的功能，可能对开发人员及永固都会产生负面

的影响。

以下关于软件测试工具的叙述，错误的是（8）。

(8)A.静态测试工具可用于对软件需求、结构设计、详细设计和代码进行评审、走查和审查

B.静态测试工具可对软件的复杂度分析、数据流分析、控制流分析和接口分析提供支持

C.动态测试工具可用于软件的覆盖分析和性能分析

D.动态测试工具不支持软件的仿真测试和变异测试

【答案】D

【解析】

测试工具根据工作原理不同可分为静态测试工具和动态测试工具。其中静态测试工具是对代码进行语法扫描，找到不符合编码规范的地方，根据某种质量模型评价代码的质量，生成系统的调用关系图等。它直接对代码进行分析，不需要运行代码，也不需要对代码编译链接和生成可执行文件，静态测试工具可用于对软件需求、结构设计、详细设计和代码进行评审、走审和审查，也可用于对软件的复杂度分析、数据流分析、控制流分析和接口分析提供支持；动态测试工具与静态测试工具不同，它需要运行被测试系统，并设置探针，向代码生成的可执行文件中插入检测代码，可用于软件的覆盖分析和性能分析，也可用于软件的模拟、建模、仿真测试和变异测试等。

企业信息化程度是国家信息化建设的基础和关键，企业信息化方法不包括(9)。

(9)A.业务流程重组　　B.组织机构变革　　C.供应链管理　　D.人力资本投资

【答案】B

【解析】本题考查企业信息化的基本方法。

企业信息化程度是国家信息化建设的基础和关键，企业信息化就是企业利用现代信息技术，通过信息资源的深入开发和广泛利用，实现企业生产过程的自动化、管理方式的网络化、决策支持的智能化和商务运营的电子化，不断提高生产、经营、管埋、决策的效率和水平，进而提高企业经济效益和企业竞争力的过程。企业信息化方法主要包括业务流程重构、核心业务应用、信息系统建设、主题数据库、资源管理和人力资本投资方法。企业战略规划是指依据企业外部环境和自身条件的状况及其变化来制定和实施战略，并根据对实施过程与结果

的评价和反馈来调整，制定新战略的过程。

中国 M 公司与美国 L 公司分别在各自生产的平板电脑产品上使用 iPad 商标，且分别享有各自国家批准的商标专用权。中国 Y 手电筒经销商，在其经销的手电筒高端产品上也使用 iPad 商标，并取得了注册商标。以下说法正确的是（10）。

(10)A.L 公司未经 M 公司许可在中国市场销售其产品不属于侵权行为

B.L 公司在中国市场销售其产品需要取得 M 公司和 Y 经销商的许可

C.L 公司在中国市场销售其产品需要向 M 公司支付注册商标许可使用费

D.Y 经销商在其经销的手电筒高端产品上使用 iPad 商标属于侵权行为

【答案】C

【解析】本题考查知识产权知识，涉及商标权的相关概念。

知识产权具有地域性的特征，按照一国法律获得承认和保护的知识产权，只能在该国发生法律效力，即知识产权受地域限制，只有在一定地域内知识产权才具有独占性（专用性）。或者说，各国依照其本国法律授予的知识产权，只能在其本国领域内受其国家的法律保护，而其他国家对这种权利没有保护的义务，任何人均可在自己的国家内自由使用外国人的知识产品，既无须取得权利人的许可，也不必向权利人支付报酬。

通过缔结有关知识产权的国际公约的形式，某一国家的国民（自然人或法人）的知识产权在其他国家也能取得权益。参加知识产权国际公约的国家，会相互给予成员国国民的知识产权保护。虽然众多知识产权国际条约等的订立，使地域性有时会变得模糊，但地域性的特征不但是知识产权最“古老”的特征，也是最基本的特征之一。&前知识产权的地域性仍然存在，如是否授予权利、如何保护权利，仍须由各成员国按照其国内法来决定。依据我国商标法 52 条规定，未注册商标不得与他人在同一种或类似商品上已经注册的商标相同或近似。若未经商标注册人的许可，在同一种商品或者类似商品上使用与他人注册商标相同或者近似的商标的，属于侵犯专用权的行为，应当承担相应的法律责任。

知识产权的利用（行使）有多种方式，许可使用是其之一，它是指知识产权人将自己的权利以一定的方式，在一定的地域和期限内许可他人利用，并由此获得报酬（即向被许可人收取一定数额的使用费）的法律行为。对于注册商标许可而言是指注册商标所有人通过订立许可使用合同，许可他人使用其注册商标的法律行为。

依据我国商标法规定，不同类别商品（产品）是可以使用相同或类似商标的，如在水泥产品和化肥产品都可以使用“秦岭”商标，因为水泥产品和化肥产品是不同类别的产品。但

对于驰名商标来说，不能在任何商品（产品），使用与驰名商标相同或类似的标识。

在下面4个协议中，属于ISO OSI/RM标准第二层的是（11）。

(11)A.LAPB B.MHS C.X.21 D.X.25 PLP

【答案】A

【解析】

LAPB是X.25公用数据网中的数据链路层协议，实际上是HDLC的子集，采用了异步平衡通信方式。MHS是CCITT在X.400标准中定义的报文处理系统（Message Handling System），它是一种在广域网平台上运行的电子邮件系统。X.21是一种物理层接口标准，终端设备通过这种接口连接公用数据网。X.25PLP是公用数据网中的分组层协议，通过虚电路为数据终端提供面向连接的服务。

下面有关无连接通信的描述中，正确的是（12）。

(12)A.在无连接的通信中，目标地址信息必须加入到每个发送的分组中

B.在租用线路和线路交换网络中，不能传送UDP数据报

C.采用预先建立的专用通道传送，在通信期间不必进行任何有关连接的操作

D.由于对每个分组都要分别建立和释放连接，所以不适合大量数据的传送

【答案】A

【解析】

计算机网络为用户提供面向连接的服务和无连接的服务。面向连接的服务需要三个阶段：建立连接，数据传送和释放连接。无连接的服务没有建立连接和释放连接的开销，而是把目标地址直接加入到传送的报文中，通过逐段路由，最后转发到达目标。在TCP/IP网络中，TCP协议提供端到端的面向连接的数据传送服务，UDP提供端到端的无连接服务，IP协议在网络层提供无连接的数据报服务。在传输层和网络层提供什么类型的服务与底层协议和网络的基础设施没有关系。在逻辑上说，下层可以提供任何类型的服务，而上层则通过自己的功能实现面向连接或无连接的通信。所以在租用专线或线路交换网络中都可以实现UDP数据报的传送。

在PPP链路建立以后，接着要进行认证过程。首先由认证服务器发送一个质询报文，终端计算该报文的Hash值并把结果返回服务器，然后服务器把收到的Hash值与自己计算的

Hash 值进行比较以确定认证是否通过。在下面的协议中，采用这种认证方式的是(13)。

(13)A.CHAP B.ARP C.PAP D.PPTP

【答案】A

【解析】

PPP 扩展认证协议可支持多种认证机制，并且允许使用后端服务器来实现货杂的认证过程，例如通过 Radius 服务器进行 Web 认证时，远程访问服务器（RAS)只是作为认证服务器的代理传递请求和应答报文，并且当识别出认证成功/失败标志后结束认证过程。通常 PPP 支持的两个认证协议是：

口令验证协议（Password Authentication Protocol，PAP)：提供了一种简单的两次握手认证方法，由终端发送用户标识和口令字，等待服务器的应答，如果认证不成功，则终止连接。这种方法不安全，因为采用文本方式发送密码，可能会被第三方窃取；

质询握手认证协议（Challenge Handshake Authentication Protoccl,CHAP)：采用三次握手方式周期地验证对方的身份。首先是逻辑链路建立后认证服务器就要发送一个挑战报文（随机数），终端计算该报文的 Hash 值并把结果返回服务器，然后认证服务器把收到的 Hash 值与自己计算的 Hash 值进行比较，如果匹配，则认证通过，连接得以建立，否则连接被终止。计算 Hash 值的过程有一个双方共享的密钥参与，而密钥是不通过网络传送的，所以 CHAP 是更安全的认证机制。在后续的通信过程中，每经过一个随机的间隔，这个认证过程都可能被重复，以缩短入侵者进行持续攻击的时间。值得注意的是，这种方法可以进行双向身份认证，终端也可以向服务器进行挑战，使得双方都能确认对方身份的合法性。

下面有关 ITU-TX.25 建议的描述中，正确的是（14)。

(14)A.通过时分多路技术，帧内的每个时槽都预先分配给了各个终端

B.X.25 的网络层采用无连接的协议

C.X.25 网络采用 LAPD 协议进行数据链路控制

D.如果出现帧丢失故障，则通过顺序号触发差错恢复过程

【答案】D

【解析】

X.25 公共数据网 PDN(Public Data Network)是在一个国家或全球范围内提供公共电信服务的数据通信网。X.25 在数据路层采用 LAPB 协议，实际上是 HDLC 的子集，采用了异步平衡方式通信。X.25 的网络层提供面向连接的虚电路服务。有两种形式的虚电路：一种是

虚呼叫(VirtualCall.VC),一种是永久虚电路（Permanent Virtual Circuit,PVC)虚呼叫是动态建立的虚电路，包含呼叫建立、数据传送和呼叫清除等几个过程。永久虚电路是网络指定的固定虚电路，像专线一样，无需建立和释放连接，可直接传送数据。

无论是虚呼叫或是永久虚电路，都是由几条虚拟连接共享一条物理信道。一对分组交换机之间至少有一条物理链路，几条虚电路可以共享该物理链路。每一条虚电路由相邻结点之间的一对缓冲区实现，这些缓冲区被分配给不同的虚电路号以示区别。建立虚电路的过程就是在沿线各结点上分配缓冲区和虚电路号的过程。

通过预先建立的虚电路通信，可以进行端到端的流量和差错控制。X.25 分组头中带有发送顺序号和应答顺序号。如果出现差错，则可以通过顺序号进行纠正。

使用海明码进行纠错，7 位码长(x1,x2,x3,x4,x5,x6,x7)其中 4 位数据位，3 位校验位，其监督关系式为

$$c_0 = x_1 + x_3 + x_5 + x_7$$
$$c_1 = x_2 + x_3 + x_6 + x_7$$
$$c_2 = x_4 + x_5 + x_6 + x_7$$

如果收到的码字为 1000101，则纠错后的码字是（15）。

(15)A.1000001　　B.1001101　　C.1010101　　D.1000101

【答案】C

【解析】

如果收到的码字为 1000101，根据监督关系式计算得到 c2c1c0=011，可知错误在第 3 位，则纠错后得到正确的码字为 1010101。

虚拟局域网中继协议（VTP)有三种工作模式，即服务器模式、客户机模式和透明模式，以下关于这 3 种工作模式的叙述中，不正确的是（16）。

(16)A.在服务器模式可以设置 VLAN 信息

B.在服务器模式下可以广播 VLAN 配置信息

C.在客户机模式下不可以设置 VLAN 信息

D.在透明模式下不可以设置 VLAN 信息

【答案】D

【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 帧，但是并不能据此更新自己的 VLAN 配置，只是起到通路的作用。

VTP 协议的优点有：

(1) 提供通过一个交换机在整个管理域中配置 VLAN 的方法；

(2) 提供跨不同介质类型（如 ATM、FDDI 和以太网）配置 VLAN 的方法；

(3) 提供跟踪和监视 VLAN 配置的方法；

(4) 保持 VLAN 配置的一致性。

千兆以太网标准 802.3Z 定义了一种帧突发方式，这种方式是指（17）

(17)A.一个站可以突然发送一个帧　　B.一个站可以不经过竞争就启动发送过程

C.一个站可以连续发送多个帧　　D.一个站可以随机地发送紧急数据

【答案】C

【解析】

1996 年 3 月 IEEE 成立了 802.3z 工作组，开始制定 1000Mb/s 以太网标桂。后来又成立了有 100 多家公司参加的千兆以太网联盟 GEA(Gibabit Ethernet Alliance)，支持 IEEE802.3z 工作组的各项活动。1998 年 6 月公布的 IEEE802.3z 和 1999 年 6 月公布的 IEEE802.3ab 已经成为千兆以太网的正式标准。实现千兆数据速率需要采用新的数据处理技术。首先是最小帧长需要扩展，以便在半双工的情况下增加跨距。另外 802.32 还定义了一种帧突发方式（frame bursting),使得一个站可以连续发送多个帧。最后吻理层编码也采用

了与 10Mb/s 不同的编码方法，即 4b/5b 或 8b/9b 编码法。

以太网最大传输单元（MTU)为 1500 字节。以太帧包含前导（preamble)、目标地址、源地址、协议类型、CRC 等字段，共计 26 个字节的开销。假定 IP 头长为 20 字节，TCP 头长为 20 字节，则 TCP 数据最大为（18）字节。

(18)A.1434　　B.1460　　C.1480　　D.1500

【答案】B

【解析】

由于以太网 MTU 为 1500 字节，从中减去 IP 头 20 个字节和 TCP 头 20 个字节，则允许的 TCP 数据最多为 1460 个字节。

以下关于网络控制的叙述，正确的是（19）。

(19)A.由于 TCP 的窗口大小是固定的，所以防止拥塞的方法只能是超时重发

B.在前向纠错系统中，当接收端检测到错误后就要请求发送端重发出错分组

C.在滑动窗口协议中，窗口的大小以及确认应答使得可以连续发送多个数据

D.在数据报系统中，所有连续发送的数据都可以沿着预先建立的虚通路传送

【答案】C

【解析】

TCP 采用可变大小的滑动窗口协议进行流量控制。在前向纠错系统干，当接收瑞检测到错误后就根据纠错编码的规律自行纠错；在后向纠错系统中，接收方会请求发送方重发出错分组。IP 协议不预先建立虚电路，而是对每个数据报独立地选择路由并一站一站地进行转发，直到送达目标地。

IETF 定义的多协议标记交换（MPLS)是一种第三层交换技术。MPLS 网络由具有 IP 功能、并能执行标记分发协议（LDP)的路由器组成。负责为网络流添加和删除标记的是（20）。

(20)A.标记分发路由器　　B.标记边缘路由器

C.标记交换路由器　　D.标记传送路由器

【答案】B

【解析】

IETF 开发的多协议标记交换 MPLS(Multiprotocol Label Switching)把第 2 层的链路状

态信息（带宽、延迟、利用率等）集成到第3层的协议数据单元中，从而简化和改进了第3层分组的交换过程。理论上，MPLS支持任何第2层和第3层协议。MPLS包头的位置界于第2层和第3层之间，可称为第2.5层。MPLS可以承载的报文通常是IP包，当然也可以直接承载以太帧、AAL5包、甚至ATM信元等。可以承载MPLS的第2层协议可以是PPP、以太帧、ATM和帧中继等。

当分组进入MPLS网络时，标记边缘路由器（Label Edge Router,LER)就为其加上一个标记，这种标记不仅包含了路由表项中的信息（目标地址、带宽、延迟等），而且还引用了IP头中的源地址字段、传输层端口号、服务质量等。这种分类一旦建立，分组就被指定到对应的标记交换通路（Label Switch Path,LSP)中，标记交换路由器（Label Switch Router,LSR)将根据标记来处置分组，不再经过第3层转发，从而加快了网络的传输速度。

HDLC是一种(21)协议，它所采用的流量控制技术是(22)。

(21)A.面向比特的同步链路控制　　B.面向字节计数的异步链路控制

C.面向字符的同步链路控制　　D.面向比特流的异步链路控制

(22)A.固定大小的滑动窗口协议　　B.可变大小的活动窗口协议

C.停等协议　　D.令牌控制协议

【答案】A　A

【解析】

数据链路控制协议可分为两大类：面向字符的协议和面向比特的协议。面向字符的协议以字符作为传输的基本单位，用10个专用字符（例如STX、ETX、ACK、NAK等）控制传输过程。面向比特的协议以比特作为传输的基本单位，它的传输效率高，能适应计算机通信技术的最新发展，已广泛应用于公用数据网中。面向比特的同步链路控制协议HDLC是国际标准化组织（ISO)根据IBM公司的SDLC(Synchronous Data Link Control)协议扩充开发而成的。HDLC协议采用固定大小的滑动窗口协议实现链路两端的流量和差错控制。

ADSL采用(23)技术在一对铜线上划分出多个信道，分别传输上行和下行数据以及话音信号。ADSL传输的最大距离可达(24)米。

(23)A.时分多路　B.频分多路　C.波分多路　D.码分多址

(24)A.500　B.1000　C.5000　D.10000

【答案】B　C

【解析】

ADSL 采用频分多路复用技术在一对铜线上划分出多个信道，分别传输上行和下行数据以及话音信号。支持上行速率 640Kb/s～IMb/s、下行速率 IMb/s～8Mb/s，有效传输距离在 3～5 公里范围以内，同时还可以提供话音服务。可以满足网上冲浪和视频点播等应用对带宽的要求。

按照网络分级设计模型，通常把局域网设计为 3 层，即核心层、汇聚层和接入层，以下关于分级网络功能的描述中，不正确的是(25)。

(25)A.核心层承担访问控制列表检查　　B.汇聚层定义了网络的访问策略

C.接入层提供网络接入功能　　D.在接入层可以使用集线器代替交换机

【答案】A

【解析】

层次型局域网结构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，层次结构的特点如下：

(1) 网络功能划分清晰，有利发挥联网设备的最大效率；

(2) 网络拓扑结构使得故障定位可分级进行，便于维护；

(3) 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。

①核心层设计要点

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。

②汇聚层设计要点

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，或者运行了八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。

③接入层设计要点

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。

在距离矢量路由协议中，防止路由循环的方法通常有以下三种：(26)。

(26)A.水平分裂、垂直翻转、设置最大度量值

B.水平分裂、设置最大度量值、反向路由中毒

C.垂直翻转、设置最大度量值、反向路由中毒

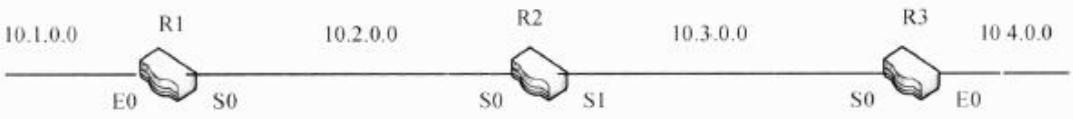
D.水平分裂、垂直翻转、反向路由中毒

【答案】B

【解析】

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

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



R1路由表

10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

R2路由表

10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

R3路由表

10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

解决路由环路问题可以采用水平分割法（Split Horizon)。这种方法规定，路由器必须有选择地将路由表中的信息发送给邻居，而不是发送整个路由表。具体地说，一条路由信息不会被发送给该信息的来源。可以对上图中 R2 的路由表项将加上一些注释，这样，每一条路由信息都不会通过其来源接口向回发送，就可以避免环路的产生。

R2 路由表

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

简单的水平分割方案是:“不能把从邻居学习到的路由发送给那个邻居”，带有反向毒化的水平分割方案（Split Horizon with Poisoned Reverse)是:“把从邻居学习到的路由费用设置为无限大，并立即发送给那个邻居”。采用反向毒化的方案更安全一些，它可以立即中断环路。相反，简单水平分割方案则必须等待一个更新周期才能中断环路的形成过程。另外，采用触发更新技术也能加快路由收敛，如果触发更新足够及时——路由器 R3 在接收 R2 的更新报文之前把网络 10.4.0.0 的故障告诉 R2，则也可以防止环路的形成。

以下关于 OSPF 协议的说法中，正确的是(27)。

(27)A.OSPF 是一种应用于不同自治系统之间外部网关协议

B.OSPF 是基于相邻结点的负载来计算最佳路由

C.在 OSPF 网络中，不能根据网络的操作状态动态改变路由

D.在 OSPF 网络中，根据链路状态算法确定最佳路由

【答案】D

【解析】

OSPF(Open Shortest Path First)是一种内部网关协议，用于在自治系统内进行路由决策。OSPF 是链路状态协议，通过路由器之间通告链路的状态来建立链路状态数据库，根据链路状态算法确定最佳路由，并构造路由表。

OSPF 网络是分层次的，把自治系统内部分为多个区域（Area),每一个区域有它自己的链路状态数据库和拓扑结构图，区域内部的路由器共享相同的路由信息。具有多个接口的路由器可以连接多个区域，这种路由器称为区域边缘路由器，它要为每个相连的区域分别保存一份链路状态数据库。

区域的划分产生了两类不同的 OSPF 路由，区别在于源和目的是在同一区域还是不同的区域，分别称为区域内路由和跨区域路由。

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

OSPF 路由器启动后以固定的时间间隔泛洪传播 Hello 报文，采用目标地址 224.0.0.5 代表所有的 OSPF 路由器。在点对点网络上每 10 秒发送一次，在 NBMA 网络中每 30 秒发送一次。管理 Hello 报文交换的规则称为 Hello 协议。Hello 协议用于发现祁居，建立毗邻关系，还用于选举区域内的指定路由器 DR 和备份指定路由器 BDR。

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

以下关于外部网关协议 BGP4 的说法，错误的是(28)。

(28)A.BGP4 是一种路径矢量路由协议　　B.BGP4 通过 UDP 传输路由信息

C.BGP4 支持路由汇聚功能　　D.BGP4 能够检测路由循环

【答案】B

【解析】

外部网关协议 BGP4 已经广泛地应用于不同 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 报文通过 TCP(179 端口）连接传送。

BGP 是一种路径矢量路由协议,BGP 路由器之间传送的路由信息由一个目标地址前缀后随一串 AS 编号组成，通过检测路径中是否出现本地 AS 编号可以发现路由循环。BGP 路由器根据收到的各个路径矢量和预订的管理策略，选择到达目标的最短通路，可见 BGP 与 RIP 协议的算法是相似的。

与 HTTP1.0 相比，HTTP1.1 最大的改进在于(29)。

(29)A.进行状态保存　　B.支持持久连接　　C.采用 UDP 连接　　D.提高安全性

【答案】B

【解析】本题考查 HTTP 协议及相关技术。

HTTP1.0 协议使用非持久连接，在非持久连接下，一个 TCP 连接只传输一个 Web 对象。HTTP/L1 默认使用持久连接(HTTP/1.1 协议的客户机和服务器可以配置成使用非持久连接)，在持久连接下，不必为每个 Web 对象的传送建立一个新的连接，一个连接中可以传输多个对象。

网管中心在进行服务器部署时应充分考虑到功能、服务提供对象、流量、安全等因素。某网络需要提供的服务包括 VOD 服务、网络流量监控服务以及可对外提供的 Web 服务和邮件服务。在对以上服务器进行部署过程中，VOD 服务器部署在(30)：Web 服务器部署在 (31)；流量监控器部署在(32)，这四种服务器中通常发出数据流量最大的是(33)。

(30)A.核心交换机端口　　B.核心交换机镜像端口

C.汇聚交换机端口　　D.防火墙 DMZ 端口

(31)A.核心交换机端口　　B.核心交换机镜像端口

C.汇聚交换机端口　　D.防火墙 DMZ 端口

(32)A.核心交换机端口　　B.核心交换机镜像端口

C.汇聚交换机端口　　D.防火墙 DMZ 端口

(33)A.VOD 服务器　　B.网络流量监控服务器

C.Web 服务器　　D.邮件服务器

【答案】A　D　B　A

【解析】本题考查服务器部署及相关技术。

在进行服务器部署时，应充分考虑到功能，服务提供对象，流量、安全等因素。VOD 服务器流量较大，应部署在核心交换机端口。Web 服务器需对外提供服务，一般部署在防火墙

DMZ 端口。网络流量监控需要监听交换网络中所有流量，但是通过普通交换机端口去获取这些流量有相当大的困难，因此需要通过配置交换机来把一个或多个端口(VLAN)的数据转发到某一个端口来实现对网络的监听，这个端口就是镜像端口，而网络流量监控服务器需要部署在镜像端口。

可提供域名服务的包括本地缓存、本地域名服务器、权限域名服务器、顶级域名服务器以及根域名服务器等，以下说法中错误的是（34）

(34)A.本地缓存域名服务不需要域名数据库

B.顶级域名服务器是最高层次的域名服务器

C.本地域名服务器可以采用递归查询和迭代查询两种查询方式

D.权限域名服务器负责将其管辖区内的主机域名转换为该主机的 IP 地址

【答案】B

【解析】本题考查域名服务器及相关技术。

可提供域名服务的包括本地缓存、本地域名服务器、权限域名服务器、顶级域名服务器以及根域名服务器。DNS 主机名解析的查找顺序是，先查找客户端本地缓存；如果没有成功，则向 DNS 服务器发出解析请求。

本地缓存是内存中的一块区域，保存着最近被解析的主机名及其 IP 地址映像。由于解析程序缓存常驻内存中，所以比其他解析方法速度快。

当一个主机发出 DNS 查询报文时，这个查询报文就首先被送往该主机的本地域名服务器。本地域名服务器离用户较近，当所要查询的主机也属于同一个本地 ISP 时，该本地域名服务器立即就能将所查询的主机名转换为它的 1P 地址，而不需要再去询问其他的域名服务器。每一个区都设置有域名服务器，即权限服务器，它负责将其管辖区内的主机域名转换为该主机的 IP 地址。在其上保存有所管辖区内的所有主机域名到 IP 地址的映射。

顶级域名服务器负责管理在本顶级域名服务器上注册的所有二级域名。当收到 DNS 查询请求时，能够将其管辖的二级域名转换为该二级域名的 IP 地址。或者是下一步应该找寻的域名服务器的 IP 地址。

根域名服务器是最高层次的域名服务器。每一个根域名服务器都要存有所有顶级域名服务器的 IP 地址和域名。当一个本地域名服务器对一个域名无法解析时，就会直接找到根域名服务器，然后根域名服务器会告知它应该去找哪一个顶级域名服务器进厅查询。

在 RMON 管理信息库中，矩阵组存储的信息是（35），警报组的作用是（36）。

(35)A.一对主机之间建立的 TCP 连接数　　B.一对主机之间交换的字节数

C.一对主机之间交换的 IP 分组数　　D.一对主机之间发生的冲突次数

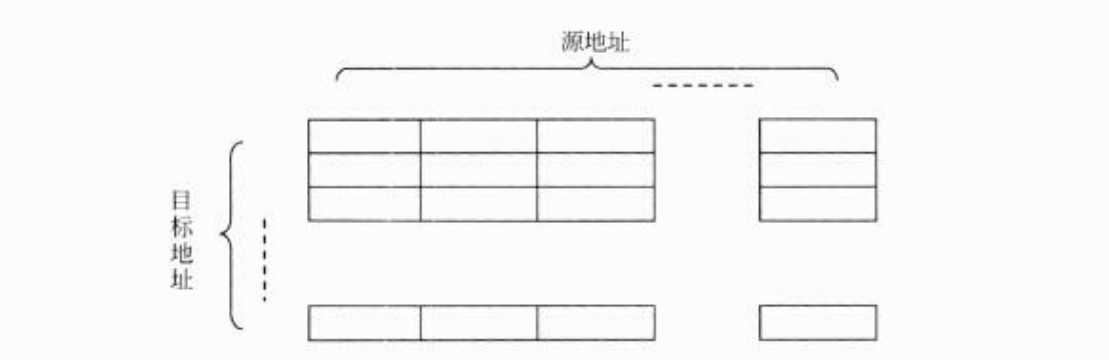
(36)A.定义了一组网络性能门限值　　B.定义了网络报警的紧急程度

C.定义了网络故障的处理方法　　D.定义了网络报警的受理机构

【答案】B　A

【解析】

矩阵组记录了子网中一对主机之间的通信量，信息以矩阵的形式存储，如下图所示。



如果监视器在某个接口上发现了一对主机会话，则在该表中记录两行，每行表示一个方向的通信量。这样，管理站可以检索到一个主机向其他主机发送的信息，也容易检索到其他主机向某一个主机发送的信息。

RMON 报警组定义了一组有关网络性能的门限值，超过门限值时向控制台产生报警事件。报警组由一个表组成，该表的一行定义了一种报警：监视的变量、采样区间和门限值。

设有下面 4 条路由：172.118.129.0/24、172.118.130.0/24、172.118.132.0/24 和 172.118.133.0/24，如果进行路由汇聚，能覆盖这 4 条路由的地址是（37）。

(37)A.172.118.128.0/21　　B.172.118.128.0/22

C.172.118.130.0/22　　D.172.118.132.0/20

【答案】A

【解析】

地址 172.118.129.0/24 的二进制形式为 10101100 01110110 10000001 00000000

地址 172.118.130.0/24 的二进制形式为 10101100 01110110 10000010 00000000

地址 172.118.132.0/24 的二进制形式为 10101100 01110110 10000100 00000000

地址 172.118.133.0/24 的二进制形式为 10101100 01110110 10000101 00000000

地址 172.118.128.0/21 的二进制形式为 10101100 01110110 10000000 00000000

所以能覆盖这 4 条路由的地址是 172.118.128.0/21 。

属于网络 202.117.200.0/21 的地址是（38）

(38)A.202.117.198.0　　B.202.117.206.0

C.202.117.217.0　　D.202.117.224.0

【答案】B

【解析】

地址 202.117.200.0/21 的二进制形式为：11001010011101011100100000000000 。

202.117.198.0 的二进制形式为：11001010011101011100011000000000。

202.117.206.0 的二进制形式为：11001010011101011100111000000000。

202.117.217.0 的二进制形式为：11001010011101011101000100000000。

202.117.224.0 的二进制形式为：11001010011101011110000000000000。

可以看出 202.117.206.0 属于网络 202.117.200.0/21 。

下面的地址中，属于单播地址的是（39）。

(39)A.172.31.128.255/18　　B.10.255.255.255

C.172.160.24.59/30　　D.224.105.5.211

【答案】A

【解析】

地址 172.31.128.255/18 的二进制形式是 10101100000011111100000011111111

可见是一个单播地址。

地址 10.255.255.255 是 A 类网络定向广播地址。

地址 172.160.24.59/30 的二进制形式是 10101100101000000001100000111011

可见是一个广播地址。

地址 224.105.5.211D 类组播地址。

在 IPv6 中，地址类型是由格式前缀来区分的。IPv6 可聚合全球单播地址的格式前缀是(40)。

(40)A.001 B.1111 111010 C.1111111011 D.11111111

【答案】A

【解析】

IPv6地址的格式前缀（Format PrefiX，FP)用于表示地址类型或子网地址，用类似于IPv4 CIDR的方法可表示为“IPv6地址/前缀长度”的形式。例如60位的池址前缀12AB00000000CD3有下列几种合法的表示形式：

12AB:0000:0000:CD30:0000:0000:0000:0000/60

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

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

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。

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
为NSAP地址保留	0000 001	1/128
为IPX地址保留	0000 010	1/128
未分配	0000 011	1/128
未分配	0000 1	1/32
未分配	0001	1/16
可聚合全球单播地址	001	1/8
未分配	010	1/8
未分配	011	1/8
未分配	100	1/8
未分配	101	1/8
未分配	110	1/8
未分配	1110	1/16
未分配	1111 0	1/32
未分配	1111 10	1/64
未分配	1111 110	1/128
未分配	1111 1110 0	1/512
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

SSL包含的主要子协议是记录协议(41)。

(41)A.AH协议和ESP协议 B.AH协议和握手协议

C.警告协议和ESP协议 D.警告协议和握手协议

【答案】D

【解析】本题考查网络安全方面关于安全协议 SSL 的基础知识。

SSL 协议主要包括记录协议、警告协议和握手协议。

记录协议用于在客户机和服务器之间交换应用数据；告警协议用来为对等实体传递 SSL 的相关警告。用于标示在什么时候发生了错误或两个主机之间的会话在什么时候终止；握手协议用于产生会话状态的密码参数，允许服务器和客户机相互验证、协商加密和 MAC 算法及秘密密钥，用来保护在 SSL 记录中传送的数据。

SET 安全电子交易的整个过程不包括 (42) 阶段。

(42)A.持卡人和商家匹配　　B.持卡人和商家注册

C.购买请求　　D.付款授权和付款结算

【答案】A

【解析】本题考查网络安全方面关于安全协议 SET 的基础知识。

SET 安全电子交易的整个过程大体可分为以下几个阶段：持卡人注册、商家注册、购买请求、付款授权和付款结算。

下列访问控制模型中，对象的访问权限可以随着执行任务的上下文环境发生变化的是 (43) 的控制模型。

(43)A.基于角色　　B.基于任务　　C.基于对象　　D.强制型

【答案】B

【解析】本题考查网络安全方面关于访问控制模型的基础知识。

强制型访问控制（MAC)模型是一种多级访问控制策略，它的主要特点是系统对访问主体和受控对象实行强制访问控制，系统事先给访问主体和受控对象分配不同的安全级别属性，在实施访问控制时，系统先对访问主体和受控对象的安全级别属性进行比较，再决定访问主体能否访问该受控对象。

基于角色的访问控制（RBAC Model,Role-based Access)：RBAC 模型的基本思想是将访问许可权分配给一定的角色，用户通过饰演不同的角色获得角色所拥有的访问许可权。

基于任务的访问控制模型（TBACModel，Task-basedAccessControlModel)是从应用和企业层角度来解决安全问题，以面向任务的观点，从任务（活动）的角度来建立安全模型和实现安全机制，在任务处理的过程中提供动态实时的安全管理。在 TBAC 中，对象的访问权限控制并不是静止不变的，而是随着执行任务的上下文环境发生变化。

基于对象的访问控制模型（OBAC Model:Object-based Access Control Model)中，将访问控制列表与受控对象或受控对象的属性相关联，并将访问控制选项设计成为用户、组或角色及其对应权限的集合；同时允许对策略和规则进行重用、继承和派生操作。

数字证书被撤销后存放于(44)。

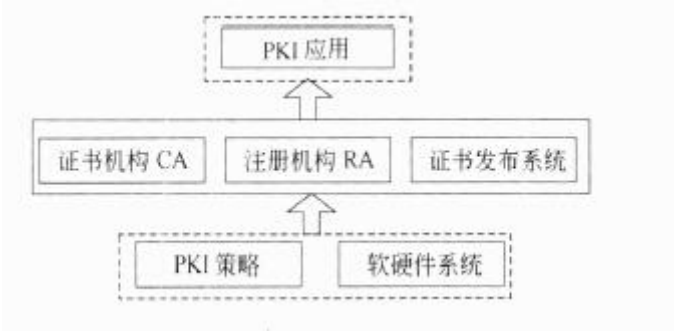
(44)A.CA　　B.CRL　　C.ACL　　D.RA

【答案】B

【解析】本题考查网络安全方面关于数字证书的基础知识。

CRL(Certificate Revocation List)的全称是证书撤销列表，用于保存被撤销的数字证书。

下图所示 PKI 系统结构中，负责生成和签署数字证书的是(45),负责验证用户身份的是(46)。



(45)A.证书机构 CA　　B.注册机构 RA　　C.证书发布系统　　D.PKI 策略

(46)A.证书机构 CA　　B.注册机构 RA　　C.证书发布系统　　D.PKI 策略

【答案】A　　B

【解析】本题考查网络安全方面关于 PKI 的基础知识。

在 PKI 系统体系中，证书机构 CA 负责生成和签署数字证书，注册机构 RA 负责验证申请数字证书用户的身份。

以下关于完美向前保护（PFS)的说法，错误的是(47)。

(47)A.PFS 的英文全称是 Perfect Forward Secrecy

B.PFS 是指即使攻击者破解了一个密钥，也只能还原这个密钥加密的数据，而不能还原其他的加密数据

C.IPSec 不支持 PFS

D.要实现 PFS 必须使用短暂的一次性密钥

【答案】C

【解析】本题考查网络安全方面关于 PFS 的基础知识。

完美向前保护 PFS(Perfect Forward Secrecy)是一种密码系统，如果一个密钥被窃取，那么只有被这个密钥加密的数据会被窃取。

在使用 PFS 之前,IPSEC 第二阶段的密钥是从第一阶段的密钥导出的,使用 PFS,使 IPSEC 的两个阶段的密钥是独立的。所以采用 PFS 来提高安全性。

PFS 要求一个密钥只能访问由它所保护的数据；用来产生密钥的元素一次一换，不能再产生其他的密钥，因此一个密钥被破解，并不影响其他密钥的安全性。

某系统主要处理大量随机数据。根据业务需求，该系统需要具有较高的数据容错性和高速读写性能，则该系统的磁盘系统在选取 RAID 级别时最佳的选择是（48）。

(48)A.RAID0　　B.RAID1　　C.RAID3　　D.RAID10

【答案】D

【解析】本题考查 RAID 的基础知识。

RAID 是由一个硬盘控制器来控制多个硬盘的相互连接，使多个硬盘的读写同步，减少错误，增加效率和可靠度的技术。RAID 技术经过不断的发展，现在已拥有了从 RAID0 到 6 七种基本的 RAH)级别。另外,还有一些基本 RAID 级别的组合形式,如 RAID10(RAID0 与 RAID1 的组合)。 RAID50(RAID0 与 RAID5 的组合）等。其中，RAID0 特别适用于对性能要求较高，而对数据安全要求低的领域；RAID1 提供最高的数据安全保障，但由于数据是完全备份所以磁捋空间利用率低，速度不高；RAID3 比较适合大文件类型且安全性要求较高的应用，如视频编辑、硬盘播出机、大型数据库等；RAID10 特别用于既有大量随机数据需要存取，同时又对数据安全性要求严格的领域，如银行、金鼬、商业超市、仓储库房、各种档案管理等。

以下关于网络存储描述正确的是（49）。

(49)A.DAS 支持完全跨平台文件共享，支持所有的操作系统

B.NAS 是通过 SCSI 线接在服务器上，通过服务器的网卡向网络上传输数据

C.FC SAN 的网络介质为光纤通道，而 IP SAN 使用标准的以太网

D.SAN 设备有自己的文件管理系统，NAS 中的存储设备没有文件管理系统

【答案】C

【解析】本题考查网络存储的基础知识。

DAS(Direct Attached Storage,直接附加存储）即直连方式存储。在这种方式中，存储设备是通过电缆（通常是 SCSI 接 U 电缆）直接连接服务器。I/O(输入/输出）请求直接发送到存储设备。DAS 也可称为 SAS(Server-Attached Storage,服务器附;存储)。它依赖于服务器，其本身是硬件的堆叠，不带有任何存储操作系统，DAS 不能提供跨平台文件共享功能，各系统平台下文件需分别存储。

NAS 是(Network Attached Storage)的简称，中文称为网络附加存储。在 NAS 存储结构中，存储系统不再通过 I/O 总线附属于某个特定的服务器或客户机，而是直接通过网络接口与网络直接相连，由用户通过网络来访问。

NAS 设备有自己的 OS，其实际上是一个带有瘦服务的存储设备，其作月类似于一个专用的文件服务器，不过把显示器，键盘，鼠标等设备省去，NAS 用于存储服务，可以大大降低了存储设备的成本，另外 NAS 中的存储信息都是采用 RAID 方式进行管理的，从而有效的保护了数据。

SAN 是通过专用高速网将一个或多个网络存储设备和服务器连接起来的专用存储系统，未来的信息存储将以 SAN 存储方式为主。SAN 主要采取数据块的方式进行数据和信息的存储，目前主要使用于以太网（IPSAN)和光纤通道（FCSAN)两类环境中。

某单位使用非 intel 架构的服务器，要对服务器进行远程监控管理需要使用（50）。

(50)A.EMP　　B.ECC　　C.ISC　　D.SMP

【答案】A

【解析】本题考查服务器远程监控管理的基础知识。

上述技术中的概念如下：

EMP(Emergency Management Port)技术是一种远程管理技术，利用 EMP 技术可以在客户端通过电话线或电缆直接连接到服务器，来对服务器实施异地操作，如关闭操作系统、启动电源、关闭电源、捕捉服务器屏幕、配置服务器 BIOS 等操作，是一种很好的实现快速服务和节省维护费用的技术手段。

ECC(Error Checking and Correcting,错误检查和纠正）不是一种内，字类型，只是一种内存技术。ECC 纠错技术也需要额外的空间来储存校正码，但其占用的位数跟数据的长度并非成线性关系。

ISC(Intel ServerControl,Intel 服务器控制)是一种网络监控技术只适用于使用 Intel 架构的带有集成管理功能主板的服务器。采用这种技术后，用户在一台普通的客户机上，就可以监测网络上所有使用 Intel 主板的服务器，监控和判断服务器是否“餡康”。一旦服务器中机箱、电源、风扇、内存、处理器、系统信息、温度、电压或第三方硬件中的任何一项出现错误，就会报警提示管理人员。

SMP(Symmetrical Multi processing,对称多处理）技术是相对非对称多处理技术而言的、应用十分广泛的并行技术。在这种架构中，多个处理器运行操作系统的单一复本，并共享内存和一台计算机的其他资源。所有的处理器都可以平等地访问内存、I/O 和外部中断。

五阶段周期是较为常见的迭代周期划分方式,将网络生命周期的一次迭代划分为需求规范、通信规范、逻辑网络设计、物理网络设计和实施阶段共五个阶段。其中搭建试验平台、进行网络仿真是（51)阶段的任务。

(51)A.需求规范　　B.逻辑网络设计　　C.物理网络设计　　D.实施阶段

【答案】B

【解析】本题考查网络规划设计生命周期及各阶段任务。

五阶段周期是较为常见的迭代周期划分方式，将一次迭代划分为五个阶段：需求规范、通信规范、逻辑网络设计、物理网络设计以及实施阶段，其“瀑布模型”，形成了特定的工作流程，如下图所示。

逻辑设计阶段主要完成网络的逻辑拓扑结构、网络编址、设备命名、交换及路由协议选择、安全规划、网络管理等设计工作，并且根据这些设计产生对设备厂商、服务提供商的选择策略。搭建试验平台、进行网络仿真是逻辑网络设计阶段的任务。

在进行网络开发过程的五个阶段中，IP 地址方案及安全方案是在（52)阶段提交的。

(52)A.需求分析　　B.通信规范分析　　C.逻辑网络设计　　D.物理网络设计

【答案】C

【解析】本题考查网络规划设计生命周期及各阶段任务。

IP 地址方案及安全方案是在逻辑网络设计阶段提交的。

某部队拟建设一个网络，由甲公司承建。在撰写需求分析报告时，与常规网络建设相比，最大不同之处是（53）。

(53)A.网络隔离需求 B.网络性能需求 C.IP 规划需求 D.结构化布线需求

【答案】A

【解析】本题考查网络需求分析相关内容。

由于拟建设的是某部队网络，故与常规网络建设相比，安全性是最为重要的考虑因素，网络隔离需求尤其重要。

采购设备时需遵循一些原则，最后参考的原则是（54）。

(54)A.尽可能选取同一厂家的产品，保持设备互连性、协议互操作性、技术支持等优势

B.尽可能保留原有网络设备的投资，减少资金的浪费

C.强调先进性，重新选用技术最先进、性能最高的设备

D.选择性能价格比高、质量过硬的产品，使资金的投入产出达到最大值

【答案】C

【解析】本题考查设备选型相关内容。

在物理网络设计阶段，根据需求说明书、通信规范说明书和逻辑网络设计说明书选择设备的品牌和型号的工作，是较为关键的任务之一。在进行设备的品牌、型号的选择时，应该考虑到以下方面的内容：

产品技术指标：产品的技术指标是决定设备选型的关键，所有可以选择的产品，都必须满足依据通信规范分析中产生的技术指标，也必须满足逻辑网络设计中形成的逻辑功能。

成本因素：除了产品的技术指标之外，设计人员和用户最关心的就是成本因素，网络中各种设备的成本主要包括购置成本、安装成本、使用成本。

原有设备的兼容性：在产品选型过程中，与原有设备的兼容性是设计人员必须考虑的内容。

产品的延续性：产品的延续性是设计人员保证网络生命周期的关键因素，产品的延续性主要体现在厂商对某种型号的产品是否继续研发、继续生产、继读保证备品配件供应、继续提供技术服务。

设备可管理性：设备可管理性是进行设备选型时的一个非关键因素，但也菇必须考虑的内容。设备的先进性也是选型时应考虑的要素，但要以考虑上述因素为前提。

网络设计时主要考虑网络效率，ATM 网络中信元的传输效率为（55）。

(55)A.50%　　B.87.5%　　C.90.5%　　D.98.8%

【答案】C

【解析】本题考查 ATM 网络中信元的传输效率。

网络效率的计算公式为效率=(帧长-帧头和帧尾）/(帧长）×100%，额外开销指不能用于传输用户数据的带宽比例，额外开销=(1-效率)；在 ATM 网络中，由于信元长度固定为 53 个字节，信元头部固定为 5 个字节，因此，ATM 的网络效率为（53-5)/53X100%=90.5%,额外开销=1-90.5%=9.5%;在传统以太网络中，由于以太网的帧头大小固定，而用户数据不固定，但有最小帧长和最大帧长，因此以太网的最小网络效率为（64-18)/64X100%=87.5%，最大额外开销为 12.5%,最大网络效率为(1518-18)/1518X100%=98.8%,最小额外开销为 0.02%,实际应用中，要根据以太网的平均帧长来计算平均网络效率。

在网络设计时需进行网络流量分析。以下网络服务中从客户机至服务器流量比较大的是（56）。

(56)A.基于 SNMP 协议的网管服务　　B.视频点播服务

C.邮件服务　　D.视频会议服务

【答案】A

【解析】本题考查网络设计的基本知识。

在进行网络设计时需进行网络流量分析，在网络流量分析时，要确定系统的业务需求、用户需求、应用需求、网络需求部分的内容，并根据通信流量的分析进行确定。

其中，应用需求要根据通信模式明确各种应用程序的估算使用量。其中，工作邮件、文件共享服务的网络通信模式为客户机-服务器模式，属于双向流量大，因此在网段流量分布上应用的总流量在两个方向上各占 50%，而浏览器-服务器模式，在估算时客户机至服务器按 20%进行估算，反向按 80%进行估算，视频点播属于单播模式，其通讯量主要在服务器到客户机，视频会议系统属于对等模式，服务器到客户机的通讯量基本一致。基于 SNMP 协议的网管服务的通讯主要是客户机向服务器发送相应状态信息，所以在该应用中从客户机至服务器流量比较大。

在分析网络性能时，(57)能有效地反应网络用户之间的数据传输量。

(57)A.吞吐量　　B.响应时间　　C.精确度　　D.利用率

【答案】A

【解析】本题考查网络性能分析的基本知识。

在进行网络设计时，对网络性能参数的考虑是设计工作的重点内容之一，需要考虑的网络性能参数包括响应时间、吞吐量、延迟、带宽、容量等。

响应时间是指以计算机或终端向远端资源发出请求时间为起始时间，以该设备接收到数据响应的时间为终点，两个时间之间的差值，这个时间直接影响到用户操作的响应效果，是评估网络用户体验的关键值。

利用率描述设备在使用时所能发挥的最大能力。在网络分析与设计过程&，通常考虑 CPU 利用率和链路利用率。

吞吐量是指在网络用户之间有效地传输数据的能力。如果说数据传输率给出了网络所能传输的比特数，那么吞吐量就是它真正有效的数据传输率。吞吐量常用来评估整个网络的性能。

可用性是指网络或网络设备(如主机或服务器)可用于执行预期任务时间所占总量的百分比。可用性百分值越高，就意味着设备或系统出现故障的可能性越小，提供的正常服务时间越多。

在分层网络设计中，汇聚层实现（58)。

(58)A.高速骨干线路　　B.用户认证　　C.MAC 绑定　　D.流量控制

【答案】D

【解析】本题考查分层网络设计的基本知识。

层次结构主要定义了根据功能要求不同将局域网络划分层次构建的方式，从功能上定义为核心层、汇聚层、接入层。层次局域网一般通过与核心层设备互连的路由设备接入广域网络，核心层为下两层提供优化的数据转移功能，它是一个高速的交换骨干，其作用是尽可能快地交换数据包而不应卷入到具体数据包的运算中（ACL,过滤等），否则会降低数据包的交换速度。汇聚层提供基于统一策略的互连性，它连接核心层和接入层，对数据包进行复杂的运算。在园区网络环境中，分布层主要提供如下功能：地址的聚集、部门和工作组的接入、广播域；组播传输域的定义 VLAN 分割、介质转换、流量控制等。

接入层的主要功能是为最终用户提供对网络访问的途径。主要提供如下功能：用户接入、带宽共享、交换带宽、MAC层过滤和网段微分。

综合布线要求设计一个结构合理、技术先进、满足需求的综合布线系统方案，(59)不属于综合布线系统的设计原则。

(59)A.综合考虑用户需求、建筑物功能、经济发展水平等因素

B.长远规划思想、保持一定的先进性

C.不必将综合布线系统纳入建筑物整体规划、设计和建设中

D.扩展性、标准化、灵活的管理方式

【答案】C

【解析】本题考查综合布线系统的设计原则。

综合布线系统就是为了顺应发展需求而特别设计的一套布线系统。对于现代化的大楼来说，它采用了一系列高质量的标准材料，以模块化的组合方式，把语音、数据、图像和部分控制信号系统用统一的传输媒介进行综合，经过统一的规划设计，综合在一套标准的布线系统中。综合布线要求设计一个结构合理、技术先进、满足需求的综合布线系统方案，必须综合考虑用户需求、建筑物功能、经济发展水平等因素，长远规划思想、保持一定的先进性，同时将综合布线系统纳入建筑物整体规划、设计和建设中，保持扩展性、标准化、灵活的管理方式。

传统数据中心机房的机柜在摆放时，为了美观和便于观察会将全部机柜朝同一个方向摆放，但实际上这种做法不是很合理，正确的做法应该是将服务器机柜按照面对面或背对背的方式布置，这样做是为了（60）。

(60)A.减小楼体荷载　　B.节省服务器资源　　C.节能环保　　D.避免电磁干扰

【答案】C

【解析】本题考查绿色数据中心机房中机柜摆放的相关知识。

在现代机房的机柜布局中，人们为了美观和便于观察会将所有的机柜朝同一个方向摆放，那么如果按照这种摆放方式，机柜盲板有效阻挡冷热空气的效果将大打折扣。这是因为当机柜朝统一方向摆放时就形成了第一排机柜背面正对着第二排机柜的正面，这样两排机柜中间的通道就会出现冷热气流混合循环，形成冷热气流短路致使第二排机柜的冷风进口温度大大提高，严重破坏了冷风通道的环境温度。正确的摆放方式应该是将服务器机柜面对面或背对

背的方式摆放，即当机柜内或机架上的设备为前进风/后出风方式冷却时，机柜或机架的布置宜采用面对面、背对背方式。这样便形成了冷风通道和热风通道。机柜之间的冷热风不会混合在一起，形成短路气流，大大提高了制冷效果，保护好了冷热通道不被破坏。
正确的选择制冷设备和机柜，以及合理的机柜布局将大大提高制冷效率，同时也将大大降低了 IT 设备运行的总拥有成本，这也将是绿色数据中心未来设计发展的方向和趋势。

某公司新建一栋 30 层的大楼，在该楼内设信息系统中心机房时，综合考虑各方面因素，对于中心机房的楼层选址建议位于（61）。

(61)A.1 层　　B.2 层　　C.5 层　　D.30 层

【答案】B

【解析】本题考查数据中心机房选址的相关知识。

对于一般的机房选址来说，大楼位置的选择可能很少受机房选址要求的影响，但是楼内机房位置的选择，却是机房使用、规划和设计部门可以认真考虑的。对于多层或高层建筑物内的电子信息系统机房，在确定主机房的位置时，应对设备运输、管线敷设、雷电感应和结构荷载等问题进行综合分析和经济比较；采用机房专用空调的主机房，应具备安装空调室外机的建筑条件。综合考虑以上因素，机房宜设置在大楼的第二、三层或裙楼的中间层。将机房设置在一楼和地下室虽然从结构荷载、雷电感应、设备搬运等方面考虑有好处，但有水浸、多尘、虫鼠害以及安保方面的担忧。机房设置在大楼的第二、三层或裙楼的中间层既有一层的优点，又克服了一层的缺点，所以是建设机房的最佳楼层，而且对安装空调室外机有更多的选择。如果大楼是高层建筑，且楼下无法安装空调室外机，或因为其他原因无法在大楼低层建设机房，则宜选择在最高层以下的几个楼层，因为顶层保温比较困难，还容易发生漏水事故。

某大型企业网络出口带宽 1000M，因为各种原因出口带宽不能再扩，随着网络的运行发现访问外网的 Web 以及使用邮件越来越慢，经过分析发现内网 P2P、视频/流媒体、网络游戏流量过大，针对这种情况考虑对网络进行优化，可以采用（62）来保障正常的网络需求。

(62)A.部署流量控制设备　　B.升级核心交换机

C.升级接入交换机　　D.部署网络安全审计设备

【答案】A

【解析】本题考查网络故障排查的相关知识。

众所周知，网络带宽资源建设的发展速度永远跟不上各种网络应用的增长速度。对企业出口带宽无尽的增长需求势必给企业带来额外的经济负担，所以对企业网络流量进行管理已是迫在眉睫的事情。广义上说安全管理设备也算流控，但其主要用途是记录和控制网络中的用户行为，比如限制用户使用 QQ、玩游戏等等，但其流控功能较弱，一般适用于上网人数较少的场合。由于安全管理设备的应用场景复杂，流控功能和性能并不专业，对带宽的优化能力很弱，采用行为管理设备充当流控设备使用还可能斤致网络延迟增大，偶尔还会导致断网现象发生。而专用的流控设备主要目的是优化带宽，通过限制带宽占用能力强的应用以保护关键应用，通过多种复杂的策略来实现合理的带宽分配。专用的流量控制设备通过应用封堵、流量限速等流量限制等手段，控制非关键应用，封堵无关应用，极大地提升现有带宽的利用价值，避免因带宽扩容带来额外的网络接入费用。同时通过数据压缩功能，大大降低了网络中传输的数据量，有效提升了当前的带宽利用价值，避免因额外租用出口带宽资源而增加网络运营成本。因此可以采用部署流量控制设备来保障正常的网络需求。

某大学 WLAN 无线校园网已经全面覆盖了校园，AP 数量、信号强度等满足覆盖需求。学校无线用户要求接入某运营商的 WLAN，针对现状可采用的最优化技术方案是(63)。

(63)A.运营商新建自己的 WLAN 无线网络

B.运营商利用学校现有无线网络，在 AP 上增加一个自己的 SSID

C.运营商利用以前部署的手机基站进行建设覆盖

D.增强 AP 功率

【答案】B

【解析】本题考查 WLAN 网络建设的相关优化知识。

根据题目要求，新建自己的 WLAN 无线网络投资大，而且可能与现有无线网的 AP 形成干扰。利用以前部署的手机基站进行建设覆盖其覆盖范围、速率等不能保证。增强 AP 功率不能满足网络接入的需求。利用学校现有无线网络，在 AP 上增加一个自己的 SSID 可以很方便的实现网络接入的需求同时又节省了投资，可以说是最合理的方案。

某学校建有宿舍网络，每个宿舍有 4 个网络端口，某学生误将一根网线接到宿舍的两个网络接口上，导致本层网络速度极慢几乎无法正常使用，为避免此类情况再次出现，管理员应该（64）。

(64)A.启动接入交换机的 STP 协议　　B.更换接入交换机

C.修改路由器配置　　D.启动交换机的 PPPoE 协议

【答案】A

【解析】本题考查网络故障排查的相关知识。

根据题意，将一根网线接到宿舍的两个网络接口上，很明显是形成了环路。网络环路会带来广播风暴、多重复数据帧、MAC 地址表不稳定等因素，解决方法就是利用生成树协议 STP。该协议可使用环路网络，解决必需的算法完成途径冗余，同时将环路修剪成无环路的树型网络，从而防止报文在环路网络中无限循环。本题中的其他方法都不能解决网络环路问题。

互联网上的各种应用对网络指标的敏感性不一，下列应用中对延迟抖动最为敏感的是（65）。

(65)A.浏览页面　　B.视频会议　　C.邮件接收　　D.文件传输

【答案】B

【解析】本题考查互联网上的应用对网络指标的敏感性。

实时视频的传输对带宽、延迟、延迟抖动和丢包率有较高的要求。而其中网络出现延迟、抖动，将会给视频会议带来声画不同步，严重影响会议质量。而对:刘览网页、接受邮件以及文件传输影响不大。

有 3 台网管交换机分别安装在办公楼的 1-3 层，财务部门在每层都有 3 台电垴连接在该层的一个交换机上。为了提高财务部门的安全性并容易管理，最快捷的解决方法是(66)。

(66)A.把 9 台电脑全部移动到同一层然后接入该层的交换机

B.使用路由器并通过 ACL 控制财务部门各主机间的数据通信

C.为财务部门构建一个 VPN，财务部门的 9 台电脑通过 VPN 通信

D.将财务部门 9 台电脑连接的交换机端口都划分到同一个 VLAN 中

【答案】D

【解析】本题考查网络管理维护的相关知识。

根据题意，A 选项需要变动财务部门的电脑，变换办公室要改变办公流程比较麻烦；B 选项要增加路由器，成本较高；C:选项需要搭建 VPN，配置以及管理成本复杂；综合来看，D 选项最快捷、成本最低。

在诊断光纤故障的仪表中，设备（67)可在光纤的一端就测得光纤的损耗。

(67)A.光功率计 B.稳定光源 C.电磁辐射测试笔 D.光时域反射仪

【答案】D

【解析】本题考查网络测试仪器的相关知识。

光功率计是指用于测量绝对光功率或通过一段光纤的光功率相对损耗的仪器。稳定光源是对光系统发射已知功率和波长的光。稳定光源与光功率计结合在一起，则能够测量光纤系统连接损耗、检验连续性，并帮助评估光纤链路传输质量。

光时域反射仪（OTDR)是通过对测量曲线的分析，了解光纤的均匀性、缺陷、断裂、接头耦合等若干性能的仪器。它根据光的后向散射与菲涅耳反向原理制作，利用光在光纤中传播时产生的后向散射光来获取衰减的信息，可用于测量光纤衰减、接头损耗、光纤故障点定位以及了解光纤沿长度的损耗分布情况等，是光缆施工、维护及监测中必不可少的工具。在诊断光纤故障的仪表中 OTDR 是最经典的也是最昂贵的仪表。与光功率计和光万用表的两端测试不同 OTDR 仅通过光纤的一端就可测得光纤损耗。

电磁辐射测试笔主要功能是检测出您周围的电磁辐射源。

某公司采用 ADSL 接入 Internet，开通一段时间来一直都比较正常，近一周经常出现间歇性的速度变慢，拔掉 Modem 的直流电源线，信号正常。更换一个新 Modem 及其直流电源适配器，仍然是呈现网速随机波动。导致该 ADSL 间歇性速度变慢的可能原因是(68)。

(68)A.电话线路过长 B.电话线腐蚀老化

C.有强信号干扰源 D.网卡质量不稳定

【答案】C

【解析】本题考查网络维护的相关知识。

根据题意，电话线路过长不会在开通的一段时间都正常，拔掉 Modem 的直流电源信号就正常，说明不是电话线路腐蚀老化和网卡质量不稳定。而更换一个新 Modem 及其直流电源适配器，仍然是呈现网速随机波动，说明不是电源的问题，只能是周边突然产生了强的信号干扰源。

在光缆施工中，应该特别注意光缆的弯曲半径问题，以下说法中不正确的是（69)。

(69)A.光缆弯曲半径太小易折断光纤

B.光缆弯曲半径太小易发生光信号的泄露影响光信号的传输质量

C.施工完毕光缆余长的盘线半径应大于光缆半径的 15 倍以上

D.施工中光缆的弯折角度可以小于90度

【答案】D

【解析】本题考查光缆施工中的注意事项。

在光缆施工中，要特别注意转弯时光缆弯折角度尽量别超过90度，否则容易折断。光缆的弯曲半径弧度不能太小，弧度太小易折断光纤，同时易造成折射损耗过大导致色散现象，也就是容易发生光信号的泄露影响光信号的传输质量。施工完毕光缆余长的盘线半径应大于光缆半径的10～15倍以上。

为满足企业互联业务需求，某企业在甲地的A分支机构与在乙地的企业中心（甲乙两地相距50km），通过租用一对ISP的裸光纤实现互联，随着企业业务的扩大，要使得甲地的另外B、C、D三个分支机构也能接入到企业中心，所采用的比较快捷和经济的做法是(70)。

(70)A.使用CWDM设备　　B.租用多对ISP的裸光纤

C.租用多条DDN专线　　D.使用DWDM设备

【答案】A

【解析】本题考查光纤传输中波分复用设备的相关知识。

把不同波长的光信号复用到一根光纤中进行传送的方式统称为波分复用（WDM)方式，这种技术利用了一根光纤可以同时传输多个不同波长的光载波的特点，把光纤可能应用的波长范围划分成若干个波段，每个波段用作一个独立的通道传输一种预定波长的光信号。通信系统的设计不同，每个波长之间的间隔宽度也有差别，按照通道间隔差异，WDM可以细分为CWDM、DWDM等。而CWDM的成本比DWDM的成本要少50%以上。根据题意，租用裸光纤和DDN专线都不是经济快捷的方式，所以选项为A。

BGP is an inter-autonomous system routing protocol; it is designed to be used between multiple autonomous (71).BGP assumes that routing within an autonomous system is done by an intra-autonomous system routing protocol. BGP does not make any assumptions about intra-autonomous system (72) protocols employed by the various autonomous systems. Specifically, BGP does not require all autonomous systems to run the same intra-autonomous system routing protocol.

BGP is a real inter-autonomous system routing protocol. It imposes no constraints on the underlying Internet topology. The information exchanged via BGP

is sufficient construct a graph of autonomous systems connectivity from which routing loops may be pruned and some routing (73) decisions at the autonomous system level may be enforced.

The key feature of the protocol is the notion of Path Attributes. This feature provides BGP with flexibility and expandability. Path (74) are partitioned into well-known and optional. The provision for optional attributes allows experimentation that may involve a group of BGP (75) without affecting the rest of the Internet. New optional attributes can be added to the protocol in much the same fashion as new options are added to the Telnet protocol, for instance.

(71)A.routers	B.systems	C.computer	D.sources
(72)A.routing	B.switching	C.transmitting	D.receiving
(73)A.connection	B.policy	C.source	D.consideration
(74)A.states	B.searches	C.attributes	D.researches
(75)A.routers	B.states	C.meters	D.costs

【答案】B A B C A

【解析】

BGP是自治系统间的路由协议，它被应用于多个自治系统之间。BGP假定，自治系统内部的路由已经由自治系统内部的路由协议搞定。BGP对于各个自治系统采用的自治系统内部路由协议没有任何假定的条件。特别，也不要求所有的自治系统都运行同样的自治系统内部路由协议。

BGP是一个实用的自治系统间的路由协议。它对底层的Internet技术没有任何限制。通过BGP交换的路由信息足以构造一个自治系统连接图，据此对路由环路进行修剪，并在自治系统这一级实施路由策略决策。

这个协议关键的特点是通路属性的表示。这个特点为BGP提供了灵活性和可扩展性。通路属性被划分为众所周知的和任选的两类。提供的任选属性可以在一组BGP路由器中进行实验而不影响因特网的其余部分。新的任选属性可以被加入到协议中，这种方式就像是新的选项被加入到Telnet协议中一样。

试题一

某大学校园网经过多年的建设已初具规模，由于校内相关的科研单位有接入到以 IPv6 为核心的下一代互联网中进行相关研究的需求，同时为了积极探索解决学校公网 IPv4 地址的短缺、现有网络安全等方面的问题，学校网络中心计划对现有校园网进行 IPv6 技术升级。学校现有的网络拓扑如图 1-1 所示。

(1) 接入层：完成 IPv4 用户接入，设备是二层接入交换机/三层接入交换机。

(2) 汇聚层：完成接入用户的汇聚，汇聚交换机是盒式或机架式三层交换机，目前不支持 IPv6 业务。

(3) 核心层：是整个网络的核心（机架式三层交换机，目前不支持 IPv6 业务），同时连接外部网络的出口，是整个园区网业务流量通往 IPv4 主干网或者 IPv6 主干网的必经之路。

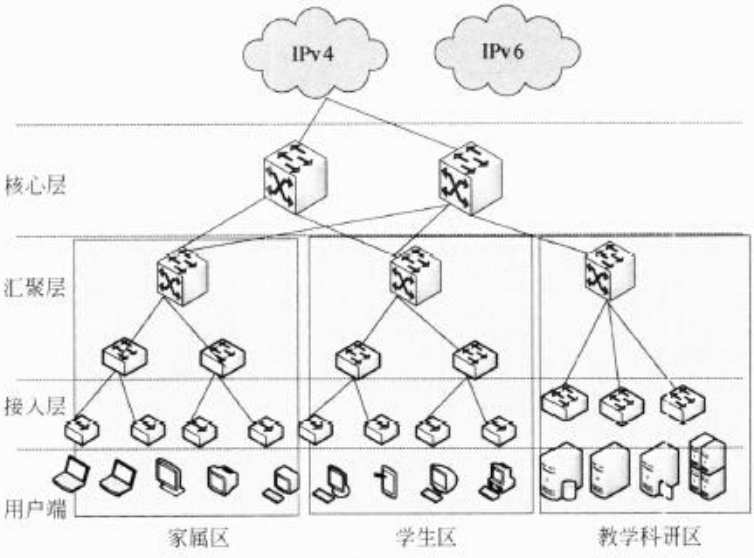


图 1-1

【问题 1】

为了实现 IPv4 网络向 IPv6 网络的过渡和转换，IETF 制订的解决过渡问题的基本技术方案有三种。在进行 IPv6 升级的初期，由于教学科研区访问 IPv6 网络的需求比较迫切，学校希望花费较少的资金就能使教学科研区访问 IPv6 网络上的相关资源，简述三种技术方案的要点，并依据需求进行过渡技术方案选择。

简述三种技术要点：

隧道技术，以现有 IPv4 网络传递 IPv6 数据，无须大量 IPv6 路由和专用链路，是过渡阶段最容易采用的技术，一般用来进行纯 IPv4 网络上的 IPv6 孤岛之间通信。

双栈技术，同时运行 IPv4 和 IPv6 两套协议栈，完全兼容 IPv4 和 IPv6。

翻译技术，在通信中间设备完成 IPv4 和 IPv6 网络之间地址转换和协议翻译，分组路由

对端节点透明。IPv4 节点访问 IPv6 节点的方法复杂，网络设备开销大，一般在其他互通方式实现不了的情况下使用。

要求在实现教学科研区访问 IPv6 网络上的相关资源功能的基础上费用花费最小，网络结构不变且部署方便，可在核心设备上采用隧道接入技术实现其功能。

为了适应大众的需要，网络业务逐步呈现出宽带化、综合化、多样化和个性化的特点，IPv4 向 IPv6 网络过渡已是大势所趋。基于 IPv6 的下一代互联网技术的迅速发展，为网络发展提供了更为有利的扩展空间，然而受到诸多条件的限制，想要很快完成从 IPv4 到 IPv6 网络的转换是不切实际的。

目前已有多种策略和技术方案及其实现可以完成从 IPv4 向 IPv6 的转换，但都仍有局限性。按工作原理划分有以下三种：隧道技术、双协议栈技术和协议翻译技术。

1. 隧道技术

隧道技术：隧道技术的工作原理是在 IPv6 网络与丨 Py4 网络间的隧道入口处，路由器将 IPv6 的数据分组封装入 IPv4 中。IPv4 分组的源地址和目的地址分别是隧.羞入口和出口的 IPv4 地址，在隧道的出口处再将 IPv6 分组取出转发给目的节点。换句话说，就是通过 IPv4 网络实现“IPv6 孤岛”之间的互通。

这种技术能充分利用现有的网络资源，但是没有解决 IPv4 和 IPv6 网络之间的互通，因此只能是是过渡初期较为方便的选择。

2. 双协议栈技术

双栈协议技术指在完全过渡到 IPv6 之前，使一部分主机或路由器同时支持 IPv4 和 IPv6 两种协议，这样双协议栈设备既能识别 IPv4 报文也能识别 IPv6 报文，从而实现与 IPv4 和 IPv6 网络的数据通信。主机具体使用 IPv4 协议还是 IPv6 协议来发送和接收数据包是由目的地址来决定的。

这种机制主要用来解决纯 IPv6 网络中的双栈主机与其他 IPv4 节点通信的问题，但没有解决 IPv4 地址的问题。

3.协议翻译技术

翻译技术实际是一种协议转换技术，即为了使 IPv4 和 IPv6 网络中的主机能相互识别对方而进行的协议头之间的转换。其中 NAT-PT 是实现翻译策略的一种主要技术。翻译转换技术的优点是不需要进行 IPv4、IPv6 节点的改造就能有效解决 IPv4 节点与 IPv6 节点相互通信的问题，根据 NAT-PT 原理，过渡初期“IPv6 孤岛”中的主机通过转换设备，将其 IPv6 地址转换成合法的 IPv4 地址进而访问 IPv4 的网络。

以上是目前存在的一些由 IPv4 网络过渡到 IPv6 的机制，无论采取哪一种机制，对 DNS 的扩展都是必须的。这些过渡机制仍不是普遍适用的，常常需要和其他技术组合使用。在实际应用时需要综合考虑各种实际情况来制定合适的过渡策略。表 1 给出三种不同技术的过渡方案对比。

表 1 采用三种不同技术的过渡方案对比

过渡技术名称	优 点	缺 点	使 用 场 合
隧道技术	以现有 IPv4 网络传递 IPv6 数据，无须大量 IPv6 路由和专用链路，是过渡阶段最容易采用的技术。	需避免路由回环和路由泄露，不能解决 IPv4 和 IPv6 网络的互联互通。	连接到纯 IPv4 网络上的 IPv6 孤岛之间通信。
双栈技术	同时运行 IPv4 和 IPv6 两套协议栈，完全兼容 IPv4 和 IPv6。	没有解决 IPv4 地址耗尽的问题。	任何 Ipv4/IPv6 网络。
翻译技术	在通信中间设备完成 Ipv4 和 IPv6 网络之间地址转换和协议翻译，分组路由对端节点透明。	IPv4 节点访问 IPv6 节点的方法复杂，网络设备开销大，一般在其他互通方式实现不了的情况下使用。	IPv6 孤岛与 IPv4 海洋之间的通信。

校园网络过渡的实质是将目前的 IPv4 网络全面向 IPv6 网络过渡。为了更充分地利用。校园网现有的网络设备，降低升级成本，从而实现平滑稳定地向 IPv6 过渡的目标，过渡的具体实施可分为四个阶段进行：

第一阶段，可根据个别用户或者部门的需求，建立起若干 IPv6 网络.这些 IPv6 网络即所谓的“IPv6 孤岛”。这些“IPv6 孤岛”通过隧道技术与学校的实验网进行联通，并经此连接到 IPv6 网络中。显然这时 IPv4 网络是占主导地位的。通过路由器访问外部 IPv6 接入主机必须是双栈主机，并通过配置隧道先连接到网络中心的 IPv6 格由器，从而访问外部 IPv6。第二阶段，越来越多的“IPv6 孤岛”逐渐变大、变多，数量与 IPv4 网络相当，与 IPv4 网络通讯增加，IPv6 网络规划越来越规范，此时可综合采用双协议栈技术和动态 NAT-PT 技术，这就需要对核心层和汇聚层的设备进行升级。为保证核心层设备性能，同时尽量减少对原网络线路的改动，建议直接将核心层设备升级为支持双协议栈技术的设备。

这个阶段 IPv4 和 IPv6 网同时存在且数量相当，因此需要解决各种网络中各种主机的通信问题。内部 IPv4 主机之间、IPv6 主机之间的数据通信没有问题，IPv6 网络和 IPv4 网络通过 NAT-PT 技术实现相互通信。IPv4 网络仍然通过原核心交换与外部 IPv4 网络联通，IPv6 网络则通过网络中心的核心设备与外部 IPv6 网络通信。

第三阶段，IPv6 将占主导地位，IPv4 网络逐渐变为“孤岛”。这个阶段与 IPv6 发展的第一个阶段非常相似，所以此时也可采用隧道技术进行部署，与第一阶段不同的是此时互联

的是 IPv4 网络。

第四阶段，经过设备的更新换代，网络中所有设备都已支持 IPv6，IPv4 网络逐渐被 IPv6 所替代，直至 IPv4 网络节点完全被淘汰，此时校园网完全升级为纯 IPv6 网络，各网络节点间也都采用基于 IPv6 的通信方式。

【问题 2】

随着网络建设的不断升级，为把校园网积极推进到以 IPv6 为核心的下一代互联网中，要求学生区和教学科研区的 IPv6 用户能够访问 IPv6 网络资源，同时实现这两个区域之间 IPv6 资源的互访。

(1)基于上述的需求，对过渡方案进行了调整，网络结构如图 1-2 所示，请在尽量节省资金的情况下给出该校园网 IPv6 技术升级的过渡方案，并进行设备升级和网络调优(网络设备调整等）的方案设计。

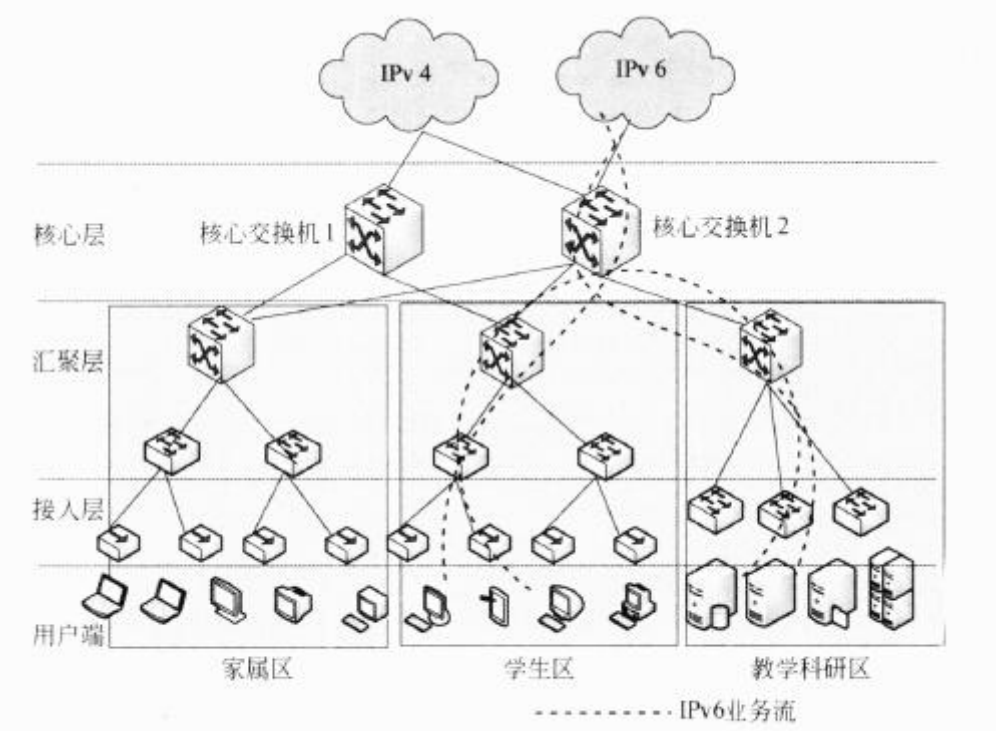


图 1-2

(2)因家属区个别用户也想接入到 IPv6 网络中访问相关资源，现在核心交换机 2 上开启 ISATAP 隧道，隧道服务器地址为 isatap.xuexiao.edu.cn。

若家属区客户机为 winxp(spl 及以上)，完成下面的步骤，使得客户机能够通过 ISATAP 隧道接入 IPv6 网络。

C:>　　①　//安装 IPv6 协议

C:> ② //设置隧道终点

(1) 实现的技术方案选择双栈模式。

设备升级模式为：新建（升级）学生区和教学科研区的核心和汇聚交换机，支持 IPv6。网络调优方案：将学生区和教学科研区的核心、汇聚交换机以及其他不能进行 IPv6 升级的设备调整到家属区的网络，以满足家属区网络的运维需求。

(2) ①netsh interface ipv6 install 或者 ipv6 install

②netsh interface ipv6 isatap set router isatap.xuexiao.edu.cn

根据题目要求，目前校园网已经发展到 IPv4 与 IPv6 的共存期。

全双栈模式适合在新建的校园网或原有网络不断更新发展到中期时使用。全双栈模式要求核心层和汇聚层选用双栈交换机，接人层可使用现有的二层交换机，其中汇聚层也可采用双栈路由设备。对于双栈终端，IPv4 网关和 IPv6 网关均部署在汇聚双栈三层交换机上。IPv4 和 IPv6 协议可以同时运行，使用协议翻译机制让纯 IPv4 节点和 I:)v6 节点进行通信。全双栈模式提供的 IPv6 接入服务范围广，可获得较大规模 IPv6 建设和使用经验。不必为不同类型的用户单独部署网络配置，开销小，方便管理，IPv4 和 IPv6 的逻辑界面清晰。

针对网络拓扑结构，可考虑购买或者升级学生区和教学科研区的核心和汇聚交换机，支持 IPv6,接入层网络设备暂时不用调整。同时为保护投资，如果学生区和教学科研区有淘汰下来的网络设备也可用在家属区的网络维护中。

ISATAP 的全名是 Intra-Site Automatic Tunnel Addressing Protocol,它将 IPv4 地址夹入 IPv6 地址中，当两台 ISATAP 主机通讯时，可自动抽取出 IPv4 地址建立 Tunnel 即可通讯，且并不需透过其他特殊网络设备，只要彼此间 IPv4 网络通畅即可。

通过 ISATAP 隧道接入 IPv6 环境的方法

学校 ISATAP 隧道路由器的 IPv4 地址是：isatap.xuexiao.edu.cn

用户设置 ISATAP 隧道的接入点为：isatap.xuexiao.edu.cn

WindowsXP/2003 下配置方法

进入命令提示符

```
C:\>netsh
netsh>int
netsh interface>IPv6
```

```
netsh interface>IPv6>install   //安装 IPv6 协议
netsh interface IPv6>ISATAP
netsh interface IPv6 ISATAP>set router isatap.xuexiao.edu.cn //设置隧道终点
```

此后，通过 ipconfig 应该可以看到一个本校前缀的 v6 地址，hostid 为 0:5efe:a b.c.d，其中 a.b.c.d 为你的真实的 IPV4 地址，这样即可访问 IPv6 资源。

【问题 3】

NDP(Neighbor Discovery Protocol,邻居发现协议）是 IPv6 的一个关键协议，它组合了 IPv4 中的 ARP、ICMP 路由器发现和 ICMP 重定向等协议，并对它们做了改进，作为 IPv6 的基础性协议，NDP 还提供了前缀发现、邻居不可达检测、重复地址监测、地址自动配置等功能。进行 IP 地址规划及路由方案设计，包括：

(1) 在现阶段网络的 IPv6 技术升级中，IPv6 地址分配的两种分配机制是什么？

(2) 在本方案中服务器端和用户端分别采用的 IPv6 地址分配机制是什么？

(3) 在 IPv4 的网络中，校园网内部路由协议采用 OSPF，在 IPv6 的网络中采用的路由协议是什么？

(4) 接入到 IPv6 网络中的边界路由器采用何种接入方式。

(1) 两种，无状态地址自动分配机制，状态地址自动分配机制。

(2) 用户端采用无状态地址自动分配机制，服务器端采用静态手工配置方式。

(3) 采用 OSPFv3，实现与 IPv4 网络的隔离与统一。

(4) 边界路由器对外出口只有一个，采用静态路由方式接入。

IPv6 地址是独立接口的标识符，所有的 IPv6 地址都被分配到接口，而非节点。由于每个接口都属于某个特定节点，因此节点的任意一个接口地址都可用来标识一个节点。IPv6 有三种类型地址：

1. 单点传送（单播）地址

一个 IPv6 单点传送地址与单个接口相关联。发给单播地址的包传送到由该地址标识的单接 U 上。但是为了满足负载平衡系统，在 RFC2373 中允许多个接口使用同一地址，只要在实现中这些接口看起来形同一个接口。

2. 多点传送（组播）地址

一个多点传送地址标识多个接口。发给组播地址的包传送到该地址标识的所有接口上。IPv6 协议不再定义广播地址，其功能可由组播地址替代。

3. 任意点传送（任播）地址

任意点传送地址标识一组接口（通常属于不同的节点），发送给任播地址的包传送到该地址标识的一组接口中根据路由算法度量距离为最近的一个接口。如果说多点传送地址适用于 one-to-many 的通讯场合，接收方为多个接口的话，那么任意点传送地址则适用于 one-to-one-of-many 的通讯场合，接收方是一组接口中的任意一个。

IPv6 地址为 128 位，如果手工设置要花费很多时间。IPv6 协议可以手工静态输入，也支持地址自动配置，地址自动配置是一种即插即用的机制。IPv6 节点通过地址自动配置得到 IPv6 地址和网关地址。

IPv6 支持无状态地址自动配置和状态地址 0 动配置两种地址自动配置方式,,在无状态地址自动配置方式下,需要配置地址的网络接口先使用邻居发现机制获得一个链路本地地址。网络接口得到这个链路本地地址之后，再接收路由器宣告的地址前缀，结合接口标识得到一个全球地址。而状态地址自动配置的方式，如动态主机配置协议（DHCP),需要一个 DHCP 服务器，通过客户机/服务器模式从 DHCP 服务器处得到地址配置的信息。

在本次升级方案中，用户端数量众多，而且 IPv6 地址长达 128 位，可采用无状态地址自动分配机制来自动分配地址，服务器端因为数量较少且固定，同时要在域名系统中配置可考虑采用静态手工配置方式。

校园网内部路由协议采用 OSPF 动态路由协议，IPv6 路由协议可采用 OSPFv3 动态路由。这样在地址规划、区域设计上就具有很大的便利性。

在出口路由方面，因为目前 IPv6 的出口只有一个，所以考虑采用静态路由的方式。

【问题 4】

近年来国家大力推进 IPv4 向 IPv6 的过渡，但是基于 IPv6 的网络部署还不能达到国家的战略要求。

(1) 你认为影响 IPv6 发展的因素主要有哪些。

(2) 对于学校现有 IPv6 网络的运维的建议。

(1) 当前影响 IPv6 发展的因素主要有软硬件设备的升级；IPv6 网络资源不足，应用缺乏；v4/v6 的透明过渡/无缝连接技术问题；运营商的需求不大等问题，其中最关键的应该是缺少杀手级的应用。

(2) 目前大多数网管产品还不支持 IPv6 下的管理功能，计费认证功能等也等待开发，因此现阶段的运维技术实力较强的学校可采用利用开源产品自主开发，技术实力一般的学校采用与厂商合作开发的方式。

IPv4 向 IPv6 过渡主要包含以下几个方面的过渡：

(1) 网络的过渡

为了支持 IPv6 协议，主要有两种方式可以选择：一是用软件升级现有的 IPv4 路由设备，使它能够运行 IPv6 协议；另一种方法是购买新的支持 IPv6 协议的路由设备，并采用相应的链路资源，这样使它们在物理上构成两个独立的网络环境。网络的过度包括网络节点的过渡、网络设备的过渡、网关的过渡。

(2) 客户端的过渡

过渡到 IPv6 协议需要升级用户的终端设备，它包括客户端的网络协议和应用程序的升级。

(3) 应用程序的过渡

由于 IPv6 协议的应用程序不及 IPv4 协议的应用程序那般普及，所以开发的应用程序对于低层协议应是透明的，即 IPv4 协议下能使用，IPv6 协议下也能使用。另外，将来 IPv6 在得到普遍支持后，用户还可以继续使用原来的纯 IPv4 应用程序。

(4) IPv4/IPv6 网络互通

校园网络正面临从传统 IPv4 到 IPv6 的过渡以及一段时期的共存。如果主机+支持双栈，那么就必然存在纯 IPv4 和纯 IPv6 节点之间的互通问题，这也是过渡时期必须面对的主要问题之一。使用网络地址翻译/协议翻译(NAT-PT)转换技术能较好地解决该问题，但它在支持数据的透明性方面存在一定的问题。校园网络的过渡各个环节紧密相扣，相辅相成。M 络的过渡脱离了客户端的过渡、应用程序的过渡及 IPv4/IPv6 的 M 络互通，网络的过渡就无法进行。因此，这四个方面的演进必须同时进行。

IPv4 向 IPv6 过渡是一个复杂的、系统的社会工程，超越了简单的技术范畴，也超出了各大运营商的职责范畴，需要产业链协同推动。IPv4 向 IPv6 过渡有其内在的规律，我们只有在认识规律并遵循规律的基础上，顺势而为，才能获得成功。这个规律就是过渡需要经历 IPv4 资产保值、IPv6 准备和 IPv6 繁荣这三个演进阶段，我们只能在有限范围内缩短或者延长某一阶段的时间，但是无法颠倒顺序。不同阶段的场景和仨务不同，所依赖的技术也不同，所以不同的技术将先后登场，是一场技术的接力赛。中间过渡技术在完成使命后，最后全部

退出舞台，只留下 IPv6 造福人类。在向 IPv6 过渡期间，重点和难点在接入网络部分，其次是互联互通部分，骨干网络基本具备。当然，在过渡过程中，基于 IPv6 的应用资源还是较少，这中间最关键的因素可能是缺少杀手级的应用来推动。

校园网 IPv6 技术升级中的网络部分改造虽然可以很快完成，但相关的支系统的建设和应用系统的迁移才刚刚开始，需要继续完善校园网网络管理与安全监控系统、接入和计费等，使其成为学校新一代先进的教学和科研信息基础设施。同时，如何建设一个安全的下一代互联网是一个全新的课题。要想将下一代互联网建设到目前 IPv4 网络的阶段，还有比较长的一段路要走。在这些方面，有实力的学校可以进行有益的探索，进行自主科研开发，也可以通过和厂商合作进行共同开发，如果有成熟的产品也可进行推广应用。

试题二

近年来，云计算技术的蓬勃发展为整个 IT 行业带来了巨大变革。传统数据中心已经难以满足新形势下日益增长的高性能及高性价比需求，并且无法支持云环境下更如灵活的按带宽租赁数据中心网络的运营方式。该集团随着信息系统业务的不断扩展上线，对高密度服务器及高度自动化管理系统的需求不断增长，建设云数据中心的需求应运而生。

【问题 1】

如图 2-1 所示，依据集团总部业务应用的需求，集团数据中心网络按功能将划分为七大区：核心交换区、核心业务区、办公区、互联网接入区、运维管理区、广域网接入区、外联业务区。二级板块及其下属子分公司可参考建立符合自身情况的局域网络。你认为这七大区域应该如何分布，请根据图 2-1 所示填写图中（1)～（7)区域名称。

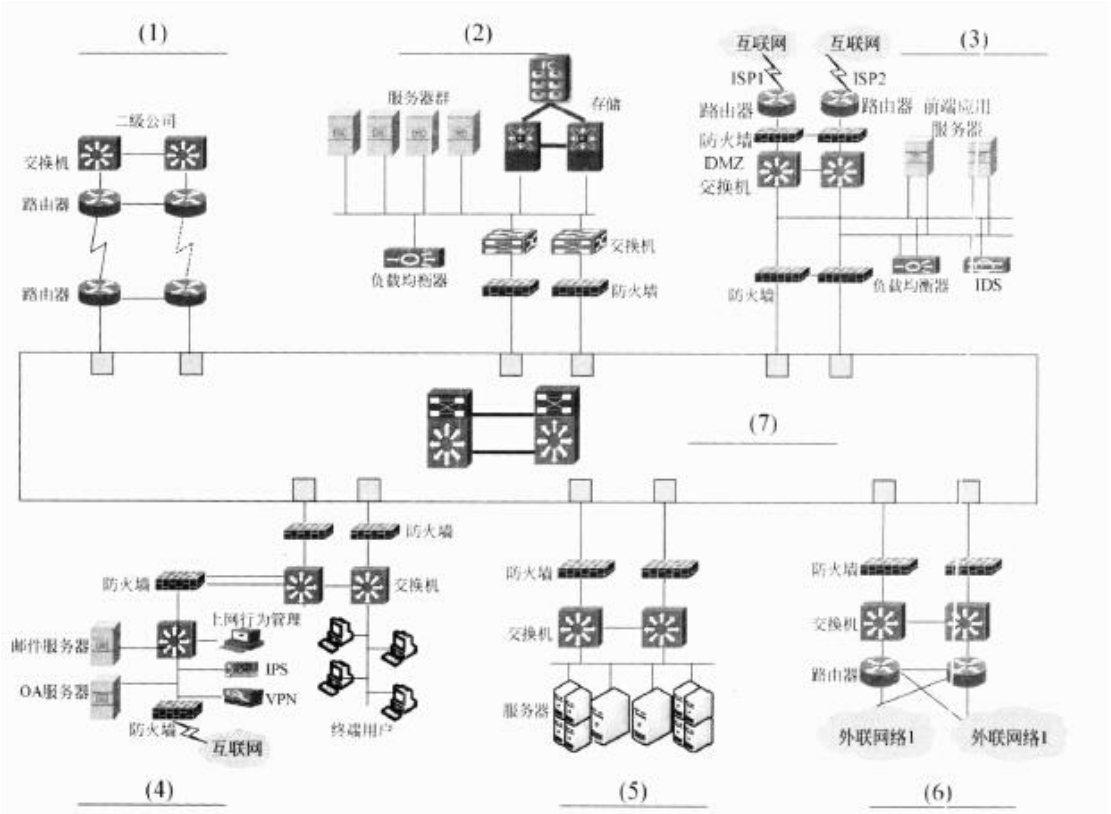


图 2-1

(1) 广域网接入区

(2)核心业务区

(3)互联网接入区

(4)办公区

(5) 运维管理区

(6)外联业务区

(7)核心交换区

集团数据中心网络按功能将划分为七大区：核心交换区、核心业务区、办公区、互联网接入区、运维管理区、广域网接入区、外联业务区。其中各部分功能大致如下：

(1) 核心交换区实现网络分区之间的通信流量路由、交换功能，是数据中心网络最核心的部分。核心交换区需要具备高可用、高性能架构，以来确保核心网络高可用及高效运行。

(2) 核心业务区将提供核心业务应用系统的网络接入功能。核心业务区域集中了核心业务应用服务器和核心业务应用数据库服务器，为内部用户、内部业务人员提供应用服务的核心区域，需要采用较高可用性和更全面的安全防护措施。

(3) 办公区包括两部分功能：一部分是办公用户网络接入提供内部员工分公电脑、移动等设备网络接入功能，满足企业内部员工访问内部业务应用系统；另一部分是用户互联网访问、办公邮件处理、内部文件传输等功能。

(4) 互联网接入区提供互联 M 业务的接入访问网络，为保证网络安全需要部署外网防火墙，用于保护业务应用前端应用；部署内网防火墙，用于保护集团内部网络的安全；采用多条冗余的互联网链路，提高网络接入的可靠性。

(5) 运维管理区提供运维管理系统（监控、信息化服务管理等）网络互联功能，运维管理系统需与公司范围内的应用、基础设施通信，安全性要求较高。

(6) 广域网接入区用于连接广域网络连接设备。

(7) 外联业务区即企业边界网区域，具有如下特点：与外网 S 联，风险较大；与内网相连进行数据通信。

根据网络拓扑结构和各大区域网络功能划分可方便的区分各区域名称。

【问题 2】

云数据中心是指以客户为中心、以服务为导向，基于高效、低能耗的 IT 与网络基础架构，利用云计算技术，自动化地按需提供各类云计算服务的新一代数据中心。云数据中心是传统数据中心的升级，是新一代数据中心的演进方向。

(1) 请简述云数据中心的特点。

(2) 云计算的关键技术有虚拟化技术、分布式计算技术、安全与隐私保护技术等，请简

要说明云数据中心在 IT 基础设施虚拟化技术方面主要包括哪些技术。

(1) 资源池化，高效智能，面向服务，按需供给，绿色低碳。

(2) 其中 IT 基础设施虚拟化技术包括网络虚拟化、服务器虚拟化及存储虚拟化。

云计算是一种将池化的集群计算能力通过互联网向内外部用户提供按需服务的互联网新业务，是传统 IT 领域和通信领域技术进步、需求推动和商业模式变化共同促进的结果，具有以网络为中心、以服务为提供方式、高扩展高可靠性、资源池化与透明化等 4 个特点，云计算的出现，使 IT 资源具备了可运营的条件。数据中心是云计算生态系统中的重要一环，在云计算模式下，信息的存储、处理、传递等功能均由网络侧完成，实际上由数据中心承担。由于传统数据中心存在资源利用率低、自动化程度低、能耗过高等一系列问题，无法有效承载云计算业务，因此基于云计算技术的新一代数据中心应运而生。

云数据中心是指以客户为中心、以服务为导向，基于高效、低能耗的 IT 与网络基础架构，利用云计算技术，自动化地按需提供各类云计算服务的新一代数据中心。云数据中心是传统数据中心的升级，是新一代数据中心的演进方向。云数据中心具有以下 5 个特点。

(1) 资源池化

云数据中心内的 IT 资源和网络资源将构成统一的资源池，实现物理资源与逻辑资源的去耦合，用户仅需对逻辑资源进行相关操作而无需关注底层实际物理设备。

(2) 高效智能

基于虚拟化、分布式计算等技术，利用低成本的集群设备实现高效廉价的信息承载、存储与处理，同时通过管理平台实现自动化的资源监控、部署与调度以及业务生命周期的智能管理。

(3) 面向服务

整体架构以服务为导向，通过松耦合的方式实现多服务的综合承载与提供，云数据中心由提供资源变成提供服务，用户通过服务 0 录选择相关的服务，对底层实际资源透明。

(4) 按需供给

底层基础架构在资源池化的基础上根据实际需求实现资源的动态伸缩，并提供完备的、细颗粒的计费功能，云数据中心还将根据上层应用的发展趋势，实现对底层物理设备的智能容量规划。

(5) 绿色低碳

通过模块化的设计以及虚拟化等绿色节能技术，降低云数据中心的设备投入成本以及运营维护成本，实现低 PUE 值的绿色低碳运营。

云计算的关键技术有虚拟化技术、分布式计算技术、安全与隐私保护技术等。

虚拟化技术是基础设施资源池建设的重要部分，虚拟化技术从软、硬件资:原中抽象出来，提供不同颗粒度，功能相同的虚拟资源。虚拟化技术将增加软、硬件的复用，提升基础设施资源的利用率、灵活性及安全性、可用性。

基础设施虚拟化技术包括网络虚拟化、服务器虚拟化及存储虚拟化。

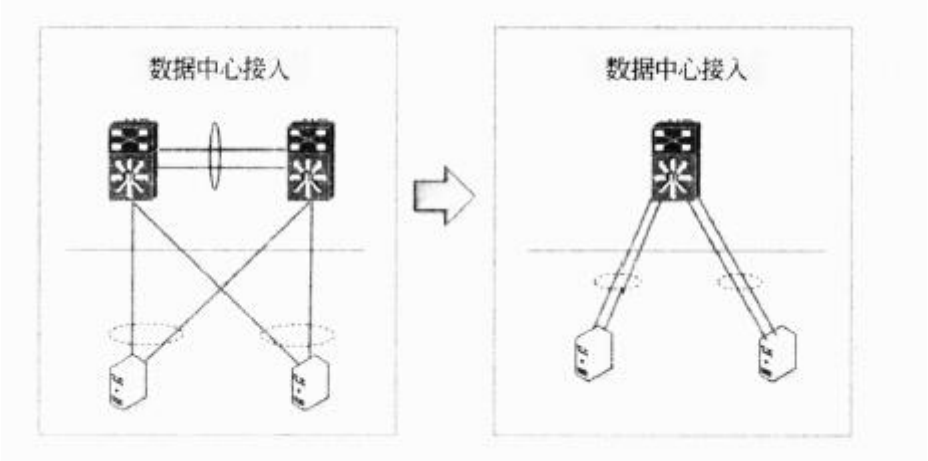
(1)网络虚拟化

相对于传统的物理网络资源，网络虚拟化能够带来的优点包括：虚拟网络资源带来了更好的灵活性及可扩展性；在不改变物理网络拓扑情况下，实现网络灵活配置满足信息系统的快速部署需求；通过共享的模式，最大限度地利用现有资源，降低成本。

常见的网络虚拟化包括：虚拟交换机、网络核心虚拟交换、虚拟防火墙等。

虚拟交换机包括基于软件或硬件设备虚拟交换机，单台交换机虚拟成多台虚拟交换机，实现虚拟服务器灵活的网络接入。主要提供虚拟服务器网络连接；实现对虚拟服务器网络配置策略的统一管理；实现物理刀片服务器的配置属性信息（网络及存储连接等）的集中管理，服务器的配置属性文件应用可加速失败服务器更换；实现虚拟服务器网络配置信息跨数据中心迁移。

M 络核心虚拟交换技术去除了由生成树协议带来的网络资源空闲的状态，将两台交换机虚拟成为一台交换机，并作单一设备进行管理和使用，在网络中表现为一个网元节点；网络核心虚拟交换将简化网络架构、简化管理及配置，进一步增强冗余可靠性。实现负载均衡，提高网络设备性能。网络核心虚拟交换如下图所示。



虚拟防火墙将一台物理防火墙虚拟成若干相互独立、功能相同的虚拟防火墙。提供网络

流量安全隔离功能，实现安全的虚拟网络环境。

(2)服务器虚拟化

服务器虚拟化的主要优点包括：提高服务器资源利用率，可减少能源消耗，降低基础设施总成本；提高运行在虚拟机上的应用系统的可用性；提高应用系统的安全性，实现快速备份及恢复。当前主流的服务器虚拟化技术包括：X86 服务器虚拟化及 Unix 服务器虚拟化。Unix 架构虚拟化技术包括分区技术及软件虚拟化技术，如下表所示。Unix 服务器架构的分区技术使操作系统能够直接访问到底层的物理资源，硬件分区技术支持的资源颗粒度较粗，例如最小单位是 1 颗 CPU;软件虚拟化技术的资源颗粒度较细，资源划分颗粒度较分区技术更小，资源调整更加灵活，例如最小单位是 0.1 颗 CPU。

技　术	特　性
硬件分区	具有硬件电气隔离功能； 分区的故障不影响其他分区，比如：HP　nPar。
逻辑分区	在硬件层上抽象出虚拟化层，对资源进行组合而成的逻辑分区； 独占的硬件资源，但没有电气隔离，比如: HP vPar, IBM Lpar。
软件虚拟化	在操作系统内，对特定应用分配计算资源。

Unix 服务器架构虚拟化使用：测试、开发环境对资源的要求灵活，需要使用多种的虚拟化技术，如硬件、逻辑分区、软件虚拟化；生产环境采用硬件分区或逻辑分区技术。X86 服务器虚拟化技术包括基于硬件的虚拟化技术和基于软件两种的虚拟化技术，

如下表所示。

技　术	特　性
基于硬件的虚拟化技术	在硬件层上抽象出虚拟化层，对资源进行组合而成的逻辑分区； 具有较高的性能；稳定性好；分区之间安全隔离。
基于软件的虚拟化技术	使用基于操作系统层之上的虚拟资源； 操作系统故障会影响所有虚拟机。

X86 服务器虚拟化使用：X86 服务器虚拟化技术已比较成熟，并且硬件虚拟化的技术已成为主流；开发、测试环境选用不同厂商基于硬件的 X86 服务器虚拟化技 X;生产环境采用基于硬件技术的 X86 服务器虚拟化技术，并选用成熟的、对 Windows 和 Linux 操作系统兼容的虚拟化技术，如 MicrosoftHyper-V、VMware 技术。

(3)存储虚拟化

存储虚拟化的优点包括：存储空间的统一分配，提高存储资源利用率；具有优异的灵活性及可扩展性；提供自动精简配置；自动数据迁移。

存储虚拟化主流技术包括基于主机的存储虚拟化，存储网络的虚拟化，以及基于存储设

备的虚拟化，如下表所示。

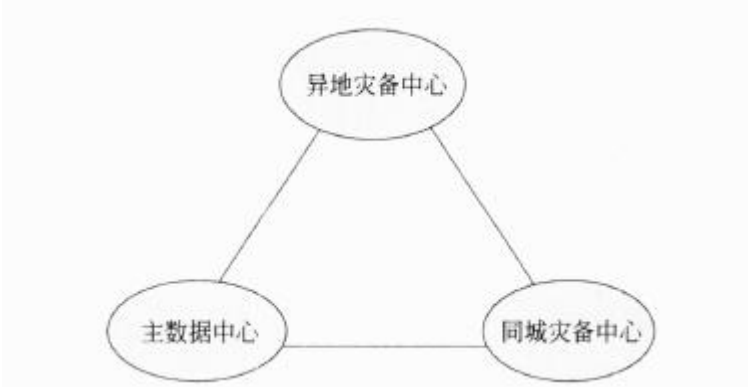
存储虚拟化主流技术	特　点
基于主机存储的虚拟化	通过在主机系统中安装额外的设备驱动和软件来提供对物理磁盘的虚拟化功能，经过虚拟化的存储空间可以跨多个异构的磁盘阵列； 存储管理占用主机性能，管理比较复杂，每台主机都需要安装管理软件。

续表

存储虚拟化主流技术	特　点
基于存储网络的虚拟化	通过向存储网中(SAN)中添加虚拟引擎，实现对异构存储设备的虚拟化管理，根据数据流向分为带内虚拟化及带外虚拟化。 带内虚拟化：带内虚拟化是在主机与存储设备之间引入一层虚拟化引擎，所有数据及控制信息传输均通过该引擎；虚拟化引擎对所有通过的数据进行运算。 带外虚拟化：带外虚拟化是指虚拟化引擎处于数据传输路径之外，数据传输并不通过该引擎，带外虚拟化引擎仅向主机传送一些控制信息来完成物理设备和逻辑卷之间的地址映射。 存储网络的虚拟化不占用主机及存储资源，扩展性较好，技术比较成熟。
基于存储设备的虚拟化	通过在存储控制器上添加虚拟化功能，实现存储磁盘的虚拟化管理；可以按需要对存储容量划分多个存储空间，实现多个主机系统的虚拟化管理；基于存储设备的虚拟化不占用主机及存储资源，扩展性较好，技术比较成熟。

【问题 3】

为增强该集团业务应用系统、重要数据的可用性，抵御灾难发生时带来的风险，该集团按照国家要求需要建设两地三中心的容灾备份方案。两地三中心是指主数据中心、同城灾备及异地灾备中心。两地三中心机房为业务应用系统建设提供基础配套设施。请画图说明两地三中心的数据中心架构采用的网络互联拓扑方案，并给出理由。



环型结构：在云计算这种多站点等同地位互联的大型数据中心组网下，环型结构不光节省设备节省费用，还能提供故障以及冗余保护。

为增强业务应用系统、重要数据的可用性，抵御灾难发生时带来的风险，集团需要建设两地三中心。两地三中心是指主数据中心、同城灾备及异地灾备中心。两地三中心机房为业务应用系统建设提供基础配套设施。

如果只有两个站点就不多说了，直接在两个站点的核心或汇聚设备之间拉两根光纤就OK了，也用不到什么特别的技术。唯一需要注意的是在两个站点之间的链路上做些报文控制，对广播和STP等报文限制一下发送速率和发送范围，避免一个站的广播风暴或拓扑收敛影响到其他站点的转发。

当站点为两个以上时，理论上有两种结构可用：

星型结构：专门找几台设备作为交换核心，所有站点都通过光纤直连到此组交换核心设备上，缺点是可靠性较低，核心不工作就都连不通了，而且交换核心放置的位置也不易规划。这种结构不是值得推荐的模型。

环型结构：推荐模型，尤其在云计算这种多站点等同地位互联的大型数据中心组网下，环型结构既省设备省钱，又能提供故障保护，以后肯定会成为建设趋势。

从技术上讲星型拓扑不需要额外的二层互联技术，只部署一些报文过滤即可，可以通过链路捆绑增强站点到核心间链路故障保护和链路带宽扩展。而环型拓扑必须增加专门的协议用于防止环路风暴，同样可以部署链路捆绑以增加带宽冗余。

环型拓扑的公共标准控制协议主要是STP和RPR(Resilient Packet Ring IEEE802.17),STP的缺点前面说了很多，RPR更适合数据中心多站点连接的环型拓扑。另外很多厂商开发了私有协议用于环路拓扑的控制，如EAPS(Ethernet Automatic Protection Switching,IETFRFC3619,Extreme Networks),RRPP(Rapid Ring Protection Protocol,H3C)MRP(Metro Ring Protocol,Foundry Networks).MMRP(Multi Mater Ring Protocol,Hitachi Cable),ERP(Ethernet Ring Protection,SiemensAG)等。未来几年的云计算数据中心建设，除非在所有站点采用相同厂家的设备还有可能使用一些私有协议组环（可能性比较低），前面提到预测会以站点为单位选择不同厂家进行建设，这时就需要公共标准用于多站点互联了。在光纤直连方式下成熟技术中最好的选择就是RPR。

根据以上分析,两地三中心的网络互联方案可考虑采用环型结构,具体拓扑结构见参考答案。

【问题4】

该集团数据存储量巨大,生产数据、安全数据以及测试数据等需要进行频繁的快速读写,为保障这种应用的需求,该集团希望在数据中心的数据存储方式上既要保证存储的可扩展性

还要保证数据的快速访问，同时对新服务器的部署也要考虑快速部署。

数据中心中数据采用的存储方式主要有 DAS、NAS、SAN 三种，请分别描述三种存储方式的原理，并根据集团要求设计在该集团的数据中心建设中应采用的存储方式，叙述采用这种方式的优点。

直连方式存储（Direct Attached Storage，DAS)。存储设备是通过电缆（通常是 SCSI 接口电缆）直接到服务器的。

网络附加存储（Network Attached Storage，NAS),是一种专门的数据存储技术的名称，它可以直接连接在标准的网络中（例如以太网），对异质网络用户提供了集中式数据访问服务。

存储区域网络（Storage Area Network,SAN)是一种连接外接存储设备和服务器的架构。采用包括光纤通道技术、磁盘阵列、磁带柜、光盘柜等各种技术进行实现。该架构的特点是，连接到服务器的存储设备，将被操作系统视为直接连接的存储设备。

本方案采用 SAN 的存储架构。优点是：扩展性，不仅存储空间可以很好的得到扩充，而且还可以得到块级数据访可功能。快速访问，对于那些要求大量磁盘访问的操作来说，SAN 具有更好的访问性能。即插即用，可以将服务器配置为没有内部存储空间的服务器，要求所有的系统都直接从 SAN(只能在光纤通道模式下实现）引导。

相比较 SAN 的优势和缺陷，并结合集团数据中心的建设需求，可以说采用 SAN 的存储架构对于大型国有集团是比较合理的。

存储技术经历了从基于服务器的存储（DAS)，基于磁盘阵列的存储（SCSI)发展到基于网络的存储模式（NAS 及 SAN)，在数据存储容量和读写速度上有较大幅度的提高，每秒传输的兆或者吉字节数和每秒完成的输入/输出量（IOPS)是存储设咎的性能的两种主要参数，目前的网络存储技术大致发展为三类：DAS、NAS 以及 SAN

(1) DAS

DAS 是一种将存储介质直接安装在服务器上或者安装在服务器外的存储方式。例如，将存储介质连接到服务器的外部 SCSI 通道上也可以认为是一种直连存储方式。

DAS 已经存在了很长时间，并且在很多情况下仍然是一种不错的存储选择。由于这种存储方式在磁盘系统和服务器之间具有很快的传输速率，在要求快速磁盘访问的情况下，DAS 仍然是--种理想的选择。更进一步地，在 DAS 环境中，运转大多数的应用程序都不会存在问题。对于那些对成本非常敏感的企业来说，在很长一段时间内，DAS 将仍然是一种比较便宜的存

储机制。当然，这是在只考虑硬件物理介质成本的情况下才有这种结论。如果与其他的技术进行一个全面的比较——考虑到管理开销和存储效率等方面的因素的话，DAS 将不再占有绝对的优势。对于那些非常小的不再需要其他存储介质的环境来说，这也是一种理想的选择。

(2) NAS

NAS 存储设备是以网络为中心面向文件服务的结构方式，NAS 存贮设备是单独作为一个文件服务器直接连接在网络上的，应用和数据存储部分不在同一服务器上，网络中设备的数据全部存贮在 NAS 存贮设备中，应用服务器通过标准 LAN 的接口与作为网络文件系统的数据服务器连接。NAS 存储系统能将数据从网络中独立出来，降'低了服务器的负载，从而较好提高了整个网络的性能。

在以下两种情形中，NAS 设备是非常合适的：首要的是网页服务，其次是常用文件的存储。这两种应用都需要大量的磁盘空间，但是很少要求直接对服务器进行数据访问。相反，通过这两种类型的存储访问的大多数数据都是通过网络来实现的。

NAS 设备适合于网页服务和文件服务，而不适合于数据库存储和 Exchange 存储。这与所谓的文件级数据访问和块级数据访问有关系。在文件级访问系统中，数据的访问是通过文件名字来实现的，因为文件名字是带有一定含义的。而在块级访问系统中，数据的访问是通过数据块的地址来实现的，这个地址是特定数据存放的位置。在一个客户机/服务器的环境中，如果需要从文件服务器读取一个文件时，要指定文件，服务器完成数据块的读取工作，并且将得到的数据返回就可以了。数据库存储和 Exchange 存储在这种方式的通信过程中存在着很多问题。所以并不适合存储于 NAS 设备中。

(3) SAN

SAN 是一种以光纤通道（FiberChannel，FC)实现服务器和存储设备之间通讯的网络结构，其中的服务器和存储系统通过高带宽 FC 交换机相连，各应用工作站通过局域网访问服务器，各存储设备之间交换数据时可以不通过服务器，能有效减少大流量数据传输时发生的阻塞和冲突，较大程度减轻服务器承受的压力，具有很强的灵活性和伸缩性。作为存储解决方案中的重要一员，SAN 是最昂贵的存储选项，同时也是最复杂的选项。然而，虽然 SAN 在初始阶段需要投入大量的费用，但是 SAN 却可以提供其他解决方案所不能提供的能力，并且可以在合适的情形下可以为公司节约一定的资金。

SAN 解决方案通常会采取以下两种形式：光纤信道以及 iSCSI 或者基于 IP 的 SAN。光纤信道是 SAN 解决方案中最熟悉的类型，但是，基于 iSCSI 的 SAN 解决方案开始大量出现在市场上，与光纤通道技术相比较而言，这种技术具有良好的性能，而且价格低廉。

SAN 真正的综合了 DAS 和 NAS 两种存储解决方案的优势。例如，在一个很好的 SAN 解决方案实现中，可以得到一个完全冗余的存储网络，这个存储网络具有不同寻常的扩展性，确切地说，可以得到只有 NAS 存储解决方案才能得到的几百太字节的存储空间，但是还可以得到块级数据访问功能，而这些功能只能在 DAS 解决方案中才能得到。对于数据访问来说，还可以得到一个合理的速度，对于那些要求大量磁盘访问的操作来说，SAN 显得具有更好的性能。利用 SAN 解决方案，还可以实现存储的集中管理，从而能够充分利用那些处于空闲状态的空间。更有优势的一点是，在某些实现中，甚至可以将服务器配置为没有内部存储空间的服务器，要求所有的系统都直接从 SAN(只能在光纤通道模式下实现）引导。这也是一种即插即用技术。

SAN 在需要容量扩容时只需要将新的 SAN 存储设备连接并入网络并进行简单的配置，即可实现在线扩容；并且 SAN 设备 RAID 组中同时损坏两块硬盘的情况下仍然可以保证数据完整不丢失，而且磁盘阵列无需重启即可更换损坏的硬盘，实现在线的数据容灾及备份性能。因此具有简易扩容及高效容错性能。

相比较 SAN 的优势和缺陷，并结合集团数据中心的建设需求，可以说采用 SAN 的存储架构对于大型国有集团是比较合理的。

试题三

某部队院校早期的一卡通建设方案主要为保障校内师生的图书、食宿、医疗等服务，系统包括了一卡通专网建设、一卡通平台建设、一卡通数据中心以及校园门禁与校园网视频监控等内容。行政办公、家属区、食堂、学生宿舍、开水房等营业网点逍过汇聚交换机接入到核心交换机，服务器及存储设备直接连接核心交换机，网络拓扑结沟如图 3-1 所示。

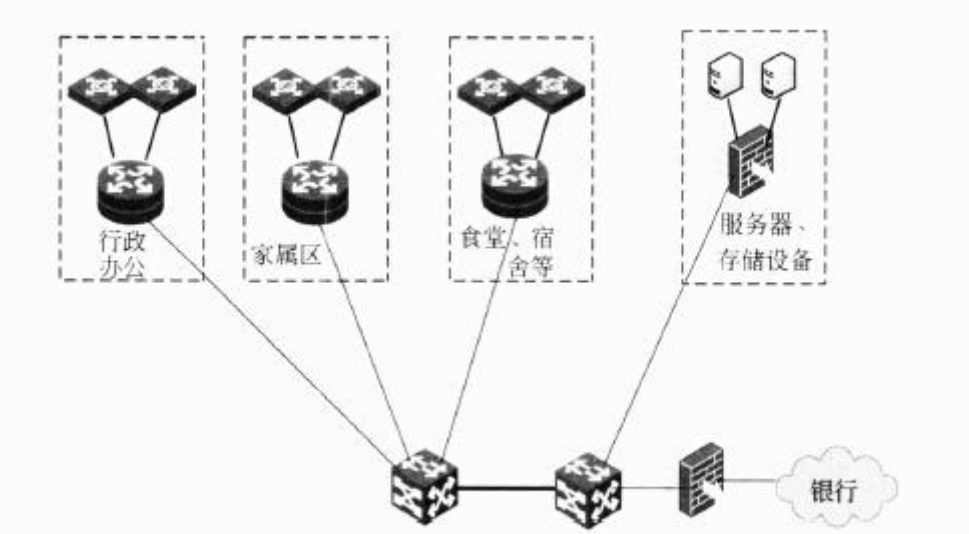


图 3-1

由于部队的医疗服务具有较高的知名度，经研究决定，扩大一卡通营业范围以方便社会人群的就医，具体安全要求如下：

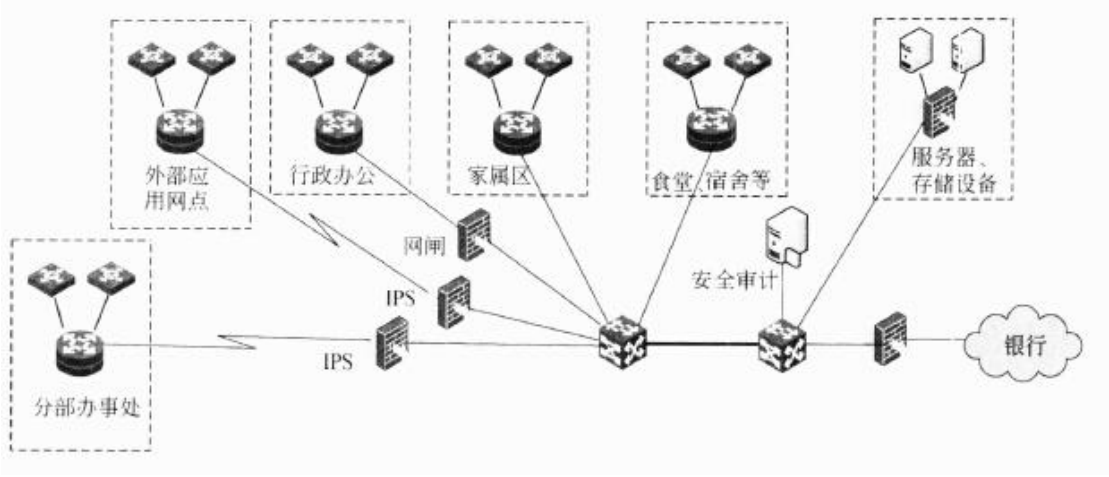
1. 新增外部应用网点和分部办事处，通过安全设备来进行远程接入，要求能提供主动、实时的防护，对网络中的数据流进行逐字节的检查，对攻击性的流量进行自动拦截。

2. 由于互联网的引入，需要相应的安全措施来保障部队院校行政办公的安全。

3. 需要提供安全审计功能，来识别、存储安全相关行为。

【问题 1】

依据一卡通业务扩大的需求及安全要求，设计解决方案，画出修改后的网络拓扑结构，并标注采用的硬件设备及相关安全技术。



(1) 外部网点要求外部网点和分部办事处能提供主动、实时的防护，对网络中的数据流进行逐字节的检查，对攻击性的流量进行自动拦截，合适的技术为 IDS 防火墙。

(2) 行政办公部门要保障安全，需采用网闸进行连接。

(3) 安全审计需接在核心交换机上，进行审计分析。

由于新增外部应用网点和分部办事处，通过安全设备来进行远程接入，要求能提供主动、实时的防护，对网络中的数据流进行逐字节的检查，对攻击性的流量进行自动拦截，因此需要采用具有 IPS 功能的防火墙。

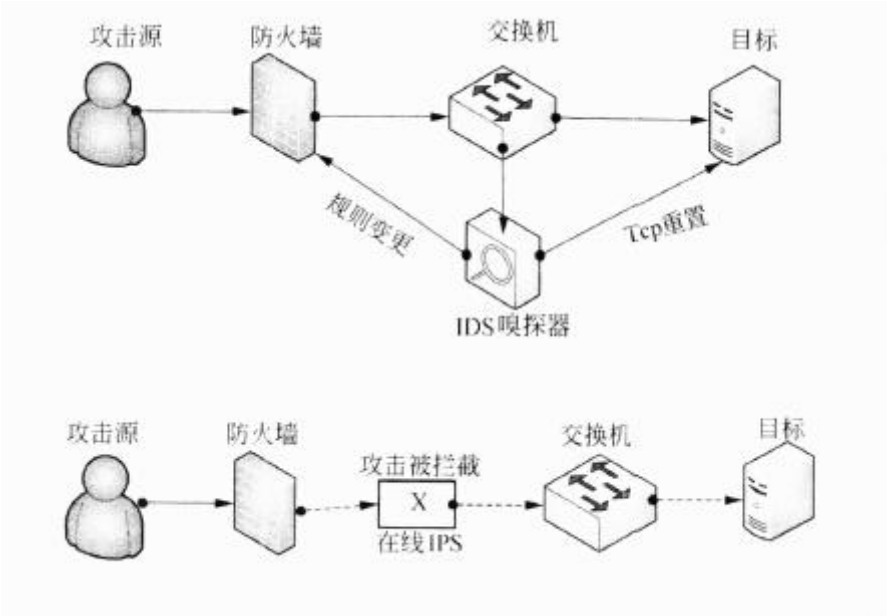
由于引入了互联网，部队院校行政办公的安全需要采用网闸来与 Internet 进行物理隔离。

安全审计功能需对所有进出系统的流量进行记录，来识别、存储安全相关行为。相应修改的拓扑结构见参考答案。

【问题 2】

传统的防火墙存在只能对网络层和传输层进行检查，无法阻止内部人员的攻击等缺点。IDS 和 IPS 技术却能在应用层对数据流进行分析，并在网络遭受攻击之前进行报警和响应，针对部署的方式和实现的原理对 IDS 和 IPS 进行比较。

IPS 和 IDS 的部署方式不同。串接式部署是 IPS 和 IDS 区别的主要特征，IDS 产品在网络中是旁路式工作，IPS 产品在网络中是串接式工作。



IPS 工作原理是：

(1) 根据数据包头和流信息如源目的地址源目的端口和应用层关键的信息每个数据包都会被分类，同时协议类型和流量统计等信息都送到流处理模块分析、审计。

(2) 根据数据报的分类，相关的过滤器将被调用，用于检查数据包的流状态信息。

(3) 所有相关过滤器都是并行使用，如果任何数据报符合过滤规则，与之相关的流信息将更新，指示系统删除关于该数据流的信息。

和 IDS 相比，IPS 检测到数据流中的恶意代码，核对策略，在未转发到服务器之前，将信息包或数据流拦截。

IPS 增加了网络负载。

【问题 3】

随着加密、隧道、认证等技术的发展，在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条安全的通讯线路，就可以为企业各部门提供安全的 M 络互联服务。针对该单位网络情况，请给出至少两种新增外部应用网点与公司核心交换机远程接入方案。

(1) 采用 VPN 技术，利用公共网络建立私有专用网络，数据通过安全的“加密隧道”在公共网络中传播，连接在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通讯线路，就好比是架设了一条专线一样。

(2) 端到端加密技术，通过加密算法，保障传输数据的安全性。

在 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条安全的通讯线路，主要的实现技术是采用 VPN 技术和端到端加密。

【问题 4】

直连方式存储（Direct Attached Storage，DAS)。存储设备是通过电缆（通常是 SCSI 接口电缆）直接到服务器的。

网络附加存储（Network Attached Storage，NAS),是一种专门的数据存储技术的名称，它可以直接连接在标准的网络中（例如以太网），对异质网络用户提供了集中式数据访问服务。

存储区域网络（Storage Area Network,SAN)是一种连接外接存储设备和服务器的架构。采用包括光纤通道技术、磁盘阵列、磁带柜、光盘柜等各种技术进行实现。该架构的特点是，连接到服务器的存储设备，将被操作系统视为直接连接的存储设备。

本方案采用 SAN 的存储架构。优点是：

扩展性，不仅存储空间可以很好的得到扩充，而且还可以得到块级数据访可功能。快速访问，对于那些要求大量磁盘访问的操作来说，SAN 具有更好的访问性能。即插即用，可以将服务器配置为没有内部存储空间的服务器，要求所有的系统都直接从 SAN(只能在光纤通道模式下实现）引导。

相比较 SAN 的优势和缺陷，并结合集团数据中心的建设需求，可以说采用 SAN 的存储架构对于大型国有集团是比较合理的。

安全审计的工作流程如下：

(1) 记录和搜集有关的审计信息，产生审计数据记录。

(2) 对数据记录进行安全违反分析，以检查安全违反与安全入侵原因。

(3) 对其分析产生相应的分析报表。

(4) 评估系统安全，并提出改进意见

安全审计主要的工作流程是搜集记录、分析检查、安全评估。具体流程如下：

(1) 记录和搜集有关的审计信息，产生审计数据记录。

(2) 对数据记录进行安全违反分析，以检查安全违反与安全入侵原因。

(3) 对其分析产生相应的分析报表。

(4) 评估系统安全，并提出改进意见。

试题一

随着网络技术的发展和企业规模的壮大，企业在全球各地的分支机构不断增多，员工及各分支机构要求能随时随地安全可靠地访问企业内部资源，这就需要提供一种安全接入机制来保障通信以及敏感信息的安全。传统的租用专用线路的方法实现私有网络连通给企业带来很大的经济负担和网络维护成本。VPN(Virtual Private Network)技术成为当今企业实现异地多网络互连以及远程访问网络的经济安全的实现途径。

请围绕“网络规划与设计中的 VPN 技术”论题，依次对以下三个方面进行论述。

1. 简要论述常用的 VPN 技术。
2. 详细叙述你参与设计和实施的大中型网络项目中采用的 VPN 方案。
3. 分析和评估你所采用的 VPN 方案的效果以及相关的改进措施。

一、对 VPN 技术和方案的叙述要点

1. VPN 技术的概念

虚拟专用网（VirtualPrivateNetwork,VPN)就是建立在公用网上的、由某一组织或某一群用户专用的通信网络，其虚拟性表现在任意一对 VPN 用户之间没有专用的物理连接，而通过 ISP 提供的公用网络来实现通信，其专用性表现在 VPN 之外的用户无法访问 VPN 内部的网络资源，VPN 内部用户之间可以实现安全通信。

2. 实现 VPN 的关键技术

隧道技术、加解密技术、密钥管理技术、身份认证技术。

3. VPN 的解决方案

(1) 内联网 VPN(IntranetVPN)：企业内部虚拟专用网也叫内联网 VPN，用于实现企业内部各个 LAN 之间的安全互联。

(2) 外联网 VPN(ExtranetVPN)：企业外部虚拟专用网也叫外联网 VPN，用于实现企业与客户、供应商和其他相关团体之间的互联互通。

(3) 远程接入 VPN(AccessVPN)：解决远程用户访问企业内部网络的传统方法是采用长途拨号方式接入企业的网络访问服务器（NAS)。这种访问方式的缺点是通信成本高，必须支付价格不菲的长途电话费，而且 NAS 和调制解调器的设备费用，以及租用接入线路的费用也是一笔很大的开销。采用远程接入 VPN 就可以省去这些费用。如果企业内部人员有移动或远程办公的需要，或者商家要提供 B2C 的安全访问服务，可以采用 AccessVPN。

4.虚拟专用网 VPN 的协议实现

隧道协议（例如 PPTP 和 L2TP），把数据封装在点对点协议（PPP)的帧中在互联网上传输，创建隧道的过程类似于在通信双方之间建立会话的过程，需要就地址分配、加密、认证和压缩参数等进行协商，隧道建立后才进行数据传输。

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

安全套接层(SecureSocketLayer,SSL)是传输层安全协议，用于实现 Web 安全通信。SSL 的安全连接是通过应用层的 Web 连接建立的，更适合移动用户远程访问公司的虚拟专用网。

二、叙述自己参与设计和实施的计算机网络项目，该项目应有一定的规模，自己在该项目中担任的主要工作应有一定的份量，说明项目中选用的 VPN 方案以及选用该方案的理由。

三、对选择的网络系统设计中 VPN 方案的效果以及需要进一步改进的地方，应有具体的着眼点，不能泛泛而谈。

试题二

校园网的建设有利于校内的资源共享与信息交换，有利于学校与外界的资源共享和信息共享。校园网的规划、设计、硬件建设、软件建设以及已有网络设备的使用及调优，都要从全局、长远的角度出发，充分考虑网络的安全性、易用性、可靠性和经济性等。资源调优、光纤连接和无线解决方案是保障校园网络可靠易用的几项关键技术。

请围绕“校园网设计关键技术及解决方案”论题，依次对以下三个方面进行论述。

1. 以你负责规划、设计及实施的校园网项目为例，概要叙述针对实际需求的设计要点，以及如何充分利用已有的软硬件，或对现有硬件资源的调优措施。

2. 具体讨论在校园网/企业网网络规划与设计中高性能的光纤连接关键技术、采用的无线技术及解决方案。

3. 具体讨论在上述关键技术的实施过程中遇到的问题和解决措施，以及实际运行效果。

以你负责规划、设计及实施的校园网项目为例，概要叙述针对实际需求的设计要点，以及如何充分利用已有的软硬件，或对现有硬件资源的调优措施。

(1) 叙述自己参与设计和实施的计算机网络项目。该项目应有一定的规模，自己的主要工作应有-定的份量。

(2) 项目中对软硬件的重新利用及调优方案。已有软硬件资源不适合整个网络环境的应该淘汰，可以用在要求较低环境中的可重利用，更高要求的要重新购置。

二、具体讨论在校园网/企业网网络规划与设计中光纤连接关键技术、采用的无线技术及解决方案。

在光纤连接技术方面：

(1) 光纤连接的总体环境。在光纤网络部署时首先要考虑距离、所要求达致的速率。

(2) 介质选择。依据距离、速率以及成本选择采用单模还是多模，考虑室内或是室外选择不同的光纤。

(3) 接口模块与成本预算。在介质选择完成后，需要考虑光纤接口模块，计算成本。

(4) 冗余。考虑到光纤日后扩展及链路备份，需要冗余链路。

在无线技术方面：

(1) 无线网络需求。不同的无线网络环境需要不同的速率和安全要求，需要描述所涉及网络的要求环境。

(2) 采用的无线局域网络标准。不同的速率和安全要求需要采用不同的标准，注意选择标准与需求相匹配。

(3) 无线网络的网络结构及覆盖范围。

(4) 选用的无线接入设备，包括无线路由器、AP 等。

三、具体讨论在上述关键技术的实施过程中遇到的问题和解决措施，以及实际运行效果。

(1) 在光纤连接和无线技术使用过程中遇到的问题及解决措施。

(2) 网络部署完成后实际的效果、达到的性能。