活动定义是项目时间管理中的过程之一，(1)是进行活动定义时通常使用的一种工具。

(1)A.Gantt 图　　B.活动图　　C.工作分解结构（WBS）　　D.PERT

**【答案】C**

**【解析】**

项目时间管理包括使项目按时完成所必须的管理过程。项目时间管理中的过程包括：活动定义、活动排序、活动的资源估算、活动历时估算、制定进度计划以及进度控制。为了得到工作分解结构（Work Break down Structure,WBS)中最底层的交付物，必须执行一系列的活动，对这些活动的识别以及归档的过程就叫做活动定义。

基于 RUP 的软件过程是一个迭代过程。一个开发周期包括初始、细化、构建和移交四个阶段，每次通过这四个阶段就会产生一代软件，其中建立完善的架构是（2）阶段的任务。采用迭代式开发，(3)。

(2)A.初始　　B.细化　　C.构建　　D.移交

(3)A.在每一轮迭代中都要进行测试与集成

B.每一轮迭代的重点是对特定的用例进行部分实现

C.在后续迭代中强调用户的主动参与

D.通常以功能分解为基础

**【答案】B　A**

**【解析】**

RUP 中的软件过程在时间上被分解为 4 个顺序的阶段，分别是初始阶段、细化阶段、构建阶段和移交阶段。

初始阶段的任务是为系统建立业务模型并确定项目的边界。细化阶段的任务是分析问题领域，建立完善的架构，淘汰项目中最高风险的元素。在构建阶段，要开发所有剩余的构件和应用程序功能,把这些构件集成为产品。移交阶段的重点是确保软件对最终用户是可用的。基于 RUP 的软件过程是一个迭代过程，通过初始、细化、构建和移交 4 个阶段就是一个开发周期，每次经过这 4 个阶段就会产生一代产品，在每一轮迭代中部要进行测试与集成。

以下关于白盒测试方法的叙述，不正确的是（4）。

(4)A.语句覆盖要求设计足够多的测试用例，使程序中每条语句至少被执行一次

B.与判定覆盖相比，条件覆盖增加对符合判定情况的测试，增加了测试路径

C.判定/条件覆盖准则的缺点是未考虑条件的组合情况

D.组合覆盖要求设计足够多的测试用例，使得每个判定中条件结果的所有可能组合最多出现一次

**【答案】**D

**【解析】**

白盒测试也称为结构测试，主要用于软件单元测试阶段，测试人员按照程序内部逻辑结构设计测试用例，检测程序中的主要执行通路是否都能按预定要求正确工作。白盒测试方法主要有控制流测试、数据流测试和程序变异测试等。

控制流测试根据程序的内部逻辑结构设计测试用例，常用的技术是逻辑覆盖。主要的覆盖标准有语句覆盖、判定覆盖、条件覆盖、条件/判定覆盖、条件组合覆盖、修正的条件/判定覆盖和路径覆盖等。

语句覆盖是指选择足够多的测试用例，使得运行这些测试用例时，被测程序的每个语句至少执行一次。

判定覆盖也称为分支覆盖，它是指不仅每个语句至少执行一次，而且每个判定的每种可能的结果（分支）都至少执行一次。

条件覆盖是指不仅每个语句至少执行一次，而且使判定表达式中的每个条件都取得各种可能的结果。

条件/判定覆盖同时满足判定覆盖和条件覆盖。它的含义是选取足够的测试用例，使得判定表达式中每个条件的所有可能结果至少出现一次，而且每个判定本身的所有可能结果也至少出现一次。

条件组合覆盖是指选取足够的测试用例，使得每个判定表达式中条件结果的所有可能组合至少出现一次。

修正的条件/判定覆盖。需要足够的测试用例来确定各个条件能够影响到包含的判定结果。

路径覆盖是指选取足够的测试用例，使得程序的每条可能执行到的路径都至少经过一次（如果程序中有环路，则要求每条环路路径至少经过一次）。

某企业拟生产甲、乙、丙、丁四个产品。每个产品必须依次由设计部门、制造部门和检验部门进行设计、制造和检验，每个部门生产产品的顺序是相同的。各产品各工序所需的时间如下表：

| 项目 | 设计（天） | 制造（天） | 检验（天） |
|---|---|---|---|
| 甲 | 13 | 15 | 20 |
| 乙 | 10 | 20 | 18 |
| 丙 | 20 | 16 | 10 |
| 丁 | 8 | 10 | 15 |

只要适当安排好项目实施顺序，企业最快可以在（5）天全部完成这四个项目。

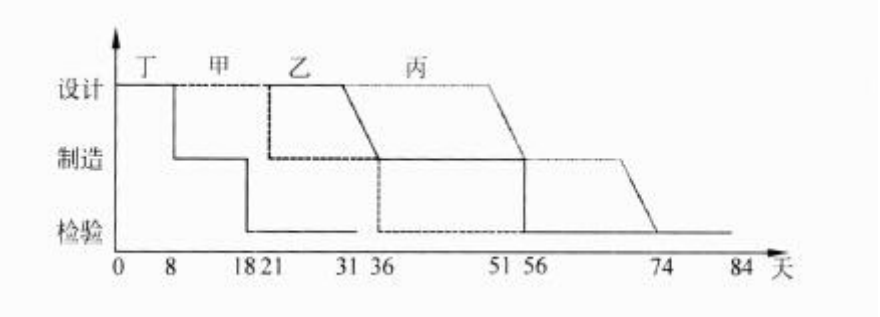
(5)A.84　　B.86　　C.91　　D.93

**【答案】A**

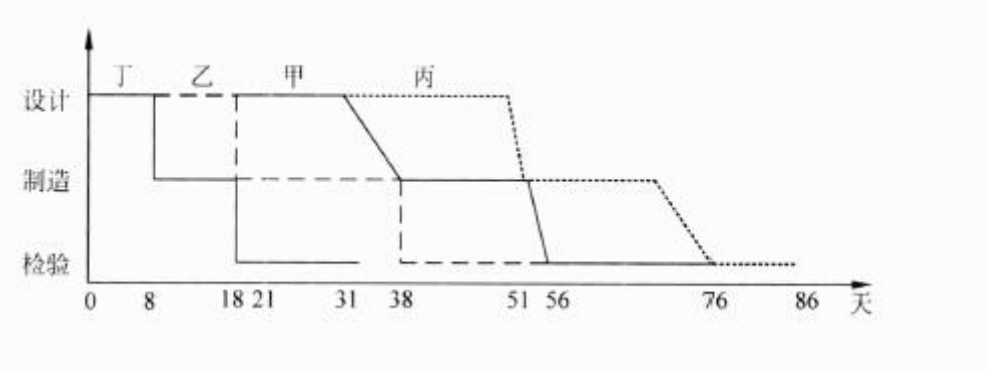
**【解析】本题考查数学应用的能力（优化运筹）。**

节省时间的安排方法必然是紧随衔接和尽可能并行安排生产。

第 1 个产品的设计和最后 1 个产品的检验是无法与其他工作并行进行的，因此，应安排“首个设计时间+末个检验时间”尽可能短。为此，应先安排生产丁，最后安排生产丙。如果按丁、甲、乙、丙顺序实施，则共需 84 天，如下图所示。




如果按丁、乙、甲、丙顺序实施，则共需 86 天，如下图所示。




下列关于面向对象软件测试的说法中，正确的是（6）。

(6)A.在测试一个类时，只要对该类的每个成员方法都进行充分的测试就完成了对该类充分的测试

B.存在多态的情况下，为了达到较高的测试充分性，应对所有可能的绑定都进行测

试

C.假设类B是类A的子类，如果类A已经进行了充分的测试，那么在测试类B时不必测试任何类B继承自类A的成员方法

D.对于一棵继承树上的多个类，只有处于叶子节点的类需要测试

**【答案】**B

**【解析】**

面向对象系统的测试目标与传统信息系统的测试目标是一致的，但面向对象系统的测试策略与传统结构化系统的测试策略有很大的不同，这主要体现在两个方面，分别是测试的焦点从模块移向了类，以及测试的视角扩大到了分析和设计模型。

与传统的结构化系统相比，面向对象系统具有三个明显特征，即封装性、继承性与多态性。封装性决定了面向对象系统的测试必须考虑到信息隐蔽原则对测试的影响，以及对象状态与类的测试序列，因此在测试一个类时，仅对该类的每个方法进行测试是不够的；继承性决定了面向对象系统的测试必须考虑到继承对测试充分性的影响，以及误用引起的错误；多态性决定了面向对象系统的测试必须考虑到动态绑定对测试充分性的影响、抽象类的测试以及误用对测试的影响。

以下关于自顶向下开发方法的叙述中，正确的是（7），

(7)A.自顶向下过程因为单元测试而比较耗费时间

B.自顶向下过程可以更快地发现系统性能方面的问题

C.相对于自底向上方法，自顶向下方法可以更快地得到系统的演示原型

D.在自顶向下的设计中，如发现了一个错误，通常是因为底层模块没有满足其规格说明（因为高层模块已经被测试过了）

**【答案】**C

**【解析】**

自顶向下方法是一种决策的策略。软件开发涉及作什么决策、如何决策和决策顺序等决策问题。

自顶向下方法在任何时刻所作的决定都是当时对整个设计影响最大的那些决定。如果把所有决定分组或者分级，那么决策顺序是首先作最高级的决定，然后依次地作较低级的决定。同级的决定则按照随机的顺序或者按别的方法。一个决定的级别是看它距离要达到的最终目的（因此是软件的实际实现）的远近程度。从问题本身来看，或是由外(用户所见的）向内

（系统的实现）看，以距离实现近的决定为低级决定，远的为高级决定。

在这个自顶向下的过程中，一个复杂的问题（任务）被分解成若干个较小较简单的问题（子任务），并且一直继续下去，直到每个小问题（子任务）都简单到能够直接解决（实现）为止。

自顶向下方法的优点是：

•可为企业或机构的重要决策和任务实现提供信息。

•支持企业信息系统的整体性规划，并对系统的各子系统的协调和通信提供保证。

•方法的实践有利于提高企业人员的整体观察问题的能力，从而有利于寻找到改进企业组织的途径。

自顶向下方法的缺点是：

•对系统分析和设计人员的要求较高。

•开发周期长，系统复杂，一般属于一种高成本、大投资的工程。

•对于大系统而言，自上而下的规划对于下层系统的实施往往缺乏约束力。

•从经济角度来看，很难说自顶向下的做法在经济上市合算的。

企业信息集成按照组织范围分为企业内部的信息集成和外部的信息集成。在企业内部的信息集成中，(8)实现了不同系统之间的互操作，使得不同系统之间能够实现数据和方法的共享；(9)实现了不同应用系统之间的连接、协调运作和信息共享。

(8)A.技术平台集成　　B.数据集成　　C.应用系统集成　　D.业务过程集成

(9)A.技术平台集成　　B.数据集成　　C.应用系统集成　　D.业务过程集成

**【答案】**C　　D

**【解析】本题考查企业信息集成的基础知识。**

企业信息集成是指企业在不同应用系统之间实现数据共享，即实现数据在不同数据格式和存储方式之间的转换、来源不同、形态不一、内容不等的信息资源进行系统分析、辨清正误、消除冗余、合并同类，进而产生具有统一数据形式的有价值信息的过程。企业信息集成是一个十分复杂的问题，按照组织范围来分，分为企业内部的，言息集成和外部的信息集成两个方面。按集成内容，企业内部的信息集成一般可分为以T四个方面：技术平台集成，数据集成，应用系统集成和业务过程集成。其中，应用系统集成是实现不同系统之间的互操作，使得不同应用系统之间能够实现数据和方法的共享；业务过程集成使得在不同应用系统中的流程能够无缝连接，实现流程的协调运作和流程信息的充分共享。

以下关于为撰写学术论文引用他人资料的说法，(10)是不正确的。

(10)A.既可引用发表的作品，也可引用未发表的作品

B.只能限于介绍、评论或为了说明某个问题引用作品

C.只要不构成自己作品的主要部分，可引用资料的部分或全部

D.不必征得著作权人的同意，不向原作者支付合理的报酬

**【答案】**A

**【解析】**

作品实际上是在吸纳和借鉴前人的多种智力成果的基础上而逐渐创作出来的。为了让作品能被更多的人所传播、利用与掌握，以有利于技术和文化的进步、发展，著作权法一方面向著作人授予精神、经济专有权利并保护这些权利所带来的利益，同时又对权利人行使其专有权利给予了一定的限制，便于公众接触、使用作品，为进一步提高技术和文化提供条件。著作权的限制主要体现在合理使用、法定许可使用两个方面。合理使用是指在特定的条件下，法律允许他人自由使用享有著作权的作品而不必征得著作权人的同意，也不必向著作权人支付报酬的行为，但应当指明作者姓名、作品名称，并且不得侵犯著作权人依照本法享有的其他权利。法定许可使用是指除著作权人声明不得使用外，便用人在未经著作权人许可的情况下，在向著作权人支付报酬时，指明著作权人姓名、作品名称，并且不侵犯著作权人依法享有的合法权利的情况下进行使用的行为。法定许可使用与合理使用的相同处在于：以促进社会公共利益、限制著作权人权利为目的；使用的作品限于已发表作品；无须征得著作权人的同意，但必须注明作者姓名、作品名称。我国著作权法第二十二条具体规定了合理使用的12种情形，一种情形是“为介绍、评论某一作品或者说明某一问题，在作品中适当引用他人已经发表的作品。”题干所述“引用是合理使用的一种，引用目的仅限于介绍、评论某一作品或者说明某一问题，所引用部分不能构成引用人作品的主要部分或者实质部分。

在ISO/OSI参考模型中，传输层采用三次握手协议建立连接，采用这种协议的原因是(11)。

(11)A.为了在网络服务不可靠的情况下也可以建立连接

B.防止因为网络失效或分组重复而建立错误的连接

C.它比两次握手协议更能提高连接的可靠性

D.为了防止黑客进行DOS攻击

【答案】B

【解析】

传输层协议使用三次握手过程建立连接，这种方法可以防止出现错误连接。大部分错误连接是由于迟到的或网络中存储的连接请求引起的。由于三次握手过程强调连接的双方都要提出自己的连接请求标识，也要应答对方的连接请求标识，所以不会受到过期的连接请求的干扰。

设卫星信道的传播延迟为270ms，数据速率为64kb/s，帧长4000比特，采用停等ARQ协议，则信道的最大利用率为（12）。

(12)A.0.480　　B.0.125　　C.0.104　　D.0.010

【答案】C

【解析】

停等ARQ协议的信道利用率为

$$E=\frac{1}{2a+1}$$

其中a= $t_p$ / $t_f$，$t_p$为信道延迟，$t_f$为帧发送或接收时间，这是在停等协议下链路的最高利用率，也可以认为是停等协议的效率。

本题中，卫星信道的传播延迟 $t_p$=270ms，$t_f$=4000÷64=62.5ms，所以：

$$a=270 / 62.5=4.32$$

于是

$$E=\frac{1}{2a+1}=\frac{1}{2\times 4.32+1}=\frac{1}{9.64}=0.104$$

在相隔2000km的两地间通过电缆以4800b/s的速率传送3000比特长的数据包，从开始发送到接收完数据需要的时间是（13），如果用50kb/s的卫星信道传送，则需要的时间是（14）。

(13)A.480ms　　B.645ms　　C.630ms　　D.635ms

(14)A.70ms　　B.330ms　　C.500ms　　D.600ms

【答案】D　B

【解析】

从开始发送到接收完数据需要的时间为信道传播延迟+数据包的接收（或发送）时间。通过电缆传送数据包的传播延迟=2000km÷200m/μs=10ms，数据包的接收时间=3000÷4800=625ms，所以从开始发送到接收完数据需要的时间为635ms。

通过卫星信道传送数据包时，信道传播延迟=270ms，数据包的接收时间=3000÷50k=60ms，所以从开始发送到接收完数据需要的时间为330ms。

10 个 9.6kb/s 的信道按时分多路复用在一条线路上传输，在统计 TDM 情况下，假定每个子信道只有 30%的时间忙，复用线路的控制开销为 10%，那么复用线路的带宽应该是(15)。

(15)A.32kb/s　　B.64kb/s　　C.72kb/s　　D.96kb/s

**【答案】A**

**【解析】**

根据题意计算如下：9.6Kb/sX10X30%÷90%=32kb/s

关于 HDLC 协议的流量控制机制，下面的描述中正确的是（16）。

(16)A.信息帧(I)和管理帧（S)的控制字段都包含发送顺序号

B.当控制字段 C 为 8 位长时，发送顺序号的变化范围是 0～127

C.发送完一个信息帧(I)后，发送器就将其发送窗口向前移动一格

D.接收器成功接收到一个帧后，就将其接收窗口后沿向前移动一格

**【答案】D**

**【解析】**

HDLC 协议采用固定大小的滑动窗口协议进行流量控制。信息帧和控制帧是编号帧,管理帧是无编号帧；当控制字段为 8 位长时，帧编号只有 3 位长，取值范围为 0～7;发送器只有在收到肯定应答后才能向前移动窗口;接收器成功收到一个帧后,就将其窗口向前移动一格，并送回肯定应答信号。

由域名查询 IP 地址的过程分为递归查询和迭代查询两种，其中递归查询返回的结果为(17),而迭代查询返回的结果是（18）。

(17)A.其他服务器的名字或地址　　B.上级域名服务器的地址

C.域名所对应的 IP 地址或错误信息　　D.中介域名服务器的地址

(18)A.其他服务器的名字或地址　　B.上级域名服务器的地址

C.域名所对应的 IP 地址或错误信息　　D.中介域名服务器的地址

**【答案】C　A**

**【解析】**

IP 地址的解析过程分为递归查询和迭代查询两种，递归查询返回的结果为域名对应的 IP 地址或错误信息，而迭代查询返回的结果是其他服务器（包括中介域名服务器和上级域

名服务器）的名字或地址。

为了满足不同用户的需求，可以把所有自动获取 IP 地址的主机划分为不同的类别，下面的选项列出的划分类别的原则中合理的是（19）。

(19)A.移动用户划分到租约期较长的类　　B.固定用户划分到租约期较短的类

C.远程访问用户划分到默认路由类　　D.服务器划分到租约期最短的类

**【答案】**C

**【解析】**

在配置动态 IP 地址时对用户进行分类的原则是：移动用户划分到租约;钥较短的类别；固定用户划分到租约期较长的类别；远程访问用户划分到默认路由类；服务器分配静态 IP 地址。

TCP 协议在建立连接的过程中可能处于不同的状态，用 netstat 命令显示出 TCP 连接的状态为 SYN_SEND，则这个连接正处于（20）。

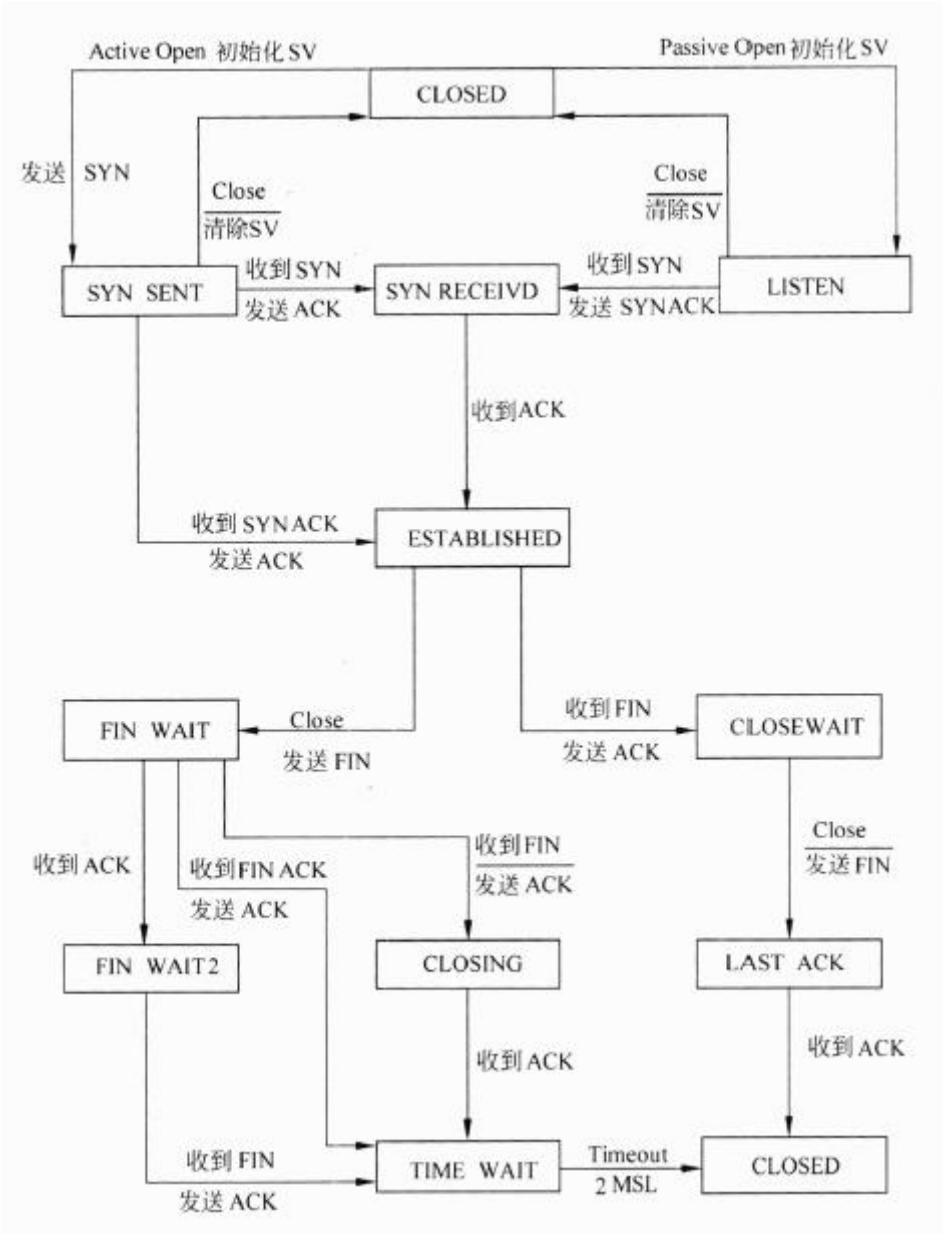
(20)A.监听对方的建立连接请求　　B.已主动发出连接建立请求

C.等待对方的连接释放请求　　D.收到对方的连接建立请求

**【答案】**B

**【解析】**

TCP 的连接状态如图 1 所示，由图看出，当 TCP 实体主动发出连接请求（SYN)后处于 SYN_SEND 状态。




自动专用 IP 地址（Automatic Private IP Address,APIPA)是 IANA 保留的一个地址块，其地址范围是（21）。

(21)A.A 类地址块 10.254.0.0～10.254.255.255

B.A 类地址块 100.254.0.0～100.254.255.255

C.B 类地址块 168.254.0.0～168.254.255.255

D.B 类地址块 169.254.0.0～169.254.255.255

**【答案】**D

**【解析】**

自动专用 IP 地址 APIPA 的范围是 B 类地址块 169.254.0.0～169.254.255.255。

下面关于 GPRS 接入技术的描述中，正确的是（22）。

(22)A.GPRS 是一种分组数据业务

B.GPRS 是一种第三代移动通信标准

C.GPRS 提供的数据速率可以达到 1Mb/s

D.GPRS 是一种建立在 CDMA 网络上的数据传输技术

**【答案】A**

**【解析】**

通用分组无线业务 GPRS(General Packet Radio Service)是一种 2.5G 移动通信系统。2.5G 系统能够提供 3G 系统中才有的一些功能，例如分组交换业务，也能共享 2G 时代开发出来的 TDMA 或 CDMA 网络。GPRS 分组网络重叠在 GSM 网络之上，利用 GSM 网络中未使用的 TDMA 信道，为用户提供中等速度的移动数据业务。

GPRS 是基于分组交换的技术，多个用户可以共享带宽，每个用户只有在传输数据时才会占用信道,所有的可用带宽可以立即分配给当前发送数据的用户,适合于 Web 浏览、E-mail 收发和即时消息那样的共享带宽的间歇性数据传输业务。通常，GPRS 系统是按交换的字节数计费，而不是连接时间计费。GPRS 系统支持 IP 协议和 PPP 协议。理论上的分组交换速度大约是 170kb/s,而实际速度只有 30～70kb/s。

对 GPRS 的射频部分进行改进的技术方案称为增强数据速率的 GSM 演进(Enhanced Datarates for GSM Evolution,EDGE)。EDGE 又称为增强型 GPRS(EGPRS：',可以工作在已经部署 GPRS 的网络上，只需要对手机和基站设备做一些简单的升级。EDGE 被认为是 2.75G 技术，采用 8PSK 的调制方式代替了 GSM 使用的高斯最小移位键控（GMSK)调制方式，使得一个码元可以表示 3 比特信息。理论上说,EDGE 提供的数据速率是 GSM 系统的 3 倍。2003 年 EDGE 被引入北美的 GSM 网络，支持从 20～200kb/s 的高速数据传输，最大数据速率取决于同时分配到的 TDMA 帧的时隙的多少。

IEEE802.3 规定的 CSMA/CD 协议可以利用多种监听算法来减小发送冲突的概率，下面关于各种监听算法的描述中，正确的是（23）。

(23)A.非坚持型监听算法有利于减少网络空闲时间

B.坚持型监听算法有利于减少冲突的概率

C.P 坚持型监听算法无法减少网络的空闲时间

D.坚持型监听算法能够及时抢占信道

【答案】D

【解析】

以太网的监听算法分为3种：

非坚持型监听算法可以最大限度地减少冲突概率，但是可能会延迟发送，引起带宽的浪费；坚持型监听算法能及时抢占信道，但是会增加冲突的概率。P-坚持型监听算法既可以及时抢占信道，也不会增加冲突的概率，但是算法复杂，需要根据网络的负载情况进行仔细的调整。

采用以太网链路聚合技术将（24）。

(24)A.多个逻辑链路组成一个物理链路　　B.多个逻辑链路组成一个逻辑链路

C.多个物理链路组成一个物理链路　　D.多个物理链路组成一个逻辑链路

【答案】D

【解析】

IEEE802.3ad定义了链路聚合控制协议（Link Aggregation Control Protocol,LACP),它的功能是将多个物理链路聚合成一个逻辑链路。链路汇聚技术可以将多个链路绑定在一起，形成一条高速链路，以达到更高的带宽，并实现链路备份和负载均衡。

RIP是一种基于（25）的内部网关协议，在一条RIP通路上最多可包含的路由器数量是（26）。

(25)A.链路状态算法　B.距离矢量算法　C.集中式路由算法　D.固定路由算法

(26)A.1个　　B.16个　　C.25个　　D.无数个

【答案】B　　B

【解析】

RIP是一种基于距离矢量算法的内部网关协议，在一条RIP通路上最多V包含的路由器数量是16个。

关于实现QoS控制的资源预约协议RSVP，下面的描述中正确的是（27）。

(27)A.由发送方向数据传送路径上的各个路由器预约带宽资源

B.由发送方向接收方预约数据缓冲资源

C.由接收方和发送方共同商定各条链路上的资源分配

D.在数据传送期间，预约的路由信息必须定期刷新

【答案】D

【解析】

资源预约协议 RSVP 是根据用户要求的服务质量，由连接的接收方（或下游结点）向中间路由器（或上游结点）预约资源。预约的资源是一种“软状态”，必须定期进行更新。

OSPF 协议使用（28）分组来保持与其邻居的连接。

(28)A.Hello B.Keepalive C.SPF(最短路径优先） D.LSU(链路状态更新）

【答案】A

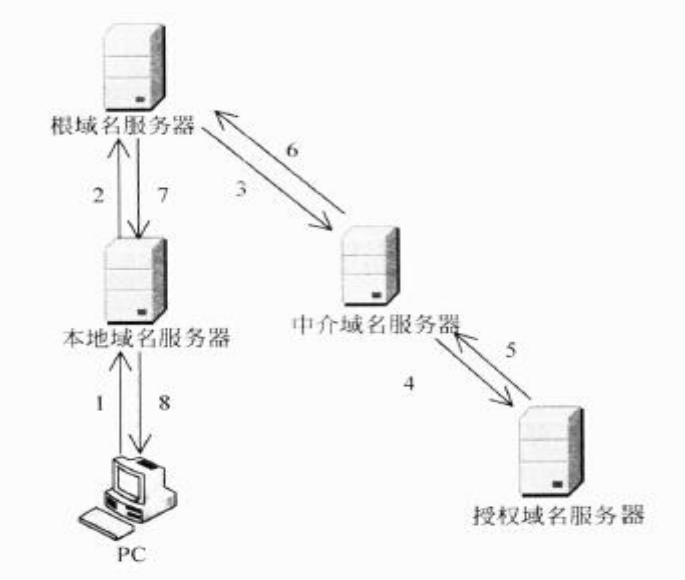
【解析】

OSPF 的 5 种报文如表 1 所示，这些报文通过 TCP 连接传送。OSPF 路由器启动后以固定的时间间隔传播 Hello 报文，采用的目标地址 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 协议用于发现邻居，建立毗邻关系，还用于选举区域内的指定路由器 DR 和备份指定路由器 BDR。

表 1 OSPF 的 5 种报文类型

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

主机 PC 对某个域名进行查询，最终由该域名的授权域名服务器解析并返回结果，查询过程如下图所示。这种查询方式中不合理的是（29）。




(29)A.根域名服务器采用递归查询，影响了性能

B.根域名服务器采用迭代查询，影响了性能

C.中介域名服务器采用迭代查询，加重了根域名服务器负担

D.中介域名服务器采用递归查询，加重了根域名服务器负担

**【答案】**A

**【解析】本题考查 DNS 服务器及其原理。**

DNS 查询过程分为两种查询方式：递归查询和迭代查询。

递归查询的查询方式为：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。

迭代查询的查询方式为：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。

根域名服务器为众多请求提供域名解析，若采用递归方式会大大影响性能。

如果 DNS 服务器更新了某域名的 IP 地址，造成客户端无法访问网站，在客户端通常有两种方法解决此问题：

1. 在Windows命令行下执行（30）命令;

2. 停止系统服务中的（31）服务。

(30)A.nslookup　　B.ipconfig/renew

C.ipconfig/flushdns　　D.ipconfig/release

(31)A.SNMP Client　　B.DNS Client

C.Plug and Play　　D.Remote Procedure Call (RPC)

**【答案】C　B**

**【解析】本题考查DNS服务器及其原理。**

当DNS服务器更新了某域名的IP地址后,客户端可能由于缓存中的域名记录尚未更新，无法访问网站，此时可以通过命令ipconfig/flushdns或停止服务DNSClient来更新。

某单位采用DHCP进行IP地址自动分配，经常因获取不到地址受到用户的抱怨，网管中心决定采用Networking Monitor来监视客户端和服务器之间的通信。为了寻找解决问题的方法，重点要监视（32）DHCP消息。

(32)A.Dhcp Discover　B.Dhcp Offer　C.Dhcp Nack　D.Dhcp Ack

**【答案】C**

**【解析】本题考查DHCP服务器及其原理。**

由于用户获取不到地址，说明服务器没能正常的提供Offer,因此需要从DhcpNack报文中查找原因。

网络需求分析包括网络总体需求分析、综合布线需求分析、网络可用性与可靠性分析、网络安全性需求分析，此外还需要进行（33）。

(33)A.工程造价估算　B.工程进度安排　C.硬件设备选型　D.IP地址分配分

**【答案】A**

**【解析】本题考查网络需求分析。**

工程造价估算是网络需求分析中的一个重要环节。

某金融网络要求网络服务系统的可用性达到5个9,也就是大于99.999%,那么每年该金融网络系统的停机时间小于（34）方能满足需求。

(34)A.5分钟　B.10分钟　C.60分钟　D.105分钟

【答案】A

【解析】本题考查网络服务系统可用性的计算方法。

性达到99.999%，则每年的平均无故障时间为：

每年的平均修复时间为MTBR=(1-0.99999)X365X24X60=5.256分钟。所以每年的停机时间必须小于5分钟才能满足要求。

采用可变长子网掩码可以把大的网络划分成小的子网，或者把小的网络汇聚成大的超网。假设用户U1有4000台主机，则必须给他分配（35）个C类网络，如果分配给用户U1的超网号为196.25.64.0,则指定给U1的地址掩码为（36）;假设给用户U2分配的C类网络号为196.25.16.0～196.25.31.0，则U2的地址掩码应为（37）；如果路由器收到一个目标地址为11000100.00011001.01000011.00100001的数据报，则该数据报应送给用户（38）。

(35)A.4　　B.8　　C.10　　D.16

(36)A.255.255.255.0　　B.255.255.250.0

C.255.255.248.0　　D.255.255.240.0

(37)A.255.255.255.0　　B.255.255.250.0

C.255.255.248.0　　D.255.255.240.0

(38)A.U1　　B.U2　　C.U1或U2　　D.不可到达

【答案】D　D　D　A

【解析】

用户U1有4000台主机，则必须给他分配16个C类网络（256X16），则指定给U1的地址掩码应为255.255.240.0。

给用户U2分配的C类网络号为196.25.16.0～196.25.31.0,其中包含16八C类网络，所以用户U2的地址掩码应为255.255.240.0。

用户U1的网络地址196.25.64.0/20：11000100.00011001.01000000.00000000

用户U2的网络地址196.25.64.0/20：11000100.00011001.00100000.00000000

路由器收到的数据报目标地址为： 11000100.00011001.01000011.00100001

根据最长匹配原则，该数据报应送给用户U1。

在IPv6地址无状态自动配置过程中，主机首先必须自动形成一个唯一的(39),然后向路由器发送（40）请求报文，以便获得路由器提供的地址配置信息。

(39)A.可聚集全球单播地址　　B.站点本地单播地址

C.服务器本地单播地址　　D.链路本地单播地址

(40)A.Neighbor Solicitation　　B.Router Solicitation

C.Router Advertisement　　D.Neighbor Discovery

**【答案】D　B**

**【解析】**

在无状态自动配置过程中，主机通过两个阶段分别获得链路本地地址和可聚合全球单播地址。首先主机将其网卡 MAC 地址附加在地址前缀 1111111010 之后，产生一个链路本地地址，并发出一个 ICMPv6 邻居发现请求报文，以验证其地址的唯一性。如果请求没有得到响应，则表明主机自我配置的链路本地地址是唯一的。否则，主机将使用一个随机产生的接口 ID 组成一个新的链路本地地址。获得链路本地地址后，主机以该地址为源地址，向本地链路中所有路由器组播路由器请求（Router Solicitation)报文，路由器以一个包含可聚合全球单播地址前缀的路由器公告（Router Advertisement)报文响应。主机用从路由器得到的地址前缀加上自己的接口 ID，自动配置一个全球单播地址，这样就可以与 Internet 中的任何主机进行通信了。

下面 ACL 语句中，准确表达“允许访问服务器 202.110.10.1 的 WWW 服务”的是(41)。

(41)A.access-list 101 permit any 202.110.10.1

B.access-list 101 permit tcp any host 202.110.10.1 eq www

C.access-list 101 deny any 202.110.10.1

D.access-list 101 deny tcp any host 202.110.10.1 eq www

**【答案】B**

**【解析】本题考查 ACL 语句。**

正确的 ACL 语句为：access-list 101 permit tcp any host 202.110.10.1 eq www。

SSL 协议共有上下两层组成，处于下层的是（42）。

(42)A.SSL 握手协议（SSL Handshake protocol)

B.改变加密约定协议（Change Cipher spec protocol)

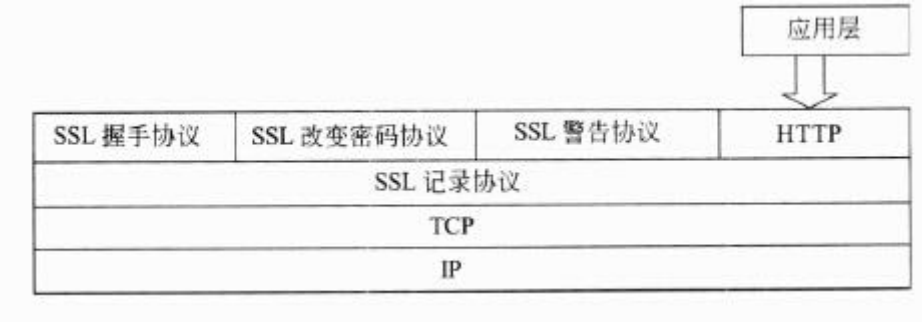
C.报警协议（Alert protocol)

D.SSL 记录协议（SSL Record Protocol)

【答案】D

【解析】本试题考查 SSL 协议及组成。

SSL 协议分为两层，底层是 SSL 记录协议，运行在传输层协议 TCP 之上，用于封装各种上层协议。一种被封装的上层协议是 SSL 握手协议，由服务器和客户端用来进行身份认证，并且协商通信中使用的加密算法和密钥。SSL 协议栈如下图所示。




ISO 7498-2 标准规定的五大安全服务是（43）。

(43)A.鉴别服务、数字证书、数据完整性、数据保密性、抗抵赖性

B.鉴别服务、访问控制、数据完整性、数据保密性、抗抵赖性

C.鉴别服务、访问控制、数据完整性、数据保密性、计费服务

D.鉴别服务、数字证书、数据完整性、数据保密性、计费服务

【答案】B

【解析】本试题考查 ISO7498-2 标准。

ISO7498-2 标准中描述了开放系统互联安全的体系结构，提出设计安全的 f1 息系统的基础架构中应该包含 5 种安全服务（安全功能)、能够对这 5 种安全服务提供支持的 8 类安全机制和普遍安全机制，以及需要进行的 5 种 OSI 安全管理方式。其中 5 神安全服务为：鉴别服务、访问控制、数据完整性、数据保密性、抗抵赖性；8 类安全机制：加密、数字签名、访问控制、数据完整性、数据交换、业务流填充、路由控制、公证。

下面关于第三方认证服务说法中，正确的是（44）。

(44)A.Kerberos 认证服务中保存数字证书的服务器叫 CA

B.第三方认证服务的两种体制分别是 Kerberos 和 PKI

C.PKI 体制中保存数字证书的服务器叫 KDC

D.Kerberos 的中文全称是“公钥基础设施”

【答案】B

【解析】本题考查认证服务。

Kerberos 可以防止偷听和重放攻击，保护数据的完整性。Kerberos 的安全机制如下。

• AS(Authentication Server)：认证服务器，是为用户发放 TGT 的服务器。

• TGS(Ticket Granting Server)：票证授予服务器，负责发放访问应用服务器时需要的票证。认证服务器和票据授予服务器组成密钥分发中心（Key Distribution Center,KDC)。

• V：用户请求访问的应用服务器。

• TGT(Ticket Granting Ticket)：用户向 TGS 证明自己身份的初始票据，即 KTGS(A,KS) 。

公钥基础结构（Public Key Infrastructure,PKI)是运用公钥的概念和技术来提供安全服务的、普遍适用的网络安全基础设施，包括由 PKI 策略、软硬件系统、认证中心、注册机构（Registration Authority,RA)、证书签发系统和 PKI 应用等构成的安全体系。

下面安全协议中，IP 层安全协议是（45)。

(45)A.IPsec　　B.L2TP　　C.TLS　　D.PPTP

【答案】A

【解析】本题考查安全协议的工作层次。

IPsec、L2TP、PPTP 均是隧道协议，其中 L2TP、PPTP 工作在数据链路层，IPsec 工作在 IP 层；TLS 是传输层安全协议。

采用 Kerberos 系统进行认证时，可以在报文中加入（46）来防止重放攻击。

(46)A.会话密钥　　B.时间戳　　C.用户 ID　　D.私有密钥

【答案】B

【解析】本题考查 Kerberos 系统认证。

时间戳可用来进行防重放攻击.

某单位建设一个网络,设计人员在经过充分的需求分析工作后,完成了网络的基本设计。但是，由于资金受限，网络建设成本超出预算，此时，设计人员正确的做法是(47)。

(47)A.为符合预算，推翻原设计，降低网络设计标准重新设计

B.劝说该单位追加预算，完成网络建设

C.将网络建设划分为多个周期，根据当前预算，设计完成当前周期的建设目标

D.保持原有设计，为符合预算降低设备性能，采购低端设备

**【答案】C**

**【解析】本题考查网络的需求分析与设计。**

若网络建设成本超出预算，需根据当前预算，设计完成当前周期的建设目标。

某数据中心根据需要添加新的数据库服务器。按照需求分析，该数据库服务器要求具有高速串行运算能力，同时为了该服务器的安全，拟选用 Unix 操作系统。根据以上情况分析，该服务器应选择（48）架构的服务器。其中（49）系列的 CPU 符合该架构。若选用了该 CPU，则采用（50）操作系统是合适的。

| | | | |
|---|---|---|---|
| (48)A.RISC | B.CISC | C.IA-32 | D.VLIW |
| (49)A.Opteron | B.Xeon | C.Itanium | D.Power |
| (50)A.HP-UX | B.Solaris | C.AIX | D.A/UX |

**【答案】A D C**

**【解析】本题考查服务器的基础知识。**

按服务器的处理器架构(即服务器 CPU 所采用的指令系统)可把服务器划分犬 RISC 架构服务器和 IA 架构服务器。后者包括 CISC 架构服务器和 VLIW 架构服务器两种。

其中 RISC 的指令系统相对简单，它只要求硬件执行很有限且最常用的那部分指令，大部分复杂的操作则使用成熟的编译技术，由简单指令合成。目前在中高档服务 I#特别是高档服务器普遍采用 RISC 指令系统的 CPU。

配备 RISC 架构 CPU 的服务器一般采用 Unix 操作系统，其具备高速运算能力，并且由于使用 Unix 操作系统，其安全性、可靠性较高。

根据题目要求需要选择数据库服务器，数据库服务器对于处理器性能要求很高。数据库服务器需要根据需求进行查询，然后将结果反馈给用户。如果查询请求非常多，比如大量用户同时查询的时候，如果服务器的处’理能力不够强，无法处理大量的查询请求并做出应答。同时为了数据库服务器的安全，拟选用 Unix 操作系统，所以此时应选取 RISC 架构服务器。IBM 公司的 Power 系列处理器是 RISC 处理器芯片，Opteron(皓龙）是美国 AMD 公司生产基于 X86-64 架构的 CPU,Xeon 则是 Intel 公司的 X86 架构的 CPU,而 Itanium(官方中文名称为安腾)，是 IntelItanium 架构（通常称之为 IA-64)的 64 位处理器。根据问题（48)可以判定，此处应选择 Power 系列的 CPU。

由于确定采用IBM公司的Power系列处理器，所以操作系统的选取就应该为AIX。这是因为RISC架构服务器采用的主要是封闭的发展策略，即由单个厂商提供垂直的解决方案，从服务器的系统硬件到系统软件都由这个厂商完成。AIX是IBM开发的一套Unix操作系统，其全面支持IBM公司的Power系列处理器;HP-UX全称为Hewlett Packard UniX,是惠普9000系列服务器的操作系统，可以在HP的PA-RISC处理器、Intel的Itanium处理器的电脑上运行；Solaris是Sun Microsystems研发的Unix操作系统操作系统，其支持多种系统架构：SPARC,x86andx64； A/UX(Apple Unix)是苹果电脑(AppleComputer)公司所开发的UNIX操作系统，此操作系统可以在该公司的一些麦金塔电脑(Macintosh)上运行。

网络安全设计是网络规划与设计中的重点环节，以下关于网络安全设计原则的说法，错误的是（51）。

(51)A.网络安全应以不能影响系统的正常运行和合法用户的操作活动为前提

B.强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽可能快地恢复网络信息中心的服务，减少损失

C.考虑安全问题解决方案时无需考虑性能价格的平衡,强调安全与保密系统的设计应与网络设计相结合

D.充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测，是设计网络安全系统的必要前提条件

**【答案】**C

**【解析】本题考查网络安全设计。**

网络安全应以不能影响系统的正常运行和合法用户的操作活动为前提；强调安全防护、监测和应急恢复。要求在网络发生被攻击的情况下，必须尽可能快地恢复网络信息中心的服务，减少损失；考虑性能价格的平衡，强调安全与保密系统的设计应与网络设计相结合；充分、全面、完整地对系统的安全漏洞和安全威胁进行分析、评估和检测，是设计网络安全系统的必要前提条件。

某财务部门需建立财务专网，A公司的李工负责对该网络工程项目进行逻辑设计，他调研后得到的具体需求如下：

①用户计算机数量40台，分布在二层楼内，最远距离约60米；

②一共部署7个轻负载应用系统,其中5个系统不需要Internet访问,2个系统需要Internet

访问；

李工据此给出了设计方案，主要内容可概述为：

①出口采用核心交换机+防火墙板卡设备组成财务专网出口防火墙，并通过防火墙策略将需要 Internet 访问的服务器进行地址映射；

②财务专网使用 WLAN 为主，报账大厅用户、本财务部门负责人均可以访问财务专网和 Internet；

③采用 3 台高性能服务器部署 5 个不需要 Internet 访问的应用系统，1 台高性能服务器部署 2 个需要 Internet 访问的应用系统。

针对用户访问，你的评价是（52）。

针对局域网的选型，你的评价是（53）。

针对服务器区的部署，你的评价是（54）。

(52)A.用户权限设置合理

B.不恰当，报账大厅用户不允许访问 Internet

C.不恰当，财务部门负责人不允许访问 Internet

D.不恰当，财务部门负责人不允许访问财务专网

(53)A.选型恰当　　B.不恰当，WLAN 成本太高

C.不恰当，WLAN 不能满足物理安全要求　D.不恰当，WLAN 不能满足覆盖范围的要

(54)A.部署合理

B.不恰当，7 个业务系统必须部署在 7 台物理服务器上

C.不恰当，没有备份服务器，不能保证数据的安全性和完整性

D.不恰当，所有服务器均需通过防火墙策略进行地址映射

**【答案】**B　C　C

**【解析】本题考查逻辑网络设计、物理网络设计的相关知识。**

从用户的主要需求可以看出，覆盖范围最远距离未超出 90 米，可以覆盖；

财务专网是安全级别比较高的财务部门内部网络，如果采用 WLAN 为主，不能满足物理安全要求，要求一般财务人员只能访问财务专网进行办公，不能访问 Internet。

业务系统最好按照允许访问对象划分部署，通过防火墙进行安全防火和地址转换，但是业务系统中数据非常重要，所以必须有备份服务器来保证数据的安全性和完整性。

按照 IEEE802.3 标准，以太帧的最大传输效率为（55）.

(55)A.50% B.87.5% C.90.5% D.98.8%

**【答案】D**

**【解析】本题考查以太帧的基础知识。**

按照 IEEE802.3 标准，标准以太帧的最大 MTU 值为 1500Bytes，而在以太帧申头标记和 CRC(Cyclic Redundancy Check)共有 18Bytes，所以其最大传输效率 1500/1518=98.8%。

以下关于层次化网络设计原则的叙述中，错误的是（56）。

(56)A.层次化网络设计时，一般分为核心层、汇聚层、接入层三个层次

B.应当首先设计核心层，再根据必要的分析完成其他层次设计

C.为了保证网络的层次性，不能在设计中随意加入额外连接

D.除去接入层，其他层次应尽量采用模块化方式，模块间的边界应非常清晰

**【答案】B**

**【解析】本题考查层次化网络设计原则的基础知识。**

层次化网络设计应该遵循一些简单的原则,这些原则可以保证设计出来的网络更加具有层次的特性：

①在设计时，设计者应该尽量控制层次化的程度，一般情况下，由核心层、汇聚层、接入层三个层次就足够了，过多的层次会导致整体网络性能的下降，并且会提高网络的延迟，同时也方便网络故障排查和文档编写。

②在接入层应当保持对网络结构的严格控制,接入层的用户总是为了获得更大的外部网络访问带宽，而随意申请其他的渠道访问外部网络，这是不允许的。

③为了保证网络的层次性,不能在设计中随意加入额外连接,额外连接是指打破层次性，在不相邻层次间的连接，这些连接会导致网络中的各种问题，例妇缺乏汇聚层的访问控制和数据报过滤等。

④在进行设计时，应当首先设计接入层，根据流量负载、流量和行为的分析，对上层进行更精细得容量规划，再依次完成各上层的设计。

⑤除去接入层的其他层次，应尽量采用模块化方式，每个层次由多模块或者设备集合构成，每个模块间的边界应非常清晰。

在以下各种网络应用中，节点既作为客户端同时又作为服务端的是（57）。

(57)A.P2P 下载 B.B/S 中应用服务器与客户机之间的通信

C.视频点播服务　　D.基于 SNMP 协议的网管服务

**【答案】A**

**【解析】本题考查网络应用的基础知识。**

B/S 中应用服务器与客户机之间的通信、视频点播服务和基于 SNMP 协议的网管服务在工作是基于 Client/Server 和 Browse/Server 模式，这些模式的特点是：它们都是以应用为核心的，在网络中必须有应用服务器，用户的请求必须通过应用服务器完成。而 P2P 下载服务是对等网络结构，网上各台节点有相同的功能，无主从之分，一个节点都是既可作为服务器，又可以作为工作站。

在 OSPF 中，路由域存在骨干域和非骨干域，某网络自治区域中共有 10 个路由域，其区域 id 为 0～9,其中(58)为骨干域。

(58)A.Area 0　　B.Area 1　　C.Area 5　　D.Area 9

**【答案】A**

**【解析】本题考查 OSPF 的基础知识。**

在 OSPF 中，采用分区域计算，将网络中所有 OSPF 路由器划分成不同的区域，每个区域负责各自区域精确的 LSA 传递与路由计算,然后再将一个区域的 LSA 简化和汇总之后转发到另外一个区域。区域的命名可以采用整数数字，如 1、2、3、4,也可以采用 IP 地址的形式，0.0.0.1、0.0.0.2,因为采用了 Hub-Spoke 的架构，所以必须定义出一个核心，然后其他部分都与核心相连，OSPF 的区域 0 就是所有区域的核心，称为 BackBone 区域（骨干区域)，而其他区域称为 Normal 区域（常规区域)。

测试工具应在交换机发送端口产生（59）线速流量来进行链路传输速率测试。

(59)A.100%　　B.80%　　C.60%　　D.50%

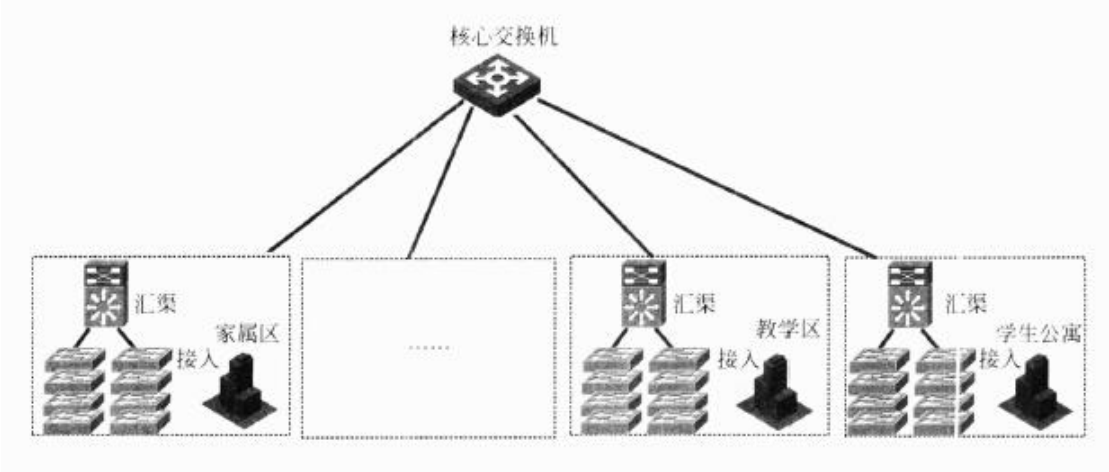
**【答案】A**

**【解析】本题考查网络系统测试过程中，针对交换机发送端口进行链路传输速率测试的标准。**

在交换机发送端口产生 100%满线速流量，在 HUB 发送端口产生 50%线速流量。

某高校的校园网由 1 台核心设备、6 台汇聚设备、200 台接入设备组成，网络拓扑结构如下图所示，所有汇聚设备均直接上联到核心设备，所有接入设备均直接上联到汇聚设备，

在网络系统抽样测试中，按照抽样规则，最少应该测试(60)条汇聚层到核心层的上联链路和(61)条接入层到汇聚层的上联链路。




(60)A.3　　B.4　　C.5　　D.6

(61)A.20　　B.30　　C.40　　D.50

**【答案】**D　A

**【解析】本题考查网络系统抽样测试中的抽样规则**

对核心层的骨干链路，应进行全部测试;对汇聚层到核心层的上联链路，应进行全部测试；对接入层到汇聚层的上联链路，以不低于10%的比例进行抽样测试，抽样链路数不足10条时，按10条进行计算或者全部测试。

该网络中汇聚层到核心层，共6条上联链路，接入层到汇聚层一共200条上联链路。根据该抽样规则，则一共应测试6条汇聚层到核心层上联链路，20条接入层到汇聚层的上联链路。

某公司主营证券与期货业务，有多个办公网点，要求企业内部用户能够高速地访问企业服务器，并且对网络的可靠性要求很高。工程师给出设计方案：

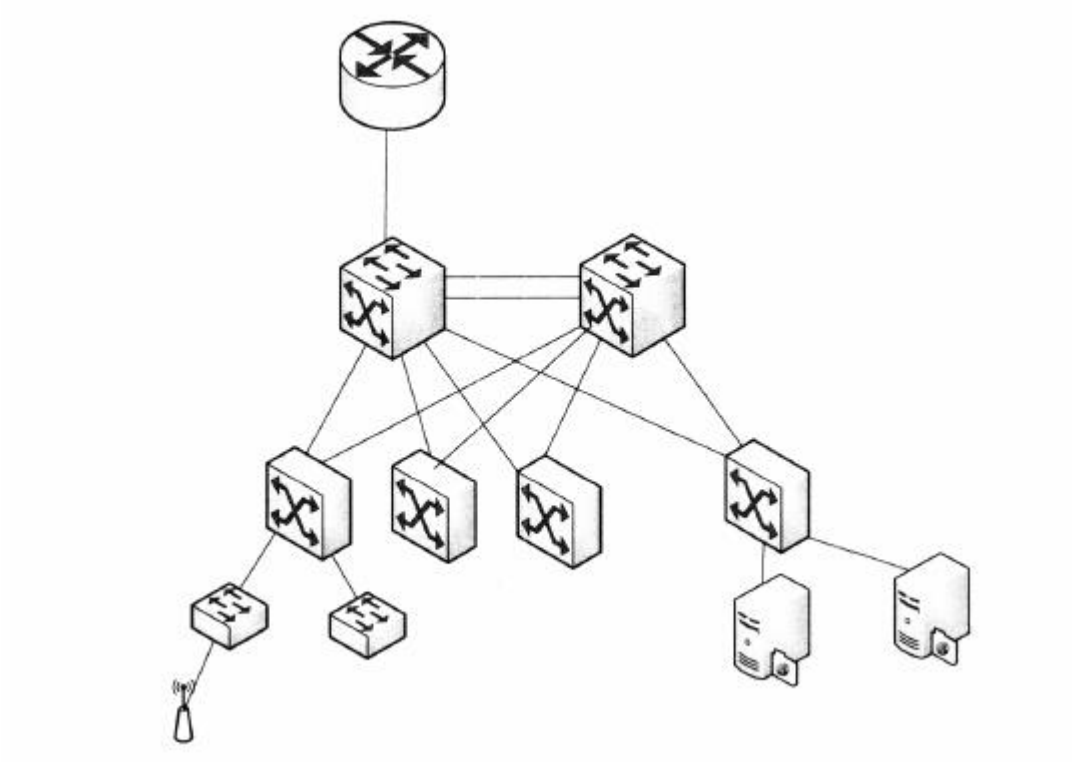
①采用核心层、汇聚层、接入层三层结构；

②骨干网使用千兆以太网；

③为了不改变已有建筑的结构，部分网点采用WLAN组网；

④根据企业需求，将网络拓扑结构设计为双核心来进行负载均衡，当其中一个核心交换机出现故障时，数据能够转换到另一台交换机上，起到冗余备份的作用。

网络拓扑如下图所示。



针对网络的拓扑设计，你的评价是（62）。

(62)A.恰当合理

B.不恰当，两个核心交换机都应直接上联到路由器上，保证网络的可靠性

C.不恰当，为保证高速交换，接入层应使用三层交换机

D.不恰当，为保证核心层高速交换，服务器应放在接入层

**【答案】B**

**【解析】本题考查网络规划与设计。**

两个核心交换机都应直接上联到路由器上，采用冗余连接保证网络的可靠性：接入层只是保障用户接入，无需三层交换机；服务器放在接入层影响访问速度。

一台 CISCO 交换机和一台 H3C 交换机相连，互联端口都工作在 VLAN TRUNK 模式下，这两个端口应该使用的 VLAN 协议分别是（63）.

(63)A.ISL 和 IEEE 802.10　　B.ISL 和 ISL

C.ISL 和 IEEE 802.1Q　　D.IEEE 802.1Q 和 IEEE 802.1Q

**【答案】D**

**【解析】本题考查 VLANTRUNK 的基本知识。**

在交换设备之间实现 VLANTRUNK 功能，必须遵守相同的 VLAN 协议标准。

目前，在交换设备中常用的VLAN协议有ISL(Cisco公司内部交换链路协议)、IEEE802.10(原为FDDI的安全标准协议)和国际标准IEEE802.1Q。其中，ISL(Inter-SwitchLink)是Cisco交换机内部链路的一个VLAN协议，它是个私有协议，仅适用于Cisco设备。IEEE802.10的正式名称是IEEE802.10InteroperableLAN/MAN Security Standard,是一个OSI第二层的协议，包括了验证（Authentication)和加密（Encryption)等机制。其目的是在数据链路层内安全地交换数据，为此它定义了称为安全数据互换（SDE:Secure Data Exchange)的协议数据单元（PDU)。虽然802.10确实是一个标佳，但它毕竟只是一个安全性标准，并不能完全满足虚拟网的需要，而且目前对802.10报头中域的使用，各厂家仍是各自为政，互不兼容。IEEE802.1Q标准提供了对VLAN明确的定义及其在交换式网络中的应用。该标准的发布，确保了不同厂商产品的互操作能力，并在业界获得了广泛的推广。它成为VLAN发展史上的里程碑。IEEE802.1Q的出现打破了VLAN依赖于单一厂商的僵局，从一个侧面推动了VLAN的迅速发展。因此，在不同厂家交换机互连要实现VLANTRUNK.功能时，必须在直接相连的两台交换机端口都封装IEEE802.1Q协议，从而保证协议的一致性，否则不能正确地传输多个VLAN信息。

在进行无线WLAN网络建设时，现在经常使用的协议是IEEE 802.11b/g/n，采用的共同工作频带为（64）。其中为了防止无线信号之间的干扰，IEEE将频段分为13个信道，其中仅有三个信道是完全不覆盖的，它们分别是（65）。

(64)A.2.4GHz　　B.5 GHz　　C.1.5GHz　　D.10GHz

(65)A.信道1、6和13　　B.信道1、7和11

C.信道1、7和13　　D.信道1、6和11

**【答案】A　D**

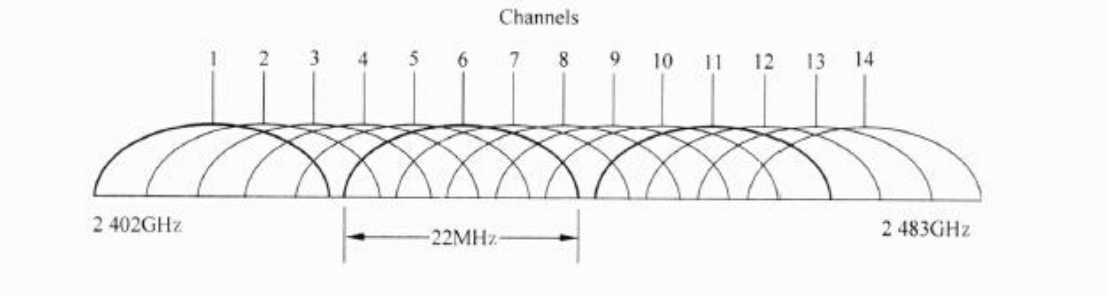
**【解析】本题考查WLAN的有关基本知识。**

(64)802.11是IEEE最初制定的一个无线局域网标准，主要用于解决网络用户与甲户终端的无线接入；其中802.11a工作在5.4G频段、最高速率54兆、主要用在远距离的无线连接；802.11b工作在2.4G频段、最高速率11兆、目前已经逐步被淘汰；802.11g工作在2.4G频段、最高速率54兆；802.11n工作在2.4GHz或者5GHz、最高速率可达600兆。因此IEEE802.11b/g/n，采用的共同工作频带为2.4GHz。

(65) 目前主流的无线WIFI网络设备不管是802.11b/g还是802.11b/g/n一般都支持13个信道。它们的中心频率虽然不同，但是因为都占据一定的频率范围，所以会有一些相互重

叠的情况。信道也称作通道（Channel)、频段，是以无线信号（电磁波）作为传输载体的数据信号传送通道。无线网络（路由器、AP 热点、电脑无线网卡）可在多个信道上运行。在无线信号覆盖范围内的各种无线网络设备应该尽量使用不同的信道，以避免信号之间的干扰。下表是常用的 2.4GHz(=2400MHz)频带的信道划分。实际一共有 14 个信道（图中画出了第 14 信道)，但第 14 信道一般不用。表中列出的是信道的中心频率。每个信道的有效宽度是 20MHz，另外还有 2MHz 的强制隔离频带。即对于中心频率为 24:2MHz 的 1 信道，其频率范围为 2401～2423MHz。

| 信道 | 中心频率 | 信道 | 中心频率 | 信道 | 中心频率 |
|---|---|---|---|---|---|
| 1 | 2412MHz | 2 | 2417MHz | 3 | 2422MHz |
| 4 | 2427MHz | 5 | 2432MHz | 6 | 2437MHz |
| 7 | 2442MHz | 8 | 2447MHz | 9 | 2452MHz |
| 10 | 2457MHz | 11 | 2462MHz | 12 | 2467MHz |
| 13 | 2472MHz | | | | |




从上图中很容易看到其中 1、6、11 这三个信道（红色标记）之间是完全没有交叠的，也就是三个不互相重叠的信道，每个信道 20MHz 带宽。图中也很容易看清楚其他各信道之间频谱重叠的情况。另外，如果设备支持，除 1、6、11 三个一组互不干扰的信道外，还有 2、7、12;3、8、13；4、9、14 三组互不干扰的信道。

在网络数据传输过程中都是收、发双向进行的。一般来说，对于光纤介质也就需要两条光纤分别负责数据的发送和接收。近年来已经有了在单条光纤上同时传输收发数据的技术，下面支持单条光纤上同时传输收发数据的技术是（66）。

(66)A.WiFi 和 WiMAX　B.ADSL 和 VDSL　C.PPPoE 和 802.1x　D.GPON 和 EPON

**【答案】D**

**【解析】**

无源光网络（Passive Optical Network,PON)是一种纯介质网络，PON 目前主要有 GPON(ITU 协议）和 EPON(IEEE 协议）两种协议技术。

通过 PON，单根光纤从服务提供商的设备延伸到靠近居民区或商务中心的位置。“无源”是指该系统在服务提供商和客户之间不需要电源和有源的电子组件。它仅由光纤、分路器、接头和连接器组成。一根光纤可为多个客户提供服务，而此前的系统要求每个客户都有独立的光纤，这样就大大节省了光纤资源。

光缆布线工程结束后进行测试是工程验收的关键环节。以下指标中不属于光缆系统的测试指标的是（67）。

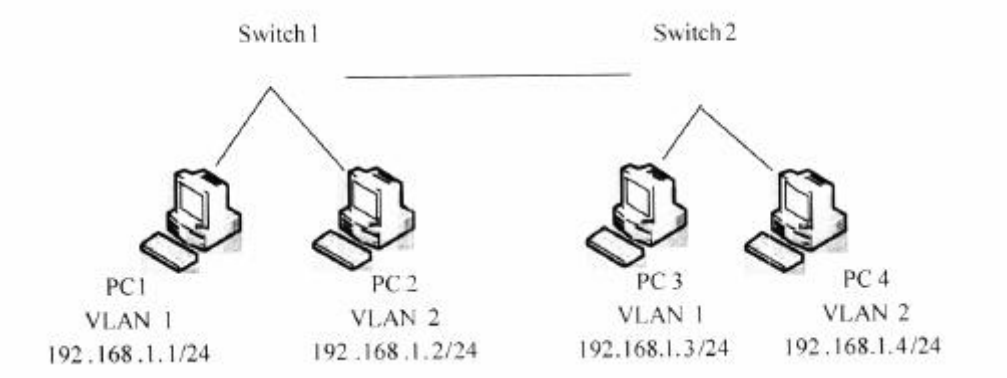
(67)A.最大衰减限值　　B.回波损耗限值　　C.近端串扰　　D.波长窗口参数

**【答案】**C

**【解析】本题主要考察光缆布线工程中对光缆系统的测试指标。**

其中近端串扰(NearEndCross-Talk(NEXT))是指在 UTP 电缆链路中一对线与另一对线之间的因信号耦合效应而产生的串扰，是对性能评价的最主要指标，近端串扰用分贝（dB)来度量，不属于光缆系统的测试指标。

如图所示网络结构，当 Switch1 和 Switch2 都采用默认配置，那么 PC2 和 PC4 之间不能通信，其最可能的原因是（68）。如果要解决此问题，最快捷的解决方法是（69）。




(68)A.PC2 和 PC4 的 IP 地址被交换机禁止通过

B.PC2 和 PC4 的 VLAN 被交换机禁止通过

C.PC2 和 PC4 的 MAC 地址被交换机禁止通过

D.PC2 和 PC4 的接入端口被交换机配置为 down

(69)A.把 Switch1 和 Switch2 连接端口配置为 trunk 模式

B.把 Switch1 和 Switch2 连接端口配置为 access 模式

C.把 Switch1 和 Switch2 设备配置为服务器模式

D.把 Switch1 和 Switch2 设备配置为客户端模式

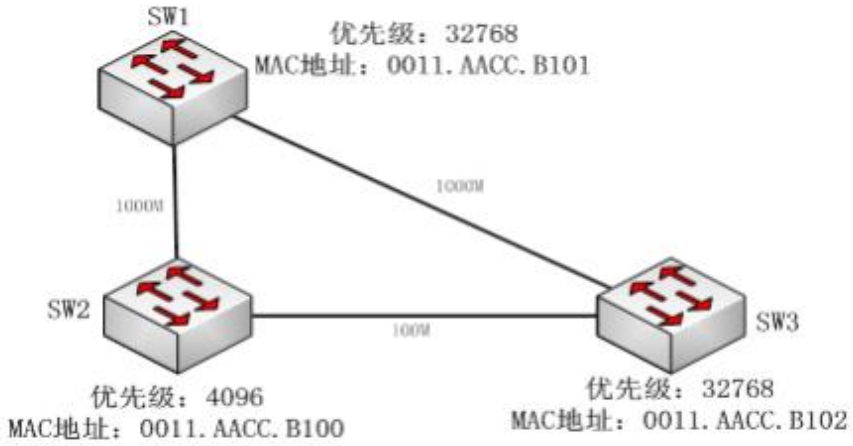
**【答案】B A**

**【解析】本题考查交换机基本配置的相关知识。**

根据题意及图中所示，Switch1 和 Switch2 采用默认配置，则 IP 地址、MAC 地址都不会被禁止，端口也为激活状态。在没有配置 VLAN 之前，由交换机互连的网终默认同属于 VLAN1。VLAN1 也是默认的本征 VLAN。本征 VLAN 是指交换机允许默认传输信息的 VLAN。对于不是本征 VLAN 的其他 VLAN 默认是不允许在交换机之间传输信息的。

PC2 和 PC4 的 IP 地址为同一网段，也属于同-•VLAN(VLAN2)。PC2 和 PC4 之间不能通信的原因可能是 Switch1 和 Switch2 的连接端口不允许除本征 VLAN 之外的其他 VLAN(VLAN2)通过，默认情况下 Switch1 和 Switch2 连接端口为 access 模式，因此，要解决此问题，最快捷的解决方法是把 Switch1 和 Switch2 连接端口配置为 trunk 模式，该模式下允许多个不同的 VLAN 通过。

在 STP 生成树中，断开的链路并不是随意选择的，而是通过设备、接口、链路优先级等决定的。在下图所示的连接方式中，哪条链路是作为逻辑链路断开而备份使用的？(70)。




(70)A.SW1 和 SW2 之间的链路　　B.SW1 和 SW3 之间的链路

C.SW2 和 SW3 之间的链路　　D.任意断开一条皆可

**【答案】C**

**【解析】本题考查 STP 生成树的有关知识。**

在 STP 生成树中，断开的链路并不是随意选择的，而是通过设备、接口、链路优先级等决定的。具体的原则为：首先在局域网中找一台设备为根桥，根桥由桥 ID 的大小决定，桥 ID 值最小的设备为根桥。桥 ID=桥优先级+桥 MAC 地址 ，其中“桥”就是“网桥”，即交换

机。默认情况下交换机的优先级都是 32768,如果需要某一台设备为根桥的话，直接将其优先级改小即可，不过交换机的优先级规定必须为 4096 的倍数。

如图所示，SW2 是根桥，SW3 到 SW2 有两条路径，要根据两条链路的成本值决定应该逻辑断开哪一条。其中 100M 的路径成本为 19,1000M 的路径成本为 4。所以 SW2-SW3 的直连链路成本为 19,SW3-SW1-SW2 的链路成本为 8,所以应该断开 SW2-SW3 之间的逻辑链路，备份使用。

The API changes should provide both source and binary (71) for programs written to the original API. That is, existing program binaries should continue to operate when run on a system supporting the new API. In addition, existing (72) that are re-compiled and run on a system supporting the new API should continue to operate. Simply put, the API (73) for multicast receivers that specify source filters should not break existing programs. The changes to the API should be as small as possible in order to simplify the task of converting existing (74) receiver applications to use source filters. Applications should be able lo detect when the new (75) filter APIs are unavailable (e.g., calls fail with the ENOTSUPP error) and react gracefully (e.g., revert to old non-source-filter API or display a meaningful error message to the user).

| | | | |
|---|---|---|---|
| (71)A.capability | B.compatibility | C.labiality | D.reliability |
| (72)A.systems | B.programs | C.applications | D.users |
| (73)A.connections | B.changes | C.resources | D.considerations |
| (74)A.multicast | B.unicast | C.broadcast | D.anycast |
| (75)A.resource | B.state | C.destination | D.source |

**【答案】**B C B A D

**【解析】**

对于 API 的改变应该与用原来 API 编写的程序的源代码和二进制代码兼容。亦即，原有程序的二进制代码应该可以运行在支持新 API 的系统上。此外，现有的应用经过重新编译，也可以运行在支持新 API 的系统上。简言之，对于说明了源过滤的组播接收器，API 的改变不能破坏现有的程序。API 的改变应该尽量小，以便简化转换现有的使用源过滤的组播接收器应用的工作。当新的源过滤 API 不可用时，应用程序应该能够检测到（例如调用失败，出

现 ENOTSUPP 错误)，并且给出温和的反应（例如转向老的非源过滤 API,或者向用户显示有用的错误信息)。

**试题一**

企业网络拓扑结构如图 1-1 所示。

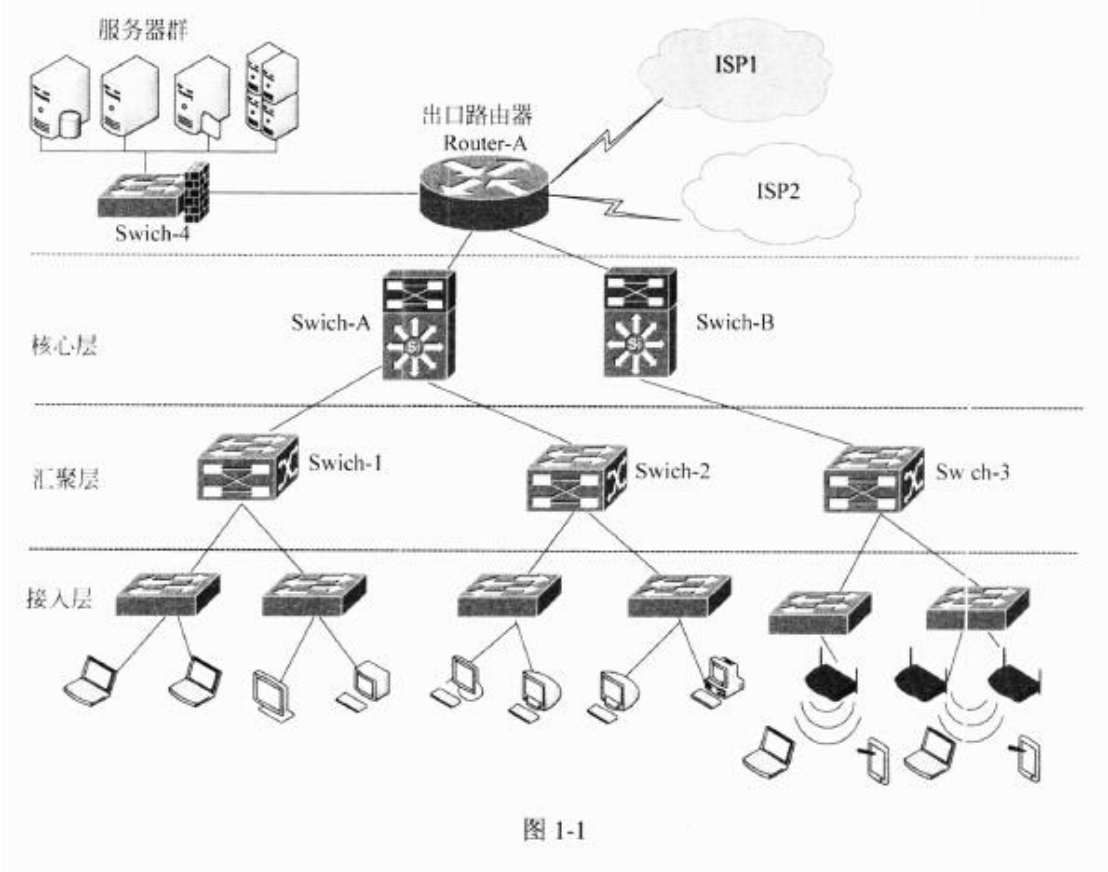



图 1-1

**【问题 1】**

企业网络的可用性和可靠性是至关重要的，经常会出现因网络设备、链路损坏等导致整个网络瘫痪的现象。为了解决这个问题，需要在已有的链路基础上再增加一条备用链路，这称作网络冗余。

(1)对于企业来说，直接增加主干网络链路带宽的方法有哪些？并请分析各种方法的优缺点。

(2)一般常用的网络冗余技术可以分为哪两种。

(1) 一般有两种方法，一是直接升级主干网络带宽。优点是效果显著，不足之处是这种方法投入较大；二是采用以太网信道或者端口聚合技术。优点是投入较小，缺点是使用该技术需要两端设备都支持端口聚合技术，且进行端口捆绑的多个接口状态必须相同。

(2) 一般常用的网络冗余技术可以分为二层链路冗余和三层网关冗余。

本问题主要考查网络冗余技术。

互联网发展速度迅猛，企业对于网络的性能、网速和带宽的要求日益增加，在这种发展势头下，企业网络难免会出现链路带宽不足的现象。对于企业来说，解决链路带宽不足可以采用多种方法来解决。一是直接升级主干网络带宽，如将百兆网络升级为千兆网络，千兆网络升级为万兆网络等，这种升级效果比较明显，但是在升级中不单是要考虑更换网络连接线缆，很多设备往往也要更换，因此需要结合企业的经济状况和业务需求综合考虑。

另外一种方法是将关键设备间的链路数量增加，这样一来升级成本就大大降低。但是直接在设备之间连接多条线缆的话可能会造成环路，导致广播风暴。所以还要采用相应的技术限制环路的产生，一般这里使用的技术被称为以太网信道或者端口聚合。使用该技术首先需要两端的设备都要支持端口聚合技术（以太网信道技术），同时进行端口捆绑的多个接口状态必须相同，如带宽、速度、双工模式等，最好用相邻的端口。

随着 Internet 的发展，大型园区网络从简单的信息承载平台转变成一个公共服务提供平台。作为终端用户，希望能时时刻刻保持与网络的联系，因此健壮、高效和可靠成为园区网发展的重要目标，而要保证网络的可靠性，就需要使用到冗余技术。高冗余网络就是在网络设备、链路发生中断或者变化的时候，用户几乎感觉不到。一般常用的网络冗余技术可以分作二层链路冗余和三层网关冗余。在二层链路中实现冗余的方式主要有两种，生成树协议和链路捆绑技术。其中生成树协议是一个纯二层协议，但是链路捆绑技术在二层接口和三层接口上都可以使用。三层链路冗余技术较二层链路冗余技术丰富很多，依靠各种路由协议可以实现三层链路冗余和负载均衡。另外三层链路捆绑技术也提供了路由协议之外的一种选择。对于使用网络的终端用户来讲，也需要一种机制来保证其与园区网络的可靠连接，这就是三层网关级冗余技术。VRRP(Virtual Router Redundancy Protocol，虚拟路由冗余协议)、HSRP(Hot Stand by Router Protocol,热备份路由器协议）及 GLBP(Gateway Load Balancing Protocol,网关负载均衡协议）都是比较常用的网关冗余方法。但是 HSRP 和 GLBP 是思科的专有协议，VRRP 协议是开放的。所以在设备比较复杂的大型网络里面，大都使用 VRRP 协议实现网关冗余。

**【问题 2】**

(1) 网络冗余是当前网络为了提高可用性、稳定性必不可少的技术，在本企业网络中要求使用双核心交换机互做备份实现两种网络冗余技术，同时出口路由器因为负载过重也需要进行网络结构调整优化，请画图说明在不增加网络设备的情况下完成企业主干网络结构调

优。

(2) 在两台核心交换机上配置 VRRP 冗余，以下为部分配置命令。根据需求，完成(或解释）核心交换机 Switch-A 的部分配置命令。

```
Switch-A:
Switch-A(config)#track 100 interface F0/1 line-protocol
//_____①_____
Switch-A(config-track)#exit
Switch-A(config)#int VLAN 1
Switch-A(config-if)#vrrp 1 ip 192.168.1.254
//在 VLAN1 中配置 VRRP 组 1，并指定虚拟路由器的 IP 地址为 192.168.1.254
Switch-A(config-if)#_____②_____
//开启主路由器身份抢占功能
Switch-A(config-if)#vrrp lauthentication md5 key-string Cisco
//配置 VRRP 协议加密认证
Switch-A(config-if)#vrrp 1 track 100 decrement 30
//_____③_____
```

(1)如图 1-3 所示，虚线为增加的链路。首先在两台核心交换机之间实现链路聚合以增加主干网络带宽。其次是要把两台核心交换机定义为 STP 的根桥；同时要做网关备份，主要是在双核心交换机上配置 VRRP 协议。最后为了减少出口路由器的负担，考虑把服务器群接入到核心交换机 A 或者 B 上。

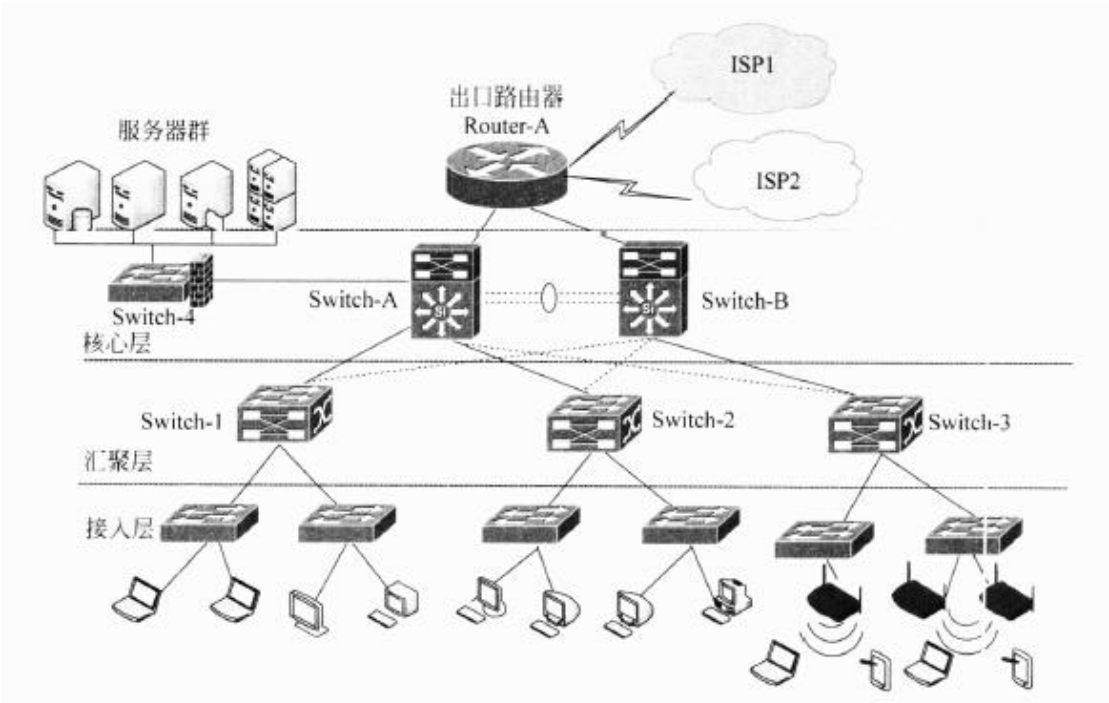



图 1-3 优化后的企业网络拓扑图

(2) ①开启路由器端口跟踪功能。

②vrrp 1 preempt,,

③端口跟踪，当发现链路故障时，自动将优先级降低 30,以便其他可用链路的设备抢夺 VRRP 主路由器身份。

本问题主要考查网络的优化及基于 VLAN 的多层网络冗余配置。

在图 1-1 中，整个企业网络在网络冗余方面几乎没有做任何设置，如两台核心交换机之间没有互联，汇聚交换机到核心交换机之间没有链路冗余，这样主干网的带宽和链路冗余都得不到保障，因此整个网络的可靠性会很差。其次，在网络出口路由器上接入了服务器群，这样在网络进出口流量比较大的时候，出口路由器负担就会比较重，会影响网络的正常访问速度，需要调整服务器群的接入位置。’

如图 1-2 所示，优化整个网络布局。其中虚线为增加的链路。首先在两台核心交换机之间实现链路聚合以增加主干网络带宽。其次按照图中的连接方法已经构成了二层环路，链路冗余已经产生，关键是要把两台核心交换机定义为 STP 的根桥；三层网关冗余技术主要是做网关备份，因此，需要在双核心交换机上配置 VRRP 协议。最后为了减少出口路由器的负担，考虑把服务器群接入到核心交换机 A 或者 B 上。

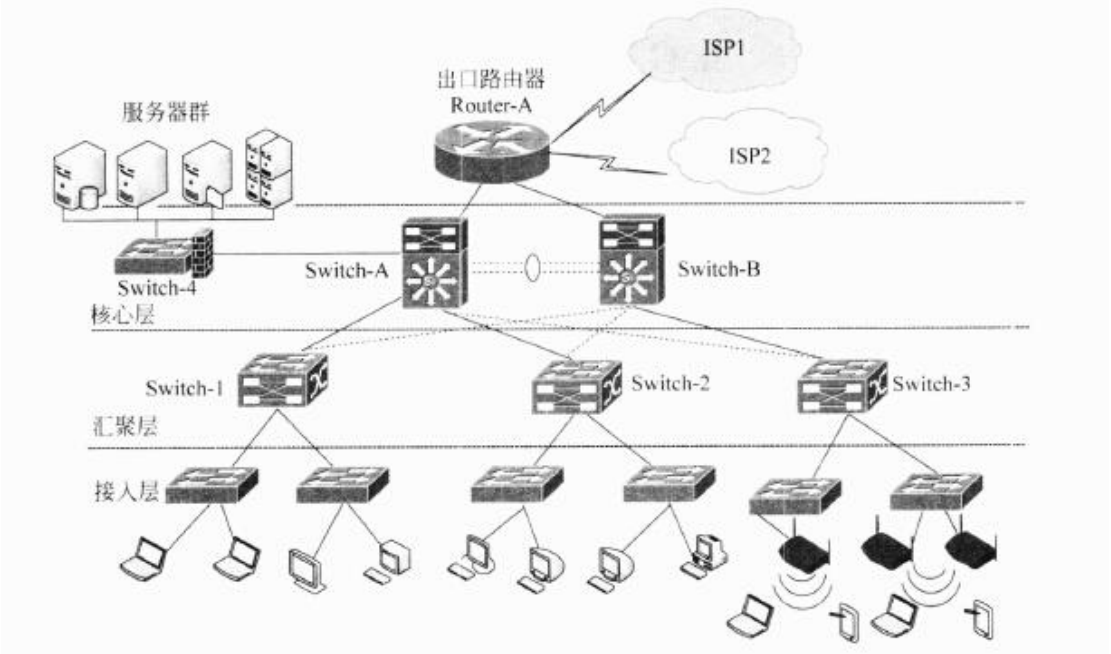



图 1-2 优化后的企业网络拓扑图

三层链路冗余技术主要是做网关备份，在配置之前首先要确保网络访问畅通。所以要正

确配置接口 IP 地址及合适的路由。在配置网关冗余时主要使用 VRRP 协议.每一个 VLAN 作为一个 VRRP 组进行配置，按照题目要求，为双核心三层交换机的 VLAN 配置 VRRP 协议的部分配置命令如下：

```
Switch-A:
Switch-A(config)#track 100 interface F0/1 line-protocol
//开启路由器端口跟踪功能，当三层交换机上端链路故障时可通过接口 F0/1 的跟踪功能判断整条链路故障，从而使 VRRP 主路由器身份跳转。
Switch-A(config-track)#exit
Switch-A(config)#int VLAN 1
Switch-A(config-if)#vrrp 1 ip 192.168.1.254
//在 VLAN1 中配置 VRRP 组 1，并指定虚拟路由器的 IP 地址为 192.168.1.254
Switch-A(config-if)# vrrp 1 preempt
//开启主路由器身份抢占功能
Switch-A(config-if)#vrrp lauthentication md5 key-string Cisco
```

```
//配置 VRRP 协议加密认证
Switch-A(config-if)#vrrp 1 track 100 decrement 30
// 端口跟踪，当发现链路故障时，自动将优先级降低 30，以便其他可用链路的设备抢夺 VRRP 主路由器身份。
```

**【问题 3】**

随着企业网络的广泛应用，用户对于移动接入企业网的需求不断增加，无线网络作为有线网络的有效补充，凭借着投资少、建设周期短、使用方便灵活等特点越来越受到企业的重视，近年来企业也逐步加大无线网络的建设力度。

(1) 构建企业无线网络如何保证有效覆盖区域并尽可能减少死角？

(2) IEEE 认定的四种无线协议标准是什么？

(3) 简单介绍三种无线安全的加密方式。

(1) 构建企业无线网络为了减少死角，必须让两个 AP 覆盖的无线区域重叠。除此之外，选择 AP 时也要考虑当前物理环境，如果是空旷的环境可以选择使用放射信号为球形的 AP 设备，如果是在楼层中可以考虑使用向某个区域放射信号的 AP 设备。

(2) 目前，主流的无线协议都是由 ffiEE 所制定，IEEE 认定的四种无线协议标准分别为 IEEE802.11a、IEEE802.11b,IEEE802.11g 和 IEEE802.11n。

(3) 第一种：WEP 加密 WEP(有线对等保密）协议

第二种：WPA 加密 WPA 和 WPA2

第三种：WPA-PSK 加密 WPA-PSK 和 WPA2-PSK

本问题主要考查 WLAN 无线网络建设的相关知识。

(1) 在架设无线网络过程中，因为无线网络并不像有线网络那么直观，所以在架设无线网络时一般为了减少死角，必须让两个相邻的 AP 覆盖的无线区域重叠。因为一个 AP 覆盖的无线网络区域一般是球形的，只有两个区域部分相互重叠才能确保无线信号更全面。除此之外，选择 AP 时也要考虑当前物理环境，如果是空旷的环境可以选择使用放射信号为球形的 AP 设备（全向天线），如果是在楼层中可以考虑使用向某个区域放射信号的 AP 设备（定向天线）。

(2) 目前，主流的无线协议都是由 ffiEE 所制定，IEEE 认定的四种无线协议标准分别为 IEEE802.11a、IEEE802.11b、IEEE802.11g 和 IEEE802.1In。IEEE802.11a 标准工作在 5GHzU-NII 频带，物理层速率最高可达 54Mbps，传输层速率最高可达 25MbpsJEEE802.11b 是无线局域网的一个标准。其载波的频率为 2.4GHz，传送速度为 11Mbit/s。IEEE802.11b 是所有无线局域网标准中最著名，也是普及最广的标准。IEEE802.11b 的后继标准是 IEEE802.11g，其载波的频率为 2.4GHz(跟 802.1 比相同)，原始传送速度为 54\11)说，净传输速度约为 24.7Mbit/s(跟 802.11a 相同)。IEEE802.11n 于 2009 年 9 月正式批准。使用 2.4GHz 频段和 5GHz 频段，传输速度 300Mbps，最高可达 600Mbps，可向下兼容 802.11b、802.11g。

(3) 无线网络通过无线信号进行信息传输，数据的安全性难以保障，因此为了保障无线网络数据的安全性，各种各样的无线加密算法应运而生。第一种：WEP 加密，WEP(有线对等保密）协议，它主要用于 WLAN 中链路层信息数据的加密，采用的是静态的密钥。第二种：WPA 加密，如 WPA 和 WPA2,WPA 算法主要用于增强 WLAN 系统的数据保护和访问控制水平，采用了动态的密钥，WPA2 是在 WPA 的基础之上经 WiFi 联盟验证过的 IEEE802.11i 标准的验证形式，是目前公认的比较安全的无线加密算法。第三种：WPA-PSK 加密，如 WPA-PSK 和 WPA2-PSK，由于 WPA 操作复杂，因此经常采用其简化版 WPA-PSK 和 WPA2-PSK，不需要设置复杂的身份证明等信息，因而在实际使用中最为普遍。

**【问题 4】**

随着企业关键网络应用业务的发展，在企业网络中负载均衡的应用需求也越来越大。

(1) 负载均衡技术是什么？负载均衡会根据网络的不同层次（网络七层）只划分。其中，

第二层的负载均衡是什么技术？

(2) 服务器集群技术和服务器负载均衡技术的区别是什么？

(1) 负载均衡(LoadBalancing)技术建立在现有网络结构之上，它提供了一种廉价有效透明的方法，扩展网络设备和服务器的带宽，增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。第二层的负载均衡指将多条物理链路当作一条单一的聚合逻辑链路使用，即链路聚合（Trunking)技术。

(2) 集群（Cluster):是一组独立的计算机系统构成一个松耦合的多处理器系统，它们之间通过网络实现进程间的通信。应用程序可以通过网络共享内存进行消息传送，实现分布式计算。主要解决高可靠性（HA)和高性能计算（HP)。负载均衡技术提供了一种廉价有效的方法，扩展服务器带宽和增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。主要解决的是大量的并发访问或数据流量分担到多台节点设备上分别处理，减少用户等待响应的时间。

本问题主要考查负载均衡技术的相关知识。

(1)负载均衡（LoadBalancing)技术建立在现有网络结构之上，它提供了一种廉价有效透明的方法，扩展网络设备和服务器的带宽，增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。

负载均衡有两方面的含义：首先，单个重负载的运算分担到多台节点设备上做并行处理，每个节点设备处理结束后，将结果汇总，返回给用户，系统处理能力得到大幅度提高，这就是常说的集群（Clustering)技术。第二层含义就是：大量的并发访问或数据流量分担到多台节点设备上分别处理，减少用户等待响应的时间，这主要针对 Web 服务器、FTP 服务器、企业关键应用服务器等网络应用。通常，负载均衡会根据网络的不同层次（网络七层）来划分。其中，第二层的负载均衡指将多条物理链路当作一条单一的聚合逻辑邊路使用，这就是链路聚合（Trunking)技术，它不是一种独立的设备，而是交换机等网络设备的常用技术。现代负载均衡技术通常操作于网络的第四层或第七层，这是针对网络应用的负载均衡技术，它完全脱离于交换机、服务器而成为独立的技术设备。近年来，四到七层网络负载均衡首先在电信、移动、银行、大型网站等单位进行了应用，因为其网络流量瓶颈的现象最突出。这也就是为何每通一次电话，就会经过负载均衡设备的原因。另外，在很多企业，随着企业关键网络应用业务的发展，负载均衡的应用需求也越来越大了。

(2)集群（Cluster):集群就是一组连在一起的计算机，从外部看它是一个系统，各节点可以是不同的操作系统或不同硬件构成的计算机。如一个提供 Web 服务的集群，对外界来看是一个大 Web 服务器。不过集群的节点也可以单独提供服务。因此可以说集群是一组独立的计算机系统构成一个松耦合的多处理器系统，它们之间通过网络实现进程间的通信。应用程序可以通过网络共享内存进行消息传送，实现分布式计算机。主要解决高可靠性（HA)和高性能计算（HP)。

负载均衡建立在现有网络结构之上，它提供了一种廉价有效的方法扩展服务器带宽和增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。它主要完成以下任务：解决网络拥塞问题，服务就近提供，实现地理位置无关性；为用户提供更好的访问质量；提高服务器响应速度；提高服务器及其他资源的利用效率；避免了网络关键部位出现单点失效。区别是集群系统（Cluster)主要解决下面几个问题：高可靠性（HA)，利用集群管理软件，当主服务器故障时，备份服务器能够自动接管主服务器的工作，并及时切换过去，以实现对用户的不间断服务；高性能计算（HP):即充分利用集群中的每一台计算机的资源，实现复杂运算的并行处理，通常用于科学计算领域，比如基因分析，化学分析等。负载平衡：即把负载压力根据某种算法合理分配到集群中的每一台计算机上，以减轻主服务器的压力，降低对主服务器的硬件和软件要求。主要解决的是大量的并发访问或数据流量分担到多台节点设备上分别处理，减少用户等待响应的时间。

**试题二**

某高校校园网使用 3 个出口，新老校区用户均通过老校区出口访问互联网，其中新老校区距离 20 公里，拓扑结构如图 2-1 所示，学校服务器区网络拓扑结构如图 2-2 所示。

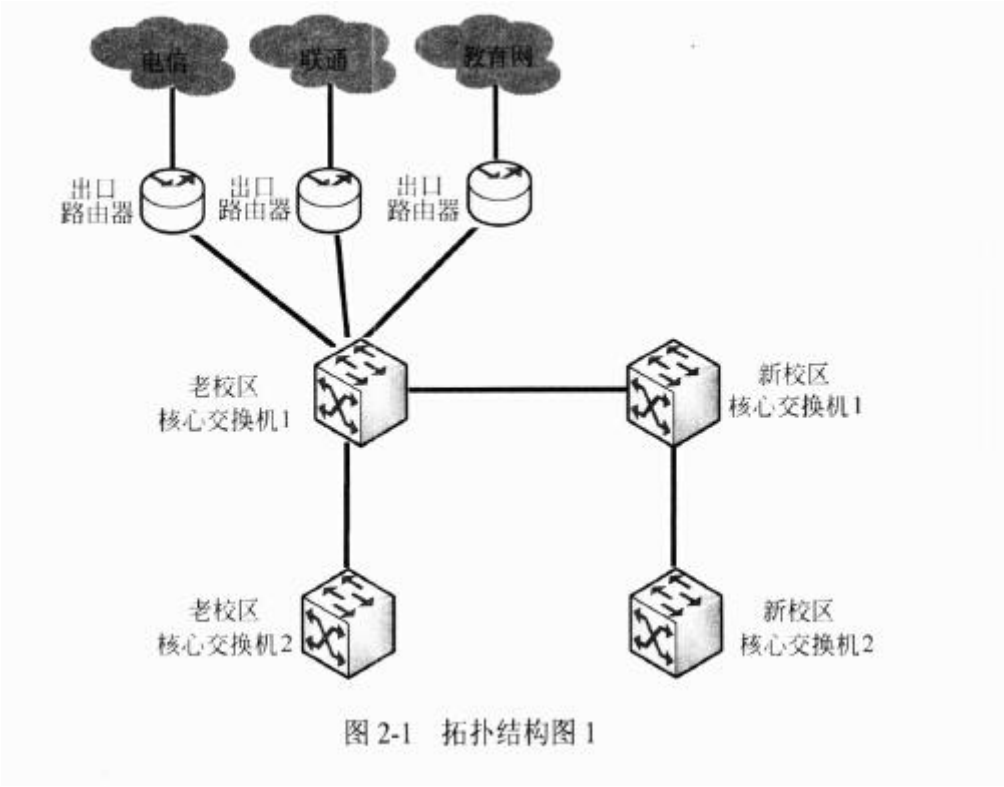



图 2-1 拓扑结构图 1

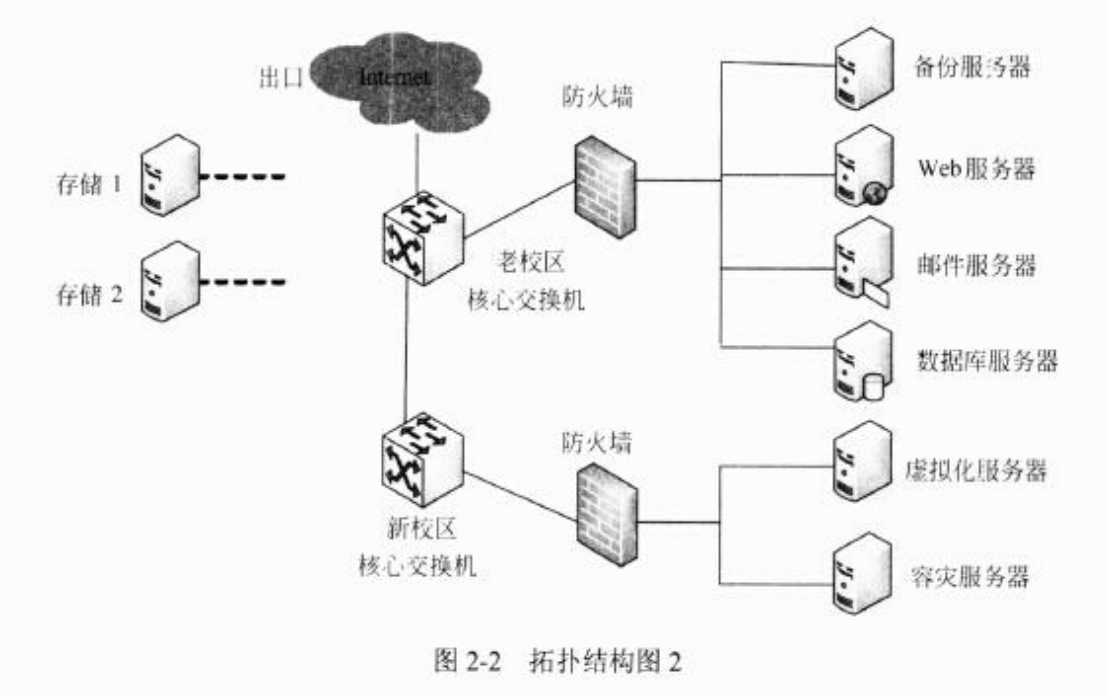



图 2-2 拓扑结构图 2

**【问题 1】**

实现多出口负载均衡通常有依据源地址和目标地址两种方式，分别说明两种方式的实现原理和特点。

依据源地址负载均衡：根据源 IP 地址来选择不同外网出口，可以根据各出口带宽按比例划分对应的源 IP 子网段，达到出口负载均衡的作用，但是访问同一资源时，部分用户响应快，部分用户响应慢。

依据目的地址负载均衡：根据目的 IP 地址来选择不同外网出口，内部用户可以根据不同运营商提供的资源，选择相应运营商的出口，但是会导致提供资源丰富的运营商出口负载过大，提供资源相对比较少的运营商出口负载很轻，造成各出口不均衡的现象。

本问题考查依据源地址和目的地址的负载均衡的实现原理和优缺点，是理论性知识。依据源地址负载均衡根据源 IP 地址来选择不同外网出口，可以根据各出口带宽按比例划分对应的源 IP 子网段，达到出口负载均衡的作用，但是访问同一资源时，部分用户响应快，部分用户响应慢。

依据目的地址负载均衡根据目的 IP 地址来选择不同外网出口，内部用户可以枝据不同运营商提供的资源，选择相应运营商的出口，但是会导致提供资源丰富的运营而出口负载过大，提供资源相对比较少的运营商出口负载很轻，造成各出口不均衡的现象。

**【问题 2】**

根据学校多年实际运行情况，现需对图 2-1 所示网络进行优化改造，要求：

(1) 在只增加负载均衡设备的情况下，且仅限通过老校区核心交换机 1 连接出口路由器；

(2) 采用网络的冗余，解决新老校区互联网络中的单点故障；

(3) 通过多出口线路负载，解决单链路过载；

(4) 考虑教育网的特定应用，需采用明确路由。

试画出图 2-1 优化后的网络拓扑结构，并说明改造理由。

改造后的出口网络拓扑如图 2-3 所示。

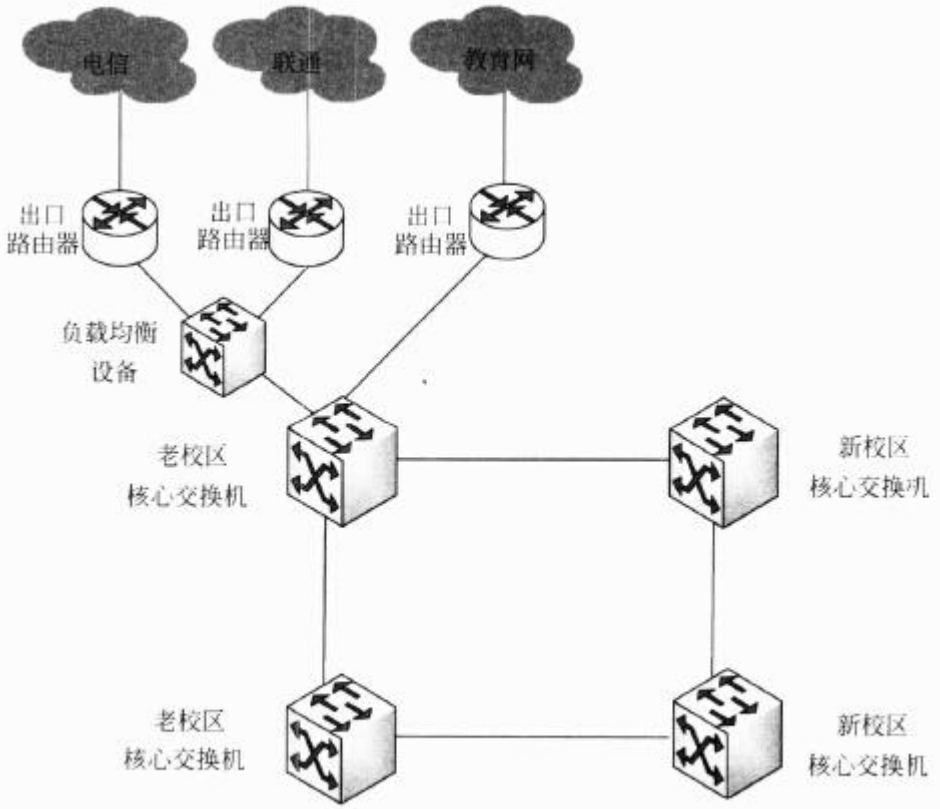



图 2-3 改造后的出口网络拓扑

改造原因：

(1) 将 4 台核心交换机组成环网结构，避免新老校区设备或单链路故障造成新老校区网络中断；

(2) 在电信、联通链路增加负载均衡设备，平衡各出口的负载和加快内部用户访问外网的速度；

(3) 同时考虑教育网的特定应用，配置教育网走明确路由。

整合改造方案中，要根据题目中的限制条件进行设计优化改造方案。

根据题目要求，可以看出需要改造的地方：

(1) 将 4 台核心交换机组成环网结构，避免新老校区设备或单链路故障造成所老校区网络中断；

(2) 在电信、联通链路增加负载均衡设备，平衡各出口的负载和加快内部用户访问外网的速度；

(3) 同时考虑教育网的特定应用，配置教育网走明确路由。

**【问题 3】**

现学校有两套存储设备，均放置于老校区中心机房，存储 1 是基于 IP-SAN 技术，存储 2 是基于 FC-SAN 技术。试说明图 2-2 中数据库服务器和容灾服务器应采用哪种存储技术，并说明理由。

(1) 容灾服务器：容灾服务器和存储设备距离 20 公里，需要远距离传输，所以只能选择 IP-SAN 技术；

(2) 数据库服务器：需要高性能、大并发、快速响应，最合理的应该选择 FC-SAN 技术。

本问题考查 IP-SAN 技术和 FC-SAN 技术的优缺点，结合实际应用选择。

(1) 容灾服务器：容灾服务器和存储设备距离 20 公里，需要远距离传输，听以只能选择 IP-SAN 技术。

(2) 数据库服务器：需要高性能、大并发、快速响应，最合理应该选择 FC-SAN 技术。

**【问题 4】**

当前存储磁盘柜中通常包含 SAS 和 SATA 磁盘类型，试说明图 2-2 中数据库服务器和容灾服务器各应选择哪种磁盘类型，并说明理由。

数据库服务器选择 SAS 磁盘，容灾服务器选择 SATA 磁盘。原因如下：

(1) SAS 是双端口，采用全双工的工作方式传输数据，而 SATA 是单端口，采用半双工的工作方式传输数据；

(2) SAS 使用 SCSI 命令进行错误校正和错误报告，这比 SATA 采用的 ATA 命令集有更多的功能；

(3) SAS 磁盘容量小，价格比较昂贵，SATA 磁盘容量大，价格比较便宜。

数据库服务器和容灾服务器相比，数据库服务器数据容量小，读写频繁，要求速度快，而容灾服务器不追求速度，侧重于大容量。

所以综合 SAS 磁盘和 SATA 磁盘在传输速率、安全型和性价比方面的优缺点，采取数据库服务器选择 SAS 磁盘，容灾服务器选择 SATA 磁盘。

**【问题 5】**

目前存储中使用较多的是 RA1D5 和 RAID10,试说明图 2-2 中数据库服务器和容灾服务器（数据级）各应选择哪种 RAID 技术，并说明理由。

数据库服务器选择 RAID10,容灾服务器选择 RAID5。原因如下：

(1) 1/0：读操作上，RAHM0 和 RAID5 是相当的，写操作上，RAID10 好于 RAID5;

(2) 数据重构：在一块磁盘失效，进行数据重构期间，RAID5 要比 RAID10 耗时长，负荷大，数据丢失可能性高，可靠性低。

数据库服务器性能、安全级别都比容灾服务器要求高，所以数据库服务器选择 RAID10,容灾服务器选择 RAID5。原因如下：

(1)1/0：读操作上，RAID10 和 RAID5 是相当的，写操作上，RAID10 好于 RAID5;

(2)数据重构：在一块磁盘失效，进行数据重构期间，RAID5 要比 RAID10 耗时长，负荷大，数据丢失可能性高，可靠性低。

**试题三**

某高校网络拓扑结构如图 3-1 所示。

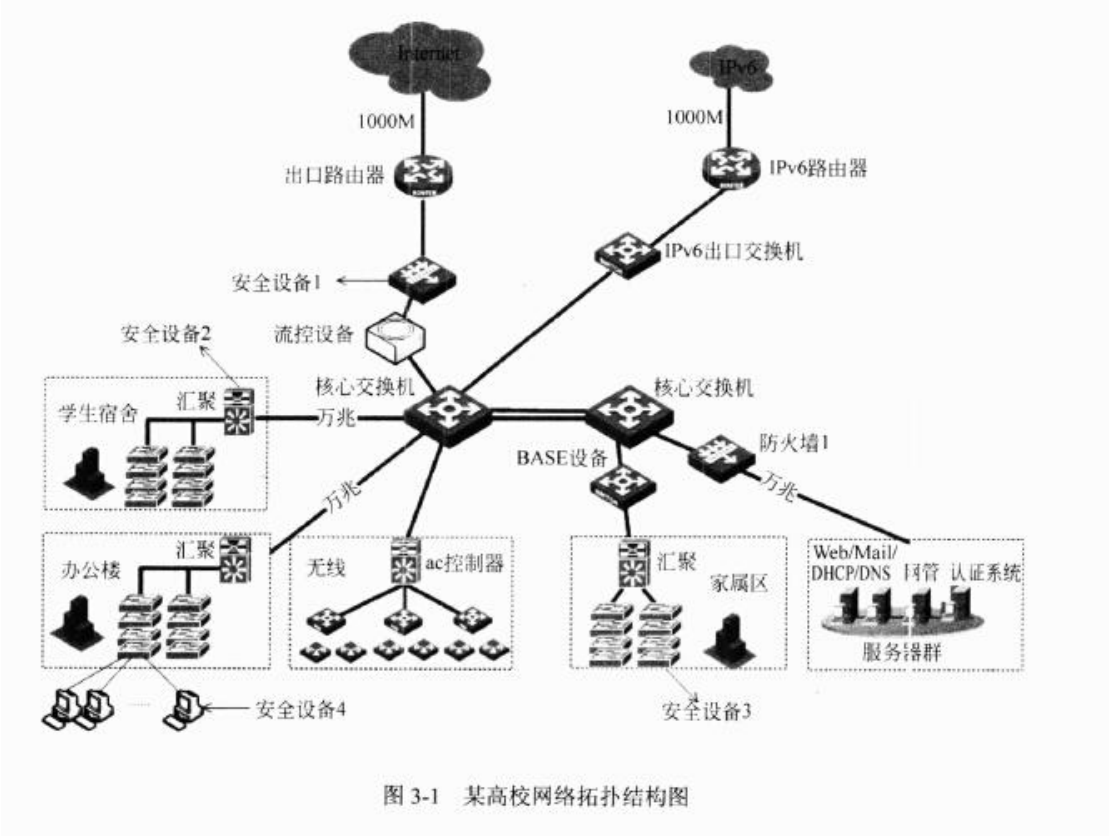



图 3-1 某高校网络拓扑结构图

**【问题 1】**

目前网络中存在多种安全攻击，需要在不同的位置部署不同的安全措施进行防范。常见的安全防范措施有：

1. 防非法 DHCP 欺骗
2. 用户访问权限控制技术
3. 开启环路检测(STP)
4. 防止 ARP 网关欺骗
5. 广播风暴的控制
6. 并发连接数控制
7. 病毒防治

其中：在安全设备 1 上部署的措施有：（1）；

在安全设备 2 上部署的措施有：（2）：

在安全设备 3 上部署的措施有：（3）；

在安全设备 4 上部署的措施有：（4）。

(1)6. 并发连接数控制

(2)2. 用户访问权限控制技术

(3)1. 防非法 DHCP 欺骗

3. 开启环路检测（STP）

4. 防止 ARP 网关欺骗

5. 广播风暴的控制

(4)7. 病毒防治

本问题主要考查安全技术加载的位置。

从 DHCP 工作原理可以看出，如果客户端是第一次、重新登录或租期已满不能更新租约，客户端都是以广播的方式来寻找服务器，并且只接收第一个到达的服务器提供的网络配置参数，如果在网络中存在多台 DHCP 服务器（有一台或更多台是非授权的），谁先应答，客户端就采用其提供的网络配置参数。假如非授权的 DHCP 服务器先应答，这样客户端最后获得的网络参数即是非授权的，客户端即被欺骗了。而在实际应用 DHCP 的网络中，基本上都会采用 DHCP 中继，这样的话，本网络的非授权 DHCP 服务器一般都会先于其余网络的授权 DHCP 服务器的应答（由于网络传输的延迟），在这样的应用中，DHCP 欺骗更容易完成。对 DHCP 欺骗的防范方法主要是在交换机上启用 DHCP SNOOPING 功能。

用户访问权限控制通常读取第三层及第四层包头中的信息如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。通常加载在汇聚层交换机上。

频繁改动网络时很容易引发网络环路，网络环路引起的网络堵塞现象常常具有较强的隐蔽性，不利于故障现象的高效排除。开启环路检测（STP)通常加载在接入交换机上，通过配置交换机的环回监测功能，快速地判断局域网中是否存在网络环路。

ARP 网关欺骗是局域网中一台机器，反复向其他机器，特别是向网关，发送假冒的 ARP 应答信息包，造成严重的网络堵塞。解决的方法是在某个网络内采用检测技术，防止欺骗。

并发连接数控制整个网络中的连接数，需在核心层完成。

病毒防治在网络内，通常在单机上完成。

**【问题 2】**

学校服务器群目前共有 200 台服务器为全校提供服务，为了保证各服务器能提供正常的服务，需对图 3-1 所示防火墙 1 进行安全配置，设计师制定了 2 套安全方案，请根据实际情况选择合理的方案并说明理由。

方案一：根据各业务系统的重要程度，划分多个不同优先级的安全域，每个安全域采用一个独立子网，安全域等级高的主机默认允许访问安全域等级低的主机，安全域等级低的主机不能直接访问安全域等级高的主机，然后根据需要添加相应安全策略。

方案二：根据各业务系统提供的服务类型，划分为数据库、Web、认证等多个不同虚拟防火墙，同一虚拟防火墙中相同 VLAN 下的主机可以互访，不同 VLAN 下的主机均不允许互访，不同虚拟防火墙之间主机均不能互访。

1. 选择方案二

2. 理由：

(1) 如果服务器规模比较大，方案一按照主机添加安全策略，所以防火墙的安全策略数量比较多，对防火墙的资源消耗也会比较大，方案二按照服务添加安全策略，所以防火墙安全策略数量不多，对防火墙的资源消耗也会比较小；

(2) 如果某一主机感染病毒或木马时，方案一安全域级别低或者相同的其他主机会受到影响，方案二相同虚拟防火墙中相同 VLAN 主机会受到影响，其余主机不会影响；

(3) 后期服务器数量大幅增加，方案一需新增加多条安全策略，方案二服务类型不新增的情况下，安全策略基本不需增加。

本问题主要考查防火墙安全技术的设计。

方案一按照主机添加安全策略，防火墙的安全策略数量比较多，对防火墙的资源消耗也会比较大，方案二按照服务添加安全策略，所以防火墙安全策略数量不多，对防火墙的资源消耗也会比较小。

如果某一主机感染病毒或木马时，方案一安全域级别低或者相同的其他主机会受到影响，方案二相同虚拟防火墙中相同 VLAN 主机会受到影响，其余主机不会影响；而且后期服务器数量大幅增加，方案一需新增加多条安全策略，方案二服务类型不新增的情况下，安全策略基本不需增加。

综上，选择方案二。

**【问题 3】**

为了防止资源的不合理使用，通常在核心层架设流控设备进行流量管理和终端控制，请列举出 3 种以上流控的具体实现方案。

(1) 针对地址进行带宽限制。针对源 IP 地址、目的 IP 地址进行带宽限制，防止某地址独占带宽。

(2) 针对子网进行带宽限制。针对子网进行带宽限制，防止某子网独占带宽，如某个部门划分一个子网。

(3) 针对服务进行带宽限制。针对服务进行带宽限制，防止某服务独占带宽，如视频、BT 等。

本问题主要考查流量管理的实现技术。

通常在核心层架设流控设备进行流量管理和终端控制，有以下 3 种：

(1) 针对地址进行带宽限制。针对源 IP 地址、目的 IP 地址进行带宽限制，防止某地址独占带宽。

(2) 针对子网进行带宽限制。针对子网进行带宽限制，防止某子网独占带宽，如某个部门划分一个子网。

(3) 针对服务进行带宽限制。针对服务进行带宽限制，防止某服务独占带宽，如视频、BT 等。

**【问题 4】**

非法 DHCP 欺骗是网络中常见的攻击行为，说明其实现原理并说明如何防范。

1. 非法 DHCP 欺骗原理：客户端第一次登录、重新登录或租期已满不能更新租约时，以广播方式寻找服务器，并且只接收第一个到达的服务器提供的网络配置参数，如果在网络中存在多台 DHCP 服务器（有一台或更多台是非授权的），并且非授权的 DHCP 服务器先应答，那么客户端就会获得非授权的网络参数。

2. 防范：可以在交换机上开启 DHCP SNOOPING,通过建立和维护 DHCP SNOOPING 绑定表并过滤不可信任的 DHCP 信息，只让合法的 DHCP 应答通过交换机，阻断非法应答，从而防止

DHCP 欺骗。

本问题主要考查非法 DHCP 欺骗原理。

客户端第一次登录、重新登录或租期已满不能更新租约时，以广播方式寻找服务器，并且只接收第一个到达的服务器提供的网络配置参数，如果在网络中存在多台 DHCP 服务器（有一台或更多台是非授权的），并且非授权的 DHCP 服务器先应答，那么客户端就会获得非授权的网络参数。可以在交换机上开启 DHCP SNOOPING，通过建立和维护 DHCP SNOOPING 绑定表并过滤不可信任的 DHCP 信息，只让合法的 DHCP 应答通过交换机，阻断非法应答，从而防止 DHCP 欺骗。

**试题一**

云计算是一种网络计算模式，在这种模式下可以随时随地、方便快捷地按需使用互联网上的计算资源。自从 2006 年 Google 等公司提出了云计算的构想以来，这种计算模式得到了学术界和工业界的广泛关注，近年来出现了众多研究成果和云计算平台，许多云计算服务已经出现在各种终端应用上。政府和企业都把云计算作为战略竞争的关键技术，在财力和物力上进行了大量的投入。

请围绕“云计算的体系架构和关键技术”论题，从以下三个方面进行论述。

1. 通过应用实例解释云计算的基本概念。

2. 就下面的分层模型简要描述云计算的体系架构，各个层次包含的主要构件和需要解决的主要问题。


3.选择云计算的关键技术进行深入论述，例如数据存储技术、虚拟化技术、任务调度技术、编程模型等（或者你熟悉的其他技术）。

一、云计算的基本概念和应用实例

从用户的角度看，云计算是一种信息基础设施，包含硬件设备、软件平台、系统管理和信息服务设施，用户可以按照需求定制云服务，利用网络资源进行需要的计算，而系统维护和安全管理都由云端负责，用户只需按照使用的服务量支付一定的费用。云计算真正实现了用户像使用自来水和电力一样使用网络计算机资源的梦想。

云安全是网络信息安全方面的新进展。通过对网络中大量客户端的监现 I，可以获得互联网中各种恶意程序发生的最新信息，并推送到服务器端进行分析和处理，再把有关病毒和木马的解决方案分发到各个客户端。云计算强大的数据处理能力和同步调度能力极大地提升了网络安全公司对新威胁的响应速度。

云计算对信息检索带来了巨大影响。云存储改变了数据存储的模式，由单个服务器独立存储变成了分布式存储基础上的集中数据管理，从而可以使过去在单个服务器上的串行检索改变为云存储模式下的分布式并行数据处理。当云服务界面中的检索代理接受了用户的信息检索请求时，就将检索提问分发给云端的各个存储服务器，分布式检索的结果在检索代理中进行相关度排序后呈现在用户面前。

二、云计算的体系架构


三、云计算的关键技术

数据存储技术：采用分布式文件系统实现海量数据的分布式存储，分布式数据库技术用以实现结构化数据检索服务。

虚拟化技术：实现物理资源的逻辑抽象和统一表示，可以根据用户需求进行资源配置，实现动态的负载均衡，并通过自愈功能来提高系统的可靠性。

任务调度技术：求解的问题被拆分为若干子任务，分派到若干云节点中进行分布式计算，通过多个处理器协同工作，并将计算结果进行排序、合并和汇总，这需要在各个独立的操作系统之间进行任务调度。

编程模型：云计算需要有一种特殊的编程模式，能够把云计算能力封装成标准的 Web Services。在这种编程环境下，大的计算任务被映像为多个细小的可计算单元，通过云节点处理后再归约为最终的计算结果。

**试题二**

随着网络技术的飞速发展和普及，无线网络也逐步发展起来，近年来，无线网络已经成为网络扩展的一种重要方式，人们对无线网络依赖的程度也越来越高。无线网络具有安装简便、可移动性、开放性、高灵活性等特点，这些都为人们带来了极大的方便。但也正是因为这些特点，决定了无线网络面临许多安全问题，这些安全问题迫使技术人员开发了相应的安全防范技术和方法。

请围绕“无线网络中的安全问题及防范技术”论题，依次对以下四个方面进行论述。

1. 简要论述无线网络面临的安全问题。
2. 详细论述针对无线网络主要安全问题的防范技术。
3. 详细论述你参与设计和实施的无线网络项目中采用的安全防范方案。
4. 分析和评估你所采用的安全防范方案的效果以及进一步改进的措施。

一、对无线网络面临的安全问题的叙述要点：

1. 无线网络的类型

根据网络覆盖范围、传输速率和用途的差异，无线网络大体可分为无线广域网、无线城域网、无线局域网、无线个域网和无线体域网。

从网络拓扑结构角度，无线网络又可分为有中心网络和无中心、自组织网络。

2. 无线网络安全与有线网络安全的区别

无线网络的开放性使得网络更容易受到被动窃听或主动干扰等各种攻击；

无线网络的移动性使得安全管理难度更大；

无线网络动态变化的拓扑结构使得安全方案的实施难度更大；

无线网络传输信号的不稳定性带来无线通信网络及其安全机制的健壮性问题；

无线网络终端设备具有与有线网络终端设备不同的特点。

3. 无线网络面临的主要攻击威胁 WEP 攻击

MAC 地址欺骗 DoS 攻击 AP 口令攻击伪装 AP 攻击

二、对无线网络主要安全问题的防范技术的论述要点：

1. 访问控制

利用 MAC 地址访问控制和服务区认证 ID(SSID)技术来防止非法的无线设备入侵。由于每台计算机的网卡拥有唯一的 MAC 地址，因此可以使用 MAC 地址过滤的策略来防止非法的地

址入侵。SSID 使得只有计算机的 SSID 与无线路由器的 SSID一致时才能访问，因此可以采用隐蔽 SSID 的方法来拒绝非法访问。

2. 数据加密

数据加密是无线网络安全的基础，对传输的数据进行加密是为了防止其在未授权的情况下数据被泄露、破坏或篡改。各个组织和国家提出了多种解决方案，从开妁的 WEP 协议，经历 WPA，到 802.11i 协议，安全技术不断地进步。

3. 端口访问技术（802.1X)控制网络接入

IEEE802.1x 协议是一种基于端口访问的控制协议，能够实现对局域网设备的安全认证和授权。

三、叙述自己参与设计和实施的无线网络项目，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分量，说明项目中设计的安全方案以及选用该方案的理由。

四、具体讨论在方案实施过程中遇到的问题和解决措施，以及实际运行效果。

**试题三 数字化技术的运用及关键技术**

随着网络信息技术的进步和社会信息化程度的不断提高，一个由庞大的网终产业带动，并导致整个经济社会产生巨大变革的数字经济时代已经离我们越来越近。目前，“数字化校园”、“数字企业”、“数字城市”等一系列项目快速上马，在这些项目中，信息的数字化与数字信息的网络传输起着举足轻重的作用。

结合工程实践，围绕“数字化技术的运用及关键技术”论题，依次对以下四个方面进行论述。

1. 简要介绍单位具体需求，叙述数字化建设的必要性。
2. 叙述数字化建设中整体框架及数字化资源。
3. 叙述数字化建设中的网络支撑平台。 .
4. 分析在数字化建设中涉及的关键技术及采用的具体举措。

一、对数字化建设的必要性的叙述

从单位具体实际出发，介绍原有资源的组织形式，描述清楚数字化建设的必要性，给单位资源利用带来的好处。

二、数字化建设中整体框架及数字化资源的叙述

1. 描述数字化建设常采用的框架，本单位建设框架的选择及理由；
2. 对那些资源进行了数字化。

三、数字化建设中的网络支撑平台的叙述

1. 描述整体网络架构；
2. 实现资源快速共享采用的主要技术；
3. 数字化资源模块的网络组织形式。

四、涉及的关键技术及采用的具体举措的叙述

1. 在方案实施迂程中遇到的问题，采用的关键技术；
2. 关键技术产生的实际运行效果。