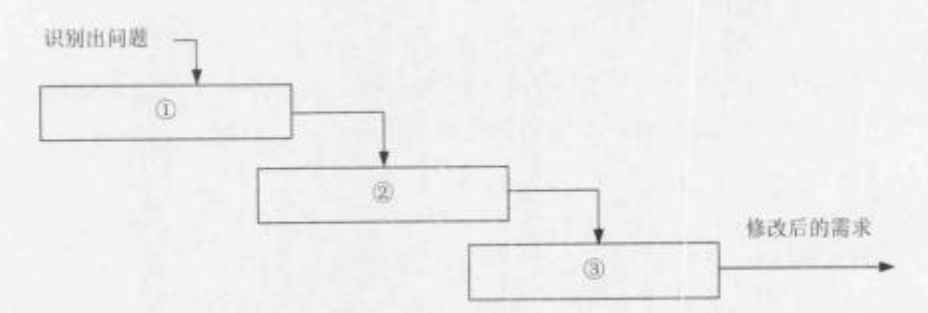
一个大型软件系统的需求总是有变化的。为了降低项目开发的风险，需要一个好的变更控制过程。如下图所示的需求变更管理过程中，①②③处对应的内容应是（1）；自动化工具能够帮助变更控制过程更有效地运作，（2）是这类工具应具有的特性之一。



(1)A.问题分析与变更描述、变更分析与成本计算、变更实现

B.变更描述与变更分析、成本计算、变更实现

C.问题分析与变更分析、变更分析、变更实现

D.变更描述、变更分析、变更实现

(2)A.变更维护系统的不同版本

B.支持系统文档的自动更新

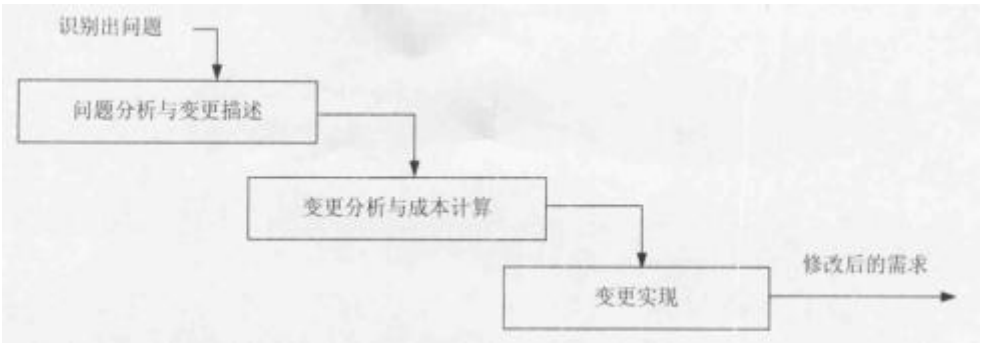
C.自动判定变更是否能够实施

D.记录每一个状态变更的日期和做出这一变更的人

【答案】A　D

【解析】

一个大型的软件系统的需求总是有变化的。对许多项目来说，系统软件总需要不断完善，一些需求的改进是合理的而且不可避免，要使得软件需求完全不变更，也许是不可能的，但毫无控制的变更是项目陷入混乱、不能按进度完成，或者软件质量无法保证的主要原因之一。一个好的变更控制过程，给项目风险承担者提供了正式的建议需求变更机制，可以通过变更控制过程来跟踪已建议变更的状态，使已建议的变更确保不会丢失或疏忽。需求变更管理过程如下图所示：



①问题分析和变更描述。这是识别和分析需求问题或者--份明确的变更提议，以检查它的有效性，从而产生一个更明确的需求变更提议。

②变更分析和成本计算。使用可追溯性信息和系统需求的一般知识，对需求变更提议进行影响分析和评估。变更成本计算应该包括对需求文档的修改、系统修改的设计和实现的成本。一旦分析完成并且确认，应该进行是否执行这一变更的决策。

③变更实现。这要求需求文档和系统设计以及实现都要同时修改。如果先对系统的程序做变更，然后再修改需求文档，这几乎不可避免地会出现需求文档和程序的不一致。

自动化工具能够帮助变更控制过程更有效地运作。许多团队使用商业问题跟踪工具来收集、存储和管理需求变更。用这样的工具创建的最近提交的变更建议清单，可以用作 CCB 会议的议程。问题跟踪工具也可以随时按变更状态分类报告出变更请求的数目。

因为可用的工具、厂商和特性总在频繁地变化，所以这里无法给出有关工具的具体建议。但工具应该具有以下几个特性，以支持需求变更过程：

①可以定义变更请求中的数据项；

②可以定义变更请求生命周期的状态转换模型；

③可以强制实施状态转换模型，以便只有授权用户可以做出允许的状态变更；

④可以记录每一个状态变更的日期和做出这一变更的人；

⑤可以定义当提议者提交新请求或请求状态被更新时，哪些人可以自动接收电子邮件通知；

⑥可以生成标准的和定制的报告和图表。

有些商业需求管理工具内置有简单的变更建议系统。这些系统可以将提议的变更与某一特定的需求联系起来，这样无论什么时候，只要有人提交了一个相关的变更请求，负责需求的每个人都会收到电子邮件通知。

用例（use case）用来描述系统对事件做出响应时所采取的行动。用例之间是具有相关性的。在一个会员管理系统中，会员注册时可以采用电话和邮件两种方式。用例“会员注册”

和“电话注册”、“邮件注册”之间是（3）关系。

(3)A.包含（include） B.扩展(extend)

C.泛化（generalize） D.依赖（depends on）

【答案】C

【解析】

用例之间的关系主要有包含、扩展和泛化，利用这些关系，把一些公共的信息抽取出来，以便于复用，使得用例模型更易于维护。

①包含关系。当可以从两个或两个以上的用例中提取公共行为时，应该使用包含关系来表示它们。其中这个提取出来的公共用例称为抽象用例，而把原始用例称为基本用例或基础用例。

②扩展关系。如果一个用例明显地混合了两种或两种以上的不同场景，即根据情况可能发生多种分支，则可以将这个用例分为一个基本用例和一个或多个扩展用例，这样使描述可能更加清晰。

③泛化关系。当多个用例共同拥有一种类似的结构和行为的时候，可以将它们的共性抽象成为父用例，其他的用例作为泛化关系中的子用例。在用例的泛化关系中，子用例是父用例的一种特殊形式，子用例继承了父用例所有的结构、行为和关系。

RUP 强调采用（4）的方式来开发软件，这样做的好处是（5）。

(4)A.原型和螺旋 B.螺旋和增量 C.迭代和增量 D.快速和迭代

(5)A.在软件开发的早期就可以对关键的，影响大的风险进行处理

B.可以避免需求的变更

C.能够非常快速地实现系统的所有需求

D.能够更好地控制软件的质量

【答案】C A

【解析】

RUP 将项目管理、业务建模、分析与设计等统一起来，贯穿整个开发过程。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。每个阶段结束时都要安排一次技术评审，以确定这个阶段的目标是否已经满足。如果评审结果令人满意，就可以允许项目进入下一个阶段。可以看出，基于 RUP 的软件过程是一个迭代和增量的过程。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软件。除非产品退役，否则通过重复同样的 4 个阶段，产品将演化为下一代产品，但每一次的侧重点都将放在不同的阶段上。这样做的好处是在软件开发的早期就可以对关键的、影响大的风险进行处理。

（6）的目的是检查模块之间，以及模块和已集成的软件之间的接口关系，并验证已集成的软件是否符合设计要求。其测试的技术依据是（7）。

(6)A.单元测试　　B.集成测试　　C.系统测试　　D.回归测试

(7)A.软件详细设计说明书　　B.技术开发合同

C.软件概要设计文档　　D.软件配置文档

【答案】B　C

【解析】

根据国家标准 GB/T15532-2008，软件测试可分为单元测试、集成测试、配置项测试、系统测试、验收测试和回归测试等类别。

单元测试也称为模块测试，测试的对象是可独立编译或汇编的程序模块、软件构件或面向对象软件中的类(统称为模块)，其目的是检查每个模块能否正确地实现设计说明中的功能、性能、接口和其他设计约束等条件，发现模块内可能存在的各种差错。单元测试的技术依据是软件详细设计说明书。

集成测试的目的是检查模块之间，以及模块和已集成的软件之间的接口关系，并验证已集成的软件是否符合设计要求。集成测试的技术依据是软件概要设计文档。

系统测试的对象是完整的、集成的计算机系统，系统测试的目的是在真实系统工作环境下，验证完整的软件配置项能否和系统正确连接，并满足系统/子系统设计文档和软件开发合同规定的要求。系统测试的技术依据是用户需求或开发合同。

配置项测试的对象是软件配置项，配置项测试的目的是检验软件配置项与软件需求规格说明的一致性。

确认测试主要验证软件的功能、性能和其他特性是否与用户需求一致。

验收测试是指针对软件需求规格说明，在交付前以用户为主进行的测试。

回归测试的目的是测试软件变更之后，变更部分的正确性和对变更需求的复合型，以及软件原有的、正确的功能、性能和其他规定的要求的不损害性。

甲、乙、丙、丁 4 人加工 A、B、C、D 四种工件所需工时如下表所示。指派每人加工一

种工件，四人加工四种工件其总工时最短的最优方案中，工件 B 应由（8）加工。

	A	B	C	D
甲	14	9	4	15
乙	11	7	7	10
丙	13	2	10	5
丁	17	9	15	13

(8)A.甲　　B.乙　　C.丙　　D.丁

【答案】D

【解析】本题考查数学(运筹学)应用的能力。

本题属于指派问题：要浓在 4X4 矩阵中找出四个元素，分别位于不同行、不同列，使其和达到最小值。

显然，任一行(或列)各元素都减(或加)一常数后，并不会影响最优解的位置，只是目标值(指派方案的各项总和)也减(或加)了这一常数。

我们可以利用这一性质使矩阵更多的元素变成 0，其他元素保持正，以利于求解。

$$\begin{pmatrix}14&9&4&15\\11&7&7&10\\13&2&10&5\\17&9&15&13\end{pmatrix}\xrightarrow{\begin{array}{l}\text{第 1 列都减 11}\\\text{第 2 列都减 2}\\\text{第 3 列都减 4}\\\text{第 4 列都减 5 得}\end{array}}\begin{pmatrix}3&7&0&10\\0&5&3&5\\2&0&6&0\\6&7&11&8\end{pmatrix}$$

$$\xrightarrow{\text{第 4 行都减 6 得}}\begin{pmatrix}3&7&0&10\\0&5&3&5\\2&0&6&0\\0&1&5&2\end{pmatrix}$$。累计减数 11+2+4+5+6=28。

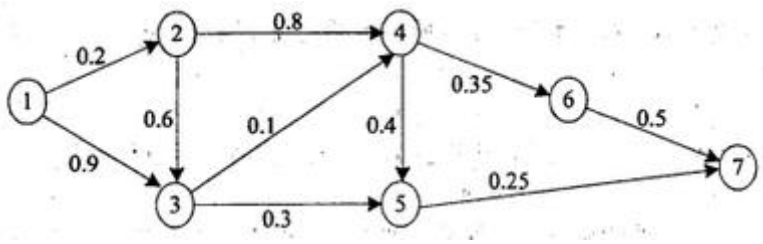
对该矩阵，并不存在全 0 指派。位于(1，3)、(2，1)、(3，4)、(4，2)的元素之和为]是最小的。因此，分配甲、乙、丙、丁分别加工 C、A、D、B 能达到最少的总工时 28+1=29。更进一步，再在第三行上都加 1，第 2、4 列上都减 1，可得到更多 0 元素。

$$\begin{pmatrix}3&6&0&9\\0&4&3&4\\3&0&7&0\\0&0&5&1\end{pmatrix}$$，这样就断定上述位置是唯一的全 0（最优）指派。

本题也可用试验法解决，但比较烦琐，需要仔细，不要遗漏。

小王需要从①地开车到⑦地，可供选择的路线如下图所示。图中，各条箭线表示路段及其行驶方向，箭线旁标注的数字表示该路段的拥堵率（描述堵车的情况，即堵车概率）。拥堵率=1-畅通率，拥堵率=0 时表示完全畅通，拥堵率=1 时表示无法行驶。根据该图，小王选

择拥堵情况最少（畅通情况最好）的路线是（9）。

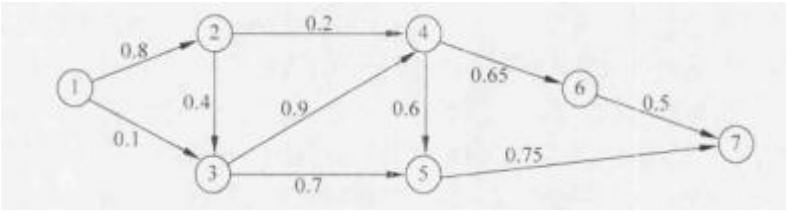


(9)A.①②③④⑤⑦　　B.①②③④⑥⑦　　C.①②③⑤⑦　　D.①②④⑥⑦

【答案】C

【解析】本题考查数学(概率)应用的能力。

首先将路段上的拥堵率转换成畅通率如下图：



每一条路线上的畅通率等于所有各段畅通率之乘积。两点之间的畅通率等于两点之间所有可能路线畅通率的最大值。以下用T(ijk...)表示从点i出发，经过点j、k...等的路线的畅通率。

据此原则，可以从①开始逐步计算到达各点的最优路线。

T(①②)=0.8；对应路线①②

T(①③)=max(0.1，0.8×0.4)=0.32；对应路线①②③

T(①④)=max(0.8×0.2，0.32×0.9)=0.288；对应路线①②③④

T(①⑤)=max(0.32×0.7，0.288×0.6)=0.224；对应路线①②③⑤

T(①⑥)=0.224×0.65=0.1456；对应路线①②③⑥

T(①⑦)=max(0.1456×0.5，0.224×0.75)=0.168；对应路线①②③⑤⑦

结论：小王应选择路线①②③⑤⑦，该线路有最好的畅通率0.168，或最小的拥堵率0.832。

软件设计师王某在其公司的某一综合信息管理系统软件开发项目中、承担了大部分程序设计工作。该系统交付用户，投入试运行后，王某辞职离开公司，并带走了该综合信息管理系统的源程序，拒不交还公司。王某认为综合信息管理系统源是他独立完成的，他是综合信息管理系统源程序的软件著作权人。王某的行为（10）。

(10)A.侵犯了公司的软件著作权　　B.未侵犯公司的软件著作权

C.侵犯了公司的商业秘密权　　D.不涉及侵犯公司的软件著作权

【答案】A

【解析】本题考查知识产权基本知识。

《计算机软件保护条例》第13条规定“自然人在法人或者其他组织中任职期间所开发的软件有下列情形之一的，该软件著作权由该法人或者其他组织享有，该法人或者其他组织可以对开发软件的自然人进行奖励：

(一)针对本职工作中明确指定的开发目标所开发的软件；

(二)开发的软件是从事本职工作活动所预见的结果或者自然的结果；

(三)主要使用了法人或者其他组织的资金、专用设备、未公开的专门信息等物质技术条件所开发并由法人或者其他组织承担责任的软件。”

根据《计算机软件保护条例》规定，可以得出这样的结论，当公民作为某单位的职工时，如果其开发的软件属于执行本职工作的结果，该软件著作权应当归单位享有。而荜位可以给予开发软件的职工奖励。需要注意的是，奖励软件开发者并不是单位的一种法定义务，软件开发者不可援引《计算机软件保护条例》强迫单位对自己进行奖励。

王某作为公司的职员，完成的某一综合信息管理系统软件是针对其本职工作中明确指定的开发目标而开发的软件。该软件应为职务作品，并属于特殊职务作品。公司对该软件享有除署名权外的软件著作权的其他权利，而王某只享有署名权。王某持有该软件源程序不归还公司的行为，妨碍了公司正常行使软件著作权，构成对公司软件著作权的侵犯，应承担停止侵权责任，即交还软件源程序。

下面的网络中不属于分组交换网的是（11）。

(11)A.ATM　　B.POTS　　C.X.25　　D.IPX/SPX

【答案】B

【解析】

ATM网络是分组交换网，交换的单元是信元；X.25是分组交换网，交换的单元是X.25分组；IPS/SPX也是分组交换网，在网络层交换的是IPX分组，只有POTS(Plain Old Telephone Service，普通老式电话业务)，不是分组交换网，这种网终中传输的是用模拟信号表示的语音流。

ADSL 采用（12）技术把 PSTN 线路划分为话音、上行和下行三个独立的信道，同时提供话音和联网服务，ADSL2+技术可提供的最高下载速率达到（13）Mb/s。

(12)A.时分复用　　B.频分复用　　C.空分复用　　D.码分多址

(13)A.8　　B.16　　C.24　　D.54

【答案】B　　C

【解析】

ADSL 采用频分复用技术把 PSTN 线路划分为话音、上行和下行三个独立的信道，同时提供话音和联网服务，ADSL2+技术可提供的最高下行速率达到 24Mb/s。

下面 4 组协议中，属于第二层隧道协议的是（14），第二层隧道协议中必须要求 TCP/IP 支持的是（15）。

(14)A.PPTP 和 L2TP　　B.PPTP 和 IPSec　　C.L2TP 和 GRE　　D.L2TP 和 IPSec

(15)A.IPSec　　B.PPTP　　C.L2TP　　D.GRE

【答案】A　　B

【解析】

PPTP 和 L2TP 都属于第二层隧道协议，PPTP 和 L2TP 都便用 PPP 协议对数据进行封装，然后添加包头用于在互联网络上传输。两个协议存在以下几方面的区别。

①PPTP 要求因特网络为 IP 网络，L2TP 只要求隧道媒介提供面向数据包的点对点连接。L2TP 可以在 1P(使用 UDP)、帧中继永久虚拟电路(PVCs)、X.25 虚电路(VCs)或 ATM 网络上使用。

②PPTP 只能在两端点间建立单一隧道，L2TP 支持在两端点间使用多个隧道。使用 L2TP，用户可以针对不同的服务质量创建不同的隧道。

③L2TP 可以提供包头压缩。当压缩包头时，系统开销占用 4 个字节，而在 PPTP 协议下要占用 6 个字节。

④L2TP 可以提供隧道验证，而 PPTP 则不支持隧道验证。但是，当 L2TP 或 PPTP 与 IPSec 共同使用时，可以由 IPSec 提供隧道验证，不需要在第 2 层协议上验证隧道。

IP 数据报的分段和重装配要用到报文头部的标识符、数据长度、段偏置值和（16）等四个字段，其中（17）字段的作用是为了识别属于同一个报文的各个分段，（18）的作用是指示每一分段在原报文中的位置。

(16)A.IHL B.M 标志 C.D 标志 D.头校验和

(17)A.IHL B.M 标志 C.D 标志 D.标识符

(18)A.段偏置值 B.M 标志 C.D 标志 D.头校验和

【答案】B D A

【解析】

在 DoD 和 ISO 的 IP 协议中使用了 4 个字段处理分段和重装配问题。一个是报文 ID 字段，它唯一地标识了某个站某一个协议层发出的数据。在 DoD 的 IP 协议中，ID 字段由源站和目标站地址、产生数据的协议层标识符以及该协议层提供的顺序号组成。第二个字段是数据长度，即字节数。第三个字段是偏置值，即分段在原来数据报中的位置，以 8 个字节(64 位)的倍数计数。最后是 M 标志，表示是否为最后一个分段。

当一个站发出数据报时对长度字段的赋值等于整个数据字段的长度，偏置值为 0，M 标志置为 False(用 0 表示)。如果一个 IP 模块要对该报文分段，则按以下步骤进行。

①对数据块的分段必须在 64 位的边界上划分，因而除最后一段外，其他段长都是 64 位的整数倍。

②对得到的每一分段都加上原来数据报的 IP 头，组成短报文。

③每一个短报文的长度字段置为它包含的字节数。

④第一个短报文的偏置值置为 0，其他短报文的偏置值为它前边所有报文长度之和(字节数)除以 8。

⑤最后一个报文的 M 标志置为 0(False)，其他报文的 M 标志置为 1(True)。

TCP 使用的流量控制协议是（19），TCP 段头中指示可接收字节数的字段是（20）。

(19)A.固定大小的滑动窗口协议 B.可变大小的滑动窗口协议

C.后退 N 帧 ARQ 协议 D.停等协议

(20)A.偏置值 B.窗口 C.检查和 D.接收顺序号

【答案】B B

【解析】

TCP 的流量控制机制是可变大小的滑动窗口协议，由接收方在窗口字段中指明接收缓冲区的大小。发送方发送了规定的字节数后等待接收方的下一次请求。固定大小的滑动窗口协议用在数据链路层的 HDLC 中。可变大小的滑动窗口协议可以应付长距离通信过程中线路延迟不确定的情况，而固定大小的滑动窗口协议则适合链路两端点之间通信延迟固定的情况。

AAA 服务器（AAA server）是一种处理用户访问请求的框架协议，它主要功能有 3 个，但是不包括（21），通常用来实现 AAA 服务的协议是（22）。

(21)A.身份认证　　B.访问授权　　C.数据加密　　D.计费

(22)A.Kerberos　　B.RADIUS　　C.SSL　　D.IPSec

【答案】C　B

【解析】

AAA 服务器的主要目的是管理用户访问网络服务器权限，具体为：

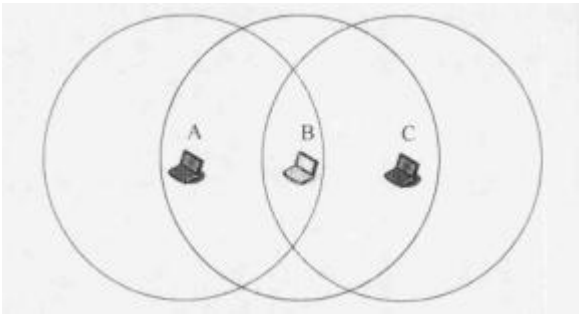
1. 验证(Authentication):验证用户是否可以获得访问权限。

2. 授权(Authorization):授权用户可以使用哪些服务。

3. 记账(Accounting):记录用户使用网络资源的情况。

通常用来实现 AAA 服务的协议是 RADIUS(Remote Authentication Dial In User Service)协议，这是基于 UDP 的一种客户机/服务器协议。RADIUS 客户机是网络访问服务器，它通常是一个路由器、交换机或无线访问点。RADIUS 服务器通常是在 UNIX 或 Windows 2000 服务器上运行的一个监护程序。

由无线终端组成的 MANET 网络，与固定局域网最主要的区别是（23），在下图所示的由 A、B、C 三个结点组成的 MANET 中，圆圈表示每个结点的发送范围，结点 A 和结点 C 同时发送数据，如果结点 B 不能正常接收，这时结点 C 称为结点 A 的（24）。



(23)A.无线访问方式可以排除大部分网络入侵

B.不需要运行路由协议就可以互相传送数据

C.无线信道可以提供更大的宽带

D.传统的路由协议不适合无线终端之间的通信

(24)A.隐蔽终端　　B.暴露终端　　C.干扰终端　　D.并发终端

【答案】D A

【解析】

IEEE802.il 标准定义的 AdHoc 网络是由无线移动结点组成的对等网，无须网络基础设施的支持，能够根据通信环境的变化实现动态重构，提供基于多跳无线连接的分组数据传输服务。在这种网络中，每一个结点既是主机，又是路由器，它们之间相互转发分组，形成一种自组织的 MANET(Mobile Ad Hoc Network)网络。

与传统的有线网络相比，MANET 有如下特点：

•网络拓扑结构是动态变化的，由于无线终端的频繁移动，可能导致结点之间的相互位置和连接关系难以维持稳定。

•无线信道提供的带宽较小，而信号衰落和噪声干扰的影响却很大。由于各个终端信号覆盖范围的差别，或者地形地物的影响，还可能存在单向信道。

•无线终端携带的电源能量有限，应采用最节能的工作方式，因而要尽量减小网络通信开销，并根据通信距离的变化随时调整发射功率。

•由于无线链路的开放性，容易招致网络窃听、欺骗、拒绝服务等恶意攻击的威胁，所以需要特别的安全防护措施。

路由算法是 MANET 网络中重要的组成部分，由于上述特殊性，传统有线网络的路由协议不能直接应用于 MANET。IETF 成立的 MANET 工作组开发了 MANET 路由规范，使其能够支持包含上百个路由器的自组织网络，并在此基础上开发支持其他功能的路由协议，例如支持节能、安全、组播、QoS 和 IPv6 的路由协议。

无线移动自组织网络中有一种特殊的现象，这就是隐蔽终端和暴露终端问题。在本题的图中，如果结点 A 向结点 B 发送数据，则由于结点 C 检测不到 A 发出的载波信号，它若试图发送，就可能干扰结点 B 的接收。所以对 A 来说，C 是隐蔽终端。另一方面，如果结点 B 要向结点 A 发送数据，它检测到结点 C 正在发送，就可能暂缓发送过程。但实际上 C 发出的载波不会影响 A 的接收，在这种情况下，结点 C 就是暴露终端。这些问题不但会影响数据链路层的工作状态，也会对路由信息的及时交换以及网络重构过程造成不利影响。

移动通信 4G 标准与 3G 标准主要的区别是（25），当前 4G 标准有（26）。

(25)A.4G 的数据速速率更高，而 3G 的覆盖范围更大

B.4G 是针对多媒体数据传输的，而 3G 只能传送话音信号

C.4G 是基于 IP 的分组交换网，而 3G 是针对语音通信优化设计的

D.4G 采用正交频分多路复用技术，而 3G 系统采用的是码分多址技术

(26)A.UMB 和 WiMAX Ⅱ B.LTE 和 WiMAX Ⅱ C.LTE 和 UMB D.TD-LTE 和 FDD-LTE

【答案】C B

【解析】

移动通信 4G 标准与 3G 标准最主要的区别是：4G 是基于 IP 的分组交换网，而 3G 是针对语音通信优化设计的，当前 4G 标准有 LTE 和 WiMAX II。

在从 IPv4 向 IPv6 过渡期间，为了解决 IPv6 主机之间通过 IPv4 网络进行通信的问题，需要采用（27），为了使得纯 IPv6 主机能够与纯 IPv4 主机通信，必须使用（28）。

(27)A.双协议栈技术 B.隧道技术 C.多协议栈技术 D.协议翻译技术

(28)A.双协议栈技术 B.隧道技术 C.多协议栈技术 D.协议翻译技术

【答案】B D

【解析】

IETF 的 NGTRANS 工作组研究了从 IPv4 向 IPv6 过渡的问题，提出了一系列的过渡技术和互连方案。过渡初期要解决的问题可以分成两类：第一类是解决 IPv6 孤岛之间互相通信的问题，第二类是解决 IPv6 孤岛与 IPv4 海洋之间的通信问题。目前提出的过渡技术可以归纳为以下 3 种：

①隧道技术：用于解决 IPv6 结点之间通过 IPv4 网络进行通信的问题；

②双协议栈技术：使得 IPv4 和 IPv6 可以共存于同一设备和同一网络中；

③翻译技术：使得纯 IPv6 结点与纯 IPv4 结点之间可以进行通信。

原站收到“在数据包组装期间生存时间为 0”的 ICMP 报文，出现的原因是（29）。

(29)A.IP 数据报目的地址不可达 B.IP 数据报目的网络不可达

C.ICMP 报文校验差错 D.IP 数据报分片丢失

【答案】D

【解析】本题考查 ICMP 报文及使用情况相关基础知识。

在 IP 报文传输过程中出现错误或对对方主机进行探测时发送 ICMP 报文。ICMP 报文报告的差错有多种，其中源站收到“在数据包组装期间生存时间为 0”的 ICMP 报文时，说明 IP 数据报分片丢失。IP 报文在经历 MTU 较小的网络时，会进行分片和重装，在重装路由器上对同一分组的所有分片报文维持一个计时器，当计时器超时还有分片没到，重装路由器会

丢弃收到的该分组的所有分片，并向源站发送“在数据包组装期间生存时间为0”的ICMP报文。

下列DHCP报文中，由客户端发送给DHCP的服务器的是（30）。

(30)A.DhcpOffer B.DhcpDecline C.DhcpAck D.DhcpNack

【答案】B

【解析】本题考查DHCP报文相关基础知识。

DhcpOffer是服务器在收到客户端发现报文，且可为其分配IP地址时发送的响应报文；DhcpAck是服务器端在接收到客户端请求报文后，为客户端分配地址时采用的报文;DhcpAck是服务器端在接收到客户端请求报文后，不能为客户端分配地址时采用的报文;如果客户端发现DHCP SERVER分配的IP地址已经被别人使用,会发出DhcpDecline报文通知DHCP SERVER禁用这个IP地址，以免引起IP地址冲突。

在windows用户管理中，使用组策略A-G-DL-P，其中DL表示（31）。

(31)A.用户账号 B.资源访问权限 C.域本地组 D.通用组

【答案】C

【解析】本题考查Windows用户组策略相关基础知识。

组策略A-G-DL-P中，A是用户账号，G表示全局组，DL表示域本地组，P表示资源访问权限。

在光纤测试过程中，存在强反射时，使得光电二极管饱和，光电二极管需要一定的时间由饱和状态中恢复，在这一时间内，它将不会精确地检测后散射信号，在这一过程中没有被确定的光纤长度称为盲区。盲区一般表现为前端盲区，为了解决这一问题，可以（32），以便将此效应减到最小。

(32)A.采用光功率计进行测试 B.在测试光缆后加一条长的测试光纤

C.在测试光缆前加一条测试光纤 D.采用OTDR进行测试

【答案】C

【解析】本题考查光纤测试实际工程项目知识。

在测试光缆前加一条长的测试光纤来解决前端盲区问题。

S/MIME 发送报文的过程中对消息 M 的处理包括生成数字指纹、生成数字签名、加密数字签名和加密报文 4 个步骤，其中生成数字指纹采用的算法是（33），加密数字签名采用的算法是（34）。

(33)A.MD5　　B.3DES　　C.RSA　　D.RC2

(34)A.MD5　　B.RSA　　C.3DES　　D.SHA-1

【答案】A　C

【解析】本题考查安全协议 S/MIME 对报文的处理过程。

S/MIME 发送报文的过程中，对消息 M 的处理包括生成数字指纹、生成数字签名、加密数字签名和加密报文 4 个步骤。首先生成的数字指纹是对消息采用 Hash 运算之后的摘要，四个选项中只有 MD5 是摘要算法；生成数字签名通常采用公钥算法；加密数字签名需采用对称密钥，四个选项中只有 3DES 是对称密钥；加密报文也得采用对称密钥，计算复杂性较小。

下列 DNS 查询过程中，采用迭代查询的是（35），采用递归查询的是（36）。

(35)A.客户端向本地 DNS 服务器发出查询请求

B.客户端在本地缓存中找到目标主机的地址

C.本地域名服务器缓存中找到目标主机的地址

D.由根域名服务器找到授权域名服务器的地址

(36)A.转发查询非授权域名服务费

B.客户端向本地域名服务器发出查询请求

C.由上级域名服务器给出下级服务器的地址

D.由根域名服务器找到授权域名服务器的地址

【答案】D　B

【解析】

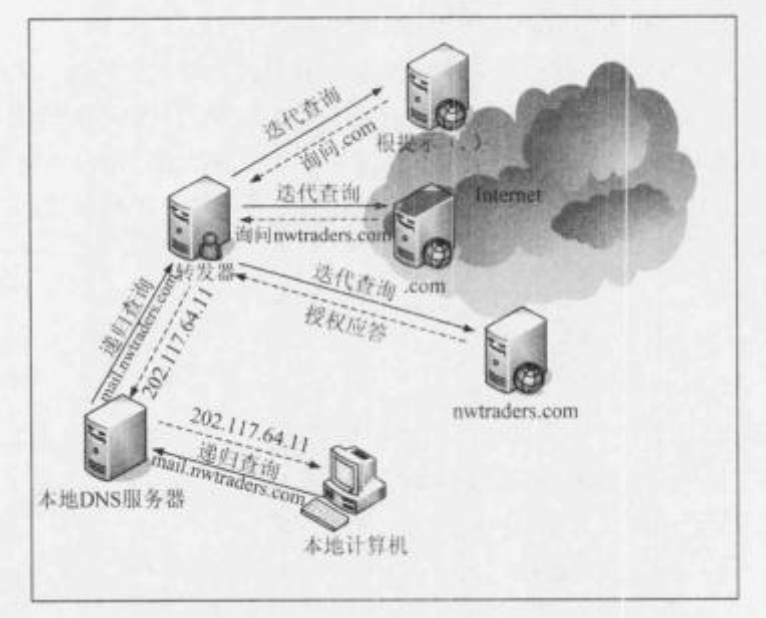
DNS 查询过程分为两种查询方式：

①递归查询：当用户发出查询请求时，本地服务器要进行递归查询。这种查询方式要求服务器彻底地进行名字解析，并返回最后的结果一一 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由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 1P 地址，则本地服务器要把查询请求发送给这些服务器做进一步的查询。

②迭代查询：服务器与服务器之间的查询采用迭代的方式进行，发出查询请求的服务器

得到的响应可能不是目标的 IP 地址，而是其他服务器的引用(名字和地址)，那么本地服务器就要访问被引用的服务器，做进一步的查询。如此反复多次，每次都更接近目标的授权服务器，直至得到最后的结果——目标的 IP 地址或错误信息。

关于递归查询和迭代查询应用的具体场合可参见下图，首先是本地计算机向本地 DNS 服务器进行递归查询，本地服务器查找不到需要的记录，则向转发器发出递归查询请求。转发器通过迭代查询得到需要的结果后，转发给本地 DNS 服务器，并返回本地计算机。



DHCP 服务器分配的默认网关地址是 220.115.5.33/28，（37）是该子网主机地址。

(37)A.220.115.5.32　　B.220.115.5.40　　C.220.115.5.47　　D.220.115.5.55

【答案】B

【解析】

由于默认网关的地址为 220.115.5.33/28，所以与其同一子网的主机地址为 220.115.5.40，参见下面的二进制表示。

220.115.5.33/28：1101 1100.0111 0011.0000 0101.0010 0001

220.115.5.40：1101 1100.0111 0011.0000 0101.0010 1000

主机地址 122.34.2.160 属于子网（38）。

(38)A.122.34.2.64/26　B.122.34.2.96/26　C.122.34.2.128/26 D.122.34.2.192/26

【答案】C

【解析】

主机地址 122.34.2.160 的二进制表示为：0111 1010.0010 0010.0000 0010.1010 0000
与其匹配的子网地址为 122.34.2.128/26：0111 1010.0010 0010.0000 0010.1000 0000

某公司的网络地址为 192.168.1.0，要划分成 5 个子网，每个子网最多 20 台主机，则适用的子网掩码是（39）。

(39)A.255.255.255.192　　B.255.255.255.240

C.255.255.255.224　　D.255.255.255.248

【答案】C

【解析】

子网掩码应为 255.255.255.224，其二进制表示为：
1111 1111.1111 1111.1111 1111.1110 0000
最后 3 个 1 用来区分 5 个子网，最右边的 5 位可提供最多 30 个主机地址。

以下关于 IPV6 的论述中，正确的是（40）。

(40)A.IPv6 数据包的首部比 IPv4 复杂　B.IPv6 的地址分为单播、广播和任意播 3 种

C.IPv6 地址长度为 128 比特　　D.每个主机拥有唯一的 IPv6 地址

【答案】C

【解析】

IPv6 地址增加到 128 位，并且能够支持多级地址层次；地址自动配置功能简化了网络地址的管理；在组播地址中增加了范围字段，改进了组播路由的可伸缩性；增加的任意播地址比 IPv4 中的广播地址更加实用。

IPv6 地址是一个或一组接口的标识符。IPv6 地址被分配到接口，而不是分配给结点。IPv6 地址有 3 种类型：

①单播(Unicast)地址

②任意播(AnyCast)地址

③组播(MultiCast)地址

在 IPv6 地址中，任何全“0”和全“1”字段都是合法的，除非特别排除的之外。特别是前缀可以包含“0”值字段，也可以用“0”作为终结字段。一个接口可以被赋予任何类型的多个地址(单播、任意播、组播)或地址范围。

与 IPv4 相比，IPv6 首部有下列改进：

①分组头格式得到简化：IPv4 头中的很多字段被丢弃，IPv6 头中字段的数量从 12 个降到了 8 个，中间路由器必须处理的字段从 6 个降到了 4 个，这样就简化了路由器的处理过程，提高了路由选择的效率。

②改进了对分组头部选项的支持：与 IPv4 不同，路由选项不再集成在分组头中，而是把扩展头作为任选项处理，仅在需要时才插入到 IPv6 头与负载之间。这种方式使得分组头的处理更灵活，也更流畅。以后如果需要，还可以很方便地定义新的扩展功能。

③提供了流标记能力：IPv6 增加了流标记，可以按照发送端的要求对某些分组进行特别的处理，从而提供了特别的服务质量支持，简化了对多媒体信息的处理，可以更好地传送具有实时需求的应用数据。

按照 RSA 算法，取两个最大素数 p 和 q，n=p*q，令 Φ(n)=(p-1)*(q-1)，取与 Φ(n)互质的数 e，d=e-1 mod Φ(n)，如果用 M 表示消息，用 C 表示密文，下面（41）是加密过程，（42）是解密过程。

(41)A. C=Me mod n　　B. C=Mn mod d　　C. C=Md mod Φ(n)　　D. C=Mn mod Φ(n)

(42)A. M=Cn mod e　　B. M=Cd mod n　　C. M=Cd mod Φ(n)　　D. M=Cn mod Φ(n)

【答案】A　B

【解析】本题考查 RSA 算法的基础知识。

RSA(Rivest Shamirand Adleman)是一种公钥加密算法。方法是按照下面的要求选择公钥和密钥。

1. 选择两个大素数 p 和 q(大于 10100)。

2. 令 n=p×q 和 z=(p-1)×(q-1)

3. 选择 d 与 z 互质。

4. 选择 e，使 e×d=1(mod z)

明文 P 被分成 k 位的块，k 是满足 2k<n 的最大整数，于是有 0≤P<n。加密时计算

C=Pe(mod n)

这样公钥为(e，n)。解密时计算

P=Cd(mod n)

即私钥为(d，n)。

A 和 B 分别从 CA1 和 CA2 两个认证中心获取了自己的证书 IA 和 IB，要使 A 能够对 B 进

行认证，还需要（43）。

(43)A.A 和 B 交换各自公钥　　B.A 和 B 交换各自私钥

C.CA1 和 CA2 交换各自公钥　　D.CA1 和 CA2 交换各自私钥

【答案】C

【解析】本题考查 CA 数字证书认证的基础知识。

CA 为用户产生的证书应具有以下特性。

①只要得到 CA 的公钥，就能由此得到 CA 为用户签署的公钥。

②除 CA 外，其他任何人员都不能以不被察觉的方式修改证书的内容。

如果所有用户都由同一 CA 签署证书，则这一 CA 就必须取得所有用户的信任。如果用户数量很多，仅一个 CA 负责为所有用户签署证书就可能不现实。通常应有多个 CA，每个 CA 为一部分用户发行和签署证书。用户之间需要进行认证，首先需要对各自的认证中心进行认证，要认证 CA，则需 CA 和 CA 之间交换各自的证书。

如图所示，①、②和③是三种数据包的封装方式，以下关于 IPSec 认证方式中，所使用的封装与其对应模式的匹配，（44）是正确的。

(44)A.传输模式采用封装方式①　　B.隧道模式采用封装方式②

C.隧道模式采用封装方式③　　D.传输模式采用封装方式③

【答案】C

【解析】本题考查 IPSec 数据封装的基础知识。

IPSec 传送认证或加密的数据之前，必须就协议、加密算法和使用的密钥进行协商。密钥交换协议提供这个功能，并且在#钥交换之前还要对远程系统进行初始的认证。

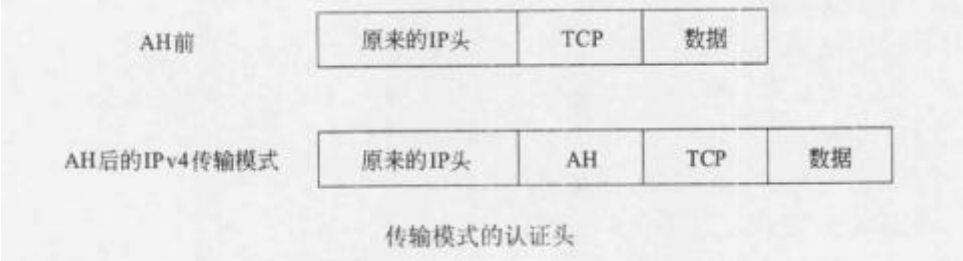
IPSec 认证头提供了数据完整性和数据源认证，但是不提供保密服务。AH 包含了对称密钥的散列函数，使得第三方无法修改传输中的数据。IPSec 支持下面的认证算法。

①HMAC-SHAKHashedMessageAuthenticationCode-SecureHashAlgorithm1)，128 位密钥。

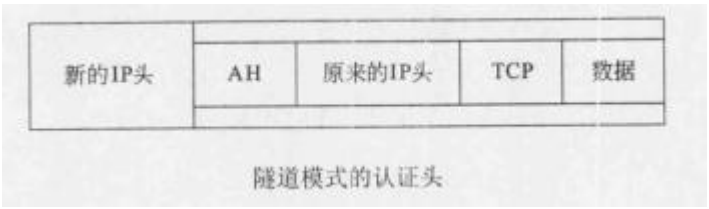
②HMAC-MD5(HMAC-MessageDigest5)，160 位密钥。

IPSec 有两种模式：传输模式和隧道模式。在传输模式中，IPSec 认证头插入原来的 IP 头之后(如下图所示)，IP 数据和 IP 头用来计算 AH 认证值。IP 头中的变化字段(例如跳步计

数和 TTL 字段)在计算之前置为 0，所以变化字段实际上并没有被认证。



在隧道模式中，IPSec 用新的 IP 头封装了原来的 IP 数据报(包括原来的 IP 头)，原来 IP 数据报的所有字段都经过了认证，如下图所示。



下列协议中，不用于数据加密的是（45）。

(45)A.IDEA　　B.Differ-hellman　　C.AES　　D.RC4

【答案】B

【解析】本题考查加密算法基础知识。

现代密码体制使用的基本方法仍然是替换和换位,但是采用更加复杂的加密算法和简单的密钥，而且增加了对付主动攻击的手段，例如加入随机的冗余信息，以防止制造假消息；加入时间控制信息，以防止旧消息重放。

常见的加密算法有 DES(Data Encryption Standard)加密算法、三重 DES(Triple-DES)加密算法、IDEA(International Data Encryption Algorithm)加密算法、高级加密标准(AdvancedEncryptionStandard，AES)加密算法、流加密算法和 RC4。

Diffie-Hellman 是一种确保共享 KEY 安全穿越不安全网络的方法，它是由 Whitefield 与 Martin Heilman 在 1976 年提出的一种奇妙的密钥交换协议，称为 Diffie-Hellman 密钥交换协议/算法(Diffie-HellmanI Cey Exchange/Agreement Algorithm)。这个机制的巧妙在于需要安全通信的双方可以用这个方法确定对称密钥。然后可以用这个密钥进行加密和解密。但是注意，这个密钥交换协议/算法只能用于密钥的交换.而不能进行消息的加密和解密。双方确定要用的密钥后，要使用其他对称密钥操作加密算法实际加密和解密消息。

下列关于数字证书的说法中，正确的是（46）。

(46)A.数字证书是在网上进行信息交换和商务活动的身份证明

B.数字证书使用公钥体制，用户使用公钥进行加密和签名

C.在用户端，只需维护当前有效的证书列表

D.数字证明用于身份证明，不可公开

【答案】A

【解析】本题考查数字证书的基础知识。

数字证书是各类终端实体和最终用户在网上进行信息交流及商务活动的身份证明，在电子交易的各个环节，交易的各方都需验证对方数字证书的有效性，从而解决相互间的信任问题。

数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密和解密。每个用户自己设定一个特定的仅为本人所知的私有密钥(私钥)，用它进行解密和签名，同时设定一个公共密钥(公钥)，并由本人公开，为一组用户所共享，用于加密和验证。公开密钥技术解决了密钥发布的管理问题。一般情况下，证书中还包括密钥的有效时间、发证机构(证书授权中心)的名称及该证书的序列号等信息。数字证书的格式遵循 ITUTX.509 国际标准。

PPP 协议不包含（47）。

(47)A.封装协议　　B.点对点隧道协议（PPTP）

C.链路控制协议（LCP）　　D.网络控制协议（NCP）

【答案】B

【解析】本题考查 PPP 协议的基础知识。

PPP 协议(Point-to-Point Protocol)可以在点对点链路上传输多种上层协议的数据包。PPP 是数据链路层协议，最早是替代 SLIP 协议用来在同步链路上封装 IP 数据报的，后来也可以承载诸如 DECnet、Novell IPX、Apple Talk 等协议的分组。PPP 是一组协议，包含下列成分。

①封装协议。用于包装各种上层协议的数据报。PPP 封装协议提供了在同一链路上传输各种网络层协议的多路复用功能，也能与各种常见的支持硬件保持兼容。

②链路控制协议(Link Control Protocol，LCP)。通过以下三类 LCP 分组来建立、配置和管理数据链路连接。

③网络控制协议。在 PPP 的链路建立过程中的最后阶段将选择承载的网络层协议，例如 IP、IPX 或 Apple Talk 等。PPP 只传送选定的网络层分组，任何没有入选的网络层分组将被

丢弃。

以下关于数据备份策略的说法中，错误的是（48）。

(48)A.完全备份是备份系统中所有的数据

B.增量备份是只备份上一次完全备份后有变化的数据

C.差分备份是指备份上一次完全备份后有变化的数据

D.完全、增量和差分三种备份方式通常结合使用，以发挥出最佳的效果

【答案】B

【解析】本题考查数据备份策略的基础知识。

完全备份就是备份系统中所有的数据，并不依赖文件的存档属性来确定备份哪些文件。在备份过程中，任何现有的标记都被清除，每个文件都被标记为已备份。换言之，清除存档属性。差分备份仅对自上一次完全备份之后有变化的数据进行备份。差分备份过程中，只备份有标记的那些选中的文件和文件夹。它不清除标记，也即备份后不标记为已备份文件。换言之，不清除存档属性。增量备份自上一次备份(包含完全备份、差分备份、增量备份)之后有变化的数据。增量备份过程中，只备份有标记的选中的文件和文件夹，它清除标记，即备份后标记文件，换言之，清除存铛属性。完全、增量和差分三种备份方式通常结合使用，以发挥出最佳的效果。

假如有 3 块容量是 80G 的硬盘做 RAID 5 阵列，则这个 RAID 5 的容量是（49）。而如果有 2 块 80G 的盘和 1 块 40G 的盘，此时 RAID 5 的容量是（50）。

(49)A.240G　　B.160G　　C.80G　　D.40G

(50)A.40G　　B.80G　　C.160G　　D.200G

【答案】B　B

【解析】本题考查 RAID 的基础概念。

RAID(Redundant Arrayof Independent Disks)的中文简私为独立冗余磁盘阵列。简单的说，RAID 是一种把多块独立的硬盘(物理硬盘)按不同的方式组合起来形成一个硬盘组(逻辑硬盘)，从而提供比单个硬盘更高的存储性能和提供数据备份技术。组成磁盘阵列的不同方式称为 RAID 级别(RAIDLevels)。在用户看起来，组成的磁盘组就像是一个硬盘，用户可以对它进行分区，格式化等。总之，对磁盘阵列的操作与单个硬盘一模一样。不同的是，磁盘阵列的存储速度要比单个硬盘高很多，而且可以提供自动数据备份。数据备份的功能是在

用户数据一旦发生损坏后，利用备份信息可以使损坏数据得以恢复，从而保障了用户数据的安全性。RAID 技术分为几种不同的等级，分别可以提供不同的速度，安全性和性价比。根据实际情况选择适当的 RAID 级别可以满足用户对存储系统可用性、性能和容量的要求。常用的 RAID 级别有以下几种:NRAID，JBOD，RAIDO，RAID1，RAID1+0，RAID3，RAID5 等。目前经常使用的是 RAID5 和 RA1D(1+0)。如果使用物理硬盘容量不相等的硬盘做 RAID，那么创建的 RAID 阵列的总容量为较小的硬盘的计算方式。

RAID5 的存储机制是两块存数据，一块存另外两块硬盘的交易校验结果。RAID5 建立后，坏掉一块硬盘，可以通过另外两块硬盘的数据算出第三块的，所以至少要 3 块。RAID5 是一种旋转奇偶校验独立存取的阵列方式，它与 RAID3、RAID4 不同的是没有固定的校验盘，而是按某种规则把奇偶校验信息均匀地分布在阵列所属的硬盘上，所以在每块硬盘上，既有数据信息也有校验信息。这一改变解决了争用校验盘的问题，使得在同一组内并发进行多个写操作。所以 RAID5 既适用于大数据量的操作，也适用于各种事务处理，它是一种快速、大容量和容错分布合理的磁盘阵列。当有 N 块阵列盘时，用户空间为 N-1 块盘容量。

根据以上原理，共有 3 块 80G 的硬盘做 RAID5，则总容量为(3-1)×80=160G；如果有 2 块 80G 的盘和 1 块 40G 的盘，则以较小的盘的容量为计算方式.总容量为(3-1)×40==80G。

以下关于网络分层模型的叙述中，正确的是（51）。

(51)A.核心层为了保障安全性，应该对分组进行尽可能多的处理

B.汇聚层实现数据分组从一个区域到另一个区域的高速转发

C.过多的层次会增加网络延迟，并且不便于故障排查

D.接入层应提供多条路径来缓解通信瓶颈

【答案】C

【解析】本题考查网络需求分析中分层模型的各层功能。

核心层的目的是保障高速转发，需要对分组进行尽可能少的处理：汇聚层实现由接入层传递数据的汇聚，实现包过滤等安全处理；接入层负责用户的接入，无须冗余路径。的确，过多的层次会增加网络延迟，并且不便于故障排查。

以下关于网络规划设计过程叙述中，属于需求分析阶段任务是（52）。

(52)A.依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境

B.制定对设备厂商、服务提供商的选择策略

C.根据需求范文和通信规范，实施资源分配和安全规划

D.确定网络设计或改造的任务，明确新网络的建设目标

【答案】D

【解析】本题考查网络需求分析中各阶段的功能。

依据逻辑网络设计的要求，确定设备的具体物理分布和运行环境是物理设计阶段的任务；制定对设备厂商、服务提供商的选择策略是逻辑设计阶段的任务；根据需求规范和通信规范，实施资源分配和安全规划是逻辑设计阶段的任务；确定网络设计或改造的任务，明确新网络的建设目标是需求阶段的任务。

某高校欲构建财务系统，使得用户可通过校园网访问该系统。根据需求，公司给出如下2套方案。

方案一：

1)出口设备采用一台配置防火墙板卡的核心交换机，并且使用防火墙策略将需要对校园网做应用的服务器进行地址映射；

2)采用4台高性能服务器实现整体架构，其中3台作为财务应用服务器、1台作为数据备份管理服务器；

3)通过备份管理软件的备份策略将3台财务应用服务器的数据进行定期备份。

方案二：

1)出口设备采用1台配置防火墙板卡的核心交换机，并且使用防火墙策略将需要对校园网做应用的服务器进行地址映射；

2)采用2台高性能服务器实现整体架构，服务器采用虚拟化技术，建多个虚拟机满足财务系统业务需求。当一台服务器出现物理故障时将业务迁移到另外一台物理服务器上。

与方案一相比，方案二的优点是(53)。方案二还有一些缺点，下列不属于其缺点的是(54)。

(53)A.网络的安全性得到保障　　B.数据的安全性得到保障

C.业务的连续性得到保障　　D.业务的可用性得到保障

(54)A.缺少企业级磁盘阵列，不能将数据进行统一的存储与管理

B.缺少网闸，不能实现财务系统与Internet的物理隔离

C.缺少安全审计，不便于相关行为的记录、存储与分析

D.缺少内部财务用户接口，不便于快速管理与维护

【答案】C　B

【解析】本题考查网络规划与设计案例。

与方案一相比，方案二服务器采用虚拟化技术，当一台服务器出现物理故障时将业务迁移到另外一台物理服务器上，保障了业务的连续性。网络的安全性、数据的安全性、业务的可用性都没有发生实质性变化。

当然方案二还有一些缺陷，首先是缺少将数据进行统一的存储与管理的企业级磁盘阵列；其次缺少安全审计，不便于相关行为的记录、存储与分析；而且缺少内部财务用户接口，不便于快速管理与维护。但是如果加网闸，就不能实现对财务系统的访问。不能实现用户可通过校园网对财务系统的访问。

某大学拟建设无线校园网，委托甲公司承建，甲公司的张工带队去进行需求调研，获得的主要信息有：

校园面积约 4km2，要求在室外绝大部分区域及主要建筑物内实现覆盖，允许同时上网用户数量为 5000 以上，非本校师生不允许自由接入，主要业务类型为上网浏览、电子邮件、FTP、QQ 等，后端与现有校园网相连。

张工据此撰写了需求分析报告，提交了逻辑网络设计方案，其核心内容包括：

①网络拓扑设计

②无线网络设计

③安全接入方案设计

④地址分配方案设计

⑤应用功能配置方案设计

以下三个方案中符合学校要求，合理可行的是：

无线网络选型的方案采用（55）；室外供电的方案是（56）；无线网络安全接入的方案是（57）。

(55)A.基于 WLAN 的技术建设无线校园网

B.基于固定 WiMAX 的技术建设无线校园网

C.直接利用电信运营商的 3G 系统

D.暂缓执行，等待移动 WiMAX 成熟并商用

(56)A.采用太阳能供电　　B.地下埋设专用供电电缆

C.高空架设专用供电电缆　　D.以 PoE 方式供电

(57)A.通过 MAC 地址认证　　B.通过 IP 地址认证

C.通过用户名与密码认证　　D.通过用户的物理位置认证

【答案】A　D　C

【解析】本题考查网络规划与设计案例。

首先，无线网络选型时基于 WLAN 的技术建设无线校园网是经济可行的方案；其次室外供电的方案是以 PoE 方式供电，太阳能供电不能保障不间断，地下埋设专用供电电缆以及高空架设专用供电电缆覆盖的范围较大，工程复杂。无线网络安全接入的方案是通过用户名与密码认证，其他方式都不适用。

互联网上的各种应用对网络 QoS 指标的要求不一，下列应用中对实时性要求最高的是（58）。

(58)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】本题考查网络应用及 QoS。

浏览页面、邮件接收以及文件传输对实时性没有太高要求，视频会议必须保障实时性。

下列关于网络测试的说法中，正确的是（59）。

(59)A.接入-汇聚链路测试的抽样比例应不低于 10%

B.当汇聚-核心链路数量少于 10 条时，无需测试网络传输速率

C.丢包率是指网络空载情况下，无法转发数据包的比例

D.连通性测试要求达到 5 个 9 标准，即 99.999%

【答案】A

【解析】本题考查网络测试的基础知识。

网络系统测试主要是测试网络是否为应用系统提供了稳定、高效的网络平台，如果网络系统不够稳定，网络应用就不可能快速稳定。对常规的以太网进行系统测试，主要包括系统连通性、链路传输速率、吞吐率、传输时延及链路层健康状况测试等基本功能测试。

所有联网的终端都必须按使用要求全部连通。

连通性测试方法一般有：

①将测试工具连接到选定的接入层设备的端口，即测试点；

②用测试工具对网络的关键服务器、核心层和汇聚层的关键网络设备(如交换机和路由器)，进行 10 次 Ping 测试,每次间隔 1s,以测试网络连通性。测试路径要覆盖所有的子网和 VLAN。

③移动测试工具到其他位置测试点，重复步骤②，直到遍历所有测试抽样设备。抽样规则以不低于接入层设备总数10%的比例进行抽样测试，抽样少于10台设备的，全部测试；每台抽样设备中至少选择一个端口，即测试点应能够覆盖不同的子网和VLAN。

合格标准分为单项合格判据和综合合格判据两种。

单项合格判据：测试点到关键节点的Ping测试连通性达到100%时，则判定单点连通性符合要求。

综合合格判据：所有测试点的连通性都达到100%时，则判定系统的连通性符合要求；否则判定系统的连通性不符合要求。

网络测试技术有主动测试和被动测试两种方式，（60）是主动测试。

(60)A.使用Sniffer软件抓包并分析　　B.向网络中发送大容量ping报文

C.读取SNMP的MIB信息并分析　　D.查看当前网络流量状况并分析

【答案】B

【解析】本题考查网络测试的基础知识。

网络测试有多种方法，根据测试中是否向被测网络注入测试流量，可以将网络测试方法分为主动测试和被动测试。

主动测试是指利用测试工具有目的地主动向被测网络注入测试流量，并根据这些测试流量的传送情况来分析网络技术参数的测试方法。主动测试具备良好的灵活性，它能够根据测试环境明确控制测量中所产生的测量流量的特征，如特性、采样技术、时标频率、调度、包大小、类型(模拟各种应用)等，主动测试使测试能够按照测试者的意图进行，容易进行场景仿真。主动测试的问题在于安全性。由于主动测试主动向被测网络注入测试流量，是“入侵式”的测量，必然会带来一定的安全隐患。如果在测试中进行细致的测试规划，可以降低主动测试的安全隐患。

被动测试是指利用特定测试工具收集网络中活动的元素(包括路由器、交换机、服务器等设备)的特定信息，以这些信息作为参考，通过量化分析，实现对网络性能、功能进行测量的方法。常用的被动测试方式包括：通过SNMP协议读取相关MIB信息，通过Sniffer、Ethereal等专用数据包捕获分析工具进行测试。被动测试的优点是它的安全性。被动测试不会主动向被测网络注入测试流量，因此就不会存在注入DDoS、网络欺骗等安全隐患；被动测试的缺点是不够灵活，局限性较大，而且因为是被动地收集信息，并不能按照测量者的意愿进行测试，会受到网络机构、测试工具等多方面的限制。

以下关于网络故障排除的说法中，错误的是（61）。

(61)A.ping 命令支持 IP、AppleTalk、Novell 等多种协议中测试网络的连通性

B.可随时使用 debug 命令在网络设备中进行故障定位

C.tracert 命令用于追踪数据包传输路径，并定位故障

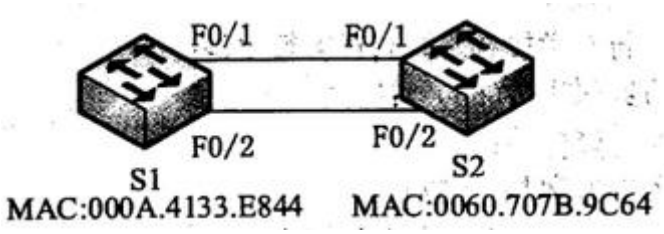
D.show 命令用于显示当前设备或协议的工作状况

【答案】B

【解析】本题考查网络故障排除的基础知识。

debug 命令是用于在网络中进行故障排查和故障定位的命令，该命令运行时，需耗费网络设备相当大的 CPU 资源，且会持续较长的时间，通常会造成网络效率的严重降低，甚至不可用。基于此，当需要使用 debug 命令来排查网络中的故障时，通常需在网络压力较小的时候进行，例如凌晨 2:00～6:00 这个时间段。

如图所示，交换机 S1 和 S2 均为默认配置，使用两条双绞线连接，（62）接口的状态是阻塞状态。



(62)A.S1 的 F0/1　　B.S2 的 F0/1　　C.S1 的 F0/2　　D.S2 的 F0/2

【答案】D

【解析】本题考查生成树协议的基础知识。

当两台交换机之间存在冗余链路时，势必会造成环路，为避免该情况的发生，交换机中自动开启的生成树协议会根据一定的选举规则将其中一个端口的状态调整为阻塞状态，以断开环路连接，以免造成网络风暴。选举规则是：首先确定根桥，优先级较高的交换机会被选举为根桥，优先级默认情况下相同，当优先级相同时，交换机 MAC 地址较小者会被选举为根桥，根桥上的端口均为根端口，根端口不会被设置为阻塞状态，非根桥交换机上的端口优先级较高(值小)者为指定端口，较低者为非指定端口(阻塞端口)，当接口优先级相同时，则比较接口编号，接口编号较大者将会被置为阻塞状态。

以下关于网络布线子系统的说法中，错误的是（63）。

(63)A.工作区子系统指终端到信息插座的区域

B.水平子系统是楼层接线间配线架到信息插座，线缆最长可达100m

C.干线子系统用于连接楼层之间的设备间，一般使用大对数铜缆或光纤布线

D.建筑群子系统连接建筑物，布线可采取地下管道铺设，直理或架空明线

【答案】B

【解析】本题考查综合布线的基础知识。

在综合布线系统中，分为工作区子系统、水平子系统、垂直干线子系统、管理子系统、建筑群子系统和设备间子系统。

工作区子系统的目的是实现工作区终端设备与水平子系统之间的连接，由终端设备连接到信息插座的连接线缆所组成。

水平子系统的目的是实现信息插座和管理子系统(跳线架)间的连接，将用户工作区引至管理子系统，并为用户提供一个符合国际标准，满足语音及高速数据传输要求的信息点出口，当使用双绞线为传输介质时，其最大传输距离为100米，而水平子系统连接着工作区与其他子系统，需为工作区子系统预留有一定长度的线缆余量，因此水平子系统的电缆长度一般不应超过100米。

垂直干线子系统的目的是实现计算机设备、程控交换机(rox)、控制中心与各管理子系统间的连接，是建筑物干线电缆的路由。

管理子系统由交连、互连配线架组成。管理点为连接其他子系统提供连接手段。交连和互连允许将通讯线路定位或重定位到建筑物的不同部分，以便能更容易地管理通信线路，使在移动终端设备时能方便地进行插拔。

建筑群子系统将一个建筑物的电缆延伸到建筑群的另外一些建筑物中的通信设备和装置上，是结构化布线系统的一部分，支持提供楼群之间通信所需的硬件。

设备间子系统主要是由设备间中的电缆、连接器和有关的支撑硬件组成，作用是将计算机、PBX、摄像头、监视器等弱电设备互连起来并连接到主配线架上。

某学生宿舍采用ADSL接入Internet，为扩展网络接口，用双绞线将两台家用路由器连接在一起，出现无法访问Internet的情况，导致该为题最可能的原因是（64）。

(64)A.双绞线质量太差　　B.两台路由器上的IP地址冲突

C.有强烈的无线信号干扰　　D.双绞线类型错误

【答案】B

【解析】本题考查网络故障排查的基本知识。

通常，目前市面上出售的家用路由器在默认情况下具备 DHCP、NAPT、扩展网络接口、简单的流量控制等功能。根据题目说明，使用 ADSL 接入 Internet，家用路由器应该采用的是动态 IP 地址的设置，如将两台家用路由器简单地使用双绞线相连时，两台路由器会将彼此认为是客户端，其上默认打开的 DHCP 服务器均会为对方分配 IP 地址，这样就会造成 IP 地址冲突，而导致无法通信。

IP SAN 区别于 FC SAN 以及 IB SAN 的主要技术是采用（65）实现异地间的数据交换。

(65)A.I/O　　B.iSCSI　　C.InfiniBand　　D.Fibre Channel

【答案】B

【解析】本题考查网络应用及 QoS。

IP SAN 区别于 FC SAN 以及 IB SAN 的主要技术是采用 iSCSI 实现异地间的数据交换，IB SAN 的主要技术是采用 InfiniBand。

如果本地域名服务器无缓存，当采用递归法解析另一个网络的某主机域名时，用户主机、本地域名服务器发送的域名请求消息分别为（66）。

(66)A.一条，一条　　B.一条，多条　　C.多条，一条　　D.多条，多条

【答案】A

【解析】本题考查域名解析中递归法解析的基础知识。

递归查询是最常见的查询方式，域名服务器将代替提出请求的客户机(下级 DNS 服务器)进行域名查询，若域名服务器不能直接回答，则域名服务器会在域名树中的各分支的上下进行递归查询，最终将查询结果返回给客户机。在域名服务器查询期间，客户机将完全处于等待状态。

如果本地域名服务器无缓存，当采用递归法解析另一个网络的某主机域名时，用户主机发送的域名请求消息数为一条，这时本地域名服务器发送的域名请求消息数也为一条。

由于 OSI 各层功能具有相对性，在网络故障检测时按层排查故障可以有效发现和隔离故障，通常逐层分析和排查的策略在具体实施时（67）。

(67)A.从低层开始　　B.从高层开始　　C.从中间开始　　D.根据具体情况选择

【答案】D

【解析】本题考查网络故障检测的基础知识。

在网络故障检测时按 OSI 模型的各层排查故障可以有效发现和隔离故障，通常逐层分析和排查的策略在具体实施时要根据具体情况来判断。因为通常故障的表现可以让我们选择具体的故障到底是在物理层、数据链路层或者网络层等，这样就可以省时省力快速判断并解决问题。

在网络故障检测中，将多个子网断开后分别作为独立的网络进行测试，属于（68）检查。

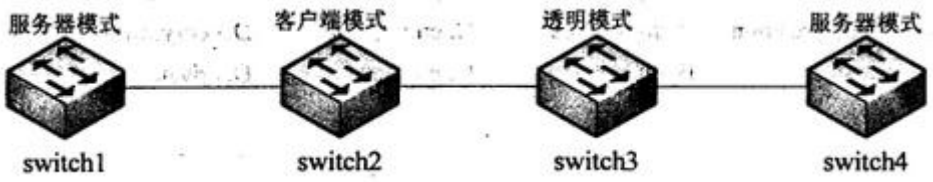
(68)A.整体　　B.分层　　C.分段　　D.隔离

【答案】C

【解析】本题考查网络故障检测的基础知识。

将多个子网断开后分别作为独立的网络进行测试，属于分段检查。既然断开就不可能是整体检查，而在断开子网的时候并没有分层或者按照 OSI 的参考模型来检测，另外断开子网并不是隔离网络。

某网络拓扑如下图所示，四个交换机通过中继链路互连，且被配置为使用 VTP，向 switch1 添加一个新的 VLAN，（69）的操作不会发生。



(69)A.switch1 将 1 个 VTP 更新发送给 switch2

B.switch2 将该 VLAN 添加到数据库，并将更新发送给 switch3

C.switch3 将该 VTP 更新发送给 switch4

D.switch3 将该 VLAN 添加到数据库

【答案】D

【解析】本题考查 VTP 的基础知识。

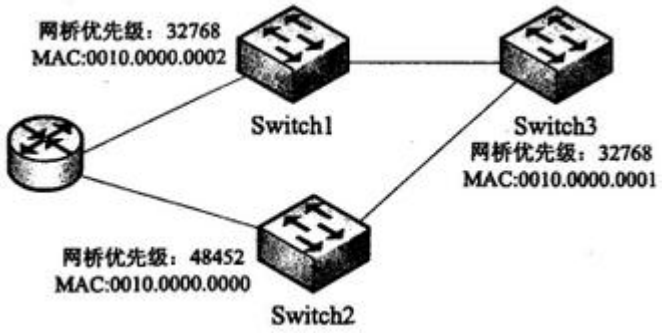
VTP(VLAN Trunking Protocol)：是 VLAN 中继协议，也被称为虚拟局域网干道协议。它是思科私有协议。作用是十几台交换机在企业网中，配置 VLAN 工作量大，可以使用 VTP 协议，把一台交换机配置成 VTP Server，其余交换机配置成 VTP Client，这样它们可以自动

学习到 Server 上的 VLAN 信息。

VTP 有 3 种工作模式：VTP Server、VTP Client 和 VTP Transparent。新交换机出厂时的默认配置是预配置为 VLAN1，VTP 模式为服务器。一般，一个 VTP 域内的整个网络只设一个 VTP Server。VTP Server 维护该 VTP 域中所有 VLAN 信息列表，VTPServer 可以建立、删除或修改 VLAN，发送并转发相关的通告信息，同步 VLAN 配置，会把配置保存在 NVRAM 中。VTPClient 虽然也维护所有 VLAN 信息列表，但其 VLAN 的配置信息是从 VTPServer 学到的，VTP Client 不能建立、删除或修改 VLAN，但可以转发通告，同步 VLAN 配置，不保存配置到 NVRAM 中。VTP Traisparent 相当于是一项独立的交换机，它不参与 VTP 工作，不从 VTPServer 学习 VLAN 的配置信息，而只拥有本设备上自己维护的 VLAN 信息。VTP Transparent 可以建立、删除和修改本机上的 VLAN 信息，同时会转发通告并把配置保存到 NVRAM 中。

从图中可以看出，switch3 处于透明模式下，那么它将不会把自己的 VLAN 数据库与收到的通告同步，因此不会发生 switch3 将该 VLAN 添加到数据库的处理。

如下图，生成树根网桥选举的结果是（70）。



(70)A.switch1 将成为根网桥　　B.switch2 将成为根网桥

C.switch3 将成为根网桥　　D.switch1 和 switch2 将成为根网桥

【答案】C

【解析】本题考查生成树根网桥的选举过程。

网桥 ID 是生成树算法所使用的第一个参数。STP 使用网桥 ID 来决定根网桥或者根交换机。网桥 ID 参数是 1 个 8 字节域，由一对有序数字组成。最开始的 2 字节的十进制数称为网桥优先级，接下来是 6 字节(十六进制)的 MAC 地址。网桥优先级是一个十进制数，用来在生成树算法中衡量一个网桥的优先度。其值的范围是 0-65535，默认设置为 32768。网桥 ID 中的 MAC 地址是交换机的 MAC 地址，每个交换机都有一个 MAC 地址池，每个 STP 实例使用一个作为 VLAN 生成树的实例的网桥 ID。

比较两个网桥 ID 的原则是：

①首先比较网桥优先级，网桥优先级小的网桥 ID 优先；

②如果两个网桥优先级相同，再比较 MAC 的地址，MAC 地址小的网桥 ID 优先。

根据上述原则，在上图中 Switch3 的网桥 ID 最小，则其优先为根网桥。

Symmetric, or private-key, encryption is based on a secret key that is shared by both communcating parties. The （71） party uses the secret key as part of the mathematical operation to encrypt （72） text to cipher text. The receiving party uses the same secret key to decrypt the cipher text to plain text. Asymmetric, or public-key, encryption uses two different keys for each user: one is a （73） key known only to this one user; the other is a corresponding public key, which is accessible to anyone. The private and public keys are mathematically related by the encryption algorithm. One key is used for encyption and the other for decryption, depending on the nature of the communication service being implemented. In addition, public key encryption technoligies allow digital （74） to be placed on messages. A digital signature uses the sender's private key to encrypt some portion of the message. When the message is received, the receiver uses the sender's （75） key to decipher the digital signature to verify the sender's identity.

(71)A.host B.terminal C.sending D.receiving

(72)A.plain B.cipher C.public D.private

(73)A.plain B.cipher C.public D.private

(74)A.interpretation B.signatures

C.encryption D.decryption

(75)A.plain B.cipher C.public D.private

【答案】C A D B C

【解析】

对称加密或私钥加密的基础是通信双方共享同一密钥。发送方使用一个密钥作为数学运算的一部分把明文加密成密文。接收方使用同一密钥把密文解密变成明文。在非对称或公钥加密方法中，每个用户使用两种不同的密钥：一个是只有这个用户知道的私钥;另一个是与其对应的任何人都知道的公钥。根据加密算法，私钥和公钥是数学上相关的。一个密钥用于

加密，而另一个用于解密，依赖于实现的通信服务的特点而用法有所不同。此外，公钥加密技术也可以用于报文的数字签名。数字签名时使用发送方的私钥来加密一部分报文。当接收方收到报文时，就用发送方的公钥来解密数字签名，以便对发送方的标识进行验证。

试题一

【说明】

某企业网络拓扑如图 1-1 所示。

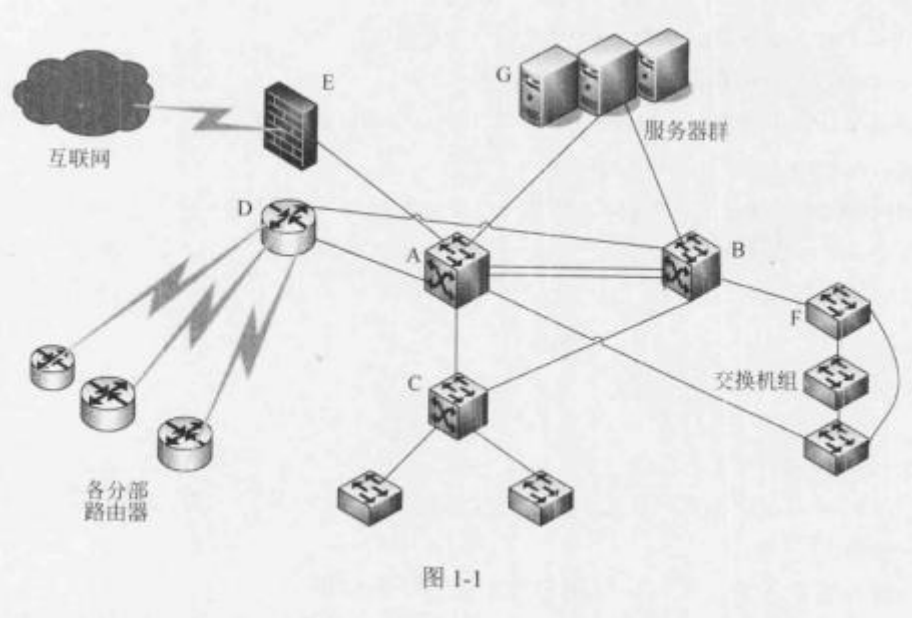


图 1-1

【问题 1】

根据图 1-1，对该网络主要设备清单表 1-1 所示内容补充完整。

表 1-1

设备名	在网络中的编号	产品描述
Cisc06509	A,B	核心主、备交换机
Cisc04506	(1)	(2)
Ws-c3550-48	交换机组 F	接入层交换机
Cisc03745	(3)	(4)
Netscreen-500	(5)	(6)

(1) C

(2) 汇聚交换机

(3) D

(4) 核心路由器

(5) E

(6) 边界防火墙

本题考查接入网技术和网络规划及配置的相关知识。

此类题目要求考生认真阅读题目或给出的网络拓扑图，对网络拓扑中采用组网技术进行分析说明。

要求对组网设备的性能和功能分析，结合网络拓扑图和设备列表补充完善表格中的空白处。网络拓扑中没有在设备列表中标注的有 C、D、E、G 等设备。看图例可知 D、E 分别是路由器和防火墙，C 是介于 A、B 和 F 的交换机设备。根据 D、E、C 设备在网络中承担的任务，参照表中的产品描述，C 为汇聚交换机、D 为核心路由器、E 为核心路由器。

【问题 2】

1．网络中 A.B 设备连接的方式是什么？依据 A.B 设备性能及双链路连接，计算两者之间的最大宽带。

2．交换机组 F 的连接方式是什么？采用这种连接方式的好处是什么？

1.链路聚合或捆绑 2G(或答 20G 也正确)

2.堆叠扩大接入规模，简化网络管理

网络中 A、B 设备连接的方式是链路聚合或捆绑。链路聚合是将两个或更多数据信道结合成一个单个的信道，该信道以一个单个的更高带宽的逻辑链路出现。链路聚合一般用来连接一个或多个带宽需求大的设备，例如连接骨干网络的服务器或服务器群。A、B 设备可以配置千兆或者万兆的接口，在双链路聚合的前提下，最大带宽是 2G 或 20G。

交换机组 F 的连接方式是堆叠，堆叠需要专用的堆叠模块和堆叠线缆。堆叠可以扩大网络接入规模，对所有的交换机进行统一配置和管理，达到提高交换机背板容量，实现所有交换机高速连接的目的。

【问题 3】

该网络拓扑中连接到各分部可采用租赁 ISP 的 DDN、Frame Relay、ISDN 线路等方式，请简要介绍这几种连接方式。

DDN 是利用数字信道提供永久性连接电路，用来传输数据信号的数字传输网络。帧中继是一种数据包交换技术，可以动态共享网络介质和可用带宽。

ISDN 是一个数字电话网络标准，是一种典型的电路交换网终系统。

DDN 专线接入向用户提供的是永久性的数字连接，沿途不进行复杂的软件处理，因此延时较短，避免了传统的分组网中传输协议复杂、传输时延长且不固定的缺点；DDN 专线接入采用交叉连接装置，可根据用户需要，在约定的时间内接通所需带宽的线路，信道容量的分配和接续均在计算机控制下进行，具有极大的灵活性和可靠性，使用户可以开通各种信息业务，传输任何合适的信息。

帧中继是一种局域网互联的 WAN 协议，它工作在 OSI 参考模型的物理层和数据链路层。

它为跨越多个交换机和路由器的用户设备间的信息传输提供了快速和有效的方法。帧中继是一种数据包交换技术，与 X.25 类似。它可以使终端站动态共享网络介质和可用宽带。

ISDN 综合业务数字网(Integrated Services Digital Network)是一个数字电话网络国际标准，是一种典型的电路交换网络系统。在 ITU 的建议中，ISDN 是一种在数字电话网 IDN 的基础上发展起来的通信网络，ISDN 能够支持多种业务，包括电话业务和非电话业务。

【问题 4】

若考虑到成本问题，对其中一条连接用 VPN 的方式，在分部路由器上做下列配置：

```
sub-company(config)#crypto isakmp policy 1
sub-company(config-isakmp)#encry des
sub-company(config-isakmp)#hash md5
sub-company(config-isakmp)#authentication pre-share
sub-company(config)# crypto isakmp key 6 cisco address x.x.x.x
```

该命令片段配置的是(7)。

(7)备选答案：

A、定义 ESP

B、IKE 策略

C、IPSce VPN 数据

D、路由映射

在该配置中，IP 地址 x.x.x.x 是该企业总部 IP 地址还是分布 IP 地址？

(7)B

总部 IP 地址

采用 VPN 连接,网络对等端需要建立信任关系,必须交换某种形式的认证密钥。Internet 密钥交换(Internet Key Exchange,IKE)是一种为 IPSec 管理和交换密钥的标准方法。该过程一般包括定义策略、定义加密算法、定义散列算法、定义认证方式等步骤。

在分部路由器上配置 IKE 策略，x.x.x.x 是对端地址。

试题二

【说明】

传统业务结构下，由于多种技术之间的孤立性，使得数据中心服务器总是提供多个对外I/O接口。在云计算模式发展的推动下，数据中心正在从过去的存储处理中心演变成为应用中心，并逐步向服务中心和运营中心转变。而对客户来说，由于技术、经验、资金等限制，在转变过程中会遇到各种挑战，例如：虚拟化带来的技术复杂性，规模扩大带来的运维压力，系统和数据迁移的困难以及数据中心的高能耗等。

传统业务结构存储下的数据中心网络扑结构图如图2-1所示。

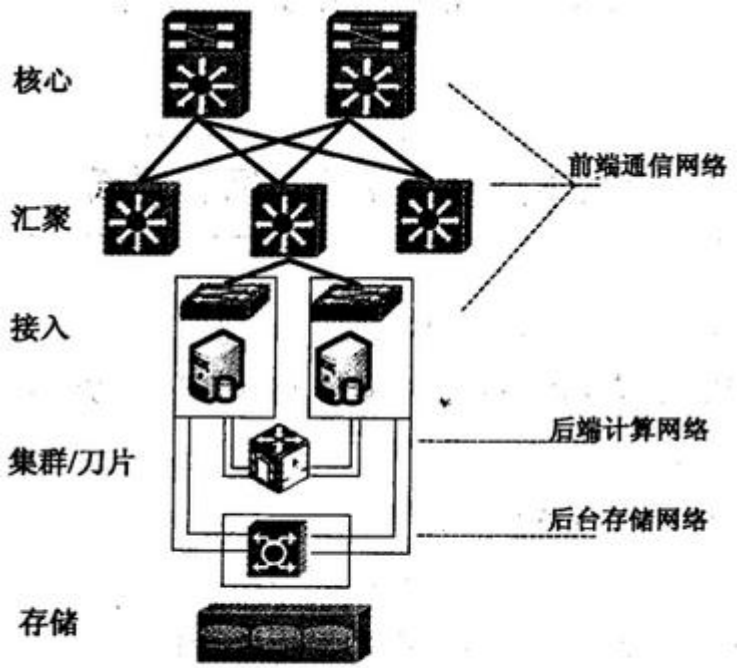


图2-1

【问题1】

(1)如图2-1所示，数据中心有多个网络，一个是前端用户通信网络，一个是后端做数据更新或者做集群计算的通讯网络，还有后台光纤存储网络。针对这三种网络分别举出一个例子。

(2)如上所述，除以上三种网络外有的数据中心还有专门用于虚拟机迁移的网络，都会在服务器上做集中。这样一台服务器最多需要几块网卡与之相连？随着TRILL等技术的出现，这个专用网络还需要吗？

(3)网络成为数据中心资源的交换枢纽，当前数据中心纷为IP数据网络、存储网络、服务器集群网络。随着数据中心规模的逐步增大，简单分析带来的问题。

(1)前端：以太网

后端：高性能计算 Infmiband 网络

后台：FC 光纤

(2)8 个网卡

不需要

(3)每个服务器要多个专用适配器(网卡)以及不同的布线系统；

机房要支持更多设备；

管理的复杂性增加；

部署/配置/运维困难。

成本增加(人员，能耗，运维成本等)

本题考查云计算模式下的数据中心的相关知识及应用。

本问题主要考查传统数据中心的问题及 I/O 融合趋势。

传统业务结构下，由于多种技术之间的孤立性(LAN 与 SAN)，使得数据中心服务器总是提供多个对外 I/O 接口(在此，可理解成服务器的网卡)，即用于数据计算与交互的 LAN 接口以及数据访问的存储接口，某些特殊环境如特定 HPC(高性能计算)环境下的超低时延接口。服务器的多个 I/O 接口导致了数据中心环境下多个独立运行的网络同时存在，不仅使得数据中心布线复杂，不同的网络、接口形体造成的异构还直接增加了额外人员的运行维护、培训管理等高昂成本投入，特别是存储网络的低兼容性特点，使得数据中心的业务扩展往往存在约束。

数据中心里会有两个网络，一个是前端 IP 网络，后端可能会是光纤网络，都会在服务器上做。因此，集中服务器上以太网卡、光纤网卡，跟外部数据交互时通过 IP 网络进行交互。如果说得更极端一点，在大型窣据中心会存在：一是前端的用户通信网络(以太网)；二是后台存储网络光纤的通道(FC 光纤网络)；三是后端做数据更新或者做集群计算的通信网络(高性能计算 Infmiband 网络)；四是专门用于虚拟机迁移的网络(各个服务器上有一个普通的以太网网卡，连接到独立的交换机组成的网络上，专门做虚拟机迁移。随着 TRILL 等技术的出现，这个专用的网络不再需要)。在这种情况下最多会有八个网卡，这些都是现有的设计视为理所当然的。

网络渐渐成为数据中心资源的交换枢纽。当前数据中心分为 IP 数据网络、存储网络、

服务器集群网络。但随着数据中心规模的逐步增大，也带来以下问题：每个服务器要多个专用适配器(网卡)，要有不同的布线系统；机房要支持更多设备：空间、耗电、制冷;多套网络无法统一管理，不同的维护人员；部署/配置/管理/运维困难。

【问题 2】

FCoE 采用增强型以太网作为物理网络传输架构，是专门为低延迟性、高性能、二层数据中心网络所设计的网络协议。目前国际标准化组织已经开发了针对以太网标准的扩展协议族，即“融合型增强以太网(CEE)”，这些扩展协议族可以进行所有类型的传输。试简述 FCoE 技术的优点。

光纤存储和以太网共享同一个端口；
更少的线缆和适配器；
软件配置 I/O;
与现有的 SAN 环境可以互操作。

FCoE 采用增强型以太网作为物理网络传输架构，能够提供标准的光纤通道有效内容载荷，避免了 TCP/IP 协议开销，而且 FCoE 能够像标准的光纤通道那样为上层软件层 (包括操作系统、应用程序和管理工具)服务。

FCoE 可以提供多种光纤通道服务，比如发现、全局名称命名、分区等，而且这些服务都可以像标准的光纤通道那样运作。不过，由于 FCoE 不使用 TCP/IP 协议，因此 FCoE 数据传输不能使用 IP 网络。FCoE 是专门为低延迟性、高性能、二层数据中心网络所设计的网络协议。

和标准的光纤通道 FC 一样，FCoE 协议也要求底层的物理传输是无损失的。因此，国际标准化组织已经开发了针对以太网标准的扩展协议族，尤其是针对无损 10Gb 以太网的速度和数据中心架构。这些扩展协议族可以进行所有类型的传输。这些针对以太网标准的扩展协议族被国际标准组织称为“融合型增强以太网(CEE)”(思科称为“数据中心以太网(DCE)”)。数据中心 FCoE(FC over Ethernet)技术实现在以太网架构上映射 FC(Fibre Channel)中贞，使得 FC 运行在一个无损的数据中心以太网络上(需要无损的以太网(CEE/DCE/DCB)保证不丢包)。FCoE 技术有以下的一些优点：光纤存储和以太网共享同一个端口；更少的线缆和适配器；软件配置 I/O;与现有的 SAN 环境可以互操作。

基于 FCoE 技术的数据中心统一 I/O 能够实现用少数的 C:NA(Converged NetworkAdapter)代替数量较多的 NIC、HBA、HCA,所有的流量通过 CNA 万兆以太网传输。

使用 FCoE 后的好处：每个服务器只需要一个专用适配器(网卡)，一套布线(以太网)系统(以前需要多个网卡，多套布线(以太网和光纤)系统)；机房不再要支持更多设备：空间、耗电、制冷，更加节能绿色；只有一套网络，统一管理维护简单(原来是多套网络无法统一管理，不同的维护人员维护困难)；部署/配置/管理/运维简单。

【问题 3】

为了实现统一管理、简化运维，采用基于 FCoE 技术的数据中心统一 I/O 能够实现用少数的 CNA(Converged Network adapter)代替数量较多的 NIC.HBA.HCA，所有的流量通过 CNA 万兆以太网传输。

按照 18 台服务器（单网卡）为例，使用 FCoE 后每台服务器只需要一块专用适配器（网卡），一套布线（以太网）系统，统一管理维护简单。表 2-1 为使用 FcoE 前 18 台服务器需要的网卡、交换机、电缆以及上联端口的数量；请核算出使用 FCoE 后的相应部件数量，填充表 2-2。

表 2-1 使用 FCoE 前

18 台服务器	Ethernet	FC	合计
网卡	18	18	36
交换机	2	2	4
电缆	36	36	72
上联端口	2	4	6

表 2-2 使用 FCoE 后

18 台服务器	CEE	Ethernet	FC	合计
网卡	18	(1)	(5)	(9)
交换机	2	(2)	(6)	(10)
电缆	36	(3)	(7)	(11)
上联端口	2	(4)	(8)	(12)

(1) 0 (2) 0 (3) 0 (4) 0 (5) 0 (6) 0

(7) 0 (8) 4 (9) 18 (10) 2 (11) 36 (12) 6

使用前(按照 18 台服务器为例，如下表)

表 2-1 使用 FCoE 前

18 台服务器	Ethernet	FC	合计
网卡	18	18	36
交换机	2	2	4
电缆	36	36	72
上联端口	2	4	6

1. 72 根光纤、36 个网卡(36 根以太网光纤、36 个以太网网卡，18 根 FC 光纤、18 个 FC 光纤网卡)

2. 4 台交换机(2 台以太网交换机，2 台 FC 光纤交换机)

3. 上联端口(6 个，以太网交换机要 2 个，光纤交换机需要 4 个)

使用后(按照 18 台服务器为例，如下表)

表 2-2 使用 FCoE 后

18 台服务器	CEE	Ethernet	FC	合计
网卡	18	0	0	18
交换机	2	0	0	2
电缆	36	0	0	36
上联端口	2	0	4	6

1. 36 根光纤、18 个网卡(36 根光纤、18 个 CNA 网卡)

2. 2 台交换机(2 台 FCoE 交换机)

3. 上联端口(6 个，以太网交换机要 2 个，光纤交换机需要 4 个)

【问题 4】

(1)随着数据中心的发展，数据中心的能耗已经成为一个严峻的问题，PUE 已经成为国际上比较通行的数据中心电力使用效率的衡量指标。请问 PUE 是什么，它的基准是多少，其越接近多少表示一个数据中心的绿色化程度越高？

(2)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。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。正确的摆放方式是什么？请简述其原因。

(3)水冷空调系统是目前新一代大型数据中心制冷的首选方案，采用水冷空调在部分地区可以采取免费冷却技术以节能。免费冷却技术是什么？

(1) PUE=数据中心总设备能耗/IT 设备能耗，基准是 2,越接近 1 表明能效水平越好。

(2) 将服务器机柜面对面或背对背的方式摆放。

因为这样将会形成“冷”通道和“热”通道，提高制冷效果。

(3) 免费冷却(Free Cooling)技术指全部或部分使用自然界的免费冷源进行制冷从而减少压缩机或冷冻机消耗的能量。

本问题主要考查数据中心能耗的相关知识。

随着能源成本上升，我们越来越关注 IT 对环境的影响，技术管理人员现在面临着双重任务：创造和保持高可用性的 IT 环境，并推行绿色倡议。用于数据中心保证设备运行的能源消耗需求惊人。

(1) PUE 是 Power Usage Effectiveness 的简写，是评价数据中心能源效率的指标，是数据中心消耗的所有能源与 IT 负载使用的能源之比，是 DCIE(Data Center Infrastructure Efficiency)的反比。PUE=数据中心总设备能耗/IT 设备能耗，PUE 是一个比值，基准是 2，越接近 1 表明能效水平越好。PUE(Power Usage Effectiveness,电源使用效率)值已经成为国际上比较通行的数据中心电力使用效率的衡量指标。PUE 值是指数据中心消耗的所有能源与 IT 负载消耗的能源之比。PUE 值越接近于 1，表示一个数据中心的绿色化程度越高。

(2) 以往在机柜的布局中，人们为了美观和便于观察，常常会将所有的机柜朝同一个方向摆放。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。正确的摆放方式应该是将服务器机柜面对面或背对背的摆放方式摆放，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，有效提高制冷效果，保护好冷热通道不被破坏。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。

(3) 水冷式空调的发明源于生活的细节，夏季人站在海边感觉特别凉爽，这是因为海水吸收空气中的热量而蒸发，使空气温度下降，从而带给我们凉爽的冷空气。细心的人们发现了这一现象，并将这一现象巧妙地运用到温度调节中来，进而发明了节能环保的水冷空调。水冷空调又叫环保空调，是一种利用自来水的温度，来达到冷却室内温度的空调机。

水冷空调系统是目前新一代大型数据中心制冷的首选方案,采用水冷空调在部分地区可以采取免费冷却技术以节能。免费冷却技术指全部或部分使用自然界的免费冷源进行制冷从而减少压缩机或冷冻机消耗的能量。目前常用的免费冷源主要是冬季或者春秋季的室外空气，因此，如果可能的话，数据中心的选址应该在天气比较寒冷或低温时间比较长的地区。在中国，北方地区都是非常适合采用免费制冷技术。

试题三

【说明】

某学校拥有内部数据库服务器 1 台，邮件服务器 1 台，DHCP 服务器 1 台，FTP 服务器 1 台，流媒体服务器 1 台，Web 服务器 1 台，要求为所有的学生宿舍提供有限网络接入服务，要求为所有的学生宿舍提供有线网络接入服务，对外提供 Web 服务，邮件服务，流媒体服务，内部主机和其他服务期对外不可见。

【问题 1】

请划分防火墙的安全区域，说明每个区域的安全级别，指出各台服务器所处的安全区域。

整个网络分为 3 个不同级别的安全区域：

1. 内部网络：安全级别最高，是可信的、重点保护的区域。包括所有内部主机，数据库服务器、DHCP 服务器和 FTP 服务器。

2. 外部网络：安全级别最低，是不可信的、要防备的区域。包括外部因特网用户主机和设备。

3. DMZ 区域(非军事化区)：安全级别中等，因为需要对外开放某些特定的服务和应用，受一定的保护，是安全级别较低的区域。包括对外提供 WWW 访问的 Web 服务器、邮件服务器和流媒体服务器。

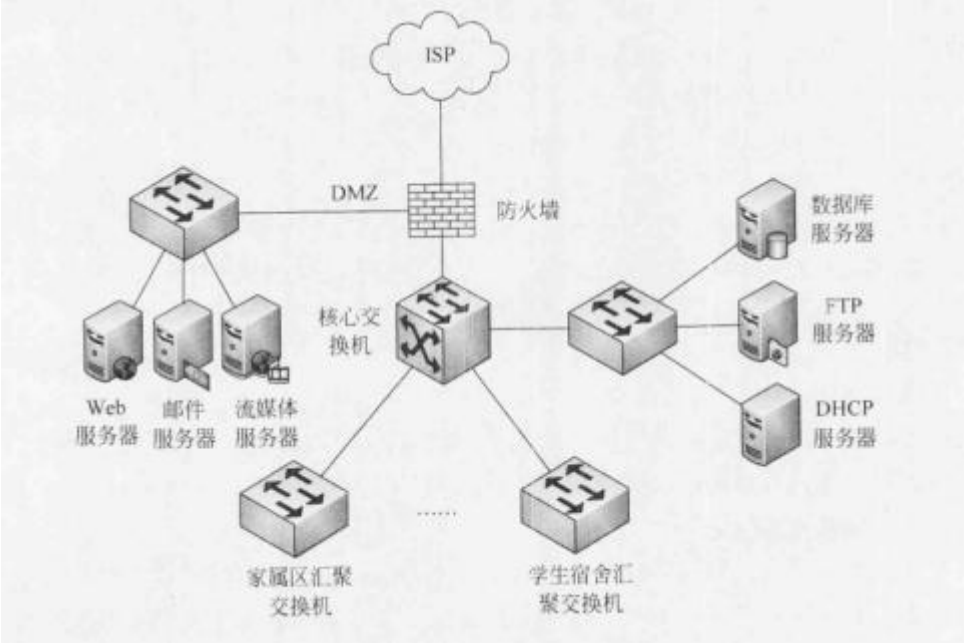
本题考查局域网安全部署的基本知识及应用。

根据题目中关于该学校所拥有的服务器类型和服务器数量、基本要求以及服务器对用户的访问权限等说明，考虑到防火墙的 3 种区域划分，可将网络分为内部网络、外部网络和 DMZ 区 3 个区域，这 3 个区域中，内部网络的安全要求级别最高，DMZ 区次之，外部网络的安全要求级别最高。

【问题 2】

请按照你的思路为该校进行服务器和防火墙部署设计，对该校网络进行规划，画出网络拓扑结构图。

拓扑结构图如下：



注：1.DMZ 区服务器群，内网服务器群放置位置，防火墙位置，网络层次结构，学生宿舍汇聚接入。

2.合理的服务器放置和防火墙配置也正确，比如出口防火墙采用端口映射来区别是否为外网提供服务。

根据问题 1 对该学校网络区域的划分，将不同的服务器放置在相应的区域即可，对于具体的网络连接细节则不必过多地考虑，在防火墙的 DMZ 区中，由于需要连接多台服务器，应使用一台局域网交换机进行连接。

【问题 3】

学校在原有校园网络基础上进行了扩建，采用 DHCP。服务器动态分配 IP 地址，运行一段时间后，网络时常出现连接不稳定、用户所使用的 IP 地址被“莫名其妙”修改、无法访问校园网的现象。经检测发现网络中出现多个未授权 DHCP 地址。

请分析上述现象及遭受攻击的原理，该如何防范？

攻击原理：

(1) 当 DHCP 客户端第一次连接网络、重新连接或者地址租期已满时，会以广播的方式向 DHCP 服务器发送 DHCP Discover 消息，以获取/重新获取 IP 地址；

(2) 若网络中存在多台 DHCP 服务器，均能收到该消息并应答；

(3) 非授权 DHCP 服务器会先于授权 DHCP 服务器发出应答；

(4) 客户端使用非授权服务器发出的应答包，并用作自己的 IP 地址；

(5) 客户端地址被修改，无法访问校园网。

防范措施：

(1) 启用接入层交换机的 DHCP Snooping 功能；

(2) DHCPS nooping 功能将交换机接口分为信任接口和非信任接口；

(3) 连接客户端的接口为非信任接口，上连到汇聚交换机的接口为信任接口；

(4) 非信任接口上接收到 DHCP Offer、DHCP ACK、DHCPNCK 报文时，交换机会将其丢弃；

(5) DHCPS nooping 功能可阻止连接在非信任接口上的非授权 DHCP 服务器为客户端提供 IP 地址配置信息。

当采用 DHCP 服务器为客户端动态分配 IP 地址时，出现网络连接不稳定、用户的地址会被“莫名其妙”修改，导致无法访问校园网的现象，经查是出现了多个未授权的 DHCP 服务器所致。这些所谓“未授权”的服务器为客户机分配了其他的非法 IP 地址，导致用户无法访问网络。这类攻击为 DHCP 攻击，DHCP 攻击的原理是距离客户端较近的 DHCP 服务器会先于授权 DHCP 服务器相应客户端的请求，而导致客户端接收到非法 IP 地址，无法访问网络。防范的方法一般是在接入层交换机上启用 DHCP Snooping 功能，以过滤非信任接口上收到的 DHCP offer、DHCP ACK 和 DHCPNCK 报文，从而防止非法的 DHCP 服务器为客户端分配 IP 地址。

【问题 4】

学生宿舍区经常使用的服务有 Web、即时通信、邮件、FTP 等，同时也因视频流寻致大量的 P2P 流量，为了保障该区域中各项服务均能正常使用，应采用何种设备合理分配每种应用的带宽？该设备部署在学校网络中的什么位置？一般采用何种方式接入网络？

应采用流量控制设备，部署在核心交换机与学生宿舍区汇聚交换机之间，采用串接方式接入网络。

根据问题的描述，由于网络中存在大量的 P2P 流量，而导致其他各项服务正常工作，应对 P2P 流量进行控制。要实现该功能，一般所选用的设备为流控设备，流控设备一般部署在

被控流量区域的主干区域，应采用串接方式接入网络。

【问题 5】

当前防火墙中，大多都集成了 IPS 服务，提供防火墙与 IPS 的联动。区别于 IDS，IPS 主要增加了什么功能？通常采用何种方式接入网络？

区别于 IDS，IPS 提供主动防护，增加了深入检测和分析功能，提供高效处理(拦截或阻断)能力。采用串接方式接入网络。

随着网络攻击技术的发展，对安全技术提出了新的挑战。防火墙技术和 IDS 自身具有的缺陷阻止了它们进一步的发展。防火墙不能阻止内部网络的攻击，对于网络上流行的各种病毒也没有很好的防御措施；IDS 只能检测入侵而不能实时地阻止攻击，而且 roS 具有较高的漏报和误报率。

在这种情况下入侵防御系统(Intrusion Prevention System，IPS)成了新一代的网络安全技术。IPS 提供主动、实时的防护，其设计旨在对网络流量中的恶意数据包进行检测，对攻击性的流量进行自动拦截，使它们无法造成损失。IPS 如果检测到攻击企图，就会自动地将攻击包丢掉或采取措施阻断攻击源，而不把攻击流量放进内部网络。

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。串接式工作保证所有网络数据都经过 IPS 设备，IPS 检测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。由于是在线操作，因而能保证处理方法适当而且可预知。

IPS 系统根据部署方式可以分为 3 类：基于主机的入侵防护(HIPS)、基于网络的入侵防护(N1PS)、应用入侵防护(AIP)。

试题一 局域网络中信息安全方案设计及攻击防范技术

信息化的发展与信息安全保障是密切相关的，两者相辅相成、密不可分。信息安全在国家安全中占有极其重要的战略地位，已经成为国家安全的基石和核心，并迅速渗透到国家的政治、经济、文化、军事安全中去，成为影响政治安全的重要因素。

请以“局域网络中信息安全方案设计及攻击防范技术“为题，依次对以下四个方面进行论述：

1．简要论述你参与建设的局域网络环境及建立在网络之上的业务。

2．详细论述局域网络中信息安全涉及到的主要问题及相应防范技术。

3．详细论述你参与设计和实施的网络项目中采用的安全方案。

4．分析所采用方案遵循的原则，评估安全防范方案的效果以及进一步改进的措施。

写作要点：

1. 简要论述安全方案遵循标准及分级。
2. 简要介绍局域网络环境拓扑结构，分层模型。
3. 简要介绍公司网络业务，安全需求分析。
4. 详细论述局域网络层次架构中各层遇到的安全问题及如何设计防范措施。
5. 详细论述你采用的安全方案。
6. 对安全方案进行评估。
7. 介绍实际运行过程中安全防范方案出现的问题，如何解决方案上有何改进措施。

试题二 智能小区 WIFI 覆盖解决方案

WIFI 使用无线传输介质，是实现移动计算机网络的关键技术之一。智能小区规划与设计常用的无线接入解决方案，是对有线网络接入方式的一种补充。目前，WIFI 网络已经成为人们日常生活中不可或缺的组成部分。

请以“智能小区覆益解决方案”为题，依次对以下四个方面进行论述：

1．概述 WLAN 的通信技术、体系结构、工业标准、以及安全措施。

2．简要阐述你参与建设的智能小区无线网络的需求分析。

3．根据需求详细论述你参与设计和实施的无线网络组网方案，包括中心机房、有线骨干网、有线 / 无线中间层、节点交换机，无线接入点的分布，网络拓扑结构图和无线覆盖效果图，用户认证、访问控制和计费管理，AP 的控制和管理等。

4．分析你在网络建设和管理过程中遇到的问题，评估安全防范方案的效果以及进一步改进的措施。

写作要点：

1. 概述 WLAN 的通信技术、体系结构、工业标准，以及安全措施。

2. 园区无线网络建设的需求分析。

3. 根据需求导出的组网方案：

•中心机房；

•有线骨干网、有线/无线中间层、节点交换机；

•无线接入点的分布(频率规划，覆盖方式，室内/外设备的选型、安装和供电)；

•网络拓扑结构图和无线覆盖效果图；

•用户认证、访问控制和计费管理(802.1x、PPPoE 和 Web 认证，AAA 和 Radius)；

•AP 的控制和管理。

4. 网络建设和管理过程中问题：

•流量监测及报警；

•安全管理和防雷电措施；

•漫游切换；

•可扩展性。