全国计算机技术与软件专业技术资格（水平）考试参考用书

网络工程师考试同步辅导
(下午科目)(第3版)

全国计算机专业技术资格考试办公室推荐

徐军　赵鹏　陈志荣　主编

清华大学出版社

全国计算机技术与软件专业技术资格（水

网络工程师考试同步辅导
(下午科目)(第3版)

全国计算机专业技术资格考试办公室推荐
徐军 赵鹏 陈志荣 主编

清华大学出版社
北京

内 容 简 介

本书是按照国家人力资源和社会保障部、工业和信息化部最新颁布的全国计算机技术与软件专业技术资格(水平)考试大纲和指定教材编写的考试辅导书。全书共分为6章，主要包括网络系统规划和设计、交换机配置与VLAN、路由器与网络互联、Windows应用服务器的配置、Linux应用服务器的配置、网络安全等内容，主要从考试大纲要求、考点辅导、典型例题分析和同步练习几个方面对各部分内容进行系统的阐释。

本书具有考点分析透彻、例题典型、习题丰富等特点，非常适合备考网络工程师的考生使用，也可作为高等院校或培训班的教材。

图书在版编目(CIP)数据

网络工程师考试同步辅导(下午科目)/徐军，赵鹏，陈志荣主编. --3版. --北京：清华大学出版社，2013
(全国计算机技术与软件专业技术资格(水平)考试参考用书)
ISBN 978-7-302-33257-2

Ⅰ. ①网… Ⅱ. ①徐… ②赵… ③陈… Ⅲ. ①计算机网络—工程技术人员—资格考试—自学参考资料 Ⅳ. ①TP393

中国版本图书馆CIP数据核字(2013)第165725号

责任编辑：章忆文
封面设计：何凤霞
责任校对：周剑云
责任印制：何　芊

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn,010-62791865

印 刷 者：北京密云胶印厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185mm×260mm　**印　张**：21.75　**插　页**：1　**字　数**：525千字
版　　次：2005年6月第1版　2013年8月第3版　**印　次**：2013年8月第1次印刷
印　　数：1～4000
定　　价：45.00元

产品编号：053029-01

前　言

全国计算机技术与软件专业技术资格(水平)考试自实施起至今已经历了二十多年，在社会上产生了很大的影响，其权威性得到社会各界的广泛认可。为了适应我国信息化发展的需求，国家人力资源和社会保障部同工业和信息化部在2009年对网络工程师级别考试大纲进行了重新调整，以满足社会上对各种信息技术人才的需求。本书第1版自2005年出版以来，被众多考生选用为考试参考书，多次重印，深受广大读者好评。为了帮助考生复习迎考，根据2009年考试大纲的最新变化及网络新技术的发展，本书第2版对第1版同名书进行了修订。本书依据最新教程进行修认，并将2013年最新考试真题贯穿其中。修订后本书的特色如下。

(1) 知识点全面。2009年新大纲对知识点有所调整与变动，使其更注重实践性。本书与2009年网络工程师考试大纲考试科目2——网络系统设计与管理基本一致，又兼顾网络技术发展和知识更新，对属于大纲要求的知识点但指定教材没有阐述的部分进行了必要的补充。

(2) 结构与官方教程同步。本书参考最新指定官方教程、最新考试大纲及最新题型编写章名、节名，便于考生使用《网络工程师教程(第3版)(修订版)》进行同步复习，同时更加突出重点与难点，针对性强，减轻考生复习的工作量。

(3) 例题与习题经典。最近四年(2010—2013年)7次考试真题全部被分类解析到例题中，并在其中增加了根据最新考试大纲精心设计的例题，这些例题均具有典型性和代表性，而2009年及之前的考试真题被分类归入同步练习中，使考生能从以前的考题中更好地了解考试的难度与广度，顺利地通过考试。

(4) 重点突出。第3版沿袭前两版的框架，每一小节分为4个模块：考点辅导、典型例题分析、同步练习和同步练习参考答案。其中，考点辅导部分主要以专题的方式，重点介绍网络工程师下午考试所需的各个方面的知识；典型例题分析是本书的重点，它详尽细致地剖析了所有近四年(2010—2013年)的真题和例题；同步练习中的每一道题都配有标准的答案，对读者所学的知识和能力可起到巩固、拓宽和提高的作用。

(5) 语言更准确，概念更清晰，能覆盖所有大纲考点，并突出重、难点。

(6) 对书中所有例题与习题进行了精选，确保所有题目符合考纲要求。例题选取典型、有梯度、有广度，分析详尽；题目的难易度、分布率与真实考试相当；题目答案正确、解析科学。

本书可作为备考网络工程师的考生的辅导用书，也可作为高等院校相关专业或培训班的教材。

本书由徐军(解放军装甲兵学院)、赵鹏(江苏第二师范学院)、陈志荣(江苏师范大学)主编。此外，参与本书编写的还有王珊珊、周海霞、卢振侠、石雅琴、许娟、史国川、李海、赵明、张凌云、陈海燕、陈智、程勇、郭龙源、何光明、蒋道霞、马常霞、祁云嵩等。在

此对原作品作者及全体参与人员表示衷心的感谢。在本书编写的过程中，参考了许多相关的书籍和资料，从中汲取了许多营养，在此也对这些参考文献的作者表示感谢。需要特别感谢的是来自互联网的各位不知道姓名的网友们的无私奉献，正是由于你们，才使本书的内容更完善、更详尽。

由于时间仓促和作者水平所限，书中难免存在错漏和不妥之处，敬请广大读者批评指正。联系邮箱：iteditor@126.com。

编　者

目　录

第 1 章　网络系统规划和设计

大纲要求：

- 应用需求分析，包括应用需求的调研、网络应用的分析。
- 现有网络系统分析，包括现有网络系统结构调研、现有网络体系结构分析。
- 需求分析，包括功能需求、通信需求、性能需求、可靠性需求、安全需求、维护和运行需求、管理需求。
- 技术和产品的调研和评估，包括收集信息、采用的技术和产品的比较研究、采用的技术和设备的比较要点。
- 网络系统的设计，包括确定协议、确定拓扑结构、确定连接(链路的通信性能)、确定节点(节点的处理能力)、确定网络的性能、确定可靠性措施、确定安全性措施、网络设备的选择、制定选择标准、通信子网的设计、资源子网的设计。
- 新网络业务运营计划。
- 设计评审。
- 安装工作。
- 测试和评估。
- 转换到新网络的工作计划。
- 用户措施，包括用户管理、用户培训、用户协商。
- 制定维护和升级的策略和计划，包括确定策略、设备的编址、审查的时间、升级的时间。
- 维护和升级的实施，包括外部合同要点、内部执行要点。
- 备份与数据恢复，包括数据的存储与处置、备份、数据恢复。
- 网络系统的配置管理，包括设备管理、软件管理、网络配置图。
- 网络系统的监视，包括网络管理协议(SNMP、MIB-2、RMON)、利用工具监视网络性能、利用工具监视网络故障、利用工具监视网络安全(入侵检测系统)、性能监视的检查点、安全监视的检查点。
- 故障恢复分析，包括故障分析要点(LAN 监控程序)、排除故障要点、故障报告的撰写要点。
- 系统性能分析，包括性能要点。
- 危害安全的对策，包括危害安全的情况分析、入侵检测要点、对付计算机病毒的要点。
- 系统评价，包括系统能力的限制、潜在的问题分析、系统评价要点。
- 改进系统的建议，包括系统生命周期、系统经济效益、系统的可扩充性。

1.1 网络系统的需求分析

1.1.1 考点辅导

1.1.1.1 应用需求分析

1. 应用需求的调研

需求分析是构建网络的第一个阶段，通过需求分析，可以帮助网络设计者更好地理解网络功能，更好地评价现有网络，更客观地做出决策；有助于为网络设计者提供更加完善的交互功能和移植功能，使其更合理地使用用户资源等。

应用需求的调研内容包括应用系统性能、信息产生和接收点、数据量和频度、数据类型和数据流向等。

1) 应用系统性能

用户系统中的应用有许多类型，其中一些应用在整个系统中占有相当重要的地位。应用系统的性能往往是用户最为关注的，常见的性能指标包括可靠性/可用率、响应时间、安全性、可实现性和实时性等。

2) 信息产生和接收点

网络上的信息流都有其产生和接收的位置，产生信息的称为源，接收信息的则称为宿(即目的)。在进行需求分析时，分清信息的源和宿是非常必要的。

3) 数据量和频度

网络中的通信类型包括数据、视频信号和音频信号等，不同类型的流量使用不同的量度，数据的流量一般用平均或高峰时每秒传送的位数(比特每秒，简写为 bps)来表示。视频信号的流量用电视通道数来表示，每个通道占 6 MHz 带宽，音频信号的流量则用欧拉数来表示。

频度是指数据在单位时间内传送的次数，不同类型的数据，传送的频度不同。

流量估计应该先分析用户的网络应用，分别估计每种应用产生的分流量，然后再把各种分流量乘以频度，累计得出系统的总流量。

准确的流量估计可以避免网络系统因带宽过窄而形成瓶颈，导致网络吞吐量和性能的下降，因此，对网络通信业务量的估计必须留有足够的余量。

4) 数据类型和数据流向

网络服务一般分为 3 种：共享数据服务、综合语音服务和多媒体应用服务。其中共享数据服务是最常见的业务，综合语音服务主要是电话类业务，而多媒体应用服务则包括语音、图形、图像等多种服务。不同的服务有不同的数据类型。

数据流向是指数据流传输的方向，在客户机/服务器工作模式中，数据的流向既可以是客户机到服务器的，也可以是服务器到客户机的。

因此，网络设计人员必须根据用户具体的应用情况，详细分析网络承载的数据类型和数据流向，合理地分配网络容量。

2. 网络应用的分析

网络的主要功能是通过数据传输实现数据共享，目前应用在科研、教育、金融证券、企业管理、制造、办公自动化、电子商务、家庭娱乐等许多领域。

网络应用按照响应时间可以分为两种：实时应用和非实时应用。不同的应用有着不同的网络响应性能需求，对网络延迟和带宽有不同的影响。

实时应用要求将节点机产生的数据立即传送出去，一般不需要用户干预。实时应用要求信息传输的速率稳定，具有可预测性。令牌传递网络(令牌环网或 FDDI)和面向连接的服务(如 ATM)可以为这些应用提供支持，但在网络分析与设计中通常不考虑实时应用。

通常所说的应用指的是非实时应用，此类应用对网络带宽和数据传输能力的要求比较高，当暂时争用不到网络介质时，只要介质可以承受任何突发性的数据收发任务，非实时应用就不会出现问题。所以，这种应用适合于类似以太网的共享介质网络。

另外，按照应用是否共享，又可以把应用分为独立应用和共享应用两种类型。

不同的应用对网络功能和性能方面的需求不同，网络设计人员应对网络应用需求加以分析，以便确定网络的应用目标及其他相关指标。

1.1.1.2　现有网络系统分析

1. 现有网络系统结构调研

如果需要在已有网络上构建新系统，那么就应该全面了解现有网络情况，尽可能考虑旧系统的利用，这样既可保护用户原有投资，又能让用户在使用新系统时有一个平滑的过渡，从而大大节省培训的时间和费用。

网络系统的建设一般需要分成几个阶段来实施，每个阶段都是在前期网络的基础之上进行的，不可能完全抛弃现有网络。因此，必须对现有网络进行仔细调研，以考查在原有网络中哪些部分是可以利用的，哪些部分是需要升级的，哪些部分是无用而必须舍弃的。重点考查的内容有以下几个方面。

1)　服务器的数量和位置

服务器是网络中提供专门服务的设备，是网络中的稀缺资源，新网络应该尽量将它们包括进去。在建设新网络之前，需要清楚了解服务器的台数、位置、型号、使用的软件、提供的服务类型以及其他各项性能指标。

2)　客户机的数量和位置

客户机是用户使用网络服务的窗口，有的客户机只供单个用户使用，而有的则供多人使用(如图书馆的查询机)；另外，在客户机上运行的应用系统有差别，对网络服务的需求也不一样。网络中包含的客户机的数量及承担的任务决定了网络的负载，因而有关客户机的信息对网络系统的设计也非常重要，新建网络时必须仔细考虑它们。

3)　使用情况

网络的使用情况包括客户机的数量、访问类型、每天的用户数、每次使用的时间、每次数据传输的数据量、网络拥塞的时间段等，这些数据都可以通过查询网络管理系统的日志文件获得。如果没有完整的日志数据，也可以通过与用户交谈获得有用信息。这些数据虽然不需要十分准确，但其准确性将影响今后网络的设计方案。

4) 采用的协议

协议是网络通信的基础，原有网络可能包含有多种协议，协议间存在着一定的差异。这就需要进行详细的调查，以便新建网络时能够很好地照顾到多种协议间的差异，以方便不同协议数据之间的转换。

5) 通信模式

通信模式就是用户接入网络的方式。网络设计要兼顾各种通信模式。

2. 现有网络体系结构分析

网络体系结构是定义和描述一组用于计算机及其通信设备之间互联的标准和规范的集合，遵循这组规范就可以实现计算机设备之间的通信。目前有两大主流体系结构标准：一个是国际标准 OSI(开放系统互联)参考模型，另一个是工业标准 TCP/IP 模型。

OSI 参考模型通过分层和抽象，将网络划分为七个功能各异的层次，同一端系统中的低层为高层提供服务，不同端系统中的对等层之间进行通信并交换协议数据单元。它是一个开放系统模型，概念清晰，但偏重于理论研究，复杂而不实用，目前实现的范例还较少。

TCP/IP 简化了 OSI 参考模型的分层结构，层次明显减少，实现简单，功能强大，目前为大多数厂商支持，已成为网络通信协议事实上的标准，并已得到普遍的推广。其他还有 IBM 的系统网络体系结构(SNA)和 DEC 的数字网络体系结构(DNA)等著名的体系结构。

通过对现有网络体系结构进行分析，可以为建设新网络提供参考依据。同时在设计新网络时也应该照顾到原有网络的体系结构，尽量发挥其优势，而不应该完全抛弃。

1.1.1.3 需求定义

网络系统的需求包括功能需求、通信需求、性能需求、可靠性需求、安全需求、维护和运行需求以及管理需求等，下面逐一介绍。

1. 功能需求

功能需求即是网络在用户单位业务中应该提供的功能，可以通过了解用户单位所从事的行业、该单位在行业内的地位以及和其他单位的关系等来确定其功能需求。另外，还可以通过了解项目背景来明确用户单位建网的目的，从而有助于描述详细的功能需求。

2. 通信需求

在网络中，网络通信是个人通信模式和流量的组合。通信模式以发生在节点(客户机)之间的通信方式为基础。通常有以下几种通信方式。

- 对等通信方式。
- 客户机/服务器通信方式。
- 服务器/客户机通信方式。

独立节点之间可以在一种或多种方式下通信，如何选择通信方式取决于网络的资源、节点和应用程序的性能。例如，在对等通信方式下，各工作站之间可共享资源；在客户机/服务器通信方式下，可以访问中央文件服务器上的核心数据库。

1) 对等通信方式

对等通信方式是在一种结构和功能相似的节点之间的通信，通信节点具有相似的应用和通信能力。在该种网络中，每个节点与网络中的其他节点相连接，没有明显的源通信模

式和目的通信模式。

2)　客户机/服务器通信方式

客户机/服务器通信方式是网络中的客户机和服务器之间的通信。客户机可以是任何类型的节点，这些节点可以访问一些共享的资源。服务器在大小和功能上有所不同，既可以是基于 PC 机的服务器，也可以是中型计算机和大型计算机。

3)　服务器/客户机通信方式

数据库服务器应用程序使数据从服务器流向客户机。通常情况下，客户机请求比服务器响应所传送的通信量要少。例如，在典型的 Web 方案中，服务器根据客户机浏览器的请求向客户机发送大量的 Web 页面，这就是所说的服务器/客户机分布。

4)　相关指标

为了确定用户的通信需求，需要了解用户单位的建筑物布局、入网站点的分布情况，并记录下述信息。

- 网络中心(或计算中心)及各级设备间的位置。
- 用户数量及其位置。
- 任何两个用户之间的最大距离。
- 用户群组织(即在同一楼里或同一楼层里的用户，尤其注意那些地理上分散，却属于同一部门的用户)。
- 特殊的需求或限制(例如，网络覆盖的地理范围内是否有道路、山丘；建筑物之间是否有阻挡物；电缆等介质布线是否有禁区；是否存在可以利用的介质系统等)。

3. 性能需求

在需求分析中要分析网络的多种性能特性，包括响应时间、延迟、等待时间、利用率、带宽、容量、吞吐量、可用性、可靠性、可恢复性、冗余度、适应性、可伸缩性、效率和费用等。有些需求用户不是很关心，但对于设计者却是必须考虑的。随着计算机网络数量的增长、规模的扩大，如何提高网络性能成为十分重要的问题。与衡量单机系统的性能不同，网络性能是衡量一群计算机系统的性能。了解网络用户的需要，设定恰当的性能目标，合理选择网络结构和组成，便能得到满足用户需求且性能比较好的网络。

网络用户关心的网络性能是能否获得最快的响应，网络管理员关心的网络性能是能否获得最高的资源利用率，两者需要很好地平衡。这种平衡包括两个方面：一方面是性能和价格的折中，另一方面是吞吐量和响应时间的平衡。

4. 可靠性需求

可靠性需求就是用户需要什么样的可靠性。一个系统的可靠性定义为在指定的条件和时间内，系统能够实现指定功能的概率。而整个系统的可靠性又取决于组成系统的各个部件的可靠性。

可靠性指标一般包括平均无故障时间(MTBF)和平均修复时间(MTTR)、可用性和故障率等。

5. 安全需求

1)　安全需求概述

网络安全性包括对物理产品的布局和对过程的操作，合理的物理产品布局与安全设置

可以保护网络和系统的完整性、可行性及可靠性。现代的网络安全性是把基本的网络安全性概念运用在分布式网络环境中。网络安全性的目的是对资源的保护，目前还没有彻底的解决方法。

安全设计包括安全服务和实施两方面。原则上讲，每一个网络系统都具有独立和通用的安全协议，而基于安全服务的安全信息则是存放在管理信息库(MIB)中的，只有授权人员或系统才可访问、修改或删除这些机密信息。通过对网络易损点的识别，可使这些易损点得到保护和监控，要确保安全，应采取一种分层管理策略。

安全性策略的3个属性定义为保密性、完整性和可信性。信息损失通常由以下原因引起：更改、破坏和泄露。对网络安全构成威胁的形式很多，而且它们常导致网络失常和重要信息的毁坏。

采取何种安全措施需要视用户需要而定，不同单位或一个单位的不同部门要求的安全等级往往是有差异的，并不是安全等级越高越好，较高的安全等级意味着额外的系统开销和高昂的费用。

2) 安全性标准

网络系统是否达到一定的安全性主要依照相关的安全性标准来判断，最早的信息系统安全性标准由美国国防部颁布的黄皮书(TC-SEC-NCSC，可信计算机系统)规定。该手册将IT系统划分为A(A1)、B(B1、B2、B3)、C(C1、C2)、D(D1)4类，共7个安全等级。

(1) D类安全等级。D类安全等级只包括D1一个级别，D1的安全等级最低，它只为文件和用户提供安全保护。D1系统最常见的形式是本地操作系统，或者是一个完全没有保护的网络。

(2) C类安全等级。C类安全等级能够提供审慎的保护，并为用户的行动和责任提供审计能力。C类安全等级可划分为C1和C2两类。

(3) B类安全等级。B类安全等级可划分为B1、B2和B3 3类。B类系统具有强制性保护功能，这就意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。

(4) A类安全等级。A类系统的安全级别最高。目前，A类安全等级只包含A1一个安全类别。A1类与B3类相似，对系统的结构和策略不作特别要求。A1系统的显著特征是：系统的设计者必须按照一个正式的设计规范来分析系统。对系统进行分析后，设计者必须运用核对技术来确保系统符合设计规范。A1系统必须满足下列要求：系统管理员必须从开发者那里接收一个安全策略的正式模型；所有的安装操作都必须由系统管理员进行；系统管理员进行的每一步安装操作都必须有正式文档。

欧洲等价的分类手册是ITSEC(信息技术安全评估标准)。与美国的黄皮书类似，ITSEC标准目录将IT系统划分为7个安全等级(E0～E6)，这些等级与黄皮书中的各个等级大致对应。

6. 维护和运行需求

维护和运行是网络系统投入正常运行后的日常管理工作，这项工作主要由网络管理人员承担。网络管理人员通过网络管理系统可以完成系统的配置、监控和统计等事务的处理，有时还要对网络设备进行检修。网络设计人员需要根据用户需求，提供必要的网络管理工具和策略，以方便网络管理人员对整个网络进行管理和维护，提高网络的运行效率，保证

网络的可靠性。

7. 管理需求

从用户的角度来讲，一个网络管理系统应该满足以下要求。

- 同时支持网络监视和控制两方面的能力。
- 能够管理所有的网络协议。
- 尽可能大的管理范围。
- 尽可能小的系统开销。
- 可以管理不同厂家的联网设备。
- 容纳不同的网络管理系统。
- 网络管理的标准化。

在 OSI 网络管理框架模型中，基本的网络管理功能被分为 5 个功能域：配置管理(Configuration Management)、性能管理(Performance Management)、故障管理(Fault Management)、安全管理(Security Management)和计费管理(Accounting Management)。

网络管理的标准化产品包括 ISO 的 CMIS/CMIP(Common Management Information Service/Common Management Information Protocol)、Internet 体系结构委员会(Internet Architecture Board，IAB)的 SNMP 和管理信息库(MIB)，这些内容将在第 5 章详细介绍。

1.1.2　典型例题分析

例 1　阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。(2010 年下半年下午试题一)

【说明】某企业网拓扑结构如图 1-1 所示。

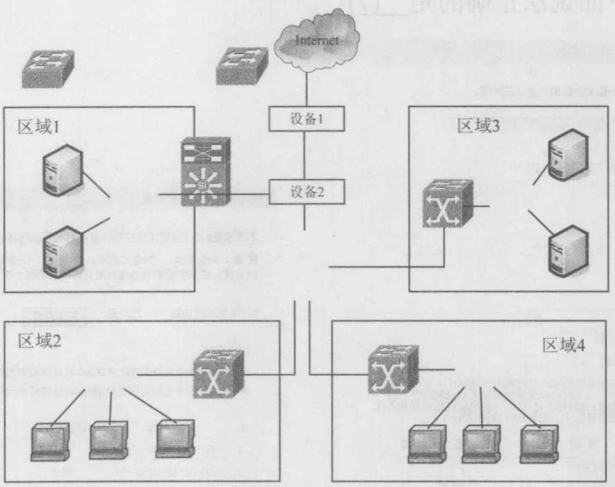

图 1-1　某企业网拓扑图

【问题 1】(4 分)

企业根据网络需求购置了如下设备，其基本参数如表 1-1 所示。

表 1-1　设备基本参数表

设备类型	参　数
A	模块化接入，固定广域网接口+可选广域网接口，固定局域网接口 100/1000 Base-TX
B	背板带宽=1.2 Tbps，包转发率=285 Mpps，传输速率=10/100/1000 Mbps，交换方式为存储转发，应用层级别为三层
C	背板带宽=140 Gbps，包转发率=100 Mpps，传输速率=10/100 Mbps，交换方式为存储转发
D	24 个固定百兆 RJ45 接口，1 个 GBIC 插槽，包转发率=7.6 Mpps
E	并发连接数=280 000，安全过滤带宽=135 Mbps，支持 IDS 及 VPN

根据网络需求、拓扑图和设备参数类型，图 1-1 中设备 1 应选择类型为__(1)__的设备，设备 2 应选择类型为__(2)__的设备。

【问题 2】(4 分)

该网络采用核心层、汇聚层、接入层的三层架构，所有计算机都采用静态 IP 地址。为了防止恶意用户盗用 IP 地址，网管员可采用__(3)__的策略来防止 IP 地址盗用，该策略应在三层架构中的__(4)__层实施。

企业架设 Web 服务器对外进行公司及产品宣传，同时企业内部需架设数据库服务器存放商业机密数据，则 Web 服务器应放置在图 1-1 中的区域__(5)__，数据库服务器应放置在区域__(6)__。

【问题 3】(4 分)

若网络管理员决定在企业内部增加 WLAN 接入功能，无线路由器基本参数设置如图 1-2 所示。

网络管理员决定在无线 AP 上开启 MAC 地址过滤功能，若该 AP 的 MAC 地址过滤表如图 1-3 所示，则下面说法正确的是__(7)__。

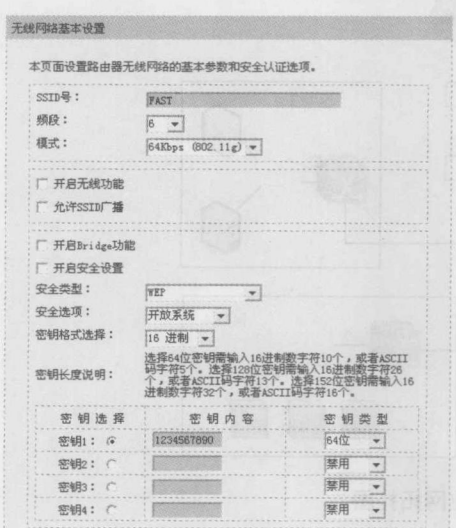

图 1-2　无线路由器基本参数设置

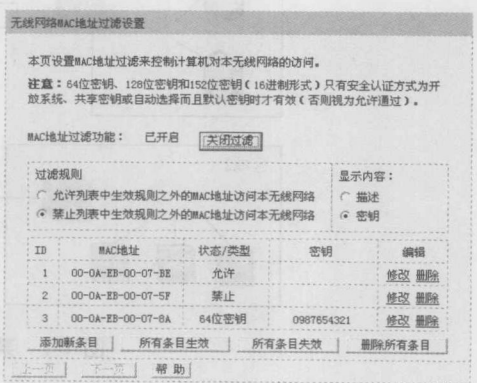

图 1-3　MAC 地址过滤表

A．MAC 地址为“00-0A-EB-00-07-5F”的主机可以访问 AP

B．MAC 地址为“00-0A-EB-00-07-8A”的主机可以使用 64 位 WEP 密钥“1234567890”来访问 AP

C．MAC 地址为“00-0A-EB-00-07-8A”的主机可以使用 64 位 WEP 密钥“0987654321”来访问 AP

D．其他主机均可以访问本无线网络 AP

若将 MAC 地址过滤规则设为“允许列表中生效规则之外的 MAC 地址访问本无线网络”，则下面说法正确的是__(8)__。

A．MAC 地址为“00-0A-EB-00-07-5F”的主机可以访问 AP

B．MAC 地址为“00-0C-EC-00-08-5F”的主机可以访问 AP，不需要输入 WEP 密码

C．MAC 地址为“00-0C-EC-00-08-5F”的主机可以访问 AP，需使用 64 位 WEP 密码“0123456789”

D．MAC 地址为“00-0A-EB-00-07-8A”的主机可以访问 AP，不需要输入 WEP 密码

【问题 4】(3 分)

若 MAC 地址过滤规则如图 1-4 所示，MAC 地址为“00-0A-EB-00-07-5F”的主机能访问该 AP 吗？请说明原因。

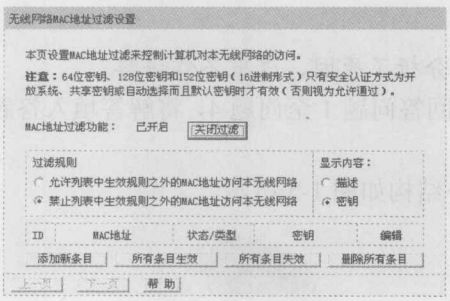

图 1-4　MAC 地址过滤规则

答案：

【问题 1】(1) A　(2) E

【问题 2】(3) MAC 地址与 IP 地址绑定　(4) 接入　(5) 1　(6) 3

【问题 3】(7) C　(8) C

【问题 4】不能。MAC 地址过滤功能已开启，并设置过滤规则为“禁止列表中生效规则之外的 MAC 地址访问本无线网络”。由于 MAC 地址为“00-0A-EB-00-07-5F”的主机在列表中的状态是“禁止”，因此不能访问 AP。

解析：

【问题 1】设备 1 应为路由器，设备 2 应为防火墙。设备类型 B、C、D 分别为核心交换机、汇聚交换机和接入交换机。设备 A 为路由器，设备 E 为防火墙，并发连接数，是指防火墙能够同时处理的点对点连接的最大数目，它反映出防火墙设备对多个连接的访问控制能力和连接状态跟踪能力。

【问题 2】IP 地址的修改非常容易，而 MAC 地址存储在网卡的 EEPROM 中，而且网卡的 MAC 地址是唯一确定的。因此，为了防止内部人员进行非法 IP 盗用(如盗用权限更高

人员的IP地址，以获得权限外的信息)，可以将内部网络的IP地址与MAC地址绑定，这样修改了IP地址，也会因MAC地址不匹配而导致盗用失败；而且由于网卡MAC地址的唯一确定性，网络管理员可以根据MAC地址查出使用该MAC地址的网卡，进而查出非法盗用者。

MAC地址过滤是接入层的功能，MAC地址与IP地址绑定在接入层实施。

本题中，内网在Internet接入的时候利用防火墙将网络分割为内外网和一个DMZ(DeMilitarized Zone，“隔离区”，也称“非军事化区”)。DMZ区域对于外部用户是可以访问的，Web服务器、Email服务器等一般都放置在DMZ区域。数据库服务器存放商业机密数据，不能允许外部用户访问，因此要放入内网中。图1-1中，区域1是DMZ，Web服务器应放置在该区域。区域3是内部网络中的区域，用于放置外网不能访问的服务器，数据库服务器应放置在该区域。

【问题3】 由图1-3可知，MAC地址为“00-0A-EB-00-07-BE”的主机可以访问AP，MAC地址为“00-0A-EB-00-07-5F”的主机不能访问AP，MAC地址为“00-0A-EB-00-07-8A”的主机可以使用64位WEP密钥“0987654321”来访问AP。

若将MAC地址过滤规则设为“允许列表中生效规则之外的MAC地址访问本无线网络”，由图1-2可知，列表中生效规则之外的MAC地址访问本无线网络需要使用64位WEP密码“0123456789”。

【问题4】答案中已经分析了原因，这里不作讲解。

例2 阅读以下说明，回答问题1至问题4，将解答填入答题纸对应的解答栏内。(2010年上半年下午试题一)

【说明】某校园网拓扑结构如图1-5所示。

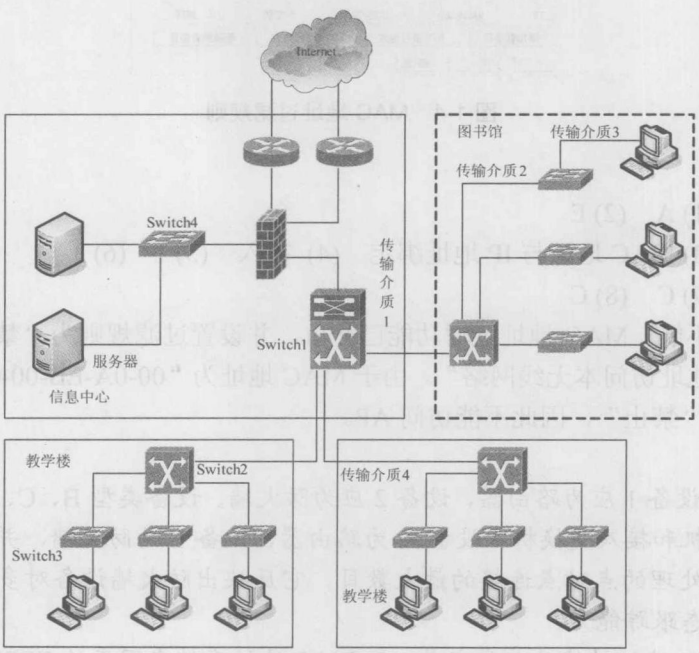

图1-5 某校园网络拓扑图