21

21世纪高职高专规划教材
网络专业系列

计算机网络安全与管理

（第2版）

田庚林 田华 张少芳 编著

清华大学出版社

21世纪高职高专规划教材

网络专业系列

计算机网络安全与管理

（第2版）

田庚林 田华 张少芳 编著

清华大学出版社
北京

内 容 简 介

本书是面向高职高专计算机网络技术专业学生的教材。

本书以一个模拟网络工程为主线，分析网络工程中的安全管理需求，根据需求制定工程任务，按照任务介绍必备的知识，提出模拟工程中的解决方案，完成方案配置。

本书共分7章，内容包括模拟网络工程环境和模拟网络工程中的项目介绍及网络安全基础、访问控制列表技术、网络地址转换、VPN技术、防火墙、局域网安全、网络管理技术。

本书可以作为高职高专计算机网络技术及相关专业学生的教材，也可以作为网络工程技术人员和本科院校学生的参考书。

图书在版编目(CIP)数据

计算机网络安全与管理/田庚林，田华，张少芳编著. --2版. --北京：清华大学出版社，2013
21世纪高职高专规划教材. 网络专业系列
ISBN 978-7-302-32407-2

Ⅰ. ①计… Ⅱ. ①田…②田…③张… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2013)第096000号

责任编辑：刘　青
封面设计：傅瑞学
责任校对：刘　静
责任印制：李红英

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，010-62795764
印 装 者：北京密云胶印厂
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：20.25　　**字　　数**：461千字
版　　次：2010年3月第1版　2013年10月第2版　　**印　　次**：2013年10月第1次印刷
印　　数：1～2500
定　　价：39.00元

产品编号：049875-01

出版说明

高职高专教育是我国高等教育的重要组成部分，担负着为国家培养并输送生产、建设、管理、服务第一线高素质技术应用型人才的重任。

进入21世纪后，高职高专教育的改革和发展呈现出前所未有的发展势头，学生规模已占我国高等教育的半壁江山，成为我国高等教育的一支重要的生力军；办学理念上，“以就业为导向”成为高等职业教育改革与发展的主旋律。近两年来，教育部召开了三次产学研交流会，并启动四个专业的“国家技能型紧缺人才培养项目”，同时成立了35所示范性软件职业技术学院，进行两年制教学改革试点。这些举措都表明国家正在推动高职高专教育进行深层次的重大改革，向培养生产、建设、管理、服务第一线真正需要的应用型人才的方向发展。

为了顺应当前我国高职高专教育的发展形势，配合高职高专院校的教学改革和教材建设，进一步提高我国高职高专教育教材质量，在教育部的指导下，清华大学出版社组织出版了“21世纪高职高专规划教材”。

为推动规划教材的建设，清华大学出版社组织并成立了“高职高专教育教材编审委员会”，旨在对清华版的全国性高职高专教材及教材选题进行评审，并向清华大学出版社推荐各院校办学特色鲜明、内容质量优秀的教材选题。教材选题由个人或各院校推荐，经编审委员会认真评审，最后由清华大学出版社出版。编审委员会的成员皆来自教改成效大、办学特色鲜明、师资实力强的高职高专院校、普通高校以及著名企业，教材的编写者和审订者都是从事高职高专教育第一线的骨干教师或专家。

编审委员会根据教育部最新文件和政策，规划教材体系，比如部分专业的两年制教材；“以就业为导向”，以“专业技能体系”为主，突出人才培养的实践性、应用性的原则，重新组织系列课程的教材结构，整合课程体系；按照教育部制定的“高职高专教育基础课程教学基本要求”，教材的基础理论以“必要、够用”为度，突出基础理论的应用和实践技能的培养。

本套规划教材的编写原则如下：

（1）根据岗位群设置教材系列，并成立系列教材编审委员会；

（2）由编审委员会规划教材、评审教材；

（3）重点课程进行立体化建设，突出案例式教学体系，加强实训教材的出版，完善教学服务体系；

（4）教材编写者由具有丰富的教学经验和多年实践经历的教师共同组成，建立“双师型”编者体系。

本套规划教材涵盖了公共基础课、计算机、电子信息、机械、经济管理以及服务等大类的主要课程,包括专业基础课和专业主干课。目前已经规划的教材系列名称如下:

- **公共基础课**

  公共基础课系列

- **计算机类**

  计算机基础教育系列
  计算机专业基础系列
  计算机应用系列
  网络专业系列
  软件专业系列
  电子商务专业系列

- **电子信息类**

  电子信息基础系列
  微电子技术系列
  通信技术系列
  电气、自动化、应用电子技术系列

- **机械类**

  机械基础系列
  机械设计与制造专业系列
  数控技术系列
  模具设计与制造系列

- **经济管理类**

  经济管理基础系列
  市场营销系列
  财务会计系列
  企业管理系列
  物流管理系列
  财政金融系列
  国际商务系列

- **服务类**

  艺术设计系列

本套规划教材的系列名称根据学科基础和岗位群方向设置,为各高职高专院校提供"自助餐"形式的教材。各院校在选择课程需要的教材时,专业课程可以根据岗位群选择系列;专业基础课程可以根据学科方向选择各类的基础课系列。例如,数控技术方向的专业课程可以在"数控技术系列"选择;数控技术专业需要的基础课程,属于计算机类课程的可以在"计算机基础教育系列"和"计算机应用系列"选择,属于机械类课程的可以在"机械基础系列"选择,属于电子信息类课程的可以在"电子信息基础系列"选择。依此类推。

为方便教师授课和学生学习,清华大学出版社正在建设本套教材的教学服务体系。本套教材先期选择重点课程和专业主干课程,进行立体化教材建设:加强多媒体教学课件或电子教案、素材库、学习盘、学习指导书等形式的制作和出版,开发网络课程。学校在选用教材时,可通过邮件或电话与我们联系获取相关服务,并通过与各院校的密切交流,使其日臻完善。

高职高专教育正处于新一轮改革时期,从专业设置、课程体系建设到教材编写,依然是新课题。希望各高职高专院校在教学实践中积极提出意见和建议,并向我们推荐优秀选题。反馈意见请发送到 E-mail: gzgz@tup.tsinghua.edu.cn。清华大学出版社将对已出版的教材不断地修订、完善,提高教材质量,完善教材服务体系,为我国的高职高专教育出版优秀的高质量的教材。

高职高专教育教材编审委员会

第2版前言

本书以一个模拟网络工程为主线，分析网络工程中的安全需求与管理任务；按照需求制定工程任务，按照任务需要介绍必备的知识，提出模拟工程中的解决方案，完成方案的配置。本书内容以工程需求为主，同时还兼顾了知识体系的完整性与系统性。为了便于学生在实验室中对解决方案的配置、验证和测试，书中给出一个网络安全与管理实训工程环境，实训环境可使用实际网络设备实现，也可使用模拟器软件实现。第2章至第7章的每章后都有实训内容和实训指导，让学生根据在模拟工程实践中学到的知识技能完成实训项目，增强学生的动手能力与实践技能。

本书在第1版的基础上进行了部分修改，除了根据教学中的反馈信息对内容排列顺序进行调整之外，主要增加了H3C设备的内容。第1版主要以Cisco设备为例，但目前国内企业所用的网络设备大都以国内厂商的设备为主，而在网络安全配置方面，不同厂家的设备配置方法差异较大，所以在第2版中，同时兼顾了Cisco设备及H3C设备。书中主要以H3C设备配置为例进行介绍，而后给出Cisco设备的配置方案。

本书共分7章。第1章介绍模拟网络工程环境和模拟网络工程中的项目介绍及网络安全基础；第2章介绍访问控制列表技术，根据工程任务安全需求分析，解决网络边界访问控制配置问题；第3章介绍网络地址转换，根据工程任务安全需求分析，解决网络中使用路由器进行内外网地址转换的配置问题；第4章介绍VPN技术，根据工程任务安全需求分析，解决利用Internet线路进行安全通信配置问题；第5章介绍防火墙，根据工程任务安全需求分析，解决网络边界安全中防火墙基本配置问题；第6章介绍局域网安全，根据工程任务安全需求分析，解决局域网中安全配置问题；第7章介绍网络管理技术，包括基本网络管理知识和常用的网络管理工具。附录中介绍了如何利用网络模拟器GNS3搭建模拟实训环境、iMC安装指导，并配有各章习题参考答案。

本书由田庚林主持编写，具体内容由田华、张少芳编写完成。其中田庚林主要参与了内容的组织策划和统稿审订工作，第6章、第7章由田华编写，其余部分由张少芳编写。

由于计算机网络技术发展更新较快，编者水平有限，书中的不足之处望广大读者批评指正。作者E-mail：tiangl163@163.com。

编　者

2013年6月

第 1 版前言

本书是一本面向高等职业教育的教材，是计算机网络技术专业系列教材之一。

在计算机网络技术专业建设中，从网络工程、网络管理岗位需求出发，我们将专业技能重点放在网络技术和网站技术两个方面。该专业系列教材中，将网络技术分为《计算机网络技术基础》、《计算机网络集成技术》、《计算机网络安全与管理》和《网络操作系统》4 门课程；网站技术主要包括《网页制作工具》、《网络数据库》、《动态网站技术》和《.NET 网站技术》4 门课程。本书主要介绍网络安全技术和基本的网络管理知识与基本管理技能。

本书以一个模拟的网络工程为主线，分析网络工程中的安全需求与管理任务；按照需求制定工程任务，按照任务需要介绍必备的知识，提出模拟工程中的解决方案，完成方案配置。本书内容既以工程需求为主，同时还照顾了知识体系的完整性与系统性。为了便于学生在实验室中对解决方案的配置、验证和测试，书中给出了一个网络安全与管理实训工程环境，实训环境可使用实际网络设备实现，也可使用模拟器软件实现。第 2 章至第 7 章的每章章后都有实训内容和实训指导，让学生根据在模拟工程实践中学到的知识技能完成实训项目，提高学生的动手能力与实践技能。

本书共分 7 章。第 1 章介绍模拟网络工程环境和模拟网络工程中的网络安全与管理需求分析；第 2 章介绍访问控制列表技术，根据工程任务安全需求分析，解决网络边界访问控制配置问题；第 3 章介绍局域网安全，根据工程任务安全需求分析，解决局域网中安全配置问题；第 4 章介绍网络地址转换技术，根据工程任务安全需求分析，解决网络中使用路由器进行内外网地址转换的配置问题；第 5 章介绍 VPN 技术，根据工程任务安全需求分析，解决利用 Internet 线路进行安全通信配置问题；第 6 章介绍防火墙技术，根据工程任务安全需求分析，解决网络边界安全中防火墙基本配置问题；第 7 章介绍网络管理技术，包括基本网络管理知识和常用的网络管理工具。附录中介绍了如何利用网络模拟器 GNS3 搭建模拟实训环境。本书中的网络设备都是以 Cisco 为例介绍的。

本书由田庚林主持编写，具体章节由田华、张少芳编写完成。其中，田庚林主要参与了内容的组织策划和统稿审订工作，第 3 章和第 4 章由张少芳编写完成，其余章节由田华编写完成。

由于计算机网络技术发展更新较快，编者水平有限，书中的不足之处望广大读者批评指正。编者 E-mail：tiangl163@163.com。

编　者

2009 年 12 月

目　录

第 1 章

项目介绍及网络安全基础

随着网络技术的不断发展和普及，网络安全技术也越来越受到人们的关注。人们都知道如果一台 PC 仅仅安装了操作系统，而没有安装任何杀毒软件、防火墙（单机软件）等安全防护软件，那么可能在很短的时间内系统就会因为受到病毒等的攻击而瘫痪，而网络作为一个开放的信息系统同样会存在诸多的安全隐患。在实际中，任何一个计算机网络系统，特别是较大型的企业网络系统，为保证其安全、可靠地运行，必须建立相应的网络安全与管理方案，以减少各种潜在网络安全风险和网络性能瓶颈对信息系统正常运行的影响。本书以一个典型的跨地区公司网络系统为例，按照实际网络工程项目过程，先分析其中的网络安全与管理问题，然后介绍解决这些问题所需的知识和技术，最后给出这些问题的相应的解决方案。

1.1 网络安全与管理项目介绍

1.1.1 模拟公司网络环境

1. 企业网络应用情况

某大型新兴产业公司为提高生产效率，拟新建联通各地分公司的计算机网络。该公司的总公司及其直属 3 个分支机构在 A 市，并在 B 市和 C 市分别设有一个分公司和两个分支机构。总公司和分公司主要负责产品的研发和生产，设有管理部门、研发部门、市场部门、售后服务部门和生产部门。各分支机构主要负责产品销售和售前、售后服务，设有市场部门、售后服务部门和管理部门。

公司所建网络将主要承载公司内部 OA、邮件、FTP、远程教育等系统和面向公众提供服务的电子商务网站系统。受业务发展、系统性能等诸多方面因素影响，以上网络应用系统设计在总公司、分公司分别设有网络应用及数据库服务器，而在分支机构只设网络终端。

2. 企业网络拓扑结构

全公司的网络拓扑结构如图 1-1 所示。总公司与分公司利用电信专线互联，而为节约线路成本，总/分公司与其下属分支机构通过宽带线路接入本地 Internet 实现互联。

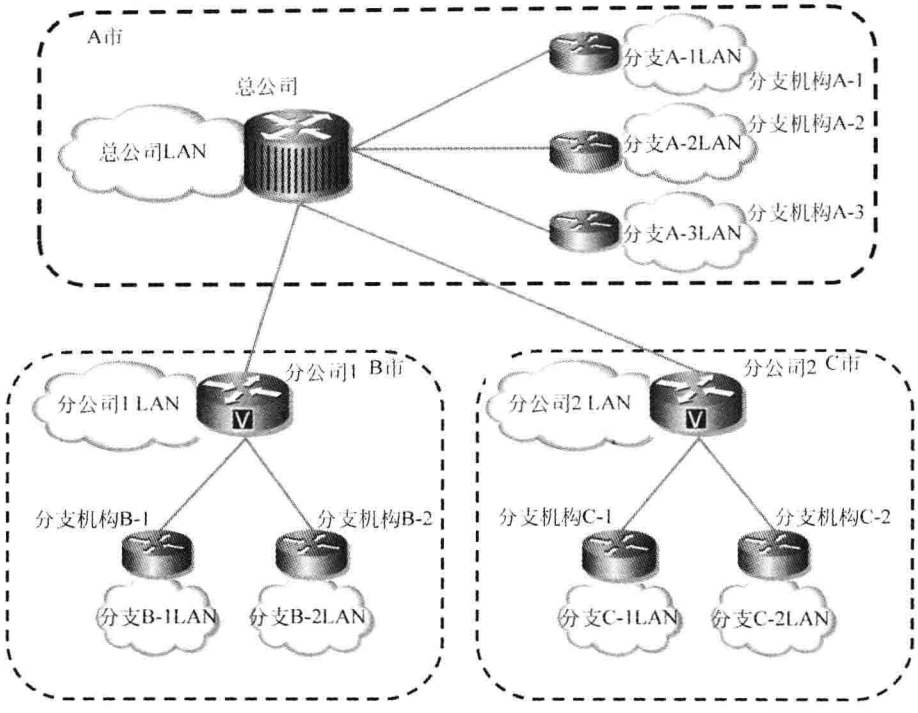


图 1-1　模拟公司网络拓扑结构示意图

总公司局域网的网络拓扑结构按照网络应用需求分为核心、汇聚、接入3层，图1-2为总公司局域网网络拓扑结构示意图。为了保证系统安全可靠性，在各交换机上使用了双冗余线路设计。

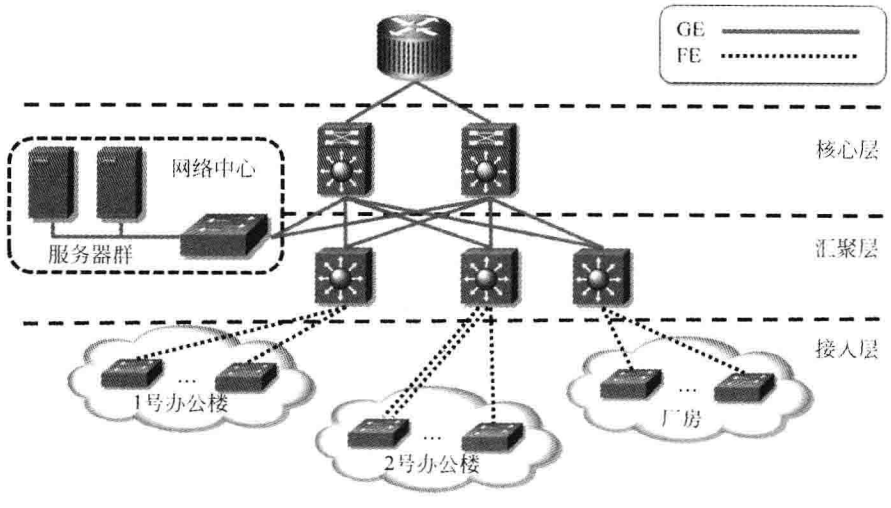
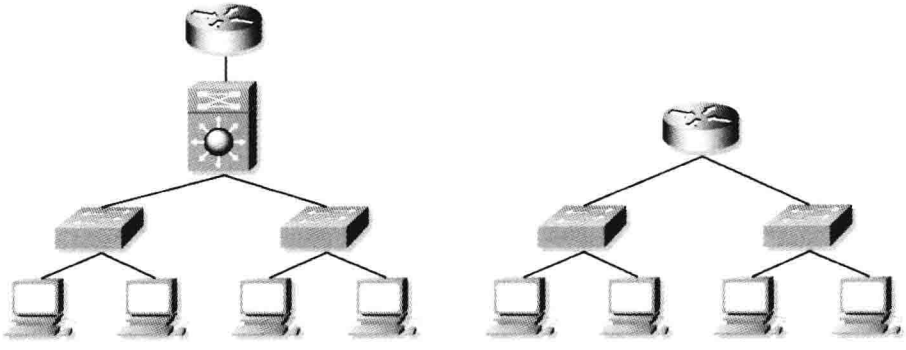


图 1-2　总公司局域网网络拓扑结构图

分公司在局域网结构、链路冗余等方面与总公司类似。但分支机构 B-1、C-1 网络规模较大，而分支机构 B-2、C-2 网络规模较小，分支机构的网络拓扑结构分别如图 1-3 所示。



(a) 分支机构B-1、C-1网络拓扑　　(b) 分支机构B-2、C-2网络拓扑

图 1-3　分支机构网络拓扑结构图

1.1.2　模拟公司网络安全及管理需求

1. 网络安全需求

目前计算机网络面临着多方面的安全威胁，例如物理安全威胁、网络通信威胁、网络服务威胁、网络管理威胁等，模拟公司网络也不能例外。从模拟公司网络环境和业务需求分析可以发现，要保证该网络安全运行，需要解决以下网络安全问题。

(1) 由于连接到 Internet，所以必须解决来自 Internet 的网络入侵和攻击问题。

(2) 模拟公司与分支机构间使用 Internet 线路通信，必须解决通信数据安全问题。

(3) 由于公司租用的 IP 地址有限，随着企业网络规模发展，必须解决公司网络中 IP 地址资源不足的问题。

(4) 模拟公司网络不是单纯的生产网络，办公局域网的接入使得网络管理人员必须面对局域网中各种潜在安全威胁，如病毒问题、非授权访问网络资源问题、非授权变更网络结构等。

2. 网络管理需求

要保证模拟公司网络安全、可靠地运行，必须对网络进行管理和维护。在网络管理过程中，需要解决以下问题。

(1) 根据网络需求变化，使用工具对网络进行配置、调整。

(2) 当网络发生故障时，能够发现、跟踪故障现象，记录故障状态信息，分析故障原因，解决网络故障。

(3) 监控、记录网络性能变化，根据需求适当调整网络，以提高网络性能。

(4) 监控、记录网络受到安全威胁的情况，检查网络可能存在的安全漏洞或隐患，并通过访问控制等手段对网络的薄弱环节进行改善。

1.1.3　网络安全与管理实验环境

本书将根据以上网络安全及管理方案基本设计思路,逐个解决模拟公司网络中的安全及管理方面的问题,介绍相关知识,提出解决方案,完成相应系统配置。另外,在每一章后面都给出了相关知识的实验,下面对实验环境进行简单的介绍。

1. 物理实验环境

物理实验环境中共有8个学习岛,每一个学习岛由1台机柜和5台计算机组成。实验环境的物理规划如图1-4所示。

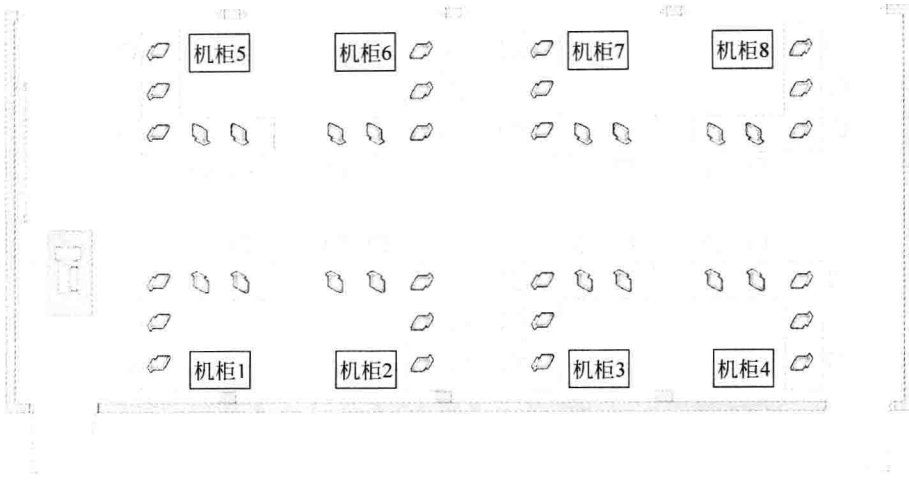


图1-4　实验环境物理规划图

为满足实验的需要,每台机柜中包含的设备如下:

(1) 路由器4台;

(2) 二层交换机2台;

(3) 三层交换机2台;

(4) 防火墙1台。

由于在本书中涉及H3C和Cisco两种设备的配置,因此读者可以根据具体情况配备H3C设备或Cisco设备,Cisco设备也可以通过Packet Tracer或GNS3等模拟器软件来代替。在本书中H3C设备和Cisco设备配置使用相同的网络实验环境,但两个厂商对接口的命名方式存在区别,在书中所有的网络拓扑图中给出的接口均以H3C设备的命名方式进行命名,Cisco设备接口与H3C设备接口的对应表如表1-1所示。

表1-1　Cisco与H3C接口名称对应表

Cisco设备接口	H3C设备接口
FastEthernet0/0	Ethernet0/0
FastEthernet0/1	Ethernet0/1
Serial0/0	Serial1/0
Serial0/1	Serial2/0

2. 逻辑实验环境

(1) 逻辑网络拓扑与 IP 地址规划

为使各个学习岛可以访问外部网络，在实验网络的出口处使用一台路由器和一台三层交换机来进行校园网与实验网络以及实验网络内各个学习岛网络之间的连接。实验网络具体的逻辑拓扑与 IP 地址规划如图 1-5 所示。

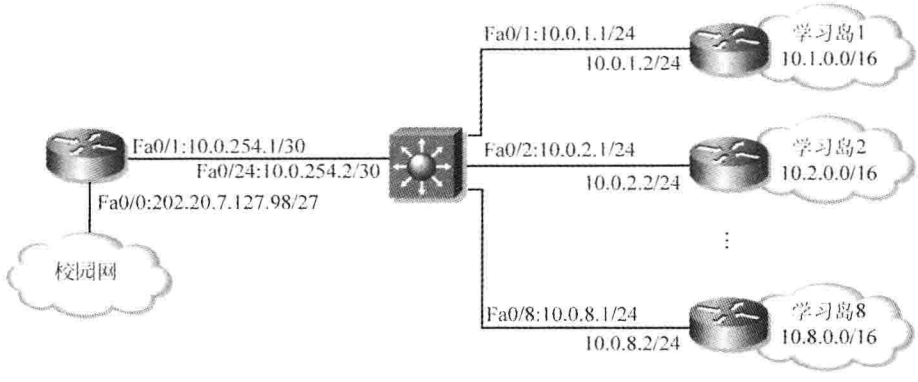


图 1-5　实验网络的逻辑拓扑与 IP 地址规划图

从图 1-5 可以看出，学习岛 1～学习岛 8 的 WAN 接口分别连接到了出口三层交换机的 Fa0/1～Fa0/8 接口上，出口三层交换机向上连接到出口路由器上，出口路由器向上连接到校园网。

在 IP 地址的规划上，具体的规划原则和 IP 地址分配情况如下：

① 三层交换机与各个学习岛之间链路分配的 IP 网段为 10.0.x.0/24，其中 x 为学习岛的编号。当学习岛上的实验网络拓扑为计算机通过二层网络设备连接到 WAN 接口上时，为计算机分配 10.0.x.0/24 网段的 IP 地址，网关为 10.0.x.1。

② 为每一个学习岛预留的 IP 网段为 10.x.0.0/16。当学习岛上的实验网络拓扑为通过三层网络设备连接到 WAN 接口上时，实验网络内可以使用网段 10.x.0.0/16，并可以根据实验的需求将 10.x.0.0/16 划分成若干个子网。

为实现 10.x.0.0/16 到达其他网段的网络联通性，在出口三层交换机上为每一个学习岛的预留网段均配置了一条静态路由，为学习岛 1 配置的静态路由如下：

```
Switch(config)#ip route 10.1.0.0 255.255.0.0 10.0.1.2
```

从上面的配置命令可以看出，指定的下一跳地址为 10.0.x.2，因此学习岛上与 WAN 接口(即与出口三层交换机)相连的三层网络设备接口 IP 地址一定要配置为 10.0.x.2。另外需要注意的是，在出口三层交换机上只能使用静态路由来实现各个学习岛的联通性，而不能使用动态路由。如果使用了动态路由协议，例如 RIPv2，则在学习岛上的实验环境中也存在 RIPv2 的情况下，任何一个学习岛都会学习到其他学习岛内部的实验环境路由，从而会造成学生实验的混乱。

在出口三层交换机上，除了为每一个学习岛配置了一条静态路由外，还配置了一条指