Information

全国高职高专应用型规划教材

信息技术类

网络互联及路由器技术

宁芳露　韩晓霞　主编

北京大学出版社
PEKING UNIVERSITY PRESS

全国高职高专应用型规划教材·信息技术类

网络互联及路由器技术

主　编　宁芳露　韩晓霞
副主编　刘晓健　汪　洋

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 简 介

本书以设计实施校园网工程为蓝本，采用案例的方式对与网络互联中涉及的交换、路由和远程接入技术进行了详尽的、富有针对性的介绍。全书共分 11 章、以目前工程中流行的网络技术为主线、华为设备为操作基础，主要内容包括：IP 地址及子网划分，网络设计三层模型，交换式以太网技术，无线局域网络，局域网互连技术，广域网接入技术，接入控制与管理以及网络安全技术等。

本书着重体现该系列教材的编写思想，以职业能力的培养为目标应用来架构章节内容，并依照学生接受知识的一般规律以及网络工程施工过程来进行讲述，通过实际案例的方式帮助学生掌握要求的知识点。

本书由多年从事计算机网络技术教学工作、富有实际网络工程经验的多位教师及工程技术人员编写而成。可作为高职高专计算机及相关专业的教材，也适用于网络高级应用技术的培训、自学用书。此外，还可供网络设计开发工程技术人员和管理人员参考。

图书在版编目(CIP)数据

网络互联及路由器技术/宁芳露，韩晓霞主编．—北京：北京大学出版社，2009.8

（全国高职高专应用型规划教材·信息技术类）

ISBN 978-7-301-15278-2

Ⅰ. 网… Ⅱ. ①宁… ②韩… Ⅲ. ①互联网络—高等学校：技术学校—教材②计算机网络—路由选择—高等学校：技术学校—教材 Ⅳ. TP393 TN915.05

中国版本图书馆 CIP 数据核字（2009）第 091399 号

书　　名：网络互联及路由器技术
著作责任者：宁芳露　韩晓霞　主编
策 划 编 辑：周　伟
责 任 编 辑：葛昊晗
标 准 书 号：ISBN 978-7-301-15278-2/TP·1014
出　版　者：北京大学出版社
地　　址：北京市海淀区成府路 205 号　100871
网　　址：http://www.pup.cn
电　　话：邮购部 62752015　发行部 62750672　编辑部 62765126　出版部 62754962
电 子 信 箱：xxjs@pup.pku.edu.cn
印　刷　者：
发　行　者：北京大学出版社
经　销　者：新华书店
787 毫米×980 毫米　16 开本　15.5 印张　372 千字
2009 年 8 月第 1 版　2009 年 8 月第 1 次印刷
定　　价：26.00 元

目　录

前　言

计算机网络已经深入到社会的各个角落，在人类社会的发展中起着越来越重要的作用。局域网络是构成 Internet 的基础，而在构建这些局域网时，使用的就是交换机和路由器这些基础设备。熟练地操作管理这些网络设备，是网络管理人员必须要作的工作。

本书以设计实施校园网工程为蓝本，采用案例的方式对与网络互联中涉及的交换、路由和远程接入技术进行了详尽的、富有针对性的介绍。全书共分 11 章、以目前工程中流行的网络技术为主线、华为设备为操作基础，主要内容包括：校园网络工程项目概述（第 1 章），IP 地址（第 2 章），网络设计三层模型（第 3 章），连接交换式以太网（第 4 章），建立高可靠的以太网（第 51 章），无线用户的接入（第 6 章），局域网络互联（第 7 章），局域网络间互通技术（第 8 章），接入到广域网（第 9 章），接入控制与管理（第 10 章）以及网络安全方面的考虑（第 11 章）。

本书根据《高职高专教育基础课程教学基本要求》和《高职高专教育专业人才培养目标及规格》的精神，着重体现“北大版”高职高专系列教材的编写思想，以职业能力的培养为目标应用来架构章节内容，并依照学生接受知识的一般规律以及网络工程施工过程来进行讲述，通过实际案例的方式帮助学生掌握要求的知识点，使得读者能够设计并管理校园网、企业网等大型局域网等，具备实际的操作与管理技能。

本书由多年从事计算机网络技术教学工作、富有实际网络工程经验的多位教师及工程技术人员编写而成。每章节配有相应的实验和练习题，使读者可以全面、深入地理解、掌握所要求的知识点。本书适用于具有一定计算机网络基础的读者，可作为高职高专计算机及相关专业的教材，也适用于网络高级应用技术的培训、自学用书。此外，还可供网络设计开发工程技术人员和管理人员参考。

本书由辽东学院的宁芳露、河北软件职业学院的韩晓霞担任主编，辽东学院的刘晓健、四川管理职业学院汪洋担任副主编。第 1、10 章由韩晓霞编写，第 2、4、5 章由汪洋编写，第 3、6、7 章由宁芳露编写，第 8、9、11 章由刘晓健编写。

在编写的过程中，参考了大量的相关资料，许多同仁也给予了大量帮助，在此深表谢意。由于编者水平有限，时间仓促，不妥之处在所难免，衷心希望广大读者批评指正。

编　者

2009 年 3 月

第 1 章　校园网络工程项目概述

教学目标

本章主要以某校园网络项目为蓝本，初步简介项目的基本情况以及主要网络技术要求。描述完成上述网络工程的大致实施过程。

教学要求

知识要点	能力要求	关联知识
网络系统设计	了解网络系统设计的相关概念。	网络系统设计基本原则
校园网工程主要技术要求	了解局域网的相关概念、IP 地址、网络系统分层、网络设备的作用及连接及网络安全管理	局域网、广域网、网络设备的配置和连接，网络安全及访问控制
网络工程实施过程	了解网络工程实施步骤	网络工程实施步骤

引例

我们可以看到，随着网络通信技术、数据库技术、多媒体教育等信息技术的飞速发展，数字化正进

入社会生活的各个层面。各种信息技术正在被大规模地引入教育领域中，如校园网络、远程教学、课件开发技术、多媒体技术，电子教学、电子图书等全新的教学手段和技术日益为教育界认可并加以运用。这些技术的广泛应用，无疑将对校园的信息化进程和大力培育二十一世纪所需的各类人才，产生十分重要的、不可替代的作用。

在我国，近年来校园网建设发展迅速。为我国校园内部实现教育的资源共享、信息交流和协同工作提供了较好的范例。然而，随着我国各地校园网数量的迅速增加，校园网之间如何实现教育的资源共享、信息交流和协同工作的要求越来越强烈。

在第 1 章中，我们将了解什么是校园网络工程，设计校园网络的技术要求及网络工程的大致实施过程。

1.1　校园网络工程概述

1.1.1　网络系统设计概述

网络系统设计是针对具体用户所需网络中的所有软、硬件系统方案设计，从基础网络

拓扑结构、综合布线系统，到 Office 办公系统、文件打印系统，再到电子商务应用系统，最后到 Internet 应用和外网的互联，这一切都是网络系统设计需要解决的内容。

因为网络系统设计所需设计的项目非常多，涉及面非常广，这就涉及各具体项目之间的关联与综合考虑，在进行网络系统设计时需要考虑以下及几方面：

（1）当前系统应用及与之关联的其他系统的应用与互联；

（2）网络应用需求及网络安全需求；

（3）在未来一段时间内的应用需求发展；

（4）不仅要考虑到关键应用性能需求，还要尽可能平衡各用户节点的性能；

（5）不仅要考虑到高性能，还要追求高的性价比，这是一项综合的系统工程。

因此，在进行网络系统设计时一定要有全局观念，否则很可能设计出来的网络系统局部、甚至全部不能满足用户的需求。

另外，如今的网络应用不再仅局限于单一局域网中，许多关键性的应用通常是涉及多个局域网的互联（如通过 VPN 互联而实现的不同局域网系统数据库等），或者与其他外部网络的连接，如电子商务。在这样一个彼此关联的网络系统中，网络应用所需的带宽和安全需求就成了重中之重。而网络连接性能和安全性能则遵循着木桶原理，最终的性能不是取决于网络中最好的那部分，而是取决于最差的那部分。

通常的局域网系统设计包括：机房规划、基本网络拓扑结构、综合布线结构、IP 地址规划、域系统结构、各种网络服务器（如 DNS 服务器、DHCP 服务器、WINS 服务器等）部署、服务器选型（包括服务器档次、服务器架构、所支持的磁盘阵列级别等）、操作系统的选择、数据存储系统、数据备份与容灾系统、防火墙系统、病毒防护系统、入侵检测系统等。

对广域网系统设计要充分考虑的是：网络接入方式、网络中继传输方式和数据交换方式。在这些网络选型中一定要结合所支持的业务类型和成本综合考虑。另外，选择合适的 ISP（Internet 服务提供商）也是非常重要的。

以上这些局域网系统设计和广域网系统设计项目在具体实施前都需要建立在全面、详细的用户调查之上。这虽然是前期工作，但对于整个系统设计关系重大，稍有不慎就可能导致最终付出了高昂代价的系统不能满足用户需求，甚至产生与用户之间的矛盾。

1.1.2 网络系统设计的基本原则

根据目前计算机网络现状和需求分析以及未来的发展趋势，在网络设计时应遵循以下几个原则。

1．可用性

它决定了所设计的网络系统是否能满足用户应用和稳定运行的需求。网络系统的“可用性”通常是由网络设备的“可用性”决定的，主要体现在交换机、路由器、防火墙、服务器等重负荷设备上。这就要求在选购这些设备时不要一味地贪图廉价，而要选择一些国内、国际主流品牌，应用主流技术和成熟型号产品，以及拥有良好售后服务的产品。

2．实用性与先进性兼顾

在网络系统设计时应该以注重实用为原则，紧密结合具体应用的实际需求。考虑先进性不等于在网络系统中无原则地采用新技术和新设备，在选择具体的网络技术时一定要同时考虑当前及未来一段时间内主流应用的技术。

3．开放性和标准化

首先采用国家标准和国际标准，其次采用广为流行的、实用的工业标准，只有这样，网络系统内部才能方便地从外部网络快速获取信息。同时还要求在授权后网络内部的部分信息可以对外开放，保证网络系统适度的开放性。

4．安全性

如何保证网络运行和通信的安全是在网络设计中的重要问题。网络安全涉及许多方面，最明显、最重要的就是对外界入侵、攻击的检测与防护。现在的网络几乎时刻都要受到外界的安全威胁，稍有不慎就会被那些病毒、黑客入侵，致使整个网络陷入瘫痪。在一个安全措施完善的计算机网络中，不仅要部署病毒防护系统、防火墙隔离系统，还可能要部署入侵检测、木马查杀系统和物理隔离系统等。当然所选用系统的具体等级要根据相应网络规模大小和安全需求而定，并不一定要求每个网络系统都全面部署这些防护系统。
除了病毒、黑客入侵外，网络系统的安全性需求还体现在用户对数据的访问权限上，一定要根据对应的工作需求为不同用户、不同数据配置相应的访问权限，对安全级别需求较高的数据则要采取相应的加密措施。同时，用户账户，特别是高权限账户的安全也应受到高度重视，要采取相应的账户防护策略（如密码复杂性策略和账户锁定策略等），保护好用户账户，以防被非法用户盗取。

5．易扩展性

易扩展性是为了适应用户业务和网络规模发展的需求必须遵循的原则。网络的可扩展性保证主要是通过交换机端口、服务器处理器数、内存容量、磁盘数等方面来保证。通常要求核心交换机的高速端口要有两个以上用于维护和扩展（通常用来加连新增的下级交换机），在设计之初，不能只想到当前所需的这类端口数，把所有高速端口全部占用。在服务器的扩展性方面，要求所选的服务器支持“按需扩展”理念，就是可以在需要时随时扩展，而不用在购买时一次到位。服务器的可扩展性主要是通过其支持对称处理器数、内存最大容量、磁盘数等指标来决定。

6．可管理性

随着网络规模和复杂程度的增加，管理和故障排除就越来越困难。在网络设计中，我们将提供先进而完善的网络管理的软、硬件系统。 一个可管理的网络可以使管理员很方便地对网络进行监测、维护和升级。

7．高性价比

高性价比强调用尽可能少的资金来组建一个满足用户需求，高效、稳定、具备良好扩展性、易管理与维护的网络，也就是通常所说的“用最少的钱，办最多、最好的事”。

1.1.3 校园网络工程项目概述

校园网连接了包括教学楼、办公楼、实验楼、图书馆、学生宿舍楼、教职工生活区等大量的信息点，学校管理、教育科研、电子教学、远程教育和互联网的引入以及对外技术交流与合作服务等大量的业务，因此，要求校园网必须是一个实用的、高可靠、高效率、高扩展性、高安全性系统。下面我们以某校园网络工程为例，对该项目进行简要描述。

某大学两个校区有 17 栋教学楼，两栋办公楼，10 栋教工住宅楼。综合布线信息点约需 4000 个。学校部门按职能划分约 20 个，按公共机房划分约 40 个，按教工住宅楼划分约 10 个。为了提高系统的安全性，抑制广播风暴，方便网络构建和维护，合理配置信息资源，需要采用 VLAN（Virtual Local Area Network，虚拟局域网）技术。这样的 VLAN 约需 70 个。

校园网络分成核心层、汇聚层和接入层。核心层与汇聚层设备采用 1000Mbit/s 连接。网络系统设计采用三层体系架构，利用多层交换（包括二层交换和三层交换）网络技术（包括 VLAN 技术），实现核心层、汇聚层和接入层的构建及通信。

校区主干网以校园网络中心的机房为中心节点向外辐射，通过各部门（如信息学院、图书馆等）所在建筑楼宇节点构成主干网。中心节点中高档三层交换机作为主干网的核心交换机。

学校的新校区和本部之间距离大约 5km，考虑到传输距离以及信息的安全性，采用 VPN 使两校区互联。

从应用需求方面考虑，无线网络很适合学校的一些不易于网络布线或者需要变动布线结构的场所应用。一个无线网络可以使教师、学生在校园内的任何地方接入网络。因此我们在网络设计中考虑了有线网与无线网的融合。

各楼宇之间采用光缆进行连接，楼内垂直级水平布线采用超 5 类 UTP 电缆。

设备间采用 UPS 供电，并分别对弱电和强电设计防雷装置。

该校园网主干网络的拓扑结构如图 1.1 所示。

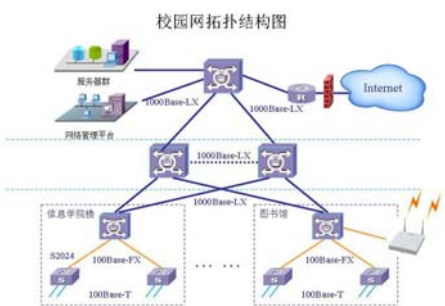

图 1.1 校园网主干网络拓扑图

1.2　项目主要技术要求及分析

为了实现网络设备的统一，本设计方案中采用同一厂家的网络产品，即华为公司的网络设备构建。全网使用同一厂商设备的好处是可以实现各种不同网络设备功能的互相配合和补充。

本校园网设计方案主要由以下几大部分构成：交换部分、广域网接入部分、访问控制部分、网络安全部分、服务器群。本书将详细论述交换部分、广域网接入部分、访问控制部分、网络安全部分，整个网络系统的拓扑结构图如图 1.1 所示。在后面的章节中我们将根据该图分块进行介绍。

1.2.1　OSI 参考模型与网络设备

在对校园网设计方案分析之前，先对 OSI 参考模型及主要网络设备作一个简单介绍。

1．OSI 参考模型

OSI（Open System Interconnection，开放式系统互联）参考模型是应用在局域网和广域网的一套普遍适用的规范集合，它说明了网络的架构体系和标准，对发生在网络设备间的信息传输过程进行理论化的描述。采用同一标准的层次化模型后，各设备生产商遵循标准进行设计开发，有效保证了产品之间的兼容性，使不同类型的主机实现数据的传输。国际标准化组织 ISO 将整个通信功能划分为七个层次，如图 1.2 所示。

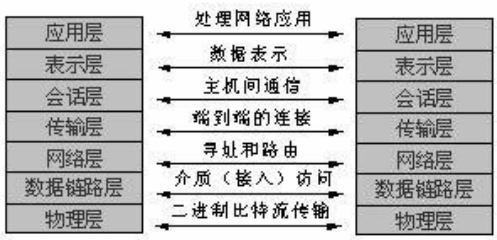

图 1.2　OSI 参考模型

（1）物理层

定义了数据传输所需要的机械、电气、功能及规程特性，包括对数据传输速率、接口、电压、电缆线的定义等。物理层涉及的是信道上传输的原始比特流。

（2）数据链路层

为网络层提供服务，并对物理层进行控制，检测并纠正可能出现的错误，为物理链路提供可靠的数据传输。数据传输单位是帧，以太网交换机是工作在数据链路层的设备。

（3）网络层

确定数据从远端到目的端如何选择路由，根据路由信息完成数据包报文的转发。数据传输单位是包，路由器是工作在网络层的设备。

（4）传输层

保证在不同子网的两台设备间的数据包可靠、顺序、正确地传输。传输层数据的传送

单位是段。

（5）表示层

利用传输层提供的端到端的服务，向表示层或会话用户提供服务。

（6）会话层

将应用层的信息表示成一种格式，对端设备能够正确识别。

（7）应用层

提供 OSI 用户服务，如文件传输、数据检索、文件管理、电子邮件等。

2．主要网络设备

常用的网络设备有网卡、交换机、集线器、路由器、防火墙、VPN 设备、光纤设备等。

（1）网卡

又称为网络适配器，它安装在可以接入网络的计算机上，通过传输介质与集线器或交换机相连，是将计算机接入局域网的必备设备。

（2）集线器与交换机

集线器的作用可以简单地理解为将一些机器连接起来组成一个局域网。所构成的网络物理上是星型的拓扑结构，集线器采用的工作方式是共享带宽，就是说如果网络中有 1000 台计算机，即使采用 100Mbps 的设备，每台计算机的带宽仅为 100Kbps，这样的性能是我们难以接受的。

集线器存在的缺陷是由共享带宽带来的，由于采用广播方式向所有节点发送数据，不能识别目的地址，降低了传输速率并且会带来安全隐患。交换机的产生解决了这些问题，在接收到数据包后，处理端口会查找内存中的 MAC 地址表来确定目的 MAC 的网卡挂接在哪个端口上，然后直接将数据包传送到目的节点，只有在目的 MAC 不存在时才广播到所有的端口。这种采用独享带宽的方式只对目的地址发送数据，传输效率高，不浪费网络资源，传输安全，发送数据时其他节点难以侦听到所发送的信息。因此交换机几乎已经完全取代了集线器。

（3）路由器

用于广域网之间的连接，可以把数据包从一个网络经过合理的路径选择转发到另一个网络。路由器是用来连接不同的网络和子网的，所以它出现在需要连接外部网络，或者在局域网中有多个子网，需要互联互通的网络环境中，在单纯的局域网、单一子网的环境中是不需要路由器的。

（4）三层交换机

三层交换机具有路由的功能，将 IP 地址信息用于网络路径选择，并实现不同网段之间的线速交换（能够按照网络通信线上的数据传输速度实现无瓶颈的数据交换）。当网络规模较大时，需要将网络划分为多个 VLAN，以提高安全性，减小广播风暴的产生。三层交换机用于大中型网络结构中的汇聚层和核心层的连接，通常三层交换机采用模块化结构，以适应不同配置的需要。

（5）防火墙

是用来保护内部网络或者内部网络中特定用户的，应用于需要外部网络连接或者需要

对局域网中某特定用户的网络环境中，在单纯局域网、且无特殊保护需要的网络中是不需要使用防火墙的。

（6）VPN 设备

用于在远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的安全连接，保证数据传输的安全性。

1.2.2　交换部分

1．VLAN 及 IP 地址规划

整个校园网中 VLAN 及 IP 编址方案见表 1.1。

表 1.1　VLAN 及 IP 编址方案

VLAN ID	VLAN NAME	网络地址	默认网关	说明
VLAN 1	guanli	172.16.0.0/24	172.16.0.254	管理 VLAN
VLAN 10	shuji	172.16.1.0/24	172.16.1.254	数计学院 VLAN
VLAN 20	sheke	172.16.2.0/24	172.16.2.254	社科系 VLAN
VLAN 30	jingguan	172.16.3.0/24	172.16.3.254	经管系 VLAN
VLAN 40	fuwuqi	172.16.4.0/27	172.16.4.254	服务器组 VLAN
VLAN 50	xinxi	172.16.5.0/24	172.16.5.254	信息学院 VLAN
VLAN 60	tushu	172.16.6.0/24	172.16.6.254	图书馆 VLAN
VLAN 70	renshi	172.16.7.0/24	172.16.7.254	人事处 VLAN
VLAN 80	jicai	172.16.8.0/24	172.16.8.254	计财处 VLAN

除表中的内容外，拨号用户从 172.16.100.0/24 中动态取得 IP 地址。

为了简单起见，这里我们只规划了 8 个 VLAN，同时为每个 VLAN 定义了一个由拼音缩写组成的 VLAN 名称。

2．配置接入层交换机

接入层交换机为终端用户提供接入服务。对接入层交换机端口基本参数的配置包括以下几个方面。

（1）根据实际业务需求合理划分 VLAN

伴随局域网的发展，用户对安全隔离以及广播报文泛滥问题解决的要求越来越迫切。以 802.1Q 标准为基础的 VLAN 技术正是为了解决这一问题而产生的。

VLAN 除了能将网络划分为多个广播域，从而有效地控制广播风暴的发生，使网络的拓扑结构变得非常灵活的优点外，还可以用于控制网络中不同部门、不同站点之间的访问。

（2）端口双工配置

以太网端口可以工作在全双工或者半双工状态下，通过接口视图下 duplex 命令，可以对以太网端口的双工状态进行设置。缺省情况下，以太网端口的双工状态为自协商（auto）状态，即自动与对端协商是工作在全双工状态还是半双工状态。在实际组网中与对端交换

机对接时，一般强制对方的端口都工作在全双工状态。

（3）端口速率配置

QuidwayS2024 系列交换机的 24 个 10BASE-T/100BASE-TX 端口可以支持 10Mbit/s 和 100Mbit/s 两种速率。缺省情况下，以太网端口的速率为 auto，即在实际组网时通过与所连接的对端自动协商确定本端的速率。

（4）端口类型配置

对于一台支持 802.1Q 标准的交换机来说，在端口上传送的数据帧需要进行区别对待，根据所传送数据的不同可以将链路分为 Trunk（干道链路）、Access（接入链路）、Hybrid（混杂模式）三种模式。

Trunk 链路用于连接支持 VLAN 技术的网络设备的端口，如交换机与交换机之间的连接。Trunk 端口接收到的数据帧一般都包含 VLAN 标签，在向外发送数据时，必须保证接收端能够区分不同的 VLAN 数据帧，所以每个数据帧都加入了一个 Tag 标识，只有当 Trunk 端口 VLAN ID 和数据帧的 VLAN ID 相同时才不会加入 Tag 标识。

Access 链路用于连接交换机与终端设备。该链路只能够传送某一特定的 VLAN 数据帧，并禁止携带 Tag 标识的数据帧通过。

Hybrid 链路用于某些特殊情况。即可以用于交换机与交换机之间的连接，也可以用于交换机与终端之间的连接。

在实际应用中，我们需要注意区分各种链路的使用条件，从而避免由于链路类型错误而导致的网络不通。

为了提高主干道的吞吐量，可以采用链路捆绑（快速以太网信道）技术增加可用带宽。例如，可以将接入层交换机的多个连续端口捆绑在一起实现快速以太网信道。

3．配置汇聚层交换机

汇聚层除了负责将接入层交换机进行汇集外，还为整个交换网络提供 VLAN 间的路由选择的功能。这里的汇聚层交换机采用的是 H3C S3528TP-EA 交换机。作为三层交换机，S3528TP-EA 交换机拥有 24 个 10Base-T/100Base-TX 以太网端口，同时还有两个千兆 SFP 端口，两个 10/100/1000MBase-T 以太网端口供上连使用，运行的软件系统是 Comware。

对汇聚层交换机的基本参数的配置方法与对接入层交换机的基本参数的配置类似。我们将在第 4 章给出具体的配置步骤。

（1）集群技术

当网络中交换机数量很多时，需要分别在每台交换机上创建很多重复的 VLAN，这样工作量很大、过程很繁琐，并且容易出错。因此，我们常采用集群技术来解决这个问题。

级联技术可以实现多台交换机之间的互联；堆叠技术可以将多台交换机组成一个单元，从而提更大的端口密度和更高的性能；集群技术可以将相互连接的多台交换机作为一个逻辑设备进行管理，从而大大降低了网络管理成本，简化管理操作。

集群技术就是将多台互相连接（级联或堆叠）的交换机作为一台逻辑设备进行管理。集群中，一般只有一台起管理作用的交换机，称为命令交换机，它可以管理若干台其他交换机。在网络中，这些交换机只需要占用一个 IP 地址（仅命令交换机需要），节约了宝贵

的 IP 地址。在命令交换机统一管理下，集群中多台交换机协同工作，大大降低管理强度。例如，管理员只需要通过命令交换机就可以对集群中所有交换机进行版本升级。

（2）汇聚层交换机功能配置

汇聚层交换机需要为网络中的各个 VLAN 提供路由功能。我们选用三层交换机作为汇聚层交换机。关于三层交换机的配置使用，我们将在第 7 章——局域网络互联一章中讲述。

此外，还需要定义通往 Internet 的路由。关于路由的具体配置，我们将在第 8 章——局域网络互通技术一章中详细讲述。

4．配置核心层交换机

核心层将各汇聚层交换机互联起来进行穿越园区网骨干的高速数据交换。

本实例中的核心层交换机采用的是 H3C S7502E 交换机。该产品基于 Comware V5 操作系统，主要基于 Web 界面进行管理。

对核心层交换机基本参数的配置步骤与对接入层交换机基本参数的配置类似。

核心层交换机通过端口同接入到 Internet 的路由器相连。因此，需要启用核心层交换机的路由功能。同时，还需要定义通往 Internet 的路由。如何配置路由协议呢？我们将在本书的第 8 章——局域网络间互通技术一章中详细论述。

1.2.3　广域网部分

在本设计中，接入广域网的功能是由路由器来完成的。除了完成主要的路由任务外，利用访问控制列表（Access Control List，ACL）和 QoS 技术，广域网接入路由器还可以完成以自身为中心的流量控制和过滤功能并实现一定的安全功能。

1．配置接入路由器的基本参数

对接入路由器的基本参数的配置步骤详见本书第 7 章——局域网络互联。

对接入路由器的各接口参数的配置主要是对局域网接口以及广域网接口的 IP 地址、子网掩码的配置。我们将在第 2 章详细讲述 IP 地址及子网掩码的使用及配置。

2．配置接入路由器

在接入路由器上需要考虑的问题包括：

（1）采用何种接入技术接入到广域网？

广域网连接可以采用不同类型的封装协议，如 HDLC、PPP、帧中继等。其中，PPP 除了提供身份认证功能外，还可以提供很多可选项配置，包括多链路捆绑、回叫等，因此更具优势，是本设计所采用的广域网协议。我们将在本书第 9 章——接入到广域网对各种接入技术及接入方式的配置进行详细讲述。

（2）定义两个方向上的路由。

即到校园网内部的静态路由以及到 Internet 上的缺省路由。

到 Internet 上的路由需要定义一条缺省路由。其中，下一跳指定从本路由器的接口 Serial 0/0 送出。关于路由协议的配置，我们将在本书的第 8 章——局域网络间互通技术一章中进

行详细论述。

（3）配置接入路由器上的 NAT

由于目前 IP 地址资源非常稀缺，不可能给校园网内部的所有工作站都分配一个公有 IP（Internet 可路由的）地址。为了解决所有工作站访问 Internet 的需要，必须使用 NAT（网络地址转换）技术。

为了接入 Internet，本校园网向当地 ISP 申请了四个 IP 地址。其中一个 IP 地址 202.97.38.57 被分配给了 Internet 接入路由器的串行接口，另外三个 IP 地址 202.206.22.1～202.206.22.3 用作 NAT。关于 NAT 技术将在第 9 章——接入到广域网部分详细介绍。

1.2.4 访问控制部分

1．配置接入路由器上的 ACL

路由器是外网进入校园网内网的第一道关卡，是网络防御的前沿阵地。路由器上的访问控制列表（Access Control List，ACL）是保护内网安全的有效手段。一个设计良好的访问控制列表不仅可以起到控制网络流量、流向的作用，还可以在不增加网络系统软、硬件投资的情况下完成一般软、硬件防火墙产品的功能。由于路由器介于企业内网和外网之间，是外网与内网进行通信时的第一道屏障，所以即使在网络系统安装了防火墙产品后，仍然有必要对路由器的访问控制列表进行缜密的设计，来对企业内网实施保护。

在本实例中，我们将针对服务器以及内网工作站的安全给出广域网接入路由器上 ACL 的配置方案。

2．配置接入路由器上的 QoS

传统网络所面临的服务质量问题，主要是由网络拥塞引起的。

虽然增加网络带宽是解决资源不足的一个直接途径，但是它并不能解决所有导致网络拥塞的问题。解决网络拥塞问题的一个更有效的办法是在网络中增加流量控制和资源分配的功能，为有不同服务需求的业务提供有区别的服务，正确地分配和使用资源。在进行资源分配和流量控制的过程中，尽可能地控制好那些可能引发网络拥塞的直接或间接因素，减少拥塞发生的概率；在拥塞发生时，依据业务的性质及其需求特性权衡资源的分配，将拥塞对 QoS 的影响减到最小。关于 ACL 和 QoS 技术我们将在本书第 10 章——接入控制与管理一章中讲述。

1.2.5 网络安全部分

1．防火墙技术

防火墙是校园网信息安全保障的核心点，它负责校园网中最基本的信息服务系统的安全，一旦被非法进入，就存在着内容被窃取、泄密、篡改、损坏等巨大风险，属于安全等级中最严重的事件。通过部署防火墙，把这些信息系统集中隔离到一个逻辑安全区中，在防火墙集中控制点处定制严格的访问控制策略，实施严格的数据流监控。

防火墙的安全性源于其强大的访问控制能力，可做到基于 IP、协议、用户的访问控制，