全国高等职业教育规划教材 信息安全系列

网络安全系统集成与建设

唐乾林 主编

电子课件下载
www.cmpedu.com

机械工业出版社
CHINA MACHINE PRESS

全国高等职业教育规划教材·信息安全系列

网络安全系统集成与建设

主　编　唐乾林
副主编　赵　怡　田淋风
参　编　刘　涛　胡　云　李治国

机械工业出版社

本书以一个真实的校园网为案例，介绍网络安全系统集成与建设的工作过程。主要包括网络安全系统集成与建设的方案设计、综合布线、交换机的基本配置与安全配置、路由器的基本配置与安全配置、常见服务器的安装与安全配置、主流安全产品的配置与应用、系统集成工程项目管理等内容。

本书适合高等院校计算机科学与技术、信息安全、网络工程等专业的学生使用，也适合作为系统集成培训的教材和网络工程技术人员的工具书。

本书配套授课电子课件，需要的教师可登录 www. cmpedu. com 免费注册、审核通过后下载，或联系编辑索取（QQ：81922385，电话：010 - 88379739）。

图书在版编目(CIP)数据

网络安全系统集成与建设/唐乾林主编. —北京：机械工业出版社，2010. 8
全国高等职业教育规划教材. 信息安全系列
ISBN 978 - 7 - 111 - 31518 - 6

Ⅰ. ①网… Ⅱ. ①唐… Ⅲ. ①计算机网络—安全技术—高等学校：技术学校—教材 Ⅳ. ①TP393. 08

中国版本图书馆 CIP 数据核字（2010）第 152490 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)
责任编辑：鹿 征 马 超
责任印制：杨 曦
北京蓝海印刷有限公司印刷
2010 年 9 月第 1 版 · 第 1 次印刷
184mm × 260mm · 12. 75 印张 · 310 千字
0001— 3000 册
标准书号：ISBN 978 - 7 - 111 - 31518 - 6
定价：23. 00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务	网络服务
社服务中心：(010)88361066	门户网：http://www. cmpbook. com
销 售 一 部：(010)68326294	教材网：http://www. cmpedu. com
销 售 二 部：(010)88379649	封面无防伪标均为盗版
读者服务部：(010)68993821	

全国高等职业教育规划教材
计算机专业编委会成员名单

主　　任　周智文

副 主 任　周岳山　林　东　王协瑞　张福强
　　陶书中　龚小勇　王　泰　李宏达
　　赵佩华　陈　晴

委　　员　（按姓氏笔画排序）
　　马　伟　马林艺　卫振林　万雅静
　　王兴宝　王德年　尹敬齐　卢　英
　　史宝会　宁　蒙　刘本军　刘新强
　　刘瑞新　余先锋　张洪斌　张　超
　　杨　莉　陈　宁　汪赵强　赵国玲
　　赵增敏　贾永江　陶　洪　康桂花
　　曹　毅　眭碧霞　鲁　辉　裴有柱

秘 书 长　胡毓坚

出 版 说 明

根据《教育部关于以就业为导向深化高等职业教育改革的若干意见》中提出的高等职业院校必须把培养学生动手能力、实践能力和可持续发展能力放在突出的地位，促进学生技能的培养，以及教材内容要紧密结合生产实际，并注意及时跟踪先进技术的发展等指导精神，机械工业出版社组织全国近60所高等职业院校的骨干教师对在2001年出版的“面向21世纪高职高专系列教材”进行了全面的修订和增补，并更名为“全国高等职业教育规划教材”。

本系列教材是由高职高专计算机专业、电子技术专业和机电专业教材编委会分别会同各高职高专院校的一线骨干教师，针对相关专业的课程设置，融合教学中的实践经验，同时吸收高等职业教育改革的成果而编写完成的，具有“定位准确、注重能力、内容创新、结构合理和叙述通俗”的编写特色。在几年的教学实践中，本系列教材获得了较高的评价，并有多个品种被评为普通高等教育“十一五”国家级规划教材。在修订和增补过程中，除了保持原有特色外，针对课程的不同性质采取了不同的优化措施。其中，核心基础课的教材在保持扎实的理论基础的同时，增加实训和习题；实践性较强的课程强调理论与实训紧密结合；涉及实用技术的课程则在教材中引入了最新的知识、技术、工艺和方法。同时，根据实际教学的需要对部分课程进行了整合。

归纳起来，本系列教材具有以下特点：

1）围绕培养学生的职业技能这条主线来设计教材的结构、内容和形式。

2）合理安排基础知识和实践知识的比例。基础知识以“必需、够用”为度，强调专业技术应用能力的训练，适当增加实训环节。

3）符合高职学生的学习特点和认知规律。对基本理论和方法的论述要容易理解、清晰简洁，多用图表来表达信息；增加相关技术在生产中的应用实例，引导学生主动学习。

4）教材内容紧随技术和经济的发展而更新，及时将新知识、新技术、新工艺和新案例等引入教材。同时注重吸收最新的教学理念，并积极支持新专业的教材建设。

5）注重立体化教材建设。通过主教材、电子教案、配套素材光盘、实训指导和习题解答等教学资源的有机结合，提高教学服务水平，为高素质技能型人才的培养创造良好的条件。

由于我国高等职业教育改革和发展的速度很快，加之我们的水平和经验有限，因此在教材的编写和出版过程中难免出现问题和错误。我们恳请使用这套教材的师生及时向我们反馈质量信息，以利于我们今后不断提高教材的出版质量，为广大师生提供更多、更适用的教材。

机械工业出版社

此为试读，需要完整PDF请访问：www.ertongbook.com

前　言

本书根据职业能力培养的要求，在编写过程中提出“基于工作过程，基于真实的工作案例”的实践教学理念。全书以一个真实的校园网建设项目作为主线，介绍了网络安全系统集成分析与方案设计、综合布线、交换机的基本配置与安全配置、路由器的基本配置与安全配置、常见服务器的安装与安全配置、主流安全产品的配置和应用、系统集成工程项目管理等内容。

本书内容侧重于网络安全系统集成的方案设计以及交换机、路由器、服务器、主流安全产品的安全配置，强调了网络安全系统集成与建设项目的工作过程及项目管理。

通过本书的学习，读者应达到以下的职业能力目标：

1）会设计：学会根据不同的企业、不同的预算设计出符合企业要求的方案。

2）会配置：学会交换机、路由器和主流安全产品的配置。

3）会集成：学会各种软件、常见服务器、各种网络设备的集成方法。

4）会管理：学会整个安全系统、项目的管理方法。

本书由重庆电子工程职业学院唐乾林任主编，赵怡、田淋风任副主编。参加编写的还有刘涛、胡云、李治国。全书统稿、定稿由唐乾林完成。在编写本书的过程中，作者参阅了一些文献资料，在此向这些作品的作者表示衷心的感谢！

由于编者水平有限，书中不妥或错误之处在所难免，恳请广大读者批评指正。

编　者

目　录

第1章　网络安全系统集成分析与方案设计

网络安全系统集成就是根据客户的应用需求和投入资金的规模，综合应用计算机网络、计算机安全等相关技术，适当选择软硬件设备，经过专业人员的集成设计，安装调试与维护，应用开发等大量技术性工作和相应的管理性及商务性工作，使集成后的系统能够满足客户对实际工作的要求，具有良好的性能、适当的价格和强健的安全策略的计算机网络系统的全过程。

网络安全系统集成有以下几个显著特点。

1）网络安全系统集成要以满足客户的需求为根本出发点。

2）网络安全系统集成不是选择最好的产品的简单行为，而是要选择最适合客户的需求和投资规模的产品和技术。

3）网络安全系统集成不是简单的设备供货，体现得更多的是设计、调试与开发，是技术含量很高的行为。

4）网络安全系统集成涉及技术、管理和商务等方面，是一项综合性的系统工程。技术是安全系统集成工作的核心，管理和商务活动是系统集成项目成功实施的可靠保障。

总之，网络安全系统集成是一种商业行为，也是一种管理行为，其本质是一种技术行为。

1.1　任务一　需求分析

一个企业或单位的网络安全系统集成与建设项目的方案是建立在各种各样的需求之上的。这些需求来自客户的实际需求。由于一般客户对网络安全系统集成与建设的理解和需求是不同的，所以，对客户需求的理解，在很大程度上决定了项目的成败。

如何通过了解、分析、明确客户的需求，并且能够准确、清晰地以文档的形式表达出来，提供给项目实施的每个成员，保证实施过程按照满足客户需求的目的正确进行，是每个网络安全系统集成项目管理者需要面对的问题。

1.1.1　系统需求分析

在客户需求分析中，首先要确定网络安全系统集成项目的目标。目标通常应该由专业人士和客户共同讨论确定。在目标中应该明确设计的是一个新的网络安全集成系统，还是一个现有网络安全集成系统的改造。下面就以某职业学院的需求为例，来设计一个网络安全系统集成与建设的方案。

1）学院的网络覆盖情况：18 幢楼宇约 8100 个信息点。其中 1 幢办公楼 500 个信息点，3 幢教学楼 600 个信息点，3 幢教师宿舍楼 600 个信息点，7 幢学生宿舍楼 6000 个信息点，1 幢实验楼 200 个信息点，1 幢图书馆大楼 100 个信息点，2 个食堂 100 个信息点。

2）综合布线：网络运行的基础是通信设施。在现有的通信条件下，楼群之间、楼内各

室之间计算机网络线路的敷设、修改和维护，经常要消耗网络管理人员大量的时间与精力，并有可能会浪费器材和施工资金，影响信息工程的建设和发展。结构化布线系统可以解决上述问题。作为一项半永久性的基础设施，结构化布线系统主要采用光纤和双绞线形成楼宇之间和楼宇内的通信线路系统，支持语音、数据和视频的综合信息传输。结构化布线系统的优点是技术先进，适于今后长期发展，网络安装和维护工作简单方便，线路系统灵活性好，长期投资效益高。

由于校园比较大，建筑物多、布局比较分散，因此，在设计校园网主干结构时既要考虑到目前实际应用的侧重点，又要兼顾未来的发展需求。主干网以网络中心机房为中心，设几个主干交换结点，包括网络中心机房、实验楼、图书馆、教学楼、宿舍楼。中心交换机和主干交换机采用千兆光纤交换机。网络中心机房与教学楼、实验楼、图书馆、宿舍楼等之间全部采用8芯室外光缆；楼内选用进口6芯室内光缆和5类线。

3）服务器的配置要根据学院的实际应用。

目前的网络应用中，要使用各种各样的服务器。Internet上使用的服务器包括代理服务器、WWW服务器、E－mail服务器、DNS服务器；信息管理系统和办公自动化使用的服务器，包括OA服务器以及为整个校园应用服务的数据库服务器、文件服务器等。

以上服务器是从逻辑上划分的，并不一定要求每一种逻辑服务器对应一台物理上的服务器级的主机。具体要采用多少台主机，要根据实际情况决定。根据学院的具体要求，大致可以分为3类服务器，它们分别为Web服务器、数据/数据库服务器、视频服务器。

主机系统可以有3大类选择，分别为大型机系统、小型机系统和PC服务器系统。采用大型机系统的做法，在历史上曾经流行过，这主要是因为当时的应用系统所要求的处理能力只有大型机能够提供。另外，那时候的终端的处理能力很有限，并且价格很贵，同时虽然大型机的处理能力可以满足应用的需要，但是价格更加昂贵。为了节省成本，只好采用有足够处理能力的大型机加基本没有处理能力的终端这种方式。随着大规模集成电路和计算机技术的发展，小型机、PC服务器的性能有了极大的提高，大型机逐渐失去了它的优势。

小型机系统是处于大型机和PC服务器之间的一种选择。通常，小型机的性能可以很高，甚至可以接近大型机的水平。小型机的CPU通常采用RISC（Reduced Instruction Set Computer，精简指令集计算机）技术，程序执行效率较采用CISC（Complex Instruction Set Computer，复杂指令集计算机）技术的机器有极大的提高。小型机的可靠性较PC服务器高，因为小型机的元器件大多经过严格筛选和优化；另外小型机通常有与之相配套的操作系统，且大多是UNIX操作系统。可以选择使用的小型机有HP－9000、IBM RS－6000等。

PC服务器的性能跟小型机大致相当，之所以称其为PC服务器，通常认为PC服务器是采用Wintel体系结构的，即采用Intel的CPU和微软的Windows操作系统。因为Intel和微软都是大规模生产，所以这种组合的价格非常具有竞争力，是大多数用户的选择。

本例建议采用PC服务器作为应用系统的硬件平台。在这里，可以选择IBM的服务器，即选择两台NF5100分别用于Web服务器和数据/数据库服务器，另外选择一台NF7100用于视频服务器。

服务器的具体配置见表1-1。

此为试读，需要完整PDF请访问：www.ertongbook.com

表 1-1　服务器的配置

设备名称	配置型号	数量	单位
主服务器	8658 - 41Y NF5100 PIII866 MHz, 128 MB, 36 GB/10000 转 SCSI, CD - ROM, 网卡, 15in	1	台
Web 服务器	8658 - 41Y NF5100 PIII866 MHz, 128 MB, 36 GB/10000 转 SCSI, CD - ROM, 网卡, 15in	1	台
数据/数据库服务器	8658 - 51Y NF5100 PIII933 MHz, 128 MB, 1 × 72 GB/10000 转 SCSI, CD - ROM, 网卡, 15in	1	台
视频服务器	8666 - 31Y NF7100 PIII/Xeon700 MHz/1 MB, 256 MB, 3 × 72 GB/10000 转 SCSI, CD - ROM, 15in	1	台
千兆网卡	3C985 - Sx	4	块
软件防火墙	天网防火墙（网络版）	1	套

其中主服务器装有 Windows 操作系统，负责整个校园网的管理，尤其是教育资源的管理。其中一台服务器装有 DNS，负责整个校园网中各个域名的解析，另一台服务器装有电子邮件（E - mail）系统，负责整个校园网中各个客户的邮件管理。

Web 服务器装有 Windows 2003 操作系统，负责远程服务管理及 Web 站点的管理。Web 服务器采用现在比较流行的 IIS 服务器，使用 ASP. NET 语言进行开发，连接 SQL Server 数据库，形成了较完整的动态网站。

4）学院网络建设的目标如下。

- 主干网络提供 1000Mbit/s 带宽，到桌面提供 100Mbit/s 带宽，共连接 18 幢楼宇，可以实现学院内互连，为学院各部门子系统提供校园主干网的接口，从而实现各网段内、各网段之间计算机互访和校内资源共享。
- 实现与 Internet 相连，局域网内的计算机通过 Web 服务器代理上网。
- 核心内部网络建设，包括各种服务器的建设。这些服务器对外能与 Internet 互连，对内提供校内各种局域网的接口，提供 Internet 的服务有电子邮件、远程登录、文件传输、信息查询等。

在充分考虑学院未来的应用后，整个校园的信息节点设计为 9000 个左右，交换机总数约 50 台左右，其中主干交换机 5 台，配有千兆光纤接口，最终建设成一个以办公自动化、计算机辅助教学、现代计算机校园文化为核心，以现代网络技术为依托，技术先进、扩展性强、能覆盖全校主要楼宇的校园主干网络，同时要将学校的各种工作站、终端设备和局域网连接起来，并与有关广域网相连，以便在网络上宣传自己和获取 Internet 上的教育资源。这不仅需要形成结构合理、内外沟通的校园计算机网络系统，在此基础上还要建立能够满足教学、科研和管理工作等需要的软硬件环境，同时开发各类信息库和应用系统，为学校各类人员提供不同的网络信息服务。系统总体设计将本着总体规划、分步实施的原则，充分体现系统的技术先进性、安全可靠性、开放性和可扩展性。

1.1.2　安全需求分析

目前，校园内部网络可能受到的威胁包括黑客入侵、内部信息泄漏和不良信息进入内网等。因此，采取的网络安全措施既要保证学院办公系统和网络的稳定运行，又要保护运行在

内部网上的敏感数据与信息的安全。归结起来，应充分保证以下几点。

1）网络可用性：网络是学院管理系统的载体，需防止对内部网络设施的入侵和攻击、防止通过消耗带宽等方式破坏网络的可用性，在某部分系统出现问题的时候，不影响学院网络系统的正常运行，具有很强的可用性和及时恢复性。

2）业务系统的可用性：学院内部的各主机及各种应用服务器系统的安全运行同样十分关键，网络安全体系必须保证这些系统不会遭受来自网络的非法访问、恶意入侵和破坏。

3）数据的安全性：对于学院的内部网络，网络安全系统应保证内网机密信息在存储与传输时的保密性。全面有效地保护学院网络系统的安全，保护计算机硬件、软件、数据、网络不因偶然或恶意破坏遭到更改、泄漏和丢失，确保数据的完整性和安全性。

4）访问的可控性：对关键网络、系统和数据的访问必须得到有效的控制，这要求系统能够可靠地确认访问者的身份，谨慎授权，并对任何访问进行跟踪记录。

5）网络操作的可管理性：网络安全系统应具备审记和日志功能，对相关重要操作提供可靠而方便的管理和维护功能。

6）全方位杜绝不健康信息在校园网上的出现，杜绝校园内部互联网不良信息的传播，净化校园内部网络环境，这要求网络具有较强的管理功能，使管理员能够对出现的问题及时发现、及时处理、防止扩散，在学生未受影响之前进行消除。

7）所采用的安全设备和技术应具有我国安全产品管理部门的合法认证，产品的运行和维护要简单，运行费用要低廉。

8）有效地提高计算机和网络使用的效率，同时对学生起到有效的督促作用，保证学生不会因为使用网络而有意或无意地浏览一些有黄、毒内容的网站。

9）能够保证在校园内部对网络犯罪或破坏活动进行日志跟踪，能够防止学生利用网络从事犯罪活动。

10）对学生的网络访问进行管理，并对信息进行记录存储，对符合教育要求的网络教育资源进行组织。

11）减轻网络管理员在学生上网时的监管压力，同时提高监管的效率，能够既满足校园自身管理的需要，又满足公安管理部门对公共网络监控管理的需要。

1.2 任务二 系统的总体方案设计

1.2.1 网络安全集成系统设计的原则

随着现代计算机技术的高速发展，特别是诸如图形、语音、视频等多媒体信息和技术在信息管理系统、科研设计等领域的广泛应用，为网络平台的设计提出了更高的要求。为了更好地满足用户的需求，保证系统能正常稳定运行，且在较长的时间内不落后，所以在网络系统方案设计中，应当把握以下几个原则。

（1）稳定性

只有运行稳定的网络才是可靠的网络，而网络的可靠运行取决于诸多因素，如网络的设计和产品的可靠性，同时，选择一个对此类规模的网络有一定运营经验的网络合作厂商尤为重要。另外，稳定的网络还要求有物理层、数据链路层和网络层的备份技术。

（2）高带宽

为了支持数据和语音、视频等多媒体信息的传输能力，同时在技术上要达到目前的国际先进水平，因此要采用最先进的网络技术，这样不仅可以适应大量数据和多媒体信息的传输，又可以满足目前的业务需求，同时又充分考虑了未来的发展。为此，应选用具有高带宽的先进的网络技术。

（3）先进性

网络硬件和软件平台的先进性体现在如何选择性价比好的硬件和软件并通过先进的网络技术进行组网，以保证系统的基础环境在未来一段时间内不落后。

（4）标准性和开放性

选择具有统一性的网络结构与软硬件平台，有利于系统的建立与开发。制定信息管理的规范，即组织有关人员对信息管理系统进行系统分析，制定数据流图和数据结构，为信息管理系统的开发奠定基础。为了实现与各种网络的互访，要选择开放的网络体系结构，即既要选择目前的主流产品，又要具有开放性，以便于以后的扩充。

（5）可扩展性

系统要有可扩展性和可升级性，随着业务的增长和应用水平的提高，网络中的数据和信息流将按指数增长，需要网络有很好的可扩展性，并能随着技术的发展而不断升级。可扩展不仅仅指设备端口的扩展，还指网络结构的易扩展性，即只有在网络结构设计合理的情况下，新的网络结点才能方便地加入已有网络；网络协议的可扩展性指无论是选择第三层网络路由协议，还是规划第二层虚拟网的划分，都应注意其扩展能力。

（6）容易控制和管理

因为上网用户很多，如何管理好他们的通信，做到既保证一定的用户通信质量，又合理地利用网络资源，这是建设好一个网络后所面临的首要问题。

（7）经济性

充分利用原有的软件、硬件资源，减少投资浪费，使系统具有很高的性价比。

（8）安全性

网络系统应具有良好的安全性，以保证数据的安全及网络使用的安全。同时应支持VLAN的划分，并能在VLAN之间进行第三层交换时同时进行有效的安全控制，以保证系统的安全。

（9）符合IP发展趋势的网络

在目前任何一个提供服务的网络中，对IP的支持服务是最普遍的，而IP技术本身又处在发展变化中，如IPv6，IP QoS，IP over SONET等新兴的技术不断出现，校园网络也必须紧跟IP发展的步伐，也就是说尽量选择IP发展处于领先地位的网络厂商。

1.2.2 网络安全集成系统的拓扑设计

计算机网络的拓扑结构是把网络系统的连接形式，用相对简单的拓扑图形式画出来，特别是计算机分布的位置以及电缆如何连接它们。设计一个网络的时候，应根据自己的实际情况选择正确的拓扑结构，常用的有：星形（广泛用于局域网）、环形（广泛用于光纤网）、总线型（早期局域网）、树形、网状形（用于复杂网络）。

在选择一种物理拓扑结构时，主要应考虑以下几个因素：安装的相对难易程度、重新配

置的难易程度、维护的相对难易程度、传输媒介发生故障时对设备的影响程度。

某学院校园网络主干采用基于树形的多星形结构，使之具有链路冗余特性，能使结构中有一线路出现故障时，只有本线路出故障，而其他部分仍然能正常运行。

最后根据需求画出网络拓扑图，如图 1-1 所示。

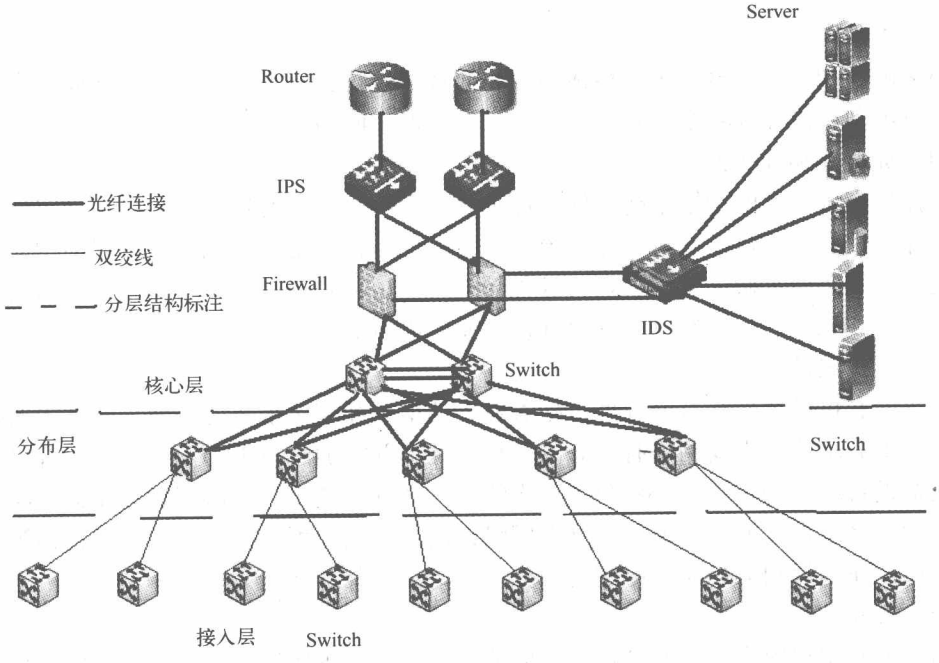

图 1-1　某学院校园网设计方案的拓扑图

网络设备制造商为网络拓扑结构的设计提出了经典的 3 层模型。3 层模型允许在 3 个连续的路由或交换层次上实现流量汇聚和过滤，这使得 3 层模型的规模可以扩大到大型国际互联网络。

网络分层设计的优点如下。

① 可扩展性：因为网络可模块化增长而不会遇到问题。

② 简单性：通过将网络分成许多小单元，降低了网络的整体复杂性，使故障排除更容易，同时能隔离广播风暴、防止路由循环。

③ 设计的灵活性：使网络容易升级到最新的技术，同时升级任意层次的网络不会对其他层次造成影响，无须改变整个环境。

④ 可管理性：层次结构使单个设备的配置的复杂性大大降低，这样更容易管理。

一个典型的网络三级拓扑结构是：由具有可用性和经过性能优化的高端路由器和交换机组成的核心层；由用于实现策略的路由器和交换机构成的汇聚层（分布层）；由用以连接用户的地段交换机和无线接入点构成的接入层。

1.2.3　网络设备选型

提供网络设备产品的厂家有很多，主要的生产厂家有 Cisco、Nortel Networks、3Com、Lucent（该公司提供网络设备的部门现已独立出来并成立 AVAYA 公司）、Alcatel、Cable-

tron、Intel、华为、联想、中兴等。

在本设计方案中选择的主要设备如下。

1. 交换设备

1）核心交换机：选择支持路由功能、带千兆光纤接口的可网管型交换机。

2）汇聚交换机（楼宇交换机）：可选择思科（Cisco）的带1000Mbit/s光接口的交换机。

3）接入交换机：普通交换机。可选择思科（Cisco）、华为、清华同方等厂家的产品。

2. 路由器

选用Cisco 2851，参数见表1-2。

表1-2 Cisco 2851路由器参数表

基本特征	
路由器类型	多业务路由器
端口结构	模块化
传输速率	10/100/1000 Mbit/s
内置防火墙	是
固定的局域网接口	2个
重量	11.4kg
网络管理	网络管理协议 Cisco ClickStart 与 SNMP
内存	最大1024MB
网络协议	IEEE 802.3X
其他端口	控制端口（Console）
扩展模块	4
尺寸	416.6mm×438.2mm×88.9mm
电源	AC 100～240V，47～63Hz
QoS	支持
VPN	支持
适用环境	工作温度：0～40℃，工作湿度：5%～95%、无凝结，存储温度：-20～65℃，存储湿度：5%～95%、无凝结

3. 安全产品选择

网络系统安全防范是通过安全技术、安全产品集成及安全管理来实现的。其中安全产品的集成就涉及如何选择网络安全产品，在进行网络安全产品选型时，应该要求网络安全产品满足两方面的要求：一是安全产品必须符合国家有关安全管理部门的政策要求；二是安全产品的功能与性能要求。

（1）政策要求

满足国家管理部门的政策性方面要求，针对相关的安全产品必须查看其是否得到相应的许可证，举例如下。

1）密码产品要满足国家密码管理委员会的要求。

2）安全产品应获得国家公安部颁发的销售许可证。

3）安全产品应获得中国信息安全产品测评认证中心的测评认证。

（2）安全产品的选型原则

安全产品的选择必须考虑产品的功能、性能、运行稳定性以及扩展性，并且还必须考查其自身的安全性。

1）防火墙。

选用天融信网络卫士防火墙系统。

防火墙 4000 - UF 采用 6Gbit/s 的系统数据总线结构，并通过使用大量独创性专利技术，构造了一个安全、高效、可靠、应用广泛、方便灵活的防火墙系统；同时为客户提供最优秀的性能及功能保证。

2）入侵检测系统。

选用天融信的网络卫士入侵检测系统。

网络卫士入侵检测系统部署于网络中的关键点，实时监控各种数据报文及网络行为，提供及时的报警及响应机制。其动态的安全响应体系与防火墙、路由器等静态的安全体系形成强大的协防体系，大大增强了用户的整体安全防护强度。网络卫士入侵检测系统是基于网络的入侵检测系统，它通过提供对付 Internet 或其他网络上的潜在攻击企图的方案及详细信息，来提供一个全面的策略，以增强企业网络的安全性。

网络卫士入侵检测系统检测网络上的入侵并做出响应，但不会降低网络速度。此外，为了支持复杂网络环境，它采用了控制中心、引擎分离的分布式构架，并可通过管理中心提供综合安全性管理功能。

网络卫士入侵检测系统提供了入侵检测、流量统计、入侵响应、入侵报表、协议还原等各种功能。

3）入侵防御系统。

选用天融信的网络卫士入侵防御系统。网络卫士入侵防御系统（Topsec Intrusion Detection and Prevention，TopIDP）是基于新一代并行处理技术开发的网络入侵防御系统，它通过设置检测与阻断策略对流经 TopIDP 的网络流量进行分析过滤，并对异常及可疑流量进行积极阻断，同时向管理员通报攻击信息，从而提供对网络系统内部资源的安全保护。TopIDP 能够阻断各种非法攻击行为，如利用薄弱点进行的直接攻击和增加网络流量负荷造成网络环境恶化的 DoS 攻击等，能够安全地保护内部资源。

1.2.4 路由交换设计

在校园网络安全系统集成的设计和建设中，交换机和路由器是使用最多的设备，是构建整个网络安全系统集成项目的基本设备。

交换机根据每一个数据包中的目的 MAC 地址做简单的转发，转发决策并不需要判断数据包内详细的其他信息。交换机能以非常低的延迟转发数据包，具有比桥接的网络更接近于单一局域网段的性能。交换机把网络分段成更小的冲突域，为每个终端站点提供更高的平均带宽。

路由器通过相互连接的网络把信息从源端移动到目的端，一般来说，在路由过程中，信息会经过一个或多个中间结点。在普通的用户看来，交换机和路由器所实现的功能是完全一样的，但是交换机和路由器有所不同，它们的主要区别就是交换机工作在 OSI 参考模型的第 2 层（数据链路层），而路由器工作在在第 3 层（网络层）。

此为试读，需要完整PDF请访问：www.ertongbook.com