

网络工程系统应用

——教育城域网设计

摘要：随着信息技术的飞速发展，我国教育行业的信息化建设也更加深入的展开。教育城域网的建设成为该“校校通”工程的重点，同时，教育城域网也成为实现远程教学、多媒体教学及教学资源共享的关键。目前国内许多城市的教育城域网已经快速发展起来，本文应用高性能网络系统集成技术，对教育城域网系统的结构、系统集成、功能特点进行全面系统的分析和设计，最终得出符合地/市教育信息化发展需求的教育城域网解决方案。

首先，本文介绍了教育城域网的发展，并对地/市教育城域网工程做了需求分析。

然后，对整个工程做了总体设计，并依据教育城域网系统的技术模型，按照网络通讯平台、网络资源平台、网络安全与管理平台、网络应用平台和设备的选型的顺序展开讨论。

在网络通讯平台的设计中，重点确定了网络结构和功能的设计，介绍了 VPN 技术构建教育城域网的原理和方法以及 IP 地址分配和网络接入的技术和方法。

在网络资源平台的设计中，运用网络服务器、网络存储和网络备份系统的最新技术，构建了以 B/S 服务器体系结构和以 SAN 存储网络技术、服务器群集技术为基础的网络资源平台。

在网络安全与管理平台的设计中，根据教育城域网用户数量多、覆盖范围大的特点，运用网络安全与管理的最新技术，创建以防火墙与 IDS 联动技术为的网络安全和网络管理方案。

在网络应用平台的设计中，介绍了教育信息网、教育管理中心、教育资源中心、远程教育中心和城域网管理和服务中心等应用模块的结构和功能。

在设备的选型中，介绍了主要设备的技术参数。

最后，对本论文进行总结性评估，并提出了今后进一步完善的设想。

关键词：教育城域网；网络存储；VPN；教育信息；远程教育；网络安全。

Network engineering applications

——EMAN design education

Abstract:With the rapid development of information technology, education in China's information industry is also more in-depth start, MAN education is the focus of the "Xiao Xiao tong" project, At the same time, education has become MAN achieve distance learning, multimedia teaching and learning resources to share the key, Many cities now MAN education has developed rapidly, In this paper, high-performance network systems integration technology, MAN education system to the structure, systems integration, features a comprehensive systems analysis and design, with the final draw / Municipal Education Information development needs of education MAN solution.

First of all, this paper, the development of education MAN, and / municipal engineering education MAN done a needs analysis.

Then, on the whole project done a design, based on education MAN system and technical model, According to network communications platform, platform network resources, network security and management platforms, network application platform and equipment to discuss the order of selection.

In the design of network communications platform, Focus on determining the structure and function of network design, Construction on the VPN technology education MAN principles and methods of distribution and IP addresses and network access technology and methods.

In the design of network resources platform, Use of network servers, network storage and backup systems to the latest network technology, Construction of a B / S server architecture and SAN storage networking technology, server clustering technology-based platform for network resources.

In the design of network security and management platform, According to the MAN number of users, coverage of the major characteristics of network security and management use the latest technology to create a firewall and IDS technology linked to the network security and network management solutions

In the design of network application platform, On the education information network, the management center, education resource centre, tele-education centres and MAN management and service centre application modules such as the structure and function.

Selection of the equipment, introduced the main equipment of the technical parameters.

Finally, the summary of this paper, and to put forward the idea of the future to further improve.

MAN education, network storage, VPN, education, distance education, network security.

Keywords:MAN education, network storage, VPN, Education Information, distance education, network security

目 录

1. 绪论	1
1.1 背景	1
1.2 作用和目标	1
1.3 用户需求	2
1.4 设计需求	3
2. 网络总体设计	3
2.1 设计原则	3
2.2 网络拓扑结构设计	4
3. 网络通信平台的设计	5
3.1 教育城域网平台	5
3.1.1 连接方式	5
3.1.2 VPN 技术	5
3.1.3 IP 地址分配	6
3.1.4 教育城域网接入 Internet	6
3.2 教育局机关局域网	7
3.2.1 综合布线设计	7
3.2.2 局域网 VLAN 的划分	8
3.2.3 局域网接入 Internet	9
3.2.4 无线局域网	9
4 网络资源平台的设计	10
4.1 网络服务器的设计	10
4.1.1 网络服务器技术	10
4.1.2 教育城域网服务器结构设计	11
4.2 网络存储系统设计	12
4.2.1 网络存储技术	12
4.3 教育城域网存储系统设计	13
5. 网络安全与管理平台的设计	14
5.1 网络安全技术	14
5.1.1 主要的网络安全问题	14
5.1.2 网络安全策略	15
5.2 教育城域网安全系统设计	16
5.2.1 教育城域网系统采用的安全措施	16
5.2.2 地/市教育城域网安全系统设计	17
5.3 网络管理技术	18
5.3.1 网络管理的功能	18
5.3.2 网络管理的模式	18
5.4 网络管理系统设计	19
5.4.1 地/市教育城域网网络管理模式	19
5.4.2 地/市教育城域网用户认证和计费系统	20
6. 网络应用平台的设计	21

6.1	教育信息网	21
6.2	教育管理中心	22
6.2.1	教育行政办公系统	22
6.2.2	教育教学管理系统	22
6.2.3	基础教育信息统计系统	23
6.3	教育资源中心的组成	23
6.3.1	优秀教案库	23
6.3.2	CAI 课件素材库	23
6.3.3	题库	24
6.3.4	数字图书馆	24
6.4	远程教育中心	24
6.4.1	远程教育系统的类型	24
6.4.2	地/市教育城域网远程教育模式	25
7.	教育城域网网络设备的选型	26
7.1	网络设备选型原则	26
7.1.1	影响交换机选择的因素:	26
7.1.2	核心交换机选购原则:	26
7.1.3	核心交换机主要参数:	27
7.1.4	路由器的选择	29
7.1.5	防火墙和 IDS 的选择	29
7.1.6	不间断电源	30
7.2	网络设备选型分析	30
7.2.1	交换机	30
7.2.2	路由器	34
7.2.3	防火墙	35
7.2.4	入侵检测系统	36
7.3	服务器选型	37
7.3.1	硬件选型	37
7.3.2	软件选型	38
8.	总结	48
9.	致谢语	50
10.	参考文献:	51

1. 绪论

1.1 背景

教育城域网在国内的发展已经有四年之久。教育城域网最早在 1999 年出现，那时教育部《关于在中小学实施“校校通”工程的通知》还没有颁布，对多数教育行业人士来说“教育城域网”还是个新名词。2000 年，城域教育网开始在国内部分发达地区破土而出；2001 年，教育城域网进入高速发展期；到 2002 年，国内出现了数以百计的教育城域网，其中大部分是经济中等以上发达程度地区兴建的，以北京、上海、深圳等为代表的发达地区则加大教育城域网的覆盖面，比如在 2002 年上海的教育城域网就覆盖了 80% 以上的地区。教育城域网的建设是推进素质教育、迎接知识经济时代的需要。目前世界各国都在加快教育现代化的步伐，其信息化程度的高低也已成为当今世界衡量一个国家综合国力的重要标志。随着“校校通”工程的快速推进，教育信息化应用的不断深入，迫切需要一个地区性的教育资源库和教育管理信息系统。

1.2 作用和目标

教育城域网是学校信息化建设的关键，它的作用体现在如下几个方面：

- 1) 教育城域网能促进各校教师和学生尽快提高应用信息技术的水平。信息技术是一门不断发展的应用型学科，为了让学生掌握更加实用的信息技术，必须给他们提供一个信息化的环境，教育城域网是提供信息化环境的基础。
- 2) 教育城域网为教师提供了一种先进的辅助教学工具、提供了丰富的教学资源库，教育城域网是学校进行教学体制改革、推行素质教育一种必不可少的工具。
- 3) 教育城域网提供了各校交流的桥梁，通过教育城域网与教育网以及互联网的连接，实现了教育资源的最大共享和信息的最快获取。

地/市教育城域网是为实现地/市各校与市教育局相联，并通过市教育局网络中心接入省教育城域网，在市教育局信息中心建立网络资源平台，让各个教育机构互相提供教学资源共享，远程教育，视频点播。使项目有利于学生进行网络协作式和探究式学习，为教师，学生提供全方位的资源服务，分为面向教师教学教研、面向学生学习、面向使用者个人应用、面向师生公共应用四大中心。其对学校教务和教学活动进行综合管理，是一个学校和地区教育信息化的基础信息平台，具有良好的开放性、扩展性、安全性、高效性。

1.3 用户需求

1) 实用性

由于各学校的规模、办学层次和所需要的服务不尽相同，因此用户的类别也比较复杂。同时地/市教育信息中心是全市的教育信息中心、教育管理中心、教育资源中心和城域网管理中心，数据量大、数据结构比较复杂。特别是教育资源库拥有大量的多媒体教育教学资源，容量可达几百 G 甚至上千 G，并且这些数据还经常需要补充和完善。所以本系统在要满足不同学校应用需求的前提下，应采用先进的、成熟的、实用性强的技术和产品，但始终要体现精打细算、勤俭节约的精神，不盲目的追求设备的高档、技术的超前，不贪大求全，不搞花架子。以免造成不必要的资金浪费，从而使系统具有较强的实用性。提供常规的 WWW、E-Mail、FTP、数据库服务，包括教育信息管理系统、学校信息管理系统、教育资源库、信息发布系统、视频点播、备课系统等各种教育行业应用系统。以满足网络易维护、易管理，可实施性的要求。

2) 可靠性与有效性

网络系统作为其他应用系统的基础，如发生系统瘫痪，其造成的损失是难以估量的，特别是对于远程教学，一旦网络出了问题，那势必影响教学进度，因此系统必须可靠地连续运行，即系统设计必须从系统结构、设计方案、设备选择、厂商的技术服务与维修响应能力、设备备件供应能力等方面考虑，使故障发生的可能性尽可能少，影响面尽可能小。

3) 可扩展性

教育城域网建设是一个分阶段的长期过程，而且由于计算机和通信技术的不断发展，用户的需求也在随着时间的推移不断的变化，以及由于应用软件种类和业务数量的增加，功能的强化，系统软件的升级将对主机和网络系统提出更高的要求，泉州市教育城域网的构造应具有高度的扩展性，以降低系统扩充的投入成本，并满足信息技术高速发展的需要。能适应 2-3 年内的业务增长和突发性事件的需要，确保各级系统的可扩充性和先进性，并注意设备的冗余设计以及网络的负载均衡。

4) 安全性

教育城域网接入用户多，而且杂，使得黑客有机可乘，可能出现 DDOS 攻击，存储设备破坏，服务器被非法占据，资源外泄以至造成整个网络中断，因此教育城域的信息安全相对局域网来说就更重要，维护更复杂，网络系统不但要能够实现功能，更重要的是要稳定安全，否则，会影响正常的教学活动的开展。

1.4 设计需求

1) 市教育局网络中心要实现上下与省教育厅网络中心以及各县市教育局网络中心相连，左右与区教育局及各市级学校相连。

2) 教育城域网是为了提供远程教学，视频点播，使用 FTP 协议让各教育机构资源共享,采用 B/S 模式发布通知，公告，新闻。

3) 由于教育城域网规模较大，网络连接复杂，无法对网络访问实施有效监控，网络结构变化无法控制，无法了解网络的漏洞和可能发生的攻击。因此网络建成后，应该制定完善的网络安全和网络管理策略，采用强有力的工具来帮助网络管理者对网络风险进行客观的评估，及时发现网络中的安全隐患，并提出切实可行的防范措施：

- 充分利用交换机的交换路由功能，各教育机构内部根据业务管理需要划分 VLAN，然后通过 NAT 技术接入教育城域网中
- 防火墙与 IDS 联动技术
- 虚拟专用网络（VPN）技术
- 病毒防治技术
- 使用 STARVIEW 进行实时监控

2. 网络总体设计

2.1 设计原则

城域网设计原则：

教育城域网的建设，主要目的是将同一地区、同一个城市里的所有学校、研究机构、本地的教育机构互联起来。为实现教育网络高质、高效互联的目标要求，在网络设计构建中，应始终坚持以下建网原则：

- 高安全、高性能、高可靠性

高质高效的网络性能是整个网络良好运行的基础，因此，在设计中就必须保障网络及设备的高吞吐能力，制订统一的网络安全策略，整体考虑网络平台的安全性。网络系统的稳定可靠是应用系统正常运行的关键保证，在网络设计中选用高可靠性网络产品，设备充分考虑冗余、容错能力和备份，同时合理设计网络架构，制定可靠的网络备份策略，保证网络具有故障自愈的能力，最大限度地支持系统的正常运行。主干网络设备的主要部件必须支持带电热插拔，在万一出现局部故障时应不影响网络其他部分的运行，并且故障便于诊断和排除，充分体现计算机网络的高可靠性。

➤ 可运营、可管理、可增值

对网络实行集中监测、分权管理，并统一分配带宽资源。选用先进的网络管理平台，具有对设备、端口等的管理、流量统计分析，及可提供故障自动报警。要具有良好的业务管理能力、支持对宽带用户的接入管理、身份认证、带宽许可、地址管理和服务质量保证（QoS），并针对不同的业务提供灵活的计费方式，确保网络的可运营特性。要充分考虑业务的扩展能力，针对用户需求提供丰富的宽带增值业务，使网络可持续发展与赢利。

➤ 开放性、兼容性、可扩展性

支持国际上通用标准的网络协议、国际标准的大型的动态路由协议等开放协议，有利于以保证与其它网络(如中国教育网、公共数据网、学校之间等其它网络)之间的平滑连接互通，以及将来网络的扩展。

2.2 网络拓扑结构设计

本解决方案充分结合我国城市市区教育行业用户的网络现状。以地/市教委、电教馆网络为中心，中心交换机采用锐捷 RG-S6800 产品作为网络的核心设备，整个教育城域网骨干采用锐捷网络 3 台 RG-S6800 通过万兆接口做环备份，通过 GE 链路集中来自学校 STAR-S3550-12SFP/GT, STAR-S4909 的上行数据，多节点环网主要应用于建立低成本高性能的 IP 城域网，作为城域网中 IP 业务的承载网络，由于其具有较好的 QOS 特性和带宽保证，因此也可应用于接入网和 VPN 业务。

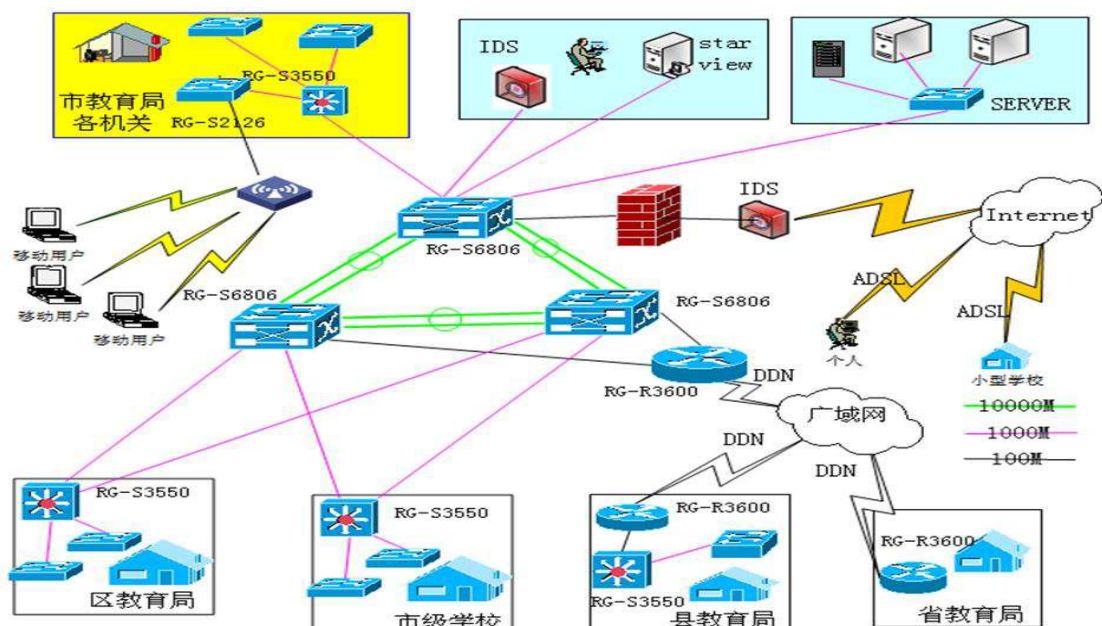


图 1 总体网络拓扑图

3. 网络通信平台的设计

网络通信平台是教育城域网最重要的网络基础设施，其功能是实现网络端到端的物理连接。地/市教育城域网的网络通信平台由教育城域网平台、市教育局机关局域网、学校校园网和市教育信息中心等组成。

3.1 教育城域网平台

3.1.1 连接方式

城域网连接有两种模式：一种模式是由电信公司将光缆铺到辖区各所学校和教育机构，所有的学校通过光缆接入教育城域网，通过访问信息中心的服务器来获取信息。这种方式因为投资大，但性能优；另一种模式是“虚拟教育城域网”，即并不建设物理上独立存在的城域网，而是通过租用电信专线，辖区的学校有条件的以光纤接入，没有条件的采用 ADSL 接入网络中，从而构成一个运行在电信公网基础之上的虚拟教育城域网。这种模式特别适合资金缺口大的地区使用，虽然带宽低、安全性差一些，但是仍不失为加速教育信息化的一种好方法。本方案采用两种模式混合方式：距离比较近的市区学校及教育机构采用第一种模式铺设千兆光缆到各个市级学校和区教育局，距离较远的省教育厅和县（市）教育局采用第二模式通过租用电信 DDN 专线相联，个人用户可以用 ADSL、无线接入方式接入。

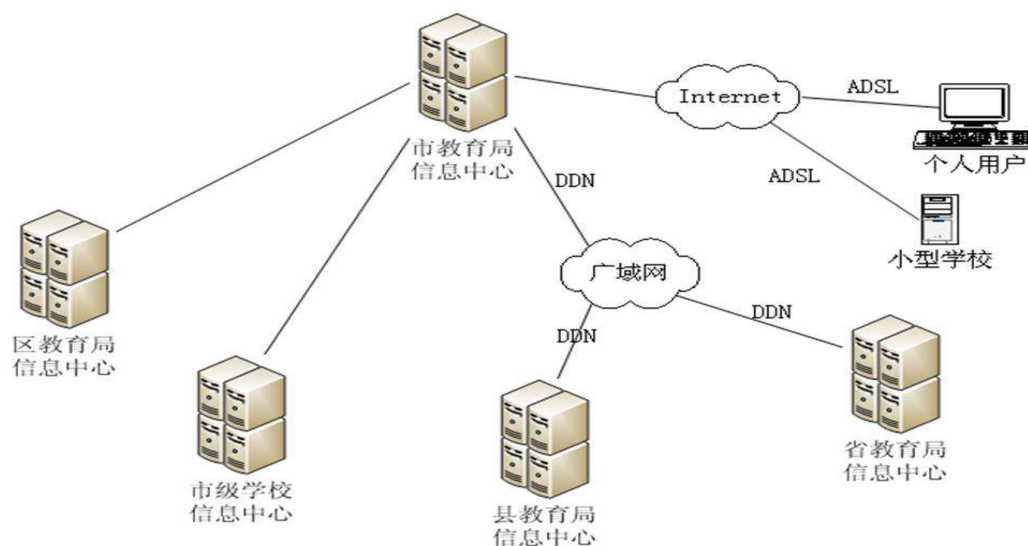


图 2 教育城域网物理结构图

3.1.2 VPN 技术

VPN (Virtual Private Network) 虚拟专用网络，它是利用公共网络基础设施通过加密、隧道等技术手段而构建的专用网络。与传统的专网相比，VPN 有以下主要

优点：

- 低成本：用户不必租用专线建设专网，节省大量的网络维护人员；
- 容易扩展：网络路由设备配置简单，无需增加太多的设备；
- 完全控制主动权：VPN 上的设施和服务可由企业自行设定；
- 覆盖范围大：能够接入 Internet 的地方，都可以实现 VPN；
- 安全性较高：通过各种安全技术的使用，VPN 具有与传统专网相同的安全性。

随着 VPN 技术的不断发展，VPN 设备的价格不断降低，VPN 技术已广泛用于教育城域网系统的建设之中。

1) 市教育局信息中心、区教育局信息中心以及市级学校，通过铺设光缆相连，运用 VPN 技术，组成海口市教育城域网系统的内部专网（Intranet VPN）；

2) 小规模学校、家庭用户、个人用户以及移动用户采用访问 VPN 技术，访问教育城域网；

3) 运用 Extranet VPN 技术，可实现地/市教育城域网与省教育厅信息中心及省属高校校园网之间的连接。随着区域间的教育交流与合作的不断增多，各地区教育城域网的连接成为一种潜在的需求。使用 Extranet VPN 技术，还可以实现与其他地区教育城域网的连接，并且不受区域限制。

3.1.3 IP 地址分配

IP 地址的合理分配，是保证网络顺利运行和网络资源有效利用的关键。为了便于教育城域网的管理，教育城域网内的用户由网管中心统一分配和管理网内用户的 IP 地址。

IP 地址分配应遵循以下原则：

IP 地址规划应该考虑教育城域网业务的发展需要，既要满足当前业务对 IP 地址的需要，又要充分考虑未来业务的发展，预留相应的地址空间；IP 地址的分配应该尽可能地利用申请到的地址空间，充分考虑地址空间的合理性，保证实现最佳的网络内地址分配及业务流量的均匀分布；IP 地址的分配应能满足用户各种业务需要，按照用户业务量的大小进行分配，保证用户业务（如 WEB 服务、接入服务以及邮件服务）的需要。

3.1.4 教育城域网接入 Internet

教育城域网用户，除了共享教育城域网内部资源、实现内部通信外，还经常需要与 Internet 实现连接，进行网页浏览、资源下载、电子邮件以及发布网页等活动。

如果不对网内用户连接 Internet 进行有效的管理，势必会给整个教育城域网系统带来安全隐患。

为了方便教育城域网的管理，提高教育城域网的整体安全性能。网内用户的 IP 地址由教育城域网管理中心统一分配和管理，它们使用教育城域网管理中心提供的 Internet 出口，共享网络中心提供的防火墙和 IDS 等安全设备。

教育城域网系统的用户分别按照以下的途径接入 Internet：

- 1) 市教育局机关局域网、市级学校校园网和市教育信息中心服务器，通过各自的路由汇集到教育城域网网管中心；
- 2) 区教育局机关局域网、区属学校校园网，通过区教育局信息中心路由器汇集到教育城域网网管中心；
- 3) 小规模学校、家庭、个人和移动用户，通过拨号路由器汇集到教育城域网网管中心；
- 4) 教育城域网的所有用户汇集到网管中心后，再通过教育城域网的出口线路接入 Internet，如图(一)所示。

3.2 教育局机关局域网

地/市教育局及所属的教育科研机构是地/市基础教育系统的指挥中心、管理中心、信息中心和服务中心，是海口市教育城域网系统的核心节点。建设市教育局机关局域网，改善市教育局机关的办公自动化条件，提高教育行政管理水平，是地/市教育城域网建设中一项十分重要的工作。

市教育局机关局域网是地/市教育城域网系统中众多节点中最重要、最关键的节点。建好市教育局机关城域网，将为其他节点（如区教育局机关局域网、校园网等）的设计和建设提供样板。

3.2.1 综合布线设计

1) 布线系统的技术要求

局域网布线系统是局域网建设中最基本的基础设施，是局域网体系结构的信道系统。布线系统的质量，直接影响局域网的整体性能和带宽。

地/市教育局机关局域网的总体设计 requirements 是：千兆主干，百兆到桌面。因此，布线系统应达到以下技术要求：

- 工作区子系统选择超 5 类墙上型斜角单口或双口模块化插座，插座到用户设备的跳线也选择超 5 类产品；

- 水平布线子系统选择超 5 类 UTP;
- 管理子系统选择超 5 类 UTP 配线架、配线板、跳线等;
- 垂直干线选择 6 芯多模分布式室内光纤, 用于分配线间与主配线间之间的连接。

2) 交换机配置

为了防范网络广播风暴, 将地/市教育局机关局域网分为若干个虚拟局域网 VLAN。由于在局域网上, 不同 VLAN 之间的通信数据量很大, 而这些通信若都经过路由器转发的话, 势必会加大路由器的负担, 影响整个网络的效率。在这种情况下, 出现了第三层交换技术, 它把路由技术和交换技术的有机地结合起来, 通过第三层交换机, 在交换机中实现路由, 从而实现减小路由器负荷, 提高网络的效率的目的。

地/市教育局机关局域网, 采用第三层交换技术, 选用具有第三层交换功能的骨干交换机作为核心交换机, 配置光纤和双绞线的千兆模块, 实现服务器与二级交换机之间的千兆连接。二级交换机采用堆叠结构, 提供百兆到桌面的连接。

3.2.2 局域网 VLAN 的划分

传统的共享介质以太网和交换式以太网中, 所有的用户在同一个广播域中, 会引起网络性能的下降, 浪费珍贵的带宽。虚拟局域网 VLAN (Virtual Local Area Network), 是一种将局域网内设备逻辑地而不是物理地划分成若干个网段, 从而实现虚拟工作组的新兴技术。

1) VLAN 的优点

- 控制广播风暴

一个 VLAN 就是一个逻辑广播域。通过对 VLAN 的创建, 隔离了广播, 缩小了广播范围, 从而可以达到控制广播风暴产生的目的。

- 提高网络的整体安全性

通过路由访问列表和 MAC 地址分配等 VLAN 划分原则, 可以控制用户的访问权限和逻辑网段的大小, 将不同的划分在不同的 VLAN 之中, 网络管理员通过第三层交换全面管理不同 VLAN 之间的信息互访。

- 网络管理更为简单、直观

对于交换式以太网, 如果对某些用户重新进行网段划分, 需要网络管理员对网络系统的物理结构进行调整, 甚至需要追加网络设备, 增大网络管理的工作量。而对于采用 VLAN 技术的网络来说, 可在不改动网络物理连接的情况下, 任意将计算机在

工作组或子网中移动,大大减轻了网络管理和维护工作的负担,降低了网络维护费用。

2) 划分 VLAN 的方法

➤ 基于端口划分 VLAN

这种划分方法是将交换机上的若干个端口划分成一个逻辑组,并可以跨越多个交换机。这种方法的优点是简单有效,缺点是如果 VLAN 用户离开了原来的端口,到了一个新的交换机端口,那么就必须重新定义。

➤ 基于 MAC 地址划分 VLAN

这种方法是每个计算机的 MAC 地址来划分的。其优点是当用户物理位置移动时,不必重新定义,缺点是初始配置 VLAN 工作量大,交换机执行效率低。

➤ 基于协议(如 IP)划分 VLAN

这种划分方法是根据每个主机的网络层地址或协议来划分的。其优点是当用户物理位置改变是,不需要重新配置 VLAN。缺点是,由于三层交换机检查每一个数据包的网络层地址都要消耗时间,所以效率稍低。

3) 海口市教育局机关局域网 IP 地址分配

上述三种 VLAN 划分方法各有其优点和不足,根据海口市教育局机关局域网的特点,综合考虑网络配置和效率等各方面因素,海口市教育采用基于协议(IP 地址)的方法划分 VLAN。其方法是,将业务性质相同或相近的部门分配同一个 IP 地址段的地址,从而实现把他们划分在同一个 VLAN 之中的目的。

地/市教育城域网网管中心分配给市教育局机关局域网(包括教育信息中心)的全球 IP 地址不多,不可能也没有必要给局域网中的每台计算机都分配一个全球 IP 地址。地/市教育局机关局域网就采用本地 IP 地址的配置方法进行分配

3.2.3 局域网接入 Internet

由于公网 IP 地址有限,达不到每个用户一个全球 IP 的要求,因此地/市教育局局域网使用本地 IP 地址系统。当局域网中的计算机需要上网时,就需要使用网络地址转换技术 NAT 将计算机的本地 IP 地址转换为公网 IP 地址才能与 Internet 上的主机进行通信。

网络地址转换技术 NAT(Network Address Translation)是在 1994 年提出的。这种方法是在专用网连接到 Internet 的路由器(或服务器)上安装 NAT 软件,装有 NAT 软件的路由器(或服务器)叫 NAT 路由器(或服务器)。

3.2.4 无线局域网

无线局域网 WLAN (Wireless LAN) 是 20 世纪 80 年代以来迅速发展起来的一种技术, 它使用无线网卡、无线访问节点 (AP, Access Point)、无线 Hub 和无线网桥等设备, 依据 802.11 标准、蓝牙 (Bluetooth) 标准以及家庭网络 (HomePF) 标准, 提供覆盖范围内任意位置计算机接入局域网的服务。

为了满足教育局机关移动办公的需要, 在充分考虑传统网线铺设的前提下, 增加部分无线接入点, 作为局域网固定布线的补充和扩展, 解决传统铺线不能覆盖地点以及临时需要建立网络通讯场合的接入问题。

地/市教育局机关无线局域网的覆盖范围是教育局办公大楼, 采用室内型 WLAN 设备, 设计带宽 11M, 首期安排 20 台移动计算机接入局域网, 其连接示意图如图 (三) 所示。

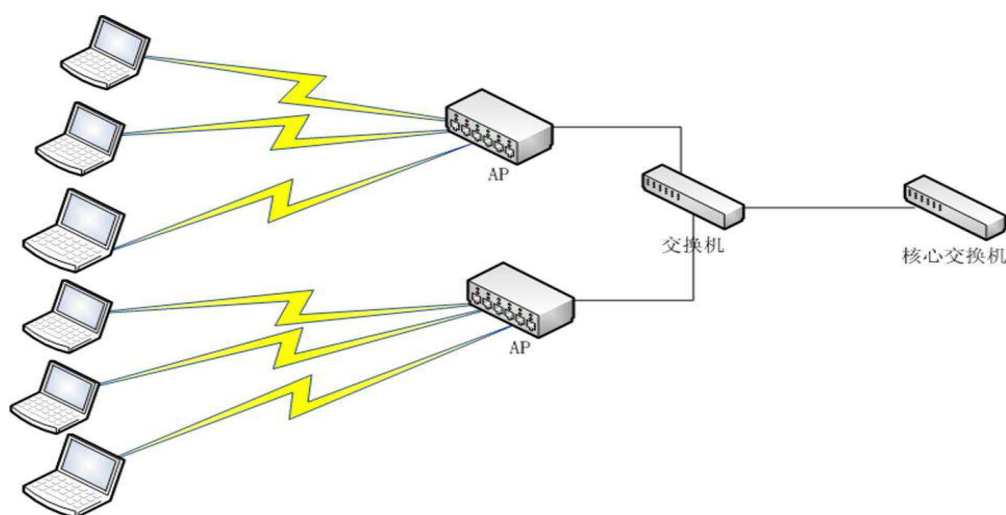


图 (三) 无线局域网示意图

4 网络资源平台的设计

网络资源平台是教育城域网中重要的网络基础设施, 是网络数据储存和处理的集散地。地/市教育城域网网络资源平台由网络服务器系统、网络存储和备份系统组成。

4.1 网络服务器的设计

4.1.1 网络服务器技术

► 负载均衡技术

在多处理器、多任务应用环境和异构系统平台中, 由于频繁, 对服务器的处理速度将会造成很大的压力, 用户的响低整个系统的性能。

负载均衡技术指的是采用一种对访问服务器的负载进行均衡（或者说分担）的措施，使两个或两个以上的服务器为客户提供相同的服务。负载均衡可以通过设置多台服务器或通过软件方式实现，用户可设置一台主服务器，指定一台或多台服务器作为以分担网络的访问流量，另一方面可以提高系统的整体安全。

► 集群技术

集群（Cluster）技术是近几年兴起的一种高性能计算技术，它是将一组相互独立的计算机通过高速的通信网络而组成的一个单一的计算机系统，并以单一系统的模式加以管理。其出发点是提供高可靠性、可扩充性和抗灾难性的服务器系统。

一个服务器集群包含多台拥有共享数据存储空间的服务器，各服务器之间通过内部局域网进行通信。当其中一台服务器发生故障时，它所运行的应用程序将由其他的服务器高速自动接管。在大多数情况下，集群中所有的计算机都拥有一个共同的名称，集群系统内任意一台服务器都可以被所有的网络用户所使用。

► Browser/Server 的体系结构

在 Browser/Server 体系结构中，客户端只需安装、配置少量的客户端软件，他们通过浏览器向网络服务器发出请求。服务器接受这些请求后，在完成对数据库的访问和应用程序的执行后，将操作结果传回客户端服务器。Browser/Server 体系可分为表示层、功能层以及数据层三个相对独立的单元。

4.1.2 教育城域网服务器结构设计

地/市教育城域网系统将采用三层 Browser/Server 服务器体系结构。该结构极大地简化了客户的工作,减少了客户端软件的维护成本，降低了用户访问教育城域网的门槛，如图 4 所示。

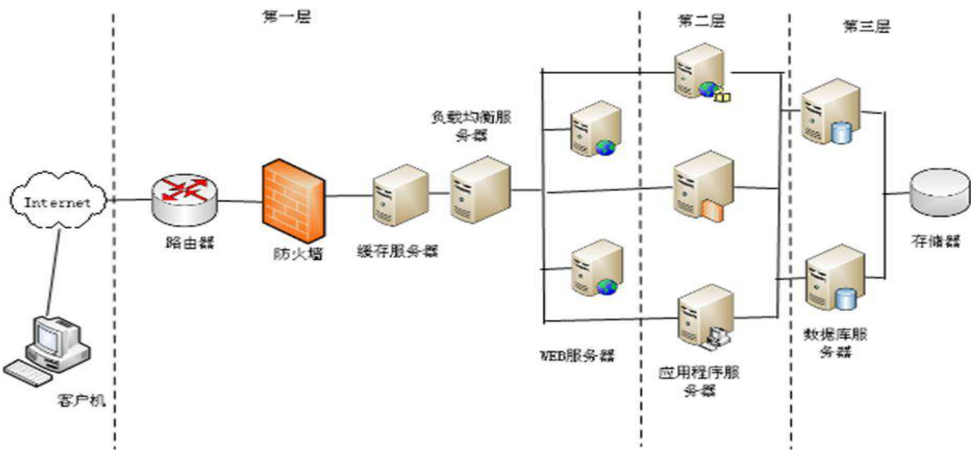


图 4 地/市教育城域网服务器结构示意图

4.2 网络存储系统设计

地/市教育城域网系统是以提供教育信息服务、教育资源共享和教育行政管理为主要服务的专用网络，教育资源库和教育数据库是教育城域网系统的重要组成部分。

教育资源库需要存储大量的各学科教育资源，包括教学实况、教学录像、视频、音频、动画、图形、图像、文字等信息。因而对存储容量、访问速度、可靠性和可管理性的要求极高，这也成为教育网络区别于其它网络的一个十分显著的标志。

教育数据是教育行政管理的重要资源，是教育行政管理系统宏观决策和科学管理的依据。确保教育数据的完整和安全，是教育城域网系统设计中必须解决的问题。

合理运用网络存储和备份技术，科学设计教育城域网存储备份系统，是解决上述问题的最佳途径。

4.2.1 网络存储技术

网络存储技术是近年来发展十分迅速的一门新兴的计算机技术，各种新技术、新产品层出不穷。目前网络存储系统主要采用以下四种技术：

1) RAID

RAID (Redundant Array of Independent Disks) 是指独立的磁盘冗余阵列，其最初所指为廉价磁盘冗余阵列。它具有设备虚拟化能力，使许多内部的磁盘驱动器看起来像一个更大的虚拟设备。RAID 阵列技术还允许将一系列磁盘分组，以实现提高可用性的目的，并提供为实现数据保护而必需的数据冗余，有些 RAID 方式还有改善性能的作用。

2) DAS

DAS (Direct Attached Storage, 直接连接存储或直接附属存储) 是指直接将存储设备连接到主机系统(服务器)上，连接方式有 SCSI 线缆和光纤通道两种。

DAS 的优点是价格低廉、配置简单、使用方便；缺点是扩展性差、管理分散、性能一般。随着需求的不断扩大，越来越多的存储设备和服务器被添加进来，DAS 环境将导致服务器和存储孤岛数量的激增，产生巨大的管理负担，并导致资源利用率低下。在该环境中，数据共享也受到了严重的限制。

3) NAS

NAS (Network Attached Storage, 网络连接存储或网络附属存储) 是将存储设备连接到网络上提供数据和文件服务，NAS 连接要使用专用的 NAS 服务器。NAS 服务器一般由存储硬件、操作系统以及文件系统组成，以方便快捷的存储服务。

NAS 的优点是：首先，它支持即插即用，支持多计算机平台。其次，设备物理位置放置灵活，既可以靠近数据中心服务器，也可以放在其它地点，通过物理链路与网络连接起来；第三，无须应用服务器干预，NAS 允许用户在网络上存取数据，这样既可以减少 CPU 的开销，也能显著改善网络的性能。

为使 NAS 设备很好地发挥其应有的性能，一般要求它以千兆速率接入 LAN，10G 以太网的出现为 NAS 系统性能的提高提供了更好的带宽保证。

4) SAN

SAN (Storage Area Network, 存储区域网络或称存储网络) 是将一个专用的网络置于存储器和服务端之间而构成的存储系统。SAN 通常由存储设备(专用磁盘阵列、磁带机)和存储交换机组成，存储交换机通常为光纤交换机。

SAN 是一个专有的、集中管理的信息存储基础结构，它支持服务器和存储器之间任意点到点的连接。SAN 集中体现了功能分拆的思想，提高了系统的灵活性和数据的安全性。SAN 以数据存储为中心，采用可伸缩的网络拓扑结构，通过具有较高传输速率的光通道连接方式，提供 SAN 内部任意节点之间的多路可选择的数据交换，并且将数据存储管理集中在相对独立的存储区域网内。

4.3 教育城域网存储系统设计

SAN 是随着光纤通道技术的出现而产生的新一代磁盘共享技术，它通过交换机、路由器等连接设备把两个或者多个存储设备和两个或者多个服务器连接起来。

由于 SAN 构建灵活，易于扩展，服务器、存储设备以及交换机可以根据网络的需求随时添加，是目前较为先进的存储技术。因此，地/市教育城域网的存储备份系统，采用 SAN 构架模式，选用磁盘阵列和磁带机为主要的存储备份设备，通过光纤存储交换机与服务器进行连接。其连接方式如图 5 所示。

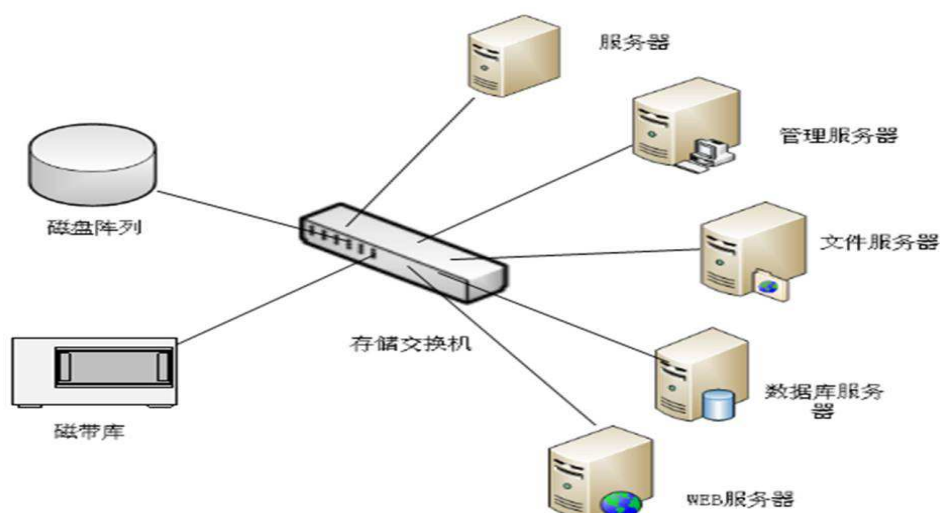


图 5 教育城域网存储备份系统连接图

采用光纤存储交换机为中心的存储备份系统，具有如下的优点：

- 1) 集中存取，更有效地利用存储资源；
- 2) 简单、集中的存储管理，降低了管理的工作量；
- 3) 存储备份设备到服务器的多对多的连接方式，提高了系统的灵活性和可扩展性；
- 4) 缩短了数据备份和恢复的时间，提高了吞吐量；
- 5) 取消了生产网络中的备份，降低了 LAN 的拥塞；
- 6) 可轻松地添加更多的服务器和存储设备；
- 7) 具有更高的安全性。

5. 网络安全与管理平台的设计

随着教育城域网络覆盖范围的逐步扩大，教育用户不断增多，教育应用的不断拓展，教育城域网的安全与管理的难度也逐步增加。因此，运用网络安全与管理的最新技术，选择适当的网络安全与管理策略，设计出适合地/市教育城域网系统的需求的网络安全与管理方案，显得十分重要。

5.1 网络安全技术

5.1.1 主要的网络安全问题

教育城域网的开放性、共享性等特点决定了网络上存在很多的安全隐患，归纳起来，大致有以下几个方面的问题：

- 网络病毒的泛滥性传播

具有开放性的 Internet 越来越成为计算机病毒泛滥性传播的有利环境，Internet 本身的安全漏洞也为培养新一代病毒提供了绝佳的条件。人们为了让网页更加漂亮、功能更加强大而开发出 ActiveX 技术和 Java 技术，然而病毒程序的制造者也利用这些技术，把病毒程序渗透到个人计算机和局域网中，并进行大面积的传播和复制。

➤ 非法访问和破坏不断升级

黑客攻击已有十几年的历史，并频频得手，黑客技术逐渐地被越来越多的人所掌握，他们组成各种各样的联盟，彼此交流黑客技术、共同实施攻击。几乎所有的操作系统，包括 LINUX、Windows 等都能被黑客攻破，全球平均每 20 秒钟就有一个网站遭到黑客的攻击。对于重要的计算机系统，包括教育城域网系统，黑客的攻击往往比计算机病毒破坏性更大。

➤ 对于网络安全缺乏重视和相应的手段

人员疏忽往往是造成安全漏洞的直接原因。人员造成的安全问题主要有三个方面：一是网络管理者对系统配置及安全缺乏清醒的认识或整体的考虑，造成系统安全性能差；二是程序员开发的软件有安全缺陷。三是用户没有保护好自己的口令和密钥。

5.1.2 网络安全策略

为了解决日益严重的网络安全问题，保障网络系统的高效运行，人们动用各种有效的技术手段，从网络安全的方方面面进行研究，制定了一些切实有效的网络安全策略。

➤ 物理隔离策略

对于许多对信息安全有特殊要求的计算机网络，为了保证万无一失，与 Internet 在物理上完全隔离。因此，在有些机构里，往往装有两套甚至更多套彼此独立的网络布线系统。

➤ 访问控制策略（入侵检测策略）

访问控制策略是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和访问，访问控制策略主要有如下几种形式：

- （1）入网访问控制
- （2）网络权限控制
- （3）目录级安全控制
- （4）属性安全控制

(5) 网络服务器安全控制

(6) 网络监测和锁定控制

(7) 网络端口和节点的安全控制

➤ 信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网络会话的完整性。网络加密可以在链路级、网络级、应用级进行。分别对应网络体系结构中不同层次形成加密通信通道。用户可以根据不同的需要，选择适当的加密方式。

➤ 安全管理策略

网络安全管理策略包括：确定安全管理等级和安全管理范围；制定有关网络操作使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施。

➤ 防火墙与入侵检测系统联动策略

防火墙和入侵检测系统是近年来发展起来的一种保护计算机网络安全的技术性措施，它是用一个用以阻止网络中黑客访问某个机构网络的屏障，也可称为控制进/出方向通信的门槛，入侵检测系统检测到网络中的入侵行为后，与防火墙建立联动的安全通信信道；入侵检测系统通过安全通信信道向防火墙发送联动内容；防火墙根据收到的联动内容，生成相应的安全规则，在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻止外部网络的侵入。

➤ 网络防病毒策略

网络防病毒的策略是：一是增加安全意识，控制文件的访问权限；二是小心邮件带来病毒，不打开来历不明的文件；三是精心挑选网络版杀毒软件，定期升级，定期杀毒。

5.2 教育城域网安全系统设计

5.2.1 教育城域网系统采用的安全措施

➤ 两级管理机制

地/市教育城域网采用两级网络安全管理机制。市教育城域网网管中心负责城域网网络平台的网络安全管理，通过安全扫描和监控软件，接收并处理各节点的安全信息，监控个节点的安全状况。各节点负责本节点的网络安全，监测并处理本节点的安全状况，根据网管中心给出的安全报告，优化、升级系统，提高系统的安全性。

➤ 防火墙技术

地/市教育城域网各用户采用由教育城域网系统统一分配的 IP 地址，通过教育城

域网系统的路由器和防火墙系统，访问 Internet。既节省了每个节点独立设置防火墙的开支，又大大地提高了整个网络的安全性。

各节点局域网使用本地的 IP 地址，通过城域网网管中心访问 Internet 之前，须经过网路地址转换 NAT 转换为全球 IP 地址，从而有效地屏蔽局域网 IP，提高局域网的安全性。

➤ VPN 技术

地/市教育城域网系统内部采用 VPN 专有的隧道技术和加密技术，构成与传统专网相同的安全策略、服务质量、可管理性和可靠性。

➤ 入侵检测

在防火墙外和防火墙内各放置一个入侵检测器。外部检测器与防火墙形成互动，抵御外来攻击。内部检测器用测来自网络内部人员滥用职权所带来的网络威胁。

➤ 安全漏洞扫描

在教育城域网网管中心安装网络漏洞扫描软件，对重要的网络设备（如：服务器、存储设备、防火墙、路由器等）进行扫描，及时修补发现的安全漏洞。

➤ 网络防病毒软件

在安装网络杀毒软件的同时，所有的服务器和客户机都安装单机版杀毒软件。

➤ 网络安全管理制度

建立完善的网络安全管理制度，严格限制操作人员滥用职权的行为；制定安全事故的应急预案，妥善处理安全事故危机。

5.2.2 地/市教育城域网安全系统设计

根据地/市教育城域网系统安全的总体要求，采用适当的网络安全策略，地/市教育城域网安全系统的设计如图 6 所示。

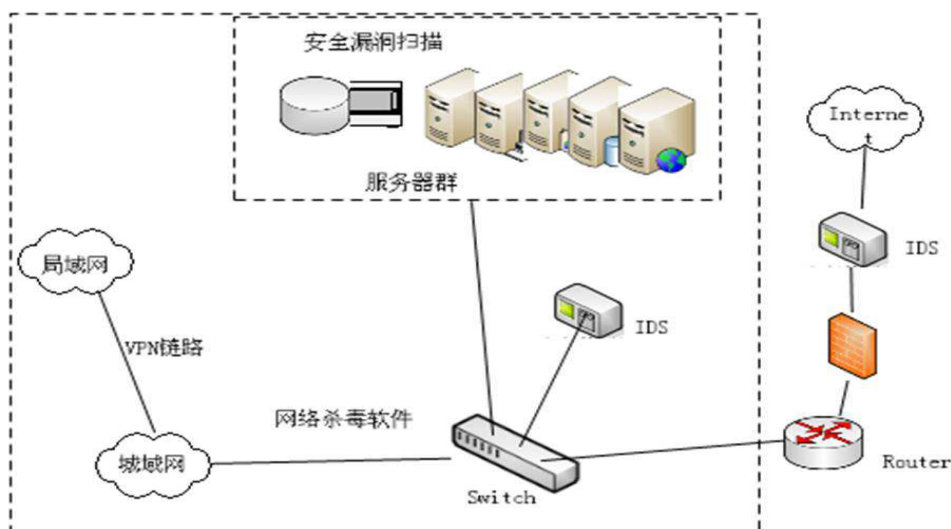


图 6 地/市教育城域网安全系统

5.3 网络管理技术

5.3.1 网络管理的功能

ISO 在 ISO/IEC7498-4 文档中定义的网络管理的 5 大功能是：

- 故障管理（1）维护并检查错误日志；（2）接受错误检测报告并做出响应；（3）跟踪、辨认错误；（4）执行诊断测试；（5）纠正错误。
- 配置管理（1）设置开放系统中有关路由操作的参数；（2）被管对象和被管对象组名字的管理；（3）初始化或关闭被管对象；（4）根据要求收集系统当前状况的有关信息；（5）获取系统重要变化的信息；（6）更改系统的配置。
- 计费管理（1）计算网络建设及运营成本；（2）统计网络及其包含资源的利用率，为确定各种不同时段的标准提供依据；（3）联机收集计费数据；（4）计算用户应支付的网络服务费用；（5）保存收费帐单及必要的原始数据，以备用户查询和质疑。
- 性能管理（1）收集统计信息；（2）维护并检查系统状况日志；（3）确定自然和人工状况下系统的性能；（4）改变系统操作模式以进行系统性能管理的操作。
- 安全管理（1）创建、删除、控制安全服务和机制；（2）与安全相关信息的发布；（3）与安全相关事件的报告。

5.3.2 网络管理的模式

1) 集中式网络管理模式

集中式网络管理模式是所有的网管代理在管理站的监视和控制下，协同工作实现

集成的网络管理。

集中式网络管理的优点是管理集中，有专人管理，有利于从整个网络系统的全局对网络实施较为有效的管理；缺点是管理信息汇总到网络管理节点上，导致网络管理信息流比较拥挤，管理不够灵活，如果管理节点发生故障则有可能影响全网的正常工作。

2) 分布式网络管理模式

分布式网络管理模式是将信息管理和智能判断分布到网络各处，使管理变得更加自动化，使得在问题源或靠近故障源的地方能够做出最基本的故障处理决策。

分布式网络管理模式优点是：提供了可扩展性，以适应全新的、不断扩大的网络应用；降低网络管理的复杂性；网络管理的响应时间更快、性能更好；提供信息管理的共享能力。

3) 集中式与分布式相结合的管理模式

当今计算机网络系统正向进一步综合、开放的方向发展。因此，网络管理模式也在向分布式与集中式相结合的方向发展。集中式与分布式相结合的管理模式大致有以下策略和方法：

- 以分布式管理为基础，制定某个或某些节点为网络管理节点，指定专人享有较高的特权，可以对网络中的其他节点进行监控管理，其它节点的报告信息也指定节点汇总。
- 部分集中，部分分布。网络中的处理能力强的中小型计算机，采用分布式管理模式；网络中的一般工作站通过指定的网络管理节点实施管理。
- 联邦制管理模式。

一个大型的网络由许多部门网络组成，各部门自己的网络采取集中管理模式，部门之间一般情况下互不干预。当涉及到网络全局的网络运行、安全和性能优化问题时，通过各部门网络管理间的通信来协调解决。

- 分级网中的分级管理。

按照行政体制的分级树型管理模式管理，部门在管理自身网络的同时，对其下属的网络进行指导和干预，同时向其上级报告网络运行状况。

5.4 网络管理系统设计

5.4.1 地/市教育城域网网络管理模式

地/市教育城域网系统采用集中式与分布式相结合的两级管理模式，即局域网网

管和教育城域网网管中心两级管理模式。

各教育局机关局域网和学校校园网网管，采取集中式网络管理模式，负责本地局域网的管理，同时向市教育城域网网管中心报告网络运行状况。

市教育城域网网管中心，除负责市教育城域网网络中心重要设备（如服务器、存储器、路由器等）的管理工作外；还采取分布式网络管理模式，协调、处理事关教育城域网全局的网络管理事务，监控管理各节点的运行状况，如图 7 所示。

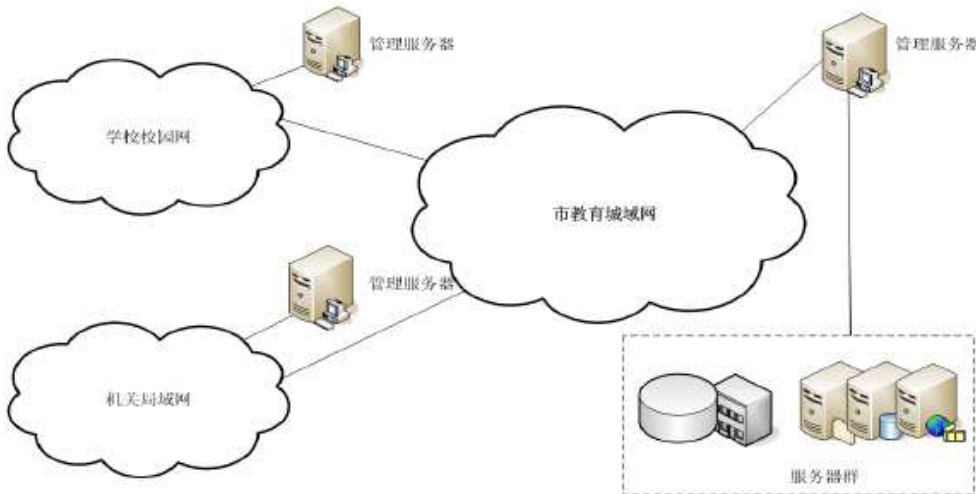


图 7 地/市教育城域网管理模式示意图

5.4.2 地/市教育城域网用户认证和计费系统

地/市教育城域网是建立在地/市宽带城域网基础上的虚拟网络，为了信息安全和便于对用户进行管理，地/市教育城域网应有一套用户认证和计费系统。

对于拥有固定 IP 地址的用户（教育局机关局域网、大规模学校校园网），系统对其账号与 IP 地址、MAC 地址进行绑定，防止了 IP 地址和客户账号盗用现象的发生，提高客户行为的唯一性，有效的，使得他们能够随时进入教育城域网。

对于没有固定 IP 地址的用户（小规模学校、家庭和个人用户），在网络运营商的配合下，通过其指定的 IP 地址段，输入帐号和密码即可进入教育城域网的相关部分。对于那些出差在外又需要获得海口市教育城域网服务的漫游用户，系统随时可提供临时帐号和密码，供他们使用。

为了弥补教育城域网建设和运行的巨大资金缺口，使地/市教育城域网的建设步入滚动发展、良性循环的轨道。地/市教育城域网应该具有一套功能强大、方便快捷的计费系统，其主要功能如下：

- 1) 多种计费功能，如包月无上限、计时包月有上限、计流量包月有上限、简单

计时、分时段计时、累计时长、分段累计时长、分时分段累计时长、简单计流量、累计流量、分段累计流量等；

- 2) 方便不同种类用户根据自己的需求，选择不同计费方式；
- 3) 给用户提供查阅详情、打印清单的服务；
- 4) 根据客户的信用状况，设定对应的信用级别，采用不同的催费方式，实现欠费停机和强制下线功能；
- 5) 支持持卡消费和自助充值。

6. 网络应用平台的设计

地/市教育信息中心是教育城域网服务的主要提供者，它通过设在其内部的教育信息门户网站、教育管理信息中心、教育资源中心，远程教育中心以及教育网络管理和服务中心，为地/市教育城域网用户提供教育信息化服务，以下分别介绍教育城域网各应用平台的组成和主要功能。

6.1 教育信息网

地/市教育城域网应用系统可分为以下三个层次：

- 1) 教育局机关的网络化办公系统和学校内部教育教学管理系统；
- 2) 市（区）教育局之间、教育局和学校之间、学校与学校之间的教育管理数据传递，优质教育资源共享。
- 3) 市（区）教育局、学校通过互联网，向社会公众提供教育政策咨询、教育信息发布和远程教育服务。

地/市教育信息网分为内部网站和外部网站两种模式。内部网站（简称内网）是各级教育机关和学校用于内部办公自动化、教育教学管理、教育资源共享的专用网络平台。它通过教育城域网的内部专网 Intranet VPN 发布，非授权用户不能对其进行访问。

外部网站（简称外网）是地/市教育局通过 Internet 发布的，面向广大社会公众的电子政务窗口。其作用是宣传教育方针政策，报道教育新闻，传递教育信息，向社会各界提供全方位的教育信息服务。

地/市教育信息网是地/市教育的门户网站，是教育电子政务的重要组成部分。教育门户网站建设、运行的好坏，直接关系到政府的形象，也影响着地/市教育管理和服务的质量和水平。因此，注重地/市教育信息网的建设，提高教育信息网的设计、

运营和管理水平，就成为教育城域网建设中一个非常重要的课题。

地/市教育信息网将开设教育概况、政策法规、教育新闻、教育热点、招生考试、教师频道、学生频道、电子政务、教学资源、远程教育、视频点播、电脑科技等教育服务栏目。作为地/市教育的门户网站，海口教育信息网还提供电子政务系统、教育资源中心和远程教育网站的入口。

6.2 教育管理中心

教育管理中心的职能是：为教育局和学校间架起电子政务的桥梁，实现政务电子化、通讯网络化和办公自动化，实施政务公开，接受社会各界的监督。教育管理中心由教育行政办公系统、教育教学管理系统和基础教育数据统计系统组成。

6.2.1 教育行政办公系统

教育行政办公系统的功能：实现市教育局、区教育局和学校之间的文件信息交换和单位内部的办公管理，主要包括：公文流转、信息管理、内部/外部 Internet 信息发布及浏览、个人事务、公共信息、会议管理和电子邮件等。

教育行政办公系统由“信息发布”、“今日工作”、“公文管理”、“会议管理”、“日程安排”、“外出登记”、“文件收发”等子系统组成。

6.2.2 教育教学管理系统

教育教学管理系统的功能：建立一系列包括学生、教师、财产在内的数据标准、数据库和管理系统，发挥其在教育教学管理的重大作用，为教育决策提供及时、可靠的数据信息。

地/市教育教学管理系统由学生管理子系统、教师管理子系统、财产管理子系统和教务管理子系统组成，如图 8 所示。

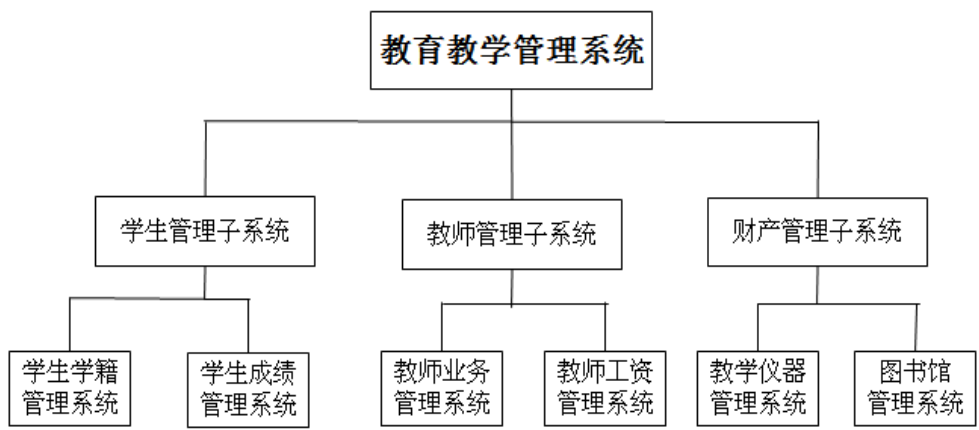


图 8 教育教学管理系统组成图

➤ 学生管理子系统

学生管理子系统对学生从入学开始到毕业为止的时间段内全方位的信息管理。从接收新生、分班、学籍变动（转入、转出、休学、退学、复学等）、考试成绩、升留级、毕业等方面的管理工作，都纳入本系统管理。并以此系统为基础，开发“家校通”管理平台，加强学校与家庭的沟通，方便学生家长了解学生在校的表现。

➤ 教师管理子系统

教师管理子系统是对教职员工各方面的信息进行综合管理。包括：教师的基本信息、人事档案、个人简历、特长爱好、奖励、培训进修、考试考核成绩、所教课程、论文、考勤等信息。

➤ 财产管理子系统

财产管理子系统是对本市各级各类学校的财产进行管理的信息系统。它包括学校固定资产、校舍、教学设施设备、教学仪器、图书等管理模块。

6.2.3 基础教育信息统计系统

基础教育信息统计系统，是根据教育系统数据统计要求专门设计，提供教育报表的任意定义功能，实现下级数据接收、统计、汇总及上级数据报送功能。该系统数据可通过网络层层上报，满足教育信息统计准确、高效的需要。

该系统还提供周全的查询功能，提供学校报表查询、教委报表查询、组合查询、比较查询、年度查询和统计查询等多种查询服务。

6.3 教育资源中心的组成

地/市教育资源中心由优秀课例教案库、CAI 课件素材库、题库和数字图书馆等组成。

6.3.1 优秀教案库

通过购买、交流等形式，收集包括全国各省市名师的教学设计和课堂实录，收集本市历年优秀课例评比的获奖作品，逐步形成与各学段、各学科教材配套的优秀教案、课堂实录体系。为全市教师继续教育工程，为提高教师的教学业务水平，提供丰富的示范资源。

6.3.2 CAI 课件素材库

积极筹措资金，购买各种格式的课件、视音频素材、视频短片和资料影片，鼓励本市教师积极研制开发适用课件，广泛组织各种优秀课件评比活动，挑选其中的精品充实到课件素材库之中。逐步形成大容量、高质量的全市教育教学课件和素材中心，

为广大教师提供丰富的备课资源。

6.3.3 题库

精心挑选小学、初中和高中各学期期中、期末考试试题和单元测试题；中考和高考各轮次的复习检测、模拟考试和升学考试试题，组成题量丰富、题型多样和具有不同难度等级多功能试题题库。该题库应具备随机拼题功能，可随意拼出同步测试和结业测试等不同要求的试卷，最大限度地满足各类测试和考试的组卷要求。

6.3.4 数字图书馆

数字图书馆是一种拥有多种媒体、内容丰富的数字化信息资源。它包括书籍、报刊等文字资料和录音、录像等多媒体资料。数字图书馆除提供图文并茂、丰富多彩的交互式界面外，符合人类联想思维与联想记忆特点的、按超文本结构组织的大规模知识库与信息库，为实现探索式学习和发现式工作创造条件。

6.4 远程教育中心

远程教育克服了传统教育在时间、空间、教育环境和受教育年龄等方面的限制，借助网络来进行多媒体教学。它采用音频、视频和超文本等多种方式，与传统的教育媒体相结合，让优秀的教育资源得以共享，使教师、学生间实现自由交流。网上远程教育成为教育体系中十分重要的一个组成部分。

6.4.1 远程教育系统的类型

基于网络通讯技术的远程教育系统，其实现方式很多，但目前应用最普遍、技术最成熟的远程教育系统主要有以下三种类型：

1) 基于 Web 的远程教育系统

该系统为非交互、非实时的应用系统，它采用大型的 Web 服务器和数据库服务器作为远程教育的服务器，学生通过计算机上的浏览器连接到 Web 服务器上，浏览教学内容。

这类系统的主要特点是对学生的终端的要求很低，学生可以自由选择时间地点上网。因此，这类远程教育系统的学生规模可以很大，非常适合于普及型、自学型的远程教育应用。

2) 实时交互的远程教育系统

这类远程教育系统为交互、实时和多点的应用系统。利用基于包交换或基于电路交换的通讯网络，采用相应的网络产品，完成实时的、交互的和多点的多媒体通讯和所需的控制功能，从而实现实时的多媒体教学。

这类系统对网络带宽和网络服务质量的要求较高。

3) 基于点播的远程教育系统

这类系统主要用于学生按需检索、观看教学资料片进行学习。教学资料片存储在视频服务器（VOD 服务器）上，可以是实时教学内容的录像，也可以是从已有录像带、VCD、DVD 等现有片源直接导入的视频资料。

视频服务器应该能支持多种压缩编码格式的视频文件，不同接入带宽的用户可以根据实际情况选择相应的播放格式。

6.4.2 地/市教育城域网远程教育模式

地/市教育城域网远程教育主要采用以下三种模式：

1) 设立名校网校

网校是具有较高教育教学水平、有一定社会声望的学校，利用其师资、教学设施和教学经验上的优势，通过 Internet 开展教育教学活动的网站。网校一般由知识导学、同步课堂、名师答疑、在线辅导等栏目。

地/市教育城域网将依托海口教育信息网，开辟“远程教育”栏目，建立优质学校的网校，对学校、家庭和社会开放。同时，地/市教育城域网还将与全国各地的知名网校的合作，整合国内优秀教育资源，实现教育资源的交流和共享。

2) 建立学科专题网站

地/市教育城域网将专门开设基础教育学科的专题网站，由市教研室教研员负责管理和维护。积极创造条件，让全市相同学科的教师在网上交流教学经验、开展教研活动，共同提高业务素质和教学能力，缩小重点学校和非重点学校、城区学校和农村学校间教学水平的差距，从而达到全面提高海口市教育教学质量的目的。同时，积极鼓励国家和省、市骨干教师在教育城域网上开设学科辅导网站，让不同层次的学生享有个性化的教学辅导服务，特别是农村学生能与城市的学生一样，可以获得优秀教师的个别指导。

学科专题网站还可用于研究性学习，如，将课程的学习目标分为若干个学习专题，学生根据自己的学习情况、兴趣爱好选择学习专题后，进入该专题的研究性学习。

3) 开设网络课堂

网络课堂是远程教育采用的主要形式之一，通过压缩优秀教师教学现场的视频、音频信号，形成教学资源流，利用网络实时传送到远端学生的电脑上。学生通过电子白板、语音等方式向老师提问，与其他同学进行讨论。网络课堂虚拟现实中的教室，

打破时空限制，让异地师生通过音视频实时交互，如同置身于同一课堂之中，实现远程教育的目的。

7. 教育城域网网络设备的选型

7.1 网络设备选型原则

7.1.1 影响交换机选择的因素：

不同位置、不同的环境、不同应用需要不同的网管交换机。因此，在选择可网管交换机时，应当考虑以下问题：

➤ 所处位置

不同位置应当选用不同的可网管交换机。核心层交换机应当选择模块化三层交换机，汇聚层交换机建议选择高性能、可扩展端口的三层交换机（如果网络规模小，也可以选择二层交换机），而接入层交换机则应当选择二层交换机就可以了。

➤ 网络应用

不同的网络应用决定着所需要设备的性能。性能越高的交换机自然价格也就越高，因此，不要盲目追求高性能，而应当根据网络应用、数据流量等诸多因素，选择最合适网络应用的、最具有性价比的交换机。

➤ 所处环境

在选择交换机时，不能将它们相互割裂开来，而应当综合地、联系地进行考虑。考虑下级交换机是否支持上级交换机的功能和应用，考虑上下级交换机在性能上应有的差别，考虑上下级交换机端口的类型与数量，考虑传输距离、网络带宽和通信线缆，从而使所有交换机相互协调，达到彼此之间的最佳组合。

➤ 设备兼容性

尽管不同的可网管交换机大多遵守相同的国际标准，但每个厂家都有一些特殊的协议，并且使用不同的网络管理软件，因此，若欲实现对可网管交换机的统一管理，实现各种复杂的网络应用，达到性能最优化，就应当尽量选择同一厂商的产品。

➤ 设备性能

设备性能也是在选择交换机时必须注重的因素。其中，背板带宽、转发数率、VLAN 数量、MAC 地址数量、插槽数量、支持的端口类型、堆叠层数等参数，都必须根据交换机所处的位置与网络应用确定。

7.1.2 核心交换机选购原则：

在选购核心交换机时，应当掌握以下几个基本原则：

➤ 需求决定一切

虽然高性能的核心交换机比比皆是，但并不意味着必须购买最好的设备，而应当购买自己报需要的设备。除了满足现有需求外，还应当在技术、性能和扩展等方面适当超前，以适应未来的发展。通常情况下，核心交换机的扩展能力和性能应当略大于未来几年内网络应用和扩展的要求。

➤ 稳定压倒一切

对于核心交换机而言，对稳定物要求高过对性能的要求。比如说：如果网络性能一般但是可以提供安全、稳定的服务，那么网络运行就总是正常的，用户也会觉得是值得信赖的。假如网络带宽很高、性能非常强劲、服务访问特别舒服，但是经常发生故障，导致服务器无法访问、Internet 无法共享，用户也一样的会没有信心的。当在网络上运行重要的应用时，网络瘫痪还将导致正常业务的中断和重要数据的丢失。

➤ 性价比

现在核心交换机产品中，美国的产品以其性能强劲、运行稳定、功能丰富而著称，只是价格过于昂贵。大陆的产品虽然在一些参数上略逊一筹，但是拥有绝对的价格优势，而且像华为的产品具有中文管理界面，方便管理。

7.1.3 核心交换机主要参数：

➤ 扩展能力

核心交换机应当全部采用模块化结构，必须拥有相当数量的插槽，具有强大的网络扩展能力，以保护原有的投资。模块化结构拥有更强劲的性能、更大的灵活性和可扩充性，可以根据现实或未来的需要选择不同数量、不同速率和不同接口类型的模块，以适应千变万化的网络需求。

可扩展性应当包括两个方面：

①插槽数量。插槽用于安装各种功能模块和接口模块。由于每个接口模块所提供的端口数量是一定的，因此插槽数量也就从根本上决定着交换机所能容纳的端口数量。所有功能模块都需要占用一个插槽，因此插槽数量也就从根本上决定着交换机的可扩展性。

②模块类型。支持的模块类型越多，交换机的可扩展性越强。以局域网接口模块为例，就应当有 RJ—45 模块、GBIC 模块、SFP 模块、10Gbps 模块等，以适应大中型网络中复杂环境和网络应用的需求。

➤ 转发速率

网络中的数据是由一个个数据包组成，对每个数据包的处理要耗费资源。转发速率是指在不丢包的情况下，单位时间内通过的数据包数量。吞吐量是三层交换机最重要的一个参数，标志着交换机的具体性能。如果吞吐量太小，就会成为网络瓶颈，给网络的传输效率带来负面的影响。交换机应当能够实现线速交换，即交换速度达到传输线上的数据速度，从而最大限度地消除交换瓶颈。对于万兆位交换机而言，若欲实现网络的无阻塞传输，要求：

吞吐量 (Mpps) = 万兆位端口数量 * 14.88Mpps + 千兆位端口数量 * 1.488Mpps + 百兆位端口数量 * 0.1488Mpps

➤ 背板带宽

背板是交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量，就像是立交桥所拥有的车道的总和。由于所有端口间的通信都需要通过背板完成，所以背板所能提供的带宽，就成为端口间并发通信的瓶颈。带宽越大，提供给各端口的可用带宽越大，数据交换速度越快；带宽越小，给各端口提供的可用带宽越小，数据交换速度也就越慢。也就是说，背板带宽决定交换机的数据处理能力，背板带宽越高，所能处理数据能力越强。因此，背板带宽越大越好，特别是对那些汇聚层交换机和中心交换机而言。若欲实现网络的全双工无阻塞传输，必须满足最小背板带宽的要求，其计算化工如下：

背板带宽 = 端口数量 * 端口速率 * 2

注：对于三层交换机而言，只有转发速率和背板带宽都达到最低要求，才是合格的交换机，二者缺一不可。

➤ 模块冗余

冗余能力是网络安全运行的保证。任何厂商都不能保证其产品运行过程中不发生故障。而故障发生时能否迅速切换就取决于设备的冗余能力。对于核心交换机而言，重要部件都应当拥有冗余能力，比如管理模块冗余、电源冗余，这样才可以在最大程度上保证网络稳定运行。

➤ 路由冗余

利用 HSRP、VRRP 协议保证核心设备的负荷分担和热备份，在核心交换机和双汇聚交换机中的某台交换机出现故障时，三层路由设备和虚拟网关能够迅速快速切换，实现双线路的冗余备份，保证整个网络的稳定性。

核心交换机是整个网络的核心和心脏，如果发生致命性的故障，将导致本地网络的瘫痪，所造成的损失也是难以估计的。对三层路由采用热备份是提高网络可靠性的必然选择。在一个三层路由完全不能工作的情况下，它的全部功能便系统中的另一个备份路由完全接管，直到出现问题的路由器恢复正常，这就是热备份路由协议 VRRP。

在网络中，一般给终端设备指定一个或者多个默认网关。如果作为默认网关的三层设备损坏，那么所有使用该网关的主机通信必然中断。就是配置了多个默认网关，如果不重新启动终端设备，也不能切换到新的网关。采用虚拟路由冗余协议 VRRP，可以很好地避免静态指定网关的缺陷。

➤ QoS

QoS（服务质量）机制具有能够识别通过交换机数据包的特征，可以根据流量的不同类别采取不同的传输策略。QoS 对于多媒体传输的意义也很重大，在实现视频点播、视频会议等多媒体信息应用时，三层交换机应当拥有 QoS 控制功能，可以给不同的应用程序分配不同的带宽。

➤ 安全性能

核心交换机应当支持 802.1x 基于端口的访问控制，支持本地和远端认证，EAP 终结或者透传；支持 RADIUS 和 TACACS+ 认证，支持 MAC 访问列表、IP 访问列表和 VLAN 访问列表，并支持私有 VLAN。可实现基于时间段控制，并限制每端口最大用户数。

➤ 技术潜力

核心交换机的技术潜力主要体现在两个方面，对万兆位和 IPv6 的支持。

7.1.4 路由器的选择

地/市教育城域网，由于大量的数据都需要与市教育局网络中心进行通信，因此，对路由器的性能要求较高，但对网络接口数量没有太高的要求，因此，建议选择性能稳定、插槽数量确定的路由器。路由器的主要考虑因素是包交换能力、系统稳定性和安全性。

7.1.5 防火墙和 IDS 的选择

地/市教育城域网，对网络安全有更高的要求，所以选择网络防火墙和 IDS 是必须的，选用防火墙关闭一些未被使用的 TCP/UDP 端口，以避免蠕虫病毒和网络木马的入侵，保证网络内部计算机和网络服务器的安全，防止重要和敏感的数据的丢失。网络防火墙建议选择支持外部攻击防范、内网安全、流量监控、邮件过滤、网页过滤、应用层过滤等功能，能够有效地保证网络的安全，支持多种 VPN 业务，可能构建多种

形式的 VPN，能够提供基本的路由能力，支持 RIP/OSPF/BGP/路由策略及策略路由和 NAT 功能；入侵检测技术，可对连接状态过程和异常命令进行检测，提供多种智能分析和处理手段，入侵检测系统检测到网络中的入侵行为后，与防火墙建立联动的安全通信信道；入侵检测系统通过安全通信信道向防火墙发送联动内容，防火墙根据收到的联动内容，生成相应的安全规则，在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，协助网络管理员完成网络的安全管理。

7.1.6 不间断电源

随着用电量的不断增加，电力供需矛盾日益突出，特别是在冬夏两季的用电高峰，断电事故频频发生，并且电压忽高忽低很不稳定。毫无疑问，不稳定的电压不仅会导致系统瘫痪，甚至还会造成服务器和网络设备的硬件故障、丢失宝贵的数据，酿成重大事故。因此，地/市教育城域网应当配置不间断电源，由 UPS 为所有设备提供稳定的电源输出，保障网络设备和服务器的正常运行。不间断电源可以采用抽屉式高智能模块化设计，可通过增减机柜内 UPS 模块来满足功率输出及可靠性要求，具有极大的弹性，实现最佳性价比。采用高效率、高性能以及高输出电压稳定度的比转换纯在线架构，兼容三相和单相市电输入，并可通过判断当前市电状态自动地在三/单相之间切换。采用高速 DSP 作为控制的 UPS 拥有强大的信息处理能力，提供人性化的操作界面和最完善的电源管理功能，不但极大地提高了 UPS 自身的运行质量，而且通过全中文液晶屏，以及与电脑和网络的完美连接，使得 UPS 的操作与管理得心应手。

7.2 网络设备选型分析

7.2.1 交换机

1) 接入层交换机：

在教育机关局域网和校园网的接入层采用 RG-S2126 设备类型：

设备类型	网管以太网交换机
是否支持全双工	全、半双工
网管功能	SNMPv1 / v2 / v3 、 Web （ JAVA ）、 CLI （Telnet/Console）、RMON(1, 2, 3, 9)、集群、SSH
传输速率(Mbps)	10/100/1000
端口类型	24 个 10Base-T/100Base-TX RJ45，2 个扩展插槽，可扩展最大 2 个百兆/千兆接口模块

特征和优势：灵活完备的安全控制策略，通过内在的多种安全机制可有效防止和控制病毒传播和网络流量攻击，控制非法用户使用网络，保证合法用户合理化地使用网络，如端口安全、端口隔离、专家级 ACL、时间 ACL、端口 ARP 报文的合法性检查、基于数据流的带宽限速、六元素绑定等，满足企业网、校园网加强对访问者进行控制、限制非授权用户通信的需求；支持 DHCP Relay，更可支持 DHCP Option 82，可方便实现对 IP 地址的精确分配和控制，并可通过交换机硬件 ARP 检查，可有效防范动态分配 IP 地址环境下的 ARP 欺骗问题；方便易用易管理 强大的菊花链式堆叠，支持 S2126G/S2150G 的混合堆叠，保证网络的高度灵活和可扩展，网络管理更加简单；提供图形化的安全策略管理平台，支持安全策略自动同步下发、升级和维护功能，安全策略智能化，可大幅度提高交换机管理和配置效率，提高网络安全；

2) 汇聚层交换机：

在教育机关局域网和校园网的汇聚层采用 RG-S3550 设备类型：

支持速率：10Mbps/100Mbps/1000Mbps 应用级别：企业级 工作协议层：三层
传输速度：千兆

产品简介：STAR-S3550-12G/S3550-24G 以及 RG-S3550-12SFP/GT 是三款线速全千兆智能多层交换机，能提供多种形式接口如 GBIC 插槽或 SFP 插槽或 10/100/1000M 自适应电口，最多可提供 24 个 GBIC 插槽，GBIC 插槽支持千兆铜缆、光纤扩展模块，支持模块热插拔，极大方便用户灵活配置网络。

功能和优势：该系列交换机硬件支持 2 至 4 层的多层线速交换，提供二到七层的智能的流分类和完善的的服务质量（QoS）以及组播管理特性，支持完善的高性能路由协议，并可以实施灵活多样的 ACL 访问控制策略。可通过 SNMP、Telnet、Web 和 Console 口等多种方式提供丰富的管理。S3550-12G/S3550-24G 以及 S3550-12SFP/GT 以极高的性价比为各类型网络提供线速多层交换、完善的端到端的服务质量、丰富的安全设置和基于策略的网管，最大化满足高速、安全、智能的企业网新需求。

完备的安全控制，具有的多种内在机制可以有效防范和控制病毒传播和黑客攻击，如预防 Dos 攻击、防黑客和病毒 IP 扫描机制等，还网络一片绿色；硬件实现端口与 MAC 地址和用户 IP 地址的绑定；通过保护端口即可方便简单地隔离用户之间信息互通，不必占用 VLAN 资源；提供加密传输的 Secure Shell（SSH），保证管理设备信息的安全性，防止黑客攻击和控制设备；高安全性，具有端口安全、动态地址锁、端口隔离、用户接入认证（802.1x）、专家级 ACL 控制、基于数据流的带宽限速等多种

安全措施，满足企业网加强对访问者进行控制、限制非授权用户通信的需求；支持 VRRP 虚拟路由器冗余协议，构建故障时的冗余路由拓扑结构，保持通讯的连续性和可靠性，有效保障网络稳定。

3) 核心层交换机：

根据教育机构的规模选择是否使用核心交换机，采用 RG-S6800 系列做核心交换机和环备份交换机：

支持速率：10Mbps/100Mbps/1000Mbps/10000Mbps 工作协议层：三层 传输速度：万兆

产品简介：RG-S6800E 是锐捷网络推出的基于 NP+ASIC 构架的新一代多业务万兆核心路由交换机，RG-S6800E 在保障高性能大容量的基础上提供强大的安全防护能力，并且拥有业务按需叠加扩展能力，达到业务和性能并重的设计需求。目前提供 10 竖插槽设计和 6 横插槽设计两种主机：RG-S6810E 和 RG-S6806E。RG-S6800E 系列多业务万兆核心路由交换机提供 2.4T/1.2T 背板带宽，并支持将来扩展到 4.8T/2.4T 的能力，高达 857Mpps/428Mpps 的二/三层包转发速率可为用户提供高速无阻塞的数据交换，强大的交换路由功能、安全智能技术可同锐捷各系列交换机配合，为用户提供完整的端到端解决方案，是大型网络核心骨干和大流量节点交换机的理想选择。RG-S6800E 交换机通过先进的第三代高性能引擎可硬件支持策略路由、IPV6 等协议，并可扩展支持 MPLS、load balancing、NAT、VPN、Firewall、IDS、web cache redirect 等丰富的业务功能，满足客户环境灵活而复杂的不同应用需求。

功能和优势：

➤ 强大数据处理设计（SPOH 设计）：RG-S6800E 的交换、路由、ACL、QOS 等复杂功能通过硬件实现，避免了软件实现同样功能对数据高速处理的影响。管理模块执行路由管理、网络管理、网络服务等任务，用户接口模块可以独立实现硬件路由、交换和组播功能；用户交换端口则独立实现硬件 ACL 和 QOS 功能，同步式处理设计（SPOH 设计）极大地提高整机处理能力。

➤ 强大的扩展能力

RG-S6800E 系列多业务万兆核心路由交换机目前提供 2.4T/1.2T 背板带宽，在不更换机箱的情况下，未来仅通过更换管理模块可以支持背板带宽扩展到 4.8T/2.4T。

➤ RG-S6800E 系列多业务万兆核心路由交换机通过先进的第三代高性能引擎可硬件支持策略路由、IPV6 等协议，并可扩展支持 MPLS、load balancing、NAT、VPN、

Firewall、IDS、web cache redirect 等丰富的业务功能。

➤ 病毒和攻击防护

面对现在网络环境越来越多的网络病毒和攻击威胁，RG-S6800E 提供强大的网络病毒和攻击防护能力：提供对发往 CPU 的数据流进行流分类和流限速，避免病毒和攻击对 CPU 的影响；提供基于 SPOH 技术的 ACL 功能；支持防源 IP 地址欺骗、防 DOS/DDOS 攻击，防 IP 扫描等功能；

提供多端口同步监控技术，支持灵活的网络监控，提升网络监控能力。

➤ 接入安全

硬件支持 IP、MAC、端口绑定，提高用户接入控制能力；

支持 802.1X 技术，满足 6 元素绑定接入限制；

支持 IGMP 源端口检查及源 IP 检查，可有效控制非法组播源，提高网络安全；IGMP V3 支持通告主机希望接收的多播源的地址，避免非法的组播数据流占用网络带宽；支持基于端口速率百分比和端口速率的广播风暴抑制；

➤ RG-S6800E 提供多种流分类技术和多种 QOS 技术，包括 SP、WRR、CBQ、WFQ、CBWFQ、LLQ、WRED、CAR、Traffic Shaping、HOL、RSVP 等，为各种应用的带宽保障提供需要的支持技术。

➤ RG-S6800E 提供目前主流的四种万兆局域网传输标准：10GBASE-R、10GBASE-W、10GBASE-LX4、10GBASE-CX4，四种传输标准在数据链路层以上都相同，差别在于物理层。10GBASE-R 和 10GBASE-CX4 用于传统的以太网环境，10GBASE-R 采用光纤作为传输介质，10GBASE-CX4 采用同轴铜缆作为传输介质，而 10GBASE-W 可与 OC-192 电路、SONET/SDH 设备一起运行，保护传统基础投资，使运营商能够在不同地区通过城域网提供端到端以太网。10GBASE-LX4 则使用 WDM 波分复用技术进行数据传输。

➤ 支持 L2 VPN (QINQ)

RG-S6800E 支持 Service Provider vlan(Double Tagging、VLAN tunnel)，允许对交换数据进行二次 VLAN 标识，外层标识用于创建 VPN，提供链路选择，内层标识用于标识业务 VLAN 信息，实现在以太网环境中的 L2 VPN，解决了传统以太网环境无法提供数据传输安全控制的问题。

➤ 基于目的 IP 地址的策略路由

在拥有多条不同链路到达同一目的地址的网络环境中，使用基于目的 IP 地址的策略路由可以在多条链路间实现等值负载均衡和相互备份。

7.2.2 路由器

采用 RG-R3600 系列：

产品简介：RG-R3600 系列模块化中心路由器是锐捷网络公司开发的面向企业级的网络产品，采用模块化设计，提供了多个网络/语音模块插槽，支持种类丰富、功能齐全、高密度的网络/语音模块，可实现更多的组合应用。64 位的微处理器技术，使用 RGNOS（锐捷网络操作系统平台），提供了极其丰富的软件特性，支持哑终端接入服务，支持 IPv4/IPv6，VoIP 特性等，提供丰富的备份方案及 QoS 特性；硬件采用模块化结构，具有更高的处理能力和更大的接入密度，既可以在中小型企业网中担当核心路由器，也可以在大型网络中担当汇聚层路由器。适合大中型企业、金融体系、各大公司的办事处和中型 Internet 服务供应商的模块化多服务访问平台，可以实现大规模、高密度的专线、拨号、宽带和 IP 语音接入。RG-R3600 系列包含二款路由器：RG-R3642 和 RG-R3662。

特征与优势：

➤ 先进高效的硬件体系结构

采用高速 3 口 PCI 桥，前端总线带宽达到 2G；每个模块上可以支持 4 个以上的 PCI 设备；高效的硬件体系架构，配合 400M 的 MPC RISC CPU，软件执行效率比 PC100 内存速度快 1.33 倍的 PC133M 服务器专用内存，运行在稳定、高效、安全 RGNOS 软件平台上，RG-R3662/R3642 包转发率可以达到 350Kpps，远远高于业界同等档次的产品。RG-R36 系列路由器的高性能是业务的高性能，在处理各种业务时转发性能基本不会下降；

➤ 主机固化 2 个 10/100M 快速以太网口

主机固化两个 10/100M 快速以太网口，在不购买任何模块的情况下，便可以实现宽带互联。

➤ 模块化结构设计

RG-R3662 具有 6 个网络/语音模块插槽，RG-R3642 具有 4 个网络/语音模块插槽，支持种类丰富、功能齐全、高密度的网络/语音模块，可实现更多的组合应用。

➤ 强大的数据处理能力

采用先进的 PowerPC 通讯专用处理器，2G 带宽的 PCI 总线技术，包转发延迟小，

高效的数据处理能力支持高密度端口，保证在高速环境下的网络应用；

➤ 良好的语音支持功能

支持 G. 711、G. 723、G. 729 等多种语音编码格式，支持 H. 323 协议栈，可以和多家 VOIP 厂商的设备互通；支持实时传真功能；支持语音网守功能。

➤ 高效安全的终端服务

提供 64 位密钥的 RC4 加密，可以实现路由器到 UNIX 服务器之间的数据安全加密；提供固定终端服务登陆的功能，确保路由器上每台终端登陆时，每次得到的终端号都是固定的，有利于管理。

➤ 良好的 VPN 功能

➤ 支持 IPSec 的 VPN 功能；支持 GRE 的 VPN 功能；支持 L2TP/PPTP 的 VPDN 应用；1 在 NAT 应用下，支持 L2TP/PPTP 的穿透功能。

➤ 完善的 QoS 策略

支持 PQ、CQ、FIFO、WFQ、CBWFQ 等排队策略；支持设置语音数据包优先级，可以为中小型企业提供满足要求的、高性价比的多功能服务平台。

➤ 高可靠性

支持链路备份、路由备份等多种方式的备份技术，提高整个网络的可靠性；支持 VRRP 热备份协议，实现线路和设备的冗余备份；1 RPS 冗余电源支持。

➤ 高安全性

完善的防火墙技术，支持基于源目的 IP、协议、端口以及时间段的访问列表控制策略；支持 IP 与 MAC 地址的绑定，有效防止 IP 地址的欺骗；支持认证、授权、记录用户信息的 AAA 认证技术，支持 Radius 认证协议；支持动态路由协议中的路由信息认证技术，保证动态路由网络中路由信息的安全和可靠；支持 PPP 协议中的 PAP、CHAP 认证及回拨技术。

➤ 方便易用易管理

采用标准 CLI 界面，操作更简单；支持 SNMP 协议，配置文件的 TFTP 上传下载，方便网络管理；支持 Telnet/Console，方便的实现远程管理和控制；多样的在线升级，为将来的功能扩展预留空间。

7.2.3 防火墙

防火墙采用 RG-WALL 1000:

设备类型	千兆级防火墙
VLAN 支持	支持 VPN, VPN 并发通道数 10000tunnels, VPN 吞吐量 400Mbps
并发连接数:	2000000
接口类型	标配 2 个 10/100BaseT+2 个 1000BaseT 接口, 另 4 个扩展槽可选配千兆电口/千兆 SX 光口模块
主要功能	多线程代理方式, 实时的状态监控功能, 动态过滤技术, 支持网桥模式和路由模式以及 NAT 模式, MTBF (平均故障间隔时间): ≥50, 000 小时, VPN 网关, 防火墙功能, 扩展的状态检测功能、防范入侵.
最大吞吐量	3000Mbps
策略数	65535 个策略数

7.2.4 入侵检测系统

在连接外网上采用 RG-IDS 500:

最大监控流量	500Mbps
管理接口	1*100Base-TX
监控接口	1*100Base-TX 和 2*1000Base-TX

在内网采用 RG-IDS 2000:

管理接口	1*1000Base-TX
监控接口	1*1000Base-TX 和 3*1000Base-SX
最大监控流量	4000Mbps

优势和特点:

➤ 灵活响应

RG-IDS 提供了丰富的响应方式, 如: 向控制台发出警告, 发提示性的电子邮件, 向网络管理平台发出 SNMP 消息, 自动终止攻击, 重新配置防火墙, 执行一个用户自定义的响应程序。

➤ 简单易用

RG-IDS 安装简单, 升级方便, 查询灵活, 并能生成适合各级管理者任意需要的多种格式的报。告。

➤ 低误报率

RG-IDS 采用基于状态的应用层协议分析技术，同时允许用户灵活地调节签名的参数和创建新的签名，大降低了误报率，提高了检测的准确性。

➤ 全面检测

检测准确率高，能够识别一千多种攻击特征。

➤ 分布式结构

RG-IDS 采用先进的多层分布式体系结构，包括控制台、事件收集器、传感器，这种结构能够更好地保证整个系统的可生存性、可靠性，也带来了更多灵活性和更可伸缩性，适应各种规模的企业网络的安全和管理需要。

7.3 服务器选型

7.3.1 硬件选型

1) 磁盘阵列选型：

IBM TotalStorage DS6000：产品容量：67.2TB, 磁盘接口：2GB/S 光纤通道，主机端口：8，控制器数量：每系统 2 个，内存/缓存容量：每控制器 2GB 高速缓存/每系统 4GB 高速缓存。

2) 磁带库

TS3200 Tape Library Express Model：最大本机容量为 400 GB，最大压缩容量为 800 GB，磁带驱动器数为 1-2，磁带进出槽数为 3，磁带存放槽数为 48，最大本机传输率为 19.2 TB。

3) FTP 服务器、DHCP，DNS，WINS、VPN 服务器、OA 服务器、数据库服务器配置：

采用 IBM xSeries 335，其基本配置如下：CPU Intel Xeon 2.8GHz，533MHz 前端总线，处理机最大支持 2 个，高速缓存为 512K，内存可扩展，最小 512K，最大 8G，扩展插槽 2 个 64 位/100MHz PCI-X (一个全长，一个半长)，磁盘控制器为 Ultra320 SCSI，4 个托架，2 个薄型热插拔，1 个软盘驱动器，硬盘驱动器可扩展 0~293.6G，集成 SCSI RAID1，集成双 10/100/1000M 以太网卡，1 个串口，3 个 USB 接口，2 个以太网接口，1 个 C2T 入口，1 个 C2T 出口，1 个 RS485 管理端口，电源功率为 332W，一个 CD-ROM 型号为 24X-10X IDE。

4) VOD 和 WEB 服务器配置：

采用 IBM xSeries 346，其基本配置如下：2 路 Intel® Xeon™ 处理器(1MB L2 缓存)，通过更高的处理性能来提升工作效率，800MHz 前端总线加速系统内的信息访问，Intel 的 EM64T 实现 64 位扩展，允许应用程序寻址更多的内存，快速 400MHz

PC2-3200 DDR2 内存，最多支持 6 个 Ultra320 热插拔硬盘驱动器，支持高达 880G 的内置存储，4 个可用的 PCI I/O 插槽(2 个 64 位 133MHz PCI-X 插槽和 2 个 low profile 64 位 100 MHz PCI-X 插槽)，支持内置磁盘驱动器选件，通过支持 PCI-Express 来升级 I/O,通过支持 SCSI 硬盘驱动器 RAID 来增强系统可用性和数据保护，无需使用 PCI 插槽，集成双 10/100/1000 以太网卡，集成 DVD-ROM 驱动器，带有热插拔/冗余电源和风扇，支持可选的 IBM Remote Supervisor Adapter II Slim Line 卡，三年现场有限部件和人工保修。

7.3.2 软件选型

1) 服务器操作系统

服务器操作系统，又名网络操作系统。相比个人版操作系统，在一个具体的网络中，服务器操作系统要承担额外的管理、配置、稳定、安全等功能，处于每个网络中的心脏部位，其网络操作系统的别称也由此而来。

服务器操作系统主要分为四大流派：WINDOWS、NETWARE、UNIX、LINUX。

➤ WINDOWS 服务器操作系统大家应该都不会陌生，这是全球最大的操作系统开发商——Microsoft 公司开发的。其服务器操作系统重要版本 WINNT 4.0 Server、Win2000/Advanced Server、Win2003/Advanced Server, 也支撑起目前市面上应用最多的服务器操作系统——Windows 服务器操作系统派应用。

a) WINNT 4.0

WINNT Server 可算得是开了直观、稳定、安全的服务器平台的先河。

当 Windows 操作系统以第一人性化的操作界面占据大片江山的时候，Windows 系列产品在当时的主流的 95、97 系列中表现出的频繁死机、后门敞开等问题，却成为竞争对手与用户同时攻击的对象。痛定思痛，在经过很长一段时间的闭门练功之后，Microsoft 对自己的 Windows 系列产品与竞争对手的产品经过各方位测试比较，总结各自的优缺点，融入新的安全观念，在人性化的直观操作基础上，开发出影响深远的新技术 NT 架构内核。尽管由于技术的发展，后来的业内人士还是找出其中不少的缺点，但是其 NT 内核技术的开发与操作直观、安全等理念的实现，对于服务器操作系统的发展来说，仍然具有划时代的意义。时至今日，虽然 Microsoft 已经取消了对 NT 版本的升级服务，但一些怀旧和追求简单实用功能的 IT 人士，还是在一些特定的应用中使用到它。

优点：操作直观，易于使用，功能实用，安全性能比较好，可用于单一的防火墙

等服务器上。

缺点：运行速度慢，功能不够完善，当进行超出系统处理能力的多项并发处理时，单个线程的不响应将会系统由于不堪重负产生死机现象，需要对服务器进行重启操作，Microsoft 已停止对其进行所有升级服务，市面上已无正版产品的销售。

b) Win2000/Advanced Server

Win2000/Advanced Server 是在 NT 技术上发展起来的，当越来越多的人指责 NT 系统运行速度慢如蜗牛时，Microsoft 对 NT 内核的壳部分进行了很大程度的响应与传输优化，并在 NT 基础上增加了很多的附加管理功能，这样就诞生了 Win2000/Advanced Server 的初始版本(Advanced Server 版本相对 Server 版本所具有的管理功能更加全面)。Win2000 系列服务器操作系统秉承了 Windows 一贯的直观易用的优良传统，并在原有的基础上实现了速度与功能的提升，在安全上也修补了所有以往的后门，是目前为止 Windows 服务器操作系统中市场使用最普遍的一款服务器，为 Windows 市场份额的直线提升立下了汗马功劳。但随着时间的推移，Windows 一贯的后门失守现象也越来越多的呈现在大众的面前，而且目前 Microsoft 公司也已经停止此系列产品的销售与系统升级服务，不免使得很多仍执着跟随的朋友产生了很多遗憾。

优点：操作直观，易于使用，功能随着时代的发展具有大幅的提升，管理更加全面，相对 NT 版本，当单个线程不响应时，其他线程的处理仍然可以继续运行，系统无需重启，现代社会的很多应用仍然能够实现。

缺点：运行速度虽然较 NT 版本有不小的提升，但是在有一部分追求完美的应用者来说，仍然有恨铁不成钢的情绪；由于是在原有完整 NT 内核的基础上对所有的高端功能应用进行开发的，系统的稳定与安全性有部分的削弱；Microsoft 已停止对 Win2000 系列服务器销售与升级服务支持。

c) Win2003/Advanced Server

Win2003/Advanced Server 继承了有历以来最具人性化的 WinXP 界面，对于原由内核处理技术进行了更大程度的改良，在安全性能上相对以前版本也有很大的提升，在管理功能上增加了许多流行的新技术，目前在 Windows 系列服务器中，其实际应用的比例与 2000 系列服务器产品基本相当。

优点：操作易用性是除了 XP 以外最人性化的版本，安全性是目前为止 Windows 全系列服务器产品中最好的，线程处理速度跟随硬件的发展有不小的提升，管理能力

也有不小的提升，是目前 Windows 服务器中主流产品。

缺点：安全性能仍有待更加完善，由于管理功能的增加，需要处理的线程更加繁杂，如果使用同样的硬件，2000 系列比 2003 系列产品在处理速度上会稍快。

➤ NetWare 服务器操作系统对现在一些 IT 圈里的朋友可能就比较陌生，由于种种原因，它的市场占有率已经非常局限，主要应用在某些特定的行业中。也就是因为此，在很多朋友在划分操作系统派系的时候，去除了 NETWARE 的代表权。其实，如果 80 年代前出生的老 IT，对于 NetWare 这个名词就会异常熟悉了，因为在当初各种设备和网络都比较落后的年代，NetWare 在局域网应用中占据着绝对的高额市场；而就算是目前，在一些特定行业和事业单位中，NetWare 优秀的批处理功能和安全、稳定的系统性能也有很大的生存空间。NetWare 目前常用的版本主要有 Novell 的 3.11、3.12、4.10、5.0 等中英文版。

Netware 服务器操作系统的诞生比较早，在信息发展相对比较落后的年代，由于其对当时主流操作系统 DOS 命令的兼容，让很多使用者的入门与提高非常容易，这样就使得其对市场的推广更加有利。而当其版本一代代进行升级后，越来越多的人看到了它对基础设备低要求、很方便的实现网络联接与支持、对无盘工作站的优化组建、支持更多应用软件的优势。这样，随着时间的推移，Netware 就渐渐成长成为当时局域网服务器操作系统的一方霸主。

随着信息技术的进一步前进以及 Windows 系统的出世，便宜性的人性化操作系统时代趋势挡住了其前进的步伐，并一再迫使其业绩走向滑坡。在目前社会的应用中，只有在金融这些需要无盘工作站的特定行业以及设备成本预算比较少的教育部门、小型企业等还维系其生存。

优点：操作相对方便，对设备的要求很低，对于网络的组建具有先天的优势，相对 DOS 能够支持更多的应用，能够支持金融行业所需的无盘工作站同时节省成本，能够支持很多游戏软件的开发环境搭建，系统稳定性和 Unix 系统基本处于对等水平。

缺点：由于操作仍然大部分依靠手工输入命令来实现，人性化显得比较弱势；对于硬盘的识别最高只能达到 1G，无法满足现在社会对于大容量服务器的需求；各版本的升级只是实现了部分功能的实现与软件支持，没有更深层次的技术革新。

➤ Unix 服务器操作系统由 AT&T 公司和 SCO 公司共同推出，主要支持大型的文件系统服务、数据服务等应用。由于一些出众的服务器厂商生产的高端服务器产品中甚至只支持 Unix 操作系统，因而在很多人的眼中，Unix 甚至成为高端操作系统

的代名词。目前市面上流传的主要有 SCO SVR、BSD Unix、SUN Solaris、IBM-AIX 。

a) SCO SVR、BSD Unix

Unix SCO SVR 就是 Unix 技术创始人之一 SCO 公司的产品。由 SCO 公司开发的 Unix SCO SVR 和由 AT&T 主导的 BSD Unix 能够支持所有 Unix 系统都能实现的网络大型文件系统、数据库系统的支持，并且随着时代发展，能够支持越来越多的软件应用。此外，由于 Unix 系列的所有系统都属于非开源代码，而其系统的技术研发层面没有得到更多的推广，在外界对其知晓并不是很多的情况下，其本来就高高在上的系统稳定性与安全性地位就更加显得无法动摇。

优点：系统安全性与稳定性犹如业界无法动摇的泰山，能够支持大型文件系统与数据库系统，处于技术创始人地位的两位元老级 Unix，一直在业界受到无数人狂热的追捧；

缺点：所有操作都需要输入代码式的命令触动，人性化显得非常差，这样也绊住了其对于中低端服务器市场的发展；虽然厂家位于技术创始人的地位，而且产品对于应用软件的支持一直都有所改善，但是临到后来，因为其本身的高端服务器操作系统定义，深层的技术研发没有得到更多的推广，导致这些改善的结果并未有太大的起色。

b) SUN Solaris、IBM-AIX

之所以把以上的四家产品只分为两组来谈，主要原因是笔者以实际应用的角度来看：四者其实都是定位于高端服务器操作系统市场的，在实际应用中，四者在处于高端定位上的技术差别非常微小，如果非要分一个具体的差别，那就从四位历史的起源与科技的进一步发展状况来区别——SCO 与 AT&T 属于创业始祖，SUN 与 IBM 属于后来居上者。而从结果中所得的猜测是，由于本组所谈的这两者的服务器产品市场占有率稍高，服务器厂商对于己身的服务器操作系统支持比较足够，这就对两这服务器的市场占有率和技术含量起了很大的推动力。

优点：支持大型文件系统与数据库，传承了 UNIX 一贯的高能级系统安全性、稳定性，对于系统应用软件的支持比较完善。

缺点：沾染了 Unix 系操作系统的通病，人性化界面肯定谈不上好了；由于 IBM-AIX 属于非开源代码，技术层面未能得到有效推广，使得相关维护人员的雇佣成本比较高，不利于占有率更多的中低端市场的进一步推广与普及；SUN 对于源代码的开放时日尚短，目前也还没有享受到开源代码比较新颖的技术创新推动；两者面向企业的服务器端都是采取收费服务的方式，用户在享受两家高稳定性与安全性的硬件产品同时与服

务器操作系统技术支持服务之时，“物美价廉”的想法是可以作罢了。

➤ Linux 服务器操作系统是国外几位 IT 前辈，在 Posix 和 Unix 基础上开发出来的，支持多用户、多任务、多线程、多 CPU。Linux 开放源代码政策，使得基于其平台的开发与使用无须支付任何单位和个人的版权费用，成为后来很多操作系统厂家创业的基石，同时也成为目前国内外很多保密机构服务器操作系统采购的首选。目前国内主流市场中使用的主要有 Novell 的中文版 Suse Linux 9.0、小红帽系列、红旗 Linux 系列等。

a) 小红帽系列、红旗 Linux

Linux 在中国的商用，很大程度上是政府采购的推动。考虑到机密数据的安全性，在前几年的一次政府采购中，具有开放的源代码基础的 Linux 操作系统似乎意外但也带有些必然性的中标，对于服务器操作系统市场来说，无意于引起了一场大地震，而官方获利最大的红旗和民间流传最广的小红帽也就成为国内 Linux 系统的代表。但其在真正的使用中，除了在图标与细枝末节的功能差别外，这两个 Linux 厂商代表的核心技术都是无差别化的雷同。

优点：源代码的开放，使得该类服务器操作系统的技术完善从民间得到了其他厂商无法比拟的雄厚力量，在此基础上所形成的一件服务器操作系统成品是任何力量都不可忽视的，因而其所具有的兼容、安全、稳定的 Linux 特性也是其他服务器操作系统厂商不容易实现的；Linux

缺点：由于其是基于 Unix 系统所做的开发修补，属于类 Unix 模式，这就决定了其系统的兼容性相比其他服务器操作系统兼容的软件来说，还是具有一定差距的；Linux 的操作基本也是利用输入代码命令进行应用实现的方式，使得其在人性化方面还是处于相当的劣势，其后果必然导致维护成本的相对偏高。

b) Suse Linux

Suse Linux Enterprise Server10 在 3D 模式启动状态下的视频播放

其实在本组中笔者要提到的是 Suse Linux10，不过因为其推出的时间只是上月末，离现在刚刚半个月的时间，在市面上最多的还是它的前辈 Suse Linux9.0，所以笔者在之前 Linux 技术与产品介绍中提到的只是大家都比较熟悉的 9.0 版本。

很幸运，在 Novell 将 Suse Linux10 正式发布后第二天，笔者一位同事通过一些渠道获得其试用版，并且在笔者身旁做完了长达三天的测试，笔者也切身体验了这个结合 Linux 开源与微软人性化的新服务器操作系统。以下的优缺点分析也就是笔者要

谈到的 Suse Linux10 的特点。

优点：具有 Linux 一贯稳定、安全的系统性能，兼容性相对目前主流的服务器操作系统也有很大的提升，具有相当于微软系列操作系统般的人性化设计，增加操作系统中绚丽而高难的三维立体空间显示，属于另一个划时代的产品。

缺点：虽然相对以前各家的软件兼容性有不小的提高，但因为市场中对于 Linux 系统支持的软件开发商本来就不多，所以它还是延续了 Linux 兼容性暂时差于微软的特性：系统所需的立体空间显示技术，并不是如同发布会当天 Novell 发言人所说的那样，只需要四五年前的主流 PC 的 CPU 性能和主板集成的显卡就可以完成。笔者看到的实际情况是，在微软系统中播放正常的一集美国大片，当在 Suse Linux10.0 上以三维立体空间技术播放时，播放了不到 30 秒钟，音频就一帧帧的跳着继续，视频更是好象播放划花的盗版光碟一样，在显示器上显示一个大花脸和不断颤动的波纹。

通过比较上述四种服务器操作系统，根据本方案的服务器规格、网络配套、软件应用、成本计算等因素来考虑，除了 VOD 服务器、OA 服务器采用 Windows 2003 Advanced Server 之外，其余服务器全部全部使用 redhat linux 9.0。

2) 服务器软件

➤ 主流 Web 服务器比较

a) Apache 1.3.19

Apache 仍然是最伟大的全能选手，也许它有些过于庞大、历史悠久，但是其优秀的性能和大量用户群，它应该会有更好的发展。就它灵活性和丰富的特性功能而言，Apache 相对于这里测试的其他 Web 服务器来说可以说是 Web 服务器的标准。除非你在过去的四年里与这个世界相隔离，否则一定会看到大量的新闻文章欢呼 Apache 的成功，并将其作为开放源码成功的典范。Apache 并不是采用 GPL 版权声明，而是采用自己的 Apache Server 版权声明，其强调自由地使用源代码。Apache 同样以“补丁服务器”而闻名，主要是因为早期 Apache 的开发是通过对 NCSA 的 httpd 代码添加补丁程序来进行的。Apache 被看做是“补丁服务器”还因为它具有模块化特性，该特性实现了 Apache 的灵活性和可扩展性，而且开发者可以利用该特性很容易地添加第三方功能模块，通过模块开发人员可以添加任何功能，模块是很多内容管理系统的功能基础，如 Midgard, Zope 等。

几乎所有的 Linux 发布都安装 Apache 作为默认配置。SuSE 7.1 甚至预安装有包括各种高级模块选项的 Apache，如 PHP3, mod_perl 和 LDAP 等等。用户会惊奇地发

现系统安装成功就会有一个功能强大的 Web 服务器可供选择。虽然安装 Apache 并不是非常简单，但是如果有具有新的特性或安全补丁的 Apache 发布，则下载源代码包并编译新的 Apache 是值得的。Apache 不但具有庞大的用户群基础，并且有丰富的配置使用文档。

很多地方都声明 Apache 并不是最快的 Web 服务器，Apache 的开发者的确是没有过多地考虑其开发一个超快的 Web 服务器。而功能和稳定性则是考虑更多的因素。然而 Apache 在很多负载很大的站点中运行非常正常，并没有得到过多的关于性能的抱怨。在我们使用 Webstone 进行性能测试中，发现 Apache 的吞吐量位居第一，并且出错最少。在测试中虽然 Apache 的可扩展性不知最强，但是仍然是提供了如此多特性的服务器中速度最快的。

b) Zeus Webserver3.3.8 服务器

Zeus 是一个商业化的 Web 服务器产品，最近它成为很多业界媒体中的头条新闻，因为有消息宣称 Zeus 服务器的性能在 2.4 内核+SMP 环境下相对于 2.2.x 内核环境下性能提升了 85%之多。速度永远是 Zeus 服务器的卖点。常常有评论说如果希望对 Linux 进行其作为服务器操作系统的性能测试，那么就运行 Zeus 进行测试。

Zeus 服务器在 SMP 环境下有优秀的可伸缩性，并实现了常见的特性集合，如访问控制、动态内容产生和安全等。它具有健壮、集成有集群支持的容错和负载平衡等特色，是高端应用的很好的选择。

Zeus 服务器的安装和管理相对比较简单。软件是以 tar.gz 格式的包格式，安装软件只需要解压软件包并运行一个安装脚本，在性能适当的机器上安装过程只需要几分钟。而且 Zeus 服务器安装以后提供 Web 方式的远程管理功能。

其功能可以与 Apache 匹敌，包含易于实现的 SSL 安全特性和其他有用的特性，如带宽控制等等。Zeus 宣称支持 PHP 和 Java Servlets。虽然易于使用的管理界面在某种程度上模糊了这些高级的配置特性。PHP4 可以通过 Zeus 支持的 API 方式(NSAPI)来运行，也可以通过 CGI 发给你是来运行。但是很多用户报告这种 API 方式存在稳定性问题。

c) iPlanet Enterprise Edition 4.1

Netscape 公司为不同操作系统平台开发了多种 WEB 服务器，但到最近它才发布了自己在 Linux 下的产品。曾经非常流行的 Netscape Enterprise Server 现今被运行在 Linux 下的同类产品 iPlanet Enterprise Edition 所替代。iPlanet 是 SUN、

Netscape 和 AOL 公司联合生产的 WEB 产品，它被力图设计成高性能、跨平台的 e-commerce 产品。iPlanet 和其它 Netscape 产品一样具有很高的性能，而且 iPlanet 具有 SUN 公司 Java 的特性。

iPlanet 可以自由下载评估版使用，也可以购买正式版本。因为在压缩包中包含 Java 的运行环境 JRE，所以 iPlanet 的压缩包相对较大。压缩包被解压后，一个基于 shell 的简单安装工具可以帮助用户完成 Administration 服务器和 Web 服务器的安装。所有关于安装的信息都在这个时候输入，当然你也可以选择安装的选项，如选择安装 Java 组件或者 LDAP 目录，以便以后利用 LDAP 管理用户和组。

现在 WEB 服务器和 WEB 应用程序服务器之间的界限变得越来越模糊，iPlanet 象其它专业 WEB 服务器一样也支持 JAVA API，以便提高自己的性能。Enterprise Edition 4.1 本身内置 JRE，可以和大多数的数据库互联，它也支持 JSP 1.1 的 API、Serverlets 2.2 的 API 和 Livewire。它拥有功能强大的软件包，其功能远远超过了动态脚本语言。Enterprise Edition 4.1 同时也支持传统的脚本方式，如 CGI、NSAPI，因而可以没有任何问题、方便的从其它产品迁移到 iPlanet。

iPlanet 具有现今高性能 WEB 服务器的特性，相对其它 WEB 服务器 iPlanet 还提供更多的 JAVA 功能。在 WebStone 环境中测试，iPlanet 的性能非常良好。虽然 iPlanet 有时会因服务器端未能响应客户端的请求而在客户端产生许多错误，但是它的吞吐量和响应时间性能卓越。作为一个昂贵的 WEB 服务器产品，希望能看到以 WebStone 作为测试基准的更多的测试结果。如果你在寻找能够运行标准 Java API，并且在 Java API 环境下运行速度良好的 WEB 服务器产品，iPlanet 当是你的首选

d) AOLserver 3.3.1

AOLserver 是一个多线程、可升级和扩展的 WEB 服务器。AOLserver 服务器使用简单而且功能强大的 Tcl 作为其内嵌式的脚本语言和服务器端的 API。就像名字所表明的那样，AOLserver 在 AOL 公司的在线服务中得到了广泛应用，随着 AOL 公司本身的发展，AOLserver 也增添了更多的特性，其速度也得到了显著提高。和其它大公司一样，AOL 公司也公布了 AOLserver 的所有源代码。该源代码遵循 AOL 公司自己的 AOLserver 版权声明，同时 AOL 公司也从此种开放式开发模型中获益。

和 Apache 相比，AOLserver 也支持源代码公开、性能也非常优异，它们都可以通过模块方式添加新的功能，但是 AOLserver 却支持 Tcl 语言，而且以不同的方式和数据库互连。AOLserver 可以连接和使用后台的关系型数据库(RDBMS)，例如 Oracle，

PostgreSQL 等。AOLserver 在 UNIX 系统中作为单个进程运行，从而使得 Web 服务器可以共享数据库连接，进而使得运行在 AOLserver 中的脚本语言拥有更高的速度。AOLserver 的脚本语言也可以通过一个抽象层同时访问许多数据库管理系统。

AOLserver 可以免费从 AOL 的官方网址或者它的开发站点 Sourceforge 下载。只要把 AOLserver 的压缩包解压，就可以非常简单的使用 gmake 编译和安装 AOLserver 服务器、可选模块、Tcl 库、工具软件及其响应文档。用户可以使用 config.tcl 配置 AOLserver 的环境。用户也可以如 Apache 那样，安装和管理权限控制、CGI、SSL 和数据库连接等模块。刚开始的时候，用户可能无法完全清楚、正确的安装和设置“软”（基于域名）虚拟服务器。AOLserver 的文档非常完整详细，但是有点略微繁琐。它包括了安装、配置的方方面面和 Tcl API 的详细说明。但是 AOLserver 并不支持基于 HTTP 1.1 的软虚拟服务器。

在许多测试环境下，AOLserver 的表现并不能令人满意。在 WebStone 环境测试 AOLserver，会出现许多错误，还有相当多的客户无法连接到 AOLserver 服务器。虽然以上的问题会使人认为 AOLserver 的性能很差，但是在负载相对较小情况下进行的测试结果并不能完全令人信服。

e) Roxen WebServer 2.1.31

当说到适应动态网页内容这个问题时，我们又使用了模块 k 化这个名词。Roxen 服务器使用了一个服务器端的语言 Pike，利用 Pike 既可以为 Roxen 开发全新的模块，也可以嵌入到 Roxen 系统中。Pike 是解释性语言，语法和 C 语言非常相似。因为 Pike 是在以前写 MUD 游戏的语言的基础上发展起来的，因而它在安全认证方面非常出色。Pike 无论从编程风格还是语法特点上都和 C 语言很接近，所以一个标准的 C 语言程序在很短的时间就可以改写成 Pike 程序。作为一个解释语言，Pike 当然比编译性语言 C 的速度要慢，但是它的调试相对简单而且开发周期也很短。在 Roxen 服务器环境下，使用 Pike 语言生成动态网页内容，速度会有所提高。

就象其它的 WEB 服务器一样，Roxen 也允许使用基于浏览器方式完成服务器配置工作。这种配置方式拥有流行的、简单的菜单系统，使用这些菜单可以设置系统的所有选项。Roxen 中也有丰富的帮助文件，这些文件涵括了 Roxen 和 Pike 的方方面面。通过模板或不使用模板生成一个新的站点都可以配置“硬”（基于 IP）虚拟服务器。模板就是 Pike 模块的基本列表，利用这些模板就可以设置 Roxen 的不同功能。任何站点或者服务器必须设置和运行特定的模块，并使用它们管理站点的内容。一个站点必

须包括文件系统模块和目录模块。利用文件系统模块可以设置文件的根目录，目录模块则管理索引文件和目录列表。在 Roxen 系统中，用户可以根据需要检查每个模块的配置内容和安全性信息。

在任何 Roxen 站点中都可以添加带宽控制、代理、中转服务等外来模块及兼容性、数据库连接、Java、PHP4 和 Perl 语言的支持模块。

Roxen 管理服务器允许同时登陆管理和 WEB 服务，并对其进行全面监控。Roxen 还提供 SSL 安全机制。对于那些习惯 Apache 系统的用户来说，安装 Roxen 可能得费些功夫。但是一旦习惯了使用 Roxen-Pike，你就会觉得 Roxen 强大的功能也是颇令人喜欢的。

f) Jigsaw

你不可能再找到象 Jigsaw 那样适应未来需要的 WEB 服务器了。它由 WWW 组织 (W3C) 开发，W3C 组织负责研究和规定网络协议的标准 (如 HTTP)。Jigsaw 刚开始被设想成 HTTP 1.1 的运行环境。它使用 JAVA 语言开发，是成功的面向对象、功能全面的服务器。因为 Jigsaw 不受测试平台的限制，所以 Jigsaw 是一个具有活力的、拥有无限潜能的优秀 WEB 服务器。

Jigsaw 使用 JAVA 作为开发语言，因而它可以方便地在所有支持 JAVA 的平台上运行。通过使用模块化的方法，Jigsaw 具有更高的灵活度和可扩展性，可以动态的把模块加入服务中。Jigsaw 利用面向对象的方法设计和开发，因而所有资源包括 CGI 脚本和文件都被视为对象，从此不难看出 Jigsaw 在未来的前景。

一旦下载了必需的 JDK (或者 SDK) 和最新的 Jigsaw 版本，安装 Jigsaw 将会非常的简单。在 Jigsaw 服务器中，帮助用户设置 Jigsaw 环境、运行服务和编译特性文件的帮助文件非常有限。但是以上的系统设置并不是很难，用户可以在几分钟完成这项工作。本地或者远程用户都可以通过浏览网页获取设置 Jigsaw 管理服务器的详细信息。

JigAdmin 拥有友好的图形控制界面，利用它可以控制本地的 Jigsaw 管理服务器。JigAdmin 有许多命令选项，其可控制的功能相当的复杂，用户可以利用它管理 Jigsaw 管理服务器和 http 服务器。JigAdmin 使用不同的树型结构代表 doc space, indexers, properties 和 realm 等的相关内容。doc space 很明显是关于 JigAdmin 的目录和文件结构。properties 指代的是 servlet 和 loggind 等的服务特性。realm 和 indexers 则对用户不透明。直观的理解这些资源的意义是很不现实的。即使你对

面向对象结构不太熟悉，仍很有必要全面的阅读 JigAdmin 的文档，因为 JigAdmin 中的很多概念难以掌握。

综上所述 Apache 占据了市场的大部份，多数 Linux 厂商和媒介机构都推荐使用 Apache 产品。在 WebStone 环境的测试数据表明，在吞吐量、客户连接数和出错率方面，Apache 比其它产品性能优异。

考虑服务器对动态脚本语言、API 的支持和数据库连接的性能等方面，本方案采用 Apache 做 Web 服务器软件。

➤ Vod 服务器软件

Helix.server(也就是 REAL 服务器)的开源版本，RM 媒体流服务器，没有任何限制的版本. 支持 RTSP 协议, 支持 RM, MP3 等格式, 即便是商业用, 也能应付的来, Windows 2003 中搭建、配置与管理 Helix Server 视频点播服务器。

➤ 其它服务器软件

FTP 服务器、DHCP, DNS, WINS、VPN 服务器、数据库服务器全部使用 redhat linux 9.0 系统上自带组件。

8. 总结

本文以计算机网络技术和高性能网络系统集成理论为基础，以城域网通信平台——资源平台——网络安全与管理平台——网络应用平台为轴线，以地/市教育信息化需求为根本，结合各地/市教育系统的现状，就教育城域网系统的基本构成、设计思想提出了自己的观点，对地/市教育城域网系统的整体结构、城域网通信平台、城域网用户节点、城域网管理和服务中心等进行总体规划设计。通过本文的设计，可以为各地/市教育城域网建设提供理论依据和建设参考。

当然本系统还有许多需要进一步完善和改进的地方：

1、由于本方案没有结合某个具体的地/市教育城域网建设的实际来讨论，所以还需要根据特定地/市教育城域网建设中进一步完善。

2、限于文章篇幅，没有具体讨论流媒体技术、视频会议技术、虚拟学习环境技术、VOD 技术、VoIP 技术在教育城域网中的应用。

3、虽然当前计算机互联技术正处在 IPv4 向 IPv6 过渡的重要时期，但是，本文还是以 IPv4 理论为基础，完成了海口市教育城域网系统的设计工作。至于 IPv6 给教育城域网络建设带来的影响以及如何从目前的 IPv4 平滑过渡到 IPv6，文中没有体现。

地/市教育城域网系统的设计和建设，是一个长期的和逐步完善的过程。在以后各地/市教育城域网系统设计和建设项目具体实施过程，不断完善教育城域网体系各部分的详细设计，形成地/市教育城域网系统设计体系。

9. 致谢语

本文从拟定题目到定稿，历时数月。在本论文完成之际，首先要向我的指导老师*老师致以诚挚的谢意。在论文的写作过程中，*老师给了我许许多多的帮助和关怀。在*老师的悉心指导下，我不仅学到了扎实的专业知识和实践技能，也在怎样处人处事等方面收益很多。在此我谨向*老师表示衷心的感谢和深深的敬意。同时，我要感谢我们学院给我们授课的各位老师，正是由于他们的传道、授业、解惑，让我学到了专业知识，并从他们身上学到了如何求知治学、如何为人处事。我也要感谢我的母校*院，是她提供了良好的学习环境和生活环境，让我的大学生活丰富多彩，为我的人生留下精彩的一笔。另外，衷心感谢我的同窗同学们和大学的朋友们，在我毕业论文写作中，与他们的探讨交流使我受益颇多；同时，他们也给了我很多无私的帮助和支持，我在次深表谢意。最后，向我的亲爱的家人和亲爱的朋友表示深深的谢意，他们给予我的爱、理解、关心和支持是我不断前进的动力。学无止境。明天，将是我终身学习另一天的开始。

10. 参考文献:

- [1]锐捷网络认证中心. 设备调试与网络优化[M]. 锐捷公司, 2005
- [2]肖帅领, 窦西河. 网络工程与实施[M]. 北京. 中国林业出版社, 北京希望电子出版社. 2006
- [3]程庆梅, 刘旸. 现代网络信息技术(下)[M]. 北京. 北京科学技术出版社. 2004
- [4]安淑梅, 武志刚. 网络设备与管理[M]. 北京. 北京希望电子出版社. 2006
- [5]雷震甲. 网络工程师教程(第二版)[M]. 北京. 清华大学出版社. 2006
- [6]杨文志. Red Hat Linux 9 网络服务[M]. 北京. 机械工业出版社. 2005
- [7]Sean Convery, CCIE No. 4232. Network Security Architectures[M]. 人民邮电出版社. 2005
- [8]安淑梅. 网络发展二十四史——模块抽取式网络实验指导书[M]. 创新网络技术. 2007
- [9]http://www.cublog.cn/u/25994/showart_207255.html(细说网络负载均衡技术)
- [10]<http://www.qqread.com/z/server/seting/>(服务器的配置)
- [11]<http://www.ruijie.com.cn/list.aspx?categoryid=54>(普教行业应用案例)
- [12]<http://itpapers.zdnet.com.cn/itpaper/detail/2/13422.shtml>(路由器的配置)
- [13]<http://www.it.com.cn/f/server/079/17/478948.htm>(VPN 服务器的配置)
- [14]<http://info.edu.hc360.com/2006/11/240932103621-4.shtml>(交换机端口镜像的配置)
- [15]http://www.net130.com/CMS/Pub/Tech/tech_zh/2007_03_19_99378_3.htm(访问控制列表的配置)