**成都信息工程学院**

**课程设计**

**题目：校园网安全整体解决方案设计**

|  |  |
| --- | --- |
| **作者姓名：** | **雷继红** |
| **班 级：** | **信安081班** |
| **学 号：** | **2008122021** |
| **指导教师：** | **张路桥** |
| **日 期：** | **2011年 12 月 15 日** |

作者签名：

目录

[1.绪论 - 1 -](#_Toc311692663)

[1.1课题背景 - 1 -](#_Toc311692664)

[1.2校园网的发展 - 2 -](#_Toc311692665)

[2.校园网的发展现状与分析 - 2 -](#_Toc311692666)

[2.1校园网现状 - 2 -](#_Toc311692667)

[2.2校园网安全需求 - 3 -](#_Toc311692668)

[2.3校园网安全面临的威胁 - 4 -](#_Toc311692669)

[3.校园网安全设计策略 - 5 -](#_Toc311692670)

[3.1校园网安全管理 - 5 -](#_Toc311692671)

[3.2校园网络安全技术 - 6 -](#_Toc311692672)

[3.2.1杀毒产品的部署。 - 6 -](#_Toc311692673)

[3.2.2采用VLAN技术。 - 6 -](#_Toc311692674)

[3.2.3内容过滤器。 - 6 -](#_Toc311692675)

[3.2.4防火墙。 - 6 -](#_Toc311692676)

[3.2.5入侵检测。 - 7 -](#_Toc311692677)

[3.2.6漏洞扫描。 - 7 -](#_Toc311692678)

[3.2.7数据加密。 - 7 -](#_Toc311692679)

[3.2.8加强网络安全管理。 - 7 -](#_Toc311692680)

[4.本校网络拓扑图 - 8 -](#_Toc311692681)

[4.1.简化拓扑图 - 8 -](#_Toc311692682)

[4.2VLAN技术的虚拟实现 - 9 -](#_Toc311692683)

[4.3防火墙功能的实现 - 9 -](#_Toc311692684)

[4.4地址映射的实现 - 9 -](#_Toc311692685)

[5.总结 - 10 -](#_Toc311692686)

[参考文献 - 10 -](#_Toc311692687)

# 1.绪论

## 1.1课题背景

校园网作为学校信息化建设的基础设施，在教学、科研、管理和对外交流等方面都起着举足轻重的作用。随着高校网络规模的急剧膨胀，网络用户的快速增长，网络数据的急剧增加，校园网的安全问题也不断暴露出来，如病毒侵蚀、恶意软件、黑象攻击等，校园网时刻都会受到来自内部和外部的威胁与危害，针对校园网的安全向题，构建完善的网络安全体系是越来越重要。而且校园网与其它网络比具有以下一些特点:

(1)校园网的数据流量大、速度快、规模大

近年来，随着高校扩招和合并，校园网的用户群体一般比较大，少则数千人、多则数万人。许多校园网已经发展为一个跨城域的网络。校园网已发展成为了一个全面信息的化阶段。多媒体教学和网络视频应用的推广对网络交换速度和数据量提出更高的要求，同时也要求网络安全部件要有更快的处理速度和更高的性能。

(2)校园网中的设备来源多样化、管理复杂

校园网是一个平台，面向高校的师生，校园网中的设备来源比较复杂。容易出现计算机病毒“交叉感染”，无法分清责任。

(3)活跃的用户群体

高校的学生是最活跃的网络用户，对网络新技术充满好奇，面对精力充沛的高校学生，网络安全更为迫切。

(4)有限的投入

校园网的后期管理容易被忽视，特别是管理和维护吧人员方面的投入明显不足，无暇顾及、也没有条件管理和维护千台、万台计算机的安全。

(5)盗版资源泛滥

从网络上随意下载的软件中可能隐藏木马、后门等恶意代码，许多系统因此被攻击者侵入和利用。

## 1.2校园网的发展

网络技术的发展，尤其是Internet的出现，使我们校园生活、学习、工作和环境发生了巨大的变化。利用学校计算机网络，采用先进的管理软件，可规范学校的管理行为，提高管理水平和工作效率；在减轻工作量的同时，利用计算机存储量大、处理快速准确的特点，为学校的决策提供准确及时的信息。在学校的办公、信息交流和通信方面充分发挥计算机网络的作用，在软件的支持下实现网上协同工作。

计算机网络将使教学模式上有比较大突破，原来的老师、学生和网络三者之间的关系将发生变化，教师不再是知识的惟一拥有者和权威者，把知识传授给学生。学生应是学习的主体，校园网为学生的探索式学习提供情景和资源，老师只作为学习的指导者。在教学过程中将采用网络技术、多媒体技术，利用网络上丰富的教学资源，激发学生的学习兴趣，提高教学质量。多媒体技术将文本、声音、图像、动画和视频技术融为一体，使的教学活动变得生动且形式多变，从而提高学生学习的积极性、效率和效果。

高校校园网早期应用主要局限于行政办公、后勤、教学与计算中心，分离性较大，大部分采用企业网模式。而现在大部分高校在规划校园网时已计划将网络覆盖至学生宿舍区以及教师家属区，向在校学生及教职工提供园区内部互连以及Internet接入服务。

# 2.校园网的发展现状与分析

## 2.1校园网现状

校园网网络信息十分丰富，网络用户的活动也非常活跃，校园网内部网络数据往往用于满足学校正常的行政办公需要、广大师生的教务教学需要、学生们的课余校园文化生活等等，这些无论是涉及个人隐私或利益的信息，还是学校行政办公的文档信息，以及用于政治宣传和管理的信息都需要进行完整性、真实性保护和控制，这就需要对进出校园网的访问行为进行必要的、有效性的控制，封堵某些禁止的行为和业务，避免损失。

校园网络系统中接入着成百上千台计算机，这些计算机的操作系统各种各样，通常分布在不同的物理位置，由不同的用户操作，用于不同的用途，由于这些差异，使得校园网网络中计算机中的漏洞问题十分严重。因为使用者的安全意识不强，或者采取措施不及时造成的损失在校园网网内时有发生，因此采用安全、及时的漏洞扫描技术对校园网网络中的系统漏洞进行扫描，在攻击发生之前发现网络和系统中的漏洞，并及时采取措施进行修复，可以进一步提高校园网络信息安全保障水平。

校园网接入互联网以后，用户通过校园网进入互联网。网络上的各种信息良荞不齐，色情、暴力、邪教内容的网站泛滥，对正在形成世界观和人生观的学生来说，有可能还不能正确地对待这类内容，这些违反人类道德标准和有关法律法规的有毒信息对他们危害极大，如果信息安全措施不好，不仅会有部分学生进入这些网站，还可能在校园内传播这类不良信息。

校园网网络的方便快捷同时也为病毒的肆意传播留下可能，下载的程序和电子邮件都有可能带有病毒。通过网络传播病毒无论在传播速度，还是破坏性和传播范围等方面都是单机病毒不能比拟的。大量病毒传播不仅占用网络资源，而且破坏服务器或单机，最终影响整个学校网络系统的正常运作，严重的还可能造成校园网网络的瘫痪，因此邮件监控和防病毒工作也是校园网络信息安全的一个重要方面。

教育信息化、校园网络化作为网络时代的教育方式和教育环境，己经成为教育发展的方向。随着各高校网络规模的急剧膨胀、网络用户的快速增长，校园网网络信息安全问题已经成为当前各高校网络建设中不可忽视的首要问题。随着网络技术的发展与普及，校园网早已成为现代化教育建设的基础设施，校园网建设己经不仅仅只是局限于实现网络内部资源共享和外部信息互换。各学校为了能够实现以网养网，对网络设计提出了更高的要求，可运营、更安全、更实用成了今天对校园网络关注的焦点。

## 2.2校园网安全需求

第一，高校面临着严峻的网络安全形势。越来越多的报道表明高校校园网己意识的淡薄，而另一方面，高校学生—这群精力充沛的年轻一族对新鲜事物有着强烈的好奇心，他们有着探索的高智商和冲劲，却缺乏全面思考的责任感。有关数字显示，目前校园网遭受的恶意攻击，70%来自高校网络内部，如何保障校园网络的安全成为高校校园网络建设时不得不考虑的问题。

第二，网络安全一定是全方位的安全。首先，网络出口、数据中心、服务器等重点区域要做到安全过滤;其次，不管接入设备，还是骨干设备，设备本身需要具备强大的安全防护,要具备强大的安全防护能力，并且安全策略部署不能影响到网络的性能，不造成网络单点故障;最后，要充分考虑全局统一的安全部署，需要能够从接入控制，到对网络安全事件进行深度探测，到现有安全设备有机的联动，到对安全事件触发源的准确定位和根据身份进行的隔离、修复措施，从而能对网络形成一个由内至外的整体安全架构。

## 2.3校园网安全面临的威胁

校园网内的用户数量较大，局域网络数目较多，认真分析可以总结出校园网面临如下的安全威胁：  
 (1) 各种操作系统以及应用系统自身的漏洞带来的安全威胁；

(2) Internet网络用户对校园网存在非法访问或恶意入侵的威胁；  
 (3) 来自校园网内外的各种病毒的威胁，外部用户可能通过邮件以及文件传输等将病毒带入校园内网。内部教职工以及学生可能由于使用盗版介质将病毒带入校园内网；  
 (4) 内部用户对Internet的非法访问威胁，如浏览黄色、暴力、反动等网站，以及由于下载文件可能将木马、蠕虫、病毒等程序带入校园内网；

(5) 内外网恶意用户可能利用利用一些工具对网络及服务器发起DOS/DDOS攻击，导致网络及服务不可用；

(6) 校园网内的学生群体是主要的OICQ用户，目前针对OICQ的黑客程序随处可见；  
 (7)可能会因为校园网内管理人员以及全体师生的安全意识不强、管理制度不健全，带来校园网的威胁；

# 3.校园网安全设计策略

校园网的安全威胁既有来自校内的，也有来自校外的，只有将技术和管理都重视起来，才能切实构筑一个安全的校园网。一般来说，构筑校园网络安全体系，要从两个方面着手：一是采用先进的技术；二是不断改进管理方法。

## 3.1校园网安全管理

针对目前高校校园网安全现状的认识与理解，在防病毒软件、防火墙或智能网关等构成的防御体系下，对于防止来自校园网外的攻击已经足够。以下五点是高校的安全策略：

1、规范出口管理，实施校园网的整体安全架构，必须解决多出口的问题。对于出口进行规范统一的管理，使校园网络安全体系能够得以实施。为校园网的安全提供最基础的保障。

2、配备完整系统的网络安全设备，在网内和网外接口处配置一定的统一网络安全控制和监管设备就可杜绝大部分的攻击和破坏，一般包括：防火墙、入侵检测系统、漏洞扫描系统、网络版的防病毒系统等。另外，通过配置安全产品可以实现对校园网络进行系统的防护、预警和监控，对大量的非法访问和不健康信息起到有效的阻断作用，对网络的故障可以迅速定位并解决。

3、解决用户上网身份问题，建立全校统一的身份认证系统 。校园网络必须要解决用户上网身份问题，而身份认证系统是整个校园网络安全体系的基础的基础，否则即便发现了安全问题也大多只能不了了之，只有建立了基于校园网络的全校统一身份认证系统，才能彻底的解决用户上网身份问题，同时也为校园信息化的各项应用系统提供了安全可靠的保证。

4、严格规范上网场所的管理，集中进行监控和管理 。上网用户不但要通过统一的校级身份认证系统确认，而且，合法用户上网的行为也要受到统一的监控，上网行为的日志要集中保存在中心服务器上，保证了这个记录的法律性和准确性。

## 3.2校园网络安全技术

前述各种网络安全威胁，都是通过网络安全缺陷和系统软硬件漏洞来对网络发起攻击的。为杜绝网络威胁，主要手段就是完善网络病毒监管能力，堵塞网络漏洞，从而达到网络安全。

### 3.2.1杀毒产品的部署。

在该网络防病毒方案中，要达到一个目的就是：要在整个局域网内杜绝病毒的感染、传播和发作。为了实现这一点，应在整个网络内可能感染和传播病毒的地方采取相应的防病毒手段；同时为了有效、快捷地实施和管理整个网络的防病毒体系，应能实现远程安装、智能升级、远程报警、集中管理、分布查杀等多种功能。

### 3.2.2采用VLAN技术。

VLAN技术是在局域网内将工作站逻辑的划分成多个网段，从而实现虚拟工作组的技术。VLAN技术根据不同的应用业务以及不同的安全级别，将网络分段并进行隔离，实现相互间的访问控制，可以达到限制用户非法访问的目的。

### 3.2.3内容过滤器。

内容过滤器是有效保护网络系免于误用和无意识服务拒绝的工具。同时，可以限制外来的垃圾邮件。

### 3.2.4防火墙。

在与Internet相连的每一台电脑上都装上防火墙，成为内外网之间一道牢固的安全屏障。在防火墙设置上按照以下原则配置来提高网络安全性:

(1)根据校园网安全策略和安全目标，规划设置正确的安全过滤规则，规则审核IP数据包的内容包括：协议、端口、源地址、目的地址、流向等项目，严格禁止来自公网对校园内部网不必要的、非法的访问。总体上遵从“不被允许的服务就是被禁止”的原则.

(2）禁止访问系统级别的服务( 如HTTP , FTP等)。局域网内部的机器只允许访问文件、打印机共享服务。使用动态规则管理，允许授权运行的程序开放的端口服务，比如网络游戏或者视频语音电话软件提供的服务。

(3）如果你在局域网中使用你的机器，那么你就必须正确设置你在局域网中的IP，防火墙系统才能认识哪些数据包是从局域网来，哪些是从互联网来，从而保证你在局域网中正常使用网络服务（如文件、打印机共享）功能。

(4）定期查看防火墙访问日志，及时发现攻击行为和不良上网记录。

(5）允许通过配置网卡对防火墙设置，提高防火墙管理安全性.

### 3.2.5入侵检测。

入侵检测系统是防火墙的合理补充，帮助系统对付网络攻击。扩展系统管理员的安全管理能力．提高信息安全基础结构的完整性。入侵检测系统能实时捕获内外网之间传输的数据，利用内置的攻击特征库，使用模式匹配和智能分析的方法，检测网络上发生的入侵行为和异常现象，并记录有关事件。入侵检测系统还可以发出实时报警，使网络管理员能够及时采取应对措施。

### 3.2.6漏洞扫描。

随着软件规模的不断增大．系统中的安全漏洞或“后门”也不可避免地存在．因此，应采用先进的漏洞扫描系统定期对工作站、服务器等进行安全检查，并写出详细的安全性分析报告，及时地将发现的安全漏洞打上“补丁”。

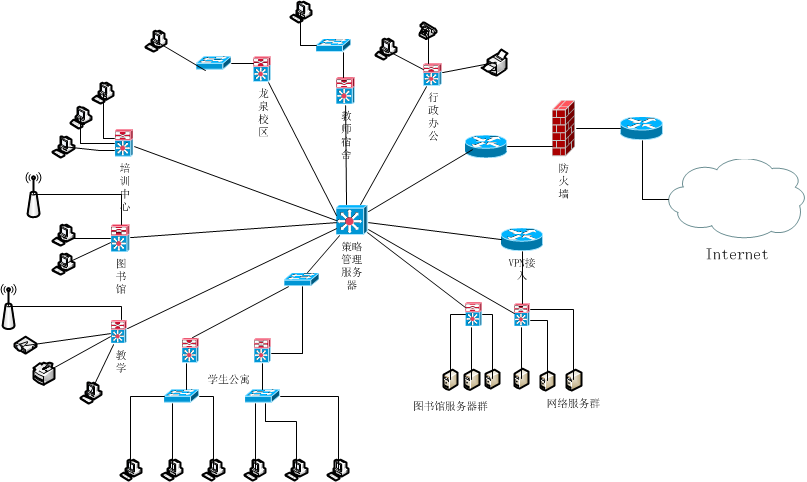
### 3.2.7数据加密。

数据加密是核心的对策，是保障数据安全最基本的技术措施和理论基础。

### 3.2.8加强网络安全管理。

加强网络管理主要是要做好两方面的工作。首先，加强网络安全知识的培训和普及；其次，是健全完善管理制度和相应的考核机制，以提高网络管理的效率。

# 4.本校网络拓扑图



## 4.1.简化拓扑图

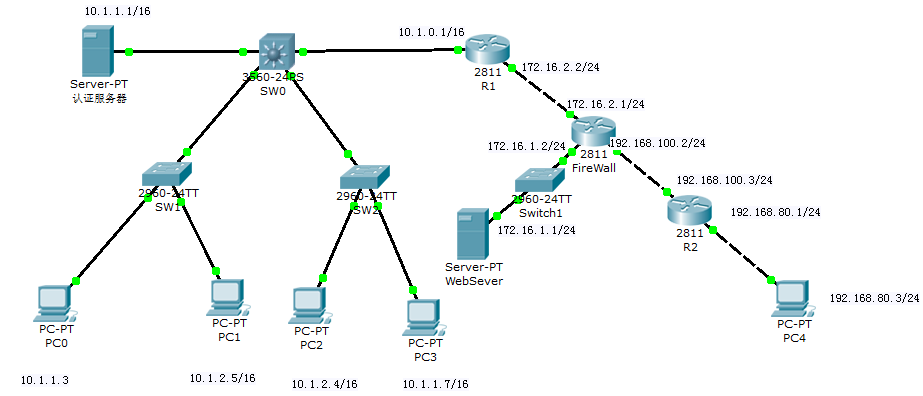


图4.1

## 4.2VLAN技术的虚拟实现

将位于不同地理位置的主机划分到同一个局域网之中，如图4.1中，pc0与pc3不在同一个物理局域网之中，可以通过配置将其逻辑划分到同一个局域网之中。

!

interface FastEthernet0/1

switchport mode trunk

!

interface FastEthernet0/2

switchport access vlan 10

!

!

interface FastEthernet0/1

switchport mode trunk

!

interface FastEthernet0/2

switchport access vlan 20

!

interface FastEthernet0/3

switchport access vlan 10

!

## 4.3防火墙功能的实现

通过对路由器端口流量规则的设置，实现外网只能访问校园网web服务器，而不能访问内外，但校园网能够正常访问外网。

!

access-list 1 deny 192.168.80.0 0.0.0.255

access-list 1 permit 10.0.0.0 0.255.255.255

!

## 4.4地址映射的实现

内网访问外网时，由于公网地址有限，往往采用地址映射来实现内网对外网的访问。

!

ip nat pool cat 192.168.3.2 192.168.3.30 netmask 255.255.255.0

ip nat inside source list 1 pool cat

ip classless

!

# 5.总结

随着网络应用的深入普及，网络安全越来越重要，国家和[企业](http://www.studa.net/company/" \t "_blank)都对建立一个安全的网络有了更高的要求。一个特定系统的网络安全方案，应建立在对网络风险分析的基础上，结合系统的实际应用而做。由于各个系统的应用不同，不能简单地把信息系统的网络安全方案固化为一个模式，用这个模子去套所有的信息系统。

本文根据网络安全系统设计的总体规划,从桌面系统安全、病毒防护、身份鉴别、访问控制、信息加密、信息完整性校验、抗抵赖、安全审计、入侵检测、漏洞扫描等方面安全技术和管理措施设计出一整套解决方案，目的是建立一个完整的、立体的、多层次的网络安全防御体系。

# 参考文献

[1]刘永华，解圣庆，张凤云。局域网组建、管理与维护[M]北京：清华大学出版社。

[2]刘钦创。网络安全技术与应用[J]2006.2.1期

[3]贾铁军，王坚，沈学东。网络安全技术及应用实践教程[M]北京：机械工业出版社，2009.2

[4]赵安军，徐邦海。网络安全及应用[M]北京：北京人民出版社。

[5]田宝玉。计算机网络与信息安全[M] 北京：北京邮电大学出版社。

[6]刘钦创。现代计算机。[J]2006.3.25 期