

《计算机网络》课程设计小组报告

（2020——2021年度第一学期）

|  |  |
| --- | --- |
| 题 目 |  |
| 专 业 | 计算机科学与技术（非师范） |
| 班 级 |  |
| 小组成员 | （组长） |
|  |  |
|  |  |
|  |  |

《 计算机网络 》课程设计

成 绩 评 定

|  |  |  |  |
| --- | --- | --- | --- |
| **学号** | **姓名** | **成绩** | **备注** |
|  |  |  | 组长 |
|  |  |  | 组员 |
|  |  |  | 组员 |
|  |  |  | 组员 |

指导教师： （签字）

目录

[摘要： 1](#_Toc59475110)

[一、课程设计内容 1](#_Toc59475111)

[1概述 1](#_Toc59475112)

[1.1大肥羊学校网络设计 1](#_Toc59475113)

[1.2计算机局域网络的主要目标 1](#_Toc59475114)

[1.3课程设计实验环境及运行环境： 1](#_Toc59475115)

[2计算机局域网络背景介绍及需求分析 2](#_Toc59475116)

[2.1 学校背景概况 2](#_Toc59475117)

[2.2网络应用和服务需求 2](#_Toc59475118)

[2.3用户概况和信息点需求 3](#_Toc59475119)

[2.4安全需求 3](#_Toc59475120)

[2.5管理需求 4](#_Toc59475121)

[2.6网络可扩展、优化需求 4](#_Toc59475122)

[3设计性原则 4](#_Toc59475123)

[4网络详细设计 5](#_Toc59475124)

[4.1本校园网网络采用层次化的设计方案 5](#_Toc59475125)

[4.2 防火墙技术和DMZ设计 6](#_Toc59475126)

[4.3 冗余/负载均衡设计 6](#_Toc59475127)

[4.4线路冗余设计 6](#_Toc59475128)

[4.5 网络设备冗余/负载均衡设计 7](#_Toc59475129)

[4.6 网管工作站设计 7](#_Toc59475130)

[5整体设计思路 7](#_Toc59475131)

[5.1网段的划分 7](#_Toc59475132)

[5.2 网络的规模和应用范围设计 7](#_Toc59475133)

[5.3 网络的应用模式 8](#_Toc59475134)

[5.4 逻辑网络拓扑设计 8](#_Toc59475135)

[5.5 网络及路由规划 10](#_Toc59475136)

[5.6 内外网NAT地址映射转换 10](#_Toc59475137)

[5.7 服务器部署 11](#_Toc59475138)

[5.8 网络虚网划分 12](#_Toc59475139)

[5.9 网络路由设计 13](#_Toc59475140)

[6 网络传输介质的设计选型 13](#_Toc59475141)

[6.1 交换机选型 13](#_Toc59475142)

[6.2 路由器选型 14](#_Toc59475143)

[7 网络安全与管理规划设计 14](#_Toc59475144)

[8 主要的计算机网络技术 15](#_Toc59475145)

[8.1 VLAN (虚拟局域网) 15](#_Toc59475146)

[8.2 NAT 的描述及策略路由的实现 15](#_Toc59475147)

[8.3 链路聚合 EC(Ethernet Channel) 16](#_Toc59475148)

[8.4 ACL (访问控制列表) 16](#_Toc59475149)

[9网络系统的测试 16](#_Toc59475150)

[9.1 设备连通性测试 16](#_Toc59475151)

[9.2网络服务访问测试 18](#_Toc59475152)

[二、总结和心得 21](#_Toc59475153)

[三、小组分工 21](#_Toc59475154)

[参考文献： 21](#_Toc59475155)

# 摘要：

科学技术的发展日新月异，在计算机技术和通信技术结合下，网络技术得到了飞速的发展。如今，不仅计算机和整个网络紧密结合，整个社会都不能脱离网络而存在。网络技术已经成为现代信息技术的主流，人们对网络的认识也随着网络应用的逐渐普及而迅速改变，网络逐渐成为人们生活中必不可少的一部分。大肥羊学校基本完成了校园网的框架，主要用于连接各教学楼、综合楼、实验楼等，在本方案中，我们将详细阐述大肥羊学校校园网的建设方案，内容大致为搭建网络、网络管理、需求分析等。

**关键字：** 局域网、需求分析、设计

# 一、课程设计内容

## 1概述

### 1.1大肥羊学校网络设计

### 1.2计算机局域网络的主要目标

### 要建立一个连接教学楼、宿舍楼、食堂、图书室、体育馆和综合楼（网络中心）等区域的校园网，能有效管理学校的各层面信息，实现信息和设备资源的及时交换与共享。要求建立一个连接教学楼、办公楼，图书馆，生活区，实训楼，网络中心等区域的校园网。

### 1.3课程设计实验环境及运行环境：

操作系统：Windows 7/10，Windows 2003 或 2012 R2 Server

虚拟仿真软件和工具： VMware Workstation Pro 12，Packet Tracer等

制图工具：Microsoft Office Visio/Word/Powerpoint，Packet Tracer 等。

协议分析工具：Wireshark 等。

## 2计算机局域网络背景介绍及需求分析

### 2.1 学校背景概况

大肥羊学校始建于2020年，位于青青草原东边，青青河北岸的羊村，占地面积260亩，在校生969人，共有48个教学班，259名教职工，学校着力培养学生全面发展，以学生自主合作探究学习打造高效课堂。

学校建筑概览图如图1所示。

****

图1 虚网间路由通信

### 2.2网络应用和服务需求：

2.2.1信息交流功能。

1. 使任何一个办公室的计算机都能实现网上浏览、查询信息的功能，使教师能够拓宽视野，充分利用互联网上的资源辅助教学，提升教学理念。
2. 可以充分利用互联网资源来宣传学校，展示学校的办学能力与办学水平。
3. 为全校师生提供相互交流、相互学习的平台。

2.2.2教学服务功能

（1）建立课件、基件、教学信息资源库，实现课件点播和辅助教学。

（2）利用网络技术。实现多媒体信息交换、远程教育。

2.2.3学生学习功能

（1）利用网络自主学习，提高学生的学习能力。

（2）利用网络查阅资料，相互交流、相互学习。

（3）可实现网上资源远程学习。

2.2.4学校管理功能

（1）行政办公系统

（2）教务管理系统

（3）学生管理系统

（4）财务管理系统

### 2.3用户概况和信息点需求：

主要信息点集中在综合楼、教学楼、实验楼、生活区等。详细分布如表1所示。

|  |  |  |  |
| --- | --- | --- | --- |
|  | 栋数 | 信息点/楼（个） | 信息点总数 |
| 综合楼（网络中心） | 1 | 107 | 67+50（网络中心）=107 |
| 教学楼 | 3 | 40、40、40 | 120 |
| 实验楼 | 1 | 38 | 38 |
| 生活区（宿舍，食堂） | 2 | 232 | 464 |
| 食堂 | 1 | 2 | 2 |
| 体育馆 | 2 | 10 | 3+7=10 |
| 门卫 | 1 | 2 | 2 |
| 合计 |  |  | 743 |

表1 主要信息点分布

综合楼主要有领导办公室、教研办公室和网络中心，领导办公室主机数量少，分配信息点数每个房间3个；教研办公室使用主机人数多，需在办公室安置4个信息点；网络中心是整个校园网的中心，一部分维护内部校园网络，一部分负责校内资源共享，信息点数较密集。

教学楼每个教室有2个信息点，会议室3个信息点。

实验楼除信息技术机房外，每个实验室2个信息点，信息技术机房每个教室52台电脑，4个信息点。

生活区，每间宿舍3个信息点，食堂2个信息点

### 2.4安全需求：

校园网的安全威胁主要来源于两大块，一块来自于内网，一块来自于网外。来源于网内的威胁主要是病毒攻击和和黑客行为攻击，根据统计，威胁校园网安全的攻击行为大概有40%左右来自内部网络。虽然计算机系统本身或多或少地具有安全防范措施，网络系统的安全防范却是整个系统安全性的第一道防线。

（1）网络硬件安全：网络系统中各通信计算机设备以及相关设备的物力保护。

（2）网络配置安全：

信息完整性：计算机系统能够防止非法修改和删除数据和程序；

保密性：信息不泄露给未经授权的人；

可用性：系统能够防止非法防止独占计算机资源和数据，合法用户的正常请求能及时、正确、安全的得到服务或回应。

### 2.5管理需求

为了便于校园网络管理人员的管理及维护，我们选购Quidview网络管理软件，该软件基于灵活的组件化结构，用户可以根据自己的管理需求和网络情况灵活选用自己需要的组件，真正实现“按需建构”。Quidview支持多种操作系统平台，并能够与多种通用网管平台集成，实现从设备级到网络级全方位的网络管理。

（1）网络集中监视

Qiudview网络管理软件提供一拓扑发现功能，实现全网监控，并根据网络运行环境变化提供合适的方式对网络参数进行配置修改，保证网络以最佳性能正常运行。

（2）故障管理

故障管理功能对全网设备的告警信息和运行信息进行实时监控，查询和统计设备的告警信息。

（3）性能监控

Quidview网管系统通过性能任务的配置，可自动获得网络的各种当前性能数据，并支持设置性能的门限。通过统计不同线路、不同资源的利用情况，为优化或扩充网络提供依据。

（4）设备配置文件管理

Quidview网络配置中心支持对设备配置文件的集中管理，包括配置文件的备份、恢复以及批量更新等操作，同时还实现了配置文件的基线化管理，可以对配置文件的变化进行比较跟踪。

（5）设备软件升级管理

使用Quidview管理员可以方便地查询设备上运行的软件版本，并利用升级分析功能来确定设备运行软件是否需要升级。当升级软件版本时，可以利用Quidview集中备份设备运行软件，然后进行批量升级。升级之后，可以使用该软件进行升级结果验证，确保升级操作万无一失

### 2.6网络可扩展、优化需求：

采用层次化结构。在网络设计中。模块化具有的特性使网络增长时的复杂性能够限制在子网中，而不会蔓延到网络的其他地方。如果采用扁平化和网状设计，任何节点的变动都将对整个网络产生很大影响。同时层次化设计可将网络拓扑分解为易于理解的子网，网络管理者可容易地确定网络故障的范围，简化排错过程，易于优化。

**3设计性原则**

本方案设计以追求性能优越、经济实用，从系统结构、技术措施、设备选择、系统应用、技术服务和实施过程等方面进行总体设计，设计一个符合该校园的网络系统。

（1）经济性原则

校园网的特点决定了网络系统需要有实用与经济性。实用性使得网络便于管理、维护，以减少网络使用人员运用网络的难度,从而降低人为操作引起的网络故障，并使更多的人掌握网络的使用。应根据学校的实际情况，由于学校的建设资金有限，所以一般都要求网络建设投入具有一定的性价比，所以在建设校园网时一定要使用性价比高的网络技术和网络设备，以节约建设资金。

（2）技术性原则

校园网网络系统要求具有较高的数据通信能力和较大的带宽;并在主干网上提供较强的可扩展性。为了及时、迅速地处理网络上传送的数据，网络应有较高的网络主干速度。

（3）可靠性原则

网络要求具有高可靠性，高稳定性和足够的冗余，提供拓扑结构及设备的冗余和备份，为了

在网络设备上要提供冗余配置，设备在发生故障时能以热插拔的方式在最短时间内进行恢复,把故障对网络系统的影响减少到最小，避免由于网络故障造成用户损失。

（4）安全性原则

校园网作为一个支持众多用户、同时和外部Internet存在连接的网络，网络安全性在整个网络中是个重要的问题，应该采用一定手段控制网络的安全性，以保证网络正常运行。网络中应采取多种技术从内部和外部同时控制用户对网络资源的访问。网络系统还应具备高度的数据安全性和保密性，能够防止非法侵入和信息泄漏。

（5）可管理性原则

对网络进行设备级和系统级的管理，并能支持通用浏览器进行网络设备的管理及配置。灵活的设置每个用户对Internet访问功能，能够对每个用户实行管理。

（6）可扩充性原则

随着应用规模的不断扩大，要求网络可以方便地扩充容量，支持更多的用户及应用;随着网络技术的不断发展，网络必须能够平滑地过渡到新的技术和设备，一直支持更新，保证现有的投资。

## 4网络详细设计

### 4.1本校园网网络采用层次化的设计方案。

（1）核心层网络设计

核心层：将各汇聚层交换机互连起来进行穿越校园网骨干的高速数据交换。实现数据包高速交换。核心层双中心星形拓扑的优点是结构较为简单，实现设备的，也可以很好的进行网络负载均衡。PortTrunking技术提高互联交换机的吞吐量，使得整个网络具备高容量、无阻塞、高性能的能力。

（2）汇聚层网络设计

汇集层：主要功能是汇聚网络流量，链路聚合、路由聚合，信号中继，负责将访问层交换机进行汇集，还为整个交换网络提供VLAN间的路由选择功能。

（3）接入层网络设计

接入层：接入层利用VLAN划分等技术隔离网络广播风暴，提高网络效率，为所有的终端用户提供一个接入点。

（4）广域网互联设计

考虑到Internet和其他网络的连接(如CHINANET等)，目前设计的局域网都要考虑对广域网络的连接，更广的资源和更多的应用将是在各种广域连接中发现。目前，越来越多的学校还开展了网络教学和建立自己的WEB。因此，能否有效地连接Internet是校园网建立的一个重要的目标。

### 4.2 防火墙技术和DMZ设计

（1）学生基本信息档案和重要的工作文件要求对数据存储、传输的安全性的性能较高，如图书管理、档案管理、学生管理、教学管理、财务管理、物资管理等可以通过分布式、集中式相集合的方法进行管理。防火墙作为网络的第一道防线，应放置在外网和需要保护的校园内网之间。这样，所有流入校园网络的数据流量都将通过防火墙，使校园内的所有客户机及服务器都处于防火墙的保护下。

（2）针对不同资源提供不同安全级别的保护, 还应构建一个“Demilitarized Zone”(DMZ)的区域，放置一些不含机密信息的公用服务器，比如Web、 Mail、FTP等。这样来自外网的访问者可以访问DMZ中的服务，但不可能接触到存放在内网中的公司机密或私人信息等。即使DMZ中服务器受到破坏，也不会对内网中的机密信息造成影响。

### 4.3 冗余/负载均衡设计

冗余设计是网络设计的重要部分，是保证网络整体可靠性能的重要手段。但是投资也将增加。部分校园网在早期的建设中由于成本的原因并未在设计中考虑冗余问题，而在优化工作中则需从网络链路和网络设备两方面着手。冗余设计可以贯穿整个层次化结构，每个冗余设计都有针对性，可以选择其中一部分或几部分应用到网络中以针对重要的应用。万一网络中某条路径失效时，冗余链路可以提供另一条物理路径。可采用GEC链路聚合（IEEE802.3ad）实现端口级冗余，以克服某个端口或线路引起的故障。也可采用生成树协议（IEEE802.1d）提供设备级的冗余连接。此外，我们在设计中提供不同物理方向的双归属、双路由保护。

### 4.4线路冗余设计

在校园网核心层，网络边界拓扑结构，我们采用10GE线路对核心层设备进行备份，并使用业界领先的VRRP（虚拟路由器冗余协议）来对其作为冗余线路的协议保障。以GEC作为N\*1000M主干链路，通过这个链路连接核心交换机，具备万兆扩展能力；接入交换机采用10/100M自适应端口连接桌面系统，多千兆链路连接到汇聚层。

GEC路具有链路聚合和冗余保证两大特性，下面我们将对它们依次进行介绍：

链路聚合：

可使用一条物理链路在不同品牌交换机之间、交换机和服务器间提供聚合的高速通道，在不增加投资的情况下，扩大交换带宽，使关键连接的传输效率更高。

冗余保证：

链路聚合中，成员互相动态备份。当某一链路中断时，其它成员能够迅速接替其工作。与生成树协议不同，链路聚合启用备份的过程对聚合之外是不可见的，而且启用备份过程只在聚合链路内，与其它链路无关，切换可在数毫秒内完成。

综合分析以上各主流方案的优缺点，从性能与成本及拓展性等方面的综合考虑出发，我们决定采用GEC骨干核心网络10GE拓展的方式作为其链路选择及备份选择。

在校园网汇聚层及接入层出于成本及性价比的考虑，我们决定采用千兆汇聚，万兆拓展；百兆到桌面的链路选择。

### 4.5 网络设备冗余/负载均衡设计

各个网络的核心部分，其数据流量和计算强度之大，使得单一设备根本无法承担。负载均衡建立在现有网络结构之上，它提供了一种廉价有效的方法扩展服务器带宽和增加吞吐量，加强网络数据处理能力，提高网络的灵活性和可用性。它主要完成以下任务:解决网络拥塞问题，服务就近提供，实现地理位置无关性 ；为用户提供更好的访问质量;提高服务器响应速度；提高服务器及其他资源的利用效率；避免了网络关键部位出现单点失效。

### 4.6 网管工作站设计

网络管理是校园网必须考虑的关键技术，这里的网络管理主要指网络设备及其系统的管理，它包括配置、性能、安全、故障管理等，网络管理设计需要在配置每个网络设备时，都选择具有网络管理代理的、驻留有网络管理协议的设备。

网络管理设计的另一方面，是配置一个网络管理中心，配置网络管理平台，在平台上运行管理每个网络设备的应用软件。网管软件应能够支持对网络进行设备级和系统级的管理，并能支持通用浏览器进行网络设备的管理及配置。

## 5整体设计思路

### 5.1网段的划分

在接入层运用交换机对相应楼宇的主机划分虚拟局域网实现网段的划分，在汇聚层采用三层交换机实现路由功能，通过启用路由功能，实现内网不同网段，不同楼宇上网络设备的相互通信，在核心层，在思科路由器上配置DHCP服务为内网的信息点分配IP地址，并配置网络地址转换服务（NAT）实现内网对外部互联网的访问。在内网里设置相应服务器，实现内网的web/DNS/FTP等服务。

在校园内设置WLAN，使校园内的网络设备也可通过连接无线网络实现网络通信和Internet访问。

### 5.2 网络的规模和应用范围设计

（1）网络覆盖整个校园，应用于校内所有网络设备。

（2）IP地址和VLAN划分，IP地址规划遵循如下原则来设计：

（3）服务器区采用私IP地址，NAT后供人员远程访问；

（4）与internet 互联设备IP地址采用公有IP地址；

（5）部分内部互连采用私有IP地址；

（6）面向用户的私有IP地址，由统一出口的边缘设备（路由器）进行地址翻译。即出口路由器互联采用合法IP地址；公共服务器如WWW/FTP/DNS等均采用合法地址（或从安全角度考虑采用私有IP）；部分接入用户采用私有保留IP地址相连。

这样设计，既可以充分利用已有的公网IP地址，解决了IP地址空间不足的，既可以方便的实现互通互连，而且将地址翻译（NAT）这种耗费设备资源的工作由网络边缘设备分担，提高网络数据传输整体性能。

同时，还可以采用VLSM。VLSM是可变长子网掩码的英文缩写，它提供了一个主类（A类、B类、C类）网络内包含多个子网掩码的能力，可以对一个子网再进行子网划分。

VLSM的优点，所以我们采取VLSM对网络进行编址，以达到节约IP地址，能够使用路由汇总的目的。

校园IP地址和VLAN分配如下表2：

|  |  |  |  |
| --- | --- | --- | --- |
| 楼宇 | IP网段 | VLAN编号 | 默认网关 |
| 综合楼 | 192.168.10.0/24 | 10 | 192.168.10.254/24 |
| 教学楼1 | 192.168.20.0/24 | 20 | 192.168.20.254/24 |
| 教学楼2 | 192.168.30.0/24 | 30 | 192.168.30.254/24 |
| 教学楼3 | 192.168.40.0/24 | 40 | 192.168.40.254/24 |
| 实验楼 | 192.168.50.0/24 | 50 | 192.168.50.254/24 |
| 宿舍（男） | 192.168.60.0/24 | 60 | 192.168.60.254/24 |
| 宿舍（女） | 192.168.70.0/24 | 70 | 192.168.70.254/24 |
| 食堂 | 192.168.60.0/24 | 60 | 192.168.60.254/24 |
| 体育馆 | 192.168.50.0/24 | 50 | 192.168.50.254/24 |
| 门卫 | 192.168.10.0/24 | 10 | 192.168.10.254/24 |
| 网管地址 | 192.168.80.0/24 | 80 | 192.168.80.254/24 |

表2 IP地址和VLAN分配

### 5.3 网络的应用模式

网络的总体框架，是集中式分布，采用浏览器/服务器模式。

### 5.4 逻辑网络拓扑设计

1） 网络拓扑结构设计

（1）网络拓扑的设计：采用混合形拓扑结构；

（2）传输介质设计：采用有线局域网无线局域网相结合，即有线介质和无线介质。

（3）层次结构设计：网络分层设计，采用三层网络架构设计。

核心层、分布层（汇聚层）和接入层。

（4）逻辑网络拓扑图仿真模拟。如图2所示。

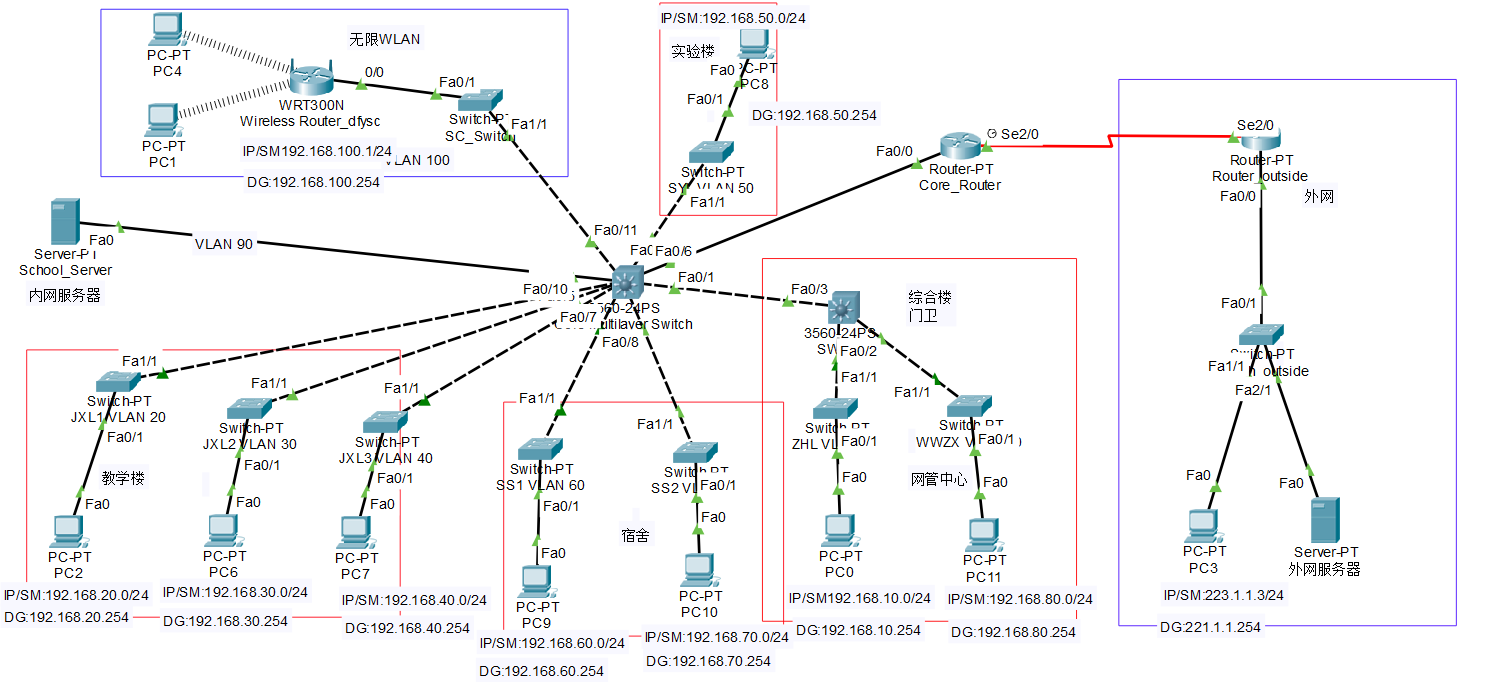


图2 校园局域网仿真拓扑图

### 5.5 网络及路由规划：内网路由和外网路由之间采用静态路由实现路由功能；虚网（VLAN）间路由通信通过三层交换机的路由功能实现。如图3所示。

|  |
| --- |
|  |
|  |

图3虚网间路由通信

### 5.6 内外网NAT地址映射转换：NAT映射配置在核心层的路由器上，使内网能访问外网。先建立外部地址池，然后建立内网的各访问列，最后建立动态地址映射。

|  |
| --- |
|  |
|  |

图4动态NAT地址转换

### 5.7 服务器部署

服务和服务器部署：部署Web 服务器、DHCP 服务器、DNS 服务器、FTP 服务器。

|  |  |
| --- | --- |
|  |  |

图5 DNS内网部署 图6 DNS外网部署

|  |  |
| --- | --- |
|  |  |

图 7 web内网部署 图 8 web外网部署

|  |  |
| --- | --- |
|  |  |

图 9 DHCP池分配IP地址 图 10 FTP服务部署

核心层的路由器建立DHCP池，并配置DHCP为校内各网段的端口分配IP地址。

DHCP通过命令配置，每个网段设立相应地址池和排除的网络地址。

通过在校内服务器部署WEB服务，使校内设备能通过IP地址和HTTP协议访问不同站点，获取信息。

在服务器上部署FTP服务，使各主机之间能传输文件和提供文件的存储和访问服务。

在服务器上部署DNS域名映射，使局域网内的主机可通过域名访问互联网。

### 5.8 网络虚网划分

虚网(VLAN)划分；

虚网(VLAN)划分：为各栋楼的接口/主机划分虚拟网段。通过划分虚网，能隔离广播域，让每个节点（比如电脑、手机）不需要收到太多无关的广播包，从而减少计算性能和网络带宽的无谓消耗。从而保证局域网的性能。如图11所示。

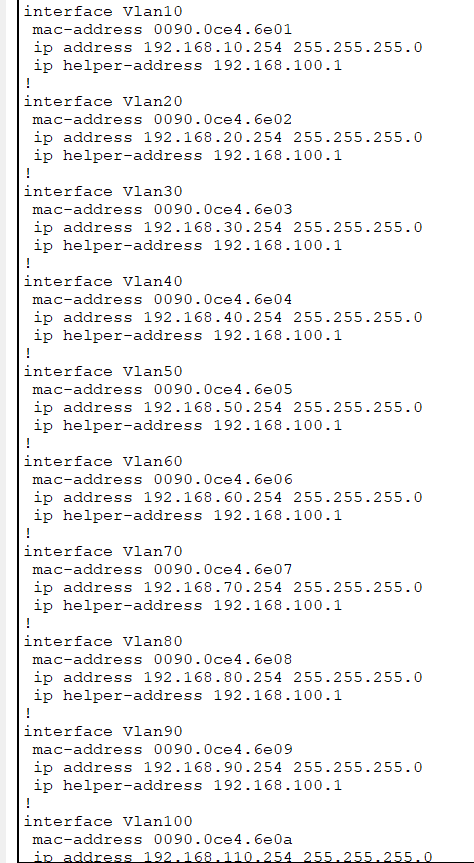


图11虚网(VLAN)划分

### 5.9 网络路由设计

为主机或相关网络设备安装无线网卡，填写正确的SSID （服务区标识符匹配），使其能正常访问互联网。

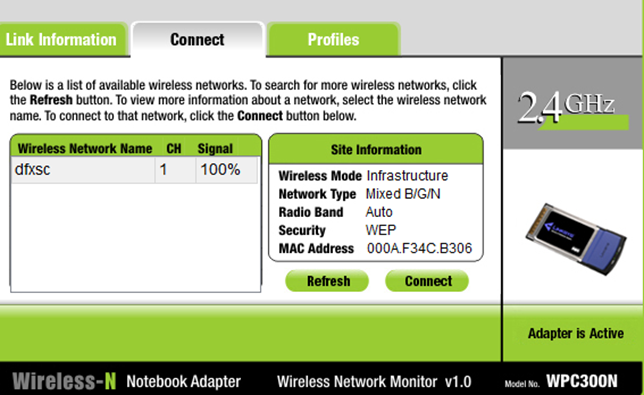


图12 wifi连接

## 6 网络传输介质的设计选型

### 6.1 交换机选型

核心层交换机：它是构成网络的重点，承担着数据快速率、大容量交换，大吞吐量等重任，以使整个网络高容量、无阻塞、高可靠的运行，所以选用Ciscoc atalyst6500。

|  |
| --- |
| 核心层 |
| 1个2端口1000BaseLx模块、24个10/100BaseTx以太网口，具有MIB管理模块，交换容量≥32Gbit/s，包过滤转发率38Mpps，16Mb缓存 |

汇聚层交换机：为满足多媒体教学要求，且综合考虑性价比，对 QoS 有良好的支持并且能提供大的带宽.所以教学楼等汇聚层交换机应Cisco3650-24PS。

|  |
| --- |
| 汇聚层 |
| 1个2端口1000BaseLx模块、1个2端口1000BaseSx以太网模块、24个10/100BaseTx以太网口，具有MIB管理模块，交换容量≥24Gbit/s，包过滤转发率≥13.2Mpps |

接入交换机：接入层设备是最终用户的最直接上联的设备，它应该具备即插即用特性以及易于维护的特点。采用cisco c2960-48TT。

|  |
| --- |
| 接入层 |
| 48口，传输速率10/100/1000Mbps，支持vlan、网管功能。 |

### 6.2 路由器选型

出于安全考虑，应该选用一个带有防火墙的边界路由。这里我建议采用

cisco 7606，模块化，内置防火墙。

## 7 网络安全与管理规划设计

网络的安全性是评价校园网的重要指标之一，对于校园网这样的大型园区网，网络的安全问题就越发重要。网络的安全问题主要是由网络的开放性、无边界性、自由性造成的，所以考虑信息网络的安全首先应该考虑把被保护的网络由开放的、无边界的网络环境中独立出来，成为可管理、可控制的安全的内部网络。也只有做到这一点，实现信息网络的安全才有可能，而最基本的分隔手段就是防火墙。利用防火墙，可以实现内部网与外部网络（如因特网）之间或是内部网不同网络安全域的隔离与访问控制，保证网络系统及网络服务的可用性。

（1）硬件实现端口与 MAC 地址和用户IP 地址的绑定，严格限定端口上用户接入；

（2） 通过VLAN的划分，利用中心交换机上高性能路由模块的管理和控制，可以控制内部各VLAN间的访问；

（3）通过 Private VLAN 可以在交换机的同一 VLAN 中提供端口之间的通讯 或安全隔离，确保数据流进入有效端口，而不会被发送到其它端口，即解决了因传统802.1QVLAN 造成全网VID资源不够的问题，同时又无需利用安全规则资源即能达到隔离不同用户以及不同；组用户之间通讯的功能，充分保护用户隐私；

（4）可实现用户账号、MAC 地址、IP 地址、交换机 IP、 交换机端口等六 大元素之间的灵活任意绑定，有效确认用户合法性和唯一性；

（5）提供极为有效的Port Blocking 功能，避免端口受到其它端口发送的广播包、多播包等报文的干扰，有效减轻端口负载负担，提高端口带宽，保护用户 PC 更高效安全地运行；

（6）基于源 IP 地址控制的 Telnet 和 Web 设备访问控制，增强了设备网管的安全性，避免黑客恶意攻击和控制设备；提供加密传输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；

（7）计算机病毒是伴随着计算机而产生的，它同时随着计算机技术的发展而发展，在网络环境中，计算机病毒更易于传播，其对系统的危害也是明显的，在校园网工程中建议采用网络与单机相结合的方式来避免计算机病毒的危害。

校园网络必须要有一整套从用户接入控制，病毒报文识别到主动抑制的一系列安全控制手段，才能有效的保证网络的稳定运行。

（8）软件与协议设计

采用 TCP/IP 协议，

## 8 主要的计算机网络技术

### 8.1 VLAN (虚拟局域网)

VLAN 虚拟局域网是一种在二层设备上隔离和划分广播域的技术，通过这种 划分，我们可以把物理位置上分离的网络设备在逻辑上划为同一个广播域，或者 把物理位置上邻近的网络设备划为不同的广播域，从而更方便我们管理和做一个 逻辑层次的划分。从技术上说 VLAN 可以分为静态 VLAN 和动态 VLAN,那么静态的 VLAN 是基于交换机端口进行划分，根据网络设备连接不同的交换机端口，则进入相应的 VLAN。动态 VLAN 则更灵活，它可以根据接入计算机的 IP 地址， MAC 地址，甚至是用户的登陆账号做出相应的处理，把计算机划分进相应的VLAN 中，这样就为我们实际的网络管理带来了比较大的方便性和灵活性。那么在我们的校园网方案中，我们希望通过使用VLAN 技术进行划分达到以下目的： 隔离、划分广播域，减小不必要的广播流量，从而提高整个网络的利用效率。

### 8.2 NAT 的描述及策略路由的实现

在组建网络时，为了节约地址，我们在内部使用保留的私有地址段中的地址，但是使用私有地址不能访问 Internet,所以必须申请多个公开地址配置在和 Internet 相连的局域网边缘设备上。应用 NAT 进行地址转换。

NAT 是网络地址翻译技术，在路由器上起用 NAT 之后，可以在部私有地址和外部公网地址之间做转换。比如我们可以把网络内部使用的 IP 翻译成外部公网的 IP。

配置基于策略的路由选择时，可使用路由映射表来指定基于IP地址，应用程序，协议或者分组长度的条件。基于策略的路由选择命令对中选的路由实现策 略。基于策略的路由和静态路由有很多共同之处。然而，静态路由根据目标网络地址来转换分组，而策略路由根据源地址来转发分组。在路由选择表中使用访问 列表时，可根据诸如目标地址，分组长度，IP 协议字段，优先级或端口号来转发数据流。这样可以指定范围更广泛，更细致的条件，并根据这些条件来决定下一跳路由器。

### 8.3 链路聚合 EC(Ethernet Channel)

以太网信道链路聚合可以让交换机之间和交换机与服务器之间的链路带宽有非常好的伸缩性，比如可以把 2 个、3 个、4 个千兆的链路绑定在一起，使链路的带宽成倍增长。链路聚合技术可以实现不同端口的负载均衡，同时也能够互为备份，保证链路的冗余性。在这些千兆以太网交换机中，最多可以支持 4 组链路聚合，每组中最大 4 个端口。链路聚合一般是不允许跨芯片设置的。生成树协议和链路聚合都可以保证一个网络的冗余性。在一个网络中设置冗余链路，并用生成树协议让备份链路阻塞，在逻辑上不形成环路。而一旦出现故障，启用备份链路。

### 8.4 ACL (访问控制列表)

访问列表为我们提供了一种对网络访问进行有效管理的方法，通过访问列 表，我们可以设置允许或拒绝数据包通过路由器，或者允许或者拒绝具体的某些 端口进行访问和使用，如果满足条件则执行相应的操作，放行这个包或者放弃这个包。我们通过这些设置来满足实际网络的灵活需求，从而达到设置网络安全策略，防止网络中的敏感设备受到非授权访问的情况。

在具体实现过程中从技术上来说我们需要了解到 ACL 分为两种类型,他们分别是标准访问列表(Standard access lists)和扩展访问列表（Extends access lists） 前者在过滤网络的时候只使用 IP 数据报的源地址，那么在使用这种访问列表的情况下它做出允许或者拒绝这个决定完全是依赖于源IP地址，它无法区分具体的流量类型。而扩展访问列表则可以提供更细的决定，它可以具体到端口，从而精确到某一个服务，比如对 WEB,FTP 的访问等，给我们网络的策略提供了更细的控制手段。我们利用这种访问列表进行协议级的控制以达到对网络一个有效的管理。标准访问控制列表一般放在靠近目标的路由器上,而扩展访问控制列表一般放于近源端的路由器上。

## 9网络系统的测试

### 9.1 设备连通性测试

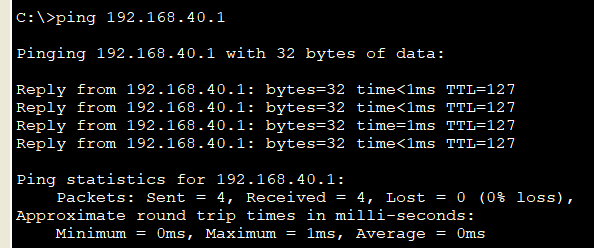


图13内网连通测试

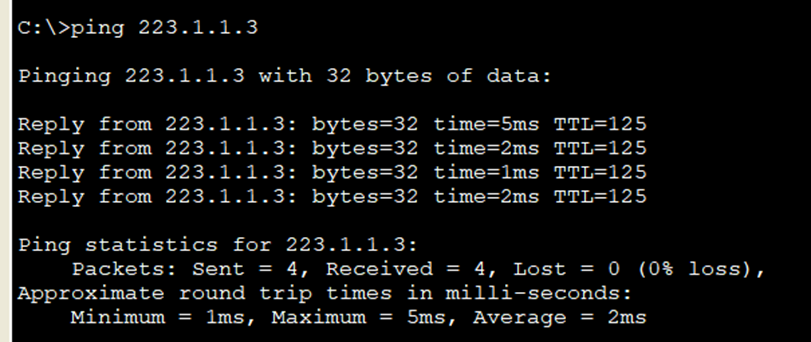


图 14内网通信外网测试

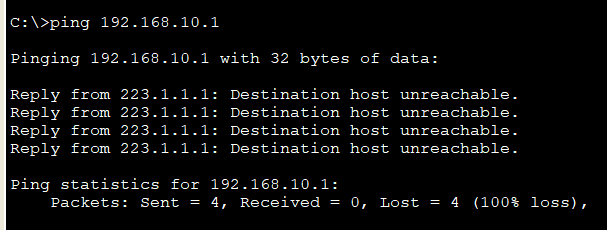


图 15外网通信内网测试

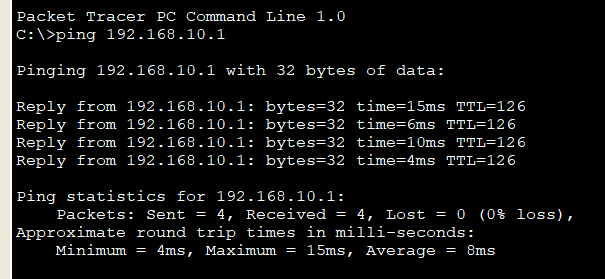


图 15 无线网测试

|  |
| --- |
|  |
|  |

图 16 路由表

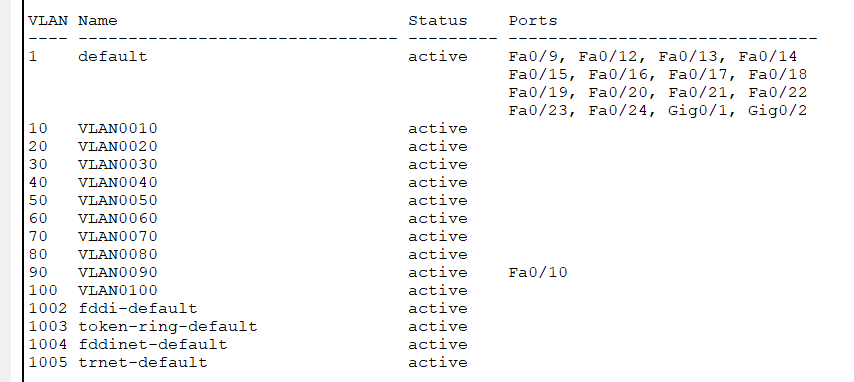


图 17 VLAN信息表

**9.2网络服务访问测试**

ftp服务查看文件信息。如图18所示。

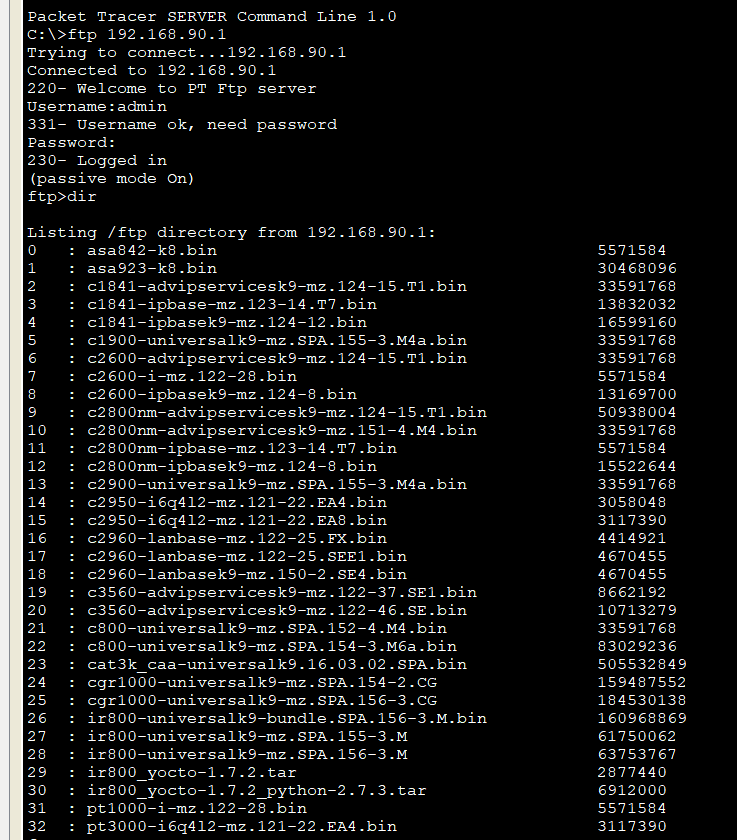


图 18 ftp访问

通过http协议访问网站（web服务）。如图19所示。

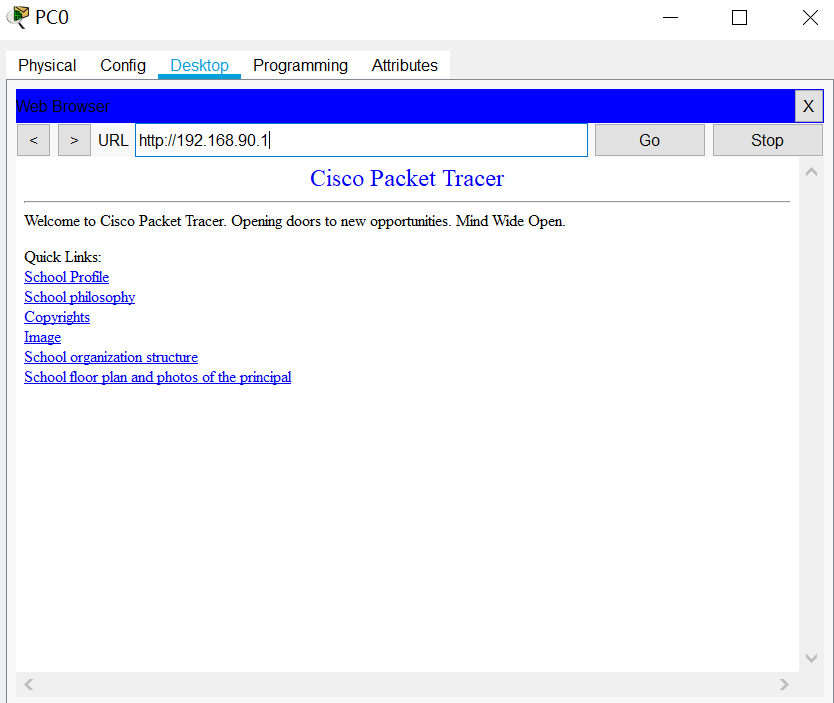


图19 Web访问

通过域名访问校内网址。如图20所示。

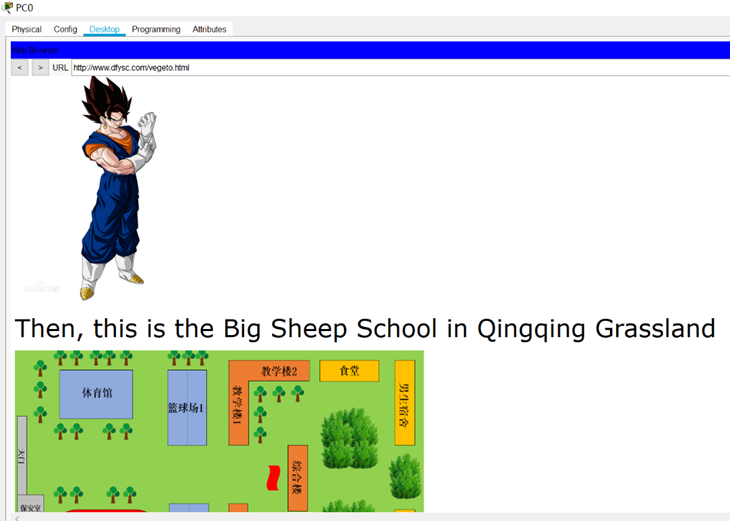


图20 内网域名访问

校内主机通过域名访问互联网。如图21所示。

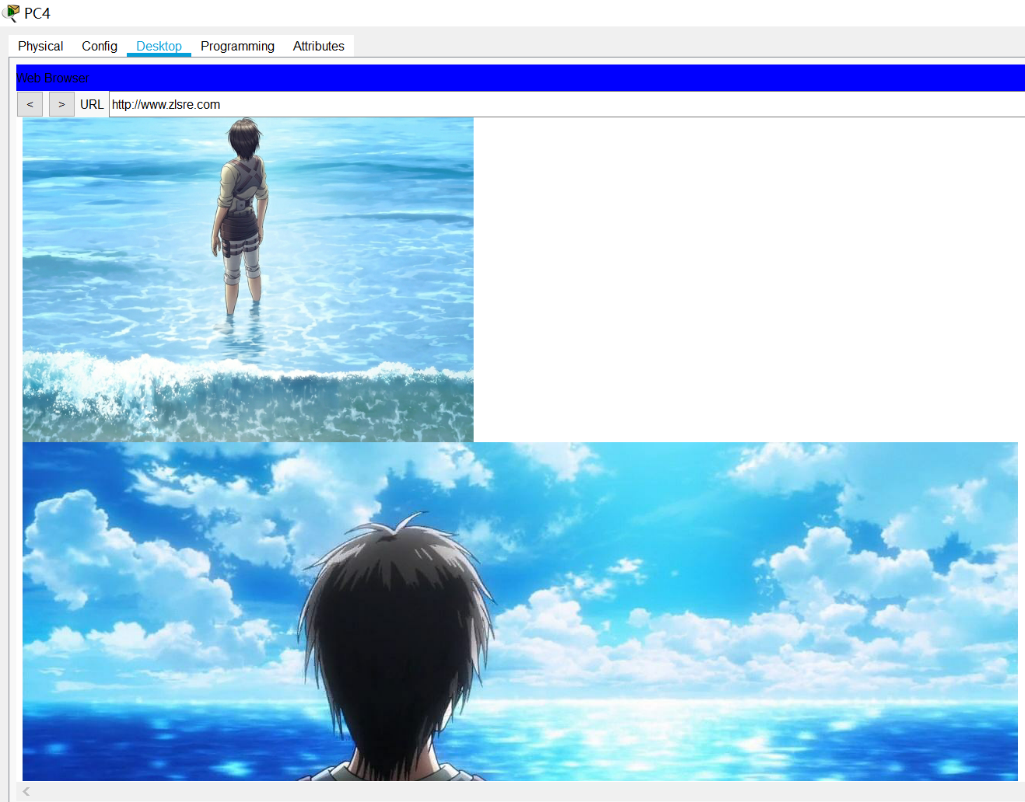


图 21外网域名访问

# 二、总结和心得

本次实验是一次全新的体验，并且，这次设计性实验，其中涉及到本学期所学习的知识，算是对本学期的一次总结，是对本学期学习成果的一个检验，之前十多次的小实验的磨练，为本次实验打下基础，就是之前实验的坚实基础，让本次实验得以完成。

在本次实验中，从提出想法、做计划、实施计划、实际检测，最后得到结果，每一个步骤都由小组讨论并且分工完成，在这个过程中，每个小组成员都有不同程度的收获。

从专业学习的角度来说，本次实验，我们对WWW、DNS、FTP等服务器的配置有了进一步的巩固，也更加熟悉了交换机、路由器等设备的作用以及它们是如何实现网络连通的，除了这些实践知识，我们还在实验中对学校对于网络的分析，比如：学校在网络管理和应用等各方面的需求、学校对于网络性能的要求、学校网络安全的实现和维护。

从生活学习的角度来说，这次实验以小组为单位，让我们学会如何团队协作，如何在团队中去取长补短，在这个过程中，我们在独立完成分工任务的同时还互相帮助，共同协作。并且，极大增加了我们的知识面。接触了绘图软件autoCAD，虽然现在只是初步接触，但会在未来继续学习它，掌握它。

本次实验我们收获了很多，但是在本次课程设计中，还存在很多需要完善的地方，比如，学校的一些功能建设还不够细化，网络的性能和需求分析还需要更明确，网络安全的建设和维护还待加强。这些问题在本次实验中未能完全解决，但是我们还会在未来的学习和生活中，在应用这些知识的过程中，去思考并完善它。让这些问题能更大程度地应用在实际地生活中，解决人们的实际问题。

# 三、小组分工

：核心技术的配置、校园局域网总体设计和仿真模拟拓扑图搭建；

：平面图、FTP服务器的配置、网络应用和服务需求、用户概括和信息点需求、网络安全及管理需求分析；

：DNS服务器的配置、设备选型、层次化设计方案的编辑、防火墙、冗余或负载均衡设计、网管工作站设计；

：设计性原则、网络安全及管理规划设计、web服务器的配置、三层交换机的配置。

# 参考文献：

[1] 王保智．局域网设计与组网实用教程．北京：清华大学出版社，2004.8.

[2] 谢希仁．计算机网络．北京：电子工业出版社，2008.1

[3] 易建勋．计算机网络设计，北京：人民邮电出版社，2007.5.