

《计算机网络》课程设计个人报告

（2020——2021 年度第一学期）

|  |  |
| --- | --- |
| 题 目 |  |
|  | ——个人设计报告 |
| 专 业 | 计算机科学与技术 |
| 班 级 |  |
| 姓 名 |  |

**《计算机网络》课程设计**

**成 绩 评 定**

|  |  |  |  |
| --- | --- | --- | --- |
| **学号** | **姓名** | **个人成绩** | **备注** |
|  |  |  | 组成员 |

指导教师： 李臻

目录

[摘要 1](#_Toc59552264)

[1 网络详细设计 1](#_Toc59552265)

[本校园网网络采用层次化的设计方案。 1](#_Toc59552266)

[1.1.1 三层网络架构 1](#_Toc59552267)

[1.1.2 三层网络设计的短板 2](#_Toc59552268)

[1.2 防火墙技术和DMZ设计 3](#_Toc59552269)

[1.2.1 防火墙技术的基本思想 3](#_Toc59552270)

[1.2.2 防火墙的优点和缺点 3](#_Toc59552271)

[1.2.3 防火墙的特性 3](#_Toc59552272)

[1.2.4 防火墙对于学校校园网的意义 4](#_Toc59552273)

[1.3 冗余/负载均衡设计 4](#_Toc59552274)

[1.4线路冗余设计 4](#_Toc59552275)

[1.5 网络设备冗余/负载均衡设计 5](#_Toc59552276)

[1.6 网管工作站设计 5](#_Toc59552277)

[2 网络设备选型 6](#_Toc59552278)

[2.1 交换机选型 6](#_Toc59552279)

[2.1.1 交换机选型的基本原则 6](#_Toc59552280)

[2.1.2 大肥羊学校的交换机选型 7](#_Toc59552281)

[2.2 路由器选型 8](#_Toc59552282)

[2.2.1 路由协议支持 8](#_Toc59552283)

[2.2.2 路由器选型的性能因素 9](#_Toc59552284)

[2.2.3 路由器选型的灵活因素 9](#_Toc59552285)

[2.2.4 大肥羊学校的路由器选型 9](#_Toc59552286)

[3 DNS服务器的配置 9](#_Toc59552287)

[3.1 互联网的域名结构 10](#_Toc59552288)

[3.2 域名服务器 10](#_Toc59552289)

[3.3 大肥羊学校的DNS服务配置 10](#_Toc59552290)

[3.4 大肥羊学校DNS配置测试 12](#_Toc59552291)

[4 总结 13](#_Toc59552292)

**摘要**

在网络发达的今天，如何合理分配经费，建设高质量的校园网络，满足学校的信息化要求是学校建设者必须解决和完善的问题。要建设高质量的网络设计，需要从网络体系结构入手，采用先进、严谨、科学的设计规划方法，根据学校的地理位置、建筑布局、学校需求、费用支出、安全性能以及后期维护等多方面考虑，规划出最适合该学校的网络设计。本次设计以大肥羊学校网络设计为背景，研究构建网络相关技术构建一个性能优越、高稳定性、高安全性的网络平台，本文主要研究了网络设计过程中的层次化结构设计、路由器设备选型、DNS服务器的配置和设备选型方面进行分析研究。

**关键词： 校园网；层次化结构设计；DNS；路由器**

# 1 网络详细设计

## 本校园网网络采用层次化的设计方案。

### 1.1.1 三层网络架构

三层网络架构是采用层次化架构的三层网络，即把复杂的网络设计分成几个层次，每个层次着重于某些特定的功能，这样就能够使一个复杂的大问题变成许多简单的小问题。三层网络架构设计的网络有三个层次：核心层（网络的高速交换主干）、汇聚层（提供基于策略的连接）、接入层（将工作站接入网络）。

（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。核心层主要承担网络的高速数据交换和数据流的汇总，作为整个调度数据网的核心，网络必须高效、高可靠，具有强大的抗故障能力。因此，在核心层应该采用高带宽的交换机，核心层的设备采用双机冗余热备份是非常必要的，也可以使用负载均衡功能来改善网络性能。网络的控制功能最好尽量少在骨干层上实施。核心层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，也可以很好的进行网络负载均衡。

（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，快速转发交换机, 接入各个功能区域, 形成万兆无阻塞、快速转发骨干网络。还为整个交换网络提供VLAN间的路由选择功能，通过VLAN技术把网络隔离成不同网段，当某一网段出现问题时，不会影响到其它网段及核心层。

（3）接入层网络设计

接入层：在网络层次结构中直接连接用户的设备称为网络接入层。在接入层中网络用户接入密度比较大，所以要求接入设备的端口密度高，通常接入层中的连接设备价格相对低廉。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。它是校园网用户认证接入点，最好选用支持多业务，易管理，高安全的交换机。

（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。

### 1.1.2 三层网络设计的短板

三层网络结构数据中心网络传输模式是不断地改变的。大多数网络都是纵向（north-south）的传输模式，也就是主机与网络中的其它非相同网段的主机通信都是“设备—交换机—路由”到达目的地。同时，三层网络结构在同一个网段的主机通常连接到同一个交换机，可以直接相互通讯。然而，三层网络结构现代数据中心的计算和存储基础设施，主要网络流量模式从已经不止是单纯的不同网段之间通讯。三层网络结构内外网的通讯、网络段分布在多个接入交换机，要求主机通过网络互连等这些环境。这些三层网络结构网络环境的变化催生了两种技术趋势：网络收敛和虚拟化。

网络收敛：三层网络结构中，储存网络和通信网络在同一个物理网络中。主机和阵列之间的数据传输通过储存网络来传输，在逻辑拓扑上就像是直接连接的一样。如ISCSI等。

虚拟化：将物理客户端向虚拟客户端转化。虚拟化服务器是未来发展的主流和趋势，它将使三层网络结构的网络节点的移动变得非常简单。

横向网络（east-west）在纵向设计的三层网络结构中传输数据会带有传输的瓶颈，因为数据经过了许多不必要的节点（如路由和交换机等设备）。如果三层网络结构上主机需要通过高速带宽相互访问，但通过层层的uplink口，会导致潜在的、非常明显的性能衰减。三层网络结构的原始设计更会加剧这种性能衰减，由于生成树协议会防止冗余链路存在环路，双上行链路接入交换机只能使用一个指定的网络接口链接。

虽然增大内部交换层的带宽有助于改善三层网络结构的传输阻塞，但这样受益的只是一个节点。E-W模式中主机之间的的数据传输并非同一时间只是存在两个节点之间。相反，三层网络结构数据中心中的主机之间在任何时间都有数据传输的。因此，三层网络结构增加带宽这种高成本低效率的投资只是治标不治本。

## 1.2 防火墙技术和DMZ设计

防火墙是防范网络攻击最常用的方法，从技术理论上看，如今的防火墙经过了多年的不断改进,已经成为一种先进和复杂的基于应用层的网关，不仅能完成传统防火墙的过滤任务，同时也能够针对各种网络应用提供相应的安全服务。

### 1.2.1 防火墙技术的基本思想

防火墙是一种保护计算机网络安全的技术性措施，它通过在网络边界上建立相应的网络通信监控系统来隔离内部和外部网络，以阻挡来自外部的网络入侵。它是一种计算机硬件和软件的结合，使Internet与Internet之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入，防火墙主要由服务访问政策、验证工具、包过滤和应用网关4个部分组成，防火墙就是一个位于计算机和它所连接的网络之间的软件或硬件。

### 1.2.2 防火墙的优点和缺点

（1）优点

保护脆弱的服务，控制对系统的访问，集中地安全管理，增强保密性，记录和统计网络利用数据以及非法使用数据情况。

1. 缺点

防火墙是不能防病毒的，尽管有不少的防火墙产品声称其具有这个功能。数据在防火墙之间的更新是一个难题，如果延迟太大将无法支持实时服务请求。并且，防火墙采用滤波技术，滤波通常使网络的性能降低50%以上，如果为了改善网络性能而购置高速路由器，又会大大增加经济预算。

### 1.2.3 防火墙的特性

（1）数据必经；

（2）网络流量的合法性；

（3）抗攻击免疫力；

### 1.2.4 防火墙对于学校校园网的意义

通过防火墙既保证整个学校内部访问数据安全性, 同时阻止外网的非法入侵。

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。

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。

## 1.3 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。

## 1.4线路冗余设计

在校园网核心层，网络边界拓扑结构由于采用了双机热备份的核心交换机系统解决方案，所以在线路冗余方面的要求较高，对于线路的冗余要求，我们采用10GE线路对核心层设备进行环行双向备份，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：

（1）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。

（2）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。

## 1.5 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。

## 1.6 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。

# 2 网络设备选型

## 2.1 交换机选型

### 2.1.1 交换机选型的基本原则

在网络设计中对于交换机的选型需要考虑适用性与先进性相结合的原则，不同品牌的交换机产品价格差异较大，功能也不一样，因此选择时不能只看品牌或追求高价，也不能只看价钱低的，应该根据应用的实际情况，选择性能价格比高，既能满足目前需要，又能适应未来几年网络发展的交换机。选择市场主流产品的原则选择交换机时，应选择在国内市场上有相当的份额，具有高性能、高可靠性、高安全性、高可扩展性、高可维护性的产品，如思科、H3C、华为的产品市场份额较大。

1）安全可靠的原则

交换机的安全决定了网络系统的安全，选择交换机时这一点是非常重要的，交换机的安全主要表现在VLAN的划分、交换机的过滤技术。

产品与服务相结合的原则：选择交换机时，既要看产品的品牌又要看生产厂商和销售商品是否有强大的技术支持、良好的售后服务。

2）选择三层交换机时的基本原则

选择三层交换机时，首先要分析各种产品的性能指标，然而面对诸如交换容量(Gbps)、背板带宽(Gbps)、处理能力(Mpps)、吞吐量(Mpps)等众多技术指标，用户必须紧紧抓住“满配置时的吞吐量”这个指标，因为其他技术指标用户一般没有能力进行测量，惟有吞吐量是用户可以使用Smart Bits和IXIA等测试仪表直接测量和验证的指标。

（1）分布式优于集中式

不同品牌的交换机所采用的交换机技术也不同，主要可分为集中式和分布式两类。传统总线式交换结构模块是集中式，现代交换矩阵模块是分布式。

（2）关注延时与延时抖动指标

企业网、校园网几乎都是高速局域网，其目的之一就是为了音频和视频等大容量多媒体数据的传输，而这些大容量多媒体数据包最忌因延时较长和数据包丢失使信息传输产生抖动。有些传统集中式交换机的延时高达2s，而某些现代分布式交换机的延时只有10ms左右，两者相差上百倍。导致延时过高的原因通常包括阻塞设计的交换结构和过量使用缓冲等，所以关注延时实际上需要关注产品的模块结构。

（3）性能稳定：

三层交换机多用于骨干和汇聚层，如果性能不稳定，则会波及网络系统的大部分主机，甚至整个网络系统。所以，只有性能稳定的第三层交换机才是网络系统连续、可靠、安全和正常运行的保证。当然，性能稳定看似抽象，似乎需要历史检测才能有说服力。其实不然，由于设备性能实际上是通过多项基本技术指标和市场声誉来实现的。所以，用户可以通过吞吐量、延迟、丢帧率、地址表深度、线端阻塞和多对一功能等多项指标以及市场应用调查来确定。

（4）安全可靠

作为网络核心设备，三层交换机是被攻击的重要对象，要求必须将三层交换机纳入网络安全防护的范围。

1. 功能齐全

产品不但要满足现有需求，还应满足未来一段时间内的需求，从而给用户一个增值空间。

### 2.1.2 大肥羊学校的交换机选型

（1）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 |

（2）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 |

（3）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。 |

## 2.2 路由器选型

在网络层次结构的设计中，又存在基于交换技术的网络架构设计和基于路由技术的网络架构设计。

由于交换技术的快速发展，交换机性能提高很快，因此，基于交换技术的网络架构设计在企业网、校园网设计中被广泛使用。但是交换技术为主的网络架构由于其网络路由功能不强大，对不同子网用户之间通信频繁的业务处理力不强，也存在一定的技术局限。[1]

### 2.2.1 路由协议支持

路由协议可分为三类：静态路由方式、动态路由方式和混合路由方式。动态路由方式又分为边界路由协议( BGP)和内部网关协议(IGP)、路由信息协议(RIP)、开放最短路径优先协议(OSPF)等。静态路由方式的优势在于：

1. 信息传输的可预知性；
2. 对路由器和链路不会造成额外的开销；
3. 对小型网络而言，静态路由易于配置。

静态路由方式也存在一定的问题，其主要表现是对网络的管理缺乏可伸缩性，其次是当网络发生变化时，就得修改网上所有路由器的配置。

动态路由方式的主要优势在于其网络管理的伸缩性和适应性。凭借动态路由协议，路由器之间相互通信，由此了解网络拓扑结构，可以方便地使网络更迅速地发展扩大。同时它还可以确保路由器适应网络故障。只要冗余链路存在，相应的网络局部故障对于路由器就相当于某些网段搬迁，网络功能虽然受到影响，但仍可坚持运行。但动态路由方式同样存在问题，主要是复杂性问题，占用路由器和链路的额外开销问题以及路由协议的通用性问题[2]。

混合路由方式就是在网络中部分采用静态路由方式，部分采用动态路由方式，一般会在网络的边缘地带使用静态路由，在核心区与分布区使用动态路由。常用的协议介绍如下：

（1）内部网关协议RIP

RIP(Routing Information Protocol)是一种分布式的基于距离向量的路由选择协议，是互联网的标准协议，其最大的优点就是简单，开销较小，缺点在于它会限制网络的规模。

RIP使用跳数作为唯一的度量值。RIP允许一条路径最多只能包含15个路由器，在RIP中，规定跳数的最大值为15跳，16跳就视为不可达。RIP进程使用UDP（用户数据报协议）的520号端口发送和接受RIP分组，RIP分组每隔30s就从每个启动的RIP的接口发送路由更新信息。

RIP协议的特点是：仅和相邻路由器交换信息；路由器交换的信息是当前本路由器所知道的全部信息，即自己现在的路由表；按固定的时间交换路由信息。

（2）内部网关协议OSPF

OSPF（Open Shortest Path First，开放式最短路径优先）协议是目前网络中应用最广泛的路由协议之一，其能够适应各种规模的网络环境，它最主要的特征是使用分布式的“链路状态协议”。OSPF通过向全网扩散设备的链路状态信息，使网络中的每台设备最终同步一个具有全网链路状态的数据库（LSDB）。路由器采用最短路径优先（SPF）算法，以自己为根，计算到达其他网络的最短路径，最终形成全网路由信息。OSPF属于无类路由协议，支持VLSM（变长子网掩码）。OSPF以组播的形式进行链路状态通告。

（3）外部网关协议BGP

边界网关协议BGP所交换的网络可达性的信息就是要到达某个网络（用网络前缀表表示）所要经过的一系列自治系统。

### 2.2.2 路由器选型的性能因素

（1）可靠性和可维修性指标；

（2）吞吐量指标；

（3）系统延时指标。

### 2.2.3 路由器选型的灵活因素

（1）配置参数的灵活性；

（2）配置方式的灵活性；

（3）扩展接口的灵活性。

### 2.2.4 大肥羊学校的路由器选型

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。

# 3 DNS服务器的配置

域名系统DNS（Domain Name System）能够把互联网上的主机名字转换为IP地址。互联网的域名系统DNS被设计成为一个联机分布式数据库系统，并采用客户服务器方式。DNS使大多数名字都在本地进行解析（resolve），仅少量解析需要在互联网上通信，因此，DNS的效率很高。运行域名服务器程序的机器成为域名服务器。

## 3.1 互联网的域名结构

http://www.baidu.com

顶级域名

二级域名

服务

mail.cctv.com

三级域名

二级域名

顶级域名

图1 互联网的域名结构

## 3.2 域名服务器

DNS服务器的管辖范围不是以“域”为单位，而是以“区”为单位。区可能等于或小于域，但一定不能大于域。域名服务器划分为四种不同的类型：

1. 根域名服务器；
2. 顶级域名服务器；
3. 权限域名服务器；
4. 本地域名服务器。

## 3.3 大肥羊学校的DNS服务配置

大肥羊学校的DNS服务分别配置在内网服务器上和外网服务器上。

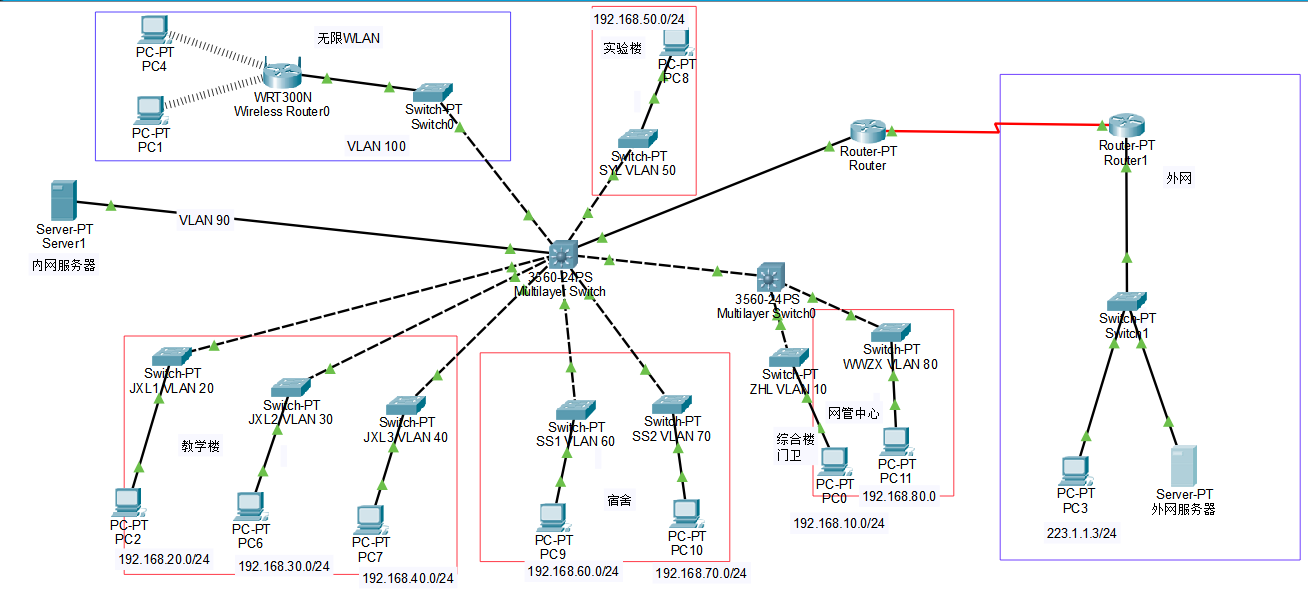


图2 网络拓扑图的DNS配置服务器

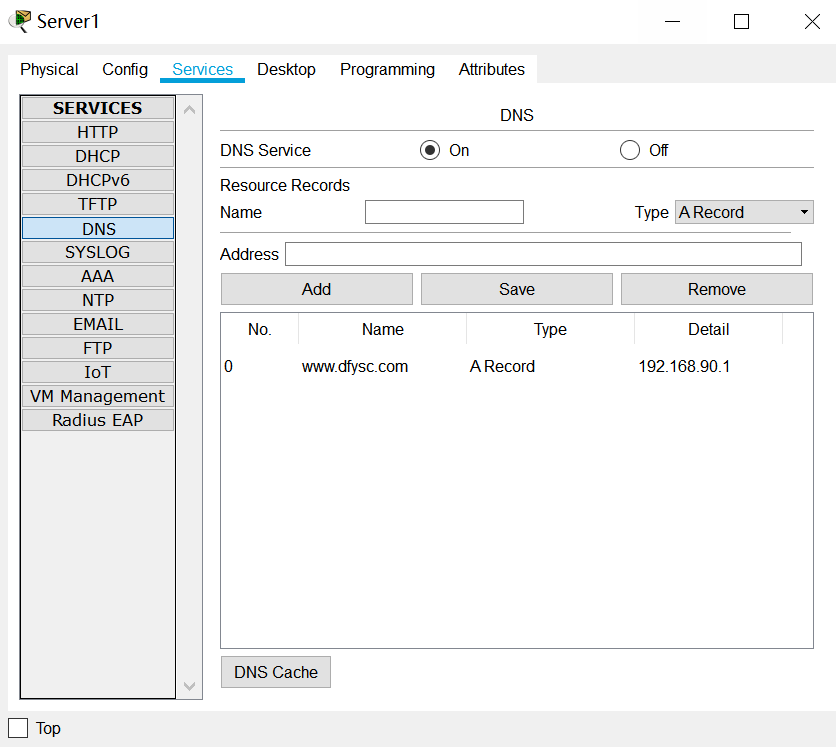


图3 内网服务器上的DNS配置

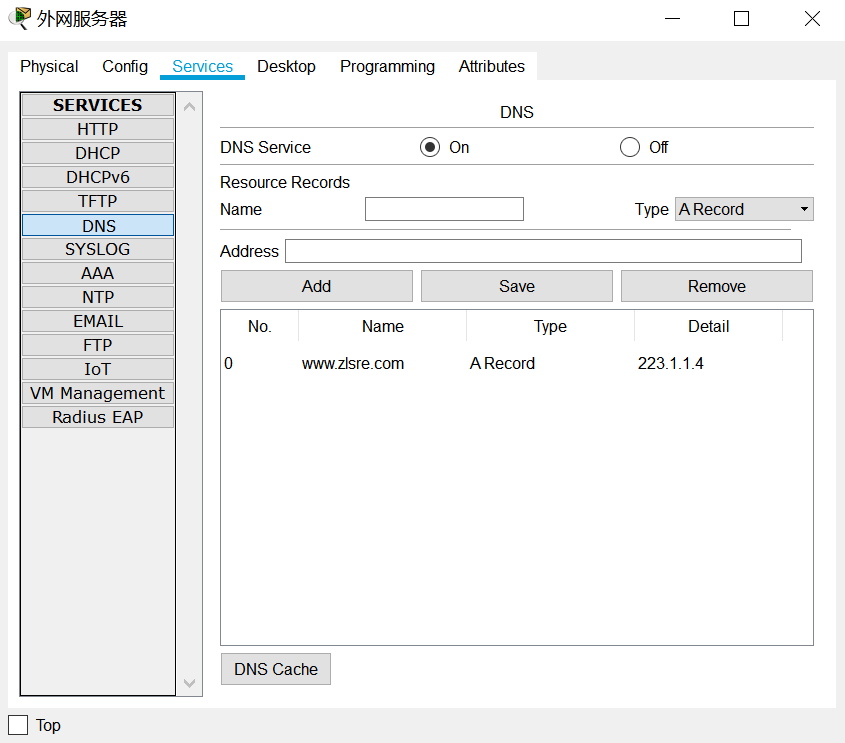


图4 外网服务器上的DNS配置

## 3.4 大肥羊学校DNS配置测试

用PC通过域名访问网页。

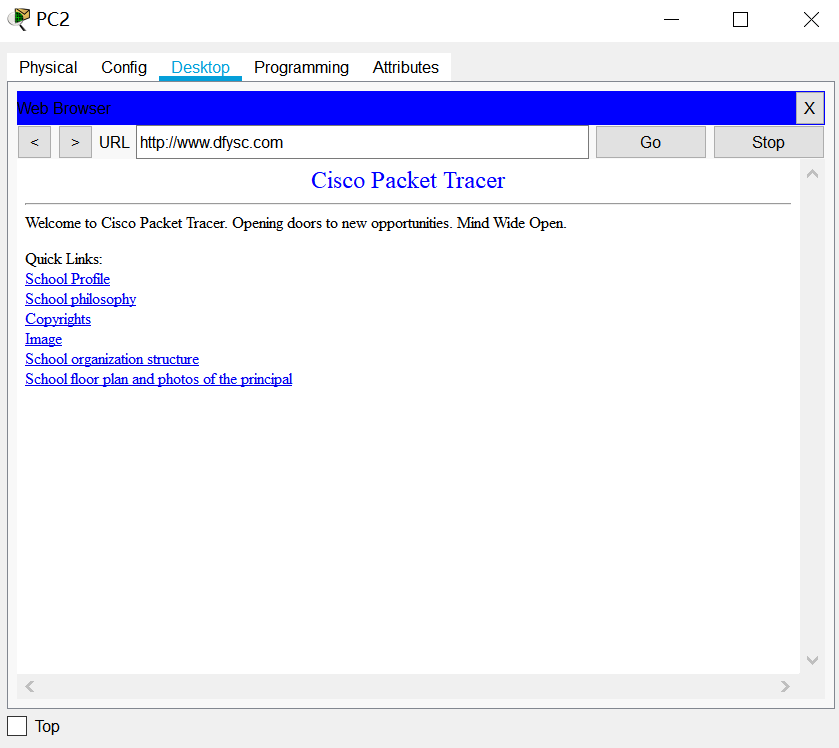


图5 通过内网服务器上的DNS域名访问网页

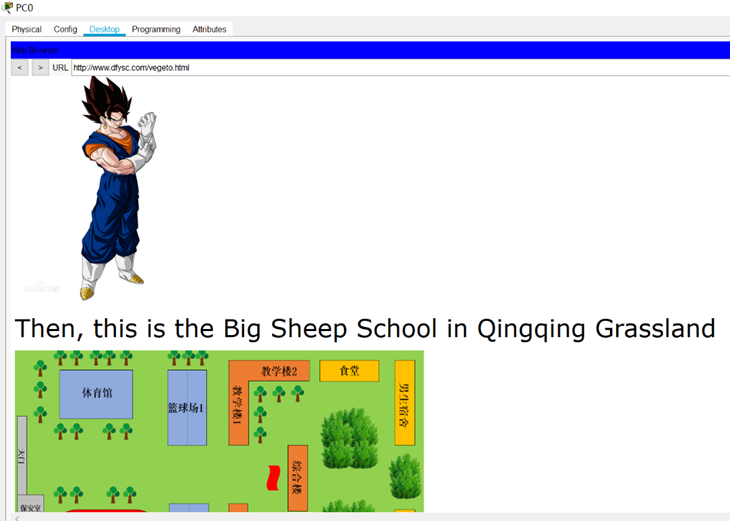


图6 通过外网服务器上的DNS域名访问网页

# 4 总结

本次课程设计是一次全新的体验，是对本学期计算机网络课程学习的一次回顾和总结。这次设计，我和小组成员经过一开始的商讨，首先确定了选题和分工，接着我们各自查询资料，学习很多自己负责部分的知识，有的知识是已经具备的，只需要细化和深挖，有些知识还需要我们开始学习，但无论是哪种，我们都秉持着一个学习的态度，对旧知识进行一遍遍地复盘，对新知识进行仔细地理解和掌握。期间，我和小组成员进行了三次地讨论，做完自己地任务后，我们一起汇总所有内容，最终形成了一份设计报告，我们彼此分享自己学到的知识，共同学习，互相帮助。

本次课程设计我们的选题是大肥羊学校的校园网络建设，为了完成这一选题，我们首先对学校的占地面积、建筑以及学校概况进行了一些资料的查阅和了解。其次，我们开始用本学期学到的一些技术建设学校的网络架构，比如交换机、路由器的设备选型；交换机和路由器的配置；WEB、FTP、DNS以及DHCP服务器的设置；NAT配置；静态路由的配置等等。我的分工是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、网管工作站设计等工作，在这个过程中，我确确实实对这些知识有了新的掌握和理解，在组员的帮助下，我也对他们的任务进行了学习，总体来说，我在这次课程设计中收获颇多，不仅仅在网络技术上有了进步，对于文字编辑、PPT的制作以及资料查阅的效率等方面得到了技能的提升，还有一个重要的收获就是我和我的组员们共同完成这个任务，我深深感受到了团队的力量以及如何在团队中扮演好一个成员的角色。

在本次网络设计中，不管是技术还是技能，我们还是有进步的空间，我们依然有很多需要学习的地方，对于这些缺点和弱势，在未来的学习和生活中，我们还会继续学习、继续努力，逐渐完善自己，让自己学有所得，学有所用。这是一次很有收获的经历，是一次很有价值的经历，我依然会抱着学习的态度虚心接着完善自己的知识和技能。