

信阳农林学院

本科生课程论文



题 目: 《信阳农林学院网络规划设计报告》

姓 名: XXXXXXXXXX

学 院: 信息工程学院

专 业: XXXXXXXXXX

班 级: XXXXXXXXXXXXXXXXXX

学 号: XXXXXXXXXXXXXX

指导教师: XXXXXXXXXXXXXXXXXX

2020 年 06 月 17 日

信阳农林学院教务处制

摘 要

随着经济的发展，信息起着越来越重要的作用。计算机、网络和多媒体等信息技术的飞速发展，信息的传递越来越快捷，信息的处理能力变得越来越强，信息的表现形式也越来越丰富，这些都对社会经济和人们的生活产生了深刻的影响。这一切促使通信网络由传统的电话网络向高速多媒体信息网发展。近几年来 Internet 得到了突飞猛进的发展，联入网络的节点和信息资源迅速增长。

为了满足广大大学生的学习需要，教职工教学办公需求。建立一个基于校园 Intranet 的信息管理和应用的网络系统，并提供相应的各种服务。将校园内各种不同应用的信息资源通过高性能的网络设备相互连接起来，形成校园园区内部的 Intranet 系统，对外通过防火墙设备接入广域网。

本文介绍了通过华为模拟器 ENSP，用网络拓扑结构设计方法规划校园网络方案。并详细给出基于此网络组建方案的规划，以及理论上的性能优化方案。合理分配了校园内的各层次的 IP 地址，作出全面规划。

关键词：校园网；防火墙；ENSP；规划

Title: Network Planning and Design Report of Xinyang Agriculture
and Forestry College

Abstract

As the economy develops, information plays an increasingly important role. The rapid development of information technology such as computers, networks and multimedia, the transfer of information is getting faster and faster, the processing power of information has become stronger and stronger, and the expression of information has become more and more rich. Had a profound impact. All this has promoted the development of communication networks from traditional telephone networks to high-speed multimedia information networks. In recent years, the Internet has developed by leaps and bounds, and the nodes and information resources connected to the network have grown rapidly.

In order to meet the learning needs of the majority of college students, the teaching and office needs of faculty and staff. Establish a network system based on campus intranet information management and application, and provide corresponding services. The information resources of various applications in the campus are connected to each other through high-performance network equipment to form an intranet system within the campus campus, and external access to the wide area network through a firewall device.

This article introduces how to use the network topology design method to plan the campus network plan through the ENSP. In addition, the planning based on this network formation scheme and the theoretical performance optimization scheme are given in detail. The IP addresses of all strata on the campus have been reasonably allocated to make a comprehensive plan.

Keywords: Campus; Firewall; ENSP; Panning

目 录

1 绪论.....	1
1.1 组网概述	1
1.2 规划目标	1
2 需求分析	2
2.1 终端接入数量、位置分布.....	2
2.2 组网技术要求	2
2.2.1 VLAN	2
2.2.2 VRRP	3
2.2.3 IPSEC	3
2.2.4 防火墙技术	3
2.2.5 ACL	4
2.2.6 Telnet	4
2.2.7 DHCP	4
2.3 其他要求	4
2.3.1 宽带要求	4
2.3.2 子网划分要求.....	5
2.3.3 安全性要求	5
2.4 网络设计	5
2.4.1 设备类型及数量	5
2.4.2 Vlan 规划	5
2.4.3 互联互通设计	6
3 模拟组网验证	7
3.1 网络拓扑图	7
3.2 设备配置	7
3.2.1 接入层 IP 划分核心代码（以 SW2 为例）	7
3.2.2 汇聚层 IP 划分核心代码（以 LSW3 为例）	7
3.2.3 核心层 IP 划分核心代码（以 LSW1 为例）	8

3.2.4 防火墙配置 IP 核心代码（以 FW2 为例）	8
3.2.5 双机热备核心代码（以 vlan1 为例）	8
3.2.6 acl 配置核心代码，应用于汇聚层	9
3.2.7 两校区间路由器的配置核心代码	9
3.2.8 IPSEC 配置，以 FW1 为例	9
3.2.9 telnet 配置（以 SW5 为例）	10
3.3 结果测试	10
3.3.1 IP 获取测试	10
3.3.2 互通测试	12
3.3.2 双机热备查看	14
3.3.3 telnet 登录测试	15
3.4 结果分析	17
体 会	18
致 谢	19
参 考 文 献	20

1 绪论

1.1 组网概述

信阳农林学院校园占地 1430 余亩，校舍建筑面积 44.5 万余平方米，包含羊山校区、浉河校区、南湾校区。在校学生 1.4 万余人，主校区羊山校区主要建筑有三大区域，分别是行政楼区域、图书馆区域、学生宿舍区域。图书馆区域主要为服务器数据中心，行政楼主要为教师上网区域人数为 300 左右，学生宿舍区域为 20 栋学生宿舍楼，学生上网人数为 1.4 万余人。

学校中心机房位于图书馆四楼，拥有教务系统、学校官网，校内办公网三台 web 服务器；整个网络通过华为防火墙接入互联网。

1.2 规划目标

（1）根据行政楼区域，学生宿舍楼区域，图书馆区域以及浉河区校区（人数较少）的上网人数需求合理分配 IP 网段，满足各区域上网需求。

（2）整个网络规划为三层网络架构，接入层、汇聚层、核心层，出口使用华为防火墙，根据需求划分好防火墙安全区域，行政楼、学生宿舍至图书馆机房带宽不低于 2000M。

（3）羊山校区内所有交换机设备可以在局域网内任意一台设备可通过 Telnet 远程管理。

（4）行政楼及学生宿舍区域上网设备可以自动获取 IP 地址。

（5）行政楼区域可对图书馆中心机房中 web 服务随意访问，学生宿舍区域不能访问校内办公网服务器，外网用户只可访问学校官网服务器。

（6）为保障网络稳定，核心交换机要部署双机热备。

（7）配置好出口 nat 地址转换，以及学校官网服务器外网访问端口映射

（8）为保证羊山校区和浉河校区通信安全，两校区通信采用 ipsec vpn 方式进行通信。

2 需求分析

2.1 终端接入数量、位置分布

信阳农林学院主要包括羊山校区、浉河校区两部分，在校生 1.4 万余人，主校区羊山校区主要建筑有三大区域，分别是行政楼区域、图书馆区域、学生宿舍区域。图书馆区域主要为服务器数据中心，行政楼主要为教师上网区域人数为 300 左右，学生宿舍区域为 20 栋学生宿舍楼，学生上网人数为 1.4 万余人。可拟出以下终端接入表格。

区域	图书馆	行政楼	学生公寓	浉河校区
人数/人	/	300	14000	人数较少

2.2 组网技术要求

熟悉防火墙技术的原理、应用，使学生了解防火墙技术的发展和分类，掌握防火墙的工作原理和功能配置，掌握防火墙在网络规划设计中具体应用方案。

2.2.1 VLAN

虚拟局域网（VLAN）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网。VLAN 是一种比较新的技术，工作在 OSI 参考模型的第 2 层和第 3 层，一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第 3 层的路由器来完成的。与传统的局域网技术相比较，VLAN 技术更加灵活，它具有以下优点：网络设备的移动、添加和修改的管理开销减少；可以控制广播活动；可提高网络的安全性。[1]

在计算机网络中，一个二层网络可以被划分为多个不同的广播域，一个广播域对应了一个特定的用户组，默认情况下这些不同的广播域是相互隔离的。不同的广播域之间想要通信，需要通过一个或多个路由器。这样的广播域就称为 VLAN。

2.2.2 VRRP

VRRP 是一种选择协议，它可以把一个虚拟路由器的责任动态分配到局域网上的 VRRP 路由器中的一台。控制虚拟路由器 IP 地址的 VRRP 路由器称为主路由器，它负责转发数据包到这些虚拟 IP 地址。一旦主路由器不可用，这种选择过程就提供了动态的故障转移机制，这就允许虚拟路由器的 IP 地址可以作为终端主机的默认第一跳路由器。是一种 LAN 接入设备备份协议。一个局域网络内的所有主机都设置缺省网关，这样主机发出的目的地址不在本网段的报文将被通过缺省网关发往三层交换机，从而实现了主机和外部网络的通信。 [2]

VRRP 是一种路由容错协议，也可以叫做备份路由协议。一个局域网络内的所有主机都设置缺省路由，当网内主机发出的目的地址不在本网段时，报文将被通过缺省路由发往外部路由器，从而实现了主机与外部网络的通信。当缺省路由器 down 掉（即端口关闭）之后，内部主机将无法与外部通信，如果路由器设置了 VRRP 时，那么这时，虚拟路由将启用备份路由器，从而实现全网通信。

2.2.3 IPSEC

互联网安全协议（英语：Internet Protocol Security，缩写为 IPsec），是一个协议包，通过对 IP 协议的分组进行加密和认证来保护 IP 协议的网络传输协议族（一些相互关联的协议的集合）。 [3]

IPsec 主要由以下协议组成：一、认证头（AH），为 IP 数据报提供无连接数据完整性、消息认证以及防重放攻击保护；二、封装安全载荷（ESP），提供机密性、数据源认证、无连接完整性、防重放和有限的传输流（traffic-flow）机密性；三、安全关联（SA），提供算法和数据包，提供 AH、ESP 操作所需的参数。

2.2.4 防火墙技术

防火墙是一个由计算机硬件和软件组成的系统，部署于网络边界，是内部网络和外部网络之前的连接桥梁，同时对进出网络边界的数据进行保护，防止恶意入侵、恶意代码的传播等，保障内部网络数据的安全 [4] 。防火墙技术是建立在网络技术和信息安全技术基础上的应用性安全技术，几乎所有的企业内部网络与外部网络（如因特网）相连接的边界设都会放置防火墙，防火墙能够起到安全过滤和安全隔离外网攻击、入侵等有害的网络安全信息和行为 [5] 。

2.2.5 ACL

访问控制列表 (ACL) 是一种基于包过滤的访问控制技术，它可以根据设定的条件对接口上的数据包进行过滤，允许其通过或丢弃。访问控制列表被广泛地应用于路由器和三层交换机，借助于访问控制列表，可以有效地控制用户对网络的访问，从而最大程度地保障网络安全。 [6]

2.2.6 Telnet

Telnet 协议是 TCP/IP 协议族中的一员，是 Internet 远程登录服务的标准协议和主要方式。它为用户提供了在本地计算机上完成远程主机工作的能力。在终端使用者的电脑上使用 telnet 程序，用它连接到服务器。终端使用者可以在 telnet 程序中输入命令，这些命令会在服务器上运行，就像直接在服务器的控制台上输入一样。可以在本地就能控制服务器。要开始一个 telnet 会话，必须输入用户名和密码来登录服务器。Telnet 是常用的远程控制 Web 服务器的方法。 [7]

2.2.7 DHCP

DHCP（动态主机配置协议）是一个局域网的网络协议。指的是由服务器控制一段 IP 地址范围，客户机登录服务器时就可以自动获得服务器分配的 IP 地址和子网掩码。默认情况下，DHCP 作为 Windows Server 的一个服务组件不会被系统自动安装，还需要管理员手动安装并进行必要的配置。 [8]

2.3 其他要求

2.3.1 宽带要求

整个网络规划为三层网络架构，接入层、汇聚层、核心层，出口使用华为防火墙，根据需求划分好防火墙安全区域，行政楼、学生宿舍至图书馆机房带宽应不低于 2000M。

图书馆宽带：1000*3=3000Mbps

行政楼宽带：1000*2=2000Mbps

学生宿舍宽带：1000*2=2000Mbps

其中图书馆三台服务器各个 1000M 宽带可以减少宽带占用

2.3.2 子网划分要求

学生公寓与行政楼终端接入需求量较大，首先进行 IP 划分，并留出足够的地址空间，进行远期规划；终端接入量较少的浉河校区及图书馆最后进行划分，按终端接入量大小一级级划分。

2.3.3 安全性要求

进行 VLAN 划分,实现广播范围的控制，减少广播风暴和网络带宽资源浪费等问题，提高网络运行效率，同时可以区分不同的用户,方便学校的管理与维护。使用防火墙技术在防止外来黑客的攻击的同时防止校园内学生的恶作剧以及限制学生访问非法站点。

2.4 网络设计

2.4.1 设备类型及数量

序号	设备	数量
1	客户端主机	14000
2	接入层交换机	200
3	汇聚层交换机	4
4	核心交换机	2
5	防火墙	2
6	服务器	3

2.4.2 Vlan 规划

区域	vlan	划分 ip
学校官网	10	22.22.11.0/26
教务系统	20	22.22.22.0/26
校内办公网	30	22.22.33.0/26
行政楼	100	172.16.0.0/22
学生公寓	200	172.14.0.0/14
(信息中心) 图书馆	300	12.0.0.0/24 13.0.0.0/24

2.4.3 互联互通设计

①学生公寓

使每个子网内的任意 PC 向其他子网的网络节点发送 ICMP 报文，检测本子网的主机能否与其他子网通信。但是无法访问校内办公室的网络。

②行政楼

使每个子网内的任意 PC 向其他子网的网络节点发送 ICMP 报文，检测本子网的主机能否与其他子网通信。但是无法访问校内办公室的网络。

③外网与校园网

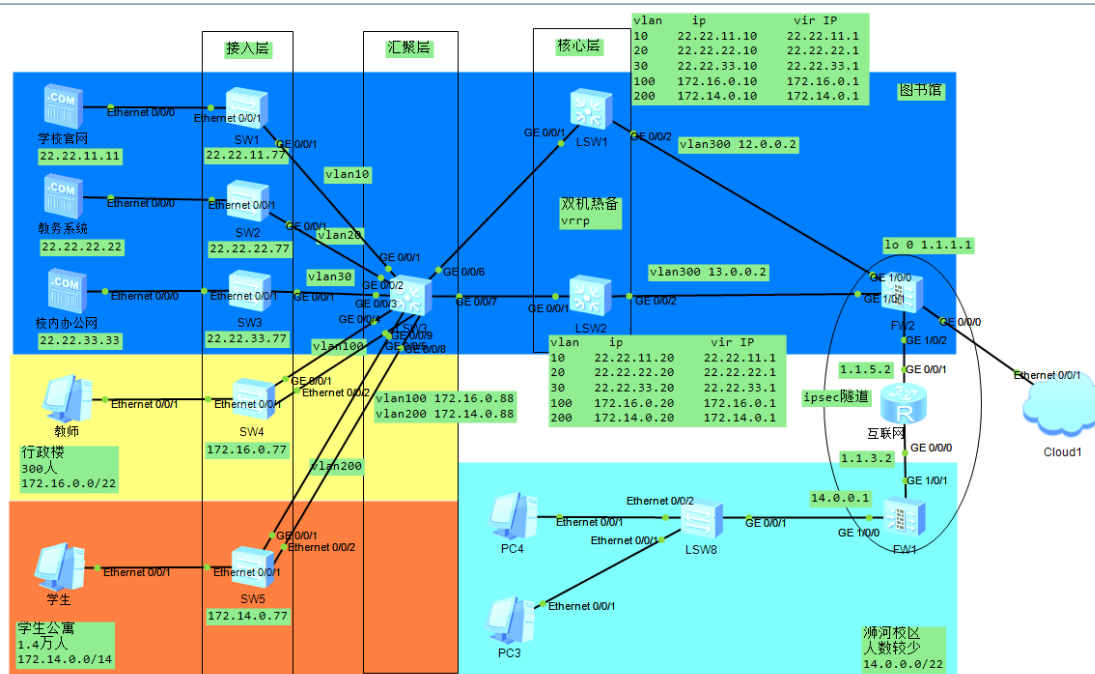
外网无法访问校内的办公网络，但是可以访问学校官网。

④交换机

羊山校区内所有交换机设备可以在局域网内任意一台设备可通过 Telnet 远程管理。

3 模拟组网验证

3.1 网络拓扑图



3.2 设备配置

3.2.1 接入层 IP 划分核心代码（以 SW2 为例）

```
[SW2]int e0/0/1
[SW2-Ethernet0/0/1]port link-type access
[SW2-Ethernet0/0/1]port default vlan 20
[SW2-Ethernet0/0/1]int g0/0/1
[SW2-GigabitEthernet0/0/1]port link-type trunk
[SW2-GigabitEthernet0/0/1]port trunk allow-pass vlan 20
```

3.2.2 汇聚层 IP 划分核心代码（以 LSW3 为例）

```
[LSW3]vlan batch 10 20 30 100 200
Info: This operation may take a few seconds. Please wait for a moment...done.
[LSW3]int g0/0/1
[LSW3-GigabitEthernet0/0/1]port link-type trunk
[LSW3-GigabitEthernet0/0/1]port trunk allow-pass vlan 10
.....
[LSW3-GigabitEthernet0/0/6]port trunk allow-pass vlan 10 20 30 100 200
```

```
[LSW3-GigabitEthernet0/0/6]int g0/0/7
[LSW3-GigabitEthernet0/0/7]port link-type trunk
[LSW3-GigabitEthernet0/0/7]port trunk allow-pass vlan 10 20 30 100 200
```

3. 2. 3 核心层 IP 划分核心代码（以 LSW1 为例）

```
[LSW1]vlan batch 10 20 30 100 200 300
[LSW1]int g0/0/1
[LSW1-GigabitEthernet0/0/1]port link-type trunk
[LSW1-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 20 30 100 200
[LSW1]int vlan 10
[LSW1-Vlanif10]ip add 22.22.11.10 24
..... 以下是配置 dhcp 服务部分 .....
[LSW1]dhcp enable
[LSW1]dhcp snooping enable
[LSW1]int vlan 100
[LSW1-Vlanif100]ip add 172.16.0.10 16
[LSW1-Vlanif100]dhcp select global
[LSW1]ip pool officebuilding
[LSW1-ip-pool-officebuilding]network 172.16.0.0 mask 255.255.255.0
[LSW1-ip-pool-officebuilding]gateway-list 172.16.0.1
[LSW1-ip-pool-officebuilding]dns-list 8.8.8.8
.....
[LSW1]int vlan 300
[LSW1-Vlanif300]ip add 12.0.0.2 24
[LSW1-Vlanif300]q
[LSW1]int g0/0/2
[LSW1-GigabitEthernet0/0/2]port link-type access
[LSW1-GigabitEthernet0/0/2]port default vlan 300
```

3. 2. 4 防火墙配置 IP 核心代码（以 FW2 为例）

```
[USG6000V1]int g1/0/0
[USG6000V1-GigabitEthernet1/0/0]ip add 12.0.0.1 24
[USG6000V1-GigabitEthernet1/0/0]int g1/0/1
[USG6000V1-GigabitEthernet1/0/1]service-manage all permit
[USG6000V1-GigabitEthernet1/0/1]ip add 13.0.0.1 24
```

3. 2. 5 双机热备核心代码（以 vlan1 为例）

```
[LSW1]ip route-static 1.1.1.0 255.255.255.0 12.0.0.1
[LSW2]ip route-static 1.1.1.0 255.255.255.0 13.0.0.1
[USG6000V1]ip route-static 22.22.11.0 255.255.255.0 12.0.0.2
[USG6000V1]ip route-static 22.22.11.0 255.255.255.0 13.0.0.2 preference 70
主
```

```

[LSW1]int vlan 10
[LSW1-Vlanif10]vrrp vrid 1 virtual-ip 22.22.11.1
[LSW1-Vlanif10]vrrp vrid 1 priority 200
[LSW1-Vlanif10]vrrp vrid 1 preempt-mode timer delay 0
[LSW1-Vlanif10]vrrp vrid 1 track interface g0/0/2 reduced 100
[LSW1-Vlanif10]vrrp vrid 1 track interface g0/0/1 reduced 100
[LSW1-Vlanif10]
备份
[LSW2]int vlan 10
[LSW2-Vlanif10]vrrp vrid 1 virtual-ip 22.22.11.1
[LSW2-Vlanif10]vrrp vrid 1 priority 150
[LSW2-Vlanif10]vrrp vrid 1 preempt-mode timer delay 0

```

3. 2. 6 acl 配置核心代码，应用于汇聚层

```

[LSW3]acl number 3000
[LSW3-acl-adv-3000]rule 5 p
[LSW3-acl-adv-3000]rule 5 permit ip source 172.14.0.0 0.0.0.255 destination 22.22.33.0 0.0.0.255
[LSW3]traffic classifier 111
[LSW3-classifier-111]if-match acl 3000
[LSW3]traffic behavior 111
[LSW3-behavior-111]deny
[LSW3]traffic policy 111
[LSW3-trafficpolicy-111]classifier 111 behavior 111
[LSW3]traffic-policy 111 global inbound

```

3. 2. 7 两校区间路由器的配置核心代码

```

[INTERNET]int g0/0/0
[INTERNET-GigabitEthernet0/0/0]ip add 1.1.3.2 24
[INTERNET]int g0/0/1
[INTERNET-GigabitEthernet0/0/1]ip add 1.1.5.2 24
[INTERNET]ospf
[INTERNET-ospf-1]area 0
[INTERNET-ospf-1-area-0.0.0.0]network 1.1.3.0 0.0.0.255
[INTERNET-ospf-1-area-0.0.0.0]network 1.1.5.0 0.0.0.255

```

3. 2. 8 IPSEC 配置，以 FW1 为例

配置到达分支机构的静态路由，此处假设下一跳地址为 1.1.3.2

```
[USG6000V1]ip route-static 0.0.0.0 0.0.0.0 1.1.3.2
```

定义被保护的数据流。

```

[USG6000V1]acl 3000
[USG6000V1-acl-adv-3000]rule permit ip source 14.0.0.0 0.0.0.255 destination 12.0.0.0 0.0.0.255
[USG6000V1-acl-adv-3000]rule permit ip source 14.0.0.0 0.0.0.255 destination 13.0.0.0 0.0.0.255

```

配置名称为 tran1 的 IPSec 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG6000V1]ipsec proposal tran1
[USG6000V1-ipsec-proposal-tran1]encapsulation-mode tunnel
[USG6000V1-ipsec-proposal-tran1]transform esp
[USG6000V1-ipsec-proposal-tran1]esp authentication-algorithm sha2-256
```

配置序号为 10 的 IKE 安全提议。（第 2 条命令开始为缺省配置可以不用配置）

```
[USG6000V1]ike proposal 10
[USG6000V1-ike-proposal-10]authentication-method pre-share
[USG6000V1-ike-proposal-10]authentication-algorithm sha2-256
```

配置名称为 b 的 IKE Peer。

```
[USG6000V1]ike peer b
[USG6000V1-ike-peer-b]ike-proposal 10
[USG6000V1-ike-peer-b]pre-shared-key huawei
```

配置名称为 map_temp 序号为 1 的 IPSec 安全策略模板。

```
[USG6000V1]ipsec proposal
[USG6000V1]ipsec policy-template map_temp 1
[USG6000V1-ipsec-policy-templet-map_temp-1]security acl 3000
[USG6000V1-ipsec-policy-templet-map_temp-1]proposal tran1
[USG6000V1-ipsec-policy-templet-map_temp-1]ike-peer b
```

在 IPSec 安全策略 map1 中引用安全策略模板 map_temp。

```
[USG6000V1]ipsec policy map1 10 isakmp template map_temp
```

在接口 GigabitEthernet 1/0/1 上应用安全策略 map1。

```
[USG6000V1]interface g1/0/1
[USG6000V1-GigabitEthernet1/0/1]ipsec policy map1
```

3.2.9 telnet 配置（以 SW5 为例）

```
[SW5]telnet server enable
[SW5]aaa
[SW5-aaa]local-user admin password cipher huawei
[SW5-aaa]local-user admin service-type telnet
[SW5]user-interface vty 0 4
[SW5-ui-vty0-4]authentication-mode aaa
[SW5-ui-vty0-4]protocol inbound telnet
[SW5]int vlan 200
[SW5-Vlanif200]ip add 172.14.0.77 24
```

3.3 结果测试

3.3.1 IP 获取测试

①PC 机通过 dhcp 自动获取 IP

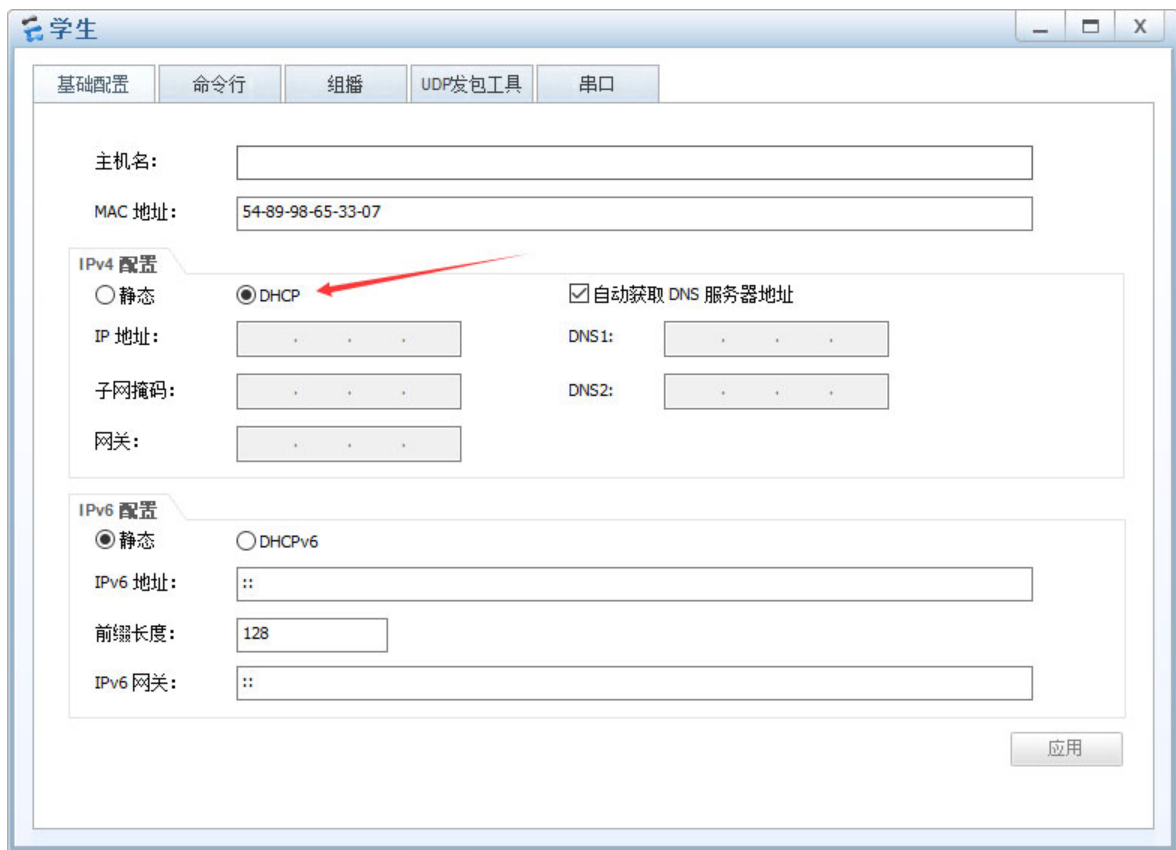


图 1 学生机开启 dhcp

②PC 机可以成功获取 IP

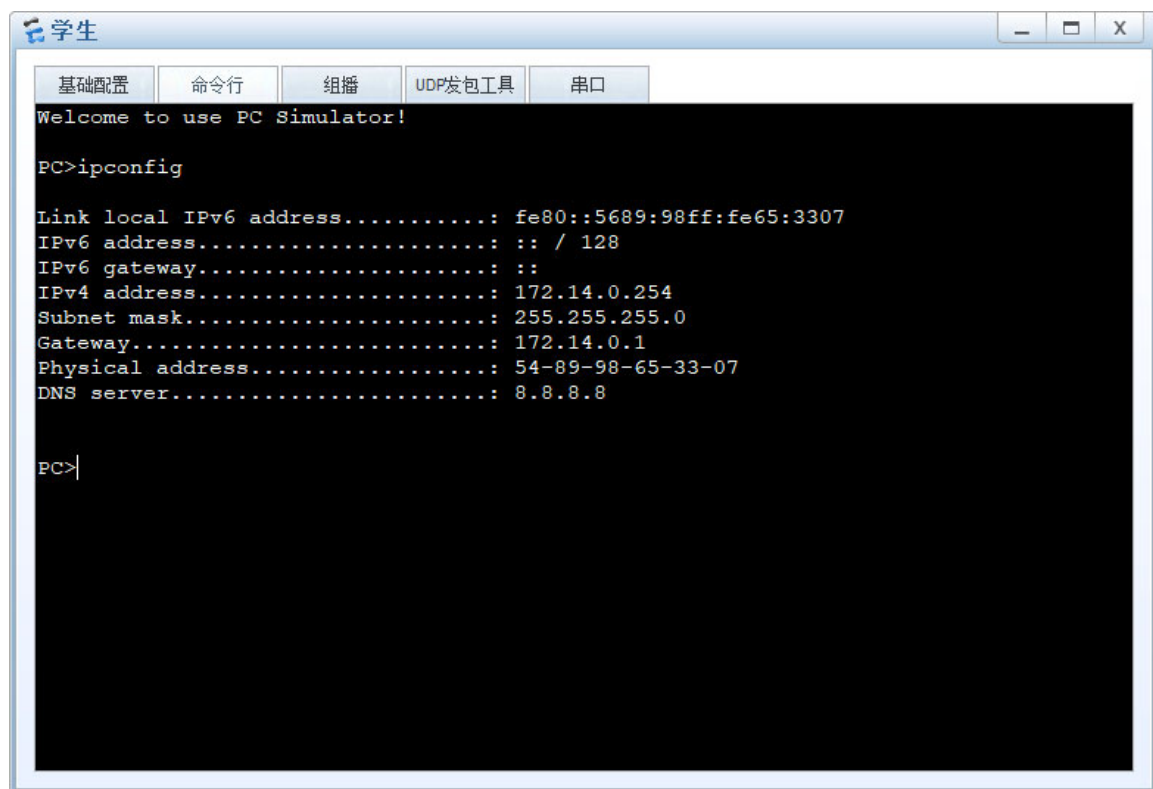


图 2 PC 机获取到 IP

3.3.2 互通测试

①学生公寓楼中的学生机可以成功连通学校官网，教务系统，无法连通校内办公网，达到设计目的。

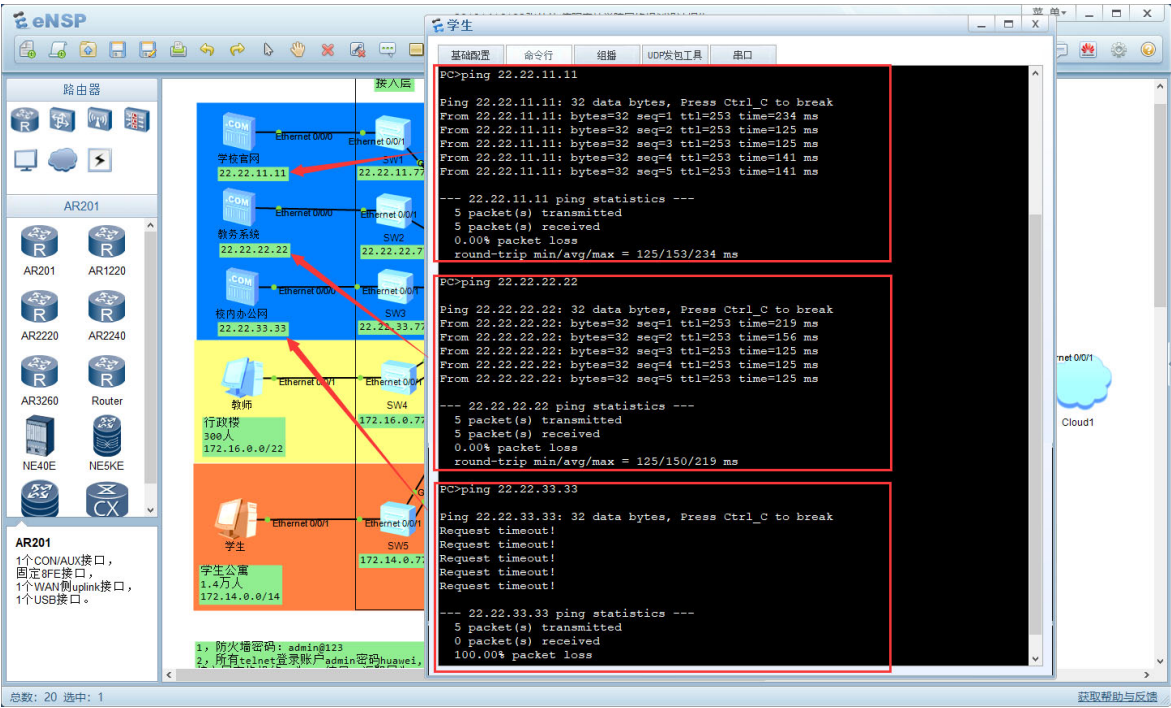


图 3 学生机连通校园网情况

②行政楼的教师机可以成功连通所有服务器。

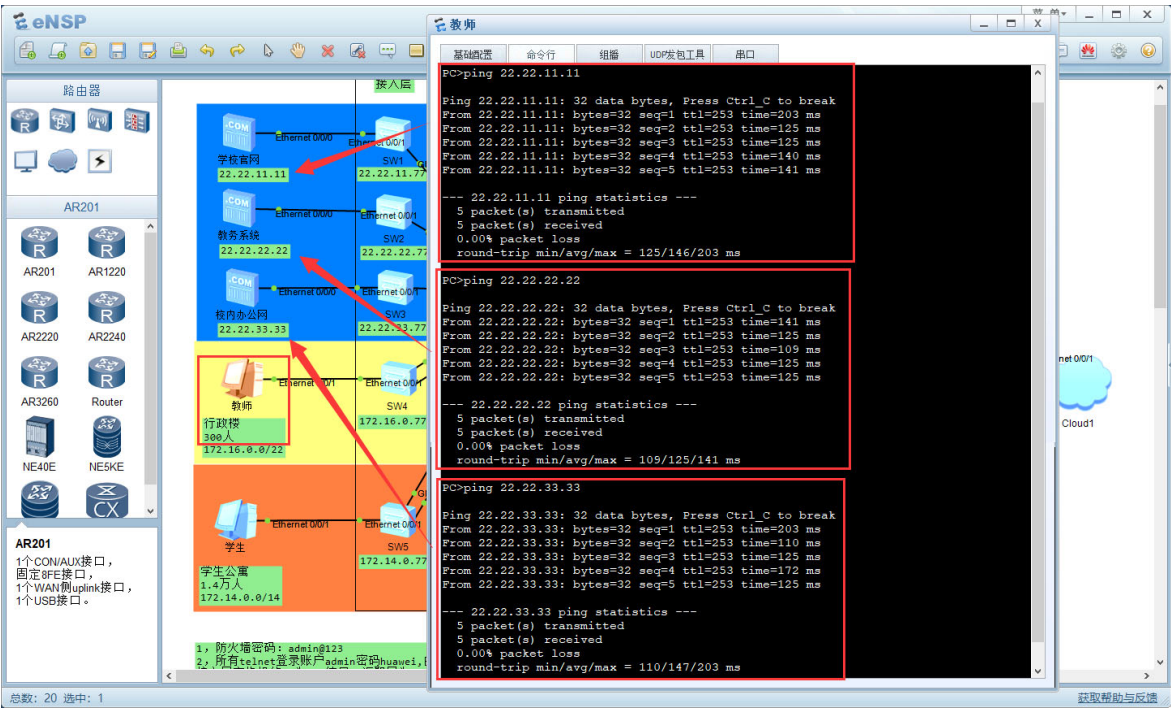


图 4 教师机连通校园网情况

③双机热备测试，即使关闭一台核心交换机内网依旧可以正常通信。

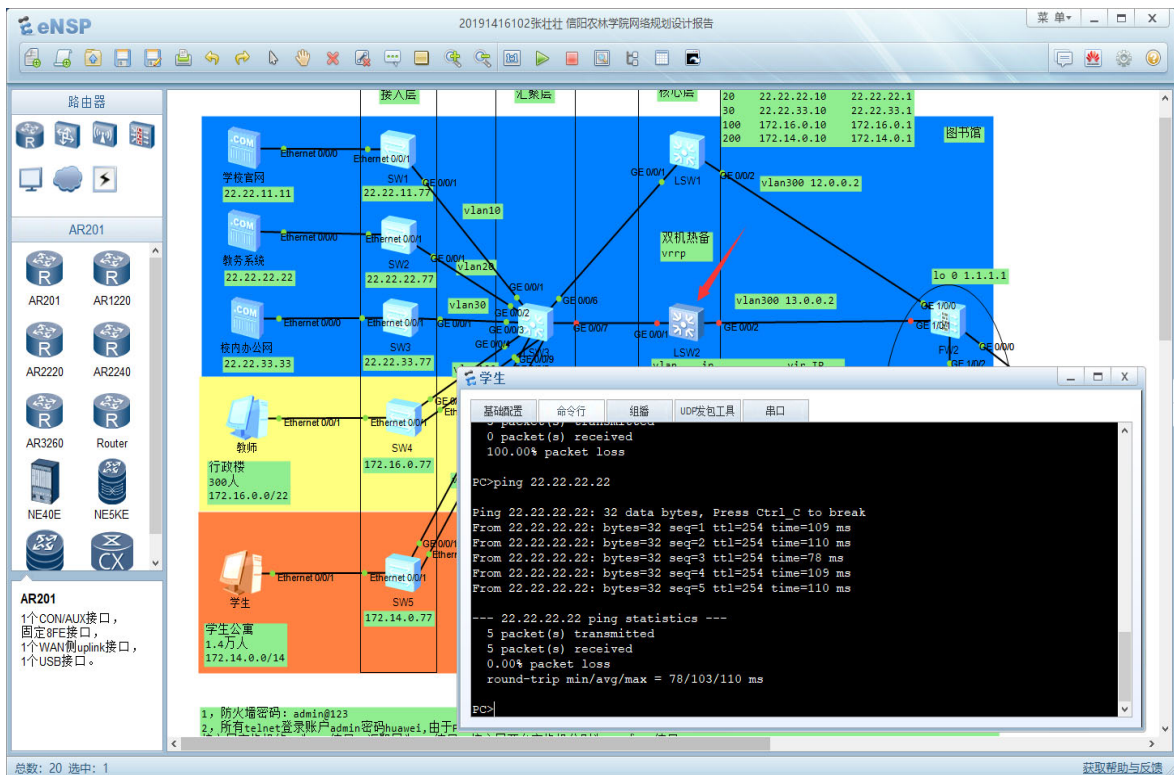


图5 关闭一台核心交换机内网可以正常访问

④双机热备测试，即使关闭一台核心交换机内网与外网依旧可以正常通信。

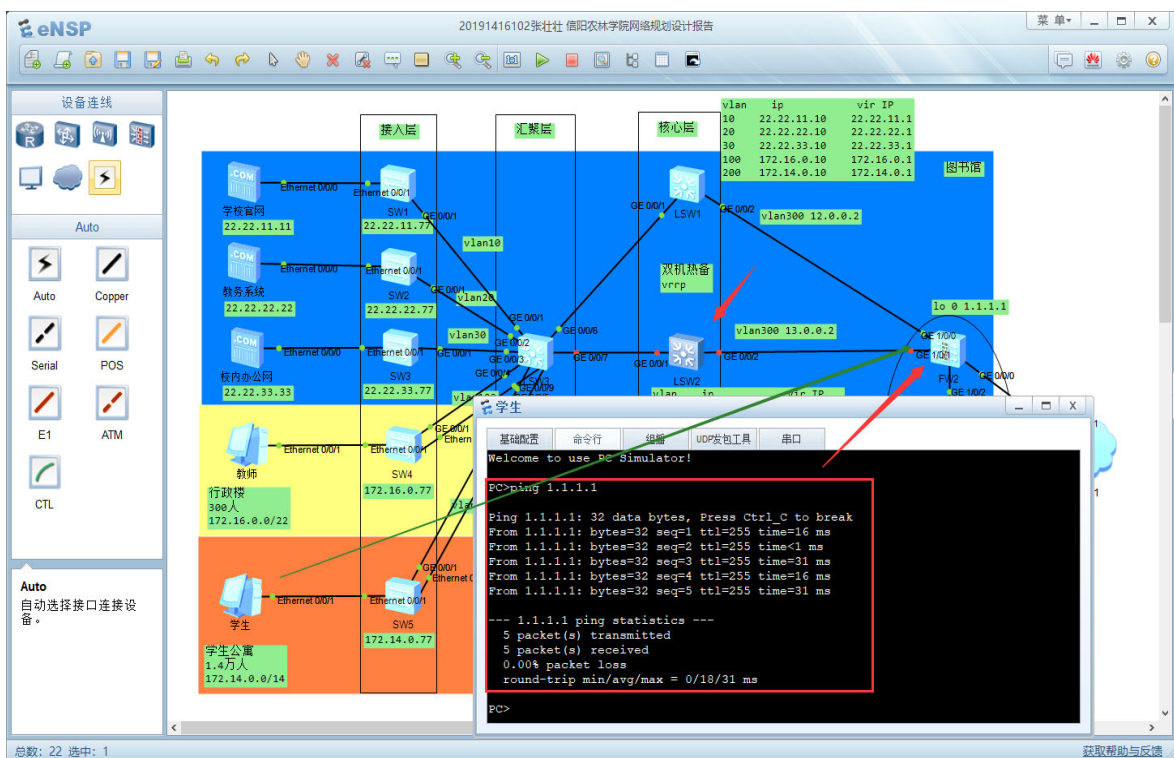


图6 关闭一台核心交换机内网可以与外网保持联通

⑤通过 IPsec 隧道，泮河校区可以成功连通羊山校区

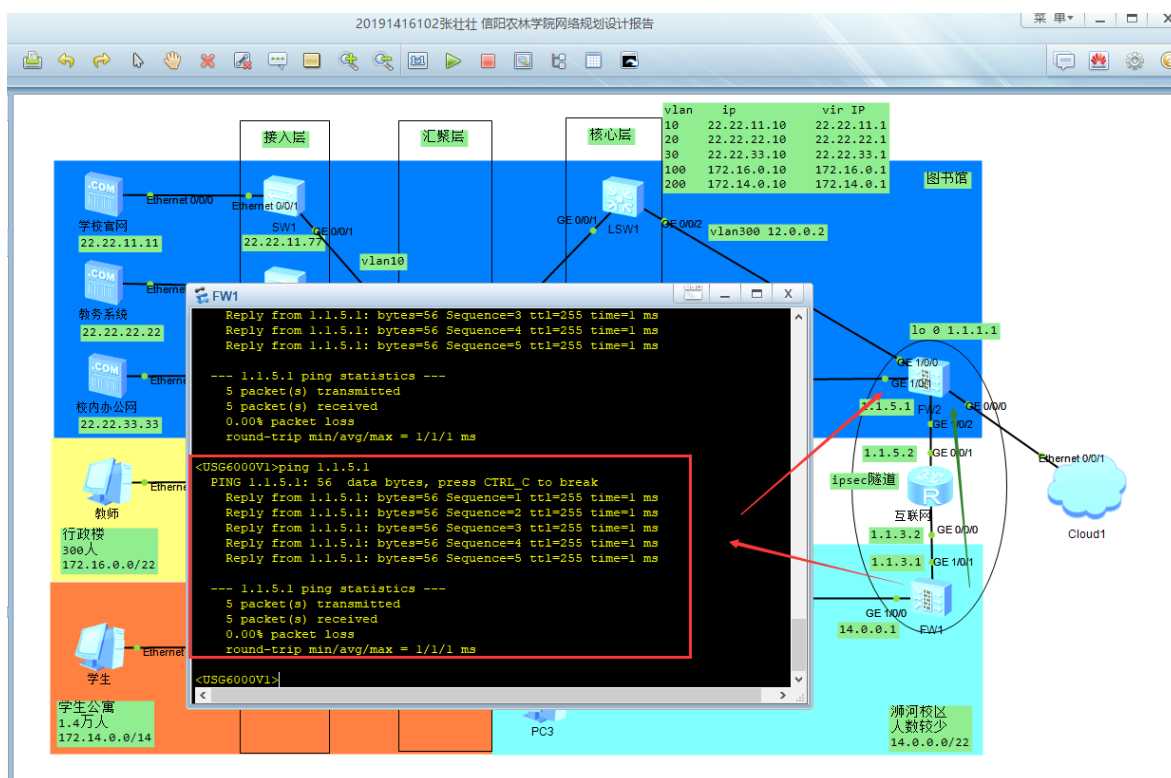


图 7 泮河校区出口 ping 通羊山校区

3.3.2 双机热备查看

①查看核心交换机 LSW1 vrrp 配置

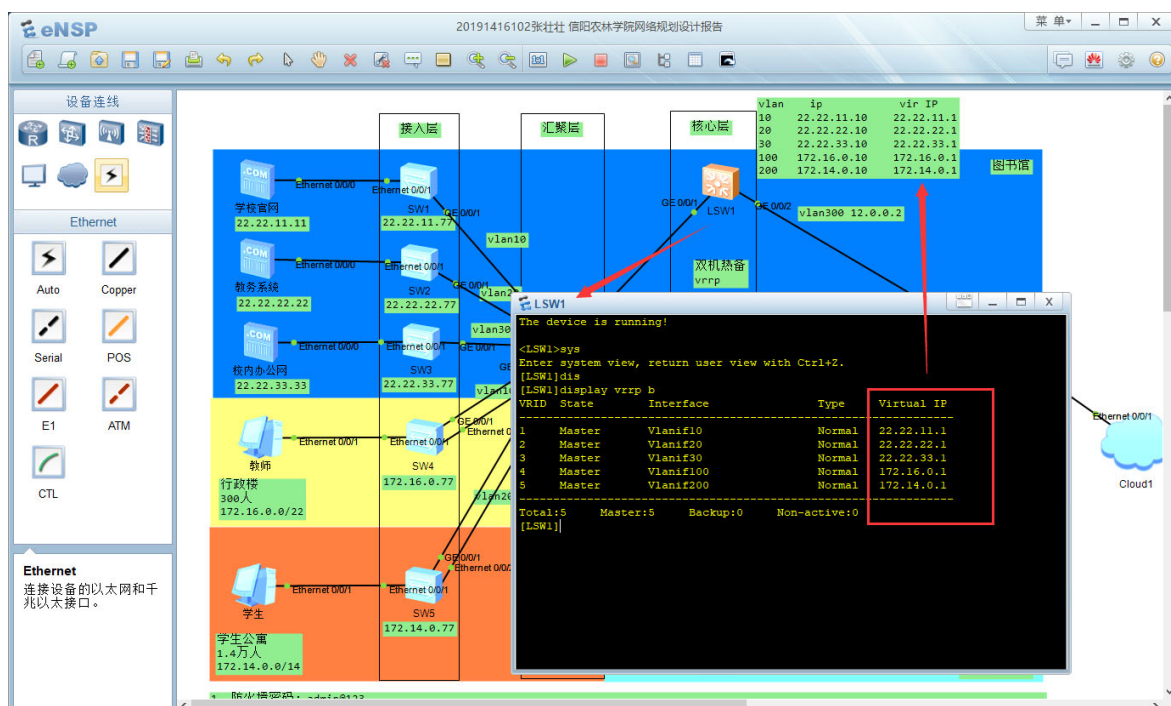


图 8 核心交换机 vrrp 配置

②查看核心交换机 LSW2 vrrp 配置

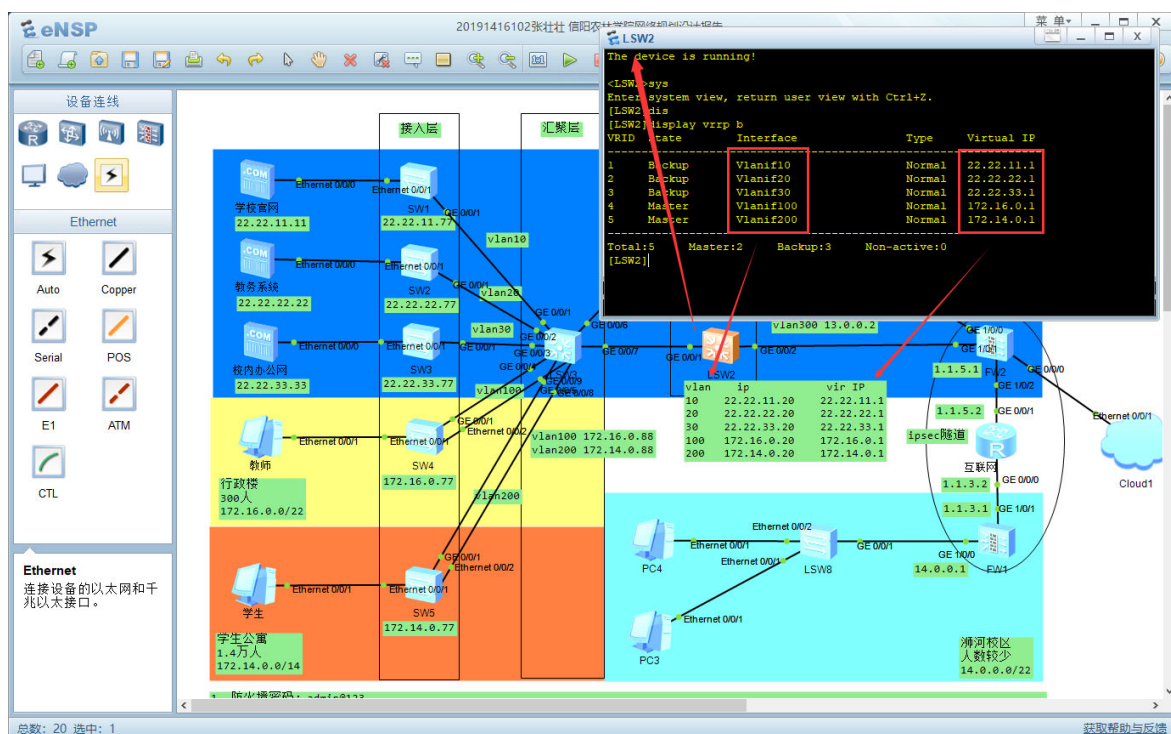


图 9 核心交换机 vrrp 配置

3.3.3 telnet 登录测试

①接入层交换机 SW5 与汇聚层交换机 LSW3 进行 telnet 连接测试, 已配置好所有交换机的 telnet 账户为 admin, 密码为 huawei

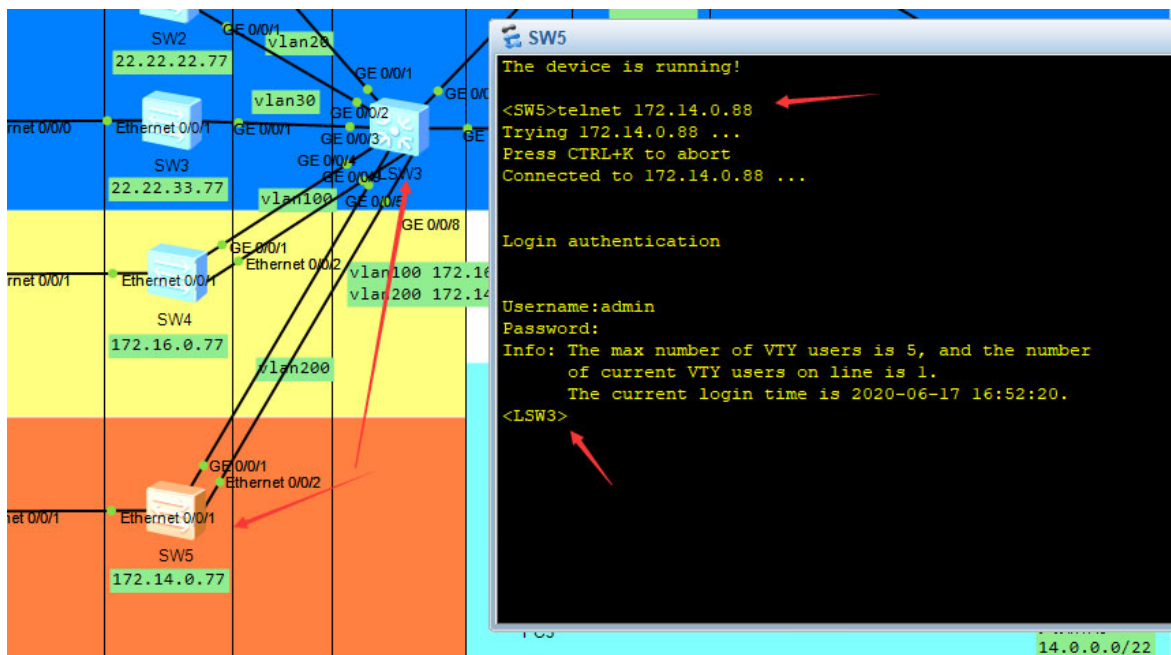


图 10 SW5 成功 telnet 到 LSW3

②汇聚层交换机 LSW3 与接入层交换机 SW4 进行 telnet 连接测试

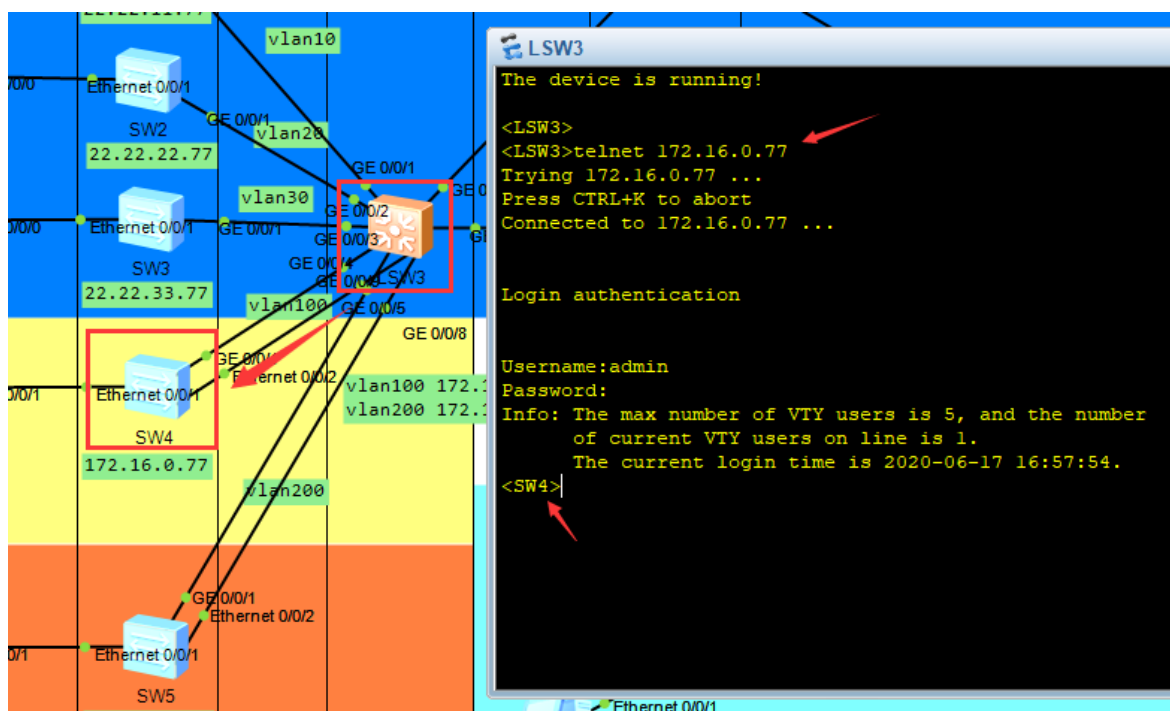


图 11 LSW3 成功 telnet 到 SW4

③接入层交换机 SW5 与核心层交换机 LSW1 进行 telnet 连接测试

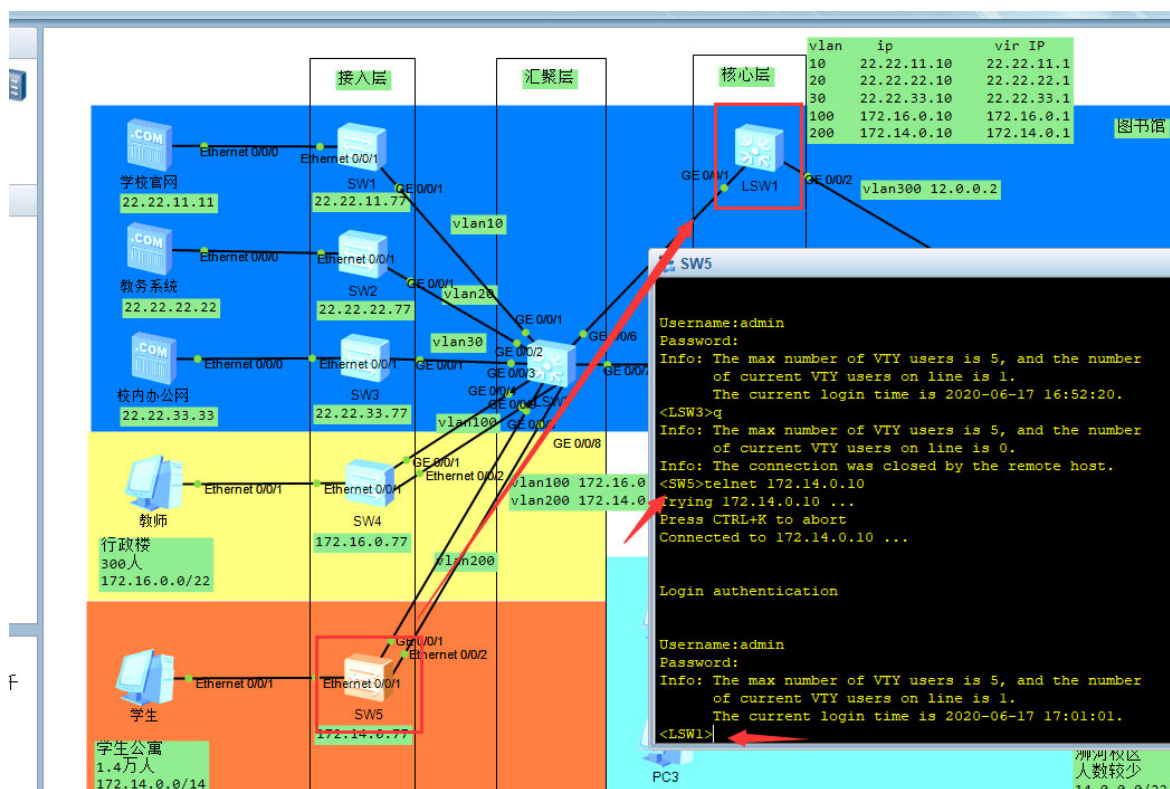


图 12 SW5 成功 telnet 到 LSW1

④核心层交换机 LSW2 与汇聚层交换机 LSW3 进行 telnet 连接测试

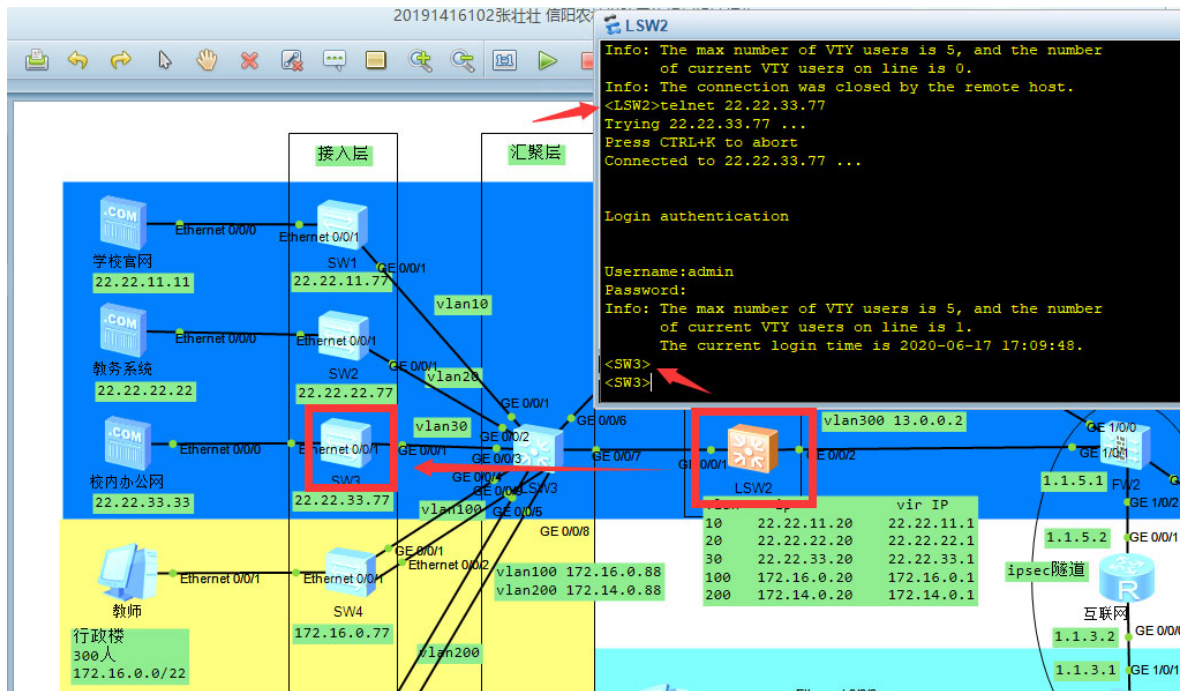


图 13 LSW2 成功 telnet 到 LSW3

3.4 结果分析

成功实现行政楼区域，学生宿舍楼区域，图书馆区域以及浉河区校区的上网人数需求 IP 网段的合理，满足各区域上网需求。规划三层网络架构，接入层、汇聚层、核心层，出口使用华为防火墙，并划分好了防火墙安全区域。且行政楼、学生宿舍至图书馆机房带宽可以达到 2000M。

羊山校区内所有交换机设备均可在局域网内任意一台设备通过 Telnet 远程管理。行政楼及学生宿舍区域上网设备可自动获取 IP 地址。行政楼区域可对图书馆中心机房中 web 服务随意访问，学生宿舍区域不能访问校内办公网服务器。

核心交换机部署了 vrrp 双机热备，实现了网络的稳定性。配置好了出口 nat 地址转换，以及学校官网服务器外网访问端口映射。羊山校区和浉河校区通信安全，两校区通信采用 ipsec vpn 方式进行通信。

体 会

高校校园网建设是一个比较复杂的大型项目，要使其能满足实际应用的要求，需要项目设计人认真的规划，合理的设备选型，合理的网络拓扑结构设计，好的 IP 及路由规划，并能通过规范的测试验收等。本次针对信阳农林学院的网络规划设计，让我充分的运用到老师课堂上讲的东西以及更深入的只是扩展。

完成本次项目耗费了我大量的时间以及精力，其中遇到了很多不容易客服的困难，使我大限度的翻阅资料。其中 IPSEC 隧道技术以及防火墙的 NAT 转换，里边内容都不是很熟悉，庆幸在老师之前发的《HCNA-Security 实验指导手册》中查到了类似的实验，从而使我可以顺利完成网络规划的设计。本项目中从出版的网络规划到最终的拓扑规划一共修改了三次，其中老师和同学给我提供了极大的帮助，让我可以更好的疏通网络设计的思路。

通过完成对信阳农林学院的网络规划，使我的路由交换以及防火墙技术的基础都得到了更好的巩固，使我对网络设备之间的通讯以及网络的信息安全有了更高层次的理解，提高了我计算机网络系统的设计、管理和集成的知识与能力。初步了解到了大型网络系统规划、设计与管理方法，掌握了中小型网络系统规划、设计与管理的基本能力。得到了独立完成搭建防火墙基本管理环境、配置防火墙基本功能、配置防火墙常见应用和配置防火墙高级功能的能力。

致 谢

首先，感谢我的防火墙老师 XXX 老师。在他悉心的教导下，不厌其烦的指导下，我的论文才可以顺利地完成。他治学严谨、一丝不苟的治学态度深深地影响了我，老师的细心、耐心，让我感受到了无比的温暖。他既给了我专业技术知识的指导，又在人格魅力上深深地影响了我，对我在以后的工作上给予了很大精神激励和鼓舞。这既是我学业收获的源泉，也是我人生路程上的巨大精神财富。

同时非常感谢我的室友 XX，他在业务上的精湛技术给予了我的巨大的指导，他拥有结合实践的运用能力，激励我将论文的实用价值和社会价值体现出来。我将保持和他的密切联系，继续学习更多更丰富的专业知识。

其次，我要感谢我的家人。这几年来他们不断在生活上支持上，让我可以全心全意认真工作和学习。在几年的在职学习过程中，他们无私的付出很多，保障了我的学习时间和精力，我才能够完成本职工作的同时，没有任何后顾之忧地投入到学习中，包括课程的学习和论文的撰写。我非常感谢家人的鼓励和帮助。

最后，我要感谢我的同学以及广大网友。感谢的话已经不足以表达我的心情，我唯有将感激之情化作无穷的动力，在今后的工作中奋发图强、兢兢业业，贡献自己大的力量。我唯有将学识运用到工作中，不断取得新的成绩，才能够无愧于自己的学习。

参 考 文 献

- [1] 王刚耀著. 网络运维亲历记[M]. 北京: 清华大学出版社, 2016.07. 第 81 页
- [2] 张岚, 王俊良, 贾颖. 浅谈 VRRP 协议在企业组网中的应用[J]. 科技创新导报, 2010, (11):249, 251.
- [3] 季庆光, 冯登国. 对几类重要网络安全协议形式模型的分析[J]. 计算机学报, 2005, 28(7):1071-1083.
- [4] 高能主编; 江伟玉, 刘丽敏副主编. 信息安全技术[M]. 北京: 中国人民公安大学出版社, 2018.04.
- [5] 秦智著. 网络系统集成[M]. 西安: 西安电子科技大学出版社, 2017.10.
- [6] 李学锋, 郑毅主编. 网络工程设计与项目实训: 东南大学出版社, 2016.06: 第 140 页
- [7] 李彪, 陈勋主编. 局域网组网技术[M]. 哈尔滨: 哈尔滨工程大学出版社, 2010.05. 第 77 页
- [8] 王灵霞, 刘永纯编. 网络管理与运维实战宝典: 中国铁道出版社, 2016.07: 第 220 页

