目录

[一、需求分析 1](#_Toc32497525)

[1.1 用户的应用需求 1](#_Toc32497526)

[1.2 通信需求 1](#_Toc32497527)

[1.3信息点和用户需求 1](#_Toc32497528)

[1.4性能需求 2](#_Toc32497529)

[1.5安全与管理需求 2](#_Toc32497530)

[二、网络系统的方案设计 3](#_Toc32497531)

[2.1 网络系统拓扑结构（平面初步拓扑方案） 3](#_Toc32497532)

[2.2 层次拓扑结构图 （接入层、核心层、汇聚层） 4](#_Toc32497533)

[2.3 详细的拓扑结构图 4](#_Toc32497534)

[2.4 子网设计方案 5](#_Toc32497535)

[三、设备选型 6](#_Toc32497536)

[四、方案预算 6](#_Toc32497537)

[五、技术实现方案 7](#_Toc32497538)

[5.1 VLAN内部通信 7](#_Toc32497539)

[5.2 VLAN间通信 9](#_Toc32497540)

[5.3 DHCP自动划分IP地址 11](#_Toc32497541)

[5.4 网络服务配置 16](#_Toc32497542)

[5.5 安全功能配置 24](#_Toc32497543)

[5.6 VPN远程接入访问配置 26](#_Toc32497544)

[六、实验结果分析 34](#_Toc32497545)

[6.1 VLAN内部通信 34](#_Toc32497546)

[6.2 VLAN间通信 40](#_Toc32497547)

[6.3 DHCP自动划分IP地址 44](#_Toc32497548)

[6.4 网络服务配置 46](#_Toc32497549)

[6.5 安全功能配置 49](#_Toc32497550)

[6.6 VPN远程接入访问配置 52](#_Toc32497551)

# 一、需求分析

## 1.1 用户的应用需求

随着高校招生规模的扩大和新校区的扩建，校园网络面临着扩建和改造，网络系统需要重新规划和设计，以满足新的管理体制以及教学、科研手段变化的需要。具体需求与分析如下：

需求1：保证部分网络中的信息安全，拒绝其他部门计算机访问。

分析1：使用VLAN技术划分子网，实现各部门安全隔离。

需求2: 部门之间能有选择实施通信，保证部门之间地网络的安全连通。

分析2: 各个VLAN间需要通过核心交换机进行VLAN间路由，保证各个网段间能够互相访问。

需求3: 实现不同校区网络之间的互连互通。

分析3:使用路由技术以链接不同校区主机。

需求4:保证所有主机连接公共服务器。

分析4:使用通过路由技术实现所有主机可连接到公共服务器。

## 1.2 通信需求

满足管理者的需求，可以实现各种信息的传递与交流，方便管理者及时处理。满足学生与老师的需求，方便查询教室信息，课程信息，成绩信息等。同时满足各个校区之间的通信，实现校园卡信息、学生信息、教师信息规范统一化。

## 1.3信息点和用户需求

**信息点：**

**表4-1 信息点分布**

|  |  |  |  |
| --- | --- | --- | --- |
| 校区 | 单位 | 信息点 | 备注 |
| 南 | 综合楼 | 100 | 每间教室1个 |
| 南 | 计算机楼 | 400 | 每台计算机1个 |
| 南 | 南苑食堂 | 50 | 每个机器1个 |
| 南 | 图书馆 | 50 | 每台计算机1个 |
| 南 | 公寓楼 | 600 | 每个寝室1个 |
| 南 | 行政楼 | 100 | 每个办公室2个 |
| 东 | 财务处 | 20 | 每个办公室1个 |
| 东 | 教学楼 | 100 | 每间教室1个 |
| 东 | 公寓楼 | 600 | 每个寝室1个 |
| 东 | 实验楼 | 50 | 每台计算机1个 |
| 东 | 图书馆 | 50 | 每台计算机1个 |
| 东 | 研究生部 | 50 | 每个教室1个 |
| 东 | 学生食堂 | 50 | 每个机器1个 |
| 西 | 教学楼 | 100 | 每间教室1个 |
| 西 | 图书馆 | 50 | 每台计算机1个 |
| 西 | 公寓楼 | 600 | 每个寝室1个 |
| 西 | 西苑食堂 | 50 | 每个机器1个 |
| 西 | 蚕业研究所 | 30 | 每台计算机1个 |
| 西 | 实验楼 | 50 | 每台计算机1个 |

**用户需求：**

管理员：通过此校园网络来实现扩招新生，管理校园卡信息，管理教室课程安排以及学生上课安排，实现跨校区管理等；

教师：可以通过次校园网络实现查询课程安排，进行空教室查询，考试安排申请，成绩登记等功能；

学生：可以通过次校园网络进行课程查询，上课教室查询，考试安排查询，成绩查询，查询公告等功能。

## 1.4性能需求

此校园网络所具有的功能如下：

教学管理，学生管理，档案管理，图书管理，财务管理，校园卡相关功能，网络多媒体学习信息传输，事物通知与查询等。

## 1.5安全与管理需求

在系统设计中，既考虑信息资源的充分共享，更要注意信息的保护和隔离，因此系统应分别针对不同的应用和不同的网络通信环境，采取不同的措施，包括系统安全机制、数据存取的权限控制等。设置基于端口的访问控制,防止对重要信息点的访问,控制信息流向，增强网络安全。由于校园网与外部网进行互联，特别是和Internet的互联。Internet是一个开放式网络系统，它的安全性是很差的。因此安全问题更加重要。应该采取一定的技术来控制网络的安全性，从内部和外部同时对网络资源的访问进行控制。

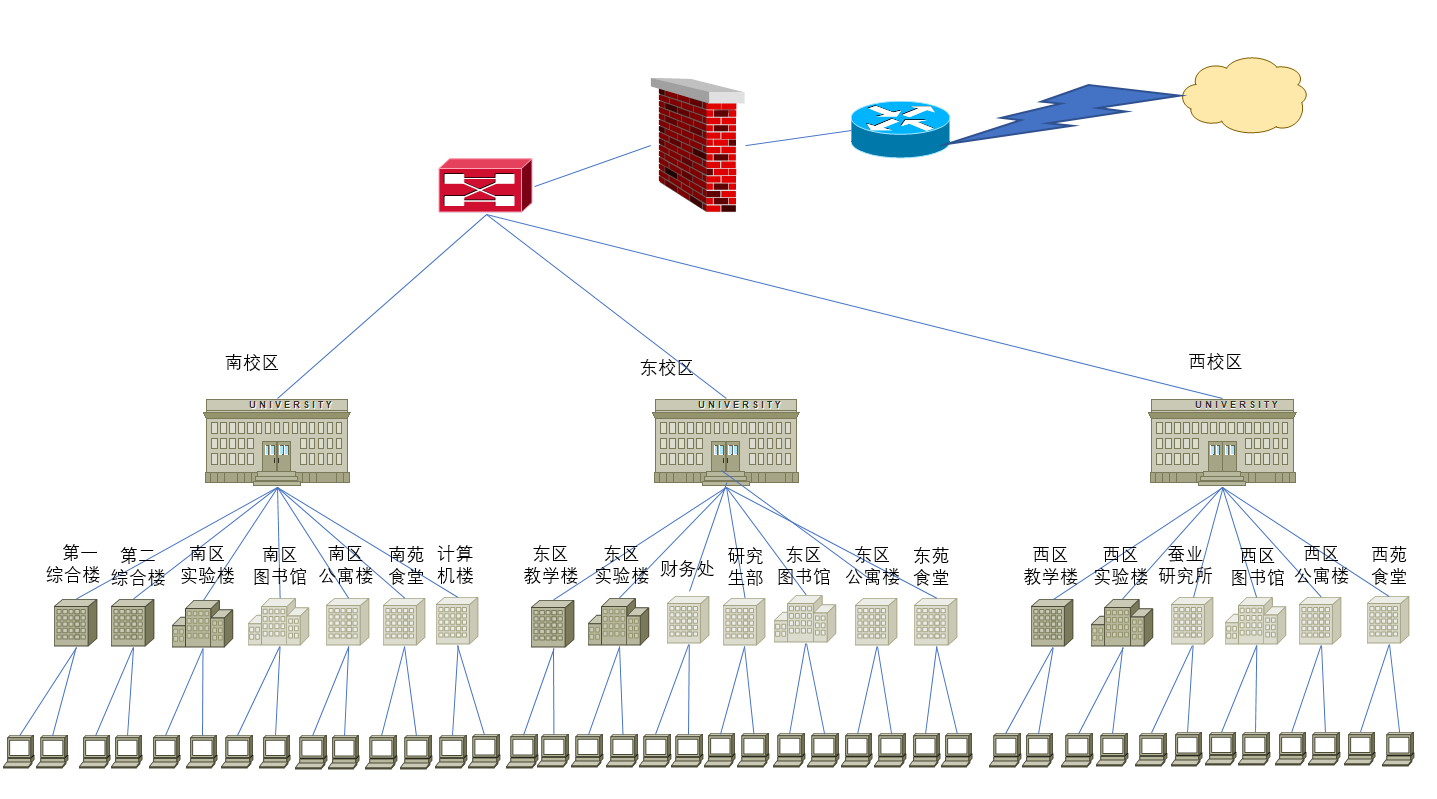
我们采取的网络安全技术有：用户身份验证，VLAN划分，防火墙等技术。

# 二、网络系统的方案设计

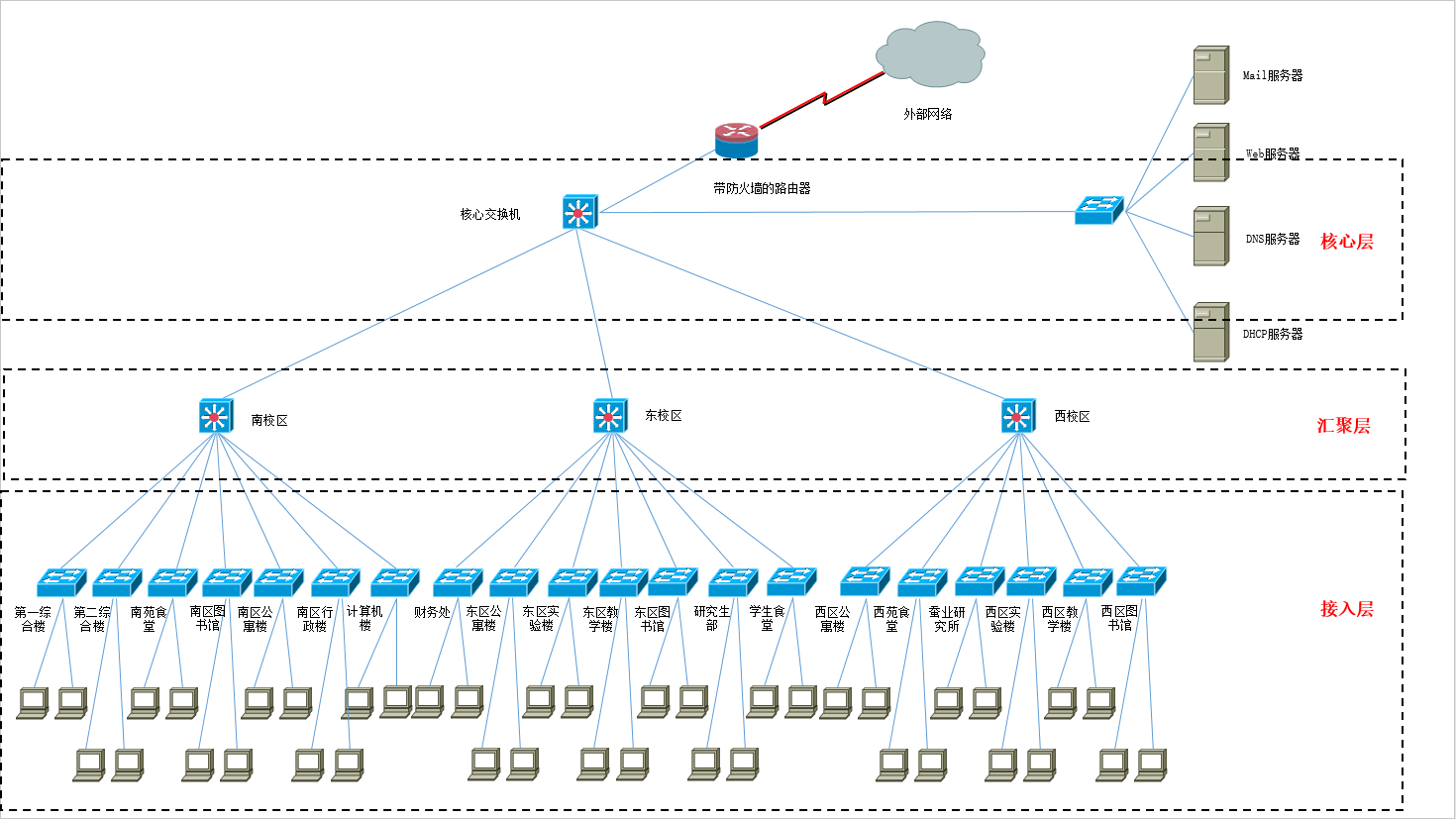
## 2.1 网络系统拓扑结构（平面初步拓扑方案）

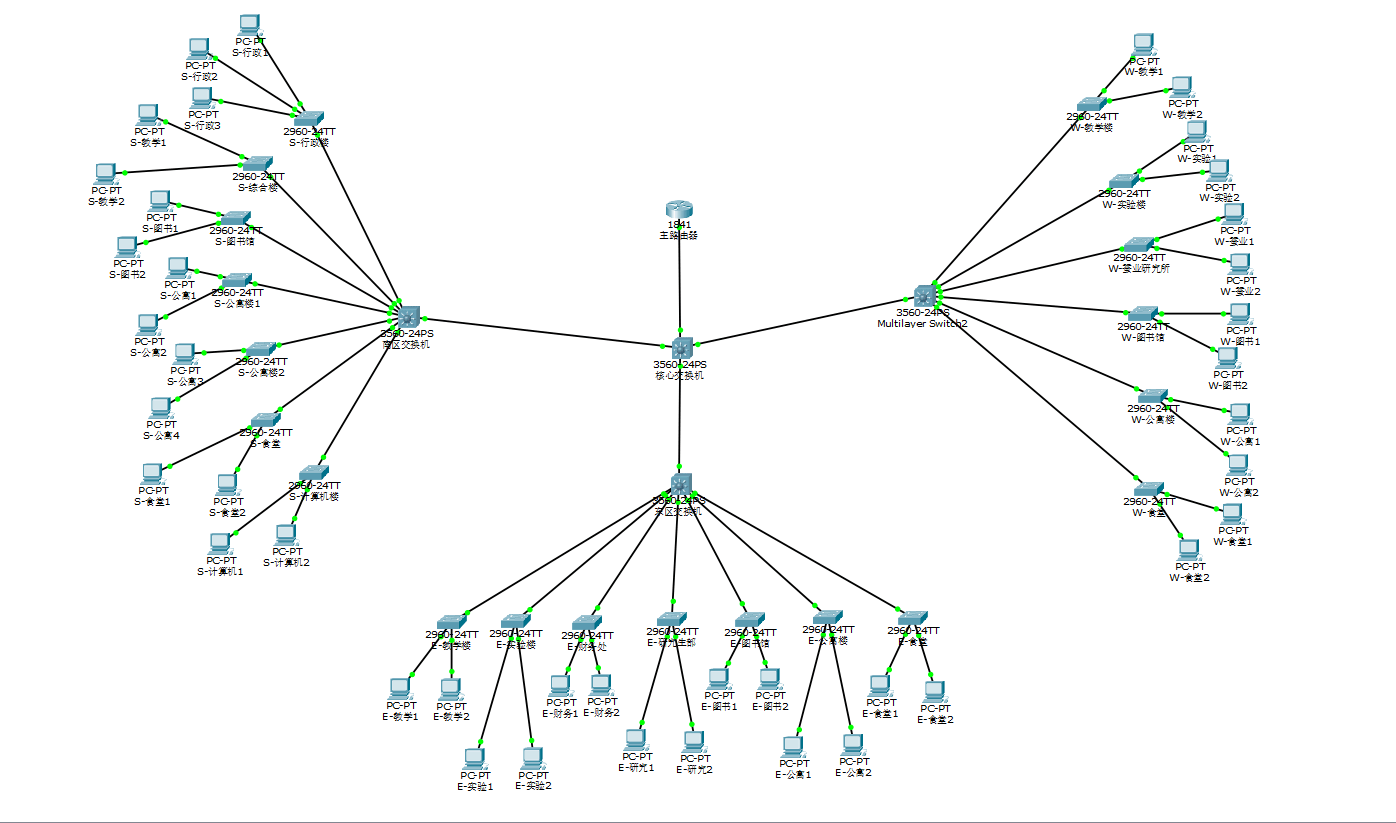
****

## 2.2 层次拓扑结构图 （接入层、核心层、汇聚层）

****

## 2.3 详细的拓扑结构图





## 2.4 子网设计方案

**2.4.1 IP地址规划原则**

唯一性：一个网络中不能有两个主机采用相同的IP地址。

连续性：连续地址在层次结构网络中易于进行路径叠合，大大缩减路由表，提高路由算法的效率。

扩展性：地址分配在每一层次上都要留有余量，在网络规模扩展时能保证地址叠合所需的连续性。

实意性：好的IP地址规划使每个地址具有实际含义，看到一个地址就可以大至判断出该地址所属的设备。

**2.4.2网络VLAN设计**

同一功能的单位在同一个VLAN中，便于相同功能单位之间的交流。同一校区可以进行跨VLAN的交流，便于校区内部的交流。

**2.4.3 VLAN及IP编址方案**

|  |  |  |  |
| --- | --- | --- | --- |
| 单位 | VLAN | IP地址配置范围 | 容量数目 |
| 学生宿舍 | V2 | 192.168.8.0/21 | 1800+25=1825 |
| 研究部门 | V3 | 192.168.16.0/22 | 530+25=555 |
| 教学楼 | V4 | 192.168.20.0/23 | 350+50=400 |
| 图书馆 | V5 | 192.168.22.0/24 | 150 |
| 食堂 | V6 | 192.168.23.0/24 | 150 |
| 财务处 | V7 | 192.168.24.0/24 | 20 |



# 三、设备选型

4台3560-24PS三层交换机

21台2960-24TT智能交换机

5台Server-PT

1台2811路由器

同校区选用双绞线

跨校区选用光纤

# 四、方案预算

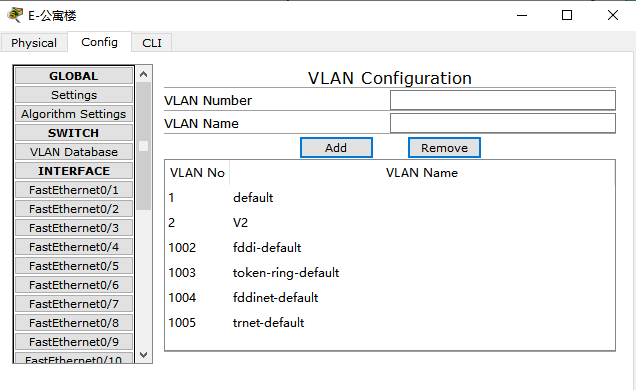
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 数量 | 单价 | 合计 | 备注 |
| 3560-24PS | 4（台） | 7500（元）/台 | 30000元 | 三层交换机 |
| 2960-24TT | 21（台） | 1520（元）/台 | 31920元 | 智能交换机 |
| Linksys-WMP300N | 5（台） | 2000(元) /台 | 10000元 | 无线网卡 |
| 2811 | 1（台） | 3850(元)/台 | 3850元 | 路由器 |
| 双绞线 | 2320m | 125（元）/100m | 2900元 | 室外防水版、国标0.5。680m（南）、680m（西）、960m（东） |
| 光纤 | 9000m | 140(元)/500m | 2520元 | 室外单芯皮线光缆 |
| 合计：81190元 | | | | |

# 五、技术实现方案

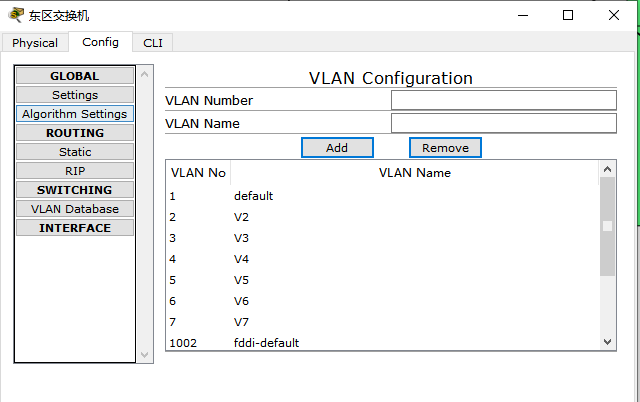
## 5.1 VLAN内部通信

以VLAN2内部的通信为例：

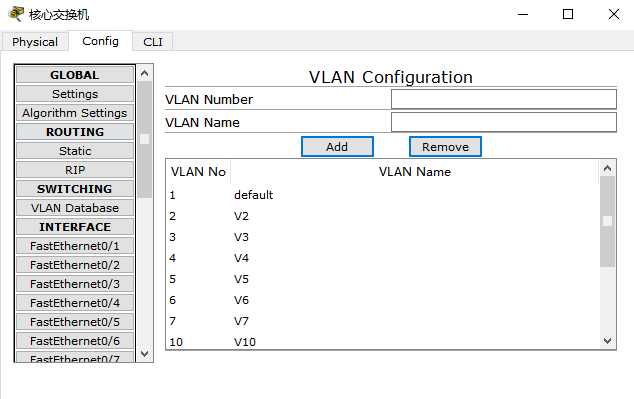
1. 在接入层交换机上添加vlan2并设置相应接口所属的vlan;



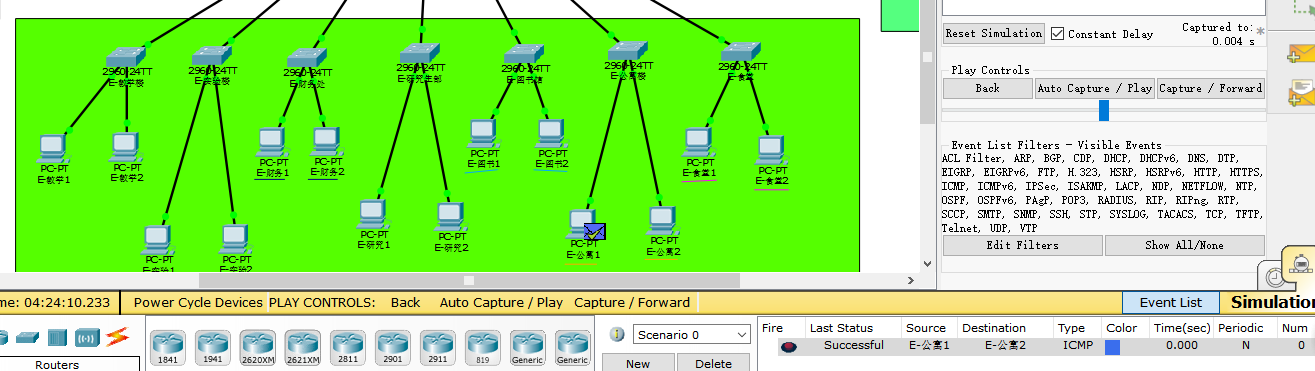
1. 在汇聚层三层交换机上添加vlan2并设置相应接口所属的vlan;



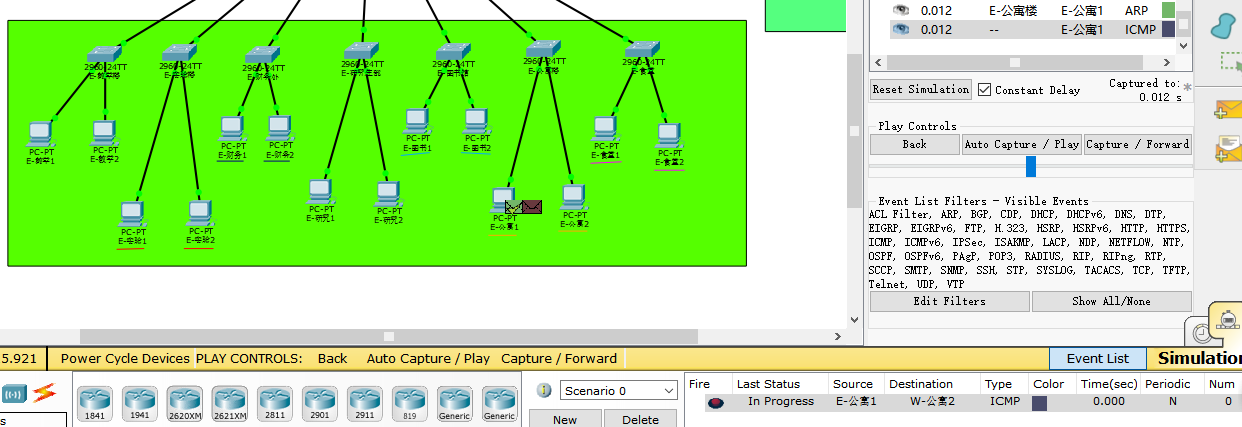
1. 在核心层三层交换机上添加vlan2并设置相应接口所属的vlan;



1. 同一校区的同一VLAN内部通信



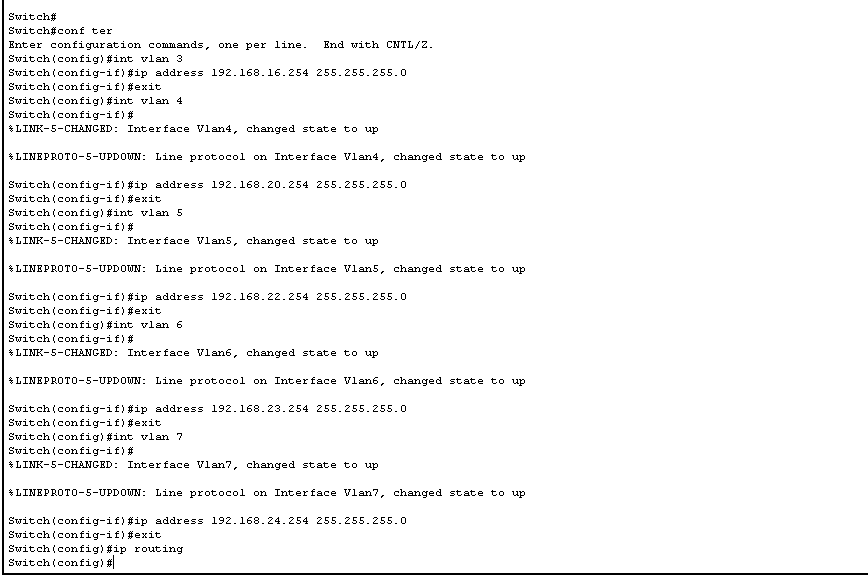
1. 不同校区的同一VLAN内部通信



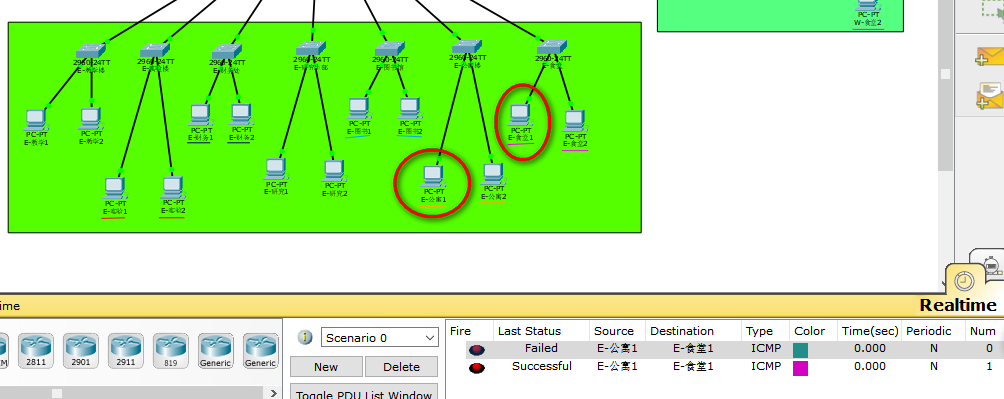
## 5.2 VLAN间通信

（1）配置好接入层、汇聚层、核心层交换机上所应包含的VLAN，以及各个端口所处的VLAN（普通接入口和共享口）

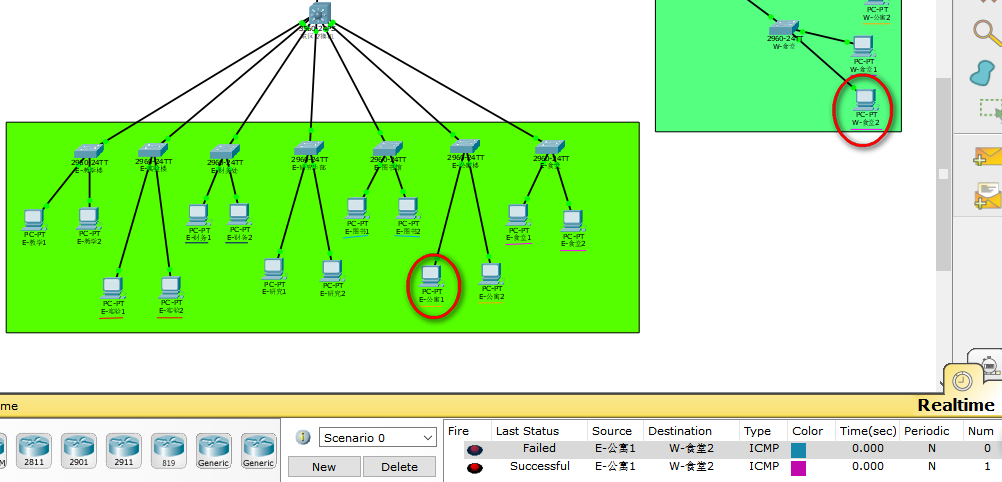
（2）在中心交换机上写入每个VLAN的默认网关及子网掩码；



（3）实现同一校区不同VLAN间通信

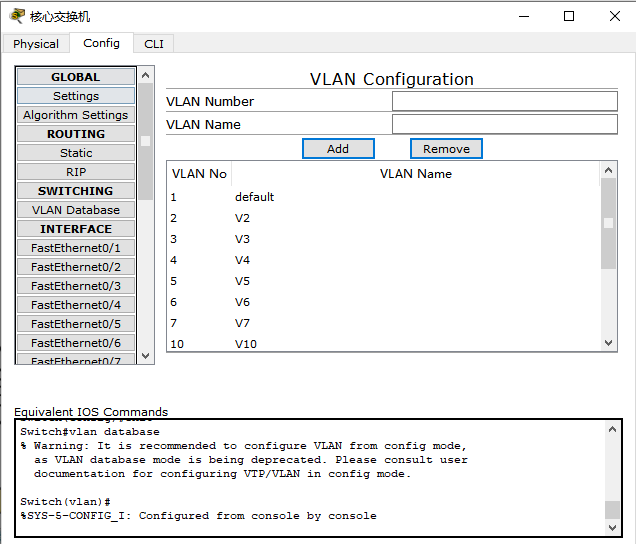


（4）实现不同校区不同VLAN间的通信



## 5.3 DHCP自动划分IP地址

5.4.1 在接入层的交换机上添加VLAN，并为各个端口划分其所属的VLAN



5.4.2 在核心层交换机输入如下代码：

Switch(config)#int vlan 2

Switch(config-if)#ip address 192.168.8.254 255.255.248.0

Switch(config-if)#exit

Switch(config)#int vlan 3

Switch(config-if)#ip address 192.168.16.254 255.255.252.0

Switch(config-if)#exit

Switch(config)#int vlan 4

Switch(config-if)#

%LINK-5-CHANGED: Interface Vlan4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up

Switch(config-if)#ip address 192.168.20.254 255.255.254.0

Switch(config-if)#exit

Switch(config)#int vlan 5

Switch(config-if)#

%LINK-5-CHANGED: Interface Vlan5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan5, changed state to up

Switch(config-if)#ip address 192.168.22.254 255.255.255.0

Switch(config-if)#exit

Switch(config)#int vlan 6

Switch(config-if)#

%LINK-5-CHANGED: Interface Vlan6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan6, changed state to up

Switch(config-if)#ip address 192.168.23.254 255.255.255.0

Switch(config-if)#exit

Switch(config)#int vlan 7

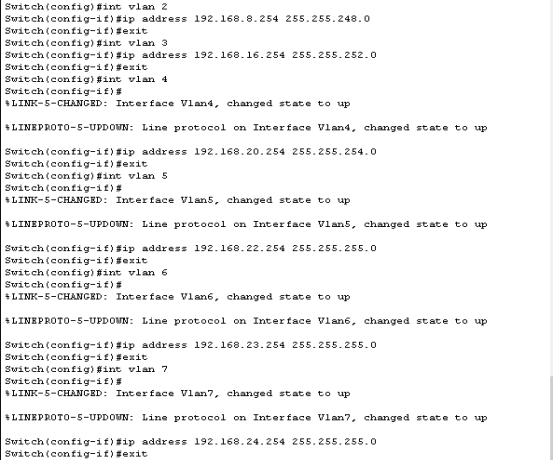
Switch(config-if)#

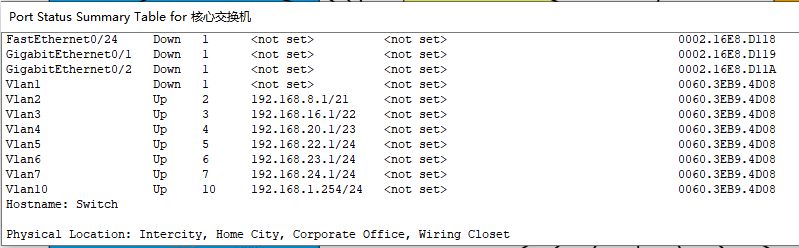
%LINK-5-CHANGED: Interface Vlan7, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan7, changed state to up

Switch(config-if)#ip address 192.168.24.254 255.255.255.0

Switch(config-if)#exit





* + 1. 在核心层代码输入如下代码实现DHCP自动分配的功能：

Switch(config)#ip dhcp pool vlan2

Switch(dhcp-config)#network 192.168.8.0 255.255.248.0

Switch(dhcp-config)#default-router 192.168.8.1

Switch(dhcp-config)#dns-server 192.168.1.3

Switch(dhcp-config)#exit

Switch(config)#ip dhcp pool vlan3

Switch(dhcp-config)#network 192.168.16.0 255.255.252.0

Switch(dhcp-config)#default-router 192.168.16.1

Switch(dhcp-config)#dns-server 192.168.1.3

Switch(dhcp-config)#exit

Switch(config)#ip dhcp pool vlan4

Switch(dhcp-config)#network 192.168.20.0 255.255.254.0

Switch(dhcp-config)#default-router 192.168.20.1

Switch(dhcp-config)#dns-server 192.168.1.3

Switch(dhcp-config)#exit

Switch(config)#ip dhcp pool vlan5

Switch(dhcp-config)#network 192.168.22.0 255.255.255.0

Switch(dhcp-config)#default-router 192.168.22.1

Switch(dhcp-config)#dns-server 192.168.1.3

Switch(dhcp-config)#exit

Switch(config)#ip dhcp pool vlan6

Switch(dhcp-config)#network 192.168.23.0 255.255.255.0

Switch(dhcp-config)#default-router 192.168.23.1

Switch(dhcp-config)#dns-server 192.168.1.3

Switch(dhcp-config)#exit

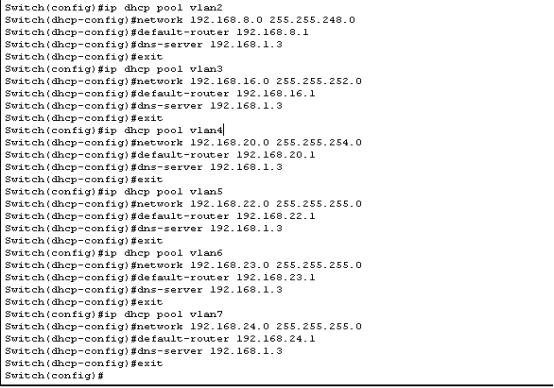
Switch(config)#ip dhcp pool vlan7

Switch(dhcp-config)#network 192.168.24.0 255.255.255.0

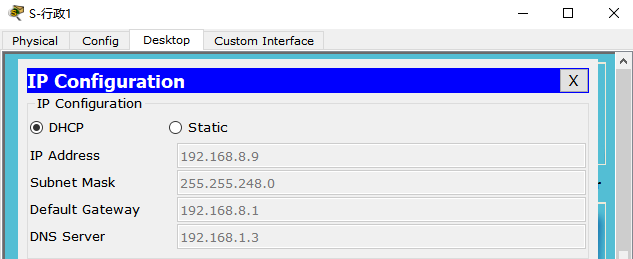
Switch(dhcp-config)#default-router 192.168.24.1

Switch(dhcp-config)#dns-server 192.168.1.3

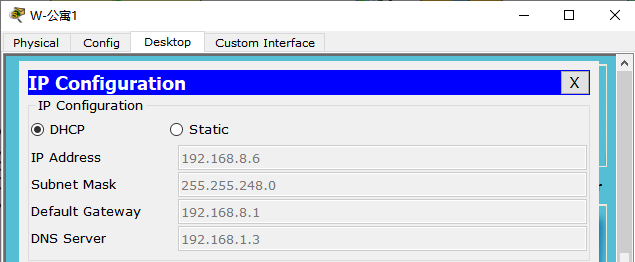
Switch(dhcp-config)#exit

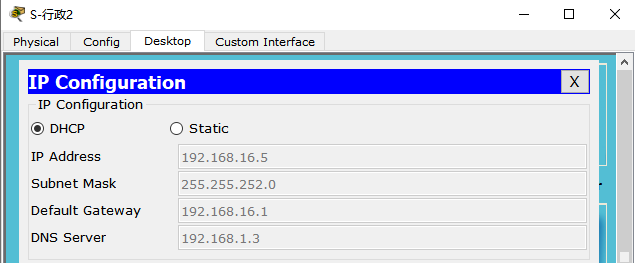


* + 1. 不同VLAN的主机通过DHCP自动获取IP地址



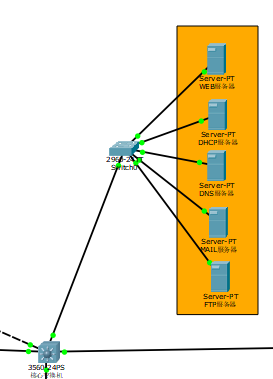






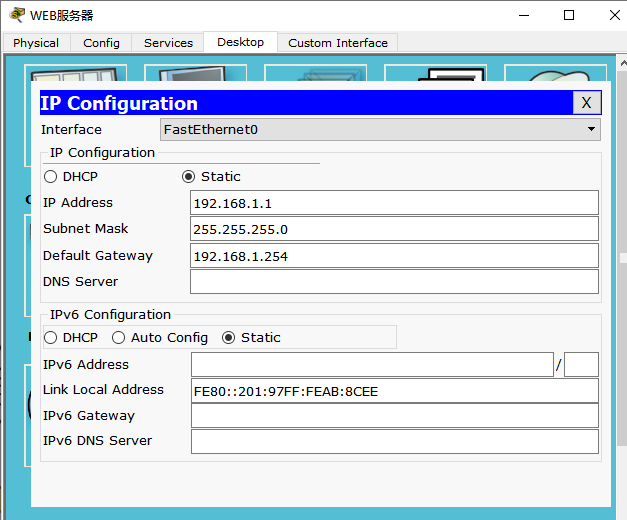
## 5.4 网络服务配置

首先将服务器划分到同一个VLAN中，并在三层核心交换机中写入该VLAN的默认网关以及子网掩码，从而让其他VLAN中的主机可以通过三层核心交换机实现访问服务器的功能。

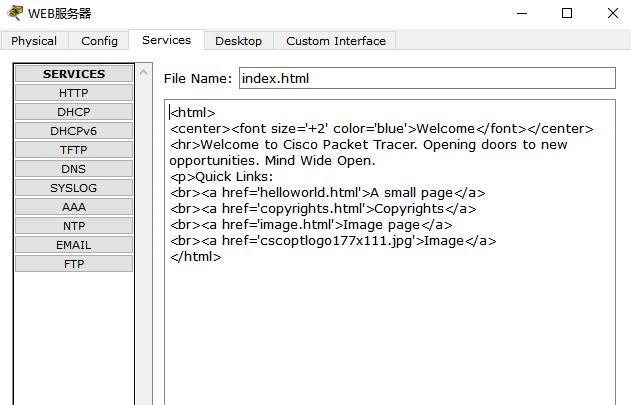


5.4.1 WEB服务器配置

（1）设置WEB服务器的IP地址、子网掩码及默认网关



（2）修改显示内容

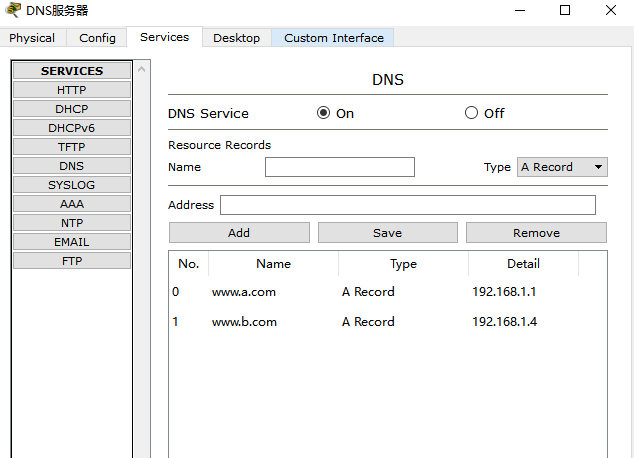


5.4.2 DNS服务器配置

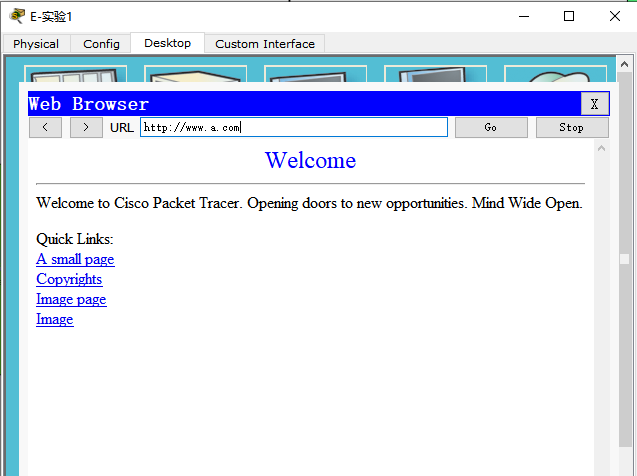
（1）设置DNS服务器的IP地址、子网掩码及默认网关



（2）增加域名解析

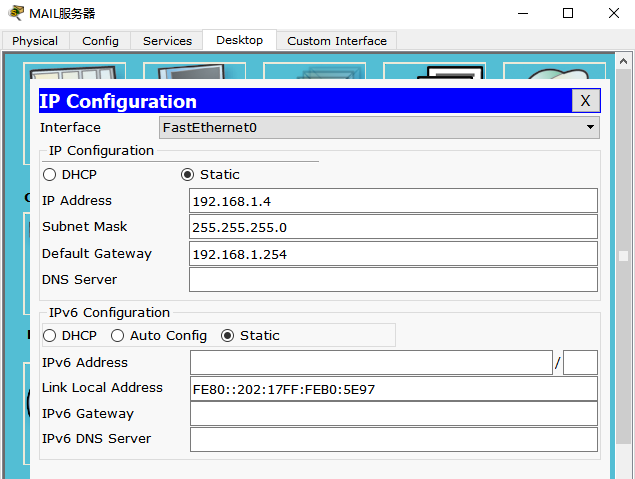


（3）通过域名就可以访问相应的服务器

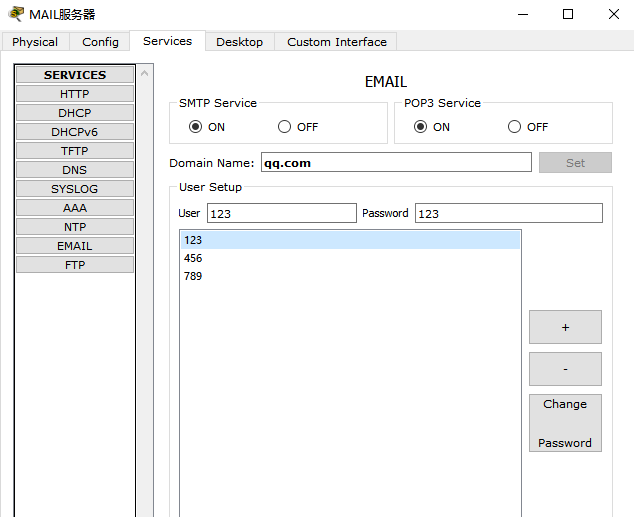


5.4.3 MAIL服务器

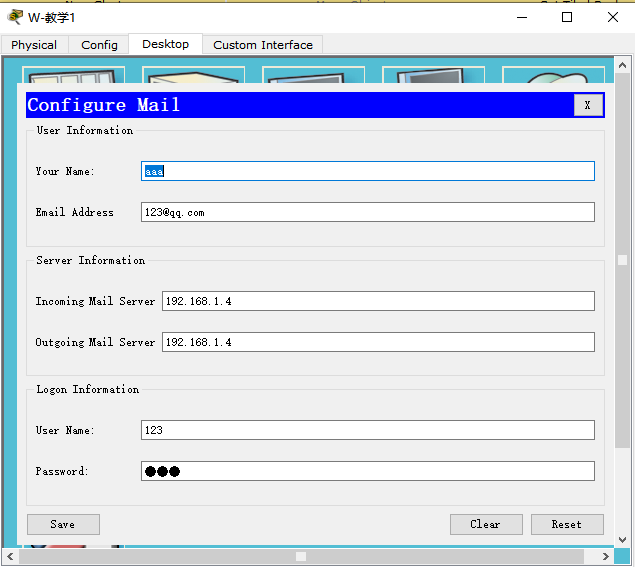
（1）设置MAIL服务器的IP地址、子网掩码及默认网关



（2）添加相应的域名、用户名及密码

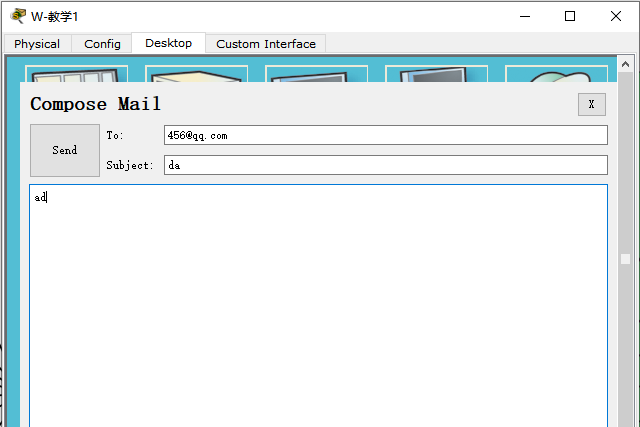


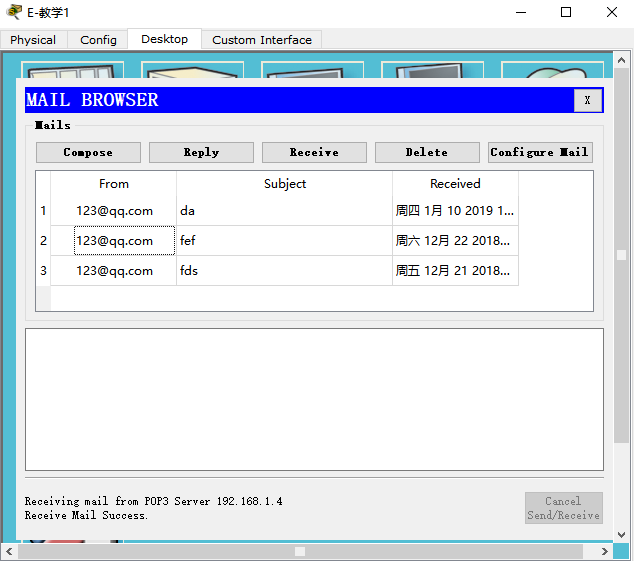
（3）在主机上进行相应的配置





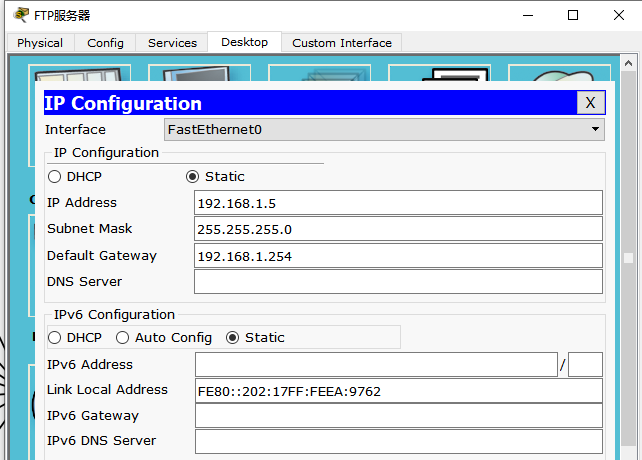
（4）尝试发送EMAIL，对应主机收到邮件



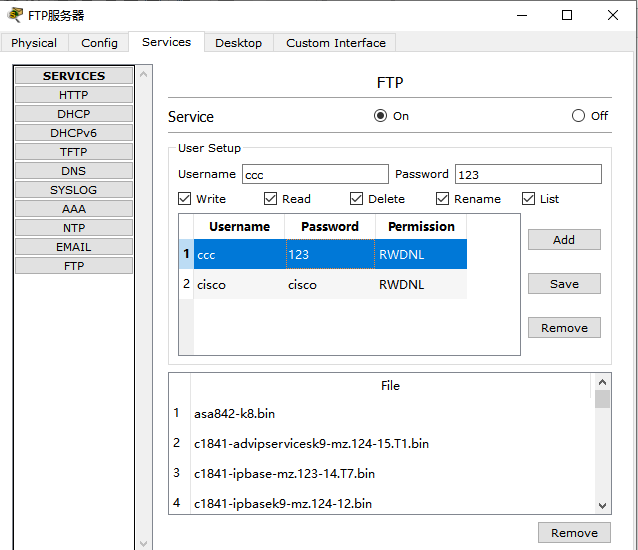


5.4.3 FTP服务器

（1）设置FTP服务器的IP地址、子网掩码及默认网关



(2)添加用户名、密码及相应权限



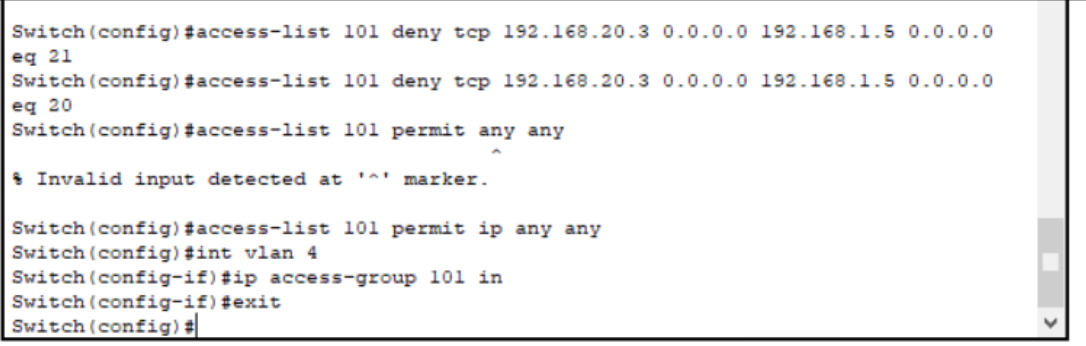
（3）在主机中使用命令访问FTP服务器

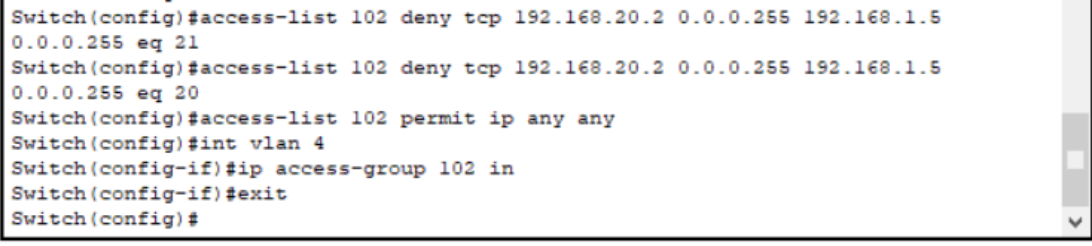




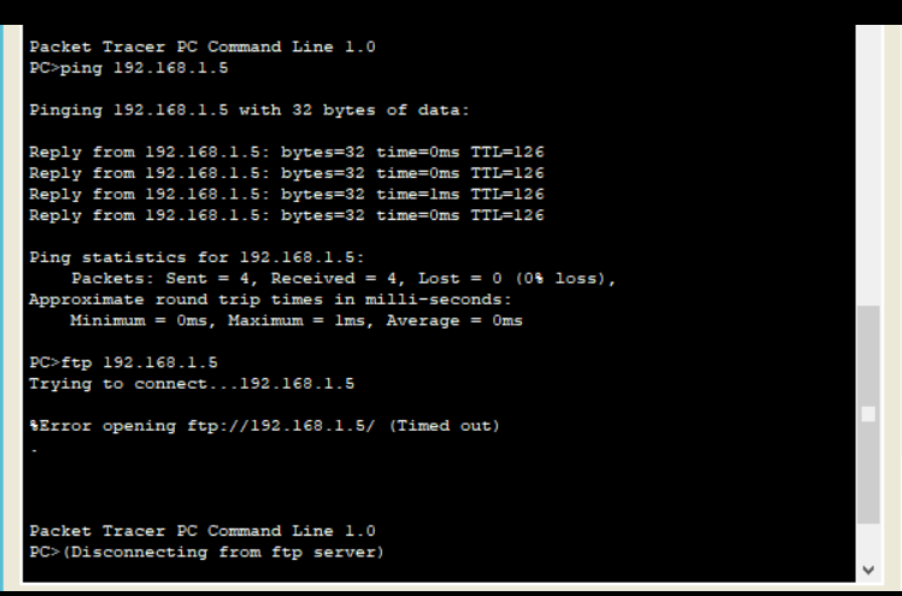
## 5.5 安全功能配置

5.5.1 在核心交换机上设置访问控制列表

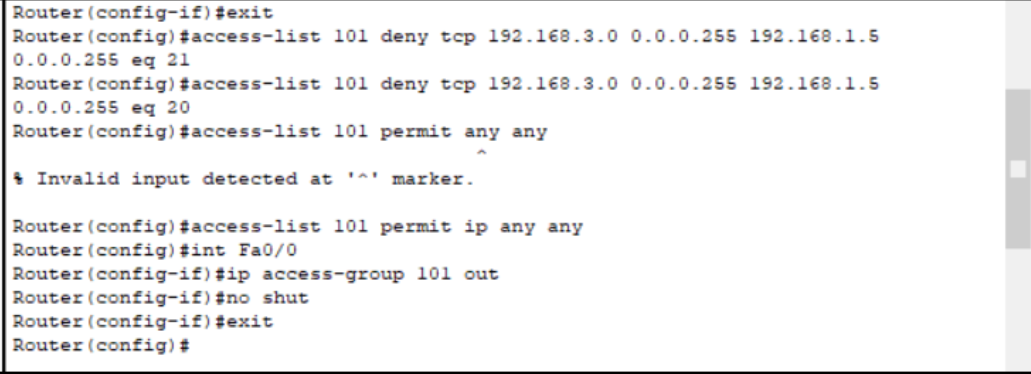




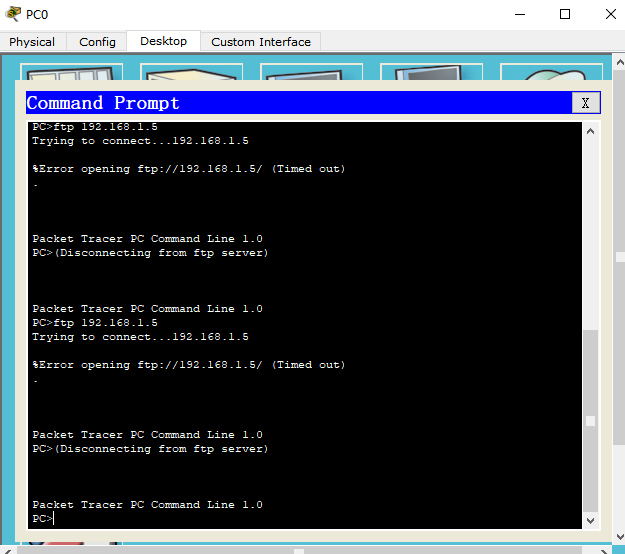
此时相应的主机无法访问FTP服务器；



5.5.2 在设置VPN的内部路由器上设置访问控制列表

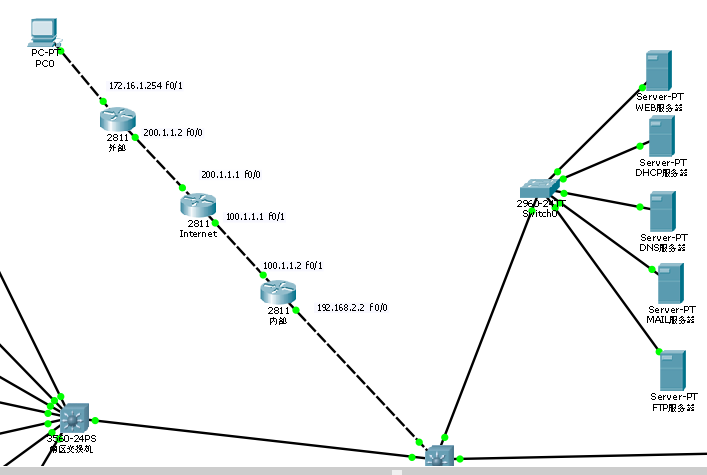


此时外部PC0无法访问FTP服务器；

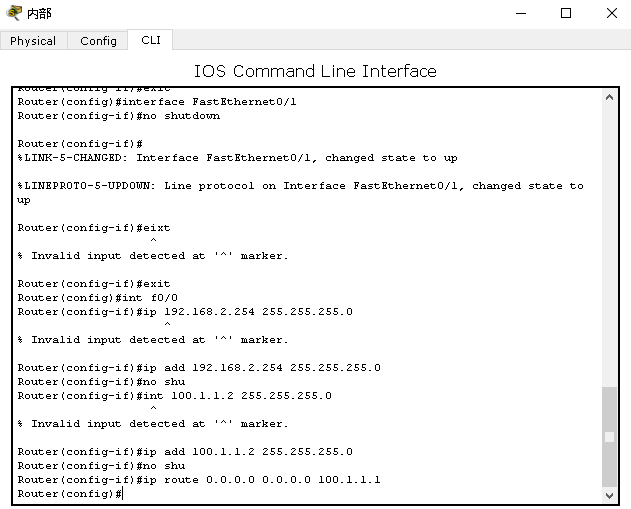


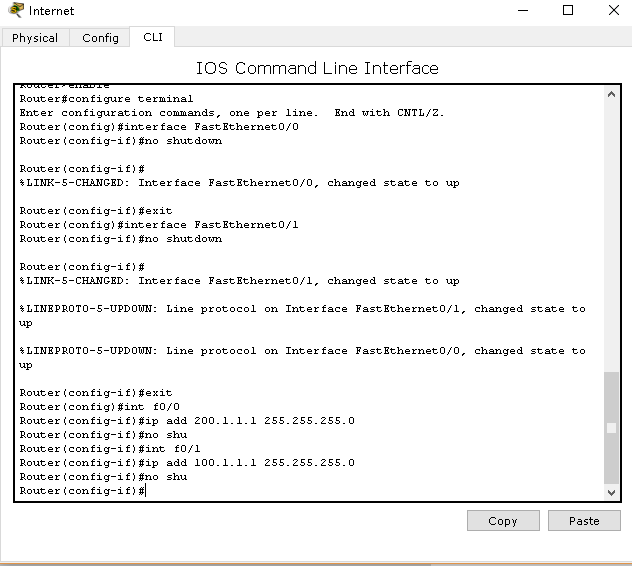
## 5.6 VPN远程接入访问配置

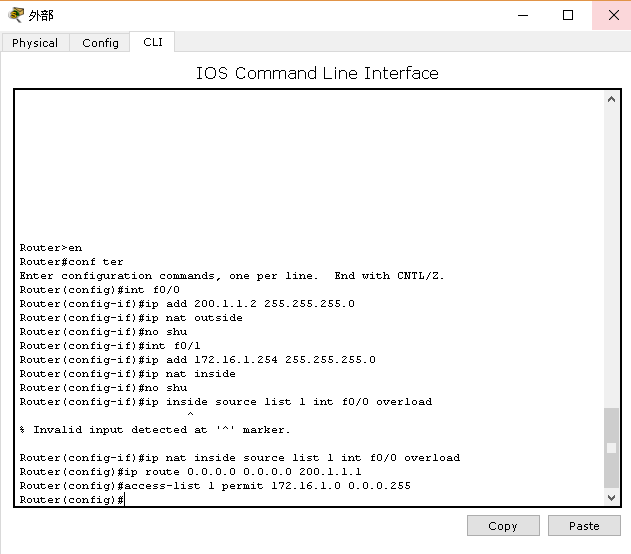
5.6.1搭建如下模型，并按注释内容设置路由器上各个端口的IP地址



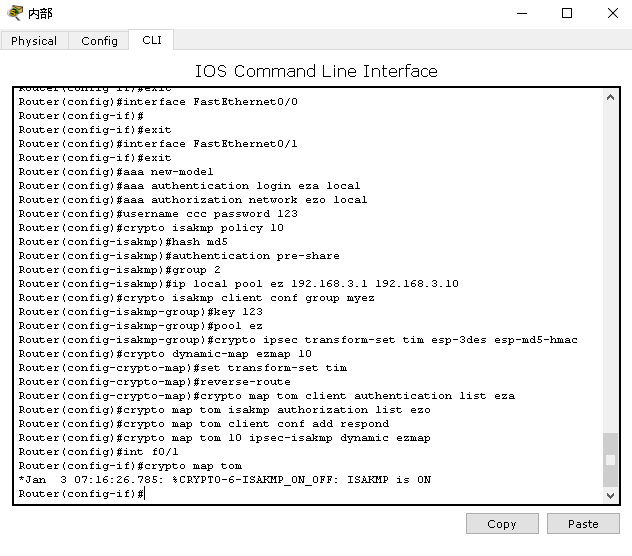
5.6.2在三个路由器分别输入代码配置静态路由和访问控制列表：



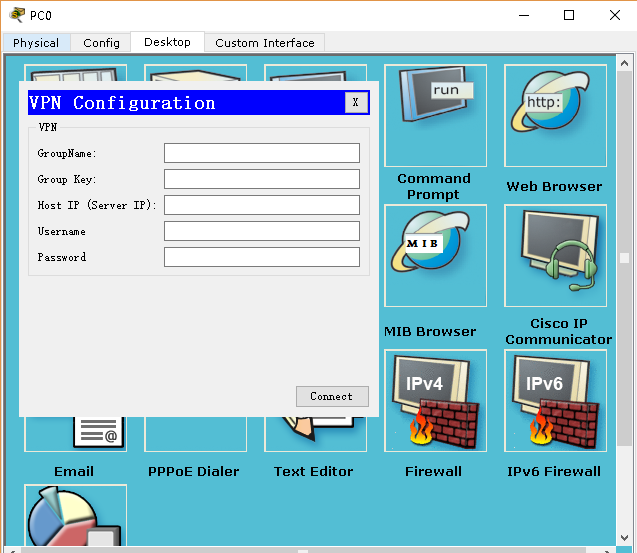


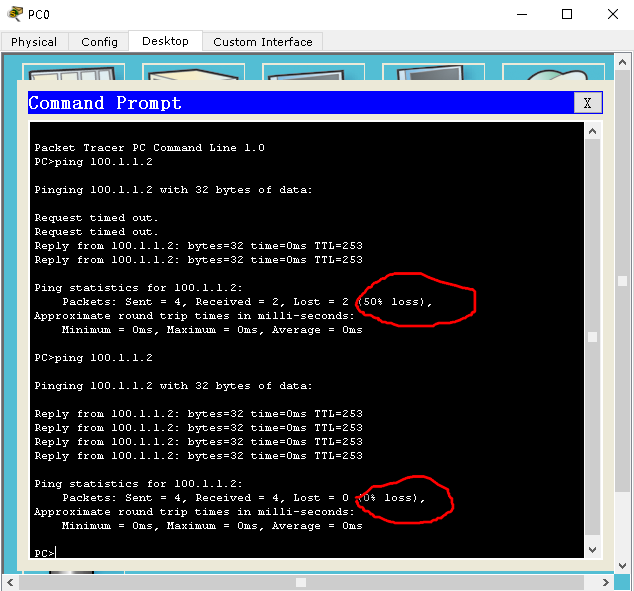


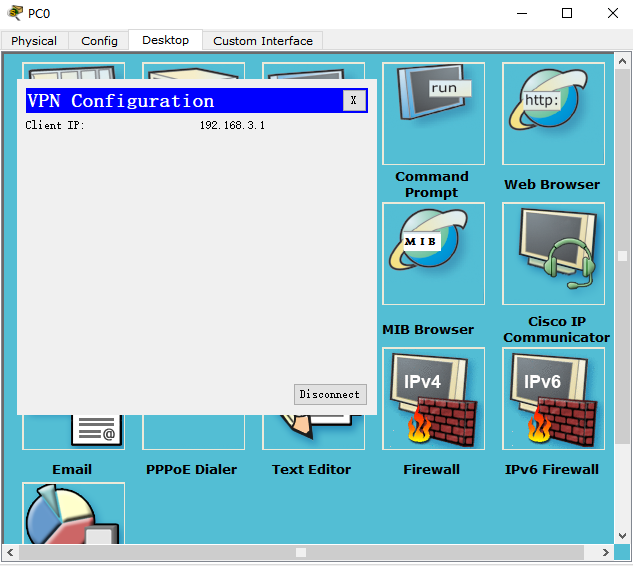
5.6.3在内部路由器上输入如下代码（实现VPN的关键步骤）：



完成这一步后，外部PC可以ping通100.1.1.2，此时在外部PC的VPN中输入组名（myez），组密码(123)，代理IP（100.1.1.2），用户名(ccc)，用户名密码(123)来连接VPN（一定要先ping一下100.1.1.2，如果出现包丢失情况多ping几次，直到数据包零丢失再去连接VPN，否则会出现连接超时无法连上的情况）；



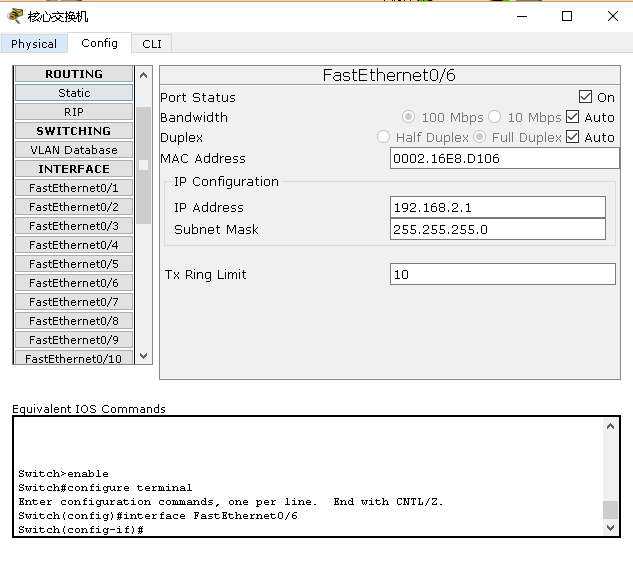




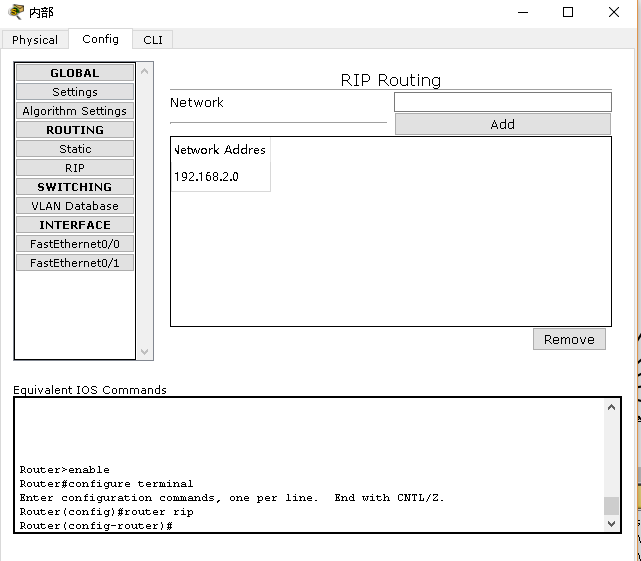
上图表示VPN连接成功，并且外部PC分配到了一个内部IP地址（192.168.3.1-192.168.3.2之间的一个IP）；

连接成功后可以传信到内部路由器上；

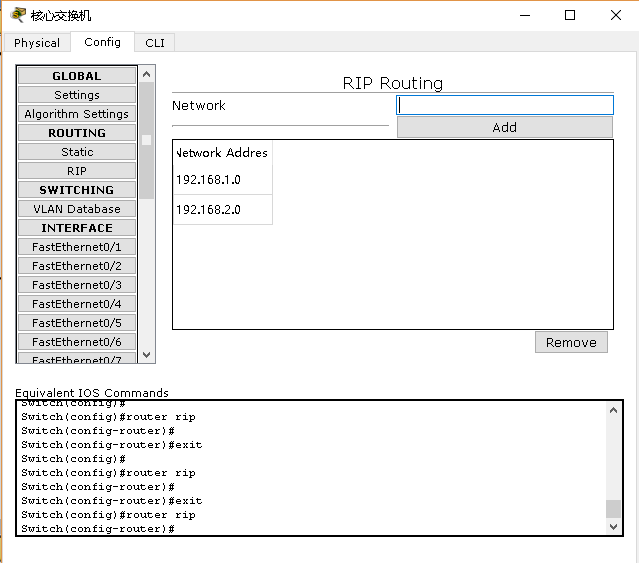
将核心交换机与内部路由器相连接的端口改为路由口（no switchport）,配置该端口上的IP为192.168.2.1,；



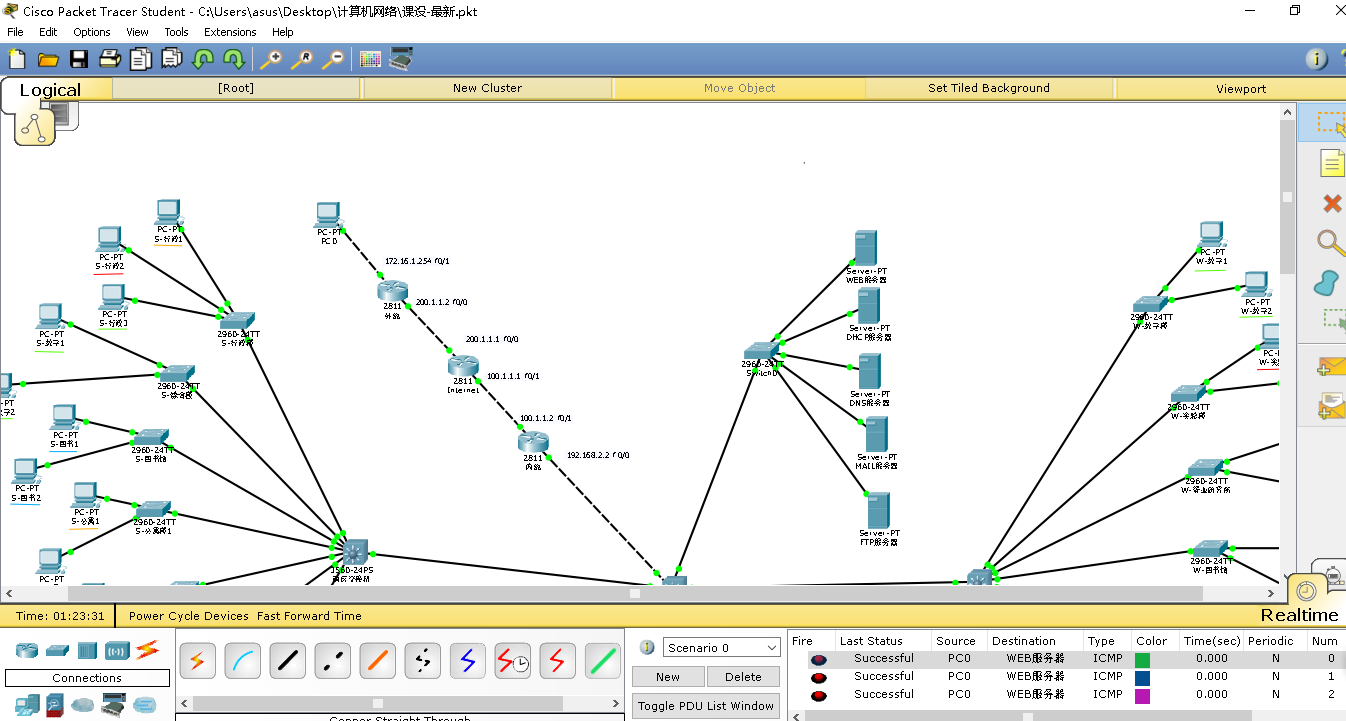
在内部路由器上添加动态路由项192.168.2.0；（完成后可传信到核心交换机上）；

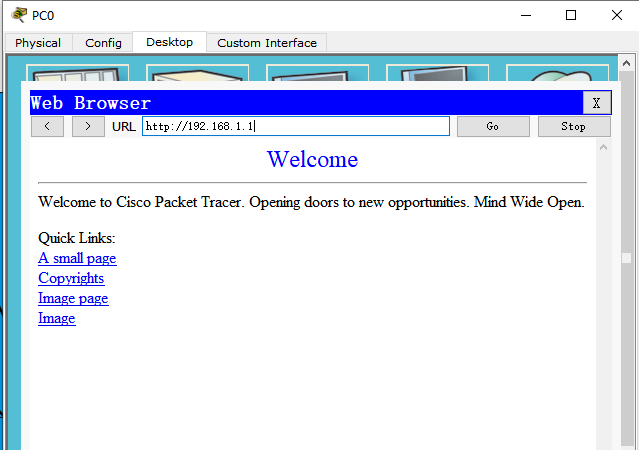


在三层交换机上添加动态路由项192.168.2.0和192.168.1.0；（完成后可传信到WEB服务器）；



完成以上步骤后外部PC可成功访问WEB服务器。

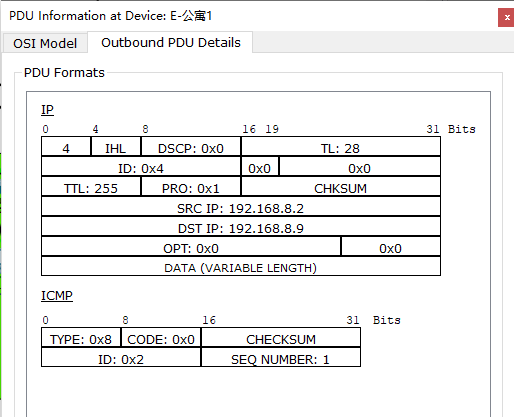


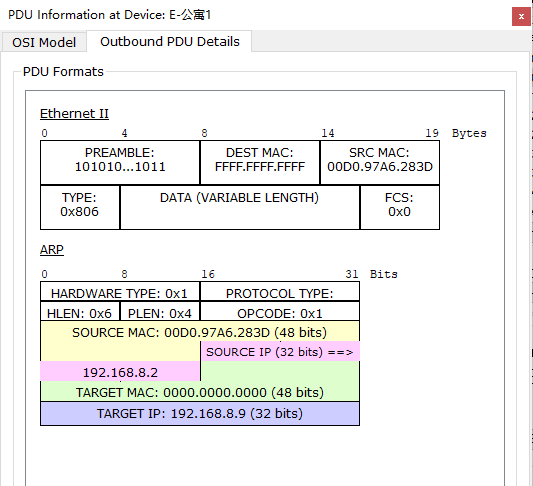


# 六、实验结果分析

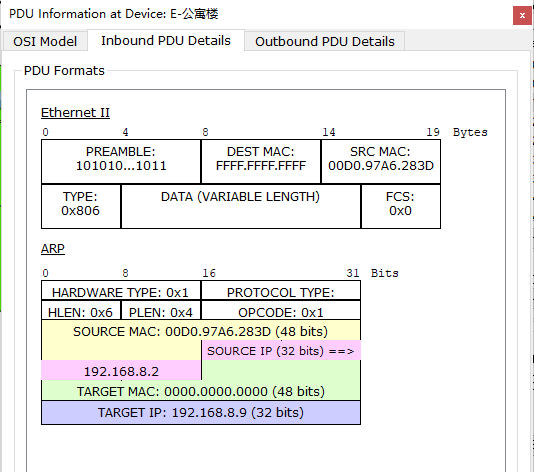
## 6.1 VLAN内部通信

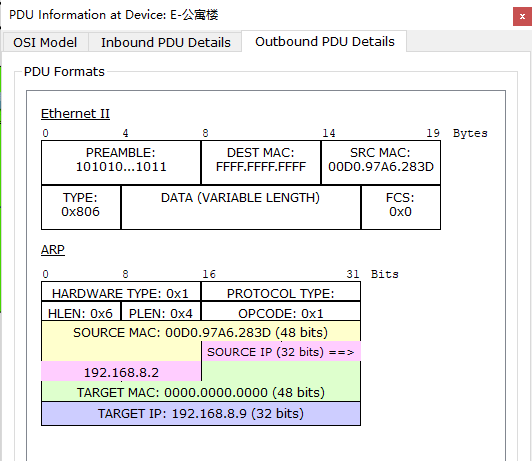
以E-公寓1向E-公寓2发信为例，在各个设备上的报文状态如下所示：

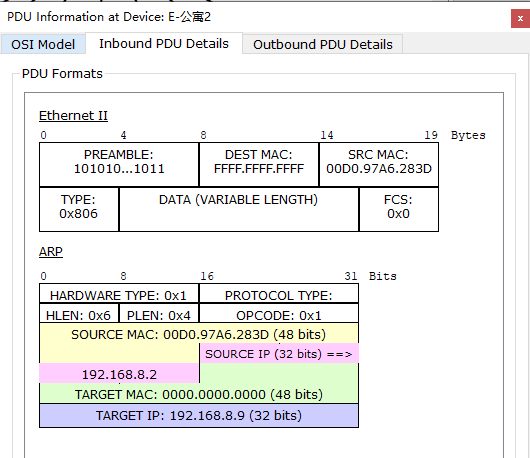


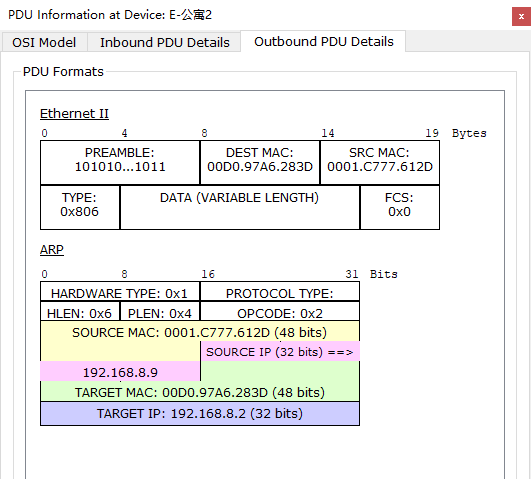


在E-公寓1这个主机上的IP报文给出了源IP地址和目的IP地址，但是此时ARP报文中只给出了源MAC地址，而没有给出目的MAC地址；

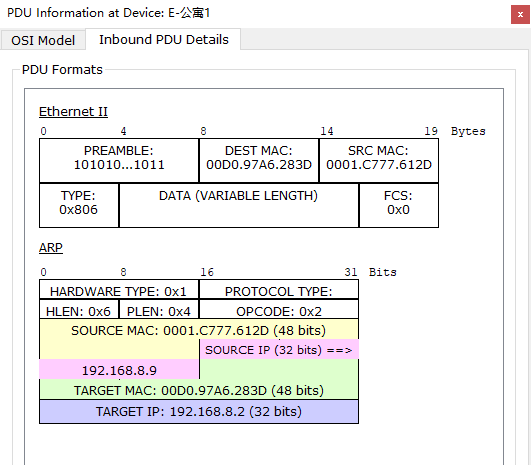


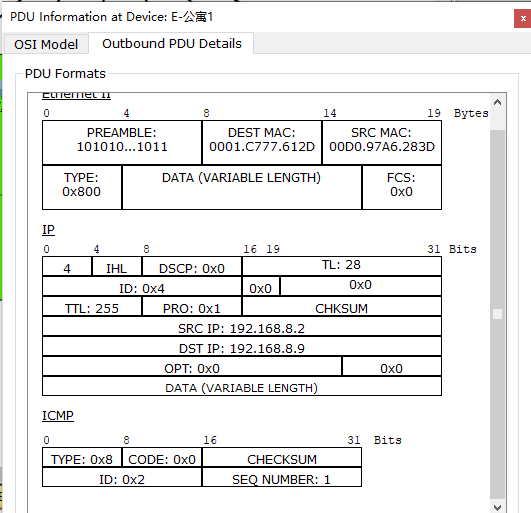






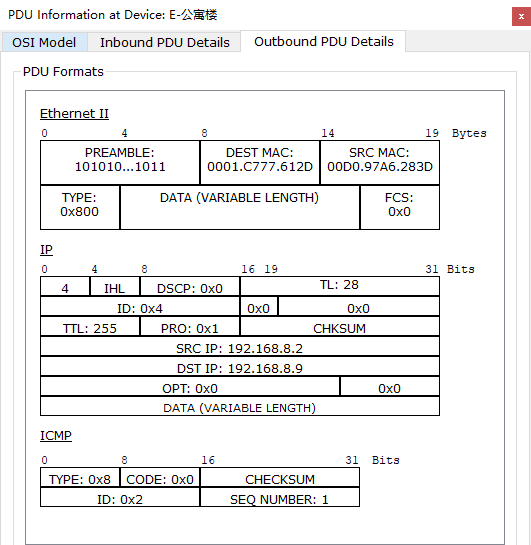
在报文到达E-公寓2后，ARP协议获取了该主机的MAC地址，也就是目的MAC地址，并将其返回给E-公寓1；





当ARP报文返回到E-公寓1后，E-公寓1再次发送报文，此时已经得知目的MAC地址；



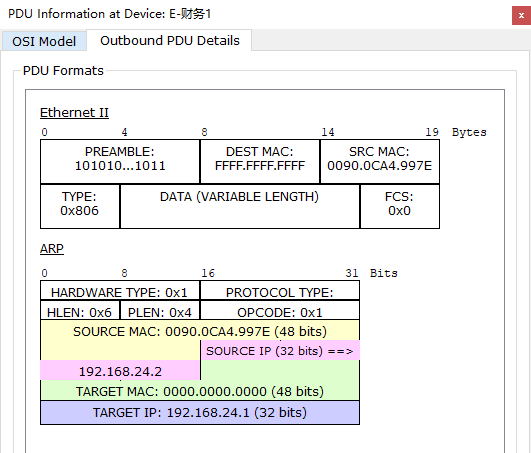


报文成功发送；

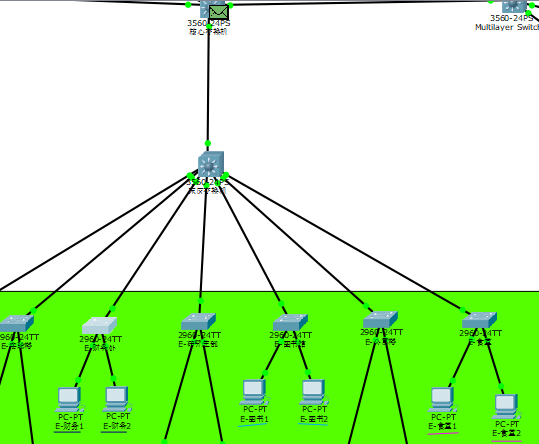
## 6.2 VLAN间通信

以E-财务1向E-食堂1发信为例，在各个设备获取的报文如下：

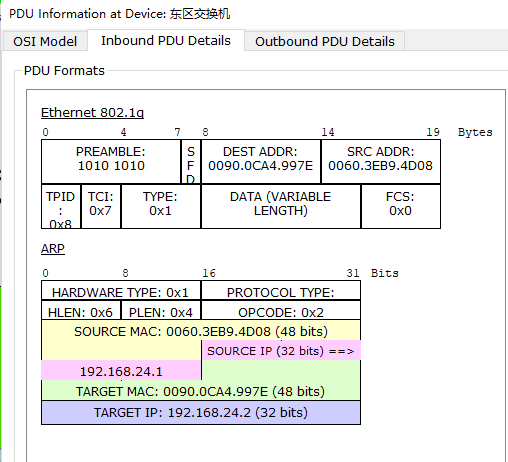




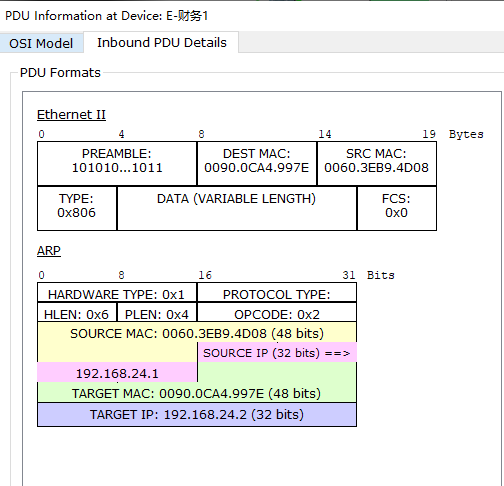
在E-财务1这个主机上的IP报文给出了源IP地址和目的IP地址，但是此时ARP报文中只给出了源MAC地址，而没有给出目的MAC地址；

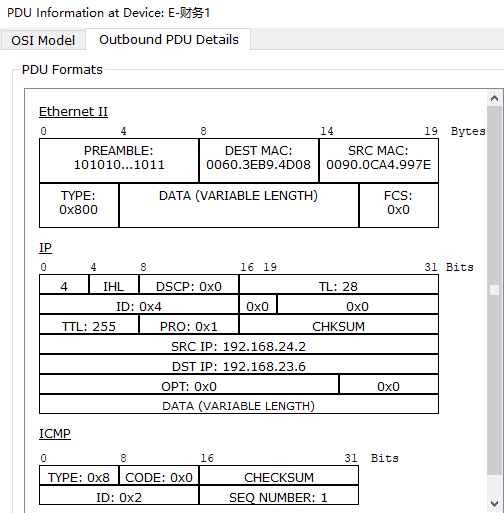


东区交换机上没有目的VALN的信息，报文先进入核心交换机查找目的VLAN的信息；

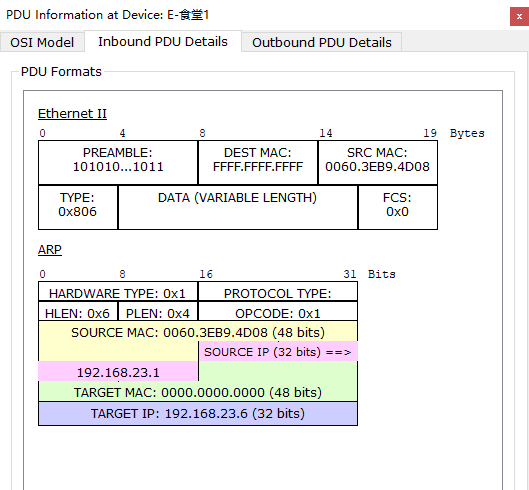


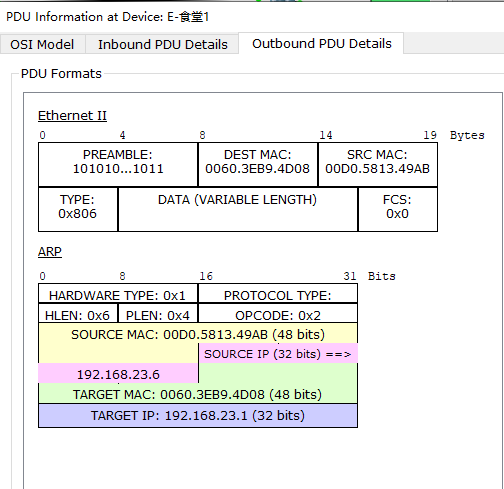
此时已经获取了目的MAC地址；





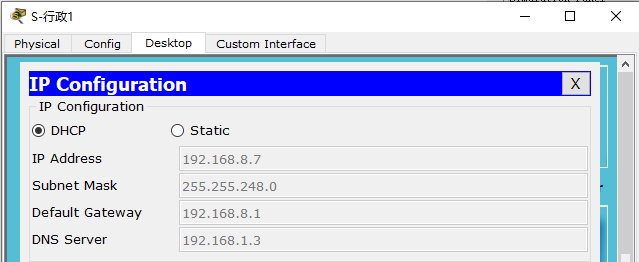
此时E-财务1再次发送报文，报文中也有了目的MAC地址信息；

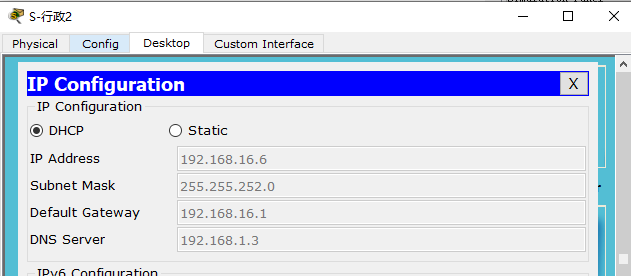


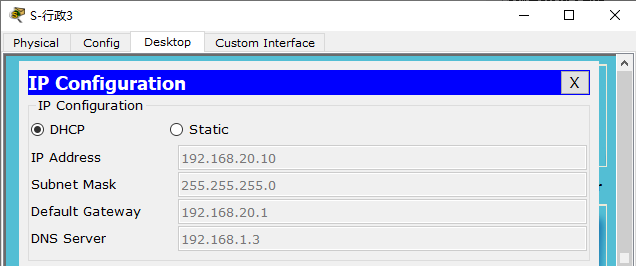


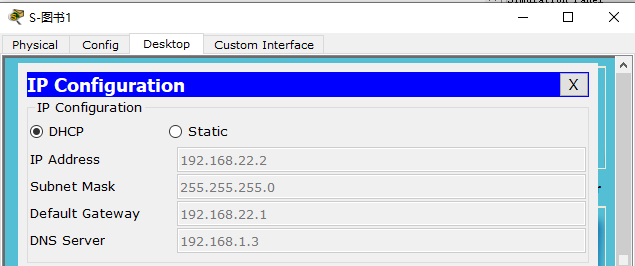
报文发送成功；

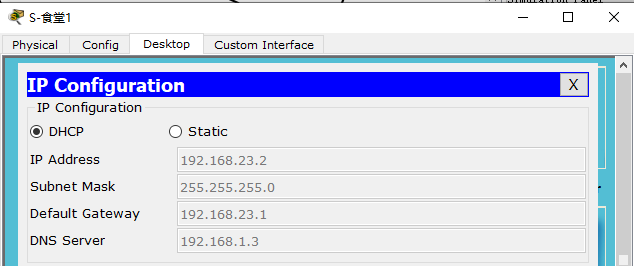
## 6.3 DHCP自动划分IP地址

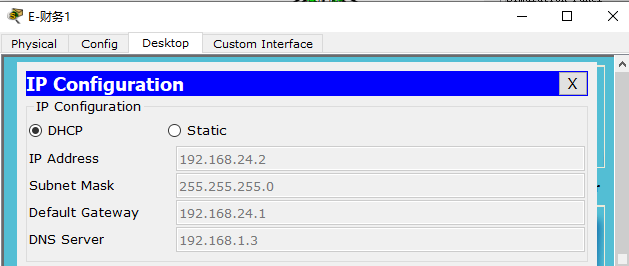




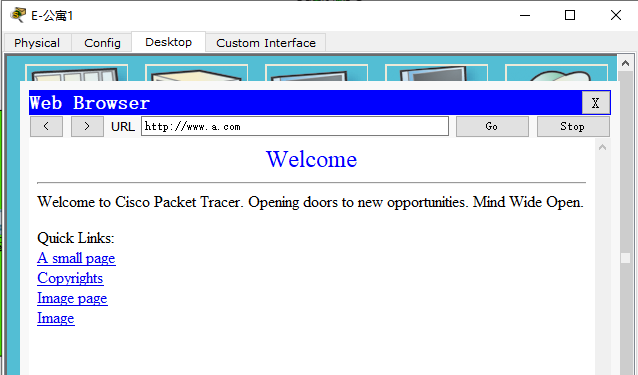


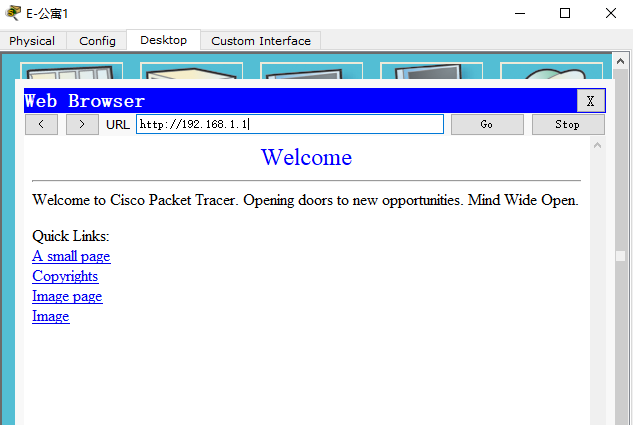


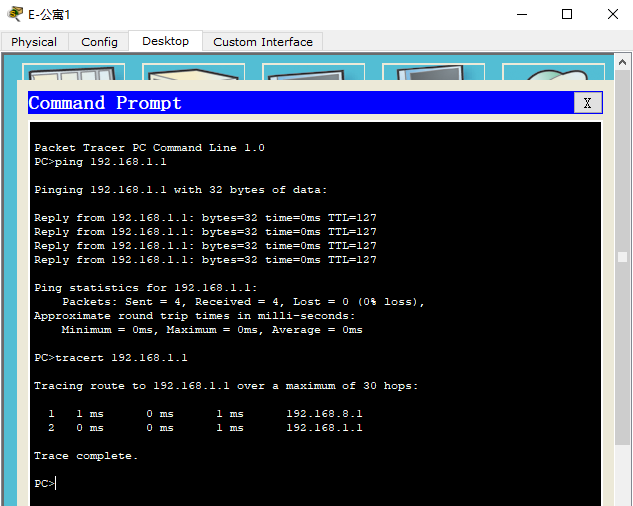




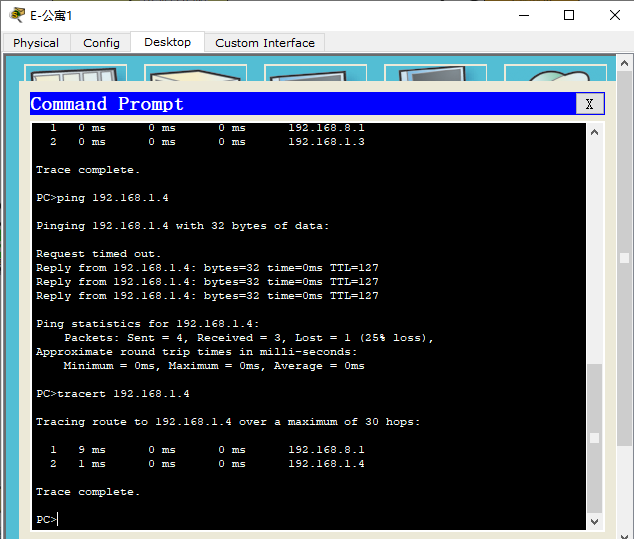
## 6.4 网络服务配置

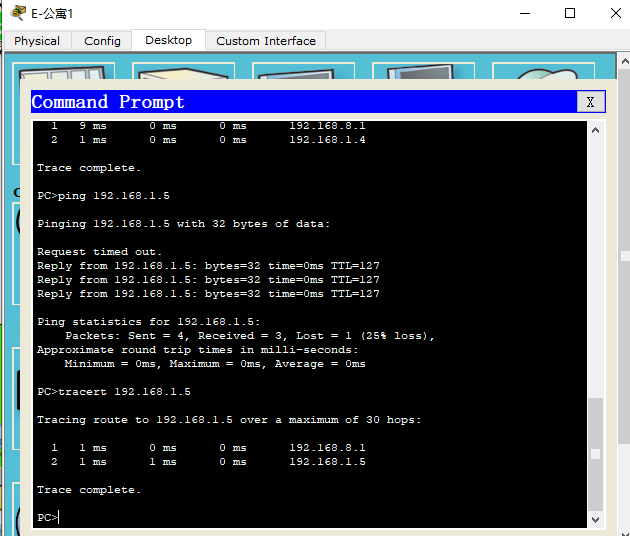




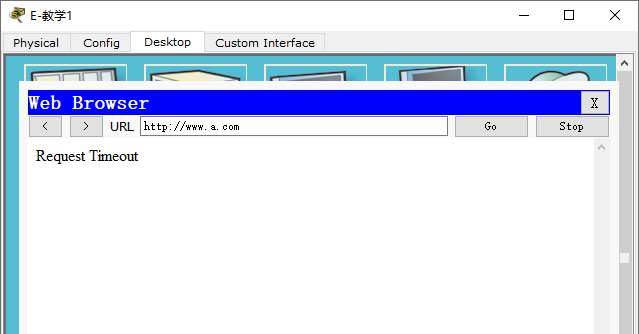


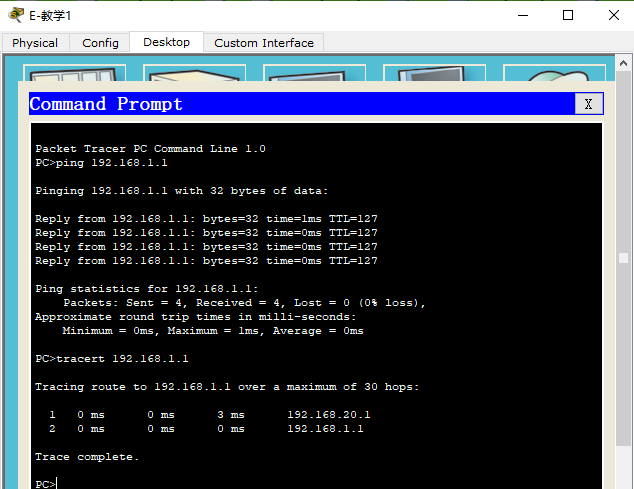




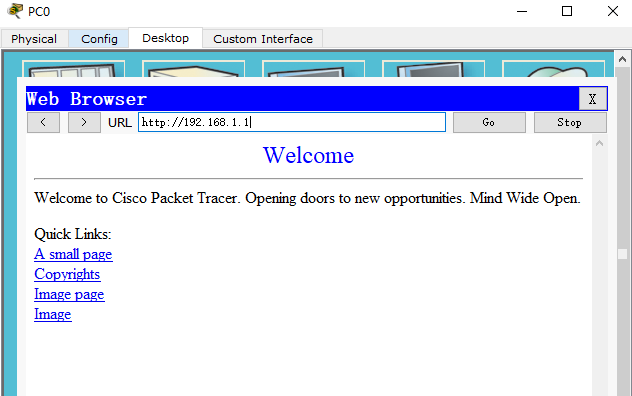


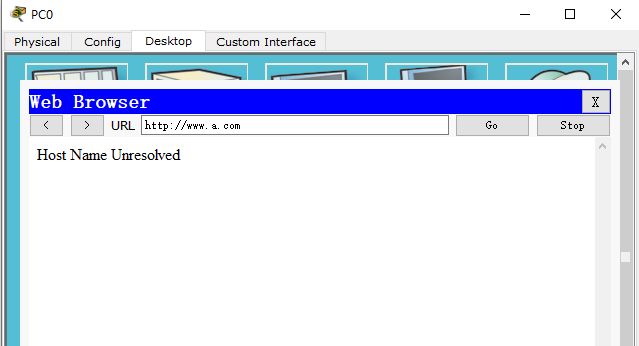
## 6.5 安全功能配置

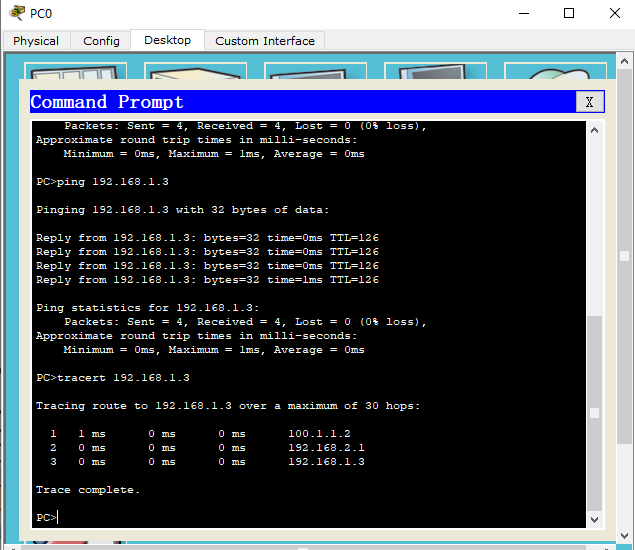




E-教学1无法通过Web Browser访问服务器，但是可以ping通WEB服务器；



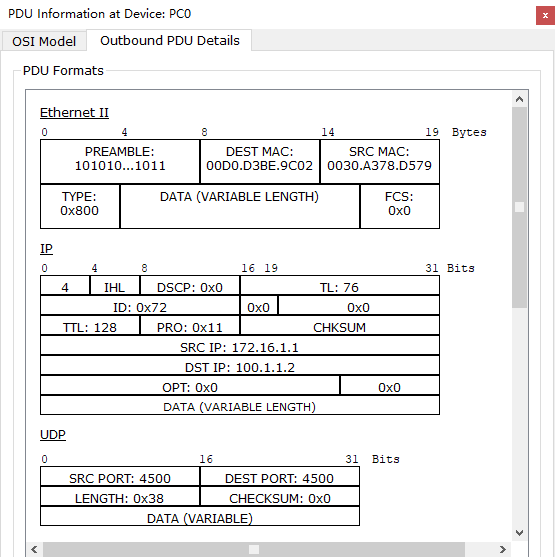


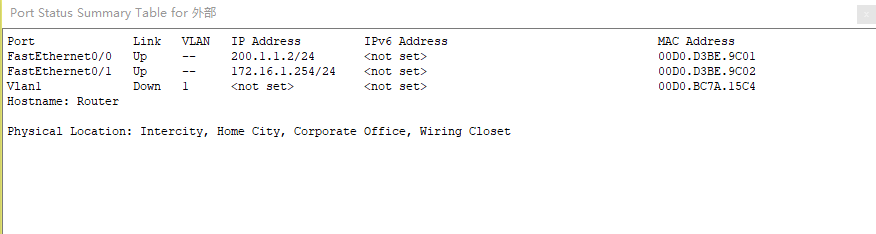


外部主机可以通过IP地址访问WEB服务器，但是不能使用域名直接访问WEB服务器，原因是域名解析协议被禁止；

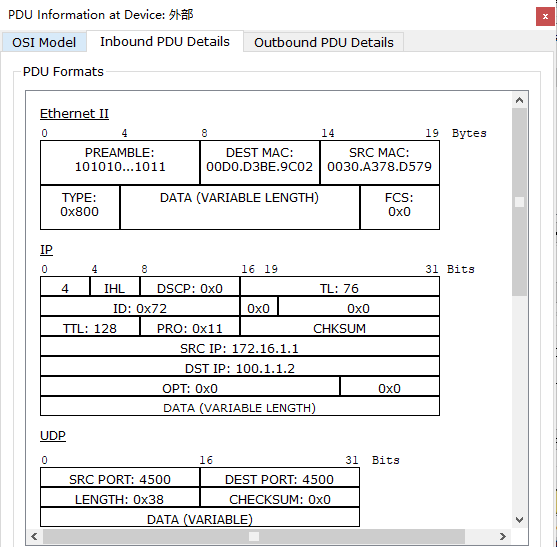
## 6.6 VPN远程接入访问配置

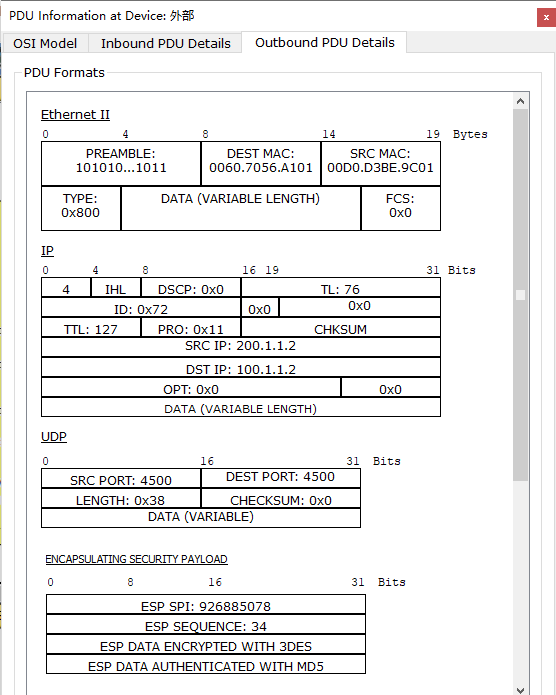
以外部主机向WEB服务器发信为例，获取在各个设备上的报文状态；



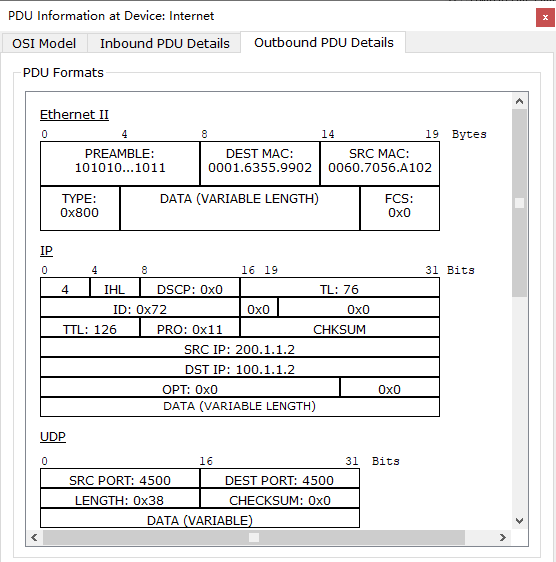


外部主机目的MAC地址即为外部路由器与其接口的MAC地址；

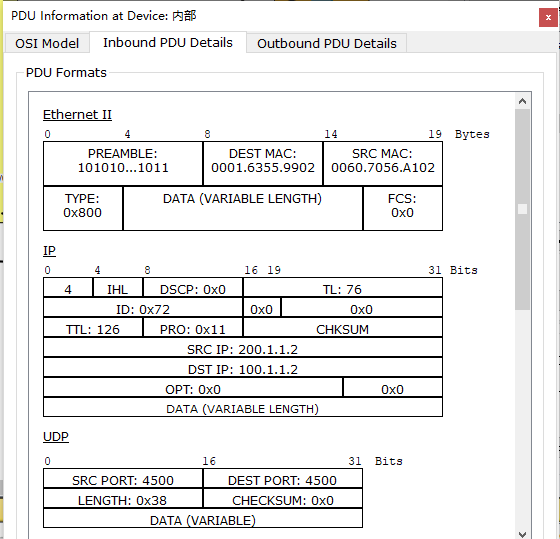


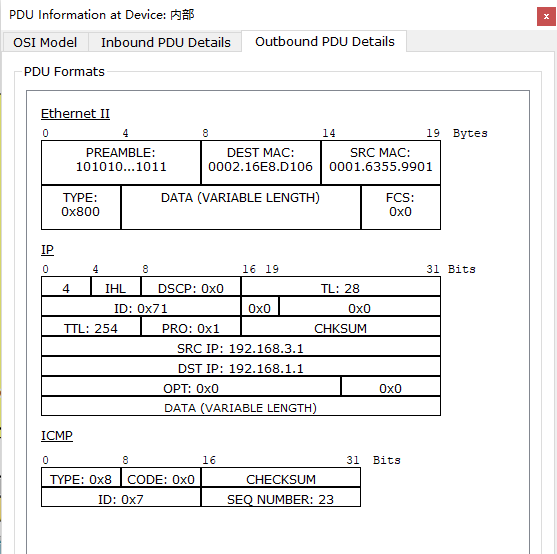


此时源MAC地址和目的MAC地址都发生了变化；

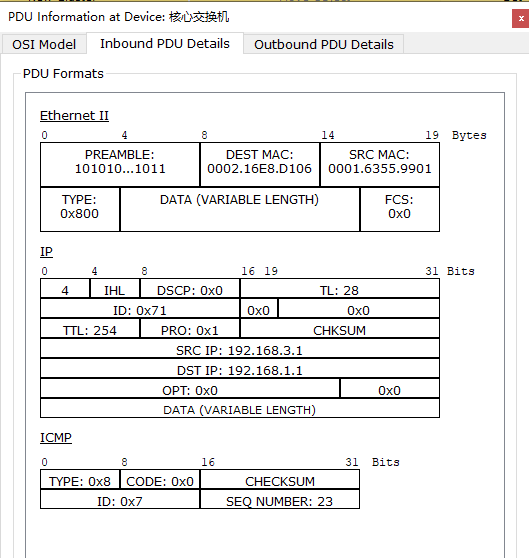


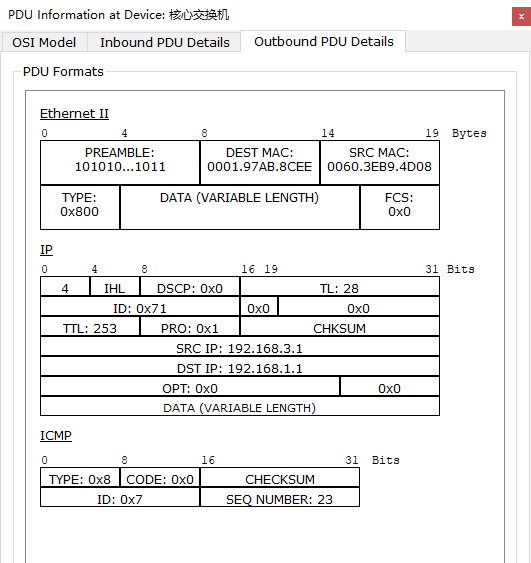
源MAC地址和目的MAC地址再次发生了变化；

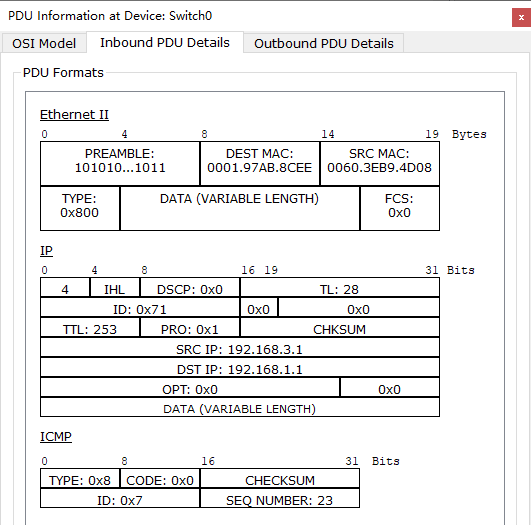


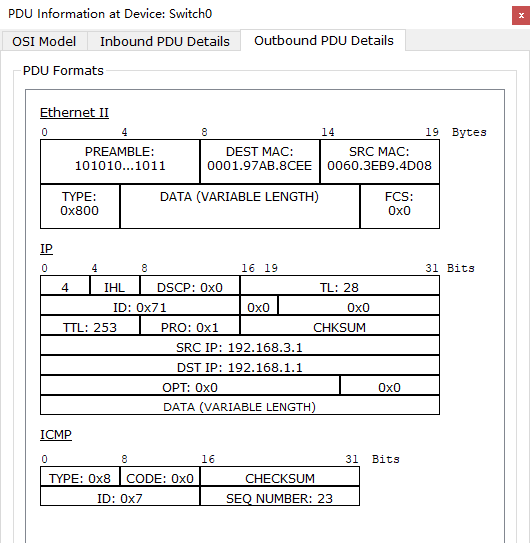


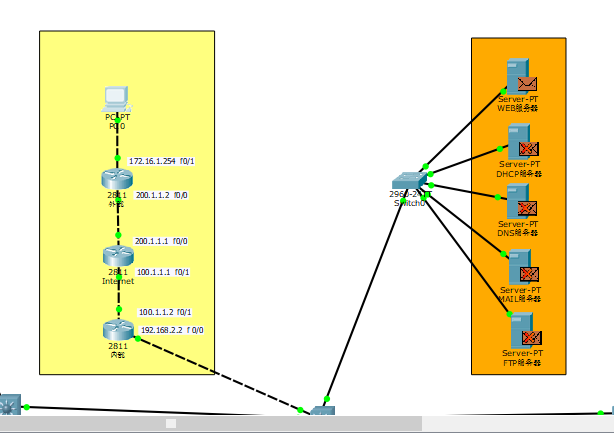
源MAC地址和目的MAC地址发生了变化，同时获得了一个内部IP地址192.168.3.1;

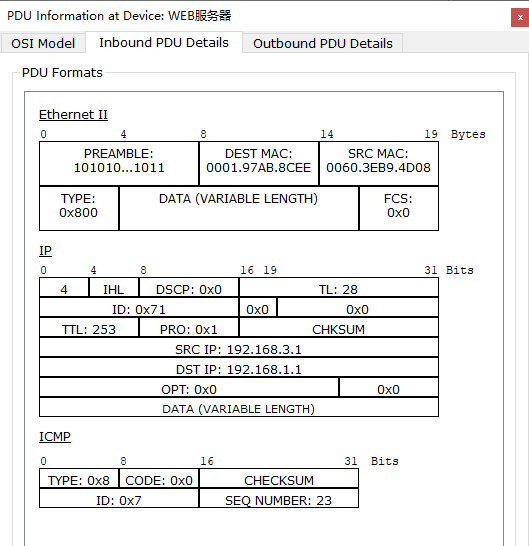






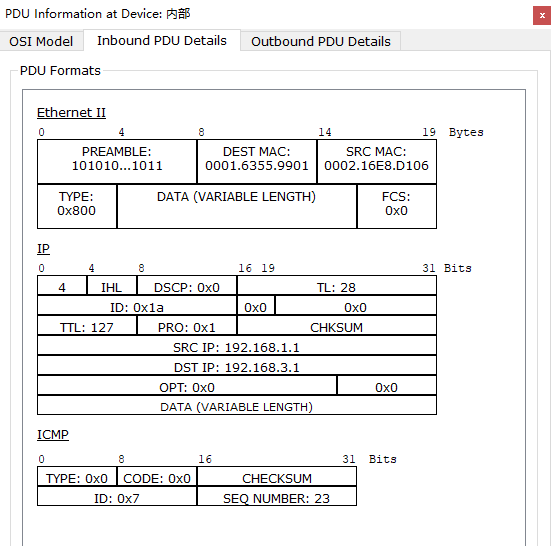


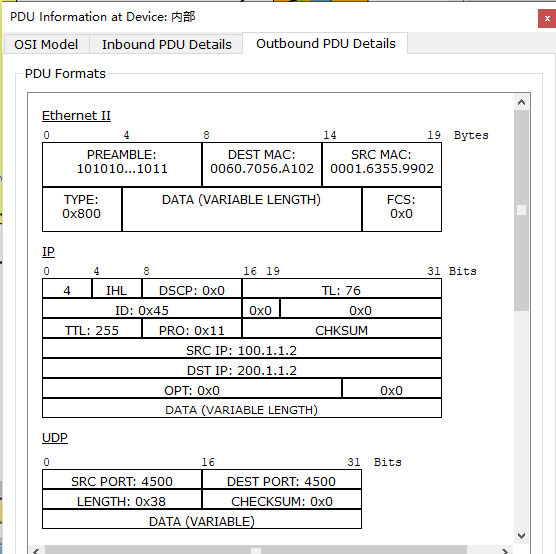






WEB服务器成功收到报文；





此时目的IP地址再次变回外部IP地址；



回发成功；