# 《计算机网络实验》综合实验项目报告

## 基于Packet Tracer的校园网搭建仿真设计

目录

[《计算机网络实验》综合实验项目报告 1](#_Toc169177961)

[基于Packet Tracer的校园网搭建仿真设计 1](#_Toc169177962)

[小组成员及分工： 3](#_Toc169177963)

[指导教师： 3](#_Toc169177964)

[一、问题描述 3](#_Toc169177965)

[二、网络拓扑结构 4](#_Toc169177966)

[三、各个部门的设计 5](#_Toc169177967)

[1.核心层 5](#_Toc169177968)

[1.1核心层拓扑图 5](#_Toc169177969)

[1.2核心层静态地址 5](#_Toc169177970)

[1.3核心层DNS配置 6](#_Toc169177971)

[2.软件学院 6](#_Toc169177972)

[2.1软件学院拓扑图 6](#_Toc169177973)

[2.2配置VLAN3 7](#_Toc169177974)

[2.3搭建软件学院服务器 7](#_Toc169177975)

[2.4配置WIFI 8](#_Toc169177976)

[3.教务处 9](#_Toc169177977)

[3.1教务处拓扑图 9](#_Toc169177978)

[3.2配置VLAN 9](#_Toc169177979)

[3.3搭建教务处服务器 10](#_Toc169177980)

[3.4配置教务处WIFI 11](#_Toc169177981)

[3.5配置教务处测试机 12](#_Toc169177982)

[4科研部门 12](#_Toc169177983)

[4.1科研部门拓扑图 12](#_Toc169177984)

[4.2配置VLAN 13](#_Toc169177985)

[4.3搭建科研部门服务器 13](#_Toc169177986)

[配置科研部门WIFI 14](#_Toc169177987)

[4.4配置科研部门主机 15](#_Toc169177988)

[5外⽹设计 15](#_Toc169177989)

[5.1外⽹部分拓扑图 15](#_Toc169177990)

[5.2外⽹静态地址 15](#_Toc169177991)

[5.3外⽹DNS配置 16](#_Toc169177992)

[四、内外⽹连通 16](#_Toc169177993)

[核心交换机配置 17](#_Toc169177994)

[网关路由器配置 18](#_Toc169177995)

[外网路由器配置 19](#_Toc169177996)

[五、ACL访问配置 20](#_Toc169177997)

[在交换机上进行ACL的配置 20](#_Toc169177998)

[验证access list的配置 21](#_Toc169177999)

[验证各个部门是否隔离 21](#_Toc169178000)

[六、网络连接测试 22](#_Toc169178001)

[软件学院测试 22](#_Toc169178002)

[教务部测试 24](#_Toc169178003)

[科研部门测试 26](#_Toc169178004)

[外网测试 28](#_Toc169178005)

[ACL测试 28](#_Toc169178006)

#### 小组成员及分工：

2252090 王麒懿：核心层与内外网连接设计

2252948 王若豪：核心层与ACL设计

2250694 刘子赫：教务处与ACL设计

2252439 王语凡：软件部门设计

2253209 刘佳朋：科研部门设计

#### 指导教师：

陈伟超

## 一、问题描述

学校有若干部门，包括各个院系，科研部门，教务处，后勤部等，请为此设计网络架构，其中需要满足的功能有：

1. 每个部门配置自己独立局域网，且包含自己的文件服务器和Web服务器，实现部门间的隔离和互访；

2. 学校统一提供接入到互联网的接口（假设学校有一个公网IPv4地址100.64.1.0/24），需配置NAT功能；

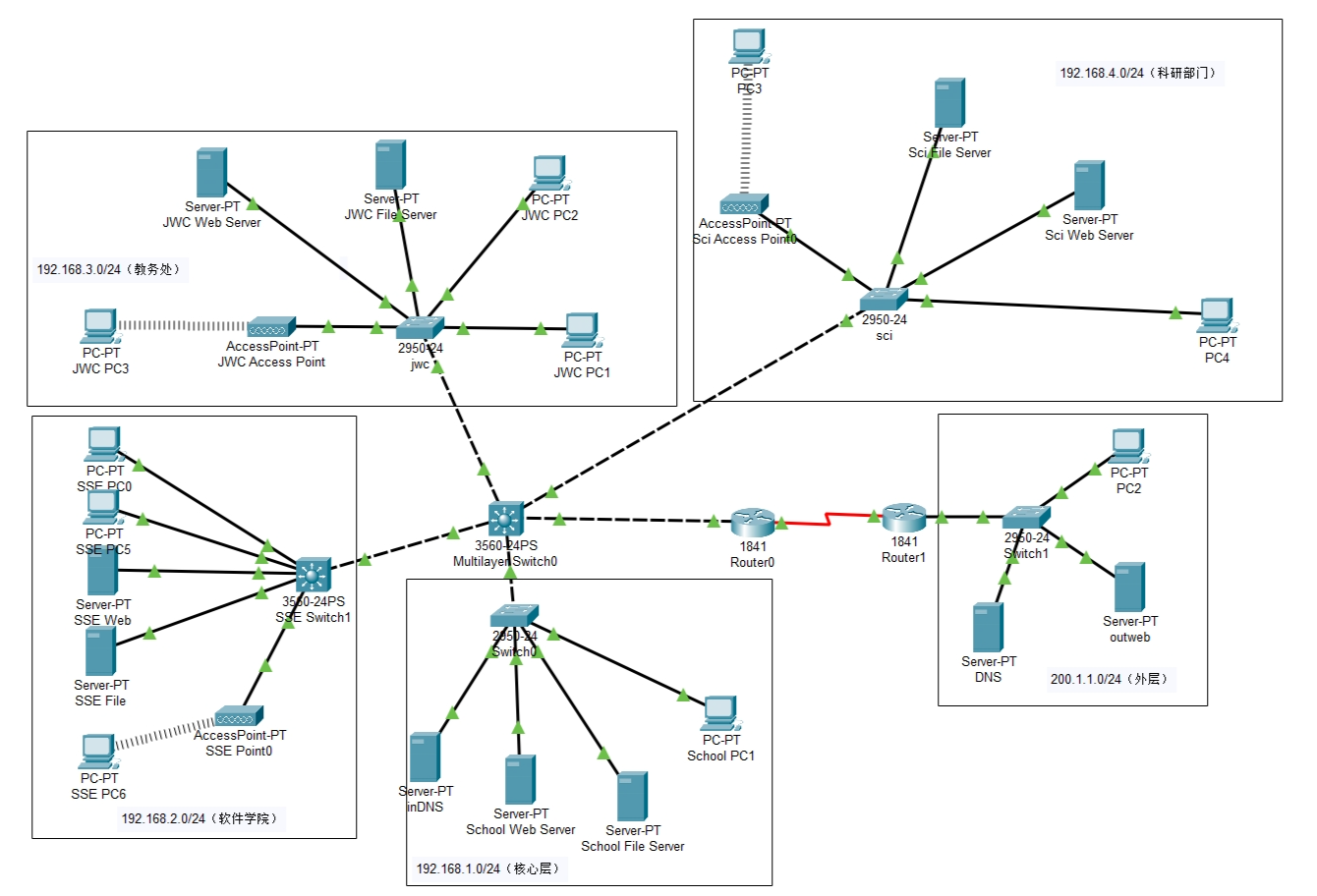
3. 学校需提供一个外网可访问的Web服务器，以及一个各部门公用的文件服务器；

4. 网络需提供WiFi接入功能；

5. 科研部门须有访问接入控制ACL设计；

6. 随机抓取（在Packet Tracer内）某类型的数据包并解读，如TCP, IP, MAC, ARP等（需现场演示）。

## 二、网络拓扑结构



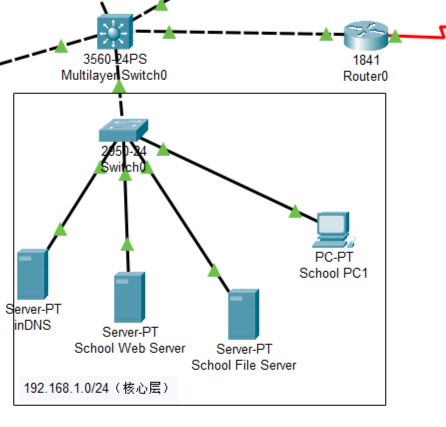
（图：总体拓扑图）

1. 内网划分为核心层、软件学院、科研部门和教务处。外网配置了多台PC机和Web、DNS服务器。
2. 核心层部署了Web服务器、DNS服务器、文件服务器和测试机，所有部门均可访问。
3. 各部门既相互独立，又各自拥有两台服务器和WiFi服务。
4. 网关路由器提供NAT功能，核心层Web服务器配置公网IP，对外开放。外网用户可通过公网IP访问。内网其他设备使用NAT池，在公网IP有限的情况下，多个设备可复用IP访问外网。大学各部门均可访问公网的外部Web和DNS服务器。

## 三、各个部门的设计

#### 1.核心层

###### 1.1核心层拓扑图

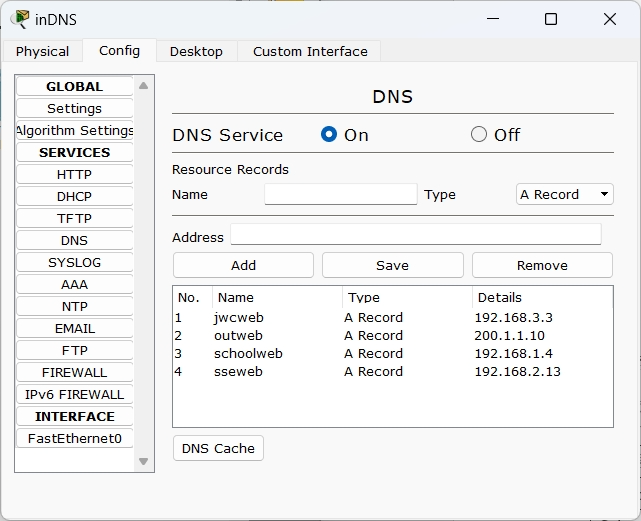


###### 1.2核心层静态地址

对于核心层来说，我们考虑为服务器分配静态IP地址，并设置一台PC机进行检验，分配如下：

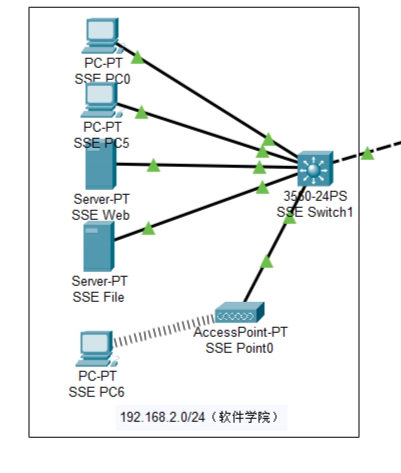
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务器 | IP | 子网掩码 | 网关 | DNS |
| School Web server | 192.168.1.4 | 255.255.255.0 | 192.168.1.1 | 192.168.1.2 |
| School inDNS server | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |  |
| School file server | 192.168.1.5 | 255.255.255.0 | 192.168.1.1 | 192.168.1.2 |
| PC1 | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 | 192.168.1.2 |

###### 1.3核心层DNS配置



#### 2.软件学院

###### 2.1软件学院拓扑图



###### 2.2配置VLAN3

核心交换机配置VLAN3

Switch(config)# vlan 3

Switch(config-vlan)# name "sse"

Switch(config-vlan)# exit

Switch(config)# interface vlan 3

Switch(config-if)# ip address 192.168.2.1 255.255.255.0

Switch(config-if)# no shutdown

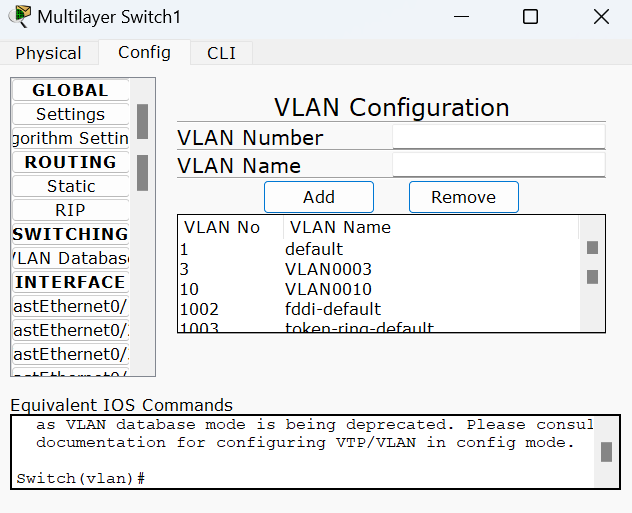
VLAN名称为VLAN3，网段为192.168.2.1，子网掩码为255.255.255.0，端口开启，并把与软件学院总交换机端口设为Access Vlan 3，并在软件学院交换机添加VLAN3。

Switch>enable

Switch#configure terminal

Switch(config)#vlan 4

Switch(config-vlan)#name sse



###### 2.3搭建软件学院服务器

Web服务器配置如下：

IP: 192.168.2.13

Subnet Mask: 255.255.255.0

Gateway: 192.168.2.1

DNS Server: 192.168.1.2

打开HTTP和HTTPS服务



File服务器配置如下：

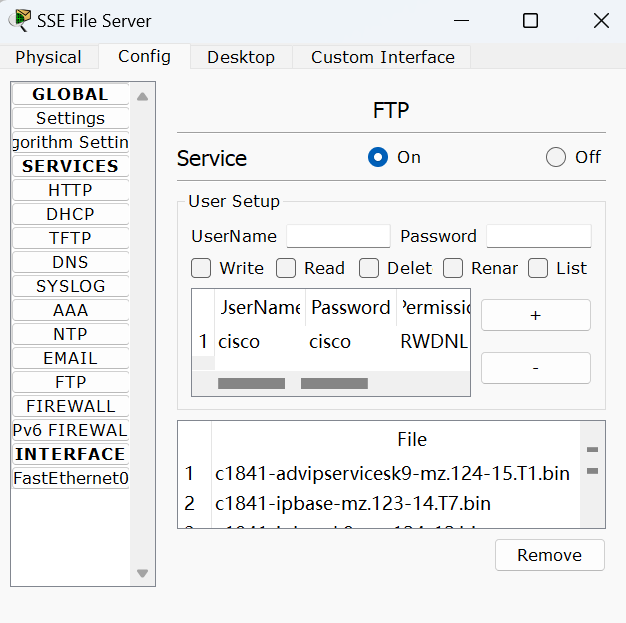
IP: 192.168.2.14

Subnet Mask: 255.255.255.0

Gateway: 192.168.2.1

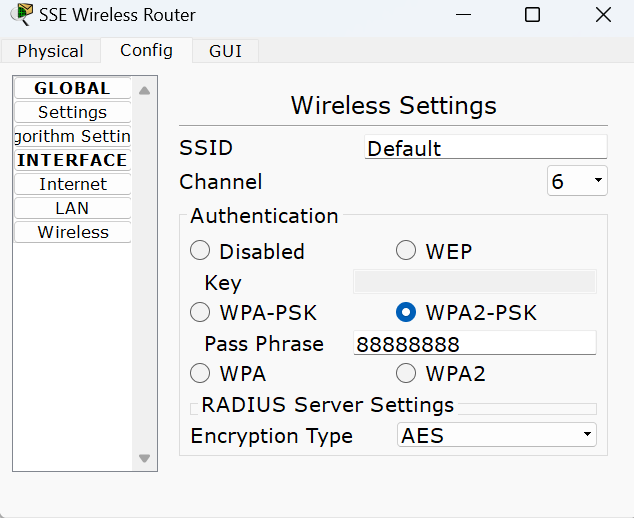
DNS Server: 192.168.1.2

实现FTP功能



###### 2.4配置WIFI

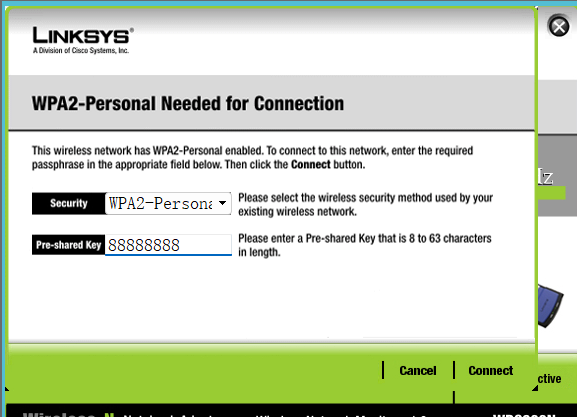
设置WIFI密码为88888888



配置PC端

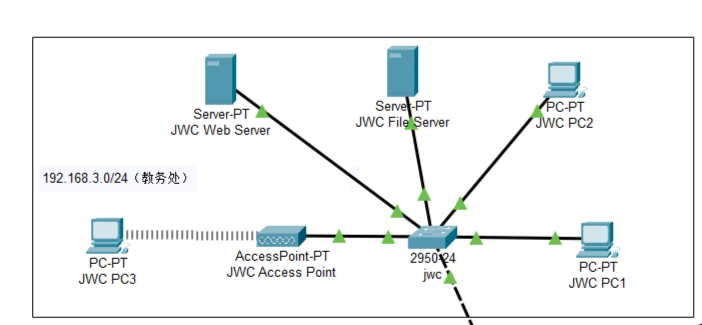
首先插入网卡

其次输入密码，连接WIFI



#### 3.教务处

###### 3.1教务处拓扑图



###### 3.2配置VLAN

在核心交换机上配置VLAN：

Switch(config)# vlan 4

Switch(config-vlan)# name "jwc"

Switch(config-vlan)# exit

Switch(config)# interface vlan 4

Switch(config-if)# ip address 192.168.3.1 255.255.255.0

Switch(config-if)# no shutdown

VLAN名称为“jwc”，网段为192.168.3.1，子网掩码为255.255.255.0，端口开启.

把与教务处交换机相连的端口（Fa 0/4）配置为 Access Vlan 4.

在教务处交换机上添加VLAN：

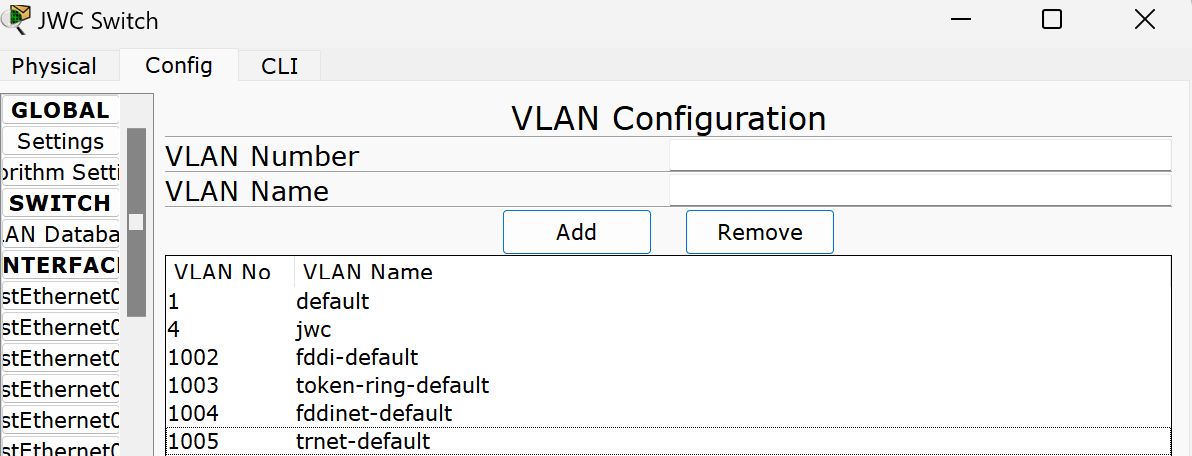
Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 4

Switch(config-vlan)#name jwc



###### 3.3搭建教务处服务器

Web服务器配置如下：

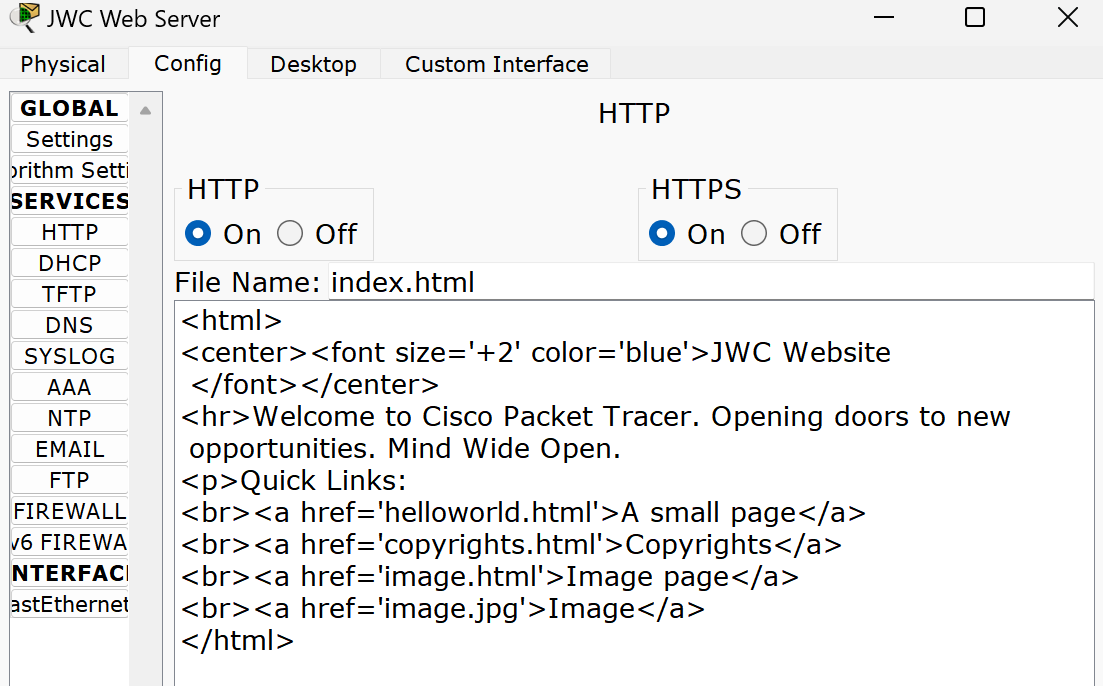
IP: 192.168.3.3

Subnet Mask: 255.255.255.0

Gateway: 192.168.3.1

DNS Server: 192.168.1.2

打开HTTP和HTTPS服务：



File服务器配置如下：

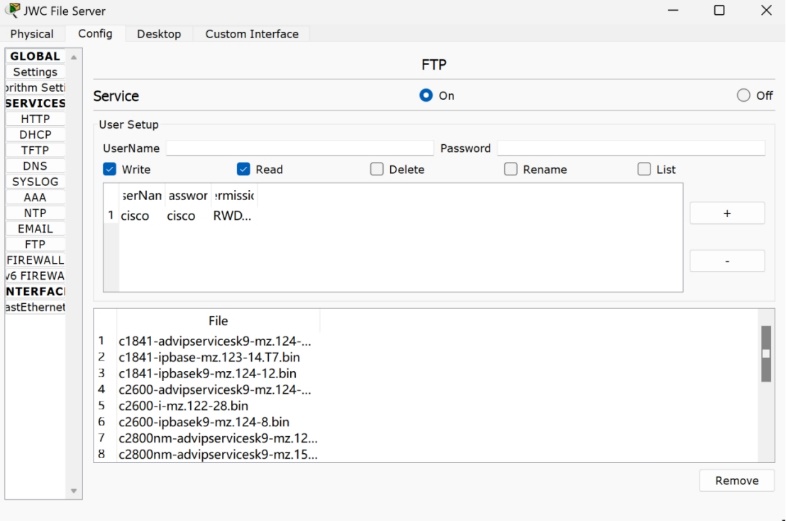
IP: 192.168.3.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.3.1

DNS Server: 192.168.1.2

打开FTP服务，赋予读、写权限：



###### 3.4配置教务处WIFI

配置教务处的 WIFI 接入点（这里是 AccessPoint-PT）：

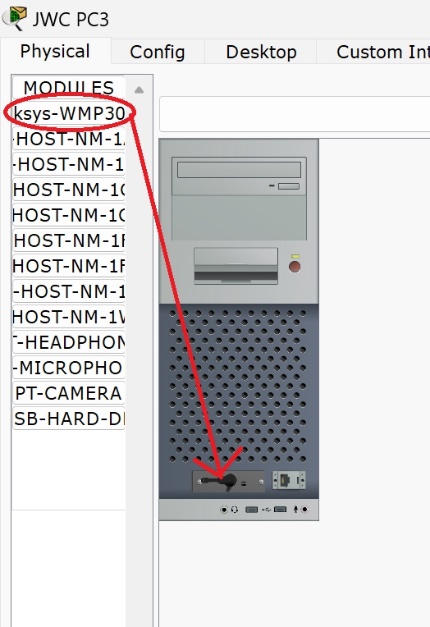
SSID: JWC-WIFI

KEY: WPA2-PSK

PASS Phrase: "11111111"

配置远程 PC 连接教务处 WIFI：

先选择PC模型为Linksys-WMP300N ：



再在PC上进行如下配置：

SSID: JWC-WIFI

Authentication: WPA2-PSK

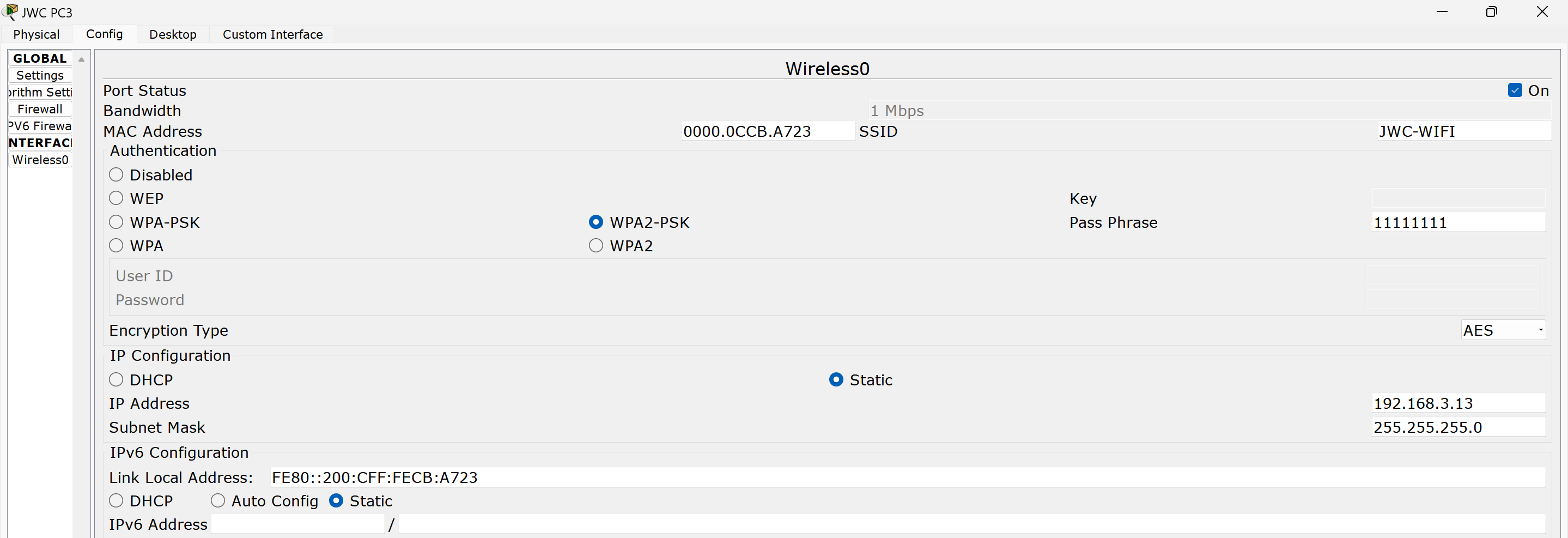
Pass Phrase: "11111111"

IP: 192.168.3.13

Subnet Mask: 255.255.255.0

Gateway: 192.168.3.1

DNS: 192.168.1.2



###### 3.5配置教务处测试机

在教务处交换机上连接两台不同的PC机用于测试，他们的配置如下：

JWC PC1：

IP: 192.168.3.11

Subnet Mask: 255.255.255.0

Gateway: 192.168.3.1

DNS: 192.168.1.2

JWC PC2：

IP: 192.168.3.12

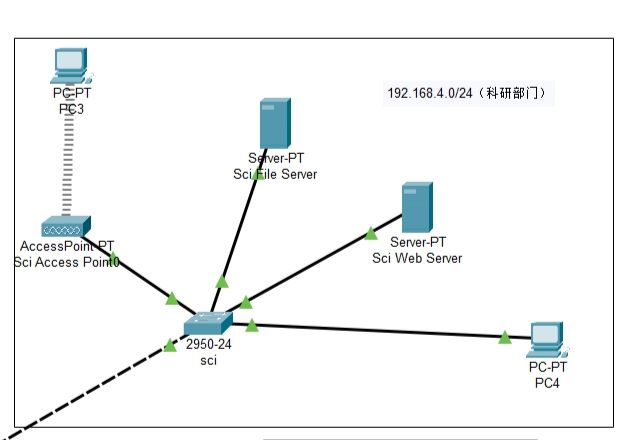
Subnet Mask: 255.255.255.0

Gateway: 192.168.3.1

DNS: 192.168.1.2

#### 4科研部门

###### 4.1科研部门拓扑图



###### 4.2配置VLAN

在核心交换机上配置VLAN：

Switch(config)# vlan 5

Switch(config-vlan)# name "Sci"

Switch(config-vlan)# exit

Switch(config)# interface vlan 4

Switch(config-if)# ip address 192.168.4.1 255.255.255.0

Switch(config-if)# no shutdown

VLAN名称为“Sci”，网段为192.168.4.1，子网掩码为255.255.255.0，端口开启.

把与科研部门交换机相连的端口（Fa 0/5）配置为 Access Vlan 5.

在科研部门交换机上添加VLAN：

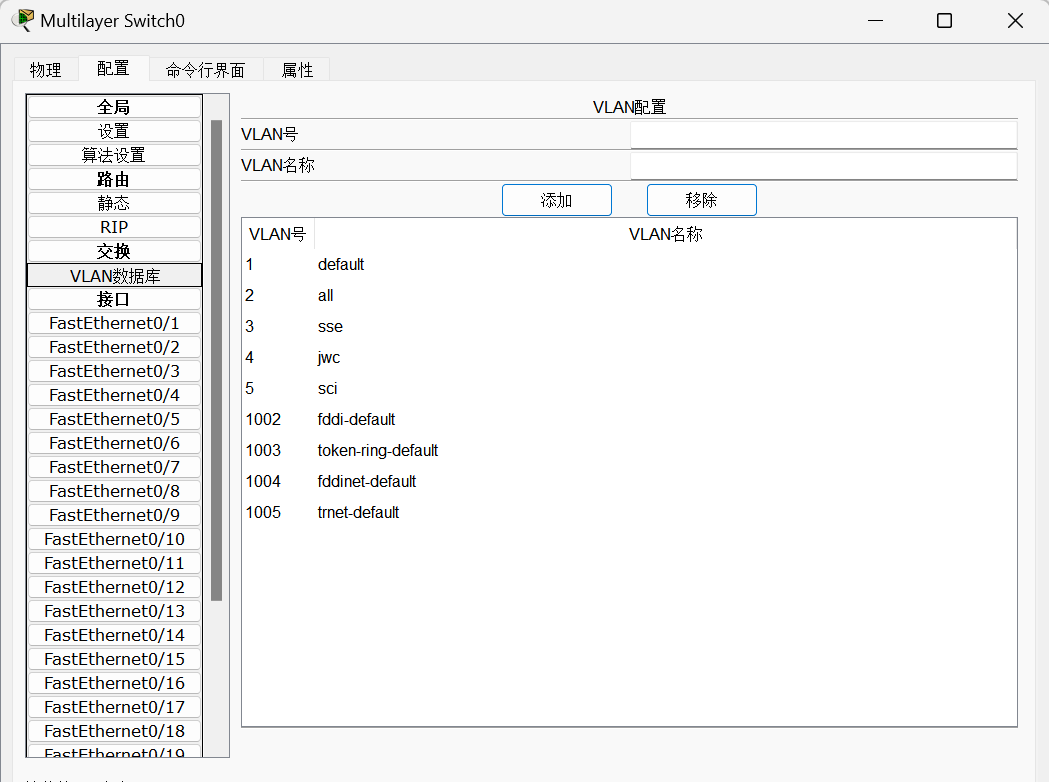
Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 5

Switch(config-vlan)#name Sci



###### 4.3搭建科研部门服务器

Web服务器配置如下：

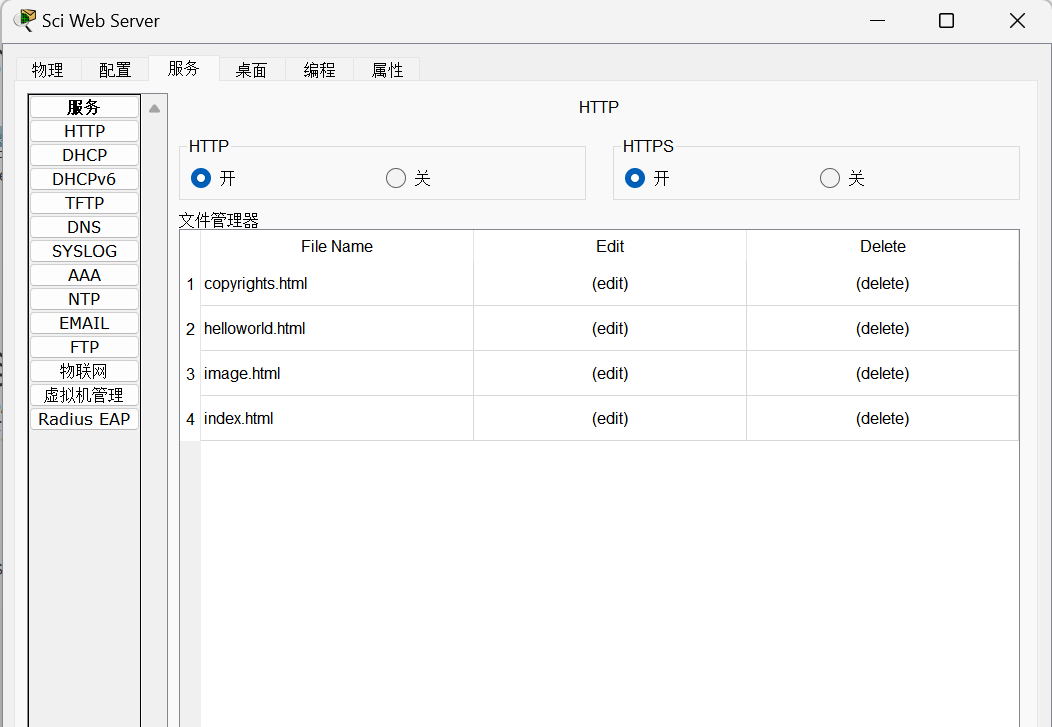
IP: 192.168.4.13

Subnet Mask: 255.255.255.0

Gateway: 192.168.4.1

DNS Server: 192.168.1.2

打开HTTP和HTTPS服务：



File服务器配置如下：

IP: 192.168.4.12

Subnet Mask: 255.255.255.0

Gateway: 192.168.4.1

DNS Server: 192.168.1.2

打开FTP服务，赋予读、写权限：



###### 配置科研部门WIFI

配置科研部门的 WIFI 接入点（这里是 AccessPoint-PT）：

SSID: Sci-WIFI

KEY: WEP

PASS Phrase: "1234567890"

配置远程 PC 连接科研部门 WIFI：

先选择PC模型为Linksys-WMP300N ,再在PC上进行如下配置：

SSID: Sci-WIFI

Authentication: WEP

Pass Phrase: "123456789"

IP: 192.168.4.11

Subnet Mask: 255.255.255.0

Gateway: 192.168.4.1

DNS: 192.168.1.2

###### 4.4配置科研部门主机

在科研部门交换机上连接两台不同的PC机用于测试，他们的配置如下：

Sci PC1：

IP: 192.168.4.14

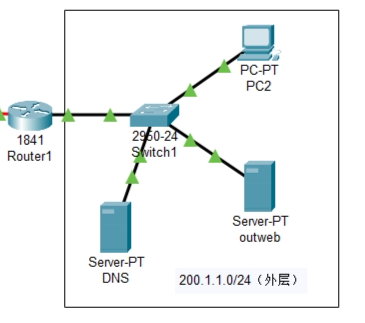
Subnet Mask: 255.255.255.0

Gateway: 192.168.4.1

DNS: 192.168.1.2

#### 5外⽹设计

###### 5.1外⽹部分拓扑图

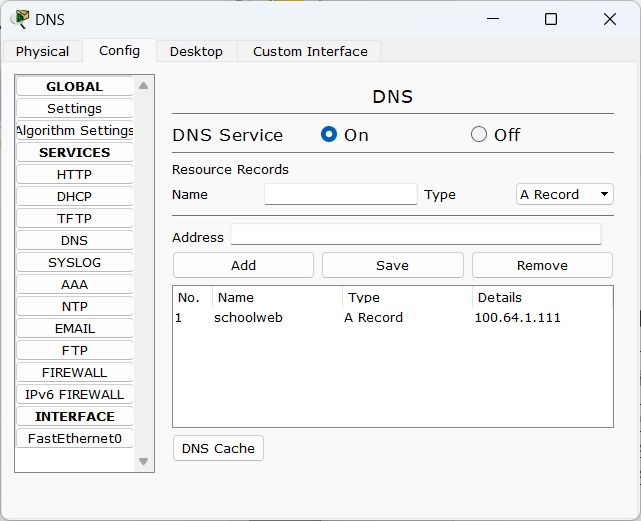


###### 5.2外⽹静态地址

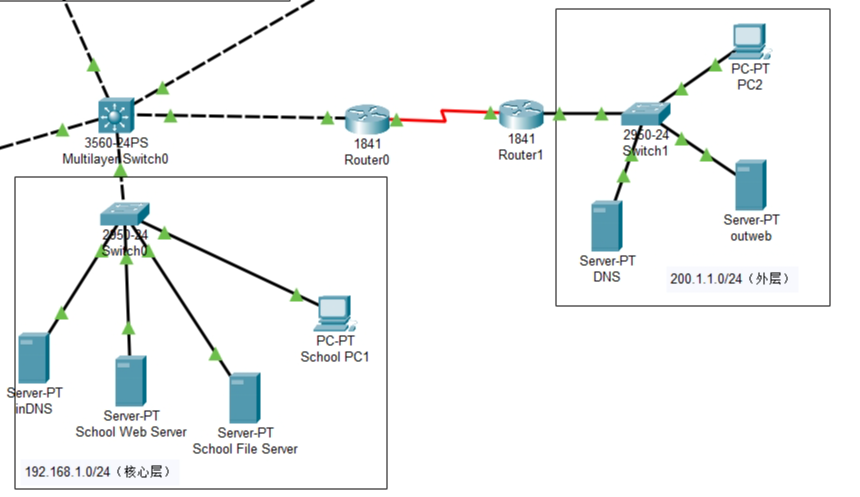
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 终端 | IP | ⼦⽹掩码 | ⽹关 | DNS |
| PC2 | 200.1.1.11 | 255.255.255.0 | 200.1.1.1 | 200.1.1.12 |
| Outside DNS | 200.1.1.12 | 255.255.255.0 | 200.1.1.1 |  |
| Outside Web | 200.1.1.10 | 255.255.255.0 | 200.1.1.1 | 200.1.1.12 |

###### 5.3外⽹DNS配置

我们使用100.64.1.111作为外网访问学校服务器的公网IP



## 四、内外⽹连通

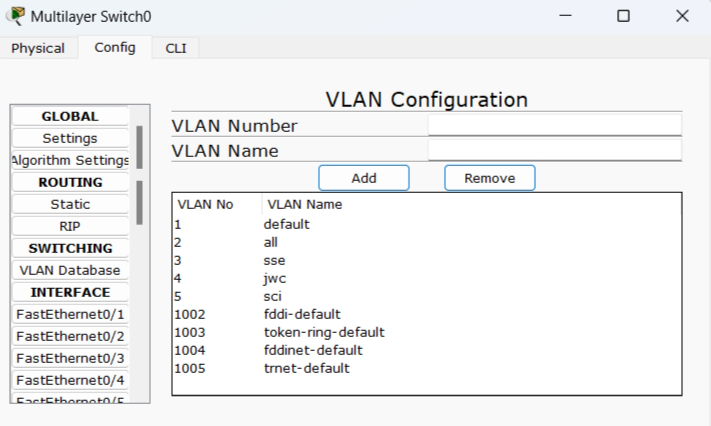


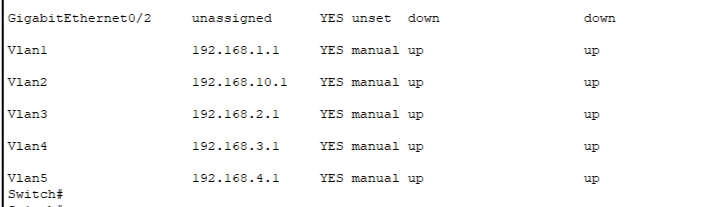
内外网的联通是实现校园网搭建的重要部分。我们计划通过以下方式实现这一目标：

1. 核心交换机配置：核心交换机将用于转发校园网中不同 VLAN 的信息。这将确保各个部门和区域的网络信息能够高效传递和交换。
2. 网关路由器设置：Router0 将作为网关路由器，负责 NAT 配置，实现内网与外网的通信。通过 NAT 配置，内网设备可以使用公用 IP 地址访问外网资源，从而保证内网的安全和 IP 地址的高效利用。
3. 外网路由器配置：Router1 将作为外网路由器，负责接收和转发来自外网的信息。这样，外网的访问请求可以被正确处理，并将相关数据传递到内网的合适位置。

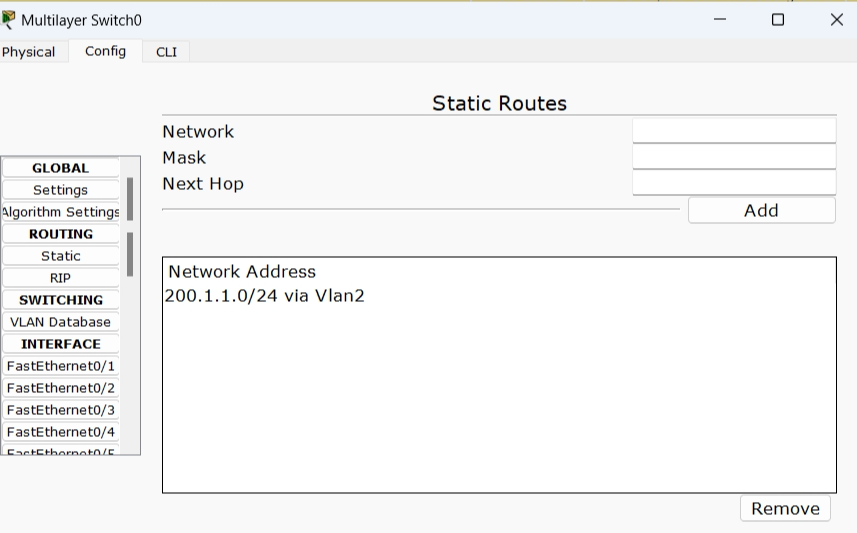
#### 核心交换机配置

我们将各部门不同子网划分为不同vlan，方便管理





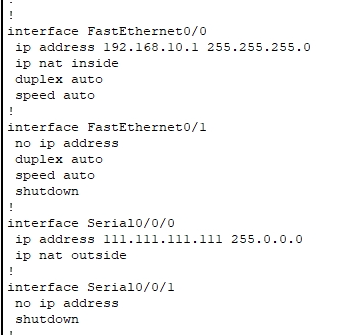
配置静态路由表实现对外网访问消息的转发



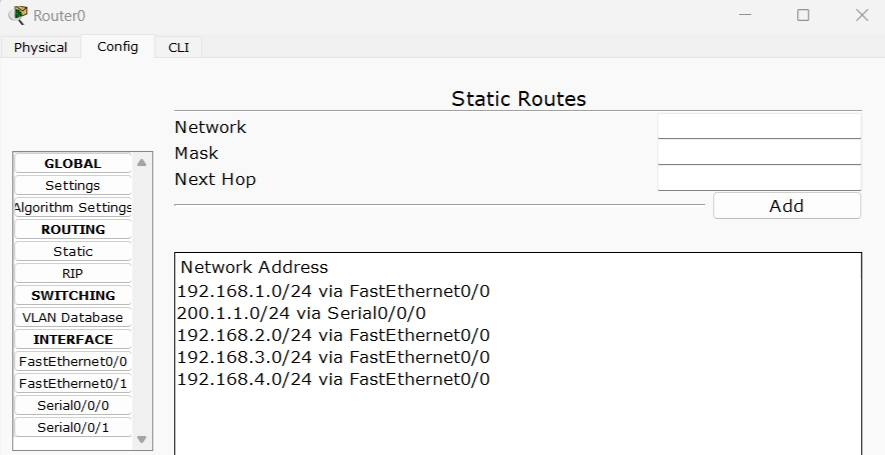
最后使用ip routing 命令，使核心交换机充当路由器，实现不同vlan的通信。

#### 网关路由器配置

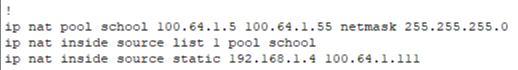
配置端口实现内网与外网的消息转发



配置静态路由实现不同子网消息的传递



配置NAT进行内网ip与公网ip的转换

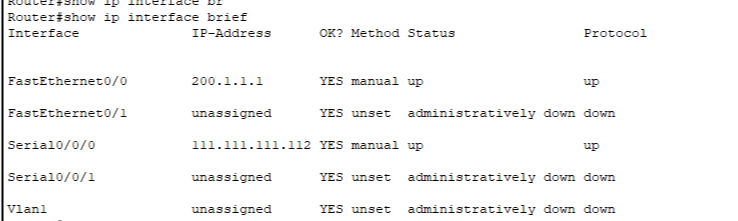


其中静态NAT中100.64.1.111为校园服务器的公网ip，192.168.1.4为其内网IP，

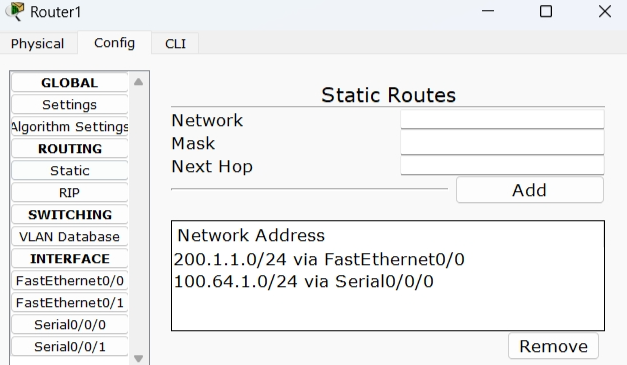
为了实现校内用户可以访问公网，我们通过配置NAT池实现内⽹IP映射到公⽹IP，从而进行访问。

#### 外网路由器配置

配置端口实现内网与外网和外网间的消息转发



配置静态路由实现不同子网消息的传递



## 五、ACL访问配置

#### 在交换机上进行ACL的配置

首先设置access list，再应用到接口上，这里我们应用到vlan4，vlan5。

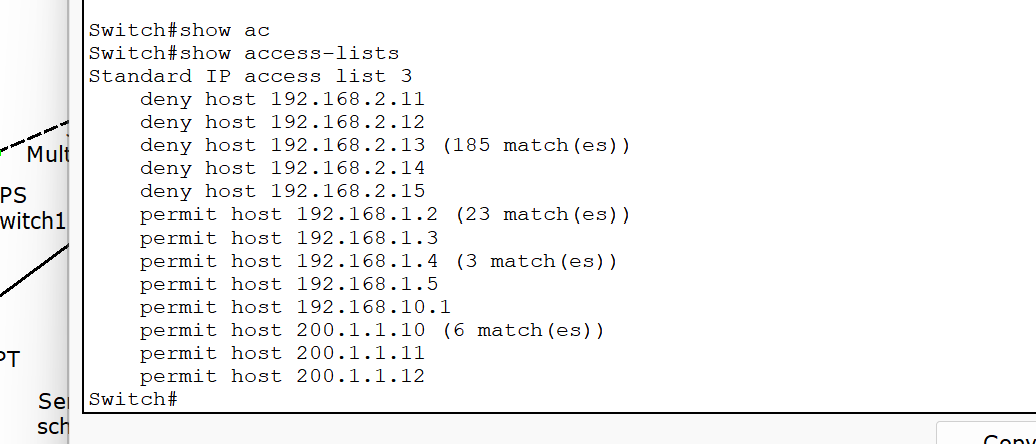
设置access list主要有两个动作，一个为deny，一个为permit。

deny指访问控制列表中的一个动作，表示拒绝符合条件的数据包，permit指接受符合条件的数据包，而在思科交换机中，访问控制列表（ACL）在处理数据包时有一个默认行为，即隐式拒绝（implicit deny）。这意味着，如果一个数据包没有匹配到ACL中的任何一条permit语句，它将被默认拒绝，所以我们将从外网和核心层传进的数据设为允许，其它则被显式或隐式拒绝了。

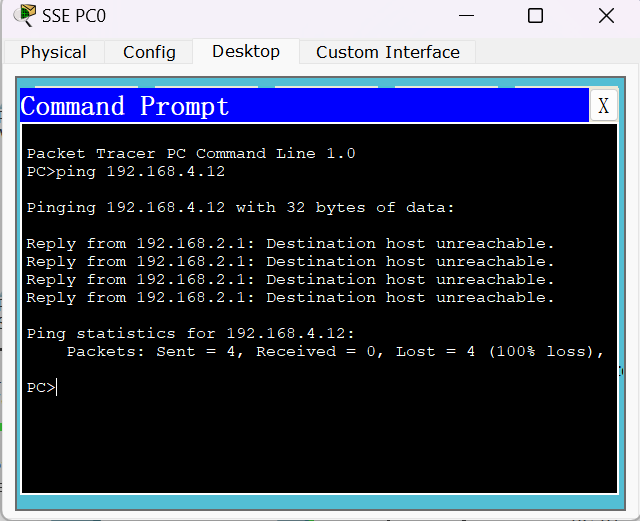


#### 验证access list的配置

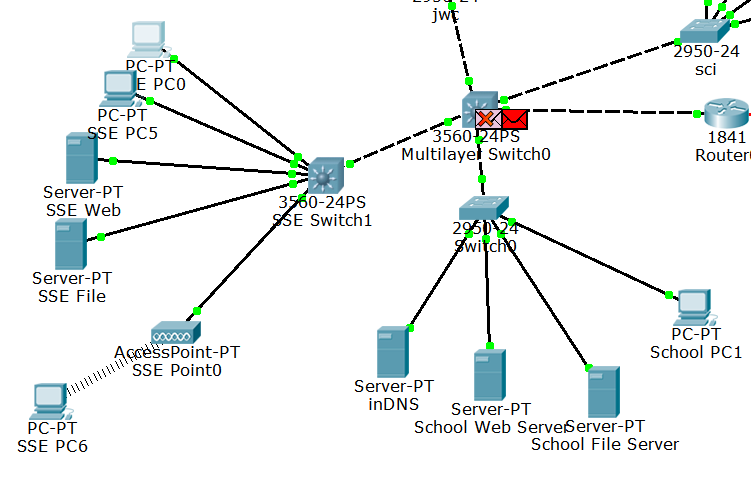
通过show access-list查看该list的内容，从这里我们可以看到从核心层传来的数据和外网传来的数据是被允许通过的。



#### 验证各个部门是否隔离



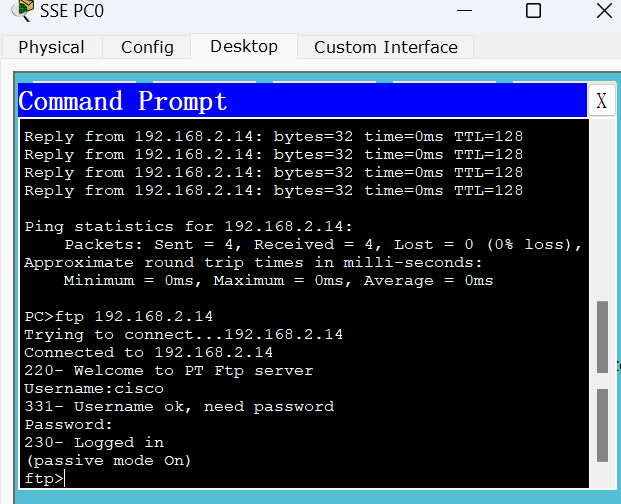
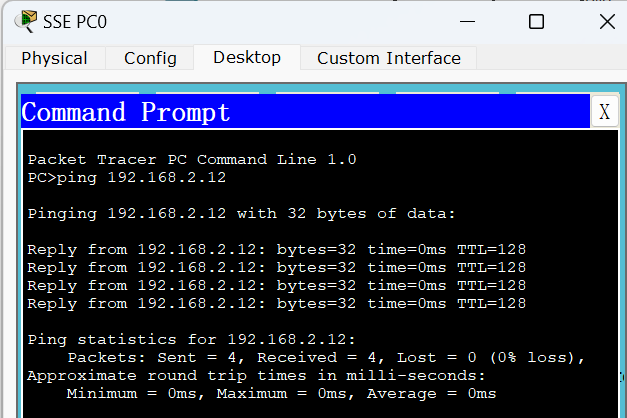
且进行模拟后确实是在核心交换机被拦截。



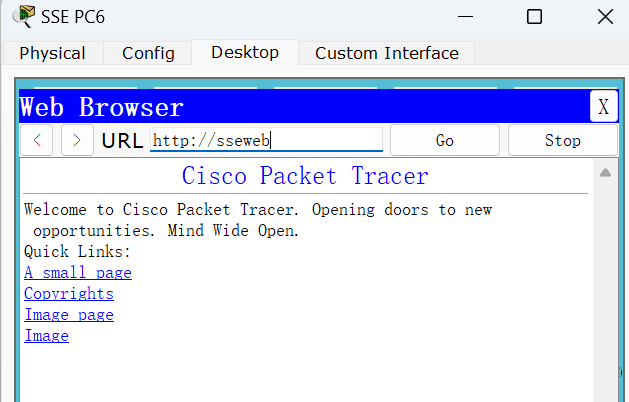
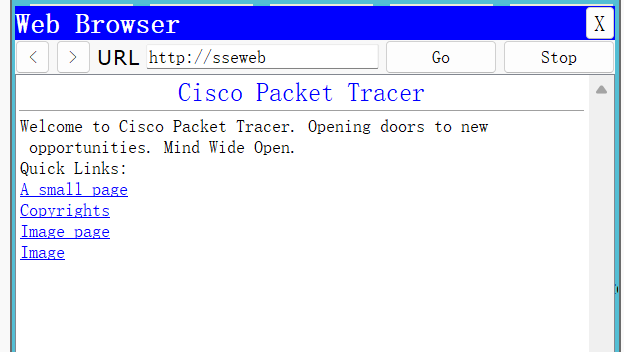
## 六、网络连接测试

#### 软件学院测试

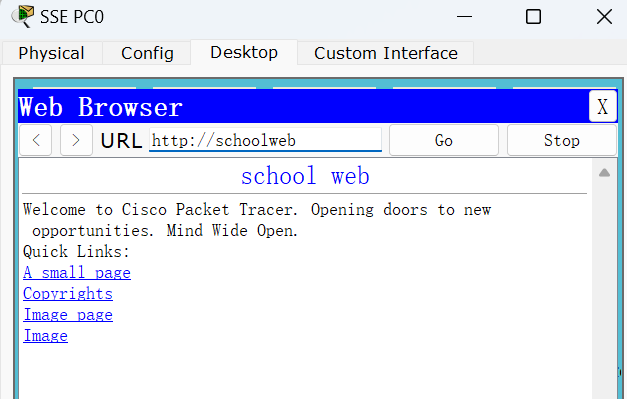
测试VLAN配置成功，PC端可以相互ping通，测试部门内部PC访问部门内File服务器：



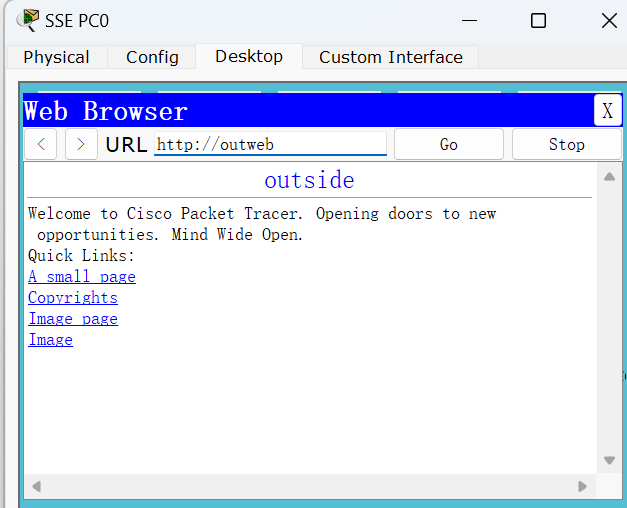
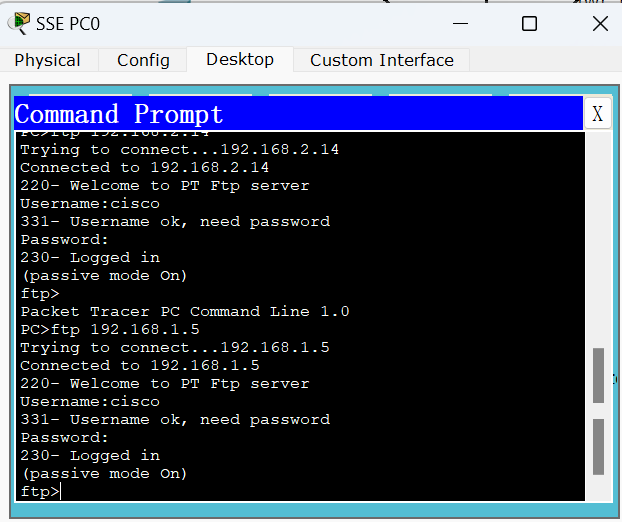
测试部门内部PC可以访问本部门Web服务器，测试连接WIFI的PC端可以访问本部门Web服务器：



测试访问学院官网

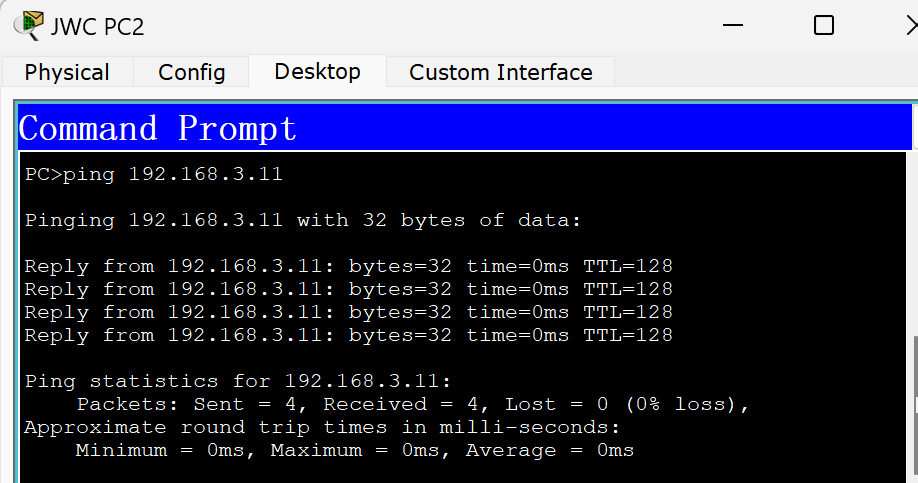


测试访问学院file服务器，测试访问外网：

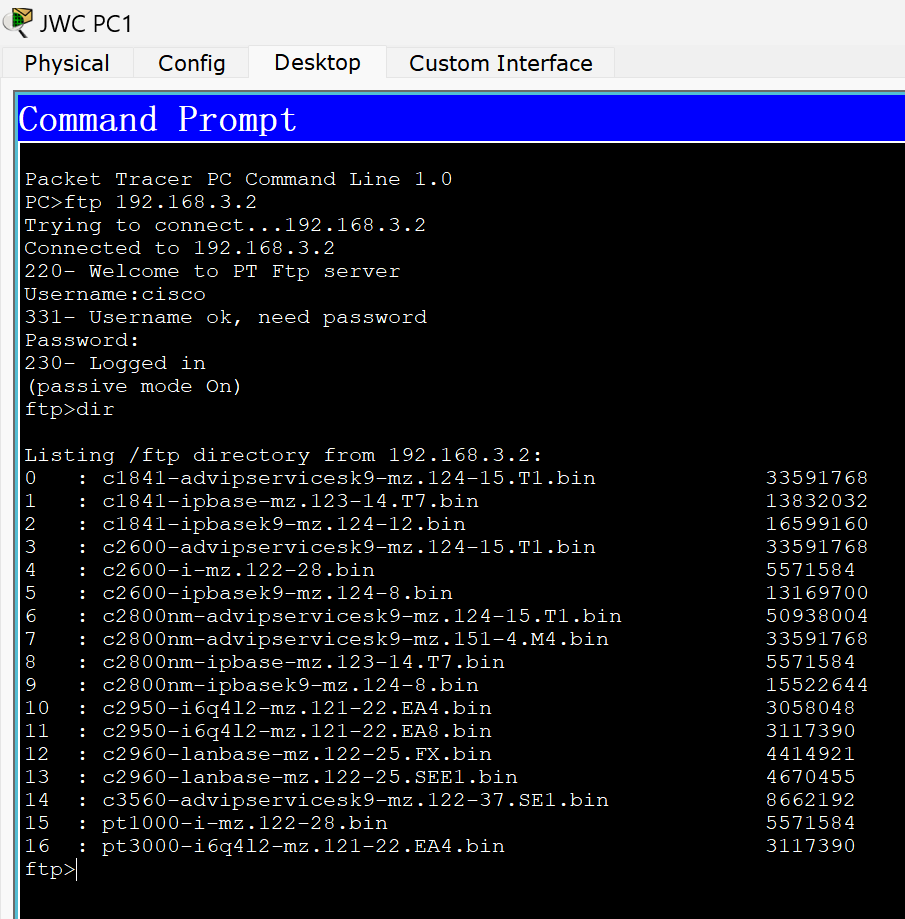


#### 教务部测试

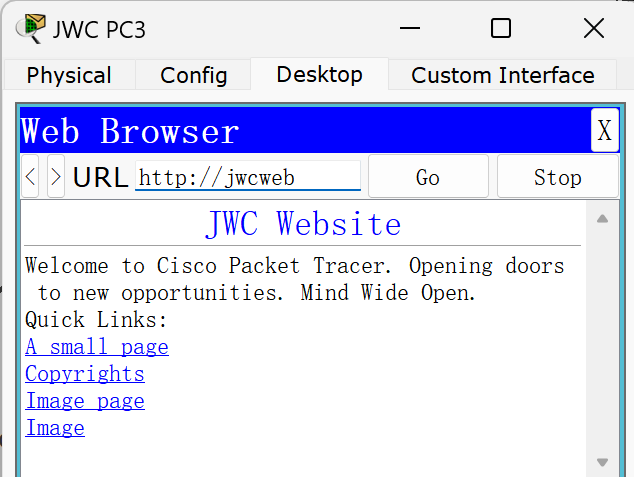
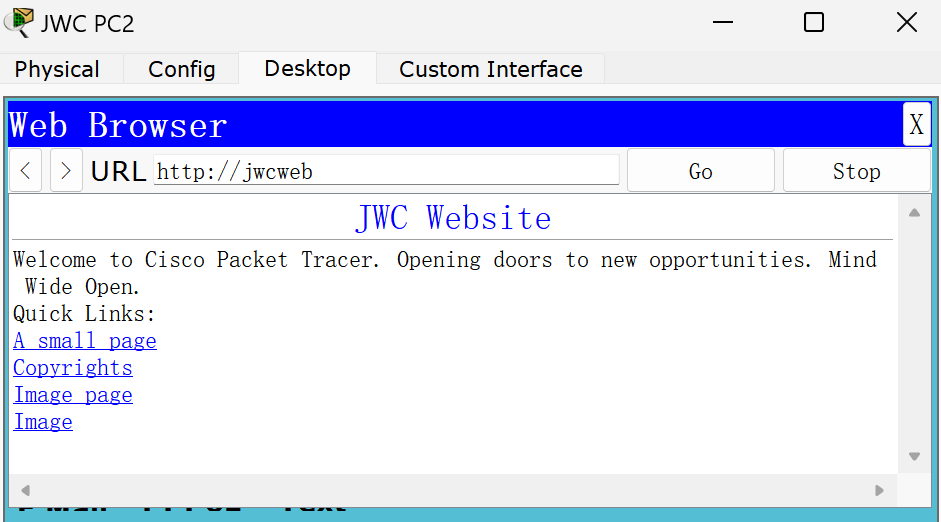
测试VLAN 配置成功，两台PC机可以ping通：



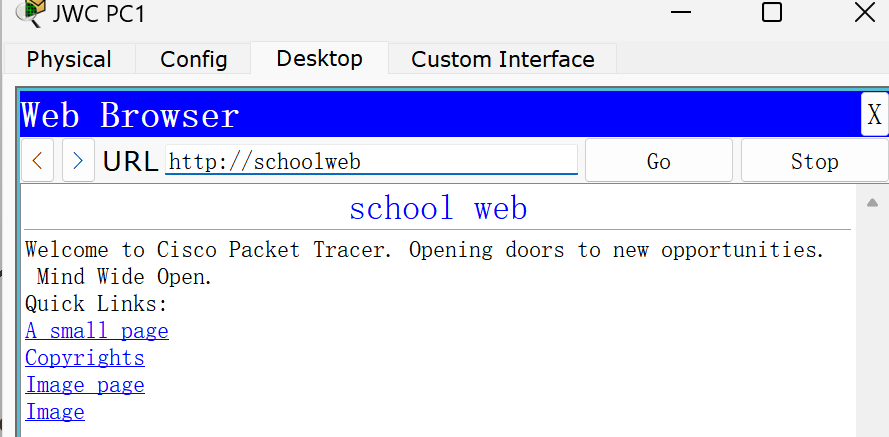
测试部门内部PC可以访问部门File服务器：



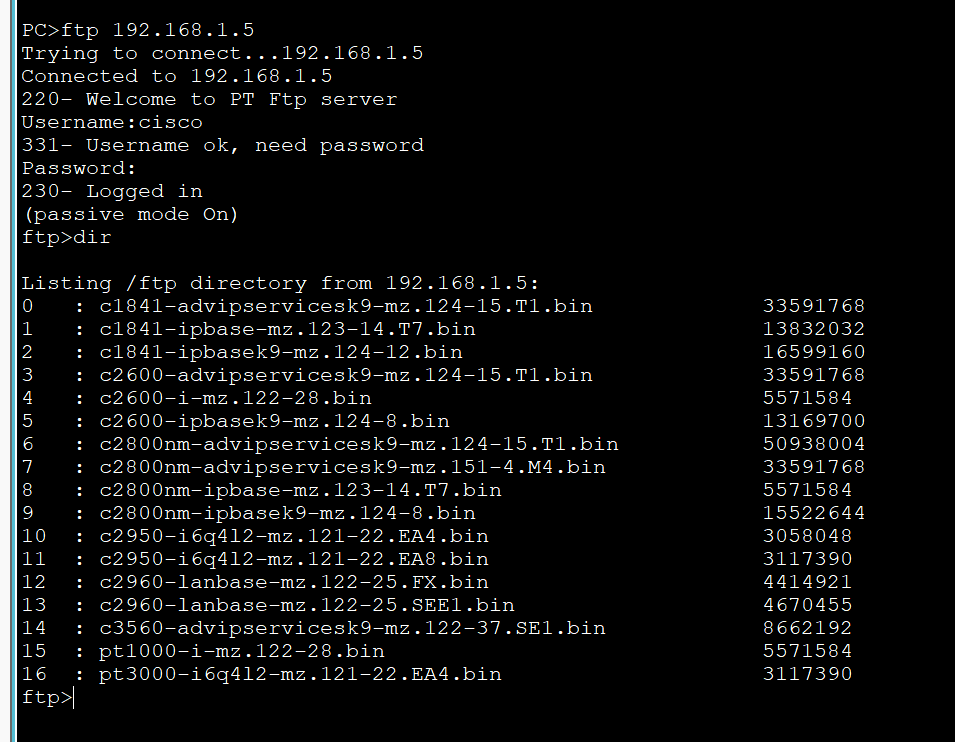
测试部门内部PC可以访问本部门Web服务器：测试连接WIFI的PC3可以访问部门服务器：



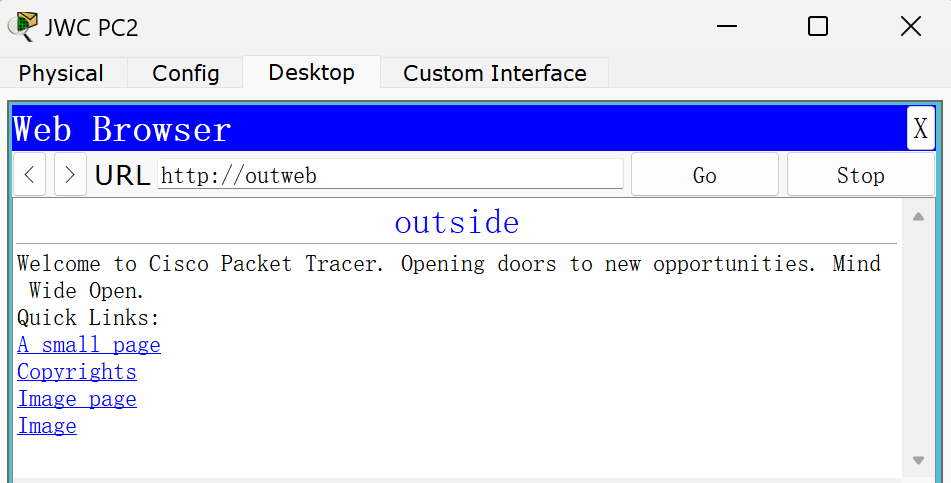
测试访问学院官网：



测试访问学院file服务器：

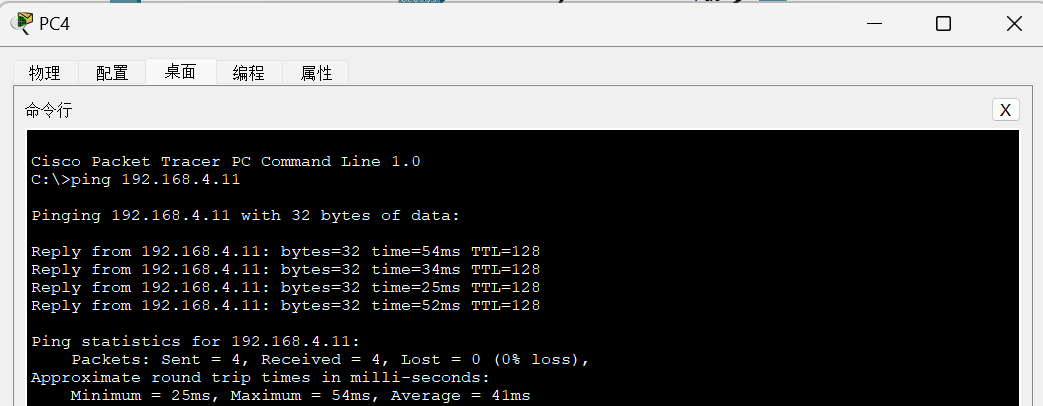


测试访问外网：

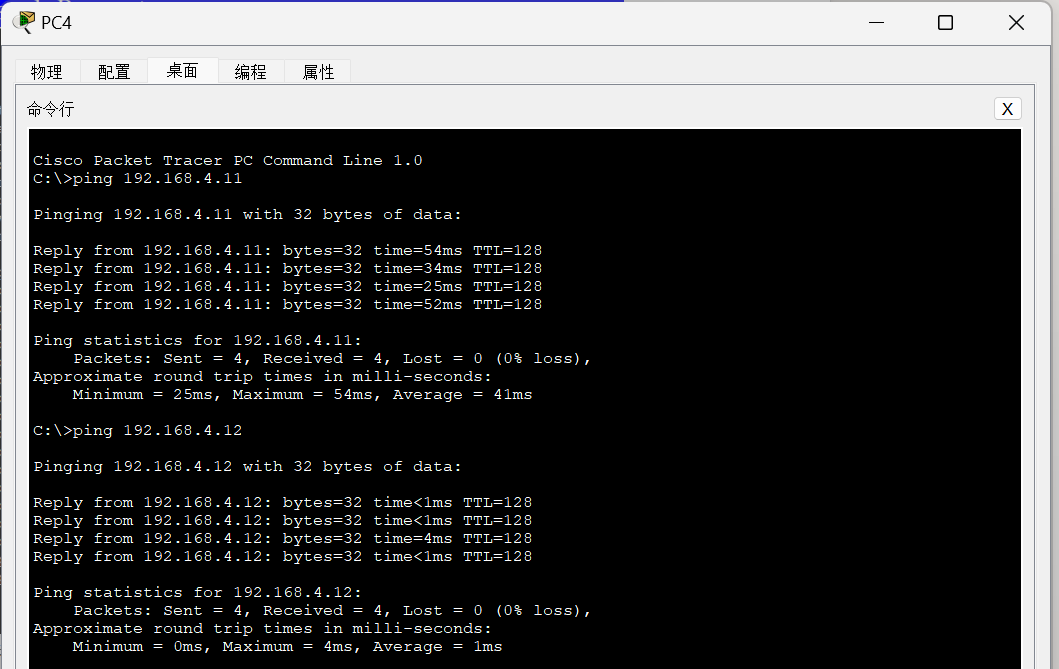


#### 科研部门测试

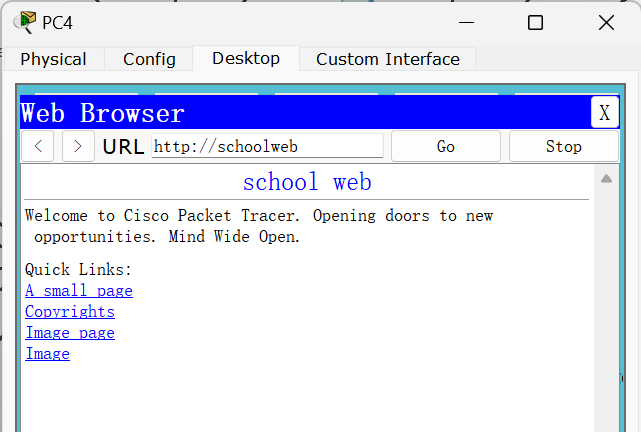
测试VLAN 配置成功，两台主机可以ping通：



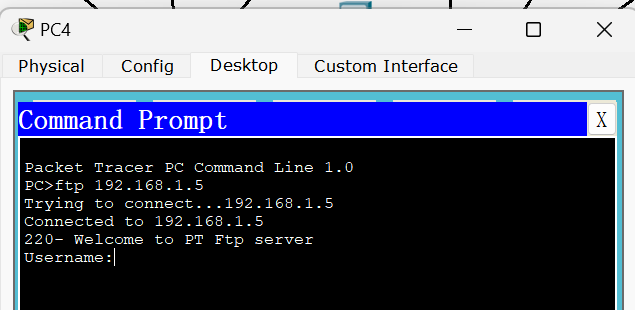
测试部门内部PC可以访问部门File服务器：



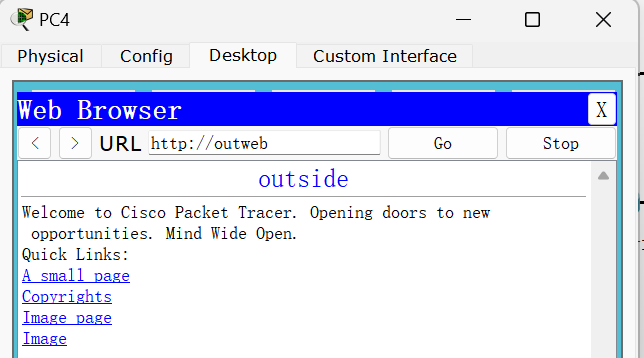
测试访问学院官网：



测试访问学院file服务器：

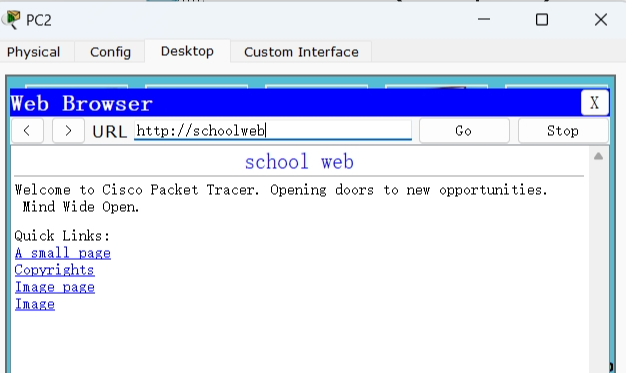


测试访问外网：



#### 外网测试

外网访问学校服务器



#### ACL测试

三部门互相访问

