计算机网络实验报告(2023)

小组成员

2151300 王蔚达

2151298 杨滕超

2151294马威

2152825 李欣

指导教师

夏波涌

1.问题描述

某大学有若干部门，如各个院系，招生部门科研部门教务处、财务部、后勤部、人事部、行政管理部门等。每个部门有自己独立局城网。且有自己的文件服务器和web服务器（内部部门用），几个部门连接成一个大的局城网，并通过学校提供接入到互联网的接口（假如学校有四个公网IP地址(IPV4）） 接入到互联网。学校统一提供一个外网访问的邮件服务器和web服务器，以及一个内部各部门公用的文件服务器。

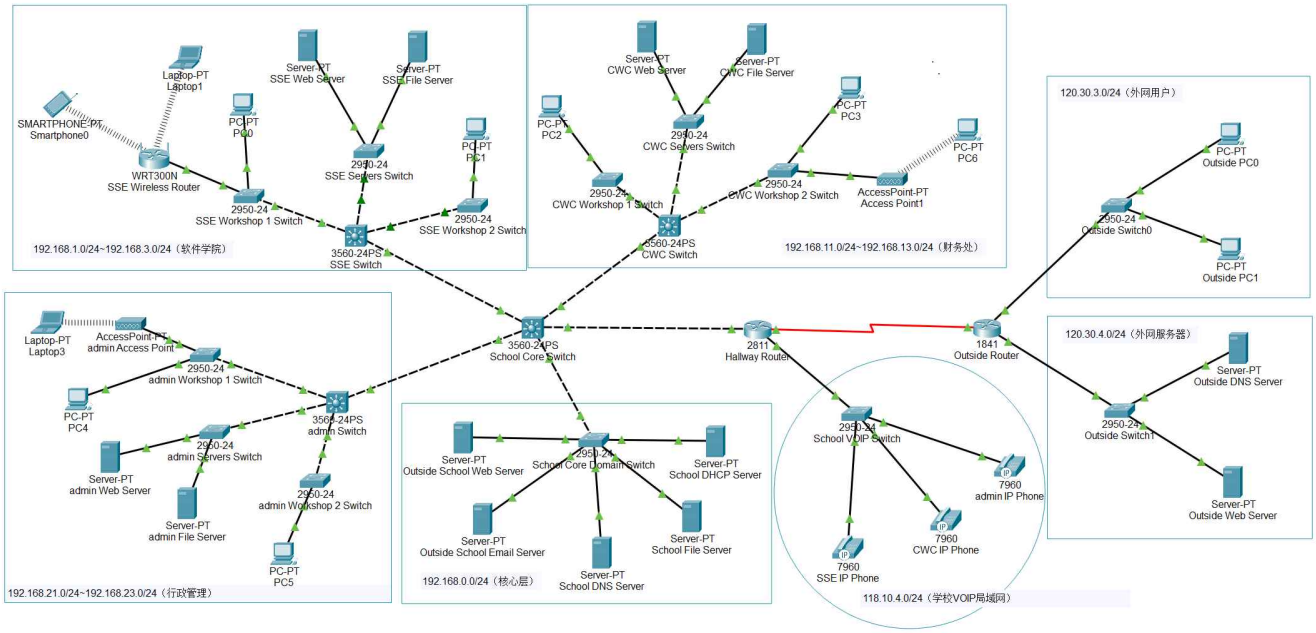
网络提供WIFI接入功能。

每个部门有若干内部独立的局域网。

学校提供VoIP服务。

2.网络拓扑结构

根据项目要求，我们设计如下大学的网络拓扑图：



1. 内网分为核心层以及每个独立部门
2. 核心层中的的E-mail服务器、DHCP服务器、Web服务器、DNS服务器以及File服务器为内网公用，它们是所有部门都可以访问的
3. 对部门而言，一方面与其他部门独立，无法访问别的部门；另一方面，部门内设有多个工作室和两台服务器，
    a. 两台服务器一台是Web服务器，一台是File服务器，部门内公用（部门以外无法访问）
    b. 工作室之间是相互独立的，即workshop 1无法访问workshop 2
    c. 部门内提供了Wifi服务，有无线接入点和无线路由器两种
4. 学校提供IP电话服务，为每一个部门配备IP电话。从需求上看，各部门间电话应当相通，甚至可以访问外网，因此IP电话服务直接由网关路由器（Hallway Router）提供，不接入内网。所以从拓扑上看，电话可能与部门不在一起，但逻辑上每台电话是隶属各部门的
5. 网关路由器（Hallway Router）提供NAT服务
    a. 给内网核心层的Web服务器和邮件服务器配置了公网IP，将这两个服务器开放给外网。外网用户可以通过公网IP访问它们。
    b. 给内网其余设备配备了NAT池，这样可以在公网IP数量有限的情况下，多个内网设备要访问外网而进行NAT转换时，可以进行复用。大学各个部门内部都可以访问公网上的外部Web服务器、DNS服务器等。

3.内网设计

3.1 VLAN配置

在本次计算机网络实验中，我们致力于通过构建虚拟局域网（VLAN）来逻辑上为每个部门建立其独立的局域网。为了实现这一目标，我们选择采用VLAN Trunking Protocol（VTP）协议来简化VLAN的管

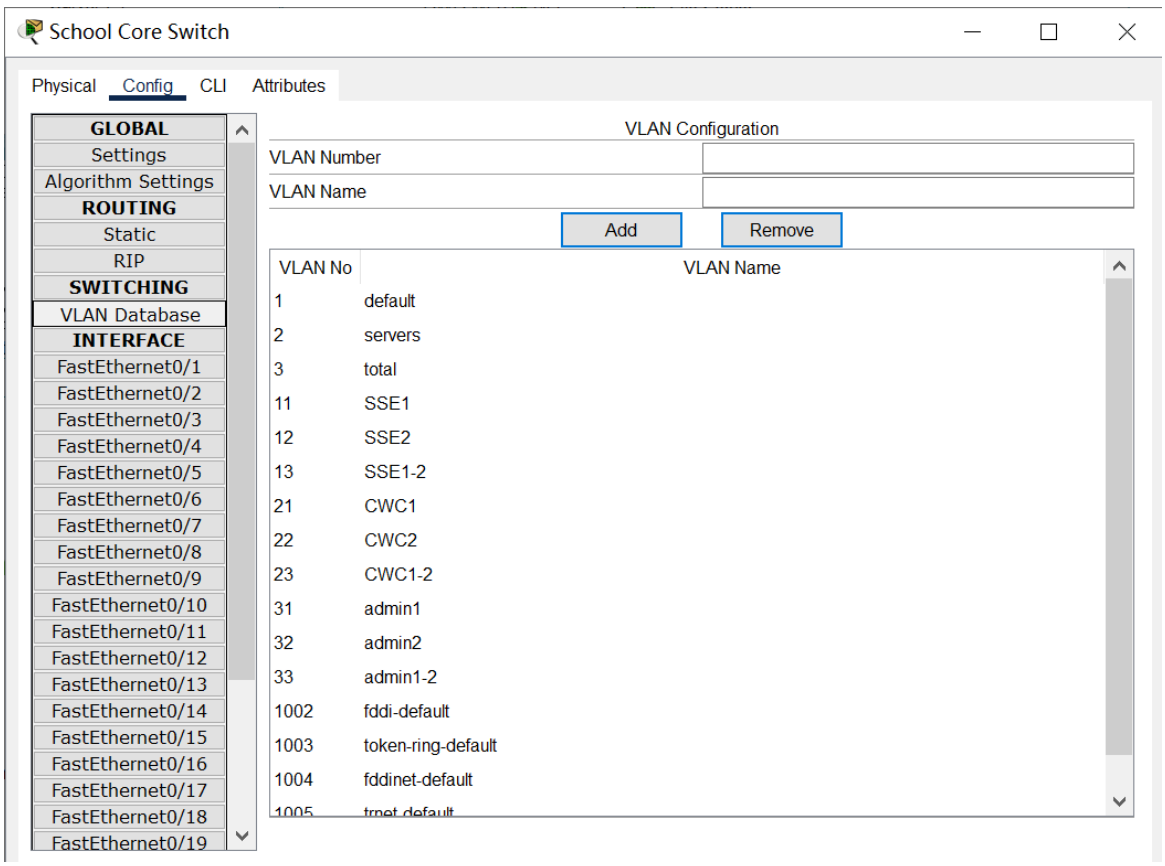
理和配置过程。

首先，我们将核心交换机配置为VTP的服务器server模式，这意味着它将成为VLAN数据库的中央管理点。

```
Switch(vlan)#vtp domain cnlab
Switch(vlan)#vtp server
```

随后，在核心交换机上进行VLAN的配置，这确保了任何新的VLAN或VLAN更改都首先在核心交换机上完成。

在核心交换机处添加VLAN2 'servers'：



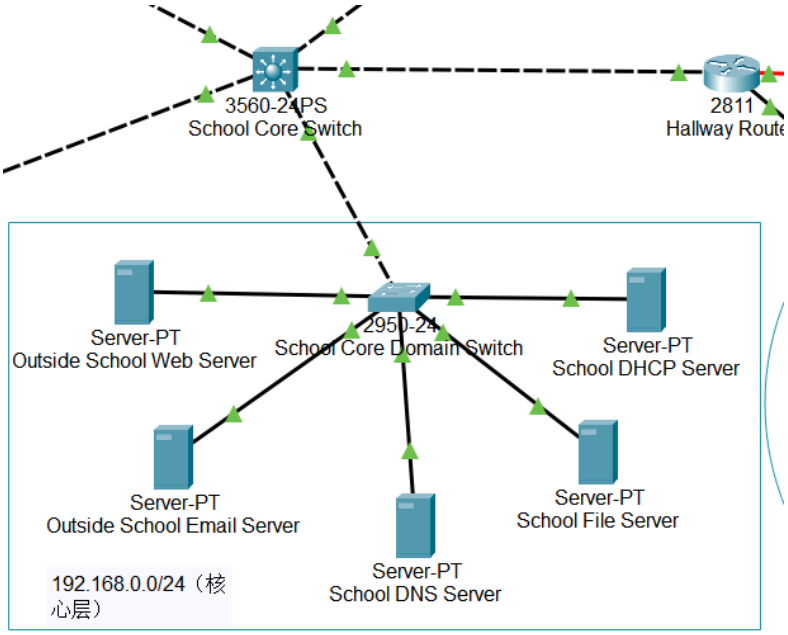
然后，通过将部门交换机配置为VTP的client模式使得它们可以同步所有VLAN

```
Switch(vlan)#vtp domain cnlab
Switch(vlan)#vtp clent
```

一旦在核心交换机上进行了VLAN的配置，VTP服务器将自动将这些更改信息广播给其他VTP客户端模式的交换机。通过这种方式，我们确保了在整个网络中的所有交换机都同步了相同的VLAN信息，从而为各个部门提供了独立且安全的通信环境。

3.2 构建核心层

3.2.1 公共核心网络配置



3.2.2 配置服务器静态地址

由于我们希望能够尽快找到网络核心中的服务器，并且这些服务器相对比较稳定不会随意增加或者删除，因此我们考虑为服务器分配静态地址，分配情况如下表：

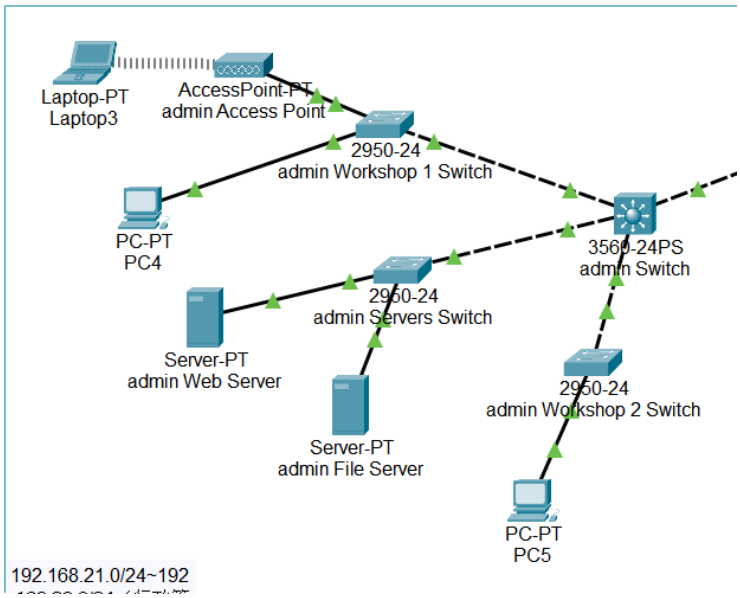
服务器	IP	子网掩码	网关	DNS
School DHCP Server	192.168.0.2	255.255.255.0	192.168.0.1	192.168.0.3
School DNS Server	192.168.0.3	255.255.255.0	192.168.0.1	
Outside School Web Server	192.168.0.4	255.255.255.0	192.168.0.1	192.168.0.3
School File Server	192.168.0.5	255.255.255.0	192.168.0.1	192.168.0.3
Outside School Email Server	192.168.0.6	255.255.255.0	192.168.0.1	192.168.0.3

3.3 各部门网络配置

3.3.1 行政管理部门

行政管理部门作为示例详述，其他部门步骤相似

3.3.1.1 行政管理部拓扑图



3.3.1.2 配置部门VLAN

1. 添加VLAN,对应行政管理部门内部的三个虚拟局域网

31 admin1

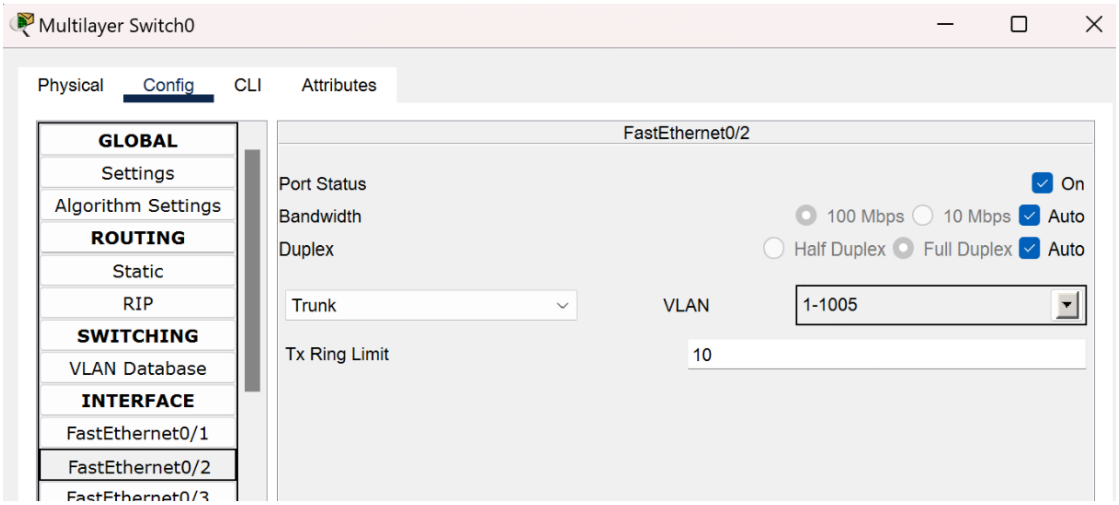
32 admin2

33 admin1-2

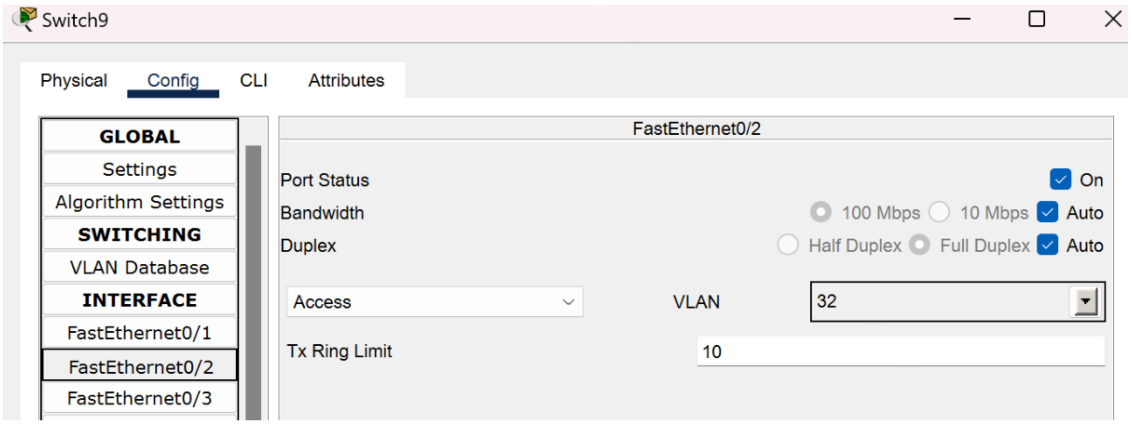
2. 核心交换机上为三个VLAN添加ip地址

VLAN编号	VLAN名称	对应区域	网段	子网掩码
31	admin1	行政管理部工作室1	192.168.21.1	255.255.255.0
32	admin2	行政管理部工作室2	192.168.22.1	255.255.255.0
33	admin1-2	行政管理部服务器	192.168.23.1	255.255.255.0

3. 将核心交换机到部门总交换机，部门总交换机到部门分交换机的接口设置为Trunk



4. 将部门分交换机到终端的接口设置为Access,并选择对应VLAN



3.3.1.3 配置ACL

ACL的主要作用是允许或拒绝通过设备的流量，以实现对网络资源的保护和管理

对于服务器VLAN（即VLAN33)

- 允许部门内的 VLAN (VLAN31, VLAN32) 访问
- 拒绝公司内部其他 VLAN 访问

配置如下

```
Switch(config-if)#exit
Switch(config)#access-list 133 permit ip 192.168.21.0 0.0.0.255 192.168.23.0 0.0.0.255
Switch(config)#access-list 133 permit ip 192.168.22.0 0.0.0.255 192.168.23.0 0.0.0.255
Switch(config)#access-list 133 deny ip 192.168.0.0 0.0.255.255 192.168.23.0 0.0.0.255
Switch(config)#access-list 133 permit ip any any
Switch(config)#int vlan 33
Switch(config-if)#ip access-group 133 in
Switch(config-if)#ip access-group 133 out
Switch(config-if)#exit
Switch(config)#exit
```

对于不同工作室

- 允许部门服务器 (VLAN33) 访问
- 允许公司服务器访问
- 拒绝公司内部其他 VLAN 访问

- 允许外部访问
- 配置如下

```
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#access-list 131 permit ip 192.168.23.0 0.0.0.255 192.168.21.0 0.0.0.255
Switch(config)#access-list 131 permit ip 192.168.0.0 0.0.0.255 192.168.21.0 0.0.0.255
Switch(config)#access-list 131 deny ip 192.168.0.0 0.0.255.255 192.168.21.0 0.0.0.255
Switch(config)#access-list 131 permit ip any any
Switch(config)#int vlan 31
Switch(config-if)#ip access-group 131 in
Switch(config-if)#ip access-group 131 out
Switch(config-if)#exit
Switch(config)#access-list 132 permit ip 192.168.23.0 0.0.0.255 192.168.22.0 0.0.0.255
Switch(config)#access-list 132 permit ip 192.168.0.0 0.0.0.255 192.168.22.0 0.0.0.255
Switch(config)#access-list 132 deny ip 192.168.0.0 0.0.255.255 192.168.22.0 0.0.0.255
Switch(config)#access-list 132 permit ip any any
Switch(config)#int vlan 32
Switch(config-if)#ip access-group 132 in
Switch(config-if)#ip access-group 132 out
Switch(config-if)#exit
Switch(config)#access-list 133 permit ip 192.168.21.0 0.0.0.255 192.168.23.0 0.0.0.255
Switch(config)#access-list 133 permit ip 192.168.22.0 0.0.0.255 192.168.23.0 0.0.0.255
Switch(config)#access-list 133 deny ip 192.168.0.0 0.0.255.255 192.168.23.0 0.0.0.255
Switch(config)#access-list 133 permit ip any any
```

3.3.1.4 配置DHCP

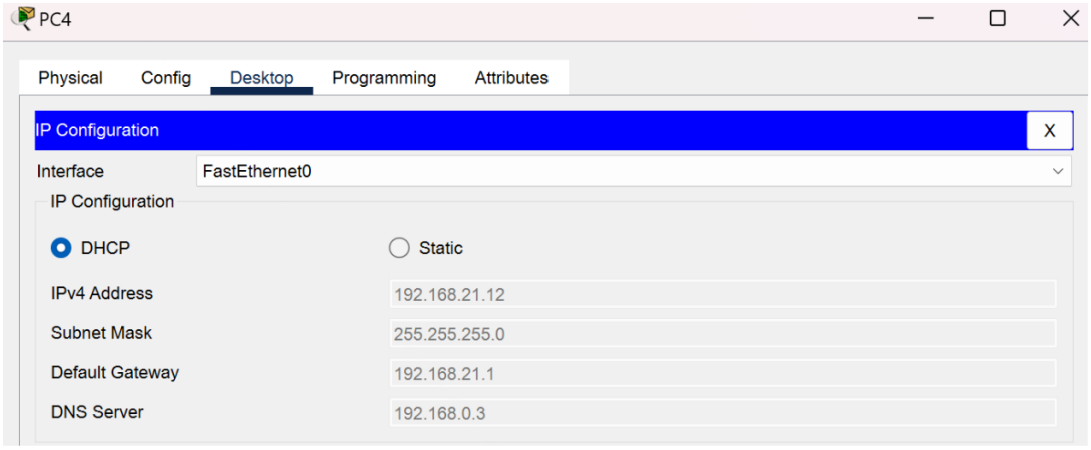
在学校服务器集群中的DHCP服务器中为每个VLAN配置DHCP池

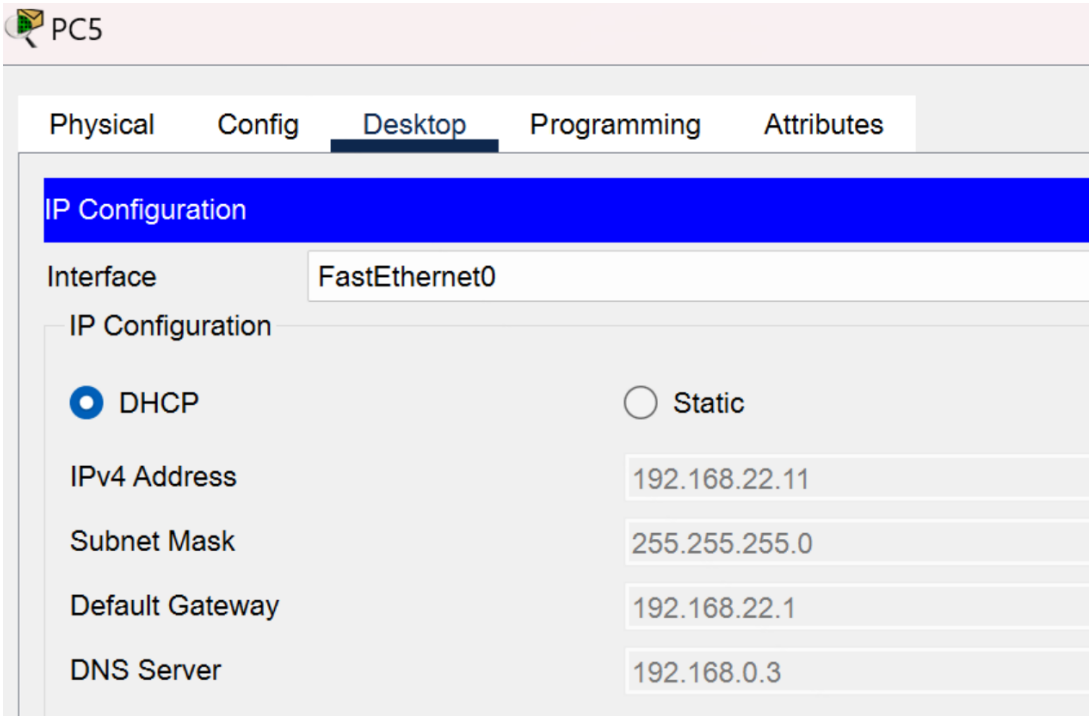
admin1-2Pool	192.168.23.1	192.168.0.3	192.168.23.11	255.255.255.0	245	0.0.0.0	0.0.0.0
admin2Pool	192.168.22.1	192.168.0.3	192.168.22.11	255.255.255.0	245	0.0.0.0	0.0.0.0
admin1Pool	192.168.21.1	192.168.0.3	192.168.21.11	255.255.255.0	245	0.0.0.0	0.0.0.0

在核心交换机将VLAN 启用了 DHCP中继功能：

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 31
Switch(config-if)#ip helper-address 192.168.0.2
Switch(config-if)#exit
Switch(config)#int vlan 32
Switch(config-if)#ip helper-address 192.168.0.2
Switch(config-if)#exit
Switch(config)#int vlan 33
Switch(config-if)#ip helper-address 192.168.0.2
Switch(config-if)#exit
Switch(config)#ip routing
```

开启不同工作室终端中的DHCP服务





可以看到自动分配了IP地址，并有合适的网关，掩码和DNS服务器

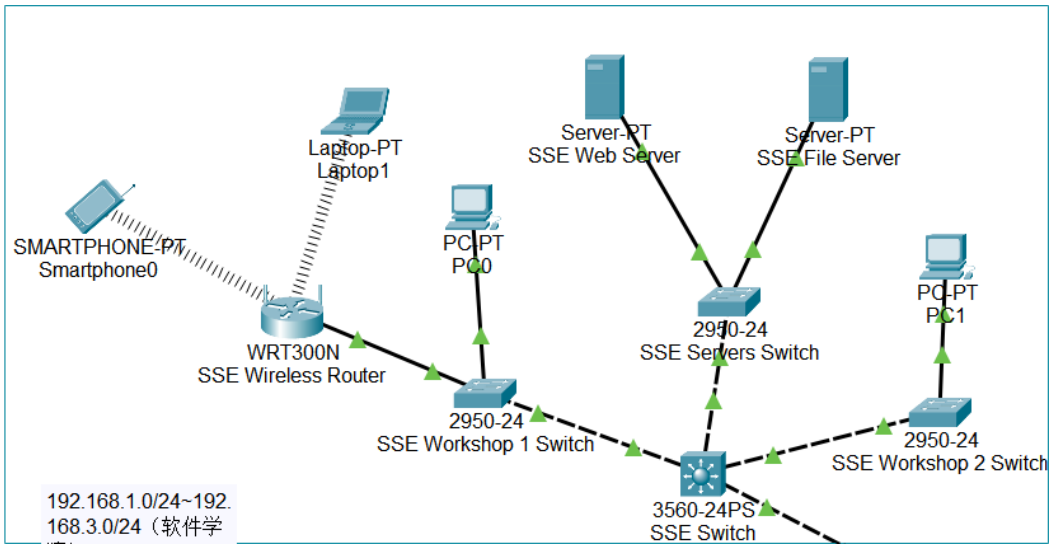
3.3.1.5 静态配置部门服务器

服务器不会轻易改变，则设置为静态

服务器	IP	子网掩码	网关	DNS
admin Web Server	192.168.23.16	255.255.255.0	192.168.23.1	192.168.0.3
admin File Server	192.168.23.25	255.255.255.0	192.168.23.1	192.168.0.3

3.3.2 软件学院

3.3.2.1 软件学院拓扑图



3.3.2.2 配置部门VLAN

VLAN编号	VLAN名称	对应区域	网段	子网掩码
11	SSE1	软件学院工作室1	192.168.21.1	255.255.255.0
12	SSE2	软件学院工作室2	192.168.2.1	255.255.255.0
13	SSE1-2	软件学院服务器	192.168.3.1	255.255.255.0

3.3.2.3 配置ACL

该部门全部ACL配置如下：

```
Extended IP access list 112
    10 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
    20 permit ip 192.168.0.0 0.0.0.255 192.168.2.0 0.0.0.255 (2 match(es))
    30 deny ip 192.168.0.0 0.0.255.255 192.168.2.0 0.0.0.255
    40 permit ip any any (2 match(es))
Extended IP access list 113
    10 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
    20 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
    30 deny ip 192.168.0.0 0.0.255.255 192.168.3.0 0.0.0.255 (4 match(es))
    40 permit ip any any
Extended IP access list 111
    10 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
    20 permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255 (2 match(es))
    30 deny ip 192.168.0.0 0.0.255.255 192.168.1.0 0.0.0.255 (4 match(es))
    40 permit ip any any (2 match(es))
```

3.3.2.4 配置DHCP

该部门所有DHCP池配置如下

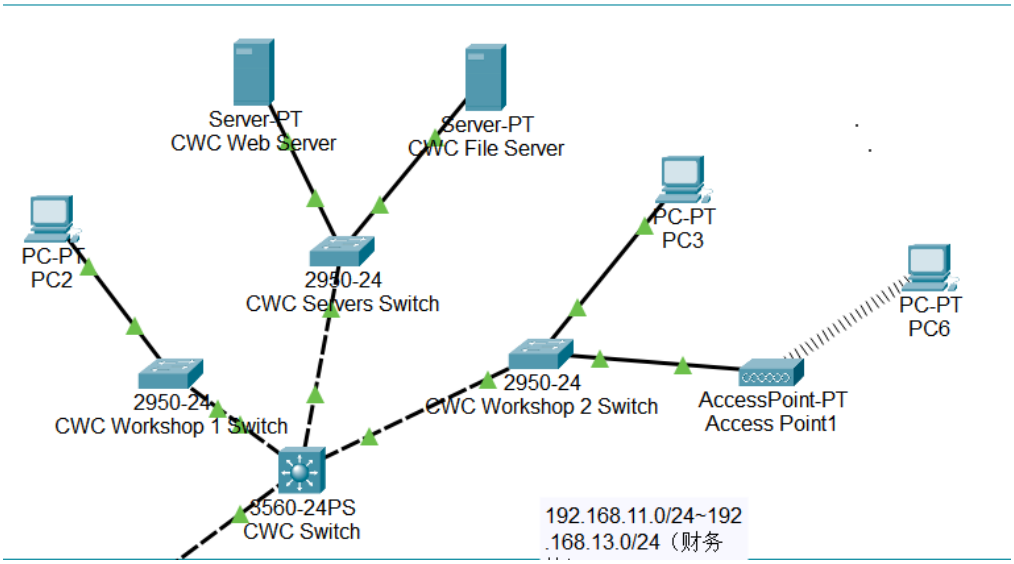
SSE1-2Pool	192.168.3.1	192.168.0.3	192.168.3.11	255.255.255.0	245	0.0.0.0	0.0.0.0
SSE2Pool	192.168.2.1	192.168.0.3	192.168.2.11	255.255.255.0	245	0.0.0.0	0.0.0.0
SSE1Pool	192.168.1.1	192.168.0.3	192.168.1.11	255.255.255.0	245	0.0.0.0	0.0.0.0

3.3.2.5 静态配置部门服务器

服务器	IP	子网掩码	网关	DNS
SSE Web Server	192.168.3.16	255.255.255.0	192.168.3.1	192.168.0.3
SSE File Server	192.168.3.25	255.255.255.0	192.168.3.1	192.168.0.3

3.3.3 财务部

3.3.3.1 财务部拓扑图



3.3.3.2 配置部门VLAN

VLAN编号	VLAN名称	对应区域	网段	子网掩码
21	CWC1	财务部工作室1	192.168.11.1	255.255.255.0
22	CWC2	财务部工作室2	192.168.12.1	255.255.255.0
23	CWC1-2	财务部服务器	192.168.13.1	255.255.255.0

3.3.3.3 配置ACL

该部门全部ACL配置如下：

```
Extended IP access list 121
    10 permit ip 192.168.13.0 0.0.0.255 192.168.11.0 0.0.0.255
    20 permit ip 192.168.0.0 0.0.0.255 192.168.11.0 0.0.0.255
    30 deny ip 192.168.0.0 0.0.255.255 192.168.11.0 0.0.0.255
    40 permit ip any any (15 match(es))
Extended IP access list 122
    10 permit ip 192.168.13.0 0.0.0.255 192.168.12.0 0.0.0.255
    20 permit ip 192.168.0.0 0.0.0.255 192.168.12.0 0.0.0.255
    30 deny ip 192.168.0.0 0.0.255.255 192.168.12.0 0.0.0.255 (4 match(es))
    40 permit ip any any (2 match(es))
Extended IP access list 123
    10 permit ip 192.168.11.0 0.0.0.255 192.168.13.0 0.0.0.255
    20 permit ip 192.168.12.0 0.0.0.255 192.168.13.0 0.0.0.255
    30 deny ip 192.168.0.0 0.0.255.255 192.168.13.0 0.0.0.255
    40 permit ip any any
```

3.3.3.4 配置DHCP

该部门所有DHCP池配置如下

CWC1-2Pool	192.168.13.1	192.168.0.3	192.168.13.11	255.255.255.0	245	0.0.0.0	0.0.0.0
CWC2Pool	192.168.12.1	192.168.0.3	192.168.12.11	255.255.255.0	245	0.0.0.0	0.0.0.0
CWC1Pool	192.168.11.1	192.168.0.3	192.168.11.11	255.255.255.0	245	0.0.0.0	0.0.0.0

3.3.3.4 静态配置部门服务器

服务器	IP	子网掩码	网关	DNS
CWC Web Server	192.168.13.16	255.255.255.0	192.168.13.1	192.168.0.3
CWC File Server	192.168.13.25	255.255.255.0	192.168.13.1	192.168.0.3

3.4 ACL访问控制

访问控制列表ACL（Access Control List）是由一条或多条规则组成的集合，规则又包括报文的形式、源地址、目的地址、端口号等。将一个ACL应用在端口上，端口就可以根据规则对报文进行过滤，从而达到访问控制的目的。

就本项目中而言，学校内每个部门内部的ACL控制遵循以下原则：

1. 对于工作室
    a. 部门服务器可以访问
    b. 核心层可以访问
    c. 其它VLAN均不可访问
2. 对于部门服务器
    a. 部门内的工作室可以访问
    b. 其它VLAN均不可访问

以软件学院工作室1为例，其配置如下（在School Core Switch上查看）：

```
Switch#show access-lists
Extended IP access list 112
    10 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
    20 permit ip 192.168.0.0 0.0.0.255 192.168.2.0 0.0.0.255 (2 match(es))
    30 deny ip 192.168.0.0 0.0.255.255 192.168.2.0 0.0.0.255
    40 permit ip any any (3 match(es))
Extended IP access list 113
    10 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
    20 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255
    30 deny ip 192.168.0.0 0.0.255.255 192.168.3.0 0.0.0.255
    40 permit ip any any
Extended IP access list 111
    10 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
    20 permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255 (10 match(es))
    30 deny ip 192.168.0.0 0.0.255.255 192.168.1.0 0.0.0.255
    40 permit ip any any (17 match(es))
```

含义如下：

1. permit ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255：允许从网段192.168.3.0/24（软件学院服务器）的数据包到网段192.168.1.0/24（软件学院工作室1）
2. permit ip 192.168.0.0 0.0.0.255 192.168.1.0 0.0.0.255：允许从网段192.168.0.0/24（核心层）的数据包到网段192.168.1.0/24（软件学院工作室1）
3. deny ip 192.168.0.0 0.0.255.255 192.168.1.0 0.0.0.255：不允许从网段192.168.0.0/16（学校内网各vlan）的数据包到网段192.168.1.0/24（软件学院工作室1）
4. permit ip any any：允许所有数据包通过

查看School Core Switch的配置发现vlan 11正在使用上述的访问控制列表111（特权模式下show running-config指令查看）：

```
!
interface Vlan2
 mac-address 000c.852e.ca01
 ip address 192.168.0.1 255.255.255.0
!
interface Vlan3
 mac-address 000c.852e.ca02
 ip address 192.168.100.1 255.255.255.0
!
interface Vlan11
 mac-address 000c.852e.ca03
 ip address 192.168.1.1 255.255.255.0
 ip helper-address 192.168.0.2
 ip access-group 111 in
 ip access-group 111 out
!
```

in表明进入该vlan的数据包使用111内的规则，显然使用了前三条

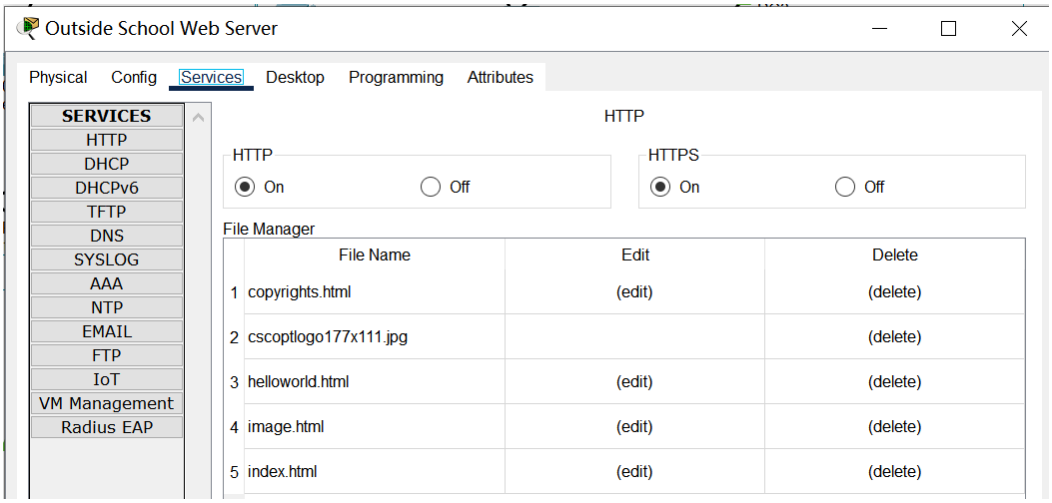
out表明从该vlan出发的数据包使用111内的规则，应该是应用了最后一条，让该vlan内的数据包可以自由发送

其它部门中的vlan配置在上文各部门网络配置中已经提到

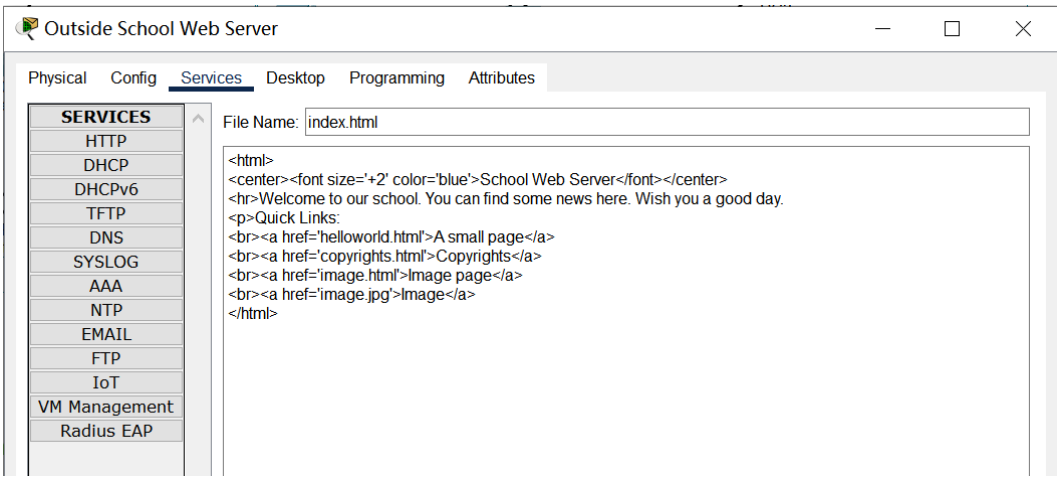
P.S. 在项目刚进行时，我们只配置了vlan而没有配置ACL，惊讶地发现各vlan可以互通。按道理，交换机分了不同的vlan应该是不能互通的。但在学习了三层交换机的功能后，我们发现，三层交换机已“进化”成了路由器（详见4.1），而之前实验中，连接在同一路由器上的不同网段是不用进行路由的，因为下一跳就是路由器自己，因此可以相通。现在这个情况就是类似的，分了多个网段到头来连到同一个路由器上了，当然会互通了。而为了满足设计要求，ACL的配置完美地解决了这个问题。

3.5 Web服务

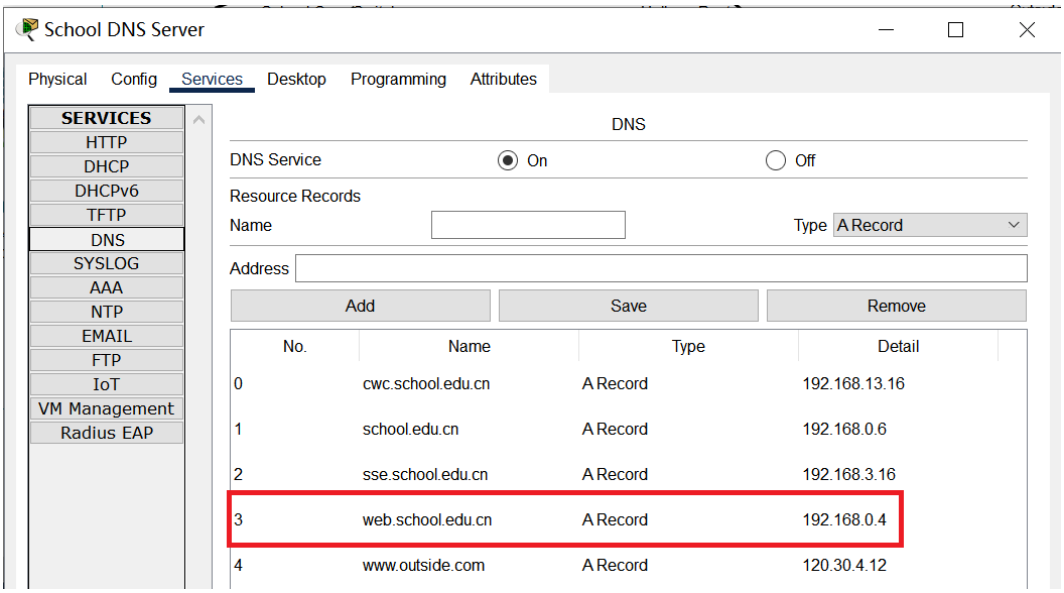
在核心层Web服务器处选择Services-HTTP，开启http和https：

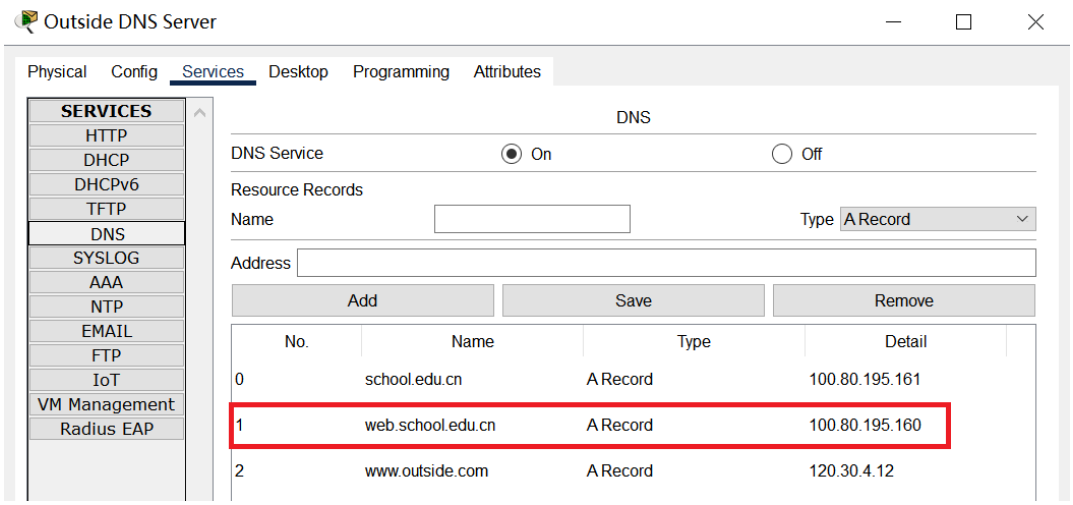


修改index.html以更改主页，方便后续测试：



在内网公用和外网DNS服务器处记录Web服务器的IP与对应的域名（外网DNS要记录公网IP）：

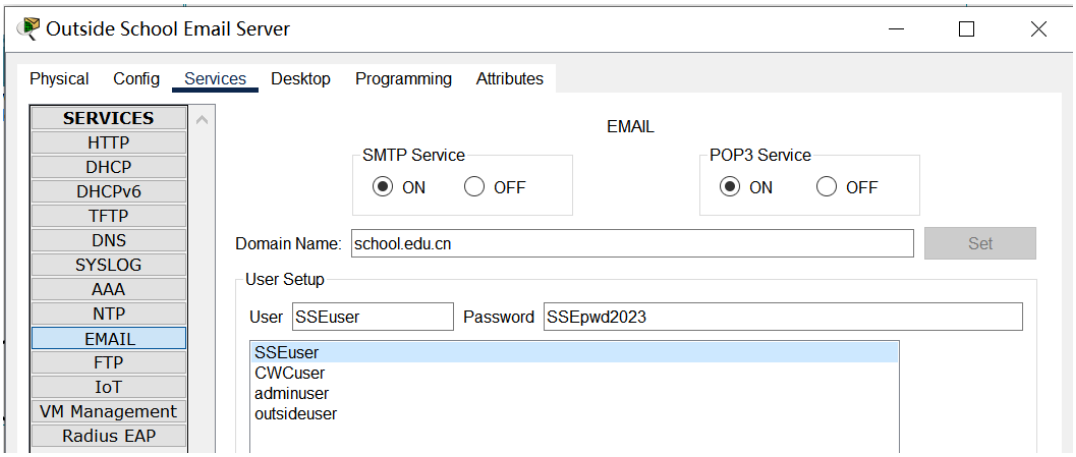




部门内用Web服务器类似，只是由于不开放给公网，无需在外网DNS服务器记录域名和IP

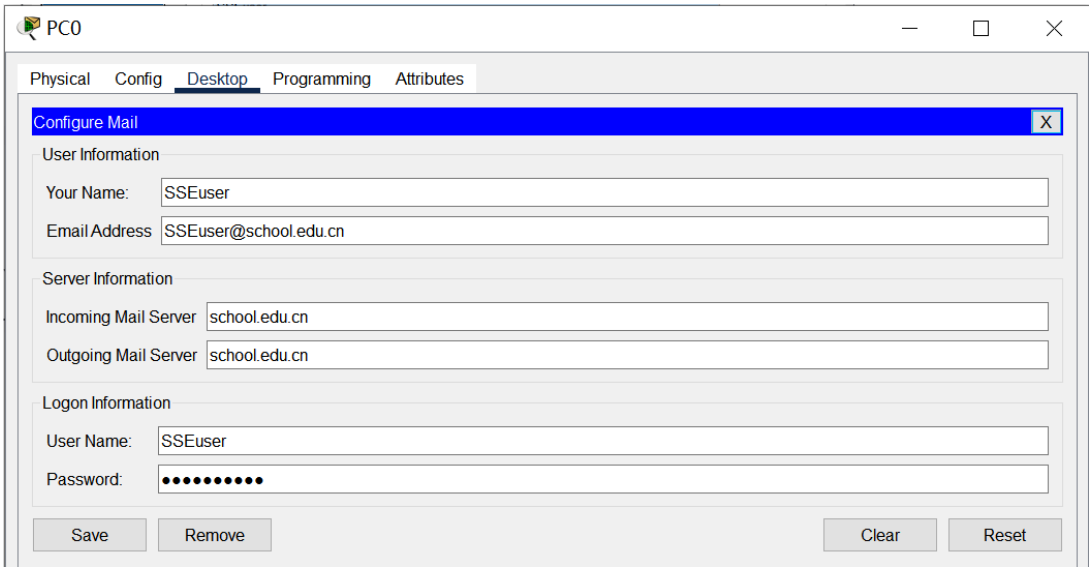
3.6 Email服务

在核心层Email服务器处选择Services-EMAIL，开启SMTP和POP3，设置域名（自取），然后配若干邮箱用户的用户名及密码：

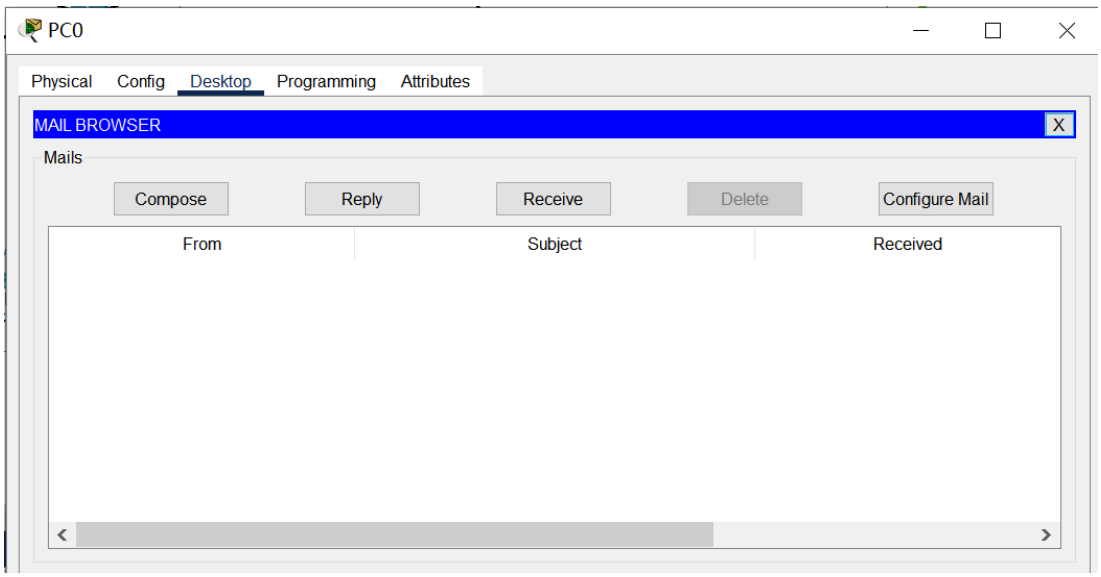


用户登录时，进入PC的Desktop-Email，从上到下配置项为：

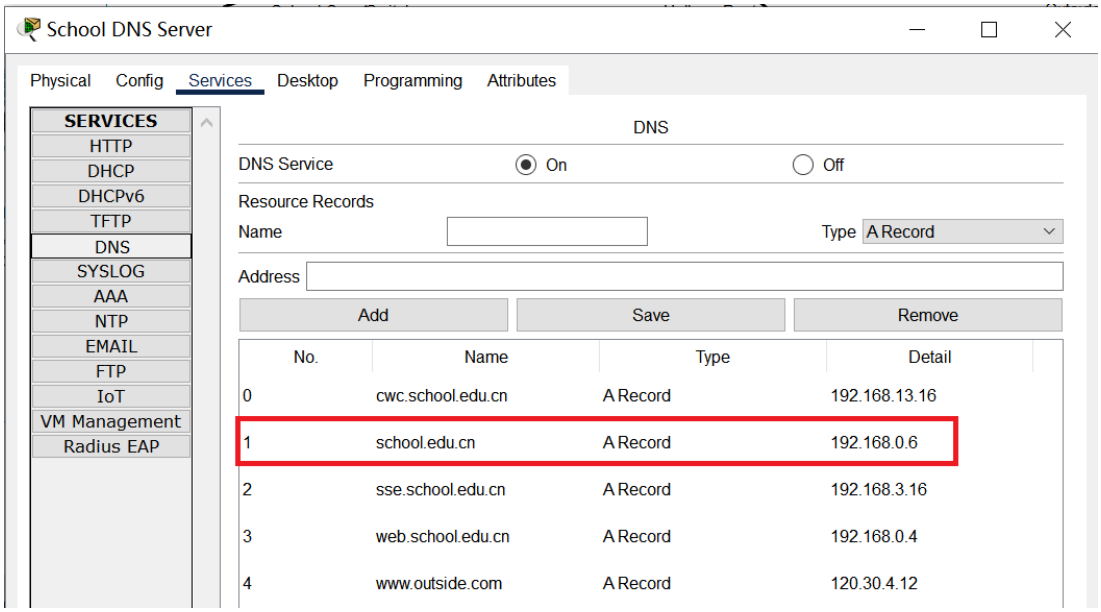
1. 名字：和用户名一致
2. 邮箱地址：名字@域名
3. 邮件客户端：域名（如果没配DNS就是Email服务器的IP）
4. 转发邮件服务器：域名（如果没配DNS就是Email服务器的IP）
5. 用户名：与Email服务器中配置一致
6. 密码：与Email服务器中配置一致

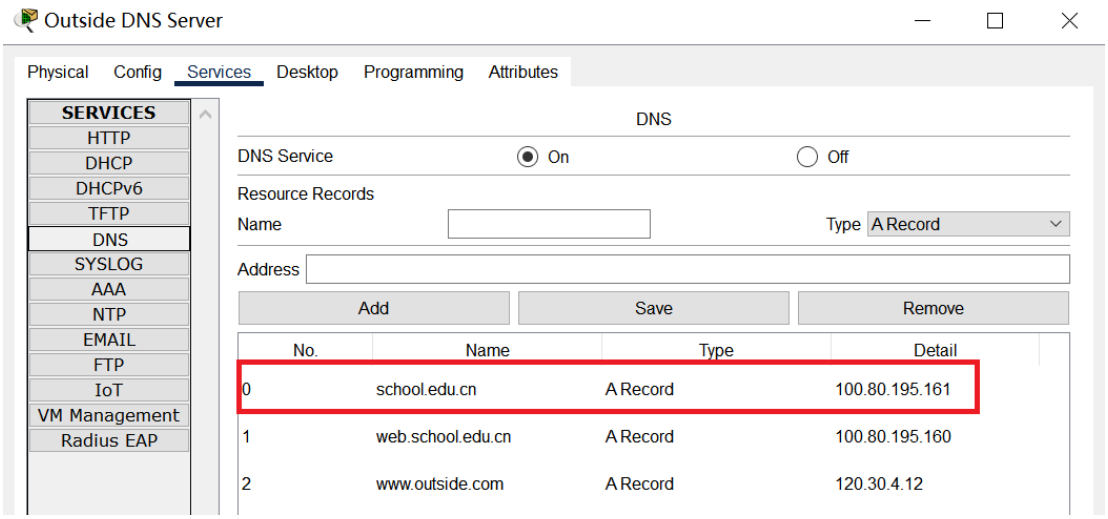


配置完成后点击Save，就可以进行邮件相应操作了：



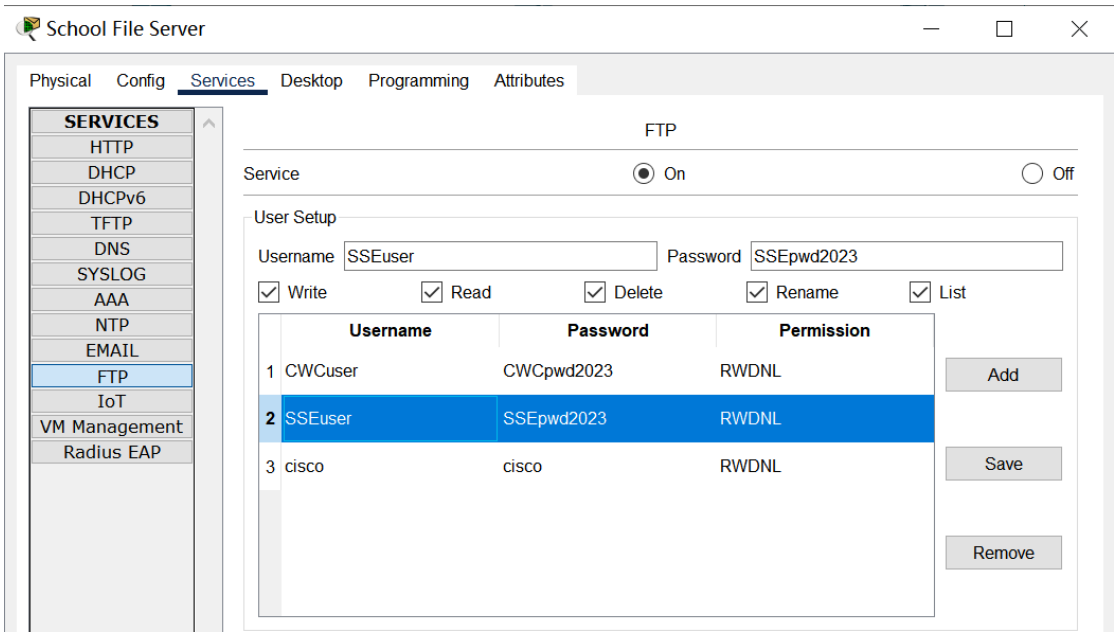
在内网公用和外网DNS服务器处记录Email服务器的IP与对应的域名（外网DNS要记录公网IP，而且域名要与Email服务器配置时的那个域名一致）：





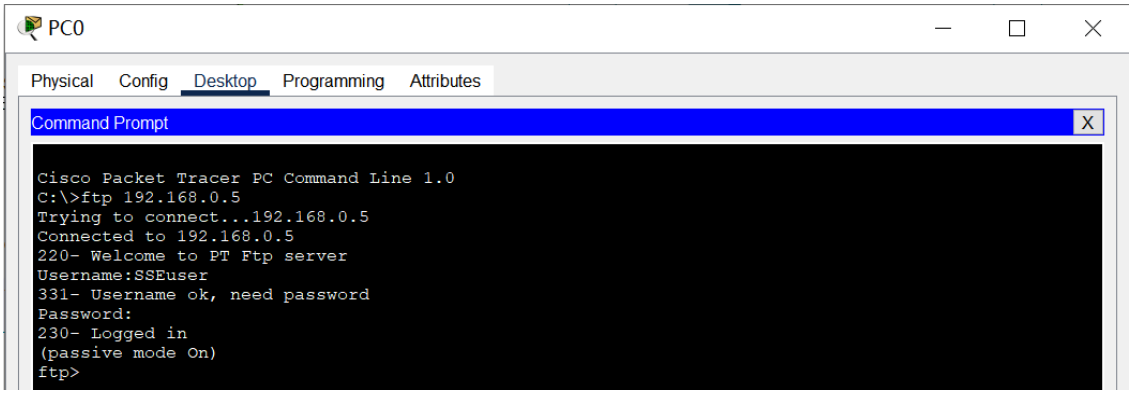
3.7 FTP服务

在核心层File服务器上选择Services-FTP，开启FTP服务，然后配若干邮箱用户的用户名、密码和文件访问权限：



从实际出发，许多高校学院的文件服务器直接通过IP访问，因此不在此配备域名。

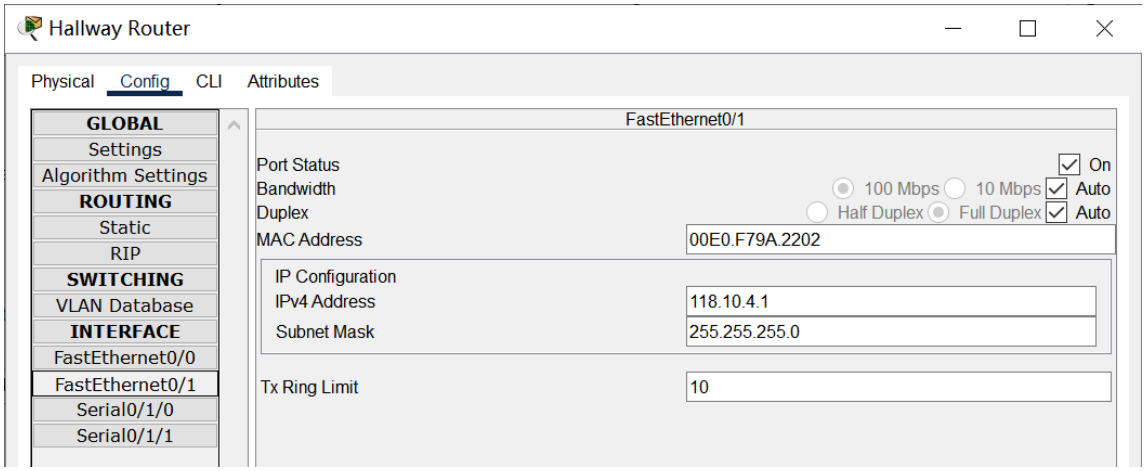
访问时进入PC的命令行，使用ftp指令访问File服务器，并输入用户名和密码：



部门内用Web服务器类似，只是由于不开放给公网，无需在外网DNS服务器记录域名和IP。

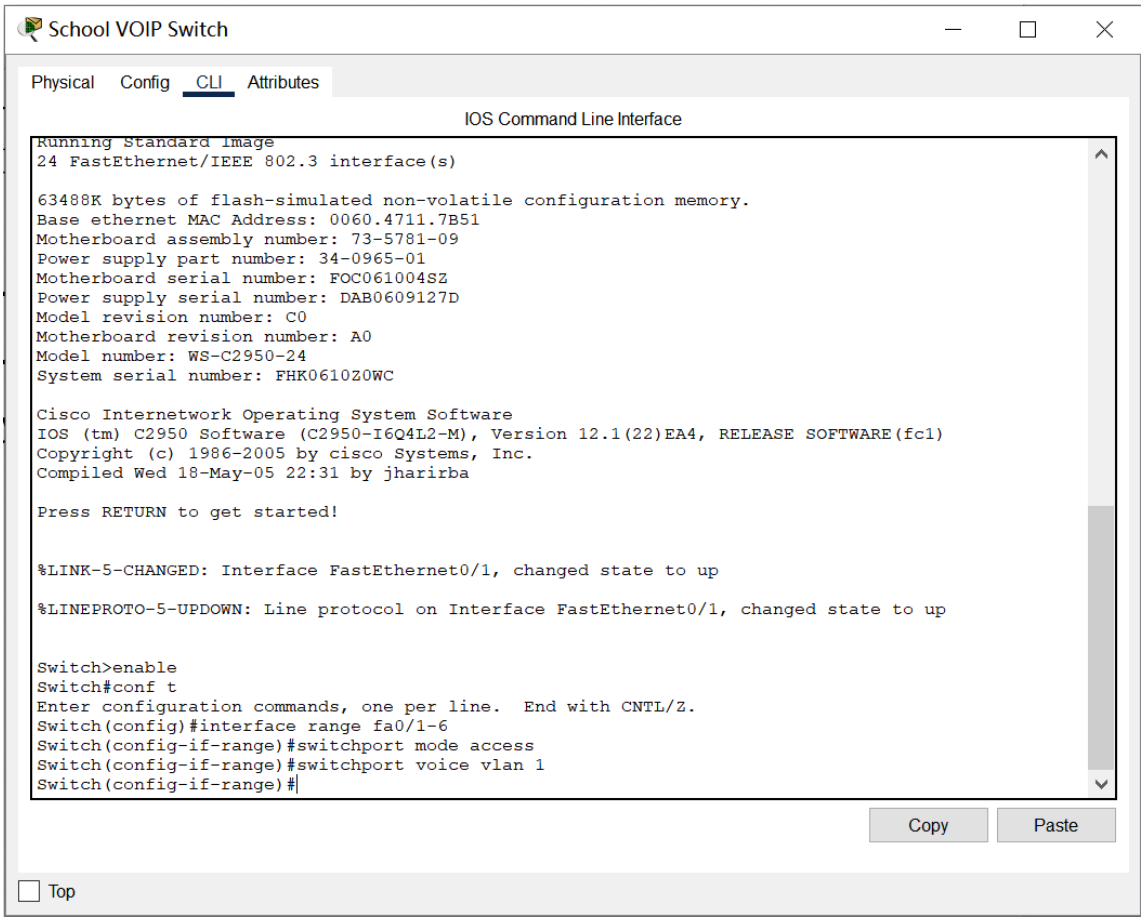
3.8 VOIP服务

由设计可知，各部门电话不接入内网，而是直接由Hallway Router提供。因此，首先配置它的FastEthernet0/1（后续电话的DHCP分配就以该地址所在网段分配）：

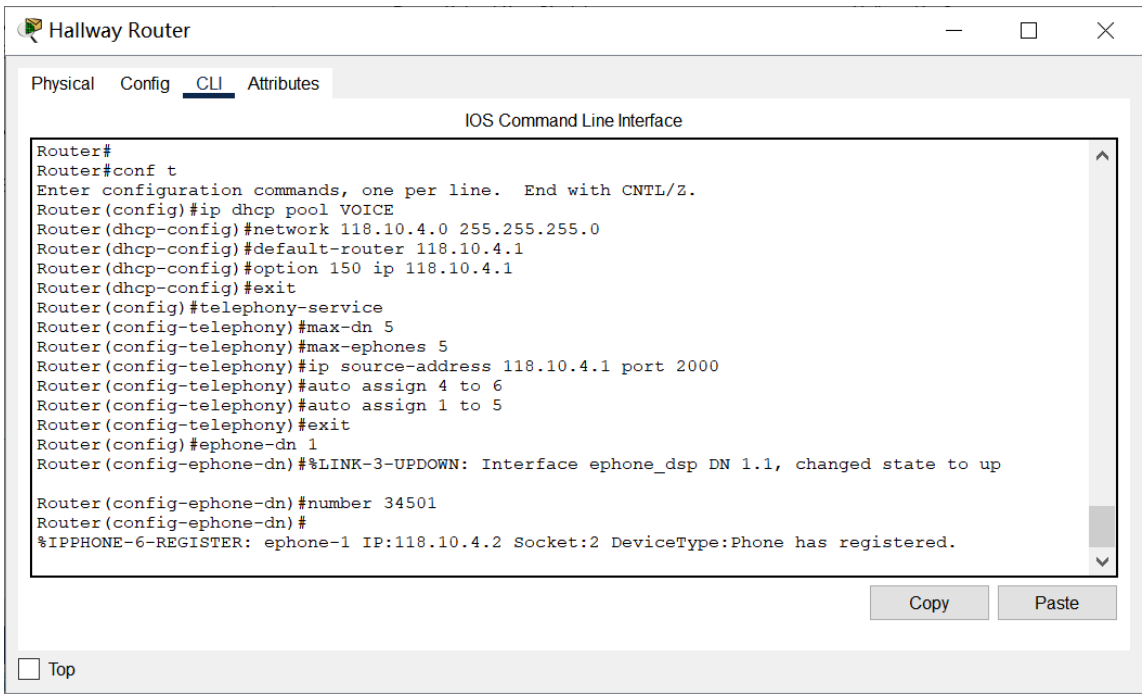


配置Hallway Router的DHCP以及电话服务（DHCP池名字一定要叫VOICE，标明这是提供VOIP服务的DHCP，否则VOIP服务不生效）：

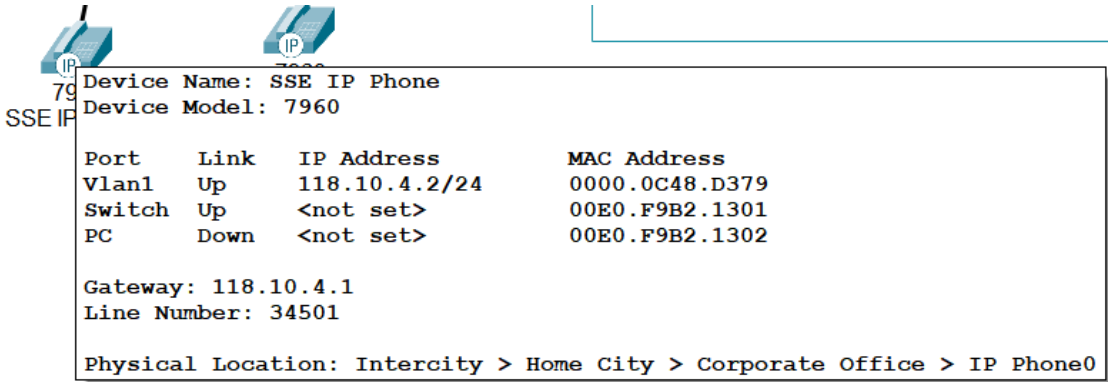
接下来在School VOIP Switch上进行配置，使得FastEthernet0/1到FastEthernet0/6都可以处理VOIP的数据包：



此时只将School VOIP Switch连接到第一台电话（如SSE IP Phone）的Switch口，给该电话插上电源线，并在Hallway Router上设置其电话号码：



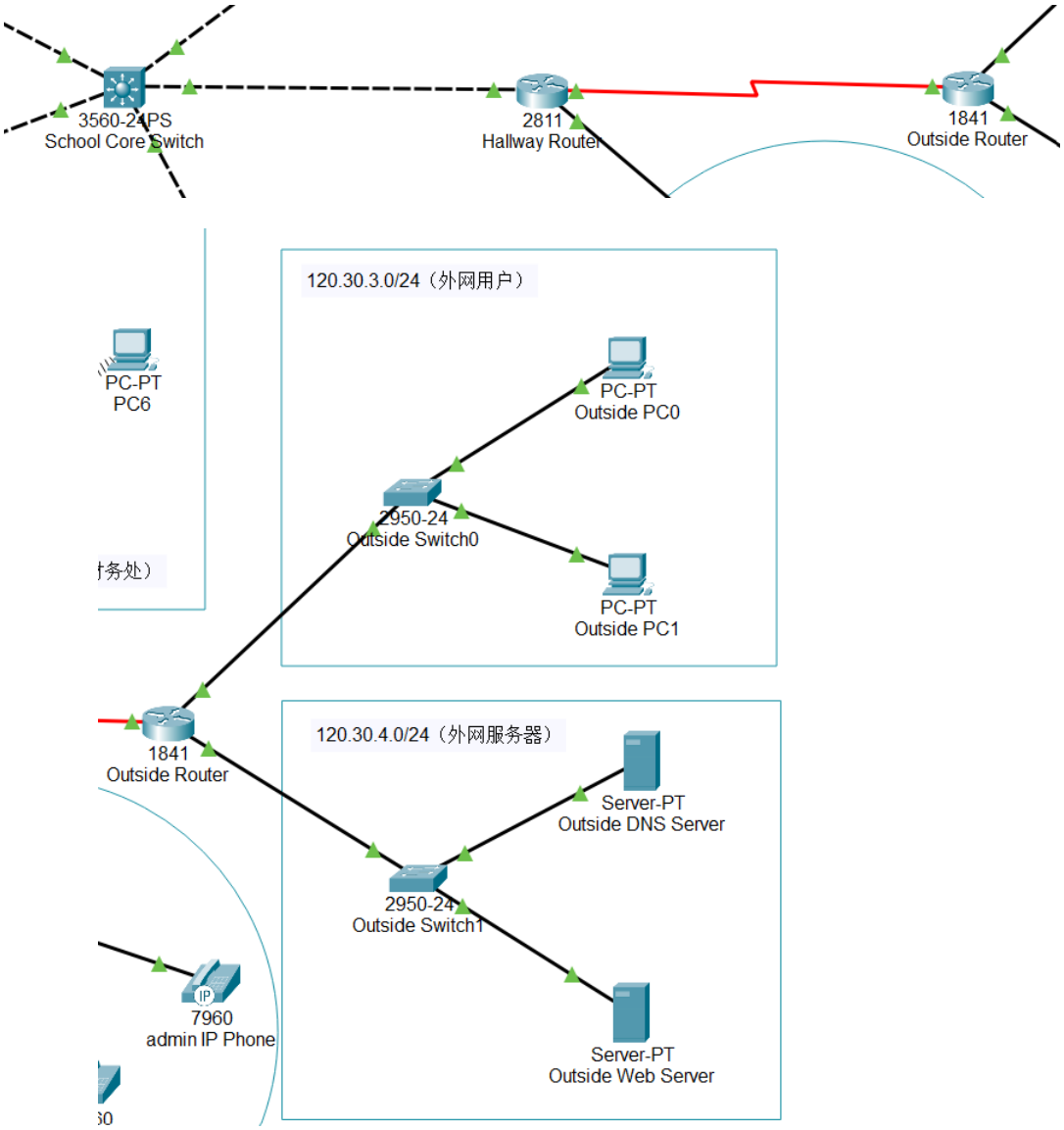
光标移动到电话上，若看到分配到的电话号码证明配置成功：



然后再连另一台IP电话到School VOIP Switch，重复配置电话号码过程。连一台配一台

4.外网设计&内外网连通

4.1 外网部分拓扑图



稍后在Hallway Router上会配置NAT转换，它就是内网的边界路由器。相对地，以串口连接的Outside Router已经位于外网。Hallway Router这个命名如何而来呢？我们在配置完成内网时发现：

1. School Core Switch通过给vlan分配IP地址进行逻辑划分后，各个vlan的网关已经在它身上了，意味着它已经“进化”为了一个有很多端口，身上有许多设备网关的路由器了
2. 但本质上它仍是交换机，无法提供NAT服务，无法作为整个学校的“网关路由器”直接连接外网
3. 一种解决方案是，把School Core Switch看成路由器，用一个新的网段将它和一个真正的路由器连接，后者提供NAT转换。这样，内外网的传输都需要经过这个网段，就好像家里有许多房间，但出入一定要经过门廊一样。所以把提供NAT的路由器叫做Hallway Router
4. 这也是为什么School Core Switch和Hallway Router一个是交换机，一个是路由器，却用交叉线连接。就是因为此时前者逻辑上已经是路由器，与后者属于同种设备了

4.2 相关设备信息

端口	IP	子网掩码
Outside Router FastEthernet0/0	120.30.3.254	255.255.255.0
Outside Router FastEthernet0/1	120.30.4.254	255.255.255.0
Outside Router Serial0/1/0	202.120.17.29	255.255.255.0
Gateway Router FastEthernet0/0	192.168.100.2	255.255.255.0
Gateway Router Serial0/1/0	202.120.17.18	255.255.255.0

终端	IP	子网掩码	网关	DNS
Outside PC0	120.30.3.11	255.255.255.0	120.30.3.254	120.30.4.11
Outside PC1	120.30.3.12	255.255.255.0	120.30.3.254	120.30.4.11
Outside DNS Server	120.30.4.11	255.255.255.0	120.30.4.254	
Outside Web Server	120.30.4.12	255.255.255.0	120.30.4.254	120.30.4.11

4.3 公网IP分配与DNS配置

我们为学校分配的4个公网IP为100.80.195.160到100.80.195.163，子网掩码为255.255.255.0。

学校为外网提供可访问的Email服务器和Web服务器使用了静态映射的NAT，把内网中192.168.9.6（Web服务器内网IP）映射到100.80.195.160，192.168.9.2（Email服务器内网IP）映射到100.80.195.160上。

编号	公网IP	内网IP	子网掩码	说明

1	100.80.195.160	192.168.0.4	255.255.255.0	Web
2	100.80.195.161	192.168.0.6	255.255.255.0	Email
3	100.80.195.162	192.168.0.0	0.0.255.255	内网访问外网
4	100.80.195.163	192.168.0.0	0.0.255.255	内网访问外网

同时，也假设学校为这两个服务器申请了域名并存放在外部DNS服务器Outside DNS Server上，这样，外部访问学校的Email和Web服务器不但可以通过公网IP访问，还可以通过域名访问。外部DNS服务器的DNS服务配置如下：

编号	域名	IP	说明
1	web.school.edu.cn	100.80.195.160	学校供外网访问的Web服务器
2	school.edu.cn	100.80.195.161	学校供外网访问的邮件服务器
3	www.outside.com	120.30.4.12	外部其他服务器

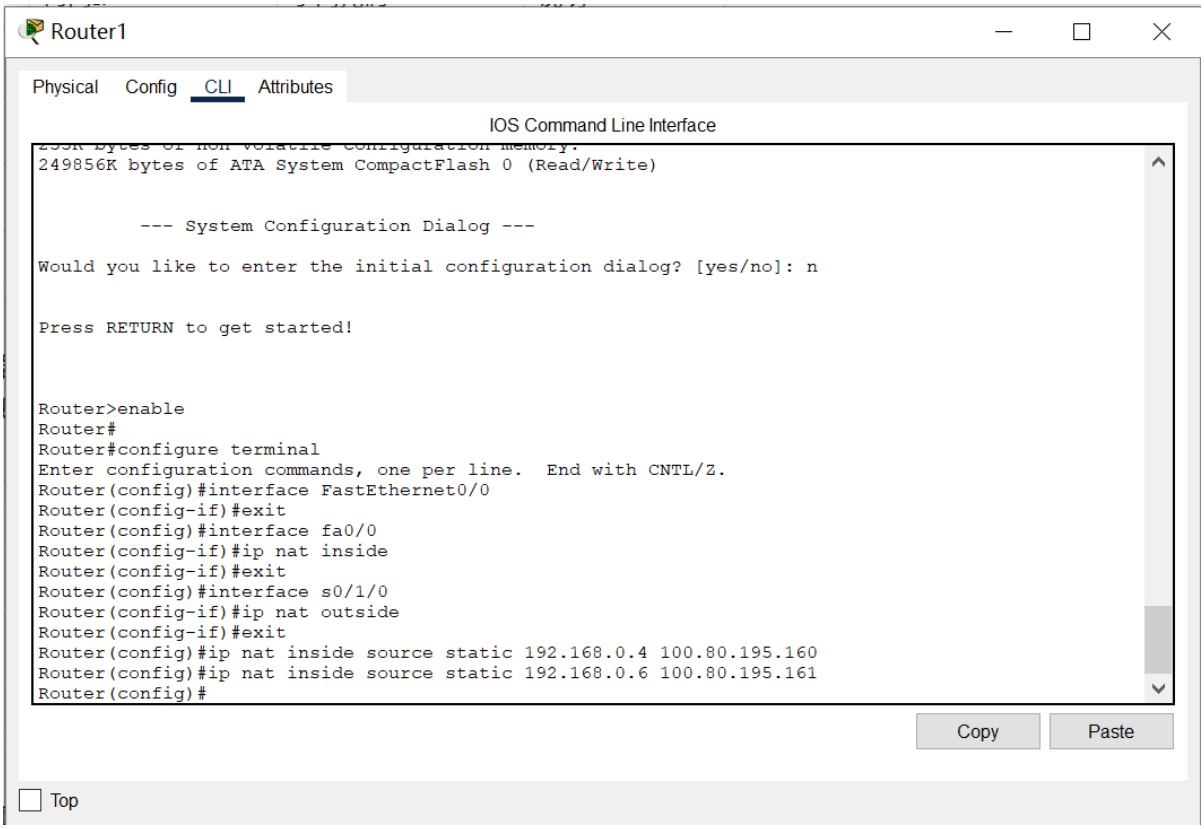
同时，为了校内用户可以访问外网，学校公用DNS服务器配置如下：

编号	域名	IP	说明
1	web.school.edu.cn	192.168.0.4	学校Web服务器（内网IP）
2	school.edu.cn	192.168.0.6	学校邮件服务器（内网IP）
3	www.outside.com	120.30.4.12	外部其他服务器

剩余的两个公网IP地址用于创建nat地址池，供学校内网主机访问外网使用。通过这种方式，内网主机可以访问外网，而外部的主机则无法访问内网的其他主机，实现了对内网主机的保护。

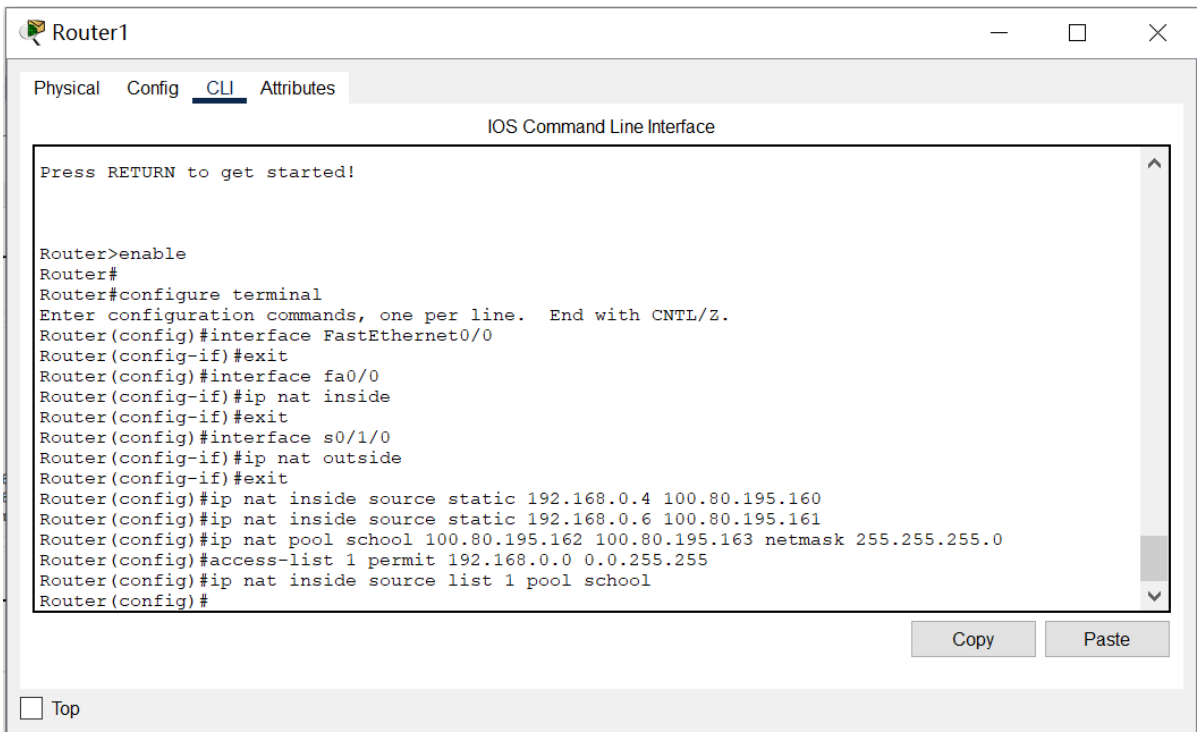
4.4 NAT配置

配置NAT内部和外部端口，并将两个供外部访问的服务器内网IP映射到公网IP：



接着进行内网访问外网的NAT：

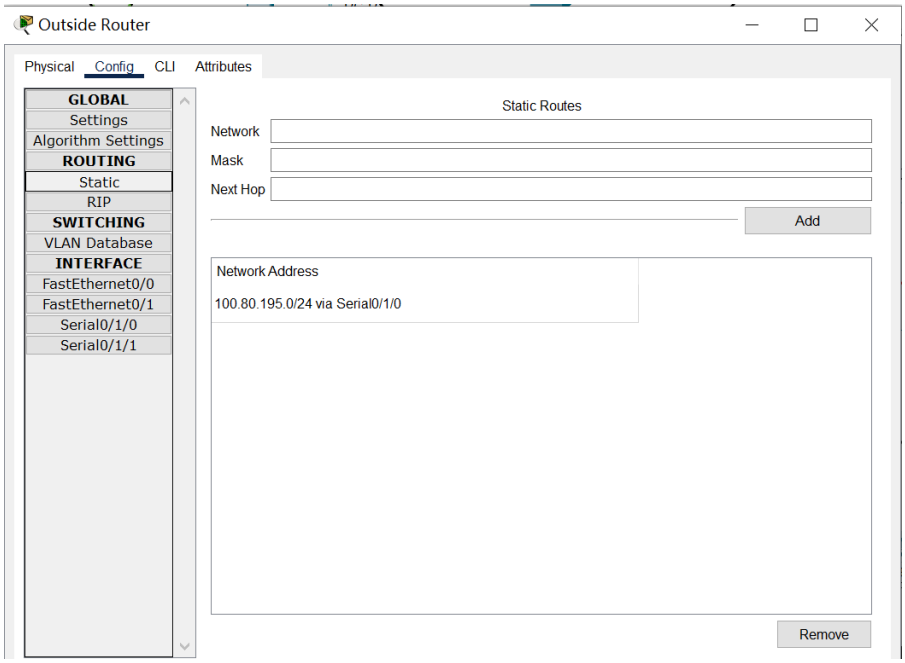
1. 创建一个NAT池school，里面包含剩下的两个公网IP
2. 创建一个192.168打头的IP地址都包括在内的访问列表
3. 将两者对应上，使得内网的主机可以复用NAT池中的地址，并访问外网



4.5 静态路由配置

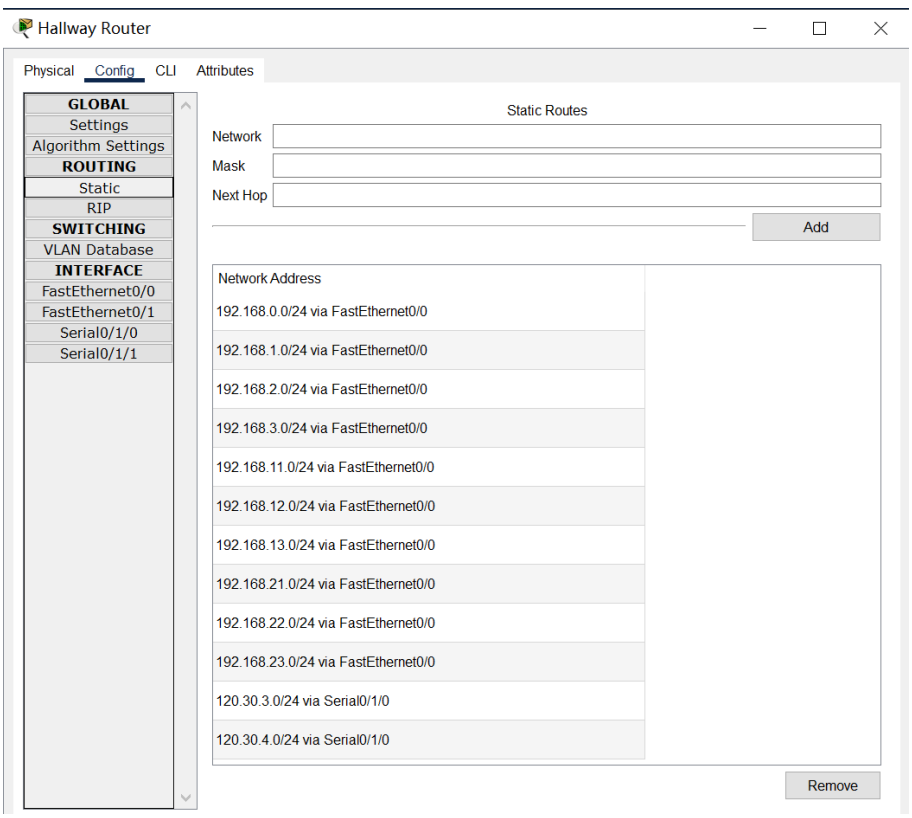
对于Outside Router：

1. 将公网访问内网的请求转发给Hallway Router，因此对于目的网段100.80.195.0/24（内网映射到的公网网段）的请求，需要从Serial0/1/0转发



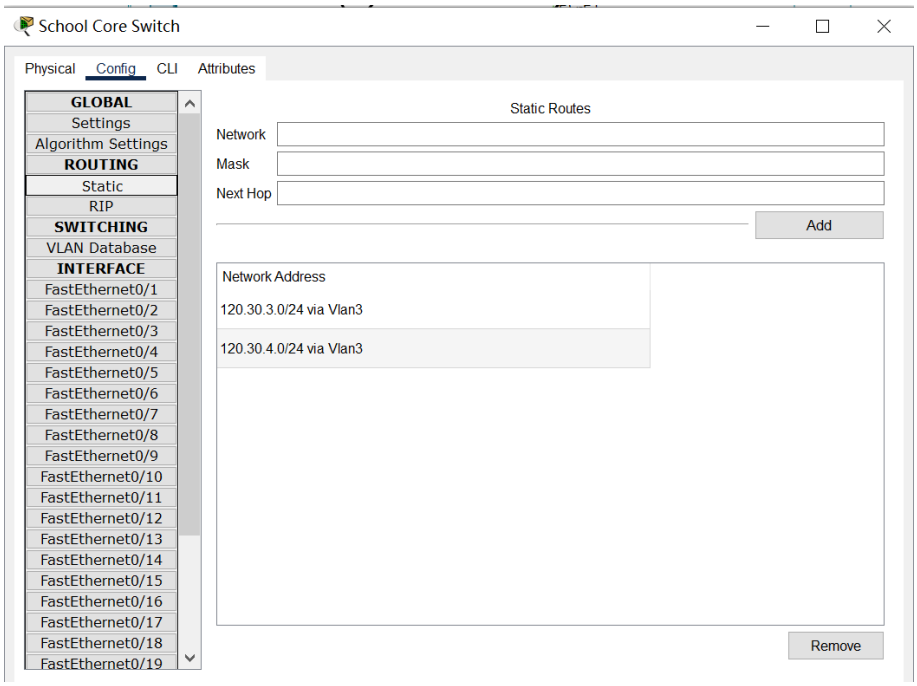
对于Hallway Router：

1. 将公网访问内网的请求转发给School Core Switch，因此对于目的网段192.168.0.0/24（核心层）的请求，需要从FastEhternet0/0转发
2. 将内网访问公网的请求转发给Outside Router，因此对于目的网段120.30.X.0/24（X为3或4，外部网段）的请求，需要从Serial0/1/0转发
3. 在上一点中，公网会返回信息给内网网段，需要Hallway Router转发给School Core Switch，因此对于目的网段192.168.X.0/24（内网各vlan网段），需要从FastEthernet0/0转发



对于School Core Switch：

1. 将内网访问公网的请求转发给Hallway Router，因此对于目的网段120.30.X.0/24（X为3或4，外部网段）的请求，需要从vlan 3转发

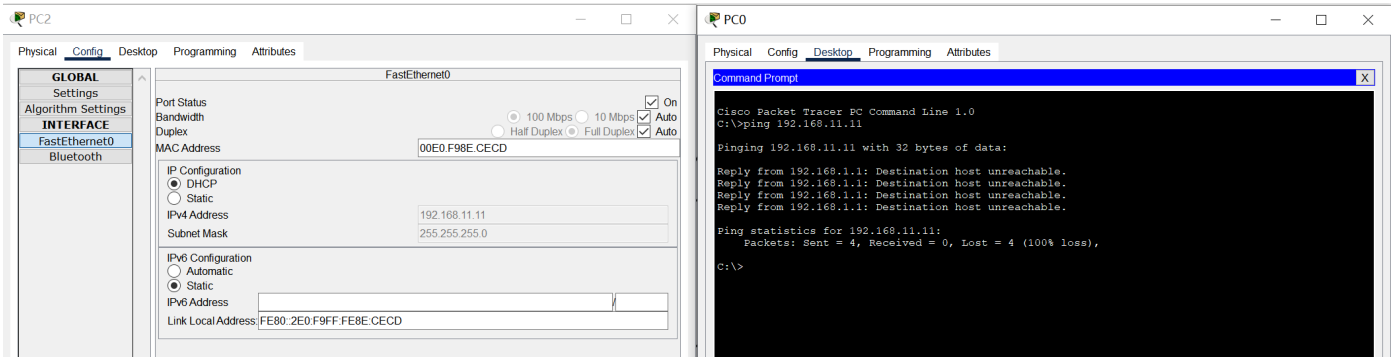


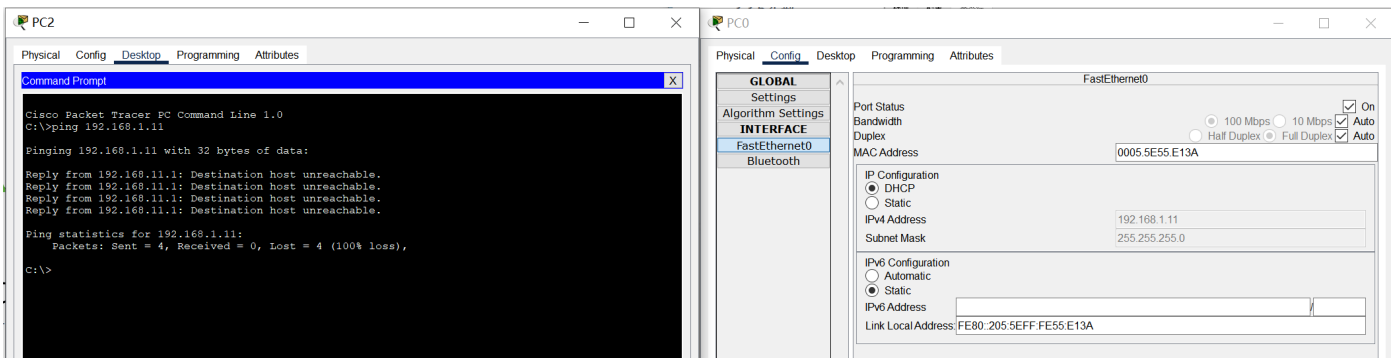
5.网络测试

5.1 局域网连通性测试

- 各部门之间网络独立
  - 不同部门的电脑相互之间无法 ping 通

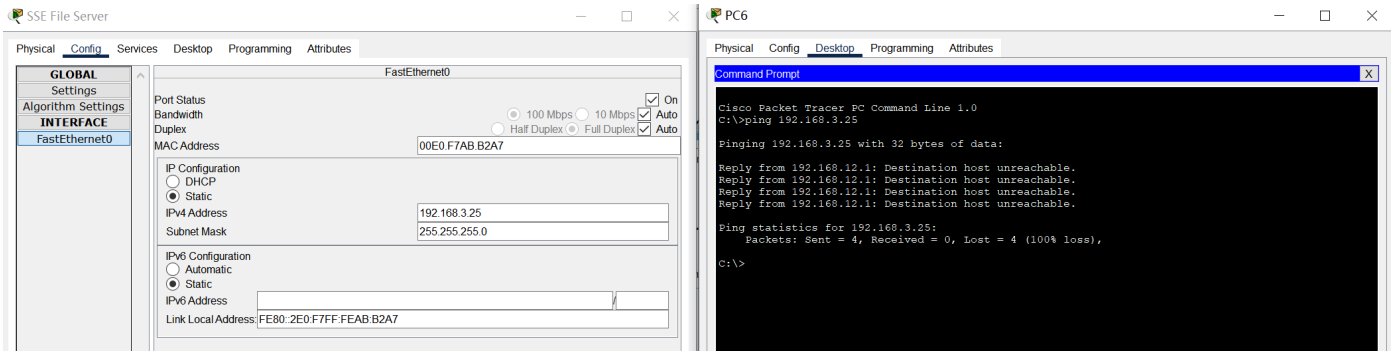
分属不同部门的 PC0 和 PC2 相互 ping 不通。



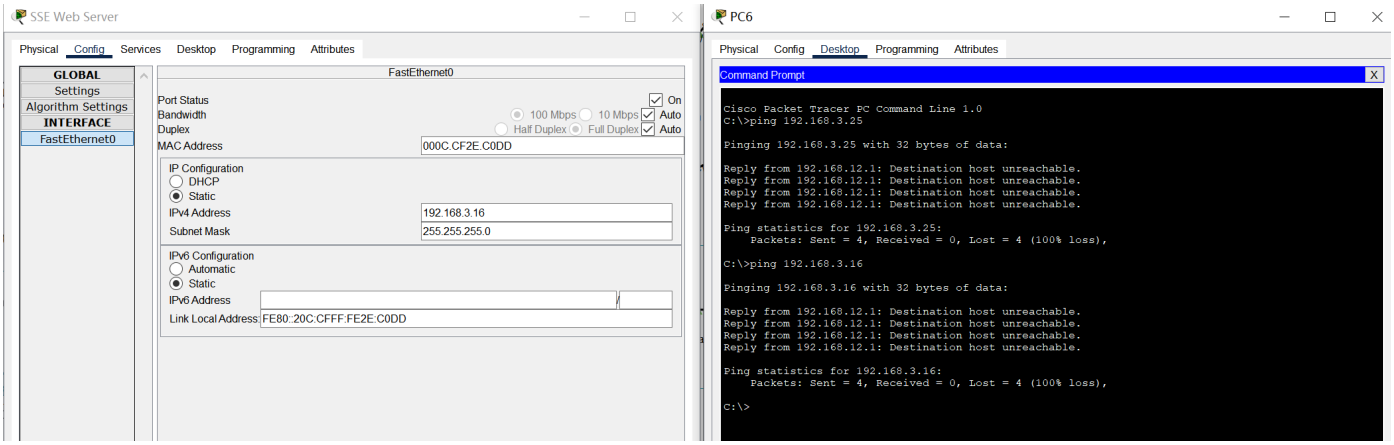


- 不同部门的电脑无法 ping 通另一个部门的服务器

分属不同部门的财务处 PC6 ping 不通软件学院部门的 SSE File Server

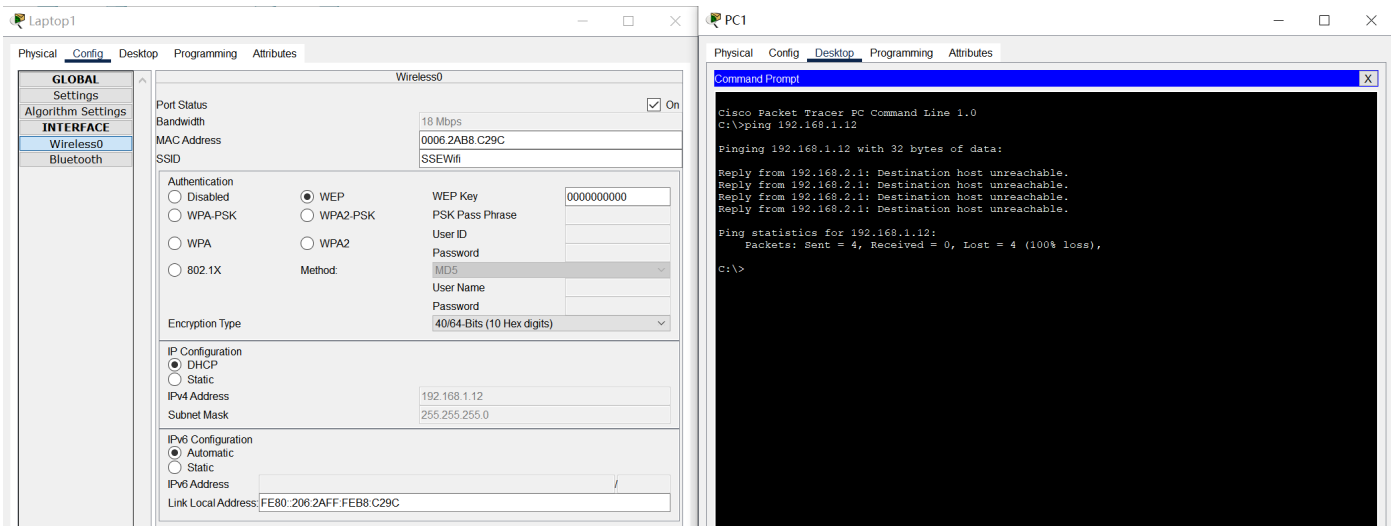


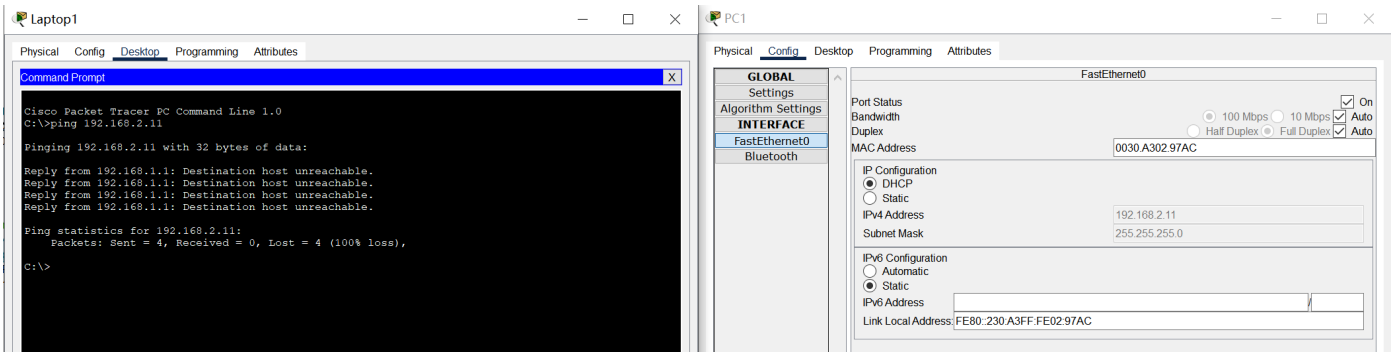
分属不同部门的财务处 PC6 ping 不通软件学院的 SSE Web Server



- 部门内存在若干局域网
  - 同一部门中不同局域网的电脑不能相互 ping 通

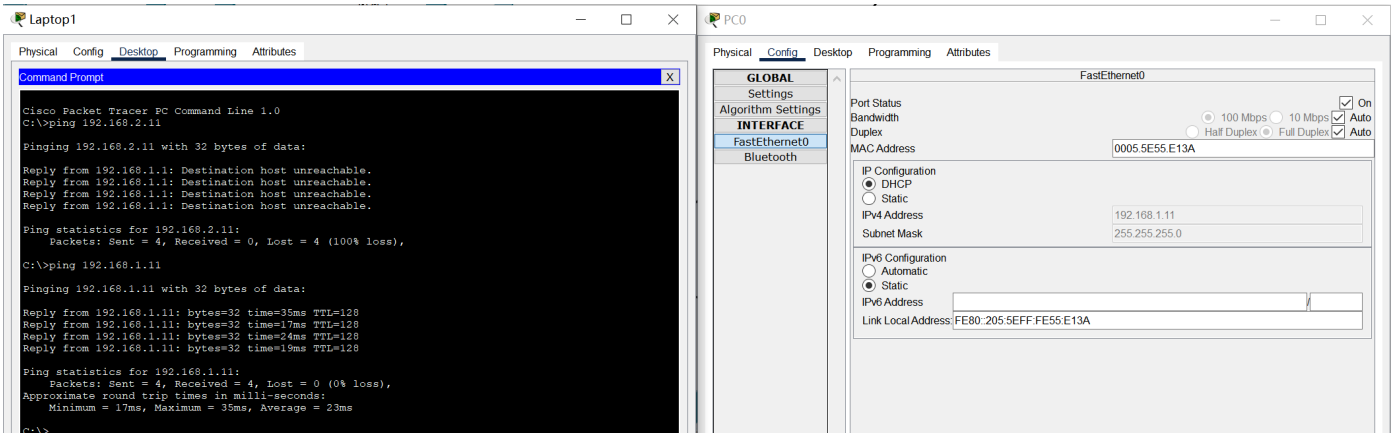
同一个部门的两个局域网之间的 Laptop1 和 PC1 相互 ping 不通。

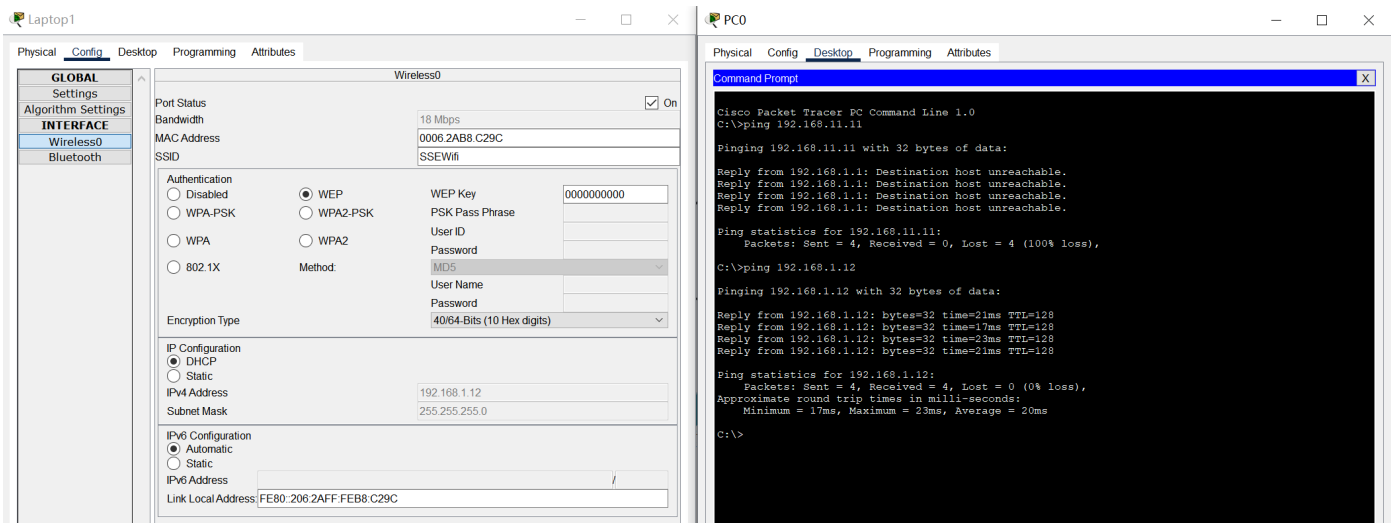




- 同一部门中同一个局域网中的电脑之间可以相互 ping 通

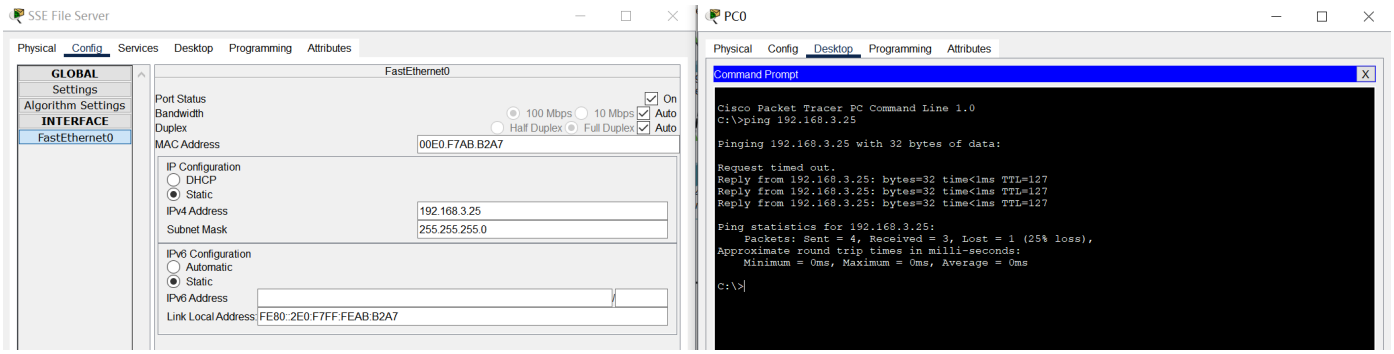
软件学院中同一局域网的Laptop1和PC0可以相互ping通



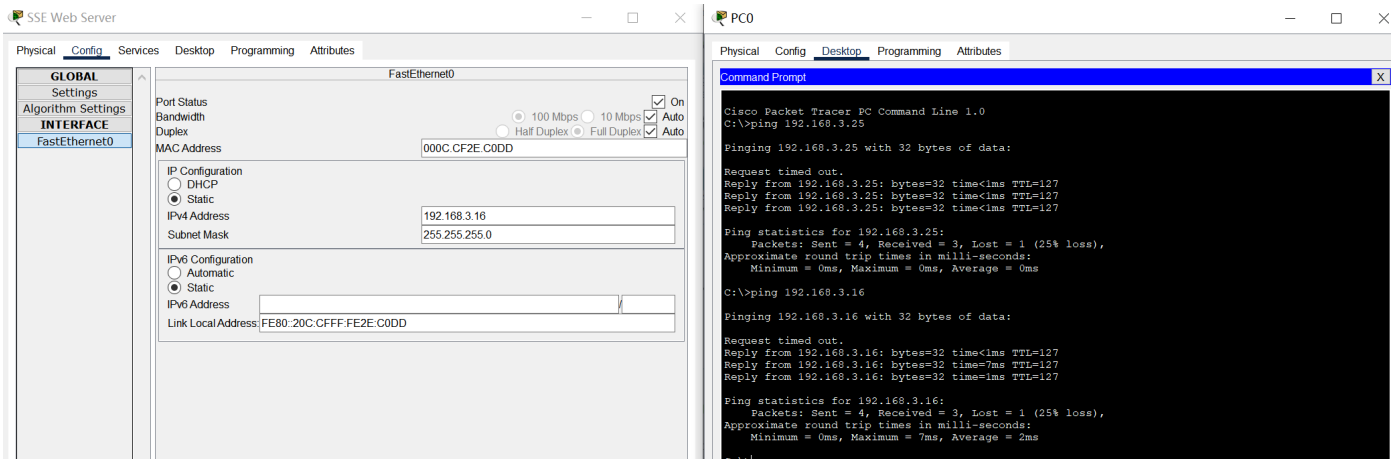


- 同一部门中的电脑可以 ping 通该部门的服务器

软件学院中电脑 PC0 可以 ping 通同部门中的的文件服务器 SSE File Server

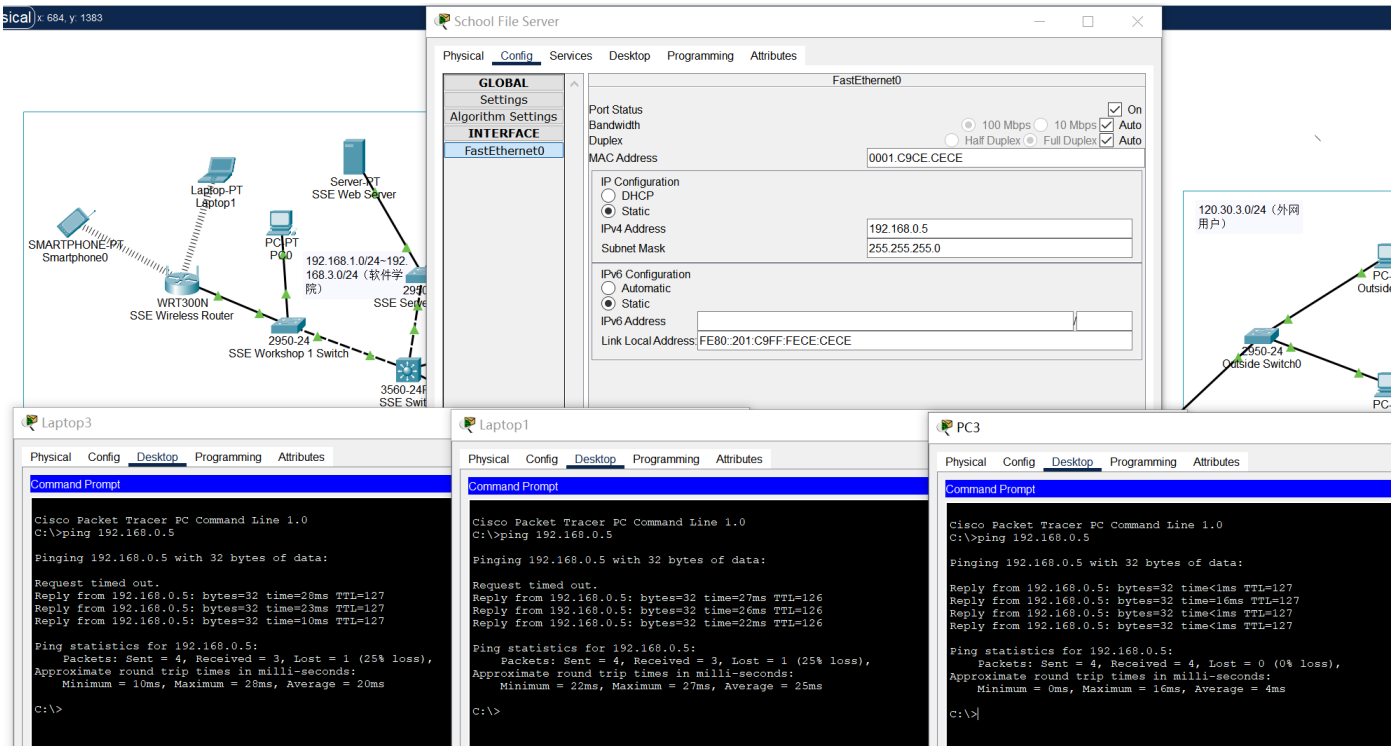


软件学院中电脑 PC0 可以 ping 通同部门中的的文件服务器 SSE File Server



- 不同部门与大学公用的服务器之间可ping通

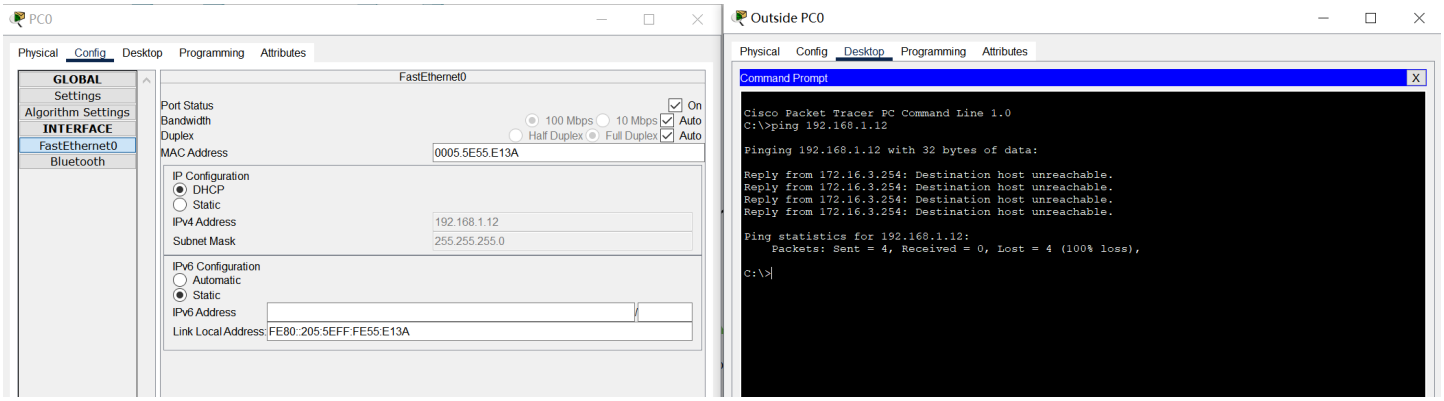
  这里软件学院的 Laptop1、财务处的 PC3以及行政管理的 Laptop3 均可以 ping 通大学共用的文件服务器



- 外网无法直接访问大学内网

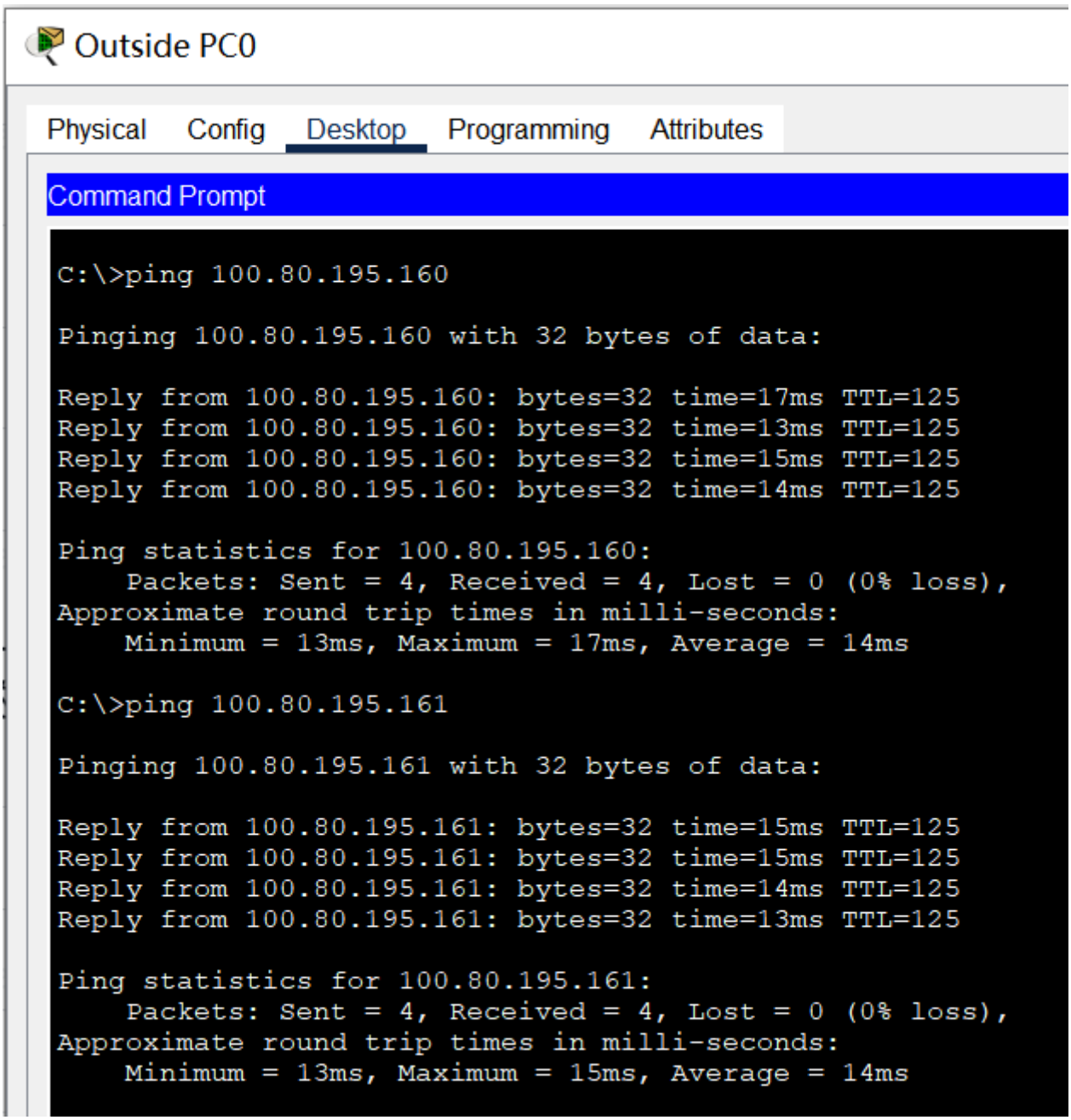
外网主机无法ping通内网主机。

这里外部电脑 Outside PC0 无法 ping 通内部电脑 PC0



- 外网可以访问大学的公网IP

外网主机 Outside PC0 能 ping 通大学的 Web、Email 服务器的公网IP。

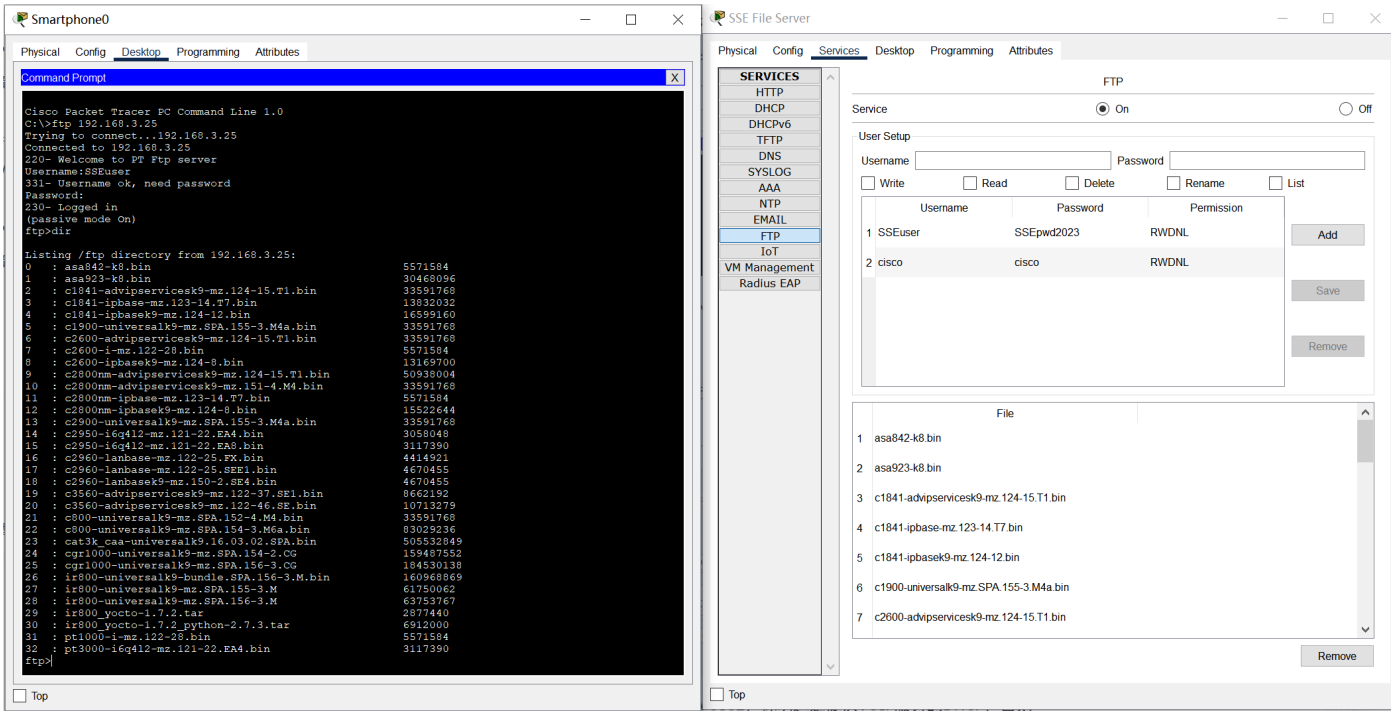


5.2 文件服务器测试

- 每个部门有自己内部的文件服务器

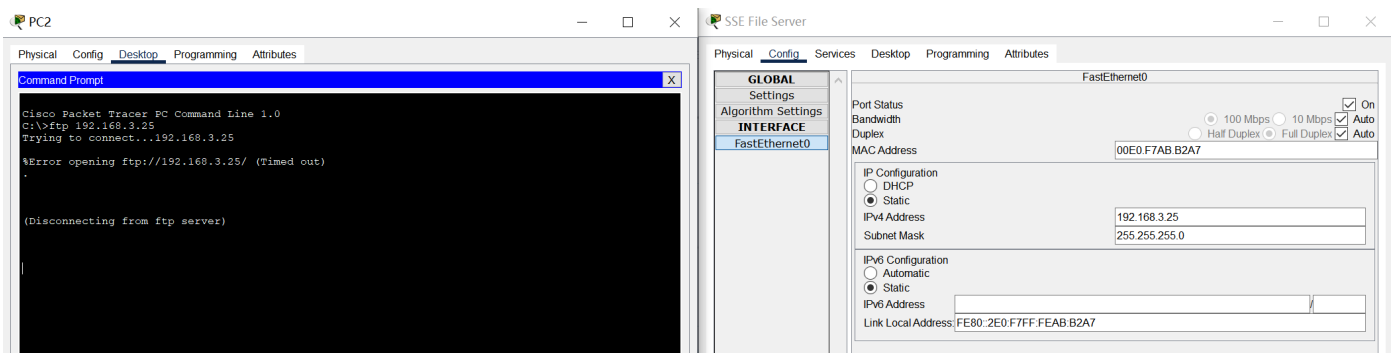
- 同一部门内的设备可以访问自己部门的文件服务器

软件学院的 Smartphone0 可以访问 SSE File Server



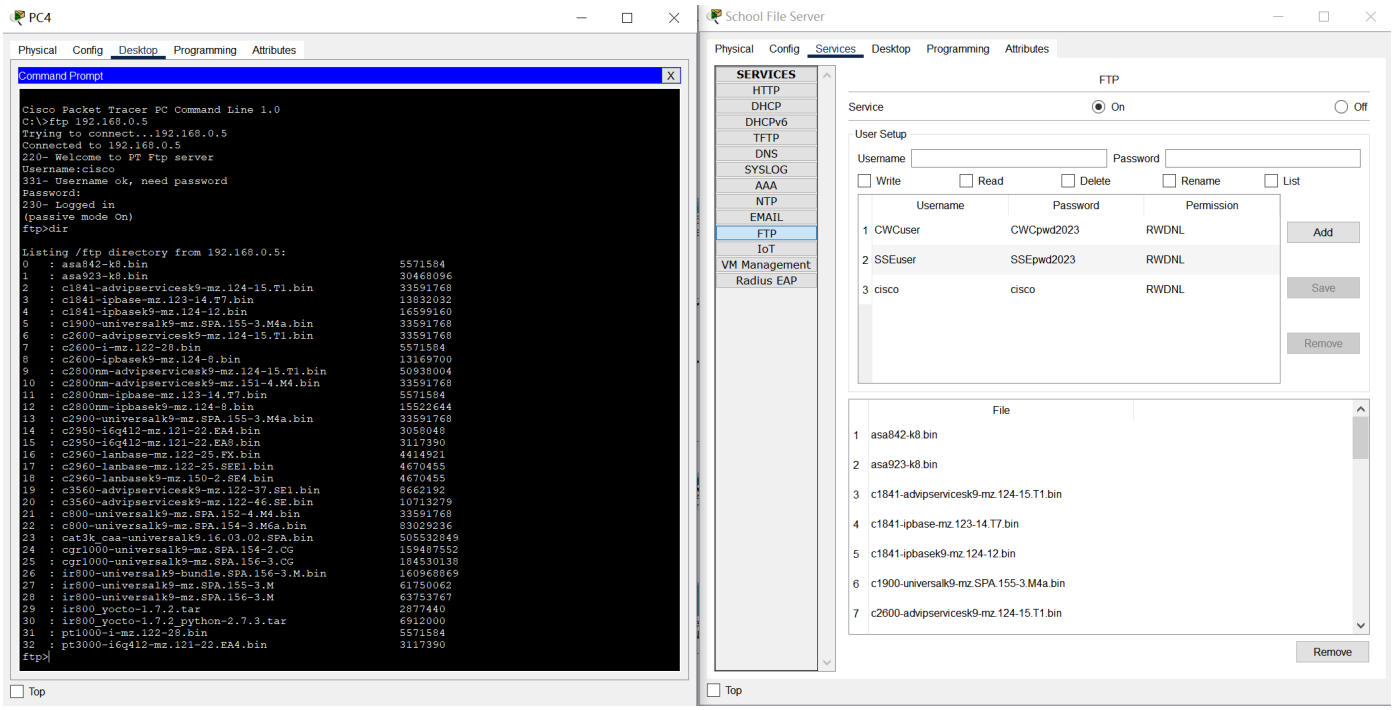
- 一个部门的设备不能访问另一个部门的文件服务器

财务部的 PC2 不能访问软件学院的文件服务器

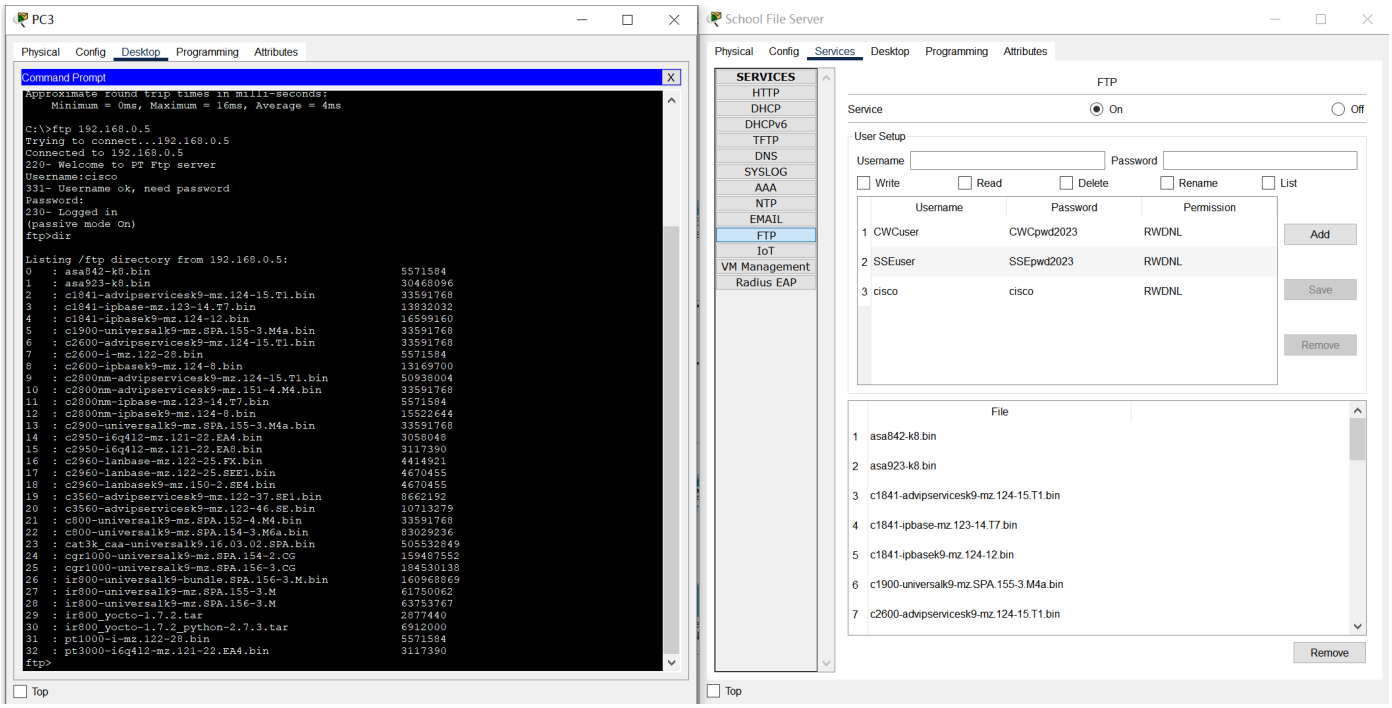


- 大学中有一个公共的文件服务器，各个部门均可以访问

行政管理的 PC4 可以访问公共的文件服务器 School File Server



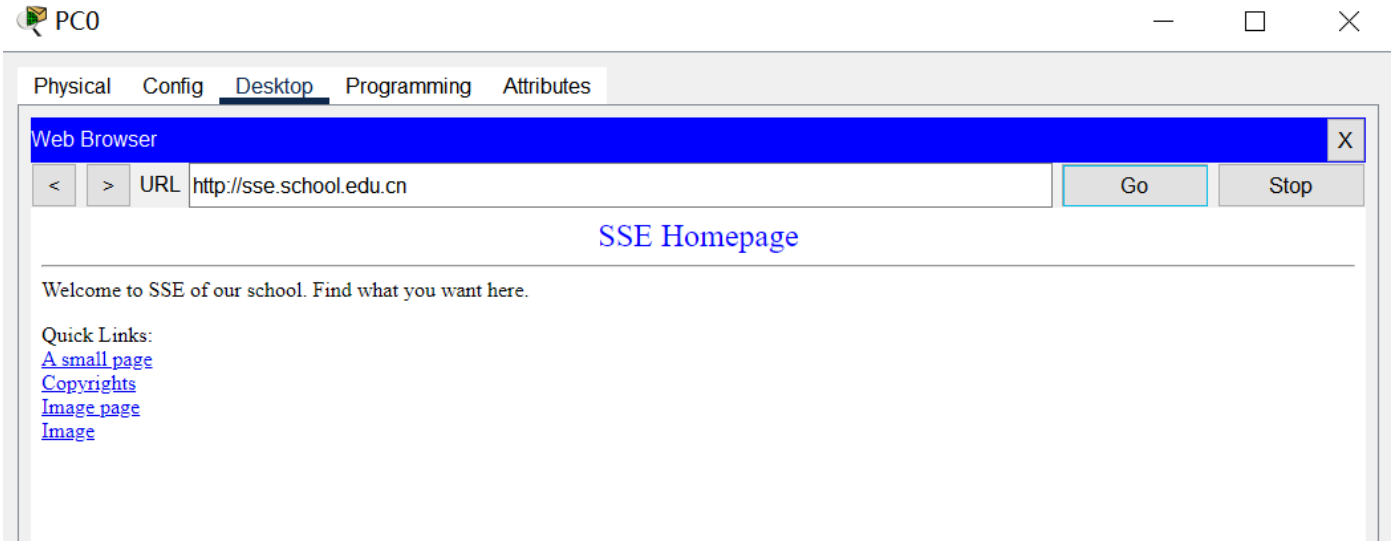
财务处的 PC3 也可以访问公共的文件服务器 School File Server



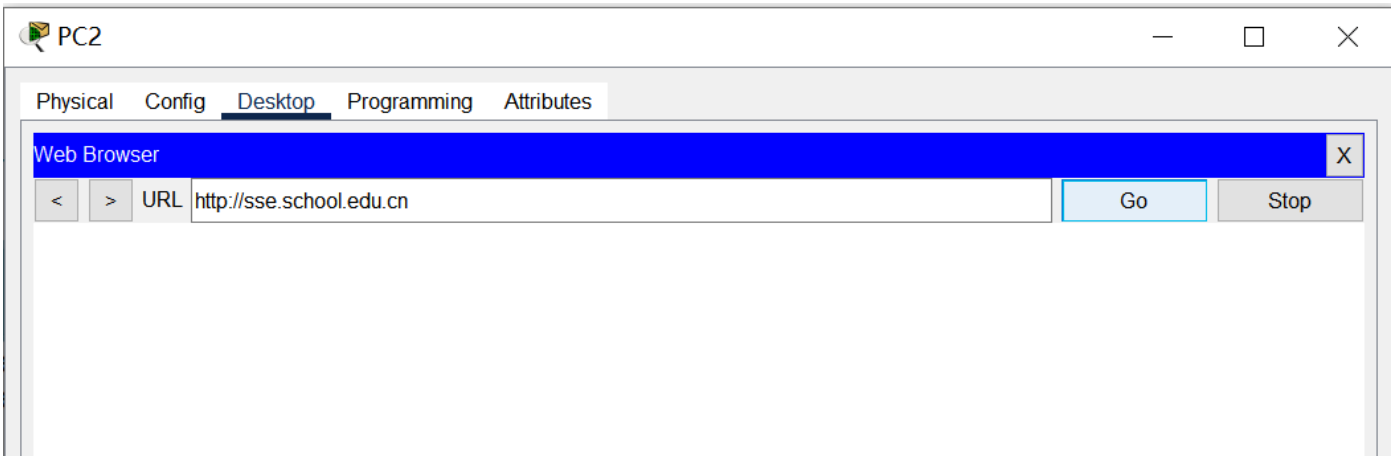
5.3 Web服务器测试

- 每个部门有自己内部的Web服务器，同一部门可以访问自己的网页，但不可以访问其他部门的网页

  软件学院的 PC0 可以访问软件学院的 Web 服务器

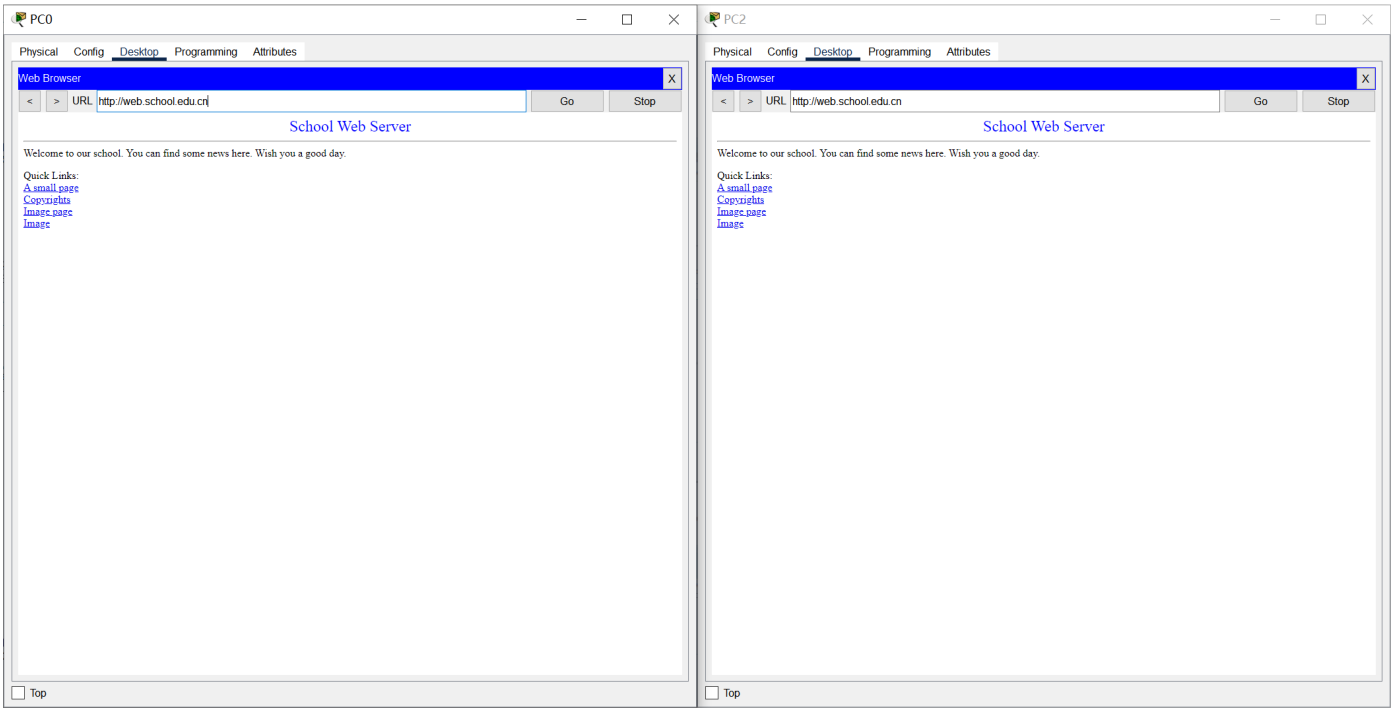


财务部的 PC2 无法访问软件学院的 Web 服务器



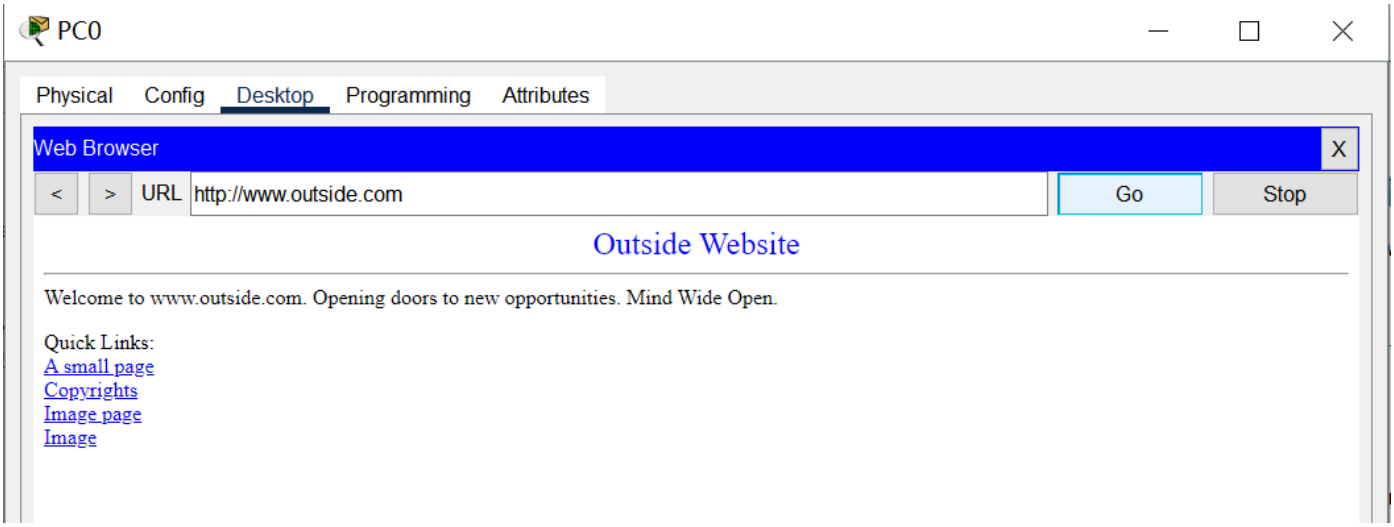
- 大学中提供一个内外网都可以访问的 Web 服务器

  软件学院的 PC0 和财务部的 PC2 均可以访问到大学公共的网页



- 大学内部也可以访问外部网页

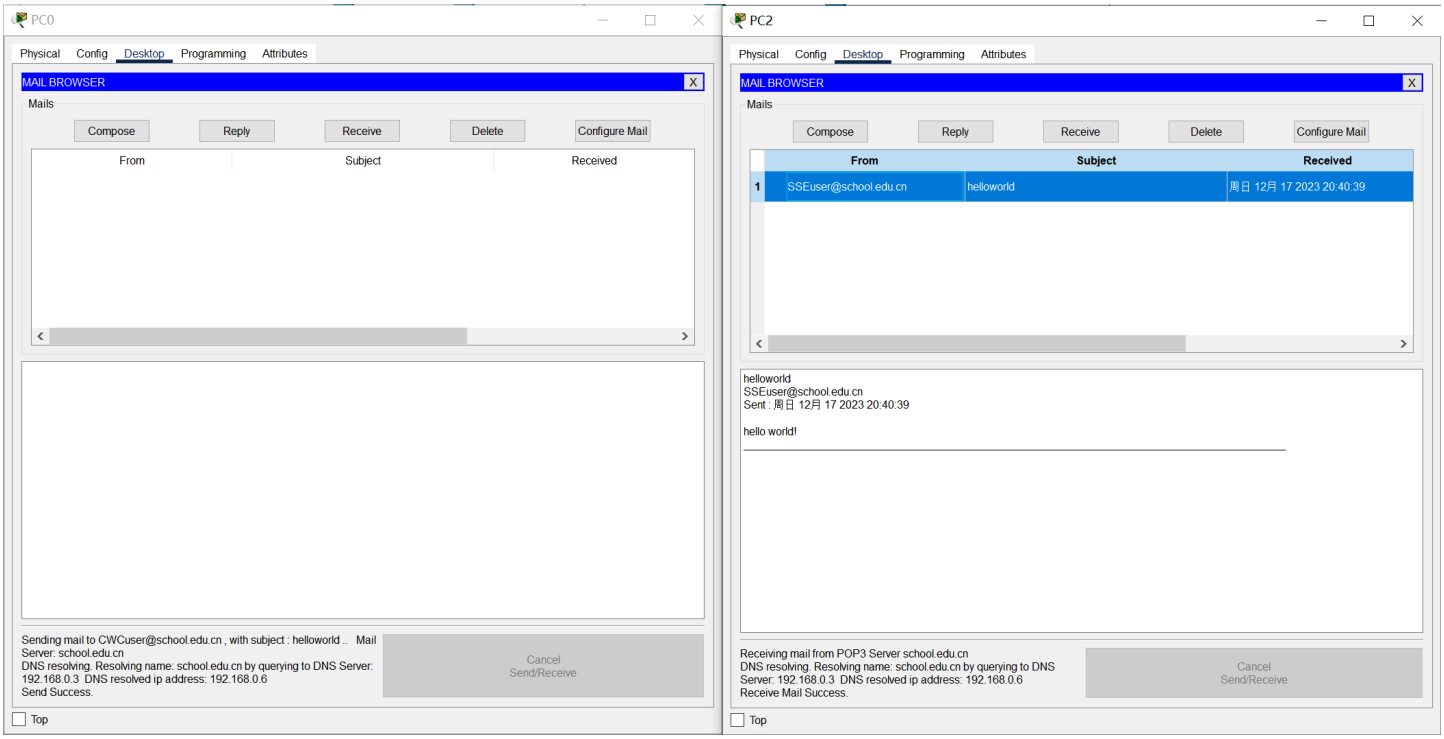
软件学院的 PC0 可以访问外部网页



5.4 Email服务器测试

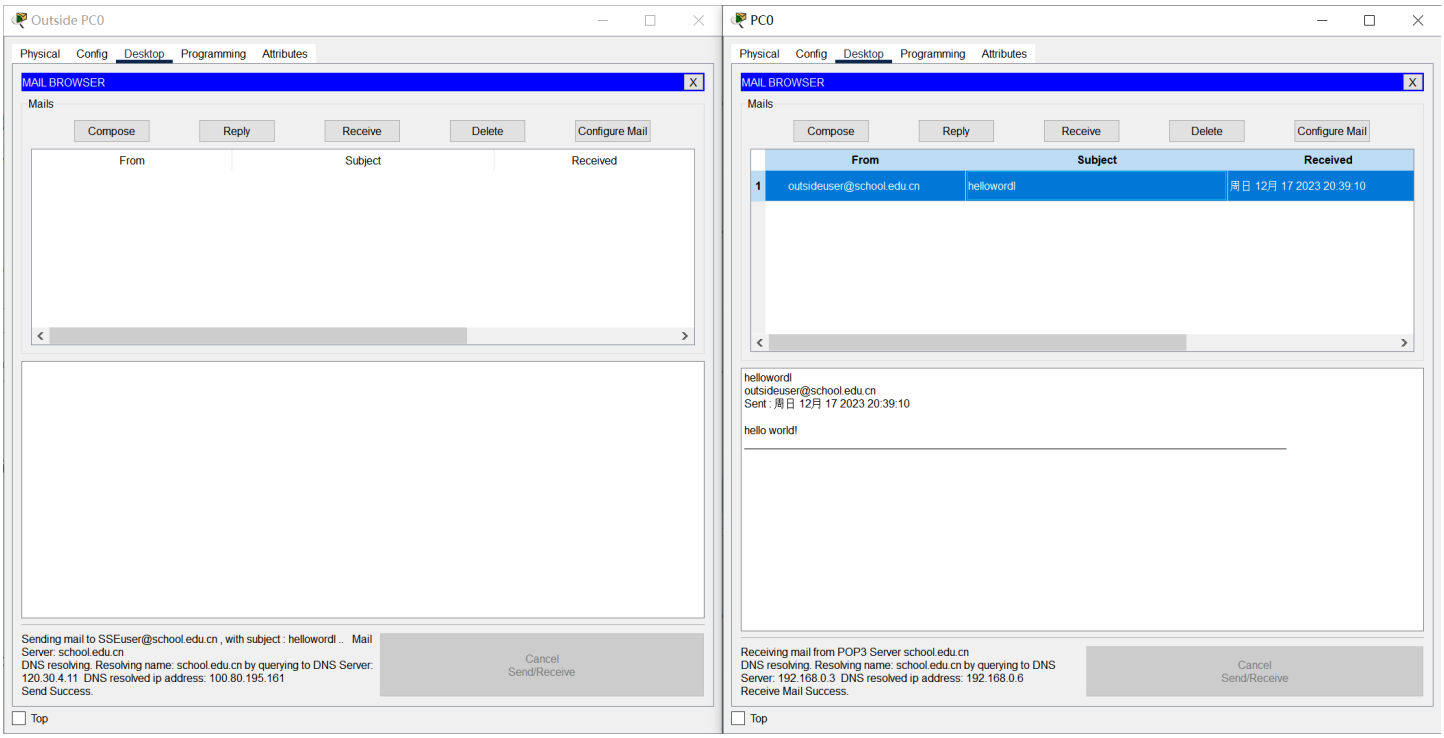
- 学校内部主机之间发邮件

软件学院的主机PC0向财务处的主机PC2发邮件成功，急诊部主机成功接收到邮件。



- 外网与学校内部之间发邮件

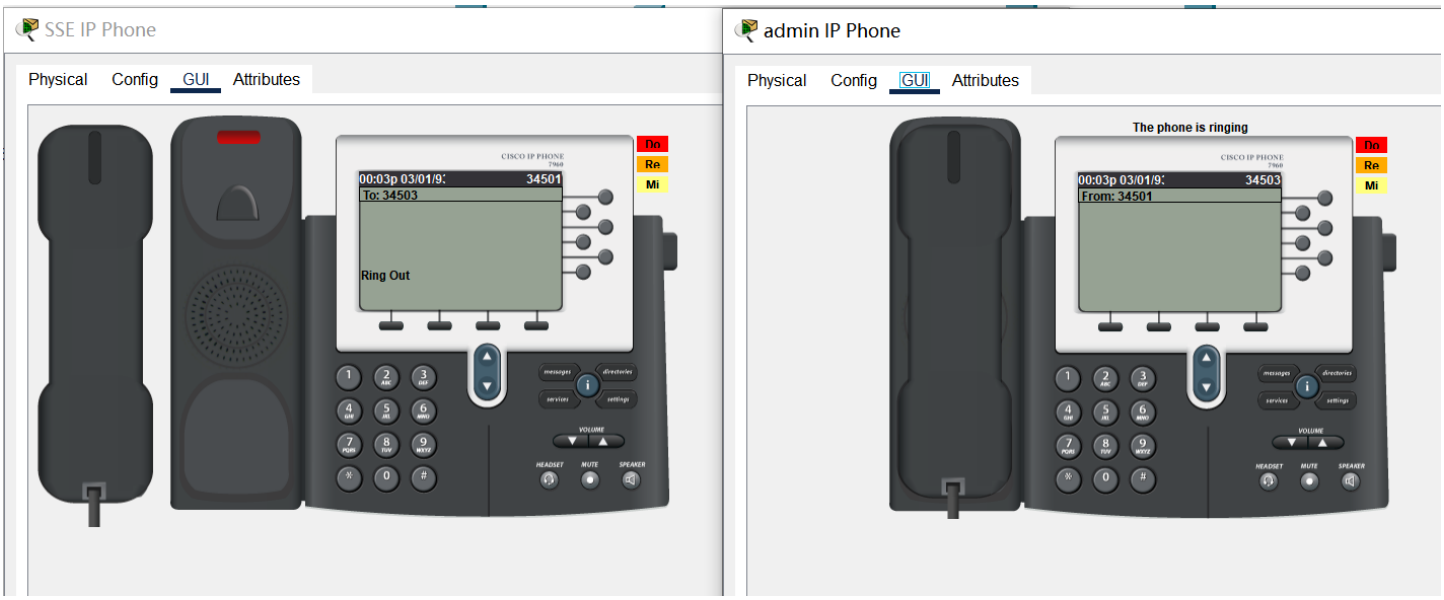
外网主机Outside PC0向软件学院连接的主机PC0发邮件成功，软件学院主机PC0成功接收到邮件



5.5 VOIP测试

部门之间的IP电话可以相互拨通。

34501拨打34503，等待34503接通：



34501与34503相互通话


SSE IP Phone
Physical
Config
GUI
Attributes
Playing 'Do'...
Do
Re
Mi
00:05p 03/01/9: 34501
To: 34503
Connected


admin IP Phone
Physical
Config
GUI
Attributes
Playing 'Re'...
Do
Re
Mi
00:05p 03/01/9: 34503
From: 34501
Connected