**计算机网络实验项目报告**

小组成员：2320241袁艺铭 2354093李雪菲 2352037郑耀辉 2353740于广淳

指导教师：冯巾松

实验地点：济事楼330

实验时间：第十六周-第十七周

人员分工：郑耀辉 于广淳：配置pkt文件 袁艺铭 李雪菲：报告撰写

PT软件版本：7.0

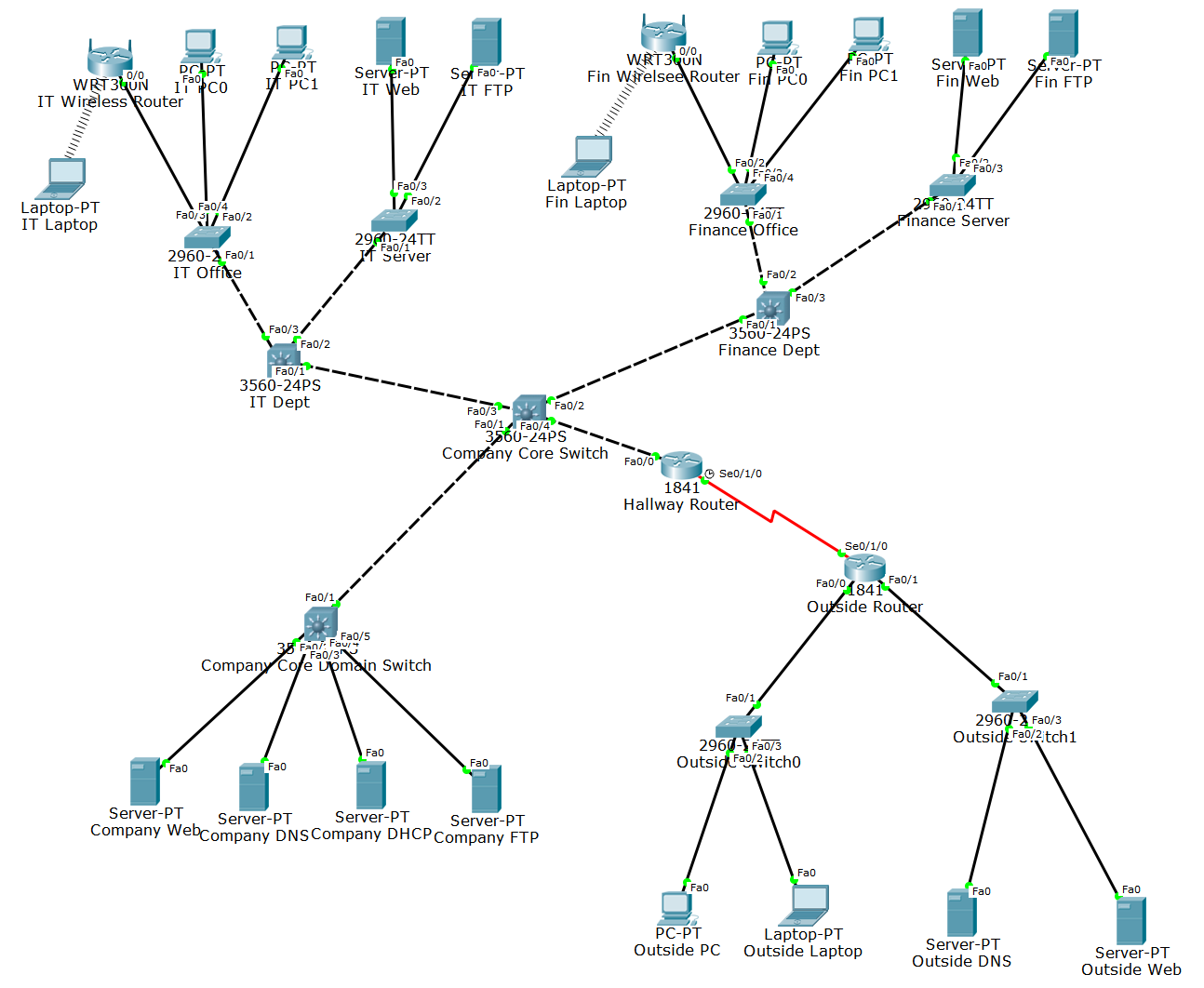
**1.** **提供功能及使用技术**

为满足企业独立运营、资源隔离、安全访问、统一上网、外部服务发布与无线接入等需求，设计并部署了一套功能完整、安全可控的网络架构，具体实现的功能及使用技术如下：

|  |  |  |  |
| --- | --- | --- | --- |
|  | 功能模块 | 说明 | 使用技术 |
| 1 | VLAN隔离与互访 | 各部门划分独立 VLAN，部门终端与服务器通过 ACL 控制互访 | VLAN、三层交换、ACL |
| 2 | DHCP 地址自动分配 | 各 VLAN 主机通过 DHCP 中继自动获取 IP 地址 | DHCP |
| 3 | DNS 名称解析服务 | 所有主机可通过域名访问企业内外的服务器资源 | DNS |
| 4 | FTP 服务 | 各部门只能访问本部门和核心层FTP 服务；核心层可访问所有部门 FTP；外部用户禁止访问 | FTP、ACL |
| 5 | Web 服务 | 各部门只能访问本部门和核心层 Web 服务；核心层可访问所有部门 Web；外部仅可访问核心 Web | HTTP/HTTPS、ACL |
| 6 | WiFi服务 | 提供 WiFi ，为移动设备提供 VLAN 地址与服务访问 | 无线路由器、DHCP |
| 7 | 内部动态路由 | 各部门与核心交换机间使用 RIP 实现动态互联路由 | RIP（v2） |
| 8 | 核心静态路由配置 | 核心交换机和边界路由器间使用静态路由 | 静态路由 |
| 9 | NAT 地址转换 | 内网通过 Hallway Router 的 NAT 功能统一访问外部网络 | NAT |
| 10 | Web 外网发布 | 公司主页通过静态 NAT 暴露到公网，允许外部访问 | 静态 NAT、公网 DNS |
| 11 | 外部 Web 访问 | 公司只有核心层可访问外部 Web 服务，各部门不可访问 | ACL |
| 12 | FTP、Web 外部屏蔽 | 外部用户无法访问各部门 FTP/Web 服务 | ACL、NAT映射策略 |

**2.网络拓扑结构**

根据需求，我们设计出如下的拓扑网络结构：



1. 该网络结构分为内网和外网两部分，内网即企业网络整体的局域网，外网即外部互联网的用户和服务器。
2. 内网包括核心层和两个独立部门（财务部、IT部）。
3. 核⼼层中的Web服务器、DNS服务器、DHCP服务器、以及FTP服务器均为内⽹公⽤，外网可访问该Web服务器，不可访问其他服务器。
4. 每个部⻔内设有多个主机和两台服务器。两台服务器为Web服务器和FTP服务器。部⻔内提供了Wifi服务，由⽆线路由器提供。两个部门均有访问接入控制ACL的设计，限制内网中的访问。
5. 内网核心交换机为三层交换机，支持三层路由，可以分配各区域vlan，便于管理。
6. ⽹关路由器（HallwayRouter）提供NAT服务。给内⽹核⼼层的Web服务器配置了公⽹

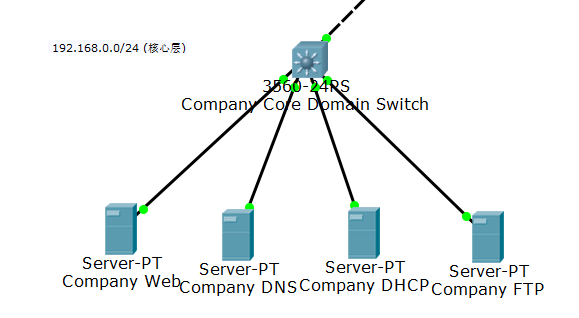
IP，将其开放给外⽹，外⽹⽤⼾可以通过公⽹IP访问它们。给内⽹其余设备配备了NAT池，这样可以在公⽹IP数量有限的情况下，多个内⽹设备要访问外⽹⽽进⾏NAT转换时，可以进⾏复⽤。企业内部都可以通过该网关路由器访问公⽹上的外部Web服务器、DNS服务器等。

**3.内网设计**

企业内网按功能划分为多个VLAN，分别对应核心服务器区、IT部门、财务部门等，采用三层交换配置，实现跨VLAN通信与访问控制。同时配置 DHCP 自动分配地址、部署 DNS、Web、FTP服务，并设置ACL限制跨部门访问，确保内网安全性。

**3.1构建核心层网络**

**3.1.1核心层网络拓扑图**



**3.1.2配置服务器静态IP**

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** |
| Web | 192.168.0.2 | 255.255.255.0 | 192.168.0.1 | 192.168.0.3 |
| DNS | 192.168.0.3 | 255.255.255.0 | 192.168.0.1 | — |
| DHCP | 192.168.0.4 | 255.255.255.0 | 192.168.0.1 | 192.168.0.3 |
| FTP | 192.168.0.5 | 255.255.255.0 | 192.168.0.1 | 192.168.0.3 |

**3.2核心层VLAN配置**

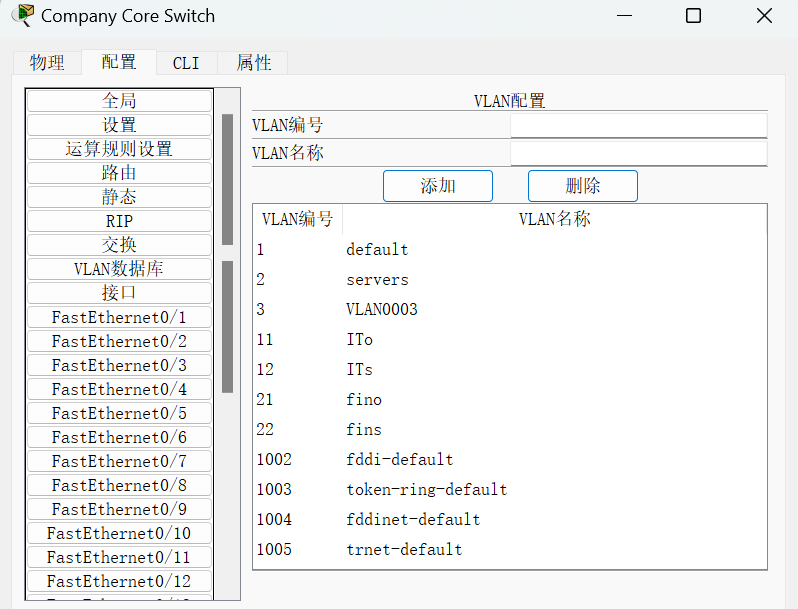
在本项目中，我们通过构建虚拟局域⽹（VLAN）来逻辑上为每个部⻔建⽴其独⽴的局域⽹。为了实现这⼀⽬标，我们选择采⽤VTP来简化VLAN的管理和配置过程。

1. 将核心交换机配置为VTP的server模式

vtp domain mycompany

vtp mode server

(2) 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。

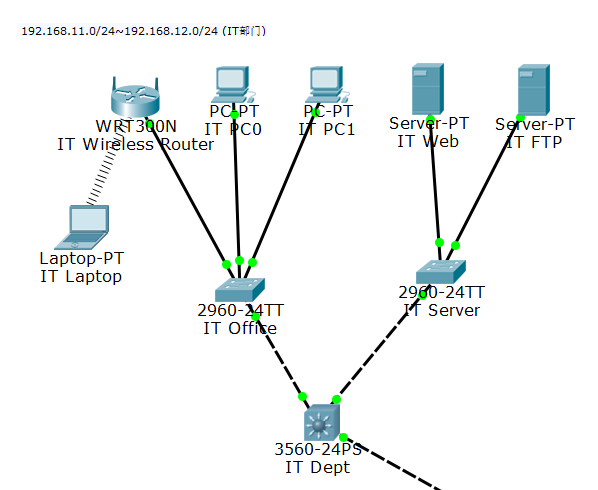


**3.3各部门网络拓扑图**

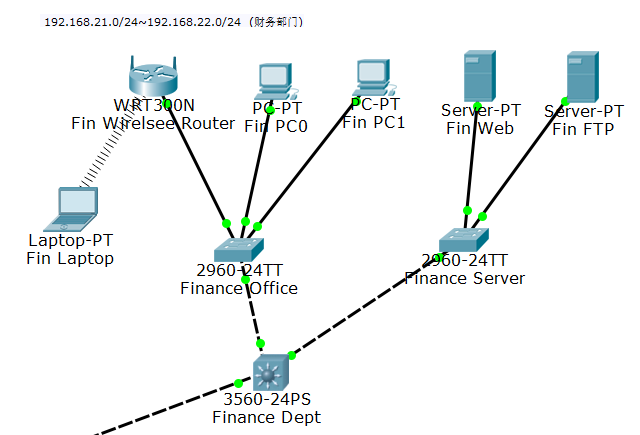
本网络系统共包括两个部门：IT部门、财务部门。

下面是每个部门的网络拓扑图。

**3.3.1 IT部门网络拓扑图**



**3.3.2 财务部门网络拓扑图**



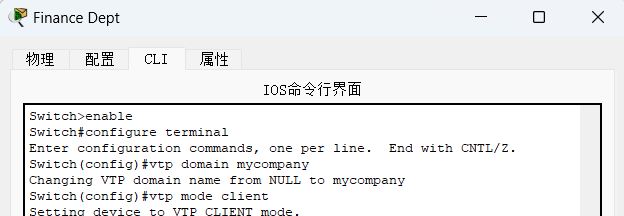
**3.4配置各部门VLAN**

**3.4.1 各部门VTP设置**

将部⻔交换机配置为VTP的client模式，使得它们可以同步所有VLAN。

vtp domain mycompany

vtp mode client



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客⼾端模式的交换机。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，从⽽为各个部⻔提供了独⽴且安全的通信环境。

**3.4.2 VLAN创建与命名**

(1) 添加VLAN，对应每个部门内部的两个虚拟局域网：

vlan 2

name servers

vlan 11

name ITo

vlan 12

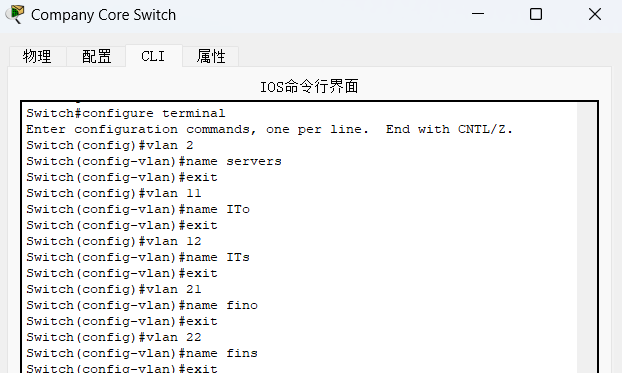
name ITs

vlan 21

name fino

vlan 22

name fins



(2) 接口划分：

终端连接端口配置为 Access 模式并绑定对应 VLAN：

# 核心层

interface f0/1

switchport access vlan 2

# IT部门

interface f0/2

switchport access vlan 11

interface f0/3

switchport access vlan 12

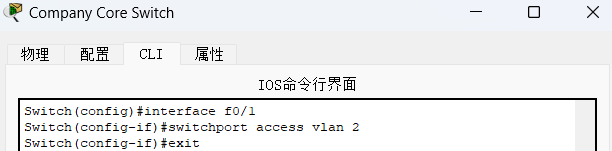
# 财务部门

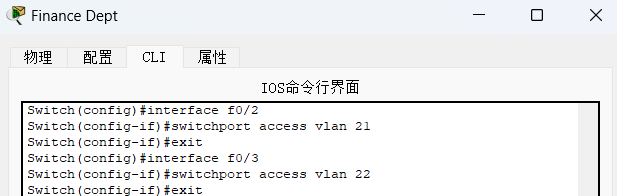
interface f0/2

switchport access vlan 21

interface f0/3

switchport access vlan 22





(3) VLAN 接口配置 IP:

interface vlan 2

ip address 192.168.0.1 255.255.255.0

interface vlan 11

ip address 192.168.11.1 255.255.255.0

interface vlan 12

ip address 192.168.12.1 255.255.255.0

interface vlan 21

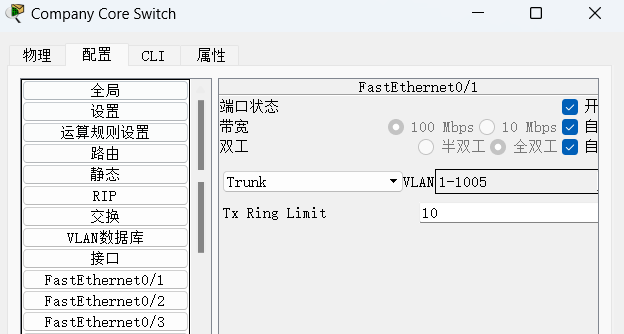
ip address 192.168.21.1 255.255.255.0

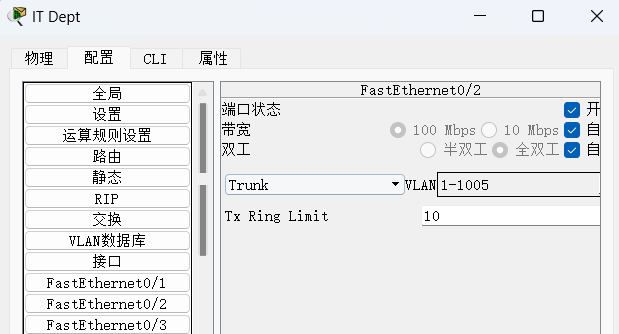
interface vlan 22

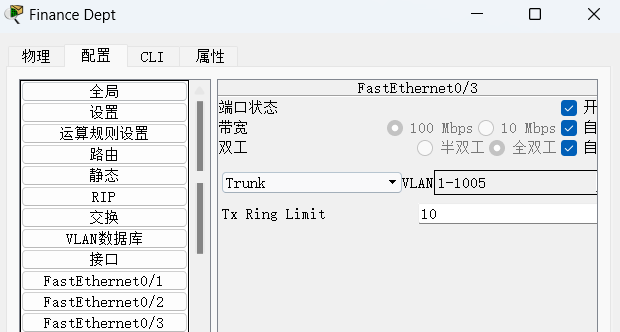
ip address 192.168.22.1 255.255.255.0



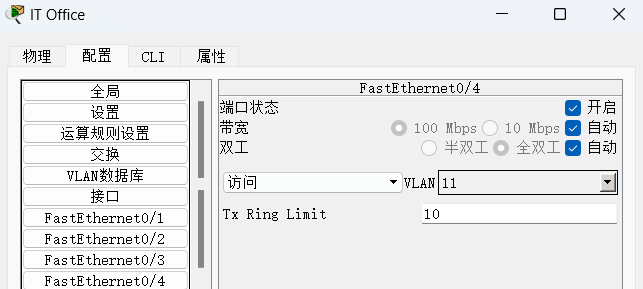
(4) 将核⼼交换机到部⻔总交换机，部⻔总交换机到部⻔分交换机的接⼝设置为**Trunk**：

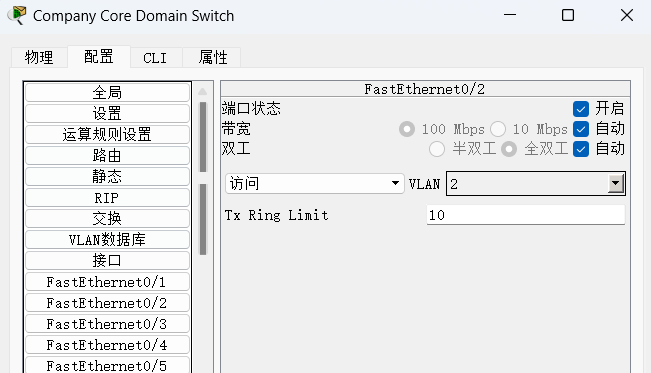






将部⻔分交换机到终端的接⼝设置为**Access**,并选择对应VLAN：





当一条线路上同时传输多个VLAN数据时，交换机之间传递数据时自动添加一个Tag，里面含有该数据原始的Vlan，数据传递到终点时，交换机去掉Tag标记，同时将数据传输给属于这个Vlan的接口。

**3.5 配置各部⻔服务器静态IP**

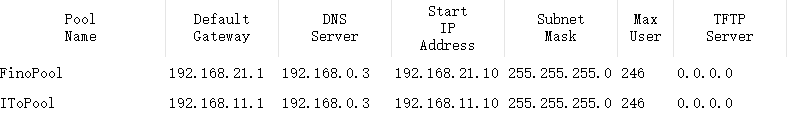
在这里设置部门内部服务器，由于服务器一般不会轻易改变，所以设置为静态IP。部门服务器静态IP配置如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **服务器** | **IP** | **⼦⽹掩码** | **⽹关** | **DNS** |
| IT Web | 192.168.12.16 | 255.255.255.0 | 192.168.12.1 | 192.168.0.3 |
| IT FTP | 192.168.12.25 | 255.255.255.0 | 192.168.12.1 | — |
| Fin Web | 192.168.22.16 | 255.255.255.0 | 192.168.22.1 | 192.168.0.3 |
| Fin FTP | 192.168.22.25 | 255.255.255.0 | 192.168.22.1 | 192.168.0.3 |

**3.6 配置DHCP**

为了给各部门的终端自动分配和管理IP地址及相关配置参数，需要配置DHCP。

(1)在核心层的DHCP服务器中为每个VLAN配置DHCP池：



(2)在核⼼交换机中为VLAN启⽤DHCP中继功能：



退出接口配置之后，启用设备的IP路由功能。ip routing 命令的意思是启用设备的IP路由能力，即让设备不仅可以作为交换机处理VLAN之间的内部数据交换，还可以作为路由器在不同网络之间转发数据包。

(3)在各个终端中请求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

**3.7 配置ACL**

已经为核心层、各部门office、各部门服务器分别配置了VLAN。不同VLAN之间无法进行通信，但在内网中，我们要求：

a.核心层可以访问部门终端，部门终端可以访问核心层终端。

b.部门office和部门服务器可以互相访问。

C.部门终端不可访问另一个部门的终端。

d.外网可以访问核心层，核心层可以访问外网，这样一来，核心层可与任何网段交互。

因此我们加入ACL访问控制来实现要求。

具体配置指令如下：

access-list 102 permit ip 192.168.11.0 0.0.0.255 192.168.0.0 0.0.0.255

access-list 102 permit ip 192.168.0.0 0.0.0.255 192.168.11.0 0.0.0.255

access-list 102 permit ip 192.168.12.0 0.0.0.255 192.168.0.0 0.0.0.255

access-list 102 permit ip 192.168.0.0 0.0.0.255 192.168.12.0 0.0.0.255

access-list 102 permit ip 192.168.21.0 0.0.0.255 192.168.0.0 0.0.0.255

access-list 102 permit ip 192.168.0.0 0.0.0.255 192.168.21.0 0.0.0.255

access-list 102 permit ip 192.168.22.0 0.0.0.255 192.168.0.0 0.0.0.255

access-list 102 permit ip 192.168.0.0 0.0.0.255 192.168.22.0 0.0.0.255

access-list 102 permit udp any eq bootpc any eq bootps

access-list 102 permit udp any eq bootps any eq bootpc

access-list 102 permit ip 192.168.0.0 0.0.0.255 any

access-list 102 permit ip any 192.168.0.0 0.0.0.255

int vlan 2

ip access-group 102 in

access-list 111 permit ip 192.168.12.0 0.0.0.255 192.168.11.0 0.0.0.255

access-list 111 permit ip 192.168.11.0 0.0.0.255 192.168.12.0 0.0.0.255

access-list 111 permit ip 192.168.0.0 0.0.0.255 192.168.11.0 0.0.0.255

access-list 111 permit ip 192.168.11.0 0.0.0.255 192.168.0.0 0.0.0.255

access-list 111 permit udp any eq bootpc any eq bootps

access-list 111 permit udp any eq bootps any eq bootpc

int vlan 11

ip access-group 111 in

access-list 112 permit ip 192.168.11.0 0.0.0.255 192.168.12.0 0.0.0.255

access-list 112 permit ip 192.168.12.0 0.0.0.255 192.168.11.0 0.0.0.255

access-list 112 permit ip 192.168.12.0 0.0.0.255 192.168.0.0 0.0.0.255

access-list 112 permit ip 192.168.0.0 0.0.0.255 192.168.12.0 0.0.0.255

int vlan 12

ip access-group 112 in

access-list 121 permit ip 192.168.22.0 0.0.0.255 192.168.21.0 0.0.0.255

access-list 121 permit ip 192.168.21.0 0.0.0.255 192.168.22.0 0.0.0.255

access-list 121 permit ip 192.168.0.0 0.0.0.255 192.168.21.0 0.0.0.255

access-list 121 permit ip 192.168.21.0 0.0.0.255 192.168.0.0 0.0.0.255

access-list 121 permit udp any eq bootpc any eq bootps

access-list 121 permit udp any eq bootps any eq bootpc

int vlan 21

ip access-group 121 in

access-list 122 permit ip 192.168.21.0 0.0.0.255 192.168.22.0 0.0.0.255

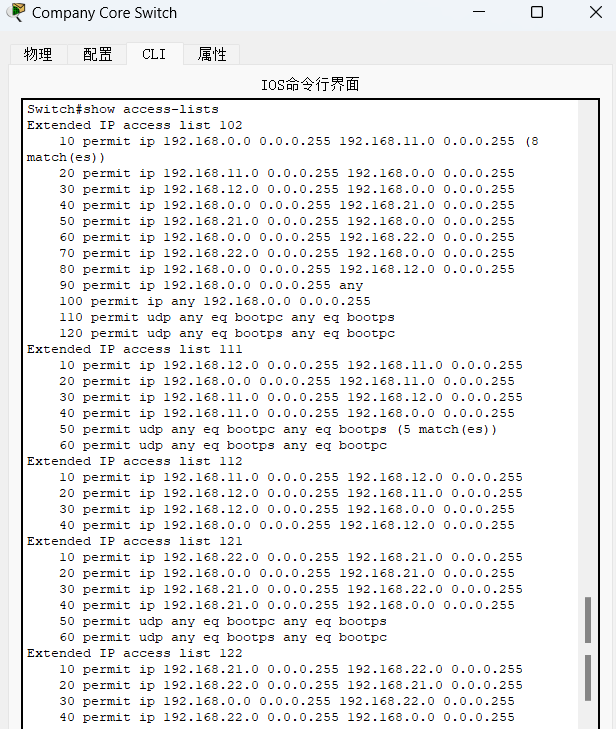
access-list 122 permit ip 192.168.22.0 0.0.0.255 192.168.21.0 0.0.0.255

access-list 122 permit ip 192.168.22.0 0.0.0.255 192.168.0.0 0.0.0.255

access-list 122 permit ip 192.168.0.0 0.0.0.255 192.168.22.0 0.0.0.255

int vlan 22

ip access-group 122 in



**3.8 配置RIP**

通过启用 ip routing 和配置 RIP v2，设备可以自动学习和广播 192.168.11.0、12.0、21.0、22.0 和 0.0 等多个网段的路由信息，使连接在不同 VLAN 和设备上的子网互通。

ip routing

router rip

version 2

no auto-summary

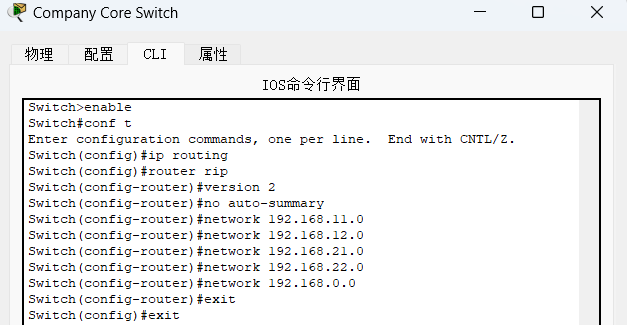
network 192.168.11.0

network 192.168.12.0

network 192.168.21.0

network 192.168.22.0

network 192.168.0.0

****

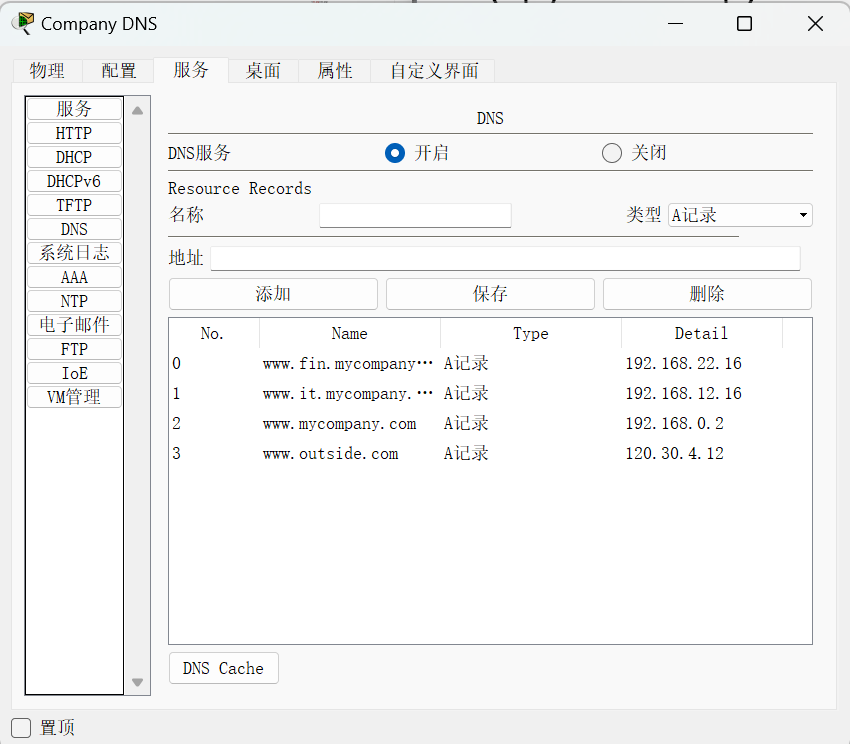
**3.9 配置Web服务**

在各个Web服务器处选择服务-HTTP，开启http和https：

****

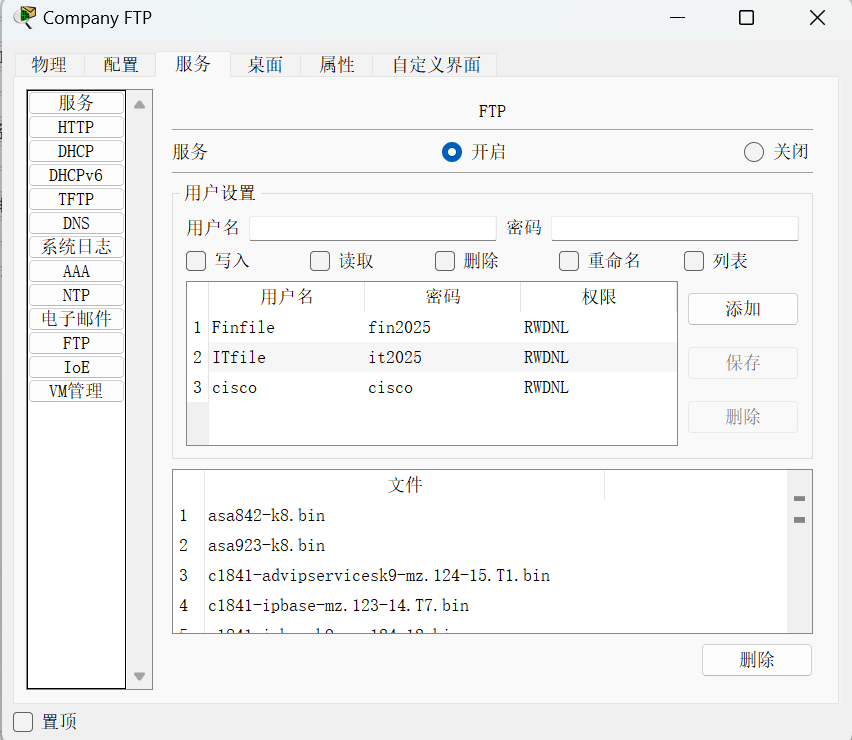
在核心层和各部门DNS服务器处记录Web服务器的IP与对应的域名：

|  |  |  |
| --- | --- | --- |
| **域名** | **IP** | **说明** |
| www.mycompany.com | 192.168.0.2 | 企业Web服务器 |
| www.it.mycompany.com | 192.168.12.16 | IT部门Web服务器 |
| www.fin.mycompany.com | 192.168.22.16 | 财务部门Web服务器 |



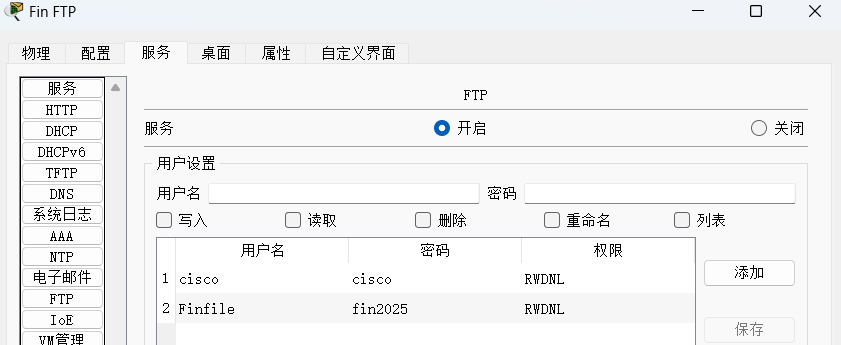
**3.10 配置FTP服务**

在核⼼层FTP服务器上选择服务-FTP，开启FTP服务，然后配若⼲邮箱⽤⼾的⽤⼾名、密码和⽂件访问权限：



在各部门FTP服务器添加该部门的⽤⼾名、密码和⽂件访问权限：

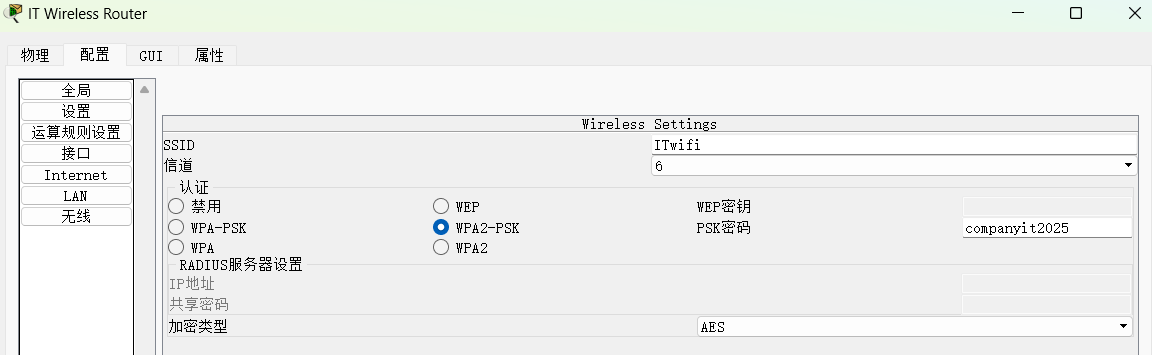




**3.11 配置WIFI**

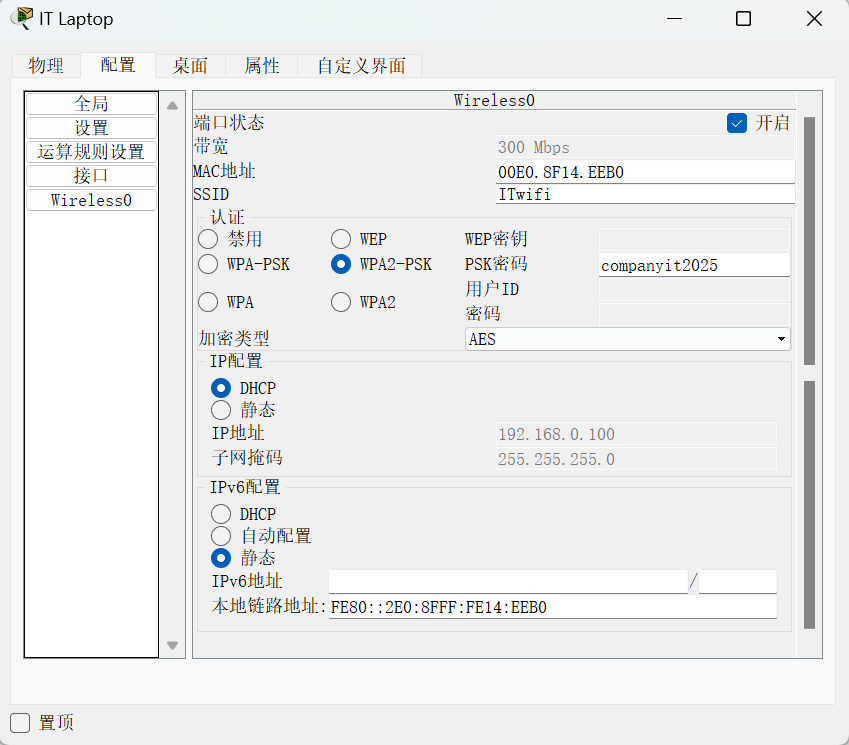
用无线路由器配置WiFi，从而把有线网络信号转换成无线信号，供支持其技术的相关终端接收，实现无线上网。

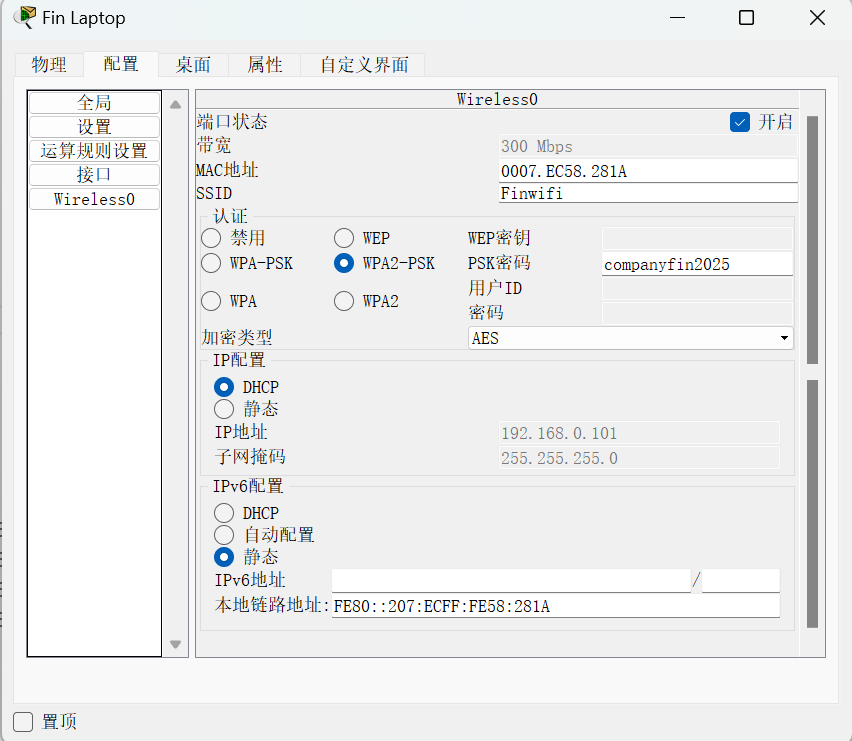
在无线路由器配置-无线中进行配置，设置ID、密码等参数。

****

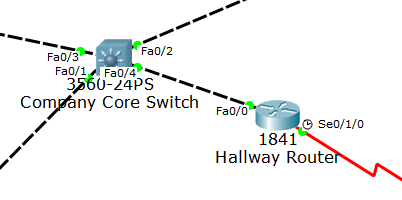
****

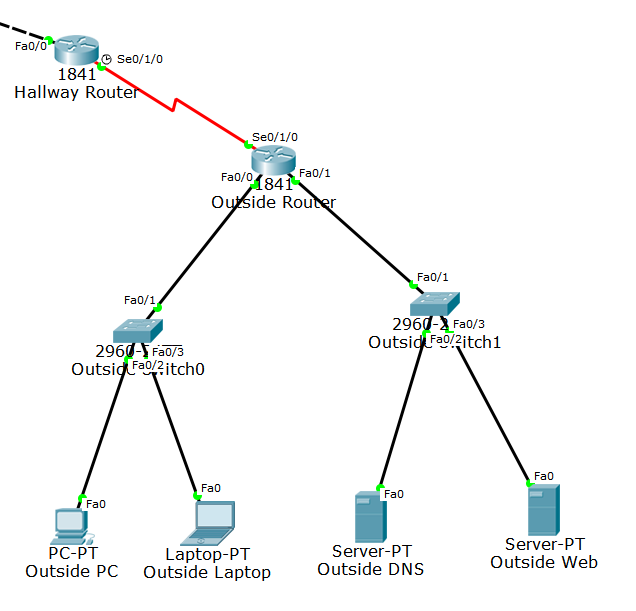
并无线设备笔记本电脑配置-Wireless0中进行配置，连接无线网络。





1. **外网设计及内外网连通**
   1. **外网区域拓扑图**



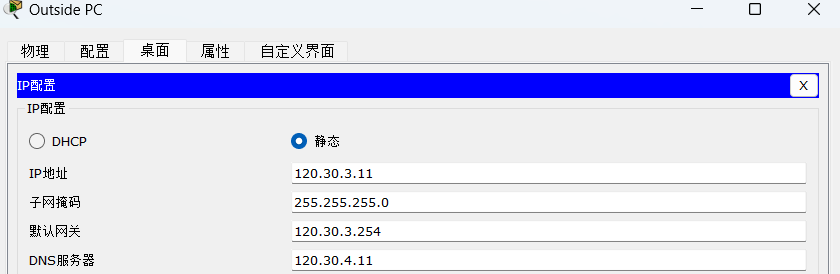


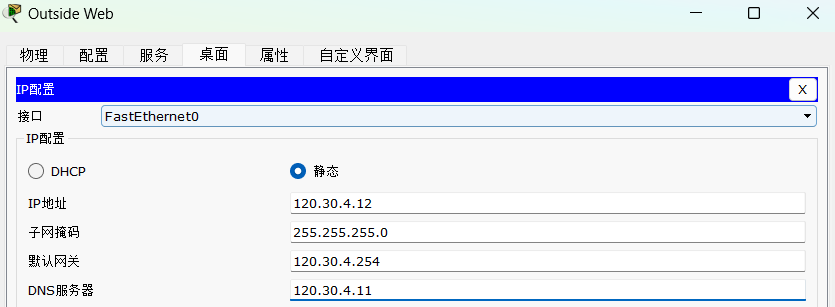
上图为外网区域的拓扑图，连接企业核心三层交换机，之后会在该交换机上配置外网的vlan（vlan3），连通内外网。直接连接的是网关路由器，路由器上需要配置NAT和静态路由，负责内外网的地址映射和连通。连接网关路由器的是外网路由器。外网区域有两台交换机分别连接主机和服务器。服务器包括Web服务器和DNS服务器，支持连接外网Web和企业核心层Web。

* 1. **外网静态IP与路由器端口配置**

项目核心在于内网设计，因此外网比较简陋，简单地用静态地址即可。静态IP配置如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **服务器** | **IP** | **⼦⽹掩码** | **⽹关** | **DNS** |
| Outside PC | 120.30.3.11 | 255.255.255.0 | 120.30.3.254 | 120.30.4.11 |
| Outside PC | 120.30.3.12 | 255.255.255.0 | 120.30.3.254 | 120.30.4.11 |
| Outside Web | 120.30.4.11 | 255.255.255.0 | 120.30.4.254 | 120.30.4.11 |
| Outside DNS | 120.30.4.12 | 255.255.255.0 | 120.30.4.254 | 120.30.4.11 |





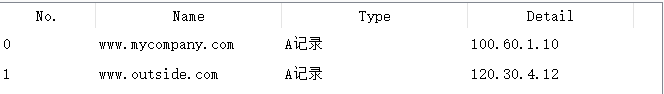
接下来，配置网关路由器和外网路由器：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **服务器** | **端口** | **IP** | **⼦⽹掩码** | **服务器** |
| Outside Router | FastEthernet0/0 | 120.30.3.254 | 255.255.255.0 | Outside Router |
| Outside Router | FastEthernet0/1 | 120.30.4.254 | 255.255.255.0 | Outside Router |
| Outside Router | Serial0/1/0 | 202.120.17.29 | 255.255.255.0 | Outside Router |
| Hallway Router | FastEthernet0/0 | 192.168.100.2 | 255.255.255.0 | Hallway Router |
| Hallway Router | Serial0/1/0 | 202.120.17.18 | 255.255.255.0 | Hallway Router |

* 1. **外网DNS配置**

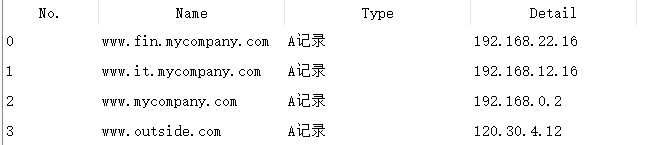
我们需要一个能连接的外部Web网络，并且能够从外网连通企业核心层Web。假设分给公司的公网地址与上次项目中学校的公网地址一致，为100.60.1.10/24。在外部DNS添加域名等信息：

|  |  |  |
| --- | --- | --- |
| **域名** | **IP** | **说明** |
| www.mycompany.com | 100.60.1.10 | 企业供外⽹访问的Web服务器 |
| www.outside.com | 120.30.4.12 | 外部其他服务器 |



其中企业核心层Web的IP为公网地址100.60.1.10/24。www.outside.com代表外部服务器。为了使企业内部能连通外部服务器，还需在核心层DNS添加外网域名，添加后的配置为：

|  |  |  |
| --- | --- | --- |
| **域名** | **IP** | **说明** |
| www.mycompany.com | 192.168.0.2 | 企业Web服务器 |
| www.it.mycompany.com | 192.168.12.16 | IT部门Web服务器 |
| www.fin.mycompany.com | 192.168.22.16 | 财务部门Web服务器 |
| www.outside.com | 120.30.4.12 | 外部其他服务器 |



* 1. **NAT配置**

由Hallway Router来提供NAT服务。由于只有核心层能与外网交互，将核心层192.168.0.2-192.168.0.5映射到100.60.1.10-100.60.1.13。

配置指令如下：

#创建NAT

interface f0/0

ip nat inside

interface s0/1/0

ip nat outside

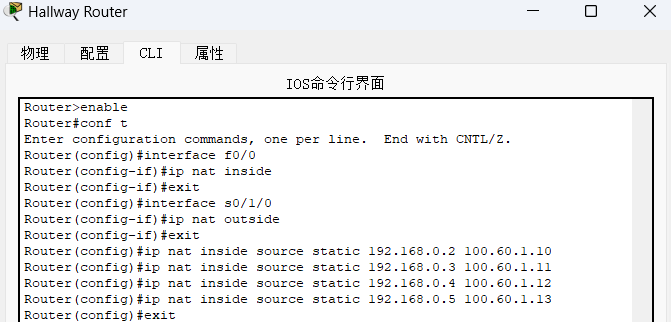
#NAT映射

ip nat inside source static 192.168.0.2 100.60.1.10

ip nat inside source static 192.168.0.3 100.60.1.11

ip nat inside source static 192.168.0.4 100.60.1.12

ip nat inside source static 192.168.0.5 100.60.1.13



* 1. **静态路由配置**

配置好NAT后，还需要在企业核心交换机、网关路由器、外网路由器上分别配置静态路由。核心交换机是一个三层交换机，为了在该交换机上配置静态路由，首先需要为外网分配一个可用的vlan，配置命令如下：

#创建vlan 3

VLAN:

vlan 3

name VLAN0003

#端口允许vlan 3

interface f0/4

switchport access vlan 3

#配置vlan 3地址

interface vlan 3

ip address 192.168.100.1 255.255.255.0

no shutdown



分配vlan 3给外网。配置成功后，开始配置静态路由，在三台设备上的配置命令分别如下：

企业核心交换机:

ip route 120.30.0.0 255.255.0.0 vlan 3

网关路由器:

ip route 120.30.0.0 255.255.0.0 s0/1/0

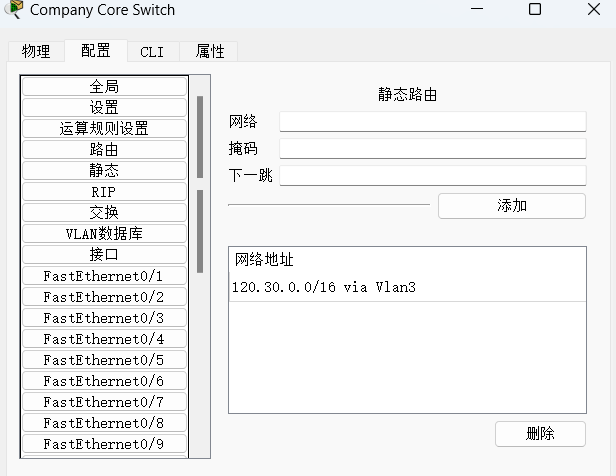
ip route 192.168.0.0 255.255.0.0 f0/0

ip route 100.60.1.0 255.255.255.0 f0/0

外部路由器:

ip route 192.168.0.0 255.255.0.0 s0/1/0

ip route 100.60.1.0 255.255.255.0 s0/1/0

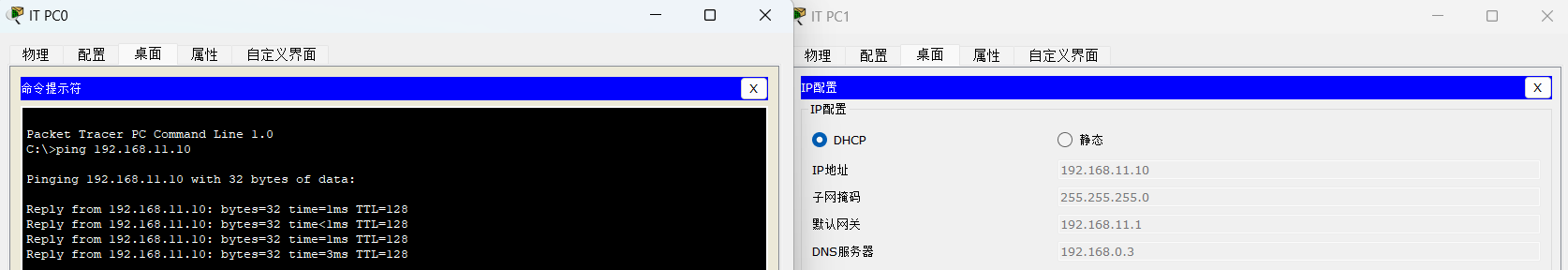


至此，内外网已经完成连通，并满足Web访问的需求。

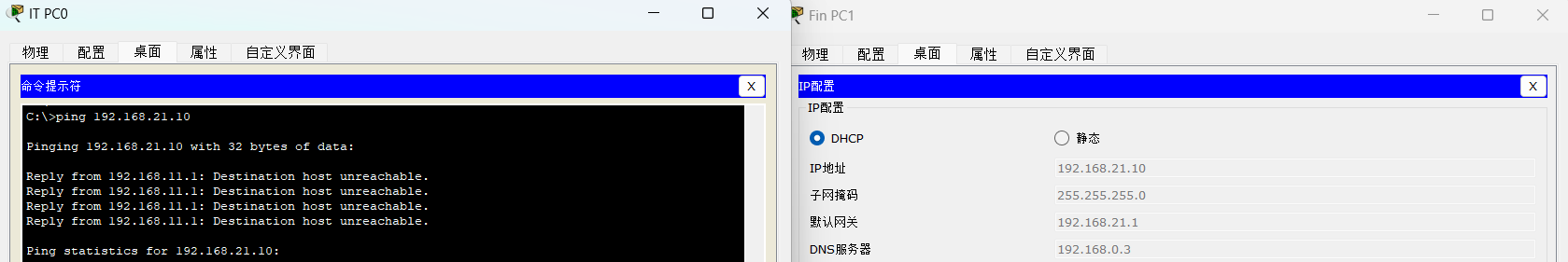
**5.网络测试**

**5.1 内网连通性测试**

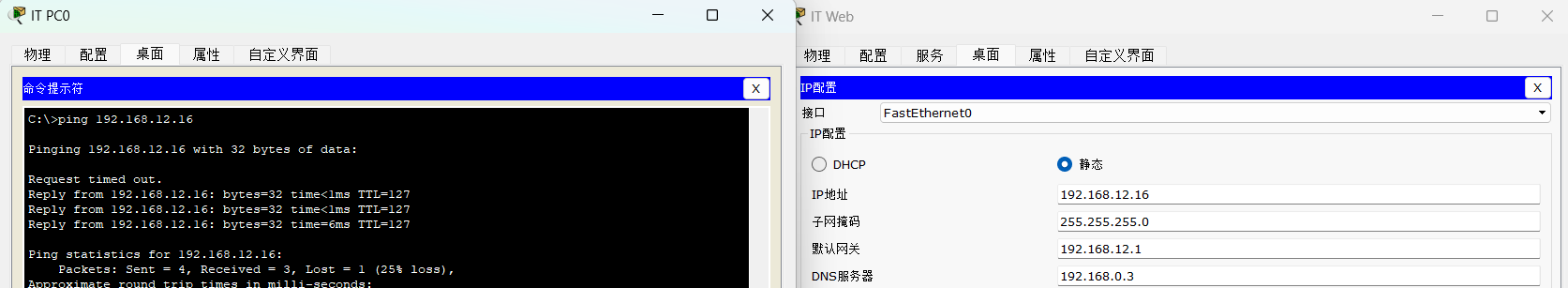
同一office中的终端相互之间：可以连通

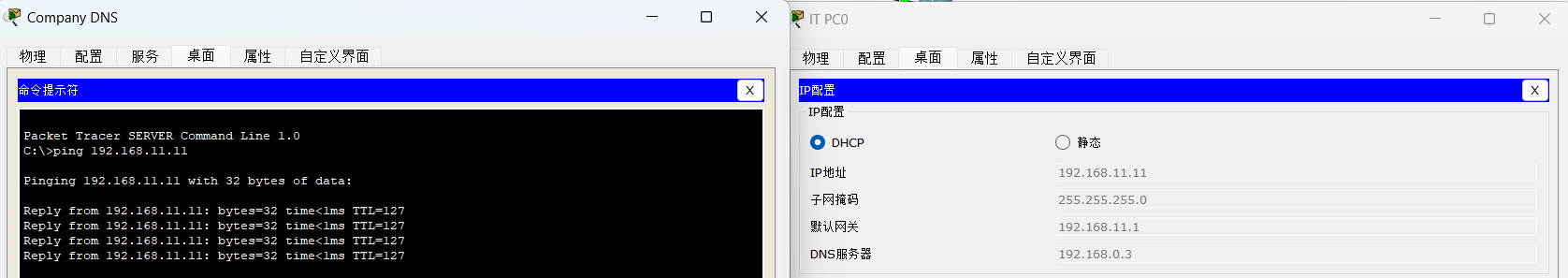


不同部门的终端之间：无法连通

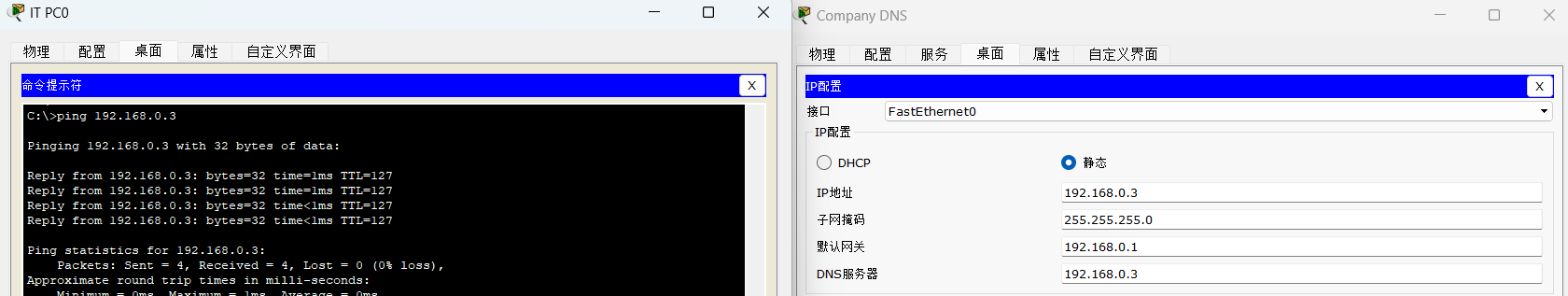


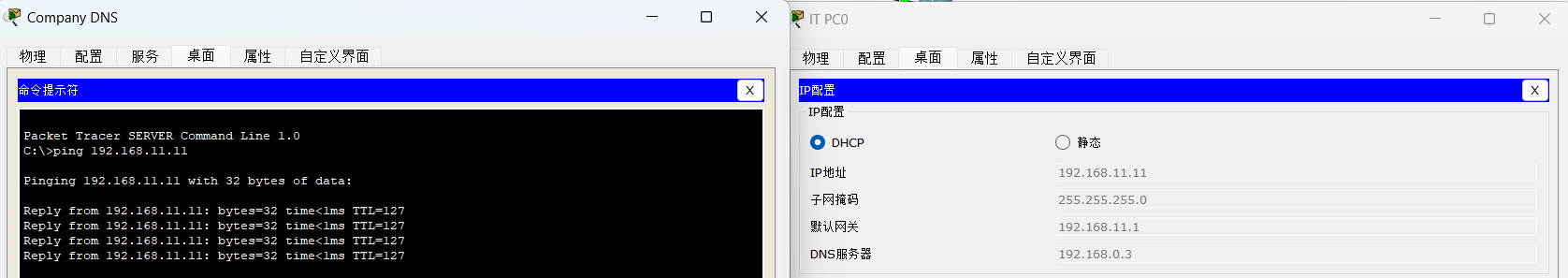
同一部门的office和服务器之间：可以相互连通





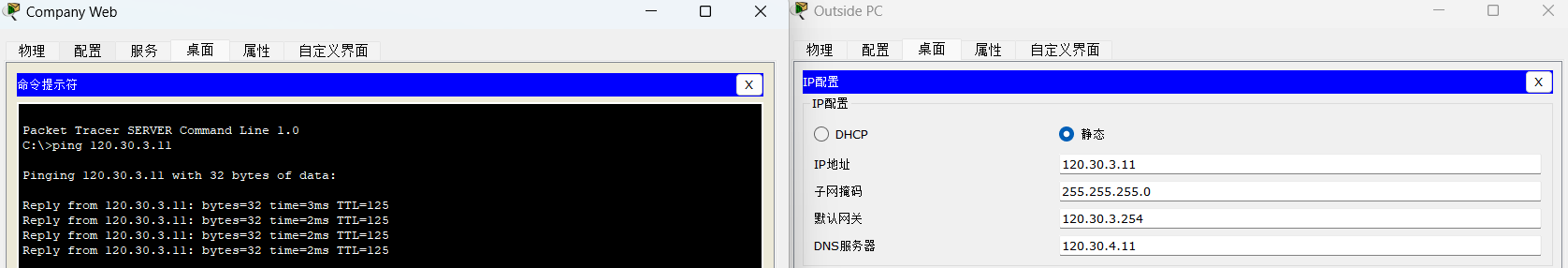
核心层与各部门终端：相互连通

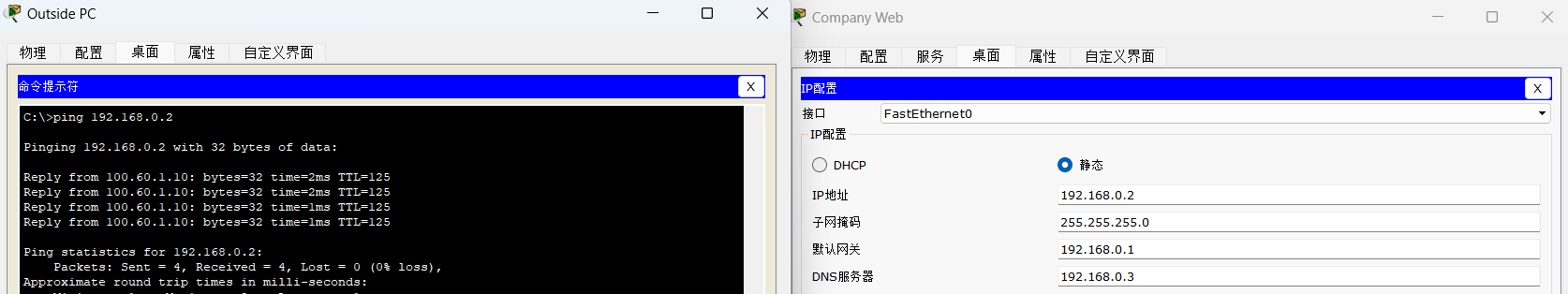




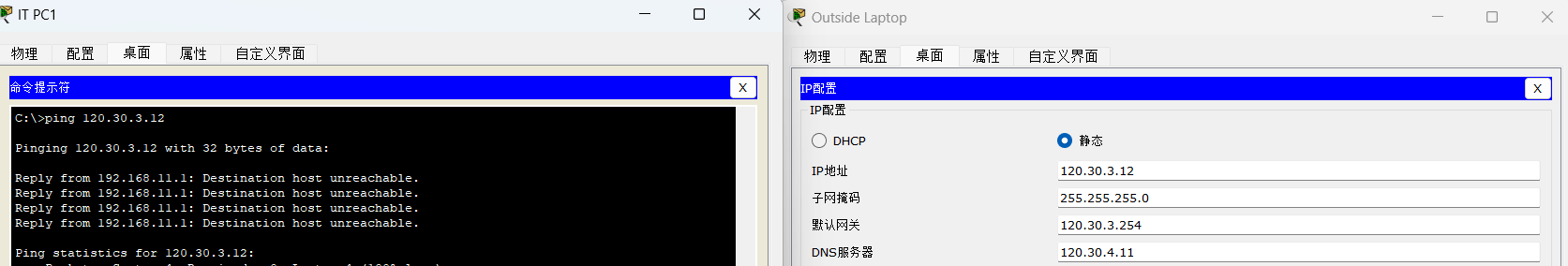
**5.2 内外网间连通性测试**

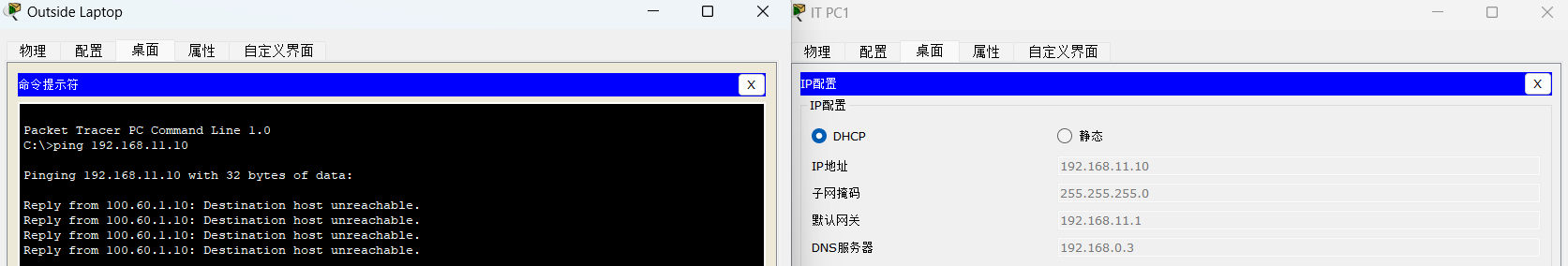
核心层与外部终端：相互连通





外部终端与各部门终端：无法连通

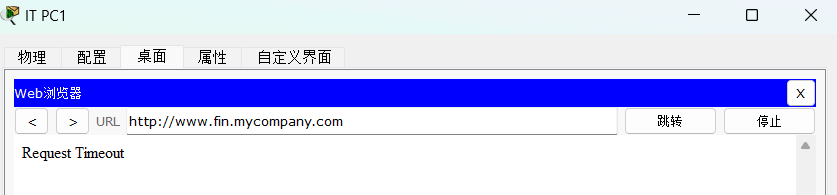




**5.3 Web服务器测试**

某部门office可访问本部门Web服务，不可访问其他部门Web服务





各部门可以访问核心层Web服务，核心层可以访问各部门Web服务



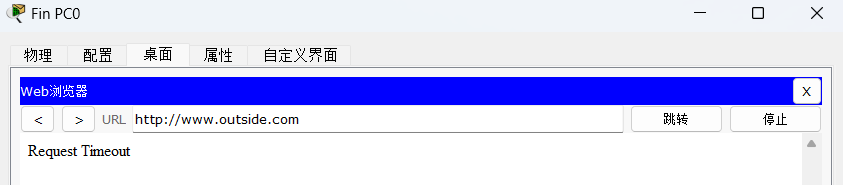


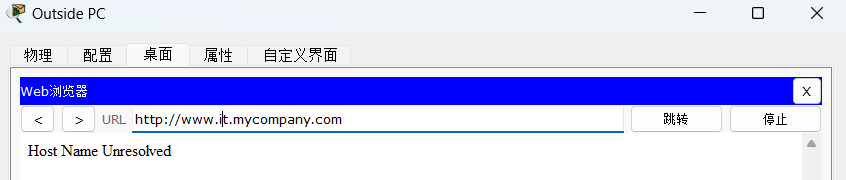
核心层可访问外部Web服务，外部终端可以访问核心层Web服务





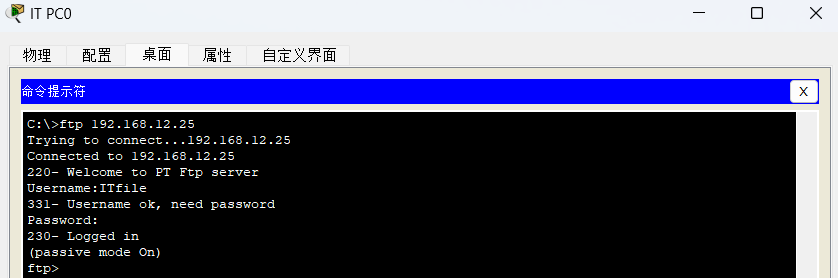
外部不可访问各部门Web服务，各部门不可访问外部Web服务

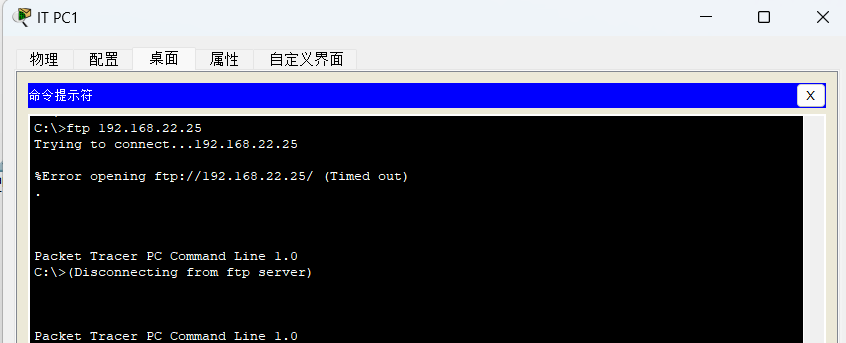




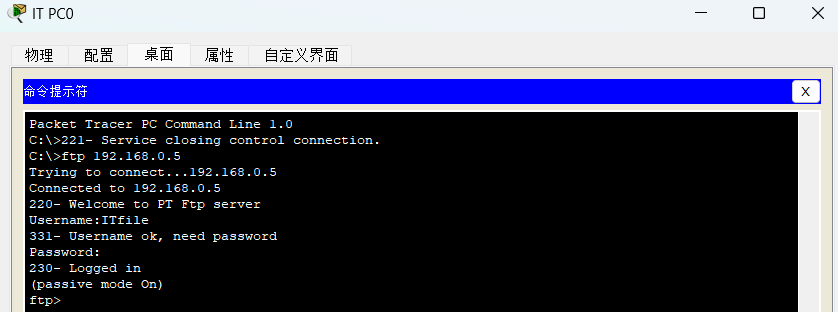
**5.4 FTP服务器测试**

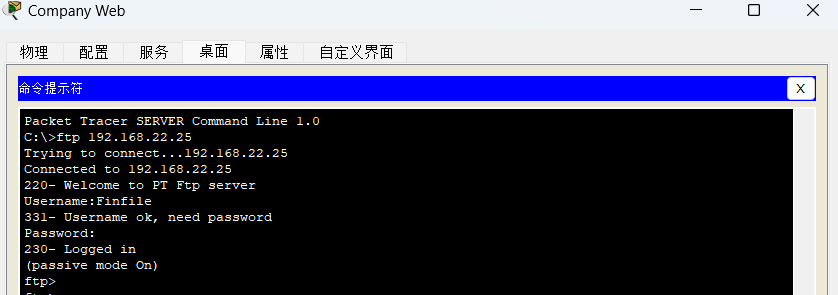
某部门office可访问本部门FTP服务，不可访问其他部门FTP服务



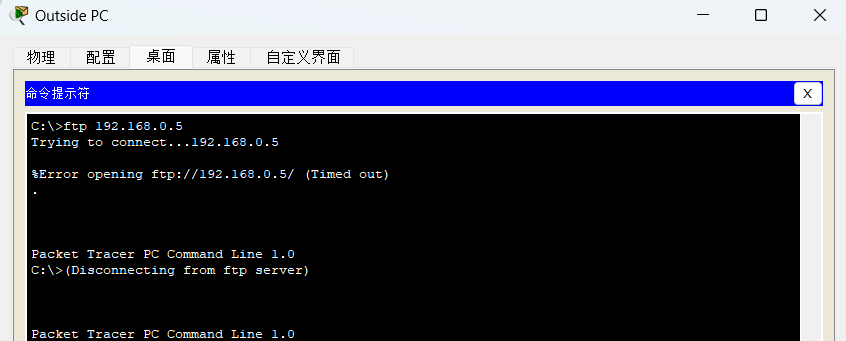


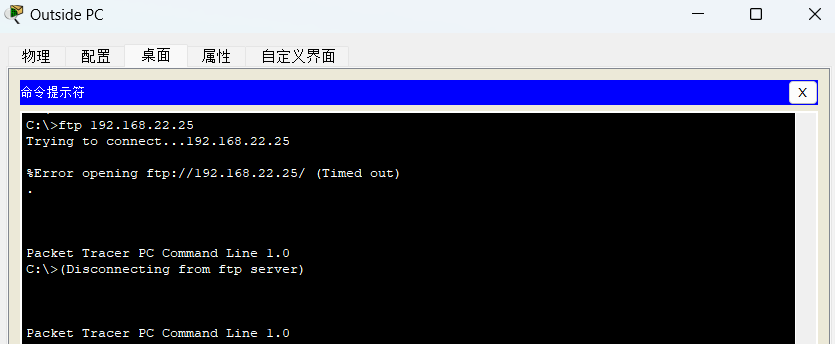
各部门可以访问核心层FTP服务，核心层可以访问各部门FTP服务





外部终端不可访问核心层FTP服务，不可访问各部门FTP服务





**6.小结**

该项目是一个小型公司的网络结构设计。在设计的过程中，我们从实际应用出发，加入了一系列vlan划分和访问控制的设计，对各个终端的功能做出限定，确保内网的安全性。核心三层交换机的选择，也使结构更加清晰、更加便于管理。动态路由RIP的设计减少了配置静态路由的冗余操作，增强了网络的安全性和可靠性。同时，选择RIP而非OSPF是考虑到了网络的规模，选择RIP更简单，开销也更小。此外，围绕合理性和安全性，还有种种细节上的设计，比如说WiFi的接入和DHCP中继功能等等。