## Appendix 1: Network Management Assignment Template 1

**College of Safety Science and Engineering**

**The First Semester of 2024-2025 Academic Year**

**Final Assessment for Network Management Course**

**TOPIC Title：典型企业网络规划与管理的设计与实现**

**CLASS NO： 22034201**

**Student NO： 221240002**

**Name： 陈书涵 **

Table of Contents

1. Background 3

2. Project Environment 3

3. Network Planning 3

4. Configuration, Verification and Testing of the Major Network devices and Functions 3

4.1 Configuration, Verification and Testing of Basic Management Configurations 4

4.2 Configuration, Verification and Testing of Routing Configuration 4

4.3 Configuration, Verification and Testing of VLAN 4

4.4 Configuration, Verification and Testing of ACLs 4

4.5 Configuration, Verification and Testing of NAT 4

4.6 Deployment, Verification and Testing of Common services 4

4.7 Configuration, Verification and Testing of Network Management Protocols (Agent) 4

4.8 Configuration, Verification and Testing of Network Management Software /Applications (Manager) 4

4.9 Configuration, Verification and Testing of Other Functions 4

5. Analysis and Summary of the Project 4

6. Summary 5

## Background（2 point）

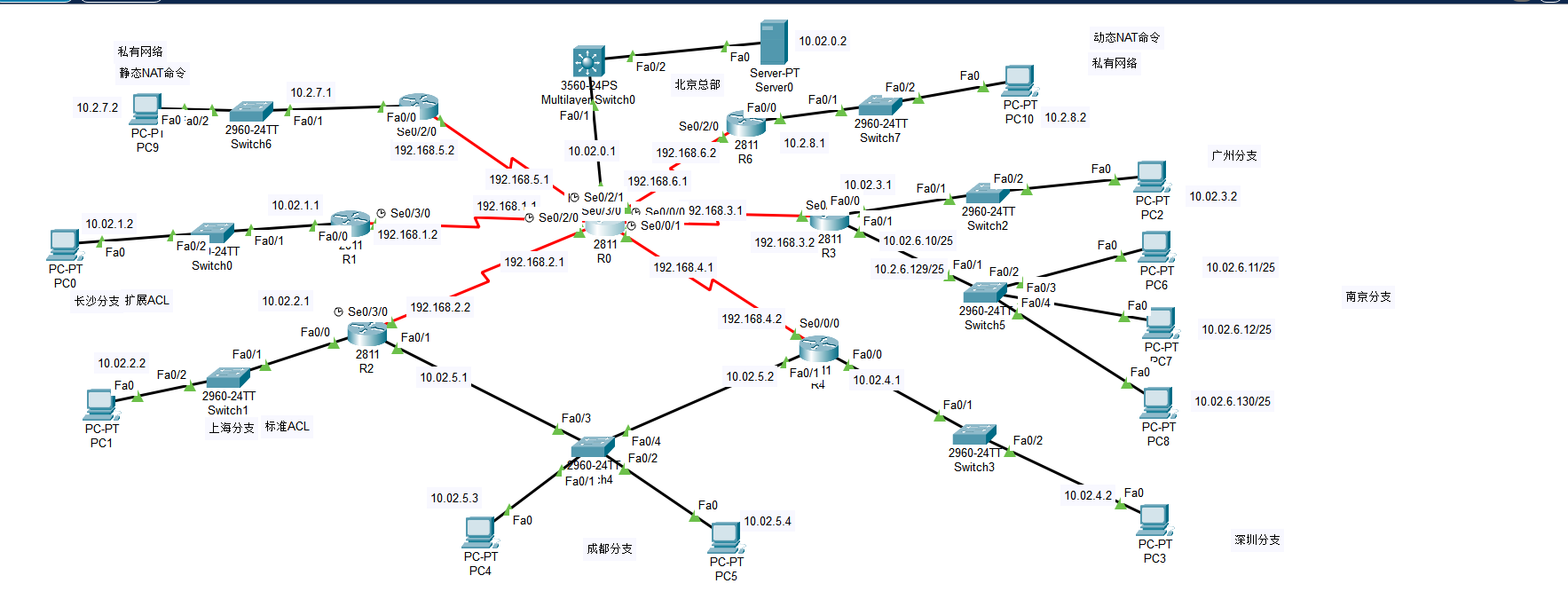
模拟一个小型企业网络环境，在各地有多个分支，并且在总部配置了服务器区域，每个分支归属于一个网，并采用备份冗余备份提高网络可靠性。使用ACL命令，限制某些分支对服务器的访问，通过配置OSPF和NAT命令，使得各个分支之间能相互通信并访问外网和内网服务器，但是

1. 限制长沙分支，只能通过http服务访问北京总部服务器
2. 限制武汉、杭州分支，只能通过虚拟地址访问外网
3. 限制上海分支只能被北京总部访问
4. 将给南京分支划分vlan分成两个不同的部门
5. R4路由器访问R0时，需要PPP认证

## Project Environment（1 point）

Cisco IOS 15.1 (4) M4，软件类型为 C2800NM-ADVIPSERVICESK9-M，发布版本（RELEASE SOFTWARE）

## Network Planning （7 points）



|  |  |  |  |
| --- | --- | --- | --- |
| Router  Designation | Host name | Fast Ethernet Address /Sub-net Mask | Serial Interface  Address /Sub-net Mask |
| R0 | R0 | F0/0: 10.02.0.1/24 | S0/3/0:192.168.1.1  S0/3/1:192.168.2.1  S0/0/0:192.168.3.1  S0/0/1:192.168.4.1 |
| R1 | R1 | F0/0: 10.02.1.1/24 | S0/3/0: 192.168.1.2 |
| R2 | R2 | F0/0: 10.02.2.1/24  F0/1:10.02.5.1/24 | S0/3/0: 192.168.2.2 |
| R3 | R3 | F0/0:10.02.3.1/24  F0/1:10.02.3.3/24 | S0/0/0:192.168.3.2 |
| R4 | R4 | F0/0:10.02.4.1/24  F0/1:10.02.5.2/24 | S0/0/0:192.168.4.2 |
| R5 | R5 | F0/0:10.02.7.1/24 | S0/2/0:192.168.5.2 |
| R6 | R6 | F0/0:10.02.8.1/24 | S0/2/0:192.168.6.2 |
| PC0 | IP Address: 10.02.1.2 netmask: 255.255.255.0 gateway: 10.02.1.1 | | |
| PC1 | IP Address: 10.02.2.2 netmask: 255.255.255.0 gateway: 10.02.2.1 | | |
| PC2 | IP Address: 10.02.3.2 netmask: 255.255.255.0 gateway: 10.02.3.1 | | |
| PC3 | IP Address: 10.02.4.2 netmask: 255.255.255.0 gateway: 10.02.4.1 | | |
| PC4 | IP Address: 10.02.5.3 netmask: 255.255.255.0 gateway: 10.02.5.1/2 | | |
| PC5 | IP Address: 10.02.5.4 netmask: 255.255.255.0 gateway: 10.02.5.2/1 | | |
| PC6 | IP Address: 10.02.6.11 netmask: 255.255.255.128 gateway: 10.02.6.10 | | |
| PC7 | IP Address: 10.02.6.12 netmask: 255.255.255.128 gateway: 10.02.6.10 | | |
| PC8 | IP Address: 10.02.6.130 netmask: 255.255.255.128 gateway: 10.02.6.129 | | |
| Serve0 | IP Address: 10.02.0.2 netmask: 255.255.255.0 gateway: 10.02.0.1 | | |
| PC9 | IP Address: 10.02.7.2 netmask: 255.255.255.0 gateway: 10.02.7.1 | | |
| PC10 | IP Address: 10.02.8.2 netmask: 255.255.255.0 gateway: 10.02.8.1 | | |

## Configuration, Verification and Testing of the Major Network devices and Functions

### 4.1 Configuration, Verification and Testing of Basic Management Configurations (8 points)

配置命令过多，此处仅展示R0配置的命令

console密码



enable密码



基于SSH的网络设备的管理配置：

R0(config)#ip domain-name chen

R0(config)#crypto key generate rsa general-keys modulus 2048

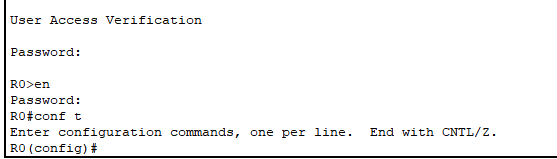
R0(config)#username chen privilege 15 secret 111

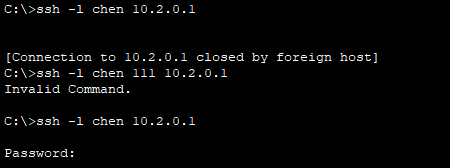
R0(config)#line vty 0 4

R0(config-line)#login local

R0(config-line)#transport input ssh

验证：

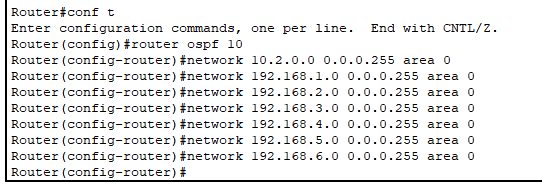




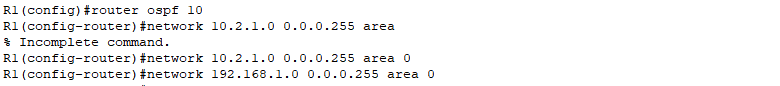
### 4.2 Configuration, Verification and Testing of Routing Configuration (8 points)

使用了OSPF协议配置动态路由，实现网段间的互通

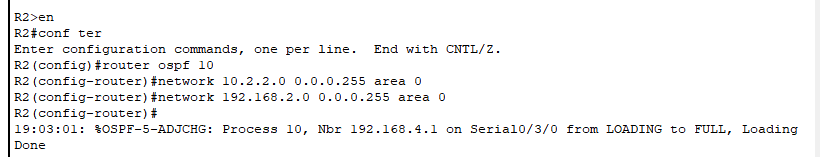
R0



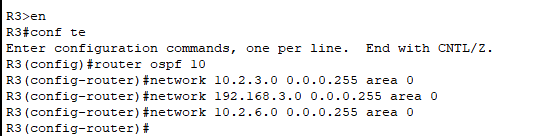
R1



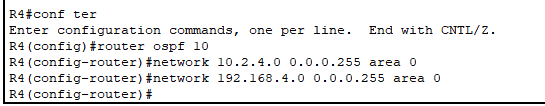
R2



R3



R4



R5（为了配置NAT命令，仅宣告了一个网段，没有宣告内网）

R5(config)router ospf 10

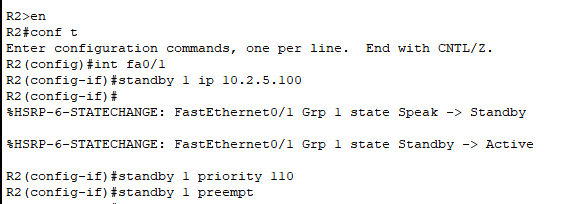
R5(config-router)#network 192.168.5.0 0.0.0.255 area 0

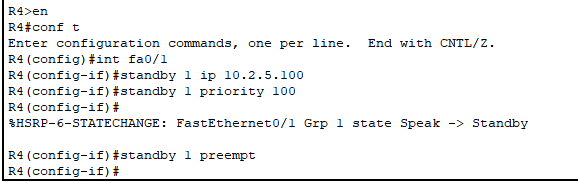
R6（为了配置NAT命令，仅宣告了一个网段，没有宣告内网）

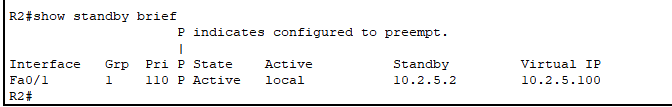
R6(config)router ospf 10

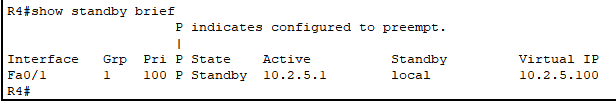
R6(config-router)#network 192.168.6.0 0.0.0.255 area 0

同时使用HSPF对R2和R4进行操作

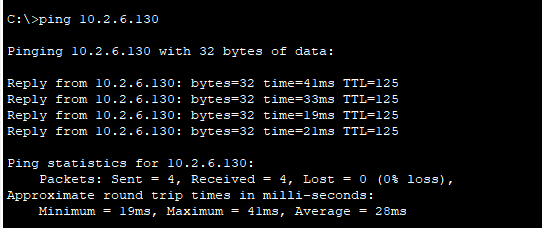
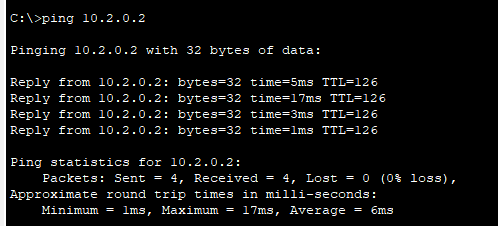






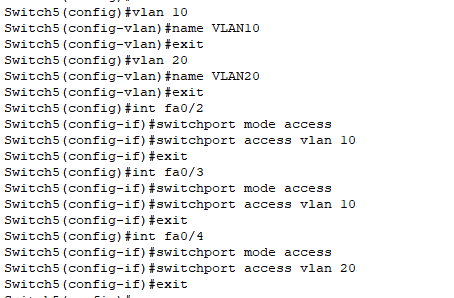


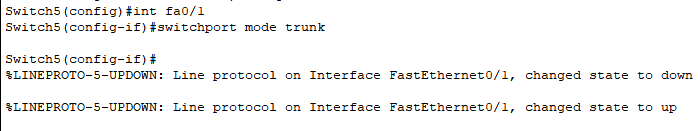
使用任意PC机ping其他PC机（此处仅展示一例）

### 4.3 Configuration, Verification and Testing of VLAN (8 points)

在交换机上配置vlan使得PC6和PC7在同一个VLAN，PC8在另外 一个 VLAN，





Vlan路由：

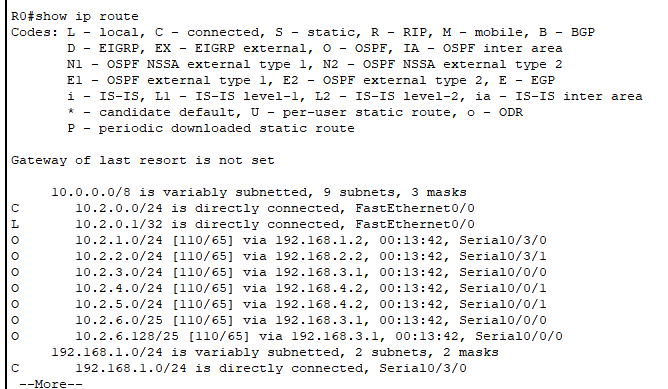
|  |  |
| --- | --- |
| PC6 | IP Address: 10.02.6.11 netmask: 255.255.255.128 gateway: 10.02.6.10 |
| PC7 | IP Address: 10.02.6.12 netmask: 255.255.255.128 gateway: 10.02.6.10 |
| PC8 | IP Address: 10.02.6.130 netmask: 255.255.255.128 gateway: 10.02.6.129 |

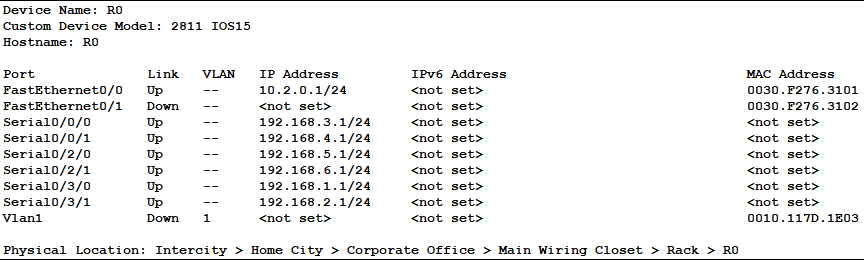
在路由器上配置VLAN路由

配置命令过多，此处仅展示R0的一个接口

R0(config)#int fa0/0

R0(config-if)#ip addr 10.2.0.1 255.255.255.0



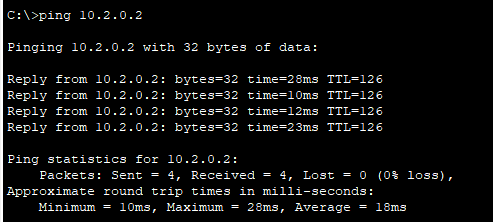


|  |  |  |  |
| --- | --- | --- | --- |
| R0 | R0 | F0/0: 10.02.0.1/24 | S0/3/0:192.168.1.1  S0/3/1:192.168.2.1  S0/0/0:192.168.3.1  S0/0/1:192.168.4.1 |

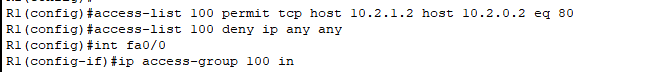
### 4.4 Configuration, Verification and Testing of ACLs (10 points)

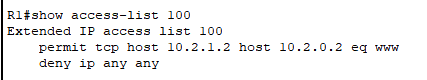
使用扩展ACL，限制PC0只能访问Server0的HTTP服务

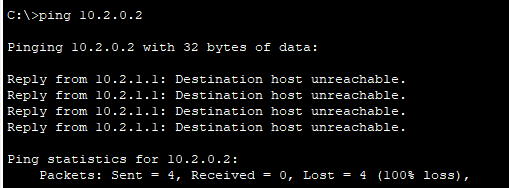
配置扩展ACL前

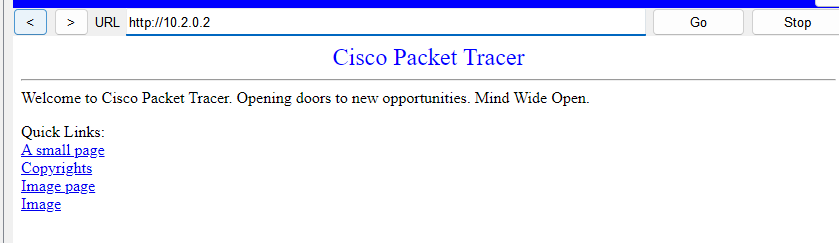


配置扩展ACL后

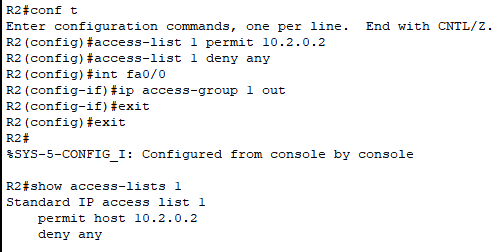




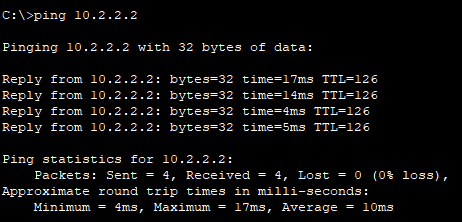




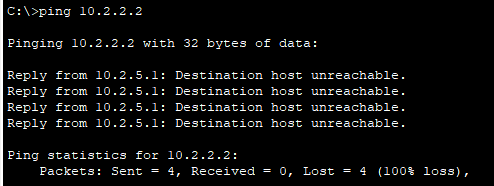
使用标准ACL，限制PC1只能被Server0访问



Server0 ping PC2



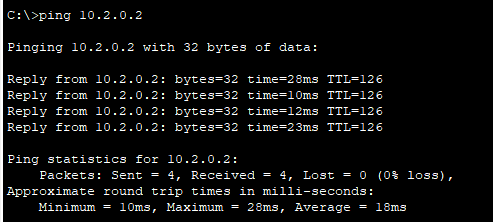
任意主机 ping PC2



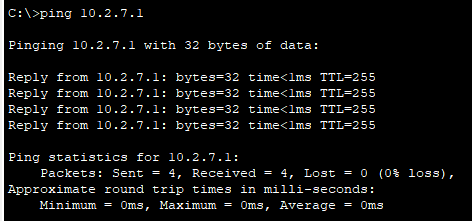
### 4.5 Configuration, Verification and Testing of NAT (8 points)

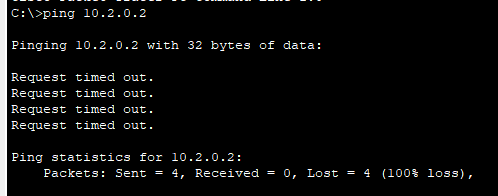
命令配置前，PC9和PC10能够ping通各自的网关，但无法ping通Server0， PC4可以ping通Server0

PC4

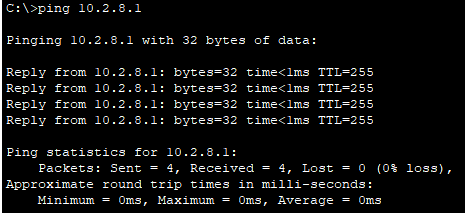


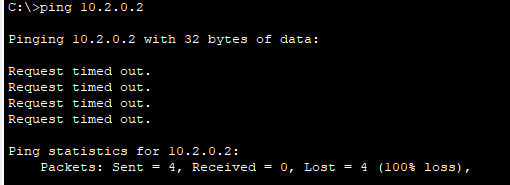
PC9





PC10

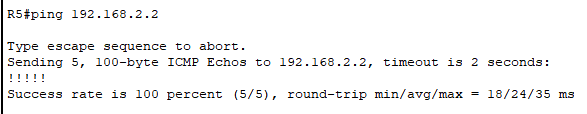




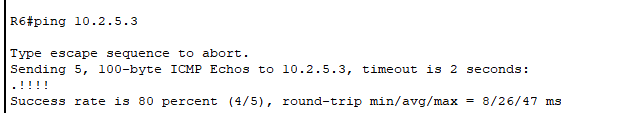
R5和R6能够ping通其他非直连网络

R5

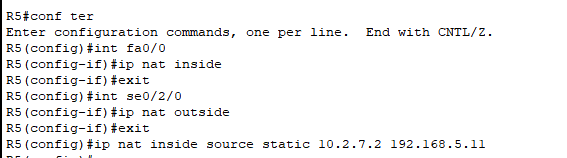




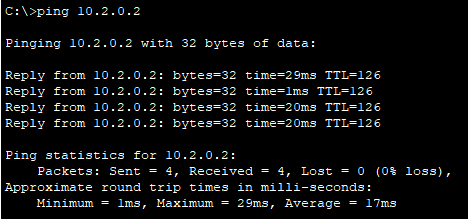
R6



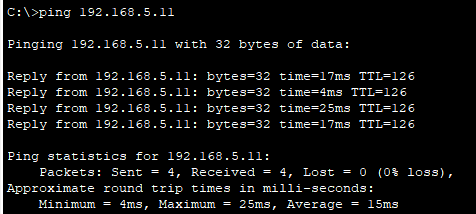
**1.为R5配置静态Nat命令**

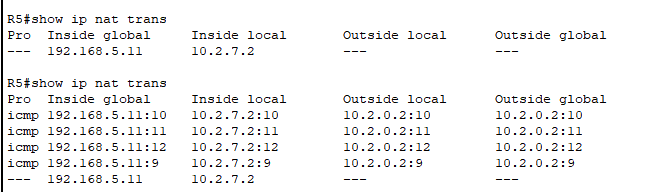


PC9 ping Server0

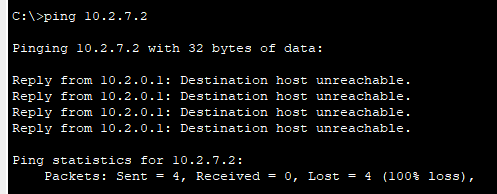


Server0 ping PC9虚拟ip

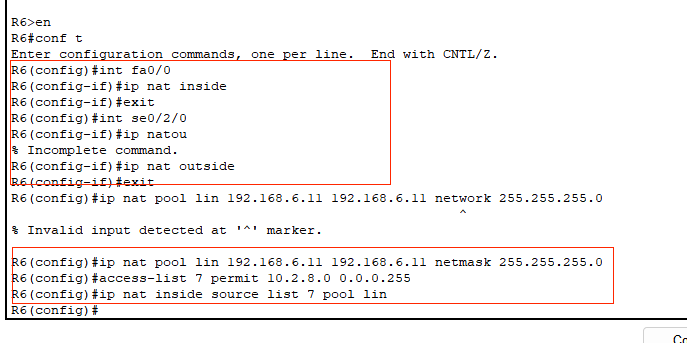




Server0 ping PC9真实ip



**2.为R6配置动态nat命令**



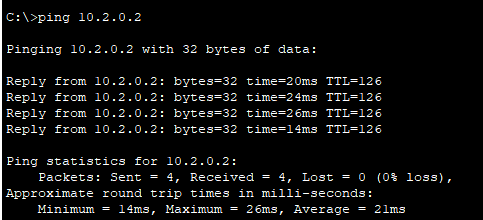
R6(config)#access-list 7 permit 10.2.8.0 0.0.0.255

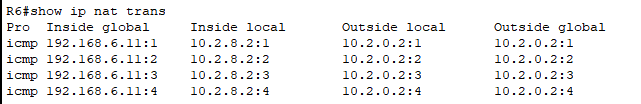
//配置标准ACL，以允许哪些内部地址可以使用动态地址转换

R6(config)#ip nat inside source list 7 pool lin

//将ACL指定的内部地址与指定的NAT地址池相关联

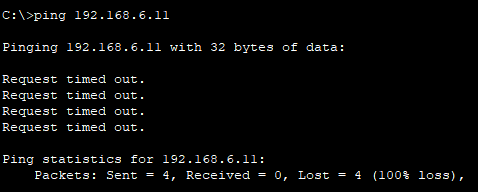
PC10 ping Server0



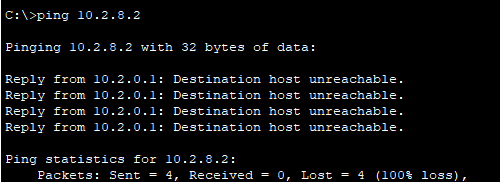


Server0 ping PC9虚拟ip

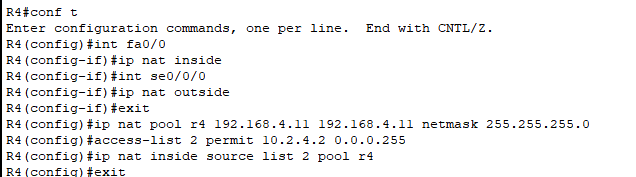
（ping失败，因为外部网络通常无法主动发起对内部网络的访问。这是因为外部网络并不知道内部主机所对应的外部地址（每次动态分配可能不同），并且没有相应的反向映射机制）



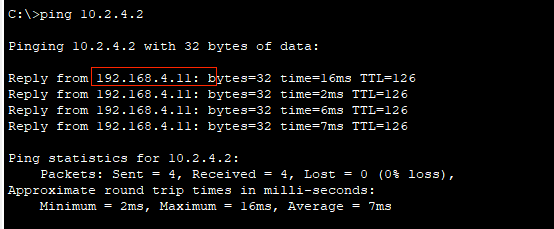
Server0 ping PC9真实ip

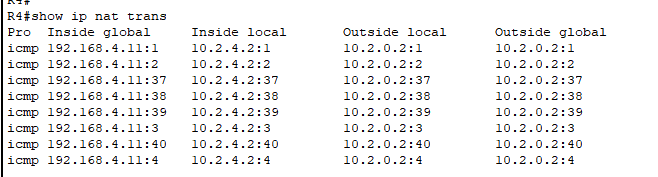


1. **为R4配置动态nat命令，此前PC4已经实现了与Server0的通信**



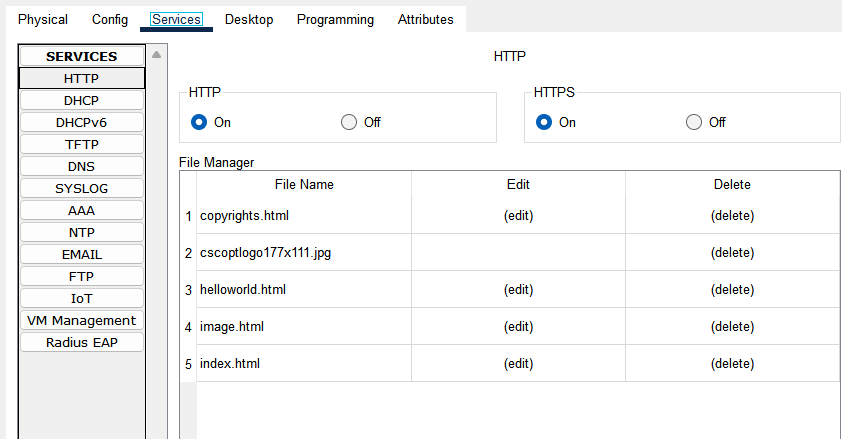
Server0 ping PC4，可以注意到，此时返回消息的地址是nat池内的ip

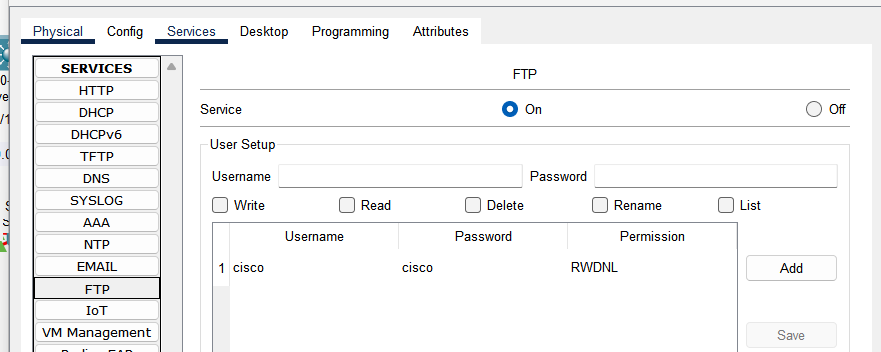




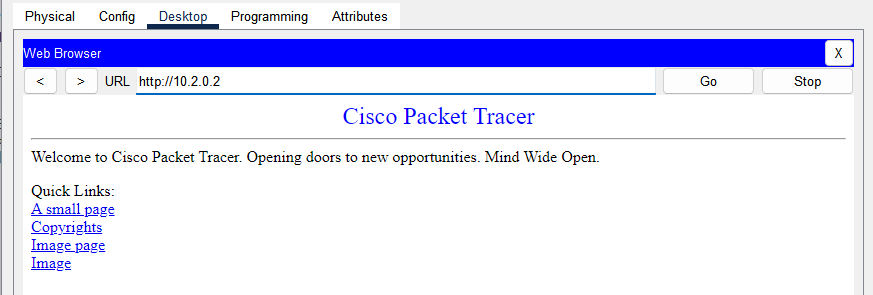
### 4.6 Deployment, Verification and Testing of Common services (8 points)

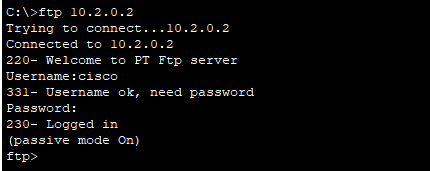
为Server0服务器配置了HTTP服务和FTP服务





使用任意PC机验证

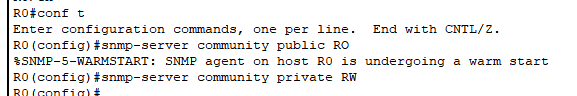


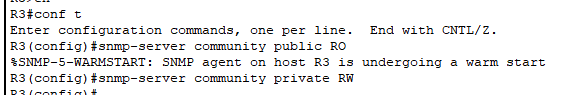


### 4.7 Configuration, Verification and Testing of Network Management Protocols (Agent) （10 points）

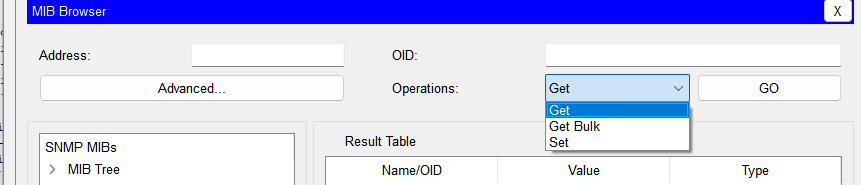
在R0、3、4上配置 SNMPv1（本次实验，路由器太多，因此只选取三台路由器进行配置和验证）

定义两个不同的团体名（Community Name），一个用于只读（Read - Only）操作，另一个用于读写（Read - Write）操作









Get 操作

解释：在 SNMP 中，Get 操作是最基本的操作之一。它用于从被管理设备（如路由器、服务器等）中获取一个或多个管理信息库（MIB - Management Information Base）对象的值。例如，网络管理员可以使用 Get 操作来查询路由器的接口流量、CPU 使用率或内存使用情况等信息。

Get Bulk 操作

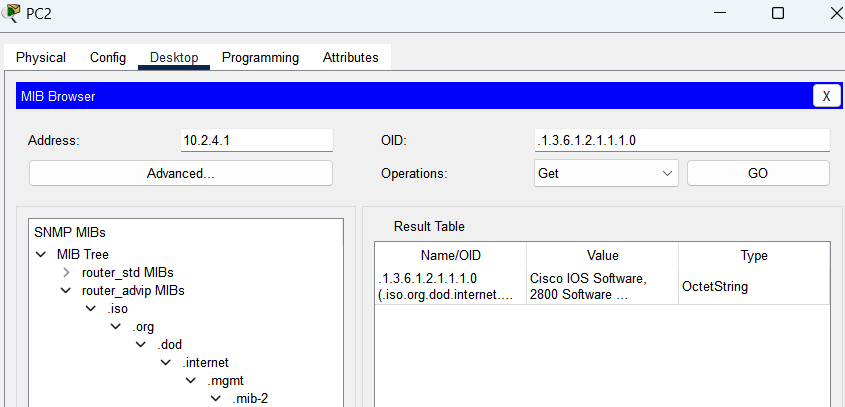
解释：Get Bulk 操作是 SNMPv2 中引入的一个功能，它允许网络管理员在一次操作中获取大量的 MIB 对象值。与 Get 操作不同，Get Bulk 操作可以有效地减少网络开销，因为它可以在一个请求中获取多个对象的值，而不是多次发送单个 Get 请求。

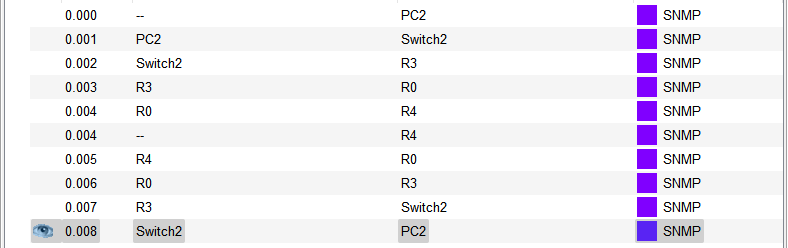
Set 操作

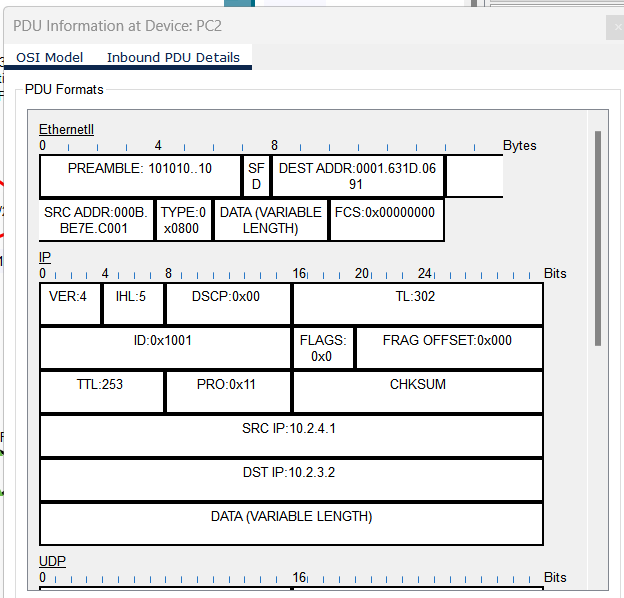
解释：Set 操作用于在被管理设备上设置一个或多个 MIB 对象的值。这意味着网络管理员可以通过 SNMP Set 操作来配置或修改设备的参数。例如，管理员可以使用 Set 操作来更改路由器的配置参数，如接口的 IP 地址、路由表项等。

### 4.8 Configuration, Verification and Testing of Network Management Software /Applications (Manager) （10 points）

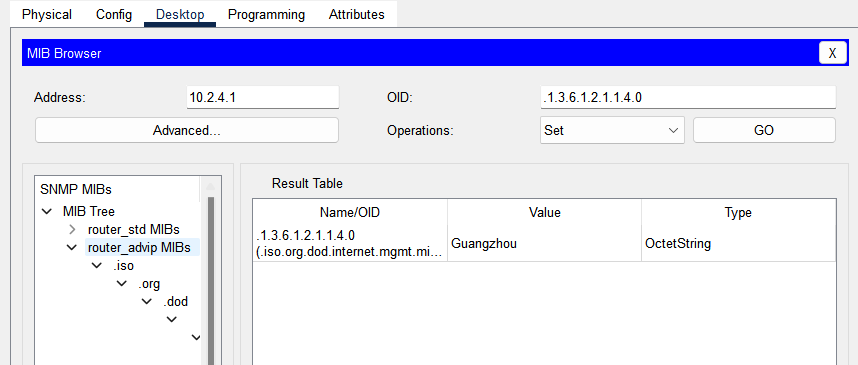
1. Get操作

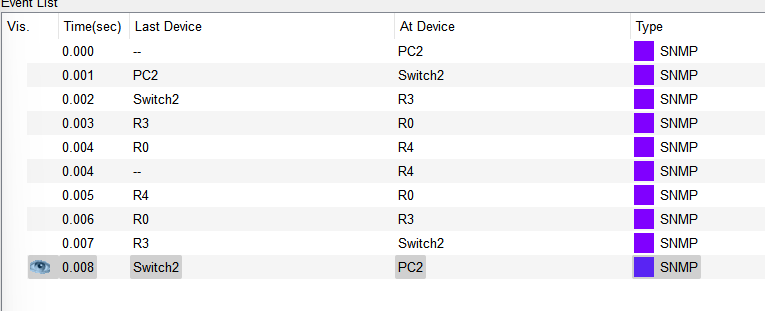


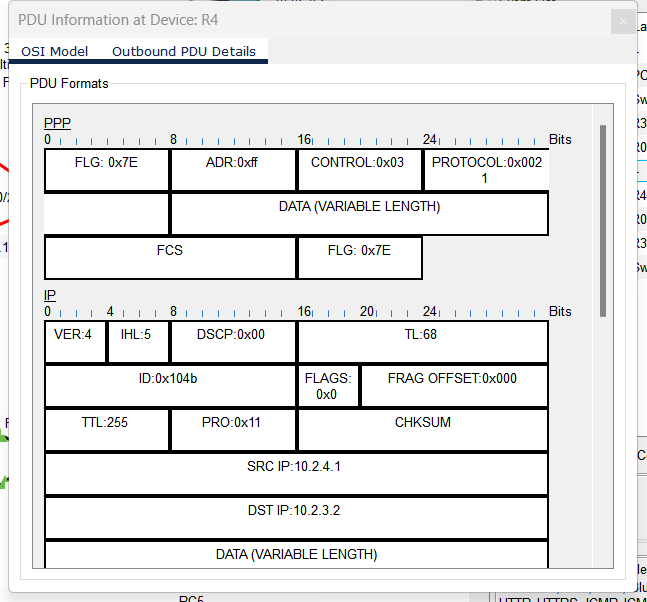




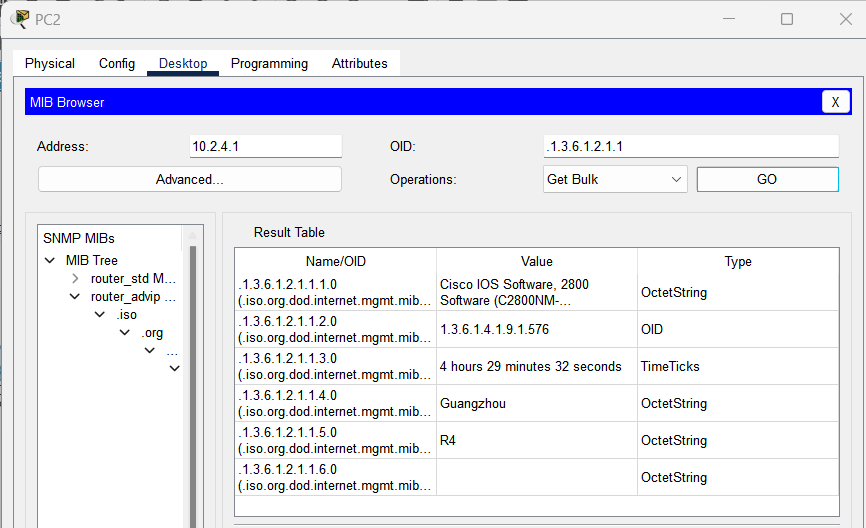
1. Set操作

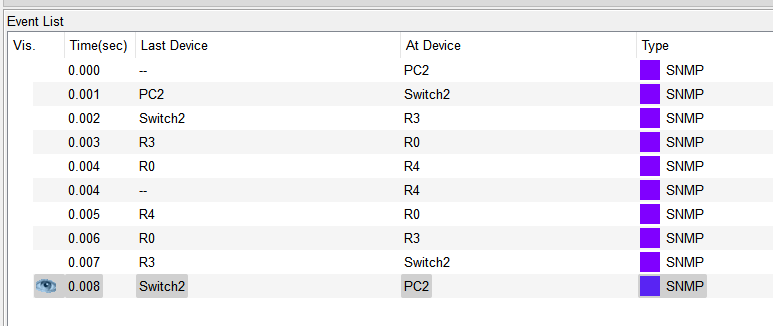


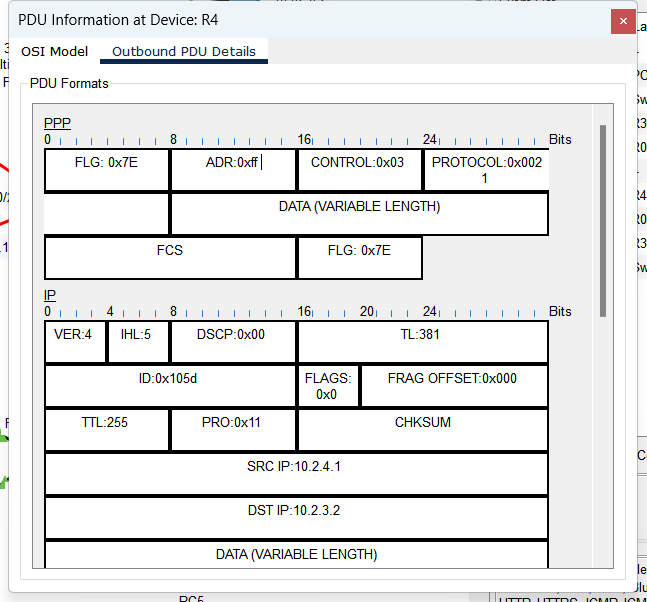




1. Get Bulk操作







### 4.9 Configuration, Verification and Testing of Other Functions (15 points)

**A.配置 PPP CHAP 认证**

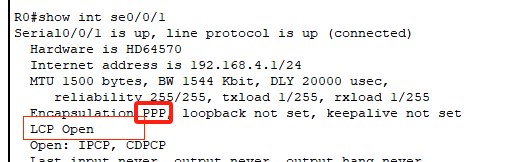
1.在被认证端上配置用户名和密码

R0(config-if)#username R4 password 111

R0(config)#int se0/0/1

R0(config-if)#encapsulation ppp

R0(config-if)#ppp authentication chap



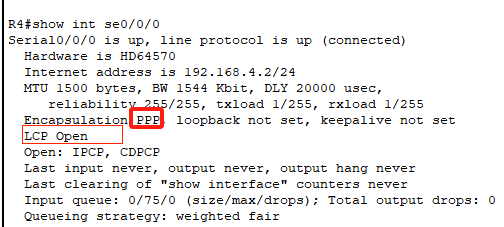
2.在认证端配置

R4(config)#username R0 password 111

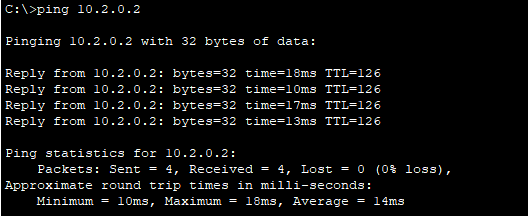
R4(config)#int se0/0/0

R4(config-if)#encapsulation ppp

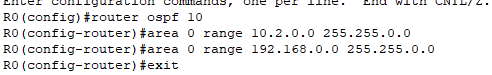
R4(config-if)#ppp authentication CHAP

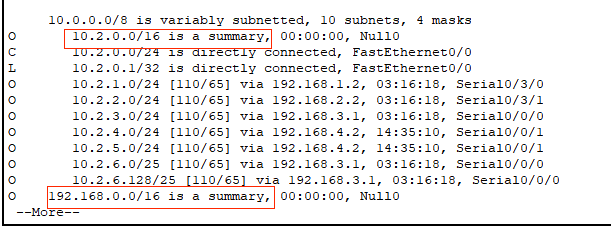


Ping测试

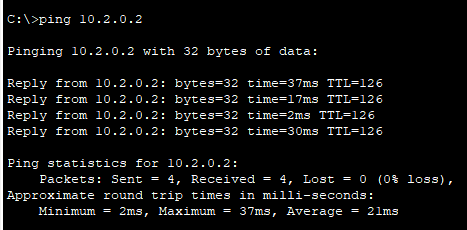


1. **配置手动路由汇总**

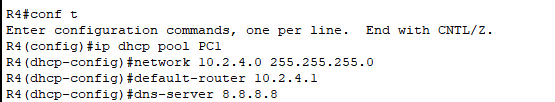




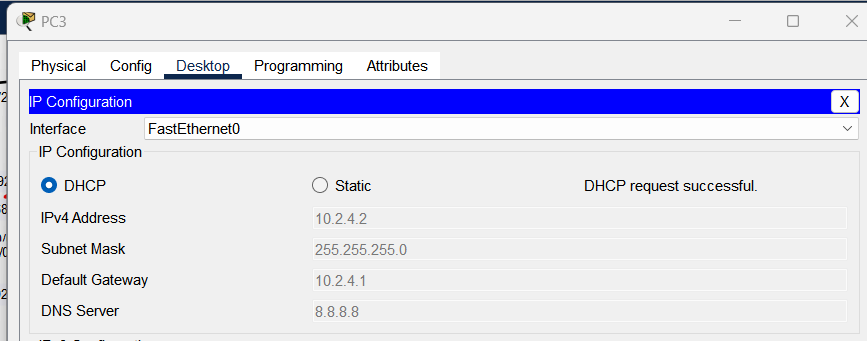
Ping测试



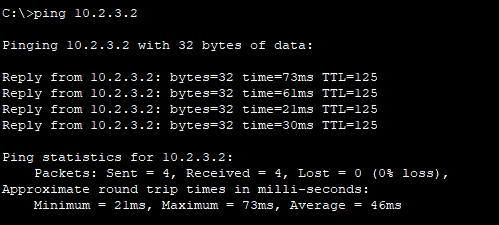
1. **DHCP服务**



将PC3的IP配置方式由静态改为DHCP

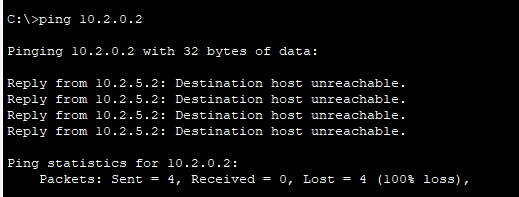


Ping任意外网主机



## Analysis and Summary of Project（2 points）

问题：配置ppp认证时，总是无法建立LCP，验证不成功，无法ping通



解决：检查后发现，CHAP服务，在创建用户和密码时，用户名不是本机，而是所需被认证端（对认证端）或认证端（对所被认证段）的hostname。

由  
 R0(config-if)#username R0 password 111

R4(config-if)#username R4 password 111

修改为

R0(config-if)#username R4 password 111

R4(config-if)#username R0 password 111

后，认证成功

## Summary （3 points）

本次实验模拟了典型企业网络环境，成功实现了多分支与总部间的互联互通及多种网络功能配置，有效提升了网络可靠性与安全性。

在实验过程中，积极运用了多种网络技术。通过 OSPF 协议实现了动态路由，确保各网段间的高效通信，如 R0 等路由器的相关配置，使不同区域的设备能够相互访问。VLAN 技术的应用，在交换机上合理划分 VLAN，优化了网络性能，增强了网络管理的灵活性。ACL 的配置，精准限制了特定分支对服务器的访问权限，提高了网络安全性。

然而，实验也遇到了问题。在配置 PPP 认证时，出现无法建立 LCP、验证不成功及无法 ping 通的情况。经过深入检查和分析，发现是 CHAP 认证中用户名配置错误，应设为对端设备的 hostname，修正后认证成功，这为今后处理类似问题积累了宝贵经验。

通过本次实验，不仅熟练掌握了网络设备的配置与管理技能，包括路由器、交换机等设备的多种命令操作，还深刻理解了网络规划、安全策略实施的重要性，为未来从事网络管理工作奠定了坚实基础。同时，也认识到在网络配置中细致检查和准确理解配置参数的必要性，以确保网络的稳定和安全运行。