**暨南大学本科实验报告专用纸**

课程名称 计算机网络实验 成绩评定

实验项目名称 综合组网与配置 指导教师 潘冰

实验项目编号 实验项目类型 实验地点 计算机网络实验室

学生姓名 赖智聪 学号 2019051118

学院 智能科学与工程 系 专业 信息安全

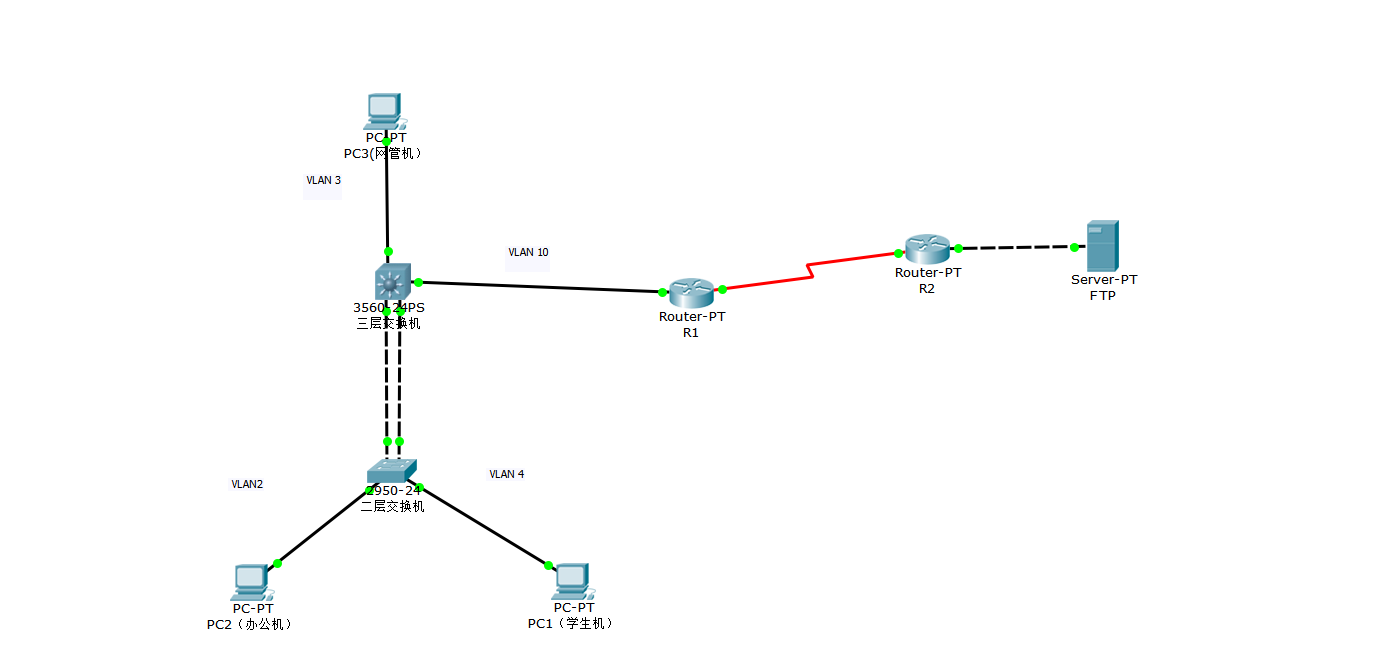
实验时间 2021 年 12 月 14 日 上 午～ 12 月 21 日 上 午

|  |
| --- |
| **一、实验目的** |
| 通过该实验的设计与配置模拟，考核学生对已学知识的掌握程度，加深对网络协议和原理的理解；培养学生利用网络技术结合实际需要分析问题、解决问题的能力；培养学生的组网技能和实际动手能力；培养学生的协调工作能力；提高学生撰写实验报告的能力。 |

|  |
| --- |
| **二、实验环境** |
| 下图是模拟某学校网络拓扑结构，在该学校网络接入层采用S2126交换机，接入层交换机划分了办公网VLAN2和学生网VLAN4，VLAN2和VLAN4通过汇聚层S3550与路由器A相连，另外S3550上有一个VLAN3存放一台网管机。路由器A和B通过路由协议获取路由信息后，办公网可以访问B路由器后面的FTP服务器。为了防止学生网内的主机访问重要的FTP服务器，A路由器采用了访问控制列表的技术作为控制手段。需要在三层交换机上建立路由表。  要求：  1、每4个人一个小组，共同完成实验；  2、本实验安排学时为4学时，实验前每个小组提交一份实验预习报告。预习报告包括实验内容、配置设计和步骤。详细描述IP地址配置、设备的连接端口号。本部分15分。  3、实验后在每个小组随机选取1-2个人汇报实验情况。实验完成并汇报成功，则实验通过。  **VLAN1**  **VLAN3**  **VLAN4**  **VLAN2**  **FTP Server**  **S2126**  **S3550**  **B**  **A**    **【基础知识】**  **（1）标准访问列表和扩展访问列表比较**  **标准**  **扩展**  基于源地址  基于源地址和目标地址  允许和拒绝完整的协议  指定TCP/IP的特定协议和端口号  编号范围 100 到 199  编号范围 1 到 99  **（2）定义访问控制列表**  在**Router(config)#**模式下定义访问控制列表的语句。每一个语句只可能添加到访问控制列表中，如果在访问控制列表（典型的）中有多于的一条语句，想将其删除，必须删除访问控制列表然后重新开始。  1）标准访问控制列表：  **Router(config)#access-list access-list-number**  **{permit/deny}**  **source ip address [widecard mask]**  2）扩展访问控制列表：  **Router(config)#access-list access-list-number { permit | deny } protocol**  **source ip source-wildcard destination ip destination-wildcard [operator port ]**  **说明：**缺省的通配符掩码 = 0.0.0.0  隐含条件为拒绝所有（deny any）  **（3）在端口上应用访问控制列表**  **Router(config-if)# ip access-group access-list-number { in | out }**  **说明：**缺省 = 出方向  **（4）删除访问列表**  **Router(config)#no access-list access-list-number**  **（5）在端口上删除访问列表**  **Router(config-if)#no ip access-group access-list-number**  **（6）访问控制列表的放置**  **将标准访问列表置于离目的设备较近的位置**  **将扩展访问列表置于离源设备较近的位置**  **（7）访问控制列表的查看和检测**  1) 检查语句并核实是否所有内容都被正确键入  **Router#show access-list access-list-number**  2) 确认访问控制列表正确应用到期望的接口上  **Router#show running-config 或者**  **Router#show ip int type solt**  3) 确认访问控制列表是否正确运行  试图从已经被禁止或者被允许的源网络传送出数据包。运行一些**Ping**等命令来测试这些访问控制列表。 |
|  |
| **三、实验内容**   * 配置、命名标准 IP 访问控制列表，并在网络接口上引用 IP 访问控制列表； * 配置、命名扩展 IP 访问控制列表，并在网络接口上引用 IP 访问控制列表； * 查看和监测 IP 访问控制列表。 |

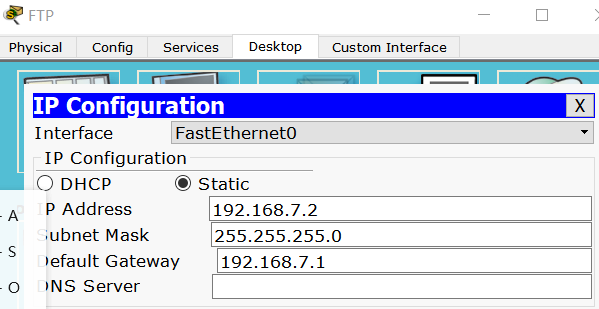
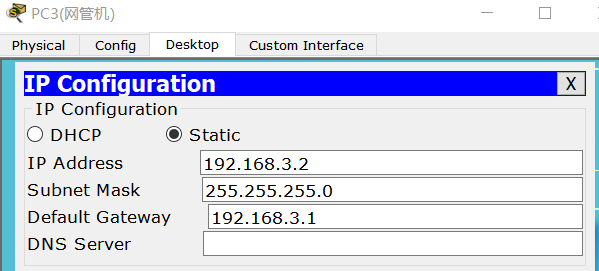
**四、实验及分析**

实验拓扑结构：



终端设备的配置：

#### IMG_256IMG_256



VLAN 2(办公机所属VLAN):192.168.2.1 255.255.255.0

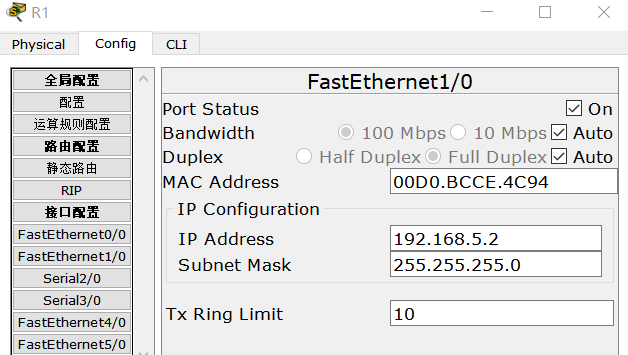
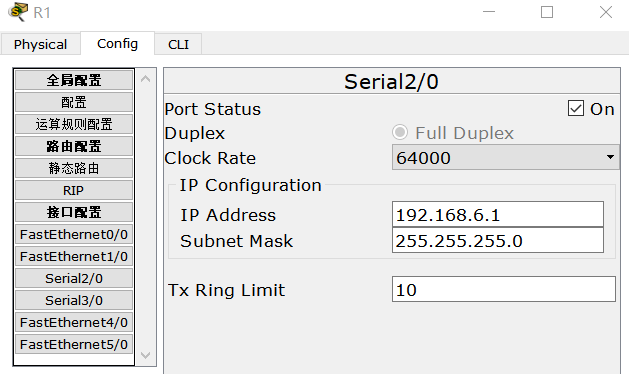
VLAN 3（网管机所属VLAN）：192.168.3.1 255.255.255.0

VLAN 4 （学生机所属VLAN）:192.168.4.1 255.255.255.0

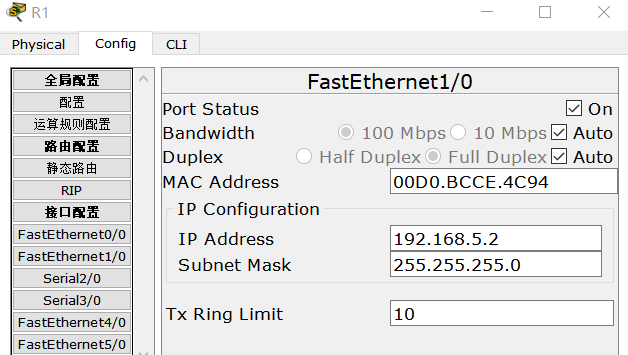
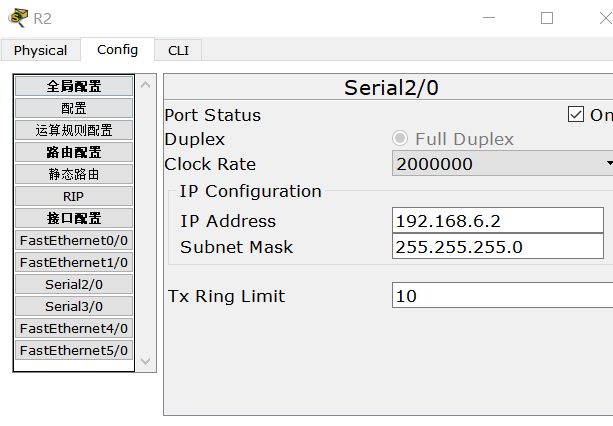
VLAN 10(三层交换机与R1之间的）：192.168.5.1 255.255.255.0

路由器IP配置：

R1:

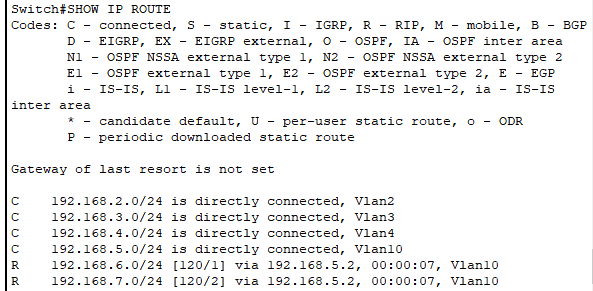


R2:

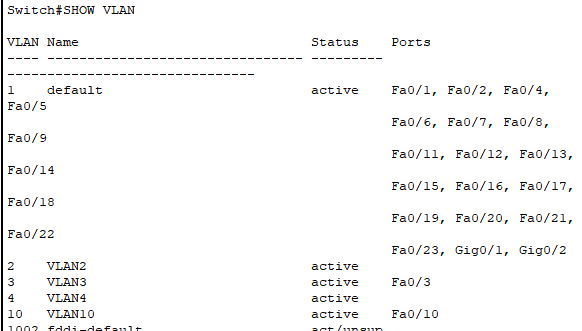


三层交换机：

RIP：

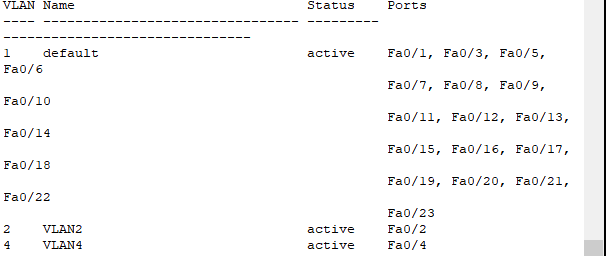


VLAN：

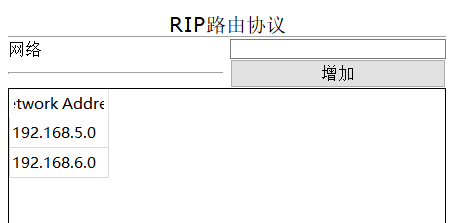


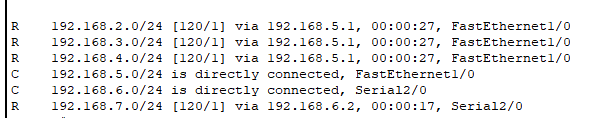
二层交换机:

VLAN:

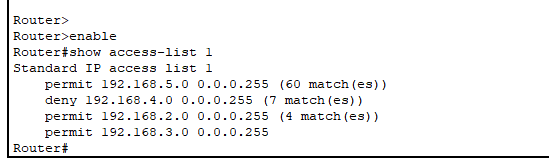


RIP:

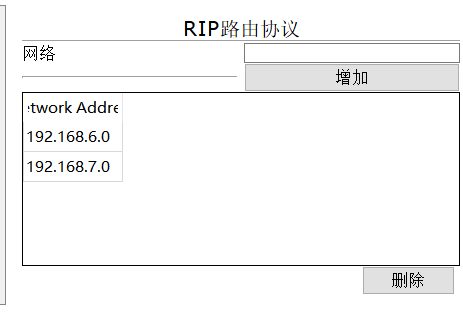




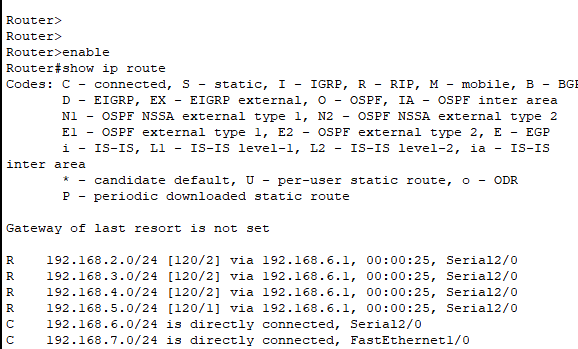
配置ACL:



配置端口和RIP:



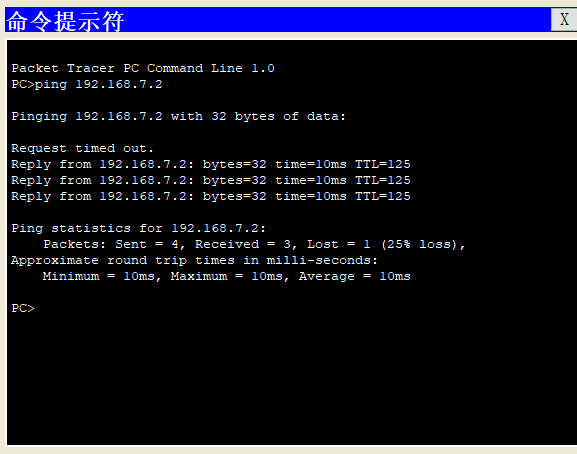
R2的IP route:



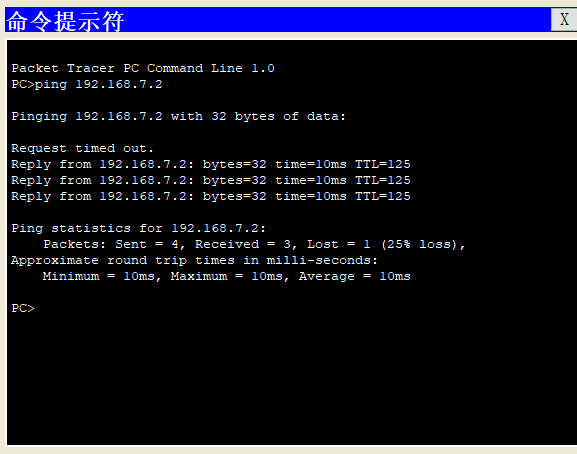
**实验结果**

进行访问控制前:

PC2学生机(Vlan4),ping ftp服务器：

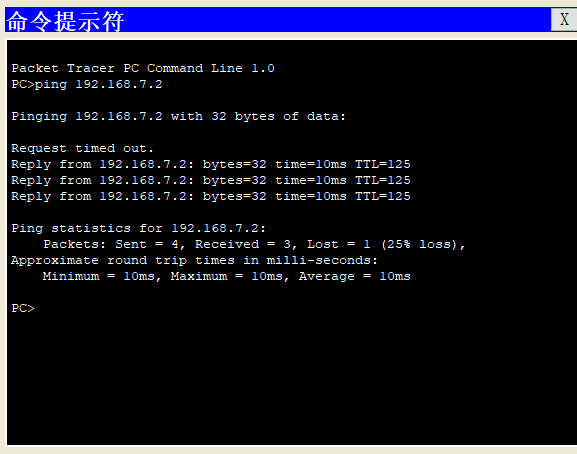


PC1办公机(Vlan2),ping ftp服务器：

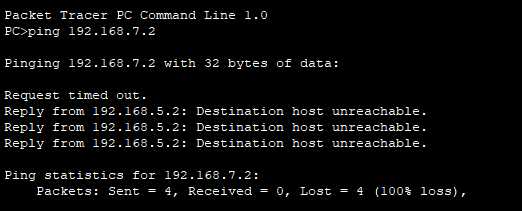


访问控制后：

PC1办公机(Vlan2),ping ftp服务器：



PC2学生机(Vlan4),ping ftp服务器：



可见设置了ACL后，PC1仍然可以访问FTP服务器，PC2则无法访问FTP服务器，访问控制取得成功。

端口镜像：

设置了端口镜像后，可以在PC3网管机监控到PC2和PC4的流量, 在三层交换机上配置后，可实现对双层交换机的数据包抓取，实现流量监听。

1、如果需要在在VLAN3的主机上运行WireShark监听其他主机，如何实现？(需要端口镜像) 5分

答：需要在相应交换机或路由器配置端口镜像,从而将其它端口的流量转到特定端口。

2、S2126和S3550之间的双线是用来做端口聚合的，可以起到交换机之间的连接冗余和增加带宽作用，如何实现？

答:

SwitchA(config)#interface aggregateport 1 ！创建聚合端口AG1

SwitchA(config)#switchport mode trunk ！配置AG模式为trunk

SwitchA(config)#interface range fastethernet 0/1-2 ！进入端口0/1、0/2

SwitchA(config-if-range)#port-group 1 ！配置端口0/1、0/2属于AG1

SwitchA#show aggregateport 1 summary ！显示聚合端口信息

3、学生网内的主机不能访问FTP服务器，能否ping通呢？为什么？如何设置wireshark显示过滤器才能监听访问是否成功？

答：

学生网内的主机不能访问FTP服务器，也ping不通。因为在路由器R1中设置了ACL表，ACL限制了192.168.4.0网段访问，从而学生无法访问FTP服务器，不能转发数据包，从而ping不通。

在服务器终端上将Wireshark过滤器的源ip地址设置为学生网，即可观测到学生网内终端无法访问到FTP服务器。

**五、实验总结**

通过运用本学期所学到的知识以及之前实验的经验,和同学合作共同解决该实验.通过实验,加深了对ACL、端口镜像、ip转发等的理解.不足之处是个人实验能力较弱,对一些步骤的操作存在失误,在同学的提醒后才改正.