**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 12 实验项目类型 验证型实验地点 B402

学生姓名 梁伟希 学号 2019051117

学院 智能科学与工程 系 信息安全 专业 2019级

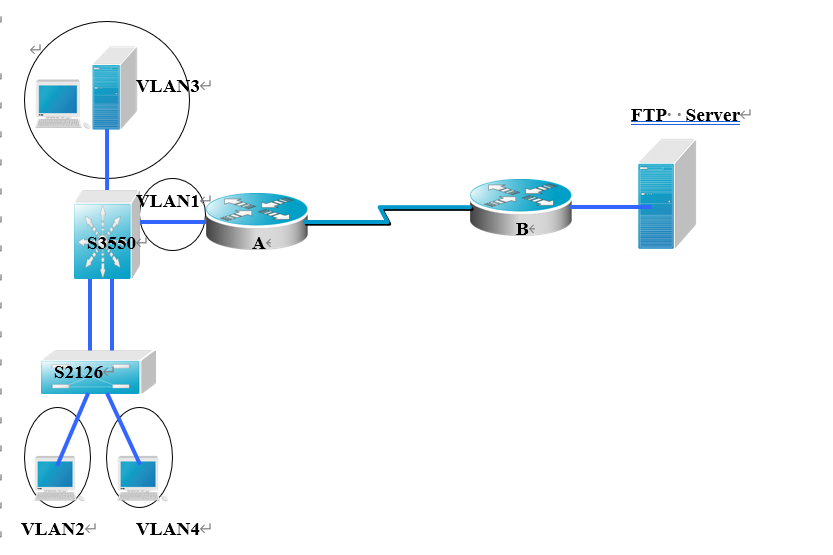
实验时间 2021 年 12 月 14上午～ 12月 14日上午 温度 ℃湿度

## （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）实验内容和要求

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。

## 实验原理

附：访问控制列表实验

**【实验目的】**

* 熟悉访问控制列表（ACL）的特点和作用；
* 学会创建、命名ACL，并将ACL放置在正确位置；
* 通过对路由器或三层交换机配置 IP 访问控制列表，实现对服务器或网络的访问控制。

**【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。

**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。

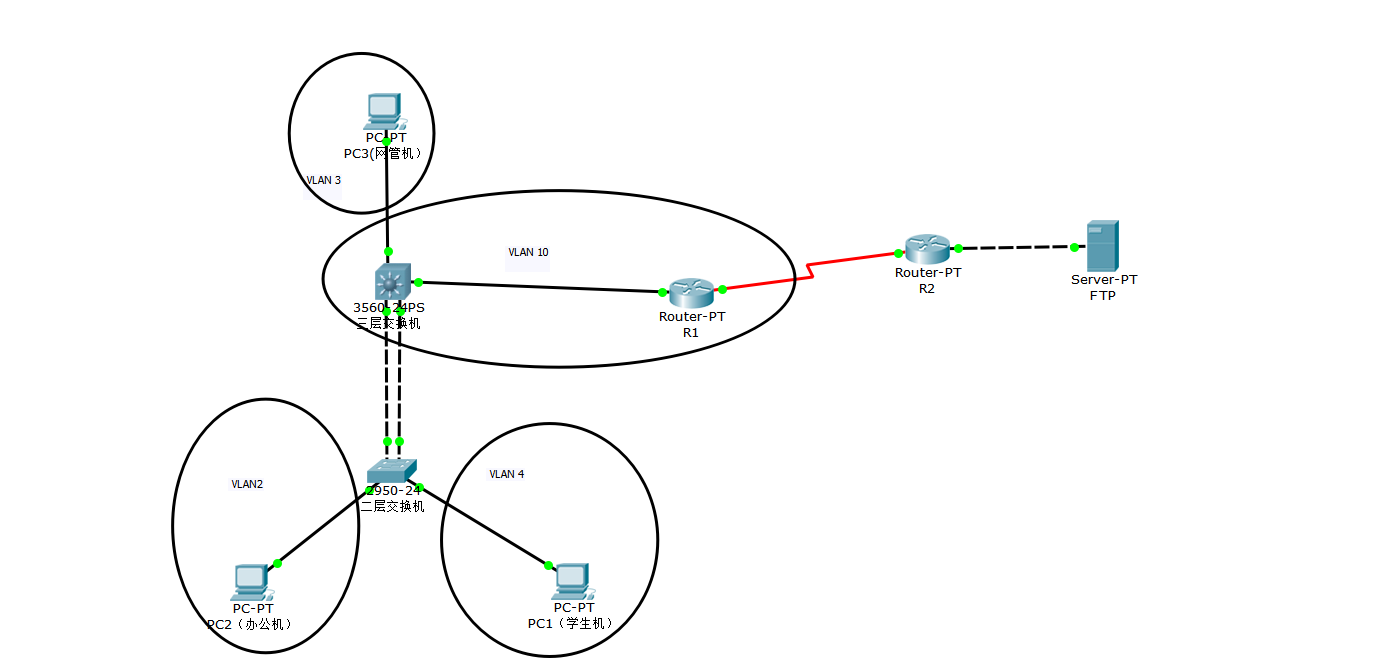
## （四）实验环境

仪器：计算机一台

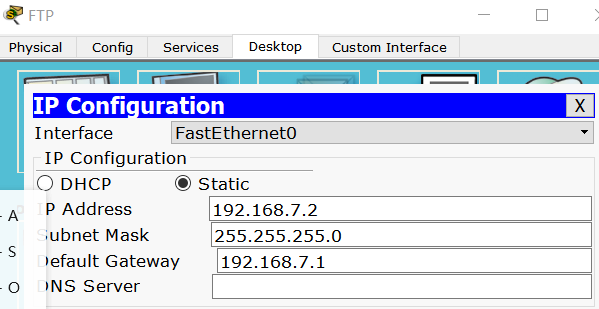
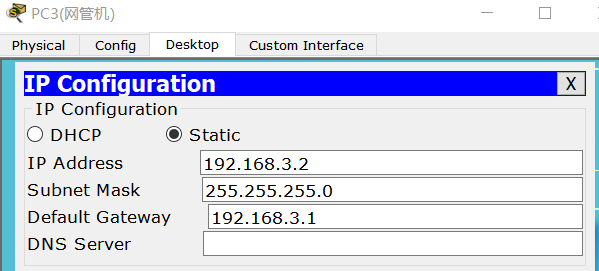
实验环境：思科模拟器

## （五）实验步骤与调试

### 实验拓扑结构：

**四台终端设备相关IP配置：**

#### IMG_256IMG_256



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

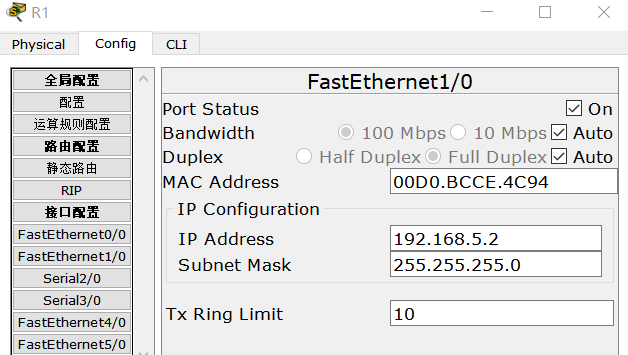
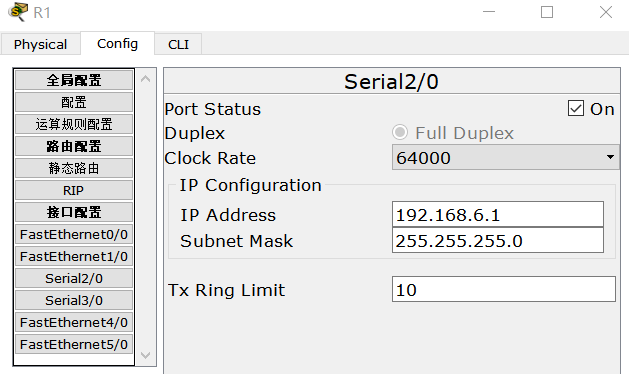
VLAN 2(办公机所属VLAN):192.168.2.1 255.255.255.0

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

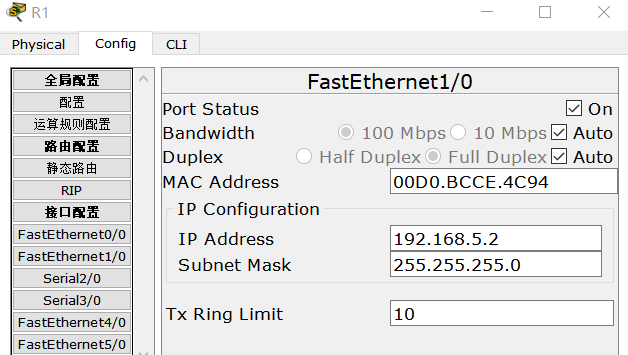
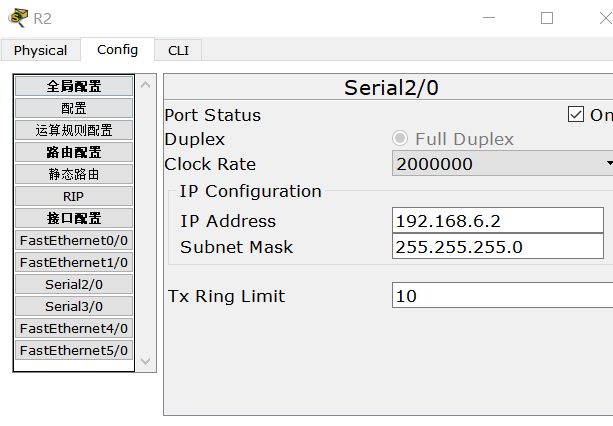
VLAN 4 （学生机所属VLAN）:192.168.4.1 255.255.255.0

##### 路由器相关IP配置：

R1:

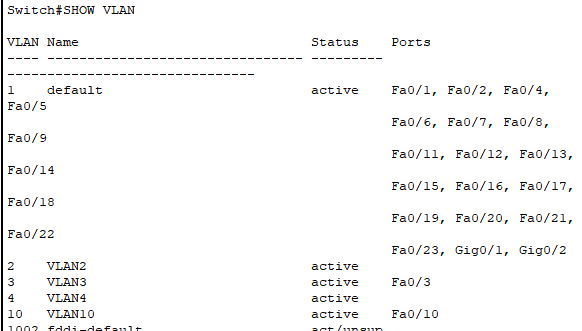


R2:

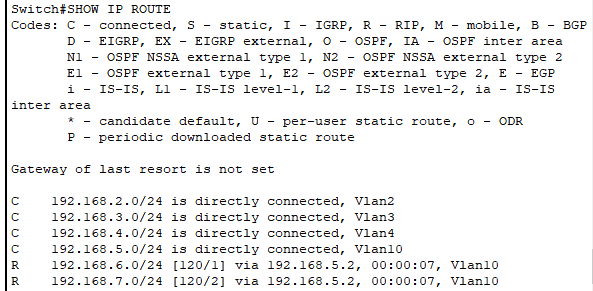


##### 三层交换机

1. VLAN

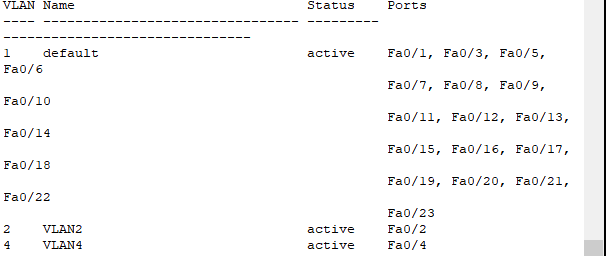


1. RIP协议



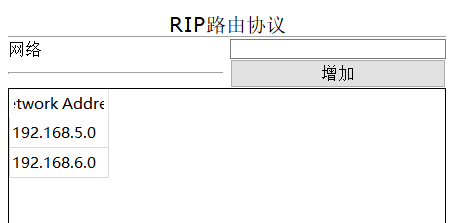
##### 二层交换机

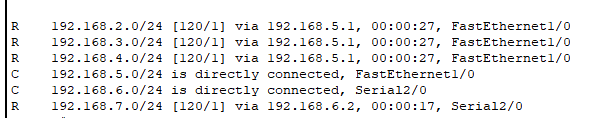
1. VLAN



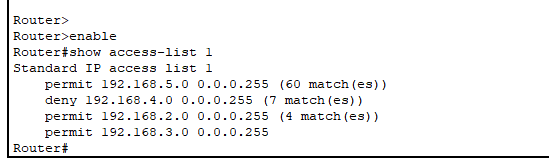
##### 路由器（R1）

1. RIP协议



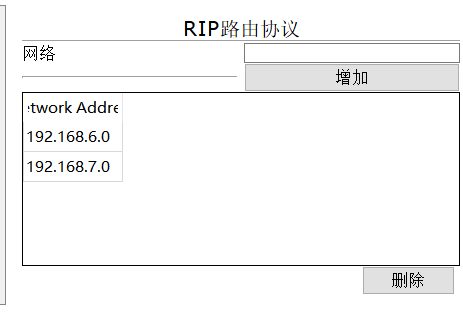


1. 配置ACL，拒绝学生机访问后面的FTP服务器

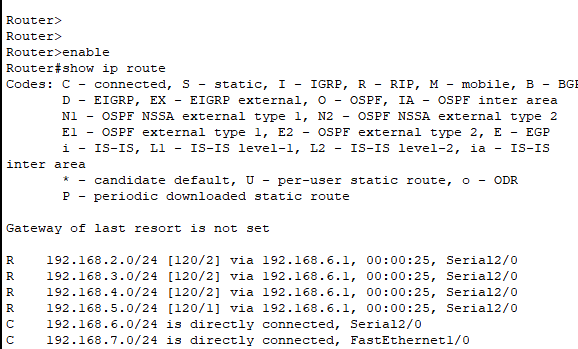


路由器（R2）

配置端口以及RIP协议：



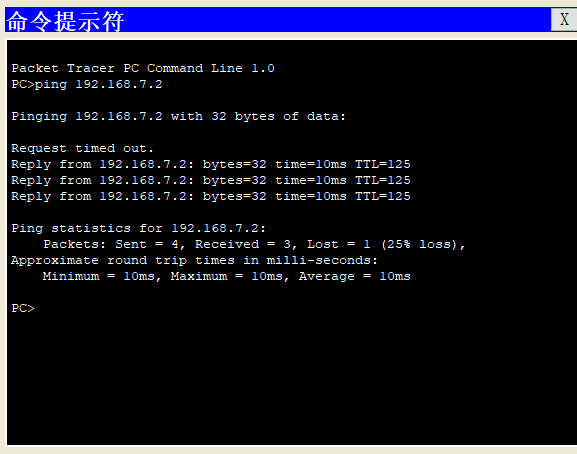
路由器R2的IP route：



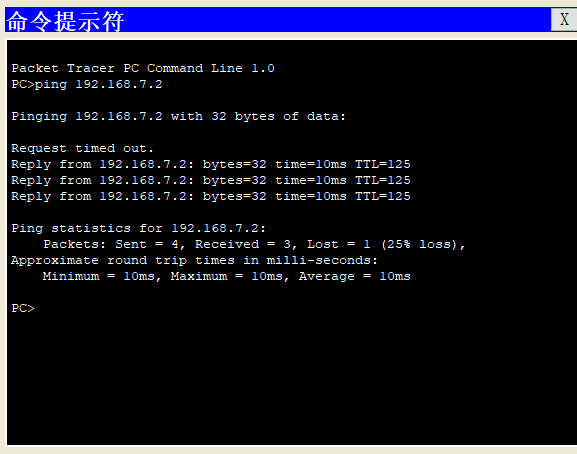
### 实验ACL：

#### 进行访问控制前：

在设置ACL前PC1办公机(Vlan2)ping ftp服务器：

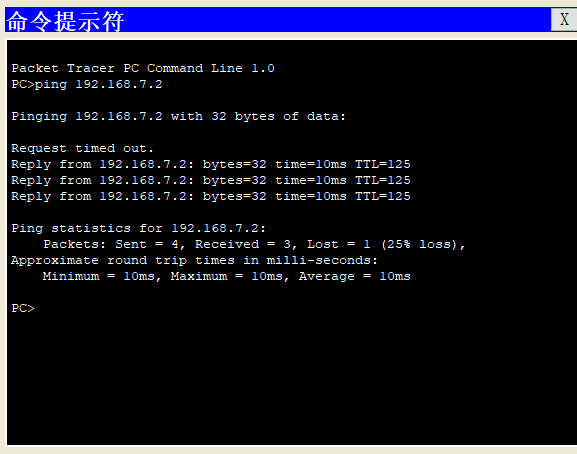


在设置ACL前PC2学生机(Vlan4)ping ftp服务器：

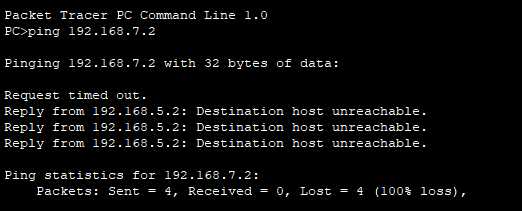


#### 访问控制后：

在设置ACL后PC1办公机(Vlan2)ping ftp服务器：



在设置ACL后PC2学生机(Vlan4)ping ftp服务器：



在设置了ACL表后，PC1仍然可以访问FTP服务器（ping得通），PC2已经无法访问FTP服务器了（即ping不通了），从而得出访问控制已经成功。

### 端口镜像：

在设置了端口镜像后，可以在PC3网管机上，监控到PC2和PC4之中的流量，即抓到包。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。

## （六）思考题

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：为实现在网管机，即PC3，VLAN3的主机上运行WireShark监听其他主机，则需要在相应的交换机或者路由器上面配置端口镜像，将若干个源端口的数据流量转发到一个特定的端口，或是说镜像端口、目的端口。这样会对源端口吞吐流量存在少许的影响，倘若影响在可接受范围内，可通过这个方式对镜像端口进行监视、并且进行分析

1. 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：可通过如下的几行命令，来进行端口聚合的功用：

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，也不能够ping得通。在路由器R1中设置了ACL表，即访问控制表，ACL限制了192.168.4.0网段访问后续，即学生区无法访问FTP服务器，不能转发数据包，自然也无法ping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（或是在设置了镜像上的网管机上进行这一操作）。

4、写好总结，把出现的问题和解决方法写出来，把收获和启发写出来，把不足和建议写出来。

答：此处附于在实验总结中。

## （七）实验总结

（1）遇到的问题及其解决方案：

1.在机房进行第二次实验时，没有正确完整地配置三层交换机连接双层交换机的端口，对于VLAN的设置与链路聚合也是一知半解，导致无法通过三层连接双层的方式进行此次实验。只好退而求其次使用了单个三层交换机完成了不完全的实验，从而也没能正确设置网管机的功效，即不能进行镜像端口的监听，使得网管机成为了另一个“办公网”即使这样也起到了ACL应有的效果，但实验效果仍是很不理想。

2.在机房进行首次实验时，没有直接使用整个实验，而是仅仅测试ACL表，发现在设置了ACL表后，在访问控制效果完成后却发现任何访问都无法直接到达被访问控制后的目的主机。推测与permit any这一条命令没有设置有关，可能也与permit相关命令设计失误有关，作为负责输入命令的人，我难辞其咎。后面在与同学重新设计命令，与设置了RIP表后，才得以解决，具体原因尚不清楚，但推测是上文中的原因。

（2）收获和启发：

1.此次实验时本学期计算机网络实验的最后一个实验。这次实验综合了本学期课堂学习中大部分的实验内容以及相当一部分的理论储备，并需要灵活运用团队合作，对于个人和团队而言都是一次考验。尤其是这次实验中没有给出具体的配置步骤，这就需要团队之中先进行拓扑图和IP、接口的设计，在操作时对输入命令的工作的要求也比较高，不再是机械的输入，而是需要灵活应变，也需要对命令有一定的了解与进行相当程度的设计与借鉴。通过这次实验，对计算机网络知识的领会得到了提升，尤其是对拓扑结构的设计这一方面。

2.通过这次实验，在知识点上，我对于ACL访问控制表的配置以及端口镜像、端口聚合等技术有了初步的认识和了解，在上手操作后，更是对如何配置这几类项目有了更深层次的了解，也认识到了它们在安全与性能方面的作用：使用端口镜像可以实现网管机对其他网络的监视，而配置ACL表更是可以实现一个“黑名单”的操作，使得学生网访问不到重要的FTP服务器。是一项与安全相关的操作，与我信息安全专业存在联系，

（3）不足与建议：

此次实验中遇到了不少问题，如PC1,PC2都无法ping到FTP服务器，PC3却可以，且在连线配置中都没有检查出问题，与成功人士的对比后也无法找出错误进行排查。初步猜测是在连线时还是不够细心，在进行命令输入时也没有专心，理论知识还不够扎实，出现了纰漏。而ACL表的设置问题则是完全的不细心，仅仅考虑到了限制，而没有想到使得相关的机器可以通过的功能。

在这些过程中，最好团队成员可在命令输入或连线的时候进行围观的操作，对于存在的错误和纰漏、疑惑都及时指出，做到及时更正的作用，同时也能提高各个成员对于每一个步骤的理解。

**暨南大学本科实验报告专用纸(附页)**