**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 钟颖谦 学号 2019051091

学院 智能科学与工程 系 专业 信息安全

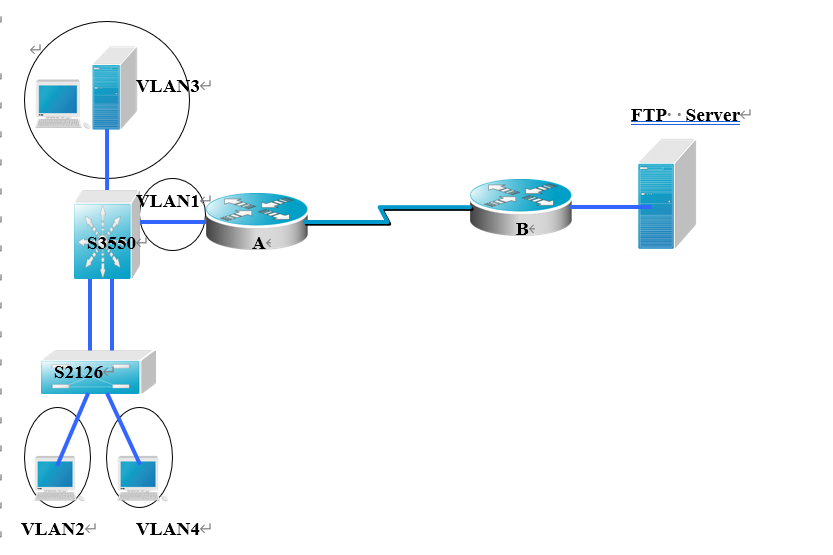
实验时间 2021 年 12 月 14上午～ 12月 14日上午 温度 ℃湿度

## （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。

## （三）实验原理

### 访问控制列表原理：

**（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。

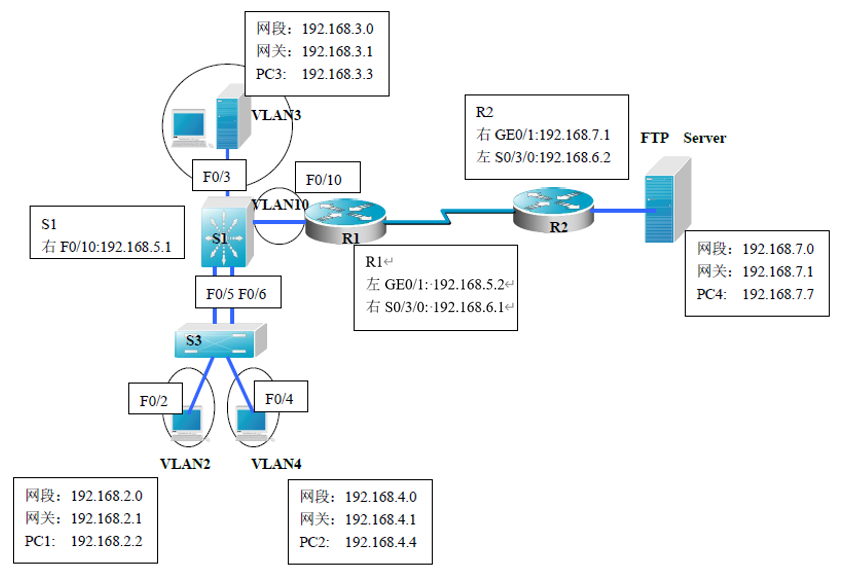
## （四）实验环境

**仪器：**计算机4台，三层交换机1台、二层交换机1台、路由器2台。

**实验环境：wireshark&cmd**

## （五）实验步骤与调试

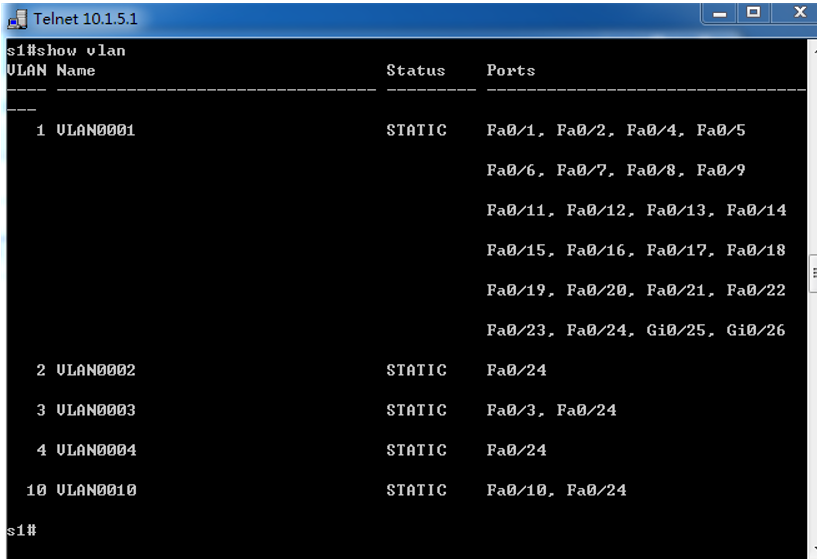
### 设计拓扑结构：



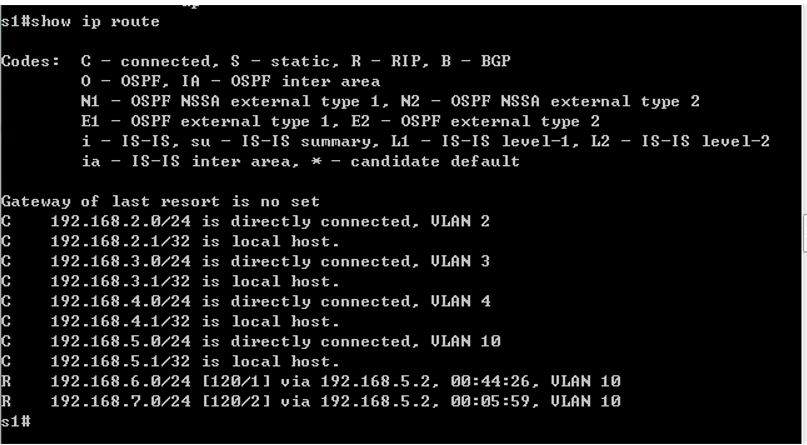
#### 配置：

##### 三层交换机

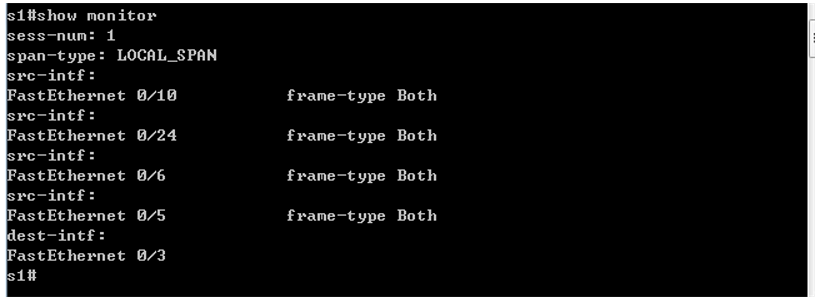
1. 划分vlan



1. 使用动态路由协议，配置RIP协议



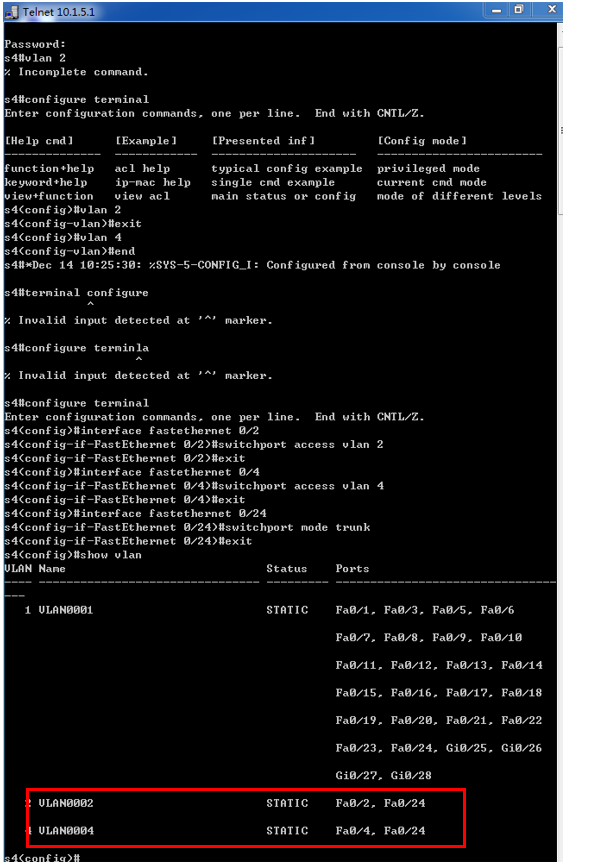
1. 端口镜像



1. 取消链路聚合

##### 二层交换机

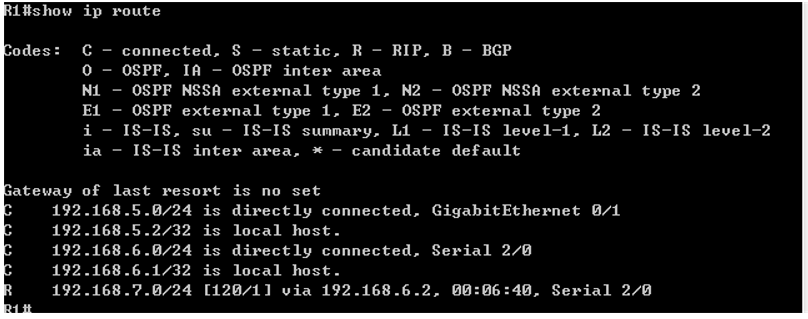
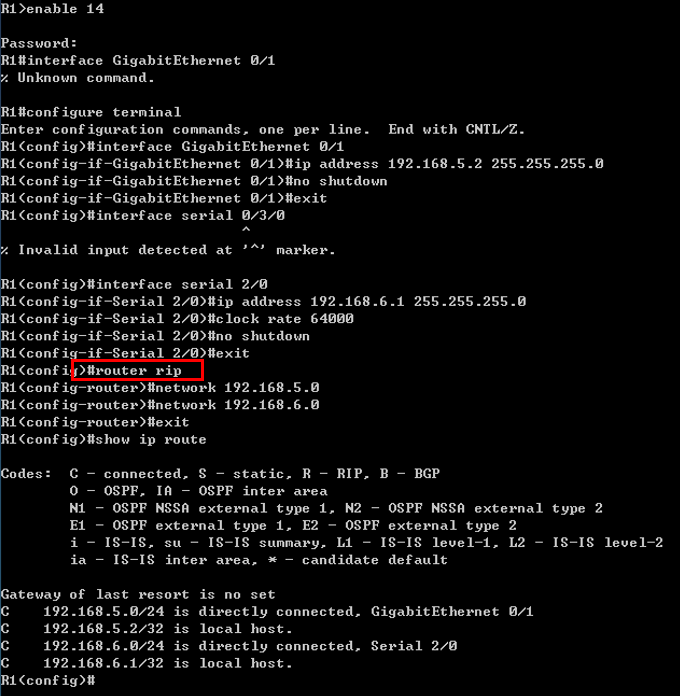
1. 划分vlan:



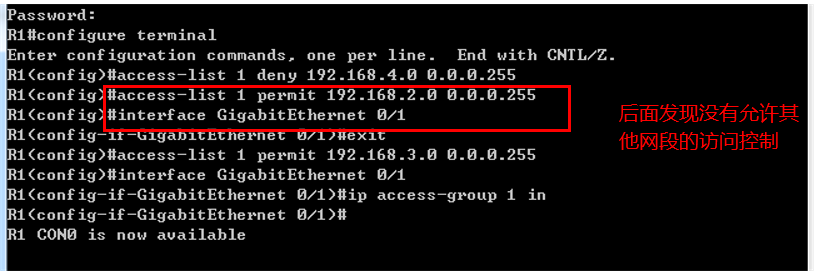
1. 取消链路聚合

##### 路由器（R1）

1. 配置好端口并且配置RIP协议



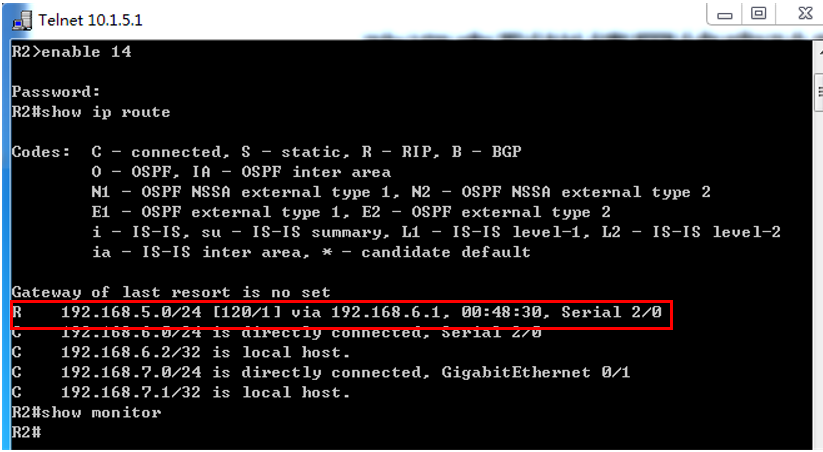
1. 配置好访问控制表，拒绝vlan4访问FTP服务器



##### 路由器（R2）

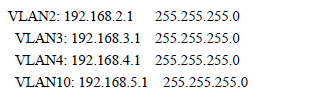
1. 配置端口以及RIP协议

路由器R2的路由信息：

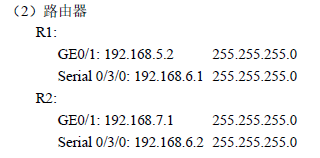


##### IP与端口配置

1. Vlan

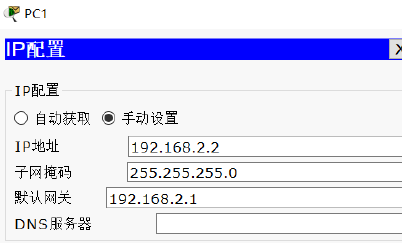


1. 路由器

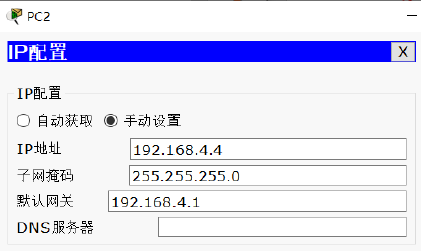


1. PC机

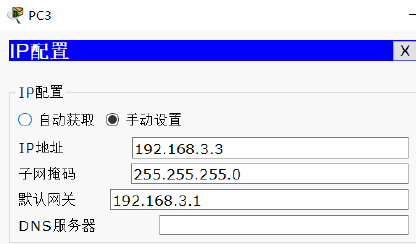
Vlan2（PC1）：



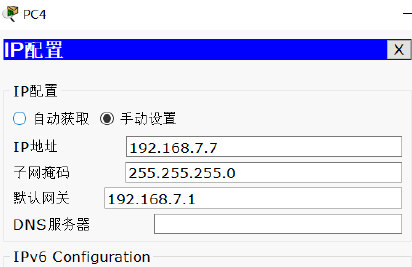
Vlan4（PC2）：



Vlan3（PC3）：



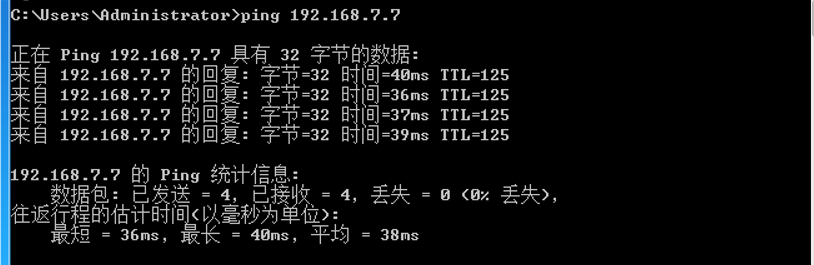
FTP（PC4）：



### 实验测试访问控制：

#### 访问控制前：

在访问控制前PC4（Vlan4）ping ftp服务器：

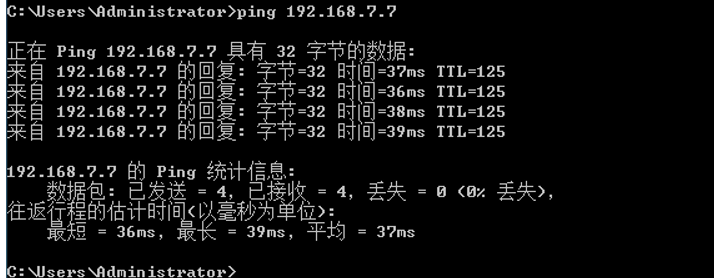


在访问控制前PC2(Vlan2)ping ftp服务器：

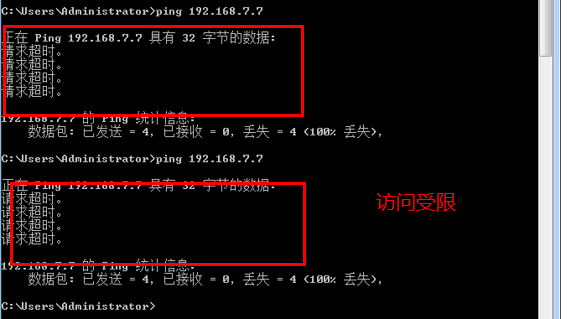


#### 访问控制后：

在访问控制后PC2(Vlan2)ping ftp服务器：

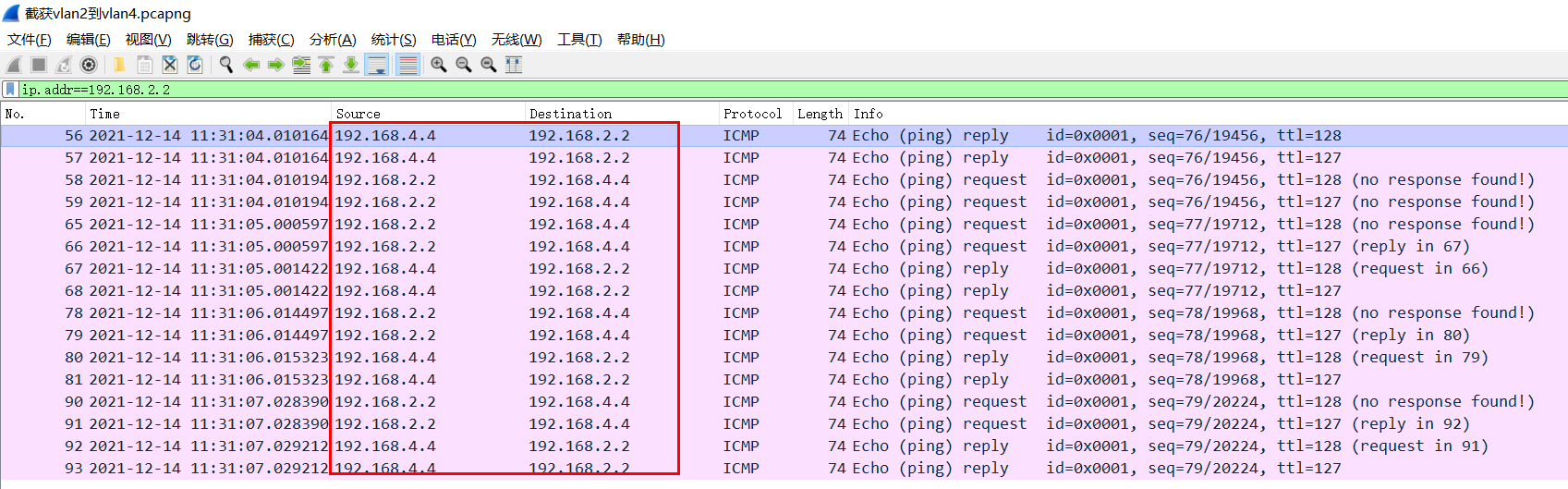


在访问控制后PC4(Vlan4)ping ftp服务器：



在设置了访问控制列表后，PC1能够访问FTP服务器，PC2则无法访问FTP服务器，从而看出访问控制成功。

### 实验测试端口镜像：



在PC3（Vlan3）中能够监控到PC2与PC4的流量访问，可见在三层交换机上配置端口镜像，可以实现对通过S1的流量数据包进行抓取，实现了流量监听，对于实际网络中的网络管理、网络安全应用有着重大的意义。

## （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VLAN3的主机上运行WireShark监听其他主机，需要配置端口镜像。端口镜像(port Mirroring〉通过在交换机或路由器上，将一个或多个源端口的数据流量转发到某一个指定端口来实现对网络的监听，指定端口称之为“镜像端口"或"“目的端口”，在不严重影响源端口正常吞吐流量的情况下，可以通过镜像端口对网络的流量进行监控分析。



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（取消）？

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：学生区(PC2、Vlan4）不能访问FTP服务器。这里是由于在路由器Rl中配置了ACL表，即访问控制表，而ACL表限制了192.168.4.0网段的通过(学生区)，即不能转发数据包，学生区也就无法访问到FTP服务器，将Wireshark的过滤器指定ip地址即可显示出学生网内的主机不能访问到FTP服务器。

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。

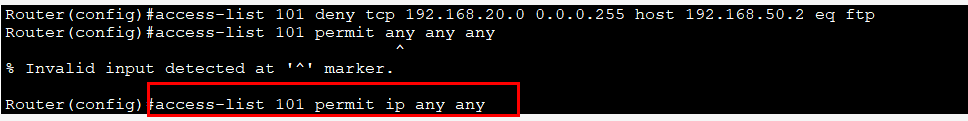
答：如下实验小结。

## （七）实验小结

（1）遇到的问题及其解决方案：

①在第一次、以及第二次在机房进行实验的时候，测试的结果都是Vlan3只能实现流量监听功能，无法ping通其余的三台主机，考虑到第一周可能是在配置了链路聚合时出现错误导致vlan3的主机无法ping到vlan2 以及vlan4的主机上，以及在第二周时可能是在设置访问控制时没有允许到vlan3的的访问，因此实验测试无法ping通，然后在思科模拟器上重新进行实验，并且按照一样的配置进行实验，发现vlan3的主机不仅能实现流量监听的功能也能够ping通其他网段的主机，因此怀疑以上实验的错误是有可能成立的，并不排除路由器的分组转发以及拓扑接线的错误实现。

②在第二次实验的时候，由于忘记在访问控制中允许其他的网络的访问，出现如下图的错误



并且经过与小组成员的讨论后，得出结果实验时第一次访问控制后能够正常按照实验需求完成访问，但在之后ftp 主机就拒绝了所有的访问，认识是在配置时没有设置permit any有关，只permit了192.168.4.0，192.168.2.0，192.168.3.0，但没有permit VLAN10所在的192.168.5.0网段。但是因为设置了交换机通过rip协议进行动态路由，那么就需要通过VLAN10去跟路由器R1交换路由信息。因为设置了对流入路由器的数据进行访问控制，那么可能仅仅是路由器接收不了交换机的路由信息，而交换机却能接收到路由器的路由信息，所以交换机是可能存在关于网段192.168.7.0的路由项。但就算是这样，交换机在解析下一跳IP的MAC地址时，也无法向路由器发送ARP报文。

至于实际的错误无法找出，但是认为讨论结果中的猜想是正确的。

1. 收获和启发：
   1. 通过进行计算机网络实验的最后一个实验，综合组网与配置实验总结了这学期大部分实验内容以及理论课的知识，并对其进行了整合利用，总体难度较大，要在实验要求的基础上，对于实验拓扑图的分析以及配置设计，还需要对每一步的设备进行自行设计的配置。通过此次实验对于计算机网络知识的掌握有了较大的提升，包括对网络拓扑结构的熟悉程度，以及对于学习到的计算机网络内容的总结。
   2. 然后是通过这次实验对之前学习的内容进行了一次很好的总结与复习，对于路由器、交换机的配置、端口聚合、VLAN的划分等有了进一步的认识，能够亲手设计实验并实验成功，能够对各种配置有了进一步的理解，并且认识到在学习计算机网络的过程中的知识的关系，在这次实验后，大大地提升了学习计算机网络的兴趣，并且，深刻地体会到了小组合作以及自我不气馁不放弃的精神，在实验效果欠佳的情况下和小组成员讨论，向老师询问，以及在自行于思科模拟器的实验后能够分析实验结果、排除实验错误。
   3. 此外，通过这次实验，还学会了ACL配置以及端口镜像，通过ACL（网络访问控制列表〉技术，可以设置类似黑白名单，对FTP服务器起到很好的保护作用，此技术在实际网络攻防中应用非常广泛，也能够体现出计算机网络对于安全性的需求，以及通过该门课程体会到信息安全专业的技术需要和实际生活中安全的重要性。在三层交换机上配置端口镜像后可以在网管机上对经过三层交换机的流量进行监控，通过这次实验，我学会了端口镜像操作，对于实际网络使用也有着重大意义，能够通过该实验使我对网络安全进行思考。

（3）不足与建议：

在本次实验中也遇到了问题，PC1、PC2、PC3之间可以互相ping通，但都ping不通PC4、流量监控后各主机没有进行正常的ping访问，检查连线配置都没有出现问题，并且思考过后也难以找出错误排除，因此感受到的不足就是对于实验的配置没有进行较为仔细的实验设计和配置，以及对于计算机网络知识的掌握没有做到熟记于心的程度，导致在实验过程中没有很好地配置好实验设施。

建议就是对于动手做实验的环节是真实地能让学生感受到学习计算机网络知识的乐趣，并且对于学习信息安全专业来说也有着很大的启示作用，因此对于实验环节可以多些指导和提供更多开放实验设施的机会。

**暨南大学本科实验报告专用纸(附页)**