**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 验证型 实验地点

学生姓名 张强 学号 2019053448

学院 智能科学与工程/人工智能产业学院

系 信息安全 专业

实验时间 2021 年 12 月 日 午～ 月 日 午 温度 ℃湿度

# 一、实验内容与目的

1.实验内容：

模拟某学校网络拓扑结构，在学校网络接入层采用S3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S1与路由器1相连，另外S1上有一个VLAN3存放一台网管机。路由器1和2通过路由协议获取路由信息后，办公网可以访问2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，路由器1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。

2. 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

【实验设备】：三层交换机（一台）、二层交换机（一台）、路由器（两台）、PC（四台）、FTP服务器（一台）。

【拓扑结构】：

网段：192.168.3.0

网关：192.168.3.1

PC3: 192.168.3.3

**VLAN3**

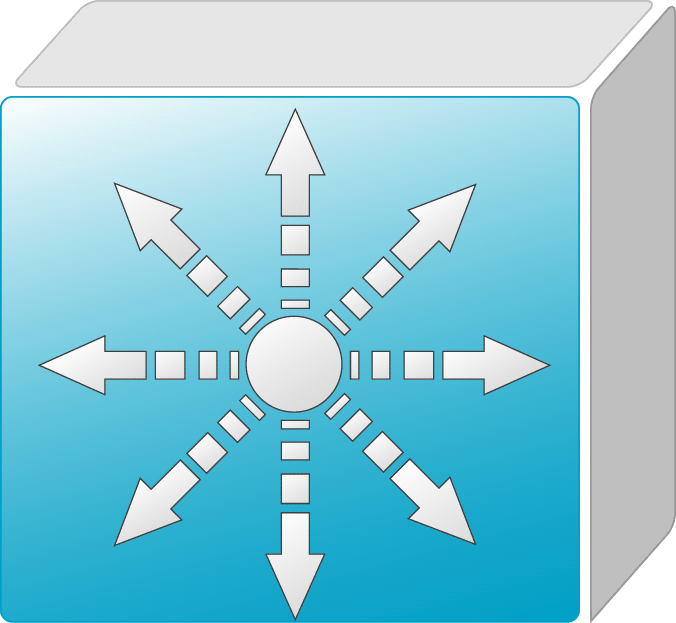
**VLAN4**

**VLAN2**

**FTP Server**

**S3**

**S1**



R2

右GE0/1:192.168.7.1

左S0/3/0:192.168.6.2

F0/10

F0/3

**VLAN10**

S1

右F0/10:192.168.5.1

**R2**

网段：192.168.7.0

网关：192.168.7.1

PC4: 192.168.7.7

**R1**

R1

左GE0/1:192.168.6.1

右S0/3/0:192.168.5.2

F0/5 F0/6

F0/4

F0/2

网段：192.168.4.0

网关：192.168.4.1

PC2: 192.168.4.4

网段：192.168.2.0

网关：192.168.2.1

PC1: 192.168.2.2

# 三、实验原理

**1.访问控制实验**

**【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。

**【实验环境】**

选2台路由器，分别命名为 R1 和 R4。拓扑结构及配置说明如图所示。 各路由器相关接口的 IP 地址分配如图中的标注。 **限制30.1.1.0/24网段主机访问10.1.1.0/24的主机。R1 路由器上配置访问控制列表。**

**R1**



GE 0/1

S2/0

**R2**



GE 0/1

S2/0

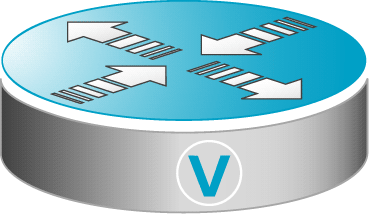
**10.1.1. 2/24**

**30.1.1.3/24**

**20.1.1. 2/24**

**20.1.1. 3/24**

**（提示：以下各步中涉及到的Serial口是以路由器r1和r2的连接为例，因不同小组有所不同，如果是路由器r3和r4的连接，请仔细参考路由器的连接图，并对实验步骤中的相关接口进行修改。）**



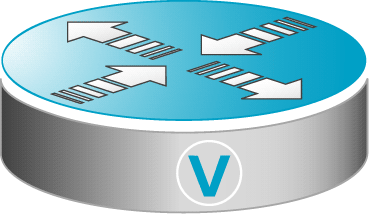
S2/0(DCE)

S2/0(DTE)

**R2**

**R1**

S3/0(DCE)



S3/0(DTE)

**R3**

**R4**

S2/0(DTE)

S2/0(DCE)

**2.RIP路由协议**

路由信息协议（Routing Information Protocol，缩写：RIP）是一种使用最广泛的内部网关协议（IGP），是基于距离矢量路由协定的协定。IGP是在内部网络上使用的路由协议(在少数情形下,也可以用于连接到因特网的网络)，它可以通过不断的交换信息让路由器动态的适应网络连接的变化，这些信息包括每个路由器可以到达哪些网络，这些网络有多远等。 IGP是应用层协议，并使用UDP作为传输协议。

同一自治系统(A.S.)中的路由器每 30秒会与相邻的路由器 交换子讯息，以动态的建立路由表。RIP 允许最大的hop数(跳数）为15 多于15跳不可达。

**具体配置如下：**

1.三层交换机（S1）

（1）划分4个VLAN：VLAN2、VLAN3、VLAN4、VLAN10.其中VLAN2对应办公区，VLAN4对应学习区，VLAN3对应网管机，VLAN10与路由器R1连通。

（2）使用动态路由，配置RIP协议，使得线路中的各个主机之间可以进行通信。

（3）使用链路聚合使得S3与S1之间能进行通信。

**2.二层交换机（S3）**

（1）划分两个VLAN：VLAN2和VLAN4，VLAN2中放PC1（教师机）端口，VLAN4中放PC2（学生机）端口。

（2）使用链路聚合使得S3和S1之间能够进行通信。

**3.端口镜像**

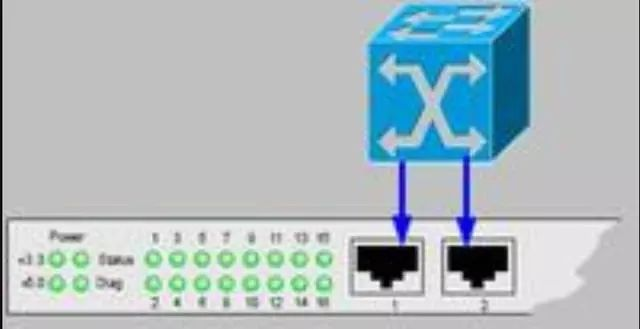
端口镜像（Port Mirroring）含义：

指将指定的源端口某些报文，镜像到指定的镜像目的端口，而不影响正常报文转发的功能；

1.端口镜像对特定端口的数据流量映射到监控端口，以便集中使用数据捕获软件进行分析。

2.端口镜像顾名思义就是针对端口所做的镜像操作。

在一些交换机中，我们可以通过对交换机的配置来实现将某个端口上的数据包，拷贝一份到另外一个端口上。



# 四、实验步骤

**1.配置三层交换机**

a:划分4个VLAN：VLAN2、VLAN3、VLAN4、VLAN10.其中VLAN2对应办公区，VLAN4对应学习区，VLAN3对应网管机，VLAN10与路由器R1连通。

b:使用动态路由，配置RIP协议，使得线路中的各个主机之间可以进行通信。

**第一步 登录到交换机**

S1>enable 14 => star

**第二步：在三层交换机S1上建立4个VLAN**

S1(config)#vlan 10

S1(config-vlan)#exit

S1(config)#vlan 2

S1(config-vlan)#exit

S1(config)#vlan 3

S1(config-vlan)#exit

S1(config)#vlan 4

S1(config-vlan)#exit

S1(config-vlan)#end //返回到特权模式

**第三步：在三层交换机S1上为4个VLAN分配IP 地址**

S1(config)#interface vlan 10

S1(config-if-vlan)#ip address 192.168.5.1 255.255.255.0

S1(config-if-vlan)#no shutdown

S1(config-if-vlan)#exit

S1(config)#interface vlan 2

S1(config-if-vlan)#ip address 192.168.2.1 255.255.255.0

S1(config-if-vlan)#no shutdown

S1(config-if-vlan)#exit

S1(config)#interface vlan 3

S1(config-if-vlan)#ip address 192.168.3.1 255.255.255.0

S1(config-if-vlan)#no shutdown

S1(config-if-vlan)#exit

S1(config)#interface vlan 4

S1(config-if-vlan)#ip address 192.168.4.1 255.255.255.0

S1(config-if-vlan)#no shutdown

S1(config-if-vlan)#exit

**第四步：将端口0/3、0/10分别放入VLAN 3和VLAN 10**

S1(config)#interface fastethernet 0/3

S1(config-if)#switchport access vlan 3

S1(config-if)#exit

S1(config)#interface fastethernet 0/10

S1(config-if)#switchport access vlan 10

S1(config-if)#exit

**第五步：把交换机S1与S3连接的0/5，0/6接口做成trunk模式。**

S1(config)#spanning-tree vlan 1 //关闭树协议

S1(config)#int range f0/5-6 //进入fastEthernet 0/5-6端口

S1(config-if-range)#channel-group 1 mode on //将这两个端口打开

S1(config-if-range)#no shutdown //开启端口

S1(config-if-range)#exit

S1(config)#int port-channel 1

S1(config-if)#switchport trunk encapsulation dot1q //给端口封装一个接口封装协议

S1(config-if)#switchport mode trunk

**第六步：配置端口镜像（为了使PC3能流量监控）**

S1(config)#monitor session 1 source interface fastethernet 0/5 – 6 rx ！5、6端口设置为源端口（要抓取流量的端口）

S1(config)# monitor session 1 source interface fastethernet 0/10 rx

S1(config)# monitor session 1 source interface fastethernet 0/1 rx

S1(config)# monitor session 1 destination interface fastethernet 0/3 ！3端口设置为目的端口

**第七步：配置动态路由（RIP协议）。**

S1(config)#ip routing //开启三层交换功能

S1(config)# router rip ！创建RIP路由进程

S1(config-router)#network 192.168.5.0 ！定义关联网络192.168.5.0（必须是直连的网络地址）

S1(config-router)#network 192.168.2.0 ！定义关联网络192.168.2.0（必须是直连的网络地址）

S1(config-router)#network 192.168.3.0 ！定义关联网络192.168.3.0（必须是直连的网络地址）

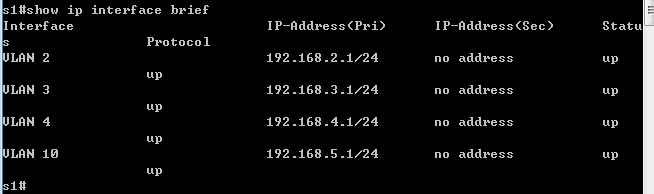
S1(config-router)#network 192.168.4.0 ！定义关联网络192.168.4.0（必须是直连的网络地址）

**第八步：查看配置信息。**

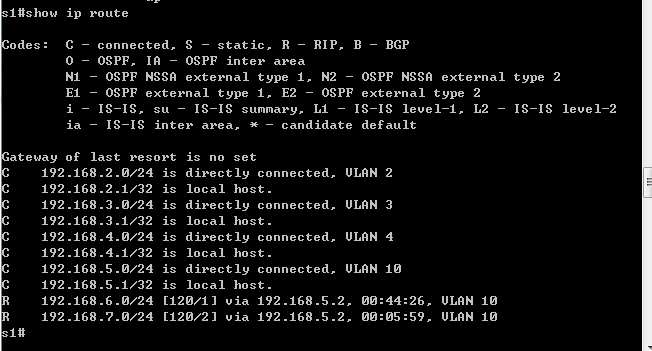
S1#show vlan !显示VLAN的配置

S1#show ip route !显示路由表

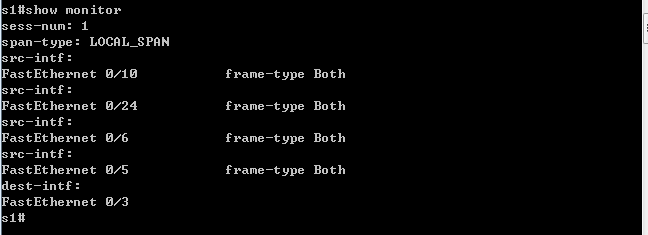
三层交换机ip配置



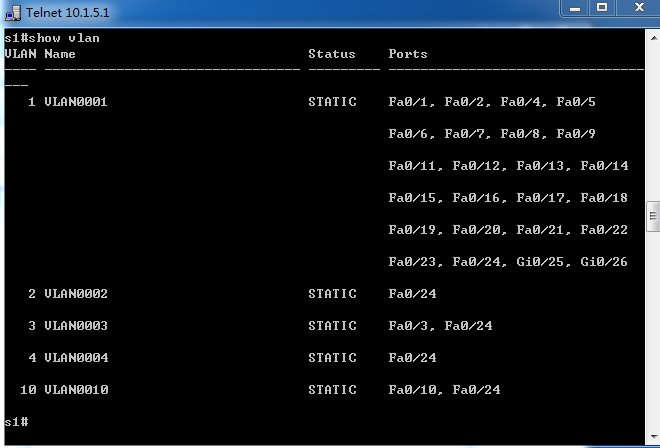
三层交换机路由配置



三层交换机端口镜像



三层交换机vlan配置表



**2.配置二层交换机**

a:划分两个VLAN：VLAN2和VLAN4，VLAN2中放PC1（教师机）端口，VLAN4中放PC2（学生机）端口。

**第一步： 登录到交换机**

S3>enable 14 => star

**第二步：在二层交换机S3上建立2个VLAN**

S3(config)#vlan 2

S3(config-vlan)#exit

S3(config)#vlan 4

S3(config-vlan)#end !返回到特权模式

**第三步：将端口0/2、0/4分别放入VLAN 2和VLAN 4**

S3(config)#interface fastethernet 0/2

S3(config-if)#switchport access vlan 2

S3(config-if)#exit

S3(config)#interface fastethernet 0/4

S3(config-if)#switchport access vlan 4

S3(config-if)#exit

**第四步：把交换机S3与S1连接的0/5，0/6接口做成trunk模式（聚合端口）。**

S3(config)#spanning-tree vlan 1 //关闭树协议

S3(config)#int range f0/5-6 //进入fastEthernet 0/5-6端口

S3(config-if-range)#channel-group 1 mode on //将这两个端口打开

S3(config-if-range)#no shutdown //开启端口

S3(config-if-range)#exit

S3(config)#int port-channel 1

S3(config-if)#switchport mode trunk

**第五步：显示VLAN配置和trunk配置。**

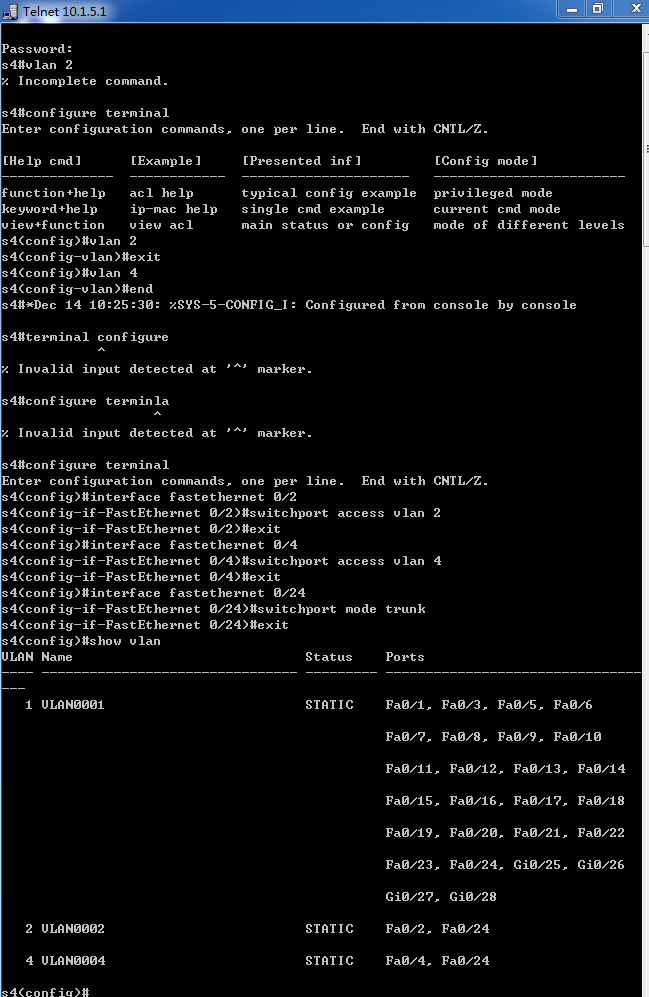
S3 #show vlan ！//显示VLAN配置信息

S3#show etherchannel summary //显示聚合端口信息

或者

S3#show etherchannel port-channel

二层交换机配置命令



**3.配置路由器R1**

**3.路由器（R1）**

A:配置好GE0/1和S2/0端口以及RIP协议，实现路由转发。

B:配置访问控制表拒绝VLAN4（学生网）访问FTP服务器。

**第一步 登录到路由器**

命令：

R1>enable 14 => star

**第二步 配置路由器接口GigabitEthernet 0/1和串行口Serial 2/0的IP地址**

R1(config)#interface GigabitEthernet 0/1 ！进入接口的配置模式

R1(config-if)#ip address 192.168.5.2 255.255.255.0 ！配置接口IP地址

R1(config-if)# no shutdown ！开启路由器的接口

R1(config-if)#exit

R1(config)#interface serial 0/3/0 ！进入串行口s0/3/0的配置模式。

R1(config-if)#ip address 192.168.6.1 255.255.255.0 ！配置接口S0/3/0的IP地址。

R1(config-if)#clock rate 64000 ！配置R1(必须为DCE)的时钟频率

R1(config-if)#no shutdown ！开启s0/3/0端口

R1(config-if)#exit

**第三步 配置动态路由（RIP协议）。**

R1(config)# router rip ！创建RIP路由进程

R1(config-router)#network 192.168.5.0 ！定义关联网络192.168.5.0（必须是直连的网络地址）

R1(config-router)#network 192.168.6.0 ！定义关联网络192.168.6.0（必须是直连的网络地址）

R1(config-router)#version 2

R1(config-router)#exit

**第四步 配置访问控制列表。**

R1(config)#access-list 1 deny 192.168.4.0 0.0.0.255 ！限制192.168.4.0/24 网段

R1(config)#access-list 1 permit 192.168.2.0 0.0.0.255 ！允许192.168.2.0/24 网段

R1(config)#access-list 1 permit 192.168.3.0 0.0.0.255 ！允许192.168.3.0/24 网段

R1(config)#access-list 1 permit any ！允许其他所有网段

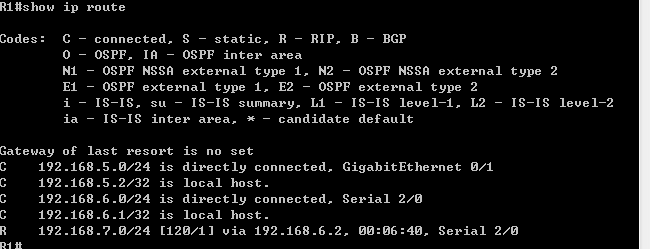
R1(config)# interface GigabitEthernet 0/1 ！在 R1 路由器 interface GigabitEthernet 0/1 接口的进入方向引用了访问控制列表 ，目的是过滤来自 192.168.4.0/24网段的数据包，允许其他两个网段的数据包通过。

R1(config-if)#ip access-group 1 in ！数据包是进入（in）,离开（out）路由器



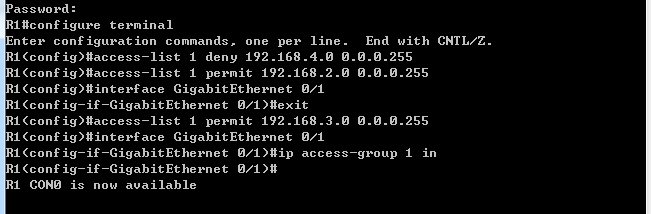
**第五步 查看配置信息。**

**R1路由表**





路由表R1的访问控制



**分析：把ip：192.168.5.2分配给了GE0/1端口，ip：192.168.6.1网段成功分配给了S0/3/0端口。此外该路由器还配置了ACL来禁止192.168.4.0网段(学生)访问FTP。路由器R1配置完毕。**

**4.配置路由器R2**

**4.路由器（R2）**

a:配置好GE0/1和S2/0端口与RIP协议，实现路由转发。

**第一步 登录到路由器**

命令：

R2>enable 14 => star

**第二步 配置路由器接口GigabitEthernet 0/1和串行口Serial 2/0的IP地址**

R2(config)#interface GigabitEthernet 0/1 ！进入接口的配置模式

R2(config-if)#ip address 192.168.7.1 255.255.255.0 ！配置接口IP地址

R2(config-if)# no shutdown ！开启路由器的接口

R2(config)#exit

R2(config)#interface serial 0/3/0 ！进入串行口s0/3/0的配置模式。

R2(config-if)#ip address 192.168.6.2 255.255.255.0 ！配置接口S0/3/0的IP地址。

R2(config-if)#clock rate 64000 ！配置R1(必须为DCE)的时钟频率

R2(config-if)#no shutdown ！开启s2/0端口

R2(config-if)#exit

**第三步 配置动态路由（RIP协议）。**

R2(config)# router rip ！创建RIP路由进程

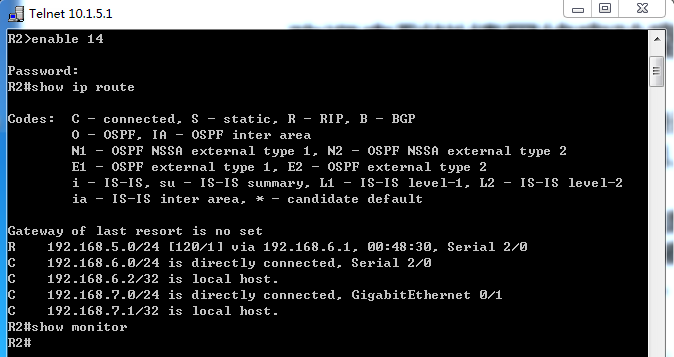
R2(config-router)#network 192.168.6.0 ！定义关联网络172.16.1.0（必须是直连的网络地址）

R2(config-router)#network 192.168.7.0 ！定义关联网络172.16.2.0（必须是直连的网络地址）

R2(config-router)#version 2

R2(config-router)#exit

**第四步 查看配置信息。**

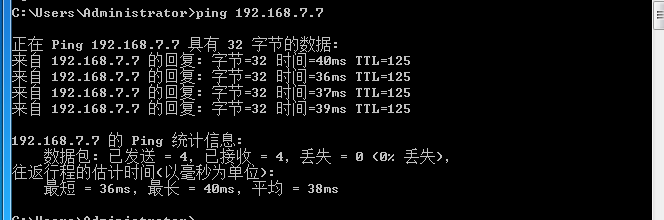


分析：可以看到，这里成功把ip：192.168.7.1分配给了GE0/1端口，ip：192.168.6.2网段成功分配给了S0/3/0端口。然后接下相应线路，就能在路由表中看到了正确的网段信息。路由器R2配置完毕。

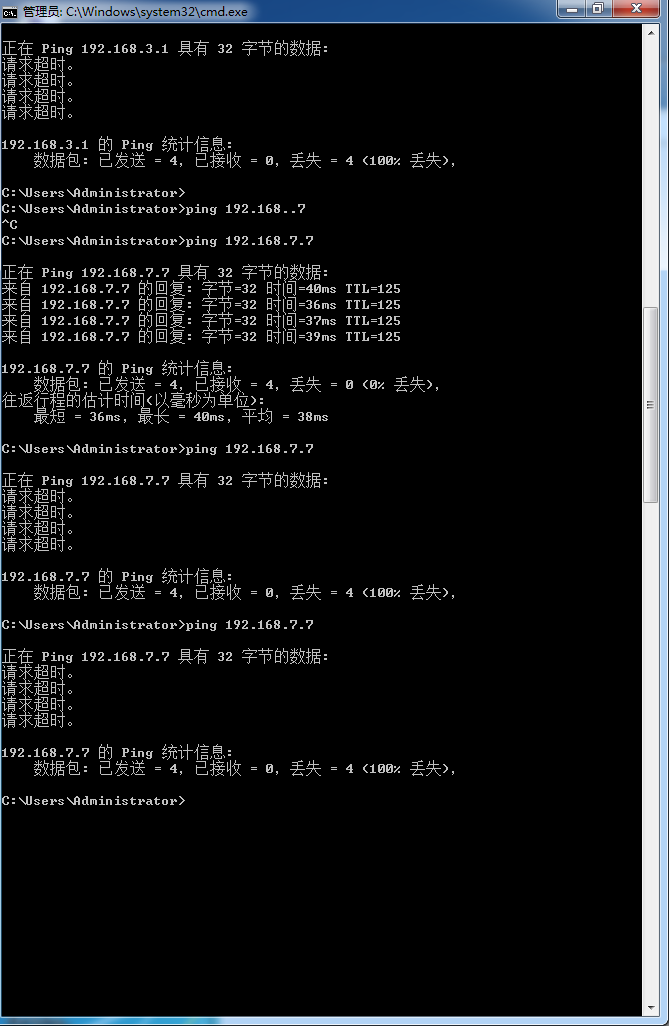
**5.测试**

**使用ping命令测试网络的连通性**

访问控制前PC2（学生区） ping PC4（FTP服务器）

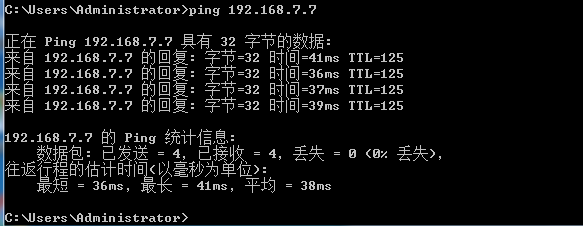


访问控制后PC2（学生区） ping PC4（FTP服务器）



Ping不通，拦截成功

访问控制前PC1（办公区） ping PC4（FTP服务器）



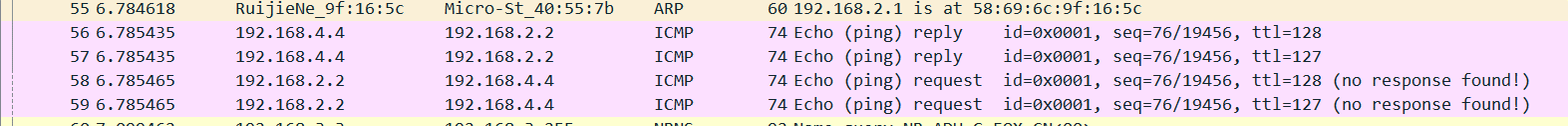
访问控制前PC1（办公区） ping PC4（FTP服务器）



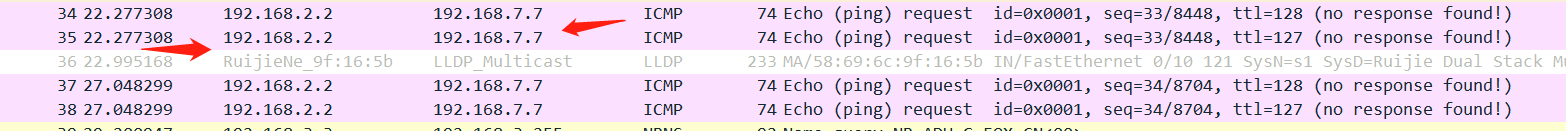
分析：PC1（教学网机子）在访问控制后可以ping通PC4（FTP服务器），PC2（学生网机子）在访问控制后不能ping通PC4（FTP服务器），实验成功。

在PC3（网管机）上开启Wireshark进行抓包。

（1）在PC1 ping PC2的过程中，在PC3上抓到了icmp数据包，包括PC1的请求包和PC2的应答包。截图如下：



（2）在PC1 ping FTP服务器的过程中，在PC3上抓到了icmp数据包，包括PC1的请求包和PC4的应答包。截图如下：

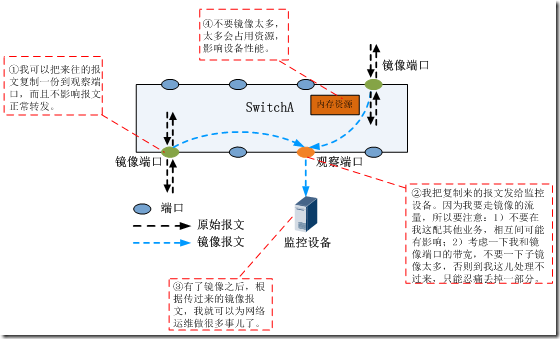


分析：通过在三层交换机S1上配置了端口镜像，PC3（网管机）可以实现对通过S1的流量数据包进行抓取，实现流量监听，通过流量抓包软件进行流量抓包验证，在监控设备上进行抓包测试，可以获取到源端口发送或接收的数据包，则端口镜像成功。

问题：

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

为实现监听FTP流量，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。



基本命令如下：

monitor session 2 source interface Gig 0/1   //配置要抓取原端口的流量

monitor session 2 destination remote vlan 100   //目的端口配置为SPAN的vlan

2、学生网内的主机不能访问FTP服务器，能否ping通呢？为什么？

学生网内的主机不能访问FTP服务器，不能ping通。因为在R1路由上配置了访问控制列表（ACL），ACL可以过滤网络中的流量，实际上，ACL的本质就是用于描述一个IP数据包，是一个以太网数据帧包含若干特征的集合，然后ACL根据这些集合去匹配网络中的流量（由大量数据包组成），同时根据策略来“允许”或“禁止”，而ACL表限制了192.168.4.0网段的通过，那么就无法转发数据包，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。

3、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

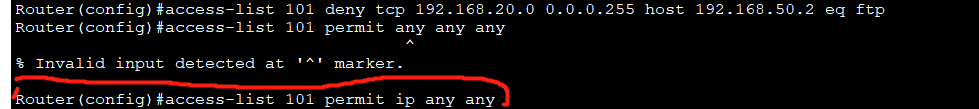
SwitchA(config-if-range)#port-group 1 ！配置端口0/1、0/2属于AG1

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

# 五、实验总结

**1.**问题及解决方案

1. 在计算机网络机房进行实验的时候，通过Vlan3（PC3）与其他三台计算机ping，发现无法ping通ping通三台主机，但通过wireshark发现却能实现流量监控的功能，由于之前我们配置了链路聚合，所以我们猜测是这一原因导致的，另外我们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。之后我们在思科模拟器上重新进行实验，相同配置进行实验，发现PC3不仅能实现流量监听的功能也能够ping通其他网段的主机，所以上诉的猜想是大概率成立的，并不排除其他原因导致的，比如常见的路由器的分组转发出现的错误。
2. 还有，在实验的时候，由于忘记在访问控制中permit其他的网络的访问，出现如下的错误



并且经过与小组成员的讨论后，之所以第一次的访问控制后能够按照实验要求完成访问，而第二次第三次再试，ftp 就不允许访问，是因为我们在配置时没有设置permit any，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。交换机是通过rip协议去进行动态路由，所以需要通过VLAN10去跟路由器R1交换路由信息。对流入路由器的数据进行了访问控制，所以也有可能是路由器仅仅接收不了交换机的路由信息，但是交换机却能接收到路由器的路由信息，交换机是可能存在关于网段192.168.7.0的路由项的。综上所述，交换机在解析下一跳IP地址的MAC地址时，无法向路由器发送对应的ARP报文。

**2**.通过这次综合组网配置实验，让我对计算机网络的学习有了更加全面的了解，本次实验工程量较大，而更加考验了我的动手实践能力以及发现问题并解决问题的能力，在不断地试错地过程中成长。

**3**.其次，通过这次实验，对之前实验中有涉及的路由器、交换机的配置、VLAN的划分内容有了更加深刻地理解；很重要的是，让我对之前非常陌生的访问控制列表（ACL）有了一定程度上的了解，端口镜像是指在交换机或者路由器上将经过指定端口（源端口）的数据报文复制一份到另一个指定端口（目标端口）上，来实现对网络流量的分析与监控。一些对实时监控比较注重的用户在网络遭受了各种攻击，需要检查流量而不希望影响原来的网络时，可以利用端口镜像，例如我国文化部和公安部要求网络服务场所安装监控软件，通过端口镜像采集相关数据，分析用户的网络使用情况。

**4**.通过一学期计算机网络学习以及每周的实验，让我对计算机网络原理以及计算机网络的实际应用有了大致的了解，让我对以后深入计算机网络的学习有了更大的兴趣。

。