**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 综合组网配置 指导教师

实验项目编号 12 实验项目类型 验证型 实验地点

学生姓名 林晓旭 学号 2019051121

学院 智能科学与工程 系 专业 信息安全

实验时间2021 年 12月 7 日 下 午～ 12 月 15 日 下午

1. **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。

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。

1. **实验原理**
2. VLAN

VLAN（Virtual Local Area Network)，虚拟局域网，用于将局域网划分成更小地子网，目的是隔离广播域，避免发生广播风暴。

目前常用的虚拟局域网标准是IEEE 802.3ac。这个标准定义了以太网的帧格式的扩展，以便支持虚拟局域网。该标准允许在在以太网帧中插入一个4字节的标识符，称为VLAN Tag。用来指定该数据帧属于哪个虚拟局域网的。在VLAN Tag的前16位是一个固定的值0x8100H，其后16位的前4位并没有什么作用，而后12为才为真正的VLAN号。该VLAN Tag插在以太网帧中MAC源地址字段和类型字段的中间。那么这样以太网帧的最大帧从原来的1518（1500+6+6+2+4）变成1522字节。

1. 端口镜像

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。如果目标端口和源端口在同一台物理网络设备上，叫做本地镜像；否侧叫做远程镜像。镜像方向指的是若监控的源端口的数据流向，有流入、流出和双向三种可选。 一般来说远程镜像通过VLAN镜像来实现。

1. 访问控制

访问控制的作用是限制某些特定数据包的传输，通过访问控制表（Access Control List）来实现。访问控制表是在路由器中定义的，访问控制表又可分为标准访问控制列表和扩展访问控制列表。区别如下：

**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

值得注意的是，在路由器实现访问控制功能的过程中，通过遍历访问控制列表来寻找与当前数据包IP信息匹配的控制列表项，若找到了一个符合条件的控制列表项，则停止遍历。所以，这隐式地表明了处在表头的控制项具有更高的优先级。

访问控制表隐含一个默认的deny any的控制表项，当没有与当前数据包IP信息匹配的控制表项时，数据包会被拒绝，所以在定义访问控制表时，需要在最后加上permit any。

1. **实验过程**

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；

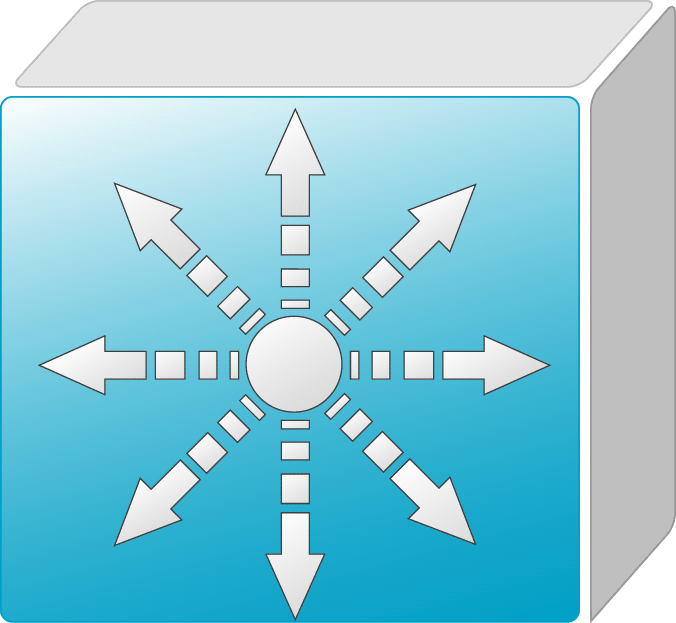
2、本实验安排学时为4学时，实验前每个小组提交一份实验预习报告。预习报告包括实验内容、配置设计和步骤。详细描述IP地址配置、设备的连接端口号。本部分15分。

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。

**VLAN4**

**VLAN2**

**VLAN3**



**FTP Server**

**S3550**

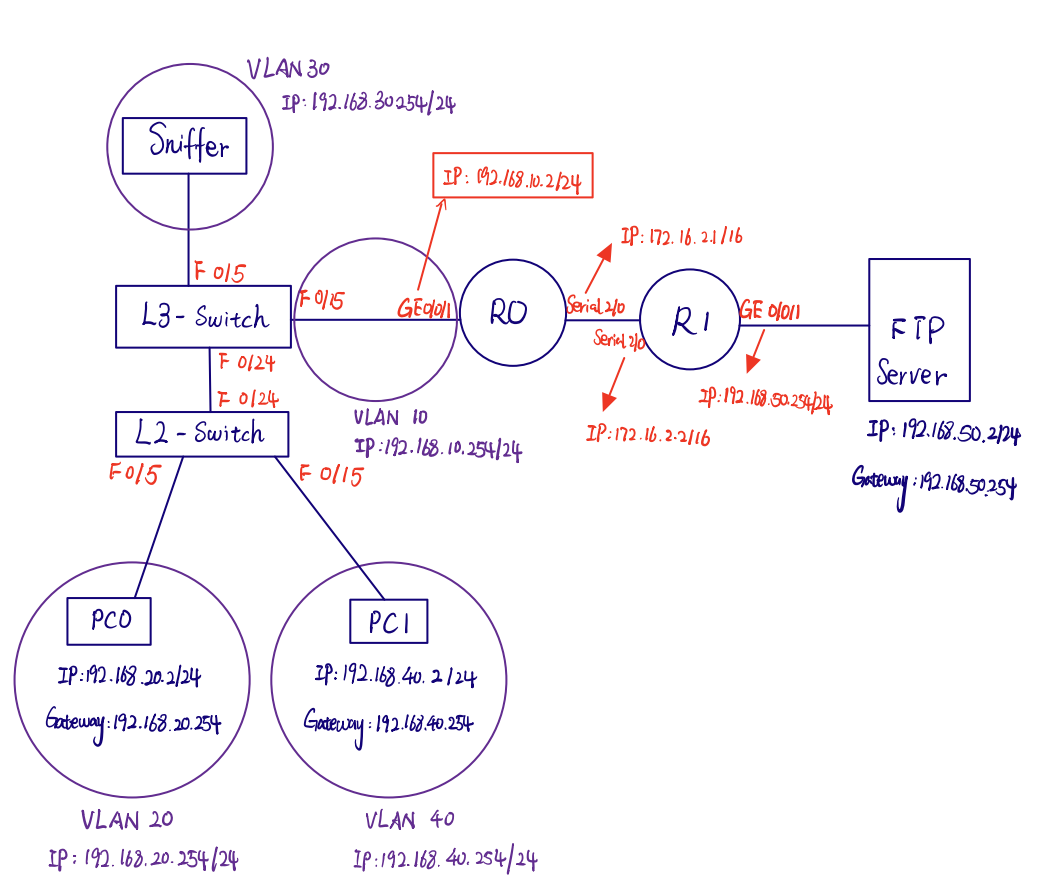
**B**

**A**

**VLAN1**

**S2126**

1. 详细化网络拓扑图，本实验中用嗅探器来替代了其中一台PC



1. 对二层交换机进行VLAN划分

SwitchA(config)#vlan 20

SwitchA(config)#vlan 40

SwitchA(config)#interface fastEthernet 0/5

SwitchA(config-if)#switchport access vlan 20

SwitchA(config)#interface fastEthernet 0/15

SwitchA(config-if)#switchport access vlan 40

SwitchA(config-if)#interface fastethernet 0/24

SwitchA(config-if)#switchport mode trunk

SwitchA(config-if)#end ！ 退出到特权模式

SwitchA #show vlan ！ 显示VLAN配置信息

SwitchA #show interface fastethernet 0/24 switchport

SwitchA #show interface fastethernet 0/24 trunk

1. 对三层交换机进行VLAN划分以及为VLAN分配IP地址

SwitchA(config)#vlan 10

SwitchA(config-vlan)#exit

SwitchA(config)#vlan 20

SwitchA(config-vlan)#exit

SwitchA(config)#vlan 30

SwitchA(config-vlan)#exit

SwitchA(config)#vlan 40

SwitchA(config-vlan)#exit

SwitchA(config)#interface fastethernet 0/5

SwitchA(config-if)#switchport access vlan 30

SwitchA(config)#interface fastethernet 0/15

SwitchA(config-if)#switch access vlan 10

SwitchA(config)#interface fastethernet 0/24

SwitchA(config-if)#switchport mode trunk

**SwitchA(config)#interface vlan 10**

**SwitchA(config-if)#ip address 192.168.10.254 255.255.255.0**

SwitchA(config-if)#no shutdown。

**SwitchA(config)#interface vlan 20**

**SwitchA(config-vlan)#ip address 192.168.20.254 255.255.255.0**

SwitchA(config-if)#no shutdown

**SwitchA(config)#interface vlan 30**

**SwitchA(config-if)#ip address 192.168.30.254 255.255.255.0**

SwitchA(config-if)#no shutdown。

**SwitchA(config)#interface vlan 40**

**SwitchA(config-vlan)#ip address 192.168.30.254 255.255.255.0**

SwitchA(config-if)#no shutdown

1. 对三层交换机进行动态路由配置

SwitchA(config)# router rip

**SwitchA(config-router)#network 192.168.10.254（必须是直连的网络地址）**

**SwitchA(config-router)#network 192.168.20.254（必须是直连的网络地址）**

**SwitchA(config-router)#network 192.168.30.254（必须是直连的网络地址）**

**SwitchA(config-router)#network 192.168.30.254（必须是直连的网络地址）**

SwitchA(config-router)#exit

1. 对路由器R0的端口进行配置并设置动态路由

RouterA(config)#**interface GigabitEthernet 0/0/1**

RouterA(config-if)# ip address 192.168.10.2 255.255.255.0

RouterA(config-if)# no shutdown

RouterA(config)#interface serial 2/0

RouterA(config-if)#ip address 172.16.2.1 255.255.255.0

RouterA(config-if)#no shutdown

RouterA(config-if)#exit

**RouterA(config)# router rip**

**RouterA(config-router)#network 192.168.10.0（必须是直连的网络地址）**

**RouterA(config-router)#network 172.16.2.0（必须是直连的网络地址）**

1. 同理，对路由器R1的端口进行配置并设置动态路由

RouterA(config)#**interface GigabitEthernet 0/0/1**

RouterA(config-if)# ip address 192.168.50.254 255.255.255.0

RouterA(config-if)# no shutdown

RouterA(config)#interface serial 2/0

RouterA(config-if)#ip address 172.16.2.2 255.255.255.0

RouterA(config-if)#no shutdown

RouterA(config-if)#exit

**RouterA(config)# router rip**

**RouterA(config-router)#network 192.168.50.0（必须是直连的网络地址）**

**RouterA(config-router)#network 172.16.2.0（必须是直连的网络地址）**

10、对R1进行访问控制列表的设置

**定义扩展访问控制列表，控制从网段192.168.20.0发送的FTP数据包流向主机192.168.50.2**

**R1(config)#access-list 101 deny tcp 192.168.20.0 0.0.0.255 host 192.168.50.2 eq ftp**

**R1(config)#access-list 101 permit ip any any**

**R1(config)#interface gigabitEthernet 0/0/1**

**R1(config-if)#ip access-group 101 out**

11、对三层交换机设置端口镜像

**SwitchA(config)#monitor session 1 source interface fastEthernet 0/24 both**

**SwitchA(config)#monitor session 1 destination interface fastEthernet 0/5**

**SwitchA(config)#show monitor**

12、

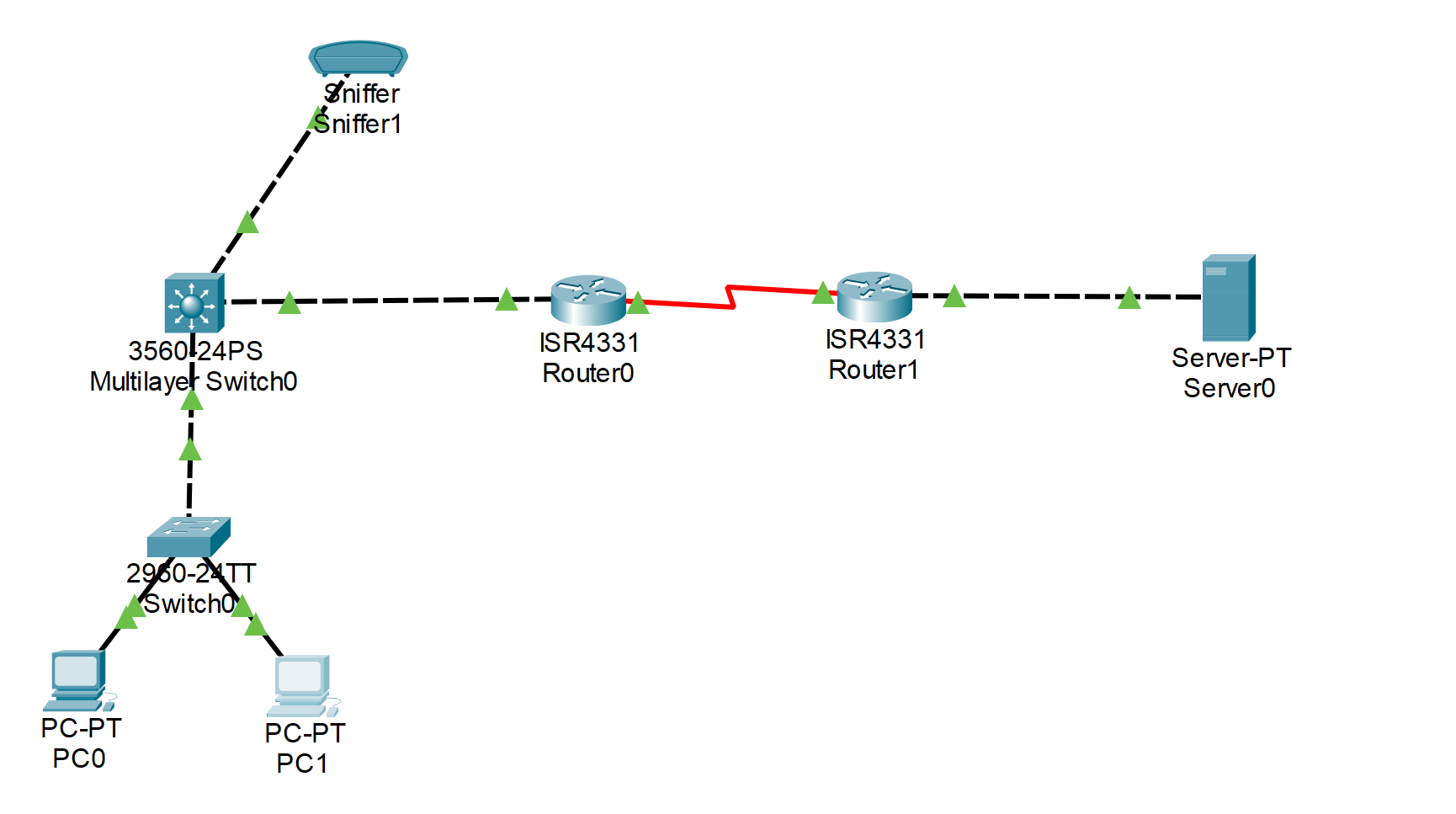
对主机PC0,PC1以及FTP服务器进行IP信息配置，将PC0,PC1的网关设置成VLAN的IP地址，将FTP服务器的网关设置成直接路由器接口的IP地址

13、

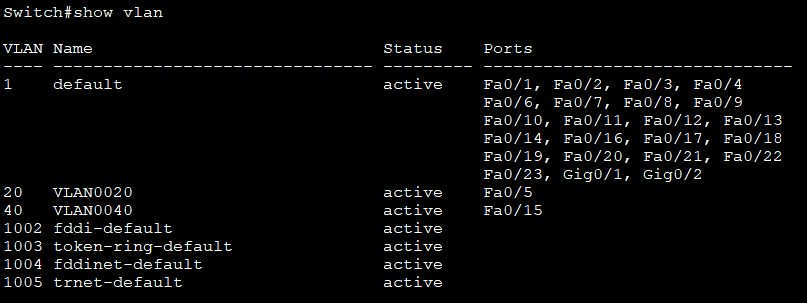
进行连通性测试

1. **实验结果**

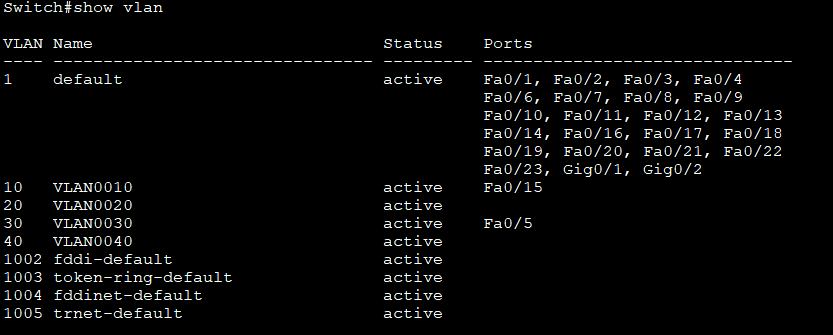
按照拓补图在Cisco packet tracer上对网络进行布局



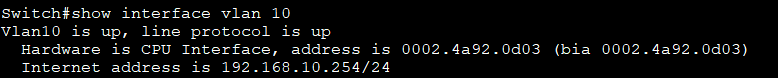
1、对二层交换机进行VLAN划分



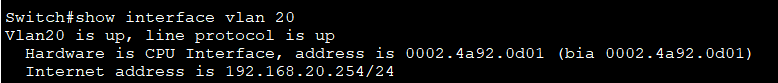
2、对三层交换机进行VLAN划分以及设置VLAN的IP地址



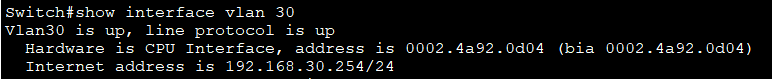
VLAN 10 IP



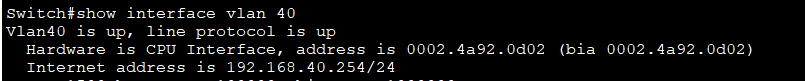
VLAN 20 IP



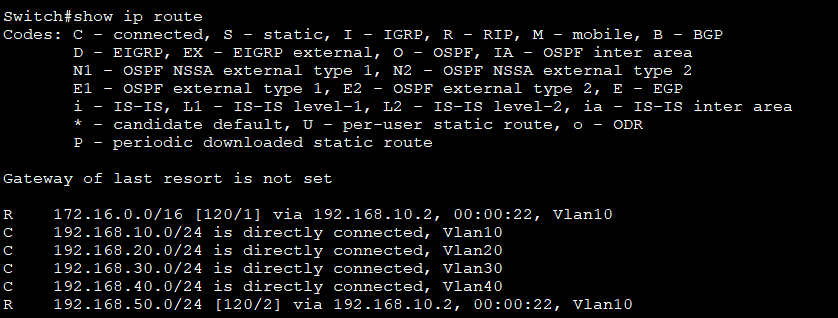
VLAN 30 IP



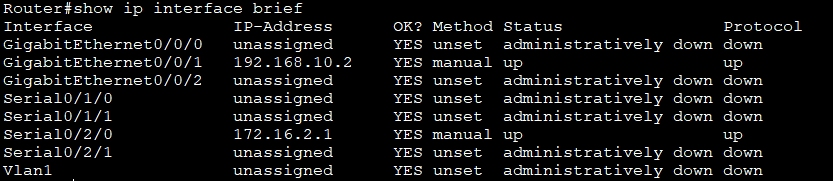
VLAN 40 IP

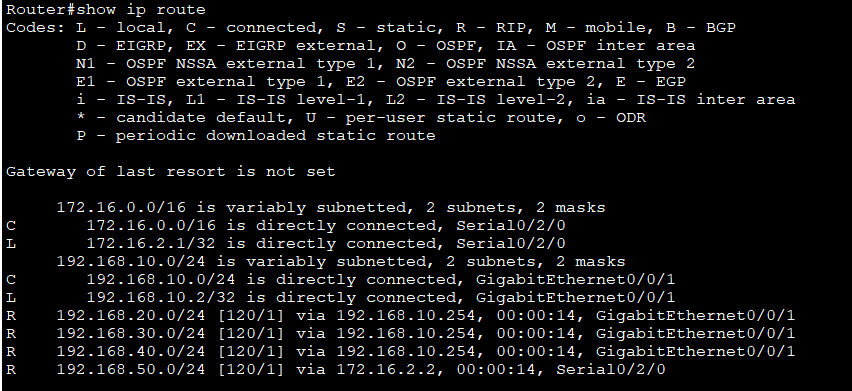


3、对三层交换机进行动态路由配置

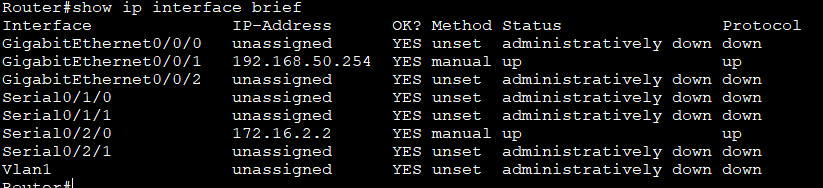


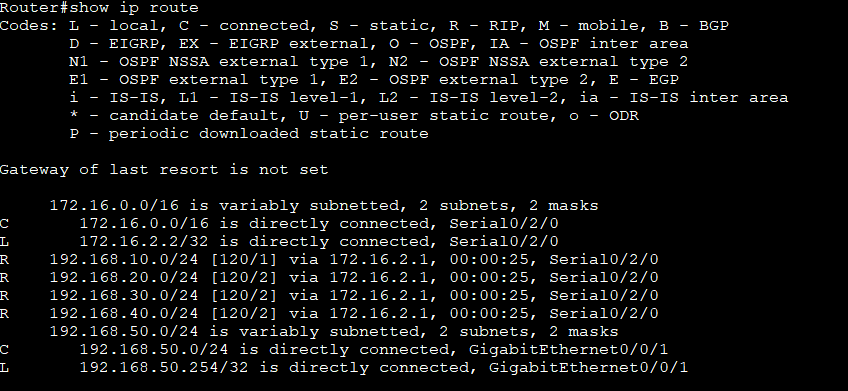
4、对路由器R0进行配置



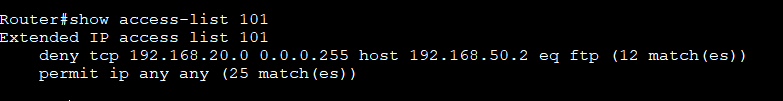


5、对路由器R1进行配置

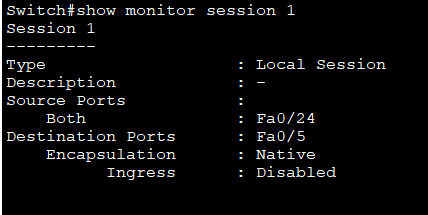




6、对R1进行扩展访问控制列表的配置

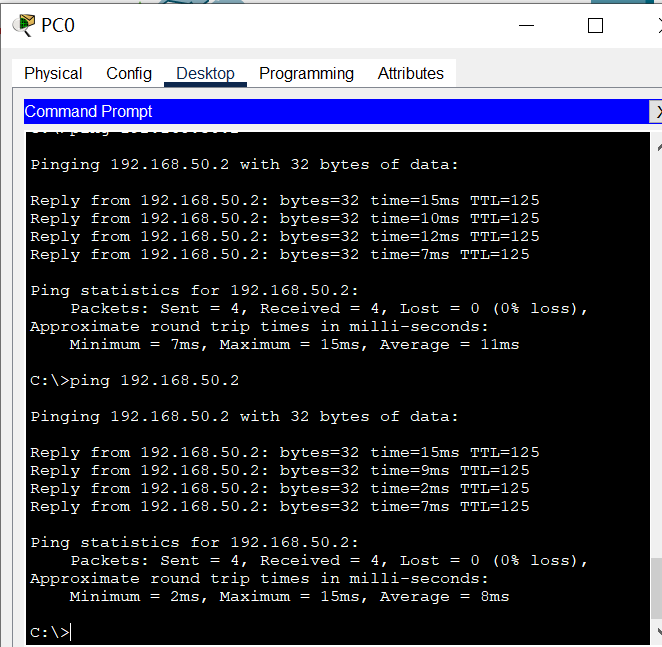


7、对交换机进行端口镜像配置

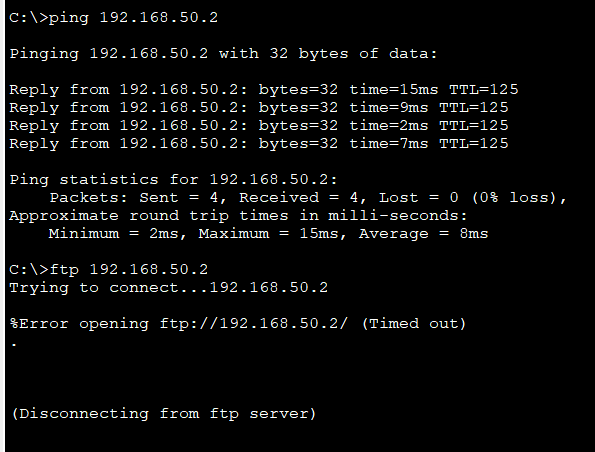


8、测试连通性

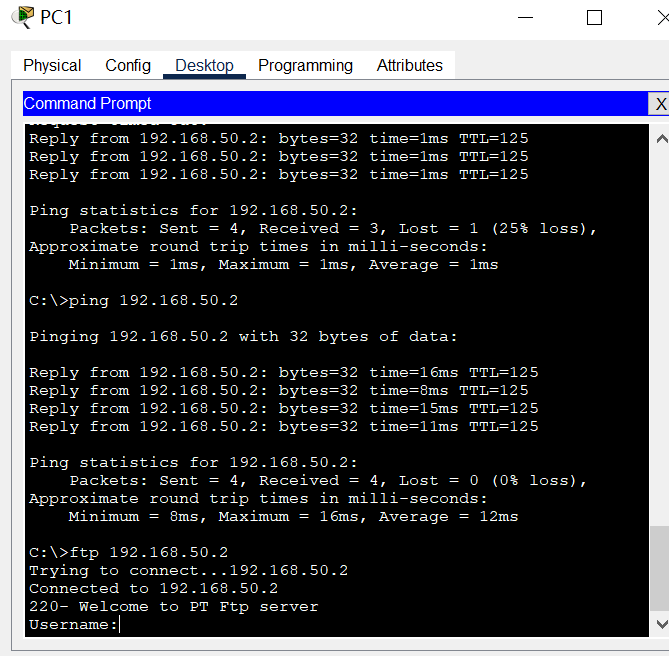
（1）、PC0 ping FTP服务器，发现能ping通



（2）、PC0访问FTP服务器的FTP服务，发现无法连接

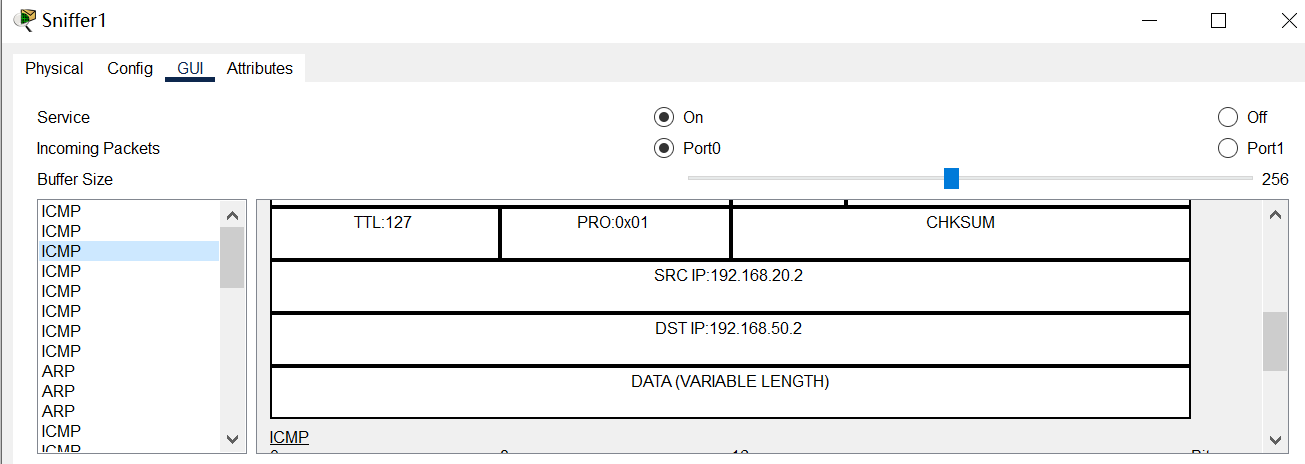


（3）、PC1 ping FTP服务器，发现能ping通；访问FTP服务器的FTP服务也能成功

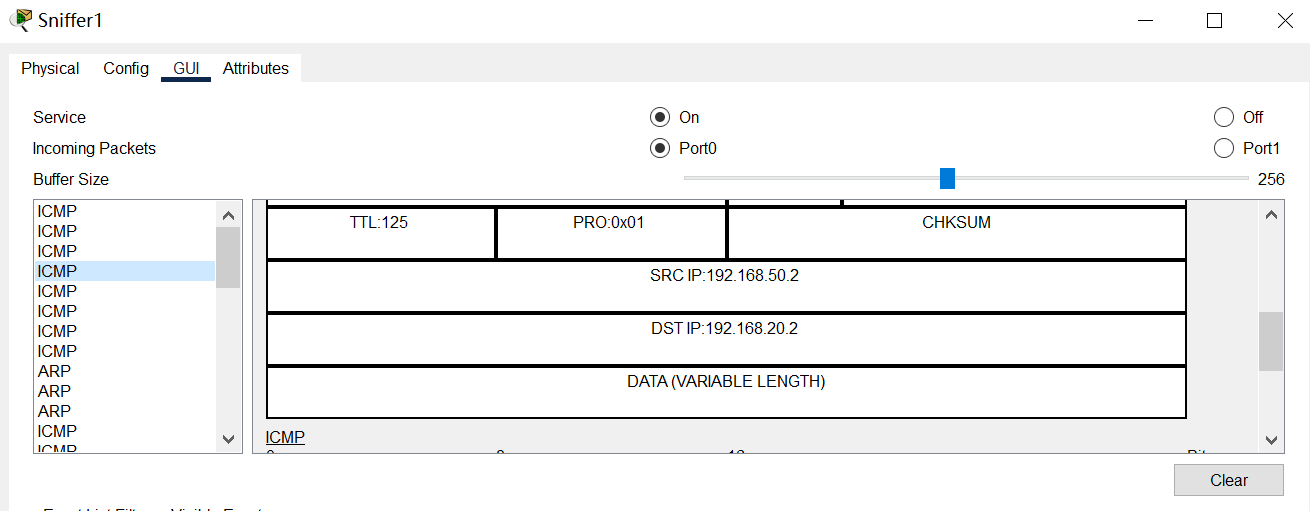


（4）、利用端口镜像进行流量监控，结果是能成功抓包

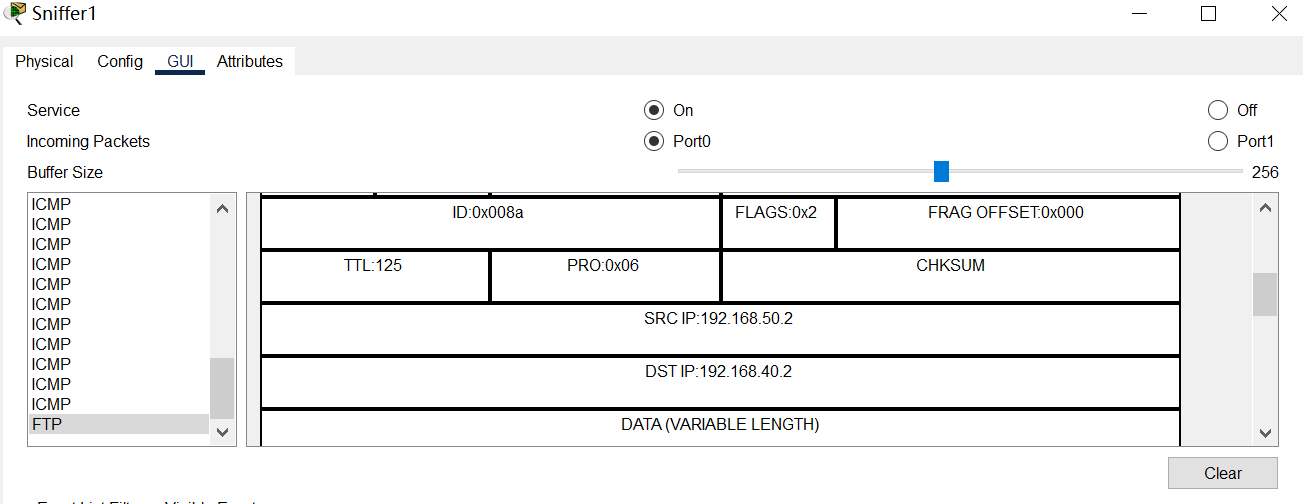
PC0 ping FTP服务器的包（ICMP Request）



FTP服务器回应PC0的包（ICMP Reply）



FTP协议包



1. **实验总结**

本实验的目的在于对以往的实验有一个综合的应用，涉及到在交换机上进行VLAN划分、VLAN间通信、路由协议配置。除了对以往实验的综合，本实验还进行了一定的延申，比如在路由器上定义访问控制列表进行流程控制，交换机上进行端口镜像操作以达到流量监控的目的。本人给予这个实验较高的评价。

由于课堂在机房实际操作时间有限且小组人数多难以协调，所以本人在思科模拟器（Cisco Packet Tracer）上进行了仿真实验，对实验中的每一个细节都能深刻把握。

本次实验所作的访问控制利用的是扩展访问控制表（Extended Access Control List），扩展访问控制的优点在于能对流量数据包进行更加精确的控制，因为它是基于源IP地址和目标IP地址以及tcp/ip特定协议端口号。这也是为什么本实验中PC0能ping得通FTP服务器但却不能访问FTP服务器的FTP服务。（ping命令基于ICMP协议，FTP服务基于FTP协议）。

在本实验中我们用一个嗅探器（sniffer）替代了监听主机，但并不影响实验的严谨性。通过设置交换机中的端口镜像让出入连接二层交换机和三层交换机的trunk口的数据包复制一份发送至嗅探器的端口。由于在交换机会时不时发送STP（spanning tree protocol）协议来防止网络中出现冗余回路，避免广播风暴，以及发送RIP报文来进行路由信息的交换，所以为了能够找到我们所需要监听的ICMP以及FTP数据包，需要将上述的数据包过滤掉。

通过本实验体验了综合组网的全过程，深刻认识到搭建一个网络系统需要对软件和硬件都有一个很好的把握，一个网络系统由边缘设备（PC机）和交换设备（交换机、路由器）组成，首先需要用合适的连接线将这些设备连接起来，其次是对这些设备进行合理的配置。在完成这个实验之后，对于网络系统的组成有了一个更加深入的认识。