计算机网络实验报告

****

|  |  |
| --- | --- |
| 实验名称 | IP访问列表 |
| 组 号 | 第三组 |
| 小组成员 | 张翔 |
|  | 钱宝强 |
| 学院(系) | 计算机科学与技术学院 |
| 专 业 | 软件工程 |
| 任课老师 | 蒋海鹰 |
| 日 期 | 2025.5.6 |

**一、实验名称**

编号的标准IP访问列表。

**二、实验目的**

掌握路由器上编号的标准IP访问列表规则及配置。

**三、背景描述**

你是一个公司的网络管理员，公司的经理部、财务部门和销售部门分属不同的三个网段，三个部门之间用路由器进行信息传递，为了安全起见，公司领导要求销售部门不能对财务部门进行访问，但经理部可以对财务部门进行访问。

PC1代表经理部的主机，PC2代表销售部门的主机、PC3代表财务部门的主机。

**四、技术原理**

IP ACL（IP访问控制列表或IP访问列表）是实现对流经路由器或交换机的数据包根据一定的规则进行过滤，从而提高网络可管理性和安全性。

IP ACL分为两种：标准IP访问列表和拓展IP访问列表。

标准IP访问列表可以根据数据包的源IP地址定义谷子额，进行数据包的过滤。

扩展IP访问列表可以根据数据包的源IP、目的IP、源端口、目的端口、协议来定义规则。进行数据包的过滤。

IP ACL基于接口进行规则的应用，分为：入栈应用和出栈应用。

入栈应用是指由外部经该接口进行路由器的数据包进行过滤。

出栈应用是指路由器从该接口往外转发数据时进行数据包的过滤。

IP ACL的配置有两种方法：按照编号的访问列表，按照命名的访问列表。

标准IP访问列表编号范围时1~99、1300~1999，拓展IP访问列表编号范围是100 ~199、2000~2699。

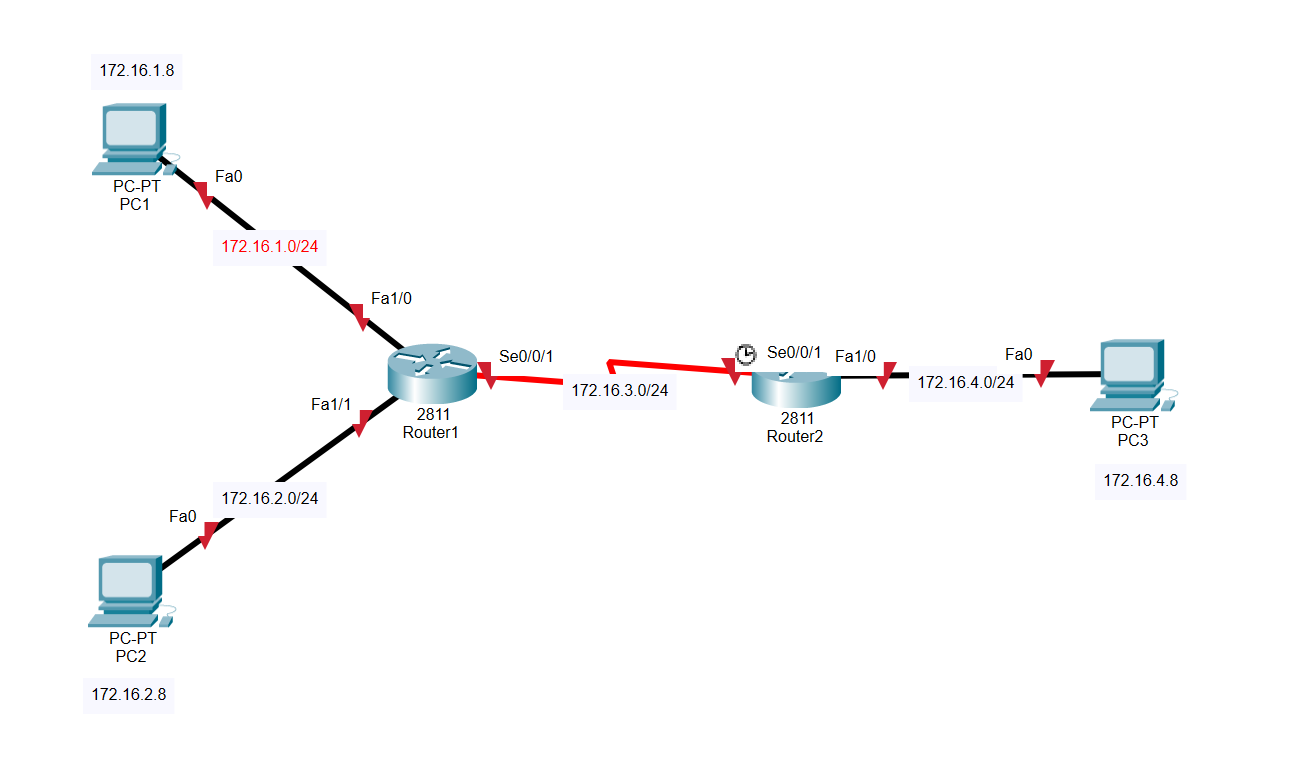
**五、实现功能**

实现网段间相互访问的安全控制。

**六、实验设备**

R1700路由器（两台）、V.35线缆（1条）、直连线或交叉线（3条）

**七、实验拓扑**



**八、实验步骤**

步骤1.基本配置

（1）Router1基本配置

R1700-1#configure terminal

R1700-1(config)#int fa 1/0

R1700-1(config-if)#ip add 172.16.1.1 255.255.255.0

R1700-1(config-if)#no sh

R1700-1(config-if)#exit

R1700-1(config)#int fa 1/1

R1700-1(config-if)#ip add 172.16.2.1 255.255.255.0

R1700-1(config-if)#no sh

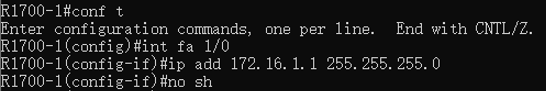
R1700-1(config-if)#exit

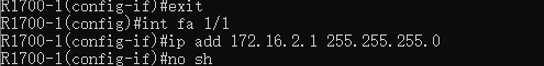
R1700-1(config)#int s 1/2

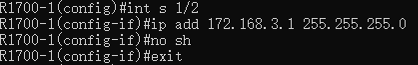
R1700-1(config-if)#ip add 172.16.3.1 255.255.255.0

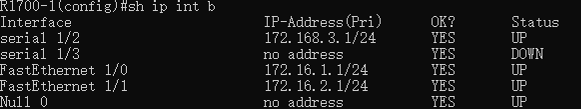
R1700-1(config-if)#no sh

R1700-1(config-if)#exit









（2）Router2基本配置

R1700-2#configure terminal

R1700-2(config)#int fa 1/0

R1700-2(config-if)#ip add 172.16.4.2 255.255.255.0

R1700-2(config-if)#no sh

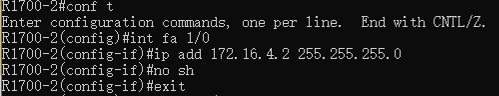
R1700-2(config-if)#exit

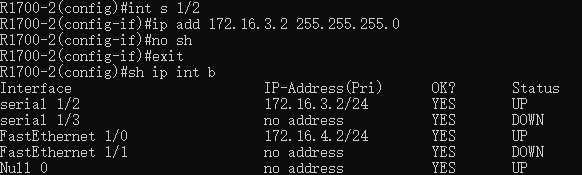
R1700-2(config)#int s 1/2

R1700-2(config-if)#ip add 172.16.3.2 255.255.255.0

R1700-2(config-if)#no sh

R1700-2(config-if)#exit





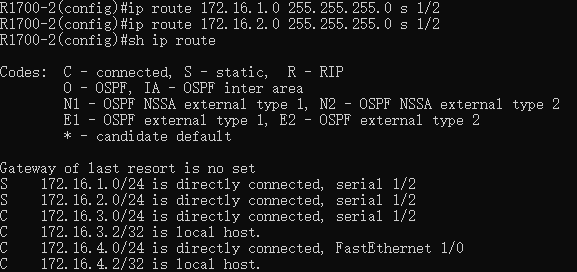
（3）配置静态路由

R1700-1(config)#ip route 172.16.4.0 255.255.255.0 s 1/2



R1700-2(config)#ip route 172.16.1.0 255.255.255.0 s 1/2

R1700-2(config)#ip route 172.16.2.0 255.255.255.0 s 1/2



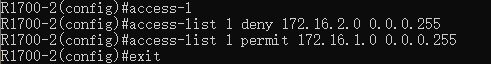
步骤2.配置标准IP访问控制列表

R1700-2(config)#access-list 1 deny 172.16.2.0 0.0.0.255

！拒绝来自172.16.2.0网段的流量通过

R1700-2(config)#access-list 1 permit 172.16.1.0 0.0.0.255

！允许来自172.16.1.0网段的流量通过





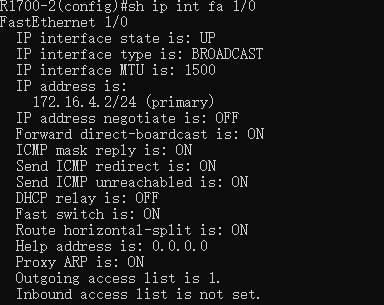
步骤3.把访问控制列表在接口下应用

R1700-2(config)#int fa 1/0

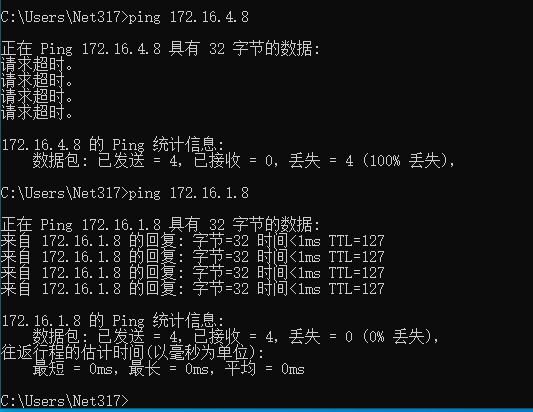
R1700-2(config-if)#int access-group 1 out

！在接口下访问控制列表出栈流量调用

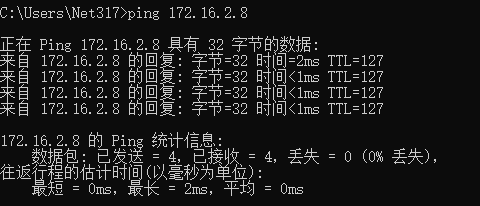




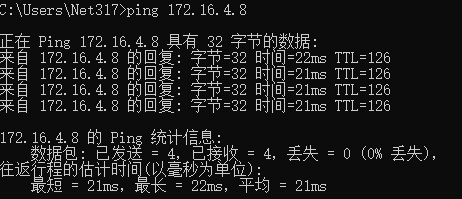
步骤4.验证测试



PC2 ping PC3(无法ping通)和PC2 ping PC1(可以ping通)测试结果



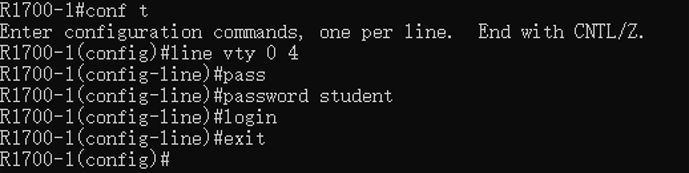
PC1 ping PC2测试结果(可以ping通)



PC1 ping PC3测试结果(可以ping通)

**九、软件抓包**

步骤1.路由器的虚拟终端配置



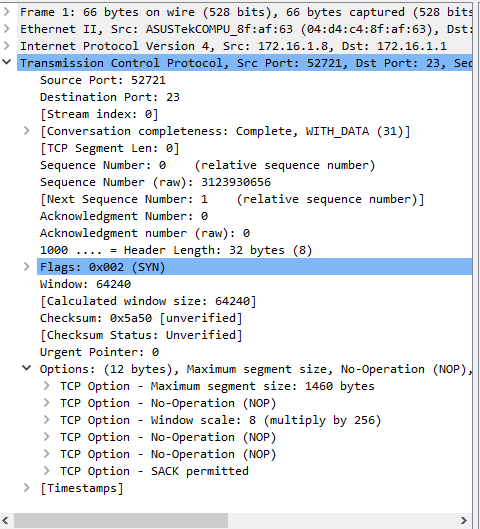
步骤2.启动wireshark，选择以太网2，设置过滤条件tcp，单击开始

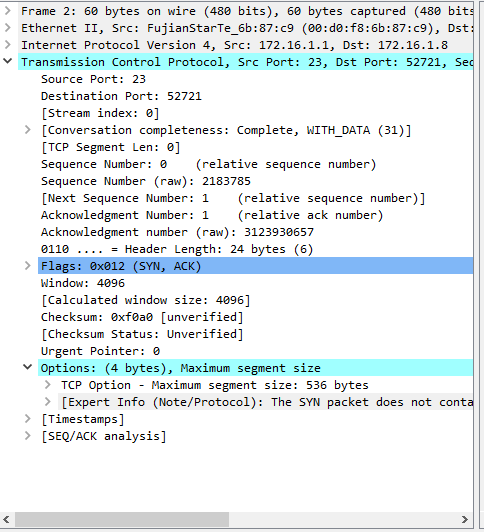
步骤3.在pc上使用telnet命令登陆路由器，输入口令，然后退出

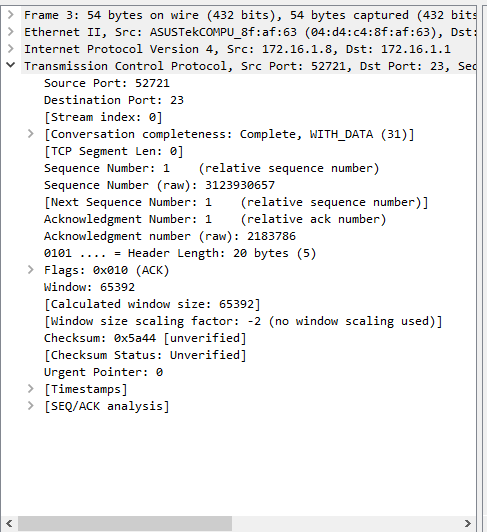


步骤4.在wireshark中单击停止按钮

步骤5.在wireshark中找到tcp建立连接的三个报文，然后进行解读并填写表格

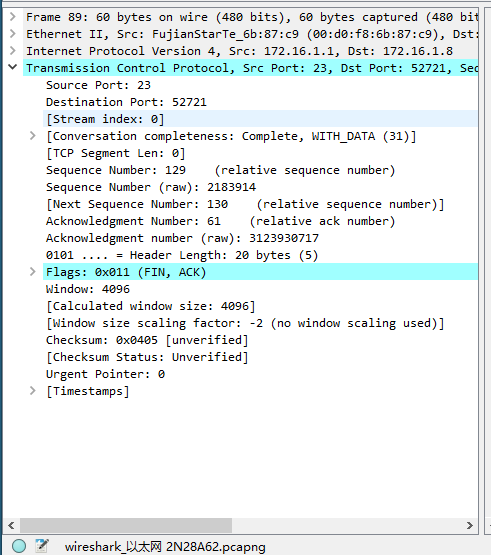


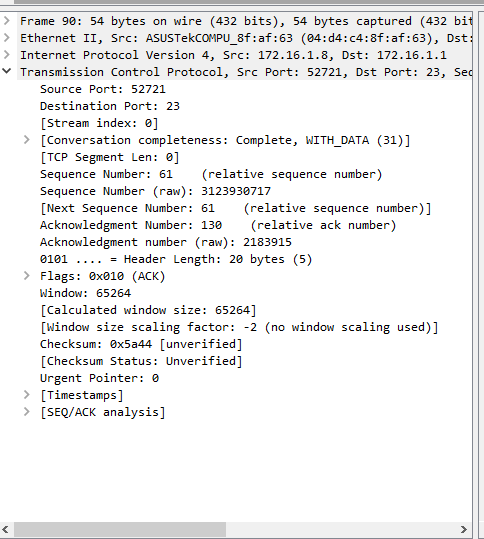


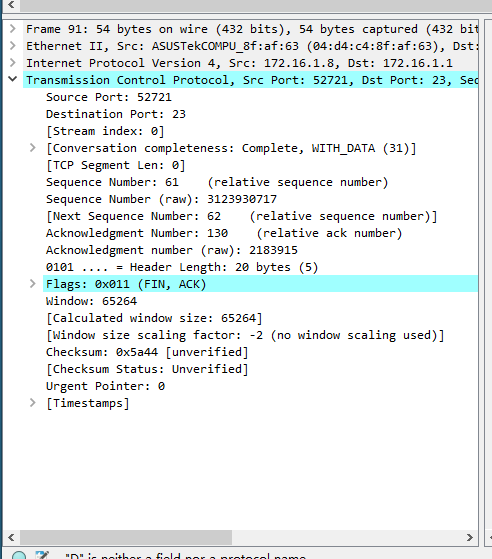


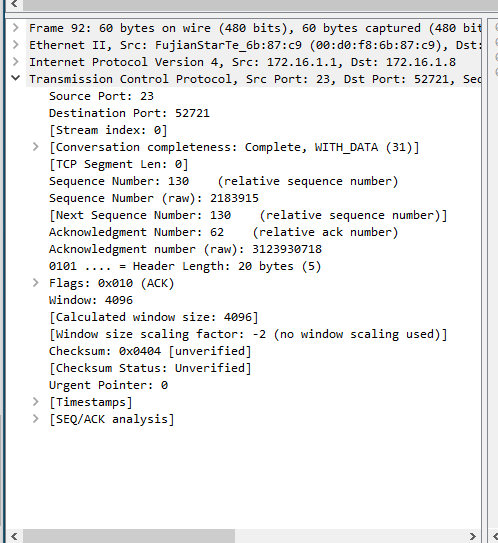
|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 连接建立的报文段 | 源端口 | 目 的端口 | 序号 | 确认号 | 头部 长度 | 数据 长度 | 标志位为1的 | 窗口 大小 | mss 选项 |
| 1 | 52721 | 23 | 0 | 0 | 32 | 0 | SYN | 64240 | 1460 |
| 2 | 23 | 52721 | 0 | 1 | 24 | 0 | SYN、ACK | 4096 | 536 |
| 3 | 52721 | 23 | 1 | 1 | 20 | 0 | ACK | 65392 | 无 |

步骤6.在wireshark中找到tcp释放连接的四个报文，然后进行解读并填写表格









|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 连接断开的报文段 | 源端口 | 目 的端口 | 序号 | 确认号 | 头部 长度 | 数据长度 | 标志位为1的 | 窗口大小 | mss选项 |
| 1 | 23 | 52721 | 129 | 61 | 20 | 0 | FIN、ACK | 4096 | 无 |
| 2 | 52721 | 23 | 61 | 130 | 20 | 0 | ACK | 65264 | 无 |
| 3 | 52721 | 23 | 61 | 130 | 20 | 0 | FIN、ACK | 65264 | 无 |
| 4 | 23 | 52721 | 130 | 62 | 20 | 0 | ACK | 4096 | 无 |

Tcp 建立连接和释放连接的数据包分析：

1. 建立连接的双方在窗口大小上可以不一样的，且在变化中。

2. Mss（最大报文段）只在建立连接的前二个报文中有且双方也可以不一样，表明通信双

方对数据段的大小要求不一样，也表明mss 在连接初期就协商好了，后面不再需要。

3. 每个TCP 段（数据包）都被赋予一个序列号，这样接收方就可以对接收到的数据进行排序，并检测重复或丢失的数据包。确认号则用于告知发送方哪些数据已经被成功接收。

它通常是期望收到的下一个数据包的序列号。

4. Tcp 报文段Len=0 只是表明没有数据只有首部，这也表明了只有首部的报文段也是可行的。