**西安电子科技大学**

**计算机与网络安全综合实验 课程实验报告**

**实验名称 配置ACL**

网络与信息安全 学院 2118021 班

成 绩

姓名 学号

同作者

实验日期 2024 年 05 月 22 日

|  |
| --- |
| 指导教师评语：  指导教师：  年 月 日 |
| **实验报告内容基本要求及参考格式**  一、实验目的  二、实验所用仪器（或实验环境）  三、实验基本原理及步骤（或方案设计及理论计算）  四、实验数据记录（或仿真及软件设计）  五、实验结果分析及回答问题（或测试环境及测试结果） |

**ACL基础**

## 一、实验目的

1. 配置H3C路由器基本ACL。

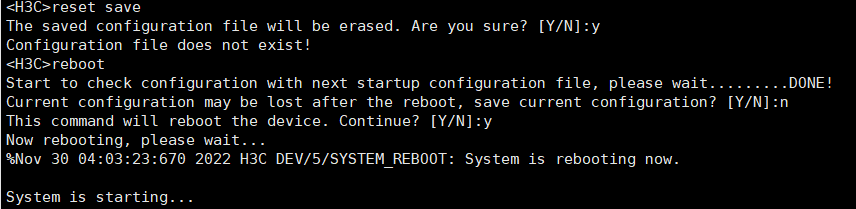
## 二、实验要求

1. 熟练掌握网络配置能力。

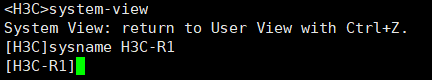
2. 熟练掌握ACL基本配置。

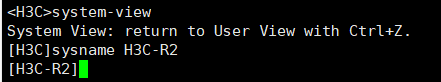
## 三、实验步骤

由于路由器已配置状态可能会对试验造成干扰，因此为消除这种干扰，在实验前对于两台使用的路由器均首先使用reset save清除原有配置，再使用reboot命令保存状态并进行重启。

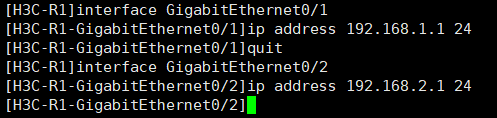


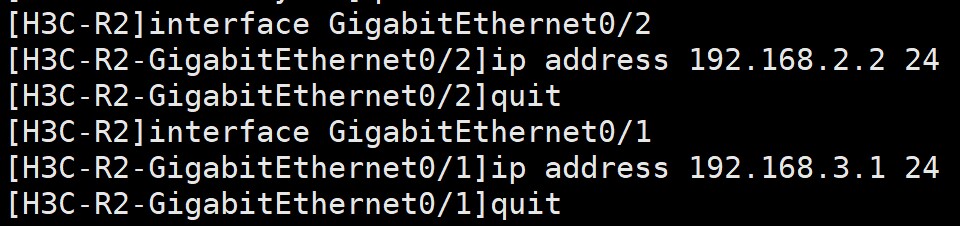
待路由器重启后，分别将其命名为H3C-R1与H3C-R2。命名时首先使用system-view进入系统视图，此后使用sysname H3C-R1与sysname H3C-R2分别命名两台路由器。



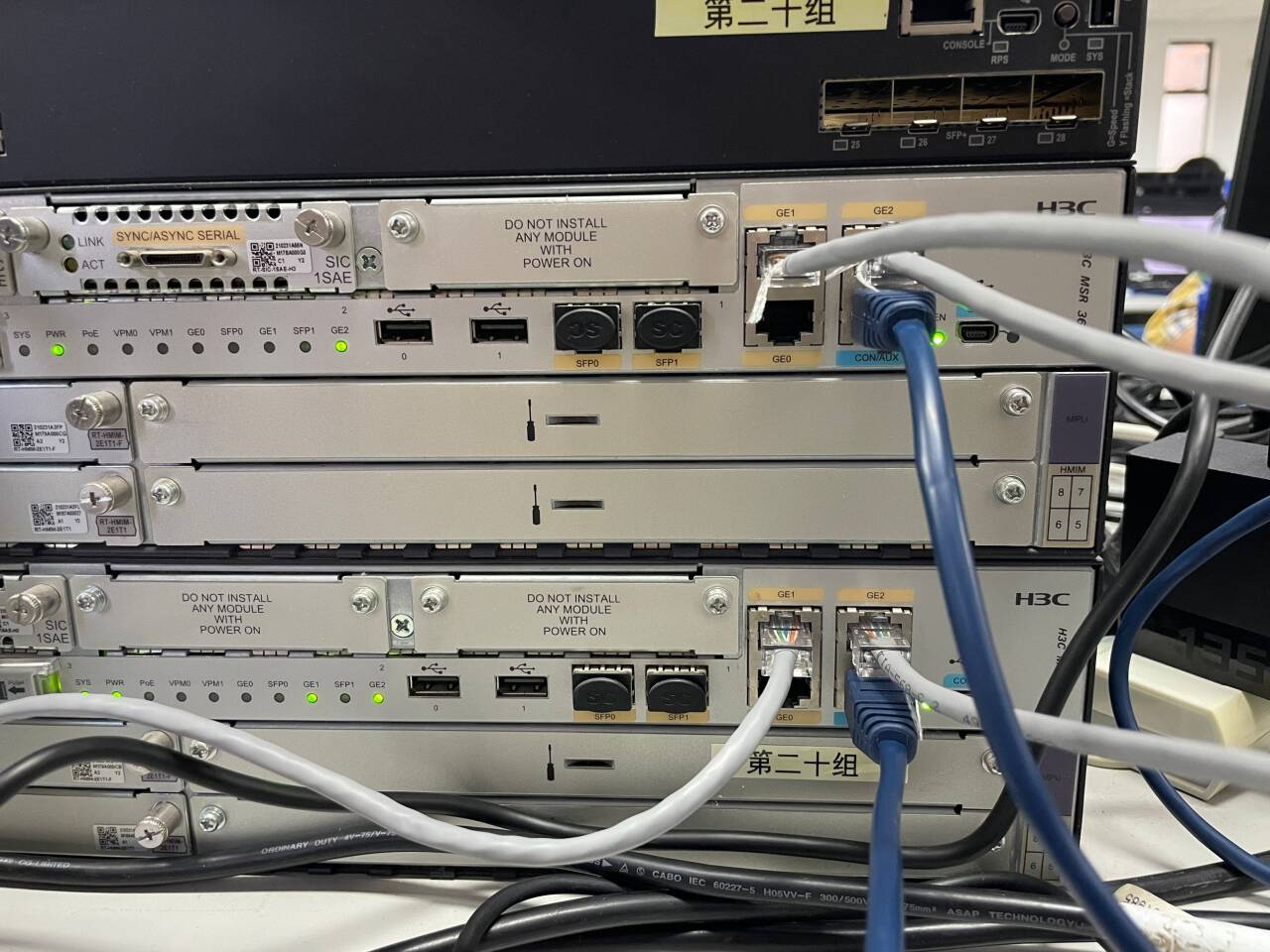


此后对两台路由器使用到的端口配置IP地址。首先对H3C-R1的GE0/1端口进行配置，使用interface GigabitEthernet0/1进入GE0/1端口视图，此后使用ip address 192.168.1.1 24配置其IP地址为192.168.1.1/24。此后对于H3C-R1的GE0/2端口与H3C-R2的GE0/1、GE0/2端口可按照相同的命令进行配置。





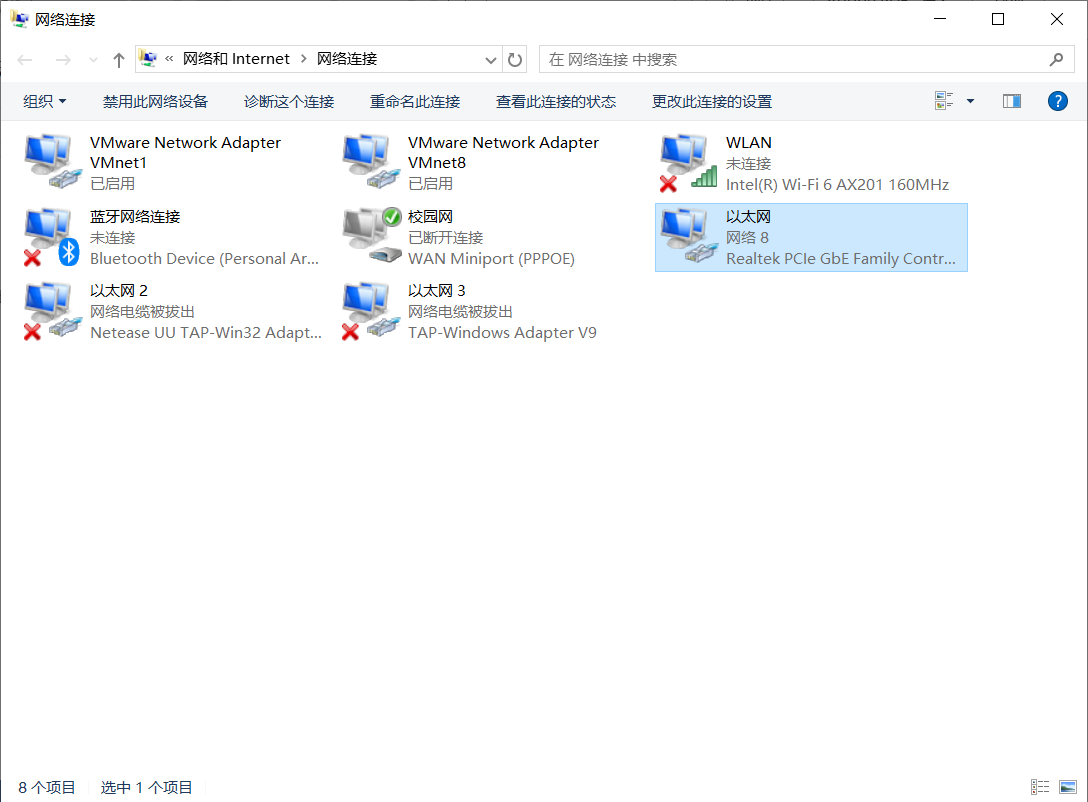
配置后PC1、PC2及两台路由器的连接如下：



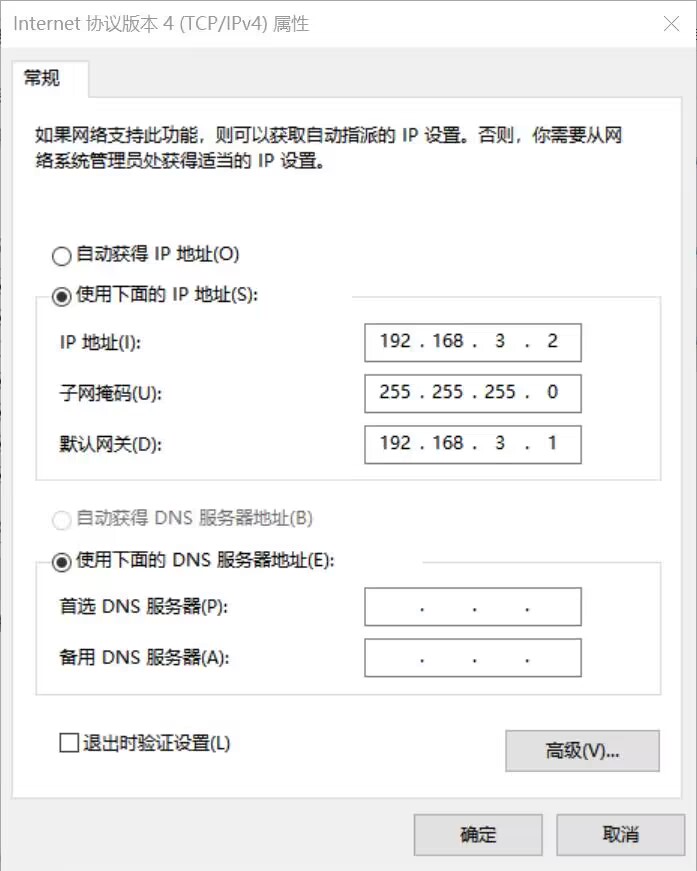
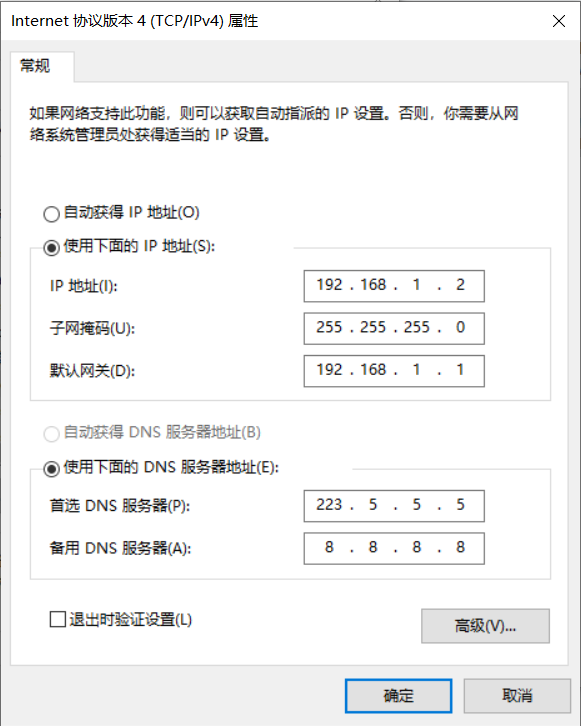
由于防火墙会对实验产生干扰，因此在控制面板中关闭PC1与PC2的防火墙。



此后在控制面板的网络连接中配置两台PC的IP地址与默认网关。在网络连接界面，选择以太网属性，配置IPv4协议IP地址。



由于两相连端口的网络地址必须相同，因此配置PC1的IP地址为192.168.1.2/24，其默认网关为与其相连的H3C-R1的GE0/1端口，即192.168.1.1。同理配置PC2的IP地址为192.168.3.2/24，其默认网关为与其相连的H3C-R2的GE0/1端口，即192.168.3.1。配置结果如下（左PC1，右PC2）：

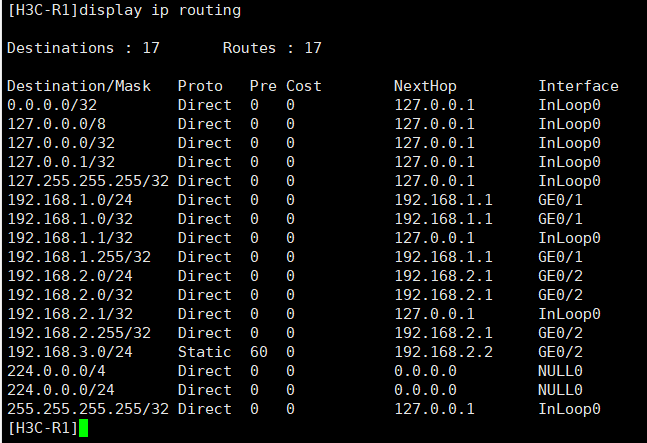


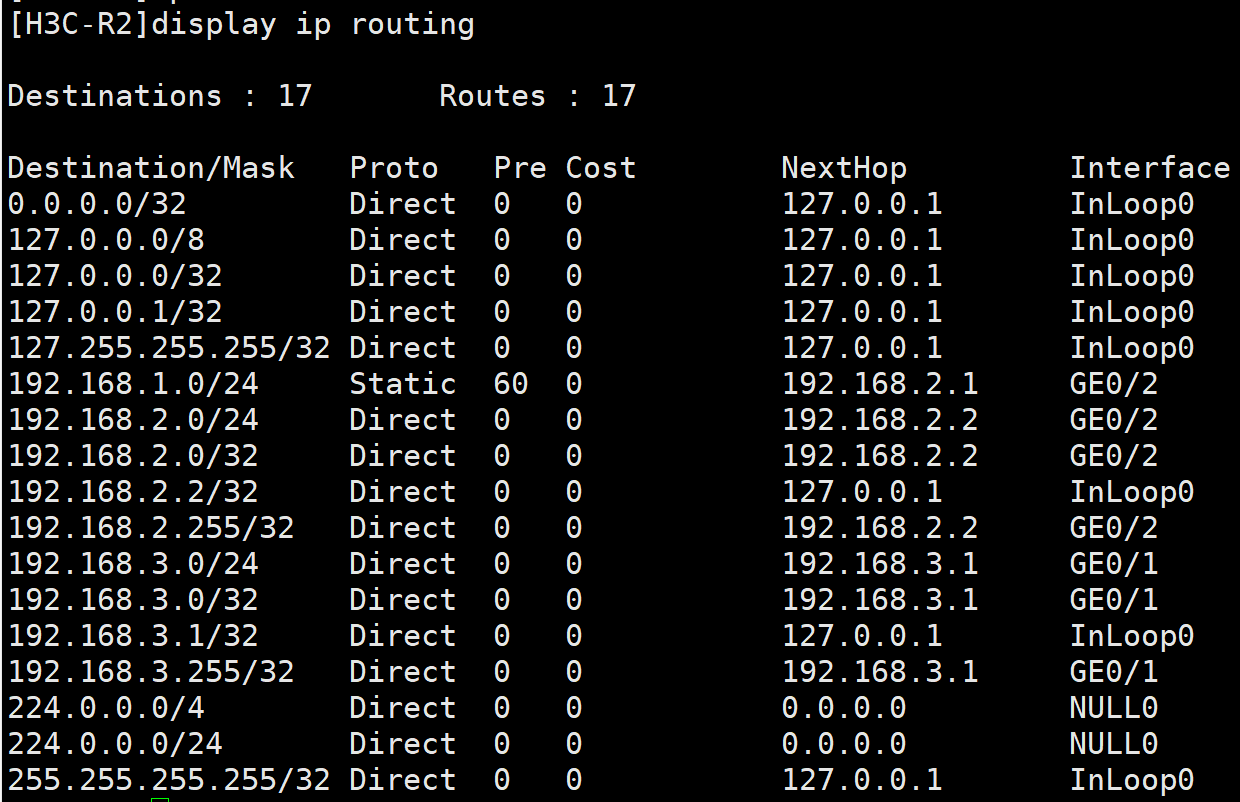
此后，在PC1上配置通往网络号为192.168.3.0/24的默认路由为192.168.2.2/24，在PC2上配置通往网络号为192.168.1.0/24的默认路由为192.168.2.1/24



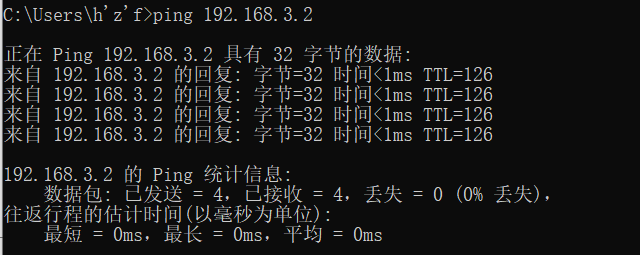


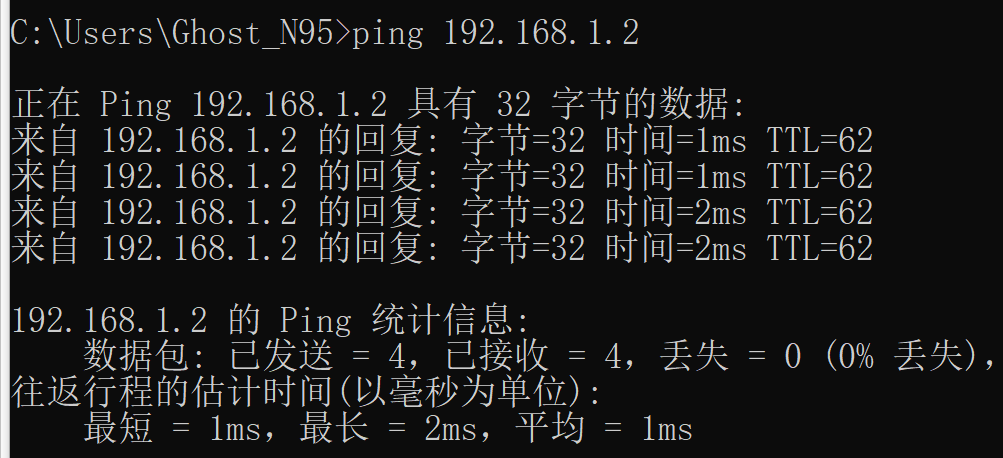
配置后使用ip routing查看其路由表，均可看到配置的默认路由：





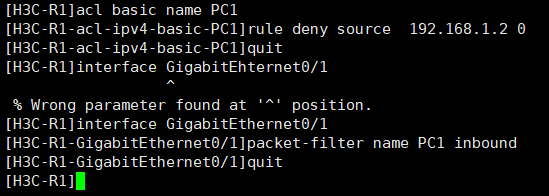
此时分别在PC1与PC2的控制台上使用ping命令测试二者之间的连通性，上图为PC1，下图为PC2.



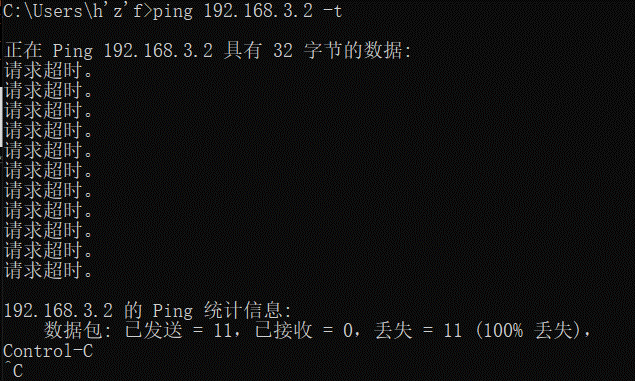


由结果可知，此时二者之间相互连通。

此后在H3C-R1上配置ACL对来自IP地址为192.168.1.2的数据包进行过滤。首先通过acl basic name PC1创建名称为PC1的ACL并进入ACL视图，使用rule deny source 192.168.1.2 0配置ACL对来自IP地址为192.168.1.2的数据包进行过滤，此后使用quit退出ACL视图，进入GE0/1视图后，使用packet-filter name PC1 inbound将PC1这一ACL应用至H3C-R1的GE0/1端口。



此时可以看到，当应用ACL后，原本连通的连接断开。



四、实验结果及分析

1. 实验过程中遇到什么问题，如何解决的？通过该实验有何收获？

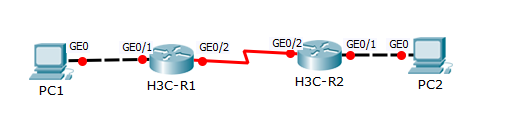
实验时，遇到PC2可以ping通PC1，而PC1不能ping通PC2的情况，在排查后发现PC2存在第三方防护软件对流量进行了过滤，使得PC1不能与PC2连通，而PC2可以与PC1连通。

通过本次实验的操作，我进一步熟悉了对H3C交换机的操作命令，并通过实验前后现象的对比，对ACL这一对数据包进行过滤的功能有了清晰的认识，熟悉了ACL技术的应用方法，进一步理解了通过ACL技术实现安全控制的原理与场景。

2. 请按照PPT中第10页表格的格式，给出你实际实验时所使用的数据。

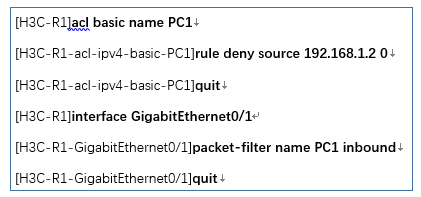
|  |  |  |
| --- | --- | --- |
| 设备名称 | 接口名称 | IP地址 |
| H3C-R1 | GE0/1 | 192.168.1.1/24 |
| H3C-R1 | GE0/2 | 192.168.2.1/24 |
| H3C-R2 | GE0/1 | 192.168.3.1/24 |
| H3C-R2 | GE0/2 | 192.168.2.2/24 |
| PC1 | GE0 | 192.168.1.2/24 |
| PC2 | GE0 | 192.168.3.2/24 |

3. 请使用Packet Tracer绘制本实验拓扑图，并且说明，如果PC1的IP地址改为192.168.5.2，H3C-R1的哪个端口要做相应修改，应该改成什么？这时候PC1的默认网关要改成什么？



由于相连端口的网络地址应相同，且PC1与H3C-R1的E0/1端口相连，因此PC1的IP地址改变后，H3C-R1的E0/1端口的IP地址需要做出相应修改，应改为192.168.5.1，PC1的默认网关应改为192.168.5.1。

4. 请使用自己的语言对以下实验核心代码做以简单解释



第1行acl basic name PC1表示创建名为PC1的基本ACL，之后进入ACL视图。

第2行rule deny source 192.168.1.2 0表示配置PC1的ACL规则：拒绝IP地址为192.168.1.2的数据包通过。

第3行quit退出ACL视图。

第4行interface GigabitEthernet0/1表示进入GE0/1端口视图。

第5行packe-filter name PC1 inbound表示将PC1这一ACL应用在GE0/1端口的入方向，从而实现对数据包的过滤。

第6行quit表示退出GE0/1端口视图。

# 配置高级ACL实现包过滤

## 一、实验目的

1. 配置H3C路由器高级ACL及实现包过滤防火墙配置；

2. 熟悉ACL查看、监测和调试的相关命令；

## 二、实验要求

1. 2台具有4个以太网接口的路由器；

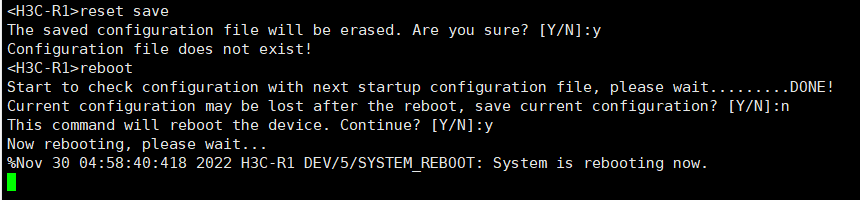
2. 3台装有Windows系列操作系统的PC（台式机或笔记本）；

3. 4条双绞跳线（交叉线）；

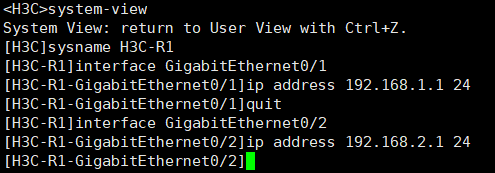
## 三、实验步骤

1. 配置高级ACL实现包过滤

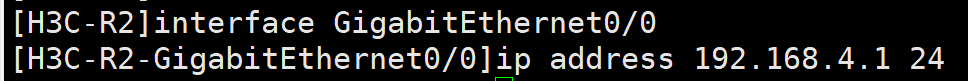
由于两个实验连续进行，因此需要首先清除上一步的配置，此处和实验一一样首先将R1的配置清空并重启，R2不需要，因为上一步并没有针对R2设置包拦截。

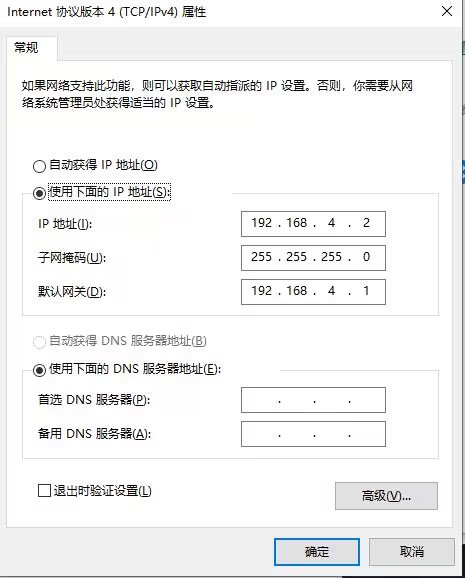


之后重新配置R1的ip地址

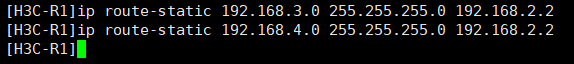


然后将R2新增连接设备PC3的E0/0端口进行配置，并设置PC3的ip地址和网关。

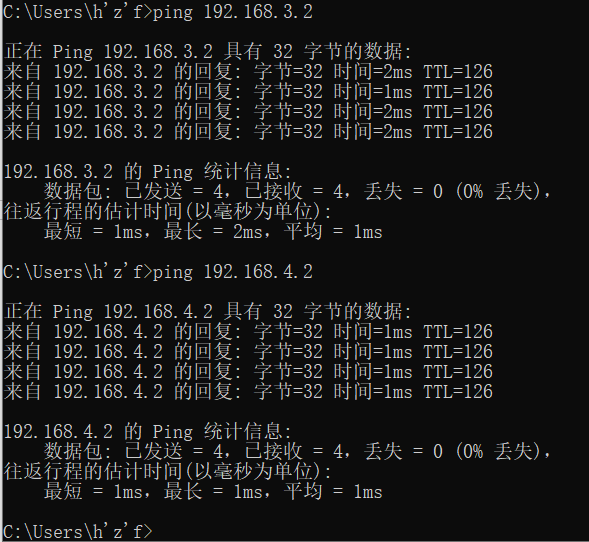




之后还需要设置静态路由，因为实验需要在设置高级ACL后验证PC1不可ping通PC2但可ping通PC3，如果不设置静态路由，则PC1也不能ping通PC3，无法达到实验目的。

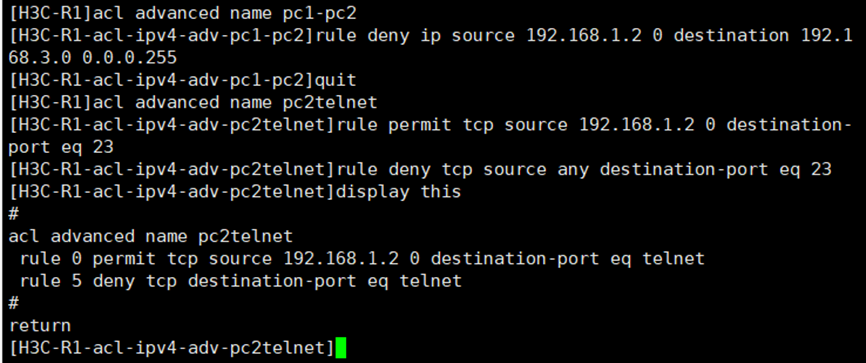


在此时首先测试一下PC1与PC2和PC3的联通性，可以看到PC1与PC2和PC3均联通。

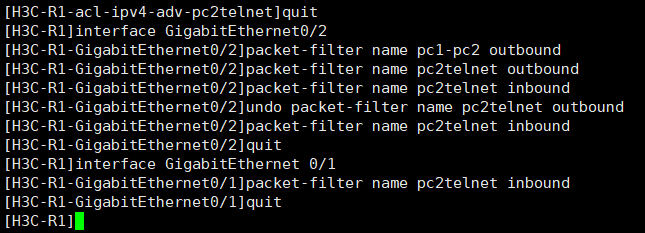


之后添加ACL规则。首先创建pc1-pc2，拒绝从源IP 192.168.1.2到目的地址范围192.168.3.0——192.168.3.255范围内的IP流量。这对应着PC1无法发送IMCP报文到PC2，即无法ping通。

之后创建pc2telnet的ACL。首先添加允许源IP地址192.168.1.2到目的端口23（telnet端口）的TCP流量，并追加拒绝任何源地址到目的端口23的TCP流量规则。这对应着只有PC1可以与R1建立链接。

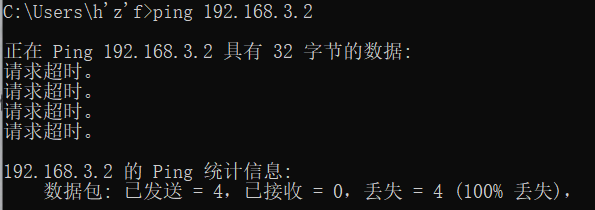


之后将ACL pc1-pc2应用到E0/2端口的出站流量，将ACL pc2telnet应用到E0/1和E0/2的入站流量。



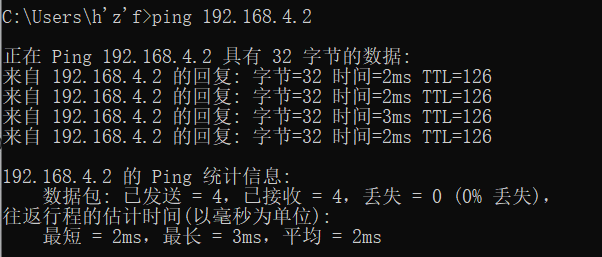
2. 从PC1上，使用ping命令访问PC2的IP地址192.168.3.2，测试连通性

可以看到，由于ACL pc1-pc2的使用，原本可以ping通的PC1和PC2之间现在无法ping通，ICMP报文被防火墙阻拦。



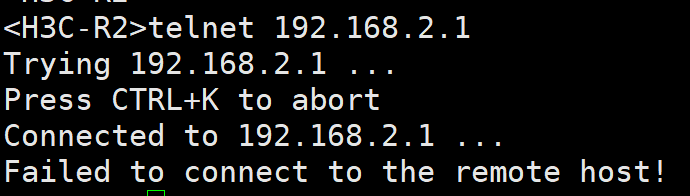
3. 从PC1上，使用ping命令访问PC3的IP地址192.168.4.2，测试连通性

可以看到，PC1和PC3之间由于没有ACL的阻碍，且正确配置了端口IP和路由，它们仍然可以ping通。

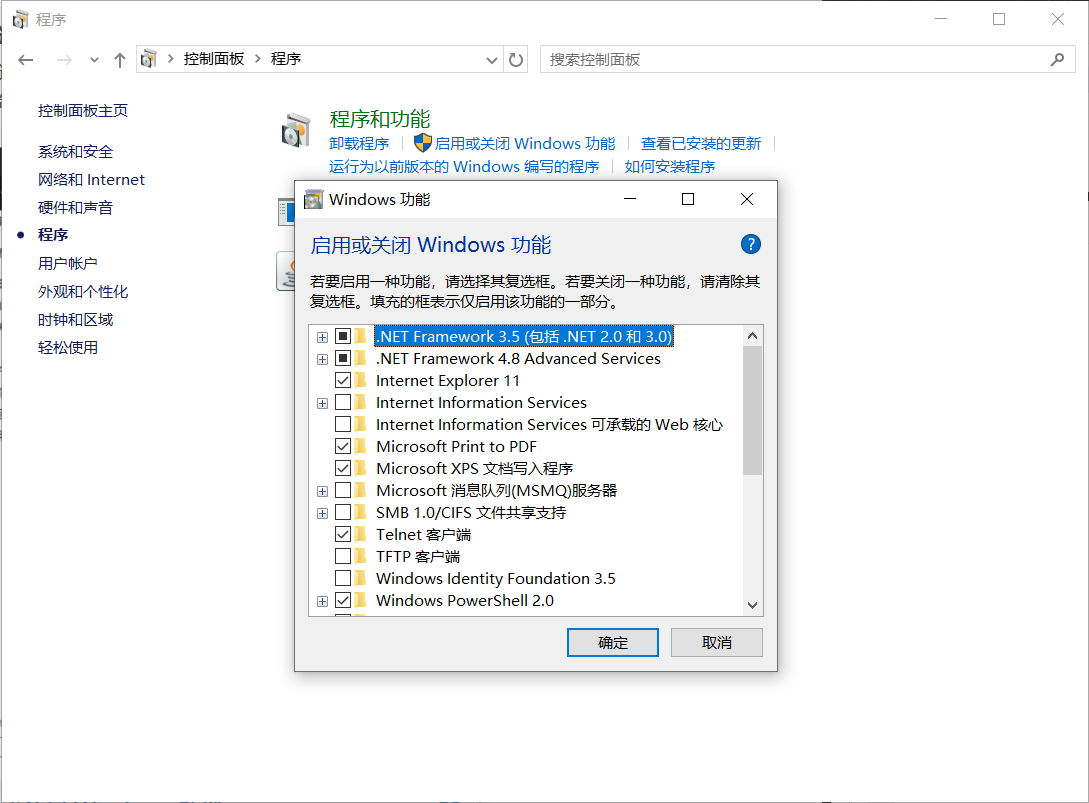


4. 在H3C-R2上测试使用telnet访问H3C-R1

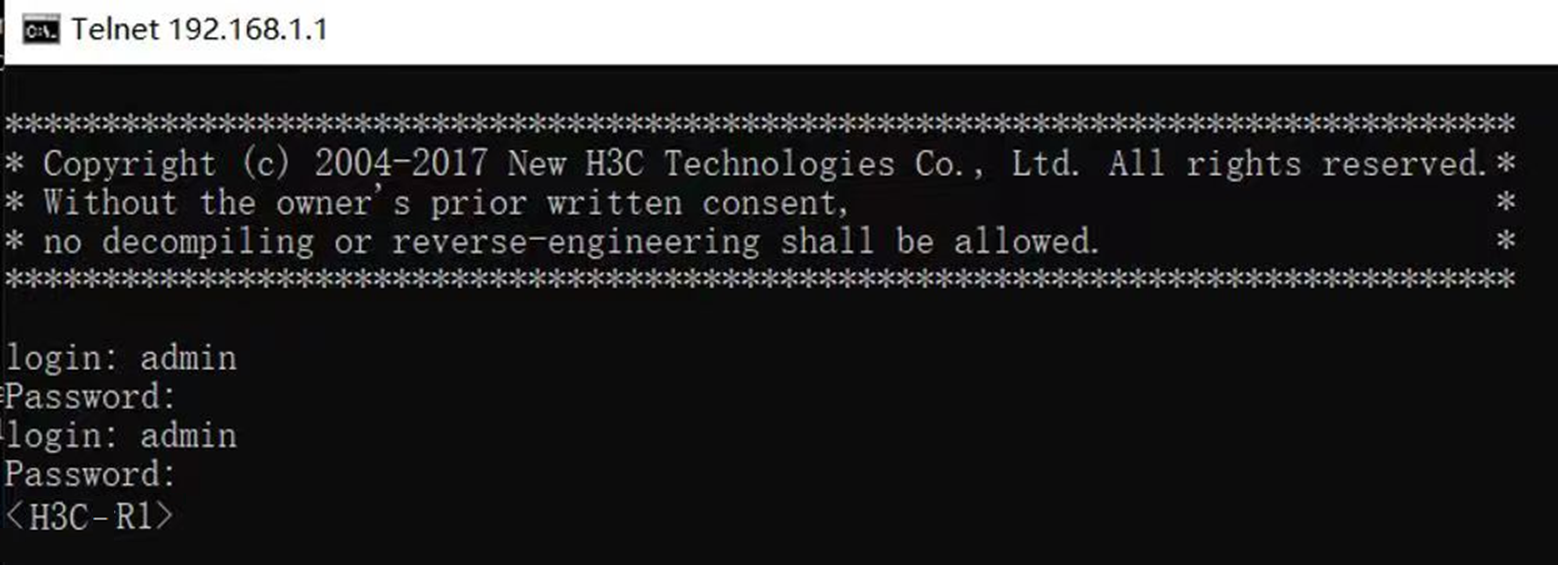
最后测试R2使用telnet访问R1，此处由于ACL pc2telnet在E0/1和E0/2端口控制入站流量，且R2与R1相连的E0/2端口的ip为192.168.2.2，并非可以通过的PC1 ip 192.168.1.2，因此telnet被拦截。



之后测试PC1是否可以使用telnet访问R1。在PC1中，首先需要安装telnet程序。



之后在cmd中使用telnet 192.168.1.1访问R1，可以发现连接成功。



五、实验结果及分析

1. 整个实验过程中遇到什么问题（有截图最好），如何解决的？通过该实验有何收获？

在做完上一个实验时，并没有清空R1的ACL规则，导致保留了上一个实验的ACL，使得在刚开始测试连通性时，PC1与PC2就不相通。最后通过删除原有配置解决了这一问题。

通过本次实验的操作，我进一步熟悉了对H3C交换机的操作命令，并通过实验前后现象的对比，对高级ACL实现包过滤的功能有了清晰的认识，更加熟悉了ACL技术的应用方法，进一步理解了通过ACL技术实现安全控制的原理与场景。