**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 盖乐 学号 21009200991

同作者

实验日期 2024 年 4 月 20 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。

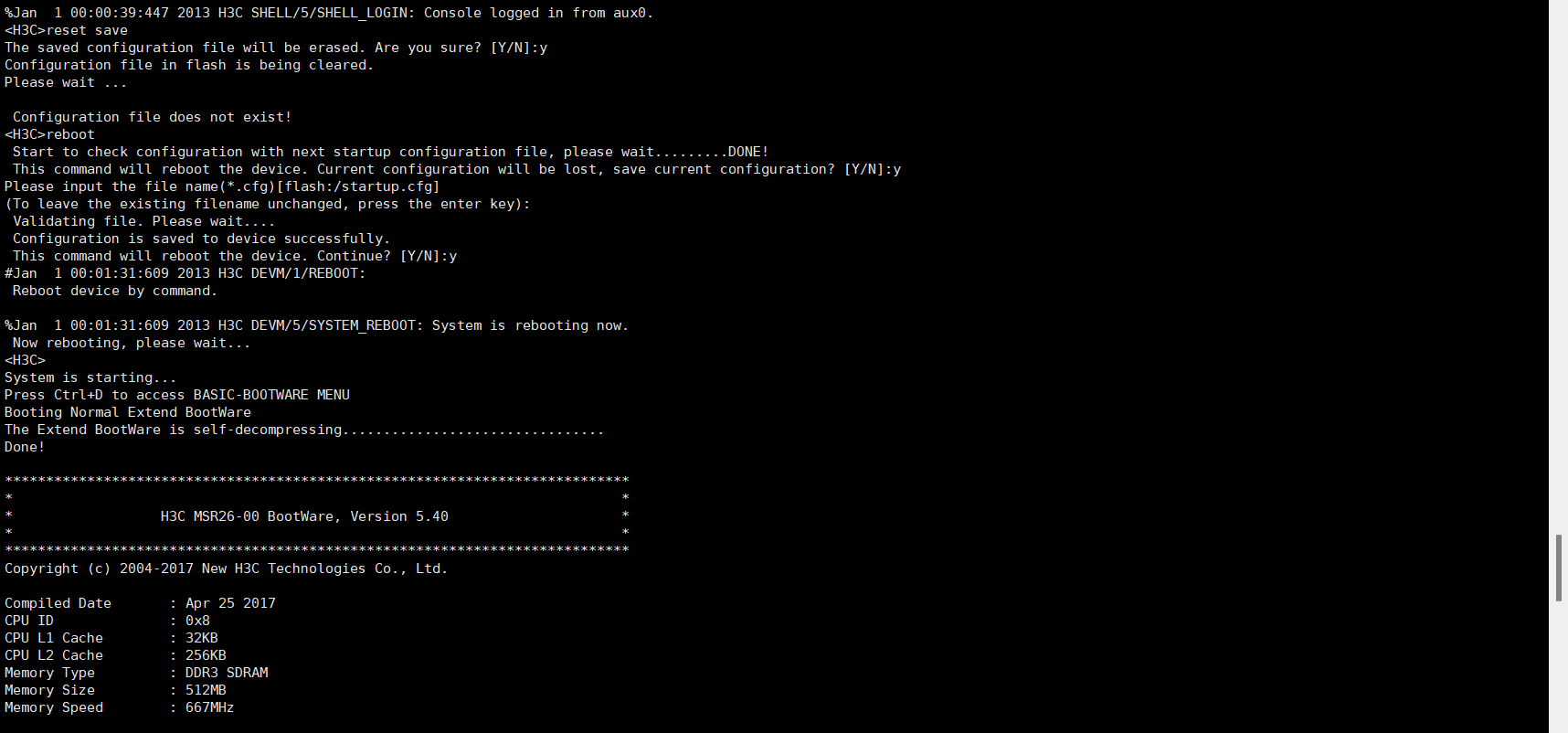
## 二、实验要求

1. 熟练掌握网络配置能力。

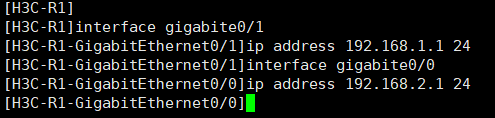
2. 熟练掌握ACL基本配置。

## 三、实验步骤

1. 连接路由器，将路由器配置清空：



1. 命名路由器，并配置路由器相关参数：

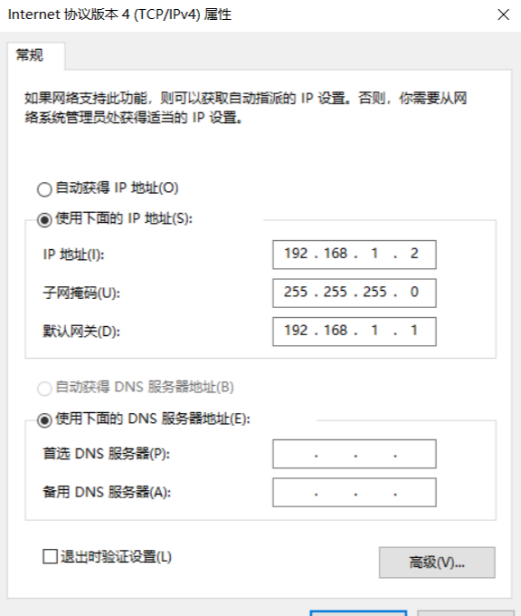




按照PPT中给的配置数据依次对Router1和2的端口地址进行设置

|  |  |  |
| --- | --- | --- |
| 设备名称 | 端口名 | 地址 |
| R1 | E0/0 | 192.168.2.1/24 |
| R1 | E0/1 | 192.168.1.1/24 |
| R2 | E0/0 | 192.168.2.2/24 |
| R2 | E0/1 | 192.168.3.1/24 |

1. 更改PC1和PC2的IP地址和默认网关（同时关闭无线网、防火墙等干扰项）

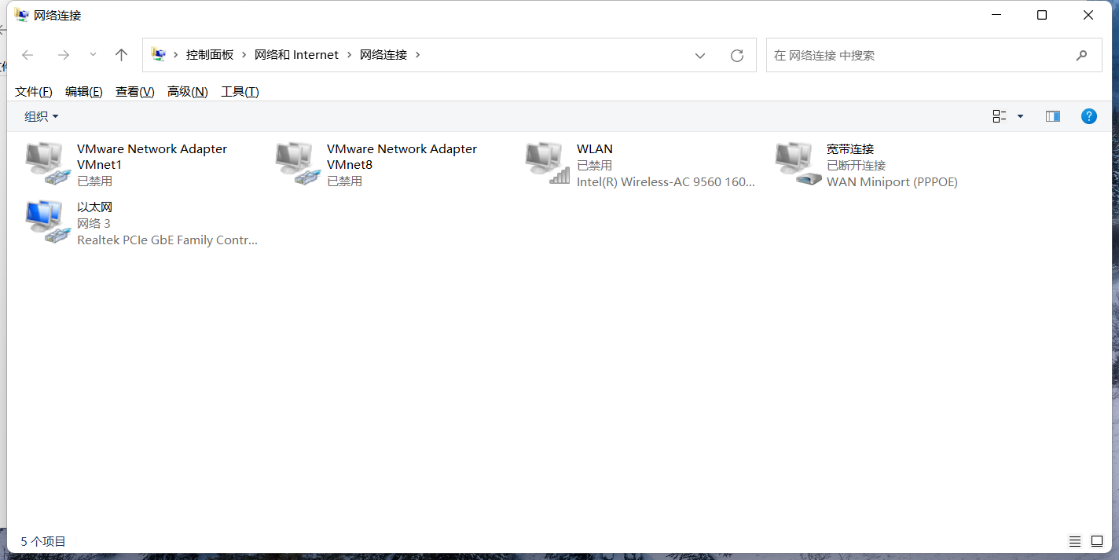


根据下面的表格信息进行更改：

|  |  |  |
| --- | --- | --- |
| 设备名称 | 端口号 | 地址 |
| PC1 | GE0 | 192.168.1.2/24 |
| PC2 | GE0 | 192.168.3.2/24 |

其中默认网关为PC机所连接的路由器端口地址。

关闭干扰项：



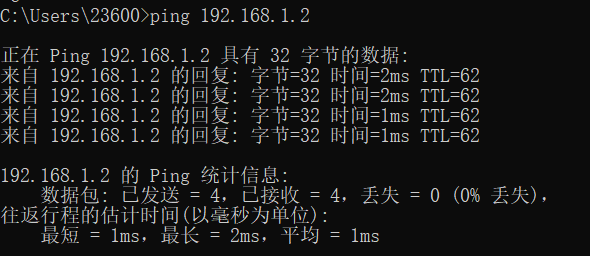


1. 在R1上设置静态路由：

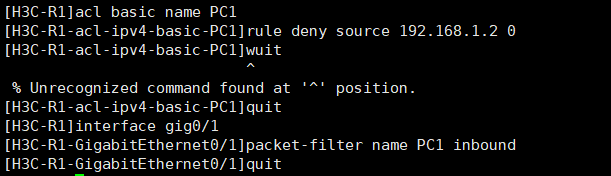


其中：192.168.3.0指向R2的E0/1端口地址所在网关，192.168.2.2为默认网关指向下一跳地址（R2的E0/0端口）

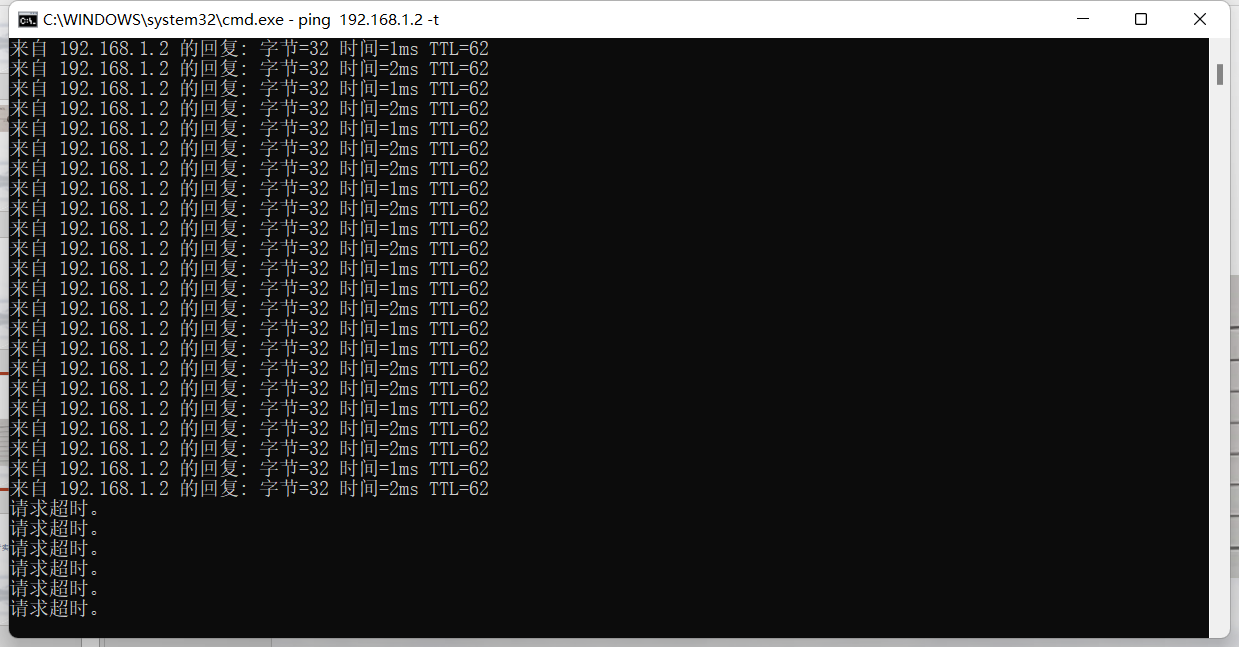
1. 测试连通性：



1. 在R1上设置ACL：



这时保持PC2一直在ping PC1,发现ACL生效后PC2和PC1无法再联通：



四、实验结果及分析

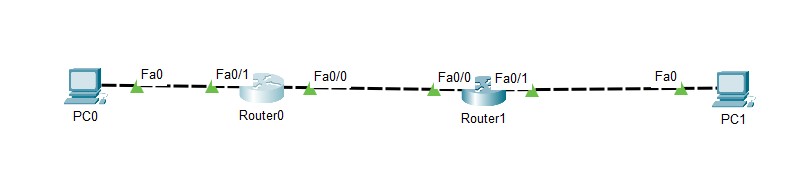
1. 实验过程中遇到什么问题，如何解决的？通过该实验有何收获？

通过该实验我认识到了ACL这一全新的概念，并学会如何利用它进行路由控制和报文过滤。

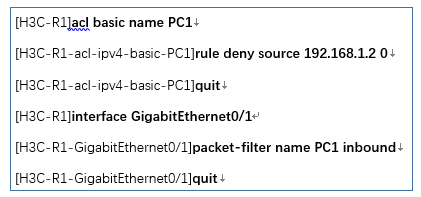
1. 请按照PPT中第10页表格的格式，给出你实际实验时所使用的数据。

|  |  |  |
| --- | --- | --- |
| 设备名称 | 端口名 | 地址 |
| R1 | E0/0 | 192.168.2.1/24 |
| R1 | E0/1 | 192.168.1.1/24 |
| R2 | E0/0 | 192.168.2.2/24 |
| R2 | E0/1 | 192.168.3.1/24 |
| 设备名称 | 端口号 | 地址 |
| PC1 | GE0 | 192.168.1.2/24 |
| PC2 | GE0 | 192.168.3.2/24 |

1. 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？



4. 请使用自己的语言对以下实验核心代码做以简单解释



acl basic name PC1：开启acl功能，命名为PC1；

rule deny source 192.168.1.2 0：拒绝一切源地址为192.168.1.2的数据包通过R1;

packet-filter name PC1 inbound：过滤掉名为PC1设备发送的数据包。

# 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

1.1．配置PC的IP地址

按照下表配置PC1、PC2、PC3的IP地址，子网掩码和默认网关。

|  |  |  |  |
| --- | --- | --- | --- |
| **设备名称** | **IP地址** | **子网掩码** | **默认网关** |
| **PC1** | 192.168.1.2 | 255.255.255.0 | 192.168.1.1 |
| **PC2** | 192.168.3.2 | 255.255.255.0 | 192.168.3.1 |
| **PC3** | 192.168.4.2 | 255.255.255.0 | 192.168.4.1 |

配置PC1的IP地址，子网掩码和默认网关如图 1所示：

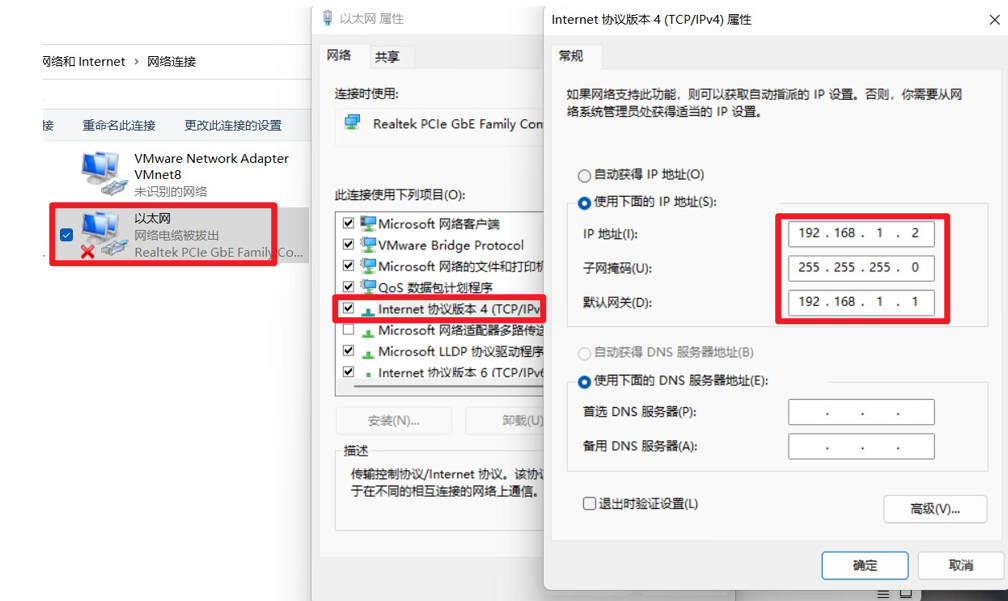


图 1 配置PC1的IP地址，子网掩码和默认网关

配置PC2的IP地址，子网掩码和默认网关如图 2所示：

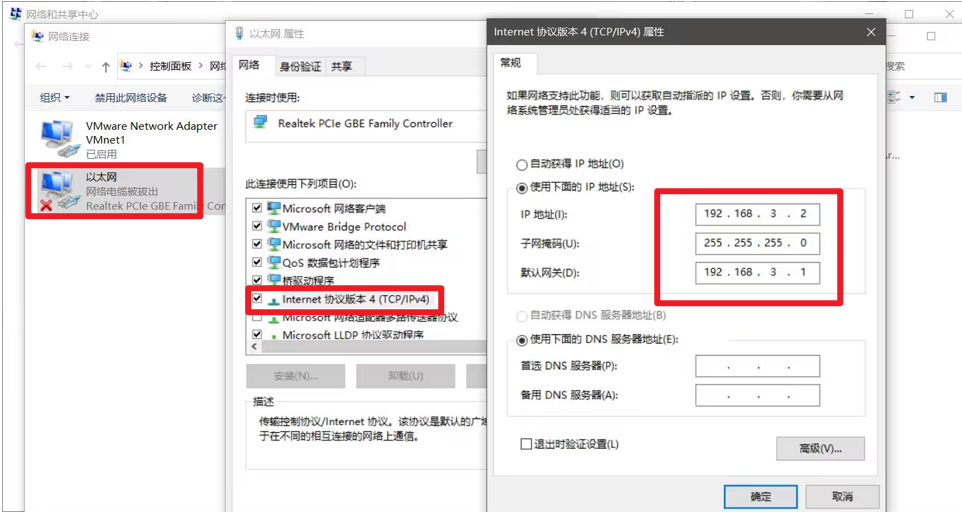


图 2 配置PC2的IP地址，子网掩码和默认网关

配置PC3的IP地址，子网掩码和默认网关如图 3所示：

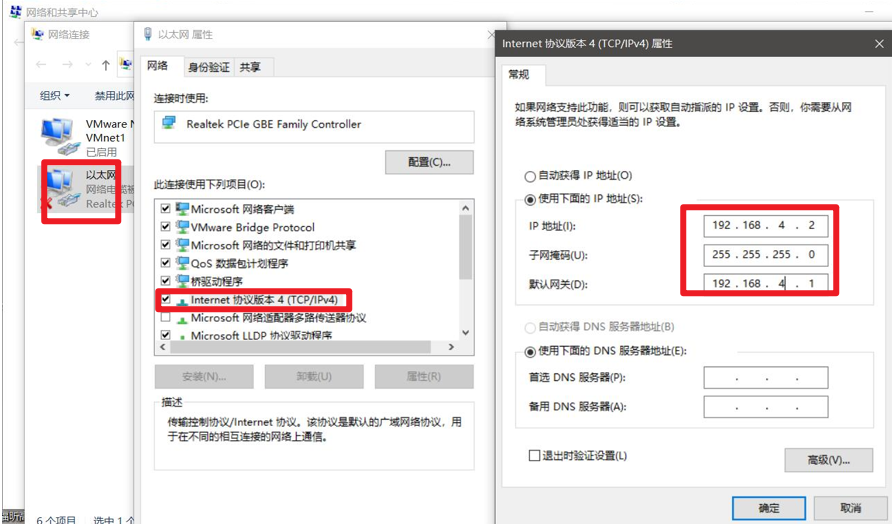


图 3 配置PC3的IP地址，子网掩码和默认网关

1.2．配置路由器的接口

按照下表配置路由器的接口。

|  |  |  |
| --- | --- | --- |
| **设备名称** | **接口名称** | **IP地址** |
| **H3C-R1** | E0/0 | 192.168.2.1/24 |
| **H3C-R1** | E0/1 | 192.168.1.1/24 |
| **H3C-R2** | E0/0 | 192.168.2.2/24 |
| **H3C-R2** | E0/1 | 192.168.3.1/24 |
| **H3C-R2** | E0/2 | 192.168.4.1/24 |

配置H3C-R1的接口如图 4所示：

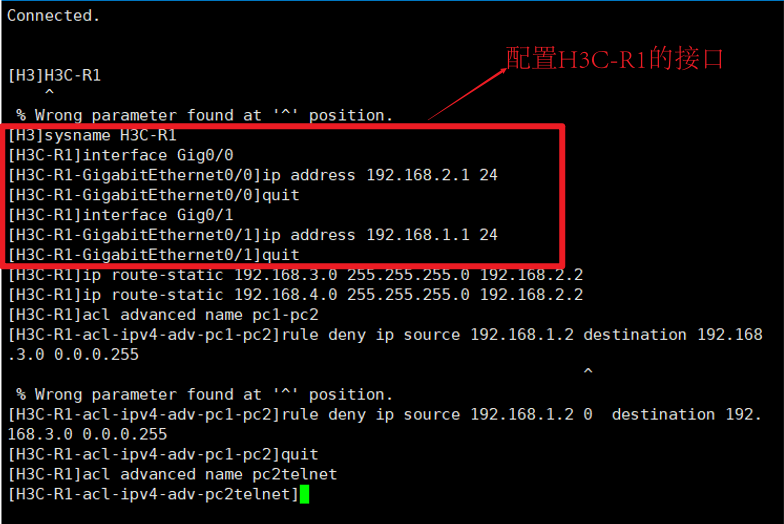


图 4 配置H3C-R1的接口

配置H3C-R2的接口如图 5所示：

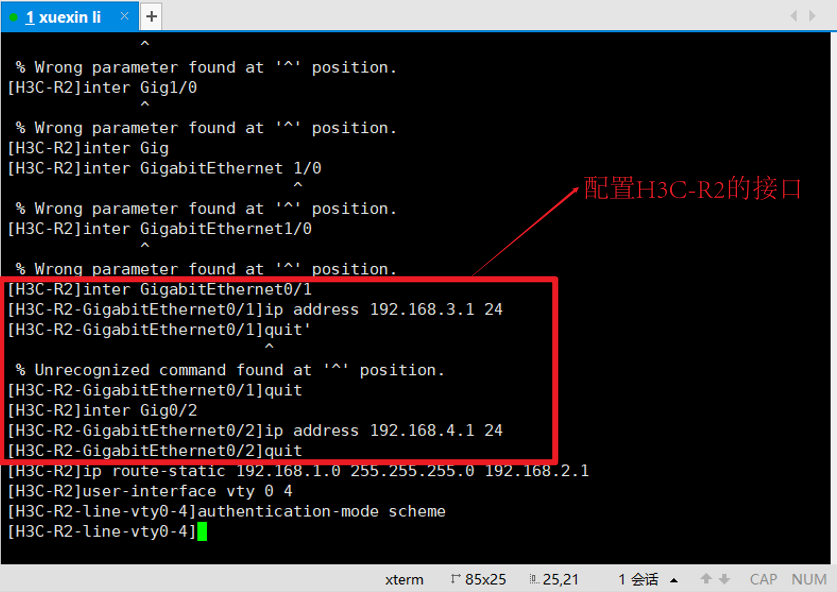


图 5 配置H3C-R2的接口

1.3．配置高级ACL实现包过滤

（1）配置H3C-R1,如图 6所示：

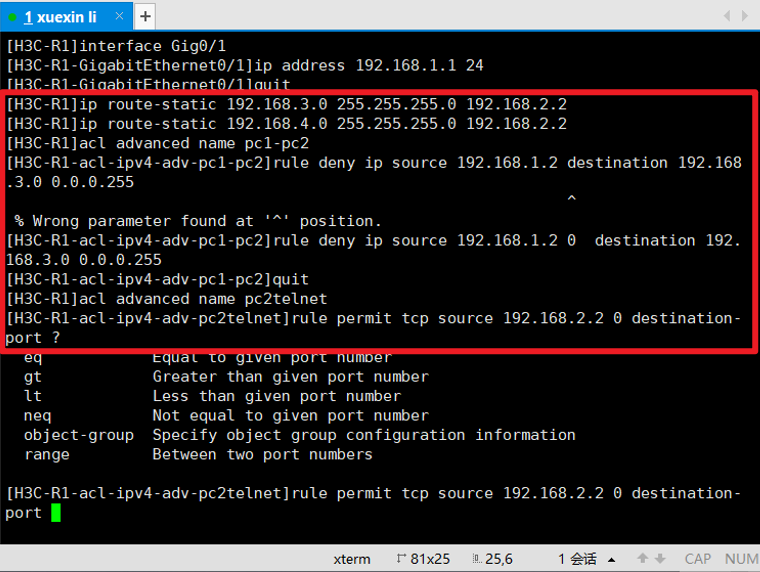
1）输入 ip route-static 192.168.3.0 255.255.255.0 192.168.2.2和ip route-static 192.168.4.0 255.255.255.0 192.168.2.2来配置静态路由。

2）输入acl advanced name pc1-pc2, 该命令的含义是创建一个名为 “pc1-pc2”的高级ACL，用于定义和控制从主机pc1到主机pc2之间的网络流量。通过配置ACL规则，可以指定允许或阻止特定类型的流量通过这两个主机之间的网络连接。

3)输入rule deny ip source 192.168.1.2 0 destination 192.168.3.0 0.0.0.255, 该命令的含义是创建一个规则，该规则拒绝源IP地址为 192.168.1.2，目标IP地址为 192.168.3.0/24（即掩码为 255.0.0.0）的IP流量通过。这样配置的规则可以帮助实现对指定源和目标地址之间的特定流量进行控制和阻止。

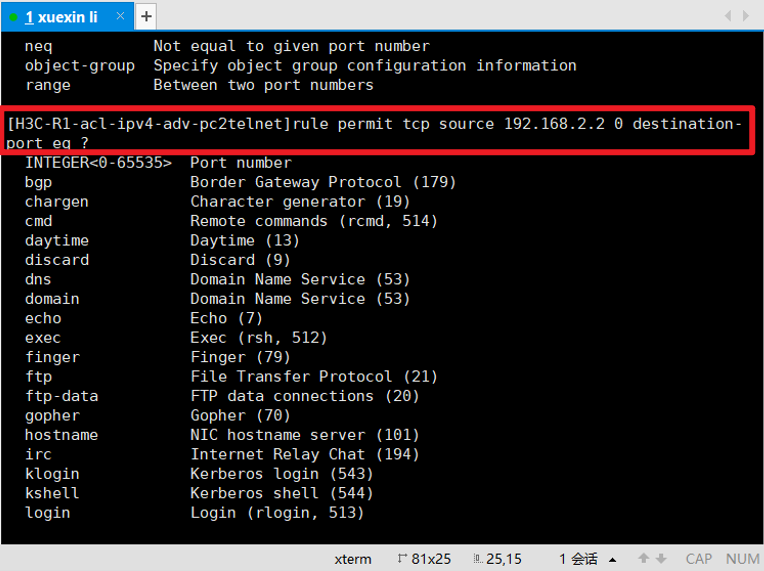
4）输入acl advanced name pc2telnet, 因此，该命令的含义是创建一个名为 “pc2telnet”的高级ACL，用于定义和控制与主机pc2之间的Telnet流量。通过配置ACL规则，可以指定允许或阻止Telnet协议流量通过与pc2的网络连接。这样可以帮助实现对Telnet流量的控制和限制。

5)输入rule permit tcp source 192.168.2.2 0 destination – port ?, 该命令的含义是创建一个规则，该规则允许源IP地址为 192.168.2.2 的TCP流量通过，目标端口号为待指定的值。通过这个命令，可以在ACL中配置一个允许特定源IP地址的TCP流量通过的规则，但目标端口号仍需根据具体情况进行进一步的指定。



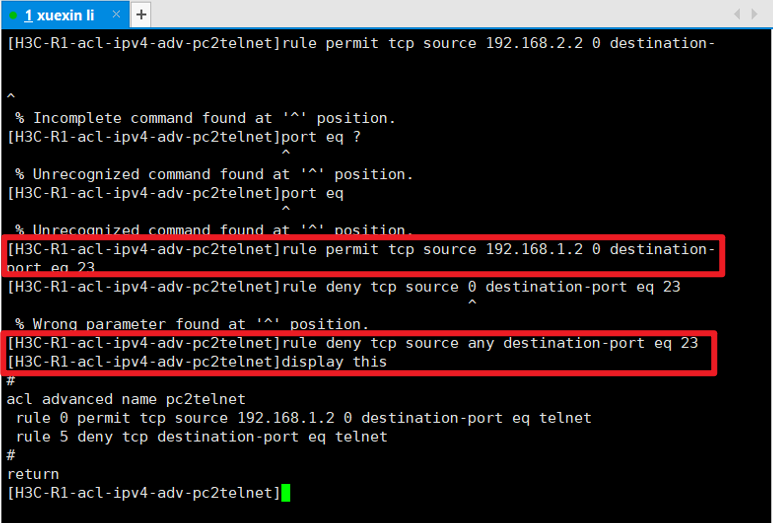
**图 6 配置H3C-R1**

6)输入rule permit tcp source 192.168.2.2 0 destination – port eq ?, 该命令的含义是创建一个规则，该规则允许源IP地址为 192.168.2.2 的TCP流量通过，但目标端口号尚未指定，并使用“eq”关键字表示匹配特定的端口号。这样配置的规则允许具有指定源IP地址的TCP流量通过，并通过进一步指定具体的目标端口号来限制允许通过的流量范围，如图 7所示：



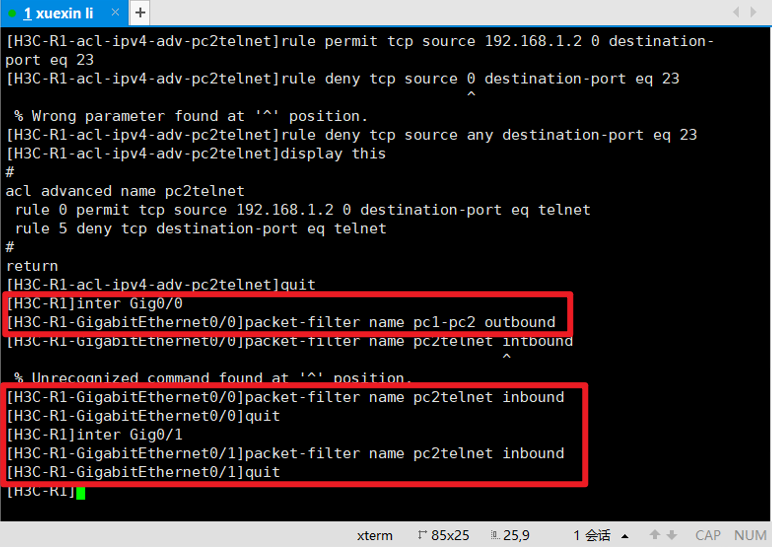
**图 7 查看配置**

7)输入rule permit tcp source 192.168.1.2 0 destination – port eq 23 、rule deny tcp source any destination – port 23、display this, “rule permit tcp source 192.168.1.2 0 destination – port eq 23 ” 的含义是创建一个允许规则，允许源IP地址为 192.168.1.2 的TCP流量通过，目标端口号为 23。其中，"eq 23" 表示要精确匹配端口号为 23 的流量；“rule deny tcp source any destination – port 23”的含义是创建一个拒绝规则，阻止任何源IP地址的TCP流量通过，目标端口号为 23。这条规则的作用是拒绝所有针对端口号为 23 的TCP流量的访问；“display this” 的含义是用于显示当前的配置或规则。具体的显示内容取决于上下文，它可以用于查看已经配置的规则或其他网络设备的相关信息。通过执行这个命令，可以查看当前配置中的某个特定规则或其他相关的配置信息，如图 8所示：



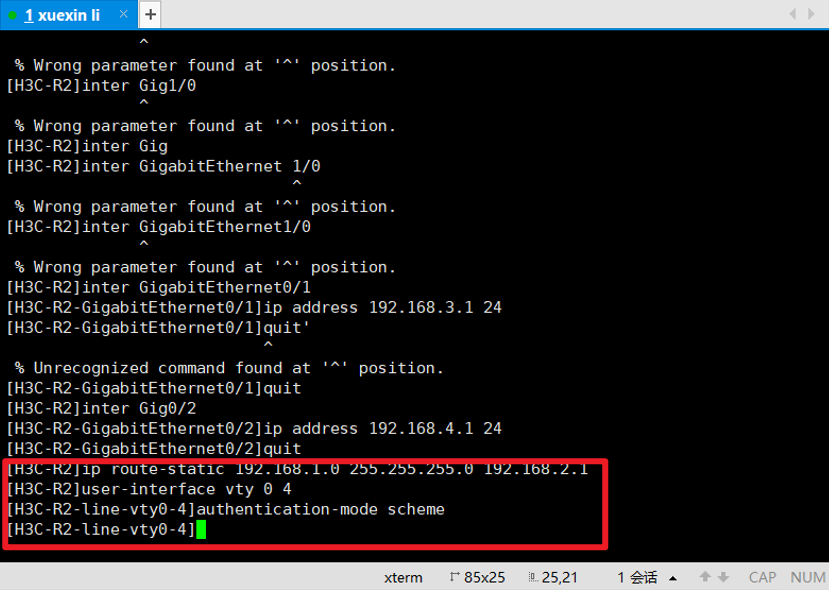
**图 8 创建规则**

8)输入interface Gigabthernet 0/0、packet-filter name pc1-pc2 outbound、packet-filter name pc2telnet inbound、interface Gigabthernet 0/1、packet-filter name pc2telnet inbound，如图 9所示：



**图 9 配置数据包过滤器**

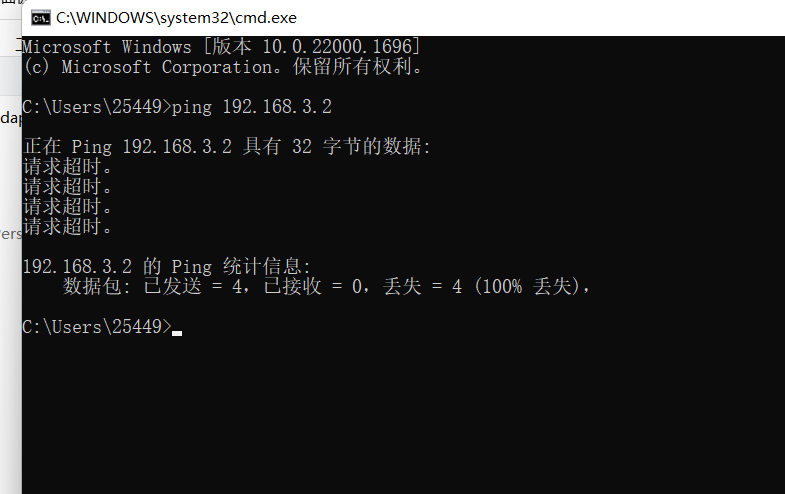
（2）配置H3C-R2，如图 10所示：



**图 10 配置H3C-R2**

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

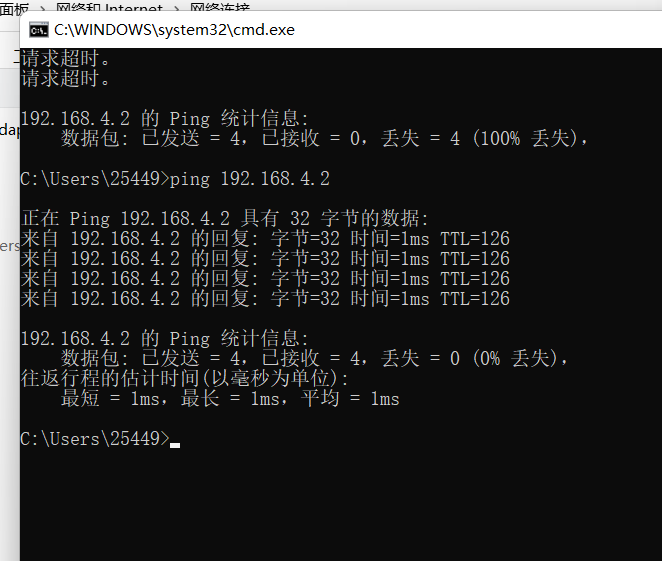
如图 11所示：



**图 11 PC1 ping PC2**

3. 从PC1上，使用ping命令访问PC2的IP地址192.168.4.2，测试连通性

如图 12所示：



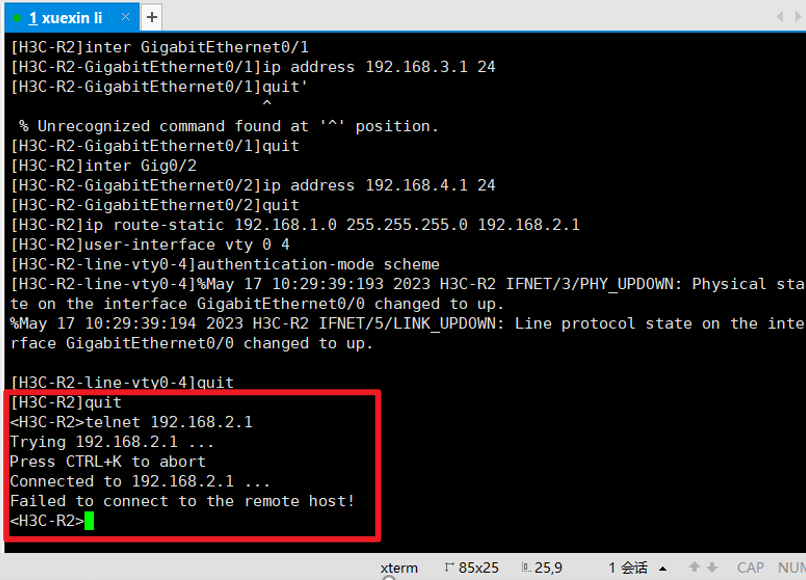
**图 12 PC1 ping PC3**

根据两次ping的测试，可以看到在Ethernet0/0接口的出方向，ACL3000过滤了数据包，组织了特定地址网段去往特定目的主机的访问。

4. 在H3C-R2上测试使用telnet访问H3C-R1

（截取你自己的配置界面，并配以简单文字解释重要命令的含义。）

如图 13所示：



**图 13 在H3C-R2上测试使用telnet访问H3C-R1**

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？

通过这次试验，我实现了对网络流量的精细控制和过滤。我可以根据源IP地址、目标IP地址、端口号、协议类型等条件，设置允许或拒绝特定类型的流量通过网络设备，从而提高网络的安全性和性能。除此之外，在实验过程中，我通过解决问题，提高了故障排除的能力和技巧，了解了网络设备的工作原理和配置细节。