**基本ACL配置指南**

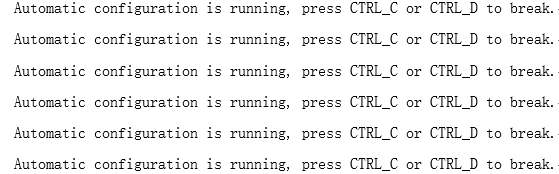
开始ACL相关配置前，需要先进行路由器的基本配置，如设备命名、接口配置等。

1. 在开始操作前，清空路由器上的原有配置，以避免原有配置造成的影响。具体使用reset saved-configuration命令和reboot命令实现该功能。

**<H3C-R1>reset save**  
The saved configuration file will be erased. Are you sure? [Y/N]:y  
Configuration file does not exist!  
**<H3C-R1>reboot**  
Start to check configuration with next startup configuration file, please wait.........DONE!  
Current configuration may be lost after the reboot, save current configuration? [Y/N]:n  
This command will reboot the device. Continue? [Y/N]:y  
Now rebooting, please wait...  
注意1：你的设备名称也许不是H3C—R1,这个没有关系，我们后面修改。

注意2：这两条命令一定要退到用户视图，否则无法操作。

注意3：在重启过程中有时候会不停报如下消息



此时按指示敲击Ctrl+C或Ctrl+D即可。

1. 给两个路由器重新命名以便区分。

将连接PC1的路由器改名为H3C-R1:

<H3C>**system-view**  
System View: return to User View with Ctrl+Z.  
[H3C]**sysname H3C-R1**  
[H3C-R1]

将连接PC2的路由器改名为H3C-R2:

<H3C>**system-view**  
System View: return to User View with Ctrl+Z.  
[H3C]**sysname H3C-R2**  
[H3C-R2]

注意：配置时一定要确保连线正确，当配置R1时网线插入R1的Console口，当配置R2时网线插入R2的Console口。

1. 配置路由器端口

配置H3C-R1上的端口

[H3C-R1]**interface GigabitEthernet0/1**  
[H3C-R1-GigabitEthernet0/1]**ip address 192.168.1.1 24**  
[H3C-R1-GigabitEthernet0/1]**quit**  
[H3C-R1]**interface GigabitEthernet0/2**  
[H3C-R1-GigabitEthernet0/2]**ip address 192.168.2.1 24**

配置H3C-R2上的端口

[H3C-R1]**interface GigabitEthernet0/2**

[H3C-R2-GigabitEthernet0/2]**ip address 192.168.2.2 24**  
[H3C-R2-GigabitEthernet0/2]**quit**  
[H3C-R2]**interface GigabitEthernet0/1**  
[H3C-R2-GigabitEthernet0/1]**ip address 192.168.3.1 24**

注意1：这里的配置端口E0/2并非教材上写的E0/0，因为老师在测试时发现

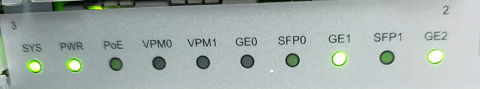
我所使用的路由器E0/0端口不通，可能是偶发事件，也可能是同学

中有人暴力插拔导致端口损坏。那么如何判断端口是否损坏？请连

好线后观察路由器背板，如图所示。



查看GE端口指示灯，如图所示，开始我的GE0灯连上线后始终不亮，我使用测线仪检查了双绞线，排除双绞线问题，考虑换到GE2端口，它就亮了。



1. 配置PC1和PC2的IP地址和默认网关

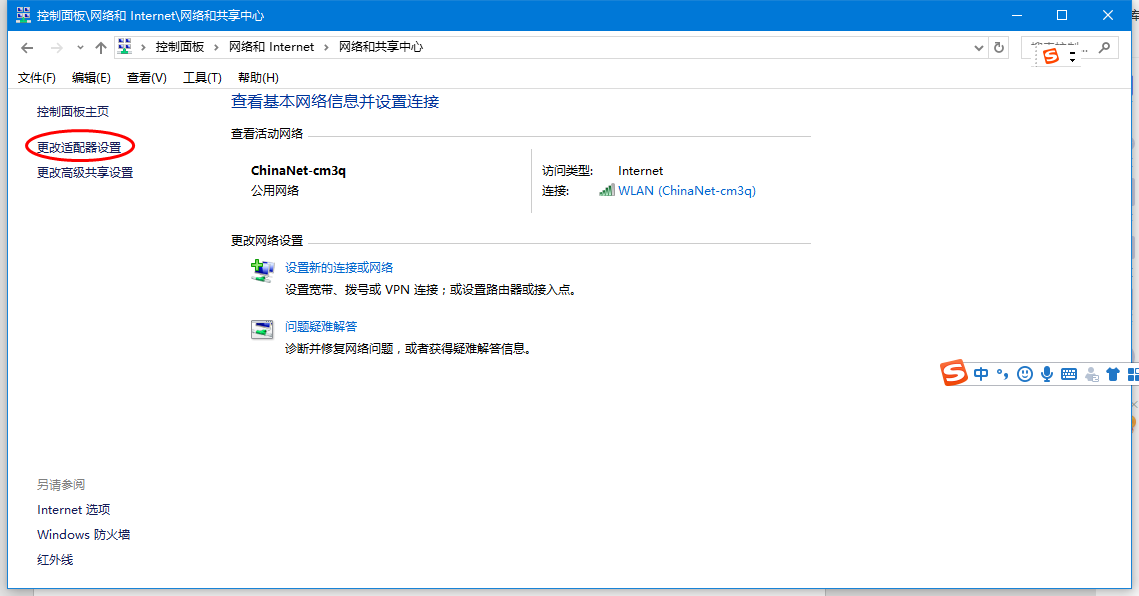
在PC1所在系统里找到“控制面板”，如图所示（如何找到你系统的控制面板可能会因为你的操作系统不同而方法不同，请自行上网查找）



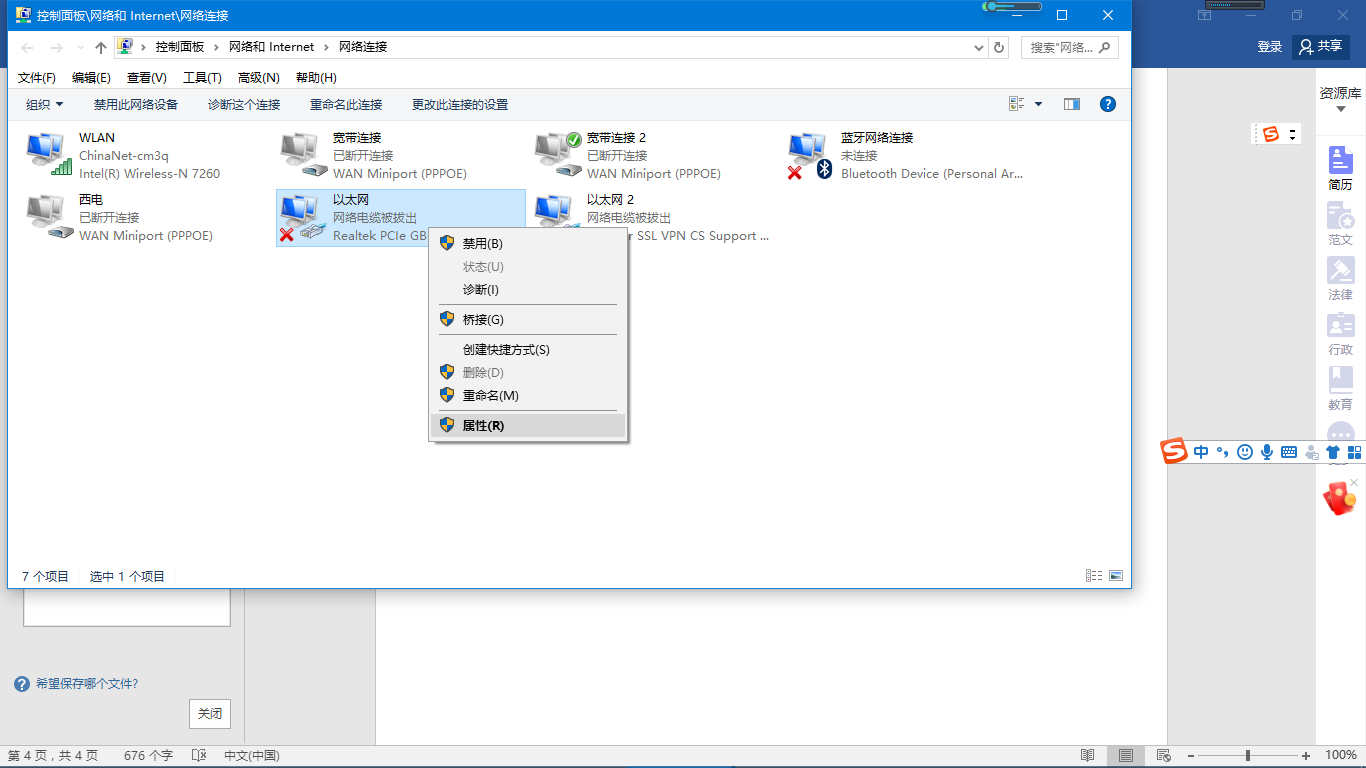
找到“网络和Internet”，点击下面的“查看网络状态和任务”，如图所示。



进入界面后，选择“更改适配器设置”，如图所示。



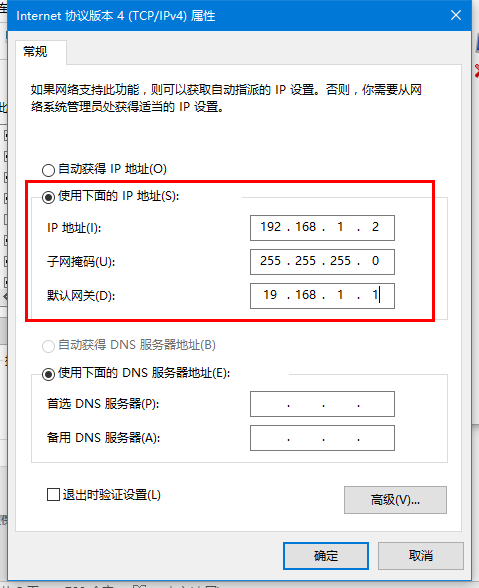
此时，会出现你的所有网络，找到网卡所在位置，单击鼠标右键，选择“属性”，如图所示



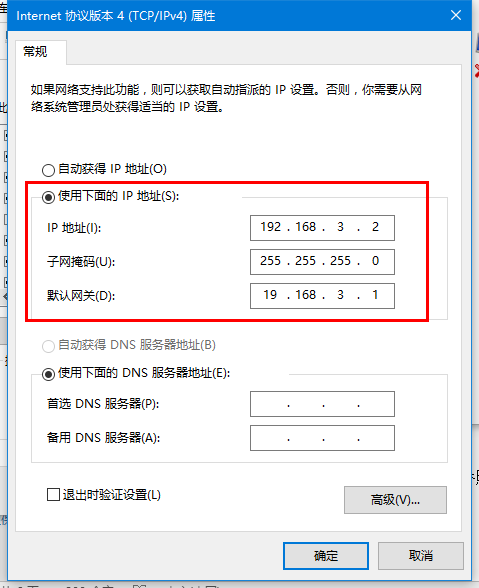
在出现的界面中选择“Internet协议版本4（TCP/IPv4）”，如图所示。



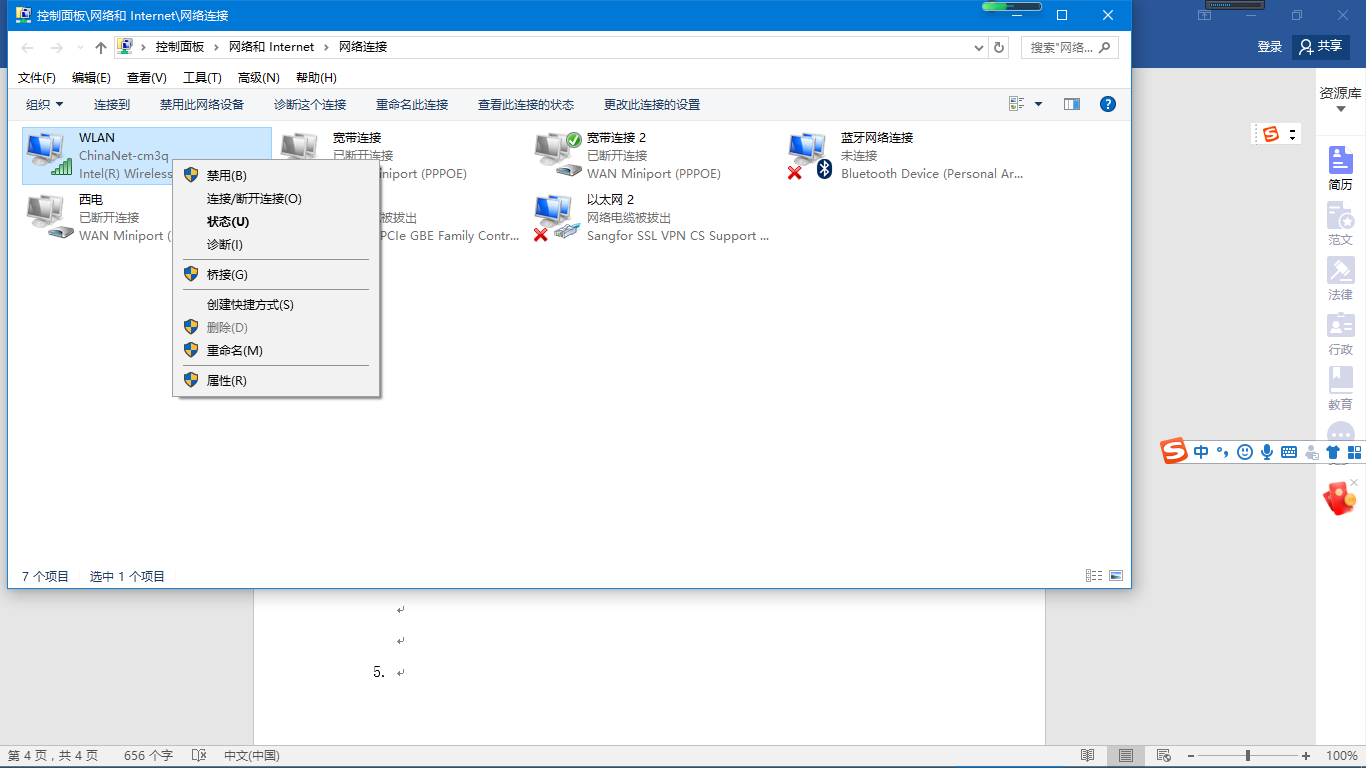
在出现界面中选择“使用下面的IP地址”，如下图所示配置PC1的IP地址和默认网关等参数。



参照以上步骤，在PC上配置IP地址和默认网关等参数，如下图所示。



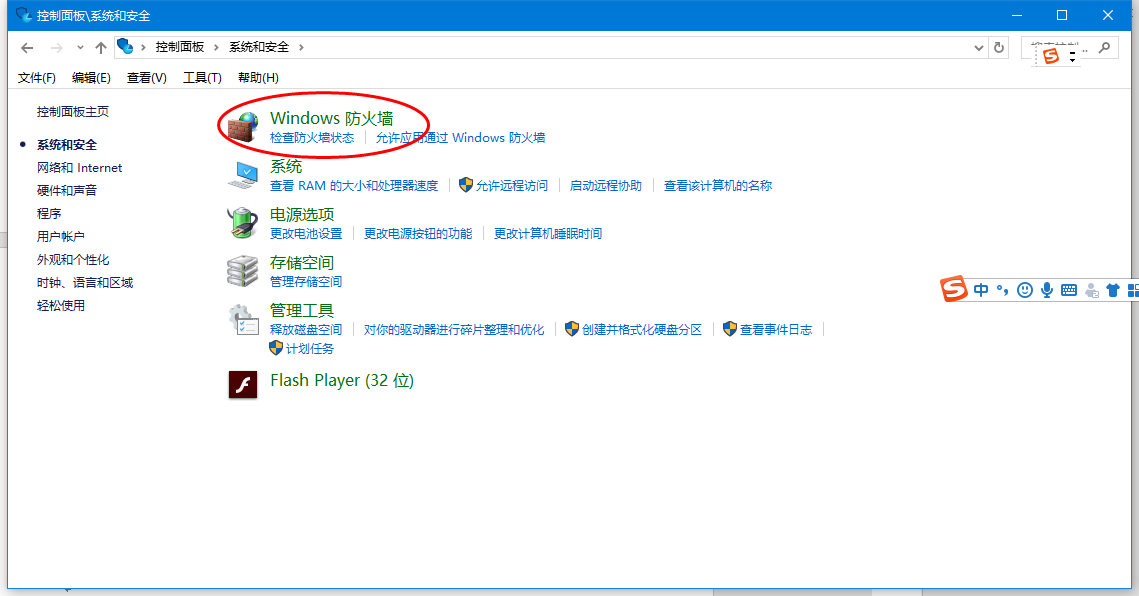
注意1：为防止干扰，这里最好关闭无线。具体操作方法：在“网络连接”中选中无线，点击右键，在其中选择“禁用”，从而关闭你的无线。



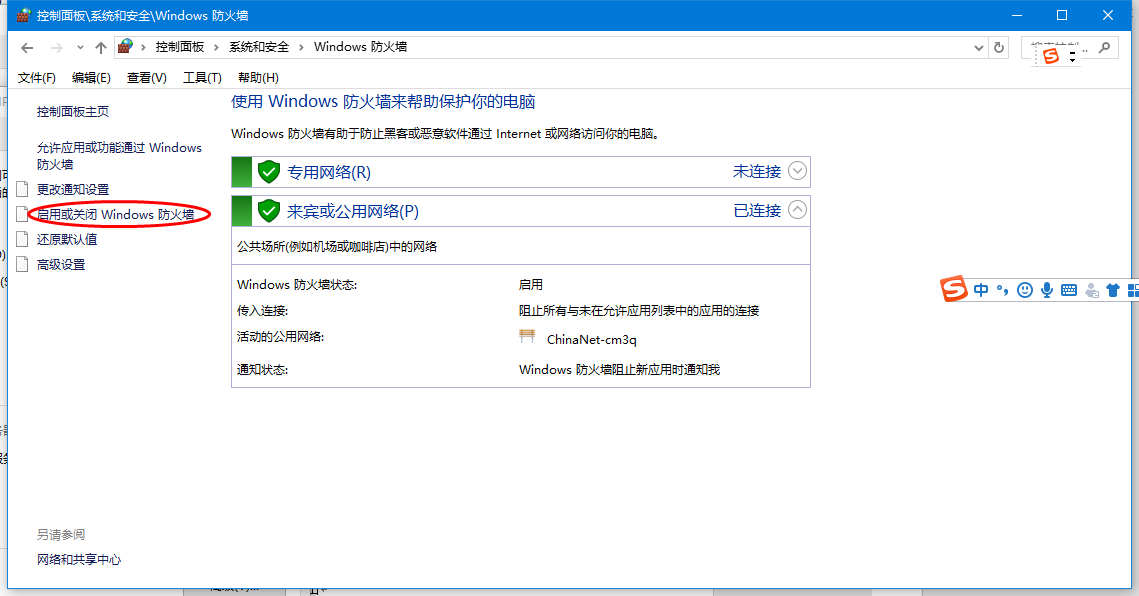
注意2：为防止干扰，这里最好也关闭防火墙。具体操作方法：“控制面板”中找到“系统与安全”，如图所示。



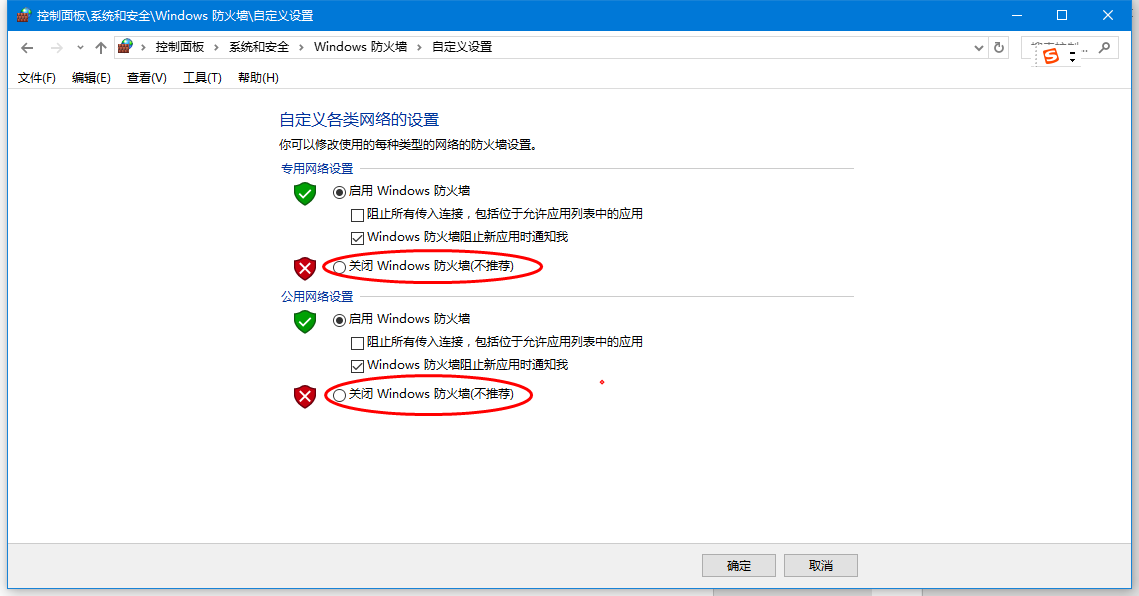
进入界面，找到Windows防火墙，如图所示，点击“检查防火墙状态”。



出现界面如下所示。找到“启动或关闭Windows防火墙”选项，如下所示。



选择“关闭”，如图所示。



注意：你的电脑可能还安装了自己定制或购买的防火墙，请自行关闭，这个问题要引起足够重视。

1. 在H3C-R1和H3C-R2上设置静态路由

在R1上设置静态路由：

你可以一句话完成该命令

[H3C-R1]**ip route-static 192.168.3.0 255.255.255.0 192.168.2.2**

也可以像我这样分步骤完成，以便了解更多关于参数的含义

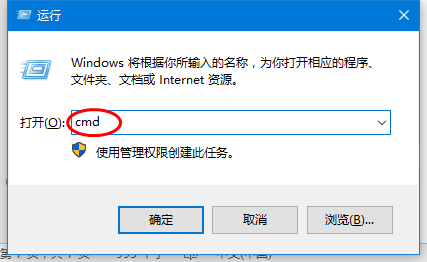
[H3C-R1]**ip route-static 192.168.3.0 ?**  
 INTEGER<0-32> Mask length of the IP address  
 X.X.X.X Mask of the IP address  
  
[H3C-R1]**ip route-static 192.168.3.0 255.255.255.0 ?** Aux Aux interface  
 GigabitEthernet GigabitEthernet interface  
 NULL NULL interface  
 Serial Serial interface  
 X.X.X.X Nexthop IP address  
 vpn-instance Destination VPN instance for gateway address  
  
[H3C-R1]**ip route-static 192.168.3.0 255.255.255.0 192.168.2.2**  
[H3C-R1]

同样，可以在R2上完成静态路由

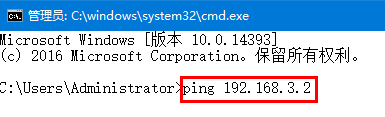
[H3C-R2]**ip route-static 192.168.1.0 255.255.255.0 192.168.2.1**  
[H3C-R2]  
注意：此时，都可以使用**display ip routing**在各自路由表中看到此条静态路由信息。

1. 测试PC1和PC2的互通性

在PC1上，键盘上同时按下 和R，在出现的运行界面中敲入cmd，如图所示



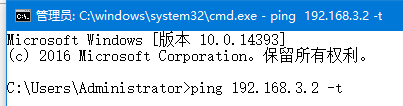
在出现的界面中敲入ping 192.168.3.2，如图所示，可以测PC1是否可以Ping通PC2。



可以在PC2端以同样方法Ping通PC1。

1. 设置基本ACL对通过接口的数据包进行过滤。

为了能看到过滤效果，或者说限制效果，我们在进行下一步操作前，在PC1上打开命令行窗口，敲入给ping指令后加上参数-t，让ping命令持续跑起来



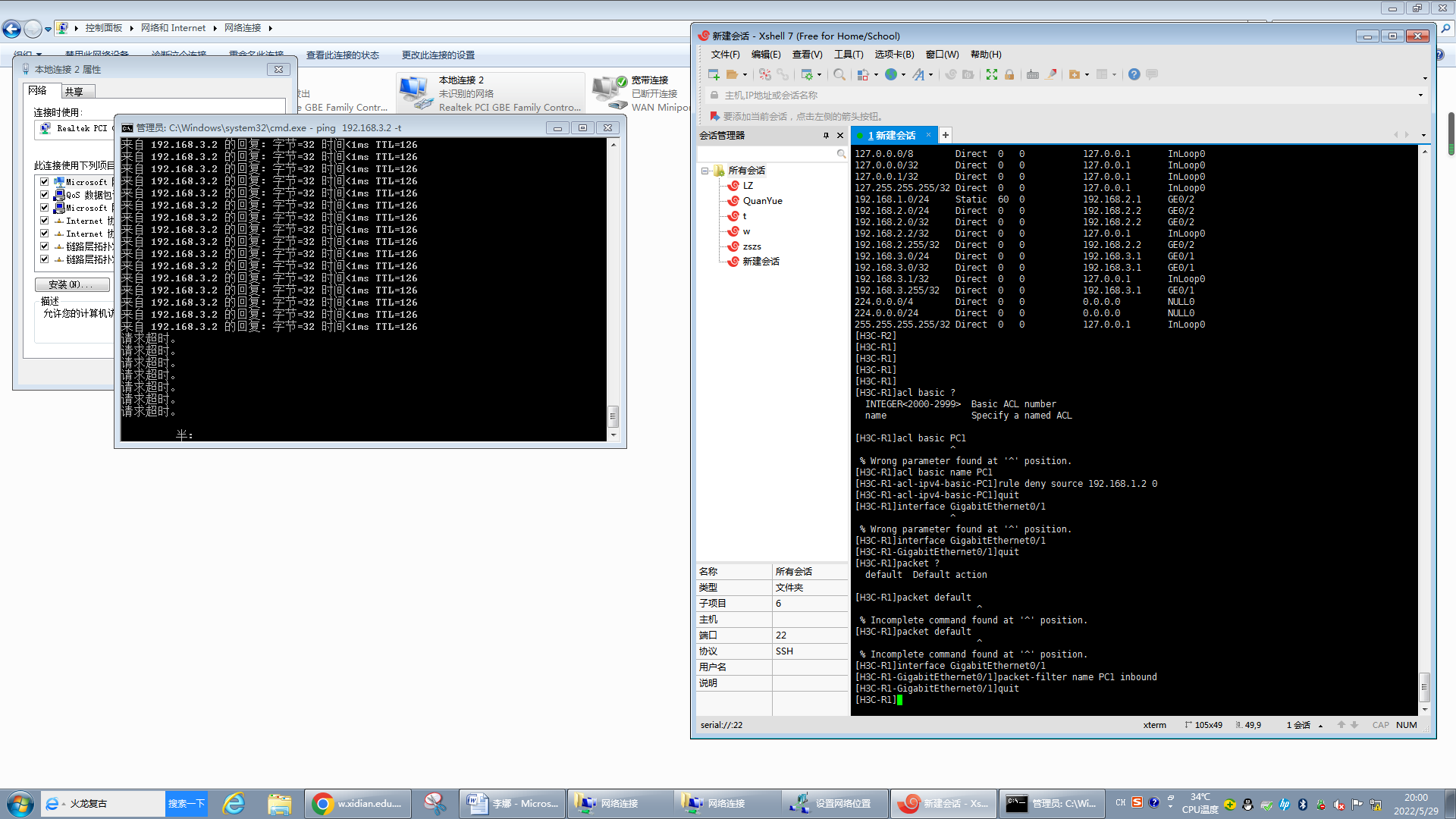
根据ACL规则指定的源IP地址，在接口的出入方向上选择性放行数据包。本实验中将PC1作为攻击机而将PC2作为靶机，为了在三层限制PC1和PC2之间的通信，可以在路由器R1上配置基本ACL来实现。

[H3C-R1]**acl basic name PC1**  
[H3C-R1-acl-ipv4-basic-PC1]**rule deny source 192.168.1.2 0**[H3C-R1-acl-ipv4-basic-PC1]**quit**  
[H3C-R1]**interface GigabitEthernet0/1**

[H3C-R1-GigabitEthernet0/1]**packet-filter name PC1 inbound**  
[H3C-R1-GigabitEthernet0/1]**quit**  
简单介绍以上配置过程含义：创建名为PC1的基本ACL，进入ACL视图，配置拒绝源IP地址为192.168.1.2数据包通过的规则。退出ACL视图，进入GE0/0接口视图，将PC1这一基本ACL应用到GE0/0接口的入方向，对接口收到的报文进行过滤。应用后PC1发送的所有数据包均无法通过路由器R1，起到了限制攻击的作用。

1. 限制效果展示。

随着配置起效，如下所示



PC1无法Ping通PC3

