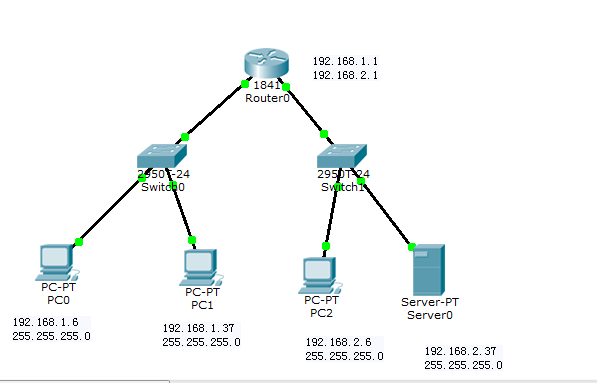
实验目的：

深入理解包过滤防火墙的工作原理

实验内容：

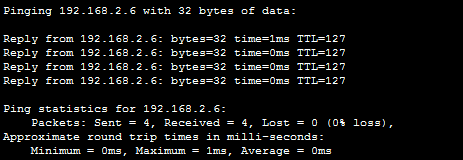
练习使用Packet Tacker 模拟软件配置ACL

实验要求：

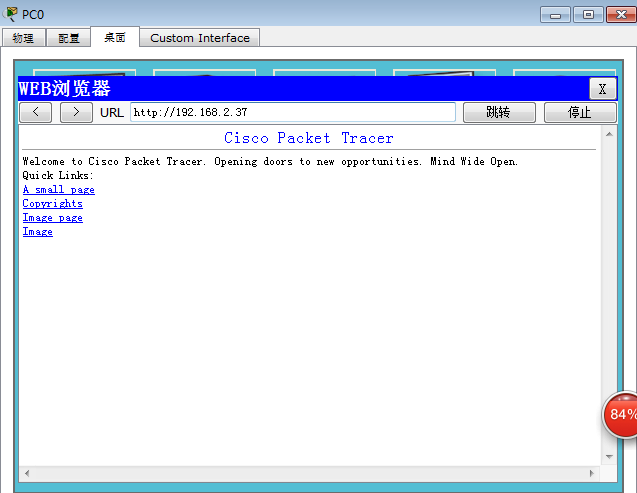


实验步骤：

1. 配置主机、服务器以及路由的ip地址以及路由表
2. 测试主机连通性，例如主机PC0与主机PC2，PC0与服务器



PC0 ping PC2



PC0 访问服务器

1. 配置标准ACL,使得主机PC0可以访问PC2与服务器，主机2不能访问PC2与服务器，使设置生效，实验验证。

ACL设置命令：

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#access-list 1 deny 192.168.1.37 255.255.255.0

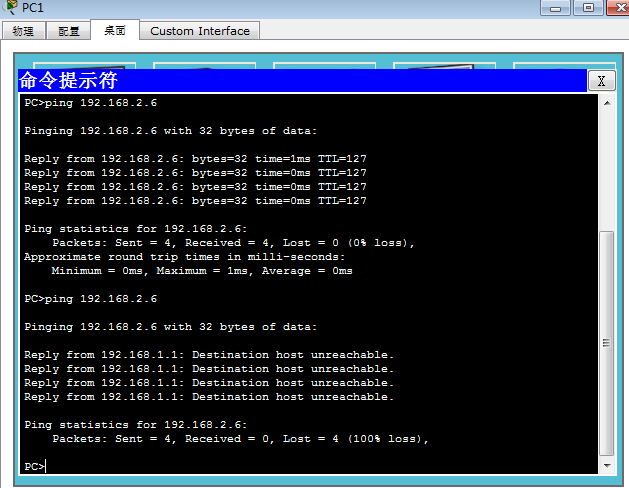
Router(config)#access-list 1 permit any

Router(config)#interface fastethernet0/1

Router(config-if)#ip access-group 1 out

Router(config-if)#exit

Router(config)#



PC1与PC2不能ping通

4.删除该条ACL，实验验证

清除ACL命令：

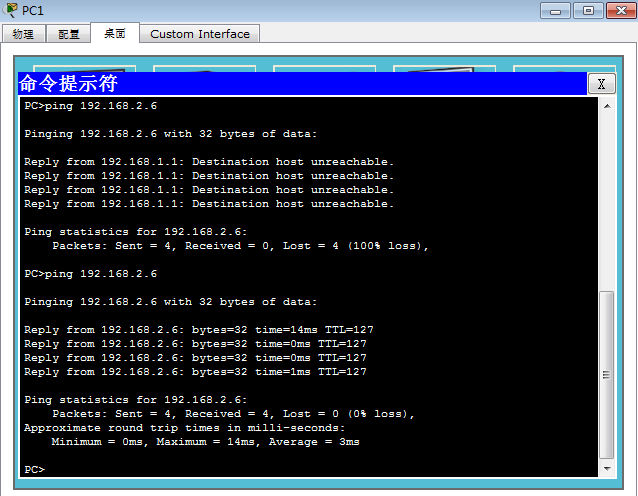
Router(config)#ip access-list standard soft

Router(config-std-nacl)#no access-list 1

Router(config)#exit

Router#

%SYS-5-CONFIG\_I: Configured from console by console



5 配置扩展ACL， 使得主机PC1可以访问服务器的www服务，主机2不能访问服务器的www服务，三个主机以及服务器间能相互ping通

ACL扩展代码：

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

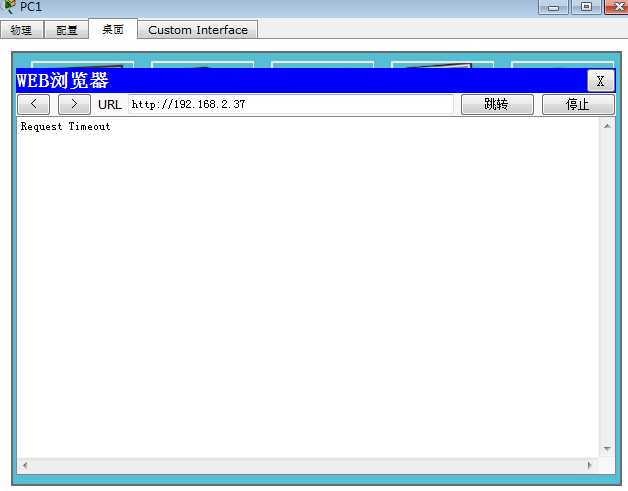
Router(config)#access-list 101 deny tcp 192.168.1.37 255.255.255.0 192.168.2.37 255.255.255.0 eq 80

Router(config)#access-list 101 permit ip any any

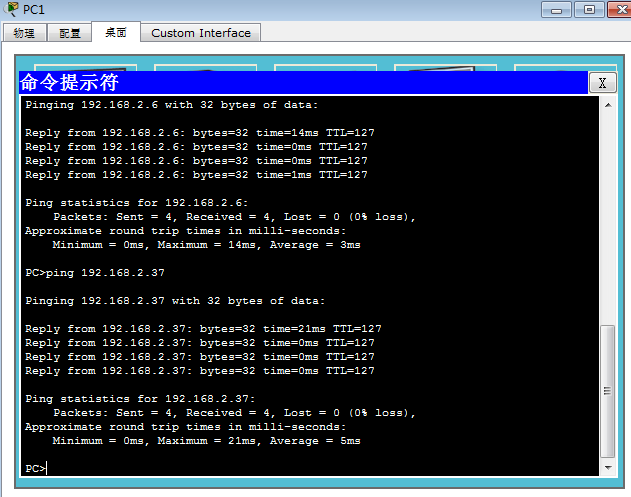
Router(config)#interface fastethernet0/1

Router(config-if)#ip access-group 101 out

Router(config-if)#exit



PC1不能访问服务器



PC1能ping通服务器

6. 删除ACL



