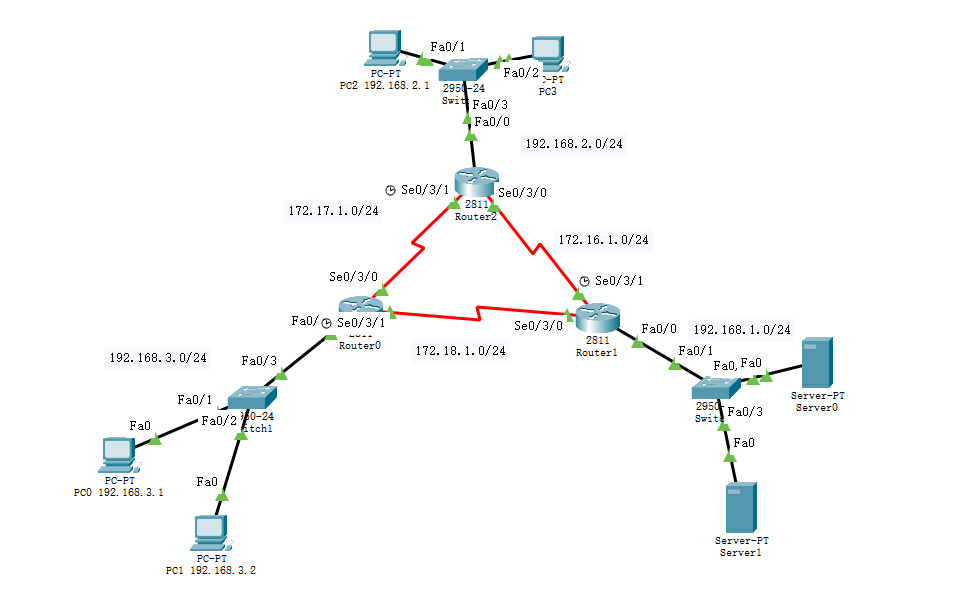
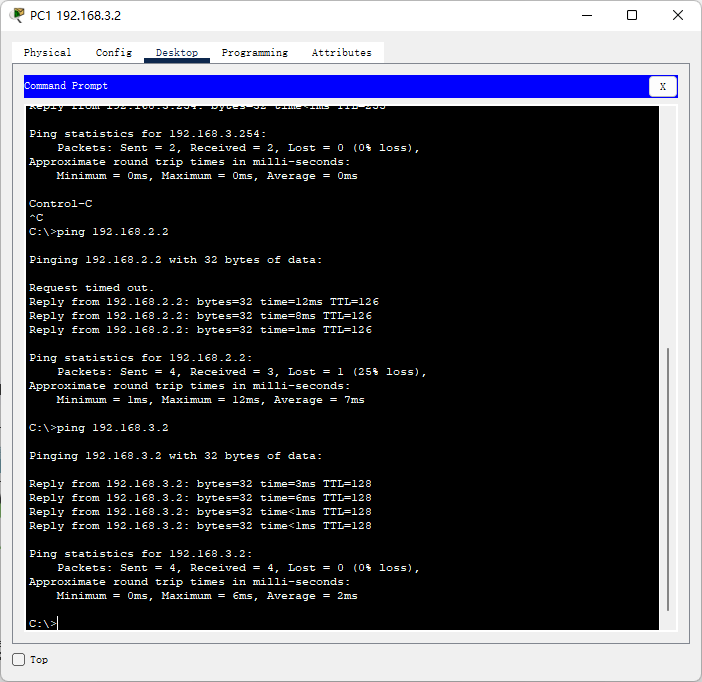
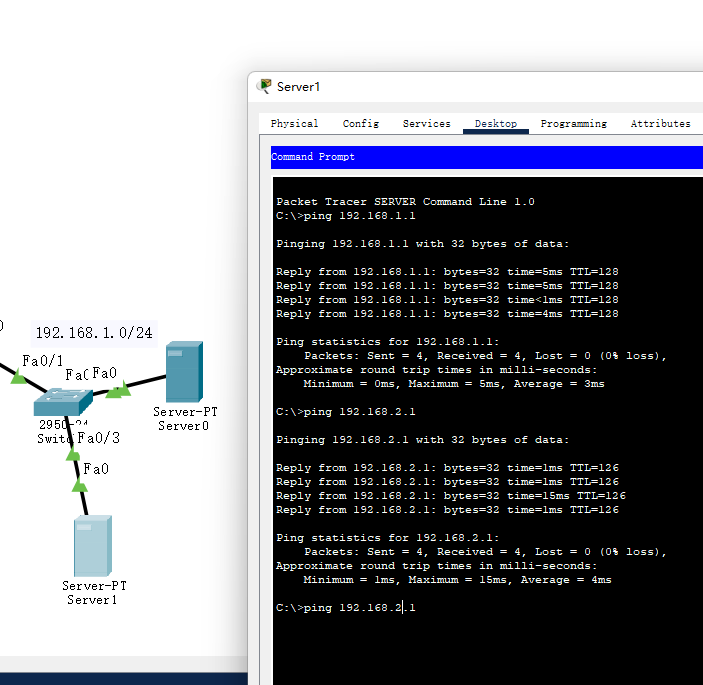
1. 实验内容
   1. 基于如下图的拓扑，对路由器进行正确的RIP协议配置，在此基础上，正确地配置ACL，满足如下要求：
      1. 限制所有主机远程登录到服务器
      2. 禁止192.168.3.0/24网段中的主机Ping192.168.1.0/24网段
      3. 禁止192.168.2.2主机访问HTTP协议
      4. 禁止192.168.2.3主机访问DNS协议

实验过程

1. 环境搭建

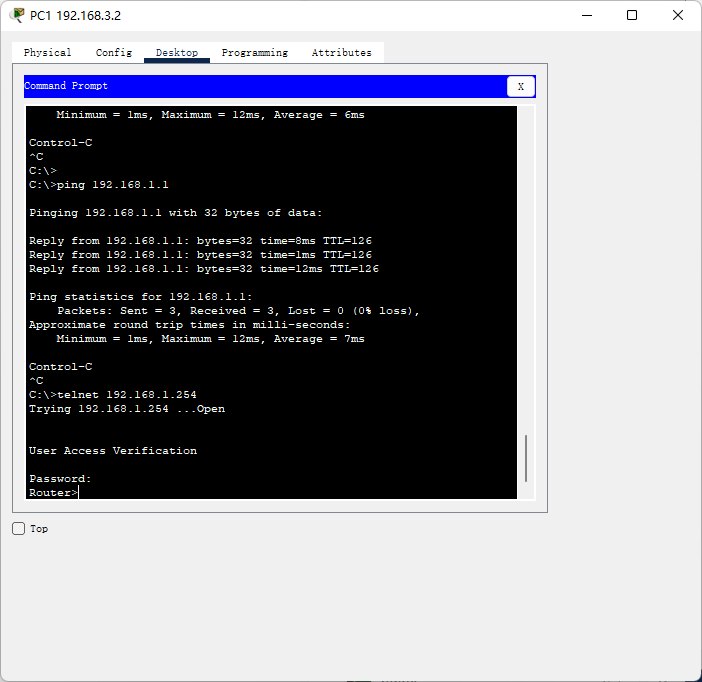
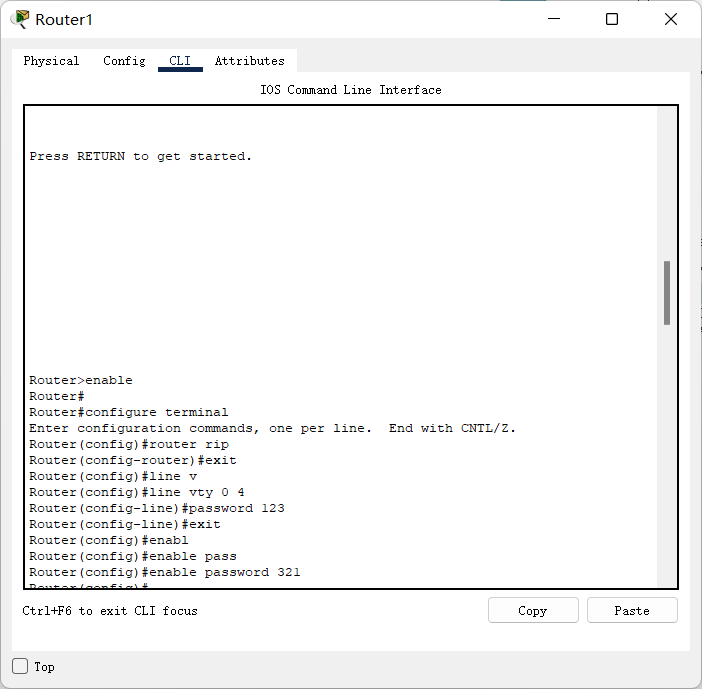


1. RIP配置，使网络下各网段间均能通讯

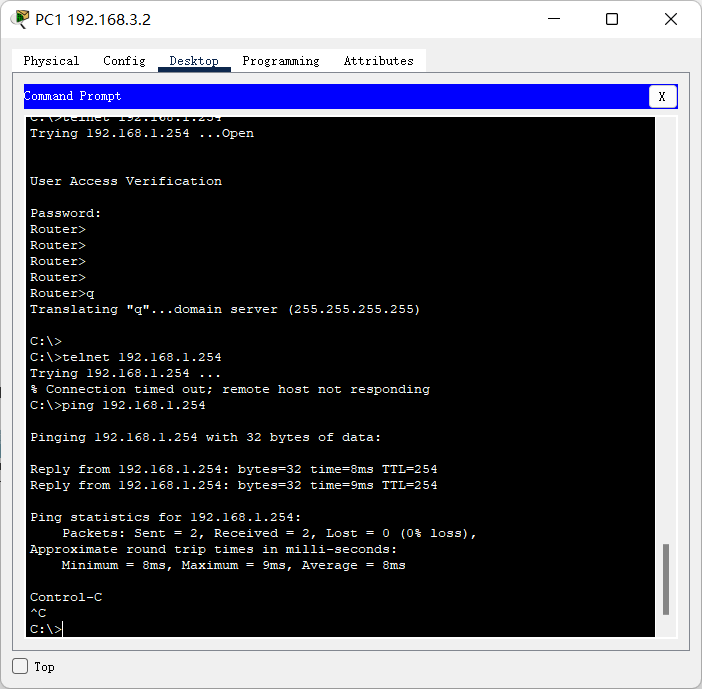
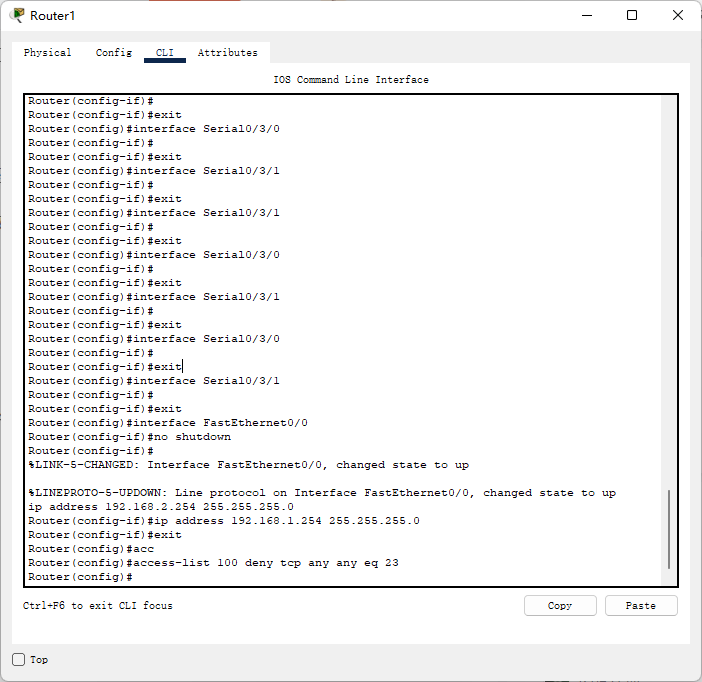


1. 使用ACL进行各类限制实验
2. 限制所有主机远程登录到路由器

首先开启路由器的远程登录

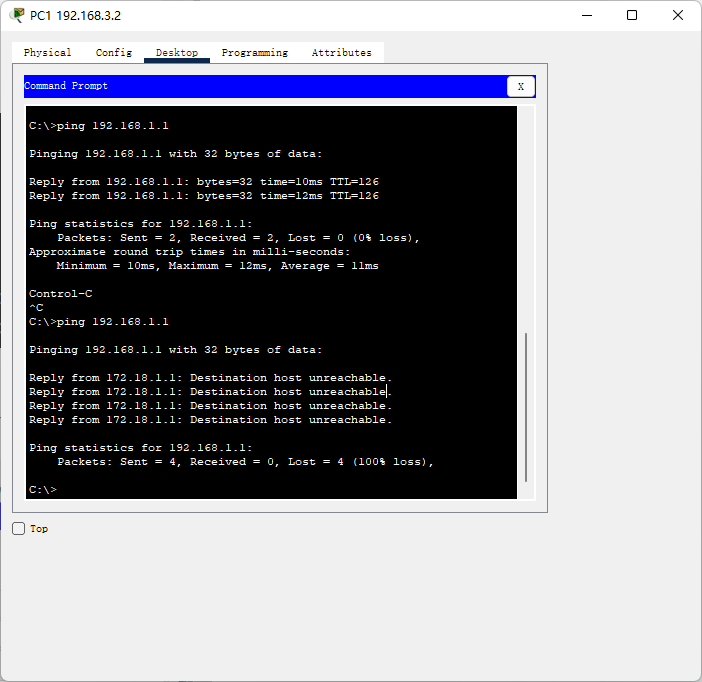
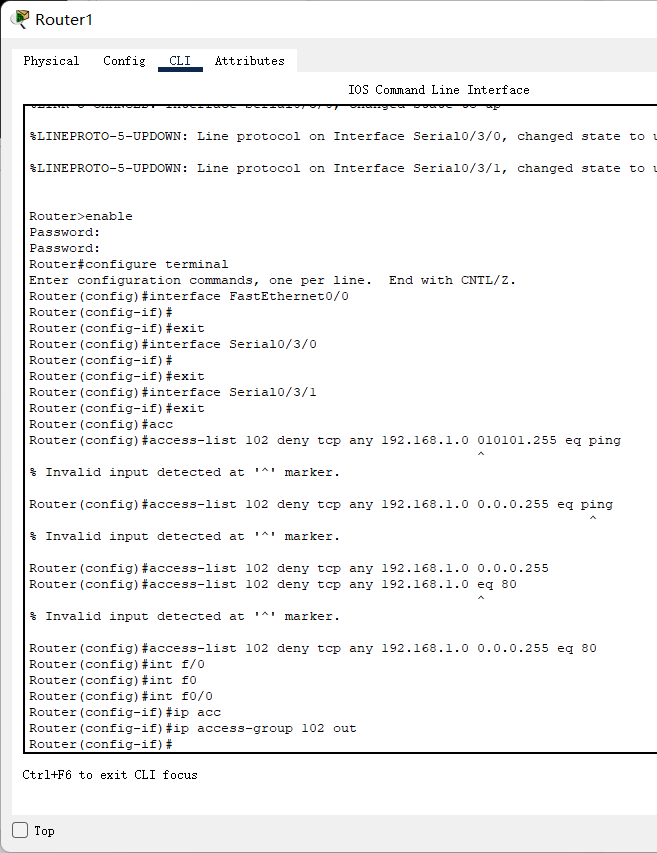


配置路由器的ACL，禁止所有ip与23端口进行TCP，此时PC能与路由器通信但无法进行远程登录



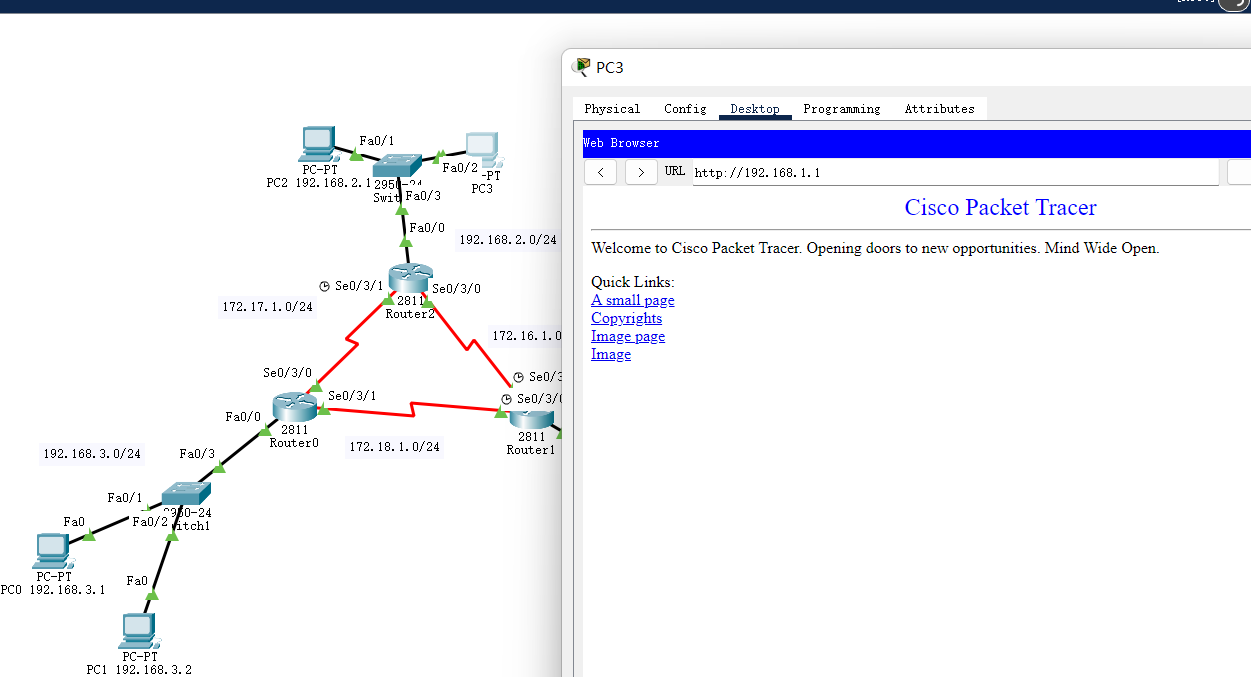
Ii. 禁止192.168.3.0/24网段中的主机Ping192.168.1.0/24网段

配置192.168.3.0/24网段的出口路由器，禁止该网段向192.168.1.0的80端口通信。配置前ping正常，配置后ping开始失效。



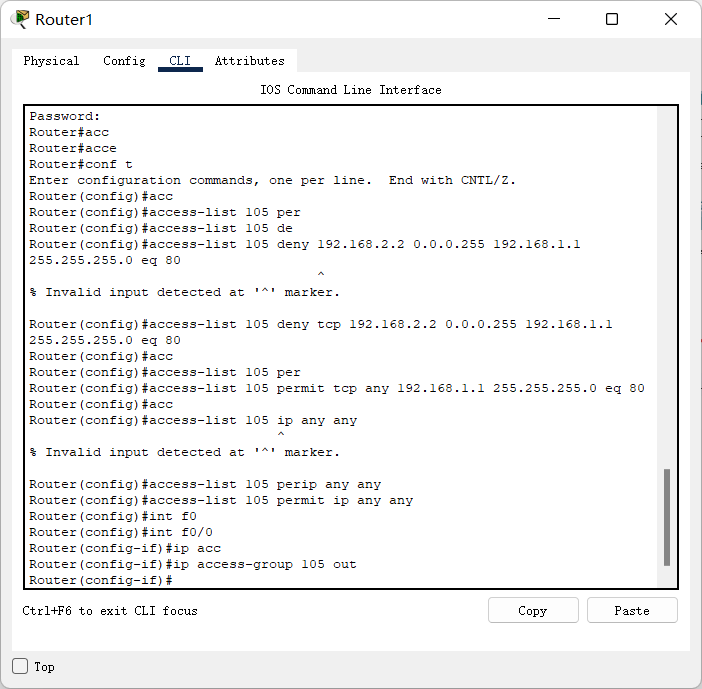
Iii. 禁止192.168.2.2主机访问HTTP协议

初始条件下192.168.2.2可以正常http请求服务器

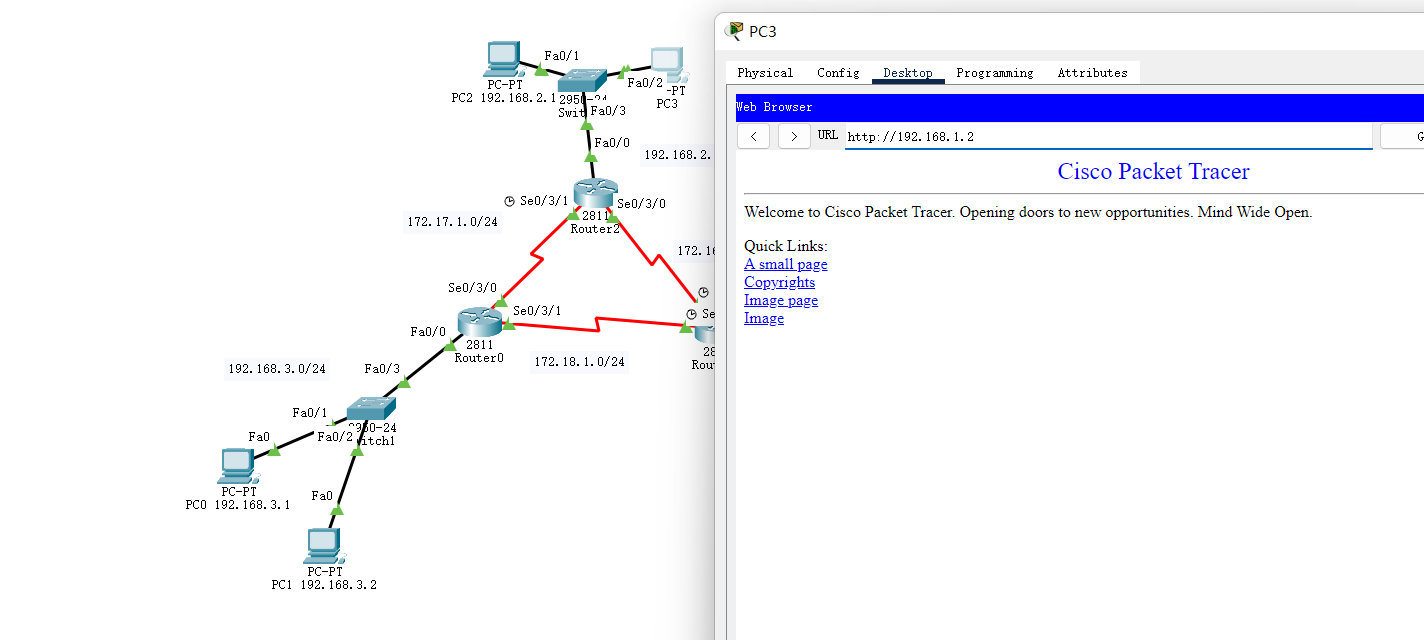
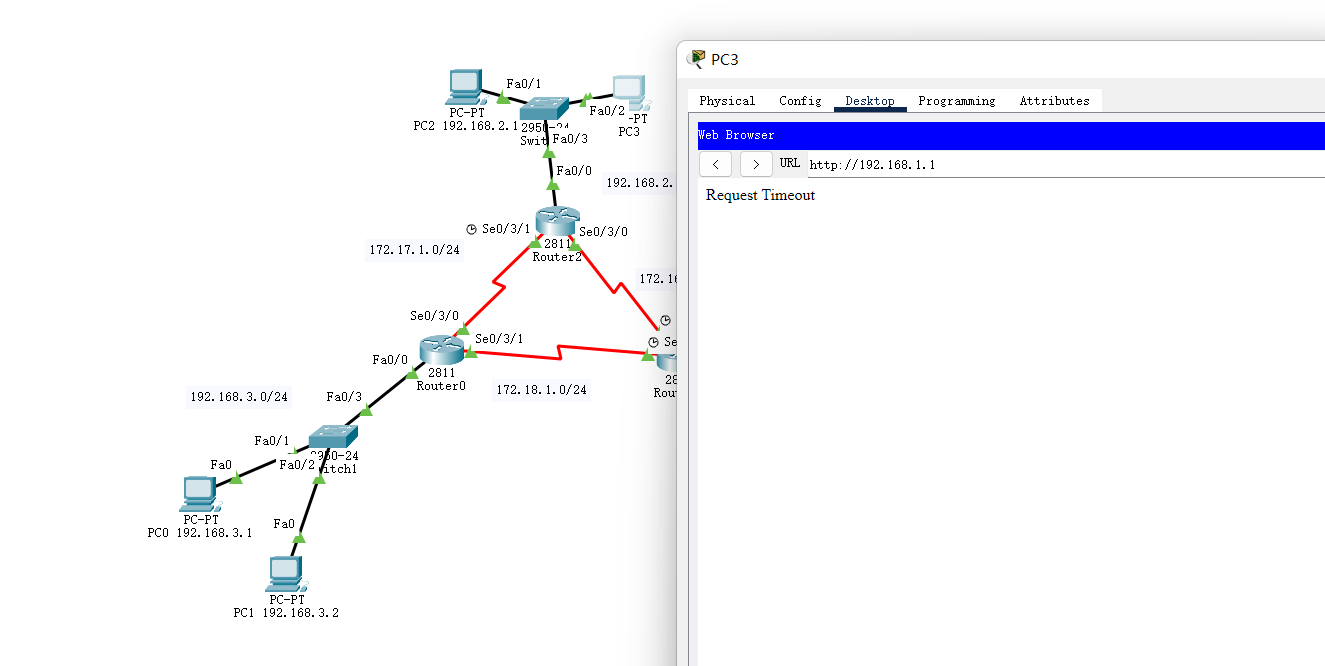


为路由器R1（服务器所在网段出口）配置ACL

access-list 105 denu tcp 192.168.2.2 0.0.0.0 192.168.1.1

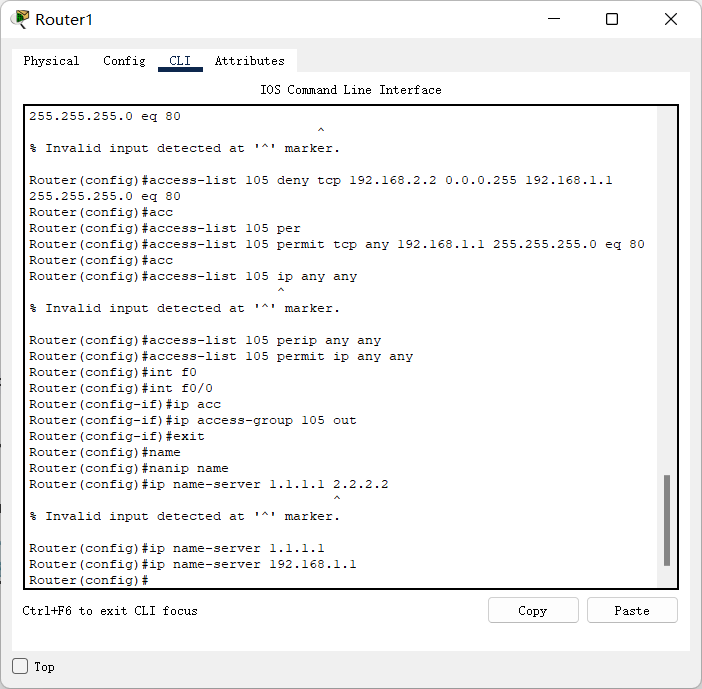
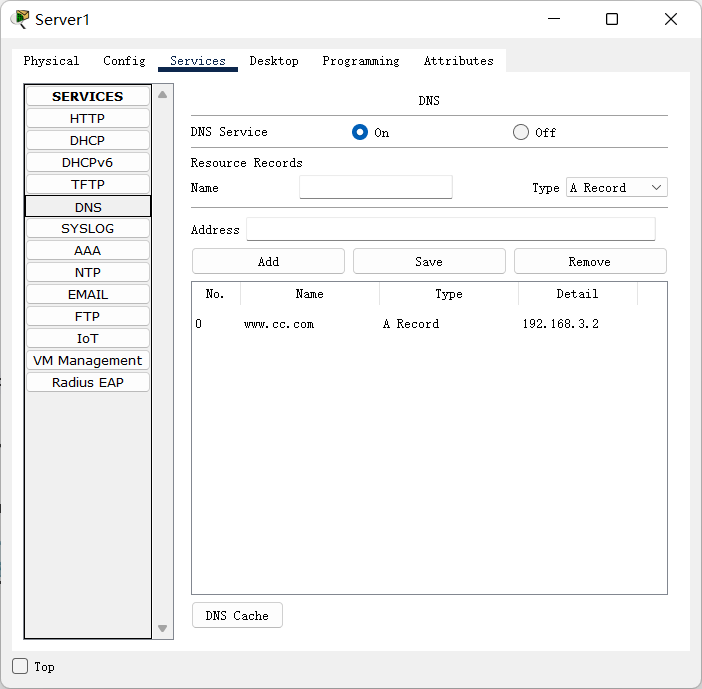


之后发现只有192.168.2.2无法访问服务器，其他PC均可正常访问，同时该PC仍可正常访问与该服务器同网段下的其他Server

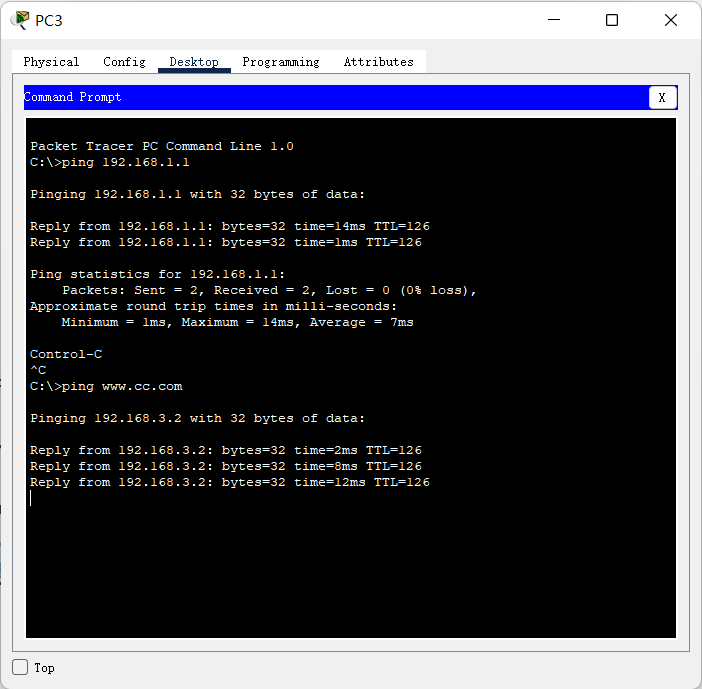


Iiii.禁止192.168.2.3主机访问DNS协议

首先将Server作为DNS服务器，配置DNS服务，并在路由器上添加



将PC 192.168.2.3配置DNS服务器后可以正常解析域名



配置路由器ACL，限制192.168.2.3解析DNS，配置完成后PC 192.168.2.3不再能ping通www，cc.com，而其他PC仍可

