实验五

一、实验题目和目的

实验题目：掌握ACL的基本配置方法

实验时间：12月5日

实验地点：翱翔学生中心104实验室

实验目的：掌握RIP协议和OLSR协议的基本配置方法

二、实验具体内容与步骤

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

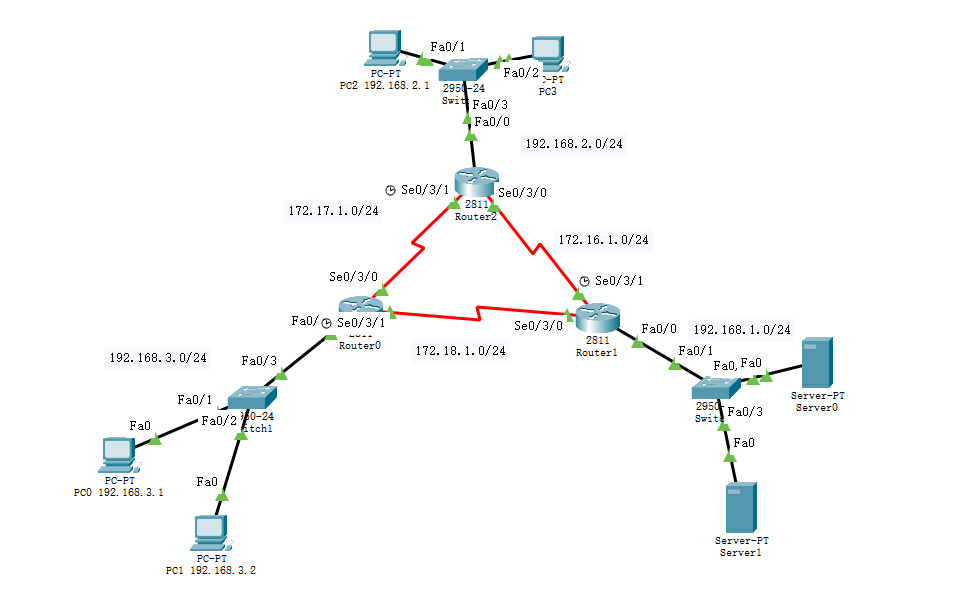
**a)**

1.实验内容：

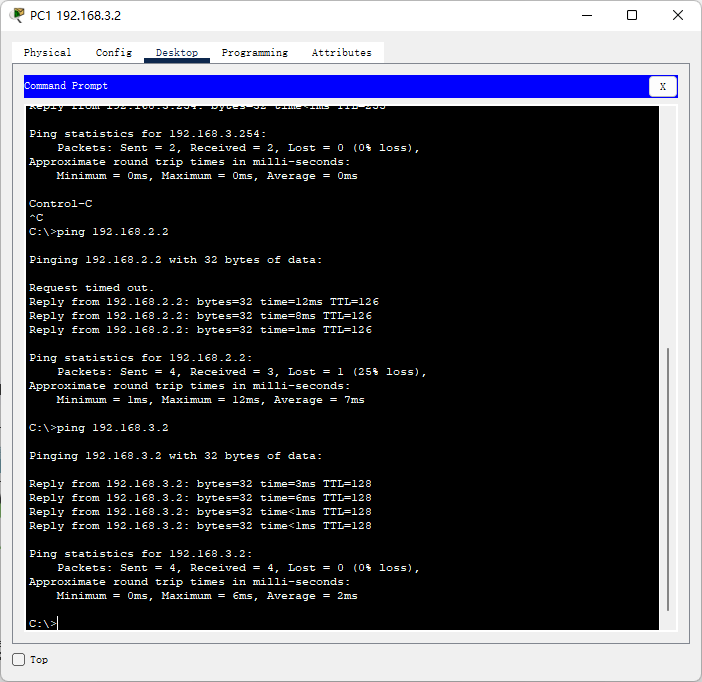
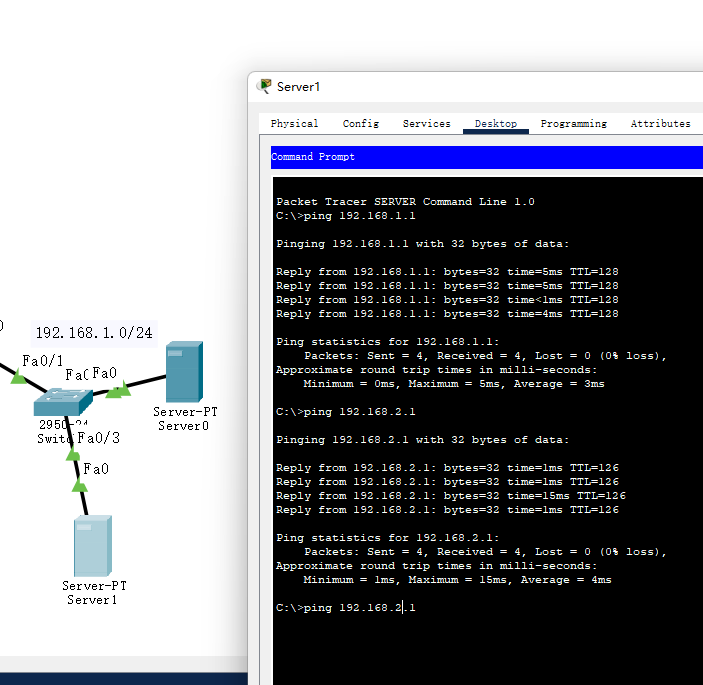
限制所有主机远程登录到服务器

2.实验步骤：

环境搭建



RIP配置，使网络下各网段间均能通讯



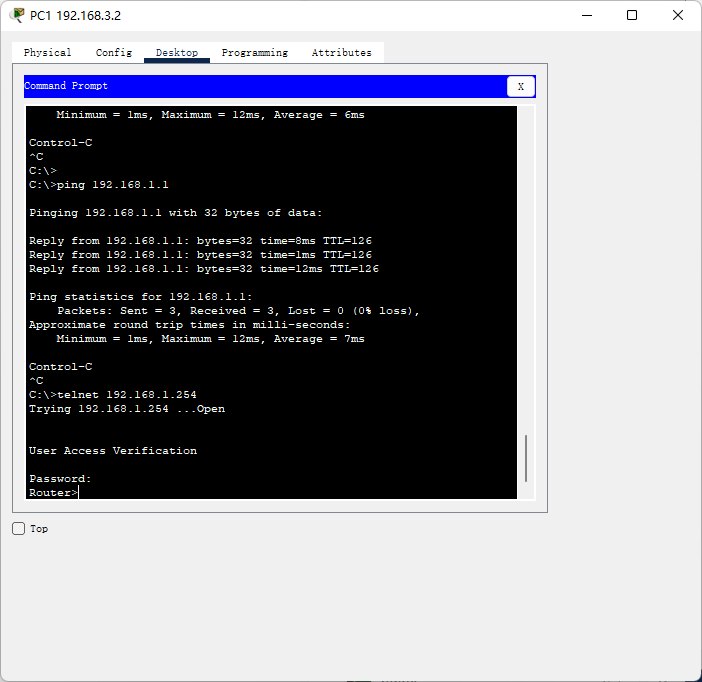
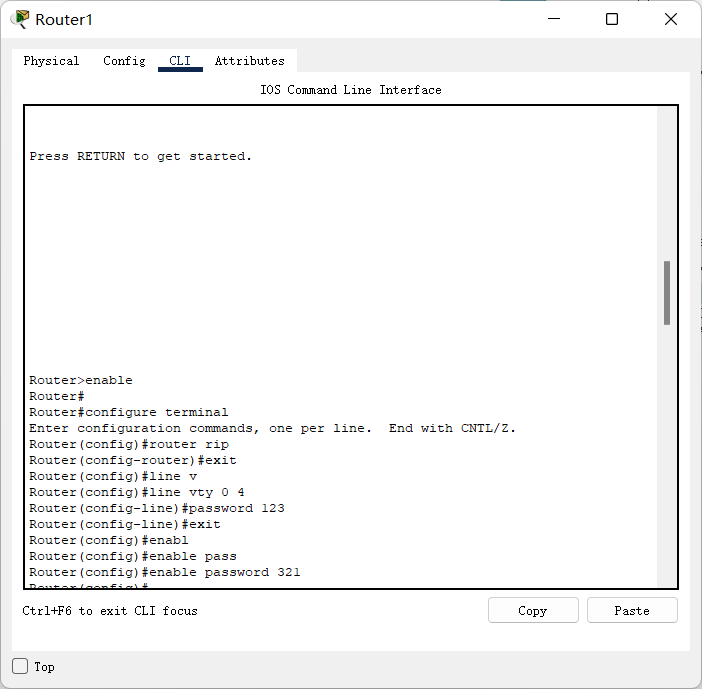
使用ACL进行各类限制实验

限制所有主机远程登录到服务器

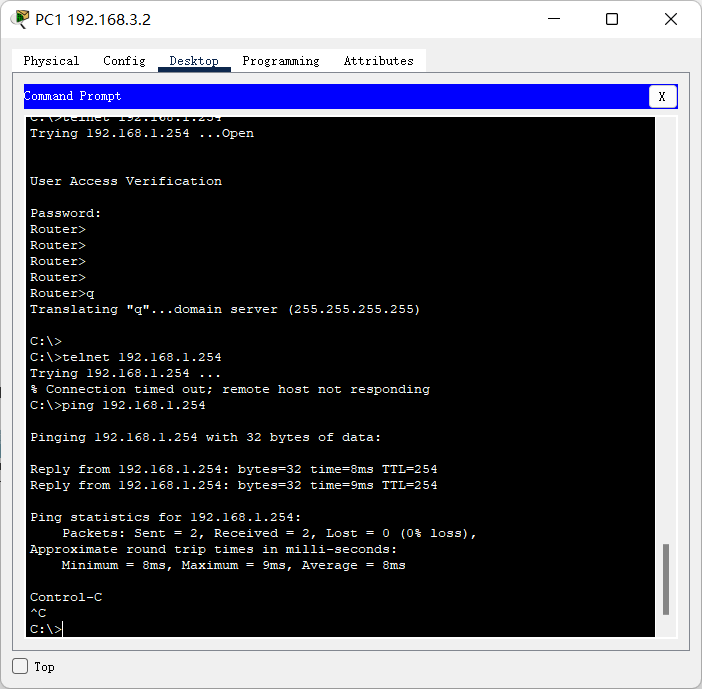
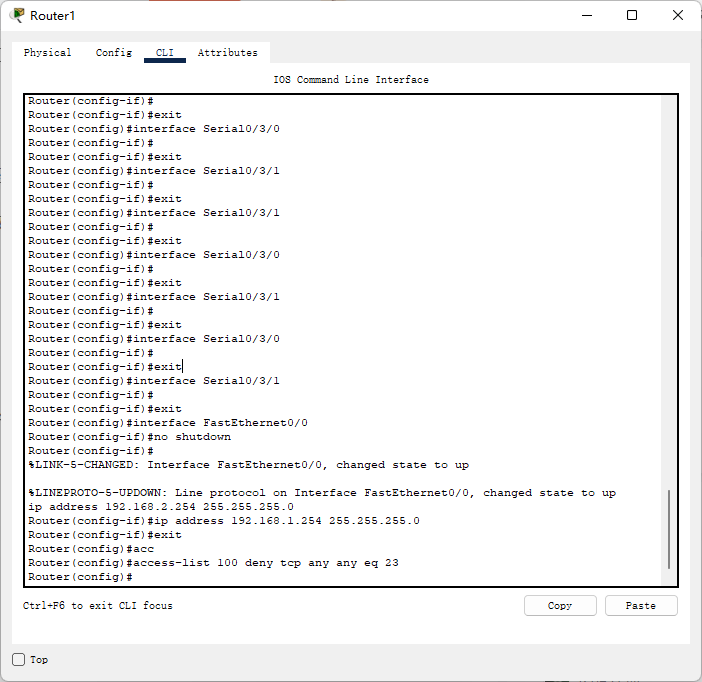
首先测试各主机能否登录到服务器

使用ping测试各PC与服务器都可通信，再使用telnet进行远程登录

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



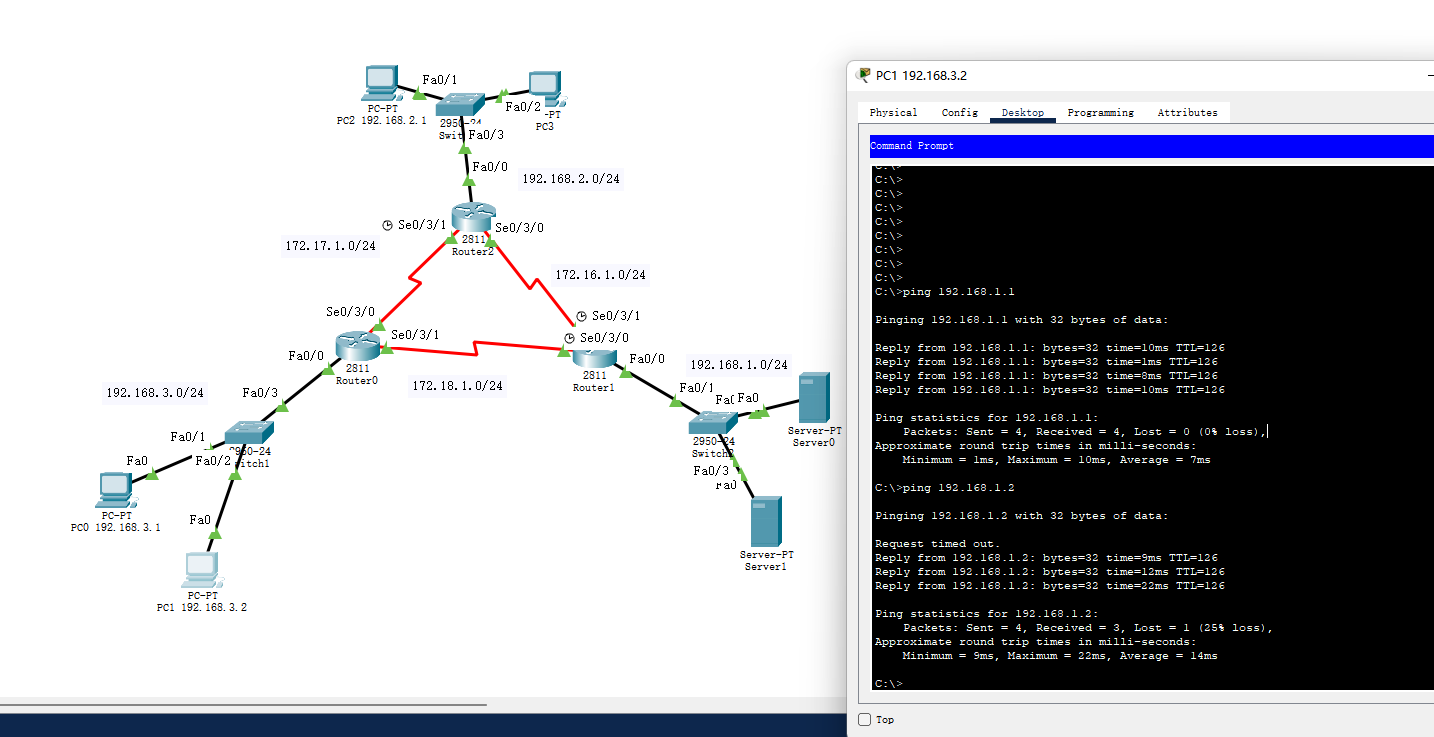
**b)**

1.实验内容：

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

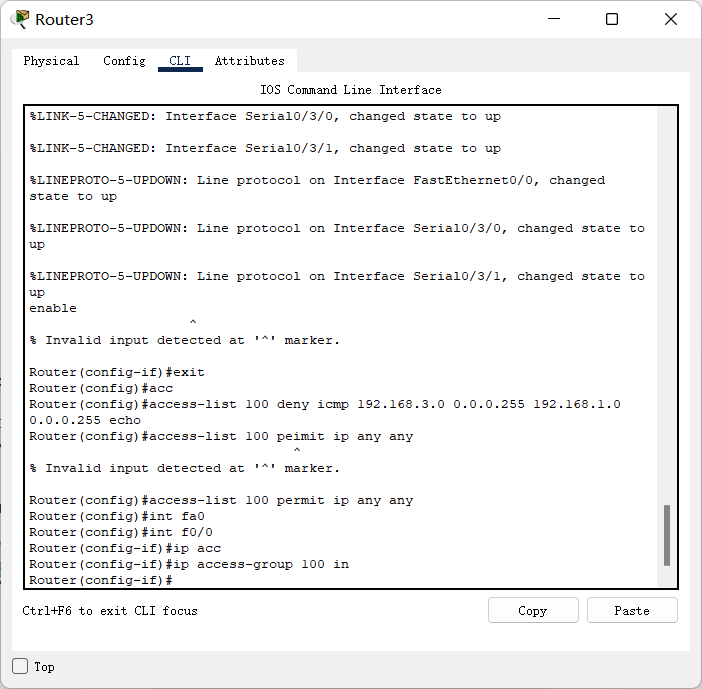
2.实验步骤：

配置ACL前，192.168.3.0/24网段中的主机与192.168.1.0/24网段的主机ping命令正常。



通过配置ACL拒绝192.168.3.0/24网段的Echo请求，阻止ping命令。用以下两条命令描述规则：

1. Router(config)#access-list 100 deny icmp 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 echo
2. Router(config)#access-list 100 peimit ip any any



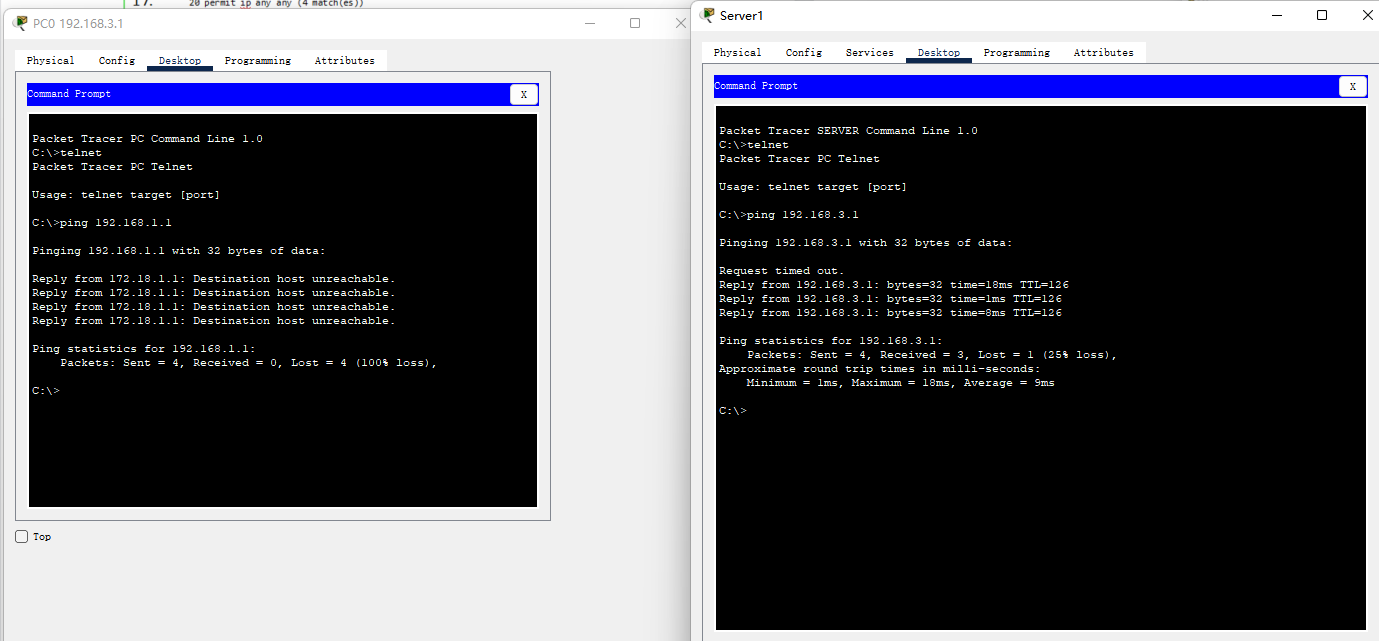
使用show ip access-lists查看配置的ACL规则，将其加入fa0/0端口的out中

完整的配置命令如下

1. Router(config-**if**)#exit
2. Router(config)#acc
3. Router(config)#access-list 100 deny icmp 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 echo
4. Router(config)#access-list 100 peimit ip any any
5. ^
6. % Invalid input detected at '^' marker.
8. Router(config)#access-list 100 permit ip any any
9. Router(config)#**int** fa0
10. Router(config)#**int** f0/0
11. Router(config-**if**)#ip acc
12. Router(config-**if**)#ip access-group 100 out
14. Router#show ip access-lists
15. Extended IP access list 100
16. 10 deny icmp 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 echo
17. 20 permit ip any any (4 match(es))

3.实验结果

192.168.3.0/24网段的PC无法与192.168.1.0/24网段的ping，而其他网段的仍正常，同时192.168.1.0/24网段PC可正常ping192.168.3.0/24网段。



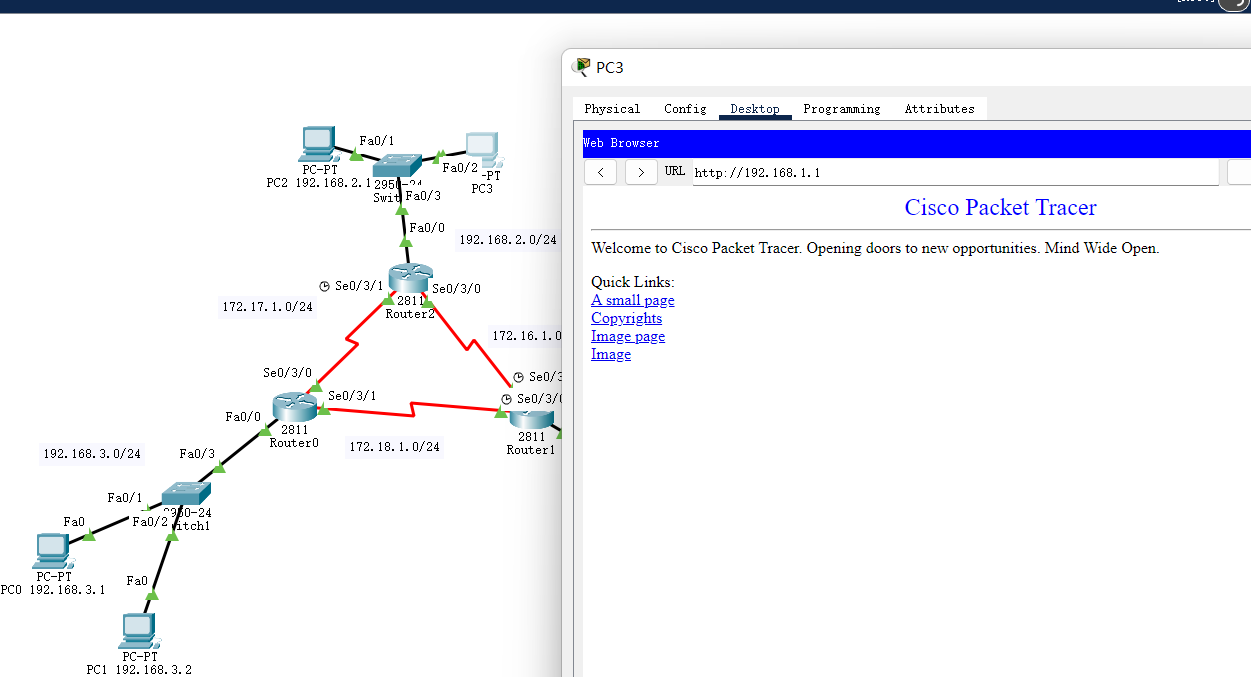
**c)**

1.实验内容：

禁止192.168.2.2主机访问HTTP协议

2.实验步骤：

初始条件下192.168.2.2可以正常http请求服务器



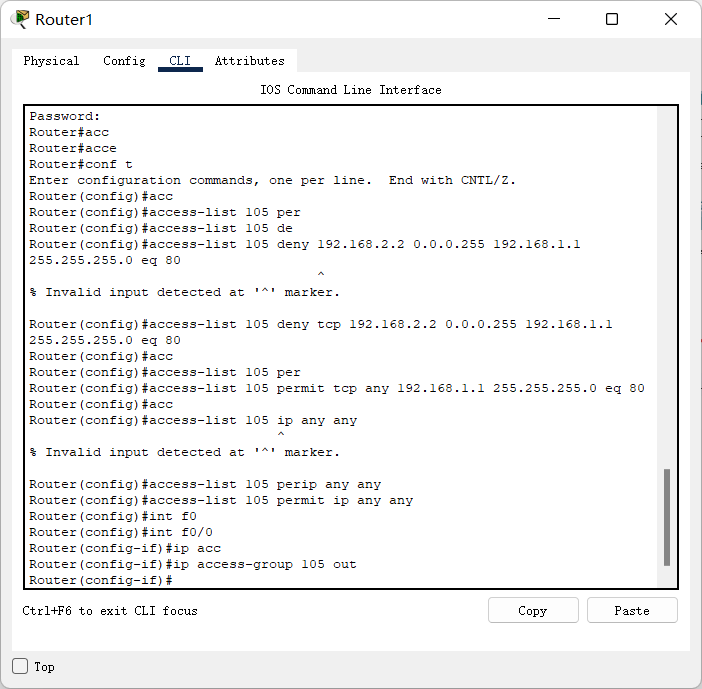
为路由器R1（服务器所在网段出口）配置ACL

配置规则如下

access-list 102 deny tcp 192.168.2.2 0.0.0.0 192.168.1.2 0.0.0.0 eq 80

access-list 102 permit ip any any

通过限制192.168.2.2访问192.168.1.2的80端口达到限制http协议的目的。

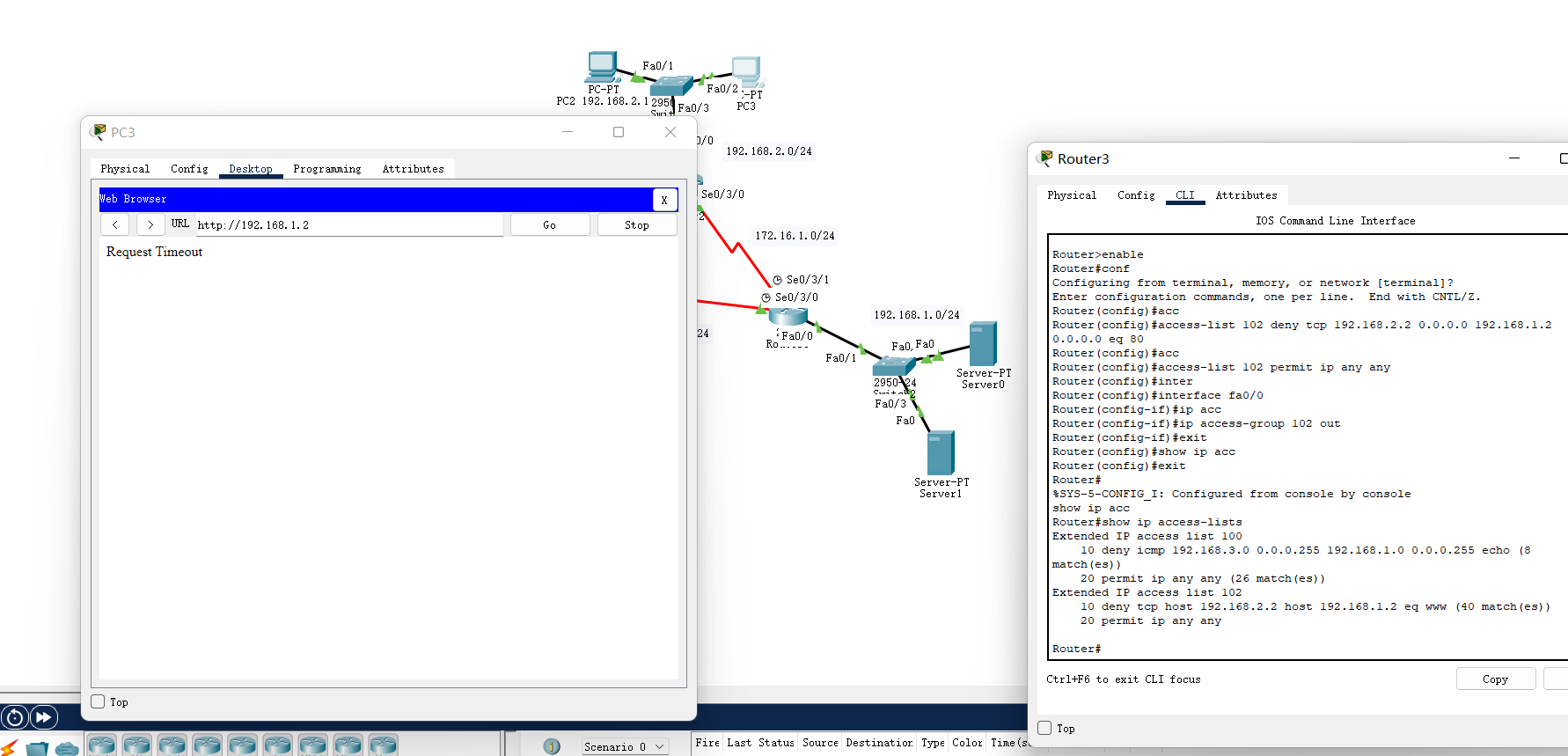


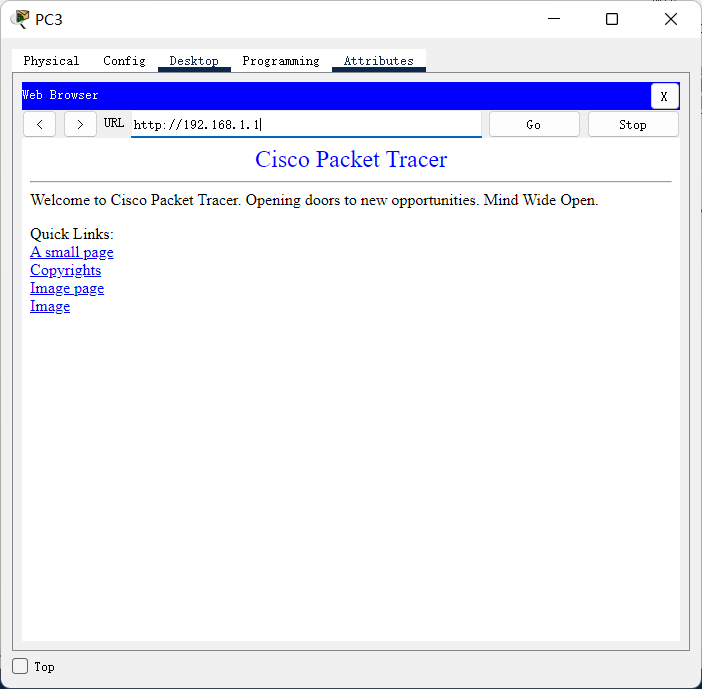
完整的配置命令如下：

1. Router>enable
2. Router#conf
3. Configuring from terminal, memory, or network [terminal]?
4. Enter configuration commands, one per line.  End with CNTL/Z.
5. Router(config)#acc
6. Router(config)#access-list 102 deny tcp 192.168.2.2 0.0.0.0 192.168.1.2 0.0.0.0 eq 80
7. Router(config)#acc
8. Router(config)#access-list 102 permit ip any any
9. Router(config)#inter
10. Router(config)#interface fa0/0
11. Router(config-**if**)#ip acc
12. Router(config-**if**)#ip access-group 102 out
13. Router(config-**if**)#exit
14. Router(config)#show ip acc
15. Router(config)#exit
16. Router#
17. %SYS-5-CONFIG\_I: Configured from console by console
18. show ip acc
19. Router#show ip access-lists
20. Extended IP access list 100
21. 10 deny icmp 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 echo (8 match(es))
22. 20 permit ip any any (26 match(es))
23. Extended IP access list 102
24. 10 deny tcp host 192.168.2.2 host 192.168.1.2 eq www (40 match(es))
25. 20 permit ip any any
27. Router#

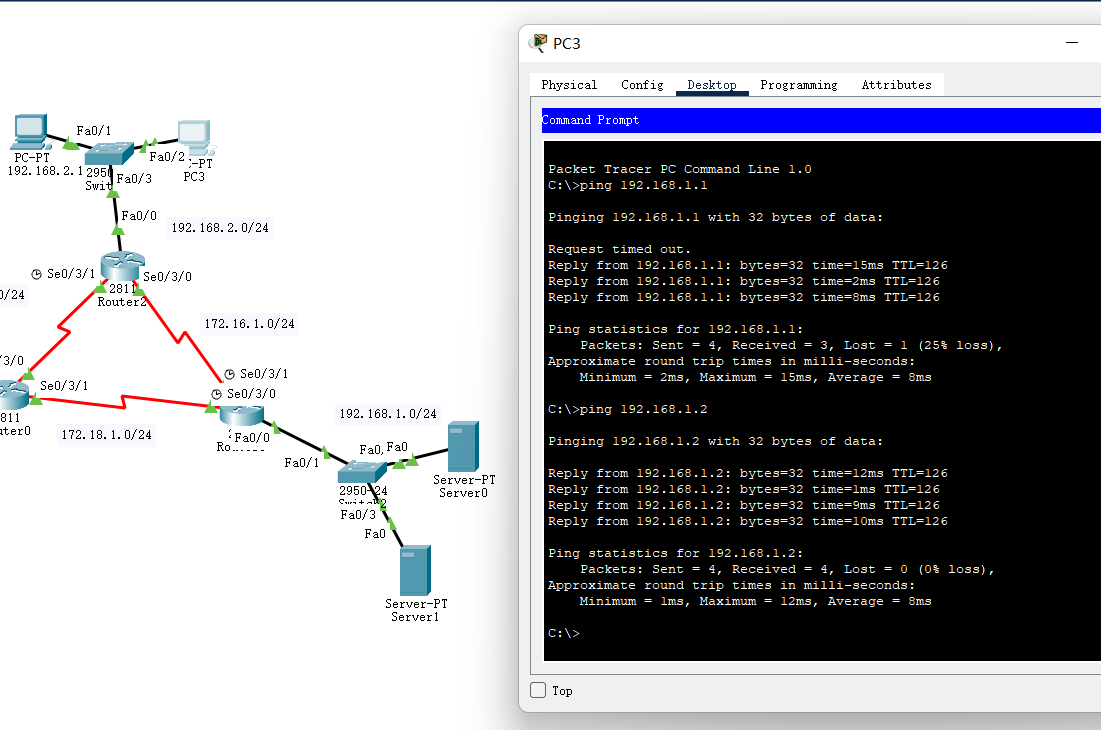
3.实验结果

配置完成后192.168.2.2无法再访问192.168.1.2的http协议而192.168.1.1的http协议仍能正常访问，其他PC机一切正常。





除了http协议的80端口，其他端口的协议（如ping）仍正常。



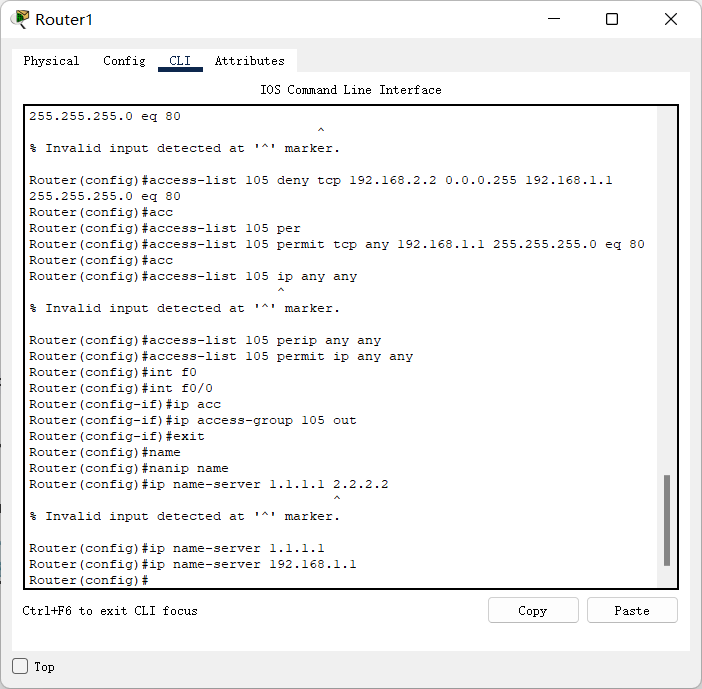
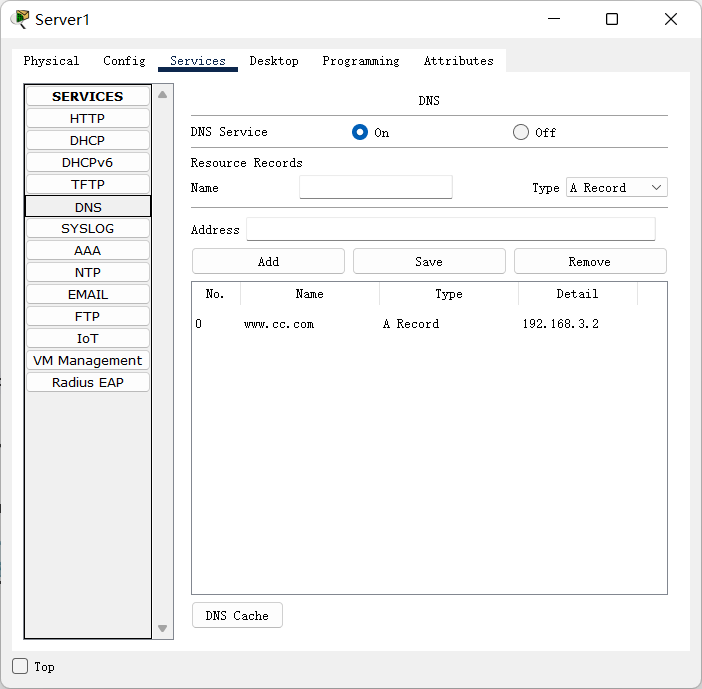
**d)**

1.实验内容：

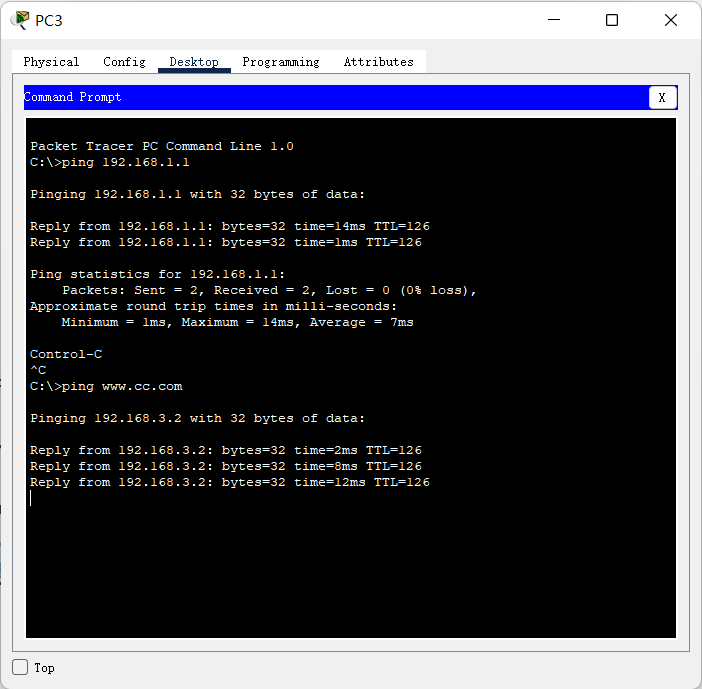
禁止192.168.2.3主机访问DNS协议

2.实验步骤：

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



DNS协议使用的是UDP，在53号端口上进行，因此如此配置ACL规则

access-list <ACL\_NUMBER> permit ip 192.168.2.3 0.0.0.0 192.168.1.1 0.0.0.0

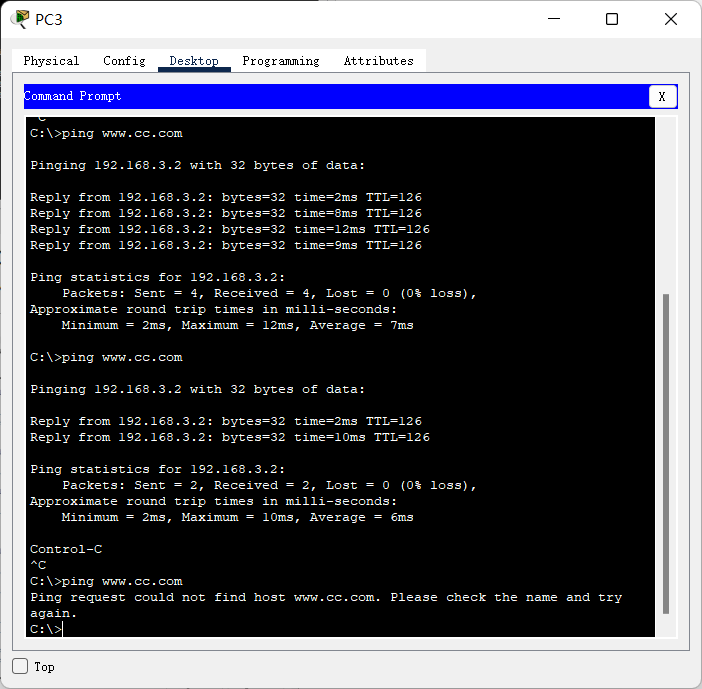
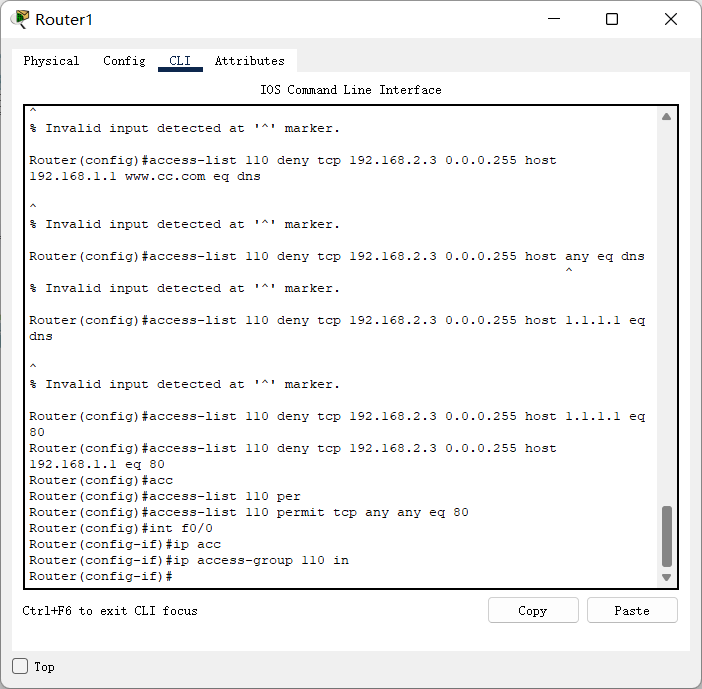
access-list <ACL\_NUMBER> permit ip any any

完整的配置命令如下

1. Router>enable
2. Router#conf
3. Configuring from terminal, memory, or network [terminal]?
4. Enter configuration commands, one per line.  End with CNTL/Z.
5. Router(config)#acc
6. Router(config)#access-list 104 deny ip 192.168.2.3 0.0.0.0 192.168.1.1 0.0.0.0
7. Router(config)#acc
8. Router(config)#access-list 104 permit ip any any
9. Router(config)#inter
10. Router(config)#interface fa0/0
11. Router(config-**if**)#ip acc
12. Router(config-**if**)#ip access-group 104 out
13. Router(config-**if**)#exit
14. Router(config)#show ip acc
15. Router(config)#exit
16. Router#
17. %SYS-5-CONFIG\_I: Configured from console by console

3.实验结果

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仍可正常解析，实验完成。



1. 体会和收获

在本次实验学习配置ACL的过程中，我认识到了ACL是一种非常强大且灵活的工具，可以用来控制网络流量。我在本次实验中配置了几条ACL，并通过使用不同的指令和参数来实现不同的限制效果。

通过配置ACL，我学会了如何控制网络中的流量，并能够根据不同的需求对特定主机或网络进行访问限制。我认为这些技术非常有价值，因为它们可以帮助我更好地管理网络，保护数据安全。

此外，我还进行了一些额外的尝试，了解更多关于ACL的技术知识。我尝试了使用不同的协议和端口来限制访问，并学习了如何应用ACL到路由器的多个端口上。这些尝试让我对ACL的功能和使用方法有了更深入的理解。我认为，这些知识和经验将在我从事网络管理工作时大有裨益。