

《计算机网络课程实验》

实验报告



姓名：

陈驰

学号：

2021303090

班级：

SC012101

日期：

2023/1/1

西北工业大学网络空间安全学院

2022 年 11 月

目录

实验 5

一、实验题目和目的	2
二、实验具体内容与步骤	2
a)	2
1. 实验内容	2
2. 实验步骤:	2
3. 实验结果	4
b)	5
1. 实验内容	5
2. 实验步骤:	5
3. 实验结果	7
c)	7
1. 实验内容	7
2. 实验步骤:	7
3. 实验结果	9
d)	10
1. 实验内容	10
2. 实验步骤:	11
3. 实验结果	12

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：

- i. 限制所有主机远程登录到服务器
- ii. 禁止 192.168.3.0/24 网段中的主机 Ping 192.168.1.0/24 网段
- iii. 禁止 192.168.2.2 主机访问 HTTP 协议
- iv. 禁止 192.168.2.3 主机访问 DNS 协议

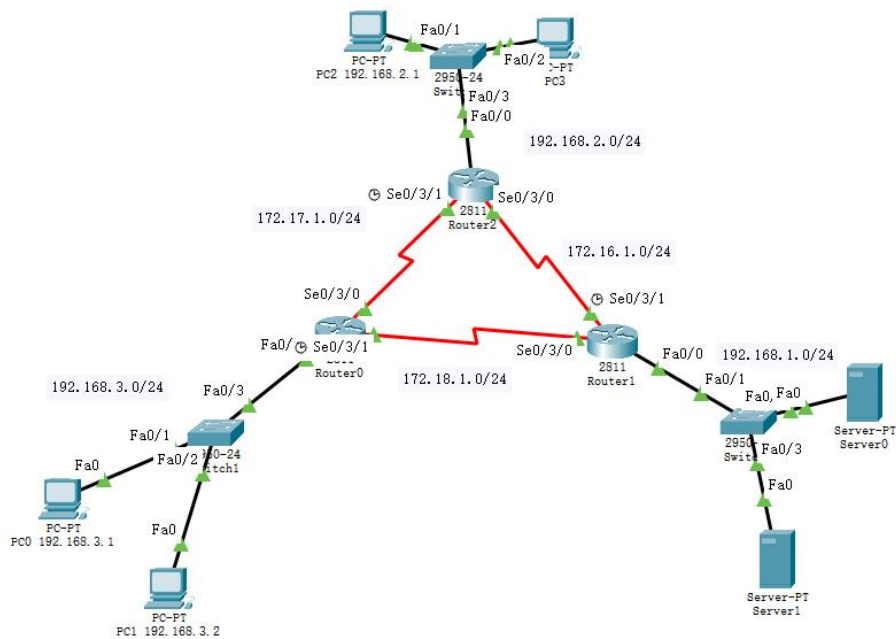
a)

1. 实验内容：

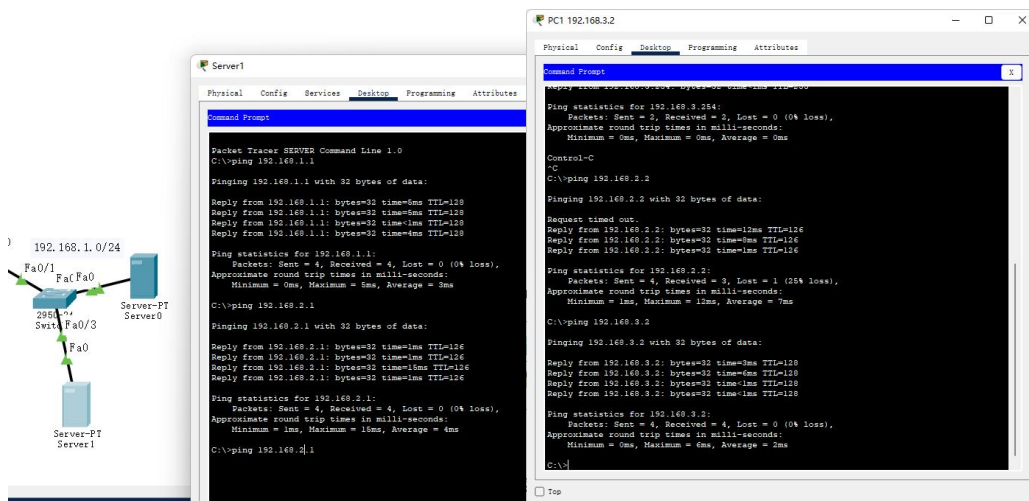
限制所有主机远程登录到服务器

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

使用 ping 测试各 PC 与服务器都可通信，并开通服务器 192.168.1.1 的 telnet 服务。

Telnet 使用 tcp 协议，在 23 端口上执行，因此配置 ACL 时只需要禁止任何向 192.168.1.1 的 23 端口传输的 tcp 报文即可。

配置指令如下：

access-list 100 deny tcp any host 192.168.1.1 eq 23

access-list 100 permit ip any any

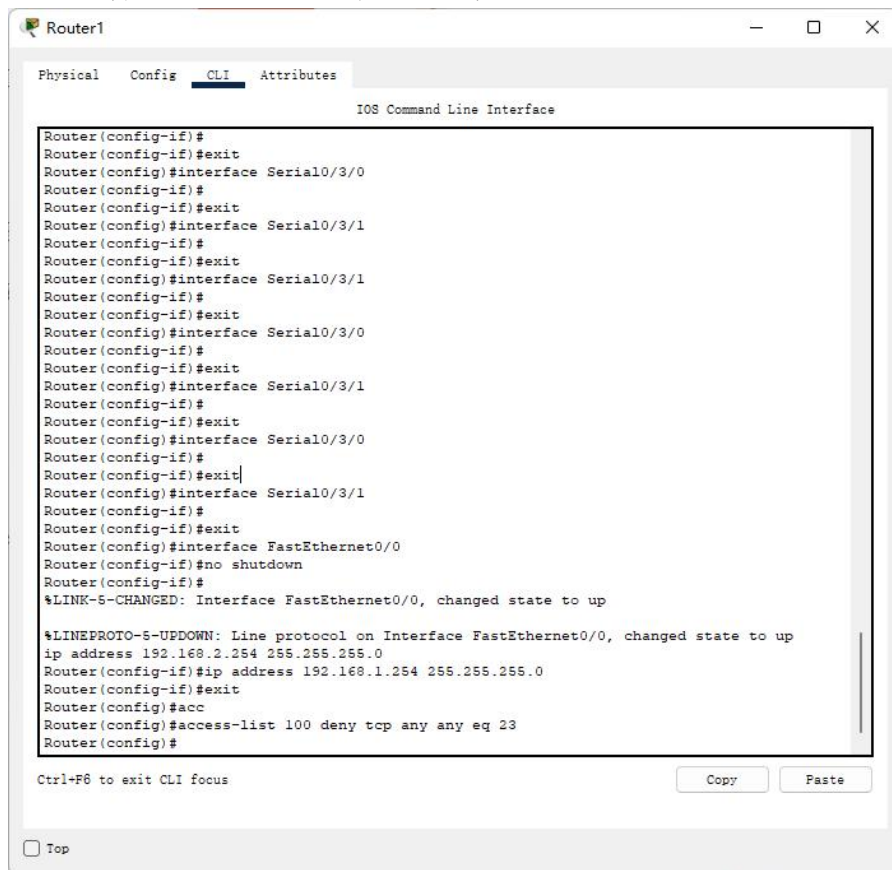
完整的配置命令如下

1. Router(config-if)#exit
2. Router(config)#acc
3. Router(config)#access-list 100 deny tcp any host 192.168.1.1 eq 23

4. Router(config)#access-list 100 peimit ip any any
5. Router(config)#access-list 100 permit ip any any
6. Router(config)#int fa0
7. Router(config)#int f0/0
8. Router(config-if)#ip acc
9. Router(config-if)#ip access-group 100 out
- 10.
11. Router#show ip access-lists
12. Extended IP access list 100
13. 10 deny tcp any host 192.168.1.1 eq 23
14. 20 permit ip any any (4 match(es))

3. 实验结果

配置路由器的 ACL，禁止所有 ip 与服务器 192.168.1.1 的 23 端口进行 TCP，可以看到此时 PC 能与路由器通信但无法进行远程登录



```
Router1
Physical Config CLI Attributes
IOS Command Line Interface

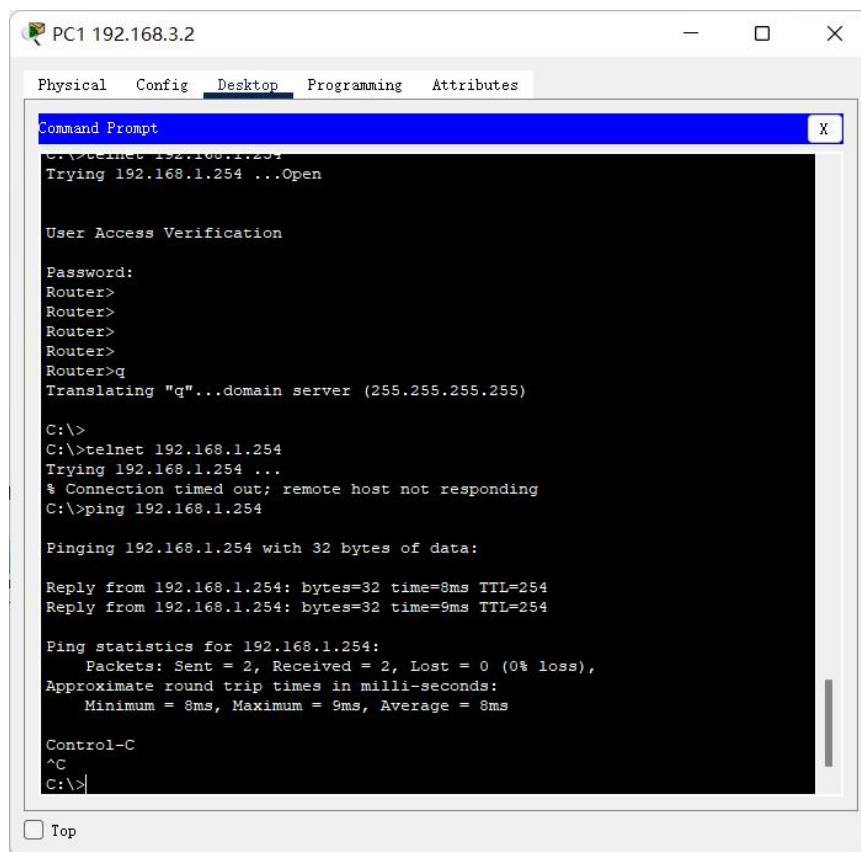
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/3/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/3/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/3/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/3/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/3/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/3/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/3/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
ip address 192.168.2.254 255.255.255.0
Router(config-if)#ip address 192.168.1.254 255.255.255.0
Router(config-if)#exit
Router(config)#acc
Router(config)#access-list 100 deny tcp any any eq 23
Router(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top



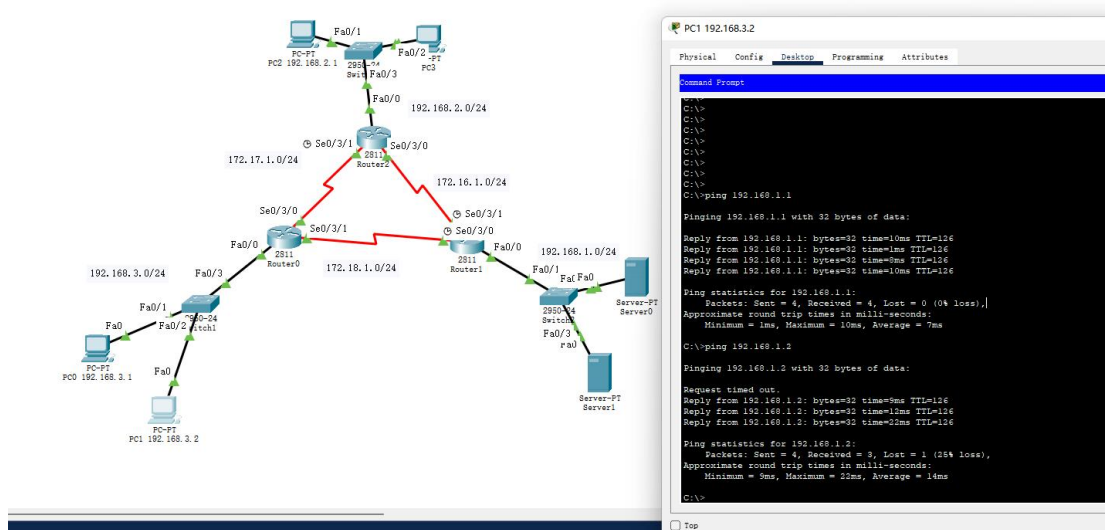
b)

1. 实验内容:

禁止 192.168.3.0/24 网段中的主机 Ping 192.168.1.0/24 网段

2. 实验步骤:

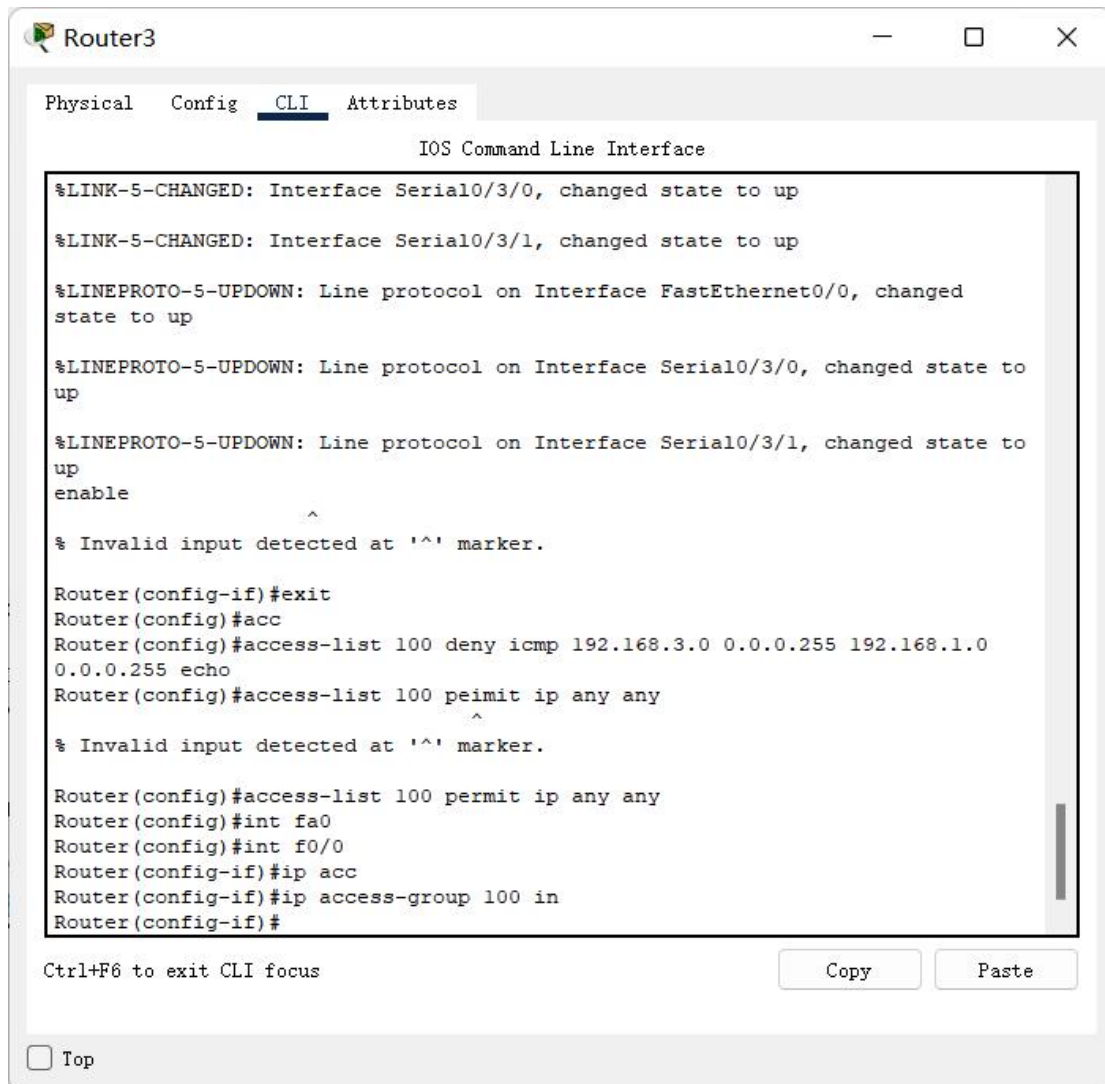
配置 ACL 前, 192.168.3.0/24 网段中的主机与 192.168.1.0/24 网段的主机 ping 命令正常。



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：

15. Router(config)#access-list 100 deny icmp 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 echo
16. Router(config)#access-list 100 permit 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

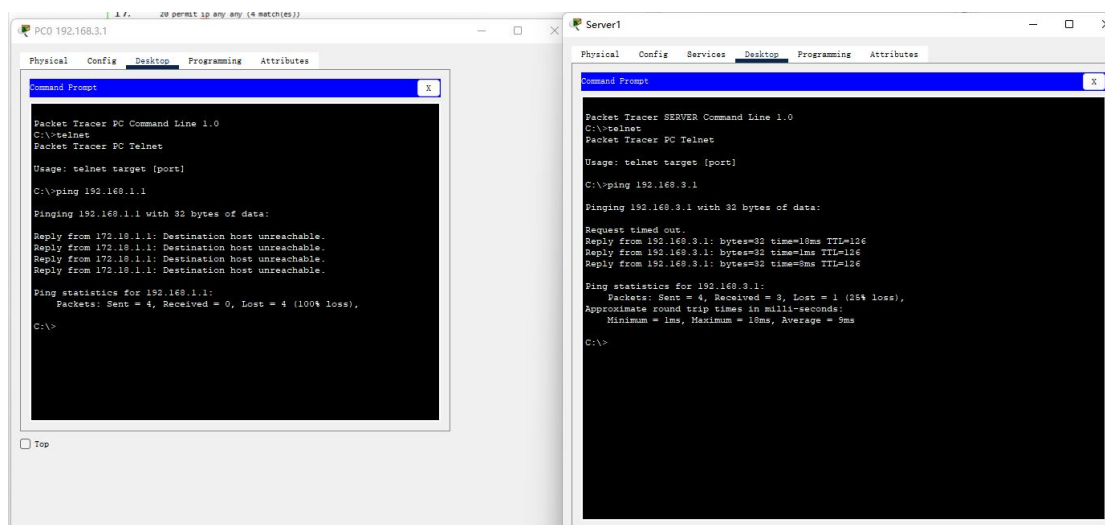
完整的配置命令如下

17. Router(config-if)#exit
18. Router(config)#acc
19. Router(config)#access-list 100 deny icmp 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 echo
20. Router(config)#access-list 100 peimit ip any any
21. ^
22. % Invalid input detected at '^' marker.
- 23.
24. Router(config)#access-list 100 permit ip any any
25. Router(config)#int fa0
26. Router(config)#int f0/0

```
27. Router(config-if)#ip acc
28. Router(config-if)#ip access-group 100 out
29.
30. Router#show ip access-lists
31. Extended IP access list 100
32. 10 deny icmp 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255 echo
33. 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 ping 192.168.3.0/24 网段。



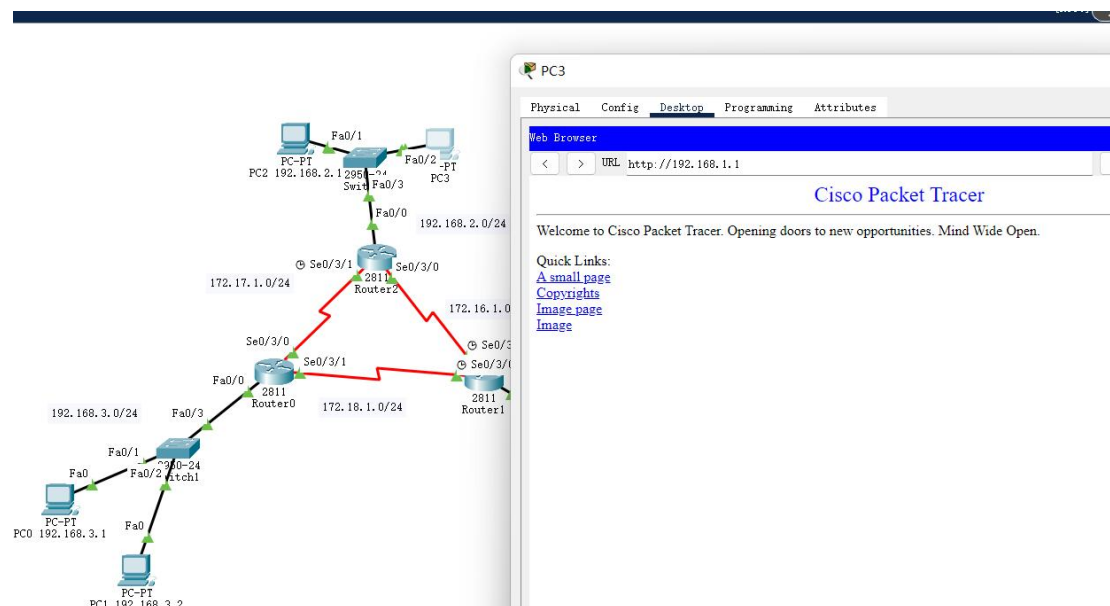
c)

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

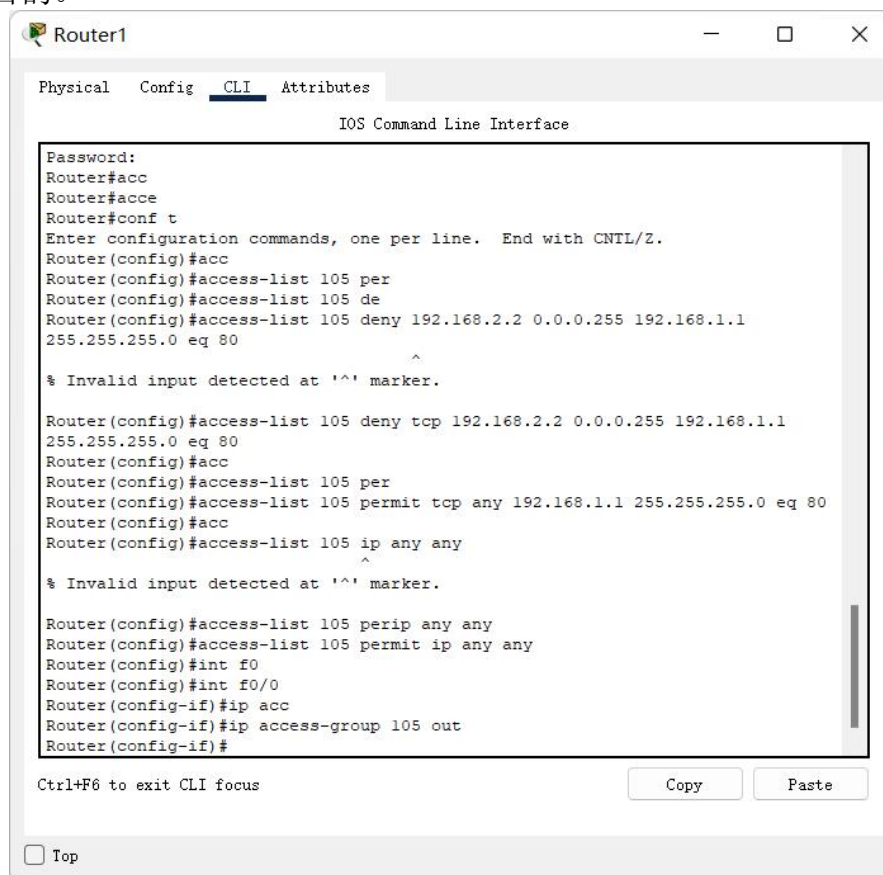


为路由器 R1（服务器所在网段出口）配置 ACL
配置规则如下

```
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。

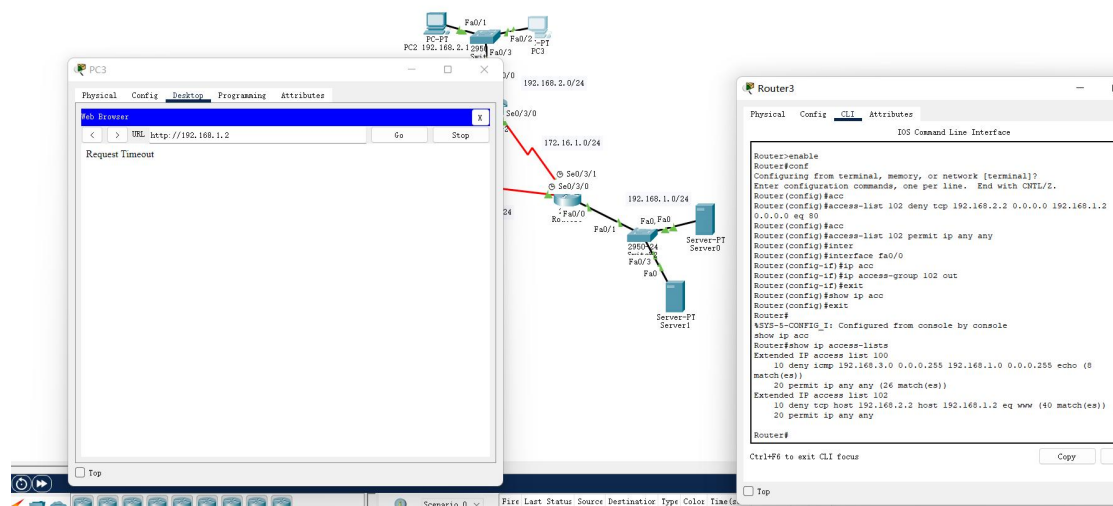


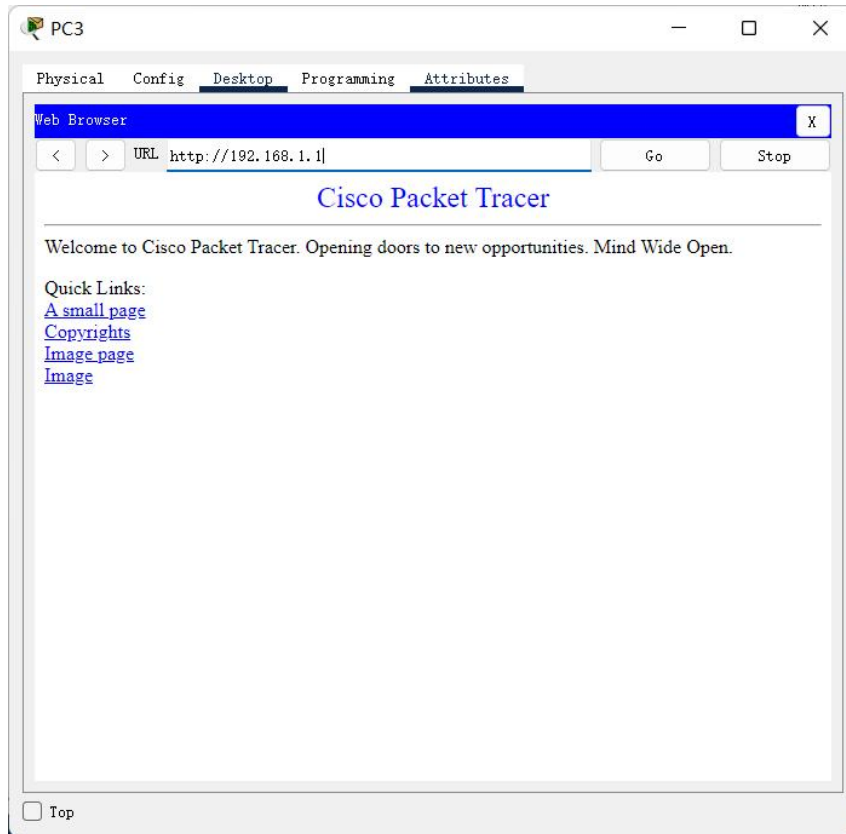
完整的配置命令如下：

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
- 26.
27. Router#

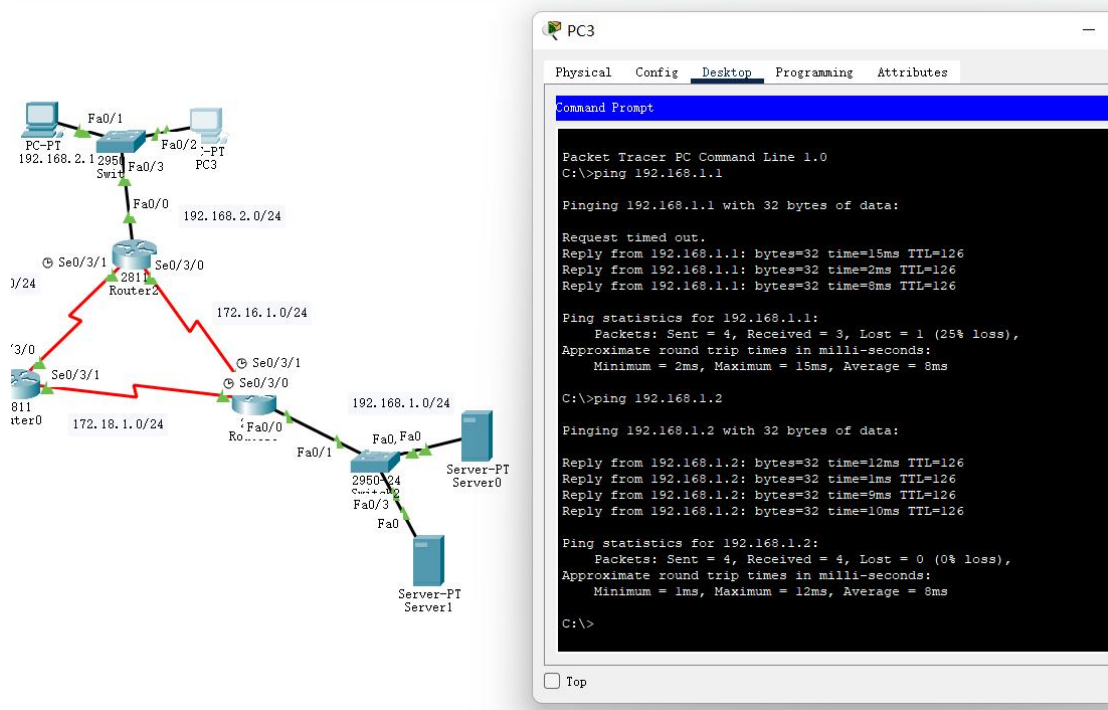
3. 实验结果

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。



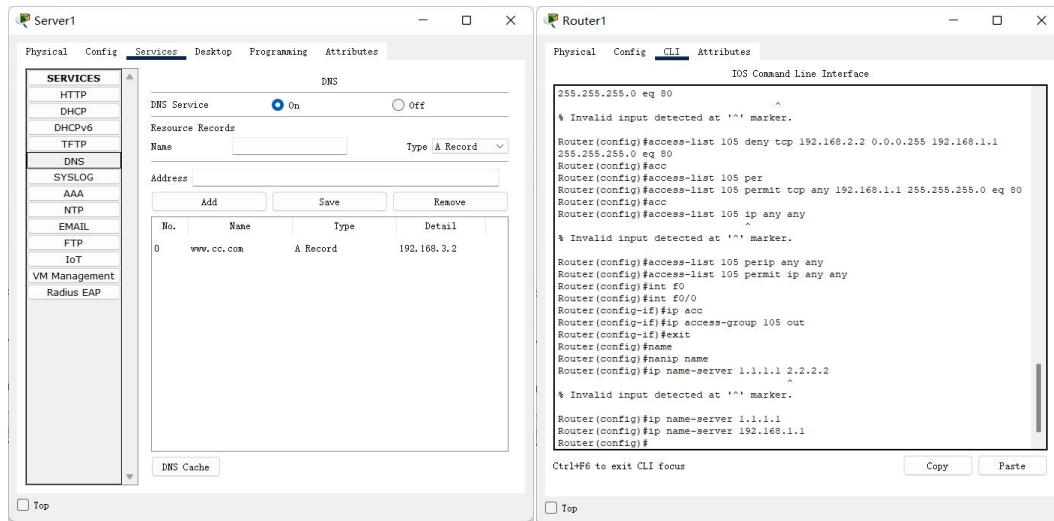
d)

1. 实验内容：

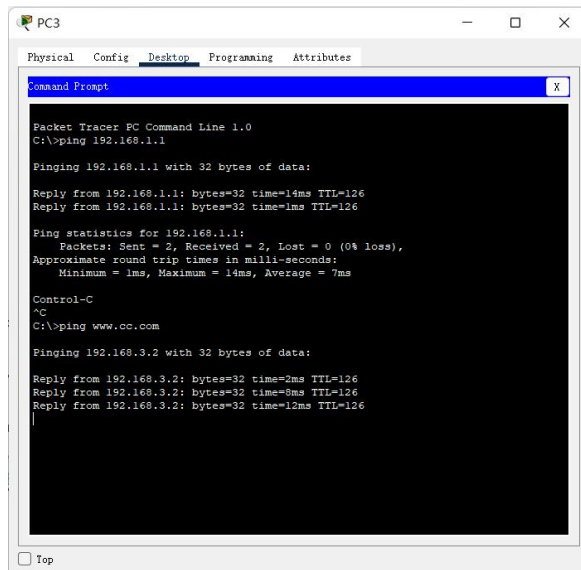
禁止 192.168.2.3 主机访问 DNS 协议

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
```

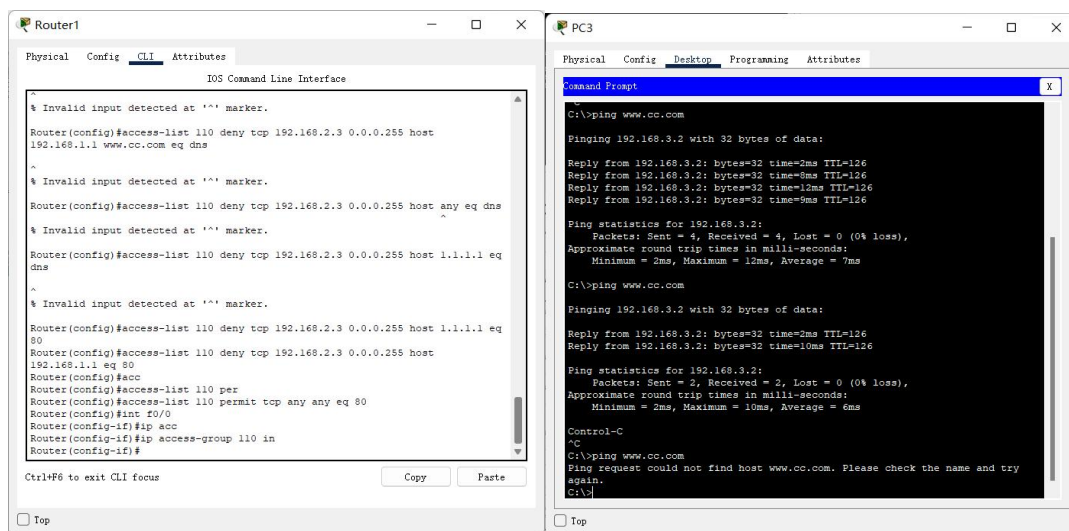
完整的配置命令如下

28. Router>enable
29. Router#conf
30. Configuring from terminal, memory, or network [terminal]?
31. Enter configuration commands, one per line. End with CNTL/Z.
32. Router(config)#acc
33. Router(config)#access-list 104 deny ip 192.168.2.3 0.0.0.0 192.168.1.1 0.0.0.0
34. Router(config)#acc
35. Router(config)#access-list 104 permit ip any any

```
36. Router(config)#inter
37. Router(config)#interface fa0/0
38. Router(config-if)#ip acc
39. Router(config-if)#ip access-group 104 out
40. Router(config-if)#exit
41. Router(config)#show ip acc
42. Router(config)#exit
43. Router#
44. %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。



三、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。