

# 西安电子科技大学

## 物联网安全实验课程 实验报告

### 实验名称 ACL 配置实验

物联网工程 1803041 班

姓名 魏红旭 学号 18030400014

同作者

实验日期 2021 年 5 月 25 日

成 绩

指导教师评语：

指导教师：

年月日

### 实验报告内容基本要求及参考格式

- 一、实验目的
- 二、实验所用仪器（或实验环境）
- 三、实验基本原理及步骤（或方案设计及理论计算）
- 四、实验数据记录（或仿真及软件设计）
- 五、实验结果分析及回答问题（或测试环境及测试结果）

## 一、实验目的：

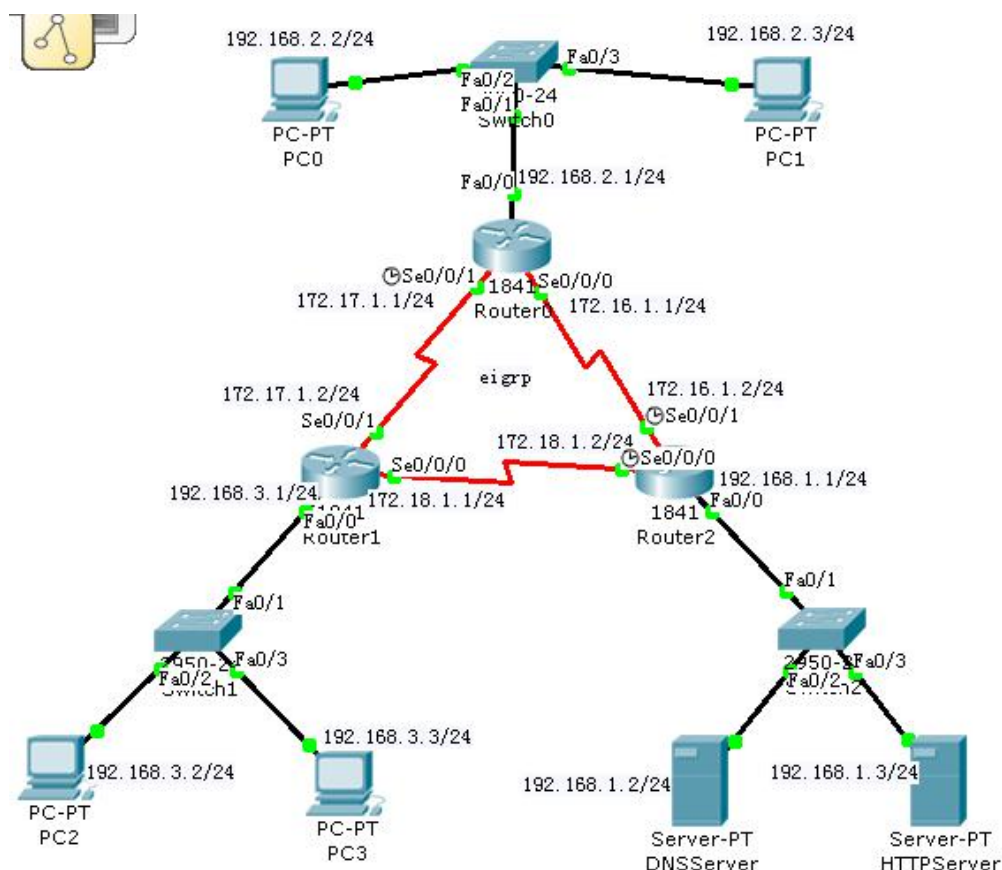
深入理解用 ACL 实现访问控制的工作原理

## 二、实验所用仪器（或实验环境）

计算机科学与技术学院实验中心，可接入 Internet 网台式机 44 台。

## 三、实验基本原理及要求

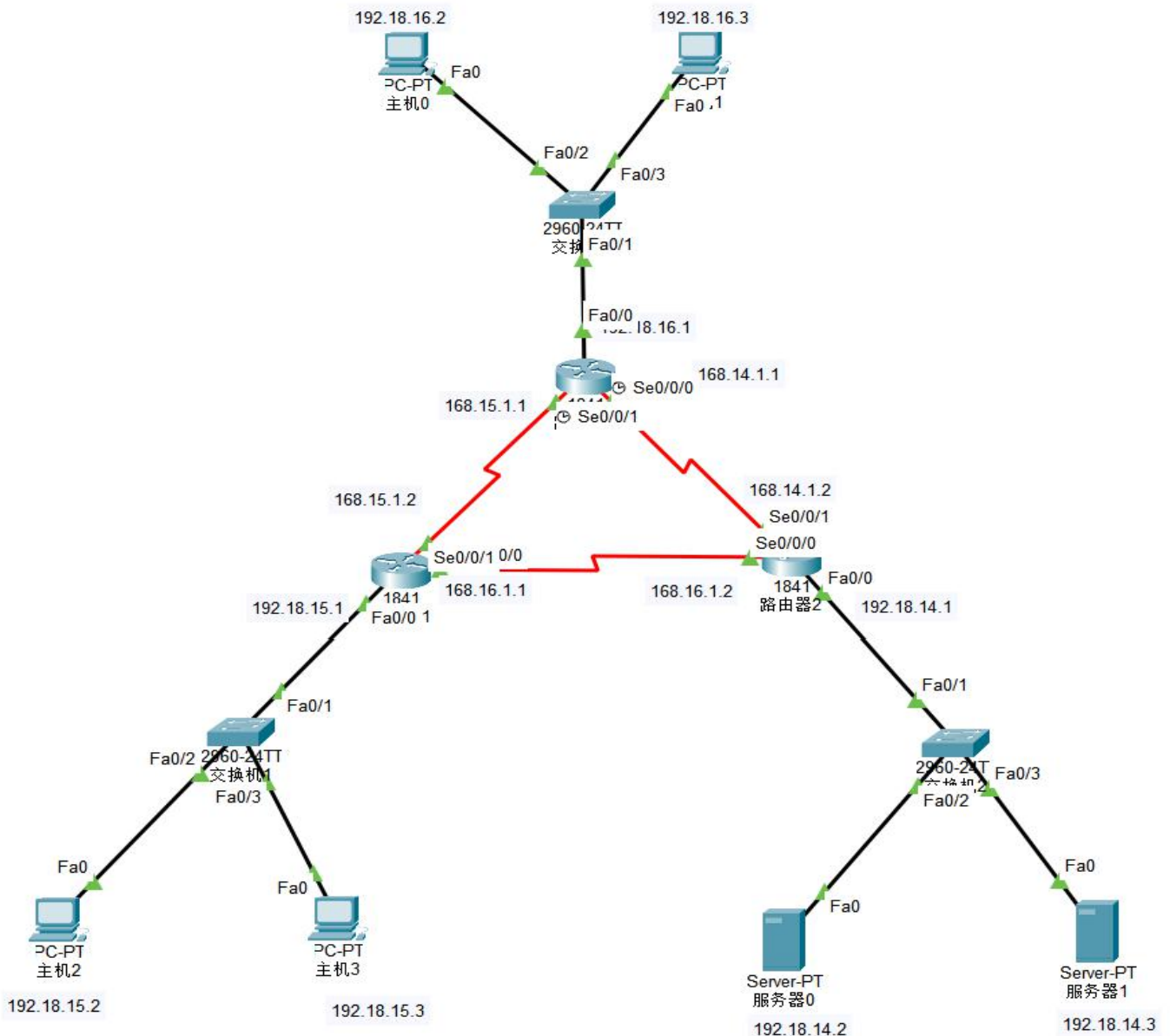
拓扑结构如下图所示(要求：跟拓扑上的 ip 地址配置不同)



- 1、配置 ACL 限制远程登录（telnet）到路由器的主机。  
路由器 R0 只允许 192.168.2.2 远程登录(telnet)。
- 2、配置 ACL 禁止 192.168.3.0/24 网段的 icmp 协议数据包通向与 192.168.1.0/24 网段。
- 3、配置 ACL 禁止特点的协议端口通讯。  
禁止 192.168.2.2 使用 www (80)端口访问 192.168.1.0  
禁止 192.168.2.3 使用 dns (53)端口访问 192.168.1.0
- 3、验证 ACL 规则,检验并查看 ACL。

## 四、实验步骤及实验数据记录：（要有文字描述和必要截图）

- 网络拓扑图如下图所示，ip 地址在图中已注明：



# 1. 配置 ACL 限制远程登录 (telnet) 到路由器的主机。路由器 R0 只允许 192.18.16.2 远程登录(telnet)。在上图的拓扑中就是路由器 R0 只允许 192.18.16.2 远程登录(telnet)

首先允许 192.18.16.2 通过 23 端口(也就是 telnet)访问路由器上的 192.18.16.1, 并且禁止其他主机通过 23 端口访问路由器上的 192.18.16.1。最后将 acl 表绑定在 fa 0/0 上, 这样就只允许 192.18.16.2 通过 telnet 访问路由器了, 需要在路由器 0 中输入如下命令:

```
access-list 100 permit tcp host 192.18.16.2 host 192.18.16.1 eq 23
access-list 100 deny tcp any host 192.18.16.1 eq 23
access-list 100 permit icmp any any
interface fa0/0
ip access-group 100 in
```

2. **配置 ACL 禁止 192.168.3.0/24 网段的 icmp 协议数据包通向与 192.168.1.0/24 网段。**  
在上图的拓扑中就是配置 ACL 禁止 192.18.15.0/24 网段的 icmp 协议数据包通向与 192.18.14.0/24 网段

同样我们只需要通过 acl 表的命令,就可以不允许 192.18.15.0/24 通过 icmp 协议 ping 192.168.14.0/24, 我们需要在路由器 1 中进行如下配置:

```
access-list 101 deny icmp 192.18.15.0 0.0.0.255 192.18.14.0 0.0.0.255
access-list 101 permit icmp any any
access-list 101 permit ip any any
access-list 101 permit tcp any any
interface se 0/0/0
ip access-group 101 out
```

3. **配置 ACL 禁止特点的协议端口通讯。**  
**禁止 192.168.2.2 使用 www (80)端口访问 192.168.1.0**  
**禁止 192.168.2.3 使用 dns (53)端口访问 192.168.1.0**  
在上图的拓扑中就是  
**禁止 192.18.16.2 使用 www (80)端口访问 192.18.14.0**  
**禁止 192.18.16.3 使用 dns (53)端口访问 192.18.14.0**

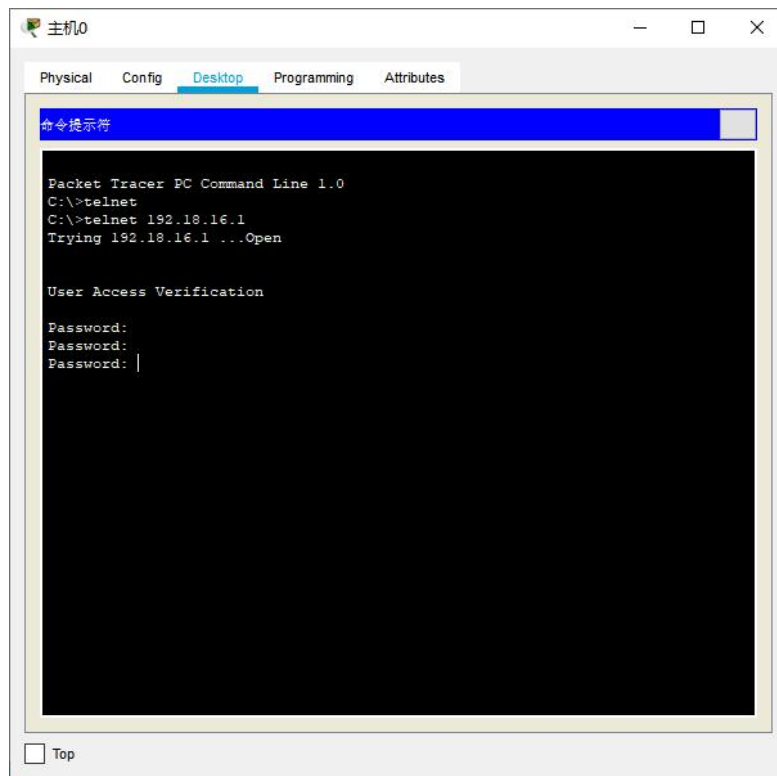
我们可以通过 host 192.168.2.2 指定特定 ip 的主机, 设置其是否允许通过某一个端口访问某一个网段, 同样的对 192.168.2.3 也是相同的操作, 最后我们只需要将 acl 表绑定在路由器 2 和 192.18.14.0/24 网段的端口之上即可实现题目要求的功能。我们需要在路由器 2 中进行如下配置:

```
access-list 100 deny tcp host 192.18.16.2 192.18.14.0 0.0.0.255 eq 80
access-list 100 deny tcp host 192.18.16.3 192.18.14.0 0.0.0.255 eq 53
access-list 100 permit ip any any
access-list 100 permit tcp any any
access-list 100 permit icmp any any
interface fa0/0
ip access-group 100 out
```

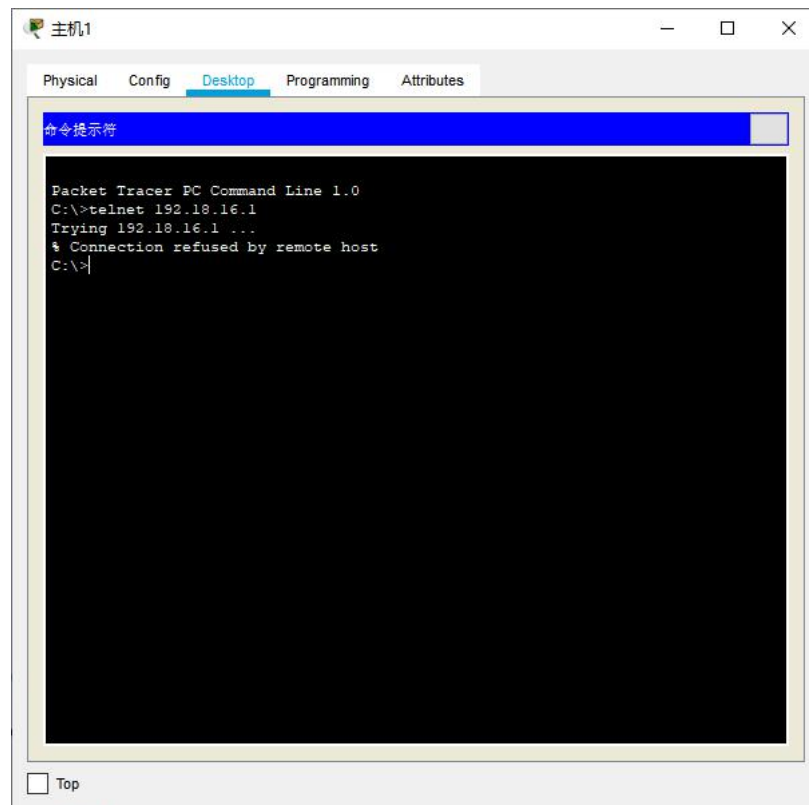
## 五、实验结果分析及实验总结与体会

1. **配置 ACL 限制远程登录 (telnet) 到路由器的主机。路由器 R0 只允许 192.168.2.2 远程登录(telnet)。**在上图的拓扑中就是路由器 R0 只允许 192.18.16.2 远程登录(telnet), 实验结果如下图所示:

- 主机 0 可以远程登陆 telnet

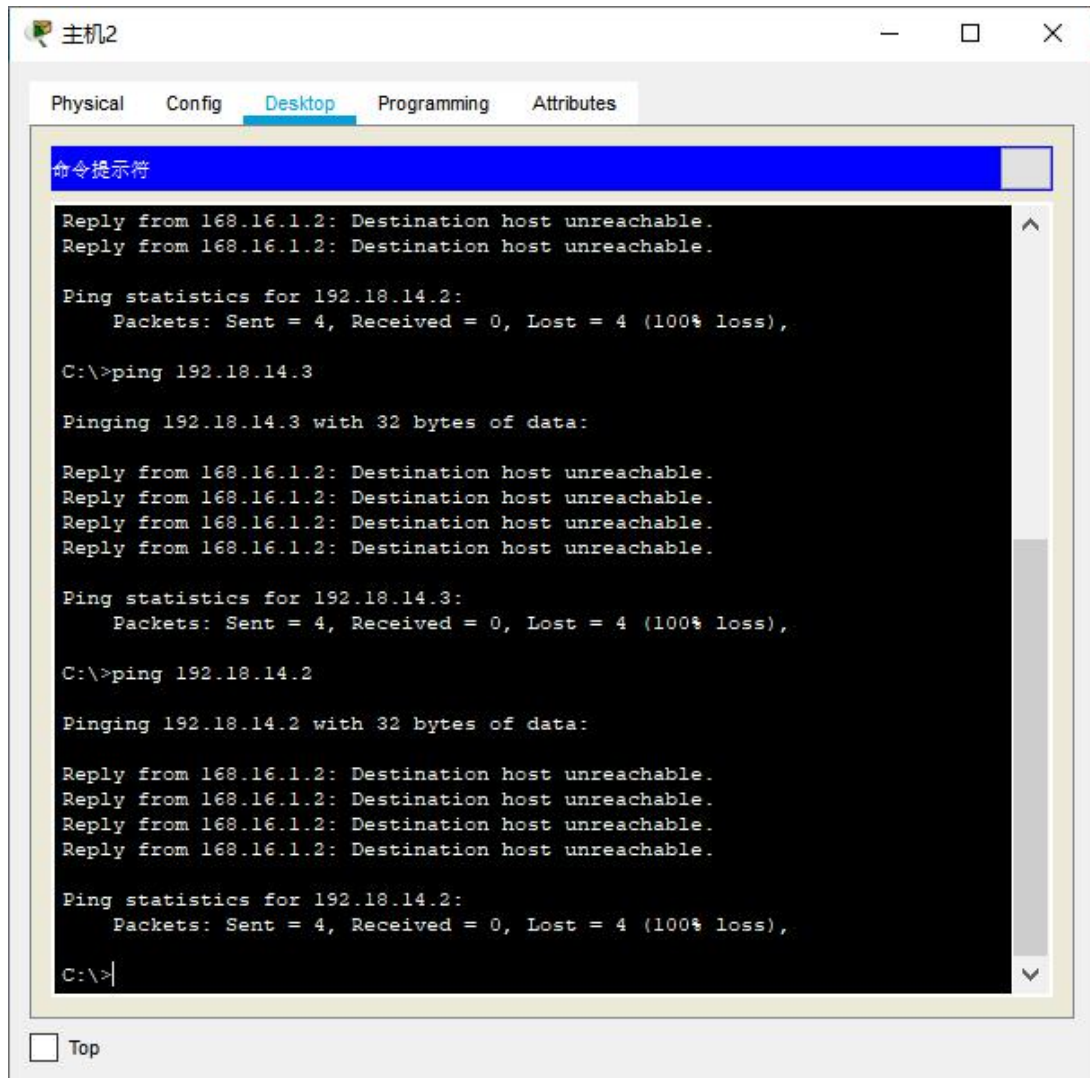


- 主机 1 无法远程登陆 telnet



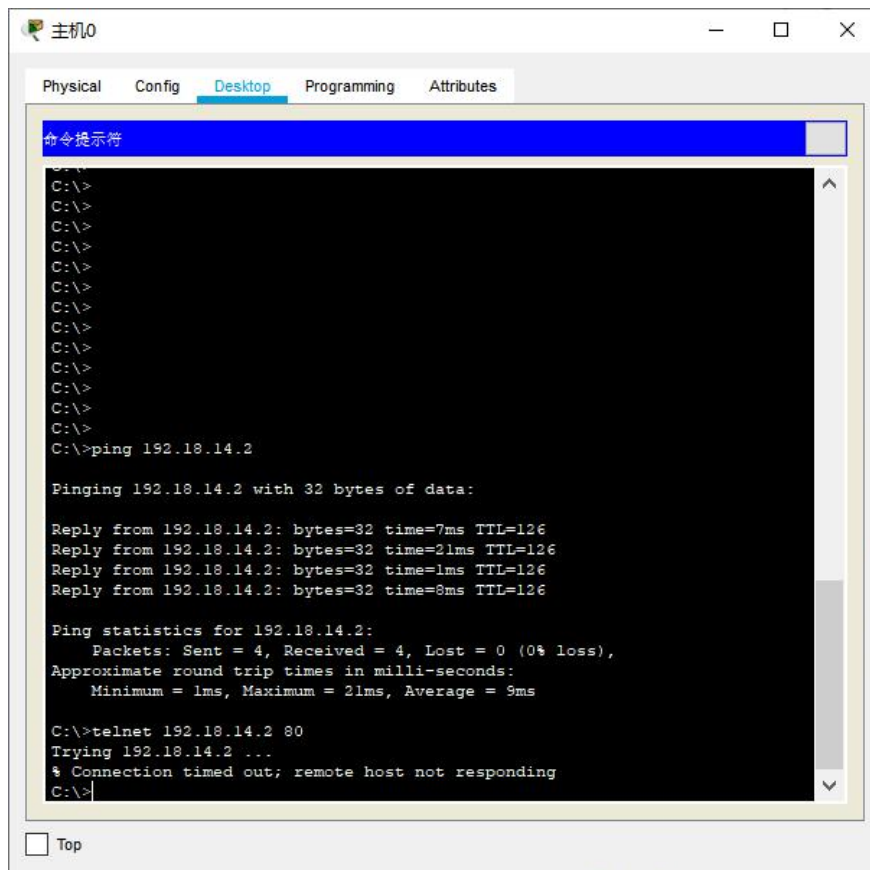
2. 配置 ACL 禁止 192.168.3.0/24 网段的 icmp 协议数据包通向与 192.168.1.0/24 网段。  
在上图的拓扑中就是配置 ACL 禁止 192.18.15.0/24 网段的 icmp 协议数据包通向与 192.18.14.0/24 网段

- 主机 2 无法 ping 通 192.18.14.0/24 网段



3. 配置 ACL 禁止特点的协议端口通讯。
- 禁止 192.168.2.2 使用 www (80)端口访问 192.168.1.0
- 禁止 192.168.2.3 使用 dns (53)端口访问 192.168.1.0
- 在上图的拓扑中就是
- 禁止 192.18.16.2 使用 www (80)端口访问 192.18.14.0
- 禁止 192.18.16.3 使用 dns (53)端口访问 192.18.14.0

- 192.18.16.2 可以 ping 通 192.18.14.2, 但是无法使用 www (80)端口访问 192.18.14.2



```
命令提示符
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.18.14.2

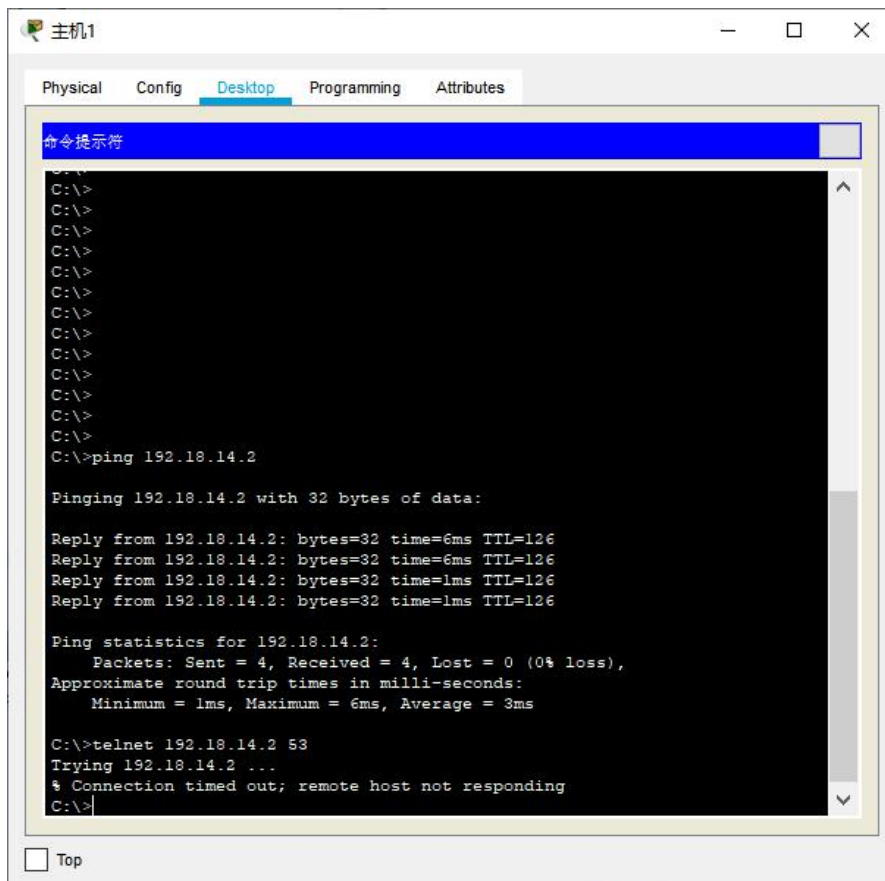
Pinging 192.18.14.2 with 32 bytes of data:

Reply from 192.18.14.2: bytes=32 time=7ms TTL=126
Reply from 192.18.14.2: bytes=32 time=21ms TTL=126
Reply from 192.18.14.2: bytes=32 time=1ms TTL=126
Reply from 192.18.14.2: bytes=32 time=8ms TTL=126

Ping statistics for 192.18.14.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 21ms, Average = 9ms

C:\>telnet 192.18.14.2 80
Trying 192.18.14.2 ...
% Connection timed out; remote host not responding
C:\>
```

- 192.18.16.3 可以 ping 通 192.18.14.2, 但是无法使用 dns (53)端口访问 192.18.14.2



```
命令提示符
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>
C:\>ping 192.18.14.2

Pinging 192.18.14.2 with 32 bytes of data:

Reply from 192.18.14.2: bytes=32 time=6ms TTL=126
Reply from 192.18.14.2: bytes=32 time=6ms TTL=126
Reply from 192.18.14.2: bytes=32 time=1ms TTL=126
Reply from 192.18.14.2: bytes=32 time=1ms TTL=126

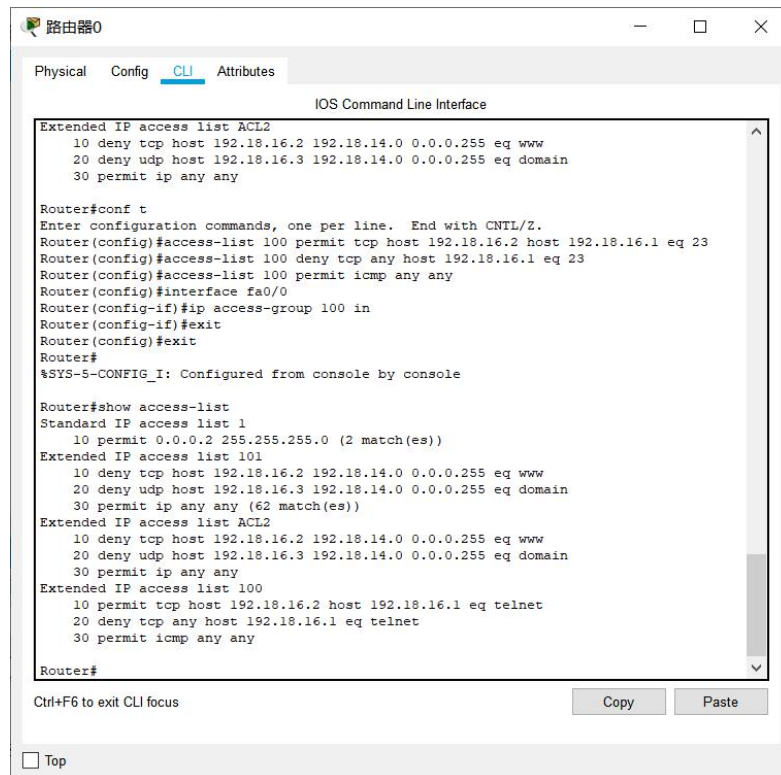
Ping statistics for 192.18.14.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 3ms

C:\>telnet 192.18.14.2 53
Trying 192.18.14.2 ...
% Connection timed out; remote host not responding
C:\>
```



- ◆ 最后我们使用 **show access-list** 命令查看一下访问控制列表

路由器 R0:



The screenshot shows the CLI of Router R0. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The title bar says '路由器0'. The main window is titled 'IOS Command Line Interface'. The text in the window is as follows:

```
Extended IP access list ACL2
10 deny tcp host 192.18.16.2 192.18.14.0 0.0.0.255 eq www
20 deny udp host 192.18.16.3 192.18.14.0 0.0.0.255 eq domain
30 permit ip any any

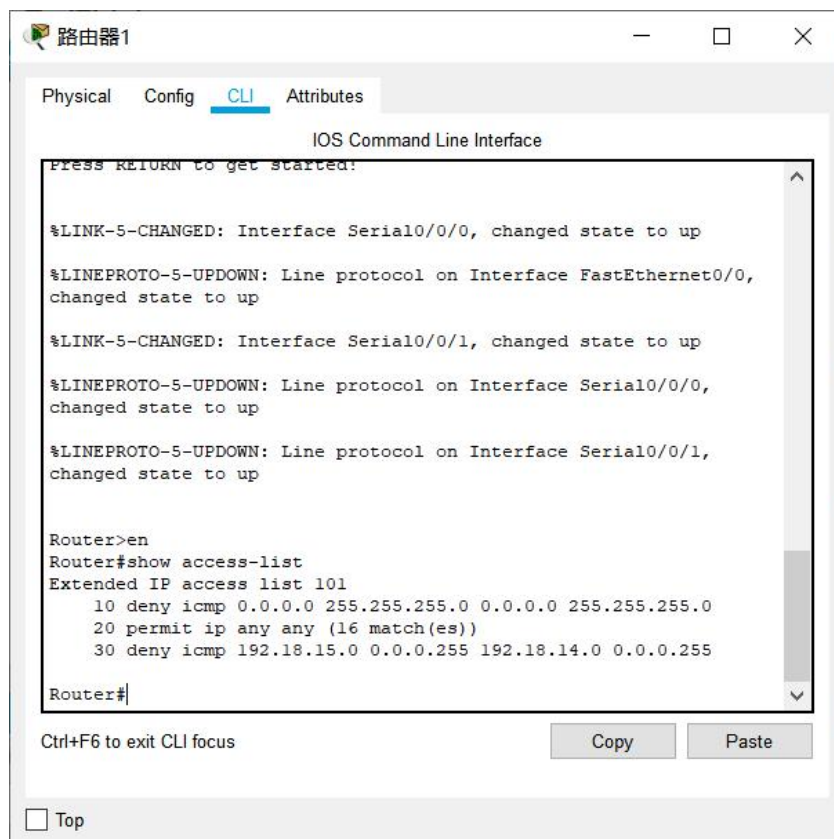
Router#conf t
Enter configuration commands, one per line. End with CNTRL/Z.
Router(config)#access-list 100 permit tcp host 192.18.16.2 host 192.18.16.1 eq 23
Router(config)#access-list 100 deny tcp any host 192.18.16.1 eq 23
Router(config)#access-list 100 permit icmp any any
Router(config)#interface fa0/0
Router(config-if)#ip access-group 100 in
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show access-list
Standard IP access list 1
10 permit 0.0.0.2 255.255.255.0 (2 match(es))
Extended IP access list 101
10 deny tcp host 192.18.16.2 192.18.14.0 0.0.0.255 eq www
20 deny udp host 192.18.16.3 192.18.14.0 0.0.0.255 eq domain
30 permit ip any any (62 match(es))
Extended IP access list ACL2
10 deny tcp host 192.18.16.2 192.18.14.0 0.0.0.255 eq www
20 deny udp host 192.18.16.3 192.18.14.0 0.0.0.255 eq domain
30 permit ip any any
Extended IP access list 100
10 permit tcp host 192.18.16.2 host 192.18.16.1 eq telnet
20 deny tcp any host 192.18.16.1 eq telnet
30 permit icmp any any

Router#
```

At the bottom, there is a 'Ctrl+F6 to exit CLI focus' message and 'Copy' and 'Paste' buttons. A 'Top' button is also visible at the bottom left.

路由器 R1:



The screenshot shows the CLI of Router R1. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The title bar says '路由器1'. The main window is titled 'IOS Command Line Interface'. The text in the window is as follows:

```
Press RETURN to get started:

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0,
changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to up

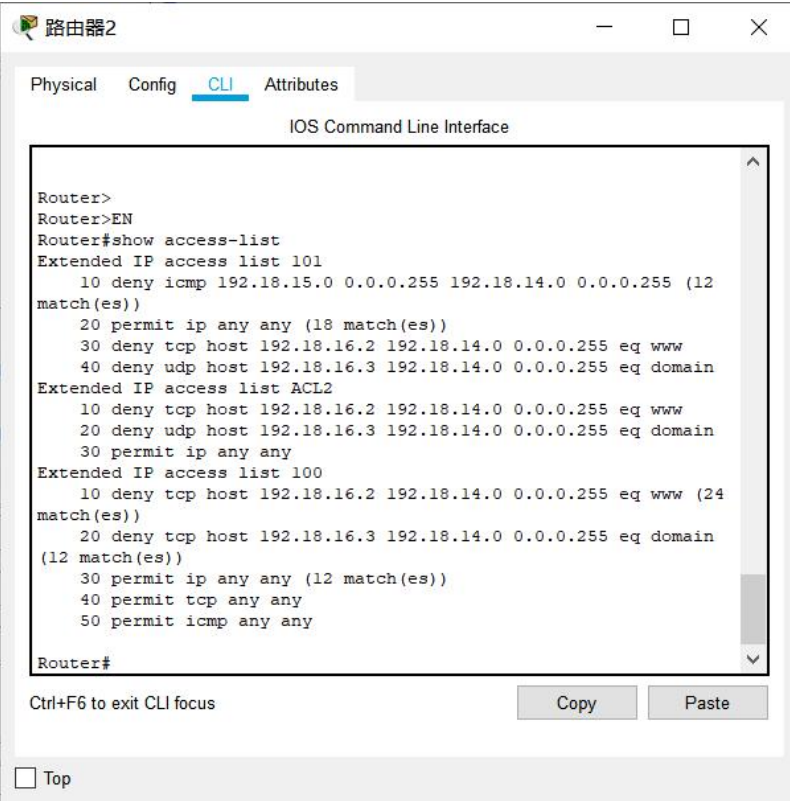
Router>en
Router#show access-list
Extended IP access list 101
10 deny icmp 0.0.0.0 255.255.255.0 0.0.0.0 255.255.255.0
20 permit ip any any (16 match(es))
30 deny icmp 192.18.15.0 0.0.0.255 192.18.14.0 0.0.0.255

Router#
```

At the bottom, there is a 'Ctrl+F6 to exit CLI focus' message and 'Copy' and 'Paste' buttons. A 'Top' button is also visible at the bottom left.



## 路由器 R2:



```
Router>
Router>EN
Router#show access-list
Extended IP access list 101
 10 deny icmp 192.18.15.0 0.0.0.255 192.18.14.0 0.0.0.255 (12
match(es))
 20 permit ip any any (18 match(es))
 30 deny tcp host 192.18.16.2 192.18.14.0 0.0.0.255 eq www
 40 deny udp host 192.18.16.3 192.18.14.0 0.0.0.255 eq domain
Extended IP access list ACL2
 10 deny tcp host 192.18.16.2 192.18.14.0 0.0.0.255 eq www
 20 deny udp host 192.18.16.3 192.18.14.0 0.0.0.255 eq domain
 30 permit ip any any
Extended IP access list 100
 10 deny tcp host 192.18.16.2 192.18.14.0 0.0.0.255 eq www (24
match(es))
 20 deny tcp host 192.18.16.3 192.18.14.0 0.0.0.255 eq domain
(12 match(es))
 30 permit ip any any (12 match(es))
 40 permit tcp any any
 50 permit icmp any any
Router#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

## ◆ 实验总结

通过此次实验进一步加深了我对于 ACL 访问控制的了解，我们可以使用 deny, permit 对能够进行访问的 ip 进行限制，有利于网络的安全性，比如一个秘密的网络, 可以通过 ACL 限制只有某些端口进来的访问才有效。通过本次的实验，我了解到如何在搭建网络的时候，限定某些 ip 用户才能够进行访问，受益匪浅。