

ACL 访问控制

学生姓名：李俊杰 1850668

合作学生：无

实验地点：济事楼 330

实验时间：2020 年 11 月 5 日 78 节

【实验目的】

- 1.了解路由器包过滤基本原理。
- 2.了解访问控制列表的运行原理。
- 3.利用访问控制列表实现网络安全。
- 4.了解网络安全相关技术。
- 5.通过实验熟悉路由器相关配置操作以及网络联通测试工具的使用。

【实验原理】

1.路由器包过滤机制

路由器包过滤机制是指路由器在转发 IP 数据包时，需要对每一个 IP 数据包头部进行分析，检查头部是否损坏并用于计算路由，为转发服务，同时头部的相关信息可以作为过滤的依据。

2.访问控制列表原理

访问控制列表（Access Control Lists, ACL），ACL 也称为防火墙，是指路由器在包过滤时，以 IP 数据包头部中的信息，如源 IP 地址和目标 IP 地址等数据定义一些访问控制规则，对网络设备接口上的数据报文进行控制，只允许满足条件的 IP 数据包通过否则丢弃，从而达到访问控制的目的，提高了网络可管理性和安全性。

ACL 分为两种：标准 IP 访问列表和扩展 IP 访问列表，编号范围分别为 1-99、1300-1999、100-199、2000-2699。标准 IP 访问列表可以根据数据包的源 IP 地址定义规则，进行数据包的过滤；扩展 IP 访问列表可以根据数据包的源 IP、目的 IP、源端口、目的端口、协议来定义规则，进行数据包的过滤。

3.ACL 的应用

在工程应用中，可以设置规则不允许访问某些网站，如禁止访问一些不安全网站，也可以对自身网络中某段地址进行保护，比如保护网站服务器。如通过访问控制列表，可以允许外部网访问 Web 服务器地址，但不允许访问数据库服务器地址，从而阻隔了访问关键主机，有效提高了网络安全性。ACL 基于接口进行规则的应用分为入栈应用和出栈应用。

【实验设备】

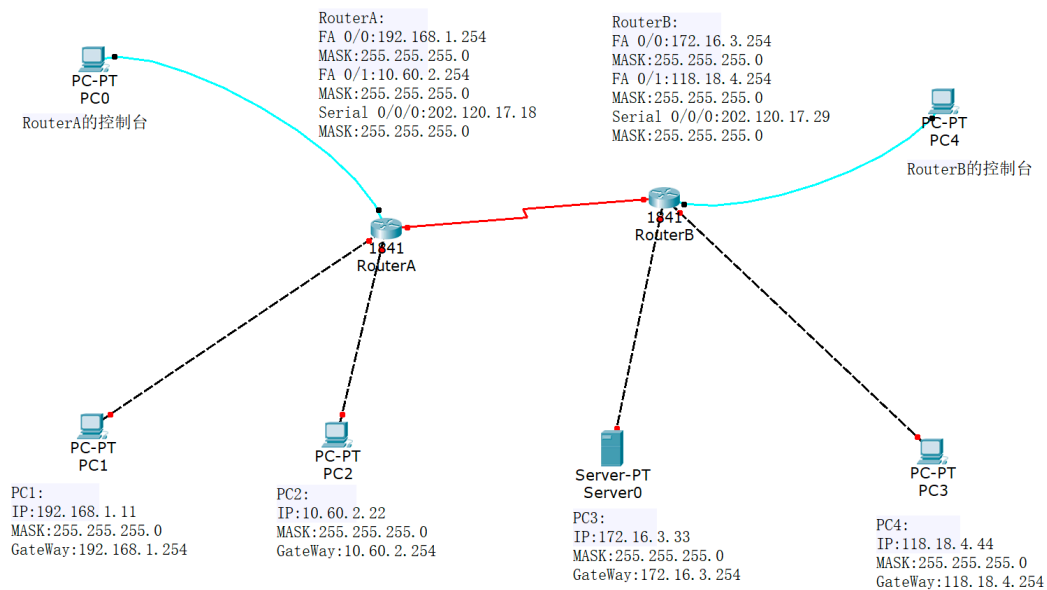
- 1.一台运行 Windows 系统的计算机
- 2.终端仿真软件 Cisco Packet Tracer。

【实验步骤】

- 1.首先规划网络地址及拓扑图。
- 2.根据网络拓扑图配置各台 PC 机、服务器和路由器的 IP 地址。
- 3.在各台路由器上配置静态路由协议，使得各台 PC 间能够相互连通，并测试。
- 4.在 Router B 上配置 ACL。
- 5.在 Router B 的串口应用 ACL。
- 6.再次验证各台 PC 之间以及 PC 与服务器的连通性以及 WWW 访问。

【实验现象】

- 1.网络规划拓扑图如图所示。



2.根据网络拓扑图配置各台 PC、服务器和路由器 IP 地址、网关、掩码。

路由器端口地址配置：

RouterA:

```

interface FastEthernet 0/0
ip address 192.168.1.254 255.255.255.0
interface FastEthernet 0/1
ip address 10.60.2.254 255.255.255.0
no shutdown

```

Router B:

```

interface FastEthernet 0/0
ip address 172.16.3.254 255.255.255.0
interface FastEthernet 0/1
ip address 118.18.4.254 255.255.255.0
no shutdown

```

路由器串口地址配置：

RouterA:

```
interface Serial 0/0/0
```

```
ip address 202.120.17.18 255.255.255.0
```

```
Clock rate 56000
```

```
no shutdown
```

RouterB:

```
interface Serial 0/0/0
```

```
ip address 202.120.17.29 255.255.255.0
```

```
Clock rate 56000
```

```
no shutdown
```

部分操作如图:

```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
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 t
o up
ip address 192.168.1.254 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#no shutdown

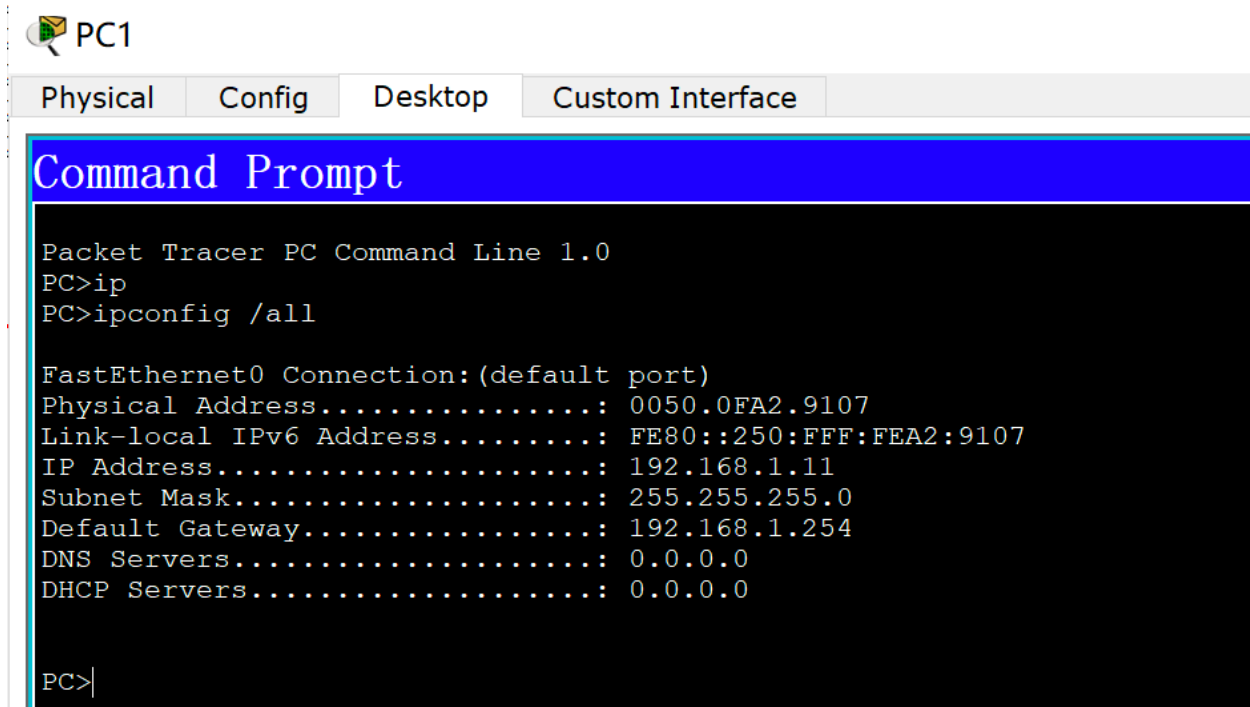
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state t
o up
ip address 10.60.2.254 255.0.0.0
Router(config-if)#ip address 10.60.2.254 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#no shutdown
Router(config-if)#ip address 202.120.17.18 255.255.255.0
Router(config-if)#clock rate 56000
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up

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

Router(config-if)#exit

```



3.配置路由器的静态路由表。

RouterA:

```
ip route 172.16.3.0 255.255.255.0 serial 0/0/0
```

```
ip route 118.18.4.0 255.255.255.0 serial 0/0/0
```

RouterB:

```
ip route 192.168.1.0 255.255.255.0 serial 0/0/0
```

```
ip route 10.60.2.0 255.255.255.0 serial 0/0/0
```

RouterA

Physical
Config
CLI

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
WITCHIN
AN Databa
INTERFAC
stEthernetf

Static Routes

Network
Mask
Next Hop

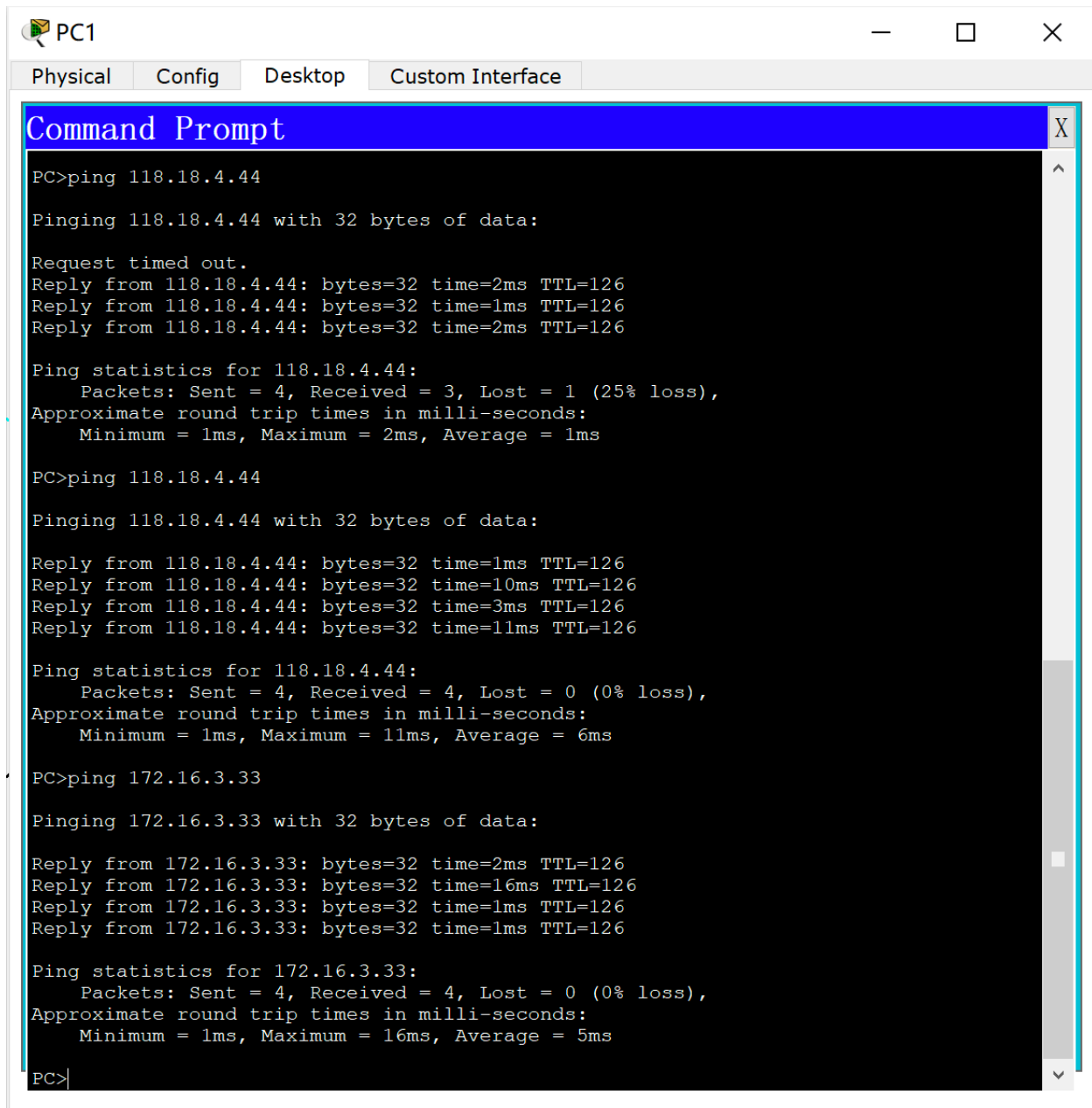
Add

Network Address
172.16.3.0/24 via Serial0/0/0
118.18.4.0/24 via Serial0/0/0

Remove

Equivalent IOS Commands
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#ip route 172.16.3.0 255.255.255.0 serial 0/0/0
Router(config)#ip route 118.18.4.0 255.255.255.0 serial 0/0/0
Router(config)#
Router(config)#

连通性测试:



The screenshot shows a window titled "PC1" with tabs for "Physical", "Config", "Desktop", and "Custom Interface". The "Desktop" tab is active, displaying a "Command Prompt" window. The Command Prompt shows the results of two ping commands. The first command is "ping 118.18.4.44", which shows a 25% loss of packets. The second command is "ping 172.16.3.33", which shows 0% loss of packets. The Command Prompt window has a blue title bar and a scroll bar on the right.

```
PC1
Physical Config Desktop Custom Interface

Command Prompt

PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Request timed out.
Reply from 118.18.4.44: bytes=32 time=2ms TTL=126
Reply from 118.18.4.44: bytes=32 time=1ms TTL=126
Reply from 118.18.4.44: bytes=32 time=2ms TTL=126

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>ping 118.18.4.44

Pinging 118.18.4.44 with 32 bytes of data:

Reply from 118.18.4.44: bytes=32 time=1ms TTL=126
Reply from 118.18.4.44: bytes=32 time=10ms TTL=126
Reply from 118.18.4.44: bytes=32 time=3ms TTL=126
Reply from 118.18.4.44: bytes=32 time=11ms TTL=126

Ping statistics for 118.18.4.44:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 6ms

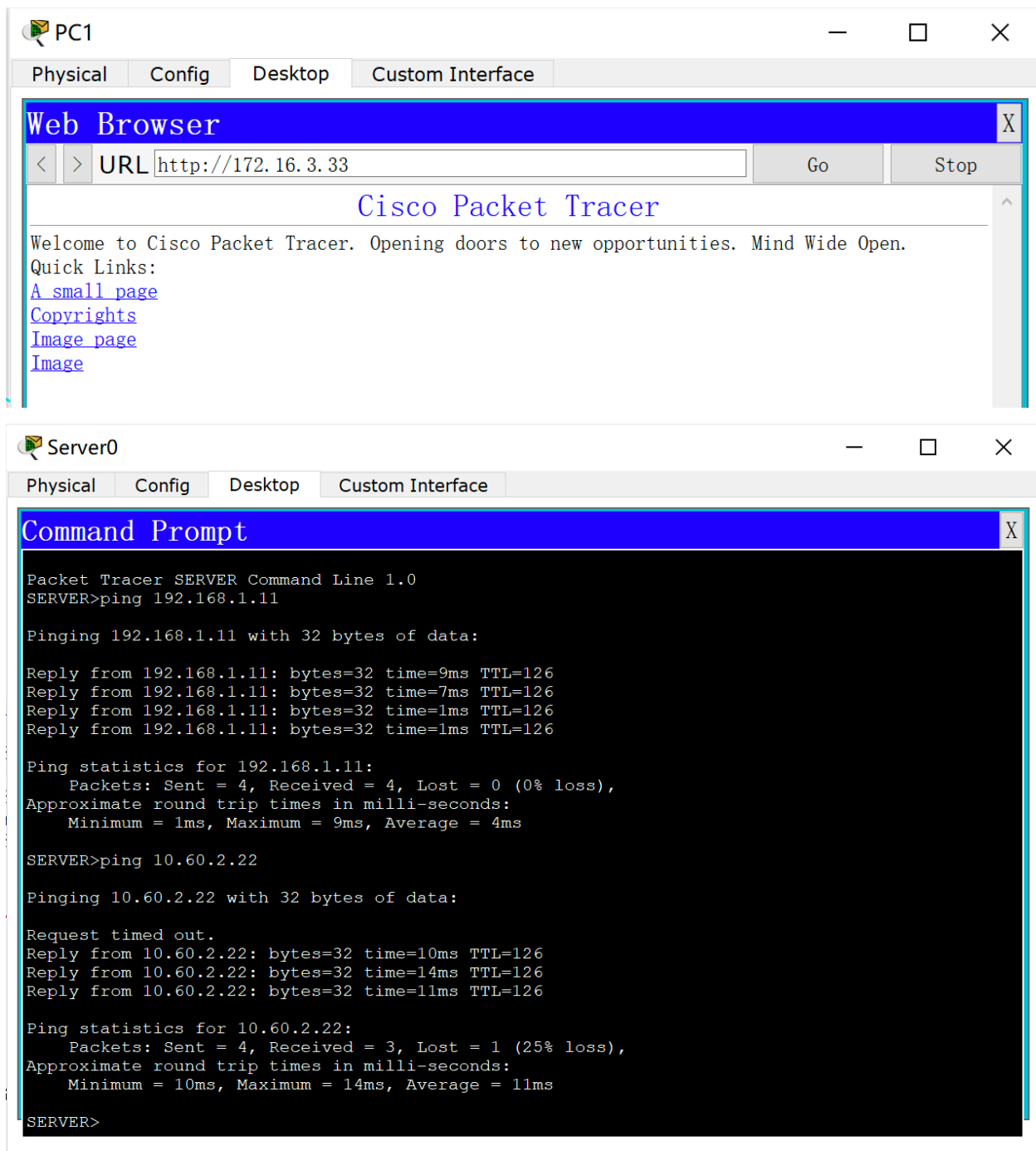
PC>ping 172.16.3.33

Pinging 172.16.3.33 with 32 bytes of data:

Reply from 172.16.3.33: bytes=32 time=2ms TTL=126
Reply from 172.16.3.33: bytes=32 time=16ms TTL=126
Reply from 172.16.3.33: bytes=32 time=1ms TTL=126
Reply from 172.16.3.33: bytes=32 time=1ms TTL=126

Ping statistics for 172.16.3.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 16ms, Average = 5ms

PC>
```

4.配置路由器 B 的扩展 ACL 表。

RouterB:

拒绝 ping 包:

```
access-list 101 deny icmp host 192.168.1.11 host 172.16.3.33
```

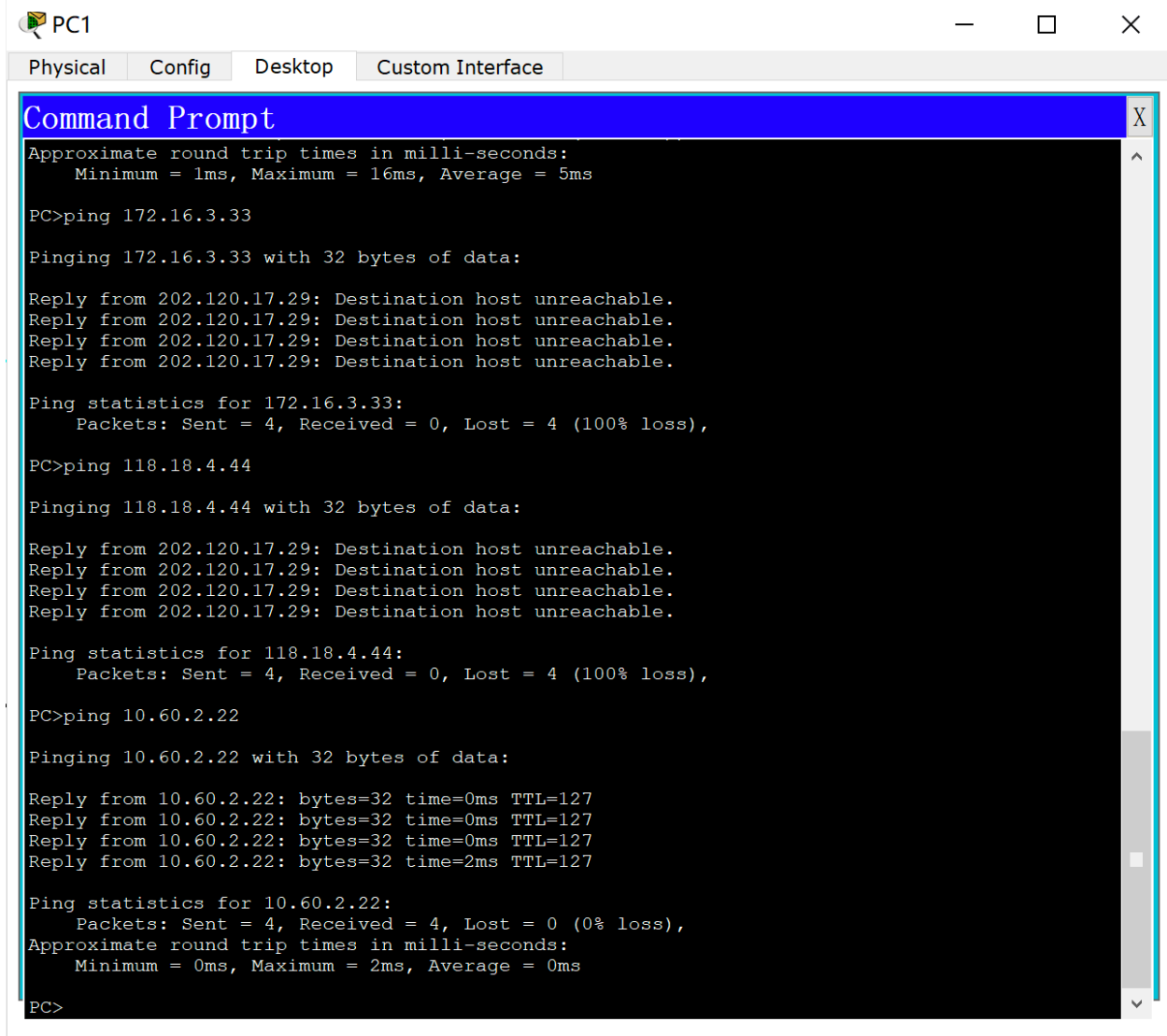
允许 www 访问:

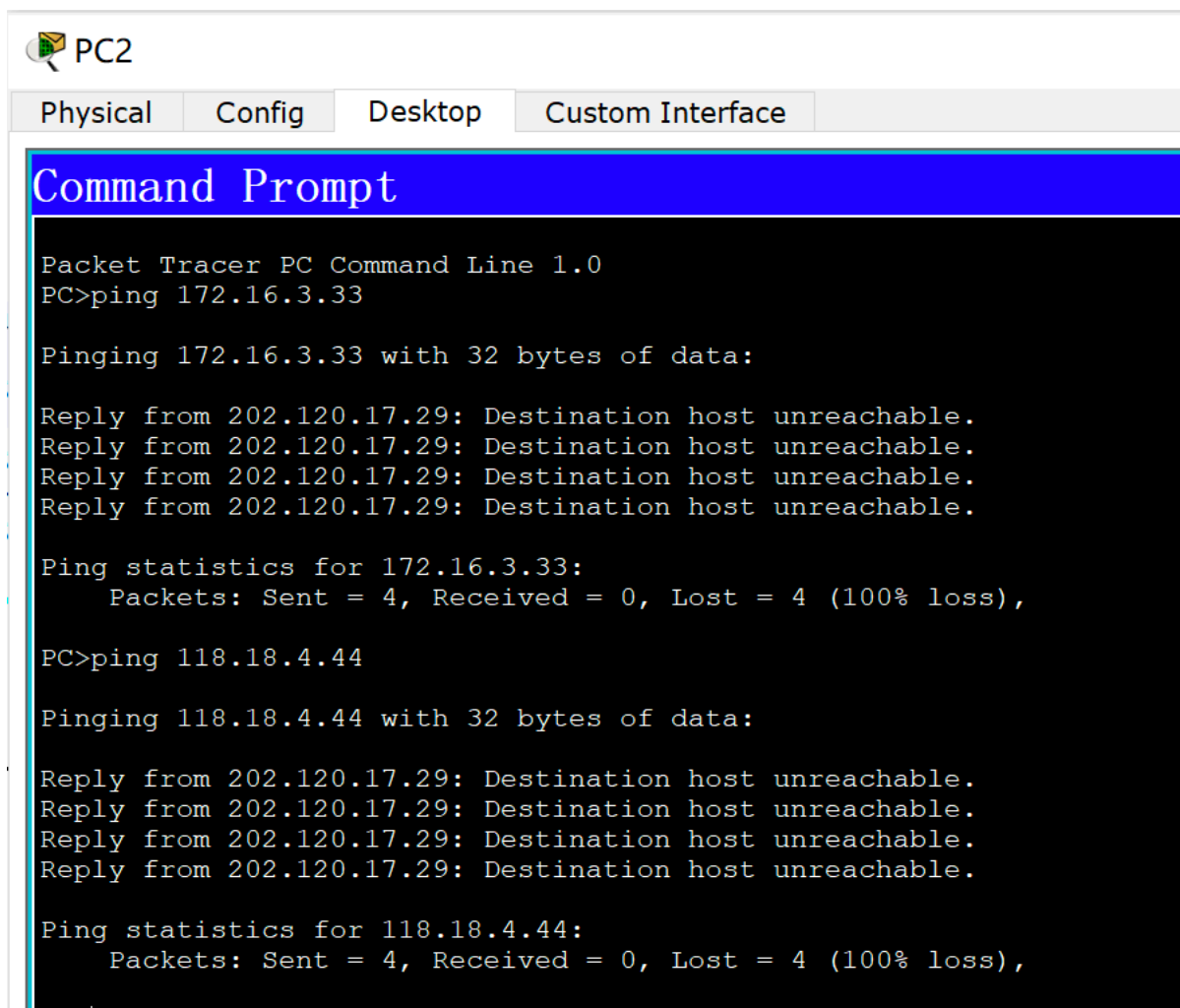
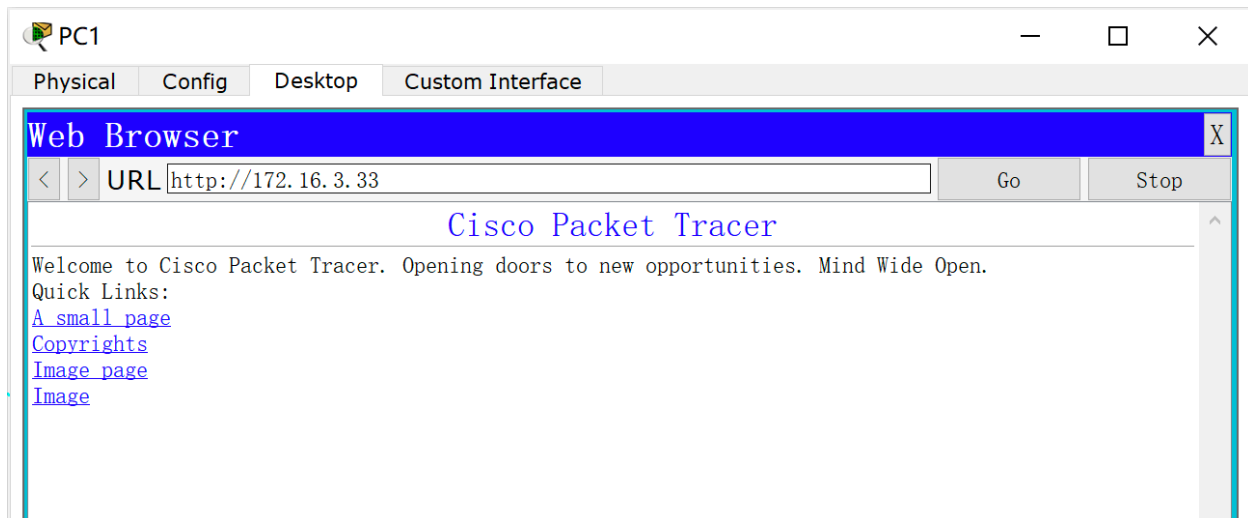
```
access-list 101 permit tcp host 192.168.1.11 host 172.16.3.33 eq www
```

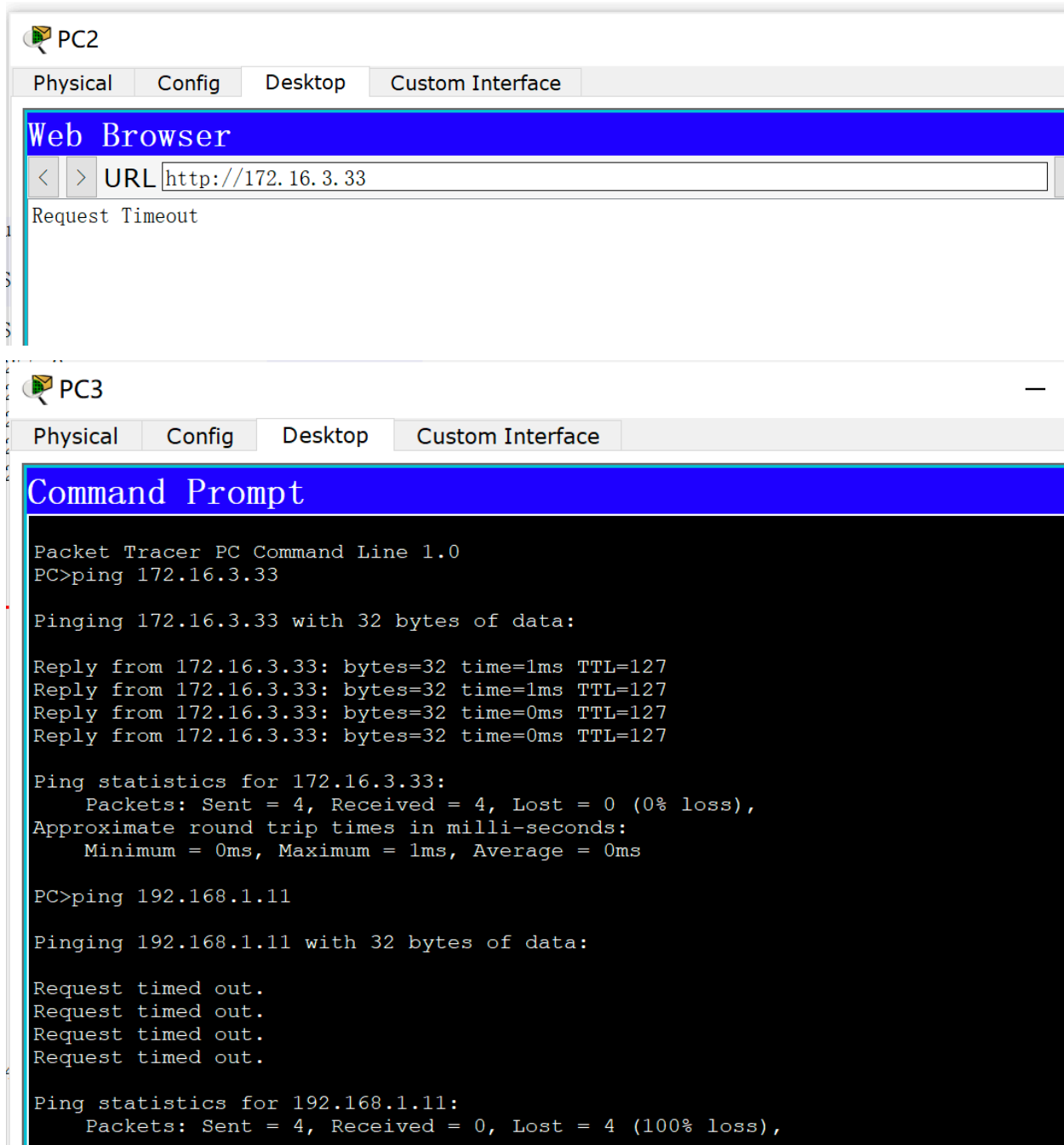
将 ACL 应用到串口 serial 0/0/0:

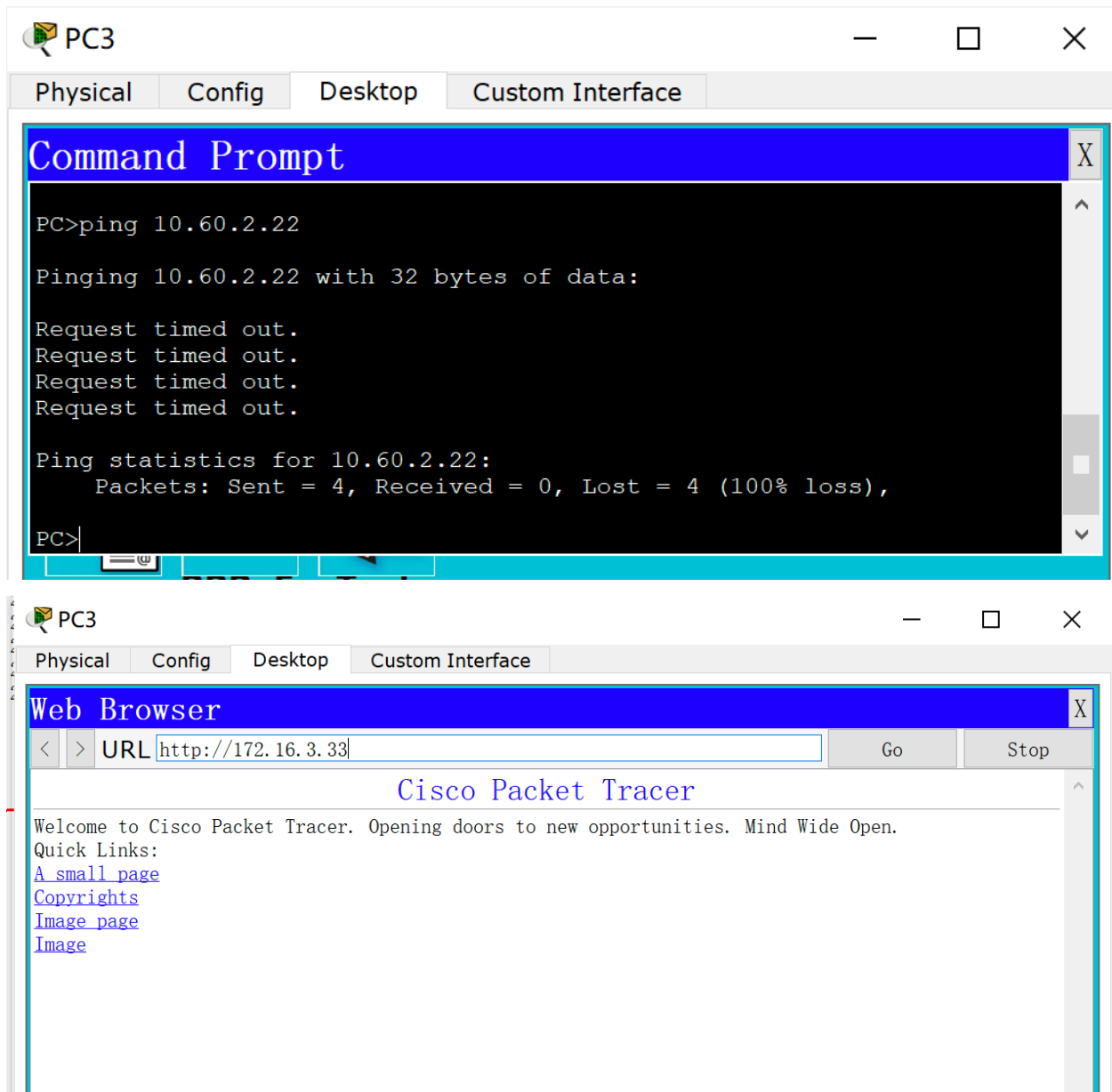
```
ip access-group 101 in
```

5.测试各台 PC 之间及 PC 与服务器连通性。









Command Prompt

```
SERVER>ping 192.168.1.11
```

```
Pinging 192.168.1.11 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 192.168.1.11:
```

```
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

```
SERVER>ping 118.18.4.44
```

```
Pinging 118.18.4.44 with 32 bytes of data:
```

```
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127
```

```
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127
```

```
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127
```

```
Reply from 118.18.4.44: bytes=32 time=0ms TTL=127
```

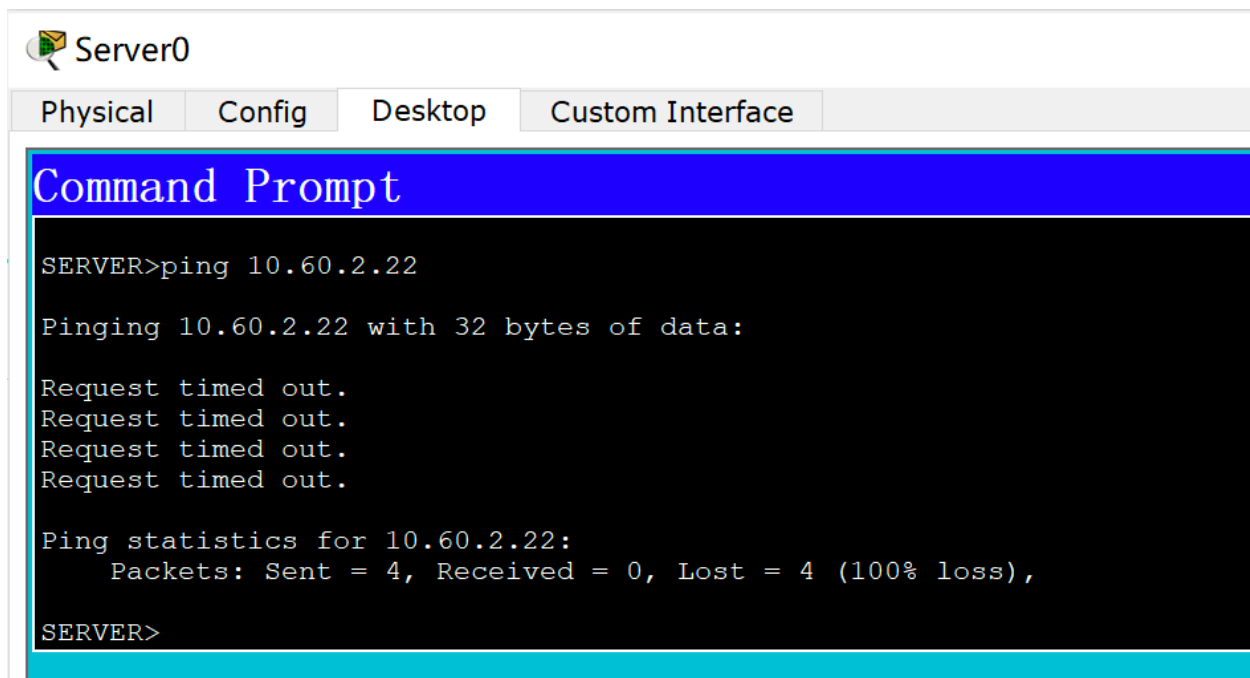
```
Ping statistics for 118.18.4.44:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
SERVER>|
```



【分析讨论】