实验 16：ACL 访问控制实验

姓名	学号	合作学生	指导教师	实验地点	实验时间
林继申	2250758	无	陈伟超	济事楼 330	2024/04/18

【实验目的】

本实验旨在通过配置和应用接入控制列表（ACL）加深学生对网络安全和数据包过滤的理解。通过规划网络拓扑、设置设备 IP 和应用 ACL 规则，学生将实践如何控制网络流量，包括允许或拒绝特定的网络访问，以此提高对网络可管理性和安全性的认知和操作技能。

【实验原理】

接入控制列表技术原理

接入控制列表（Access Control Lists，简称 ACLs）是网络设备用于增强网络可管理性和安全性的关键技术。它们作为数据包过滤系统，根据定义的规则，控制数据报文在网络设备接口上的通过或阻断。这些规则可以是非常简单的，如基于源 IP 地址的标准 IP 访问列表，也可以是更复杂的，如扩展 IP 访问列表，后者不仅包括源 IP 地址，还包括目的 IP 地址、源端口号、目的端口号和使用的协议类型。

在 ACLs 的应用中，规则可以被设置为入栈应用或出栈应用，这意味着它们可以控制进入或离开接口的数据包。通过这种方式，ACLs 充当网络的“防火墙”，不仅可以防止未授权访问，还可以有效地管理和控制网络流量，保证网络的整体安全性和效率。

接入控制列表（ACLs）在网络安全架构中的运用不仅限于阻断非授权访问，它们还承担着网络监控和数据流量分析的重要角色。例如，通过记录接口上被拒绝或允许的数据包，ACLs 可以为网络管理员提供关键的安全日志信息，帮助识别潜在的安全威胁或不正常的流量模式。此外，ACLs 可以配置为时间基础的规则，允许在特定时间段内应用特定的访问控制策略，这种灵活性使得网络策略可以更加精确地匹配企业的运营需求。

在实际部署中，ACLs 的管理和维护要求网络管理员具备高度的精确度和前瞻性。错误配置的 ACLs 可能导致服务中断或数据泄露。因此，设计和实施 ACL 策略时，需要仔细规划并进行充分的测试，以确保它们不仅有效地执行预定的安

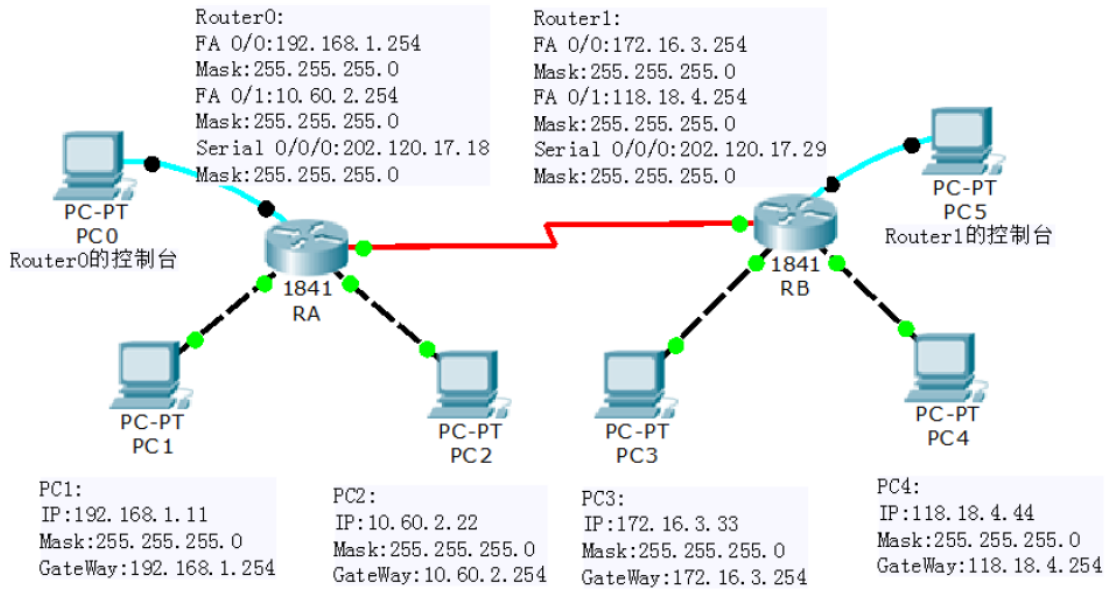
全策略，还要保持网络的最优性能。

【实验设备】

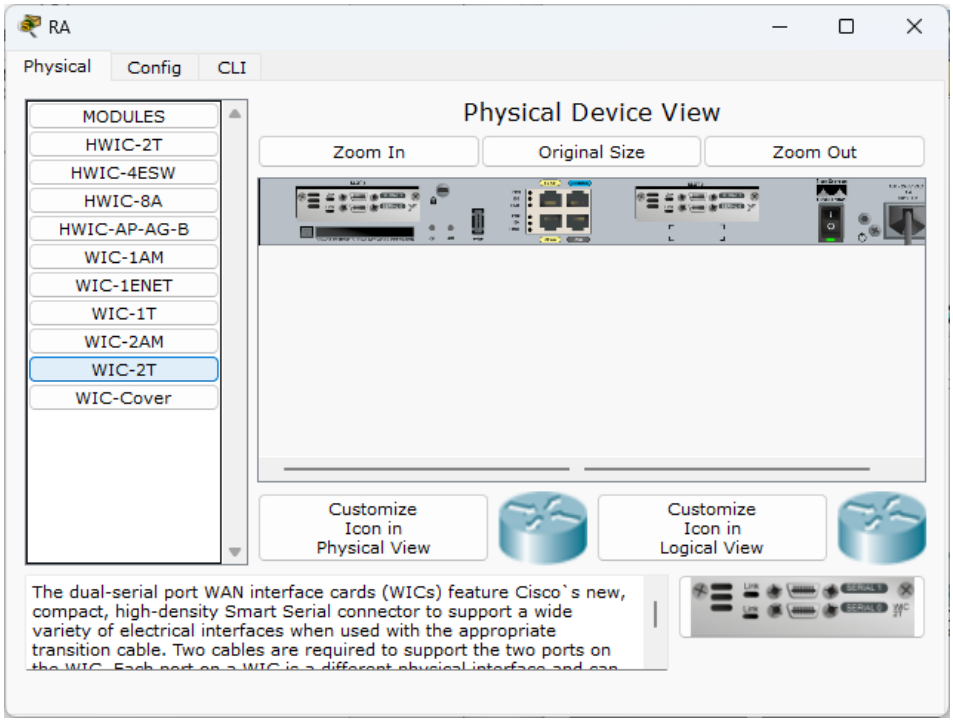
1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

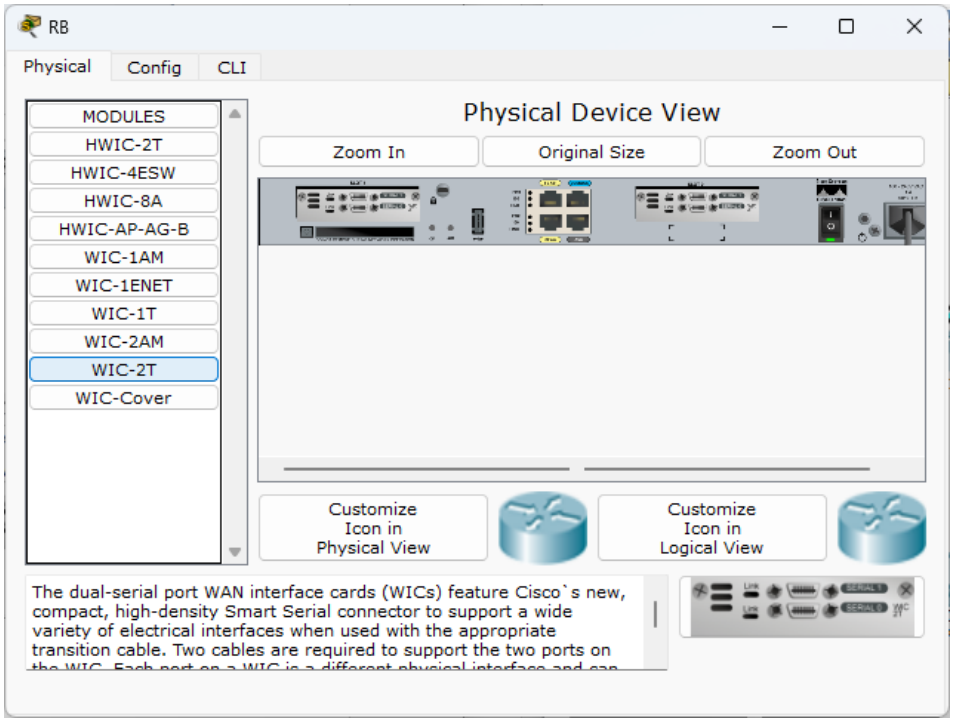
【实验步骤】

1. 规划网络地址及拓扑图。

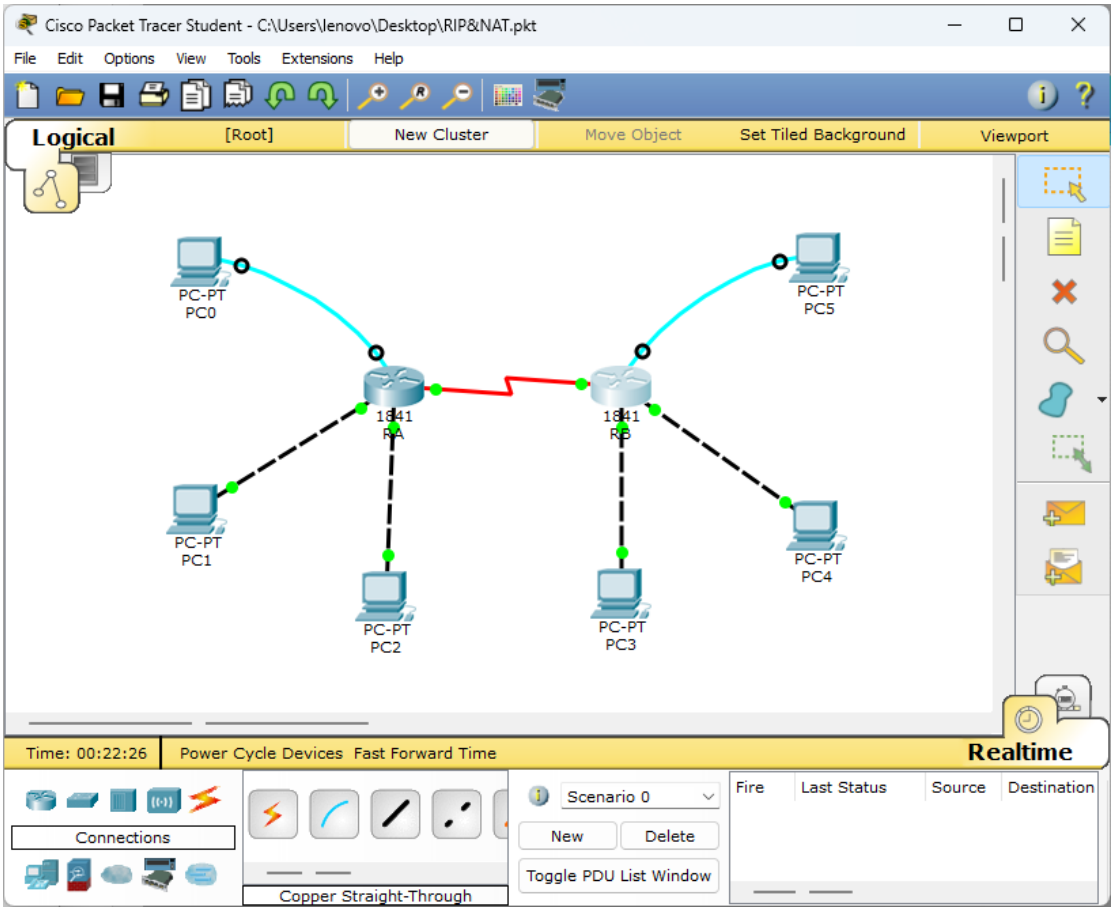


2. 在路由器 A 和路由器 B 中分别安装 WIC-2T，并重启设备。

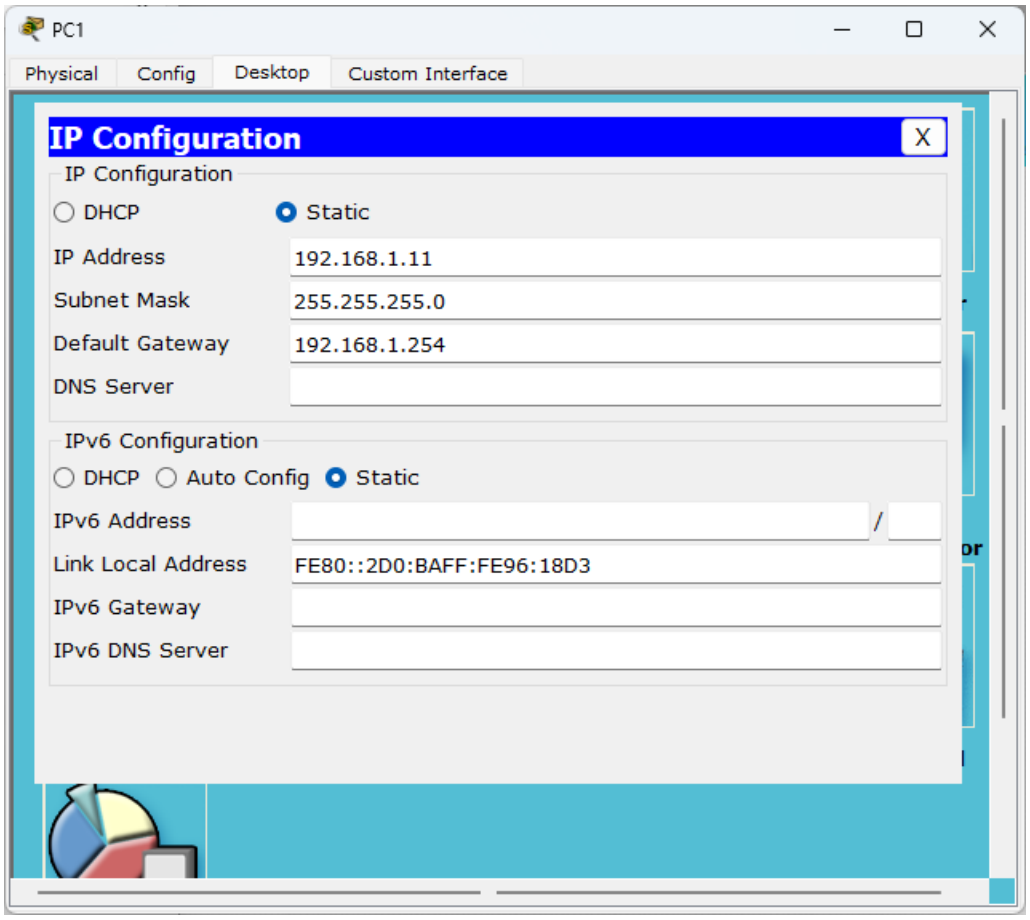


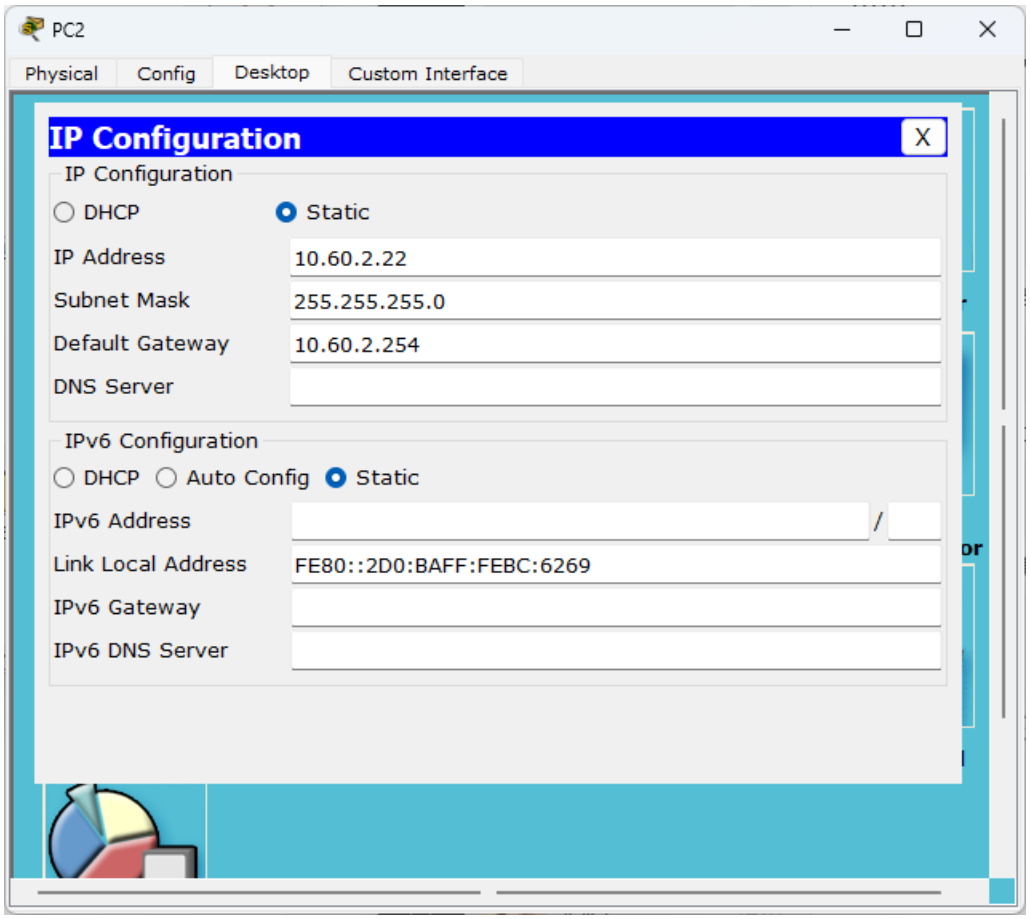


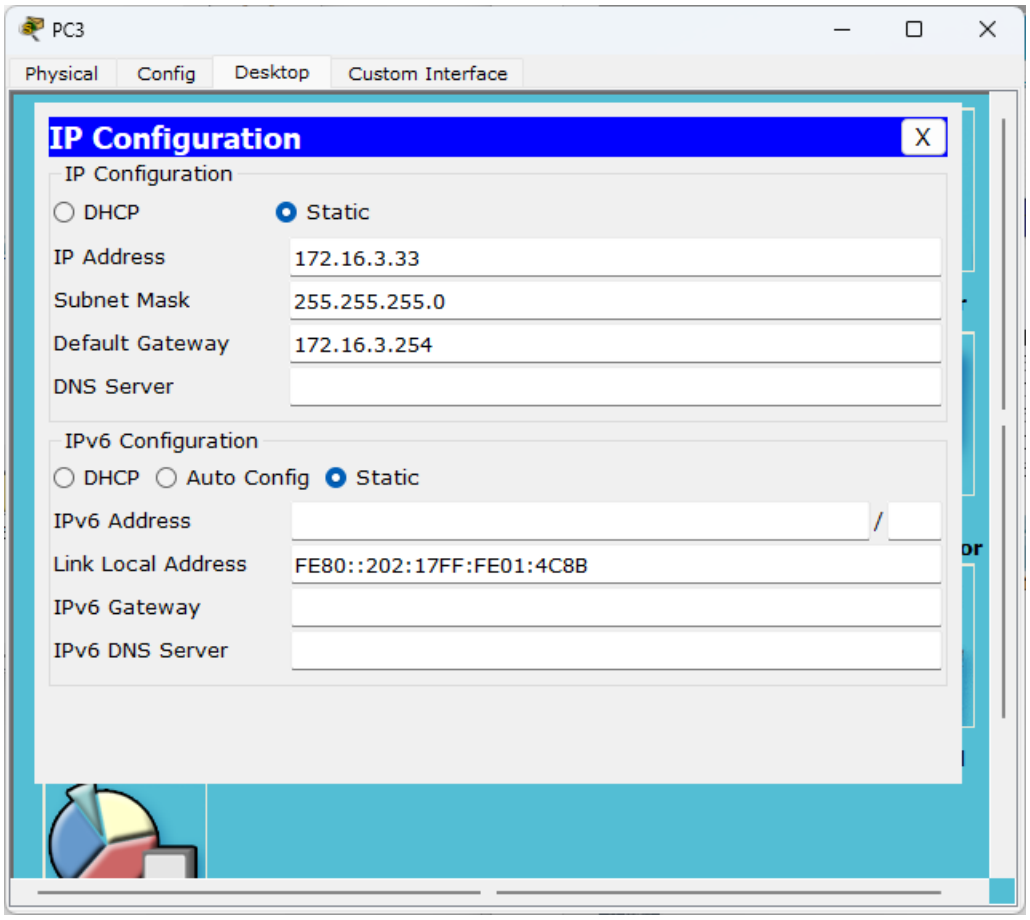
3. 启动 Cisco Packet Tracer，按照上述拓扑结构连接设备。

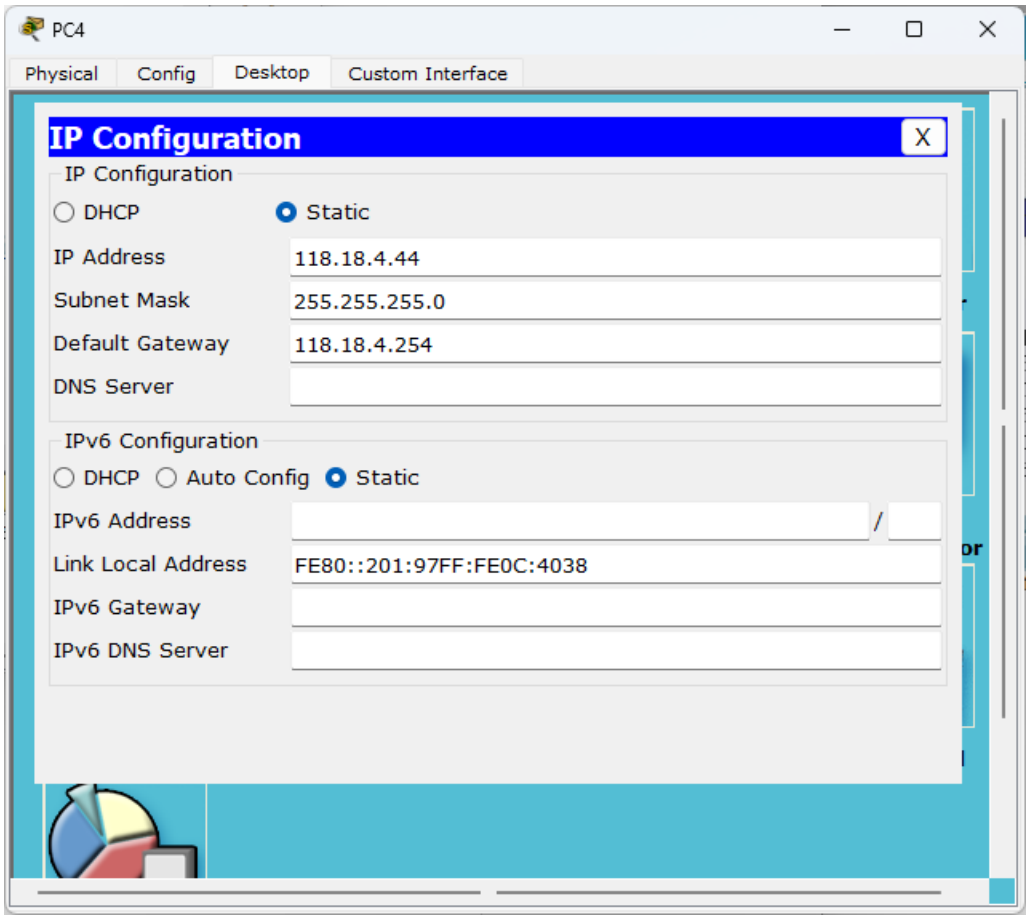


4. 配置 PC 机的 IP 地址、子网掩码和网关。


PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.1.11
Subnet Mask
255.255.255.0
Default Gateway
192.168.1.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FE96:18D3
IPv6 Gateway
IPv6 DNS Server


PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
10.60.2.22
Subnet Mask
255.255.255.0
Default Gateway
10.60.2.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BAFF:FEBC:6269
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
172.16.3.33
Subnet Mask
255.255.255.0
Default Gateway
172.16.3.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::202:17FF:FE01:4C8B
IPv6 Gateway
IPv6 DNS Server


PC4
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
118.18.4.44
Subnet Mask
255.255.255.0
Default Gateway
118.18.4.254
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE0C:4038
IPv6 Gateway
IPv6 DNS Server

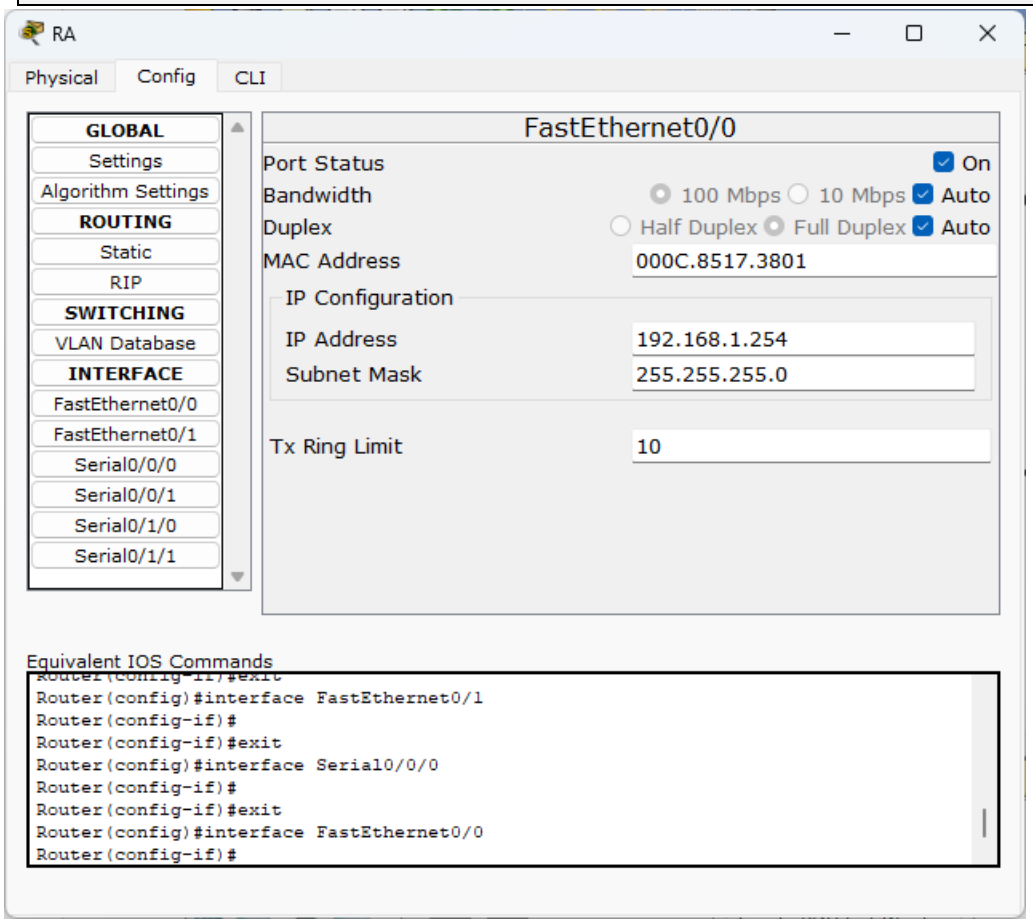
5. 配置路由器的端口地址和串口端口地址。

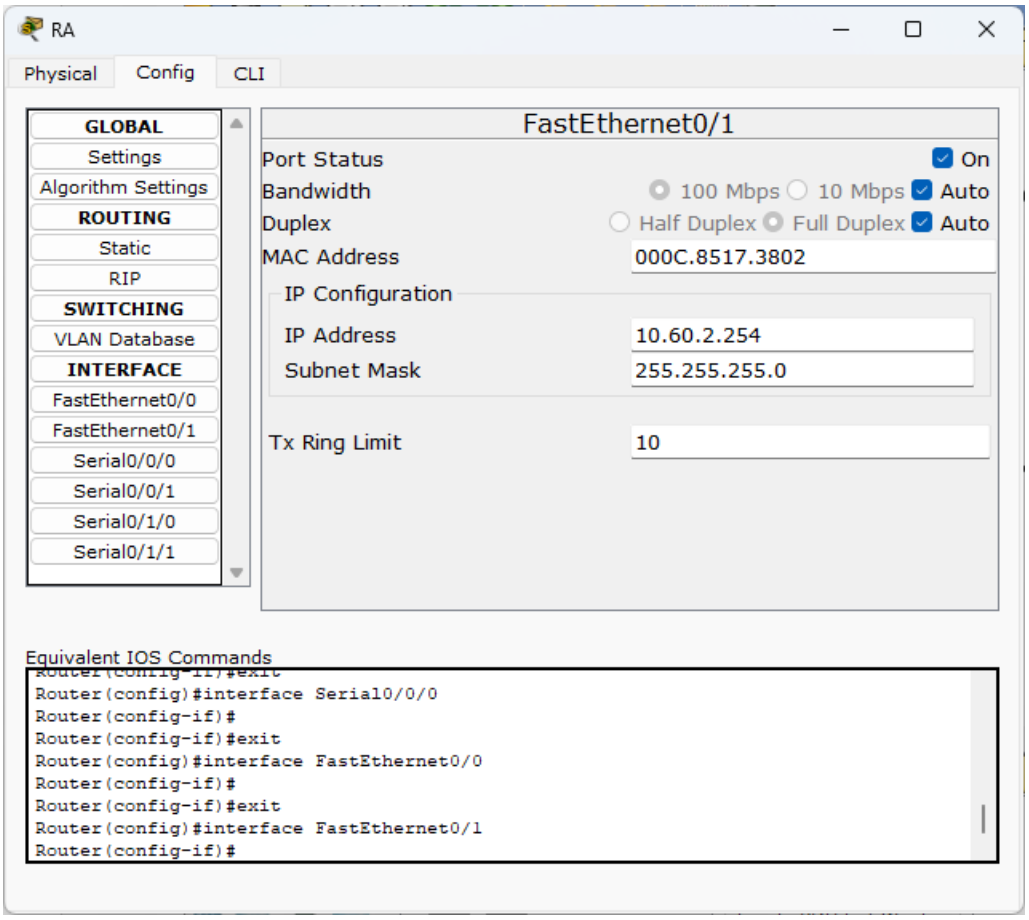
- 在路由器 A 的 CLI 中输入以下命令：

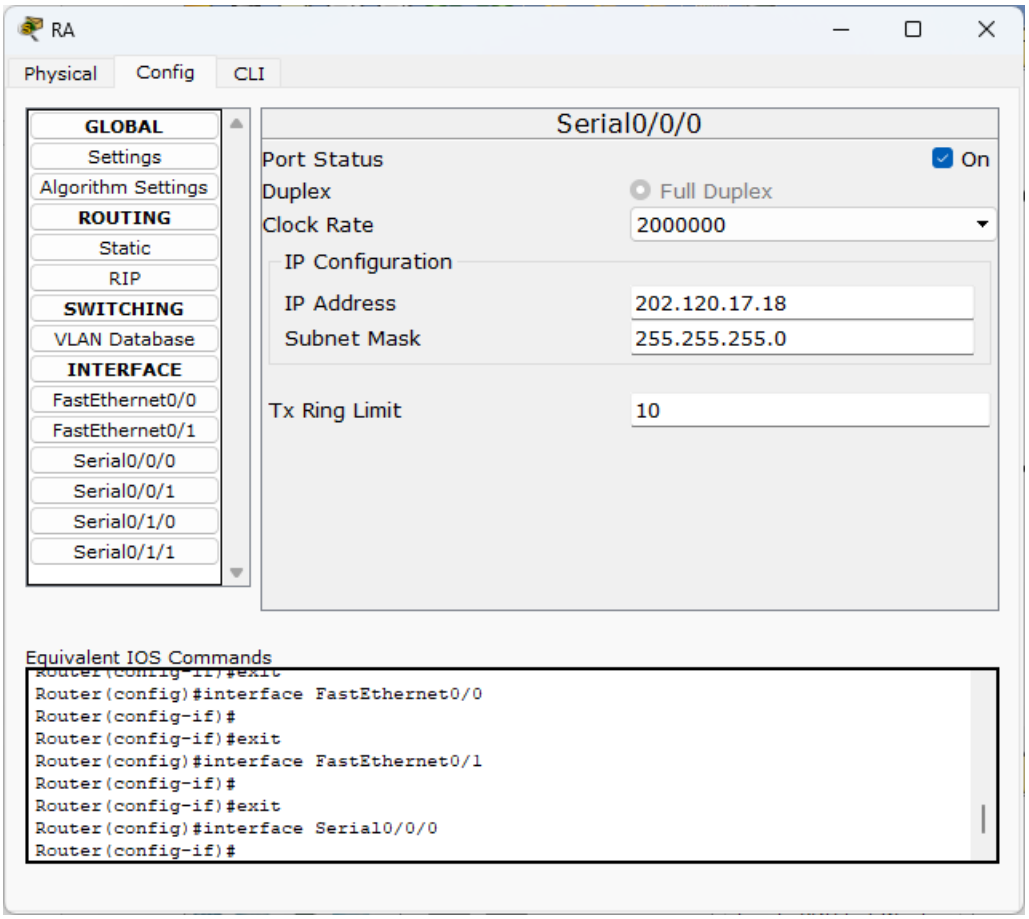
```
interface FastEthernet0/0
ip address 192.168.1.254 255.255.255.0
interface FastEthernet0/1
ip address 10.60.2.254 255.255.255.0
interface Serial 0/0/0
ip address 202.120.17.18 255.255.255.0
Clock rate 56000
```

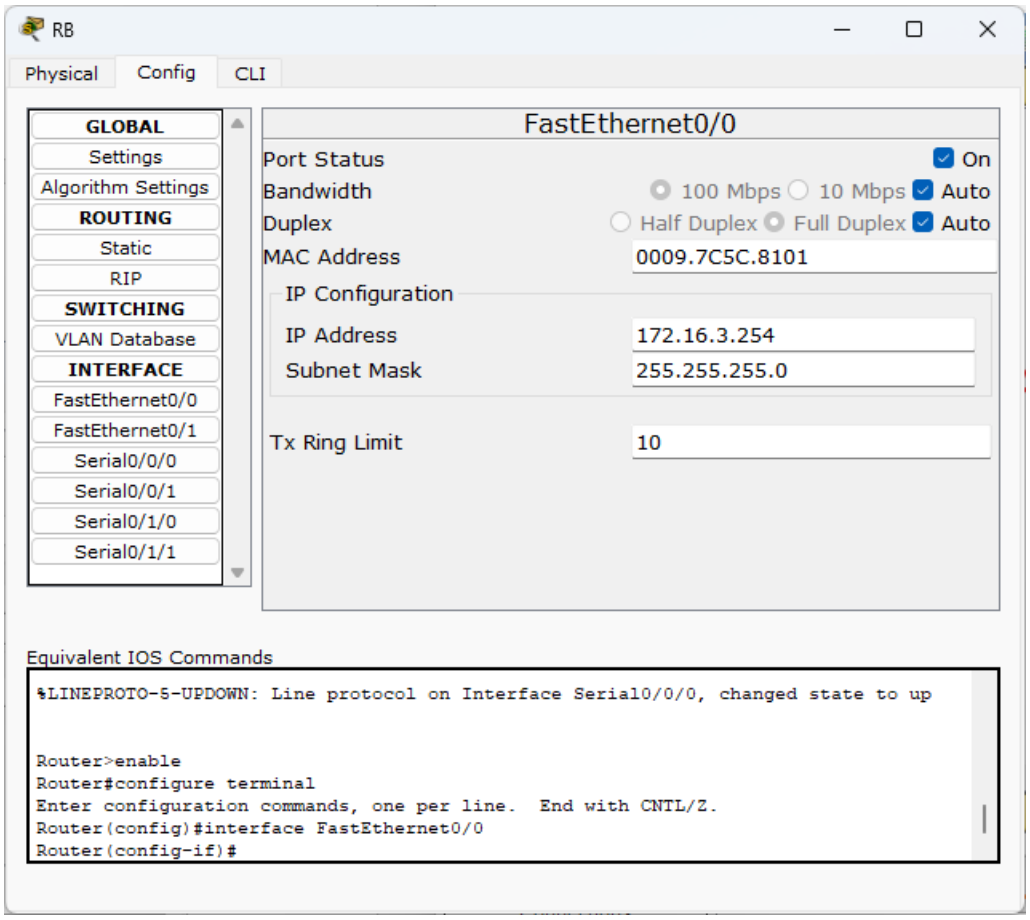
- 在路由器 B 的 CLI 中输入以下命令：

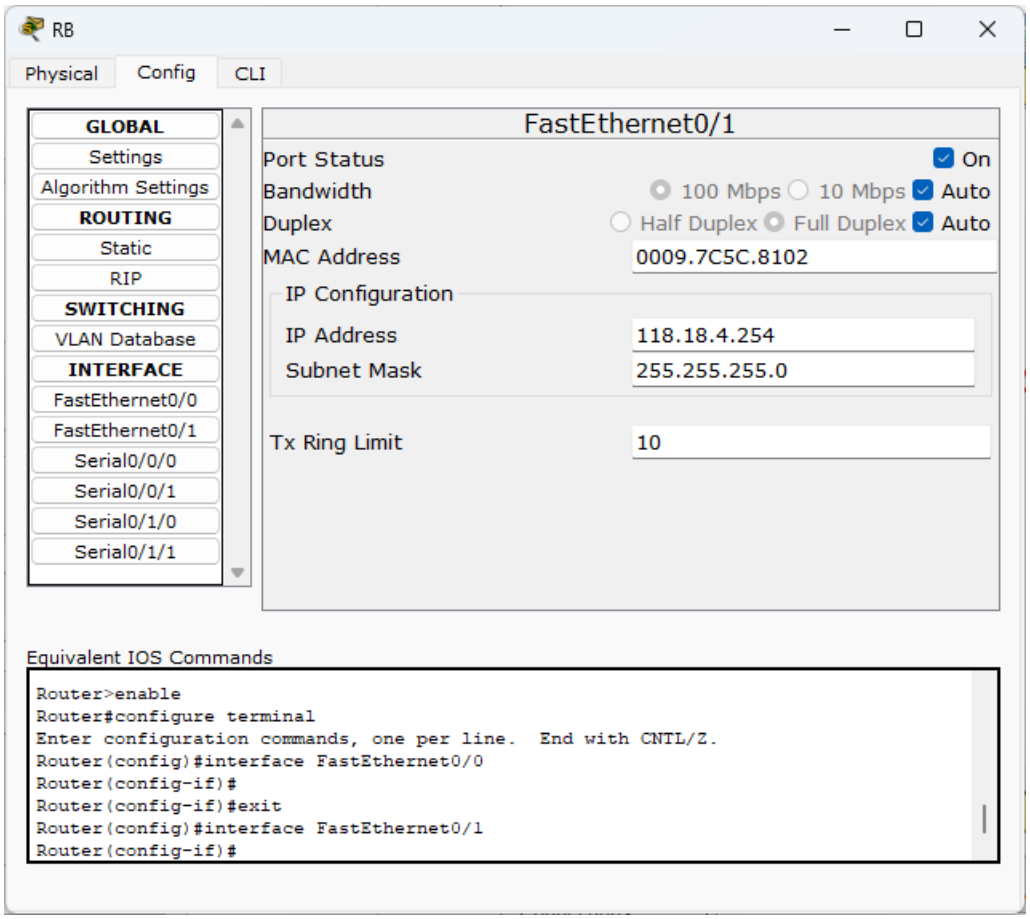
```
interface FastEthernet0/0
ip address 172.16.3.254 255.255.255.0
interface FastEthernet0/1
ip address 118.18.4.254 255.255.255.0
interface Serial 0/0/0
ip address 202.120.17.29 255.255.255.0
Clock rate 56000
```

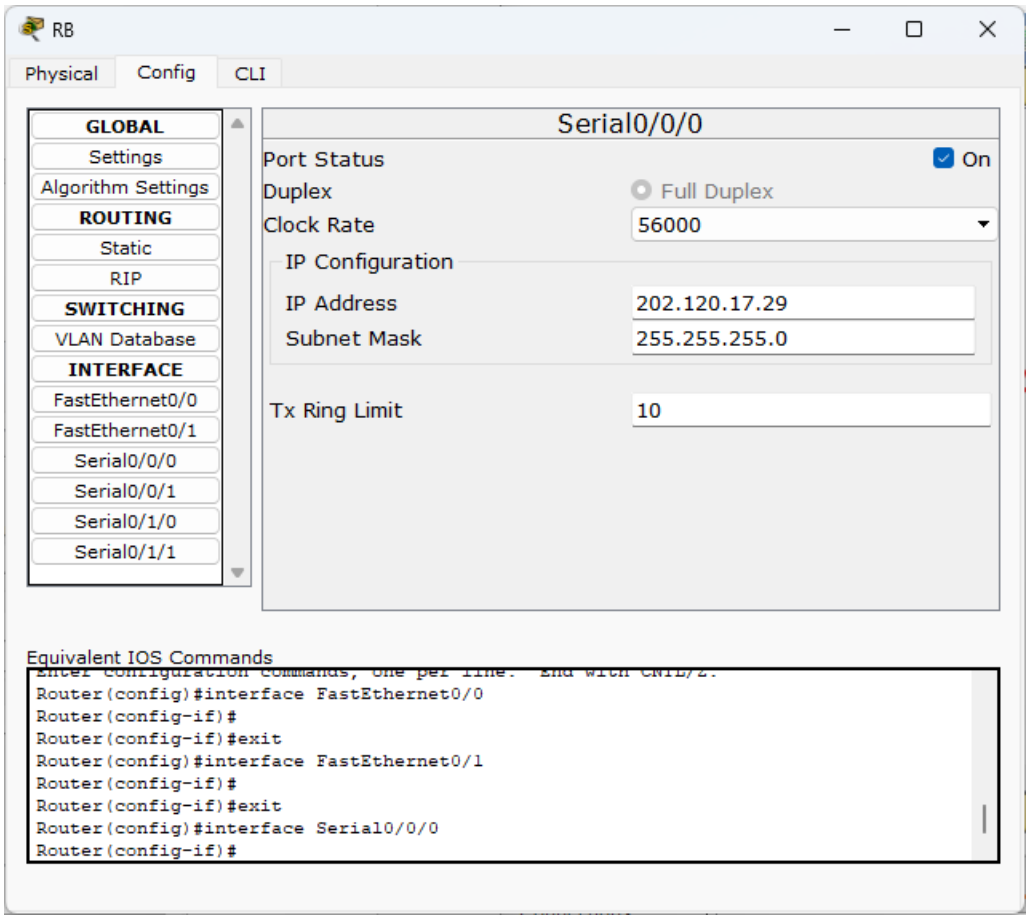



RA
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000C.8517.3802
IP Configuration
IP Address
10.60.2.254
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface Serial0/0/0
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)#


RA
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
202.120.17.18
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
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)#


RB
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0009.7C5C.8101
IP Configuration
IP Address
172.16.3.254
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#


RB
Physical
Config
CLI
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0009.7C5C.8102
IP Configuration
IP Address
118.18.4.254
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#



6. 为 RA 配置静态路由。

```
ip route 172.16.3.0 255.255.255.0 Serial0/1/0
ip route 118.18.4.0 255.255.255.0 Serial0/1/0
```

7. 为 RouterB 配置静态路由。

```
ip route 192.168.1.0 255.255.255.0 Serial0/1/0
ip route 10.60.2.0 255.255.255.0 Serial0/1/0
```

8. 在配置 ACL 前，测试各 PC 机之间能否 ping 通及其互通性。

9. 为 RouterB 配置扩展 ACL 表并应用到端口。

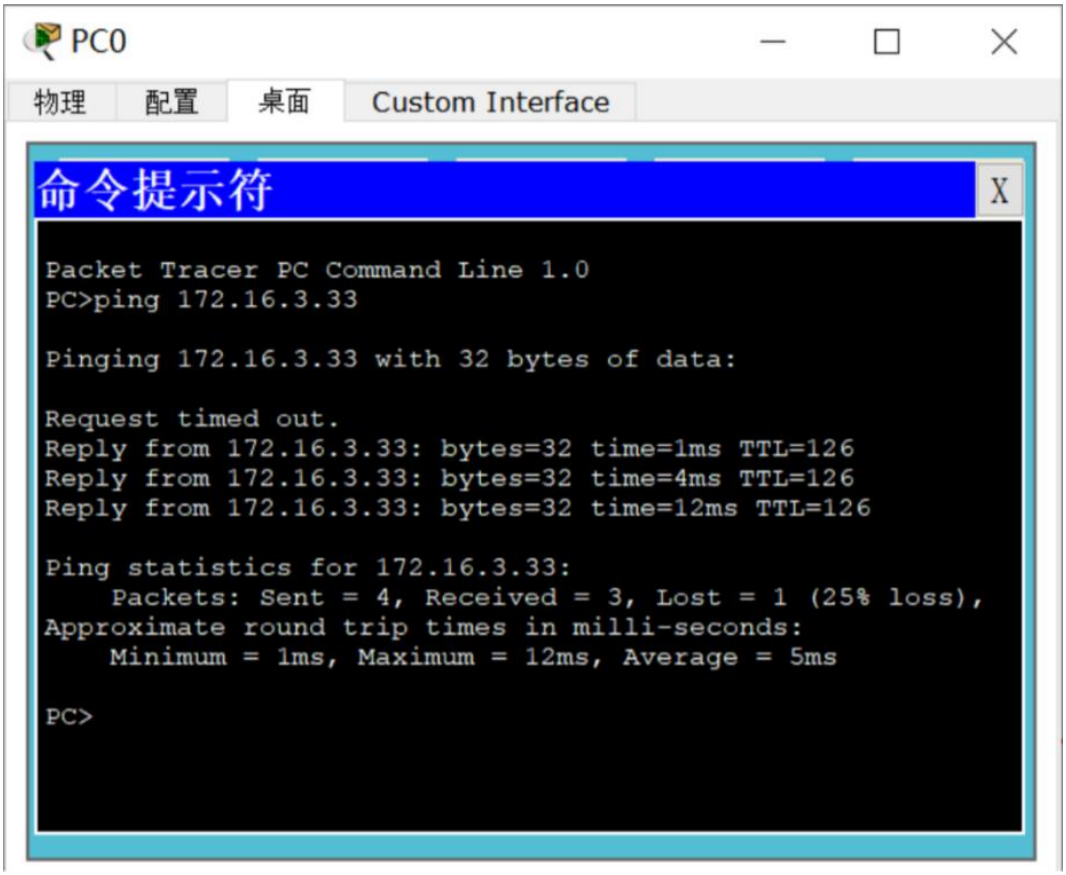
```
access-list 101 deny icmp host 192.168.1.11 host 172.16.3.33
access-list 101 permit tcp host 192.168.1.11 \
    host 172.16.3.33 eq www
interface Serial0/1/0
ip access-group 101 in
```

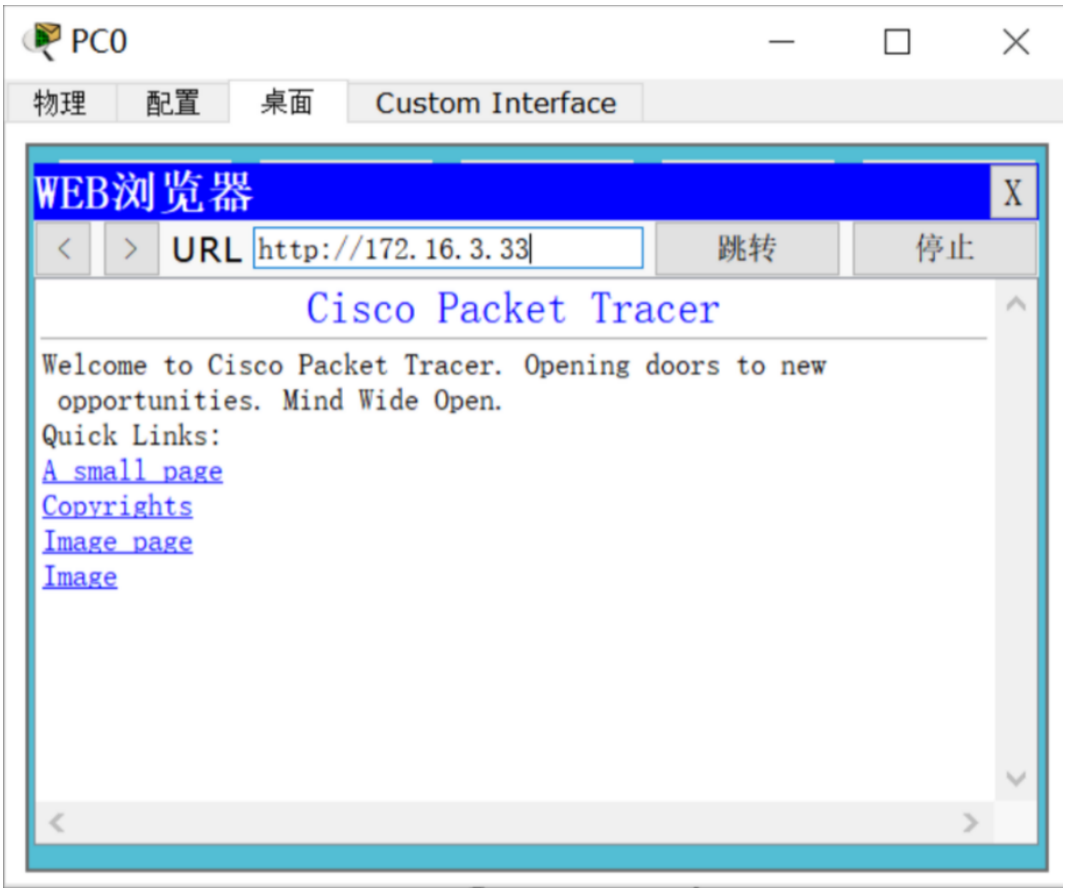
10. 在配置 ACL 后，测试各 PC 机之间能否 ping 通及其互通性。

【实验现象】

1. 在配置 ACL 前，测试各 PC 机之间能否 ping 通及其互通性。实验结果表明各

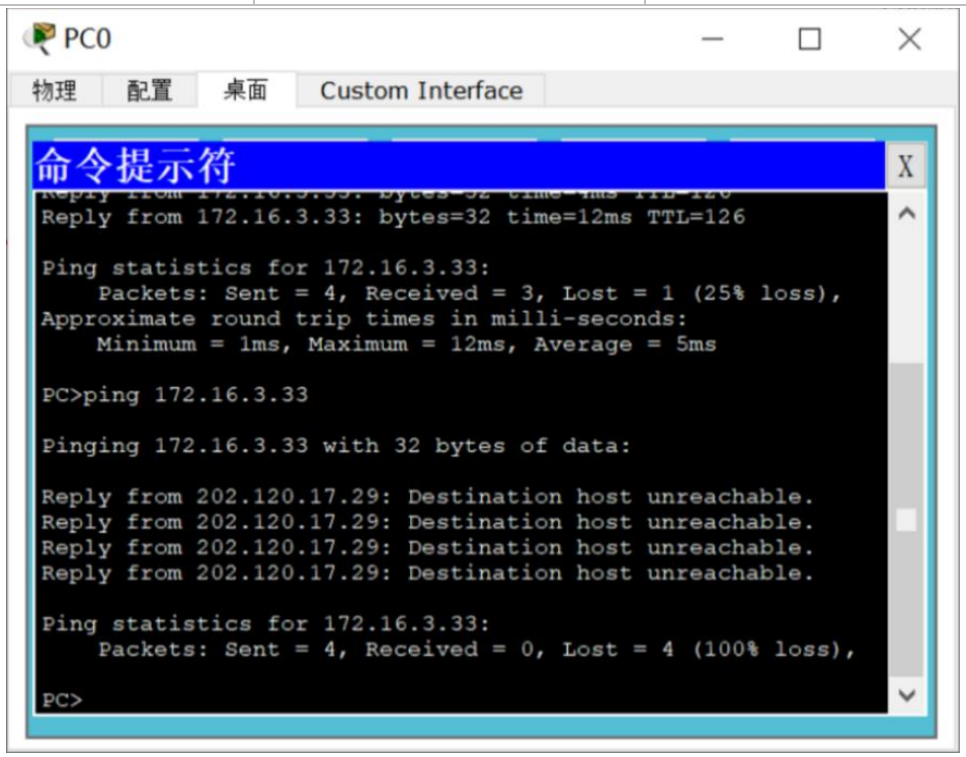
PC 机之间均访问成功。

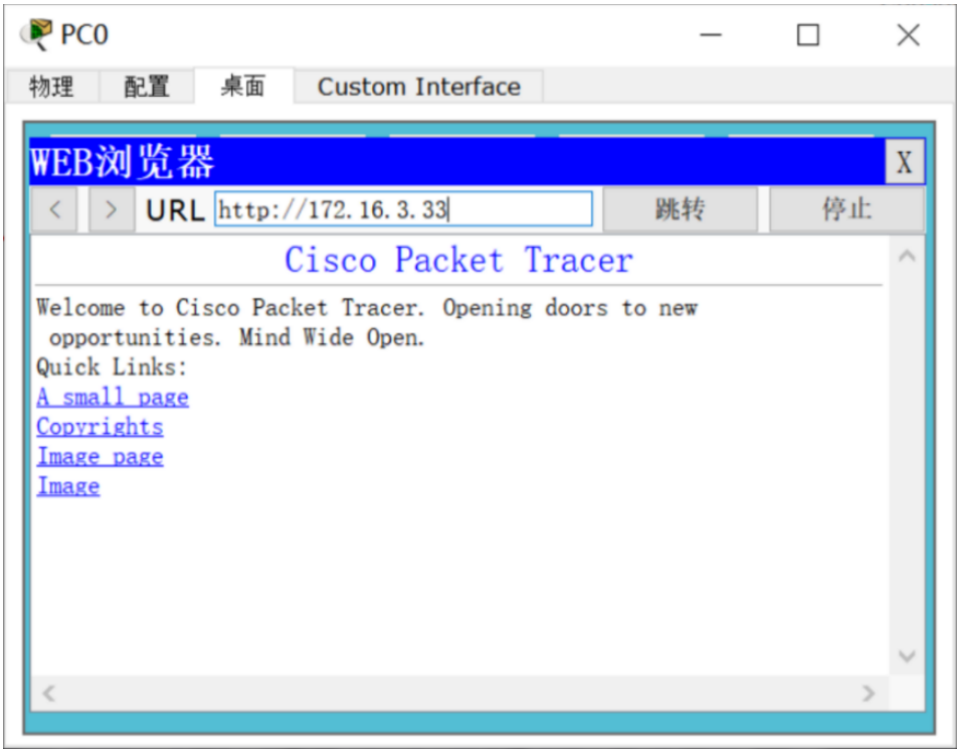

PC0
物理
配置
桌面
Custom Interface
命令提示符
X
Packet Tracer PC Command Line 1.0
PC>ping 172.16.3.33
Pinging 172.16.3.33 with 32 bytes of data:
Request timed out.
Reply from 172.16.3.33: bytes=32 time=1ms TTL=126
Reply from 172.16.3.33: bytes=32 time=4ms TTL=126
Reply from 172.16.3.33: bytes=32 time=12ms TTL=126
Ping statistics for 172.16.3.33:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 12ms, Average = 5ms
PC>


PC0
物理
配置
桌面
Custom Interface
WEB浏览器
X
URL
http://172.16.3.33
跳转
停止
Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image

2. 在配置 ACL 后，测试各 PC 机之间能否 ping 通及其互通性。

PC	ping	http
PC0	失败	成功
PC1	失败	失败
PC2	成功	成功





【分析讨论】

实验结果清楚地展示了 ACL（接入控制列表）配置对路由器网络通信行为的直接影响。通过本次实验，可以观察到不同的 ACL 规则对网络数据包传输的控制效果，特别是如何影响网络中各个 PC 机的互通性。

一、PC0 的观察结果

PC0 可以成功发起 HTTP 请求，但不能成功执行 ping 操作。这个行为是 ACL 规则直接结果，其中明确拒绝了来自 PC0 的 ICMP 包（ping 使用 ICMP 协议），但允许了 TCP 协议下的 WWW 请求（HTTP 请求）。这种配置演示了 ACLs 如何细粒度地控制网络访问，允许特定类型的网络流量同时阻止其他类型，从而增强网络的安全性和特定服务的可用性。

二、PC1 的观察结果

PC1 的所有网络请求（包括 HTTP 和 ping）均失败。这表明 ACL 中可能存在更为严格的规则，完全阻断了从 PC1 出发的网络请求。这种情况可能是由于额外的 ACL 规则设置，或者 PC1 的网络配置本身存在问题导致无法通过 ACL 的检查。这也提示了 ACL 配置需要精确，错误的规则可能导致不必要的通信阻断。

三、PC2 的观察结果

PC2 在 ACL 配置前后均能成功执行 ping 和 HTTP 请求，表明它没有受到任何 ACL 规则的限制。这显示了 ACL 规则可以被设置为仅对网络中特定节点或通信类型生效，而不影响其他节点的正常通信。