实验(十八)：ACL访问控制实验

一.实验目的

实验的目的是通过配置和应用标准和扩展的IP ACL来控制和管理网络流量，提高网络的可管理性和安全性。具体来说，实验涉及规划网络地址和拓扑，配置网络设备（如PC机、服务器和路由器）的IP地址，设置静态路由，以及配置和应用ACL。实验的最终目标是验证通过ACL配置后，主机之间的互通性和对特定服务（如WWW）的访问控制，从而展示ACL在防止未授权访问和网络攻击中的效用。

- 理解接入控制列表 (ACLs) 的原理和功能。
- 学习如何配置标准和扩展的 IP 访问列表。
- 验证 ACL 配置对网络访问的影响。

二.实验原理

- 这个实验基于接入控制列表（ACL）的技术原理，通过实际的配置和测试来探索其在网络环境中的作用。ACL主要用于网络设备接口上，对通过的数据包进行检查和控制，可以允许或拒绝特定的数据流，从而提升网络的安全性和管理性。
- 实验中，会使用两种类型的IP ACL：
    - **标准IP访问列表**：这种类型的ACL主要基于数据包的源IP地址进行过滤，对网络流量进行基本的控制，适用于简单的访问控制场景。
    - **扩展IP访问列表**：扩展的ACL提供更细致的控制选项，不仅基于源IP地址，还可以根据目的IP、源端口、目的端口和使用的协议来过滤数据包。这使得扩展ACL能够更精确地控制网络流量，适用于需要详细访问规则的复杂网络环境。
- 接口应用: IP ACL在接口上应用时，分为入栈和出栈两种方式。

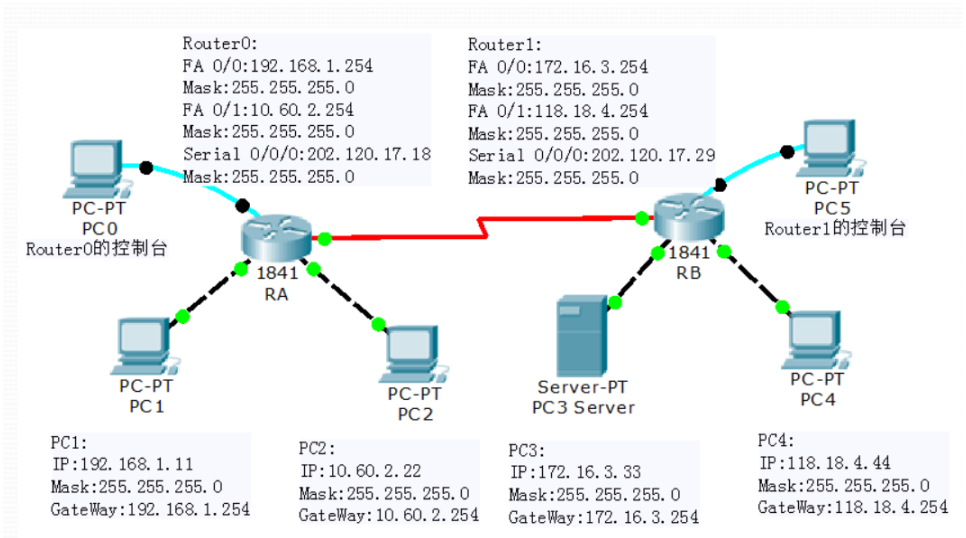
实验中，ACL将会被配置在路由器的相应接口上，并根据规则允许或拒绝特定的通信。例如，可以配置规则以阻止来自特定IP地址的ping请求，或允许来自某个IP地址的HTTP访问。通过这样的配置，可以验证ACL如何实际影响网络中的数据流通和访问控制，从而加深对网络安全技术应用的理解。

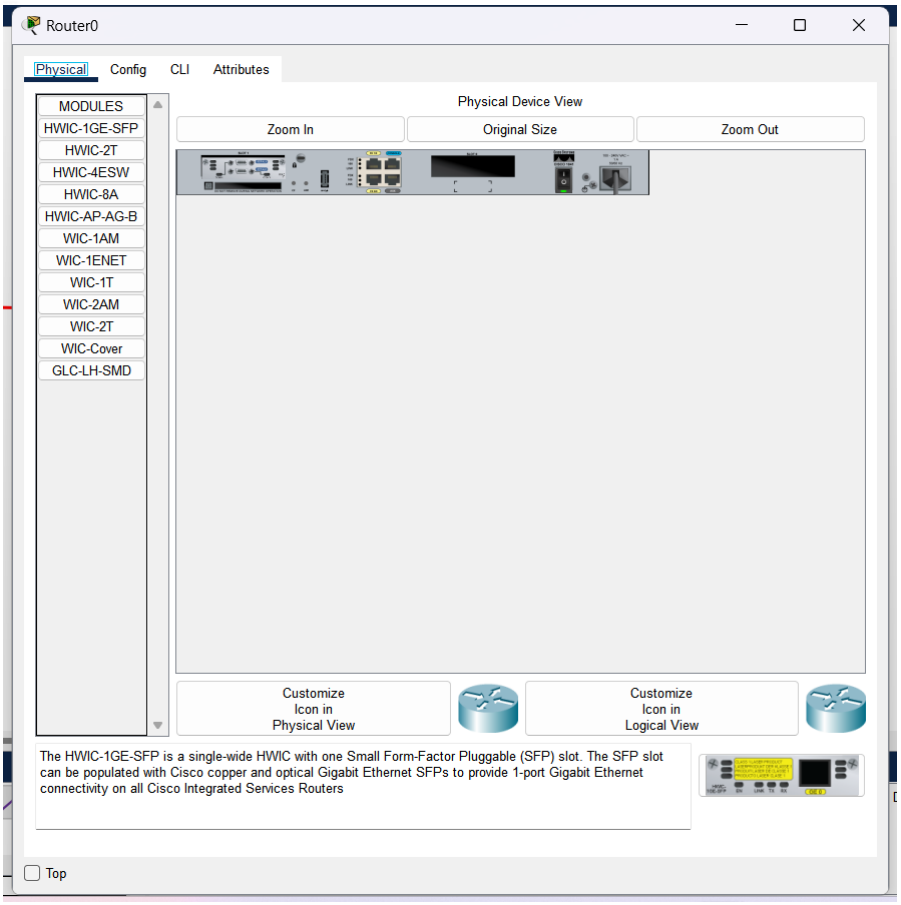
三.实验环境

- 操作系统：Windows 11
- 网络环境：局域网
- 软件：`Cisco Packet Tracer`虚拟实验环境

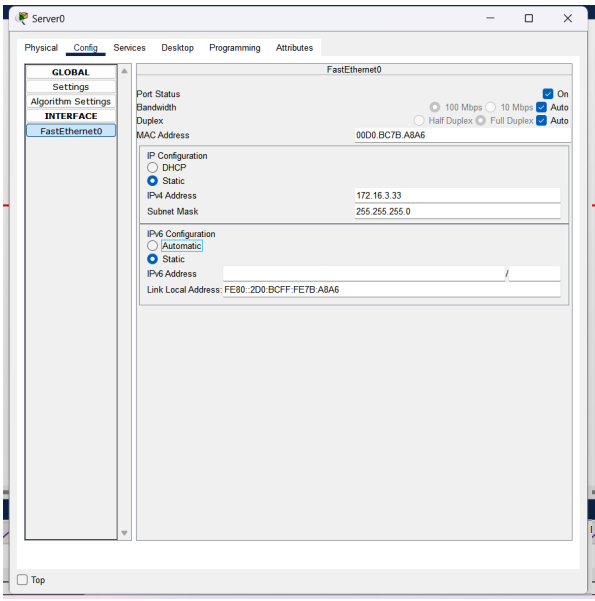
四.实验步骤

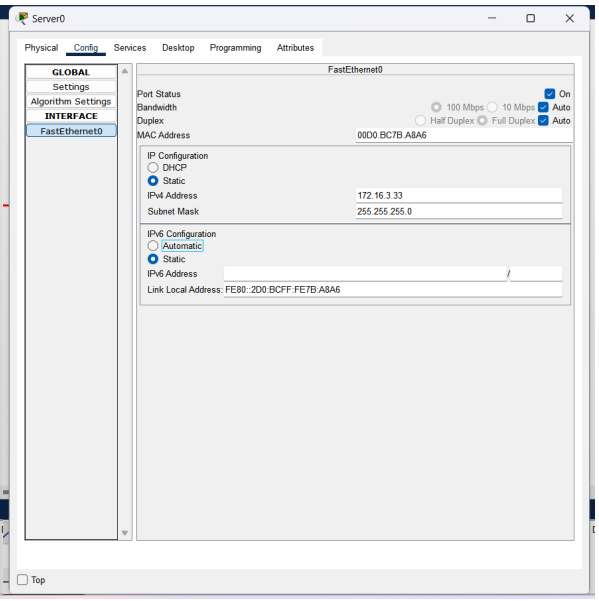
- 按照如下的网络拓补图，连接链路

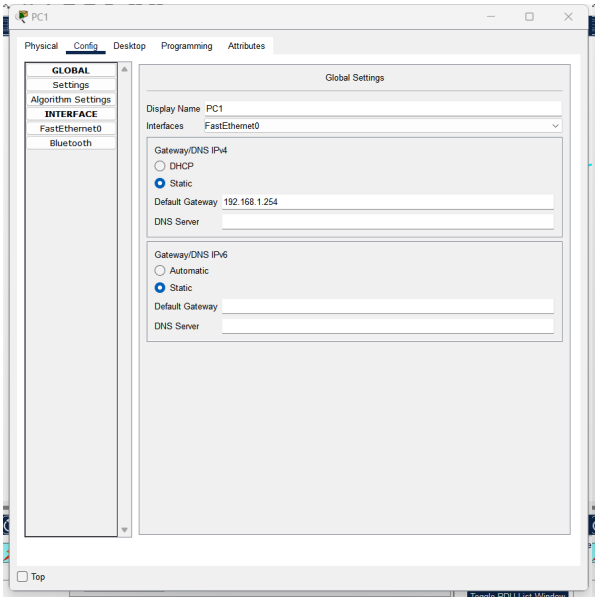


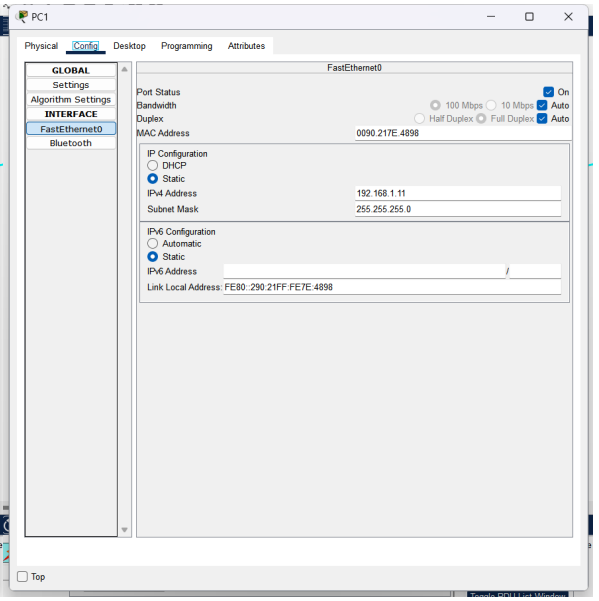


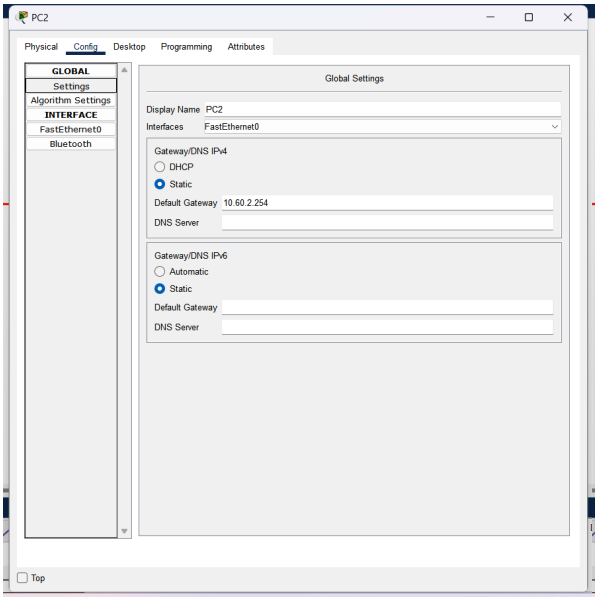
- 按照网络拓补图配置PC、服务器的地址、网关和掩码

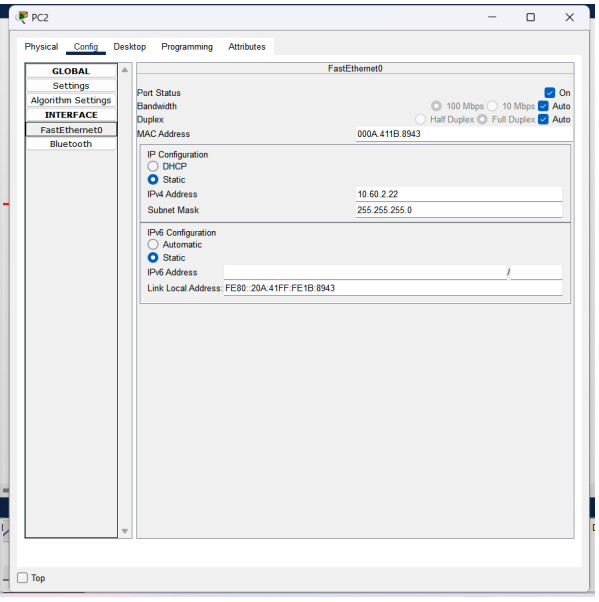

Server0
Physical
Config
Services
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BC7B.A8A6
IP Configuration
DHCP
Static
IPv4 Address
172.16.3.33
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::2D0:BCFF:FE7B:A8A6
Top

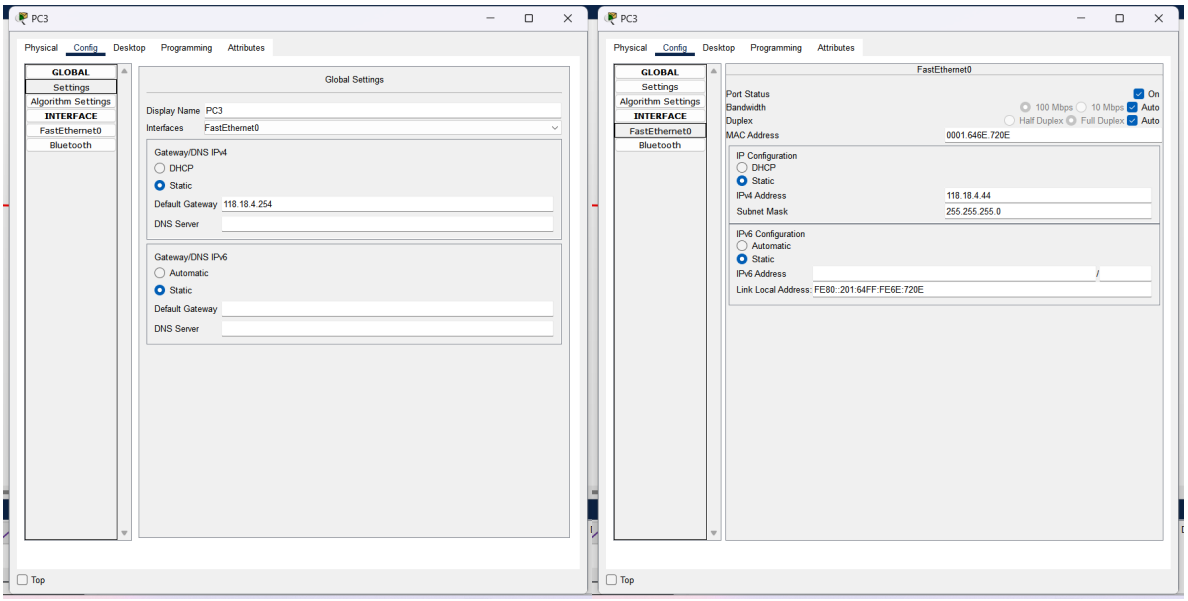

Server0
Physical
Config
Services
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BC7B.A8A6
IP Configuration
DHCP
Static
IPv4 Address
172.16.3.33
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::2D0:BCFF:FE7B:A8A6
Top


PC1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
Global Settings
Display Name
PC1
Interfaces
FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.1.254
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top


PC1
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0090.217E.4898
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.11
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::290:21FF:FE7E:4898
Top

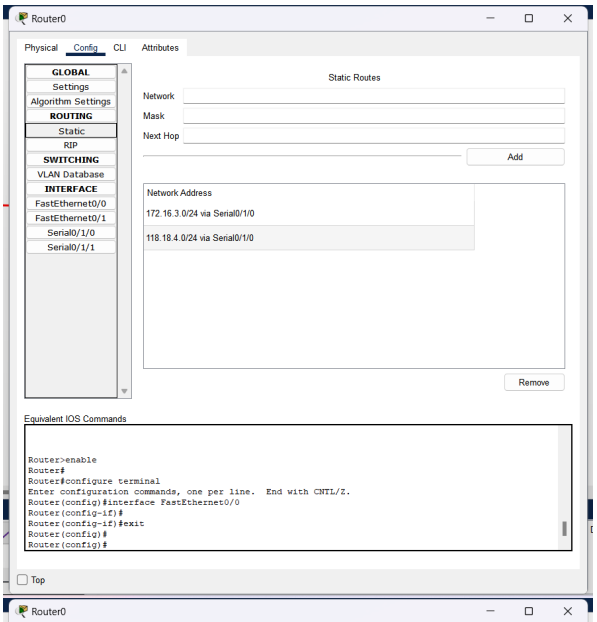

PC2
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
Global Settings
Display Name
PC2
Interfaces
FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
10.60.2.254
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top

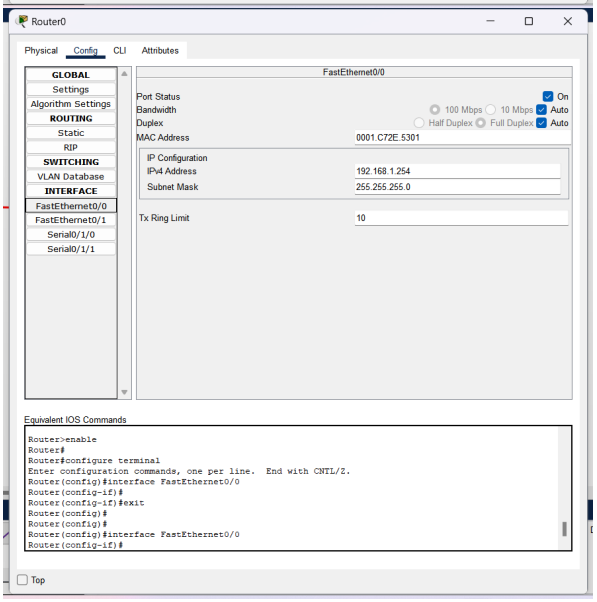

PC2
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
FastEthernet0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
000A.411B.8943
IP Configuration
DHCP
Static
IPv4 Address
10.60.2.22
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::20A:41FF:FE1B:8943
Top

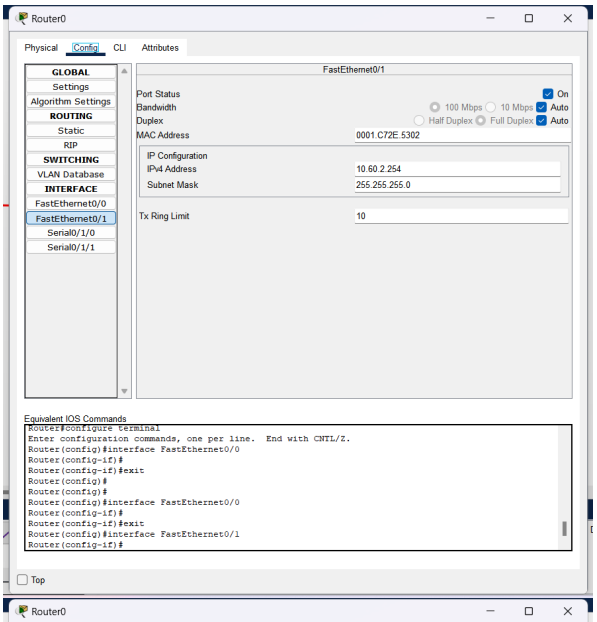


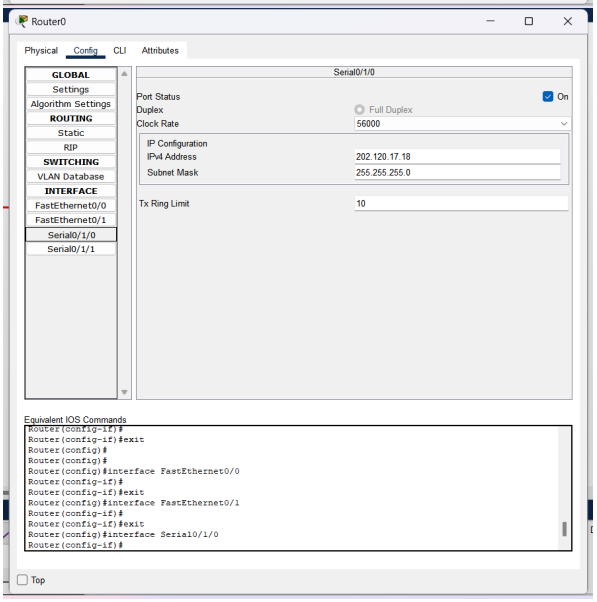
- 配置路由器的端口地址、串口地址、静态路由表
  - 对于Router0而言，在CLI中输入以下指令

```
//配置端口地址
enable
configure terminal
interface FastEthernet0/0
ip address 192.168.1.254 255.255.255.0
no shutdown
exit
interface FastEthernet0/1
ip address 10.60.2.254 255.255.255.0
no shutdown
//配置串口地址
enable
configure terminal
interface Serial0/1/0
ip address 202.120.17.18 255.255.255.0
clock rate 56000
no shutdown
//配置静态路由表
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
```


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/1/0
Serial0/1/1
Static Routes
Network
Mask
Next Hop
Add
Network Address
172.16.3.0/24 via Serial0/1/0
118.18.4.0/24 via Serial0/1/0
Remove
Equivalent IOS Commands
Router>enable
Router#
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)#
Router(config)#
Top

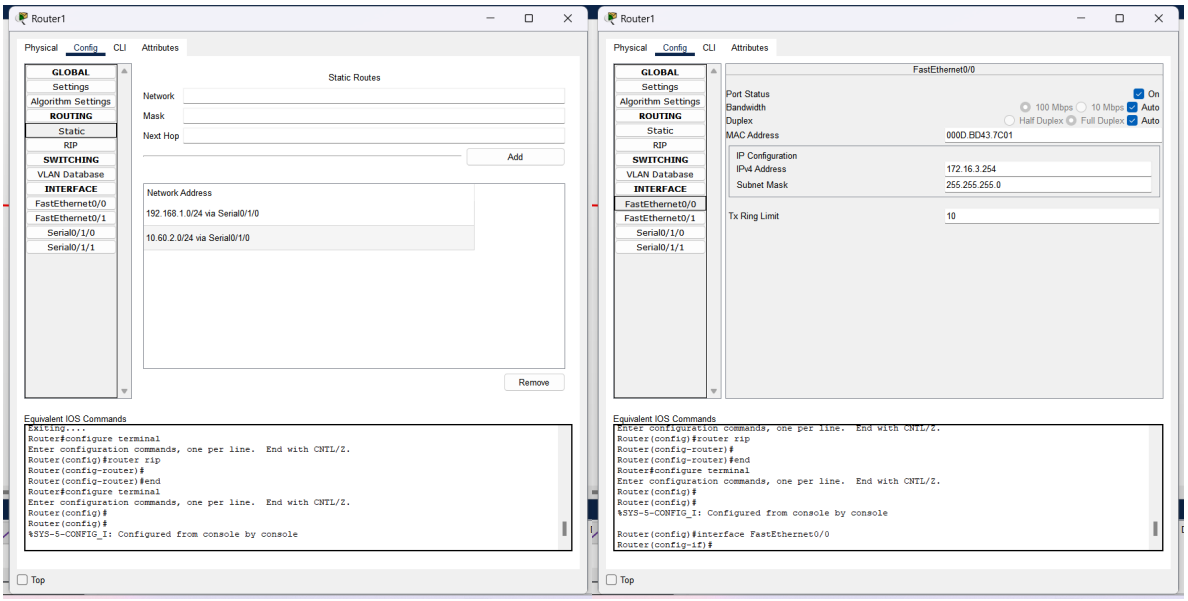

Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
0001.C72E.5301
IP Configuration
IPv4 Address
192.168.1.254
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
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)#
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#
Top

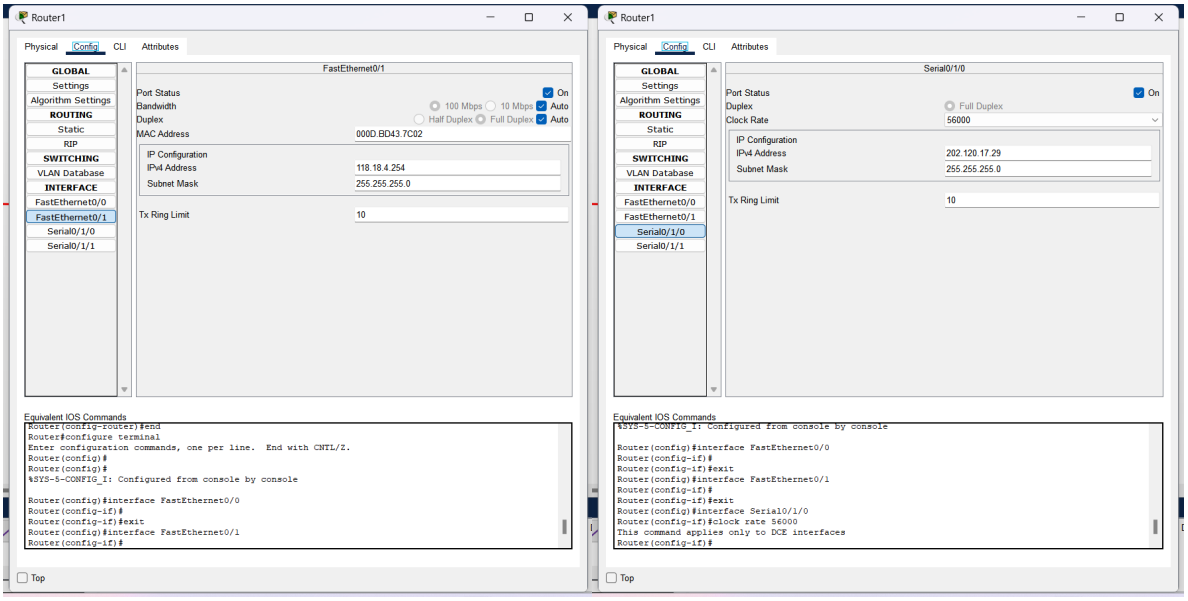




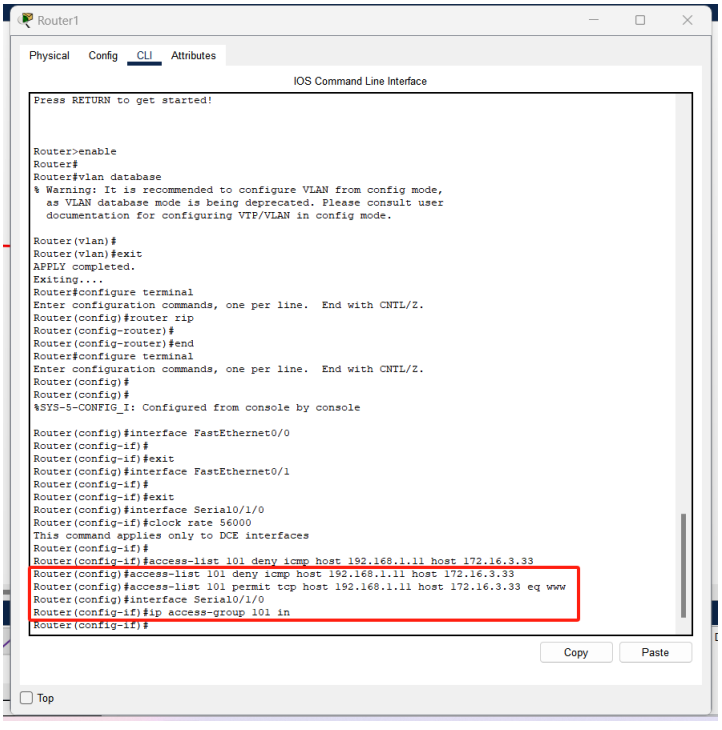
- 对于Router1而言，在CLI中输入以下指令

```
//配置端口地址
enable
configure terminal
interface FastEthernet0/0
ip address 172.16.3.254 255.255.255.0
no shutdown
exit
interface FastEthernet0/1
ip address 118.18.4.254 255.255.255.0
no shutdown
//配置串口地址
enable
configure terminal
interface Serial0/1/0
ip address 202.120.17.29 255.255.255.0
clock rate 56000
no shutdown
//配置静态路由表
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
```





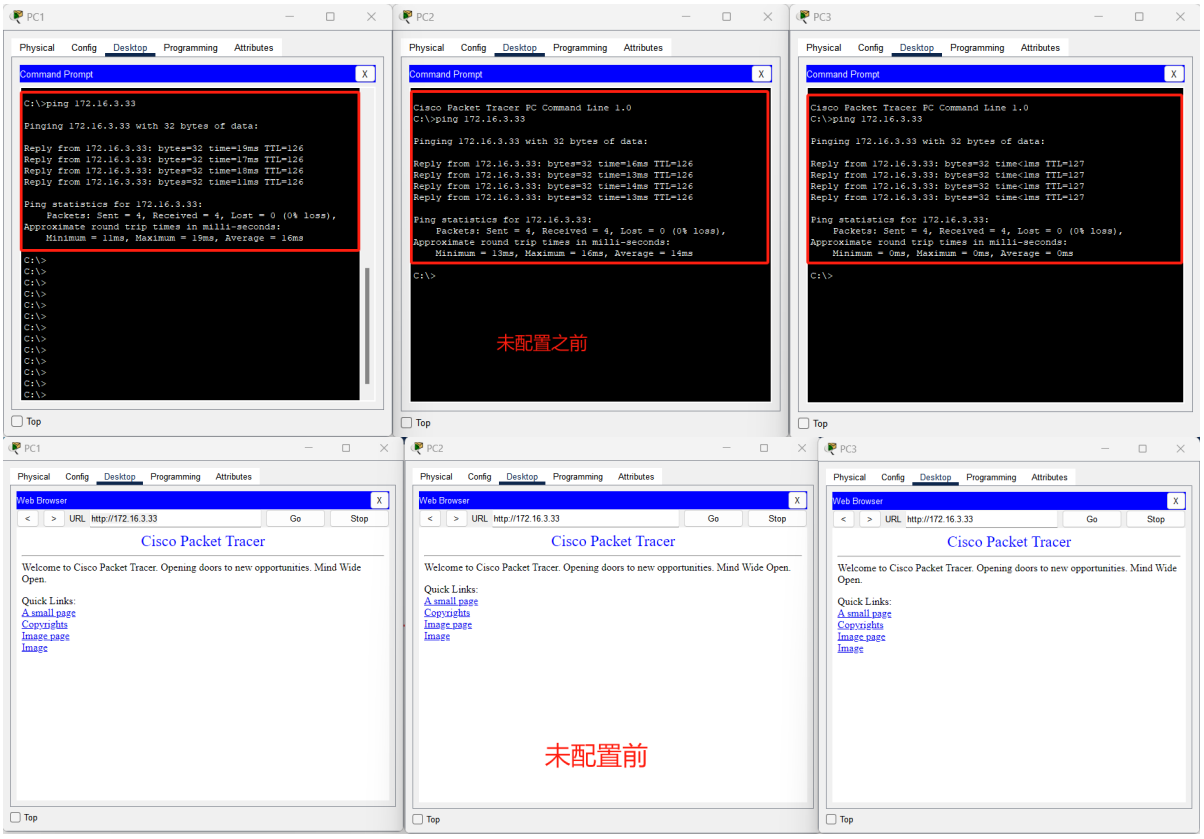
- 在其他PC上访问`172.16.3.33`服务器（通过`ping`和`http`方法），并观察结果
- 配置Router1的ACL表



- 在其他PC上重新尝试访问 `172.16.3.33` 服务器（通过 `ping` 和 `http` 方法），并观察结果

五、实验现象

- 配置ACL前，各PC访问服务器均成功



- 配置ACL后，访问各个PC端，结果如下表所示

PC	ping	http
PC1	失败	成功
PC2	失败	失败
PC3	成功	成功

六、实验结论

- 本实验通过在路由器上逐步配置访问控制列表（ACL）并观察其对网络通信的具体影响，展示了ACL在网络管理中的关键作用和强大功能。实验中明确展示了通过精确设计ACL策略可以确保网络的安全性和稳定性。具体操作包括对特定数据流的限制，例如阻止来自某台PC（PC1）的ping请求，同时允许其发起http请求，而对另一台PC（PC2）的所有请求进行拦截，而第三台PC（PC3）则未受到任何限制。
- 结果表明：
  - PC1的ping请求因ACL规则而失败，但其http请求成功通过，证明ACL成功区分了不同类型的网络请求。
  - PC2的所有网络访问尝试均未成功，可能是因为ACL中存在特定规则阻止了其访问，或其网络配置存在问题。
  - PC3的网络访问完全成功，表明其未受ACL影响。这一实验结果突出了ACL在进行细粒度网络访问控制时的有效性和重要性。