ACL控制访问

冯巾松

fengjinsong@tongji.edu.cn

ACL技术原理

- ACLs (Access Control Lists)，全称为接入控制列表，也称为访问列表（Access Lists），俗称为防火墙，有的文档中还称之为包过滤

- ACLs 通过定义一些规则对网络设备接口上的数据报文进行控制：允许通过或丢弃，从而提高网络可管理性和安全性

ACL规则

- ACL的语句顺序决定了对数据包的控制顺序。在ACL中各描述语句的放置顺序是很重要的。当路由器决定某一数据包是被转发还是被阻塞时，会按照各项描述语句在ACL中的顺序，根据各描述语句的判断条件，对数据包进行检查，一旦找到了某一匹配条件就结束比较过程，不再检查以后的其他条件判断语句；

- ACL的默认操作是“全部拒绝”，所以在ACL里一定至少有一条“允许”的语句

ACL的3P规则

- 3P 规则是指在路由器上应用ACL的一般规则，即可以为每种协议 (per protocol)、每个方向 (per direction)、每个接口 (per interface) 配置一个ACL；

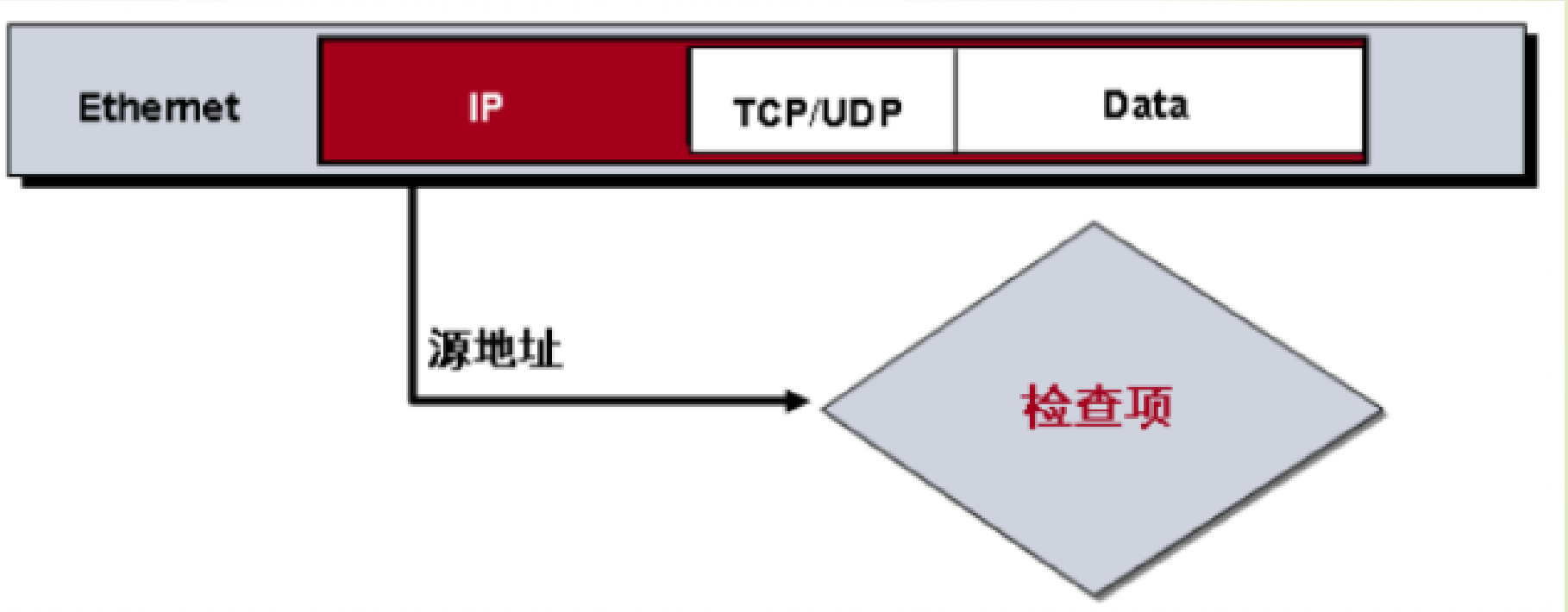
- 例如：一个ACL只能控制接口上一个方向的流量。要控制入栈流量和出栈流量，必须分别定义两个ACL来实现。

ACL的分类

- 根据定义字段（元素）
  - ✓ 标准ACL（标准IP ACL）
  - ✓ 扩展ACL（扩展IP ACL、MAC ACL、专家ACL）
- 根据定义的层次
  - ✓ 基于IP的ACL（ IP ACL ）
  - ✓ 基于MAC的ACL（ MAC ACL ）
  - ✓ 专家ACL（Expert ACL）
- 根据命名规则
  - ✓编号ACL
  - ✓命名ACL（即使用名称代替表号）

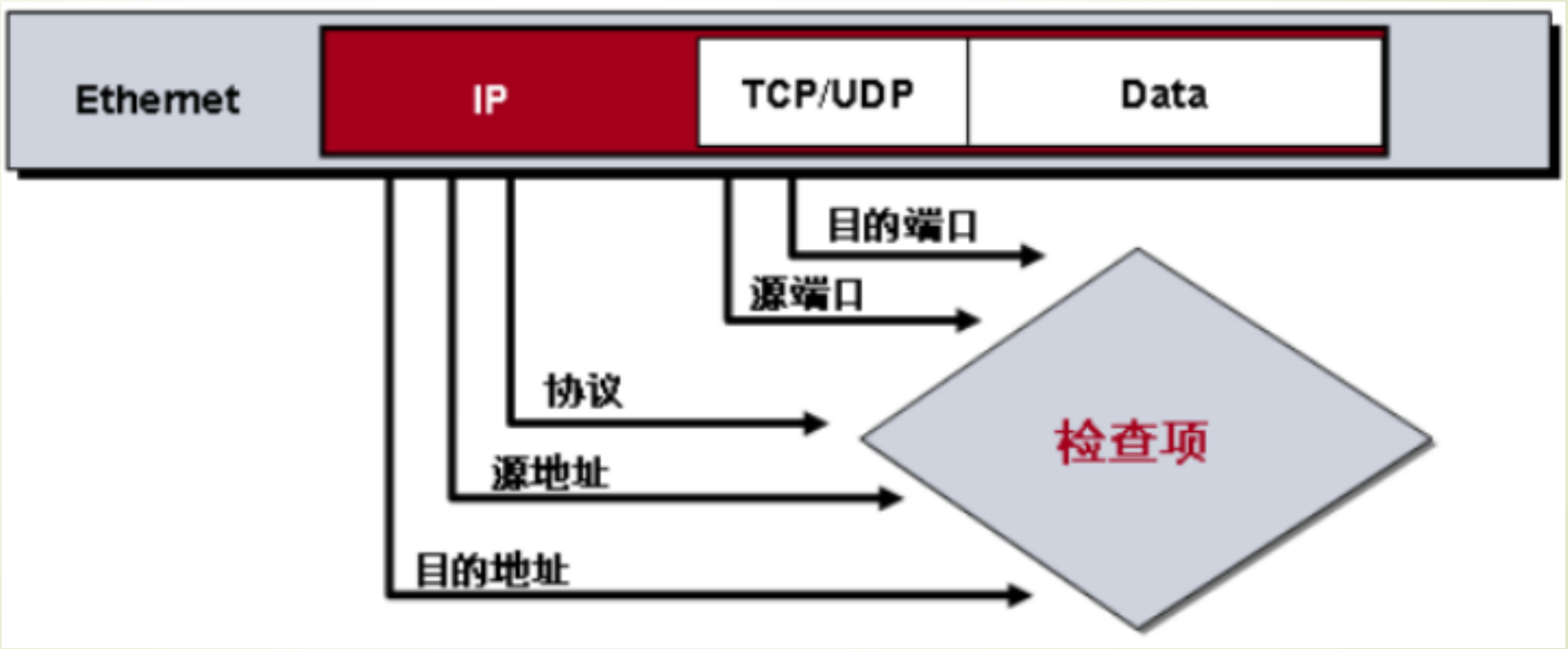
标准IP ACL

- 编号是1-99、1300-1999
- 定义元素：源IP地址信息
- 用于简单的访问控制、路由过滤等



扩展IP ACL

- 编号范围分别是100-199、2000-2699
- 定义元素：源IP地址、目的IP、 源端口、目的端口、协议
- 用于高级、精确的访问控制



access-list［编号］permit［IP地址］［通配符］

Access-list命令(标准ACL)

- 基本格式

access-list [编号] [permit/deny] [source address] [wildcard mask] [log]

- permit表示允许数据包通过，deny表示拒绝数据包通过；
- wildcard mask使用通配符掩码来指定主机或网络。
  - ✓ 在通配符掩码位中，0 表示“检查数据包的 IP 地址相对应的比特位”，1 表示“不检查（忽略）数据包中的IP 地址相对应的比特位”
  - ✓ 通配符“any”：代替 0.0.0.0 255.255.255.255，代表所有主机
  - ✓ 通配符 host：与整个 IP 主机地址的所有位相匹配，可以使用缩写字“host”

Access-list(标准ACL)命令举例

- 创建一个标准的ACL，允许HTTP流量通过

access-list 99 permit tcp any any eq www

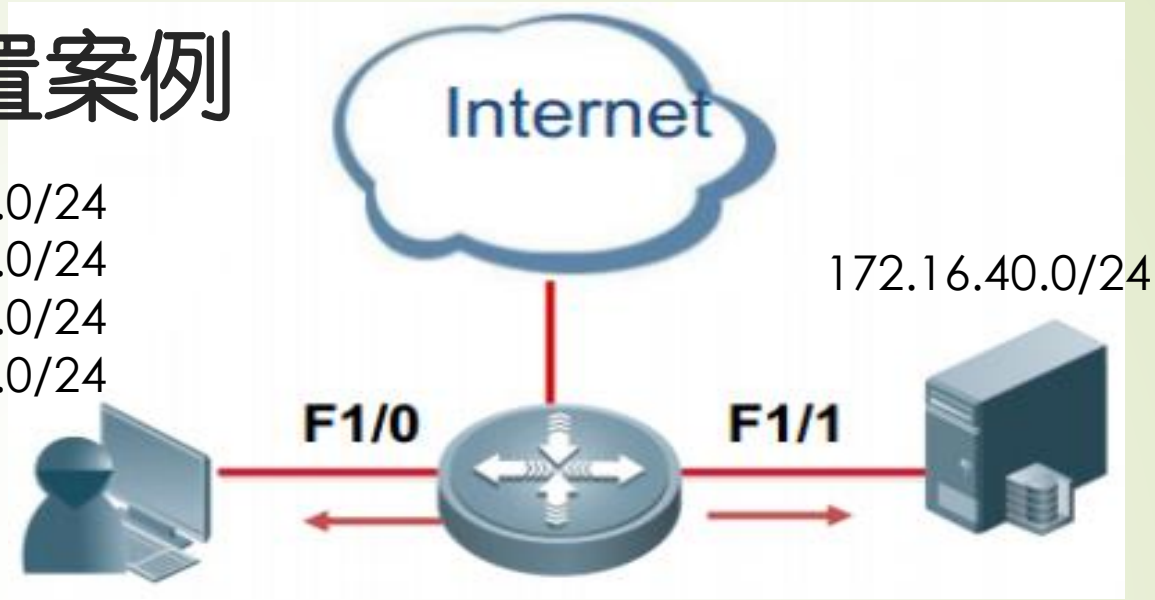
协议类型

指所有源和目的地址之间的TCP端口为80（HTTP）的流量

- access-list 1 permit ip 192.168.1.0 0.0.0.255 any

此命令首先拒绝所有其他IP地址的数据包，但允许来自192.168.1.0/24网络的数据包通过

标准ACL配置案例



需求

1.只允许172.16.3.0/24的主机访问172.16.40.0/24的服务器

2，其他网段访问Internet不受影响

```
Router(config)#ip access-list standard ACL1 //表名ACL1
Router(config-std-ACL1)#permit 172.16.3.0  0.0.0.255
Router(config-std-ACL1)#exit
Router(config)#interface f1/1
Router(config)#ip access-group 1 out
```

Access-list命令(扩展ACL)

- 基本格式

access-list [100-199][permit/deny] protocol source-ip source-wildcard [operator port] destination-ip destination-wildcard [operator port] [established] [log]

- access-list 表号[permit | deny]协议+源地址+源反码+目的地址+目的反码+操作+端口号
- operator（操作）有 lt（小于）、gt（大于）、eq（等于）、neq（不等于）几种；port指的是端口号。

Access-list(扩展ACL)命令举例

- Router(config)#access-list 100 deny icmp any any

拒绝所有icmp包，第一个any表示的是源的所有主机，第二个any表示的是目的的所有主机

- access-list 100 deny udp any any eq 134

拒绝端口等于134的所有udp包

- Router(config)#access-list 100 deny ip 172.16.0.0 0.0.255.255 192.168.1.0 0.0.0.255

不允许源为172.16.0.0的主机与192.168.1.0通信

IN 与 OUT

- 对路由其接口来说有两个方向：

IN：已经到达路由器接口的数据包，但是还没有被路由器处理。

OUT：已经 经过路由器的处理，正要离开路由器接口的数据包

应用ACL到端口

- Router(config-if)#ip access-group 100 in|out
- Router(config-if)#ip access-group acl1 in|out

显示/查看命令

- 显示全部的访问控制列表
Router#show access-lists

- 显示指定的访问控制列表
Router#show access-lists <1-199>

- 显示接口的访问列表应用
Router#show access-group interface 接口号

删除ACL

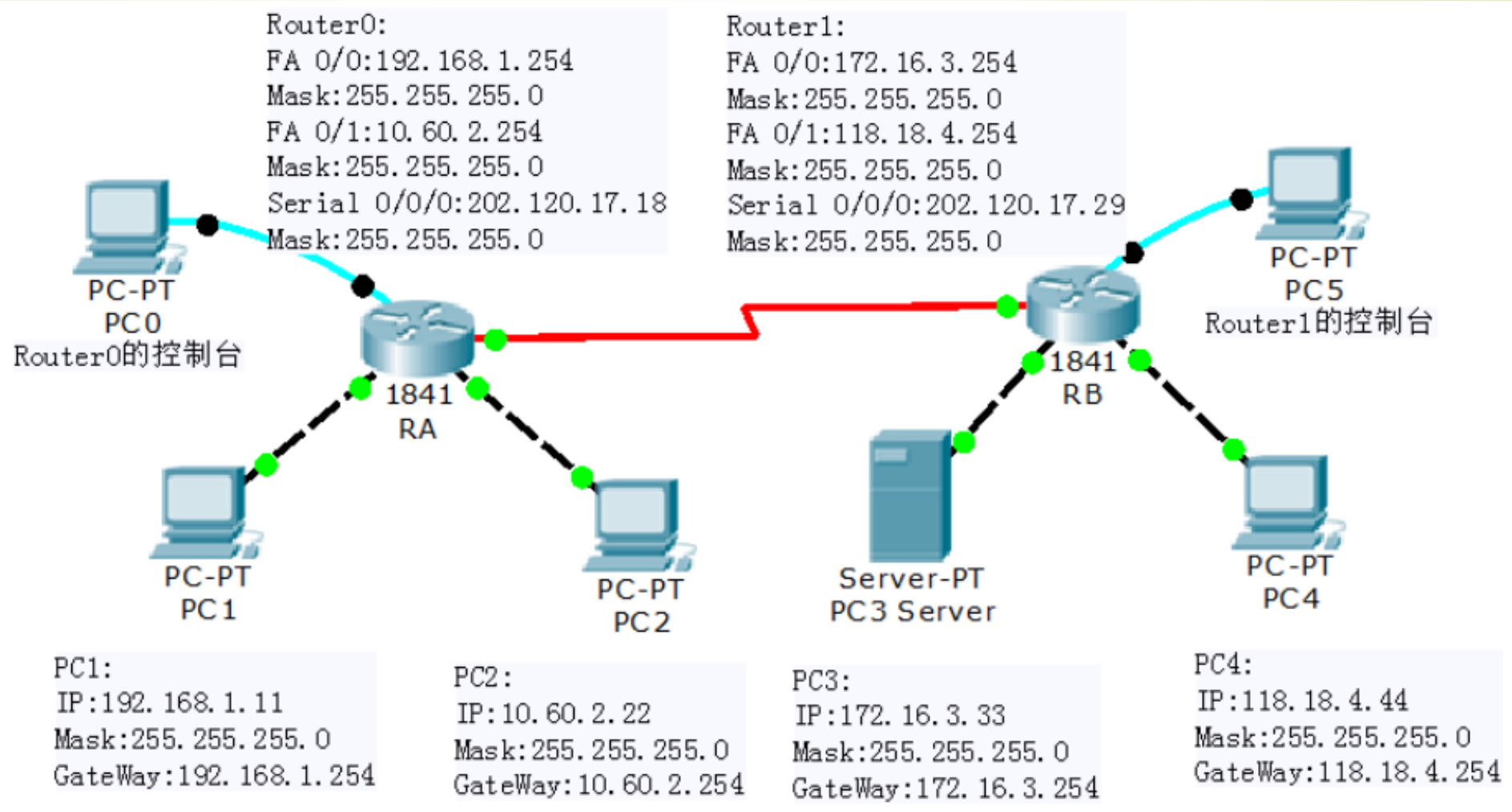
```
Router(config-std-nacl)#do show access-lists
Standard IP access list 10
    20 deny host 192.168.1.1
    30 deny host 192.168.1.2
    40 permit any
Router(config)#ip access-list standard 10
                                        //进入acl表10
Router(config-std-nacl)#no 30
Router(config-std-nacl)#do show access-lists
Standard IP access list 10
    20 deny host 192.168.1.1
    40 permit any
```

实验步骤

- 1 首先规划网络地址及拓扑图
- 2 配置PC机、服务器及路由器口IP地址
- 3 验证各PC间的互通性
- 4 各路由器上配置静态路由协议,使全网可达
- 5 验证各PC间能否相互 ping通
- 6 在RB上配置ACL：
  A,除PC1以外的电脑能ping通PC3；
  B,只有PC1可以通过WWW访问PC3；
- 7 在端口上应用ACL；
- 8 验证主机之间的互通性
- 9 查看控制访问列表

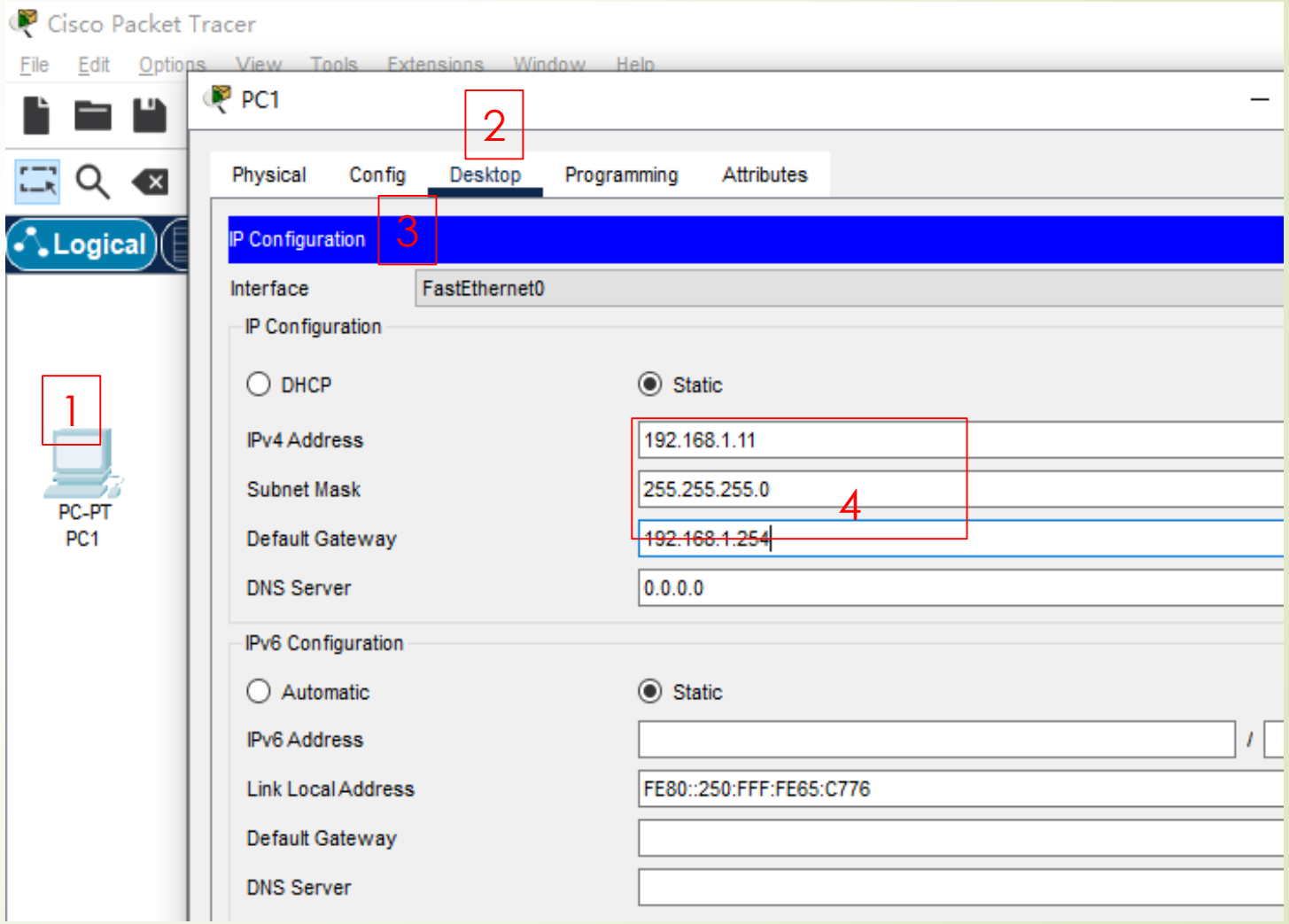
步骤1，

- 网络拓扑及地址规划



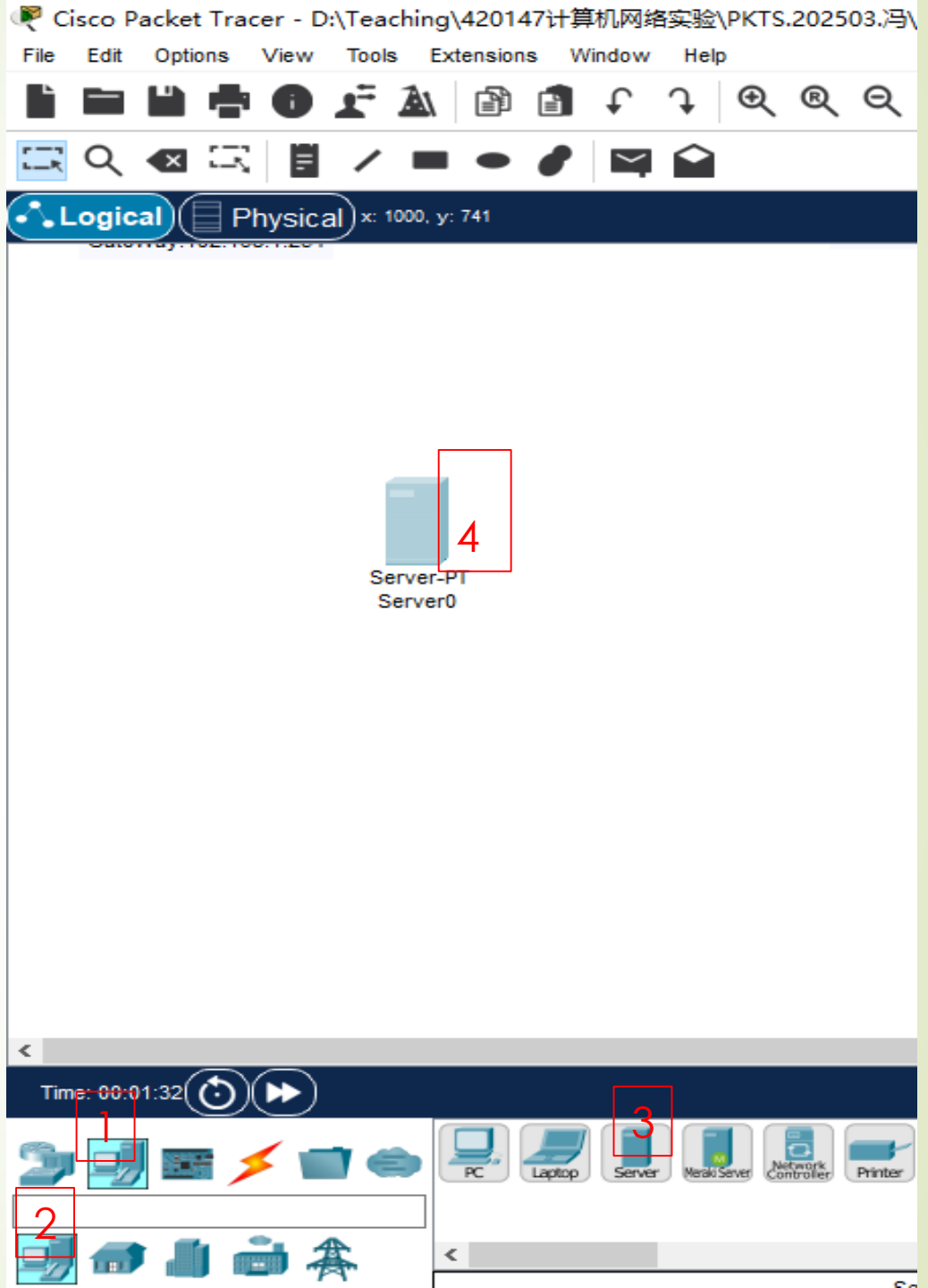
步骤2

- 配置好各PC的地址、网关及掩码；以PC1为例



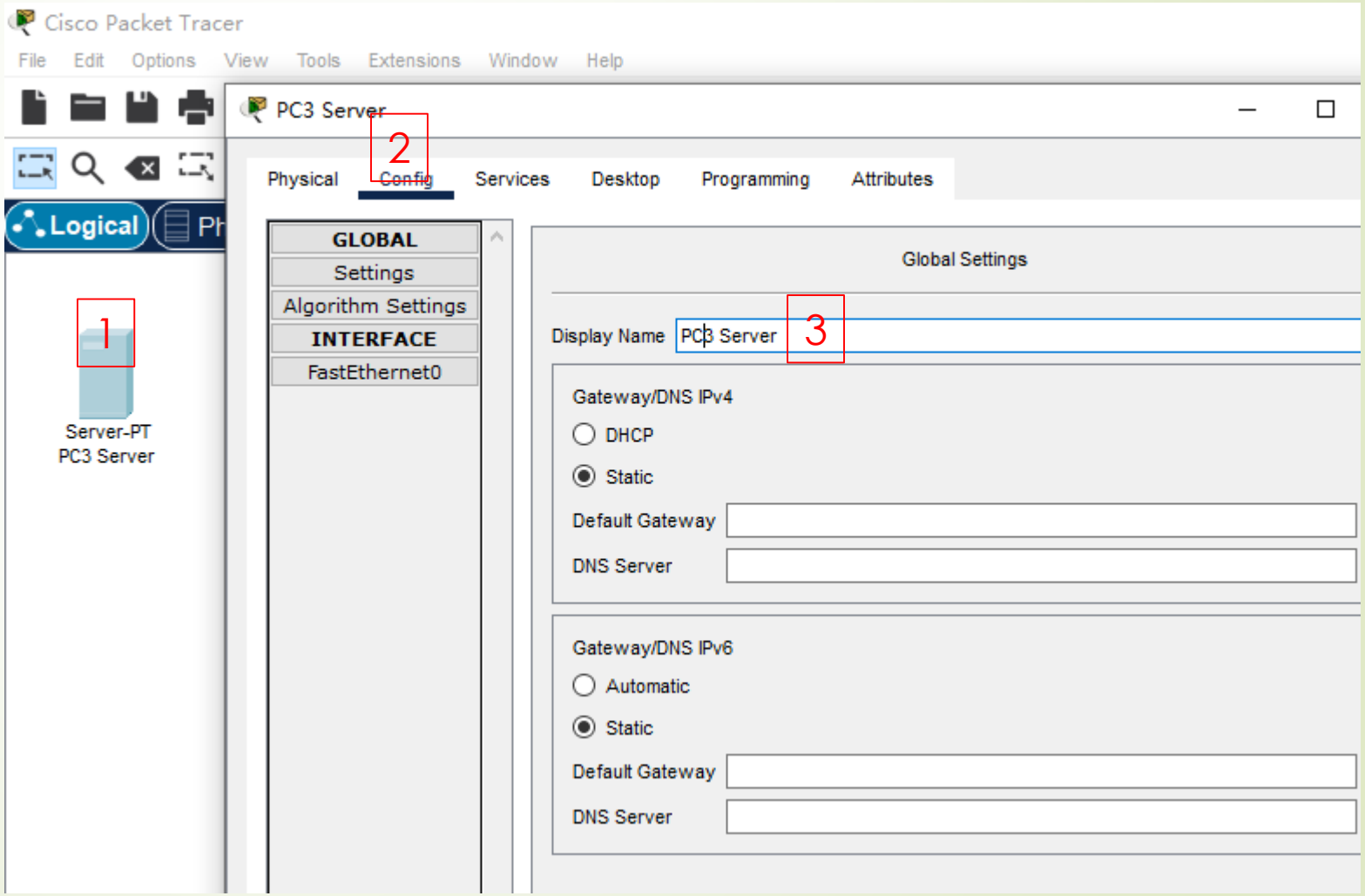
步骤2

- 添加Server-PT



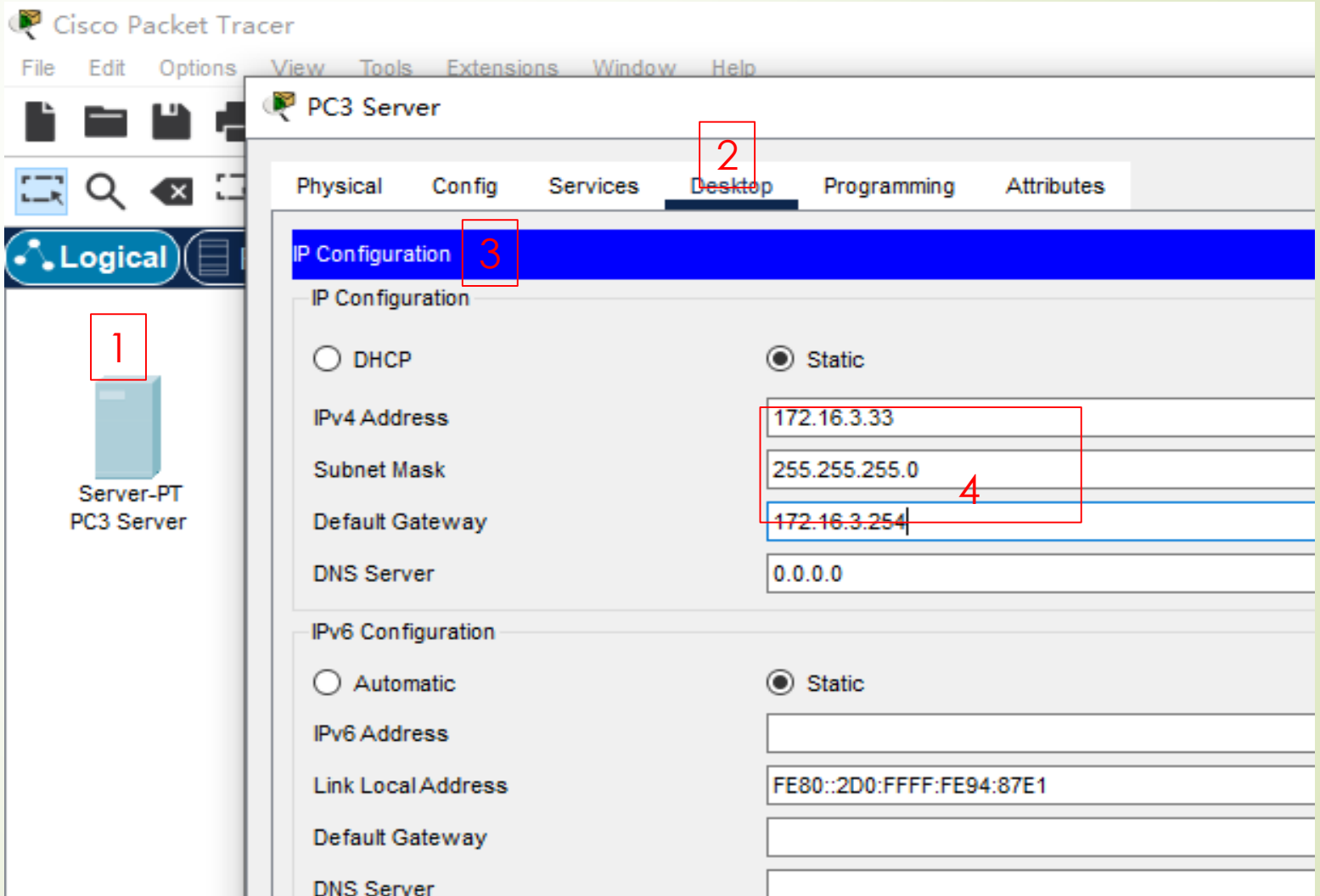
步驟2

- Server-PT重命名（Server1 -> PC3 Server)

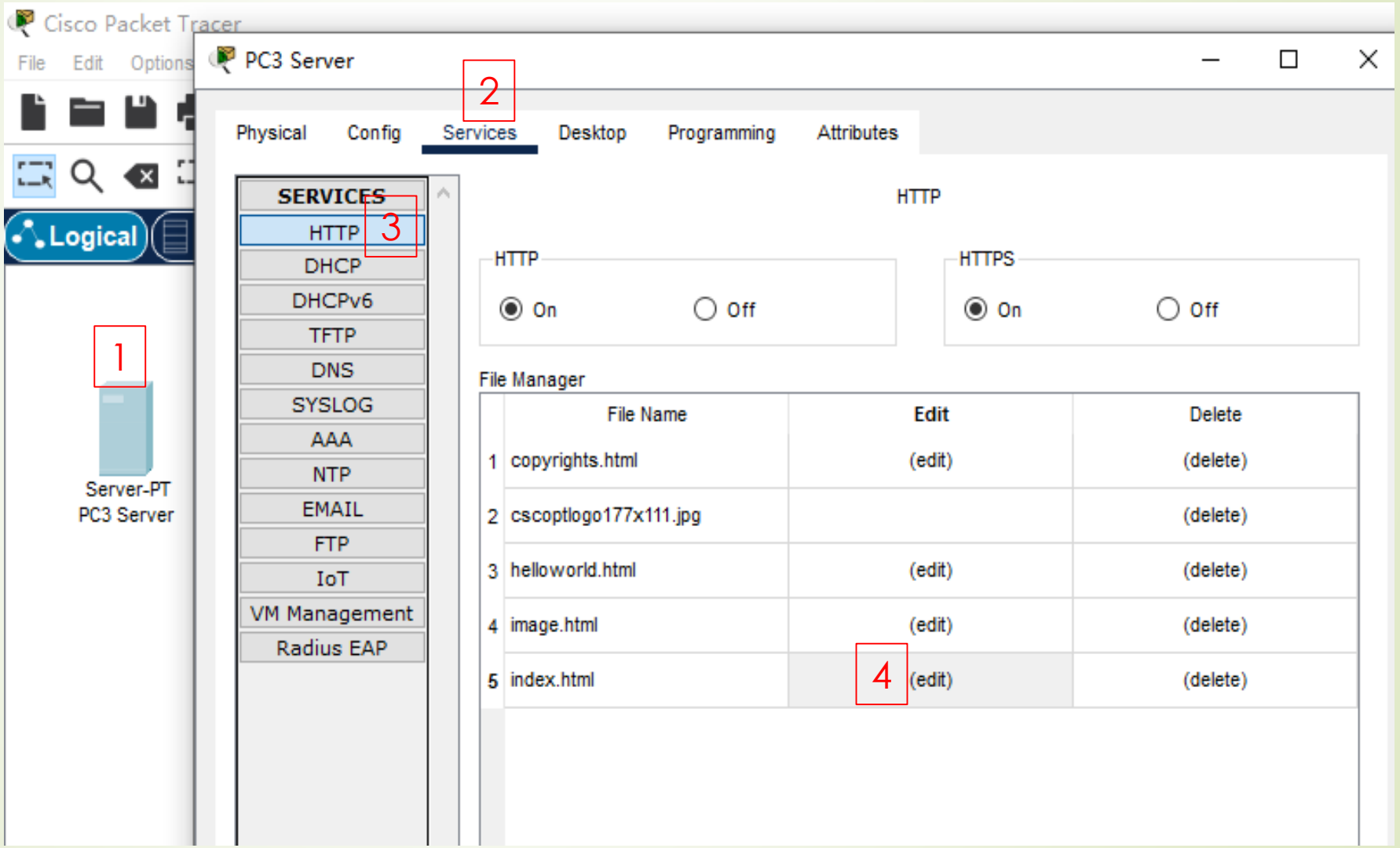


步骤2

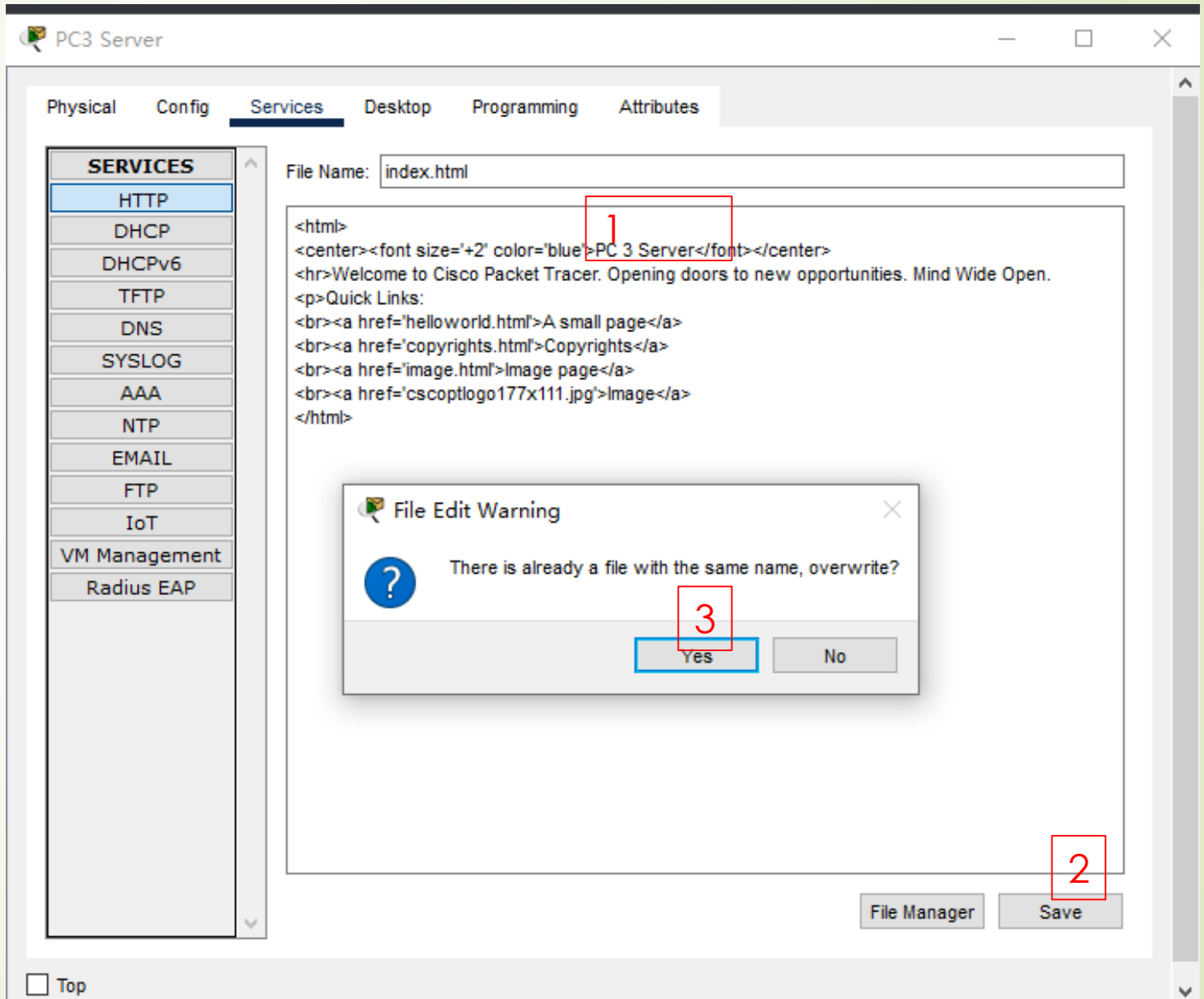
- Server-PT (PC3 Server)配置好IP、网关及掩码



网页标题更新，便于识别


Cisco Packet Tracer
File Edit Options
Logical
1
Server-PT
PC3 Server
PC3 Server
2
Physical Config Services Desktop Programming Attributes
SERVICES
HTTP
3
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
HTTP
HTTP
On Off
HTTPS
On Off
File Manager
File Name Edit Delete
1 copyrights.html (edit) (delete)
2 cscoptlogo177x111.jpg (delete)
3 helloworld.html (edit) (delete)
4 image.html (edit) (delete)
5 index.html 4 (edit) (delete)

网页标题更新为PC3 Server，便于识别



步骤2

- 配置路由器RA的端口地址；

```
interface FastEthernet0/0
 ip address 192.168.1.254 255.255.255.0
 no shutdown
 interface FastEthernet0/1
 ip address 10.60.2.254 255.255.255.0
 no shutdown
 interface Serial 0/0/0
 ip address 202.120.17.18 255.255.255.0
 Clock rate 56000
no shutdown
```

- 路由器RB：指令类似

步骤4

- 配置路由器的静态路由表

路由器RA：

ip route 172.16.3.0 255.255.255.0 Serial0/0/0

ip route 118.18.4.0 255.255.255.0 Serial0/0/0

路由器RB：指令类似

步骤6

- 配置路由器RB的扩展ACL表：

A.拒绝ping包：

RB(config)#access-list 101 deny icmp host 192.168.1.11
源地址（PC1）
host172.16.3.33
目标地址（PC1）

B.允许www访问：

RB(config)#access-list 101 permit tcp host 192.168.1.11
host 172.16.3.33 eq www

步骤7

- 应用到端口：

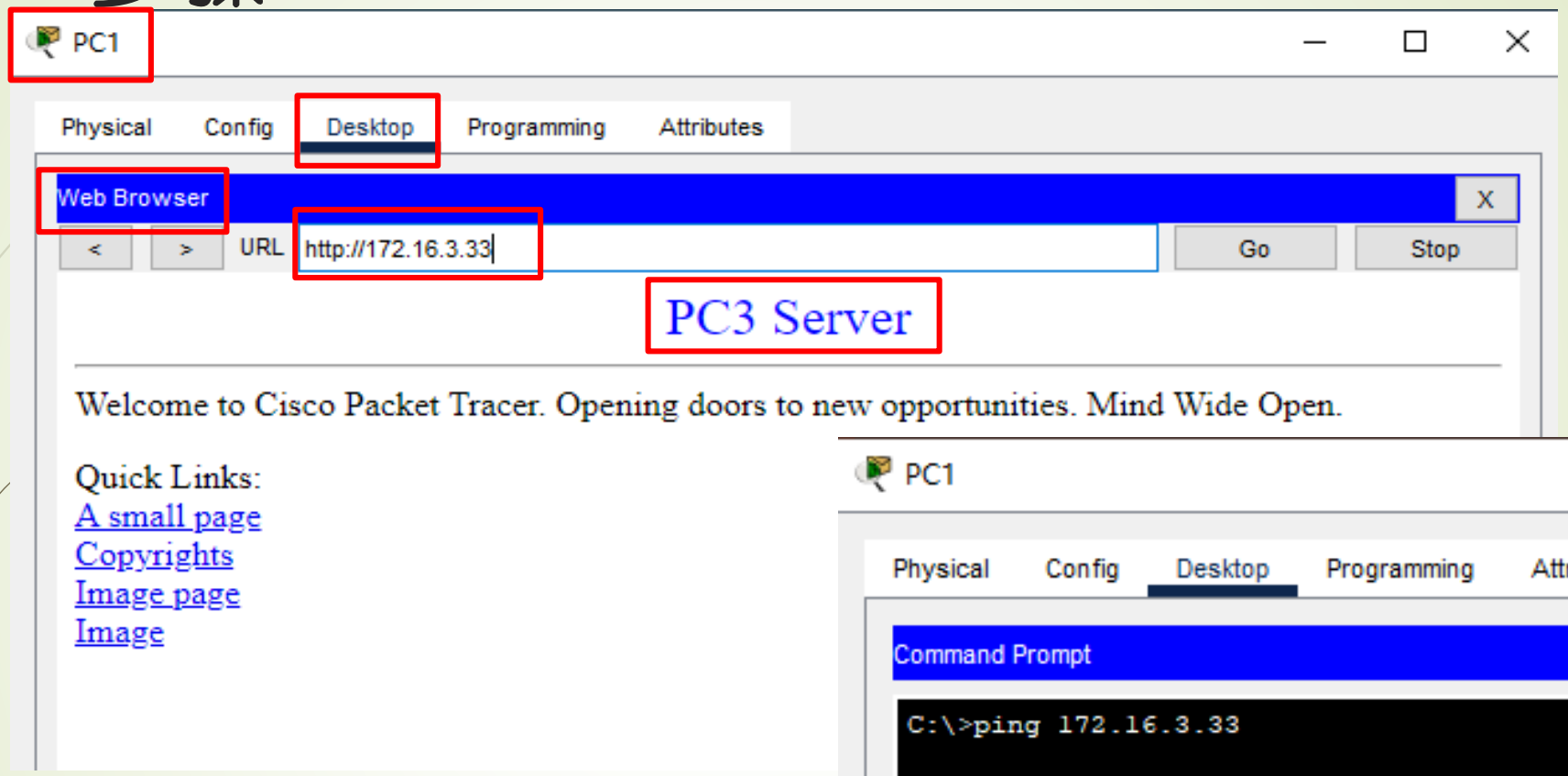
//首先进入路由器RB的Serial 0/0/0端口

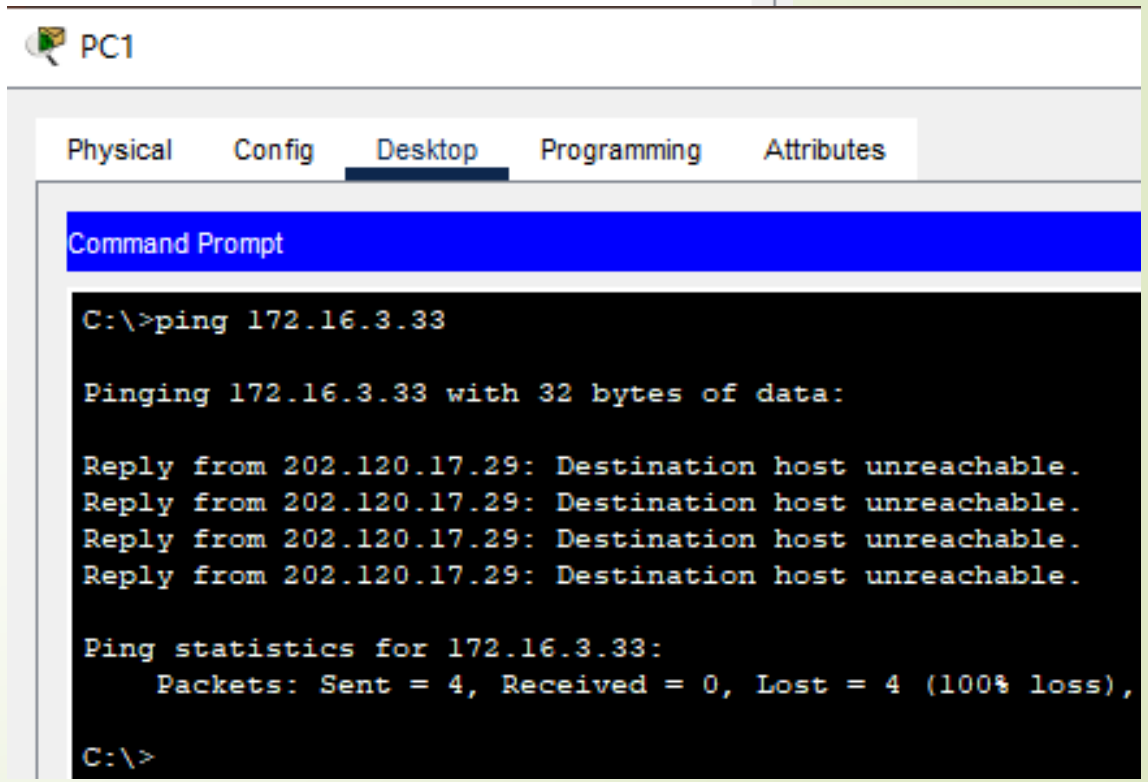
Router(config)#interface s0/0/0

//配置访问控制列表入栈流量控制

Router(config-if)#ip access-group 101 in

步驟8


PC1
Physical
Config
Desktop
Programming
Attributes
Web Browser
X
<
>
URL
http://172.16.3.33
Go
Stop
PC3 Server
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping 172.16.3.33
Pinging 172.16.3.33 with 32 bytes of data:
Reply from 202.120.17.29: Destination host unreachable.
Reply from 202.120.17.29: Destination host unreachable.
Reply from 202.120.17.29: Destination host unreachable.
Reply from 202.120.17.29: Destination host unreachable.
Ping statistics for 172.16.3.33:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>

问题分析讨论

- 打开172.16.3.33服务器端的WEB，并在其它PC端访问
1) Ping 172.16.3.33
2) http://172.16.3.33
3) 比较在配置ACL前后的区别。
- 如将步骤6中拒绝ping包的指令换成“access-list 101 deny icmp 192.168.1.0 0.0.0.255 host172.16.3.33”会有什么不同效果吗？分析说明原因