ACL访问控制

同济大学软件学院

技术原理（1）

技术原理

ACLs 的全称为接入控制列表(Access Control Lists)，也称为访问列表（Access Lists），俗称为防火墙，在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；

技术原理（2）

IP 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；

IP 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 在各路由器上配置静态路由协议，让pc间能相互ping通；

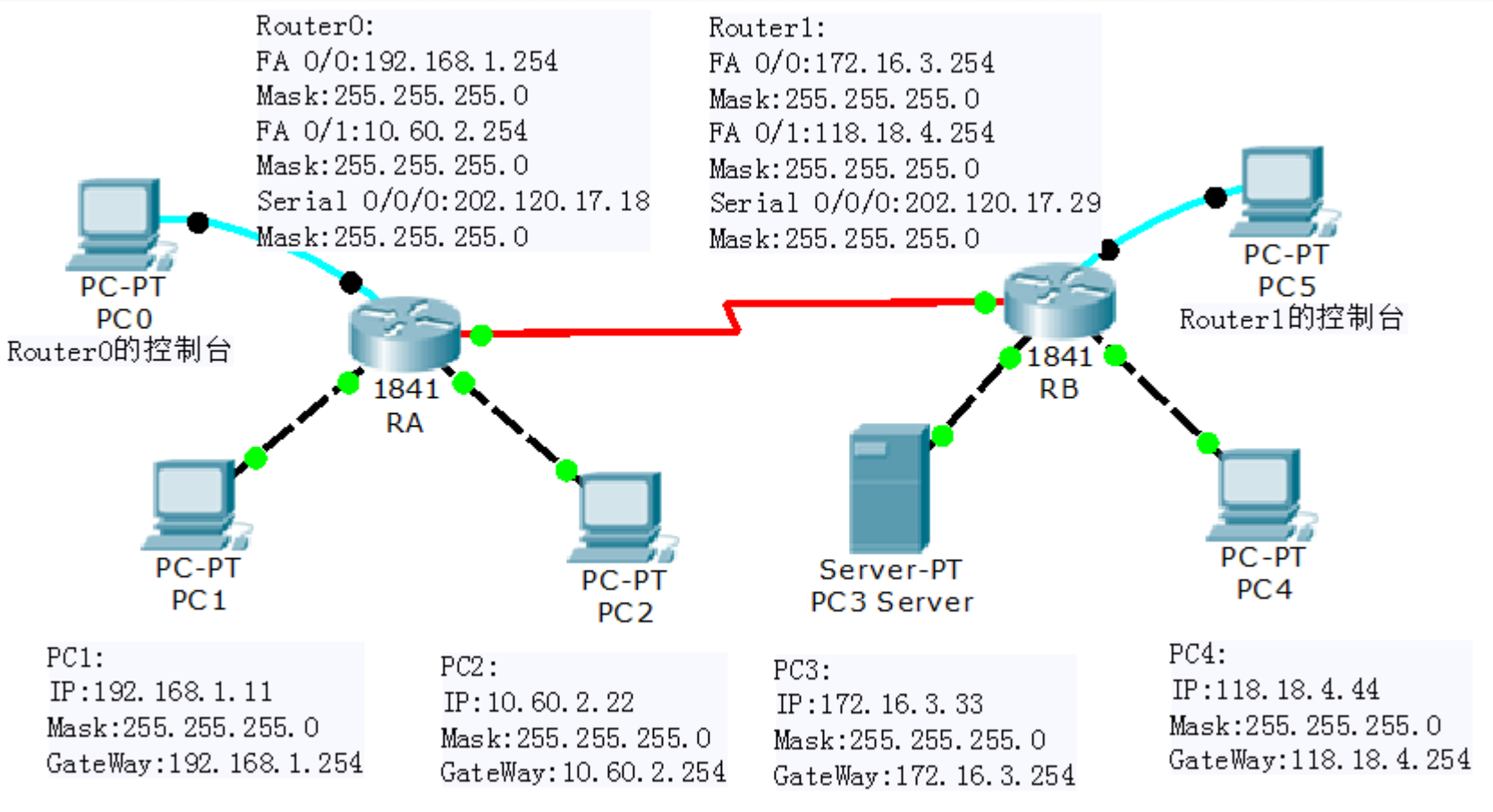
4 在RB上配置ACL；

5 在RB接口上应用ACL；

6 验证主机之间的互通性及WWW访问。

示例

- 网络拓扑及地址规划



实验过程（1）：

- （1）配置好PC的地址、网关及掩码；
- （2）配置路由器的端口地址；
- 路由器A： interface FastEtherneto/0
- ip address 192.168.1.254 255.255.255.0
- interface FastEtherneto/1
- ip address 10.60.2.254 255.255.255.0
- 路由器B： interface FastEtherneto/0
- ip address 172.16.3.254 255.255.255.0
- interface FastEtherneto/1
- ip address 118.8.4.254 255.255.255.0

注意：端口要no shutdown

实验过程（2）：

- （2）配置路由器的串口端口地址；
- 路由器A： interface Serial 0/0/0
- ip address 202.120.17.18 255.255.255.0
- Clock rate 56000
-
- 路由器B： interface Serial 0/0/0
- ip address 202.120.17.29 255.255.255.0
- Clock rate 56000
-

注意：端口要no shutdown

实验过程（3）：

- （3）配置路由器的静态路由表

  路由器A： 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B： ip route 192.168.1.0 255.255.255.0 Serial0/0/0

  ip route 10.60.2.0 255.255.255.0 Serial0/0/0

4 配置路由器B的扩展ACL表： 路由器B：

a. 拒绝ping包：

access-list 101 deny icmp host 192.168.1.11 host 172.16.3.33

b. 允许www访问：

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

实验过程（4）

- （4）应用到端口：路由器B的Serial 0/0/0

ip access-group 101 in

问题

- 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。