ACL（Acess Control List）定义一系列的规则，设备根据规则对数据包进行分类，并针对不同的报文进行不同的处理，实现对网络访问行为的控制、限制网络流量、提高网络性能、防止网络攻击等。

核心技术：包过滤

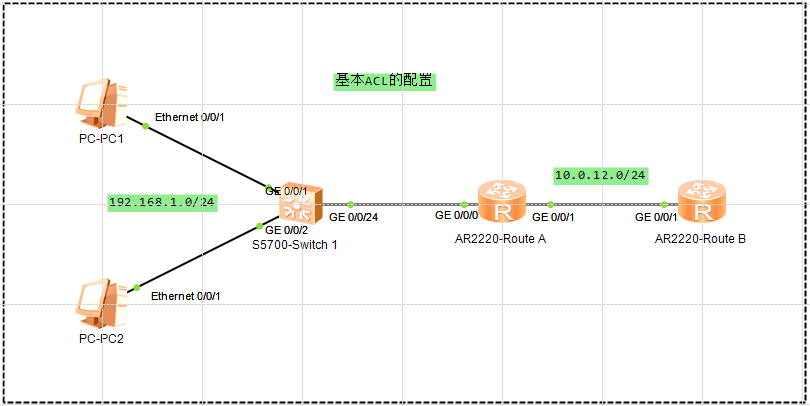
ACL的分类

|  |  |  |
| --- | --- | --- |
| 分类 | 编号范围 | 参数 |
| 基本ACL | 2000-2999 | 源IP地址等 |
| 高级ACL | 3000-3999 | 源目的IP地址、源目的端口等 |
| 二层ACL | 4000-4999 | 源目的MAC地址、以太帧协议类型等 |

ACL的规则

在接口的一个方向上，只能应用一个ACL

基本ACL的配置



创建普通ACL 2000，192.168.1.0网段除192.168.1.1可以通信外均被屏蔽

[Route A]acl number 2000

[Route A-acl-basic-2000]rule permit source 192.168.1.1 0

[Route A-acl-basic-2000]rule deny source 192.168.1.0 0.0.0.255

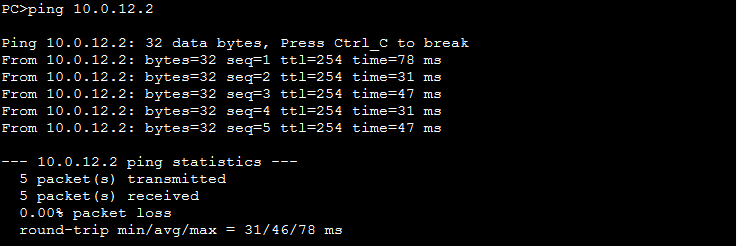
在端口上添加

[Route A]interface GigabitEthernet 0/0/0

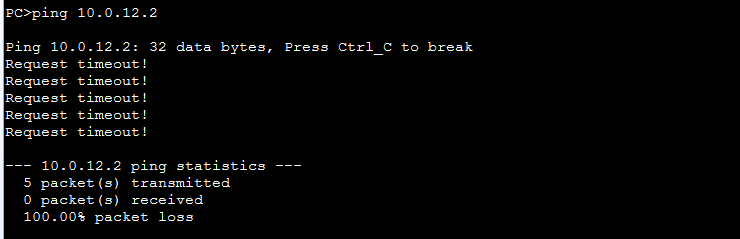
[Route A-GigabitEthernet0/0/0]traffic-filter inbound acl 2000

验证

PC1 PING测正常



PC2 PING测不通



ACL生效

<Route A>**display acl 2000**

Basic ACL 2000, 2 rules

Acl's step is 5

rule 5 permit source 192.168.1.1 0 (5 matches)

rule 10 deny source 192.168.1.0 0.0.0.255 (5 matches)

<Route A>**display traffic-filter applied-record**

-----------------------------------------------------------

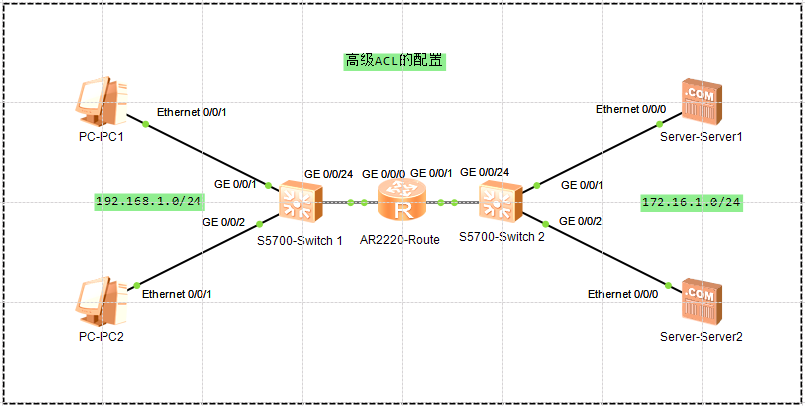
Interface Direction AppliedRecord

-----------------------------------------------------------

GigabitEthernet0/0/0 inbound acl 2000

-----------------------------------------------------------

高级ACL的配置



配置过程略

<Route>**display acl 3000**

Advanced ACL 3000, 3 rules

Acl's step is 5

rule 5 permit tcp destination 172.16.1.1 0 destination-port eq ftp

rule 10 permit icmp source 192.168.1.2 0 destination 172.16.1.2 0

rule 15 deny ip (154 matches)

<Route>**display traffic-filter applied-record**

-----------------------------------------------------------

Interface Direction AppliedRecord

-----------------------------------------------------------

GigabitEthernet0/0/0 inbound acl 3000

-----------------------------------------------------------