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。

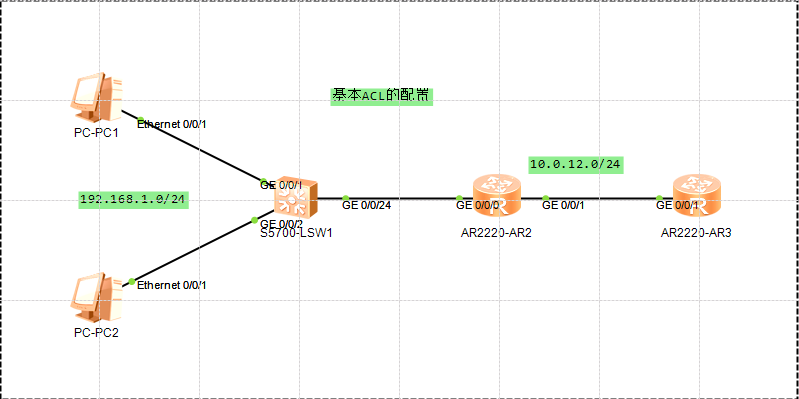
ACL的分类

|  |  |  |
| --- | --- | --- |
| 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 |

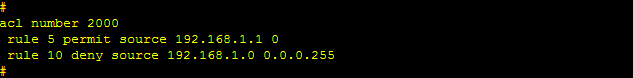
ACL的规则

基本ACL的配置

拓扑



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

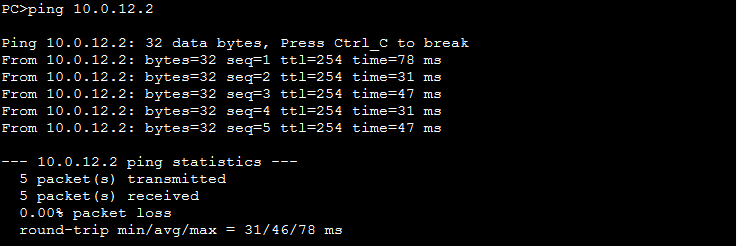


在端口上添加

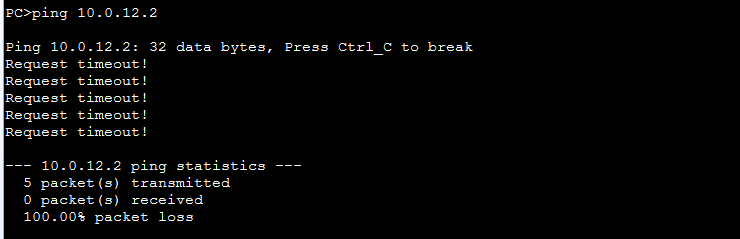


验证

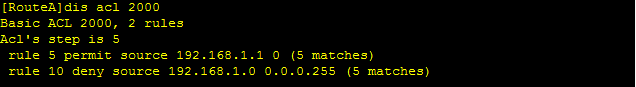
PC1 PING测正常

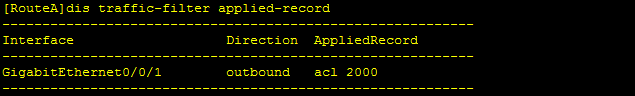


PC2 PING测不通



ACL生效





高级ACL的配置

高级ACL 3000的规则

