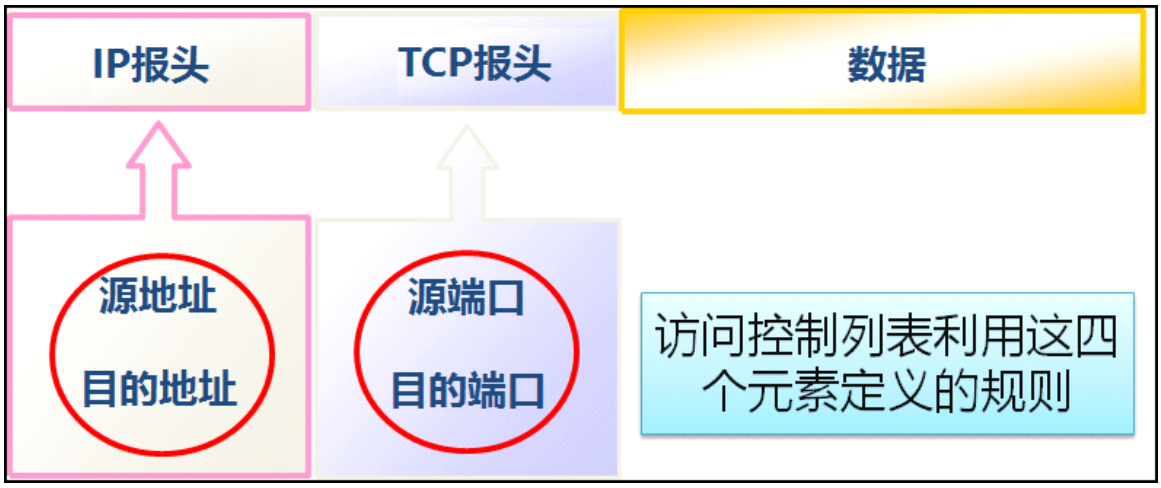
ACL

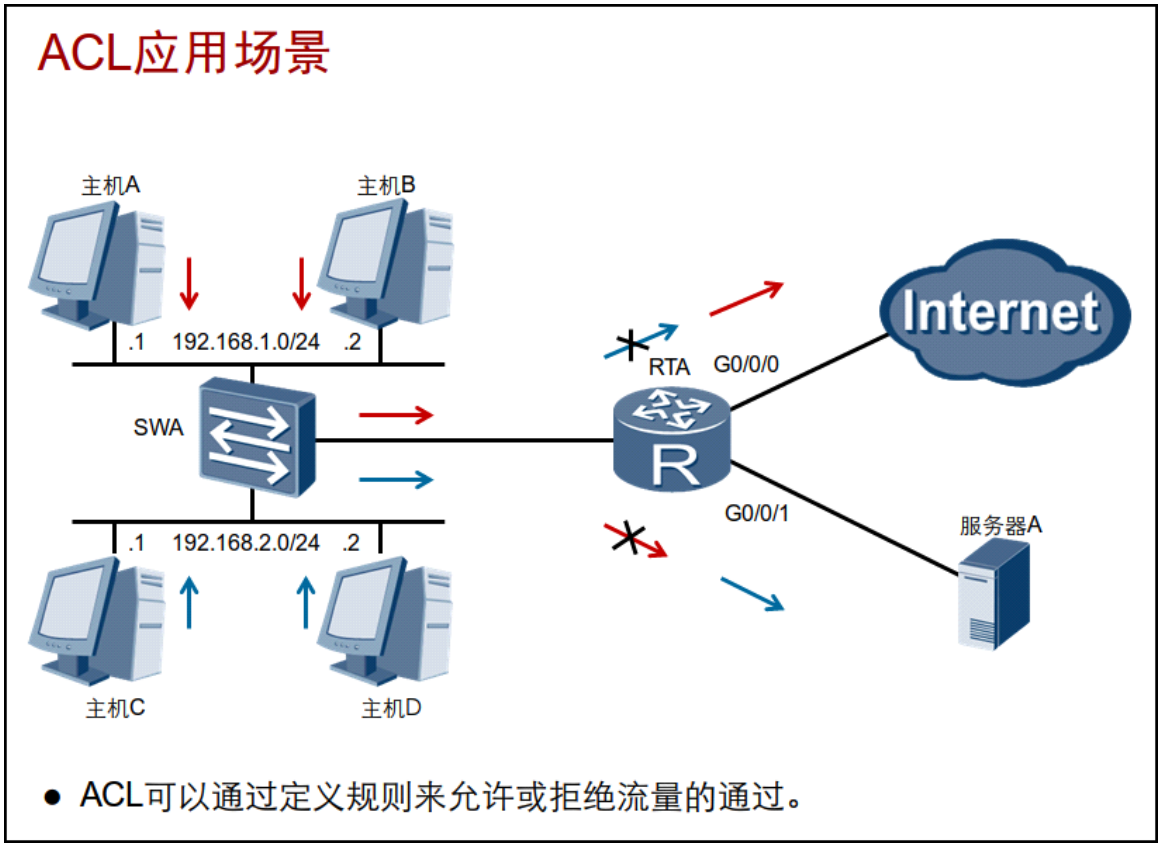
前言

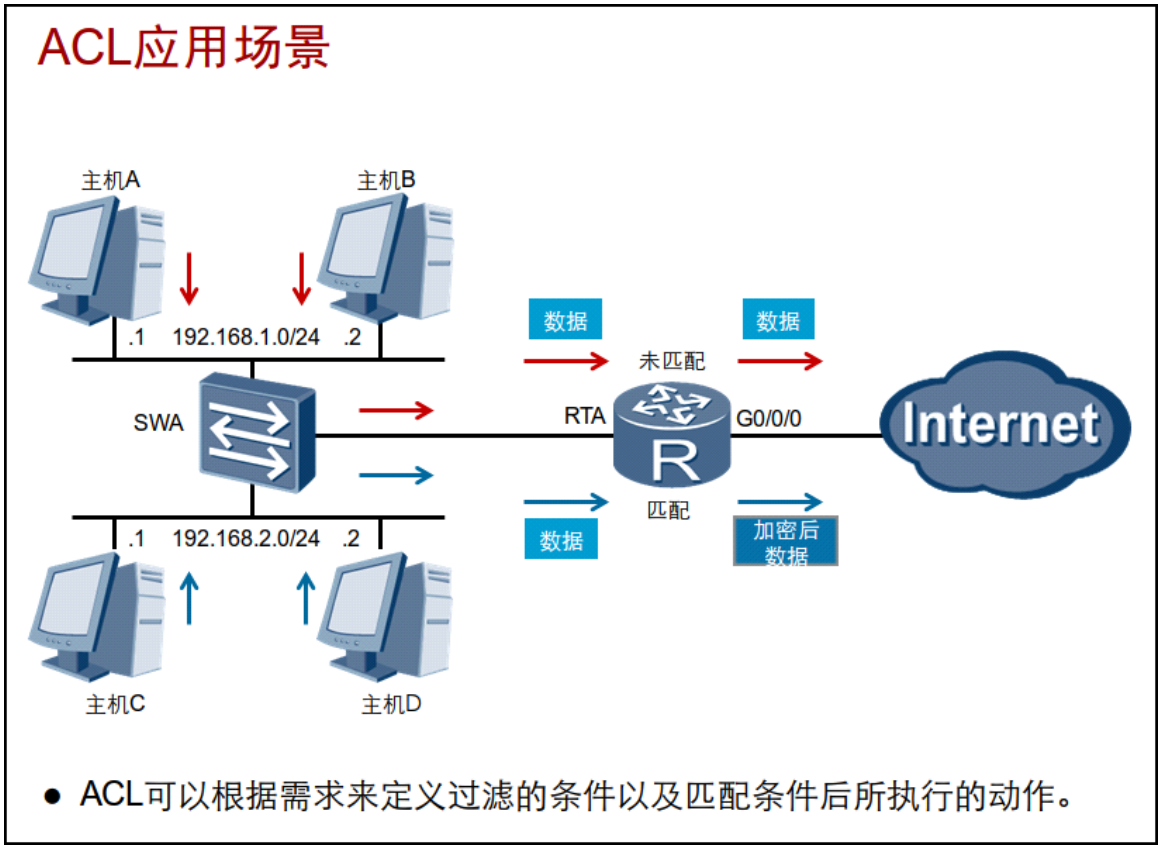
企业网络中的设备进行通信时，需要保障数据传输的安全可靠和网络的性能稳定。

访问控制列表ACL（Access Control List）可以定义一系列不同的规则，设备根据这些规则对数据包进行分类，并针对不同类型的报文进行不同的处理，从而可以实现对网络访问行为的控制、限制网络流量、提高网络性能、防止网络攻击等等。

ACL：Access Control List，访问控制列表

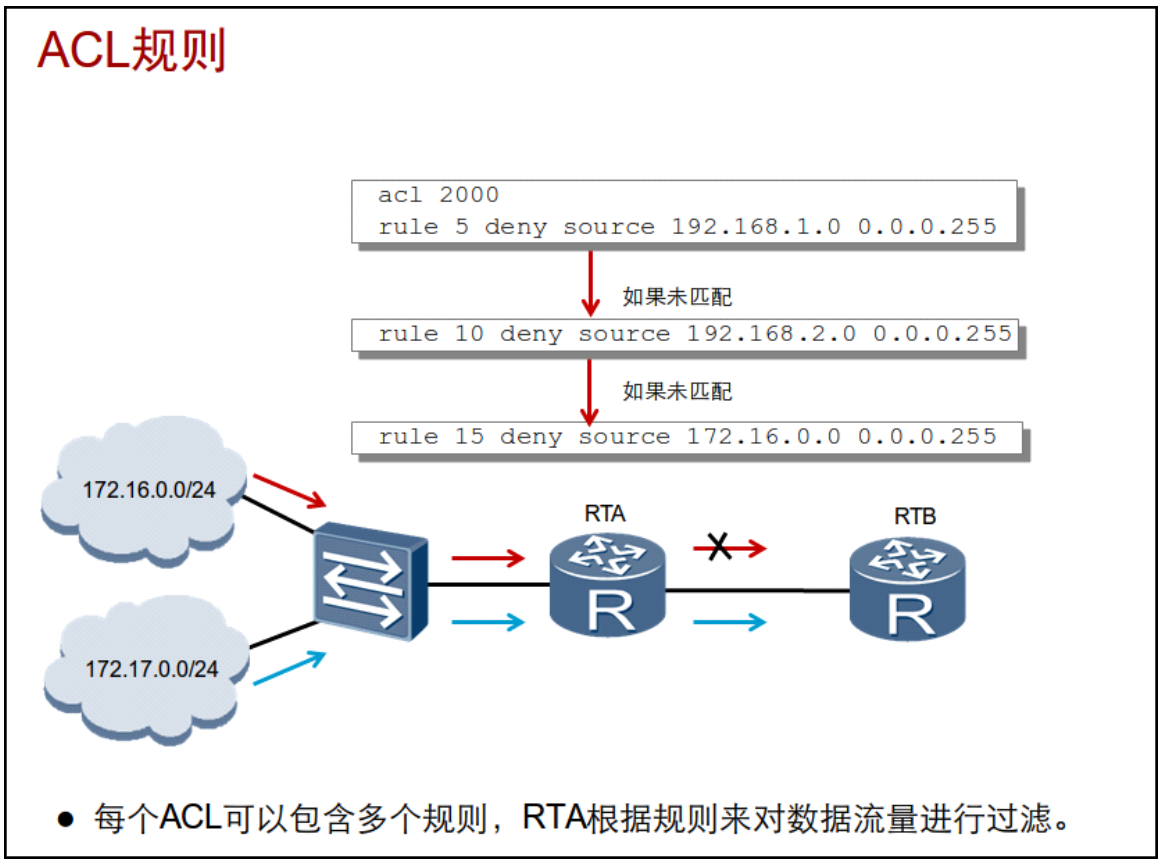
- 

- 

- 

ACL工作原理：

- ACL由一条或多条语句组成
- 每条语句必须选择动作：允许或拒绝
- 每条语句都有一个序列号

- 序列号越小越先进行比较
- ACL创建后，必须将其应用到某个接口或其他技术内才会生效
- 应用在接口时必须选择方向：入站或出站
- 方向是相对路由器来说的
- 每个接口在每个方向上只可应用一个 ACL
- 不能过滤由设备自己产生的数据
- 

ACL类型：

-

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

正掩码、反掩码、通配符区别：

-

名称	规则	作用	举例	备注
掩码	连续的1和0	IP地址	255.255.255.0	1对应网络位，0对应主机位
反掩码	连续的0和1	路由协议	0.0.0.255	0必须匹配，1无须匹配
通配符	任意的0和1	ACL	0.0.255.0	0必须匹配，1无须匹配

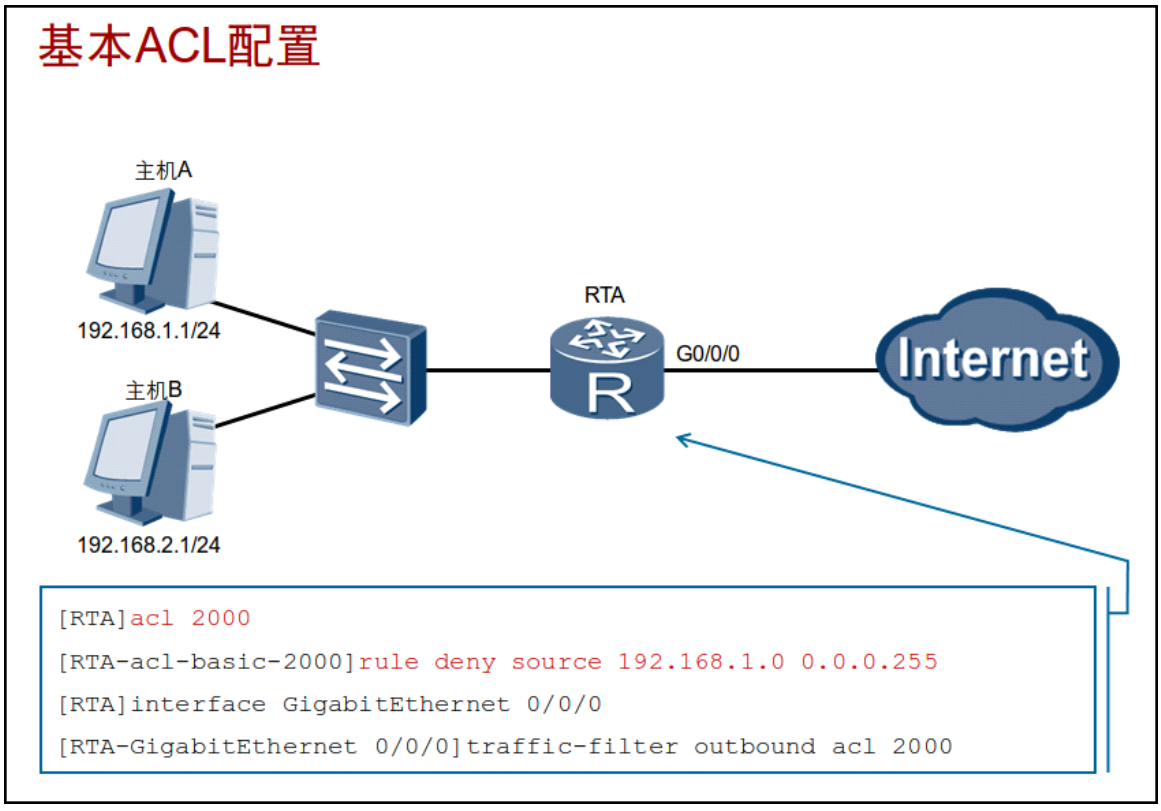
192.168.0.1 0.0.0.0/0	匹配一个主机地址
192.168.0.0 0.0.0255	匹配一个网段

- 192.168.0.1 0.0.0.254 匹配网段内奇数地址

192.168.0.0 0.0.0.254	匹配网段内偶数地址
any=0.0.0.0 255.255.255.255	匹配所有地址

ACL配置：

acl 2000	创建一个基本ACL
rule 5 deny/permit source 192.168.1.0 0.0.0.255	配置ACL的规则 拒绝或允许源地址为192.168.1.0/24网段内的所有流量
acl 3000	创建一个高级ACL
rule 5 deny/permit tcp source 192.168.1.0 0.0.0.255 destination 8.8.8.8 0 destination-port eq 80	配置ACL的规则 拒绝或允许源地址为192.168.1.0/24网段内到8.8.8.8的HTTP流量
traffic-filter inbound/outbound acl 2000	在接口调用ACL
display acl 2000	查看ACL
display traffic-filter applied-record	查看设备上所有基于ACL调用情况

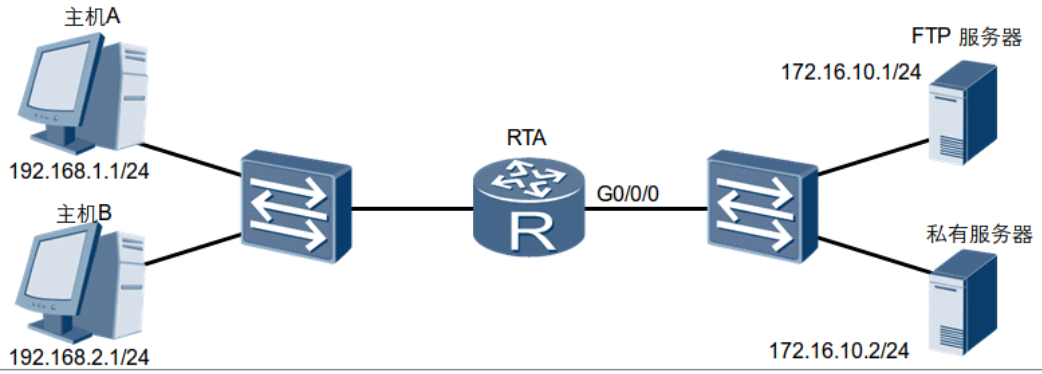
- 

配置确认

```
[RTA]display acl 2000
Basic ACL 2000, 1 rule
Acl's step is 5
 rule 5 deny source 192.168.1.0 0.0.0.255
```

```
[RTA]display  traffic-filter applied-record
------------------------------------------------------------
Interface                    Direction   AppliedRecord
------------------------------------------------------------
GigabitEthernet0/0/0         outbound    acl 2000
------------------------------------------------------------
```

高级ACL配置




```
[RTA]acl 3000
[RTA-acl-adv-3000]rule deny tcp source 192.168.1.0 0.0.0.255
destination 172.16.10.1 0.0.0.0 destination-port eq 21
[RTA-acl-adv-3000]rule deny tcp source 192.168.2.0 0.0.0.255
destination 172.16.10.2 0.0.0.0
[RTA-acl-adv-3000]rule permit ip
[RTA-GigabitEthernet 0/0/0]traffic-filter outbound acl 3000
```

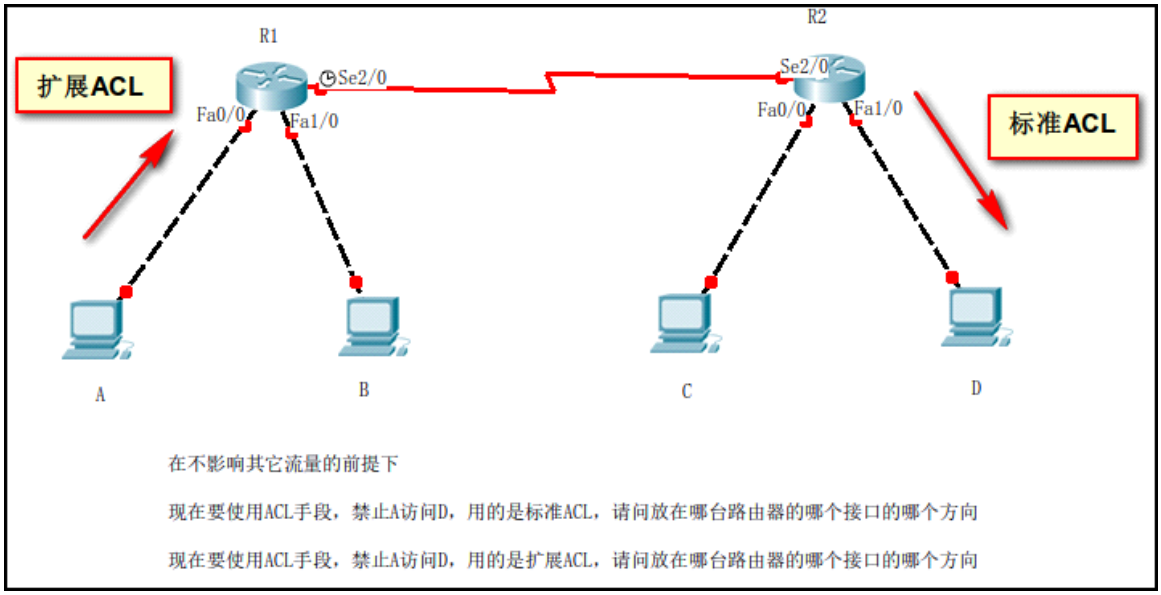
配置验证

```
[RTA]display acl 3000
Advanced ACL 3000, 3 rules
Acl's step is 5
rule 5 deny tcp source 192.168.1.0 0.0.0.255 destination 172.16.10.1 0
destination-port eq ftp
rule 10 deny tcp source 192.168.2.0 0.0.0.255 destination 172.16.10.2
0
rule 15 permit ip
```

```
[RTA]display  traffic-filter applied-record
-------------------------------------------------------------
Interface                   Direction   AppliedRecord
-------------------------------------------------------------
GigabitEthernet0/0/0        outbound    acl 3000
-------------------------------------------------------------
```

ACL接口调用方向的建议：

- 基本ACL尽量调用在离目标最近的出站接口
- 高级ACL尽量调用在离源头最近的入站接口



在不影响其它流量的前提下

现在要使用ACL手段，禁止A访问D，用的是标准ACL，请问放在哪台路由器的哪个接口的哪个方向

现在要使用ACL手段，禁止A访问D，用的是扩展ACL，请问放在哪台路由器的哪个接口的哪个方向