

- 标准访问控制列表的配置
  - 1. source-wildcard
  - 2. ACL规则匹配顺序
  - 3. ACL规则匹配方式
    - 3. 配置顺序
    - 3.2 自动顺序
    - 3.3 访问控制列表的组合
- 拓展访问控制列表的配置命令
  - tcp/udp
  - icmp
  - igmp
  - operator
- 华为acl配置步骤
- acl应用规则
- 示例
  - 访问外网限制
  - 交换机进行acl配置例子
  - 交换机应用acl

## 标准访问控制列表的配置

### 标准访问控制列表的配置

更多免费学习资料  
关注微信公众号  
教父爱分享

配置标准访问列表的命令格式如下：

```
acl acl-number [ match-order config | auto ]
```

```
rule { permit | deny } [source source-addr source-wildcard | any ]
```

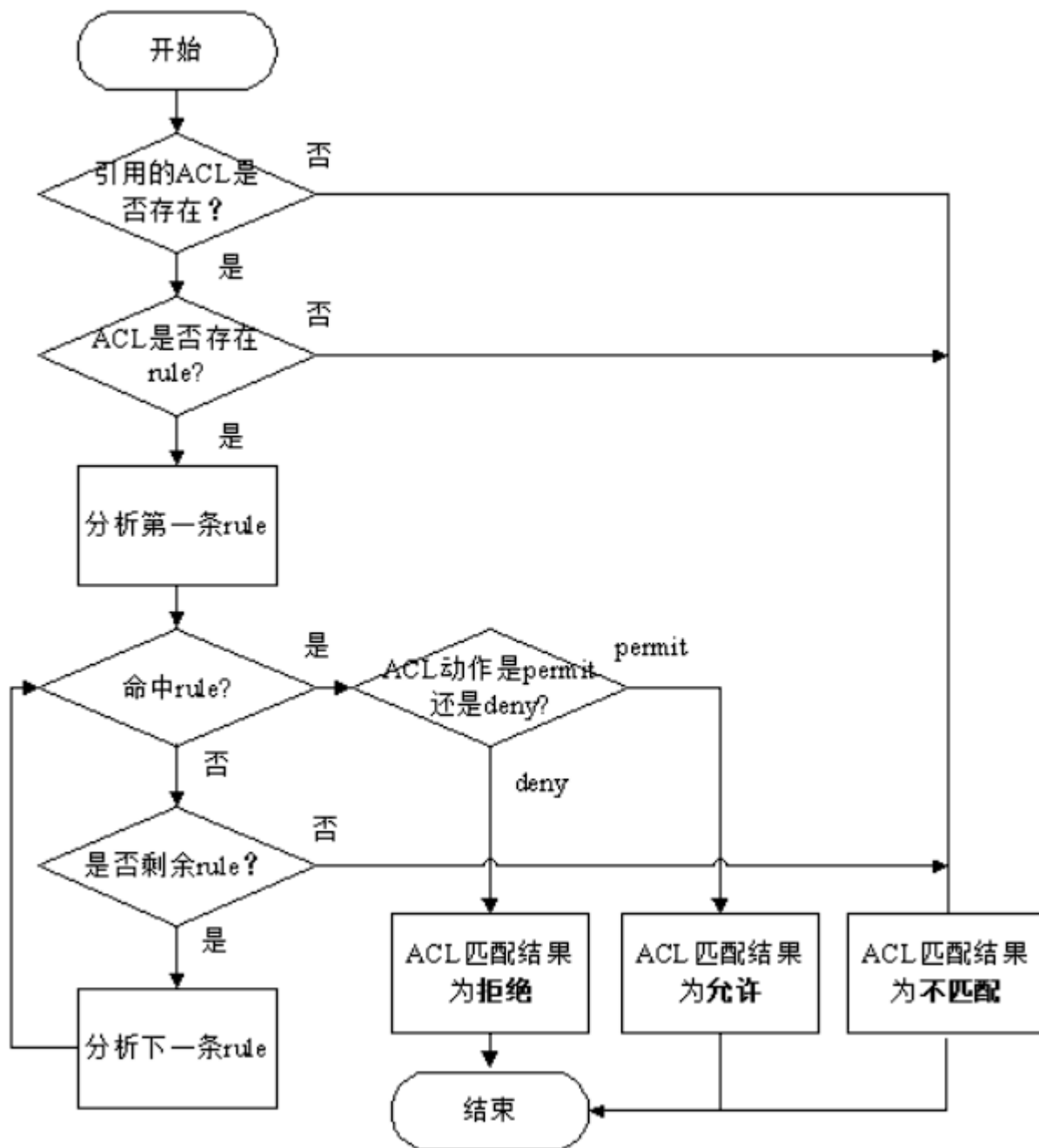
## 1. source-wildcard

怎样利用 IP 地址 和  
反掩码wildcard-mask 来表示  
一个网段？

255.255.255.255  
255.255.255.0



## 2. ACL规则匹配顺序



首先系统会查找设备上是否配置了ACL。

- 如果ACL不存在，则返回ACL匹配结果为：不匹配。
- 如果ACL存在，则查找设备是否配置了ACL规则。
  - 如果规则不存在，则返回ACL匹配结果为：不匹配。
  - 如果规则存在，则系统会从ACL中编号最小的规则开始查找。
- 如果匹配上了permit规则，则停止查找规则，并返回ACL匹配结果为：匹配（允许）。
- 如果匹配上了deny规则，则停止查找规则，并返回ACL匹配结果为：匹配（拒绝）。

- 如果未匹配上规则，则继续查找下一条规则，以此循环。如果一直查到最后一条规则，报文仍未匹配上，则返回ACL匹配结果为：不匹配。

从整个ACL匹配流程可以看出，报文与ACL规则匹配后，会产生两种匹配结果：“匹配”和“不匹配”。

- 匹配（命中规则）：指存在ACL，且在ACL中查找到了符合匹配条件的规则。不论匹配的动作是“permit”还是“deny”，都称为“匹配”，而不是只是匹配上permit规则才算“匹配”。
- 不匹配（未命中规则）：指不存在ACL，或ACL中无规则，再或者在ACL中遍历了所有规则都没有找到符合匹配条件的规则。以上三种情况，都叫做“不匹配”。

## 3. ACL规则匹配方式

ACL规则匹配方式有两种：配置顺序和自动顺序。缺省值是config，按照规则ID来排序。

### 3. 配置顺序

1.配置顺序 配置顺序根据ACL规则的ID进行排序，ID小的规则排在前面，优先进行匹配。当找到第一条匹配条件的规则时，查找结束。系统按照该规则对应的动作处理。

### 3.2 自动顺序

2.自动顺序 自动顺序也叫深度优先匹配。此时ACL规则的ID由系统自动分配，规则中指定数据包范围小的排在前面，优先进行匹配。当找到第一条匹配条件的规则时，查找结束。系统按照该规则对应的动作处理。

对于基本访问控制规则的语句，直接比较源地址通配符，通配符相同的则按配置顺序。

– 对于高级访问控制规则，首先比较协议范围，再比较源地址通配符，相同时再比较目的地址通配符，仍相同时则比较端口号的范围，范围小的排在前面，如果端口号范围也相同则按配置顺序。

对于高级访问控制规则

范围小的排在前面，深度优先

先协议 -> 源地址 -> 目的地址 -> 端口号

P.S.D. Port

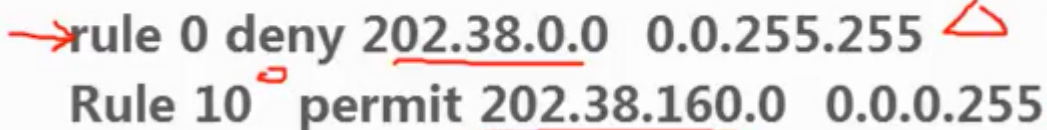
## 3.3 访问控制列表的组合

auto 与 config 的差别

一条访问列表可以由多条规则组成。对于这些规则，有两种匹配顺序：auto和config指定匹配该规则时按用户的配置顺序。规则冲突时，若匹配顺序为auto（深度优先），描述的地址范围越小的规则，将会优先考虑。深度的判断要依靠通配比较位和IP地址结合比较

Acl number 2004

→ rule 0 deny 202.38.0.0 0.0.255.255  
Rule 10 permit 202.38.160.0 0.0.0.255



两条规则结合则表示禁止一个大网段（202.38.0.0）上的主机但允许其中的一小部分主机（202.38.160.0）的访问。

规则冲突时，若匹配顺序为config，先配置的规则会被优先考虑。

## 拓展访问控制列表的配置命令

### tcp/udp

配置TCP/UDP协议的扩展访问列表：

```
rule { ID of acl rule } { permit | deny } { tcp | udp } [ source source-addr source-wildcard | any ] [ source-port operator port1 [ port2 ] ] [ destination dest-addr dest-wildcard | any ] [ destination-port operator port1 [ port2 ] ] [ logging ]
```

### icmp

配置ICMP协议的扩展访问列表：

```
rule { ID of acl rule } { permit | deny } icmp [ source source-addr source-wildcard | any ] [ destination dest-addr dest-wildcard | any ] [ icmp-type icmp-type icmp-code ] [ logging ]
```

# igmp

配置其它协议的扩展访问列表：

```
rule { ID of acl rule } { permit | deny } { ip | ospf | igmp | gre } [source source-addr source-wildcard | any ]  
[ destination dest-addr dest-wildcard | any ] [logging]
```

## operator

扩展访问控制列表操作符的含义	
操作符及语法	意义
<u>Eq</u> (equal portnumber)	等于端口号 port number
<u>Gt</u> (greater-than portnumber)	大于端口号 port number
<u>Lt</u> (less-than portnumber)	小于端口号 port number
<u>Neq</u> (not-equal portnumber)	不等于端口号 port number
<u>range</u> portnumber1 portnumber2	介于端口号 portnumber1 和 portnumber2 之间

## 华为acl配置步骤

1. 进入系统视图
- 1) 执行命令system-view，进入系统视图。
- system-view
2. 创建acl
- 2) 执行命令acl [ number ] acl-number [ match-order { config | auto } ]，//创建基本ACL，并进入相应视图. match-order 指定了ACL各个规则之间的匹配顺序：选择参数config，ACL的匹配顺序按照规则ID来排序，ID小的规则排在前面，优先匹配；选择参数auto，将使用深度优先的匹配顺序。
- acl number 200
- acl 2000
- //默认匹配顺序为config

## acl 2000 match-order auto

```
[Switch] acl 3001
[Switch-acl-adv-3001] rule deny ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255 //禁止研发部访问市场部
[Switch-acl-adv-3001] quit
```

### 3. 创建acl规则

3) 执行命令rule [ rule-id ] { deny | permit } [ logging | source { source-ip-address { 0 | source-wildcard } | address-set address-set-name | any } | time-range time-name ] \* [ description description ]  
//创建基本ACL规则。配置时没有指定编号rule-id，表示增加一条新的规则，此时系统会根据步长，自动为规则分配一个大于现有规则最大编号且为步长整数倍的最小编号。配置时指定了编号rule-id，如果相应的规则已经存在，表示对已有规则进行编辑，规则中没有编辑的部分不受影响；如果相应的规则没有存在，表示增加一条新的规则，并且按照指定的编号将其插入到相应的位置。

```
rule 2000 deny 10.10.1.2 0.0.0.255
```

```
rule 2000 deny 10.10.1.2 0.0.0.255
```

```
rule 3000 deny 10.10.3.0 0.0.0.255 destination 10.10.2.0 0.0.0.255
```

```
rule 5 deny tcp source 192.168.1.12 0 destination-port eq www
```

### 4. 应用acl到对应的接口

配置好的ACL，还要应用到相应的接口才会生效。在AR系列路由器中可以使用下面的方式应用ACL。

```
interface GigabitEthernet0/0/1
```

4) traffic-filter inbound acl 3000 //在接口上应用ACL，进行报文过滤，某些类型的设备可以使用packet-filter 3000 inbound这种方式。

```
//进入接口配置
```

```
interface GigabitEthernet 0/0/1
```

```
//入站口方向应用acl 200
```

```
traffic-filter inbound acl 200
```

## acl应用规则

- 1.标准访问控制列表，靠近目标网络
- 2.高级访问控制列表，靠近源网络



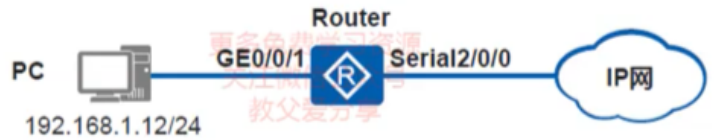
# 示例

## 访问外网限制

对内网地址192.168.1.12/24访问外网做限制，使其无法访问所有WEB界面

```
acl number 3005 //定义用于报文过滤的访问控
description deny_souce_ip_www
rule 5 deny tcp source 192.168.1.12 0 destination-port eq www
rule 10 permit tcp source 192.168.1.12 0
```

```
interface GigabitEthernet0/0/1
ip address 192.168.1.2 255.255.255.0
traffic-filter inbound acl 3005 //在接口上应用ACL，进行报文过滤
```



acl number 3005 //定义用于报文过滤的访问控

description deny\_souce\_ip\_www

rule 5 deny tcp source 192.168.1.12 0 destination-port eq www

0 是源地址的通配符掩码，表示匹配源 IP 地址的所有位。

**destination-port eq www**：目的端口匹配条件。

- **destination-port** 指定了目的端口的匹配条件。
- **eq www** 表示要匹配的目的端口是 **www**，通常是指 Web 服务的默认端口 80。
- 这个条件要求目的端口必须是 **www**（端口 80）

rule 10 permit tcp source 192.168.1.12 0

```
interface GigabitEthernet0/0/1
ip address 192.168.1.2 255.255.255.0
traffic-filter inbound acl 3005 //在接口上应用ACL，进行报文过滤
```

## 交换机进行acl配置例子

访客网段不能访问办公网可通过policy进行流量控制或者进行2层端口隔离

## 1、流量控制

```
[SWITCH]acl 3001          #新建一个高级ACL
```

```
[SWITCH-acl-adv-3001]rule 5 deny ip source 192.168.7.0 0.0.0.255 destination 192.168.2.0 0.0.0.255  
#禁止7网段访问2网段
```

```
[SWITCH-acl-adv-3001]rule 100 permit ip    #允许访问任何网段
```

```
[SWITCH-acl-adv-3001]quit          #退出当前模式
```

## 交换机应用acl

更多免费学习资源  
关注微信公众号  
教父爱分享

```
① 先定义ACL  
[SWITCH]acl 3001          #新建一个高级ACL  
[SWITCH-acl-adv-3001]rule 5 deny ip source 192.168.7.0 0.0.0.255 destination 192.168.2.0 0.0.0.255  
② 配置基于ACL的流分类  
[Switch] traffic classifier tc1    //创建流分类  
[Switch-classifier-tc1] if-match acl 3001    //将ACL与流分类关联  
[Switch-classifier-tc1] quit  
③ 配置流行为  
[Switch] traffic behavior tb1    //创建流行为  
[Switch-behavior-tb1] deny    //配置流行为动作为拒绝报文通过  
[Switch-behavior-tb1] quit  
④ 配置流策略  
[Switch] traffic policy tp1    //创建流策略  
[Switch-trafficpolicy-tp1] classifier tc1 behavior tb1    //将流分类tc1与流行为tb1关联  
[Switch-trafficpolicy-tp1] quit  
⑤ 在接口下应用流策略  
[Switch] interface gigabitethernet 0/0/1  
[Switch-GigabitEthernet0/0/1] traffic-policy tp1 inbound    //流策略应用在接口入方向
```