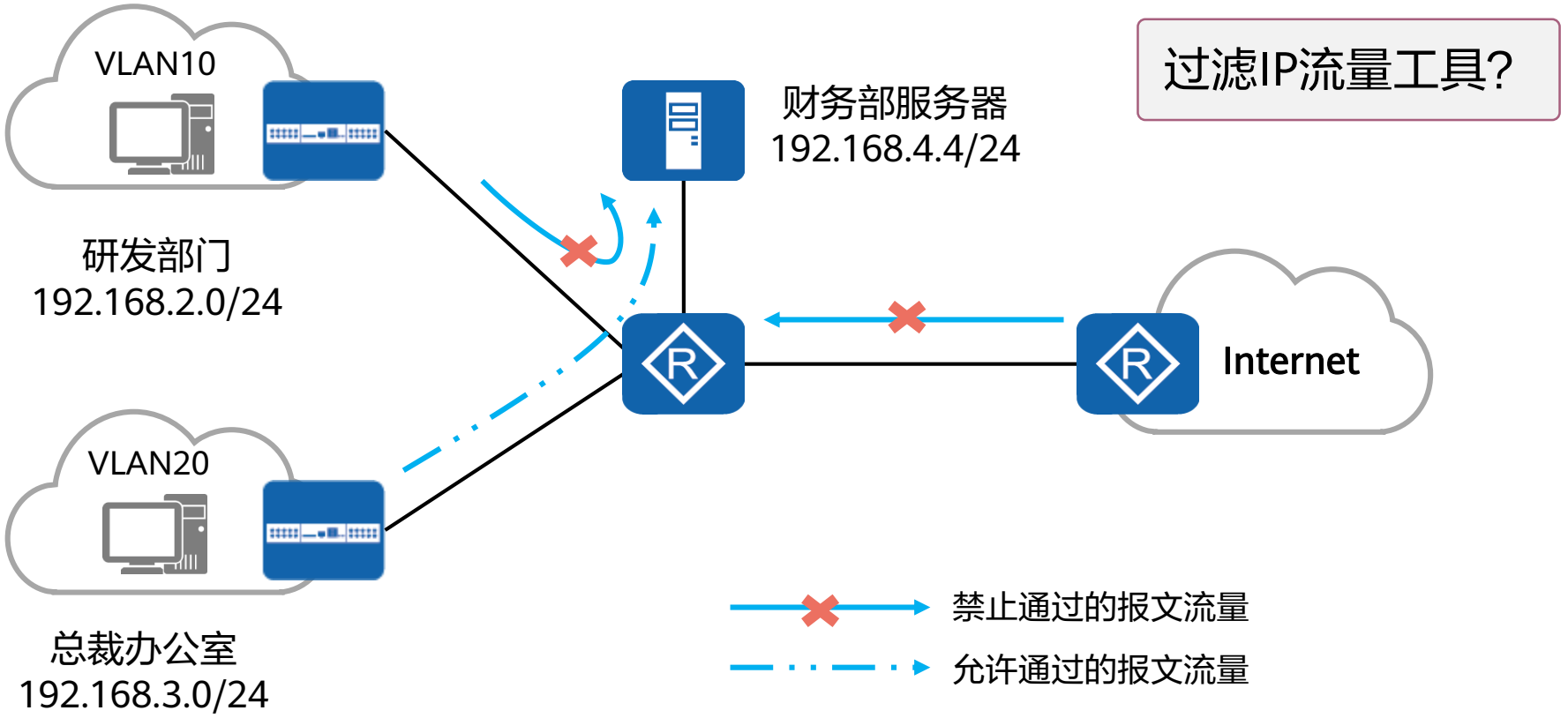
ACL原理与配置

主讲人：鲍婷婷

目录

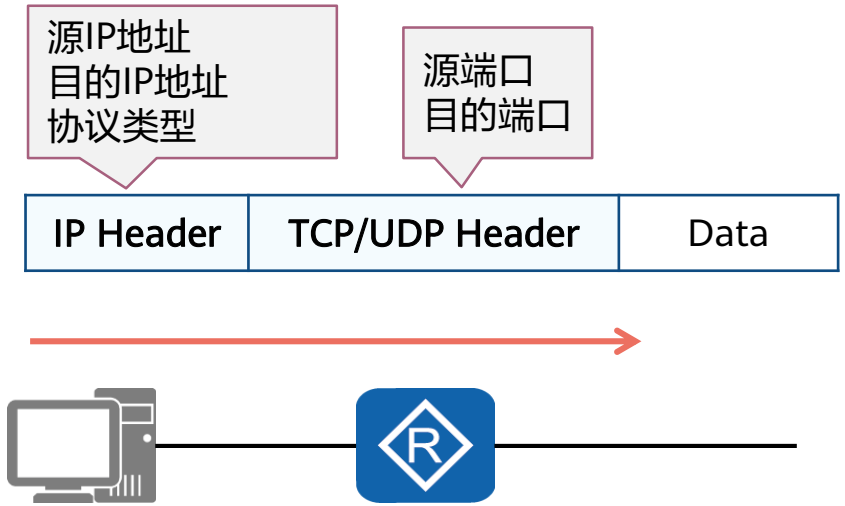
技术背景：需要一个工具，实现流量过滤



- 某公司为保证财务数据安全，禁止研发部门访问财务服务器，但总裁办公室不受限制。

ACL概述

- ACL是由一系列permit或deny语句组成的、有序规则的列表。
- ACL是一个匹配工具，能够对报文进行匹配和区分。



ACL应用

- 匹配IP流量
- 在Traffic-filter中被调用
- 在NAT（Network Address Translation）中被调用
- 在路由策略中被调用
- 在防火墙的策略部署中被调用
- 在QoS中被调用
- 其他.....

目录

ACL的组成

- ACL由若干条permit或deny语句组成。每条语句就是该ACL的一条规则，每条语句中的permit或deny就是与这条规则相对应的处理动作。

每条规则都是什么意思?

规则编号

```
acl number 2000
                 规则编号
 rule     5       deny     source  10.1.1.1  0
 rule     10      deny     source  10.1.1.2  0
 rule     15      permit   source  10.1.1.0  0.0.0.255
          步长=5
```

如果希望增加1条规则，该如何处理?

rule 11 deny source 10.1.1.3 0

```
acl number 2000
 rule     5       deny     source  10.1.1.1  0
 rule     10      deny     source  10.1.1.2  0

 rule     15      permit   source  10.1.1.0  0.0.0.255
```

规则编号与步长

- **规则编号（Rule ID）：**

  一个ACL中的每一条规则都有一个相应的编号。

- **步长（Step）：**

  步长是系统自动为ACL规则分配编号时，每个相邻规则编号之间的差值，缺省值为5。步长的作用是为了方便后续在旧规则之间，插入新的规则。

- **Rule ID分配规则：**

  系统为ACL中首条未手工指定编号的规则分配编号时，使用步长值（例如步长=5，首条规则编号为5）作为该规则的起始编号；为后续规则分配编号时，则使用大于当前ACL内最大规则编号且是步长整数倍的最小整数作为规则编号。

通配符 (1)

acl number 2000

					通配符
rule	5	deny	source	10.1.1.1	0
rule	10	deny	source	10.1.1.2	0
rule	15	permit	source	10.1.1.0	0.0.0.255

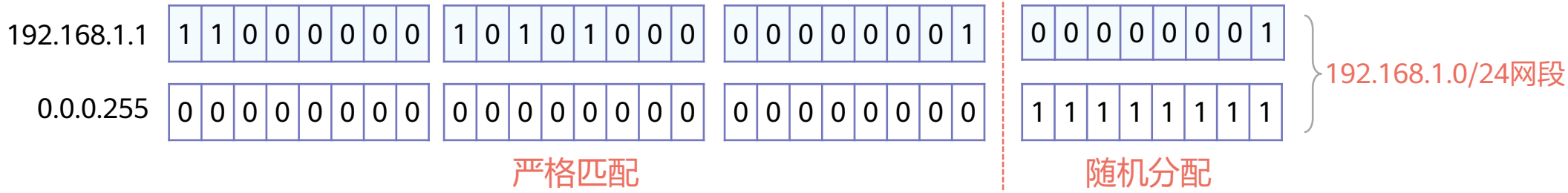
通配符 (Wildcard)

- 通配符是一个32比特长度的数值，用于指示IP地址中，哪些比特位需要严格匹配，哪些比特位无需匹配。
- 通配符通常采用类似网络掩码的点分十进制形式表示，但是含义却与网络掩码完全不同。

- 匹配规则：

  “0”表示“匹配”；“1”表示“随机分配”

如何匹配192.168.1.1/24对应网段的地址?



通配符 (2)

- 匹配192.168.1.0/24这个子网中的奇数IP地址，例如192.168.1.1、192.168.1.3、192.168.1.5等。

答案： 192.168.1.1　0.0.0.254

通配符中的1或者0可以不连续

特殊的通配符

- 精确匹配192.168.1.1这个IP地址

  192.168.1.1 0.0.0.0 = 192.168.1.1 0
- 匹配所有IP地址

  0.0.0.0 255.255.255 = any

ACL的分类与标识

- 基于ACL规则定义方式的分类

分类	编号范围	规则定义描述
基本ACL	2000~2999	仅使用报文的源IP地址、分片信息和生效时间段信息来定义规则。
高级ACL	3000~3999	可使用IPv4报文的源IP地址、目的IP地址、IP协议类型、ICMP类型、TCP源/目的端口号、UDP源/目的端口号、生效时间段等来定义规则。
二层ACL	4000~4999	使用报文的以太网帧头信息来定义规则，如根据源MAC地址、目的MAC地址、二层协议类型等。
用户自定义ACL	5000~5999	使用报文头、偏移位置、字符串掩码和用户自定义字符串来定义规则。
用户ACL	6000~6999	既可使用IPv4报文的源IP地址或源UCL（User Control List）组，也可使用目的IP地址或目的UCL组、IP协议类型、ICMP类型、TCP源端口/目的端口、UDP源端口/目的端口号等来定义规则。

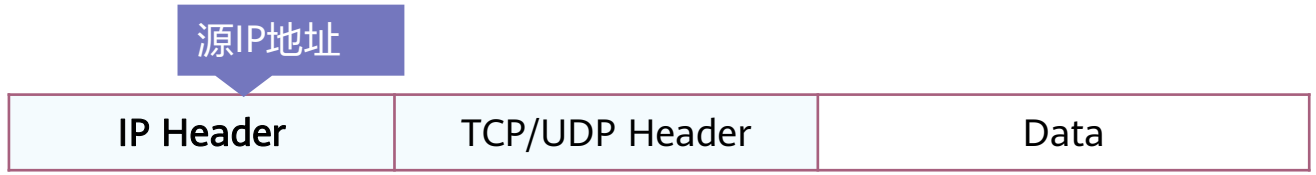
- 基于ACL标识方法的分类

分类	规则定义描述
数字型ACL	传统的ACL标识方法。创建ACL时，指定一个唯一的数字标识该ACL。
命名型ACL	通过名称代替编号来标识ACL。

基本ACL&高级ACL

- 基本ACL

编号范围：
2000-2999




```
acl number 2000
  rule      5      deny      source  10.1.1.1  0
  rule      10     deny      source  10.1.1.2  0
  rule      15     permit    source  10.1.1.0  0.0.0.255
```

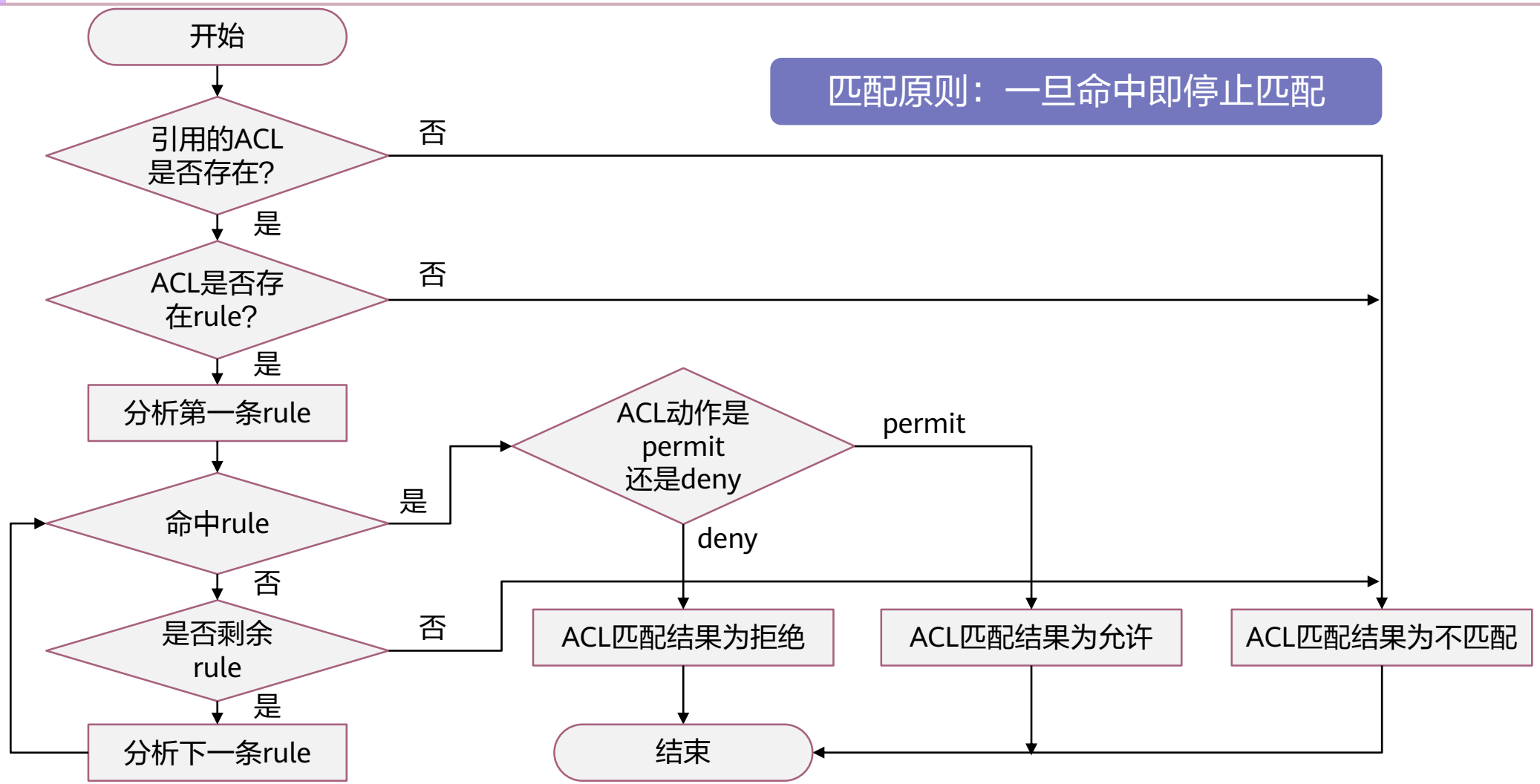
- 高级ACL

编号范围：
3000-3999


```
acl number 3000
  rule   5   permit  ip    source   10.1.1.0   0.0.0.255   destination   10.1.3.0   0.0.0.255
  rule   10  permit  tcp   source   10.1.2.0   0.0.0.255   destination   10.1.3.0   0.0.0.255   destination-port eq 21
```

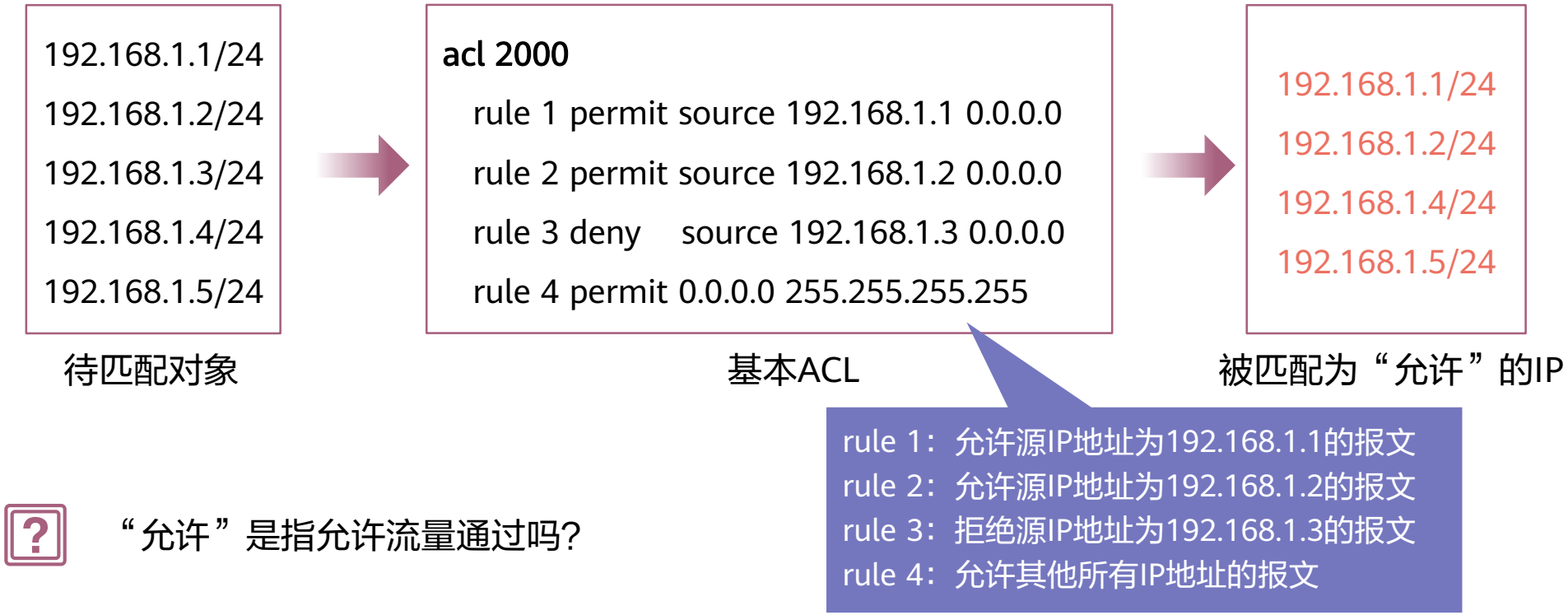
ACL的匹配机制

匹配原则：一旦命中即停止匹配



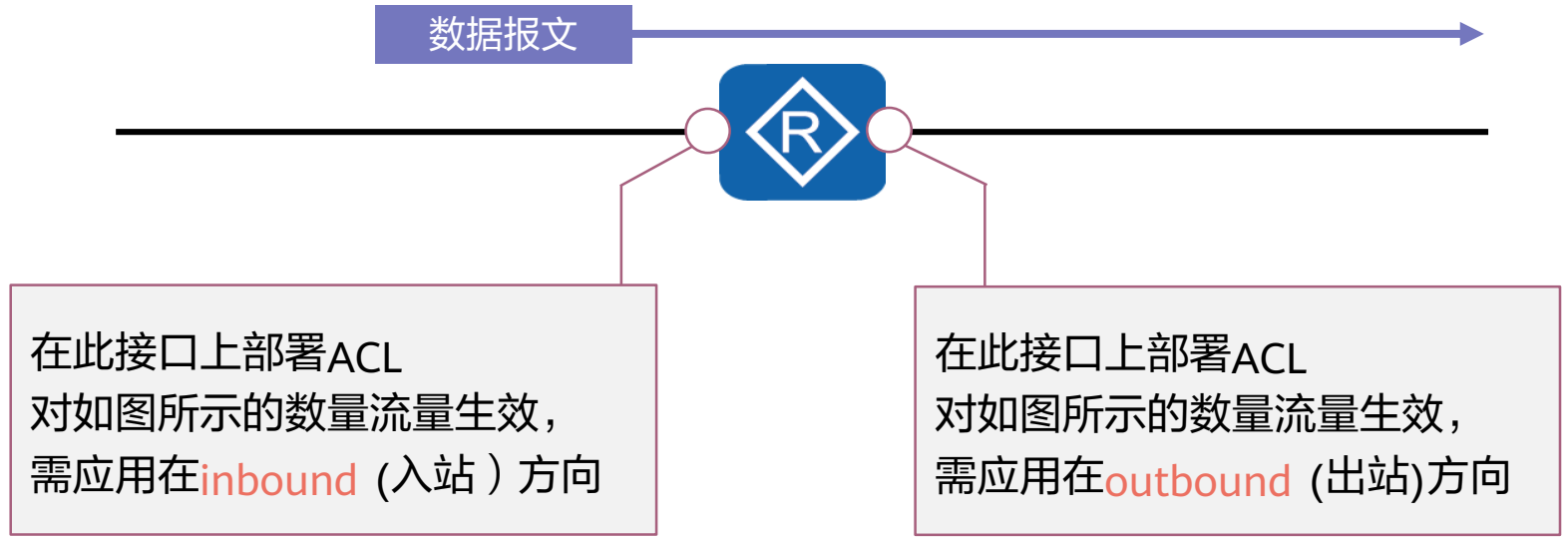
ACL的匹配顺序及匹配结果

- 配置顺序（config模式）
  - 系统按照ACL规则编号从小到大的顺序进行报文匹配，规则编号越小越容易被匹配。

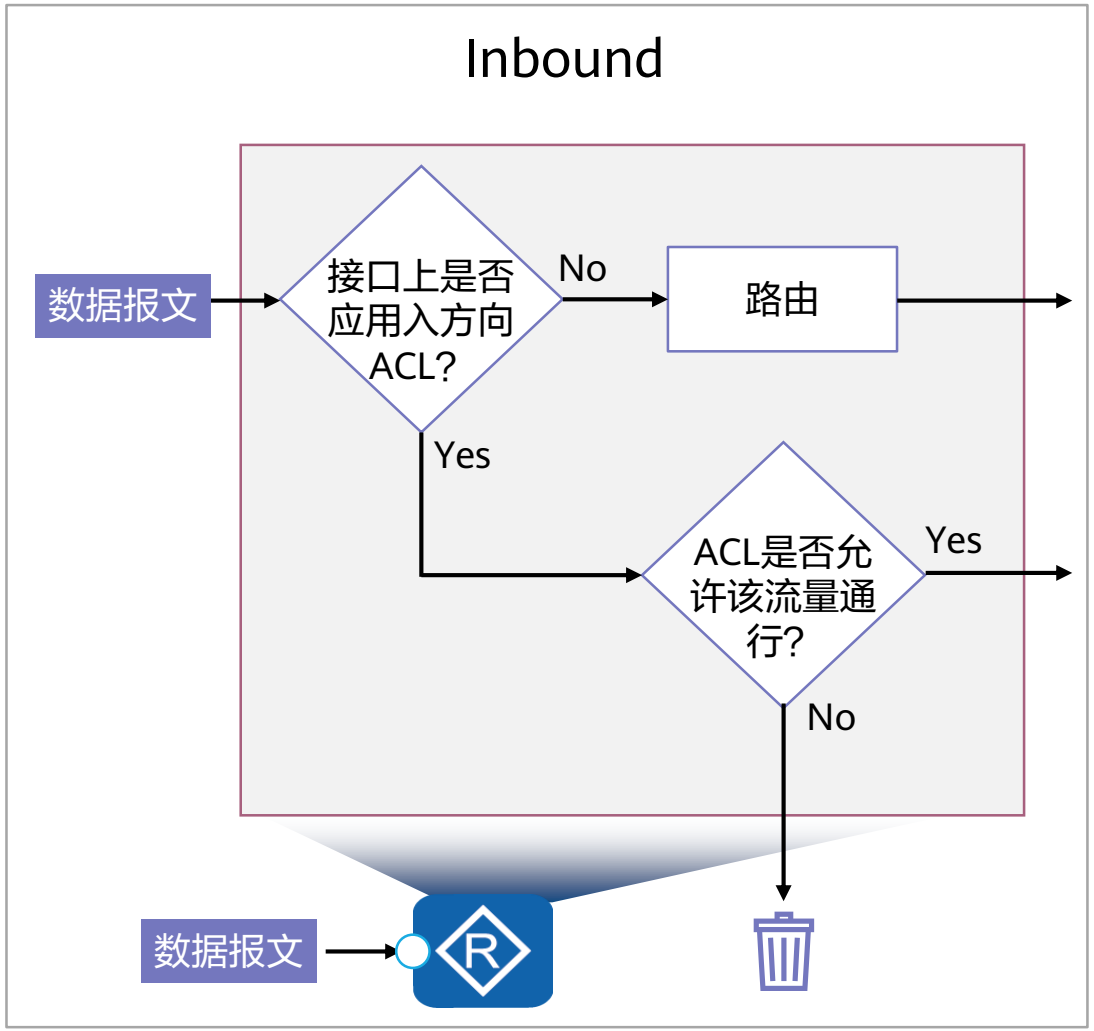


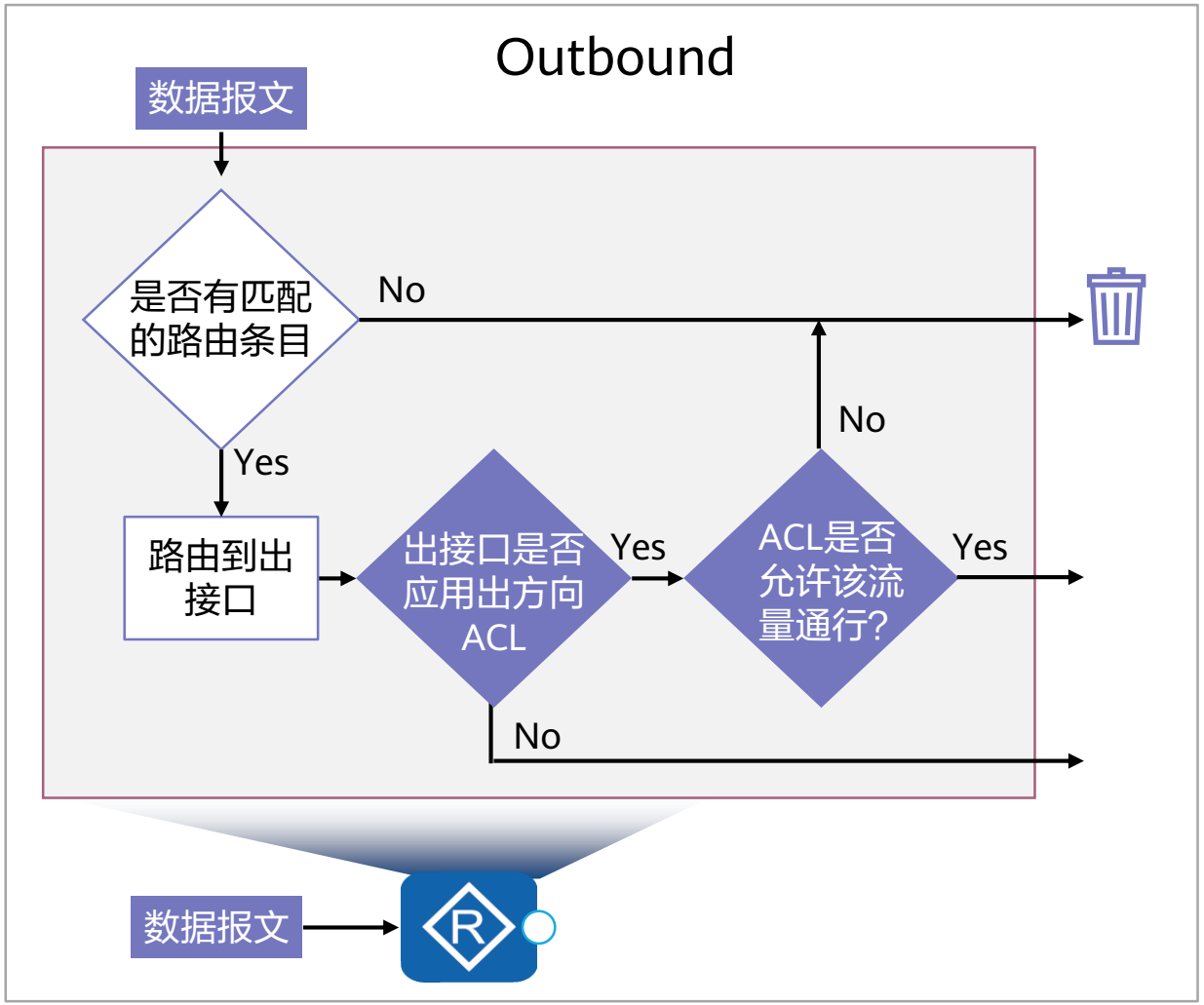
“允许”是指允许流量通过吗?

ACL的匹配位置



入站 (Inbound)及出站 (Outbound)方向





目录

基本ACL的基础配置命令

1. 创建基本ACL

[Huawei] **acl** [**number**] *acl-number* [**match-order config**]

使用编号（2000～2999）创建一个数字型的基本ACL，并进入基本ACL视图。

[Huawei] **acl name** *acl-name* { **basic** | *acl-number* } [**match-order config**]

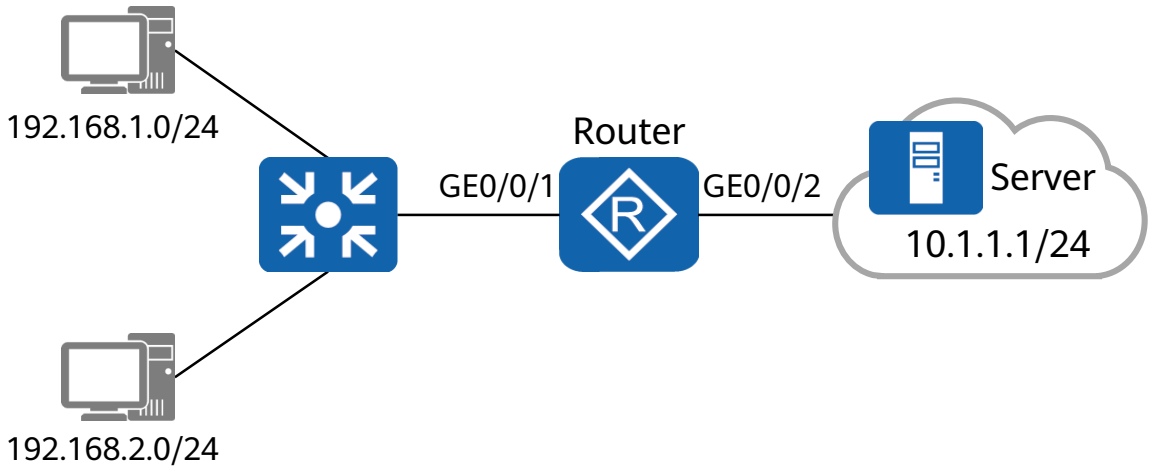
使用名称创建一个命名型的基本ACL，并进入基本ACL视图。

2. 配置基本ACL的规则

[Huawei-acl-basic-2000] **rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **time-range** *time-name*]

在基本ACL视图下，通过此命令来配置基本ACL的规则。

案例：使用基本ACL过滤数据流量



- 配置需求：

  在Router上部署基本ACL后，ACL将试图穿越Router的源地址为192.168.1.0/24网段的数据包过滤掉，并放行其他流量，从而禁止192.168.1.0/24网段的用户访问Router右侧的服务器网络。

1、Router已完成IP地址和路由的相关配置

2、在Router上创建基本ACL，禁止192.168.1.0/24网段访问服务器网络：

```
[Router] acl 2000
[Router-acl-basic-2000] rule deny source 192.168.1.0  0.0.0.255
[Router-acl-basic-2000] rule permit source any
```

3、由于从接口GE0/0/1进入Router，所以在接口GE0/0/1的入方向配置流量过滤：

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-filter inbound acl 2000
[Router-GigabitEthernet0/0/1] quit
```

高级ACL的基础配置命令（1）

1. 创建高级ACL

[Huawei] **acl** [**number**] *acl-number* [**match-order config**]

使用编号（3000～3999）创建一个数字型的高级ACL，并进入高级ACL视图。

[Huawei] **acl name** *acl-name* { **advance** | *acl-number* } [**match-order config**]

使用名称创建一个命名型的高级ACL，进入高级ACL视图。

高级ACL的基础配置命令 (2)

2. 配置基本ACL的规则
根据IP承载的协议类型不同，在设备上配置不同的高级ACL规则。对于不同的协议类型，有不同的参数组合。

- 当参数protocol为IP时，高级ACL的命令格式为

rule [*rule-id*] { **deny** | **permit** } **ip** [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*]]]

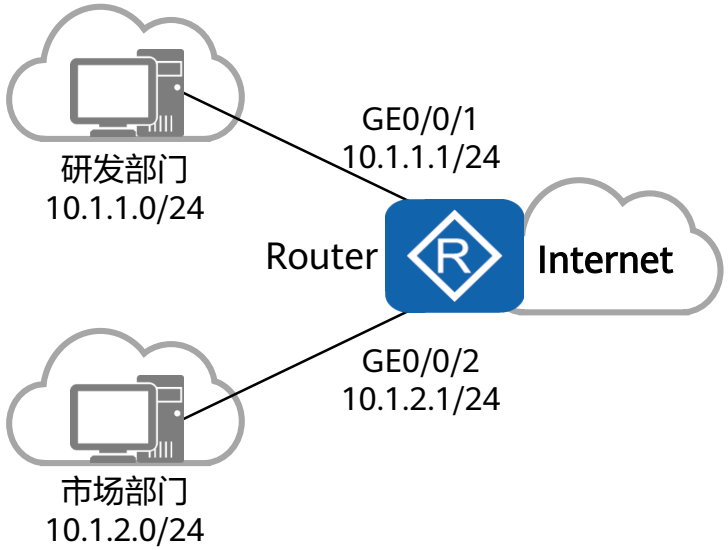
在高级ACL视图下，通过此命令来配置高级ACL的规则。

- 当参数protocol为TCP时，高级ACL的命令格式为

rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** port | **gt** port | **lt** port | **range** port-start port-end } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** port | **gt** port | **lt** port | **range** port-start port-end } | **tcp-flag** { **ack** | **fin** | **syn** } * | **time-range** time-name] *

在高级ACL视图下，通过此命令来配置高级ACL的规则。

案例：使用高级ACL限制不同网段的用户互访 (1)



配置需求：

- 某公司通过Router实现各部门之间的互连。为方便管理网络，管理员为公司的研发部和市场部规划了两个网段的IP地址。
- 现要求Router能够限制两个网段之间互访，防止公司机密泄露。

1、Router已完成IP地址和路由的相关配置。

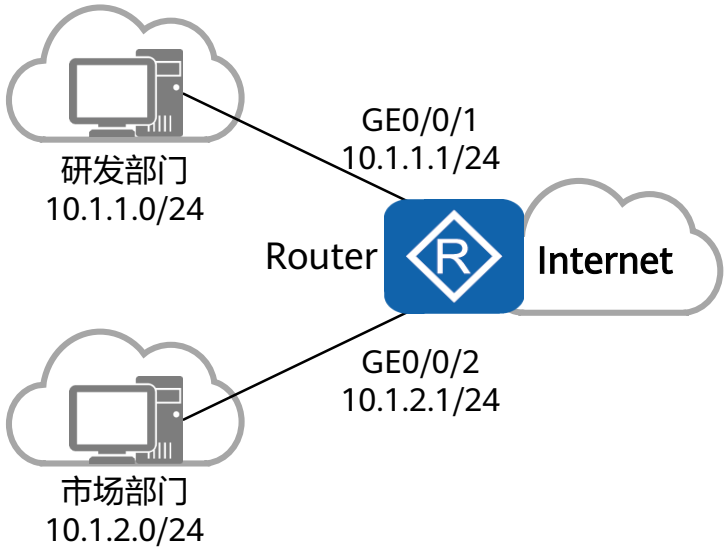
2、创建高级ACL 3001并配置ACL规则，拒绝研发部访问市场部的报文：

```
[Router] acl 3001
[Router-acl-adv-3001] rule deny ip source 10.1.1.0 0.0.0.255
destination 10.1.2.0 0.0.0.255
[Router-acl-adv-3001] quit
```

3、创建高级ACL 3002并配置ACL规则，拒绝市场部访问研发部的报文：

```
[Router] acl 3002
[Router-acl-adv-3002] rule deny ip source 10.1.2.0 0.0.0.255
destination 10.1.1.0 0.0.0.255
[Router-acl-adv-3002] quit
```

案例：使用高级ACL限制不同网段的用户互访 (2)



配置需求：

- 某公司通过Router实现各部门之间的互连。为方便管理网络，管理员为公司的研发部和市场部规划了两个网段的IP地址。
- 现要求Router能够限制两个网段之间互访，防止公司机密泄露。

4、由于研发部和市场部互访的流量分别从接口GE0/0/1和GE0/0/2进入Router，所以在接口GE0/0/1和GE0/0/2的入方向配置流量过滤：

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-filter inbound acl 3001
[Router-GigabitEthernet0/0/1] quit

[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] traffic-filter inbound acl 3002
[Router-GigabitEthernet0/0/2] quit
```

本章总结

- ACL技术总是与防火墙、路由策略、QoS、流量过滤等其他技术结合使用。
- ACL的作用，ACL的组成、匹配和分类、通配符的使用方法，以及ACL的基本配置及应用。