5 ACL 配置

关于本章

设备为了对不同类的报文进行不同的处理，需要配置一系列的规则，以对报文进行分类，这些规则就是通过访问控制列表ACL定义的。

5.1 ACL简介
介绍ACL的定义和作用。

5.2 原理描述
介绍ACL的实现原理。

5.3 应用场景
介绍ACL的应用场景。

5.4 配置注意事项
介绍配置ACL的注意事项。

5.5 配置任务概览
设备支持的ACL主要包括：基本ACL、高级ACL、二层ACL、用户ACL、基本ACL6和高级ACL6。

5.6 缺省配置
介绍ACL缺省配置，实际应用的配置可以基于缺省配置进行修改。

5.7 配置ACL
介绍ACL详细的配置过程。

5.8 维护ACL
介绍如何维护ACL。

5.9 配置举例
介绍ACL的配置举例。配置示例中包括组网需求、配置思路、操作步骤等。

5.10 常见配置错误
介绍常见配置错误的案例，避免在配置阶段引入故障。

5.11 FAQ
介绍配置过程中常见的问题，以及解决方法。

5.12 参考标准和协议

介绍ACL的参考标准和协议。

5.1 ACL 简介

介绍ACL的定义和作用。

定义

访问控制列表ACL（Access Control List）是由一条或多条规则组成的集合。所谓规则，是指描述报文匹配条件的判断语句，这些条件可以是报文的源地址、目的地址、端口号等。

ACL本质上是一种报文过滤器，规则是过滤器的滤芯。设备基于这些规则进行报文匹配，可以过滤出特定的报文，并根据应用ACL的业务模块的处理策略来允许或阻止该报文通过。

说明

配置ACL后，还需将ACL在业务模块中应用，ACL才能生效。

ACL可以应用于诸多业务模块，其中最基本的ACL应用，就是在简化流策略/流策略中应用ACL，使设备能够基于全局、VLAN或接口下发ACL，实现对转发报文的过滤。此外，ACL还可以应用在Telnet、FTP、路由等模块。业务模块之间的ACL默认处理动作和处理机制有所不同，具体请参见**5.2.7 ACL应用模块的ACL默认动作和处理机制**。

目的

随着网络的飞速发展，网络安全和网络服务质量QoS（Quality of Service）问题日益突出。

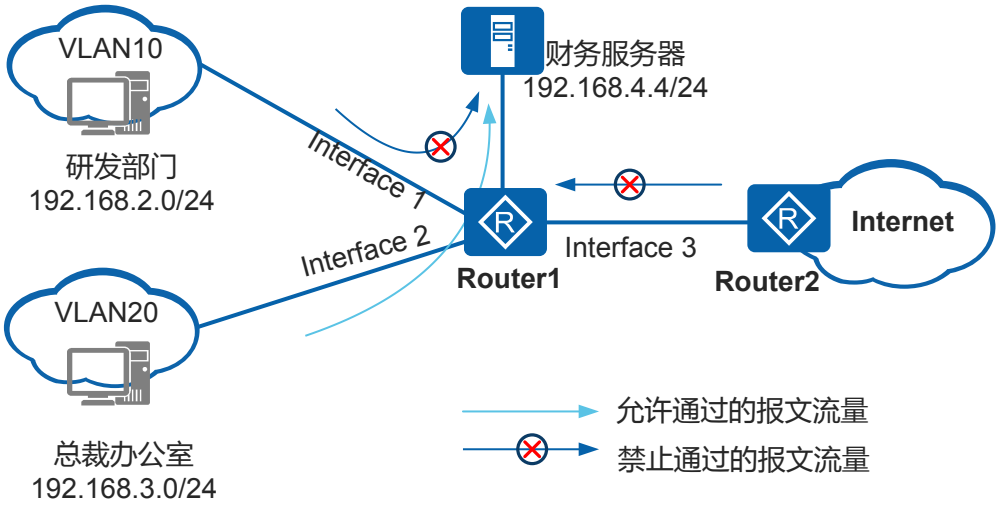
- 企业重要服务器资源被随意访问，企业机密信息容易泄露，造成安全隐患。
- Internet病毒肆意侵略企业内网，内网环境的安全性堪忧。
- 网络带宽被各类业务随意挤占，服务质量要求最高的语音、视频业务的带宽得不到保障，造成用户体验差。

以上种种问题，都对正常的网络通信造成了很大的影响。因此，提高网络安全性服务质量迫在眉睫。ACL就在这种情况下应运而生了。

通过ACL可以实现对网络中报文流的精确识别和控制，达到控制网络访问行为、防止网络攻击和提高网络带宽利用率的目的，从而切实保障网络环境的安全性和网络服务质量的可靠性。

图5-1是一个典型的ACL应用组网场景。

图 5-1 ACL 典型应用场景



- 某企业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。实现方式：

  在Interface 1的入方向上部署ACL，禁止研发部门访问财务服务器的报文通过。Interface 2上无需部署ACL，总裁办公室访问财务服务器的报文默认允许通过。
- 保护企业内网环境安全，防止Internet病毒入侵。实现方式：

  在Interface 3的入方向上部署ACL，将病毒经常使用的端口予以封堵。

5.2 原理描述

介绍ACL的实现原理。

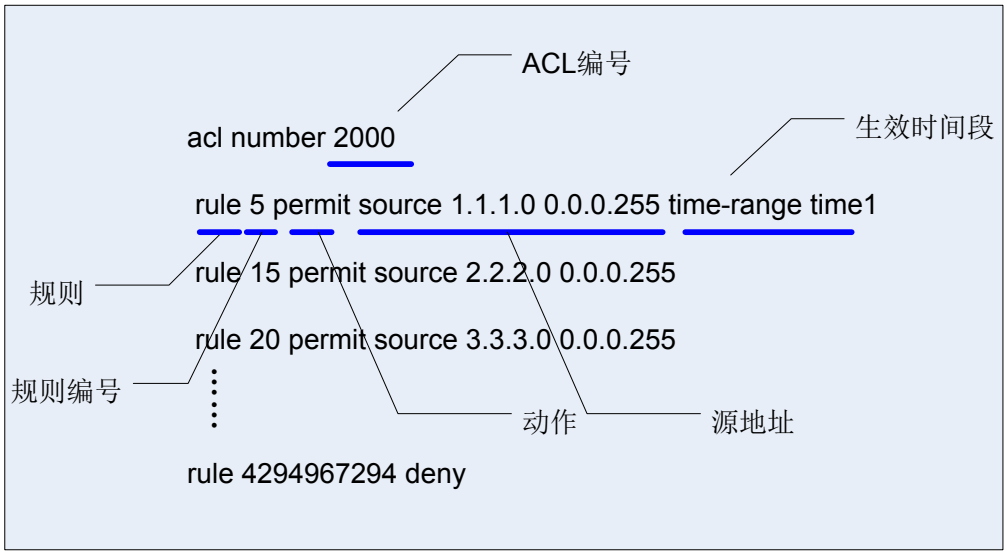
5.2.1 ACL 的基本原理

ACL由一系列规则组成，通过将报文与ACL规则进行匹配，设备可以过滤出特定的报文。

ACL 的组成

一条ACL的结构组成，如图5-2所示。

图 5-2 ACL 的结构组成



- **ACL编号**：用于标识ACL，表明该ACL是数字型ACL。

  根据ACL规则功能的不同，ACL被划分为基本ACL、高级ACL、二层ACL和用户ACL这几种类型，每类ACL编号的取值范围不同。关于每类ACL编号的详细介绍，请参见**5.2.2 ACL的分类**。

  除了可以通过ACL编号标识ACL，设备还支持通过名称来标识ACL，就像用域名代替IP地址一样，更加方便记忆。这种ACL，称为命名型ACL。

  命名型ACL实际上是“名字+数字”的形式，可以在定义命名型ACL时同时指定ACL编号。如果不指定编号，则由系统自动分配。例如，下面就是一个既有名字“deny-telnet-login”又有编号“3998”的ACL。

```
#
acl name deny-telnet-login 3998
 rule 0 deny tcp source 10.152.0.0 0.0.63.255 destination 10.64.0.97 0 destination-port eq
telnet
 rule 5 deny tcp source 10.242.128.0 0.0.127.255 destination 10.64.0.97 0 destination-port
eq telnet
#
```

- **规则**：即描述报文匹配条件的判断语句。
  - **规则编号**：用于标识ACL规则。可以自行配置规则编号，也可以由系统自动分配。

    ACL规则的编号范围是0～4294967294，所有规则均按照规则编号从小到大进行排序。所以，**图5-2**中的rule 5排在首位，而规则编号最大的rule 4294967294排在末位。系统按照规则编号从小到大的顺序，将规则依次与报文匹配，一旦匹配上一条规则即停止匹配。
  - **动作**：包括permit/deny两种动作，表示允许/拒绝。
  - **匹配项**：ACL定义了极其丰富的匹配项。除了**图5-2**中的源地址和生效时间段，ACL还支持很多其他规则匹配项。例如，二层以太网帧头信息（如源MAC、目的MAC、以太帧协议类型）、三层报文信息（如目的地址、协议类型）以及四层报文信息（如TCP/UDP端口号）等。关于每种匹配项的详细介绍，请参见**5.2.5 ACL的常用匹配项**。

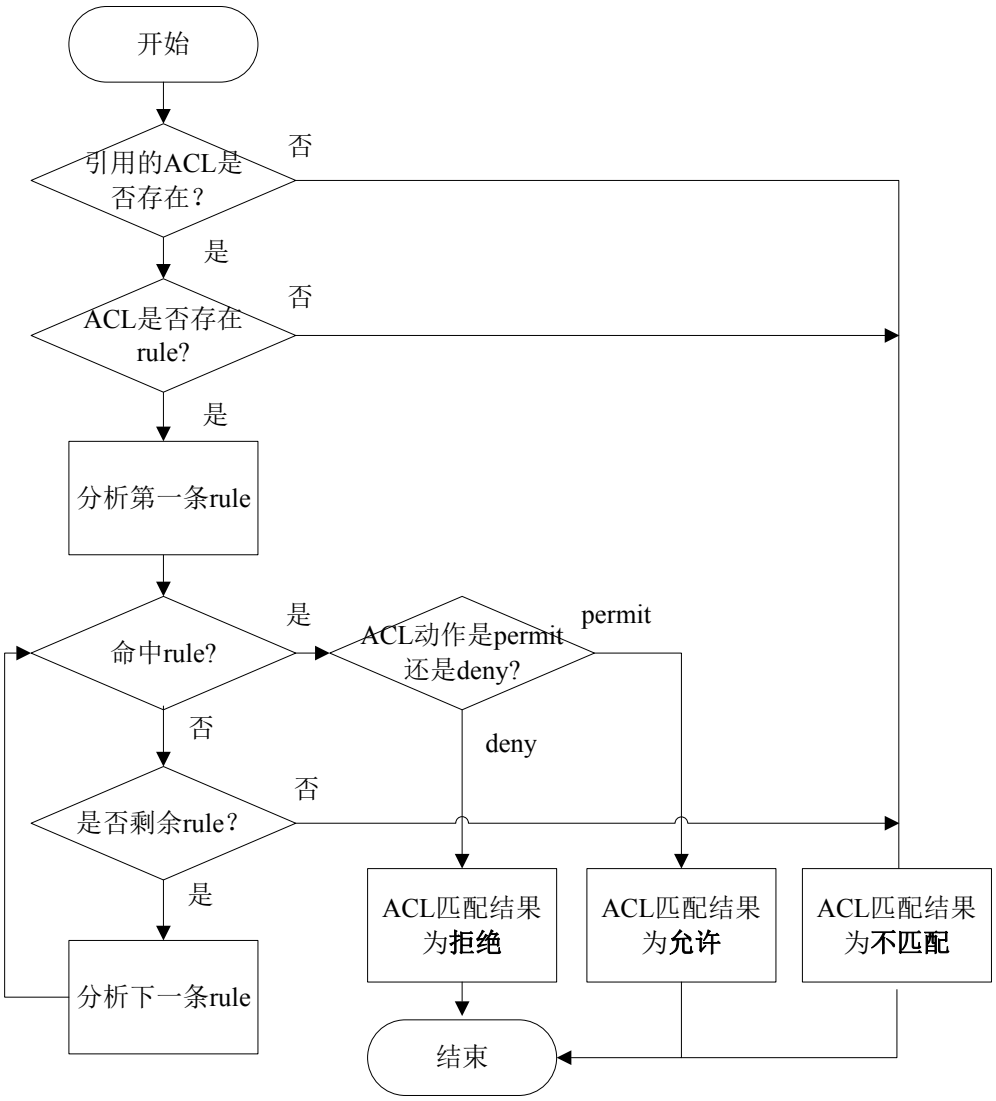
  说明

  如果设备启动使用的配置文件中配置了超规格的ACL规则，当设备启动加载该配置文件时，能生成ACL配置，但有部分配置不生效。

ACL 的匹配机制

设备将报文与ACL规则进行匹配时，遵循“一旦命中即停止匹配”的机制，如图5-3所示。

图 5-3 ACL 的匹配机制



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”。

说明

无论报文匹配ACL的结果是“不匹配”、“允许”还是“拒绝”，该报文最终是被允许通过还是拒绝通过，实际是由应用ACL的各个业务模块来决定。不同的业务模块，对命中和未命中规则报文的处理方式也各不相同。例如，在Telnet模块中应用ACL，只要报文命中了permit规则，就允许通过；而在流策略中应用ACL，如果报文命中了permit规则，但流行为动作配置的是deny，该报文仍会被拒绝通过。关于各个业务模块ACL处理机制的详细介绍，请参见**5.2.7 ACL应用模块的ACL默认动作和处理机制**。

5.2.2 ACL 的分类

基于 ACL 标识方法的划分

划分如下：

- 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。

用户在创建ACL时可以为其指定编号，不同的编号对应不同类型的ACL，如**表5-1**所示。同时，为了便于记忆和识别，用户还可以创建命名型ACL，即在创建ACL时为其设置名称。命名型ACL，也可以是“名称 数字”的形式，即在定义命名型ACL时，同时指定ACL编号。如果不指定编号，系统则会自动为其分配一个数字型ACL的编号。

说明

命名型ACL一旦创建成功，便不允许用户再修改其名称。如果删除ACL名称，则表示删除整个ACL。

仅基本ACL与基本ACL6，以及高级ACL与高级ACL6，可以使用相同的ACL名称；其他类型ACL之间，不能使用相同的ACL名称。

基于对 IPv4 和 IPv6 支持情况的划分

划分如下：

- ACL4：通常直接叫做“ACL”，特指仅支持过滤IPv4报文的ACL。
- ACL6：又叫做“IPv6 ACL”，特指仅支持过滤IPv6报文的ACL。

以上两种ACL，以及既支持过滤IPv4报文又支持过滤IPv6报文的ACL，统一称做“ACL”。各类型ACL对IPv4和IPv6的支持情况，如**表5-1**所示。

基于 ACL 规则定义方式的划分

表5-1所示，基于ACL规则定义方式的划分如下。

表 5-1 基于 ACL 规则定义方式的 ACL 分类

分类	适用的IP版本	规则定义描述	编号范围
基本ACL	IPv4	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。	2000～2999
高级ACL	IPv4	既可使用IPv4报文的**源IP地址**，也可使用**目的IP地址**、IP协议类型、ICMP类型、TCP源/目的端口、UDP源/目的端口号、生效时间段等来定义规则。	3000～3999
二层ACL	IPv4&IPv6	使用报文的**以太网帧头信息**来定义规则，如根据源MAC（Media Access Control）地址、目的MAC地址、二层协议类型等。	4000～4999
用户ACL	IPv4	既可使用IPv4报文的**源IP地址**，也可使用**目的IP地址**、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。	6000～6031
基本ACL6	IPv6	可使用IPv6报文的**源IPv6地址**、分片信息和生效时间段来定义规则。	2000～2999
高级ACL6	IPv6	可以使用IPv6报文的**源IPv6地址**、**目的IPv6地址**、IPv6协议类型、ICMPv6类型、TCP源/目的端口、UDP源/目的端口号、生效时间段等来定义规则。	3000～3999

5.2.3 ACL 的步长设定

步长的含义

步长，是指系统自动为ACL规则分配编号时，每个相邻规则编号之间的差值。

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。例如ACL中包含规则rule 5和rule 12，ACL（特指基本ACL、高级ACL、二层ACL、用户ACL）的缺省步长为5，大于12且是5的倍数的最小整数是15，所以系统分配给新配置的规则的编号为15。

说明

基本ACL6和高级ACL6不支持步长设定，缺省步长为1。

```
[Huawei-acl-basic-2001] display this
#
acl number 2001              //空ACL
#
```

```
return
[Huawei-acl-basic-2001] rule deny source 10.1.1.0 0.0.0.255 //配置首条不指定规则编号的规则
[Huawei-acl-basic-2001] display this
#
acl number 2001
 rule 5 deny source 10.1.1.0 0.0.0.255
#
return
[Huawei-acl-basic-2001] rule 12 deny source 10.2.2.0 0.0.0.255 //配置一条规则编号为12的规则
[Huawei-acl-basic-2001] display this
#
acl number 2001
 rule 5 deny source 10.1.1.0 0.0.0.255
 rule 12 deny source 10.2.2.0 0.0.0.255
#
return
[Huawei-acl-basic-2001] rule deny source 10.3.3.0 0.0.0.255 //再次配置一条不指定规则编号的规则
[Huawei-acl-basic-2001] display this
#
acl number 2001
 rule 5 deny source 10.1.1.0 0.0.0.255
 rule 12 deny source 10.2.2.0 0.0.0.255
 rule 15 deny source 10.3.3.0 0.0.0.255
#
return
```

如果重新调整了步长值（例如调整为2），系统则会自动从当前步长值开始重新排列规则编号，规则编号变成2、4、6…。恢复步长值为缺省值后，系统则会立刻按照缺省步长重新调整规则编号，规则编号变成5、10、15…。

```
[Huawei-acl-basic-2001] display acl 2001
Basic ACL 2001, 3 rules
Acl's step is 5
 rule 5 deny source 10.1.1.0 0.0.0.255
 rule 12 deny source 10.2.2.0 0.0.0.255
 rule 15 deny source 10.3.3.0 0.0.0.255

[Huawei-acl-basic-2001] step 2   //配置步长值为2
[Huawei-acl-basic-2001] display acl 2001
Basic ACL 2001, 3 rules
Acl's step is 2
 rule 2 deny source 10.1.1.0 0.0.0.255
 rule 4 deny source 10.2.2.0 0.0.0.255
 rule 6 deny source 10.3.3.0 0.0.0.255

[Huawei-acl-basic-2001] undo step   //恢复步长值为缺省值
[Huawei-acl-basic-2001] display acl 2001
Basic ACL 2001, 3 rules
Acl's step is 5
 rule 5 deny source 10.1.1.0 0.0.0.255
 rule 10 deny source 10.2.2.0 0.0.0.255
 rule 15 deny source 10.3.3.0
0.0.0.255
```

步长的作用

设置步长的作用，在于方便后续在旧规则之间插入新的规则。

假设，一条ACL中，已包含了三条规则rule 5、rule 10、rule 15。如果希望源IP地址为10.1.1.3的报文也被拒绝通过，该如何处理？

```
rule 5 deny source 10.1.1.1 0  //表示拒绝源IP地址为10.1.1.1的报文通过
rule 10 deny source 10.1.1.2 0 //表示拒绝源IP地址为10.1.1.2的报文通过
rule 15 permit source 10.1.1.0 0.0.0.255 //表示允许源IP地址为10.1.1.0/24网段地址的报文通过
```

由于ACL匹配报文时遵循“**一旦命中即停止匹配**”的原则，所以源IP地址为10.1.1.1和10.1.1.2的报文，会在匹配上编号较小的rule 5和rule 10后停止匹配，从而被系统拒绝通

过；而源IP地址为10.1.1.3的报文，则只会命中rule 15，从而得到系统允许通过。若想让源IP地址为10.1.1.3的报文也被拒绝通过，则必须为该报文配置一条新的deny规则。可以在rule 15之前插入一条新规则rule 11，这样源IP地址为10.1.1.3的报文，就会因先命中rule 11而被系统拒绝通过。插入rule 11后，该ACL的旧规则编号不受影响，且新的规则排序为rule 5、rule 10、rule 11、rule 15。

```
rule 5 deny source 10.1.1.1 0  //表示禁止源IP地址为10.1.1.1的报文通过
rule 10 deny source 10.1.1.2 0 //表示禁止源IP地址为10.1.1.2的报文通过
rule 11 deny source 10.1.1.3 0 //表示拒绝源IP地址为10.1.1.3的报文通过
rule 15 permit source 10.1.1.0 0.0.0.255 //表示允许源IP地址为10.1.1.0网段地址的报文通过
```

试想一下，如果这条ACL的规则间隔不是5，而是1（rule 1、rule 2、rule 3…），这时再想插入新的规则，就只能先删除已有的规则，然后再配置新规则，最后将之前删除的规则重新配置还原。

因此，为了避免上述操作造成的麻烦，ACL引入了步长的概念。通过设置ACL步长，使规则之间留有一定的空间，就可以轻松的在旧规则中插入新规则了。

5.2.4 ACL 的匹配顺序

一条ACL可以由多条“deny | permit”语句组成，每一条语句描述一条规则，这些规则可能存在重复或矛盾的地方。例如，在一条ACL中先后配置以下两条规则：

```
rule deny ip destination 10.1.0.0 0.0.255.255   //表示拒绝目的IP地址为10.1.0.0/16网段地址的报文通过
rule permit ip destination 10.1.1.0 0.0.0.255   //表示允许目的IP地址为10.1.1.0/24网段地址的报文通过，该网段地址范围小于10.1.0.0/16网段范围
```

其中，permit规则与deny规则是相互矛盾的。对于目的IP=10.1.1.1的报文，如果系统先将deny规则与其匹配，则该报文会被拒绝通过。相反，如果系统先将permit规则与其匹配，则该报文会得到允许通过。

因此，对于规则之间存在重复或矛盾的情形，报文的匹配结果与ACL的匹配顺序是息息相关的。

设备支持两种ACL匹配顺序：配置顺序（**config**模式）和自动排序（**auto**模式）。缺省的ACL匹配顺序是**config**模式。

配置顺序

配置顺序，即系统按照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。

- 如果配置规则时指定了规则编号，则规则编号越小，规则插入位置越靠前，该规则越先被匹配。
- 如果配置规则时未指定规则编号，则由系统自动为其分配一个编号。该编号是一个大于当前ACL内最大规则编号且是步长整数倍的最小整数，因此该规则会被最后匹配。

自动排序

自动排序，是指系统使用“深度优先”的原则，将规则按照精确度从高到低进行排序，并按照精确度从高到低的顺序进行报文匹配。规则中定义的匹配项限制越严格，规则的精确度就越高，即优先级越高，系统越先匹配。各类ACL的“深度优先”顺序匹配原则如**表5-2**所示。

关于**表5-2**中提到的IP地址通配符掩码、IP协议承载的协议类型、TCP/UDP端口号、二层协议类型通配符掩码、MAC地址通配符掩码等ACL匹配项的详细介绍，请参见**5.2.5 ACL的常用匹配项**。

表 5-2 “深度优先”匹配原则

ACL类型	匹配原则
基本ACL&ACL6	1. 先看规则中是否带VPN实例，带VPN实例的规则优先。 2. 再比较源IP地址范围，源IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 3. 如果源IP地址范围相同，则规则编号小的优先。
高级ACL&ACL6	1. 先看规则中是否带VPN实例，带VPN实例的规则优先。 2. 再比较协议范围，指定了IP协议承载的协议类型的规则优先。 3. 如果协议范围相同，则比较源IP地址范围，源IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 4. 如果协议范围、源IP地址范围相同，则比较目的IP地址范围，目的IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 5. 如果协议范围、源IP地址范围、目的IP地址范围相同，则比较四层端口号（TCP/UDP端口号）范围，四层端口号范围小的规则优先。 6. 如果上述范围都相同，则规则编号小的优先。
二层ACL	1. 先比较二层协议类型通配符掩码，通配符掩码大（协议类型通配符掩码中“1”位的数量多）的规则优先。 2. 如果二层协议类型通配符掩码相同，则比较源MAC地址范围，源MAC地址范围小（MAC地址通配符掩码中“1”位的数量多）的规则优先。 3. 如果源MAC地址范围相同，则比较目的MAC地址范围，目的MAC地址范围小（MAC地址通配符掩码中“1”位的数量多）的规则优先。 4. 如果源MAC地址范围、目的MAC地址范围相同，则规则编号小的优先。
用户ACL	1. 先比较协议范围，指定了IP协议承载的协议类型的规则优先。 2. 如果协议范围相同，则比较源IP地址范围。如果规则的源IP地址均为IP网段，则源IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 3. 如果协议范围、源IP地址范围相同，则比较目的IP地址范围。如果规则的目的IP地址均为IP网段，则目的IP地址范围小（IP地址通配符掩码中“0”位的数量多）的规则优先。 4. 如果协议范围、源IP地址范围、目的IP地址范围相同，则比较四层端口号（TCP/UDP端口号）范围，四层端口号范围小的规则优先。 5. 如果上述范围都相同，则规则编号小的优先。

在自动排序的ACL中配置规则时，不允许自行指定规则编号。系统能自动识别出该规则在这条ACL中对应的优先级，并为其分配一个适当的规则编号。

例如，在**auto**模式的高级ACL 3001中，先后配置以下两条规则：

```
rule deny ip destination 10.1.0.0 0.0.255.255    //表示拒绝目的IP地址为10.1.0.0/16网段地址的报文通过
rule permit ip destination 10.1.1.0 0.0.0.255    //表示允许目的IP地址为10.1.1.0/24网段地址的报文通过，该网段地址范围小于10.1.0.0/16网段范围
```

两条规则均没有带VPN实例，且协议范围、源IP地址范围相同，所以根据表5-2中高级ACL的深度优先匹配原则，接下来需要进一步比较规则的目的IP地址范围。由于permit

规则指定的目的地址范围小于deny规则，所以permit规则的精确度更高，系统为其分配的规则编号更小。配置完上述两条规则后，ACL 3001的规则排序如下：

```
#
acl number 3001 match-order auto
 rule 5 permit ip destination 10.1.1.0 0.0.0.255
 rule 10 deny ip destination 10.1.0.0 0.0.255.255
#
```

此时，如果再插入一条新的规则rule deny ip destination 10.1.1.1 0（目的IP地址范围是主机地址，优先级高于以上两条规则），则系统将按照规则的优先级关系，重新为各规则分配编号。插入新规则后，ACL 3001新的规则排序如下：

```
#
acl number 3001 match-order auto
 rule 5 deny ip destination 10.1.1.1 0
 rule 10 permit ip destination 10.1.1.0 0.0.0.255
 rule 15 deny ip destination 10.1.0.0 0.0.255.255
#
```

相比**config**模式的ACL，**auto**模式ACL的规则匹配顺序更为复杂，但是**auto**模式ACL有其独特的应用场景。例如，在网络部署初始阶段，为了保证网络安全性，管理员定义了较大的ACL匹配范围，用于丢弃不可信网段范围的所有IP报文。随着时间的推移，实际应用中需要允许这个大范围中某些特征的报文通过。此时，如果管理员采用的是**auto**模式，则只需要定义新的ACL规则，无需再考虑如何对这些规则进行排序避免报文被误丢弃。

5.2.5 ACL 的常用匹配项

设备支持的ACL匹配项种类非常丰富，其中最常用的匹配项包括以下几种。

生效时间段

格式：**time-range** *time-name*

所有ACL均支持根据生效时间段过滤报文。关于生效时间段的详细介绍，请参见**5.2.6 ACL的生效时间段**。

IP 承载的协议类型

格式：*protocol-number* | **icmp** | **tcp** | **udp** | **gre** | **igmp** | **ip** | **ipinip** | **ospf**

高级ACL支持基于协议类型过滤报文。常用的协议类型包括：ICMP（协议号1）、TCP（协议号6）、UDP（协议号17）、GRE（协议号47）、IGMP（协议号2）、IP（指任何IP层协议）、IPinIP（协议号4）、OSPF（协议号89）。协议号的取值可以是1～255。

例如，当设备某个接口下的用户存在大量的攻击者时，如果希望能够禁止这个接口下的所有用户接入网络，则可以通过指定协议类型为IP来屏蔽这些用户的IP流量来达到目的。配置如下：

```
rule deny ip //表示拒绝IP报文通过
```

再如，设备上打开透明防火墙功能后，在缺省情况下，透明防火墙会在域间丢弃所有入域间的报文，包括业务报文和协议报文。如果希望像OSPF这样的动态路由协议报文能正常通过防火墙，保证路由互通，这时，通过指定协议类型为OSPF即可解决问题。

```
rule permit ospf  //表示允许OSPF报文通过
```

源/目的 IP 地址及其通配符掩码

源IP地址及其通配符掩码格式：**source** { *source-address source-wildcard* | **any** }

目的IP地址及其通配符掩码格式：**destination** { *destination-address destination-wildcard* | **any** }

基本ACL支持根据源IP地址过滤报文，高级ACL不仅支持源IP地址，还支持根据目的IP地址过滤报文。

将源/目的IP地址定义为规则匹配项时，需要在源/目的IP地址字段后面同时指定通配符掩码，用来与源/目的IP地址字段共同确定一个地址范围。

IP地址通配符掩码与IP地址的反向子网掩码类似，也是一个32比特位的数字字符串，用于指示IP地址中的哪些位将被检查。各比特位中，“0”表示“检查相应的位”，“1”表示“不检查相应的位”，概括为一句话就是“检查0，忽略1”。但与IP地址子网掩码不同的是，子网掩码中的“0”和“1”要求必须连续，而通配符掩码中的“0”和“1”可以不连续。

通配符掩码可以为0，相当于0.0.0.0，表示源/目的地址为主机地址；也可以为255.255.255.255，表示任意IP地址，相当于指定**any**参数。

举一个IP地址通配符掩码的示例，当希望来自192.168.1.0/24网段的所有IP报文都能够通过，可以配置如下规则：

```
rule 5 permit ip source 192.168.1.0 0.0.0.255
```

规则中的通配符掩码为0.0.0.255，表示只需检查IP地址的前三组二进制八位数对应的比特位。因此，如果报文源IP地址的前24个比特位与参照地址的前24个比特位（192.168.1）相同，即报文的源IP地址是192.168.1.0/24网段的地址，则允许该报文通过。表5-3展示了该例的地址范围计算过程。

表 5-3 通配符掩码示例

项目	十进制等价值	二进制等价值
参照地址	192.168.1.0	11000000.10101000.00000001.00000000
通配符掩码	0.0.0.255	00000000.00000000.00000000.**11111111**
确定的地址范围	192.168.1.* *表示0～255之间的整数	11000000.10101000.00000001.**xxxxxxxx** x既可以是0，也可以是1

更多的IP地址与通配符掩码共同确定的地址范围示例，详见表5-4。

表 5-4 IP 地址与通配符掩码共同确定的地址范围

IP地址	IP地址通配符掩码	确定的地址范围
0.0.0.0	255.255.255.255	任意IP地址
172.18.0.0	0.0.255.255	172.18.0.0/16网段的IP地址

IP地址	IP地址通配符掩码	确定的地址范围
172.18.5.2	0.0.0.0	仅172.18.5.2这一个主机地址
172.18.8.0	0.0.0.7	172.18.8.0/29网段的IP地址
172.18.8.8	0.0.0.7	172.18.8.8/29网段的IP地址
10.1.2.0	0.0.254.255（通配符掩码中的1和0不连续）	10.1.0.0/24～10.1.254.0/24网段之间且第三个字节为偶数的IP地址，如10.1.0.0/24、10.1.2.0/24、10.1.4.0/24、10.1.6.0/24等。

源/目的 MAC 地址及其通配符掩码

源MAC地址及其通配符掩码格式：**source-mac** *source-mac-address* [*source-mac-mask*]

目的地址及其通配符掩码格式：**destination-mac** *dest-mac-address* [*dest-mac-mask*]

仅二层ACL支持基于源/目的MAC地址过滤报文。

将源/目的MAC地址定义为规则匹配项时，可以在源/目的MAC地址字段后面同时指定通配符掩码，用来与源/目的MAC地址字段共同确定一个地址范围。

MAC地址通配符掩码的格式与MAC地址相同，采用十六进制数表示，共六个字节（48位），用于指示MAC地址中的哪些位将被检查。与IP地址通配符掩码不同的是，MAC地址通配符掩码各比特位中，1表示“检查相应的位”，0表示“不检查相应的位”。如果不指定通配符掩码，则默认掩码为ffff-ffff-ffff，表示检查MAC地址的每一位。

MAC地址与通配符掩码共同确定的地址范围示例，如表5-5所示。

表 5-5 MAC 地址与通配符掩码共同确定的地址范围

MAC地址	MAC地址通配符掩码	确定的地址范围
00e0-fc01-0101	0000-0000-0000	任意MAC地址
00e0-fc01-0101	ffff-ffff-ffff	仅00e0-fc01-0101这一个MAC地址
00e0-fc01-0101	ffff-ffff-0000	00e0-fc01-0000～00e0-fc01-ffff

VLAN 编号及其掩码

外层VLAN及其掩码格式：**vlan-id** *vlan-id* [*vlan-id-mask*]

内层VLAN及其掩码格式：**cvlan-id** *cvlan-id* [*cvlan-id-mask*]

二层ACL支持基于外层VLAN或内层VLAN编号过滤报文。

将VLAN编号定义为规则匹配项时，可以在VLAN编号字段后面同时指定VLAN掩码，用来与VLAN编号字段共同确定一个VLAN范围。

VLAN掩码的格式是十六进制形式，取值范围是0x0～0xFFF。如果不指定VLAN掩码，则默认掩码为0xFFF，表示检查VLAN编号的每一位。

VLAN编号与掩码共同确定的VLAN范围示例，如表5-6所示。

表 5-6 VLAN 编号及其掩码共同确定的 VLAN 范围

VLAN编号	VLAN掩码	确定的VLAN范围
10	0x000	任意VLAN
10	0xFFF	仅VLAN 10
10	0xFF0	VLAN 1～VLAN 10

TCP/UDP 端口号

源端口号格式：**source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }

目的端口号格式：**destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }

在高级ACL中，当协议类型指定为TCP或UDP时，设备支持基于TCP/UDP的源/目的端口号过滤报文。

其中，TCP/UDP端口号的比较符含义如下：

- **eq** *port*：指定等于源/目的端口。
- **gt** *port*：指定大于源/目的端口。
- **lt** *port*：指定小于源/目的端口。
- **range** *port-start port-end*：指定源/目的端口的范围。*port-start*是端口范围的起始，*port-end*是端口范围的结束。

TCP/UDP端口号可以使用数字表示，也可以用字符串（助记符）表示。例如，**rule deny tcp destination-port eq 80**，可以用**rule deny tcp destination-port eq www**替代。常见TCP端口号及对应的字符串如表5-7所示，常见UDP端口号及对应的字符串如表5-8所示。

表 5-7 常见 TCP 端口号及对应的字符串

端口号	字符串	协议	说明
7	echo	Echo	Echo服务
9	discard	Discard	用于连接测试的空服务
13	daytime	Daytime	给请求主机发送日期和时间
19	CHARgen	Character generator	字符生成服务；发送无止境的字符流
20	ftp-data	FTP data connections	FTP数据端口

端口号	字符串	协议	说明
21	ftp	File Transfer Protocol(FTP)	文件传输协议（FTP）端口
23	telnet	Telnet	Telnet服务
25	smtp	Simple Mail Transport Protocol (SMTP)	简单邮件传输协议
37	time	Time	时间协议
43	whois	Nicname（WHOIS）	目录服务
49	tacacs	TAC Access Control System (TACACS)	用于基于TCP/IP验证和访问的访问控制系统（TACACS登录主机协议）
53	domain	Domain Name Service (DNS)	域名服务
70	gopher	Gopher	信息检索协议（互联网文档搜寻和检索）
79	finger	Finger	用于用户联系信息的Finger服务，查询远程主机在线用户等信息
80	www	World Wide Web (HTTP)	用于万维网（WWW）服务的超文本传输协议（HTTP），用于网页浏览
101	hostname	NIC hostname server	NIC机器上的主机名服务
109	pop2	Post Office Protocol v2	邮件协议-版本2
110	pop3	Post Office Protocol v3	邮件协议-版本3
111	sunrpc	Sun Remote Procedure Call (RPC)	SUN公司的远程过程调用（RPC）协议，用于远程命令执行，被网络文件系统（NFS）使用
119	nntp	Network News Transport Protocol (NNTP)	网络新闻传输协议，承载USENET通信
179	bgp	Border Gateway Protocol (BGP)	边界网关协议

端口号	字符串	协议	说明
194	irc	Internet Relay Chat (IRC)	互联网中继聊天（多线交谈协议）
512	exec	Exec (rsh)	用于对远程执行的进程进行验证
513	login	Login (rlogin)	远程登录
514	cmd	Remote commands	远程命令，不必登录的远程shell（rshell）和远程复制（rcp）
515	lpd	Printer service	打印机（lpr）假脱机
517	talk	Talk	远程对话服务和客户
540	uucp	Unix-to-Unix Copy Program	Unix到Unix复制服务
543	klogin	Kerberos login	Kerberos版本5（v5）远程登录
544	kshell	Kerberos shell	Kerberos版本5（v5）远程shell

表 5-8 常见 UDP 端口号及对应的字符串

端口号	字符串	协议	说明
7	echo	Echo	Echo服务
9	discard	Discard	用于连接测试的空服务
37	time	Time	时间协议
42	nameserver	Host Name Server	主机名服务
53	dns	Domain Name Service (DNS)	域名服务
65	tacacs-ds	TACACS-Database Service	TACACS数据库服务
67	bootps	Bootstrap Protocol Server	引导程序协议（BOOTP）服务端，DHCP服务使用
68	bootpc	Bootstrap Protocol Client	引导程序协议（BOOTP）客户端，DHCP客户使用
69	tftp	Trivial File Transfer Protocol (TFTP)	小文件传输协议

端口号	字符串	协议	说明
90	dnsix	DNSIX Security Attribute Token Map	DNSIX安全属性标记图
111	sunrpc	SUN Remote Procedure Call (SUN RPC)	SUN公司的远程过程调用（RPC）协议，用于远程命令执行，被网络文件系统（NFS）使用
123	ntp	Network Time Protocol (NTP)	网络时间协议，蠕虫病毒会利用
137	netbios-ns	NETBIOS Name Service	NETBIOS名称服务
138	netbios-dgm	NETBIOS Datagram Service	NETBIOS数据报服务
139	netbios-ssn	NETBIOS Session Service	NETBIOS会话服务
161	snmp	SNMP	简单网络管理协议
162	snmptrap	SNMPTRAP	SNMP陷阱
177	xdmcp	X Display Manager Control Protocol (XDMCP)	X显示管理器控制协议
434	mobilip-ag	MobileIP-Agent	移动IP代理
435	mobilip-mn	MobileIP-MN	移动IP管理
512	biff	Mail notify	异步邮件，可用来通知用户有邮件到达
513	who	Who	登录的用户列表
514	syslog	Syslog	UNIX系统日志服务
517	talk	Talk	远程对话服务器和客户端
520	rip	Routing Information Protocol	RIP路由协议

TCP 标志信息

格式：**tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** }*

在高级ACL中，当协议类型指定为TCP时，设备支持基于TCP标志信息过滤报文。

TCP报文头有6个标志位：

- URG(100000)：标识紧急指针有效

- ACK(010000)：标识确认序号有效
- PSH(001000)：标识接收方应该尽快将这个报文段上交给应用层
- RST(000100)：标识重建连接
- SYN(000010)：同步序号，用来发起一个连接
- FIN(000001)：标识发送方完成发送任务

TCP标志信息中的**established**，表示标志位为ACK(010000)或RST(000100)。

指定**tcp-flag**的ACL规则可以用来实现单向访问控制。假设，要求192.168.1.0/24网段用户可以主动访问192.168.2.0/24网段用户，但反过来192.168.2.0/24网段用户不能主动访问192.168.1.0/24。可通过在设备上连接192.168.2.0/24网段的接口入方向上，应用ACL规则来实现该需求。

由TCP建立连接和关闭连接的过程可知，只有在TCP中间连接过程的报文才会ACK=1或者RST=1。根据这个特点，配置如下两种ACL规则，允许TCP中间连接过程的报文通过，拒绝其他TCP报文通过，就可以限制192.168.2.0/24网段主动发起的TCP连接。

- 类型一：配置指定**ack**和**rst**参数的ACL规则

```
rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack  //允许ACK=1的TCP报文通过
rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst   //允许RST=1的TCP报文通过
rule 15 deny tcp source 192.168.2.0 0.0.0.255  //拒绝其他TCP报文通过
```

- 类型二：配置指定**established**参数的ACL规则

```
rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag established  // established表示ACK=1或者RST=1，表示允许TCP中间连接过程的报文通过
rule deny tcp source 192.168.2.0 0.0.0.255     //拒绝其他TCP报文通过
```

IP 分片信息

格式：**none-first-fragment**

基本ACL和高级ACL支持基于IP分片信息过滤报文。

IP分片除了首片报文外，还有后续分片报文，又叫做非首片分片报文。仅首片分片报文携带四层信息（如TCP/UDP端口号等），后续分片报文均不携带。网络设备收到分片报文后，会判断其是否是最后一个分片报文。如果不是，则为其分配内存空间，以便于最后一个分片报文到达后完成重组。黑客可以利用这一点，向接收方设备发起分片报文攻击，始终不向接收方发送最后一个分片报文，使得接收方的内存得不到及时释放（接收方会启动一个分片重组的定时器，在定时器超时前如果无法完成重组，将向发送方发送ICMP重组超时差错报文；如果定时器超时后仍未完成重组，则丢弃已存储的分片报文）。在分片报文发送数量很多并且发送速度很快的情况下，接收方的内存很容易被占满，从而导致接收方没有足够的内存资源处理其他正常的业务。

为了解决这个问题，可以配置指定**none-first-fragment**匹配项的ACL规则来阻塞非首片分片报文，从而达到防范分片报文攻击的目的。

针对非分片报文、首片分片报文、非首片分片报文这三类报文，ACL的处理方式如**表5-9**所示。

表 5-9 ACL 对 IP 分片报文的处理方式

规则包含的匹配项	非分片报文	首片分片报文	非首片分片报文
三层信息（如源/目的IP地址）	三层信息匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配	三层信息匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配	三层信息匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配
三层信息 + 四层信息（如TCP/UDP端口号）	三层和四层信息都匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配	三层和四层信息都匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配	不匹配，转下一条规则进行匹配
三层信息 + **none-first-fragment**	不匹配，转下一条规则进行匹配	不匹配，转下一条规则进行匹配	三层信息匹配上，则返回匹配结果（permit/deny）；未匹配上，则转下一条规则进行匹配

例如，ACL 3012中存在以下规则：

```
#
acl number 3012
 rule 5 deny tcp destination 192.168.2.2 0 none-first-fragment
 rule 10 permit tcp destination 192.168.2.2 0 destination-port eq www
 rule 15 deny ip
#
```

- 该报文是非分片报文或首片分片报文时：如果该报文的目的端口号是80（www对应的端口号是80），则报文与rule 10匹配，报文被允许通过；如果该报文的目的端口号不是80，则报文与rule 15匹配，报文被拒绝通过。
- 该报文是非首片分片报文时：该报文与rule 5匹配，报文被拒绝通过。

5.2.6 ACL 的生效时间段

产生背景

ACL定义了丰富的匹配项，可以满足大部分的报文过滤需求。但需求是不断变化发展的，新的需求总是不断涌现。例如，某公司要求，在上班时间只允许员工浏览与工作相关的几个网站，下班或周末时间才可以访问其他互联网网站；再如，在每天20:00～22:00的网络流量的高峰期，为防止P2P、下载类业务占用大量带宽对其他数据业务的正常使用造成影响，需要对P2P、下载类业务的带宽进行限制。

基于时间的ACL过滤就是用来解决上述问题的。管理员可以根据网络访问行为的要求和网络的拥塞情况，配置一个或多个ACL生效时间段，然后在ACL规则中引用该时间段，从而实现在不同的时间段设置不同的策略，达到网络优化的目的。

生效时间段模式

在ACL规则中引用的生效时间段存在两种模式：

- 第一种模式——周期时间段：以星期为参数来定义时间范围，表示规则以一周为周期（如每周一的8至12点）循环生效。

  格式：**time-range** *time-name start-time* **to** *end-time* { *days* } &<1-7>

  - *time-name*：时间段名称，以英文字母开头的字符串。
  - *start-time* **to** *end-time*：开始时间和结束时间。格式为[小时:分钟] to [小时:分钟]。
  - *days*：有多种表达方式。
    - **Mon**、**Tue**、**Wed**、**Thu**、**Fri**、**Sat**、**Sun**中的一个或者几个的组合，也可以用数字表达，0表示星期日，1表示星期一，……6表示星期六。
    - **working-day**：从星期一到星期五，五天。
    - **daily**：包括一周七天。
    - **off-day**：包括星期六和星期日，两天。
- 第二种模式——绝对时间段：从某年某月某日的某一时间开始，到某年某月某日的某一时间结束，表示规则在这段时间范围内生效。

  格式：**time-range** *time-name* **from** *time1 date1* [**to** *time2 date2*]

  - *time-name*：时间段名称，以英文字母开头的字符串。
  - *time1*/*time2*：格式为[小时:分钟]。
  - *date1*/*date2*：格式为[YYYY/MM/DD]，表示年/月/日。

可以使用同一名称（*time-name*）配置内容不同的多条时间段，配置的各周期时间段之间以及各绝对时间段之间的交集将成为最终生效的时间范围。

例如，在ACL 2001中引用了时间段“test”，“test”包含了三个生效时间段：

```
#
time-range test 8:00 to 18:00 working-day
time-range test 14:00 to 18:00 off-day
time-range test from 00:00 2014/01/01 to 23:59 2014/12/31
#
acl number 2001
 rule 5 permit time-range test
```

- 第一个时间段，表示在周一到周五每天8:00到18:00生效，这是一个周期时间段。
- 第二个时间段，表示在周六、周日下午14:00到18:00生效，这是一个周期时间段。
- 第三个时间段，表示从2014年1月1日00:00起到2014年12月31日23:59生效，这是一个绝对时间段。

时间段“test”最终描述的时间范围为：2014年的周一到周五每天8:00到18:00以及周六和周日下午14:00到18:00。

5.2.7 ACL 应用模块的 ACL 默认动作和处理机制

ACL 的应用模块

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。

最基本的ACL应用方式，是在简化流策略/流策略中应用ACL，使设备能够基于全局、VLAN或接口下发ACL，实现对转发报文的过滤。此外，ACL还可以应用在Telnet、FTP、路由等模块。

如表5-10所示，ACL应用的业务模块，主要分为以下几类。

表 5-10 ACL 应用的业务模块

业务分类	应用场景	涉及业务模块
对转发的报文进行过滤	基于全局、接口和VLAN，对转发的报文进行过滤，从而使设备能够进一步对过滤出的报文进行丢弃、修改优先级、重定向等处理。 例如，可以利用ACL，降低P2P下载、网络视频等消耗大量带宽的数据流的服务等级，在网络拥塞时优先丢弃这类流量，减少它们对其他重要流量的影响。	简化流策略/流策略
对上送CPU处理的报文进行过滤	对上送CPU的报文进行必要的限制，可以避免CPU处理过多的协议报文造成占用率过高、性能下降。 例如，当发现某用户向设备发送大量的ARP攻击报文，造成设备CPU繁忙，引发系统中断时，可以在本机防攻击策略的黑名单中应用ACL，将该用户加入黑名单，使CPU丢弃该用户发送的报文。	黑名单
登录控制	对设备的登录权限进行控制，允许合法用户登录，拒绝非法用户登录，从而有效防止未经授权用户的非法接入，保证网络安全性。 例如，一般情况下设备只允许管理员登录，非管理员用户不允许随意登录。这时就可以在Telnet中应用ACL，并在ACL中定义哪些主机可以登录，哪些主机不能。	Telnet、STelnet、FTP、SFTP、HTTP、SNMP
路由过滤	ACL可以应用在各种动态路由协议中，对路由协议发布、接收的路由信息以及组播组进行过滤。 例如，可以将ACL和路由策略配合使用，禁止设备将某网段路由发给邻居路由器。	BGP、IS-IS、OSPF、OSPFv3、RIP、RIPng、组播协议

应用模块的 ACL 默认动作和处理机制

在各类业务模块中应用ACL时，ACL的默认动作各有不同，所以各业务模块对命中/未命中ACL规则报文的处理机制也各不相同。

例如，流策略中的ACL默认动作是permit，在流策略中应用ACL时，如果ACL中存在规则但报文未匹配上，该报文仍可以正常通过。而Telnet中的ACL默认动作是deny，在Telnet中应用ACL时，如果遇到此种情况，该报文会被拒绝通过。

此外，黑名单模块中的ACL处理机制与其他模块有所不同。在黑名单中应用ACL时，无论ACL规则配置成permit还是deny，只要报文命中了规则，该报文都会被系统丢弃。

各类业务模块中的ACL默认动作及ACL处理机制，如表5-11所示。

表 5-11 各业务模块的 ACL 默认动作及 ACL 处理机制

业务模块	ACL默认动作	ACL处理机制				
		命中permit规则	命中deny规则	ACL中配置了规则，但未命中任何规则	ACL中未配置规则	ACL未创建
Telnet	deny	permit（允许登录）	deny（拒绝登录）	deny（拒绝登录）	permit（允许登录）	permit（允许登录）
STelnet	deny	permit（允许登录）	deny（拒绝登录）	deny（拒绝登录）	permit（允许登录）	permit（允许登录）
HTTP	deny	permit（允许登录）	deny（拒绝登录）	deny（拒绝登录）	permit（允许登录）	permit（允许登录）
SNMP	deny	permit（允许登录）	deny（拒绝登录）	deny（拒绝登录）	permit（允许登录）	permit（允许登录）
FTP	deny	permit（允许登录）	deny（拒绝登录）	deny（拒绝登录）	permit（允许登录）	permit（允许登录）
TFTP	deny	permit（允许登录）	deny（拒绝登录）	deny（拒绝登录）	permit（允许登录）	permit（允许登录）
SFTP	deny	permit（允许登录）	deny（拒绝登录）	deny（拒绝登录）	permit（允许登录）	permit（允许登录）

业务模块	ACL默认动作	ACL处理机制				
		命中permit规则	命中deny规则	ACL中配置了规则，但未命中任何规则	ACL中未配置规则	ACL未创建
流策略	permit	● 流行为是permit时:permit（允许通过） ● 流行为是deny时：deny（丢弃报文） ● 流行为是其他动作时：permit（执行流策略动作）	deny(丢弃报文) **说明** 报文命中deny规则时，只有在流行为是流量统计或流镜像的情况下，设备才会执行流行为动作，否则流行为动作不生效。	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，按照原转发方式进行转发）

业务模块	ACL默认动作	ACL处理机制				
		命中permit规则	命中deny规则	ACL中配置了规则，但未命中任何规则	ACL中未配置规则	ACL未创建
简化流策略	permit	permit（执行简化流策略动作）	● 简化流策略动作为报文过滤（traffic-filter或traffic-secure）时:deny（丢弃报文） ● 简化流策略动作为其他动作时：permit（执行简化流策略动作）	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，按照原转发方式进行转发）
本机防攻击策略（黑名单）	permit	deny(丢弃报文)	deny(丢弃报文)	permit（功能不生效，正常上送报文）	permit（功能不生效，正常上送报文）	permit（功能不生效，正常上送报文）

业务模块		ACL默认动作	ACL处理机制				
			命中permit规则	命中deny规则	ACL中配置了规则，但未命中任何规则	ACL中未配置规则	ACL未创建
路由	Route Policy	deny	● 匹配模式是permit时：permit(允许执行路由策略) ● 匹配模式是deny时：deny(不允许执行路由策略)	deny（功能不生效，不允许执行路由策略）	deny（功能不生效，不允许执行路由策略）	permit（对经过的所有路由生效）	deny（功能不生效，不允许执行路由策略）
	Filter Policy	deny	permit（允许发布或接收该路由）	deny（不允许发布或接收该路由）	deny（不允许发布或接收该路由）	deny（不允许发布或接收路由）	permit（允许发布或接收路由）
组播	igmp-snooping ssm-policy	deny	permit(允许加入SSM组播组范围)	deny(禁止加入SSM组地址范围)	deny(禁止加入SSM组地址范围)	deny（禁止加入SSM组地址范围，所有组都不在SSM组地址范围内）	deny(禁止加入SSM组地址范围，只有临时组地址范围232.0.0.0～232.255.255.255在SSM组地址范围内)

业务模块		ACL默认动作	ACL处理机制				
			命中permit规则	命中deny规则	ACL中配置了规则，但未命中任何规则	ACL中未配置规则	ACL未创建
	igmp-snooping group-policy	permit	permit(允许加入组播组)	deny(禁止加入组播组)	permit（允许加入组播组）	permit（允许加入组播组）	permit（允许加入组播组）

5.2.8 ACL 的常用配置原则

配置ACL规则时，可以遵循以下原则：

1. 如果配置的ACL规则存在包含关系，应注意严格条件的规则编号需要排序靠前，宽松条件的规则编号需要排序靠后，避免报文因命中宽松条件的规则而停止往下继续匹配，从而使其无法命中严格条件的规则。
2. 根据各业务模块ACL默认动作（请参见**5.2.7 ACL应用模块的ACL默认动作和处理机制**）的不同，ACL的配置原则也不同。例如，在默认动作为permit的业务模块中，如果只希望deny部分IP地址的报文，只需配置具体IP地址的deny规则，结尾无需添加任意IP地址的permit规则；而默认动作为deny的业务模块恰与其相反。详细的ACL常用配置原则，如**表5-12**所示。

   说明

   以下rule的表达方式仅是示意形式，实际配置方法请参考各类ACL规则的命令行格式。

   - **rule permit xxx/rule permit xxxx**：表示允许指定的报文通过，xxx/xxxx表示指定报文的标识，可以是源IP地址、源MAC地址、生效时间段等。xxxx表示的范围与xxx表示的范围是包含关系，例如xxx是某一个IP地址，xxxx可以是该IP地址所在的网段地址或**any**（表示任意IP地址）；再如xxx是周六的某一个时段，xxxx可以是双休日全天时间或一周七天全部时间。
   - **rule deny xxx/rule deny xxxx**：表示拒绝指定的报文通过。
   - **rule permit**：表示允许所有报文通过。
   - **rule deny**：表示拒绝所有报文通过。

表 5-12 ACL 的常用配置原则

业务模块的ACL默认动作	permit所有报文	deny所有报文	permit少部分报文，deny大部分报文	deny少部分报文，permit大部分报文
permit	无需应用ACL	配置**rule deny**	需先配置**rule permit xxx**，再配置**rule deny xxxx**或**rule deny** **说明** 以上原则适用于报文过滤的情形。当ACL应用于流策略中进行流量监管或者流量统计时，如果仅希望对指定的报文进行限速或统计，则只需配置**rule permit xxx**。	只需配置**rule deny xxx**，无需再配置**rule permit xxxx**或**rule permit** **说明** 如果配置**rule permit**并在流策略中应用ACL，且该流策略的流行为behavior配置为**deny**，则设备会拒绝所有报文通过，导致全部业务中断。
deny	● 路由和组播模块：需配置**rule permit** ● 其他模块：无需应用ACL	● 路由和组播模块：无需应用ACL ● 其他模块：需配置**rule deny**	只需配置**rule permit xxx**，无需再配置**rule deny xxxx**或**rule deny**	需先配置**rule deny xxx**，再配置**rule permit xxxx**或**rule permit**

举例：

- 例1：在流策略中应用ACL，使设备对192.168.1.0/24网段的报文进行过滤，拒绝192.168.1.2和192.168.1.3主机地址的报文通过，允许192.168.1.0/24网段的其他地址的报文通过。

  流策略的ACL默认动作为**permit**，该例属于“deny少部分报文，permit大部分报文”的情况，所以只需配置**rule deny xxx**。

  ```
  #
  acl number 2000
   rule 5 deny source 192.168.1.2 0
   rule 10 deny source 192.168.1.3 0
  #
  ```

- 例2：在流策略中应用ACL，使设备对192.168.1.0/24网段的报文进行过滤，允许192.168.1.2和192.168.1.3主机地址的报文通过，拒绝192.168.1.0/24网段的其他地址的报文通过。

  流策略的ACL默认动作为**permit**，该例属于“permit少部分报文，deny大部分报文”的情况，所以需先配置**rule permit xxx**，再配置**rule deny xxxx**。

  ```
  #
  acl number 2000
   rule 5 permit source 192.168.1.2 0
   rule 10 permit source 192.168.1.3 0
  ```

```
 rule 15 deny source 192.168.1.0 0.0.0.255
#
```

- 例3：在Telnet中应用ACL，仅允许管理员主机（IP地址为172.16.105.2）能够Telnet登录设备，其他用户不允许Telnet登录。

  Telnet的ACL默认动作为**deny**，该例属于“permit少部分报文，deny大部分报文”的情况，所以只需配置**rule permit xxx**。

```
#
acl number 2000
 rule 5 permit source 172.16.105.2 0
#
```

- 例4：在Telnet中应用ACL，不允许某两台主机（IP地址为172.16.105.3和172.16.105.4）Telnet登录设备，其他用户均允许Telnet登录。

  Telnet的ACL默认动作为**deny**，该例属于“deny少部分报文，permit大部分报文”的情况，所以需先配置**rule deny xxx**，再配置**rule permit**。

```
#
acl number 2000
 rule 5 deny source 172.16.105.3 0
 rule 10 deny source 172.16.105.4 0
 rule 15 permit
#
```

- 例5：在FTP中应用ACL，不允许用户在周六的00:00～8:00期间访问FTP服务器，允许用户在其他任意时间访问FTP服务器。

  FTP的ACL默认动作为**deny**，该例属于“deny少部分报文，permit大部分报文”的情况，所以需先配置**rule deny xxx**，再配置**rule permit xxxx**。

```
#
time-range t1 00:00 to 08:00 Sat
time-range t2 00:00 to 23:59 daily
#
acl number 2000
 rule 5 deny time-range t1
 rule 10 permit time-range t2
#
```

5.3 应用场景

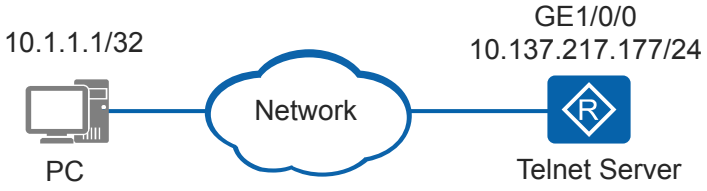
介绍ACL的应用场景。

5.3.1 使用 ACL 限制 Telnet 登录权限

ACL应用在Telnet模块中，可以使设备作为Telnet服务器时，对哪些Telnet客户端以Telnet方式登录到本设备能加以控制，从而有效防止未经授权用户的非法接入。

如图5-4所示，为简单而方便的配置和管理远程设备（Telnet Server），管理员在服务器端进行了配置，使Telnet用户必须使用AAA认证方式才能登录。同时，管理员配置了基于ACL的登录限制策略，保证只有管理员使用的PC才能登录该设备。

图 5-4 使用 ACL 限制 Telnet 登录权限

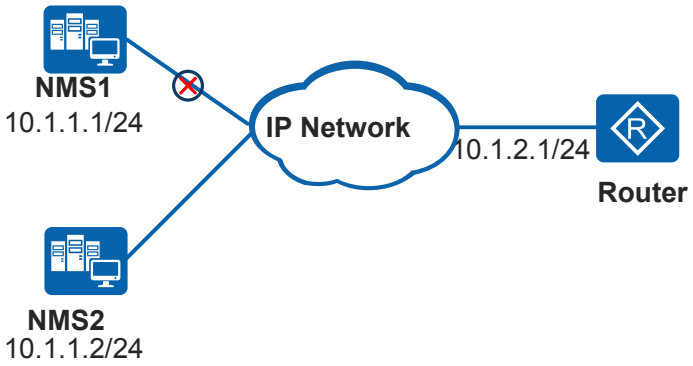


5.3.2 SNMP 中应用 ACL 过滤非法网管

ACL应用在SNMP模块中，可以使网管对设备的管理权限得到控制，从而有效防止非法网管操作设备。

如图5-5所示，为简单而方便的配置和管理远程设备（Router），管理员在Router上配置了SNMP Agent服务，Agent及时地向网管报告设备的当前状态信息，使网管可以远端控制设备。同时，管理员配置了基于ACL的网管访问权限限制，保证只有可信任的网管（NMS2）才能管理该设备。

图 5-5 SNMP 中应用 ACL 过滤非法网管

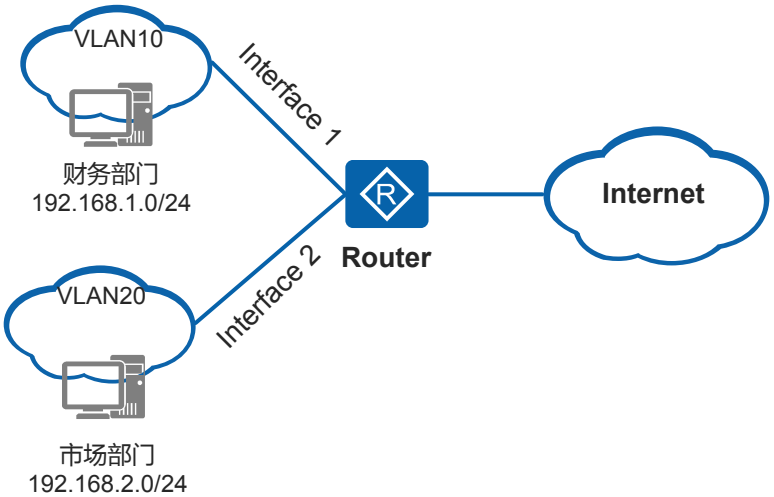


5.3.3 使用 ACL 限制不同网段用户的互访

ACL应用在QoS的流策略/简化流策略中，可以实现不同网段用户之间访问权限的限制，从而避免用户之间随意访问形成安全隐患。

如图5-6所示，某公司为财务部和市场部规划了两个网段的IP地址。为了避免两个部门之间相互访问造成公司机密的泄露，管理员在两个部门连接Router的接口（Interface1和Interface2）的入方向上应用绑定了ACL的流策略/简化流策略，禁止两个部门的互访。

图 5-6 使用 ACL 限制不同网段用户的互访

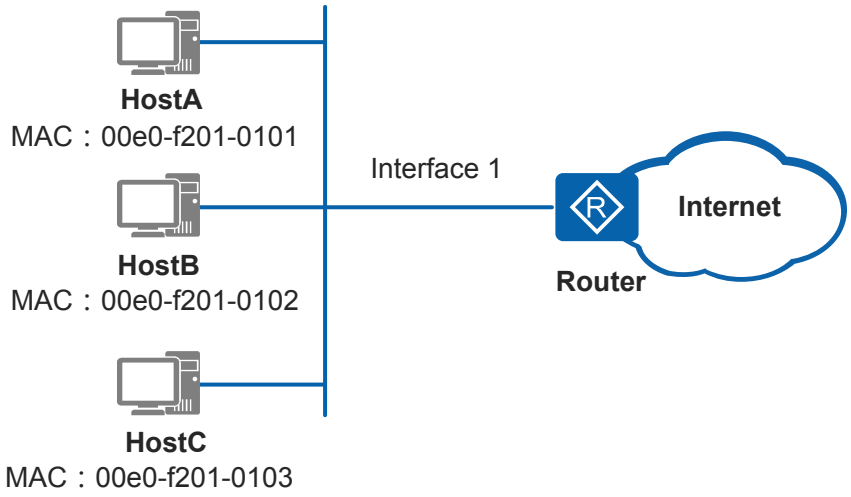


5.3.4 使用 ACL 禁止特定用户主机在特定时间内上网

ACL应用在QoS的流策略/简化流策略中，可以实现特定用户主机在特定时间范围内上网权限的限制。

如图5-7所示，某公司通过router连接到Internet。部分员工经常在上班时间访问与工作无关的网站，工作效率低下。所以，管理员配置了基于时间的ACL，并在这些用户连接router的接口（Interface 1）的入方向上应用绑定了ACL的流策略/简化流策略，禁止这些用户在工作时间内上网，其余时间均可以上网。

图 5-7 使用 ACL 禁止特定用户在特定时间内上网

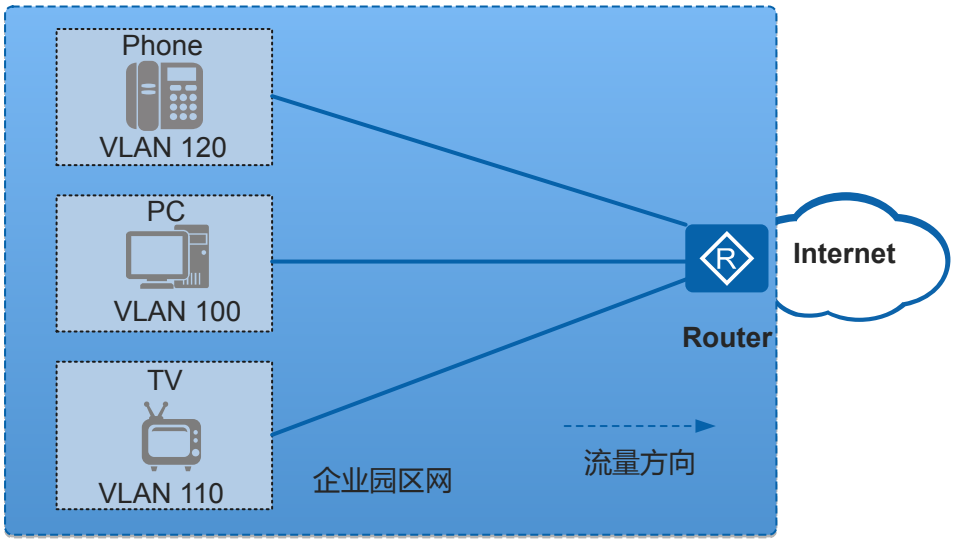


5.3.5 在 QoS 中使用 ACL 实施流量监管

ACL应用在QoS的流策略/简化流策略中，可以实现对不同流量进入网络的速率的监督，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，从而保护网络资源和用户的利益。

如图5-8所示，某公司的数据业务、视频业务、语音业务分别属于VLAN 100、VLAN 110、VLAN120。由于语音业务对服务质量的要求最高，视频业务次之，数据业务要求最低，所以管理员配置了基于ACL的流量监管功能，使设备可以对该公司不同的业务流按照VLAN ID进行分类，并对匹配ACL规则的报文进行限速，从而将不同业务的流量限制在一个合理的范围之内，保证各业务的带宽需求。

图 5-8 在 QoS 中使用 ACL 实施流量监管



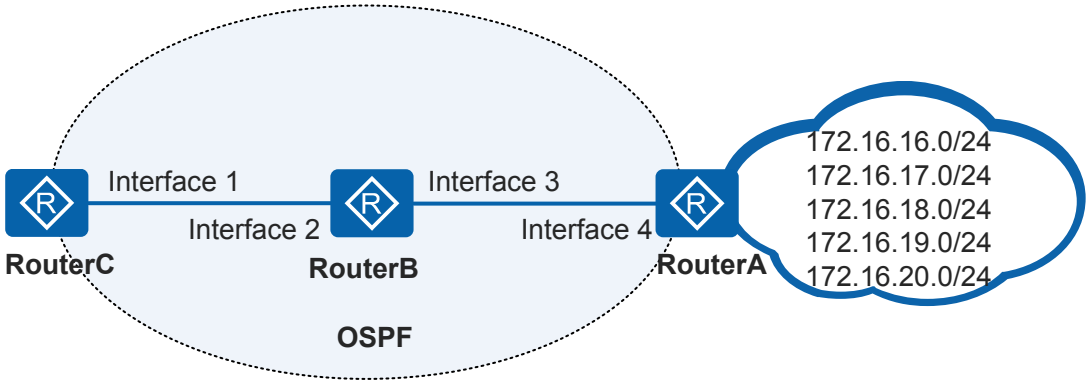
5.3.6 在 OSPF 中使用 ACL 过滤路由信息

ACL可以应用在各种动态路由协议中，对路由协议发布和接收的路由信息进行过滤。

如图5-9所示，在运行OSPF（Open Shortest Path First）协议的网络中，RouterA从Internet网络接收路由，并为OSPF网络提供了Internet路由。现要求OSPF网络中只能访问172.16.17.0/24、172.16.18.0/24和172.16.19.0/24三个网段的网络，其中RouterC连接的网络只能访问172.16.18.0/24网段的网络。

管理员可以在RouterA上配置ACL和路由策略，使其在路由发布时运用路由策略，仅提供路由172.16.17.0/24、172.16.18.0/24、172.16.19.0/24给RouterB，实现OSPF网络中只能访问172.16.17.0/24、172.16.18.0/24和172.16.19.0/24三个网段的网络；并且在RouterC上配置ACL和路由策略，使其在路由引入时运用路由策略，仅接收路由172.16.18.0/24，实现RouterC连接的网络只能访问172.16.18.0/24网段的网络。

图 5-9 在 OSPF 中使用 ACL 过滤路由信息



5.3.7 在 NAT 中使用 ACL 过滤流量

ACL可以应用在NAT过滤功能中，让NAT设备对外网发送到内网的流量进行过滤。

NAT过滤是指NAT设备对外网发到内网的流量进行过滤，包括三种类型：

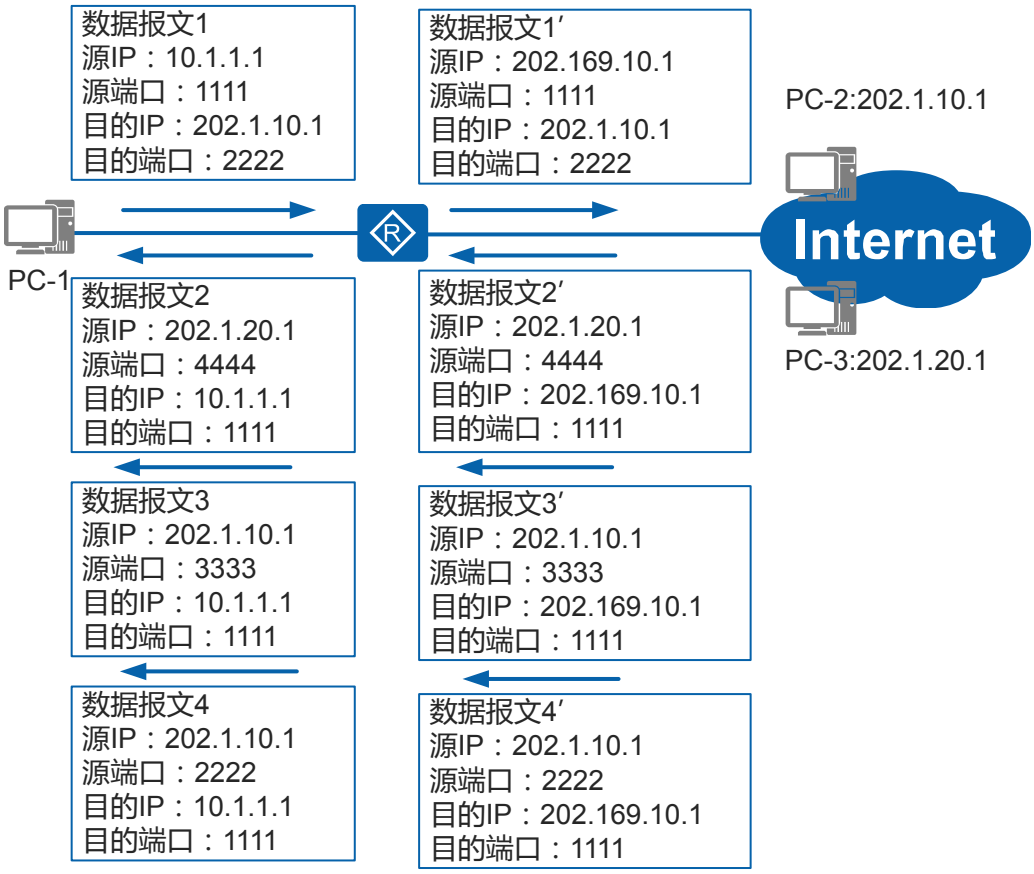
- 与外部地址无关的NAT过滤行为
- 与外部地址相关的NAT过滤行为
- 与外部地址和端口都相关的NAT过滤行为

如图5-10所示，私网用户PC-1通过NAT设备与外网用户PC-2、PC-3进行通信。数据报文1代表私网主机PC-1访问公网主机PC-2，PC-1使用的端口号为1111，访问PC-2的端口2222；经过NAT设备时，源IP转换为202.169.10.1。

当私网主机向某公网主机发起访问后，公网主机发向私网主机的流量经过NAT设备时需要进行过滤。数据报文2’、数据报文3’和数据报文4’代表三种场景，分别对应上述三种NAT过滤类型：

- 数据报文2’代表公网主机PC-3（与报文1的目的地址不同）访问私网主机PC-1，目的端口号为1111，只有配置了外部地址无关的NAT过滤行为，才允许此报文通过，否则被NAT设备过滤掉。
- 数据报文3’代表公网服务器PC-2（与报文1的目的地址相同）访问私网主机PC-1，目的端口号为1111，源端口号为3333（与报文1的目的端口不同），只有配置了外部地址相关的NAT过滤行为或者配置了外部地址无关的NAT过滤行为，才允许此报文通过，否则被NAT设备过滤掉。
- 数据报文4’代表公网服务器PC-2（与报文1的目的地址相同）访问私网主机PC-1，目的端口号为1111，源端口号为2222（与报文1的目的端口相同），这属于外部地址和端口都相关的NAT过滤行为，是缺省的过滤行为，不配置或者配置任何类型的NAT过滤行为，都允许此报文通过，不会被过滤掉。

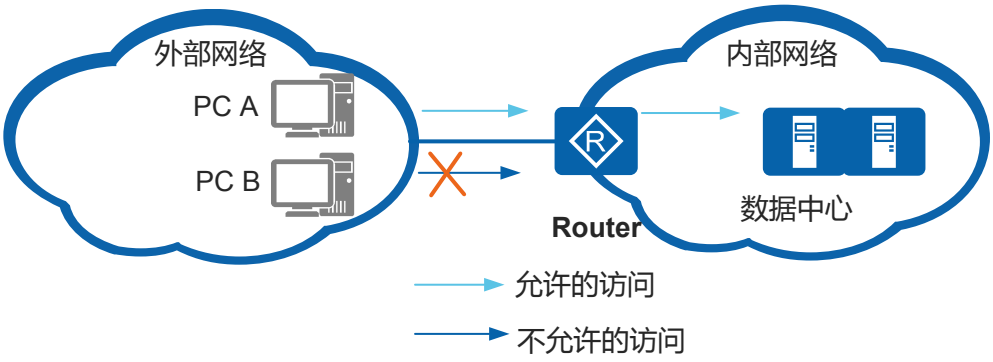
图 5-10 在 NAT 中使用 ACL 过滤流量



5.3.8 在防火墙中使用 ACL

防火墙用在内外网络边缘处，防止外部网络对内部网络的入侵，也可以用来保护网络内部大型机和重要的资源（如数据）。

图 5-11 在防火墙中使用 ACL



如图5-11所示，只允许外部特定主机PC A访问内部网络中的数据中心，别的访问都不允许。在Router上部署防火墙并配置ACL，就可以达到这个要求。

5.4 配置注意事项

介绍配置ACL的注意事项。

4GE-2S、4ES2G-S、4ES2GP-S和9ES2单板不支持ACL。

5.5 配置任务概览

设备支持的ACL主要包括：基本ACL、高级ACL、二层ACL、用户ACL、基本ACL6和高级ACL6。

ACL的配置任务如表5-13所示。各配置任务之间，是并列关系，至少要选择其中的一种ACL进行配置。

表 5-13 ACL 配置任务概览

场景	描述	对应任务
配置并应用基本ACL	基本ACL根据源IP地址、分片信息和生效时间段等信息来定义规则，对IPv4报文进行过滤。 如果只需要根据源IP地址对报文进行过滤，可以配置基本ACL。	5.7.1 配置并应用基本ACL
配置并应用高级ACL	高级ACL根据源IP地址、目的IP地址、IP协议类型、TCP源/目的端口、UDP源/目的端口号、分片信息和生效时间段等信息来定义规则，对IPv4报文进行过滤。 高级ACL比基本ACL提供了更准确、丰富、灵活的规则定义方法。例如，当希望同时根据源IP地址和目的IP地址对报文进行过滤时，则需要配置高级ACL。	5.7.2 配置并应用高级ACL

场景	描述	对应任务
配置并应用二层ACL	二层ACL根据以太网帧头信息来定义规则，如源MAC（Media Access Control）地址、目的MAC地址、VLAN、二层协议类型等，对IPv4和IPv6报文进行过滤。 如果只需要根据二层信息过滤报文，可以配置二层ACL。	**5.7.3 配置并应用二层ACL**
配置并应用用户ACL	用户ACL根据IPv4报文的源IP地址、目的IP地址、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、生效时间段等来定义规则，对IPv4报文进行过滤。 如果需要配置Portal用户的免认证规则，可以配置用户ACL。	**5.7.4 配置并应用用户ACL**
配置并应用基本ACL6	基本ACL6根据源IPv6地址、分片信息和生效时间段等信息来定义规则，对IPv6报文进行过滤。 如果只需要根据源IPv6地址对报文进行过滤，可以配置基本ACL6。	**5.7.5 配置并应用基本ACL6**
配置并应用高级ACL6	高级ACL6根据源IPv6地址、目的IPv6地址、IPv6协议类型、TCP源/目的端口号、UDP源/目的端口号、分片信息和生效时间段等信息来定义规则，对IPv6报文进行过滤。 高级ACL6比基本ACL6提供了更准确、丰富、灵活的规则定义方法。例如，当希望同时根据源IPv6地址和目的IPv6地址对报文进行过滤时，则需要配置高级ACL6。	**5.7.6 配置并应用高级ACL6**

5.6 缺省配置

介绍ACL缺省配置，实际应用的配置可以基于缺省配置进行修改。

ACL的缺省配置如表5-14所示。

表 5-14 ACL 缺省配置

参数	缺省值
规则步长	5
匹配顺序	配置顺序

5.7 配置 ACL

介绍ACL详细的配置过程。

5.7.1 配置并应用基本 ACL

5.7.1.1 （可选）配置 ACL 的生效时间段

背景信息

缺省情况下，ACL一旦被应用到业务模块后是一直生效的。通过定义生效时间段，并将时间段与ACL规则关联，可以使ACL规则在某段时间范围内生效，从而达到使用基于时间的ACL来控制业务的目的。例如，在上班时间禁止员工访问互联网网站，避免影响工作；在网络流量高峰期，限制P2P/下载类业务的带宽，避免网络拥塞等。

在ACL规则中引用的生效时间段存在两种模式：

- 第一种模式——周期时间段：以星期为参数来定义时间范围，表示规则以一周为周期（如每周一的8点至12点）循环生效。
- 第二种模式——绝对时间段：从某年某月某日的某一时间开始，到某年某月某日的某一时间结束，表示规则在这段时间范围内生效。

说明

为避免设备的系统时间与网络不同步造成ACL不生效，建议配置NTP（Network Time Protocol），实现系统时钟的自动同步，保证设备与网络中所有设备时钟的一致性。NTP的配置，请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-设备管理》中的“配置NTP基本功能”。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**time-range** *time-name* { *start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1 date1* [**to** *time2 date2*] }，创建一个时间段。

缺省情况下，设备没有配置时间段。

可以使用同一名称（*time-name*）配置内容不同的多条时间段，配置的各周期时间段之间以及各绝对时间段之间的交集将成为最终生效的时间范围。

如果要删除时间段，可参见**删除生效时间段**。

----结束

后续处理

创建生效时间段后，还需创建ACL并配置与生效时间段关联的ACL规则。基本ACL的配置，请参见**5.7.1.2 配置基本ACL**。

配置小窍门

删除生效时间段

删除生效时间段前，需要先删除关联生效时间段的ACL规则或者整个ACL。

例如，在ACL 2001中配置了rule 5，该规则关联了时间段time1。

```
#
time-range time1 from 00:00 2014/1/1 to 23:59 2014/12/31
#
acl number 2001
 rule 5 permit time-range time1
#
```

如果需要删除时间段time1，则需先删除rule 5或者先删除ACL 2001。

- 先删除rule 5，再删除time1。

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] undo rule 5
[Huawei-acl-basic-2001] quit
[Huawei] undo time-range time1
```

- 先删除ACL 2001，再删除time1。

```
<Huawei> system-view
[Huawei] undo acl 2001
[Huawei] undo time-range time1
```

相关资料

视频：**配置基于时间的ACL**

5.7.1.2 配置基本 ACL

前提条件

如果配置基于时间的ACL，则需创建生效时间段，并将其与ACL规则关联起来。具体操作请参见**5.7.1.1 （可选）配置ACL的生效时间段**。

背景信息

基本ACL根据源IP地址、分片信息和生效时间段等信息来定义规则，对IPv4报文进行过滤。

如果只需要根据源IP地址对报文进行过滤，可以配置基本ACL。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建基本ACL。可使用编号或者名称两种方式创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **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。
- 执行命令**acl name** *acl-name* { **basic** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的基本ACL，并进入基本ACL视图。

缺省情况下，未创建ACL。

关于数字型ACL和命名型ACL的详细介绍，请参见**5.2.2 ACL的分类**。

如果创建ACL时未指定**match-order**参数，则该ACL默认的规则匹配顺序为**config**。关于ACL匹配顺序的详细介绍，请参见**5.2.4 ACL的匹配顺序**。

创建ACL后，ACL的缺省步长为5。如果该值不能满足管理员部署ACL规则的需求，则可以对ACL步长值进行调整。关于步长的详细介绍，请参见**5.2.3 ACL的步长设定**；关于步长调整的具体操作，请参见**5.8.1 调整ACL规则的步长**。

如果要删除已生效的ACL，可参见**删除ACL**。

步骤3 （可选）执行命令**description** *text*，配置ACL的描述信息。

缺省情况下，未配置ACL的描述信息。

配置ACL时，为ACL添加描述信息可以方便理解和记忆该ACL的功能或具体用途。

步骤4 执行命令**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **vpn-instance** *vpn-instance-name* | [**fragment** | **none-first-fragment**] | **logging** | **time-range** *time-name*] *，配置基本ACL的规则。

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

关于生效时间段、源IP地址及其通配符掩码和IP分片信息的详细介绍，请参见**5.2.5 ACL的常用匹配项**。详细的规则配置示例，请参见**配置基本ACL规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

配置小窍门

删除ACL

系统视图下执行命令**undo acl** { [**number**] *acl-number* | **all** }或**undo acl name** *acl-name*，可以直接删除ACL，不受引用ACL的业务模块影响（简化流策略中引用ACL指定rule的情况除外），即无需先删除引用ACL的业务配置。

配置基本ACL规则

- **配置基于源IP地址（主机地址）过滤报文的规则**

  在ACL 2001中配置规则，允许源IP地址是192.168.1.3主机地址的报文通过。

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule permit source 192.168.1.3 0
```

- **配置基于源IP地址（网段地址）过滤报文的规则**

  在ACL 2001中配置规则，仅允许源IP地址是192.168.1.3主机地址的报文通过，拒绝源IP地址是192.168.1.0/24网段其他地址的报文通过，并配置ACL描述信息为Permit only 192.168.1.3 through。

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule permit source 192.168.1.3 0
[Huawei-acl-basic-2001] rule deny source 192.168.1.0 0.0.0.255
[Huawei-acl-basic-2001] description Permit only 192.168.1.3 through
```

- **配置基于时间的ACL规则**

  创建时间段working-time（周一到周五每天8:00到18:00），并在名称为work-acl的ACL中配置规则，在working-time限定的时间范围内，拒绝源IP地址是192.168.1.0/24网段地址的报文通过。

```
<Huawei> system-view
[Huawei] time-range working-time 8:00 to 18:00 working-day
[Huawei] acl name work-acl basic
[Huawei-acl-basic-work-acl] rule deny source 192.168.1.0 0.0.0.255 time-range working-time
```

- **配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**

  在ACL 2001中配置规则，拒绝源IP地址是192.168.1.0/24网段地址的非首片分片报文通过。

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule deny source 192.168.1.0 0.0.0.255 none-first-fragment
```

5.7.1.3 应用基本 ACL

背景信息

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。

最基本的ACL应用方式，是在简化流策略/流策略中应用ACL，使设备能够基于全局、VLAN或接口下发ACL，实现对转发报文的过滤。此外，ACL还可以应用在Telnet、FTP、路由等模块。

操作步骤

步骤1 应用基本ACL。

基本ACL的常见应用方式，如表5-15所示。

表 5-15 应用基本 ACL

业务分类	应用场景	各业务模块的ACL应用方式
对转发的报文进行过滤	基于全局、接口和VLAN，对转发的报文进行过滤，从而使设备能够进一步对过滤出的报文进行丢弃、修改优先级、重定向等处理。 例如，可以利用ACL，降低P2P下载、网络视频等消耗大量带宽的数据流的服务等级，在网络拥塞时优先丢弃这类流量，减少它们对其他重要流量的影响。	● 简化流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“基于ACL的简化流策略配置” ● 流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“MQC配置” ● 包过滤防火墙：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-防火墙配置》中的“**6.6 配置包过滤防火墙**” ● 动态NAT：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置动态地址转换” ● NAT Server：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置内部服务器”

业务分类	应用场景	各业务模块的ACL应用方式
对上送CPU处理的报文进行过滤	对上送CPU的报文进行必要的限制，可以避免CPU处理过多的协议报文造成占用率过高、性能下降。 例如，当发现某用户向设备发送大量的ARP攻击报文，造成设备CPU繁忙，引发系统中断时，可以在本机防攻击策略的黑名单中应用ACL，将该用户加入黑名单，使CPU丢弃该用户发送的报文。	黑名单：请参见“本机防攻击配置”中的“**8.3.2 配置黑名单**”

业务分类	应用场景	各业务模块的ACL应用方式
登录控制	对设备的登录权限进行控制，允许合法用户登录，拒绝非法用户登录，从而有效防止未经授权用户的非法接入，保证网络安全性。	● Telnet：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“配置Telnet服务器功能” ● FTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“通过FTP进行文件操作” ● SFTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“通过SFTP进行文件操作” ● TFTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的”配置设备作为TFTP客户端访问其他设备的文件“ ● Web登录：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“（可选）配置Web网管参数” ● SNMP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-网络管理与监控》中的“（可选）限制网管对设备的管理权限”（SNMPv1、SNMPv2c）和“（可选）限制网管对设备的管理权限”（SNMPv3）

业务分类	应用场景	各业务模块的ACL应用方式
路由过滤	ACL可以应用在各种动态路由协议中，对路由协议发布、接收的路由信息以及组播组进行过滤。 例如，可以将ACL和路由策略配合使用，禁止设备将某网段路由发给邻居路由器。	● BGP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“控制BGP路由信息的发布”和“控制BGP路由信息的接收” ● IS-IS（IPv4）：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“配置IS-IS发布部分外部路由到IS-IS路由域”和“配置将部分IS-IS路由下发到IP路由表” ● OSPF：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“配置OSPF对接收的路由进行过滤”、“配置OSPF对发布的路由进行过滤”和“（可选）配置Helper端GR的会话参数” ● RIP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“配置RIP引入外部路由信息”和“配置RIP对接收的路由进行过滤” ● 组播：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP组播》中的“配置根据源地址过滤IGMP报文”、“配置组播组过滤策略”、“（可选）配置接口加入的组播组范围”和“（可选）配置SSM组策略”

----结束

5.7.1.4 检查配置结果

操作步骤

- 执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }，查看ACL的配置信息。
- 执行命令**display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

5.7.2 配置并应用高级 ACL

5.7.2.1 （可选）配置 ACL 的生效时间段

背景信息

请参见“配置并应用基本ACL”中的**5.7.1.1 （可选）配置ACL的生效时间段**。

5.7.2.2 （可选）配置端口集

背景信息

配置TCP或UDP协议类型的高级ACL规则时，可以通过绑定端口集指定高级ACL规则匹配报文的源/目的端口号。在高级ACL规则匹配报文的源/目的端口号配置比较复杂，或多个ACL规则中需要定义相同的端口规则时，与在**rule（高级ACL视图）**命令中通过参数**eq** *port*、**gt** *port*、**lt** *port*或**range** *port-start port-end*直接指定端口号相比，在**rule（高级ACL视图）**命令中通过参数**port-set** *port-set-name*绑定端口集的配置方式更方便用户对高级ACL规则进行配置和维护。

说明

仅V200R008C50及更高版本支持该配置。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 执行命令**ip port-set** *port-set-name* **protocol** { **tcp** | **udp** }，创建端口集并进入端口集视图。

缺省情况下，设备没有创建端口集。

步骤3 执行命令**port** [*port-rule-id*] { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }，配置端口集的端口规则。

缺省情况下，设备没有配置端口集的端口规则。

----结束

后续处理

配置端口集后，还需创建高级ACL并配置与端口集关联的ACL规则。高级ACL的配置，请参见**5.7.2.3 配置高级ACL**。

5.7.2.3 配置高级 ACL

前提条件

- 如果配置基于时间的ACL，则需创建生效时间段，并将其与ACL规则关联起来。具体操作请参见**5.7.1.1 （可选）配置ACL的生效时间段**。
- 如果配置关联端口集的高级ACL，则需创建端口集，并配置端口集的端口规则。具体操作请参见**5.7.2.2 （可选）配置端口集**。

背景信息

高级ACL根据源IP地址、目的IP地址、IP协议类型、TCP源/目的端口、UDP源/目的端口号、分片信息和生效时间段等信息来定义规则，对IPv4报文进行过滤。

高级ACL比基本ACL提供了更准确、丰富、灵活的规则定义方法。例如，当希望同时根据源IP地址和目的IP地址对报文进行过滤时，则需要配置高级ACL。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建高级ACL。可使用编号或者名称两种方式创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **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。
- 执行命令**acl name** *acl-name* { **advance** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的高级ACL，进入高级ACL视图。

缺省情况下，未创建ACL。

关于数字型ACL和命名型ACL的详细介绍，请参见**5.2.2 ACL的分类**。

如果创建ACL时未指定**match-order**参数，则该ACL默认的规则匹配顺序为**config**。关于ACL匹配顺序的详细介绍，请参见**5.2.4 ACL的匹配顺序**。

创建ACL后，ACL的缺省步长为5。如果该值不能满足管理员部署ACL规则的需求，则可以对ACL步长值进行调整。关于步长的详细介绍，请参见**5.2.3 ACL的步长设定**；关于步长调整的具体操作，请参见**5.8.1 调整ACL规则的步长**。

如果要删除已生效的ACL，可参见“配置基本ACL”中的**删除ACL**，此处不再赘述。

步骤3 （可选）执行命令**description** *text*，配置ACL的描述信息。

缺省情况下，未配置ACL的描述信息。

配置ACL时，为ACL添加描述信息可以方便理解和记忆该ACL的功能或具体用途。

步骤4 配置高级ACL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IP承载的协议类型为ICMP时，高级访问控制列表的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- 当IP承载的协议类型为TCP时，高级访问控制列表的命令格式为：

  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* | **port-set** *port-set-name* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** | **established** } * | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- 当IP承载的协议类型为UDP时，高级访问控制列表的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- 当IP承载的协议类型为GRE、IGMP、IPINIP、OSPF时，高级访问控制列表的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

说明

如果要同时配置**precedence** *precedence*和**tos** *tos*参数，则需将**precedence** *precedence*和**tos** *tos*参数连续配置。

参数**dscp** *dscp*和**precedence** *precedence*不能同时配置。

参数**dscp** *dscp*和**tos** *tos*不能同时配置。

仅在VXLAN场景下配置参数**vni** *vni-id*才有效。

在ACL中配置首条规则时，如果未指定参数*rule-id*，设备使用步长值作为规则的起始编号。后续配置规则如仍未指定参数*rule-id*，设备则使用最后一个规则的*rule-id*的下一个步长的整数倍数值作为规则编号。例如ACL中包含规则rule 5和rule 7，ACL的步长为5，则系统分配给新配置的未指定*rule-id*的规则的编号为10。

当用户指定参数**time-range**引入ACL规则生效时间段时，如果*time-name*不存在，则该规则配置不生效。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

配置小窍门

配置高级ACL规则

- **配置基于ICMP协议类型、源IP地址（主机地址）和目的IP地址（网段地址）过滤报文的规则**

  在ACL3001中配置规则，允许源IP地址是192.168.1.3主机地址且目的IP地址是192.168.2.0/24网段地址的ICMP报文通过。

```
<Huawei> system-view
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule permit icmp source 192.168.1.3 0 destination 192.168.2.0 0.0.0.255
```

- **配置基于TCP协议类型、TCP目的端口号、源IP地址（主机地址）和目的IP地址（网段地址）过滤报文的规则**

  在名称为deny-telnet的高级ACL中配置规则，拒绝IP地址是192.168.1.3的主机与192.168.2.0/24网段的主机建立Telnet连接。

```
<Huawei> system-view
[Huawei] acl name deny-telnet
[Huawei-acl-adv-deny-telnet] rule deny tcp destination-port eq telnet source 192.168.1.3 0
destination 192.168.2.0 0.0.0.255
```

  在名称为no-web的高级ACL中配置规则，禁止192.168.1.3和192.168.1.4两台主机访问Web网页（HTTP协议用于网页浏览，对应TCP端口号是80），并配置ACL描述信息为Web access restrictions。

```
<Huawei> system-view
[Huawei] acl name no-web
[Huawei-acl-adv-no-web] description Web access restrictions
[Huawei-acl-adv-no-web] rule deny tcp destination-port eq 80 source 192.168.1.3 0
[Huawei-acl-adv-no-web] rule deny tcp destination-port eq 80 source 192.168.1.4 0
```

- **配置基于TCP协议类型、源IP地址（网段地址）和TCP标志信息过滤报文的规则**

  在ACL3002中配置规则，拒绝192.168.2.0/24网段的主机主动发起的TCP握手报文通过，允许该网段主机被动响应TCP握手的报文通过，实现192.168.2.0/24网段地址的单向访问控制。同时，配置ACL规则描述信息分别为Allow the ACK TCP packets through、Allow the RST TCP packets through和Do not Allow the other TCP packet through。

  完成以上配置，必须先配置两条permit规则，允许192.168.2.0/24网段的ACK=1或RST=1的报文通过，再配置一条deny规则，拒绝该网段的其他TCP报文通过。

```
<Huawei> system-view
[Huawei] acl 3002
[Huawei-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack
[Huawei-acl-adv-3002] display this   //如果配置规则时未指定规则编号，则可以通过此步骤查看到系统为该规则分配的编号，然后根据该编号，为该规则配置描述信息。
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack           //系统分配的规则编号是5
#
return
[Huawei-acl-adv-3002] rule 5 description Allow the ACK TCP packets through
[Huawei-acl-adv-3002] rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst
[Huawei-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack syn
 rule 5 description Allow the ACK TCP packets through
 rule 10 deny tcp source 192.168.2.0 0.0.0.255 tcp-flag rst       //系统分配的规则编号是10
```

```
#
return
[Huawei-acl-adv-3002] rule 10 description Allow the RST TCP packets through
[Huawei-acl-adv-3002] rule deny tcp source 192.168.2.0 0.0.0.255
[Huawei-acl-adv-3002] display this
#
acl number 3002
 rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack syn
 rule 5 description Allow the ACK TCP packets through
 rule 10 deny tcp source 192.168.2.0 0.0.0.255 tcp-flag rst
 rule 10 description Allow the RST TCP packets through
 rule 15 deny tcp source 192.168.2.0 0.0.0.255       //系统分配的规则编号是15
#
return
[Huawei-acl-adv-3002] rule 15 description Do not Allow the other TCP packet through
```

- **配置基于时间的ACL规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

- **配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**

  请参见“配置基本ACL”中的**配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**，不再赘述。

5.7.2.4 应用高级 ACL

背景信息

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。

最基本的ACL应用方式，是在简化流策略/流策略中应用ACL，使设备能够基于全局、VLAN或接口下发ACL，实现对转发报文的过滤。此外，ACL还可以应用在FTP、组播等模块。

操作步骤

步骤1 应用高级ACL。

高级ACL的常见应用方式，如**表5-16**所示。

表 5-16 应用高级 ACL

业务分类	应用场景	各业务模块的ACL应用方式
对转发的报文进行过滤	基于全局、接口和VLAN，对转发的报文进行过滤，从而使设备能够进一步对过滤出的报文进行丢弃、修改优先级、重定向等处理。 例如，可以利用ACL，降低P2P下载、网络视频等消耗大量带宽的数据流的服务等级，在网络拥塞时优先丢弃这类流量，减少它们对其他重要流量的影响。	● 简化流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“基于ACL的简化流策略配置” ● 流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“MQC配置” ● 包过滤防火墙：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-防火墙配置》中的“**6.6 配置包过滤防火墙**” ● 动态NAT：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置动态地址转换” ● NAT Server：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置内部服务器”

业务分类	应用场景	各业务模块的ACL应用方式
对上送CPU处理的报文进行过滤	对上送CPU的报文进行必要的限制，可以避免CPU处理过多的协议报文造成占用率过高、性能下降。 例如，当发现某用户向设备发送大量的ARP攻击报文，造成设备CPU繁忙，引发系统中断时，可以在本机防攻击策略的黑名单中应用ACL，将该用户加入黑名单，使CPU丢弃该用户发送的报文。	黑名单：请参见“本机防攻击配置”中的“**8.3.2 配置黑名单**”
登录控制	对设备的登录权限进行控制，允许合法用户登录，拒绝非法用户登录，从而有效防止未经授权用户的非法接入，保证网络安全性。	● Telnet：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“配置Telnet服务器功能” ● FTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“通过FTP进行文件操作” ● SFTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“通过SFTP进行文件操作”
路由过滤	ACL可以应用在组播协议中，实现组播组的过滤。 例如，可以将ACL和IGMP Snooping配合使用，禁止VLAN内的主机加入指定组播组。	组播：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP组播》中的“配置组播组过滤策略”、“配置根据源地址过滤IGMP报文”和“（可选）配置接口加入的组播组范围”

----结束

5.7.2.5 检查配置结果

操作步骤

- 执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }，查看ACL的配置信息。
- 执行命令**display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

5.7.3 配置并应用二层 ACL

5.7.3.1 （可选）配置 ACL 的生效时间段

背景信息

请参见“配置并应用基本ACL”中的**5.7.1.1 （可选）配置ACL的生效时间段**。

5.7.3.2 配置二层 ACL

前提条件

如果配置基于时间的ACL，则需创建生效时间段，并将其与ACL规则关联起来。具体操作请参见**5.7.1.1 （可选）配置ACL的生效时间段**。

背景信息

二层ACL根据以太网帧头信息来定义规则，如源MAC（Media Access Control）地址、目的MAC地址、VLAN、二层协议类型等，对IPv4和IPv6报文进行过滤。

如果只需要根据二层信息过滤报文，可以配置二层ACL。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建二层ACL。可使用编号或者名称两种方式创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号（4000～4999）创建一个数字型的二层ACL，并进入二层ACL视图。
- 执行命令**acl name** *acl-name* { **link** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的二层ACL，进入二层ACL视图。

缺省情况下，未创建ACL。

关于数字型ACL和命名型ACL的详细介绍，请参见**5.2.2 ACL的分类**。

如果创建ACL时未指定**match-order**参数，则该ACL默认的规则匹配顺序为**config**。关于ACL匹配顺序的详细介绍，请参见**5.2.4 ACL的匹配顺序**。

创建ACL后，ACL的缺省步长为5。如果该值不能满足管理员部署ACL规则的需求，则可以对ACL步长值进行调整。关于步长的详细介绍，请参见**5.2.3 ACL的步长设定**；关于步长调整的具体操作，请参见**5.8.1 调整ACL规则的步长**。

如果要删除已生效的ACL，可参见“配置基本ACL”中的**删除ACL**，此处不再赘述。

步骤3 （可选）执行命令**description** *text*，配置ACL的描述信息。

缺省情况下，未配置ACL的描述信息。

配置ACL时，为ACL添加描述信息可以方便理解和记忆该ACL的功能或具体用途。

步骤4 执行命令**rule** [*rule-id*] { **permit** | **deny** } [**l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | **time-range** *time-name*] *，配置二层ACL的规则。

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

关于生效时间段、源/目的MAC地址及其通配符掩码、VLAN编号及其掩码的详细介绍，请参见**5.2.5 ACL的常用匹配项**。详细的规则配置示例，请参见**配置二层ACL规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

配置小窍门

配置二层ACL规则

- **配置基于源MAC地址（单个MAC地址）、目的MAC地址（单个MAC地址）和二层协议类型过滤报文的规则**

  在ACL 4001中配置规则，允许目的MAC地址是0000-0000-0001、源MAC地址是0000-0000-0002的ARP报文（二层协议类型值为0x0806）通过。

  ```
  <Huawei> system-view
  [Huawei] acl 4001
  [Huawei-acl-L2-4001] rule permit destination-mac 0000-0000-0001 source-mac 0000-0000-0002 l2-protocol 0x0806
  ```

  在ACL 4001中配置规则，拒绝PPPoE报文（二层协议类型值为0x8863）通过。

  ```
  <Huawei> system-view
  [Huawei] acl 4001
  [Huawei-acl-L2-4001] rule deny l2-protocol 0x8863
  ```

- **配置基于源MAC地址（MAC地址段）和内层VLAN过滤报文的规则**

  在名称为deny-vlan10-mac的二层ACL中配置规则，拒绝来自VLAN10且源MAC地址在00e0-fc01-0000～00e0-fc01-ffff范围内的报文通过。

  ```
  <Huawei> system-view
  [Huawei] acl name deny-vlan10-mac link
  [Huawei-acl-L2-deny-vlan10-mac] rule deny vlan-id 10 source-mac 00e0-fc01-0000 ffff-ffff-0000
  ```

- **配置基于时间的ACL规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

5.7.3.3 应用二层 ACL

背景信息

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。

最基本的ACL应用方式，是在简化流策略/流策略中应用ACL，使设备能够基于全局、VLAN或接口下发ACL，实现对转发报文的过滤。此外，ACL还可以应用在本机防攻击等模块。

操作步骤

步骤1 应用二层ACL。

二层ACL的常见应用方式，如**表5-17**所示。

表 5-17 应用二层 ACL

业务分类	应用场景	各业务模块的ACL应用方式
对转发的报文进行过滤	基于全局、接口和VLAN，对转发的报文进行过滤，从而使设备能够进一步对过滤出的报文进行丢弃、修改优先级、重定向等处理。 例如，可以利用ACL，降低P2P下载、网络视频等消耗大量带宽的数据流的服务等级，在网络拥塞时优先丢弃这类流量，减少它们对其他重要流量的影响。	● 简化流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“基于ACL的简化流策略配置” ● 流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“MQC配置” ● 包过滤防火墙：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-防火墙配置》中的“**6.6 配置包过滤防火墙**” ● 动态NAT：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置动态地址转换” ● NAT Server：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置内部服务器”

业务分类	应用场景	各业务模块的ACL应用方式
对上送CPU处理的报文进行过滤	对上送CPU的报文进行必要的限制，可以避免CPU处理过多的协议报文造成占用率过高、性能下降。 例如，当发现某用户向设备发送大量的ARP攻击报文，造成设备CPU繁忙，引发系统中断时，可以在本机防攻击策略的黑名单中应用ACL，将该用户加入黑名单，使CPU丢弃该用户发送的报文。	黑名单：请参见“本机防攻击配置”中的“8.3.2 配置黑名单”

----结束

5.7.3.4 检查配置结果

操作步骤

- 执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }，查看ACL的配置信息。
- 执行命令**display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

5.7.4 配置并应用用户 ACL

5.7.4.1 （可选）配置 ACL 的生效时间段

背景信息

请参见“配置并应用基本ACL”中的**5.7.1.1 （可选）配置ACL的生效时间段**。

5.7.4.2 配置用户 ACL

背景信息

用户ACL根据IPv4报文的源IP地址、目的IP地址、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、生效时间段等来定义规则，对IPv4报文进行过滤。

如果需要配置Portal用户的免认证规则，可以配置用户ACL。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建用户ACL。仅支持使用编号创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号（6000～6031）创建一个数字型的用户ACL，并进入用户ACL视图。

缺省情况下，未创建ACL。

关于数字型ACL和命名型ACL的详细介绍，请参见**5.2.2 ACL的分类**。

如果创建ACL时未指定**match-order**参数，则该ACL默认的规则匹配顺序为**config**。关于ACL匹配顺序的详细介绍，请参见**5.2.4 ACL的匹配顺序**。

创建ACL后，ACL的缺省步长为5。如果该值不能满足管理员部署ACL规则的需求，则可以对ACL步长值进行调整。关于步长的详细介绍，请参见**5.2.3 ACL的步长设定**；关于步长调整的具体操作，请参见**5.8.1 调整ACL规则的步长**。

如果要删除已生效的ACL，可参见“配置基本ACL”中的**删除ACL**，此处不再赘述。

步骤3 （可选）执行命令**description** *text*，配置ACL的描述信息。

缺省情况下，未配置ACL的描述信息。

配置ACL时，为ACL添加描述信息可以方便理解和记忆该ACL的功能或具体用途。

步骤4 配置用户ACL规则。

根据IP承载的协议类型不同，在设备上配置不同的用户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ICMP时，用户访问控制列表的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- 当参数protocol为TCP时，用户访问控制列表的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **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** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- 当参数protocol为UDP时，用户访问控制列表的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **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* } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- 当参数protocol为GRE、IGMP、IP、IPINIP、OSPF时，用户访问控制列表的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

详细的规则配置示例，请参见**配置用户ACL规则**。

步骤5 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

配置小窍门

配置用户ACL规则

- **配置基于目的IP地址过滤报文的规则**

  在ACL 6000中配置规则，允许所有Portal用户可以免认证访问IP地址为10.1.1.1/24的网络。

```
<Huawei> system-view
[Huawei] acl 6000
[Huawei-acl-ucl-6000] rule permit ip destination 10.1.1.1 255.255.255.0
```

- **配置基于时间的ACL规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

5.7.4.3 应用用户 ACL

背景信息

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。

目前用户ACL仅支持在NAC特性的Portal认证中应用。通过配置Portal认证，并配置用户ACL关联Portal认证用户的免认证规则可使特定的用户不经过认证或认证失败的情况下能够访问特定的网络资源。

操作步骤

步骤1 应用用户ACL。

用户ACL的应用方式，如**表5-18**所示。

表 5-18 应用用户 ACL

业务分类	应用场景	各业务模块的ACL应用方式
对转发的报文进行过滤	将用户ACL与Portal认证用户的免认证规则绑定，可使特定的用户不经过认证或认证失败的情况下能够访问特定的网络资源。	NAC：请参见**3.7.3.5 （可选）配置免认证的授权信息**

----结束

5.7.4.4 检查配置结果

操作步骤

- 执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }，查看ACL的配置信息。
- 执行命令**display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

5.7.5 配置并应用基本 ACL6

背景信息

5.7.5.1 （可选）配置 ACL6 的生效时间段

背景信息

ACL6与ACL关联的生效时间段相同，配置方法请参见“配置并应用基本ACL”中的**5.7.1.1 （可选）配置ACL的生效时间段**。

5.7.5.2 配置基本 ACL6

前提条件

如果配置基于时间的ACL6，则需创建生效时间段，并将其与ACL6规则关联起来。具体操作请参见**5.7.5.1 （可选）配置ACL6的生效时间段**。

背景信息

基本ACL6根据源IPv6地址、分片信息和生效时间段等信息来定义规则，对IPv6报文进行过滤。

如果只需要根据源IPv6地址对报文进行过滤，可以配置基本ACL6。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建基本ACL6。可使用编号或者名称两种方式创建。

- 执行命令**acl ipv6** [**number**] *acl6-number* [**match-order** { **auto** | **config** }]，使用编号（2000～2999）创建一个数字型的基本ACL6，并进入基本ACL6视图。
- 执行命令**acl ipv6 name** *acl6-name* { **basic** | *acl6-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的基本ACL6，并进入基本ACL6视图。

缺省情况下，未创建ACL6。

数字型ACL6和命名型ACL6的原理同数字型ACL和命名型ACL，详细介绍请参见**5.2.2 ACL的分类**。

如果创建ACL6时未指定**match-order**参数，则该ACL6默认的规则匹配顺序为**config**。ACL6的规则匹配顺序同ACL匹配顺序，详细介绍请参见**5.2.4 ACL的匹配顺序**。

如果要删除已生效的ACL6，可参见**删除ACL6**。

步骤3 执行命令**rule** [*rule-id*] { **deny** | **permit** } [[**fragment** | **none-first-fragment**] | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name*] *，配置基本ACL6规则。

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

详细的规则配置示例，请参见**配置基本ACL6规则**。

步骤4 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

配置小窍门

删除ACL6

系统视图下执行命令**undo acl ipv6** { **all** | [**number**] *acl6-number* }或**undo acl ipv6 name** *acl6-name*，可以直接删除ACL6，不受引用ACL6的业务模块影响（简化流策略中引用ACL6指定rule的情况除外），即无需先删除引用ACL6的业务配置。

配置基本ACL6规则

- **配置基于源IPv6地址（主机地址）过滤报文的规则**

  在ACL6 2001中配置规则，允许源IPv6地址是fc00:1::1/128主机地址的报文通过。

  ```
  <Huawei> system-view
  [Huawei] acl ipv6 2001
  [Huawei-acl6-basic-2001] rule permit source fc00:1::1 128
  ```

- **配置基于源IPv6地址（网段地址）过滤报文的规则**

  在ACL6 2001中配置规则，仅允许源IPv6地址是fc00:1::1/128主机地址的报文通过，拒绝源IPv6地址是fc00:1::/64网段其他地址的报文通过。

  ```
  <Huawei> system-view
  [Huawei] acl ipv6 2001
  [Huawei-acl6-basic-2001] rule permit source fc00:1::1 128
  [Huawei-acl6-basic-2001] rule deny source fc00:1:: 64
  ```

- **配置基于时间的ACL6规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

- **配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**

  请参见“配置基本ACL”中的**配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**，不再赘述。

5.7.5.3 应用基本 ACL6

背景信息

配置完ACL6后，必须在具体的业务模块中应用ACL6，才能使ACL6正常下发和生效。

最基本的ACL6应用方式，是在简化流策略/流策略中应用ACL6，使设备能够基于全局、VLAN或接口下发ACL6，实现对转发报文的过滤。此外，ACL6还可以应用在Telnet、FTP、路由等模块。

操作步骤

步骤1 应用基本ACL6。

基本ACL的常见应用方式，如**表5-19**所示。

表 5-19 应用基本 ACL6

业务分类	应用场景	各业务模块的ACL应用方式
对转发的报文进行过滤	基于全局、接口和VLAN，对转发的报文进行过滤，从而使设备能够进一步对过滤出的报文进行丢弃、修改优先级、重定向等处理。 例如，可以利用ACL6，降低P2P下载、网络视频等消耗大量带宽的数据流的服务等级，在网络拥塞时优先丢弃这类流量，减少它们对其他重要流量的影响。	● 简化流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“基于ACL的简化流策略配置” ● 流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“MQC配置” ● 包过滤防火墙：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-防火墙配置》中的“**6.6 配置包过滤防火墙**” ● 动态NAT：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置动态地址转换” ● NAT Server：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置内部服务器”

业务分类	应用场景	各业务模块的ACL应用方式
登录控制	对设备的登录权限进行控制，允许合法用户登录，拒绝非法用户登录，从而有效防止未经授权用户的非法接入，保证网络安全性。 例如，一般情况下设备只允许管理员登录，非管理员用户不允许随意登录。这时就可以在Telnet中应用ACL6，并在ACL6中定义哪些主机可以登录，哪些主机不能。	● Telnet：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“配置Telnet服务器功能” ● FTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“通过FTP进行文件操作” ● SFTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“通过SFTP进行文件操作” ● SNMP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-网络管理与监控》中的“（可选）限制网管对设备的管理权限”（SNMPv1、SNMPv2c）和“（可选）限制网管对设备的管理权限”（SNMPv3）

业务分类	应用场景	各业务模块的ACL应用方式
路由过滤	ACL可以应用在各种动态路由协议中，对路由协议发布、接收的路由信息以及组播组进行过滤。 例如，可以将ACL和路由策略配合使用，禁止设备将某网段路由发给邻居路由器。	● IS-IS（IPv6）：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“配置IS-IS发布部分外部路由到IS-IS路由域”和“配置将部分IS-IS路由下发到IP路由表” ● OSPFv3：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“配置OSPFv3对接收的路由进行过滤”、“配置OSPFv3引入外部路由”和“使能OSPFv3 GR的Helper能力” ● RIPng：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“配置RIPng引入外部路由”和“控制RIPng路由信息的接收” ● 组播：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP组播》中的“配置根据源地址过滤IGMP报文”、“配置组播组过滤策略”、“（可选）配置接口加入的组播组范围”和“（可选）配置SSM组策略”

----结束

5.7.5.4 检查配置结果

操作步骤

- 执行命令**display acl ipv6** { *acl6-number* | **name** *acl6-name* | **all** }，查看ACL6的配置信息。

- 执行命令**display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

5.7.6 配置并应用高级 ACL6

背景信息

5.7.6.1 （可选）配置 ACL6 的生效时间段

背景信息

ACL6与ACL关联的生效时间段相同，配置方法请参见“配置并应用基本ACL”中的**5.7.1.1 （可选）配置ACL的生效时间段**。

5.7.6.2 配置高级 ACL6

前提条件

如果配置基于时间的ACL6，则需创建生效时间段，并将其与ACL6规则关联起来。具体操作请参见**5.7.5.1 （可选）配置ACL6的生效时间段**。

背景信息

高级ACL6根据源IPv6地址、目的IPv6地址、IPv6协议类型、TCP源/目的端口号、UDP源/目的端口号、分片信息和生效时间段等信息来定义规则，对IPv6报文进行过滤。

高级ACL6比基本ACL6提供了更准确、丰富、灵活的规则定义方法。例如，当希望同时根据源IPv6地址和目的IPv6地址对报文进行过滤时，则需要配置高级ACL6。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建高级ACL。可使用编号或者名称两种方式创建。

- 执行命令**acl ipv6** [**number**] *acl6-number* [**match-order** { **auto** | **config** }]，使用编号（3000～3999）创建一个数字型的高级ACL6，并进入高级ACL6视图。
- 执行命令**acl ipv6 name** *acl6-name* { **advance** | *acl6-number* } [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的高级ACL6，进入高级ACL6视图。

缺省情况下，未创建ACL。

数字型ACL6和命名型ACL6的原理同数字型ACL和命名型ACL，详细介绍请参见**5.2.2 ACL的分类**。

如果创建ACL6时未指定**match-order**参数，则该ACL6默认的规则匹配顺序为**config**。ACL6的规则匹配顺序同ACL匹配顺序，详细介绍请参见**5.2.4 ACL的匹配顺序**。

如果要删除已生效的ACL，可参见“配置基本ACL6”中的**删除ACL**，此处不再赘述。

步骤3 配置高级ACL6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ACL6规则。对于不同的协议类型，有不同的参数组合。

- 当参数protocol为TCP时，高级ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **dscp** *dscp* | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** | **established** } * | **logging** | **time-range** *time-name* | **tos** *tos*] *

- 当参数protocol为UDP时，高级ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **dscp** *dscp* | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **logging** | **time-range** *time-name* | **tos** *tos*] *

- 当参数protocol为ICMPv6时，高级ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmpv6** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | **any** } | **dscp** *dscp* | **icmp6-type** { *icmp6-type-name* | *icmp6-type icmp6-code* } | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name* | **tos** *tos*] *

- 当protocol为IPv6时，高级ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **ipv6** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | **any** } | **dscp** *dscp* | [**fragment** | **none-first-fragment**] | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name* | **tos** *tos*] *

- 当protocol为其他协议时，高级ACL6的命令格式为：

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **ospf** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | **any** } | **dscp** *dscp* | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name* | **tos** *tos*] *

以上步骤仅是一条permit/deny规则的配置步骤。实际配置ACL规则时，需根据具体的业务需求，决定配置多少条规则以及规则的先后匹配顺序。

详细的规则配置示例，请参见**配置高级ACL6规则**。

步骤4 （可选）执行命令**rule** *rule-id* **description** *description*，配置ACL规则的描述信息。

缺省情况下，各规则没有描述信息。

配置ACL规则时，为ACL规则添加描述信息，可以方便理解和记忆该ACL规则的功能或具体用途。

设备仅允许为已存在的规则添加描述信息，不允许先配置规则的描述信息再配置具体的规则内容。

----结束

配置小窍门

配置高级ACL6规则

- **配置基于ICMPv6协议类型、源IPv6地址（主机地址）和目的IPv6地址（网段地址）过滤报文的规则**

  在ACL6 3001中配置规则，允许源IPv6地址是fc00:1::1主机地址且目的IPv6地址是fc00:2::/64网段的ICMPv6报文通过。

  ```
  <Huawei> system-view
  [Huawei] acl ipv6 3001
  [Huawei-acl6-adv-3001] rule permit icmpv6 source fc00:1::1 128 destination fc00:2:: 64
  ```

- **配置基于TCP协议类型、TCP目的端口号、源IPv6地址（主机地址）和目的IPv6地址（网段地址）过滤报文的规则**

  在名称为deny-telnet的高级ACL6中配置规则，拒绝源IPv6地址是fc00:1::3的主机与目的IP地址是fc00:2::/64网段的主机建立Telnet连接。

  ```
  <Huawei> system-view
  [Huawei] acl ipv6 name deny-telnet
  [Huawei-acl6-adv-deny-telnet] rule deny tcp destination-port eq telnet source fc00:1::3 128
  destination fc00:2:: 64
  ```

  在名称为no-web的高级ACL6中配置规则，禁止fc00:1::3和fc00:1::4两台主机访问Web网页（HTTP协议用于网页浏览，对应TCP端口号是80）。

  ```
  <Huawei> system-view
  [Huawei] acl ipv6 name no-web
  [Huawei-acl6-adv-no-web] rule deny tcp destination-port eq 80 source fc00:1::3 128
  [Huawei-acl6-adv-no-web] rule deny tcp destination-port eq 80 source fc00:1::4 128
  ```

- **配置基于时间的ACL6规则**

  请参见“配置基本ACL”中的**配置基于时间的ACL规则**，不再赘述。

- **配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**

  请参见“配置基本ACL”中的**配置基于IP分片信息、源IP地址（网段地址）过滤报文的规则**，不再赘述。

5.7.6.3 应用高级 ACL6

背景信息

配置完ACL6后，必须在具体的业务模块中应用ACL6，才能使ACL6正常下发和生效。

最基本的ACL6应用方式，是在简化流策略/流策略中应用ACL6，使设备能够基于全局、VLAN或接口下发ACL6，实现对转发报文的过滤。此外，ACL6还可以应用在FTP、组播等模块。

操作步骤

步骤1 应用高级ACL6。

高级ACL6的常见应用方式，如**表5-20**所示。

表 5-20 应用基本 ACL6

业务分类	应用场景	各业务模块的ACL应用方式
对转发的报文进行过滤	基于全局、接口和VLAN，对转发的报文进行过滤，从而使设备能够进一步对过滤出的报文进行丢弃、修改优先级、重定向等处理。 例如，可以利用ACL6，降低P2P下载、网络视频等消耗大量带宽的数据流的服务等级，在网络拥塞时优先丢弃这类流量，减少它们对其他重要流量的影响。	● 简化流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“基于ACL的简化流策略配置” ● 流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“MQC配置” ● 包过滤防火墙：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-防火墙配置》中的“**6.6 配置包过滤防火墙**” ● 动态NAT：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置动态地址转换” ● NAT Server：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置内部服务器”

业务分类	应用场景	各业务模块的ACL应用方式
登录控制	对设备的登录权限进行控制，允许合法用户登录，拒绝非法用户登录，从而有效防止未经授权用户的非法接入，保证网络安全性。 例如，一般情况下设备只允许管理员登录，非管理员用户不允许随意登录。这时就可以在Telnet中应用ACL6，并在ACL6中定义哪些主机可以登录，哪些主机不能。	● Telnet：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“配置Telnet服务器功能” ● FTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“通过FTP进行文件操作” ● SFTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“通过SFTP进行文件操作”
路由过滤	ACL6可以应用在组播协议中，实现组播组的过滤。 例如，可以将ACL6和MLD Snooping配合使用，禁止VLAN内的主机加入指定组播组。	组播：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP组播》中的“配置MLD Snooping策略的配置组播组过滤策略”、“配置IGMP Snooping策略的配置组播组过滤策略”、“配置根据源地址过滤IGMP报文”和“（可选）配置接口加入的组播组范围”

----结束

5.7.6.4 检查配置结果

操作步骤

- 执行命令**display acl ipv6** { *acl6-number* | **name** *acl6-name* | **all** }，查看ACL6的配置信息。
- 执行命令**display time-range** { **all** | *time-name* }，查看时间段信息。

----结束

5.8 维护 ACL

介绍如何维护ACL。

5.8.1 调整 ACL 规则的步长

背景信息

在网络日常维护过程中，已部署的ACL可能无法满足新的业务需求，需要管理员为原ACL添加新的规则。由于ACL的缺省步长是5（即系统自动为ACL规则分配编号时的相邻规则编号之间的差值是5，例如rule 5、rule 10、rule 15...），所以管理员在系统分配的相邻编号的规则之间，最多只能插入4条规则（rule 6、rule 7、rule 8、rule 9）。如果新业务要求在这两个规则之间插入4条以上的规则，则可以将ACL规则的步长调大到6以上，使系统按照新步长重新调整规则编号（rule 6、rule 12、rule 18...），从而可以方便的插入4条以上的新规则（rule 7、rule 8、rule 9、rule 10、rule 11）。

关于步长的详细介绍，请参见**5.2.3 ACL的步长设定**。

说明

基本ACL6和高级ACL6不支持步长设定，缺省步长为1。

操作步骤

步骤1 执行命令**system-view**，进入系统视图。

步骤2 创建ACL，可使用编号或者名称两种方式创建。

- 执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号（2000～4999或者6000～6031）创建一个数字型的ACL，并进入ACL视图。
- 执行命令**acl name** *acl-name* [**advance** | **basic** | **link** | *acl-number*] [**match-order** { **auto** | **config** }]，使用名称创建一个命名型的ACL，并进入ACL视图。

缺省情况下，未创建ACL。

关于数字型ACL和命名型ACL的详细介绍，请参见**5.2.2 ACL的分类**。

步骤3 执行命令**step** *step*，配置ACL步长。

缺省情况下，步长值为5。

----结束

5.8.2 查看 ACL 的资源信息

背景信息

当用户发现应用ACL时设备提示失败，原因之一可能是设备上的ACL资源已分配完毕。

为了确认设备ACL资源的分配情况，可以查看ACL的资源信息。

操作步骤

- 在任意视图下执行命令**display acl resource** [**slot** *slot-id*]，查看ACL的资源信息。

  显示信息中的计数非零，表示设备仍存在空余的ACL资源。

----结束

5.8.3 优化 ACL 资源

当配置占用ACL资源的业务时，如果设备提示ACL资源不足，则表明设备的ACL资源已经超限。此时，除了可以删除非必需配置的业务以空出ACL资源外，还可以对ACL应用的范围进行调整或者对业务配置中的ACL规则进行合并，从而节省ACL资源。以流策略为例（流策略占用的ACL资源计算方法请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“MQC配置-配置注意事项”）。

假设使用命令**if-match acl** { *acl-number* | *acl-name* }配置了1K条规则，并且将引用ACL的流策略应用在8个接口的**outbound**方向上，该配置实际需要占用的ACL资源为8K，大于设备支持的下行ACL资源规格（假设为7K），此时该业务无法配置成功。通过以下两种方式，可以减少该业务占用的ACL资源，从而可以顺利配置成功。

- 方式一：调整ACL应用范围

  如果应用流策略的接口均在同一个VLAN，或者部分接口在同一个VLAN，并且未应用流策略的接口均不属于这些VLAN，则可以将ACL应用在各接口所属的VLAN下（假设为VLAN 10和VLAN 20）。调整应用范围后，上例占用的ACL资源为1K（规则数）×2（VLAN数）=2K条，满足设备ACL资源规格的限制。

- 方式二：合并ACL规则

  分析各ACL规则公用的匹配项，找出各规则之间的联系。

  假设，1K条ACL规则中包含以下内容：

```
#
acl number 3009
 rule 1 permit ip source 10.1.1.1 0 destination 10.10.1.1
0
 rule 2 permit ip source 10.1.1.2 0 destination 10.10.1.1 0
 rule 3 permit ip source 10.1.1.3 0 destination 10.10.1.1 0
 rule 4 permit ip source 10.1.1.4 0 destination 10.10.1.1 0
 ...
 rule 255 permit ip source 10.1.1.255 0 destination 10.10.1.1 0
 rule 256 permit ip source 10.1.2.1 0 destination 10.10.1.1 0
 ...
 rule 510 permit ip source 10.1.2.255 0 destination 10.10.1.1 0
 ...
 rule 801 deny tcp destination-port eq www      //80端口
 rule 802 deny tcp destination-port eq 81
 rule 803 deny tcp destination-port eq 82
 ...
 rule 830 deny tcp destination-port eq pop2  //109端口
 rule 831 deny tcp destination-port eq pop3  //110端口
 ...
 rule 1000 xxx
#
```

  由于rule 1～rule 510均用到了匹配项源IP地址和目的IP地址，且源IP地址覆盖了10.1.1.0/24和10.1.2.0/24两个网段的所有地址，因此可以利用IP地址通配符掩码，将rule 1～rule 510合并成以下两条规则：

```
#
acl number 3009
 rule 1 permit ip source 10.1.1.0 0.0.0.255 destination 10.10.1.1 0
 rule 2 permit ip source 10.1.2.0 0.0.0.255 destination 10.10.1.1 0
```

```
 ...
#
```

合并规则后，上例中的规则减少到492条，占用ACL资源数降低到492（规则数）×8（接口数）=3936条，满足设备ACL资源规格的限制。

此外，由于前rule 801～rule 831均用到了匹配项TCP目的端口号，且端口号范围覆盖了80～110整个号段，因此可以利用TCP目的端口号的**range**比较符，将rule 801～rule 831合并成以下一条规则：

```
#
acl number 3009
 ...
 rule 801 deny tcp destination-port range 80 110
 ...
#
```

合并规则后，上例中的规则再次减少到462条，占用ACL资源数降低到462（规则数）×8（接口数）=3696条，满足设备ACL资源规格的限制。

5.8.4 清除 ACL 的统计信息

背景信息

注意

清除统计信息后，以前的统计信息将无法恢复，请务必仔细确认。

操作步骤

- 在确认需要清除ACL的运行信息后，请在用户视图下执行**reset acl counter** { **name** *acl-name* | *acl-number* | **all** }命令，清除ACL统计信息。
- 在确认需要清除ACL6的运行信息后，请在用户视图下执行**reset acl ipv6 counter** { **name** *acl6-name* | *acl6-number* | **all** }命令，清除ACL6统计信息。

----结束

5.9 配置举例

介绍ACL的配置举例。配置示例中包括组网需求、配置思路、操作步骤等。

5.9.1 使用基本 ACL 限制 FTP 访问权限示例

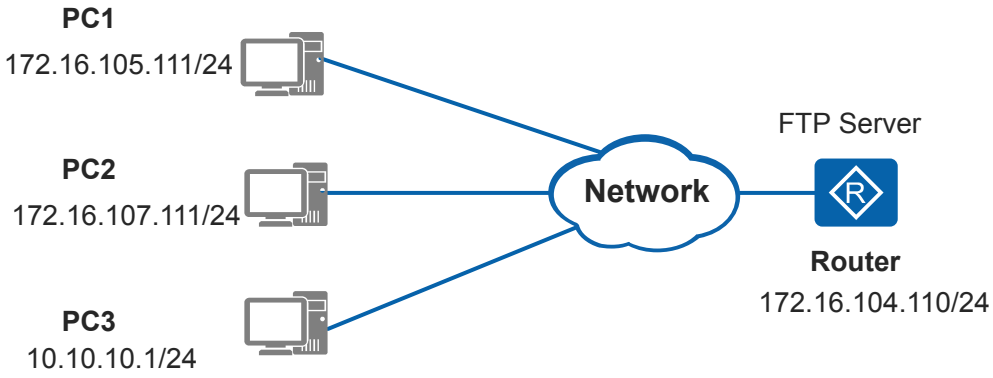
组网需求

如图5-12所示，Router作为FTP服务器，对网络中的不同用户开放不同的访问权限：

- 子网1（172.16.105.0/24）的所有用户在任意时间都可以访问FTP服务器。
- 子网2（172.16.107.0/24）的所有用户只能在某一个时间范围内访问FTP服务器。
- 其他用户不可以访问FTP服务器。

已知Router与各个子网之间路由可达，要求在Router上进行配置，实现FTP服务器对客户端访问权限的设置。

图 5-12 使用基本 ACL 限制 FTP 访问权限组网图



配置思路

采用如下的思路在Router上进行配置：

1. 配置时间段和ACL，使设备可以基于时间的ACL对网络中不同用户的报文进行过滤，从而控制不同用户的FTP访问权限。
2. 配置FTP基本功能。
3. 在FTP模块中应用ACL，使ACL生效。

操作步骤

步骤1 配置时间段

```
<Huawei> system-view
[Huawei] sysname Router
[Router] time-range ftp-access from 0:0 2014/1/1 to 23:59 2014/12/31
[Router] time-range ftp-access 14:00 to 18:00 off-day
```

步骤2 配置基本ACL

```
[Router] acl number 2001
[Router-acl-basic-2001] rule permit source 172.16.105.0 0.0.0.255
[Router-acl-basic-2001] rule permit source 172.16.107.0 0.0.0.255 time-range ftp-access
[Router-acl-basic-2001] rule deny source any
[Router-acl-basic-2001] quit
```

步骤3 配置FTP基本功能

```
[Router] ftp server enable
[Router] aaa
[Router-aaa] local-user huawei password irreversible-cipher SetUesrPasswd@123
[Router-aaa] local-user huawei privilege level 15
[Router-aaa] local-user huawei service-type ftp
[Router-aaa] local-user huawei ftp-directory flash:
[Router-aaa] quit
```

步骤4 配置FTP服务器访问权限

```
[Router] ftp acl 2001
```

步骤5 验证配置结果

在子网1的PC1（172.16.105.111/24）上执行**ftp 172.16.104.110**命令，可以连接FTP服务器。

2014年某个周一在子网2的PC2（172.16.107.111/24）上执行**ftp 172.16.104.110**命令，不能连接FTP服务器；2014年某个周六下午15:00在子网2的PC2（172.16.107.111/24）上执行**ftp 172.16.104.110**命令，可以连接FTP服务器。

在PC3（10.10.10.1/24）上执行**ftp 172.16.104.110**命令，不能连接FTP服务器。

----结束

配置文件

Router的配置文件

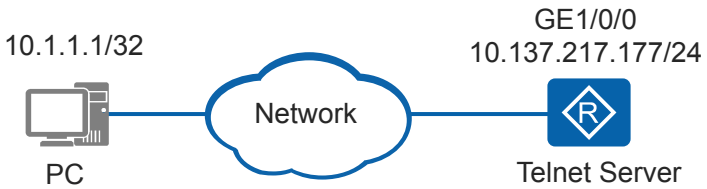
```
#
sysname Router
#
time-range ftp-access 14:00 to 18:00 off-day
time-range ftp-access from 00:00 2014/1/1 to 23:59 2014/12/31
#
acl number 2001
 rule 5 permit source 172.16.105.0 0.0.0.255
 rule 10 permit source 172.16.107.0 0.0.0.255 time-range ftp-access
 rule 15 deny
#
aaa
 local-user huawei password irreversible-cipher %^%#a/sUWg/.p1*))=~SWzIRS0N",`&aS
%'7X).m=o[PkQcv"!!TTQOI~Z)C'1<9%^%#
 local-user huawei privilege level 15
 local-user huawei ftp-directory flash:
 local-user huawei service-type ftp
#
 ftp server enable
 ftp acl 2001
#
return
```

5.9.2 使用基本 ACL 限制 Telnet 登录权限示例

组网需求

如图5-13所示，PC与设备之间路由可达，用户希望简单方便的配置和管理远程设备，可以在服务器端配置Telnet用户使用AAA认证登录，并配置基于ACL的安全策略，保证只有符合安全策略的用户才能登录设备。

图 5-13 配置通过 Telnet 登录设备组网图



说明

使用Telnet协议存在安全风险，建议使用STelnet V2登录设备。

配置思路

采用如下的思路进行配置：

1. 配置Telnet方式登录设备，以实现远程维护网络设备。
2. 配置基于ACL的安全策略，保证只有符合安全策略的用户才能登录设备。
3. 配置管理员的用户名和密码，并配置AAA认证策略，保证只有认证通过的用户才能登录设备。

操作步骤

步骤1 配置服务器的端口号以及使能服务器功能

```
<Huawei> system-view
[Huawei] sysname Telnet Server
[Telnet Server] telnet server enable
[Telnet Server] telnet server port 1025
```

步骤2 配置VTY用户界面的相关参数

配置VTY用户界面的最大个数。

```
[Telnet Server] user-interface maximum-vty 8
```

配置允许用户登录设备的主机地址。

```
[Telnet Server] acl 2001
[Telnet Server-acl-basic-2001] rule permit source 10.1.1.1 0
[Telnet Server-acl-basic-2001] quit
[Telnet Server] user-interface vty 0 7
[Telnet Server-ui-vty0-7] acl 2001 inbound
```

配置VTY用户界面的终端属性。

```
[Telnet Server-ui-vty0-7] shell
[Telnet Server-ui-vty0-7] idle-timeout 20
[Telnet Server-ui-vty0-7] screen-length 30
[Telnet Server-ui-vty0-7] history-command max-size 20
```

配置VTY用户界面的用户验证方式。

```
[Telnet Server-ui-vty0-7] authentication-mode aaa
[Telnet Server-ui-vty0-7] quit
```

步骤3 配置登录用户的相关信息

配置登录验证方式。

```
[Telnet Server] aaa
[Telnet Server-aaa] local-user admin1234 password irreversible-cipher Helloworld@6789
[Telnet Server-aaa] local-user admin1234 service-type telnet
[Telnet Server-aaa] local-user admin1234 privilege level 3
[Telnet Server-aaa] quit
```

步骤4 客户端登录

进入管理员PC的Windows命令行提示符，执行相关命令，通过Telnet方式登录设备。

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177 1025
```

输入Enter键后，在登录窗口输入AAA验证方式配置的登录用户名和密码，验证通过后，出现用户视图的命令行提示符，至此用户成功登录设备。

```
Login authentication

Username:admin1234
```

```
Password:
<Telnet Server>
```

----结束

配置文件

Telnet Server的配置文件

```
#
 sysname Telnet Server
#
acl number 2001
 rule 5 permit source 10.1.1.1 0
#
aaa
 local-user admin1234 password irreversible-cipher %^%#*~Br"; [g6Pv5Zf>$~{hY+N!`{$<[Y{;102P)B,EBz
\1FN!c+%^%#
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
 telnet server enable
 telnet server port 1025
#
user-interface maximum-vty 8
user-interface vty 0 7
 acl 2001 inbound
 authentication-mode aaa
 history-command max-size 20
 idle-timeout 20 0
 screen-length 30
#
return
```

相关资料

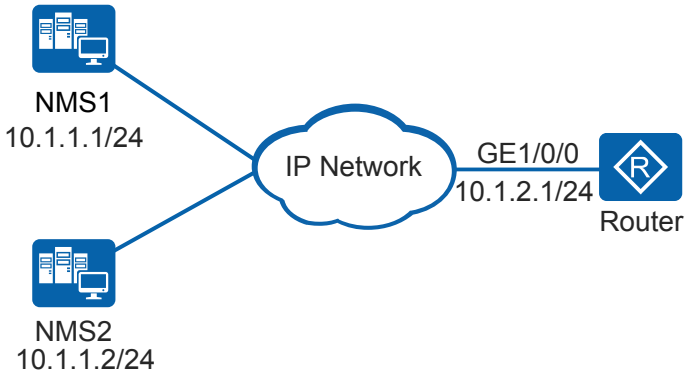
视频：远程登录设备--Telnet方式

5.9.3 SNMP 中应用基本 ACL 过滤非法网管示例

组网需求

如图5-14所示，网络中存在两个网管可以对网络中的设备进行监管。由于网络规模较小、安全性较高，管理员希望Router使用SNMPv1版本与网管进行通信，并且只有可信任的网管（NMS2）才能管理Router，禁止非法网管管理Router。此外，根据业务需要，管理员希望网管站只对设备的DNS节点进行管理，并且通过网管站的管理，可以让管理员能够快速的进行故障定位和排除。

图 5-14 SNMP 中应用基本 ACL 过滤非法网管组网图



配置思路

采用如下的配置思路：

1. 配置路由器的SNMP版本为SNMPv1。
2. 配置ACL、MIB视图和团体名，控制网管站的访问权限，使NMS2可以管理Router上RMON之外的节点，NMS1不能管理Router。
3. 配置路由器的Trap功能，使路由器产生的告警能够发送至NMS2。为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，仅允许缺省打开的模块可以发送告警。
4. 配置路由器管理员的联系方法，以便路由器出现故障时网管管理员能快速联系上就近的设备管理员，以便对故障进行快速定位和排除。
5. 配置网管站（仅NMS2）。

操作步骤

步骤1 配置路由器的IP地址和路由，使和网管站之间路由可达

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 10.1.2.1 24
[Router-GigabitEthernet1/0/0] quit
[Router] ospf
[Router-ospf-1] area 0
[Router-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[Router-ospf-1-area-0.0.0.0] quit
[Router-ospf-1] quit
```

步骤2 使能SNMP Agent

```
[Router] snmp-agent
```

步骤3 配置Router的SNMP版本为SNMPv1

```
[Router] snmp-agent sys-info version v1
```

步骤4 配置网管站的访问权限

配置ACL，使NMS2可以管理Router，NMS1不允许管理Router。

```
[Router] acl 2001
[Router-acl-basic-2001] rule 5 permit source 10.1.1.2 0.0.0.0
[Router-acl-basic-2001] rule 6 deny source 10.1.1.1 0.0.0.0
[Router-acl-basic-2001] quit
```

配置MIB视图。

```
[Router] snmp-agent mib-view dnsmib include 1.3.6.1.4.1.2011.5.25.194
```

配置团体名并引用ACL和MIB视图。

```
[Router] snmp-agent community write adminnms2 mib-view dnsmib acl 2001
```

步骤5 配置告警功能

```
[Router] snmp-agent target-host trap-paramsname trapnms2 v1 securityname adminnms2
[Router] snmp-agent target-host trap-hostname nms2 address 10.1.1.2 trap-paramsname trapnms2
[Router] snmp-agent trap queue-size 200
[Router] snmp-agent trap life 60
[Router] snmp-agent trap enable
```

步骤6 配置设备管理员联系方式

```
[Router] snmp-agent sys-info contact call Operator at 010-12345678
```

步骤7 配置网管站（NMS2）

在使用SNMPv1版本的NMS上需要设置“读写团体名”。网管的配置请根据采用的网管产品参考对应的网管配置手册。

说明

网管系统的认证参数配置必须和设备上保持一致，否则网管系统无法管理设备。如果设备上只配置了write团体名，那么网管端读和写团体名都用设备上配置的write团体名。

步骤8 验证配置结果

配置完成后，可以执行下面的命令，检查配置内容是否生效。

查看SNMP版本。

```
<Router> display snmp-agent sys-info version
  SNMP version running in the system:
        SNMPv1
```

查看团体名的配置信息。

```
<Router> display snmp-agent community write
  Community name: %^%#$X!5#d+t+OJOXL1[{O2!&Fe&OUZv'@a;R/`Y+kK$4BUGFe)&2YLuM/kMF!HPG5Mzz3DXe2&F%^%#
  Storage type: nonVolatile
  View name: dnsmib
  Acl: 2001

  Total number is 1
```

查看ACL配置。

```
<Router> display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
 rule 5 permit source 10.1.1.2 0
 rule 6 deny source 10.1.1.1 0
```

查看MIB视图。

```
<Router> display snmp-agent mib-view dnsmib
  View name: dnsmib
  MIB subtree: hwDnsMIB
  Subtree mask:
  Storage type: nonVolatile
  View type: included
  View status: active
```

查看告警的目标主机。

```
<Router> display snmp-agent target-host
  Traphost list:
  Target host name: nms2
  Traphost address: 10.1.1.2
  Traphost portnumber: 162
  Target host parameter: trapnms2

  Total number is 1

  Parameter list trap target host:
  Parameter name of the target host: trapnms2
  Message mode of the target host: SNMPV1
  Trap version of the target host: v1
  Security name of the target host: %^%#_=XqAFC_94uCS,3'<gYC*ZU6%^%#

  Total number is 1
```

配置设备管理员联系方式。

```
<Router> display snmp-agent sys-info contact
   The contact person for this managed node:
          call Operator at 010-12345678
```

----结束

配置文件

Router的配置文件

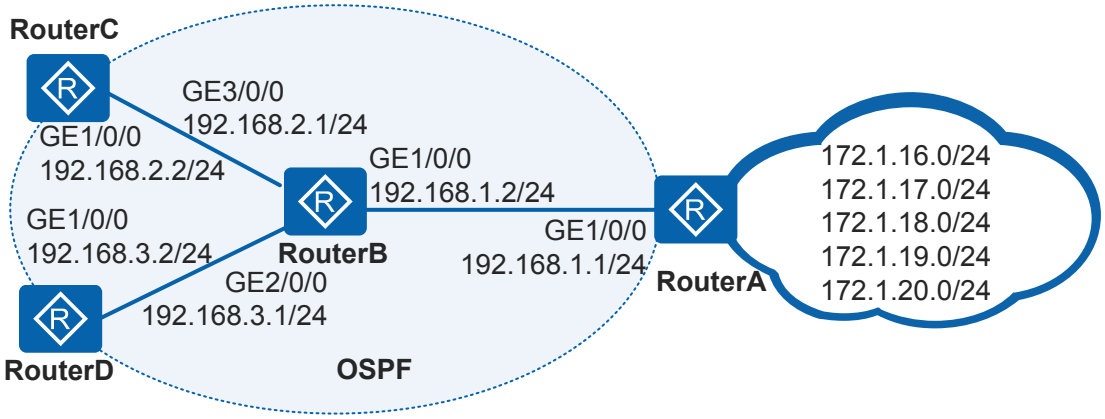
```
#
 sysname Router
#
acl number 2001
 rule 5 permit source 10.1.1.2 0
 rule 6 deny source 10.1.1.1 0
#
interface GigabitEthernet1/0/0
 ip address 10.1.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.1.2.0 0.0.0.255
#
 snmp-agent local-engineid 800007DB03548998F3A458
 snmp-agent community write %^%#$X!5#d+t+OJOXL1[{O2!&Fe&0UZv'@a;R/`Y+kK$4BUGFe)&2YLuM/kMF!
HPG5Mzz3DXe2&F%^%# mib-view dnsmib acl 2001
 snmp-agent sys-info contact call Operator at 010-12345678
 snmp-agent sys-info version v1
 snmp-agent target-host trap-hostname nms2 address 10.1.1.2 udp-port 162 trap-paramsname trapnms2
 snmp-agent target-host trap-paramsname trapnms2 v1 securityname %^%#_=XqAFC_94uCS,3'<gYC*ZU6%^%#
 snmp-agent mib-view dnsmib include hwDnsMIB
 snmp-agent trap enable
 snmp-agent trap queue-size 200
 snmp-agent trap life 60
 snmp-agent
#
return
```

5.9.4 在 OSPF 中使用基本 ACL 过滤路由信息示例

组网需求

如图5-15，运行OSPF协议的网络中，RouterA从Internet网络接收路由，并为OSPF网络提供了Internet路由。要求OSPF网络中只能访问172.1.17.0/24、172.1.18.0/24和172.1.19.0/24三个网段的网络，其中RouterC连接的网络只能访问172.1.18.0/24网段的网络。

图 5-15 配置对接收和发布的路由过滤组网图



配置思路

采用如下的思路配置对路由进行过滤：

1. 在RouterA上配置ACL，在路由发布时应用ACL，使RouterA仅提供路由172.1.17.0/24、172.1.18.0/24、172.1.19.0/24给RouterB，实现OSPF网络中只能访问172.1.17.0/24、172.1.18.0/24、172.1.19.0/24三个网段的网络。
2. 在RouterC上配置ACL，在路由引入时应用ACL，使RouterC仅接收路由172.1.18.0/24，实现RouterC连接的网络只能访问172.1.18.0/24网段的网络。

操作步骤

步骤1 配置各接口的IP地址

配置RouterA的各接口的IP地址。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] interface gigabitethernet 1/0/0
[RouterA-GigabitEthernet1/0/0] ip address 192.168.1.1 255.255.255.0
[RouterA-GigabitEthernet1/0/0] quit
```

RouterB、RouterC和RouterD的配置同RouterA此处略。

步骤2 配置OSPF基本功能

RouterA的配置

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

RouterB的配置

```
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
```

RouterC的配置

```
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

RouterD的配置

```
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
```

步骤3 在RouterA上配置5条静态路由，并在将这些静态路由引入到OSPF协议中

```
[RouterA] ip route-static 172.1.16.0 24 NULL 0
[RouterA] ip route-static 172.1.17.0 24 NULL 0
[RouterA] ip route-static 172.1.18.0 24 NULL 0
[RouterA] ip route-static 172.1.19.0 24 NULL 0
[RouterA] ip route-static 172.1.20.0 24 NULL 0
[RouterA] ospf
[RouterA-ospf-1] import-route static
[RouterA-ospf-1] quit
```

在RouterB上查看IP路由表，可以看到OSPF引入的5条静态路由。

```
[RouterB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 18       Routes : 18

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.1.16.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
     172.1.17.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
     172.1.18.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
     172.1.19.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
     172.1.20.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    192.168.1.0/24  Direct  0    0           D   192.168.1.2     GigabitEthernet1/0/0
    192.168.1.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
  192.168.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     GigabitEthernet3/0/0
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet3/0/0
  192.168.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet3/0/0
    192.168.3.0/24  Direct  0    0           D   192.168.3.1     GigabitEthernet2/0/0
    192.168.3.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
  192.168.3.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

步骤4 配置路由发布策略。

在RouterA配置ACL 2002，允许172.1.17.0/24、172.1.18.0/24和172.1.19.0/24通过。

```
[RouterA] acl number 2002
[RouterA-acl-basic-2002] rule permit source 172.1.17.0 0.0.0.255
[RouterA-acl-basic-2002] rule permit source 172.1.18.0 0.0.0.255
[RouterA-acl-basic-2002] rule permit source 172.1.19.0 0.0.0.255
[RouterA-acl-basic-2002] quit
```

在RouterA配置发布策略，引用ACL 2002进行过滤。

```
[RouterA] ospf
[RouterA-ospf-1] filter-policy 2002 export static
[RouterA-ospf-1] quit
```

在RouterB查看IP路由表，可以看到RouterB仅接收到ACL 2002中定义的3条路由。

```
[RouterB] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 16       Routes : 16

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.1.17.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
     172.1.18.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
     172.1.19.0/24  O_ASE   150  1           D   192.168.1.1     GigabitEthernet1/0/0
    192.168.1.0/24  Direct  0    0           D   192.168.1.2     GigabitEthernet1/0/0
    192.168.1.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
  192.168.1.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.1     GigabitEthernet3/0/0
    192.168.2.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet3/0/0
  192.168.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet3/0/0
    192.168.3.0/24  Direct  0    0           D   192.168.3.1     GigabitEthernet2/0/0
    192.168.3.1/32  Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
  192.168.3.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet2/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

步骤5 配置路由接收策略。

在RouterC配置ACL 2003，允许172.1.18.0/24通过。

```
[RouterC] acl number 2003
[RouterC-acl-basic-2003] rule permit source 172.1.18.0 0.0.0.255
[RouterC-acl-basic-2003] quit
```

在RouterC配置接收策略，引用ACL 2003进行过滤。

```
[RouterC] ospf
[RouterC-ospf-1] filter-policy 2003 import
[RouterC-ospf-1] quit
```

查看RouterC的IP路由表，可以看到RouterC的本地路由表中，仅接收了ACL 2003定义的1条路由。

```
[RouterC] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 8

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     172.1.18.0/24  O_ASE   150  1           D   192.168.2.1     GigabitEthernet1/0/0
    192.168.2.0/24  Direct  0    0           D   192.168.2.2     GigabitEthernet1/0/0
    192.168.2.2/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
  192.168.2.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

----结束

配置文件

- RouterA的配置文件

```
#
sysname RouterA
#
acl number 2002
```

```
 rule 5 permit source 172.1.17.0 0.0.0.255
 rule 10 permit source 172.1.18.0 0.0.0.255
 rule 15 permit source 172.1.19.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.1 255.255.255.0
#
ospf 1
 filter-policy 2002 export static
 import-route static
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
ip route-static 172.1.16.0 255.255.255.0 NULL0
ip route-static 172.1.17.0 255.255.255.0 NULL0
ip route-static 172.1.18.0 255.255.255.0 NULL0
ip route-static 172.1.19.0 255.255.255.0 NULL0
ip route-static 172.1.20.0 255.255.255.0 NULL0
#
return
```

- RouterB的配置文件

```
#
sysname RouterB
#
interface GigabitEthernet1/0/0
 ip address 192.168.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet3/0/0
 ip address 192.168.2.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.2.0 0.0.0.255
  network 192.168.3.0 0.0.0.255
#
return
```

- RouterC的配置文件

```
#
sysname RouterC
#
acl number 2003
 rule 5 permit source 172.1.18.0 0.0.0.255
#
interface GigabitEthernet1/0/0
 ip address 192.168.2.2 255.255.255.0
#
ospf 1
 filter-policy 2003 import
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
#
 ip ip-prefix in index 10 permit 172.1.18.0 24
#
return
```

- RouterD的配置文件

```
#
 sysname RouterD
#
interface GigabitEthernet1/0/0
 ip address 192.168.3.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
```

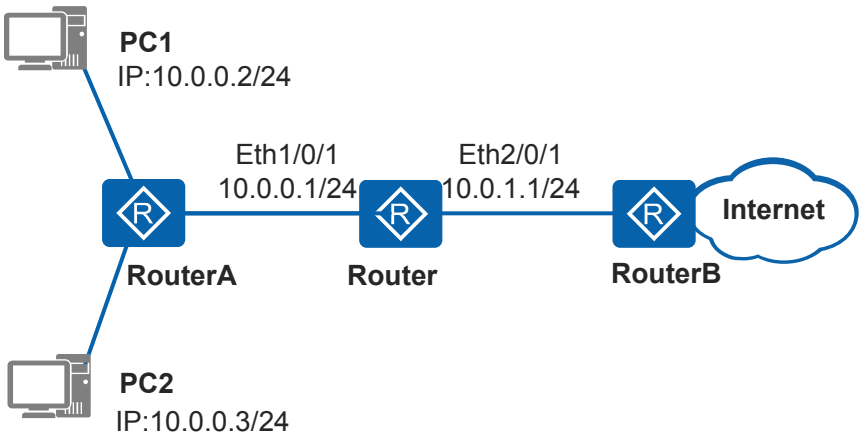
```
  network 192.168.3.0 0.0.0.255
#
return
```

5.9.5 使用基本 ACL 实现配置 URPF 来防止基于源地址欺骗示例

组网需求

如图5-16所示，Router的Eth1/0/1接口连接用户PC1和PC2，Eth2/0/1接口连接上层路由器。为防止基于源地址欺骗攻击，要求在Eth1/0/1和Eth2/0/1接口配置URPF严格检查模式。同时，要求Router只对用户PC2（IP地址是10.0.0.3）的报文进行URPF检查。

图 5-16 使用基本 ACL 实现合法报文流免受 URPF 检查组网图



配置思路

采用如下的思路在Router上进行配置：

1. 在接口Eth1/0/1配置基于ACL的URPF功能，仅对用户PC2的报文进行URPF检查。
2. 在接口Eth2/0/1配置URPF检查模式，防止源地址欺骗攻击。

操作步骤

步骤1 配置接口Eth1/0/1的基于ACL的URPF功能，仅对用户PC2的报文进行URPF检查。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] interface ethernet 1/0/1
[Router-Ethernet1/0/1] ip address 10.0.0.1 24
[Router-Ethernet1/0/1] urpf strict acl 2001
[Router-Ethernet1/0/1] quit
[Router] acl number 2001
[Router-acl-basic-2001] rule permit source 10.0.0.3 0.0.0.255
[Router-acl-basic-2001] quit
```

步骤2 配置接口Eth2/0/1的URPF检查模式。

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] ip address 10.0.1.1 24
[Router-Ethernet2/0/1] urpf strict
[Router-Ethernet2/0/1] quit
```

步骤3 验证配置结果。

查看ACL规则的配置信息

```
[Router] display acl 2001
Basic ACL 2001, 1 rule
Acl's step is 5
 rule 5 permit source 10.0.0.0 0.0.0.255
```

查看接口Eth1/0/1下的URPF配置信息

```
[Router] interface ethernet 1/0/1
[Router-Ethernet1/0/1] display this
#
interface Ethernet1/0/1
 ip address 10.0.0.1 255.255.255.0
 urpf strict acl 2001
#
return
```

查看接口Eth2/0/1的URPF配置信息

```
[Router] interface ethernet 2/0/1
[Router-Ethernet2/0/1] display this
#
interface Ethernet2/0/1
 ip address 10.0.1.1 255.255.255.0
 urpf strict
#
return
```

----结束

配置文件

Router的配置文件

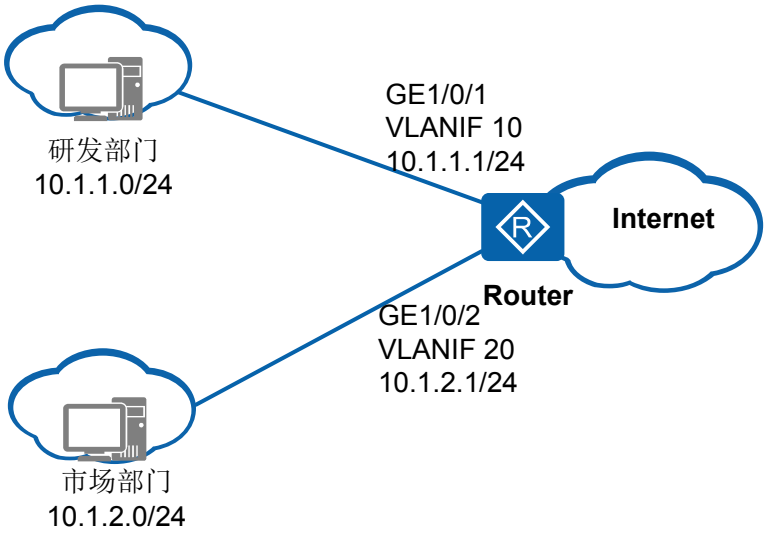
```
#
 sysname Router
#
acl number 2001
 rule 5 permit source 10.0.0.0 0.0.0.255
#
interface Ethernet1/0/1
 ip address 10.0.0.1 255.255.255.0
 urpf strict acl 2001
#
interface Ethernet2/0/1
 ip address 10.0.1.1 255.255.255.0
 urpf strict
#
return
```

5.9.6 使用高级 ACL 限制不同网段的用户互访示例

组网需求

如图5-17所示，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。同时为了隔离广播域，又将两个部门划分在不同VLAN之中。现要求Router能够限制两个网段之间互访，防止公司机密泄露。

图 5-17 使用高级 ACL 限制不同网段的用户互访示例



配置思路

采用如下的思路在Router上进行配置：

1. 配置高级ACL和基于ACL的流分类，使设备可以对研发部与市场部互访的报文进行过滤。
2. 配置流行为，拒绝匹配上ACL规则的报文通过。
3. 配置并应用流策略，使ACL和流行为生效。

操作步骤

步骤1 配置接口所属的VLAN以及接口的IP地址

创建VLAN10和VLAN20。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20
```

配置Router的接口GE1/0/1和GE1/0/2为trunk类型接口，并分别加入VLAN10和VLAN20。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] port link-type trunk
[Router-GigabitEthernet1/0/1] port trunk allow-pass vlan 10
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] port link-type trunk
[Router-GigabitEthernet1/0/2] port trunk allow-pass vlan 20
[Router-GigabitEthernet1/0/2] quit
```

创建VLANIF10和VLANIF20，并配置各VLANIF接口的IP地址。

```
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.1.1.1 24
[Router-Vlanif10] quit
[Router] interface vlanif 20
[Router-Vlanif20] ip address 10.1.2.1 24
[Router-Vlanif20] quit
```

步骤2 配置ACL

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通过。

```
[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
```

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通过。

```
[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
```

步骤3 配置基于高级ACL的流分类

配置流分类tc1，对匹配ACL 3001和ACL 3002的报文进行分类。

```
[Router] traffic classifier tc1
[Router-classifier-tc1] if-match acl 3001
[Router-classifier-tc1] if-match acl 3002
[Router-classifier-tc1] quit
```

步骤4 配置流行为

配置流行为tb1，动作为拒绝报文通过。

```
[Router] traffic behavior tb1
[Router-behavior-tb1] deny
[Router-behavior-tb1] quit
```

步骤5 配置流策略

定义流策略，将流分类与流行为关联。

```
[Router] traffic policy tp1
[Router-trafficpolicy-tp1] classifier tc1 behavior tb1
[Router-trafficpolicy-tp1] quit
```

步骤6 在接口下应用流策略

由于研发部和市场部互访的流量分别从接口GE1/0/1和GE1/0/2进入Router，所以在接口GE1/0/1和GE1/0/2的入方向应用流策略。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] traffic-policy tp1 inbound
[Router-GigabitEthernet1/0/1] quit
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] traffic-policy tp1 inbound
[Router-GigabitEthernet1/0/2] quit
```

步骤7 验证配置结果

查看ACL规则的配置信息。

```
[Router] display acl 3001
Advanced ACL 3001, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[Router] display acl 3002
Advanced ACL 3002, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
```

查看流分类的配置信息。

```
[Router] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: class1
```

```
  Operator: OR
  Rule(s) :  -none-
 Classifier: tc1
  Operator: OR
  Rule(s) :
   if-match acl 3001
   if-match acl 3002
```

查看流策略的配置信息。

```
[Router] display traffic policy user-defined tp1
 User Defined Traffic Policy Information:
 Policy: tp1
  Classifier: tc1
   Operator: OR
    Behavior: tb1
     Deny
```

研发部和市场部所在的两个网段之间不能互访。

----结束

配置文件

Router的配置文件

```
#
 sysname Router
#
vlan batch 10 20
#
acl number 3001
 rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
acl number 3002
 rule 5 deny ip source 10.1.2.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
traffic classifier tc1 operator or
 if-match acl 3001
 if-match acl 3002
#
traffic behavior tb1
 deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy tp1 inbound
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy tp1 inbound
#
return
```

相关资料

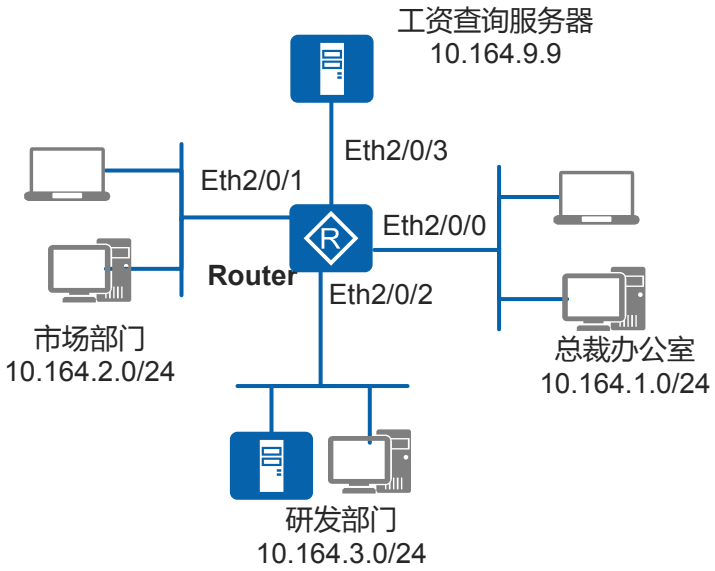
视频：**配置通过ACL禁止两个网段互访**

5.9.7 使用高级 ACL 限制用户在特定时间访问特定服务器的权限示例

组网需求

如图5-18所示，某公司通过Router实现各部门之间的互连。公司要求禁止研发部门和市场部门在上班时间（8:00至17:30）访问工资查询服务器（IP地址为10.164.9.9），总裁办公室不受限制，可以随时访问。

图 5-18 使用高级 ACL 限制用户在特定时间访问特定服务器的权限组网图



配置思路

采用如下的思路在Router上进行配置：

1. 配置时间段、高级ACL和基于ACL的流分类，使设备可以基于时间的ACL，对用户访问服务器的报文进行过滤，从而限制不同用户在特定时间访问特定服务器的权限。
2. 配置流行为，拒绝匹配上ACL的报文通过。
3. 配置并应用流策略，使ACL和流行为生效。

操作步骤

步骤1 配置接口加入VLAN，并配置VLANIF接口的IP地址。

将Eth2/0/0～Eth2/0/2分别加入VLAN10、20、30，Eth2/0/3加入VLAN100，并配置各VLANIF接口的IP地址。下面配置以Eth2/0/0和VLANIF 10接口为例，接口Eth2/0/1、Eth2/0/2和Eth2/0/3的配置与Eth2/0/0接口类似，接口VLANIF 20、VLANIF 30和VLANIF 100的配置与VLANIF 10接口类似，不再赘述。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] vlan batch 10 20 30 100
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type trunk
```

```
[Router-Ethernet2/0/0] port trunk allow-pass vlan 10
[Router-Ethernet2/0/0] quit
[Router] interface vlanif 10
[Router-Vlanif10] ip address 10.164.1.1 255.255.255.0
[Router-Vlanif10] quit
```

步骤2 配置时间段。

配置8:00至17:30的周期时间段。

```
[Router] time-range satime 8:00 to 17:30 working-day
```

步骤3 配置ACL。

配置市场部门到工资查询服务器的访问规则。

```
[Router] acl 3002
[Router-acl-3002] rule deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-
range satime
[Router-acl-3002] quit
```

配置研发部门到工资查询服务器的访问规则。

```
[Router] acl 3003
[Router-acl-3003] rule deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-
range satime
[Router-acl-3003] quit
```

步骤4 配置基于ACL的流分类。

配置流分类c_market，对匹配ACL 3002的报文进行分类。

```
[Router] traffic classifier c_market
[Router-classifier-c_market] if-match acl 3002
[Router-classifier-c_market] quit
```

配置流分类c_rd，对匹配ACL 3003的报文进行分类。

```
[Router] traffic classifier c_rd
[Router-classifier-c_rd] if-match acl 3003
[Router-classifier-c_rd] quit
```

步骤5 配置流行为。

配置流行为b_market，动作为拒绝报文通过。

```
[Router] traffic behavior b_market
[Router-behavior-b_market] deny
[Router-behavior-b_market] quit
```

配置流行为b_rd，动作为拒绝报文通过。

```
[Router] traffic behavior b_rd
[Router-behavior-b_rd] deny
[Router-behavior-b_rd] quit
```

步骤6 配置流策略。

配置流策略p_market，将流分类c_market与流行为b_market关联。

```
[Router] traffic policy p_market
[Router-trafficpolicy-p_market] classifier c_market behavior b_market
[Router-trafficpolicy-p_market] quit
```

配置流策略p_rd，将流分类c_rd与流行为b_rd关联。

```
[Router] traffic policy p_rd
[Router-trafficpolicy-p_rd] classifier c_rd behavior b_rd
[Router-trafficpolicy-p_rd] quit
```

步骤7 应用流策略。

由于市场部访问服务器的流量从接口Eth2/0/1进入Router，所以可以在Eth2/0/1接口的入方向应用流策略p_market。

```
[Router] interface ethernet2/0/1
[Router-Ethernet2/0/1] traffic-policy p_market inbound
[Router-Ethernet2/0/1] quit
```

由于研发部访问服务器的流量从接口Eth2/0/2进入Router，所以可以在Eth2/0/2接口的入方向应用流策略p_rd。

```
[Router] interface ethernet2/0/2
[Router-Ethernet2/0/2] traffic-policy p_rd inbound
[Router-Ethernet2/0/2] quit
```

步骤8 验证配置结果。

查看ACL规则的配置信息。

```
[Router] display acl all
 Total quantity of nonempty ACL number is 2

Advanced ACL 3002, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range satime(Active)

Advanced ACL 3003, 1 rule
Acl's step is 5
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range satime(Active)
```

查看流分类的配置信息。

```
[Router] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c_market
    Operator: OR
    Rule(s) :
     if-match acl 3002
   Classifier: c_rd
    Operator: OR
    Rule(s) :
     if-match acl 3003
```

查看流策略的配置信息。

```
[Router] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p_market
   Classifier: c_market
    Operator: OR
     Behavior: b_market
      Deny

  Policy: p_rd
   Classifier: c_rd
    Operator: OR
     Behavior: b_rd
      Deny
```

查看流策略的应用信息。

```
[Router] display traffic-policy applied-record
----------------------------------------------
  Policy Name:   p_market
  Policy Index:  6
     Classifier:c_market     Behavior:b_market
----------------------------------------------
```

```
*interface Ethernet2/0/1
   traffic-policy p_market inbound
     slot 0    :  success
-----------------------------------------------
  Policy Name:   p_rd
  Policy Index:  7
    Classifier:c_rd     Behavior:b_rd
-----------------------------------------------
*interface Ethernet2/0/2
   traffic-policy p_rd inbound
     slot 0    :  success
-----------------------------------------------
```

研发部门和市场部门在上班时间（8:00至17:30）无法访问工资查询服务器。

----结束

配置文件

Router的配置文件

```
#
 sysname Router
#
 time-range satime 08:00 to 17:30 working-day
#
vlan batch 10 20 30 100
#
acl number 3002
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range
satime
acl number 3003
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range satime
#
traffic classifier c_market operator or
 if-match acl 3002
traffic classifier c_rd operator or
 if-match acl 3003
#
traffic behavior b_market
 deny
traffic behavior b_rd
 deny
#
traffic policy p_market
 classifier c_market behavior b_market
traffic policy p_rd
 classifier c_rd behavior b_rd
#
interface Vlanif10
 ip address 10.164.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.164.2.1 255.255.255.0
#
interface Vlanif30
 ip address 10.164.3.1 255.255.255.0
#
interface Vlanif100
 ip address 10.164.9.9 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface Ethernet2/0/1
 port link-type trunk
```

```
 port trunk allow-pass vlan 20
 traffic-policy p_market inbound
#
interface Ethernet2/0/2
 port link-type trunk
 port trunk allow-pass vlan 30
 traffic-policy p_rd inbound
#
interface Ethernet2/0/3
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

相关资料

视频：

- 限制某时段允许上网
- 限制某时段不能上网

5.9.8 应用高级 ACL 配置防火墙示例

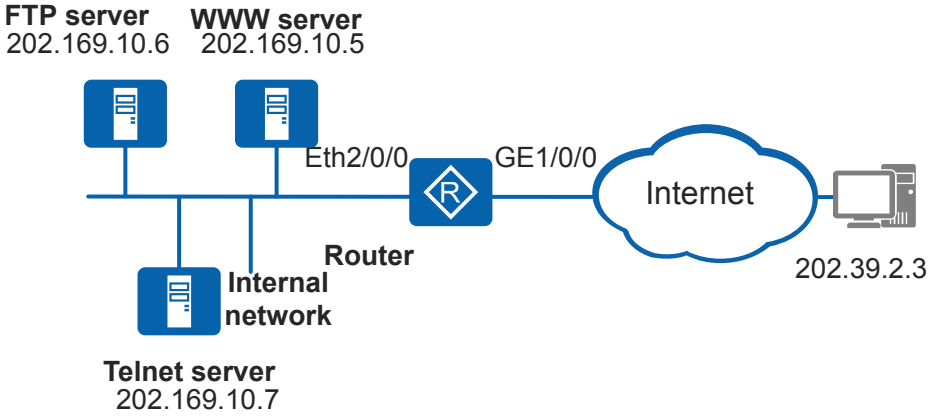
组网需求

如图5-19所示，某个对外提供Web、FTP和Telnet服务的企业通过Router的接口GE1/0/0访问外部网络，通过Router的接口Eth2/0/0加入VLAN。

已知企业的网段为202.169.10.0/24，企业内部的WWW服务器、FTP服务器和Telnet服务器IP地址分别为202.169.10.5/24、202.169.10.6/24和202.169.10.7/24。

为了实现内部网络具备较高的安全性，企业希望在Router上配置防火墙功能，使外部网络只有特定用户可以访问内部服务器，企业内只有内部服务器可以访问外部网络。

图 5-19 应用高级 ACL 配置防火墙组网图



配置思路

采用如下的配置思路：

1. 为企业内部网络和外部网络配置不同的安全区域。
2. 配置安全域间，在安全域间使能防火墙功能。
3. 配置不同的高级ACL，对可以访问内部服务器的外部网络用户以及可以访问外部网络的内部服务器进行分类。
4. 在安全域间配置基于高级ACL的包过滤。

操作步骤

步骤1 配置安全区域

为企业内部网络配置安全区域。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] firewall zone company
[Router-zone-company] priority 12
[Router-zone-company] quit
```

配置接口加入VLAN，并配置VLANIF接口的IP地址，将接口VLANIF 100加入安全区域company。

```
[Router] vlan batch 100
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] port link-type access
[Router-Ethernet2/0/0] port default vlan 100
[Router-Ethernet2/0/0] quit
[Router] interface vlanif 100
[Router-Vlanif100] ip address 202.169.10.1 255.255.255.0
[Router-Vlanif100] zone company
[Router-Vlanif100] quit
```

为外部网络配置安全区域。

```
[Router] firewall zone external
[Router-zone-external] priority 5
[Router-zone-external] quit
```

将接口GigabitEthernet1/0/0加入安全区域external。

```
[Router] interface gigabitethernet 1/0/0
[Router-gigabitethernet1/0/0] ip address 129.39.10.8 255.255.255.0
[Router-gigabitethernet1/0/0] zone external
[Router-gigabitethernet1/0/0] quit
```

步骤2 配置安全域间

```
[Router] firewall interzone company external
[Router-interzone-company-external] firewall enable
[Router-interzone-company-external] quit
```

步骤3 配置ACL 3001

创建ACL 3001。

```
[Router] acl 3001
```

配置允许特定用户从外部网络可以访问内部服务器。

```
[Router-acl-adv-3001] rule permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.5 0.0.0.0
[Router-acl-adv-3001] rule permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.6 0.0.0.0
[Router-acl-adv-3001] rule permit tcp source 202.39.2.3 0.0.0.0 destination 202.169.10.7 0.0.0.0
```

配置其他用户不能从外部网络访问企业内部的任何主机。

```
[Router-acl-adv-3001] rule deny ip
[Router-acl-adv-3001] quit
```

步骤4 配置ACL 3002

创建ACL 3002。

```
[Router] acl 3002
```

配置允许内部服务器访问外部网络。

```
[Router-acl-adv-3002] rule permit ip source 202.169.10.5 0.0.0.0
[Router-acl-adv-3002] rule permit ip source 202.169.10.6 0.0.0.0
[Router-acl-adv-3002] rule permit ip source 202.169.10.7 0.0.0.0
```

配置网络内部的其他用户不能访问外部网络。

```
[Router-acl-adv-3002] rule deny ip
[Router-acl-adv-3002] quit
```

步骤5 在安全域间配置基于高级ACL的包过滤

```
[Router] firewall interzone company external
[Router-interzone-company-external] packet-filter 3001 inbound
[Router-interzone-company-external] packet-filter 3002 outbound
[Router-interzone-company-external] quit
```

步骤6 验证配置结果

配置成功后，仅特定主机（202.39.2.3）可以访问内部服务器，仅内部服务器可以访问外部网络。

在Router上执行**display firewall interzone** [*zone-name1 zone-name2*]操作，结果如下。

```
[Router] display firewall interzone company external
interzone company external
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3001 inbound
 packet-filter 3002 outbound
```

----结束

配置文件

Router的配置文件

```
#
 sysname Router
#
 vlan batch 100
#
acl number 3001
 rule 5 permit tcp source 202.39.2.3 0 destination 202.169.10.5 0
 rule 10 permit tcp source 202.39.2.3 0 destination 202.169.10.6 0
 rule 15 permit tcp source 202.39.2.3 0 destination 202.169.10.7 0
 rule 20 deny ip
acl number 3002
 rule 5 permit ip source 202.169.10.5 0
 rule 10 permit ip source 202.169.10.6 0
 rule 15 permit ip source 202.169.10.7 0
 rule 20 deny ip
#
interface Vlanif100
 ip address 202.169.10.1 255.255.255.0
 zone company
#
firewall zone company
 priority 12
#
```

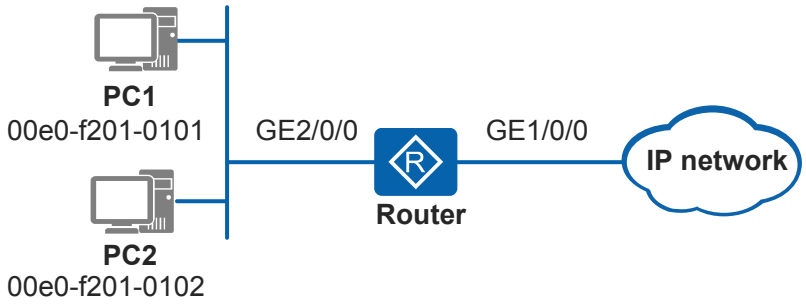
```
firewall zone external
 priority 5
#
firewall interzone company external
 firewall enable
 packet-filter 3001 inbound
 packet-filter 3002 outbound
#
interface Ethernet2/0/0
 port link-type access
 port default vlan 100
#
interface GigabitEthernet1/0/0
 ip address 129.39.10.8 255.255.255.0
 zone external
#
return
```

5.9.9 使用二层 ACL 禁止特定用户上网示例

组网需求

如图5-20所示，Router作为网关设备，下挂用户PC。管理员发现PC1（MAC地址为00e0-f201-0101）用户是非法用户，要求禁止该用户上网。

图 5-20 使用二层 ACL 禁止特定用户上网示例组网图



配置思路

采用如下的思路在Router上进行配置：

1. 配置二层ACL和基于ACL的流分类，使设备对MAC地址为00e0-f201-0101的报文进行过滤，从而禁止该地址对应的用户上网。
2. 配置流行为，拒绝匹配上ACL的报文通过。
3. 配置并应用流策略，使ACL和流行为生效。

操作步骤

步骤1 配置ACL

配置符合要求的二层ACL。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] acl 4000
```

```
[Router-acl-L2-4000] rule deny source-mac 00e0-f201-0101 ffff-ffff-ffff
[Router-acl-L2-4000] quit
```

步骤2 配置基于ACL的流分类

配置流分类tc1，对匹配ACL 4000的报文进行分类。

```
[Router] traffic classifier tc1
[Router-classifier-tc1] if-match acl 4000
[Router-classifier-tc1] quit
```

步骤3 配置流行为

配置流行为tb1，动作为拒绝报文通过。

```
[Router] traffic behavior tb1
[Router-behavior-tb1] deny
[Router-behavior-tb1] quit
```

步骤4 配置流策略

配置流策略tp1，将流分类tc1与流行为tb1关联。

```
[Router] traffic policy tp1
[Router-trafficpolicy-tp1] classifier tc1 behavior tb1
[Router-trafficpolicy-tp1] quit
```

步骤5 应用流策略

由于PC1的报文从接口GE2/0/0进入Router并流向Internet，所以可以在接口GE2/0/0的入方向应用流策略tp1。

```
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] traffic-policy tp1 inbound
[Router-GigabitEthernet2/0/0] quit
```

步骤6 验证配置结果

查看ACL规则的配置信息。

```
[Router] display acl 4000
L2 ACL 4000, 1 rule
Acl's step is 5
 rule 5 deny source-mac 00e0-f201-0101
```

查看流分类的配置信息。

```
[Router] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: tc1
    Operator: OR
    Rule(s) :
     if-match acl 4000
```

查看流策略的配置信息。

```
[Router] display traffic policy user-defined tp1
  User Defined Traffic Policy Information:
  Policy: tp1
   Classifier: tc1
    Operator: OR
     Behavior: tb1
      Deny
```

源MAC地址是00e0-f201-0101的用户无法上网。

----结束

配置文件

Router的配置文件

```
#
 sysname Router
#
acl number 4000
 rule 5 deny source-mac 00e0-f201-0101
#
traffic classifier tc1 operator or
 if-match acl 4000
#
traffic behavior tb1
 deny
#
traffic policy tp1
 classifier tc1 behavior tb1
#
interface GigabitEthernet2/0/0
 traffic-policy tp1 inbound
#
return
```

相关资料

视频：

- **限制指定IP不能上网**
- **通过配置MAC地址过滤，限制指定用户上网**

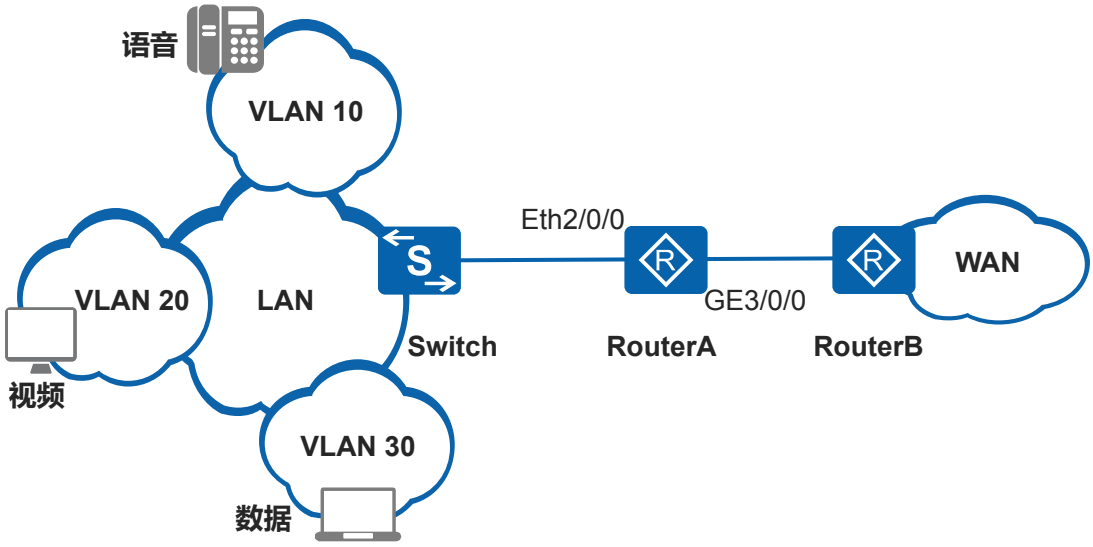
5.9.10 在 QoS 中使用二层 ACL 实施流量监管示例

组网需求

如**图5-21**所示，企业网内部LAN侧的语音、视频和数据业务对应的VLAN ID分别为10、20、30，并通过Switch连接到RouterA的Eth2/0/0上，通过RouterA的GE3/0/0接口连接到WAN侧网络。

在RouterA上需要对不同业务的报文分别进行基于流的流量监管，以将各业务流量控制在一个合理的范围之内，保证各业务的带宽要求；并对接口Eth2/0/0入方向的所有流量进行基于接口的流量监管，控制单个企业用户的总流量在一个合理范围之内。

图 5-21 配置流量监管的组网图



配置思路

采用如下的思路配置流量监管：

1. 在RouterA上创建VLAN、VLANIF，并配置各接口，使企业用户能通过RouterA访问WAN侧网络。
2. 在RouterA上配置基于VLAN ID进行流分类的匹配规则。
3. 在RouterA上配置流行为，对来自企业网内部的不同业务报文进行流量监管。
4. 在RouterA上配置流量监管策略，绑定已配置的流行为和流分类，并应用到RouterA与Switch连接的接口入方向上。
5. 在RouterA与Switch连接的接口入方向上配置基于接口的流量监管，对来自该企业网内部的所有报文进行流量监管。

操作步骤

步骤1 创建VLAN并配置各接口

在RouterA上创建VLAN10、VLAN20和VLAN30。

```
<Huawei> system-view
[Huawei] sysname RouterA
[RouterA] vlan batch 10 20 30
```

配置接口Eth2/0/0为Trunk类型端口，并允许VLAN10、VLAN20和VLAN30的报文通过。

```
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] port link-type trunk
[RouterA-Ethernet2/0/0] port trunk allow-pass vlan 10 20 30
[RouterA-Ethernet2/0/0] quit
```

说明

请配置Switch与RouterA对接的接口为Trunk类型接口，并允许VLAN10、VLAN20和VLAN30的报文通过。

创建VLANIF10、VLANIF20和VLANIF30，并为VLANIF10配置IP地址192.168.1.1/24，并为VLANIF20配置IP地址192.168.2.1/24，为VLANIF30配置IP地址192.168.3.1/24。

```
[RouterA] interface vlanif 10
[RouterA-Vlanif10] ip address 192.168.1.1 24
[RouterA-Vlanif10] quit
[RouterA] interface vlanif 20
[RouterA-Vlanif20] ip address 192.168.2.1 24
[RouterA-Vlanif20] quit
[RouterA] interface vlanif 30
[RouterA-Vlanif30] ip address 192.168.3.1 24
[RouterA-Vlanif30] quit
```

配置GE3/0/0的IP地址为192.168.4.1/24。

```
[RouterA] interface gigabitethernet 3/0/0
[RouterA-GigabitEthernet3/0/0] ip address 192.168.4.1 24
[RouterA-GigabitEthernet3/0/0] quit
```

根据实际情况配置RouterB，确保RouterB与RouterA间路由可达，具体步骤略。

步骤2 配置流分类

在RouterA上创建流分类c1～c3，对来自企业的不同业务流按照其VLAN ID进行分类。

```
[RouterA] traffic classifier c1
[RouterA-classifier-c1] if-match vlan-id 10
[RouterA-classifier-c1] quit
[RouterA] traffic classifier c2
[RouterA-classifier-c2] if-match vlan-id 20
[RouterA-classifier-c2] quit
[RouterA] traffic classifier c3
[RouterA-classifier-c3] if-match vlan-id 30
[RouterA-classifier-c3] quit
```

步骤3 配置流量监管行为

在RouterA上创建流行为b1～b3，对来自企业的不同业务流进行流量监管。

```
[RouterA] traffic behavior b1
[RouterA-behavior-b1] car cir 256
[RouterA-behavior-b1] statistic enable
[RouterA-behavior-b1] quit
[RouterA] traffic behavior b2
[RouterA-behavior-b2] car cir 4000
[RouterA-behavior-b2] statistic enable
[RouterA-behavior-b2] quit
[RouterA] traffic behavior b3
[RouterA-behavior-b3] car cir 2000
[RouterA-behavior-b3] statistic enable
[RouterA-behavior-b3] quit
```

步骤4 配置流量监管策略并应用到接口上

在RouterA上创建流策略p1，将流分类和对应的流行为进行绑定并将流策略应用到接口Eth2/0/0入方向上，对来自企业的不同业务报文进行基于流的流量监管。

```
[RouterA] traffic policy p1
[RouterA-trafficpolicy-p1] classifier c1 behavior b1
[RouterA-trafficpolicy-p1] classifier c2 behavior b2
[RouterA-trafficpolicy-p1] classifier c3 behavior b3
[RouterA-trafficpolicy-p1] quit
[RouterA] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] traffic-policy p1 inbound
```

步骤5 配置基于接口的流量监管

在RouterA的接口Eth2/0/0入方向上配置基于接口的流量监管，控制单个企业用户的总流量在一个合理范围之内。

```
[RouterA-Ethernet2/0/0] qos car inbound cir 10000
[RouterA-Ethernet2/0/0] quit
```

步骤6 验证配置结果

查看流分类的配置信息。

```
[RouterA] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
    Operator: OR
    Rule(s) :
     if-match vlan-id 20
   Classifier: c3
    Operator: OR
    Rule(s) :
     if-match vlan-id 30
   Classifier: c1
    Operator: OR
    Rule(s) :
     if-match vlan-id 10
```

查看流策略的配置信息。

```
[RouterA] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: OR
     Behavior: b1
      Committed Access Rate:
        CIR 256 (Kbps), PIR 0 (Kbps), CBS 48128 (byte), PBS 80128 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
      statistic: enable

   Classifier: c2
    Operator: OR
     Behavior: b2
      Committed Access Rate:
        CIR 4000 (Kbps), PIR 0 (Kbps), CBS 752000 (byte), PBS 1252000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
      statistic: enable

   Classifier: c3
    Operator: OR
     Behavior: b3
      Committed Access Rate:
        CIR 2000 (Kbps), PIR 0 (Kbps), CBS 376000 (byte), PBS 626000 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
      statistic: enable
```

查看在接口上应用的流策略信息。

```
[RouterA] display traffic policy statistics interface ethernet 2/0/0 inbound
```

```
 Interface: Ethernet2/0/0
 Traffic policy inbound: p1
 Rule number: 3
 Current status: OK!
Item                    Sum(Packets/Bytes)              Rate(pps/bps)
-------------------------------------------------------------------------------
Matched                             0/0                             0/0
  Passed                            0/0                             0/0
  Dropped                           0/0                             0/0
    Filter                          0/0                             0/0
    CAR                             0/0                             0/0
  Queue Matched                     0/0                             0/0
    Enqueued                        0/0                             0/0
    Discarded                       0/0                             0/0
  CAR                               0/0                             0/0
    Green packets                   0/0                             0/0
    Yellow packets                  0/0                             0/0
    Red packets                     0/0                             0/0
```

----结束

配置文件

- RouterA的配置文件

```
#
 sysname RouterA
#
vlan batch 10 20 30
#
traffic classifier c1 operator or
 if-match vlan-id 10
traffic classifier c2 operator or
 if-match vlan-id 20
traffic classifier c3 operator or
 if-match vlan-id 30
#
traffic behavior b1
 car cir 256 cbs 48128 pbs 80128 green pass yellow pass red discard
 statistic enable
traffic behavior b2
 car cir 4000 cbs 752000 pbs 1252000 green pass yellow pass red discard
 statistic enable
traffic behavior b3
 car cir 2000 cbs 376000 pbs 626000 green pass yellow pass red discard
 statistic enable
#
traffic policy p1
 classifier c1 behavior b1
 classifier c2 behavior b2
 classifier c3 behavior b3
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
 ip address 192.168.3.1 255.255.255.0
#
interface Ethernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 10 20 30
 qos car inbound cir 10000
 traffic-policy p1 inbound
#
interface GigabitEthernet3/0/0
 ip address 192.168.4.1 255.255.255.0
```

```
#
return
```

相关资料

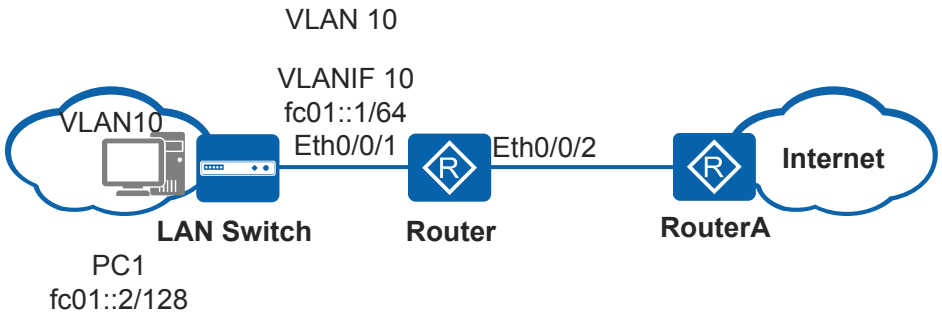
视频：配置基于接口的限速

5.9.11 使用高级 ACL6 过滤特定 IPv6 报文示例

组网需求

如图5-22所示，Router通过Eth0/0/1接口连接用户。要求Router能对来自用户的特定IPv6报文（源IPv6地址为fc01::2/128主机地址、目的IPv6地址为fc01::1/64网段地址的IPv6报文）进行过滤，并拒绝该报文通过。

图 5-22 使用高级 ACL6 过滤特定 IPv6 报文示例组网图



配置思路

采用如下思路在Router上进行配置：

1. 配置高级ACL6和基于ACL6的流分类，使设备可以对特定IPv6报文（源IPv6地址为fc01::2/128、目的IPv6地址为fc01::1/64的IPv6报文）进行过滤。
2. 配置流行为，拒绝匹配上ACL6的报文通过。
3. 配置并应用流策略，使ACL6和流行为生效。

操作步骤

步骤1 使能IPv6转发能力，并配置接口加入VLAN以及VLANIF接口的IPv6地址。

```
<Huawei> system-view
[Huawei] sysname Router
[Router] ipv6
[Router] vlan batch 10
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] port link-type trunk
[Router-Ethernet0/0/1] port trunk allow-pass vlan 10
[Router-Ethernet0/0/1] quit
[Router] interface vlanif 10
[Router-Vlanif10] ipv6 enable
[Router-Vlanif10] ipv6 address fc01::1 64
[Router-Vlanif10] quit
```

步骤2 配置高级ACL6和基于ACL6的流分类，并配置流行为和流策略，再在接口Eth0/0/1的入方向应用流策略，用于拒绝源IPv6地址为fc01::2/128、目的IPv6地址为fc01::1/64的IPv6报文通过。

```
[Router] acl ipv6 number 3001
[Router-acl6-adv-3001] rule deny ipv6 source fc01::2/128 destination fc01::1/64
[Router-acl6-adv-3001] quit
[Router] traffic classifier class1
[Router-classifier-class1] if-match ipv6 acl 3001
[Router-classifier-class1] quit
[Router] traffic behavior behav1
[Router-behavior-behav1] deny
[Router-behavior-behav1] quit
[Router] traffic policy policy1
[Router-trafficpolicy-policy1] classifier class1 behavior behav1
[Router-trafficpolicy-policy1] quit
[Router] interface ethernet 0/0/1
[Router-Ethernet0/0/1] traffic-policy policy1 inbound
[Router-Ethernet0/0/1] quit
```

步骤3 验证配置结果。

查看ACL6的配置信息。

```
[Router] display acl ipv6 3001

Advanced IPv6 ACL 3001, 1 rule
Acl's step is 5
 rule 5 deny ipv6 source FC01::2/128 destination FC01::1/64
```

查看流分类的配置信息。

```
[Router] display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: class1
    Operator: OR
    Rule(s) :
     if-match ipv6 acl 3001
```

查看流策略的配置信息。

```
[Router] display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: policy1
   Classifier: class1
    Operator: OR
     Behavior: behav1
      Deny
```

----结束

配置文件

Router的配置文件

```
#
 sysname Router
#
acl ipv6 number 3001
 rule 5 deny ipv6 source FC01::2/128 destination FC01::1/64
#
ipv6
#
vlan batch 10
#
traffic classifier class1 operator or
 if-match ipv6 acl 3001
```

```
#
traffic behavior behav1
 deny
#
traffic policy policy1
 classifier class1 behavior behav1
#
interface Vlanif10
 ipv6 enable
 ipv6 address FC01::1/64
#
interface Ethernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy policy1 inbound
#
return
```

5.10 常见配置错误

介绍常见配置错误的案例，避免在配置阶段引入故障。

5.10.1 IP 地址通配符掩码配置错误导致业务中断

故障现象

设备上部署流量重定向的流策略后，为了继续增加对某个IP地址的报文的重定向，管理员按照ACL配置原则，在流策略引用的ACL中增加了一条使用该地址作为源IP地址匹配项的规则。由于该规则中的IP地址通配符掩码配置错误，导致BGP协议报文不能上送CPU处理，从而造成设备大部分业务的中断。

操作步骤

步骤1 在新配置规则对应的ACL视图下，执行命令**display this**，查看新配置的ACL规则。

新配置的规则如下：

```
rule 100 permit ip source 10.1.1.3 255.255.255.255
```

可以看到，该规则中的IP地址通配符掩码（255.255.255.255），被配置成了正向掩码而非反向掩码，导致该规则的含义发生变化。实际上，该规则与“rule 100 permit ip”和“rule 100 permit ip source any”的含义相同，均表示设备匹配任意IP地址的报文。

而该ACL被用做流量重定向，并且引用该ACL的流策略被应用在了大量的接口下，因此设备从这些接口收到的BGP协议报文会被重定向到其他接口，而不是正常上送CPU处理，从而导致协议超时，造成大部分业务的中断。

步骤2 在新配置规则对应的ACL视图下，执行命令**rule（高级ACL视图）**，修改新配置的ACL规则中的IP地址通配符掩码。

修改后的规则如下：

```
rule 100 permit ip source 10.1.1.3 0.0.0.0 //IP地址通配符掩码为0.0.0.0，才表示单个主机的IP地址
```

规则修改后，中断的业务会恢复正常，源IP地址为10.1.1.3的报文能被正常的重定向。

----结束

5.10.2 误屏蔽 DNS 服务器地址导致用户无法上网

故障现象

配置ACL限制用户可访问的地址时，误将DNS服务器地址加入到了限制的地址范围内，导致用户访问网站时向DNS服务器发送的查询报文被屏蔽，网站域名得不到解析，从而造成用户无法上网。

操作步骤

步骤1 在系统视图下，执行命令**display acl**，查看ACL规则的配置。

发现设备上配置了如下一条规则：

```
rule 100 deny ip destination 10.102.192.0 0.0.0.255  //禁止访问10.102.192.0/24网段的报文通过
```

由于用户PC上设置的DNS服务器地址是10.102.192.68，属于10.102.192.0/24网段，因此用户向DNS服务器发送的报文也被禁止通过，导致其访问网站的域名得不到解析，从而无法上网。

步骤2 在上述规则对应的ACL视图下，执行命令**rule（高级ACL视图）**，在原规则前增加一条放行DNS服务器地址的规则。

```
rule 99 permit ip destination 10.102.192.68 0  //允许访问DNS服务器地址的报文通过
rule 100 deny ip destination 10.102.192.0 0.0.0.255  //禁止访问10.102.192.0/24网段的报文通过
```

添加新规则rule 99后，用户发送给DNS服务器地址的报文会先命中rule 99而得到允许通过，从而使用户访问网站的域名能够被DNS服务器正常解析，用户可以正常上网。

----结束

5.10.3 系统时间不正确导致基于时间的 ACL 不生效

故障现象

由于设备的系统时间与现实时间不一致，导致设备上配置的基于时间的ACL不生效。

操作步骤

步骤1 在系统视图下，执行命令**display acl**，查看ACL规则的配置。

发现设备上配置了一条基于时间的ACL规则：

```
rule 10 deny ip source 10.1.1.1 0 time-range time1 //在time1设定的时间范围内，禁止源地址是10.1.1.1的报文通过
```

步骤2 在系统视图下，执行命令**display time-range** { **all** | *time-name* }，查看生效时间段**time1**的配置。

显示信息如下：

```
Current time is 14:53:17 8-16-2013 Friday

Time-range: time1 ( Inactive )
from 00:00 2014/1/1 to 23:59 2014/12/31
Total time-range number is 1
```

可以看到，时间段**time1**设定的范围是2014年1月1日零点开始到2014年12月31日23：59分结束，并且设备上的系统时间是2013年的8月16日14:53:17秒。由于当前的实际日期是2014年8月16日，并且设备上设置的系统时间不在时间段**time1**设定的时间范围内，因此引用**time1**的ACL不生效，源地址是10.1.1.1的报文不会被设备禁止通过。

步骤3 调整系统日期和时间。

- 重新配置设备的当前日期和时间，保证设备时间与现实时间的一致。

  在用户视图下，执行命令**clock datetime**。

  ```
  clock datetime 14:53:17 2014-08-16 //将日期调整为2014-08-16
  ```

- 配置NTP，实现系统时钟的自动同步，使设备与时间可信任的设备（该设备通过网络和权威时钟同步过时钟）上的时间保持一致。

  a. 在时间可信任的设备上，配置使用本地设备时钟作为NTP主时钟以及NTP主时钟所处的层数。

  在系统视图下，执行命令**ntp-service refclock-master**。

  ```
  ntp-service refclock-master 2 //层数值越小表示时钟准确度越高
  ```

  b. 在本设备（需同步其他设备时钟的设备）上，配置NTP工作模式，具体配置请参见配置NTP工作模式。

----结束

5.11 FAQ

介绍配置过程中常见的问题，以及解决方法。

5.11.1 ACL 下发主要有哪几种方式？

配置完ACL后，必须在具体的业务模块中应用ACL，才能使ACL正常下发和生效。

最基本的ACL应用方式，是在简化流策略/流策略中应用ACL，使设备能够基于全局、VLAN或接口下发ACL，实现对转发报文的过滤。此外，ACL还可以应用在Telnet、FTP、路由等模块。

常见的ACL下发方式，如表5-21所示。

表 5-21 常见 ACL 下发方式

业务分类	应用场景	各业务模块的ACL应用方式
对转发的报文进行过滤	基于全局、接口和VLAN，对转发的报文进行过滤，从而使设备能够进一步对过滤出的报文进行丢弃、修改优先级、重定向等处理。 例如，可以利用ACL，降低P2P下载、网络视频等消耗大量带宽的数据流的服务等级，在网络拥塞时优先丢弃这类流量，减少它们对其他重要流量的影响。	● 简化流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“基于ACL的简化流策略配置” ● 流策略：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的“MQC配置” ● 包过滤防火墙：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-防火墙配置》中的“**6.6 配置包过滤防火墙**” ● 动态NAT：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置动态地址转换” ● NAT Server：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP业务配置》中的“配置内部服务器”

业务分类	应用场景	各业务模块的ACL应用方式
对上送CPU处理的报文进行过滤	对上送CPU的报文进行必要的限制，可以避免CPU处理过多的协议报文造成占用率过高、性能下降。 例如，当发现某用户向设备发送大量的ARP攻击报文，造成设备CPU繁忙，引发系统中断时，可以在本机防攻击策略的黑名单中应用ACL，将该用户加入黑名单，使CPU丢弃该用户发送的报文。	黑名单：请参见“本机防攻击配置”中的“**8.3.2 配置黑名单**”

业务分类	应用场景	各业务模块的ACL应用方式
登录控制	对设备的登录权限进行控制，允许合法用户登录，拒绝非法用户登录，从而有效防止未经授权用户的非法接入，保证网络安全性。	● Telnet：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“配置Telnet服务器功能” ● FTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“通过FTP进行文件操作” ● SFTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“通过SFTP进行文件操作” ● TFTP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的”配置设备作为TFTP客户端访问其他设备的文件“ ● Web登录：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-基础配置》中的“（可选）配置Web网管参数” ● SNMP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-网络管理与监控》中的“（可选）限制网管对设备的管理权限”（SNMPv1、SNMPv2c）和“（可选）限制网管对设备的管理权限”（SNMPv3）

业务分类	应用场景	各业务模块的ACL应用方式
路由过滤	ACL可以应用在各种动态路由协议中，对路由协议发布、接收的路由信息以及组播组进行过滤。 例如，可以将ACL和路由策略配合使用，禁止设备将某网段路由发给邻居路由器。	● BGP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“控制BGP路由信息的发布”和“控制BGP路由信息的接收” ● IS-IS（IPv4）：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“配置IS-IS发布部分外部路由到IS-IS路由域”和“配置将部分IS-IS路由下发到IP路由表” ● OSPF：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“配置OSPF对接收的路由进行过滤”、“配置OSPF对发布的路由进行过滤”和“（可选）配置Helper端GR的会话参数” ● RIP：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP单播路由》中的“配置RIP引入外部路由信息”和“配置RIP对接收的路由进行过滤” ● 组播：请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-IP组播》中的“配置根据源地址过滤IGMP报文”、“配置组播组过滤策略”、“（可选）配置接口加入的组播组范围”和“（可选）配置SSM组策略”

5.11.2 ACL 中的 permit/deny 与 traffic policy 中 behavior 的 permit/deny 之间是什么关系？

ACL与traffic policy（流策略）经常组合使用。traffic policy定义符合ACL的流分类，然后再定义符合流分类的行为，即behavior，例如允许通过、拒绝通过等等。

ACL中的permit/deny与traffic policy中behavior的permit/deny组合有如下四种情况：

表 5-22 ACL 中的 permit/deny 与 traffic policy 中 behavior 的 permit/deny 组合情况

ACL	traffic policy中的behavior	匹配报文的最终处理结果
permit	permit	permit
permit	deny	deny
deny	permit	deny
deny	deny	deny

说明

在流策略模块中，设备默认报文都是permit的，如果只是要求网段之间不能访问，则只需在ACL里配置想要deny的报文的规则即可。如果最后多添加一条**rule permit**规则，则未命中该规则之前规则的所有报文都会命中此条规则，并且如果流行为behavior被配置为deny，则设备将拒绝所有命中该规则的报文通过，导致全部业务中断。

5.11.3 如何在 VLAN 下应用 ACL？

可以通过在全局下应用指定VLAN编号的简化流策略，将ACL与业务模块（流策略或简化流策略）绑定起来，再在VLAN下应用。

说明

以下命令行表达方式仅是示意形式，实际配置方法请参考各版本的命令行格式。

可以在系统视图下，执行以下命令：

- 基于ACL的报文过滤
  - **traffic-filter vlan** *vlan-id* **inbound acl xxx**
  - **traffic-filter vlan** *vlan-id* **outbound acl xxx**
  - **traffic-secure vlan** *vlan-id* **inbound acl xxx**
- 基于ACL的流量监管
  - **traffic-limit vlan** *vlan-id* **inbound acl xxx**
  - **traffic-limit vlan** *vlan-id* **outbound acl xxx**
- 基于ACL的重定向

  traffic-redirect vlan *vlan-id* **inbound acl xxx**

- 基于ACL的重标记
  - **traffic-remark vlan** *vlan-id* **inbound acl xxx**
  - **traffic-remark vlan** *vlan-id* **outbound acl xxx**
- 基于ACL的流量统计
  - **traffic-statistic vlan** *vlan-id* **inbound acl xxx**
  - **traffic-statistic vlan** *vlan-id* **outbound acl xxx**
- 基于ACL的流镜像

  traffic-mirror vlan *vlan-id* **inbound acl xxx**

5.11.4 如何在接口上应用 ACL？

ACL无法直接在接口上应用，但可以通过以下两种方式，将ACL与业务模块（流策略或简化流策略）绑定起来，再在接口上应用。

说明

以下命令行表达方式仅是示意形式，实际配置方法请参考各版本的命令行格式。

设备不支持在VLANIF接口下应用ACL。

- 方式一：在接口上应用流策略
  a. 配置流分类
     i. 在系统视图下，执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] [**precedence** *precedence-value*]，进入流分类视图。
     ii. 执行命令**if-match acl** { *acl-number* | *acl-name* }，配置基于ACL进行分类的匹配规则。
  b. 配置流行为

     在系统视图下，执行命令**traffic behavior** *behavior-name*，定义流行为并进入流行为视图。
  c. 配置流动作。

     报文过滤有两种流动作：**deny**或**permit**。其他流动作，请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的介绍。
  d. 配置流策略
     i. 在系统视图下，执行命令**traffic policy** *policy-name*，定义流策略并进入流策略视图。
     ii. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。
  e. 应用流策略

     在接口视图下，执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，应用流策略。
- 方式二：在接口下应用简化流策略

  可以在接口视图下，执行以下命令：
  - 基于ACL的报文过滤
    - **traffic-filter inbound acl xxx**
    - **traffic-filter outbound acl xxx**
    - **traffic-secure inbound acl xxx**

- 基于ACL的流量监管
  - **traffic-limit inbound acl xxx**
  - **traffic-limit outbound acl xxx**
- 基于ACL的重定向

  traffic-redirect inbound acl xxx
- 基于ACL的重标记
  - **traffic-remark inbound acl xxx**
  - **traffic-remark outbound acl xxx**
- 基于ACL的流量统计
  - **traffic-statistic inbound acl xxx**
  - **traffic-statistic outbound acl xxx**
- 基于ACL的流镜像

  traffic-mirror inbound acl xxx

5.11.5 如何查看 ACL 的生效顺序？

在任意视图下执行命令**display acl** { *acl-number* | **name** *acl-name* | **all** }、**display acl ipv6** { *acl6-number* | **name** *acl6-name* | **all** }或在ACL视图下执行命令**display this**，可以查看ACL规则的生效顺序，如表5-23所示。

表 5-23 ACL 的生效顺序

ACL类型	ACL的生效顺序
config模式的ACL	编号小的规则优先生效
auto模式的ACL	编号小的规则优先生效
config模式的ACL6	编号小的规则优先生效
auto模式的ACL6	排序靠前的规则优先生效，规则不一定按照编号从小到大的顺序进行排序

说明

当在流策略中引用ACL并且设备上应用了多个流策略时，如果报文同时匹配上了多个流策略中的ACL规则，则ACL的生效顺序与流策略模块的处理机制相关，具体请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的介绍。

5.11.6 如何实现单向访问控制？

可以通过以下两种方式实现：

说明

以下命令行表达方式仅是示意形式，实际配置方法请参考各版本的命令行格式。

- 方式一：流策略

a. 创建高级ACL

在系统视图下，执行命令**acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }]，使用编号（3000～3999）创建高级ACL并进入高级ACL视图，或者执行命令**acl name** *acl-name* { **advance** | *acl-number* } [**match-order** { **auto** | **config** }]，使用名称创建高级ACL并进入高级ACL视图。

b. 配置高级ACL规则

执行命令**rule**，配置指定**tcp-flag**参数的高级ACL规则。

假设，要求192.168.1.0/24网段用户可以主动访问192.168.2.0/24网段用户，但反过来192.168.2.0/24网段用户不能主动访问192.168.1.0/24。

由TCP建立连接和关闭连接的过程可知，只有在TCP中间连接过程的报文才会ACK=1或者RST=1。根据这个特点，配置如下两种ACL规则，允许TCP中间连接过程的报文通过，拒绝其他TCP报文通过，就可以限制192.168.2.0/24网段主动发起的TCP连接。

- 类型一：配置指定**ack**和**rst**参数的ACL规则

```
rule 5 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag ack  //允许ACK=1的TCP报文通过
rule 10 permit tcp source 192.168.2.0 0.0.0.255 tcp-flag rst   //允许RST=1的TCP报文通过
rule 15 deny tcp source 192.168.2.0 0.0.0.255  //拒绝其他TCP报文通过
```

- 类型二：配置指定**established**参数的ACL规则

```
rule permit tcp source 192.168.2.0 0.0.0.255 tcp-flag established  // established表示ACK=1或者RST=1，表示允许TCP中间连接过程的报文通过
rule deny tcp source 192.168.2.0 0.0.0.255     //拒绝其他TCP报文通过
```

c. 配置流分类

i. 在系统视图下，执行命令**traffic classifier** *classifier-name* [**operator** { **and** | **or** }] [**precedence** *precedence-value*]，进入流分类视图。

ii. 执行命令**if-match acl** { *acl-number* | *acl-name* }，配置基于ACL进行分类的匹配规则。

d. 配置流行为

在系统视图下，执行命令**traffic behavior** *behavior-name*，定义流行为并进入流行为视图。

e. 配置流动作。

报文过滤有两种流动作：**deny**或**permit**。其他流动作，请参见《Huawei AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600系列 企业路由器 配置指南-QoS》中的介绍。

f. 配置流策略

i. 在系统视图下，执行命令**traffic policy** *policy-name*，定义流策略并进入流策略视图。

ii. 执行命令**classifier** *classifier-name* **behavior** *behavior-name*，在流策略中为指定的流分类配置所需流行为，即绑定流分类和流行为。

g. 应用流策略

在接口视图下，执行命令**traffic-policy** *policy-name* { **inbound** | **outbound** }，应用流策略。

针对上例，需在设备上连接192.168.2.0/24网段的接口入方向上应用流策略。

- 方式二：简化流策略

a. 配置高级ACL和ACL规则（同流策略方式）

b. 应用简化流策略

在接口视图下，执行命令**traffic-filter** { **inbound** | **outbound** } **acl xxx**，应用简化流策略（基于ACL的报文过滤）。

针对流策略方式中的举例，需在设备上连接192.168.2.0/24网段的接口入方向上应用简化流策略。

5.11.7 应用在流策略中的 ACL 不支持对哪些报文进行过滤？

应用在流策略中的ACL不支持对上送CPU处理的协议报文进行过滤，例如：

- VRRP使用的协议报文是目的IP地址为224.0.0.18的组播报文，该报文到达设备后会被上送CPU处理，因此流策略中的ACL对该报文不生效，VRRP组内的成员路由器仍能够协商出主备关系。
- DHCP客户端为了获取合法的动态IP地址，会与服务器之间交互DHCP报文，该报文到达设备后会被上送CPU处理，因此流策略中的ACL对该报文不生效，设备无法阻止一个接口下的用户通过DHCP自动获取IP地址。
- 用户主机Ping本设备时，ICMP报文到达设备后会被上送CPU处理，因此流策略中的ACL对该报文不生效，设备无法阻止用户主机Ping本设备。

对于上送CPU处理的协议报文，可以通过在本机防攻击中的黑名单中应用ACL进行过滤，步骤如下：

1. 在系统视图下，执行命令**cpu-defend policy** *policy-name*，进入防攻击策略视图。
2. 执行命令**blacklist** *blacklist-id* **acl** *acl-number*，创建黑名单。
3. 执行命令**cpu-defend-policy** *policy-name* [**global** | **slot** *slot-id*]，应用防攻击策略。

5.11.8 ACL 的 rule 中的 deny/permit 在各个业务模块里的场景是怎样的

ACL的rule中的deny/permit在各个业务模块里的场景不同，具体如下：

- 流策略
  a. 当ACL的rule配置为**permit**时，系统匹配该规则才执行流行为中的动作，流行为中的动作为**deny**则禁止匹配规则的流量通过，动作为**permit**则允许匹配规则的流量通过。
  b. 当ACL的rule配置为**deny**时，只要匹配该规则就执行丢弃报文动作，并且流行为中的具体动作不生效（流量统计和流镜像除外）。
  c. 当ACL里未配置rule时，则应用该ACL的流策略功能不生效。
- 简化流策略
  a. 当ACL的rule配置为**permit**时，设备执行简化流策略功能中的动作，如允许匹配该规则的报文通过、对匹配ACL规则的报文进行限速等。
  b. 当ACL的rule配置为**deny**时，如果将ACL应用在简化流策略的报文过滤功能中，设备会拒绝匹配该规则的报文通过。
  c. 当ACL里未配置rule时，则应用该ACL的简化流策略功能不生效。
- IPSec
  a. 仅当ACL的rule配置为**permit**时，设备会对匹配该规则的报文进行IPSec保护后再发送该报文。

b. 当ACL的rule配置为**deny**时，设备不允许匹配ACL规则的报文通过。

c. 当ACL未配置rule时，应用该ACL的IPSec功能不生效，即设备直接发送通过接口的报文。

- 防火墙

a. 当ACL的rule配置为**permit**时：

- 如果该ACL应用在**inbound**方向，则允许从优先级低到优先级高的安全区域并且匹配该规则的报文通过。
- 如果该ACL应用在**outbound**方向，则允许从优先级高到优先级低的安全区域并且匹配该规则的报文通过。

b. 当ACL的rule配置为**deny**时：

- 如果该ACL应用在**inbound**方向，则拒绝从优先级低到优先级高的安全区域且匹配该规则的报文通过。
- 如果该ACL应用在**outbound**方向，则拒绝从优先级高到优先级低的安全区域且匹配该规则的报文通过。

c. 当ACL里未配置rule时：

- 如果该ACL应用在**inbound**方向，则该ACL不生效，设备会拒绝从优先级低到优先级高的安全区域的所有报文通过。
- 如果该ACL应用在**outbound**方向，则该ACL不生效，设备会允许从优先级高到优先级低的安全区域的所有报文通过。

- NAT

a. 仅当ACL的rule配置为**permit**时，设备允许匹配该规则中指定的源IP地址使用地址池进行地址转换。

b. 当ACL的rule配置为**deny**或ACL未配置rule时，应用该ACL的NAT功能不生效，即不允许使用地址池进行地址转换，设备根据目的地址查找路由表转发报文。

- Telnet

a. 当ACL的rule配置为**permit**时：

- 如果该ACL应用在**inbound**方向，则允许匹配该rule规则的其他设备访问本设备。
- 如果该ACL应用在**outbound**方向，则允许本设备访问匹配该rule规则的其他设备。

b. 当ACL的rule配置为**deny**时：

- 如果该ACL应用在**inbound**方向，则拒绝匹配该rule规则的其他设备访问本设备。
- 如果该ACL应用在**outbound**方向，则拒绝本设备访问匹配该rule规则的其他设备。

c. 当ACL配置了rule，但来自其他设备的报文没有匹配该rule规则时：

- 如果该ACL应用在**inbound**方向，则拒绝其他设备访问本设备。
- 如果该ACL应用在**outbound**方向，则拒绝本设备访问其他设备。

d. 当ACL未配置rule时：

- 如果该ACL应用在**inbound**方向，则允许任何其他设备访问本设备。
- 如果该ACL应用在**outbound**方向，则允许本设备访问任何其他设备。

- HTTP

a. 当ACL的rule配置为**permit**时，则允许指定源IP地址的其他设备与本设备建立HTTP连接。
b. 当ACL的rule配置为**deny**时，则拒绝其他设备与本设备建立HTTP连接。
c. 当ACL配置了rule，但来自其他设备的报文没有匹配该rule规则时，则拒绝其他设备与本设备建立HTTP连接。
d. 当ACL未配置rule时，则允许任何其他设备与本设备建立HTTP连接。

- FTP
  a. 当ACL的rule配置为**permit**时，则允许指定源IP地址的其他设备与本设备建立FTP连接。
  b. 当ACL的rule配置为**deny**时，则拒绝任何其他设备与本设备建立FTP连接。
  c. 当ACL配置了rule，但来自其他设备的报文没有匹配该rule规则时，则拒绝其他设备与本设备建立FTP连接。
  d. 当ACL未配置rule时，则允许任何其他设备与本设备建立FTP连接。
- TFTP
  a. 当ACL的rule配置为**permit**时，则允许本设备与指定源IP地址的设备建立TFTP连接。
  b. 当ACL的rule配置为**deny**时，则拒绝本设备与任何其他设备建立TFTP连接。
  c. 当ACL配置了rule，但来自其他设备的报文没有匹配该rule规则时，则拒绝其他设备与本设备建立TFTP连接。
  d. 当ACL未配置rule时，则允许本设备与任何其他设备建立TFTP连接。
- SNMP
  a. 当ACL的rule配置为**permit**时，则允许指定源IP地址的网管访问本设备。
  b. 当ACL的rule配置为**deny**时，则拒绝其他网管访问本设备。
  c. 当ACL未配置rule时，则允许任何其他网管访问本设备。
- NTP
  a. 当ACL的rule配置为**permit**时，则使用**ntp-service access**命令配置的访问控制权限才能生效。
  b. 当ACL的rule配置为**deny**，则使用**ntp-service access**命令配置的访问控制权限不生效。
  c. 当ACL未配置rule时，则使用**ntp-service access**命令配置的访问控制权限不生效。

5.12 参考标准和协议

介绍ACL的参考标准和协议。

与ACL特性相关的参考标准及协议如下：

文档	描述	备注
RFC 4314	Defines several new access control rights and clarifies which rights are required for different IMAP (Internet Message Access Protocol) commands.	-