华为 ACL 配置教程

华为 ACL 配置中流策略的配置命令。

华为设备配置 ACL 不像 Cisco 的那样可以直接在接口下配置 ACL 来应用。

1、先配 ACL，

2、然后配流分类（traffic classifier tc1），将 ACL 和流分类绑定，

3、再配流行为（traffic behavior tb1），

4、接着配置流策略（traffic policy tp1），

5、最后把策略应用到接口下，让 ACL 生效。

具体例子如下：

步骤 1 配置 ACL

[Quidway] acl 3000

[Quidway-acl-user-3000] rule deny ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255

步骤 2 配置基于用户自定义 ACL 的流分类

配置流分类 tc1，对匹配 ACL 3000 的报文进行分类。

[Quidway] traffic classifier tc1

[Quidway-classifier-tc1] if-match acl 3000

步骤 3 配置流行为

配置流行为 tb1，动作为拒绝报文通过。

[Quidway] traffic behavior tb1

[Quidway-behavior-tb1] deny

步骤 4 配置流策略

定义流策略，将流分类与流行为关联。

[Quidway] traffic policy tp1

[Quidway-trafficpolicy-tp1] classifier tc1 behavior tb1

步骤 5 在接口下应用流策略

在接口 GE1/0/1 下应用流策略。

[Quidway] interface gigabitethernet 1/0/1

[Quidway-GigabitEthernet1/0/1] traffic-policy tp1 inbound

一、ACL 简介

访问控制列表 ACL（Access Control List）是由一系列规则组成的集合，ACL 通过这些规则对报文进行分类，从而使设备可以对不同类报文进行不同的处理。

网络中的设备相互通信时，需要保障网络传输的安全可靠和性能稳定。例如：

1、防止对网络的攻击，例如 IP(Internet Protocol)报文、TCP(Transmission Control Protocol）报文、ICMP（Internet Control Message Protocol）报文的攻击。

2、对网络访问行为进行控制，例如企业网中内、外网的通信，用户访问特定网络资源的控制，特定时间段内允许对网络的访问。

3、限制网络流量和提高网络性能，例如限定网络上行、下行流量的带宽，对用户申请

的带宽进行收费，保证高带宽网络资源的充分利用。

ACL 的出现，有效地解决了上述问题，切实保障了网络传输的稳定性和可靠性。

二、ACL 原理

ACL 负责管理用户配置的所有规则，并提供报文匹配规则的算法。

1、ACL 的规则管理

每个 ACL 作为一个规则组，可以包含多个规则。

规则通过规则 ID（rule-id）来标识，规则 ID 可以由用户进行配置，也可以由系统自动根据步长生成。

一个 ACL 中所有规则均按照规则 ID 从小到大排序。

规则 ID 之间会留下一定的间隔。如果不指定规则 ID 时，具体间隔大小由“ACL 的步长”来设定。

例如步长设定为 5，ACL 规则 ID 分配是按照 5、10、15……来分配的。如果步长值是 2，自动生成的规则 ID 从 2 开始。用户可以根据规则 ID 方便地把新规则插入到规则组的某一位置。

2、ACL 的规则匹配

报文到达设备时，设备从报文中提取信息，并将该信息与 ACL 中的规则进行匹配，只要有一条规则和报文匹配，就停止查找，称为**命中规则**。查找完所有规则，如果没有符合条件的规则，称为未命中规则。

ACL 的规则分为“permit”（允许）规则和“deny”（拒绝）规则。

综上所述，ACL 可以将报文分成三类：

1、命中“permit”规则的报文

2、命中“deny”规则的报文

3、未命中规则的报文

对于这三类报文的处理方式，各个特性不同，具体请见后面详解。

3、ACL 的实现方式

目前设备支持的 ACL，有以下两种实现方式。

1、软件 ACL：

针对与本机交互的报文(必须上送 CPU 处理的报文),由软件实现来匹配报文的 ACL，比如 FTP、TFTP、Telnet、SNMP、HTTP、路由协议、组播协议中引用的 ACL。

2、硬件 ACL：

针对所有报文（一般是针对转发的数据报文），通过下发硬件 ACL 资源来匹配报文的 ACL，比如流策略、基于 ACL 的简化流策略、自反 ACL、用户组以及为接口收到的报文添加外层 Tag 功能中引用的 ACL。

软件 acl 和硬件 acl 的主要区别在于：

1、处理不同的报文类型。

2、软件 acl 前者由软件实现；硬件 acl 由硬件实现。通过软件 acl 匹配报文时，会消耗 CPU 资源，通过硬件 acl 匹配报文时则会占用硬件资源。硬件 acl 匹配报文的速度更快。

4、ACL 的分类

ACL 的类型根据不同的划分规则可以有不同的分类。例如：

按照创建 ACL 时的命名方式分为**数字型 ACL** 和**命名型 ACL**：

创建 ACL 时指定一个编号，称为**数字型 ACL**。

编号为 ACL 功能的标示。

例如 2000～2999 为基本 ACL，3000～3999 为高级 ACL。

创建 ACL 时指定一个名称，称为**命名型 ACL**。

ACL 的功能分类，请参见下表 1：

表 1 ACL 的分类

分类	适用的 IP 版本	功能介绍	说明
基本 ACL	IPv4	可使用 IPv4 报文的**源 IP 地址、分片标记和时间段信息**来定义规则。	基本 IPv4 ACL 简称基本 ACL。编号范围为 **2000～2999**。
高级 ACL	IPv4	既可使用 IPv4 报文的**源 IP 地址**，也可使用**目的地址、IP 优先级、ToS、IP 协议类型、ICMP 类型、TCP 源端口/目的端口、UDP（User Datagram Protocol）源端口/目的端口号**等来定义规则。	高级 IPv4 ACL 简称高级 ACL。编号范围为 **3000～3999**。
二层 ACL	IPv4&IPv6	可根据报文的**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、以太帧协议类型**等。	编号范围为 **4000～4999**。
用户自定义	IPv4&IPv6	可根据**偏移位置和偏移量从报文中**	编号范围为 **5000～**

ACL		**提取出一段内容**进行匹配。	**5999**。
用户 ACL	IPv4	既可使用 IPv4 报文的源 IP 地址或源 UCL（User Control List）组，也可使用目的地址或目的 UCL 组、IP 协议类型、ICMP 类型、TCP 源端口/目的端口、UDP 源端口/目的端口号等来定义规则。	编号范围为 6000～6999。
基本 ACL6	IPv6	可使用 IPv6 报文的源 IP 地址、分片标记和时间段信息来定义规则。	基本 IPv6 ACL 简称基本 ACL6。编号范围为 2000～2999。
高级 ACL6	IPv6	可以使用 IPv6 报文的源地址、目的地址、IP 承载的协议类型、针对协议的特性（例如 TCP 的源端口、目的端口、ICMPv6 协议的类型、ICMPv6 Code）等内容定义规则。	高级 IPv6 ACL 简称高级 ACL6。编号范围为 3000～3999。

基本 ACL 和基本 ACL6、高级 ACL 和高级 ACL6 对应的编号可以相同，二者互不影响。

5、ACL 的命名规则

用户在创建 ACL 时，可以为 ACL 指定一个名称，每个 ACL 最多只能有一个名称。

命名型的 ACL 使用户可以通过名称唯一地确定一个 ACL，并对其进行相应的操作。

在创建 ACL 时，用户可以选择是否配置名称。**ACL 创建后，不允许用户修改或者删除 ACL 名称，也不允许为未命名的 ACL 添加名称。**

在指定命名型 ACL 时，也可以同时配置对应编号。如果没有配置对应编号，系统在记录此命名型 ACL 时会自动为其分配一个数字型 ACL 的编号。

ACL 的名称对于 ACL 全局唯一 ,但允许基本 ACL 与基本 ACL6 ,高级 ACL 与高级 ACL6 使用相同的名称。

6、ACL 的步长

6.1、ACL 步长的含义

步长的含义：

设备自动为 ACL 规则分配编号的时候，每个相邻规则编号之间的差值。例如，如果将步长设定为 5，规则编号分配是按照 5、10、15…这样的规律分配的。

当步长改变后，ACL 中的规则编号会自动从步长值开始重新排列。例如，原来规则编号为 5、10、15、20，当通过命令把步长改为 2 后，则规则编号变成 2、4、6、8。

当使用命令将步长恢复为缺省值后，设备将立刻按照缺省步长调整 ACL 规则的编号。例如：ACL 3001，步长为 2，下面有 4 个规则，编号为 2、4、6、8。如果此时使用命令将步长恢复为缺省值 5，则 ACL 规则编号变成 5、10、15、20。

6.2、acl 步长的作用

通过设置步长，使规则之间留有一定的空间，用户可以在规则之间插入新的规则，以控制规则的匹配顺序。例如配置好了 4 个规则，规则编号为：5、10、15、20。此时如果用户希望能在第一条规则之后插入一条规则，则可以使用命令在 5 和 10 之间插入一条编号为 7 的规则。

另外，在定义一条 ACL 规则的时候，用户可以不指定规则编号，这时，系统会从步长

值开始，按照步长，自动为规则分配一个大于现有最大编号的最小编号。假设现有规则的最大编号是 25，步长是 5，那么系统分配给新定义的规则的编号将是 30。

ACL6 不支持步长设定，缺省步长为 1，但可以配置 rule-id。

7、ACL 的匹配顺序

一个 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（一条规则可以包含另一条规则，但两条规则不可能完全相同）。

华为设备支持两种匹配顺序，即**配置顺序（config）**和**自动排序（auto）**。当将一个数据包和访问控制列表的规则进行匹配的时候，**由规则的匹配顺序决定规则的优先级，ACL 通过设置规则的优先级来处理规则之间重复或矛盾的情形。**

1、配置顺序（默认顺序）

配置顺序按 ACL 规则编号（rule-id）从小到大的顺序进行匹配。

2、自动排序

自动排序（**auto**）使用“**深度优先**”的原则进行匹配。

“深度优先”即根据规则的精确度排序，匹配条件（如协议类型、源和目的 IP 地址范围等）限制越严格越精确。例如可以比较地址的通配符，通配符越小，则指定的主机的范围就越小，限制就越严格。

若“深度优先”的顺序相同，则匹配该规则时按 rule-id 从小到大排列。

通配符掩码与反向掩码类似，以点分十进制表示，并用二进制的“0”表示“匹配”，“1”表示“不关心”，这恰好与子网掩码的表示方法相反，另外通配符 1 或者 0 可以不连续，掩码与反掩码必须连续。

比如，IP 地址 192.168.1.169、通配符 0.0.0.172 表示的网址为 192.168.1.x0x0xx01，其中 x 可以是 0，也可以是 1。

ACL 规则按照“深度优先”顺序匹配的原则如下表 1 所示。

表 1 “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（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 rule-id 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（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（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 rule-id 小的优先。
二层 ACL	1. 先比较二层协议类型通配符，通配符大（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相同，则比较源 MAC 地址范围，源 MAC 地址范围小（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（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 rule-id 小的优先。
用户自定义 ACL	用户自定义 ACL 规则的匹配顺序只支持配置顺序，即 rule-id 从小到大的顺序进行匹配。
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，否则，源 IP 地址为 IP 网段的规则优先于源 IP 地址为 UCL 组的规则。 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，否则，目的 IP 地址为 IP 网段的规则优先于目的 IP 地址为 UCL 组的规则。 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 rule-id 小的优先。

8、ACL 对分片报文的支持

华为设备支持通过 ACL 对分片报文进行三层（IP 层）匹配的包过滤功能。

1、对于不包含参数 fragment（碎片）的 ACL 规则：

如果规则中包含了匹配 TCP/UDP 端口号的参数，设备仅会匹配非分片报文和首片分片报文（首片分片报文的处理方式与非分片报文相同），对首片分片后续的分片报文不作匹配处理。

如果规则中未包含匹配 TCP/UDP 端口号的参数，设备不仅会匹配非分片报文和首片分片报文，也会匹配首片分片后续的分片报文。

2、对于包含参数 fragment 的 ACL 规则，设备则仅匹配非首片分片报文。

因此，针对网络攻击者构造分片报文进行流量攻击的情况，可以配置包含参数 **fragment** 的 ACL 规则，使设备仅过滤非首片分片报文，从而避免因过滤掉其他非分片报文而影响业务的正常运行，也可防止设备因不处理非首片分片报文而达不到防范分片报文攻击的目的。

9、ACL 生效时间段

时间段用于描述一个特殊的时间范围。用户可能有这样的需求，即一些 ACL 规则需要在某个或某些特定时间内生效，而在其他时间段则不生效。

例如某单位严禁员工上班时间浏览非工作网站，下班后才允许浏览，则可以对 ACL 规则约定生效时间段。这时，用户就可以先配置一个或多个时间段，然后通过配置规则引用该时间段，从而实现基于时间段的 ACL 过滤。

如果规则引用的时间段未配置，规则不能立即生效，直到用户配置了引用的时间段，并且系统时间在指定时间段范围内，ACL 规则才能生效。

10、Pv6 ACL

IPv6 ACL 对根据配置的规则对 IPv6 报文进行分类，其实现原理和 ACL 基本相同。

IPv6 ACL 简称 ACL6。

ACL6 的分类

按 ACL6 功能不同，分类有不同，具体请参见下表，

分类	对应编号范围	应用场景

基本 ACL6	编号范围为 2000～2999。	可以使用报文的源 IPv6 地址、VPN（Virtual Private Network）实例、分片标记和时间段信息来定义规则。
高级 ACL6	编号范围为 3000～3999。	可以使用报文的源 IPv6 地址、目的 IPv6 地址、IPv6 承载的协议类型、针对协议的特性（例如 TCP 的源端口、目的端口和 ICMPv6 协议的类型、ICMPv6 Code）等内容定义规则。

ACL6 和 ACL 命令行不同，而对应的编号可以相同，二者互不影响。

三、ACL 应用

1、ACL 应用分类

ACL 应用的业务模块非常多，但主要分为以下四类：

业务分类	应用场景	涉及业务模块
登录控制	对交换机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，一般情况下交换机只允许管理员登录，非管理员用户不允许随意登	Telnet、SNMP、FTP、TFTP、SFTP、HTTP

	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。	
对转发的报文进行过滤	对转发的报文进行过滤，从而使交换机能够进一步对过滤出的报文进行丢弃、修改优先级、重定向、IPSEC 保护等处理。 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。	QoS 流策略、NAT、IPSEC
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，发现某用户向交换机发送大量的 ARP 攻击报文，造成交换机 CPU 繁忙，引发系统中断。这时就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、白名单、 用户自定义流

路由过滤	ACL 可以应用在各种动态路由协议中，对路由协议发布和接收的路由信息进行过滤。 例如，可以将 ACL 和路由策略配合使用，禁止交换机将某网段路由发给邻居路由器。	BGP、IS-IS、OSPF、OSPFv3、RIP、RIPng、组播协议

2、ACL 应用中业务模块的处理机制

各类 ACL 应用的业务模块对命中/未命中 ACL 的处理机制是各不相同的。

例如，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；但在 Telnet 中应用 ACL，这种情况下，该报文就无法正常通过了。

再如，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，其他模块却不存在这种情况。

所以，大家在配置 ACL 规则并应用到业务模块中时，一定要格外小心。

为了方便大家查阅，重庆网管博客特地将常用 ACL 业务模块的处理机制进行了整理（转自华为官方论坛）。

业务模块	匹配上了 permit 规则	匹配上了 deny 规则	ACL 中配置了规则，但未匹配上任何规则	ACL 中没有配置规则	ACL 未创建

Telnet	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	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	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	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	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	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）
流策略	流行为是 permit 时:permit（允许通过） 流行为是 deny 时：deny（丢弃报文）	deny(丢弃报文)	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）
NAT	permit(进行 NAT 转换)	permit（功能不生效，按照原	permit（功能不生效，按照原转发方式进	permit（功能不生效，按照原转发方式进	permit（功能不生效，按照原转发方式进行转发）

			转发方式进行转发）	行转发）	行转发）	
IPSEC		permit(数据流经过 IPSec 处理后再转发)	不允许出现此情况	permit（功能不生效，按照原转发方式进行转发）	不允许出现此情况	不允许出现此情况
本机防攻击策略	白名单	permit(CPU 优先处理)	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）
	黑名单	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）
	用户自定义流	用户自定义流的处理动作是 deny 时：deny(丢弃报文) 动作是 car 时：permit(进行 CAR 限	deny(丢弃报文)	permit（功能不生效，按照原转发方式进行转发）	permit（功能不生效，正常上送报文）	permit（功能不生效，正常上送报文）

		速)				
路由	Route Policy	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	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	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)

	igmp-snooping group-policy	配置了 default-permit 时：permit(允许加入组播组) 未配置 default-permit：permit(允许加入组播组)	配置了 default-permit 时：deny(禁止加入组播组) 未配置 default-permit：deny (禁止加入组播组)	配置了 default-permit 时：permit（允许加入组播组） 未配置 default-permit：deny（禁止加入组播组）	配置了 default-permit 时：permit（允许加入组播组） 未配置 default-permit：deny（禁止加入组播组）	配置了 default-permit 时：permit（允许加入组播组） 未配置 default-permit：deny（禁止加入组播组）

一、ACL 基本配置

1、ACL 规则生效时间段配置（需要先配置设备的时间，建议用 ntp 同步时间）

某些引用 ACL 的业务或功能需要限制在一定的时间范围内生效，比如，在流量高峰期时启动设备的 QoS 功能。用户可以为 ACL 创建生效时间段，通过

在规则中引用时间段信息限制 ACL 生效的时间范围，从而达到该业务或功能在一定的时间范围内生效的目的。

[Huawei]time-range test ?

<hh:mm> Starting time

from The beginning point of the time range

[Huawei]time-range test 8:00 ?

to The ending point of periodic time-range

[Huawei]time-range test 8:00 t

[Huawei]time-range test 8:00 to ?

<hh:mm> Ending Time

[Huawei]time-range test 8:00 to 18:05 ?

<0-6> Day of the week(0 is Sunday)

Fri Friday #星期五

Mon Monday #星期一

Sat Saturday #星期六

Sun Sunday #星期天

Thu Thursday # 星期四

Tue Tuesday # 星期二

Wed Wednesday #星期三

daily Every day of the week # 每天

off-day Saturday and Sunday # 星期六和星期日

working-day Monday to Friday #工作日每一天

[Huawei]time-range test from 8:00 2016/1/17 to 18:00 2016/11/17

使用同一 time-name 可以配置多条不同的时间段，以达到这样的效果：各周期时间段之间以及各绝对时间段之间分别取并集之后，再取二者的交集作为最终生效的时间范围。

例如，时间段“test”配置了三个生效时段：

从 2016 年 1 月 1 日 00:00 起到 2016 年 12 月 31 日 23:59 生效，这是一个绝对时间段。

在周一到周五每天 8:00 到 18:00 生效，这是一个周期时间段。

在周六、周日下午 14:00 到 18:00 生效，这是一个周期时间段。

则时间段“test”最终描述的时间范围为：2016 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。

由于网络延迟等原因，可能造成网络上设备时间不同步，建议配置 NTP（Network Time Protocol），以保证网络上时间的一致。

2、ACL 类型配置

2.1、数字型 acl 配置

[Huawei]acl 2000 match-order ?

auto Auto order #自动顺序（默认）

config Config order

或

[Huawei]acl number 2000 match-order ?

auto Auto order

config Config order

2.2、命名型 acl 配置

[Huawei]acl name test ?

advance Specify an advanced named ACL # 设置高级 acl

basic Specify a basic named ACL

match-order Set ACL's match order

number Specify a number for the named ACL

<cr>

[Huawei]acl name test ad

[Huawei]acl name test advance ?

match-order Set ACL's match order

number Specify a number for the named ACL

<cr>

[Huawei]acl name test number ?

  INTEGER<2000-2999>   Number of the basic named ACL

  INTEGER<42768-75535>   Number of the advanced named ACL

2.3、ACL 类型配置

[Huawei]acl ?

  INTEGER<1000-1999>   Interface access-list(add to current using rules) # 接口访问列表 acl

  INTEGER<10000-10999>   Apply MPLS ACL   # 应用 MPLS ACL

  INTEGER<2000-2999>   Basic access-list (add to current using rules) # 基本 acl

  INTEGER<3000-3999>   Advanced access-list(add to current using rules) # 高级 acl

  INTEGER<4000-4999>   MAC address access-list(add to current using rules) # 二层 acl

  ipv6   ACL IPv6   # 基本 acl6 和高级 acl6 配置

  name   Specify a named ACL

  number   Specify a numbered ACL

2.4、ACL 描述设置（可选）

[Huawei-acl-basic-2600]description ?

          TEXT

2.5、ACL 步长设置（可选）

[Huawei-acl-basic-test]step ?

  INTEGER<1-20> Specify value of step

二、ACL 类型规则配置

1、基本 ACL 规则配置

基本 ACL 编号 acl-number 的范围是 2000 ~ 2999。

基本 ACL 可以根据报文自身的**源 IP 地址、分片标记和时间段信息**对 IPv4 报文进行分类。

[Huawei-acl-basic-test]rule 1 ?

  deny Specify matched packet deny

  permit Specify matched packet permit

 [Huawei-acl-basic-test]rule 1 deny ?

  fragment-type Specify the fragment type of packet # 分组片段类型

  source Specify source address

  time-range Specify a special time

  vpn-instance Specify a VPN-Instance

  <cr>

[Huawei-acl-basic-test]rule 1 deny source ?

X.X.X.X Address of source

any Any source

[Huawei-acl-basic-test]rule 1 deny source 192.168.1.1 ?

0 Wildcard bits : 0.0.0.0 (a host)

X.X.X.X Wildcard of source

[Huawei-acl-basic-test]rule 1 deny source 192.168.1.1 0 ?

fragment-type Specify the fragment type of packet # 对分组片段类型有效

time-range Specify a special time # 引用生效时间

vpn-instance Specify a VPN-Instance # 用于 vpn

<cr>

[Huawei-acl-basic-2600]description ? #配置规则描述

TEXT ACL description (no more than 127 characters)

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，该规则将无法绑定该生效时间段。

如果不指定参数 vpn-instance vpn-instance-name，设备会对公网和私网的报文均进行匹配。

设备在收到报文时，会按照匹配顺序将报文与 ACL 规则进行逐条匹配，一旦匹配上规则组内的某条规则，则停止匹配动作。之后，设备将依据匹配的规则对报文执行相应的动作。

2、高级 ACL 规则配置

高级 ACL 编号 acl-number 的范围是 3000～3999。

高级 acl 主要**对源/目的 IP 地址、端口号、优先级、时间段等报文进行过滤。**

```
[Huawei-acl-adv-3000]rule 1 permit ?
  <1-255>   Protocol number
  gre       GRE tunneling(47)
  icmp      Internet Control Message Protocol(1)
  igmp      Internet Group Management Protocol(2)
  ip        Any IP protocol
  ipinip    IP in IP tunneling(4)
  ospf      OSPF routing protocol(89)
```

tcp Transmission Control Protocol (6)

udp User Datagram Protocol (17)

[Huawei-acl-adv-3000]rule 1 permit udp ?

destination Specify destination address

destination-port Specify destination port

dscp Specify dscp

fragment-type Specify the fragment type of packet

precedence Specify precedence

source Specify source address

source-port Specify source port

time-range Specify a special time

tos Specify tos

vpn-instance Specify a VPN-Instance

<cr>

[Huawei-acl-adv-3000]rule 1 permit udp source ?

X.X.X.X Address of source

any Any source

[Huawei-acl-adv-3000]rule 1 permit udp source any ?

destination Specify destination address

```
  destination-port   Specify destination port
  dscp               Specify dscp
  fragment-type      Specify the fragment type of packet
  precedence         Specify precedence
  source-port        Specify source port
  time-range         Specify a special time
  tos                Specify tos
  vpn-instance       Specify a VPN-Instance
  <cr>

[Huawei-acl-adv-3000]rule 1 permit udp source any des
[Huawei-acl-adv-3000]rule 1 permit udp source any destination ?
  X.X.X.X   Specify destination address
  any       Any destination IP address

[Huawei-acl-adv-3000]rule 1 permit udp source any destination
192.168.1.1 ?
  0         Wildcard bits : 0.0.0.0 ( a host )
  X.X.X.X   Wildcard of destination

[Huawei-acl-adv-3000]rule 1 permit udp source any destination
192.168.1.1 0 ?
```

destination-port Specify destination port

dscp Specify dscp

fragment-type Specify the fragment type of packet

precedence Specify precedence

source-port Specify source port

time-range Specify a special time

tos Specify tos

vpn-instance Specify a VPN-Instance

<cr>

[Huawei-acl-adv-3000]rule 1 permit udp source any destination 192.168.1.1 0 destination-port ?

eq Equal to given port number

gt Greater than given port number

lt Less than given port number

neq Not equal to given port number # 不等于指定端口

range Between two port numbers

[Huawei-acl-adv-3000]rule 1 permit udp source any destination 192.168.1.1 0 destination-port eq ?

<0-65535> Protocol number

biff Mail notify (512)

bootpc Bootstrap Protocol Client (68)

bootps Bootstrap Protocol Server (67)

discard Discard (9)

dns Domain Name Service (53)

dnsix DNSIX Security Attribute Token Map (90)

echo Echo (7)

mobilip-ag MobileIP-Agent (434)

mobilip-mn MobilIP-MN (435)

nameserver Host Name Server (42)

netbios-dgm NETBIOS Datagram Service (138)

netbios-ns NETBIOS Name Service (137)

netbios-ssn NETBIOS Session Service (139)

ntp Network Time Protocol (123)

rip Routing Information Protocol (520)

snmp SNMP (161)

snmptrap SNMPTRAP (162)

sunrpc SUN Remote Procedure Call (111)

syslog Syslog (514)

tacacs-ds TACACS-Database Service (65)

talk Talk (517)

tftp Trivial File Transfer (69)

time Time (37)

who Who(513)

xdmcp X Display Manager Control Protocol (177)

[Huawei-acl-adv-3000]rule 1 permit udp source any destination 192.168.1.1 0 destination-port eq 21 ?

dscp Specify dscp

fragment-type Specify the fragment type of packet

precedence Specify precedence

source-port Specify source port

time-range Specify a special time

tos Specify tos

vpn-instance Specify a VPN-Instance

<cr>

高级 acl 可以匹配的功能有：

2.1、高级 acl 常用协议数值对照表

协议类型	数值
ICMP	1
IGMP	2
IPinIP	4
TCP	6

UDP	17
GRE	47
IP	
OSPF	89

2.2、高级 acl 常用功能说明

参数	说明
deny	拒绝符合条件的报文
permit	允许符合条件的报文
source{sour-addr sour-wildcard|any}	sour-addr sour-wildcard:源 ip 地址　　源通配符掩码
	any：任意源 IP 地址
destination{dest-addr dest-wildcaard|any	dest-addr dest-wildcaard：目的 IP 地址及通配符掩码
	any：任意目的 IP 地址
icmp-type{icmp-name|icmp-type icmp-code}	指定 acl 规则匹配报文的 icmp 报文的类型和消息码信息，仅在报文协议是 ICMP 的情况下有效
precedence	指定 acl 匹配报文时依据**优先级**字段进行过滤。与 tos　参数一起共同构成 DSCP 组成的二选一参数。

tos	指定 acl 匹配报文时依据**服务类型**字段进行过滤。与 precedence 参数一起共同构成 DSCP 组成的二选一参数。
dscp	指定 acl 匹配报文时区分服务代码点，依据 IP 包中的 **DSCP 优先级**字段进行过滤。
tcp-flag	指定 acl 规则匹配 TCP 报文中的 SYN 标志的类型
time-range	指定 acl 规则生效时间段
destination-port{eq prot|gt port|lt port|rage port-start port end}	指定 acl 规则匹配报文的 UDP 或 TCP 的目的端口，仅在报文协议是 UDP 或 TCP 时生效。端口号可用名称或数字表示
	eq port :指定等于目的端口
	gt port:指定大于目的端口
	lt port :指定小于目的端口
	range port-start port-end:指定目的端口范围 start 为起始端口 end 为结束端口
soure-port{eq prot|gt port|lt port|rage port-start port end}	指定 acl 规则匹配报文的 UDP 或 TCP 的源端口，仅在报文协议是 UDP 或 TCP 时生效。
loging	指定 acl 匹配的报文信息进行日志记录
fragmen	指定 acl 规则是否仅对**非首片分片报文**有效，当包含此参数时仅对非首片分片报文有效。但此参数不

	能同时与 source-port、destination-port、icmp-type、tcp-flag 参数同时配置。
ttl-expired	指定 acl 是否依据数据报文中的 ttl 值是否为 1 进行过滤。启用此命令表示过滤。5700SI 及以下版本不支持。

举例：拒绝 192.168.1.0 网段与主机 61.128.128.68 进行 UDP 9090 通信

[Huawei-acl-adv-3002]rule deny udp source 192.168.1.0 0.0.0.255 destination 61.128.128.68 0. destination-port eq 9090

3、二层 ACL 规则配置

二层 ACL 编号 acl-number 的范围是 4000～4999。

二层 acl 对**源/目的 MAC、802.1p 优先级、二层协议等二层信息**进行过滤。

[Huawei-acl-L2-4000]rule 1 ?

deny Specify matched packet deny

description Specify rule description

permit Specify matched packet permit

[Huawei-acl-L2-4000]rule 1 deny source-mac 1111-1111-1111 ?

802.3 802.3 format

8021p Vlan priority

H-H-H Source MAC address mask, default is ffff-ffff-ffff

cvlan-8021p Vlan priority of inner vlan

cvlan-id Inner vlan id

destination-mac Destination-mac

double-tag Double tag

ether-ii Ethernet II format

l2-protocol Layer 2 protocol

snap Snap format

time-range Specify a special time

vlan-id Vlan id

<cr>

[Huawei-acl-L2-4000]rule 1 deny source-mac 1111-1111-1111 destination-mac ?

H-H-H Destination MAC address value

[Huawei-acl-L2-4000]rule 1 deny source-mac 1111-1111-1111 destination-mac 2222-2222-2222 ?

802.3 802.3 format

8021p Vlan priority

H-H-H Destination MAC address mask, default is ffff-ffff-ffff

cvlan-8021p Vlan priority of inner vlan

cvlan-id Inner vlan id

double-tag Double tag

ether-ii Ethernet II format

l2-protocol Layer 2 protocol

snap Snap format

time-range Specify a special time

vlan-id Vlan id

<cr>

二层 acl 支持的常用功能

二层 acl 支持的常用功能	
参数	说明
802.3	
8021p	指定 acl 规则匹配报文的外层 vlan 的 8021p 优先级
cvlan-8021p	指定 acl 规则匹配报文的内层 vlan 的 8021p 优先级
cvlan-id cvlan-id[cvlan-id-mask]	指定 acl 规则匹配报文的内层 vlan ID
	cvlan-id-mask：指定内层 ID 值的掩码 十六进制

destination-mac	指定 acl 规则匹配报文的目的 mac 地址信息
double-tag	指定 acl 匹配报文时匹配带双层 tag 的报文
ether-ii	指定 acl 规则匹配报文的帧封装格式
l2-protocol	指定 acl 规则匹配报文的链路层协议类型
snap	
source-mac	指定 acl 规则匹配报文的源 mac 地址信息
time-range	
vlan-id	指定 acl 规则匹配报文的内层 vlan ID

4、用户自定义 ACL 规则配置

用户自定义 ACL 编号 acl-number 的范围是 5000～5999。

用户自定义 acl（简称 **ucl**），可以根据用户自定义的规则对**数据报文**做出相应的处理。

用户自定义 ACL 支持的常用功能有

用户自定义 ACL 支持的常用功能

参数	说明
STRING<3-10>	
ipv4-head	指定从 ipv4 头部开始偏移
ipv6-head	从 ipv6 头部开始偏移
l2-head	从报文的二层头部开始偏移
l4-head	从四层协议头部开始偏移
time-range	

[Huawei-acl-user-5000]rule 1 deny ?

STRING<3-10> Rule string, the string must be hexadecimal and start with '0x'

ipv4-head Offset from IP(v4) head

ipv6-head Offset from IP(v6) head

l2-head Offset from l2 head

l4-head Offset from L4 head

time-range Specify a special time

<cr>

5、用户 ACL 规则配置

用户 ACL 编号 acl-number 的范围是 6000～6999。

使用 IPv4 报文的**源 IP 地址或源 UCL（User Control List）组、目的地址或目的 UCL 组、IP 协议类型、ICMP 类型、TCP 源端口/目的端口、UDP 源端口/目的端口号**等来定义规则。

具体配置及参数同前。

6、基本 ACL6 规则配置

[Huawei]acl ipv6 ?

INTEGER<2000-2999> Specify a basic ACL6

INTEGER<3000-3999> Specify an advanced ACL6

name Specify a named ACL6

number Specify a numbered ACL6

[Huawei-acl6-basic-2000]rule 1 ?

deny Specify matched packet deny

description Specify rule description

permit Specify matched packet permit

```
[Huawei-acl6-basic-2000]rule 1 deny ?
  fragment     Check fragment packet
  logging      Log matched packet
  source       Specify source address
  time-range   Specify a special time
  <cr>

[Huawei-acl6-basic-2000]rule 1 deny source ?
  X:X::X:X     IPv6 address
  X:X::X:X/M   IPv6 source address with prefix
  any          Any source IPv6 address

[Huawei-acl6-basic-2000]rule 1 deny source any ?
  fragment     Check fragment packet
  logging      Log matched packet
  time-range   Specify a special time
  <cr>
```

7、高级 ACL6 规则配置

```
[Huawei]acl ipv6 3000
[Huawei-acl6-adv-3000]rule 1 ?
```

deny Specify matched packet deny

description Specify rule description

permit Specify matched packet permit

[Huawei-acl6-adv-3000]rule 1 ?

deny Specify matched packet deny

description Specify rule description

permit Specify matched packet permit

[Huawei-acl6-adv-3000]rule 1 deny ?

<1-255> Protocol number

gre GRE tunneling(47)

icmpv6 Internet Control Message Protocol6(58)

ipv6 Any IPV6 protocol

ospf OSPF routing protocol(89)

tcp Transmission Control Protocol(6)

udp User Datagram Protocol(17)

ACL6 相关知识将在后面的 IPV6 专题详细讲解，敬请关注重庆网管博客。

8、ACL 资源告警阈值百分比设置

[Huawei] **acl threshold-alarm** { **upper-limit** *upper-limit* | **lower-limit** *lower-limit* }*

设备运行应用 ACL 的业务后会占用一部分 ACL 资源，此时可以配置 ACL 资源的告警阈值百分比。

当 ACL 资源的使用率（即设备上实际存在的 ACL 表项占设备支持的最大 ACL 表项总数的比例）等于或高于上限告警阈值百分比时，设备将会发出超限告警。之后，如果该比例又等于或小于下限告警阈值百分比，设备会再次发出告警，表明之前的超限告警情况已经恢复正常。

9、扩展 ACL 表项空间资源模式设置

<Huawei>**display resource-assign configuration**

查看接口板扩展表项空间资源的配置信息。

[Huawei] **assign resource-mode** *mode-id* **slot** *slot-id*

配置接口板扩展表项空间资源的分配模式，用来静态分配 MAC、ACL 和 FIB 表项的底层空间大小。

[Huawei] **assign acl-mode** *mode-id* **slot** *slot-id*

配置接口板 ACL 规格的资源分配模式。

缺省情况下，扩展表项空间寄存器的资源模式为 1，仅扩展 MAC 表项。

与 ACL 表项相关的分配模式包括：

1、MACACL：表示同时扩展 MAC 表项和二层 ACL 表项。

2、IPV4ACL：表示同时扩展 IPV4 的 IP 表项和 IPV4 的三层 ACL 表项。

3、IPV6ACL：表示同时扩展 IPV6 的 IP 表项和 IPV6 的三层 ACL 表项。

4、IPV4NAC：表示同时扩展 IPV4 的三层 ACL 表项和 NAC 特性专用的 ACL 表项。

5、L2 ACL：表示扩展二层 ACL 表项。

配置接口板扩展表项空间资源的分配模式后，需要重启接口板才能生效。

当设备处于核心层时，承载的业务量很大，自身的 MAC、FIB、ACL 表项也会相应增加，但是设备的表项空间有限，当设备的表项空间满足不了设备的业务要求时，会降低业务的运行效率。

设备接口板提供扩展表项空间寄存器，通过配置扩展表项空间资源的分配模式，可以选择性扩大 MAC、ACL 和 FIB 表项的底层空间大小。

三、ACL 应用配置

1、Telnent 中应用 ACL 配置

```
[Huawei]telnet server acl ?
    INTEGER<2000-2999>
```

或

```
[Huawei-ui-vty0-4]acl ?
    INTEGER<2000-3999>    Apply basic or advanced ACL
    ipv6                                Filter IPv6 addresses
```

```
[Huawei-ui-vty0-4]acl 2000 ?
    inbound      Filter login connections from the current user
interface
    outbound    Filter logout connections from the current user
interface
```

2、http 中应用 acl 配置

```
[Huawei]http acl ?
    INTEGER<2000-2999>
```

3、SNMP（v1、v2）中应用 ACL 配置

```
[Huawei]snmp-agent community write 1 acl ?
    INTEGER<2000-2999>    Apply basic ACL
```

或

```
[Huawei]snmp-agent acl ?
```

4、FTP 中应用 acl 配置

```
[Huawei]ftp acl ?
    INTEGER<2000-2999>    Apply basic ACL
```

5、TFTP 中应用 ACL 配置

```
[Huawei]tftp-server acl ?
    INTEGER<2000-2999>    Apply basic ACL
```

6、SFTP 中应用 ACL 配置

```
[Huawei]ssh server acl ?
```

或

```
[Huawei-ui-vty0-4]acl ?
    INTEGER<2000-3999>    Apply basic or advanced ACL
    ipv6                                  Filter IPv6 addresses

[Huawei-ui-vty0-4]acl 2000 ?
    inbound      Filter login connections from the current user
interface
    outbound    Filter logout connections from the current user
interface
```

7、其他方式中应用 ACL 配置表（转自华为官方论坛）

业务模块	ACL 应用方式	可使用的 ACL 编号范围
流策略	系统视图下执行命令 traffic classifier *classifier-name* [operator { and | or }]	ACL：2000～5999 ACL6：2000～3999

	[precedence*precedence-value*]，进入流分类视图。 执行命令 if-match acl { *acl-number* | *acl-name* }，配置 ACL 应用于流分类。 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。 配置流动作。报文过滤有两种流动作：deny 或 permit。 系统视图下执行命令 traffic policy *policy-name* [match-order { auto | config }]，定义流策略并进入流策略视图。 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。在系统视图、接口视图或 VLAN 视图下，执行命令 traffic-policy *policy-name* { inbound | outbound }，应用流策略。	
NAT	方式一： 系统视图下执行命令 nat address-group *group-index start-address end-address*，配置公网地址池。	2000～3999

	执行命令 interface *interface-type interface-number.subnumber*，进入子接口视图。 执行命令 nat outbound *acl-number* address-group*group-index* [no-pat]，，配置带地址池的 NAT Outbound。 方式二： 系统视图下执行命令 interface *interface-typeinterface-number.subnumber*，进入子接口视图。 执行命令 nat outbound *acl-number*，配置 Easy IP。	
IPSEC	方式一： 系统视图下执行命令 ipsec policy *policy-name seq-number* manual，创建手工方式安全策略，并进入手工方式安全策略视图。 执行命令 security acl *acl-number*，在安全策略中引用 ACL。 方式二： 系统视图下执行命令 ipsec policy *policy-name seq-number* isakmp，创建 IKE 动态协商方式安全策略，并进入 IKE 动态协商方式安全策略视图。	3000～3999

		执行命令 security acl *acl-number*，在安全策略中引用 ACL。 方式三： 系统视图下执行命令 ipsec policy-template*template-name seq-number*，创建策略模板，并进入策略模板视图。 执行命令 security acl *acl-number*，在安全策略中引用 ACL。 系统视图下执行命令 ipsec policy *policy-name seq-number* isakmp template *template-name*，在安全策略中引用策略模板。	
本机防攻击策略	白名单	系统视图下执行命令 cpu-defend policy *policy-name*，创建防攻击策略并进入防攻击策略视图。 执行命令 whitelist *whitelist-id* acl *acl-number*，创建自定义白名单。 系统视图下执行命令 cpu-defend-policy *policy-name*[global]，或槽位视图下执行命令 cpu-defend-policy*policy-name*，应用防攻击策略。	2000～4999
	黑名单	系统视图下执行命令 cpu-defend policy *policy-name*，创建防攻击策略并进入防攻击策略视图。	2000～4999

		执行命令 blacklist *blacklist-id* acl *acl-number*，创建黑名单。 系统视图下执行命令 cpu-defend-policy *policy-name*[global]，或槽位视图下执行命令 cpu-defend-policy*policy-name*，应用防攻击策略。	
	用户自定义流	系统视图下执行命令 cpu-defend policy *policy-name*，创建防攻击策略并进入防攻击策略视图。 执行命令 user-defined-flow *flow-id* acl *acl-number*，配置用户自定义流。 系统视图下执行命令 cpu-defend-policy *policy-name*[global]，或槽位视图下执行命令 cpu-defend-policy*policy-name*，应用防攻击策略。	2000～4999
路由	Route Policy	系统视图下执行命令 route-policy *route-policy-name*{ permit | deny } node *node*，创建 Route-Policy，并进入 Route-Policy 视图。 执行命令 if-match acl { *acl-number* | *acl-name* }，配置基于 ACL 的匹配规则；或者配置 apply 子句为路由策略指定动作，如执行命令 apply cost [+ | -] *cost*，设置路由的开销值等。 应用路由策略。路由协议不同，命令行不同。例如针对 OSPF 协议，可以在 OSPF 视图下，执行命令	2000～2999

		import-route { limit *limit-number* | { bgp [permit-ibgp] | direct | unr | rip [*process-id-rip*] | static |isis [*process-id-isis*] | ospf [*process-id-ospf*] } [cost *cost* | type *type* | tag *tag* | route-policy *route-policy-name*]* }，引入其他路由协议学习到的路由信息；针对 RIP 协议，可以在 RIP 视图下，执行命令 import-route { { static | direct | unr } | { { rip | ospf |isis } [*process-id*] } } [cost *cost* | route-policy*route-policy-name*] *。	
	Filter Policy	路由协议不同，过滤方向不同，命令行不同。例如针对 RIP 协议，对引入的路由进行过滤，可以在 RIP 视图下执行命令 filter-policy { *acl-number* | acl-name *acl-name* | ip-prefix *ip-prefix-name* [gateway *ip-prefix-name*] }import [*interface-type interface-number*]；对发布的路由进行过滤，可以在 RIP 视图下执行命令 filter-policy {*acl-number* | acl-name *acl-name* | ip-prefix *ip-prefix-name* } export [*protocol* [*process-id*] | *interface-typeinterface-number*] 。	2000 ~ 2999

组播	igmp-snooping ssm-policy	VLAN 视图下执行命令 igmp-snooping ssm-policy *basic-acl-number*	2000～2999
	igmp-snooping group-policy	VLAN 视图下执行命令 igmp-snooping group-policy *acl-number* [version *version-number*] [default-permit]	2000～3999

四、基于简化流策略 ACL 配置

基于 ACL 的简化流策略是指通过将报文信息与 ACL 规则进行匹配，为符合相同 ACL 规则的报文提供相同的 QoS 服务，实现对不同类型业务的差分服务。

当用户希望对进入网络的流量进行控制时，可以配置 ACL 规则根据报文的**源 IP 地址、分片标记、目的 IP 地址、源端口号、源 MAC 地址**等信息对报文进行匹配，进而配置基于 ACL 的简化流策略实现对匹配 ACL 规则的**报文过滤、流量监管、流镜像、重定向、重标记或流量统计**。

与流策略相比，基于 ACL 的简化流策略不需要单独创建流分类、流行为或流策略，配置更为简洁；但是由于仅基于 ACL 规则对报文进行匹配，因此匹配规则没有流策略丰富。

基于 ACL 的简化流策略配置时要注意:

同一接口、VLAN 或全局下配置多条简化流策略，如果其中一条简化流策略引用的 ACL 规则发生变化，会导致此视图所有简化流策略短暂失效。

如果配置 traffic-redirect 命令将流量重定向到接口时，建议 ACL 规则匹配二层流量。

1、基于 ACL 的报文过滤配置

通过配置基于 ACL 的报文过滤，对匹配 ACL 规则**报文进行禁止/允许动作，进而实现对网络流量的控制。**

可以根据以下原则选用 traffic-filter 或 traffic-secure 命令配置报文过滤：

如果 traffic-filter 或 traffic-secure 关联的 ACL 没有同时被其他基于 ACL 的简化流策略所关联（即两个简化流策略关联的不是同一个 acl），且报文不会同时匹配报文过滤和其他简化流策略关联的 ACL 规则时，traffic-filter 和 traffic-secure 可以任选其一。

如果 traffic-filter 或 traffic-secure 关联的 ACL 同时被其他基于 ACL 的简化流策略所关联，或者报文同时匹配了报文过滤和其他简化流策略关联的 ACL 时，traffic-filter 和 traffic-secure 的区别如下：

当 traffic-secure 和其他基于 ACL 的简化流策略同时配置，且 ACL 规则中的动作为 Deny 时，仅 traffic-secure、traffic-mirror（流量镜像）和 traffic-statistics（流量统计）命令生效（即 traffic-secure 等命令配置的应用不生效），报文被过滤。

当 traffic-secure 和其他基于 ACL 的简化流策略同时配置，且 ACL 规则中的动作为 Permit 时，traffic-secure 命令和其他基于 ACL 的简化流策略均生效。

当 traffic-filter 和其他基于 ACL 的简化流策略同时配置，且 ACL 规则中的动作为 Deny 时，仅 traffic-filter、traffic-mirror 和 traffic-statistics 命令生效，报文被过滤。

当 traffic-filter 和其他基于 ACL 的简化流策略同时配置，且 ACL 规则中的动作为 Permit 时，先配置的简化流策略生效。

具体配置

1.1、在全局或 VLAN 上配置基于简化流策略 ACL 报文过滤

```
[Huawei]traffic-filter ?
  inbound     Apply the acl on inbound packets
  outbound    Apply the acl on outbound packets
  vlan            Virtual LAN

 [Huawei]traffic-filter vlan ?
  INTEGER<1-4094>   VLAN ID

[Huawei]traffic-filter vlan 2 ?
  inbound     Apply the acl on inbound packets
  outbound    Apply the acl on outbound packets
```

```
[Huawei]traffic-filter vlan 2 outbound ?
  acl   Specify ACL to match

 [Huawei]traffic-filter vlan 2 outbound acl ?
  INTEGER<2000-2999>   Basic access-list
  INTEGER<3000-3999>   Advanced access-list
  INTEGER<4000-4999>   L2 access-list
  ipv6                                Specify IPv6
  name                                Specify a named ACL

[Huawei]traffic-filter vlan 2 outbound acl 3000 ?
  rule   Specify the ID of acl rule
  <cr>

 [Huawei]traffic-filter vlan 2 outbound acl 3000 rule ?
  INTEGER<0-4294967294>   ID of acl rule
```

或

[Huawei]**traffic-secure** [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

1.2、在接口上配置基于简化流策略 ACL 报文过滤

```
[Huawei-GigabitEthernet0/0/2]traffic-filter ?
```

```
  inbound     Apply the acl on inbound packets
  outbound    Apply the acl on outbound packets

[Huawei-GigabitEthernet0/0/2]traffic-filter outbound ?
  acl    Specify ACL to match

[Huawei-GigabitEthernet0/0/2]traffic-filter outbound acl ?
  INTEGER<2000-2999>   Basic access-list
  INTEGER<3000-3999>   Advanced access-list
  INTEGER<4000-4999>   L2 access-list
  ipv6                 Specify IPv6
  name                 Specify a named ACL

[Huawei-GigabitEthernet0/0/2]traffic-filter outbound acl 3000 ?
  rule   Specify the ID of acl rule
  <cr>

[Huawei-GigabitEthernet0/0/2]traffic-filter outbound acl 3000 rule ?
  INTEGER<0-4294967294>   ID of acl rule
```

或

[Huawei-GigabitEthernet0/0/2]**traffic-secure inbound acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

基于 ACL 报文过滤 traffic-filter 和 traffic-secure 命令参数说明

参数	说明
vlan *vlan-id*	
inbound	在入方向应用报文过滤
outbound	在出方向应用报文过滤
bas-acl	基本 acl
adv-acl	高级 acl
l2-acl	二层 acl
user-acl	用户 acl
vlan	可选，在特定 vlan 上应用基于 acl 的报文过滤
acl	基于 ipv4 acl 对报文过滤
ipv6	基于 ipv6 acl 对报文进行过滤
name	采用基于命名型 acl 进行报文过滤
rule	基于 acl 中特定规则进行报文过滤

2、基于 ACL 的流量监管配置

通过配置基于 ACL 的流量监管，对匹配 ACL 规则的**报文进行限速**。

2.1、在全局或 VLAN 上配置基于简化流策略 ACL 流量监管

```
[Huawei]traffic-limit ?
  inbound     Apply the acl on inbound packets
  outbound    Apply the acl on outbound packets
  vlan            Virtual LAN

[Huawei]traffic-limit vlan 3 ?
  inbound     Apply the acl on inbound packets
  outbound    Apply the acl on outbound packets

[Huawei]traffic-limit vlan 3 outbound ?
  acl    Specify ACL to match

[Huawei]traffic-limit vlan 3 outbound acl ?
  INTEGER<2000-2999>   Basic access-list
  INTEGER<3000-3999>   Advanced access-list
  INTEGER<4000-4999>   L2 access-list
  ipv6                                Specify IPv6
  name                                Specify a named ACL

[Huawei]traffic-limit vlan 3 outbound acl 2000 ?
  cir     Committed information rate
  rule    Specify the ID of acl rule
```

```
[Huawei]traffic-limit vlan 3 outbound acl 2000 cir ?
  INTEGER<8-10000000>  Value of CIR (Unit: Kbps)

[Huawei]traffic-limit vlan 3 outbound acl 2000 cir 10240 ?
  cbs          Committed burst size
  green        Specify behavior conducted when rate no higher than CIR
  pir          Peak information rate
  red          Specify behavior conducted when rate higher than PIR
  yellow       Specify behavior conducted when rate higher than CIR, no
higher than
                PIR
  <cr>
```

2.2、在接口上配置基于简化流策略 ACL 流量监管

命令与在全局或 VLAN 上配置基于简化流策略 ACL 流量监管类似，只是需要在接口视图下配置。

基于 ACL 的流量监管配置主要参数说明

参数	说明
vlan	
inbound	
outbound	

……	同上面基于 acl 的报文过滤参数
cir cir-value	承诺信息速率，即保证能够通过的评价速率
pir	峰值信息速率，即能够通过的最大速率
cbs	承诺突发尺寸，即瞬间能够通过的承若突发流量
pbs	峰值突发尺寸，即瞬间能够通过的峰值突发流量
gree	对绿色报文进行监管，默认允许通过
yellow	对黄色报文进行监管，默认允许通过
red	对红色报文进行监管，默认被丢弃
remark *8021P-value*	指定重标记报文的 8021P 优先级
remark *dscp-value*	指定重标记报文 DSCP 优先级
drop	指定丢弃报文
pass	指定允许报文通过

3、基于 ACL 报文的重定向配置

通过配置基于 ACL 的重定向，将匹配 ACL 规则的报文**重定向到 CPU、指定接口或指定下一跳地址**。

3.1、在全局或 VLAN 上配置基于 ACL 重定向

```
[Huawei]traffic-redirect ?
    inbound    Apply the acl on inbound packets
    vlan           Virtual LAN
```

```
[Huawei]traffic-redirect vlan ?
    INTEGER<1-4094>    VLAN ID

[Huawei]traffic-redirect vlan 5 ?
    inbound    Apply the acl on inbound packets

[Huawei]traffic-redirect vlan 5 inbound ?
    acl    Specify ACL to match

[Huawei]traffic-redirect vlan 5 inbound acl ?
    INTEGER<2000-2999>    Basic access-list
    INTEGER<3000-3999>    Advanced access-list
    INTEGER<4000-4999>    L2 access-list
    INTEGER<5000-5999>    User-defined access-list
    ipv6                                  Specify IPv6
    name                                  Specify a named ACL

[Huawei]traffic-redirect vlan 5 inbound acl 3000 ?
    cpu                       Redirect to CPU
    interface           Specify the interface
    ip-nexthop        Specify the nexthop IP
```

ipv6-nexthop Specify the nexthop IPv6

rule Specify the ID of acl rule

3.2、在接口上配置基于 ACL 重定向

配置命令与在全局或 VLAN 上配置基于 ACL 重定向类似，不同之处 是在接口视图下配置。

基于 acl 报文重定向参数说明

参数	说明
vlan	
……	
cpu	指定将报文重定向到 CPU
interface	指定将报文重定向到接口
ip-nexthop	指定将报文重定向到下一跳 ipv4 地址
ipv6-nexthop	指定将报文重定向到下一跳 ipv6 地址

4、基于 ACL 报文的重标记配置

通过配置基于 ACL 的重标记，对匹配指定 ACL 规则的报文，重标记其**优先级**，如 VLAN 报文中的 802.1p、MAC 地址，IP 报文中的 DSCP 等。

4.1、在全局或 VLAN 上配置基于 acl 报文重标记

[Huawei]traffic-remark ?

inbound Apply the acl on inbound packets

outbound Apply the acl on outbound packets

```
    vlan            Virtual LAN


[Huawei]traffic-remark outbound ?
    acl    Specify ACL to match


[Huawei]traffic-remark outbound acl ?
    INTEGER<2000-2999>    Basic access-list
    INTEGER<3000-3999>    Advanced access-list
    INTEGER<4000-4999>    L2 access-list
    ipv6                                Specify IPv6
    name                                Specify a named ACL


[Huawei]traffic-remark outbound acl 2000 ?
    8021p          Remark 802.1p
    cvlan-id    Remark cvlan id
    dscp            Remark DSCP (DiffServ CodePoint)
    rule            Specify the ID of acl rule
    vlan-id      Remark vlan id
```

4.2、在接口上配置基于 ACL 报文重标记

命令与在全局或 VLAN 上配置基于 acl 报文重标记类似，不同之处是在接口视图下配置。

基于 ACL 报文重标记配置命令说明

参数	说明
vlan	
……	
8021p	指定重标记报文的 8021P 优先级
cvlan-id	指定重标记 QinQ 报文中的内层 vlan 标签
destination-mac	指定重标记报文的目的 MAC 地址
DSCP	指定重标记报文的 DSCP 的服务类型
local-precedence	指定重标记报文的本地优先级
ip-precednce	指定重标记报文的本地优先级
vlan	重标记后的 vlan 编号

5、基于 ACL 的流量统计配置

通过配置基于 ACL 的流量统计，对匹配指定 ACL 规则的报文进行流量统计。

5.1、在全局或 VLAN 上配置基于 acl 报文流量统计

```
[Huawei]traffic-statistic ?

    inbound       Apply the acl on inbound packets

    outbound     Apply the acl on outbound packets

    vlan              Virtual LAN


[Huawei]traffic-statistic inbound ?

    acl     Specify ACL to match
```

```
[Huawei]traffic-statistic inbound acl ?
    INTEGER<2000-2999>    Basic access-list
    INTEGER<3000-3999>    Advanced access-list
    INTEGER<4000-4999>    L2 access-list
    INTEGER<5000-5999>    User-defined access-list
    ipv6                                Specify IPv6
    name                                Specify a named ACL

[Huawei]traffic-statistic inbound acl 3000 ?
    by-bytes    Statistics by bytes
    rule            Specify the ID of acl rule
    <cr>

[Huawei]t raffic-statistic inbound acl 3000 by-bytes ?
    <cr>

[Huawei]traffic-statistic inbound acl 3000 rule ?
    INTEGER<0-4294967294>    ID of acl rule

[Huawei]traffic-statistic inbound acl 3000 rule 1 ?
    by-bytes    Statistics by bytes
```

<cr>

[Huawei]traffic-statistic inbound acl 3000 rule 1 by-bytes ?

<cr>

5.2、在接口上配置流量统计配置基于 acl 报文流量统计

配置命令与在全局或 VLAN 上配置基于 acl 报文流量统计类似，不同之处在于在接口视图下配置。

基于 acl 报文流量统计参数说明

参数	说明
vlan	
……	
by-byes	按照字节数量统计。默认按照报文数据（packets）统计

6、基于 ACL 的流镜像配置

通过配置基于 ACL 的流镜像，将匹配 ACL 规则的报文镜像到指定接口，以便于对报文进行分析。

6.1、在全局或 VLAN 上配置基于 ACL 的流镜像

[Huawei]traffic-mirror ?

inbound Apply the acl on inbound packets

vlan Virtual LAN

```
[Huawei]traffic-mirror inbound ?
    acl    Specify ACL to match

[Huawei]traffic-mirror inbound acl ?
    INTEGER<2000-2999>    Basic access-list
    INTEGER<3000-3999>    Advanced access-list
    INTEGER<4000-4999>    L2 access-list
    INTEGER<5000-5999>    User-defined access-list
    ipv6                                Specify IPv6
    name                                Specify a named ACL

[Huawei]traffic-mirror inbound acl 2000 ?
    rule    Specify the ID of acl rule
    to        Mirror to

[Huawei]traffic-mirror inbound acl 2000 rule ?
    INTEGER<0-4294967294>    ID of acl rule

[Huawei]traffic-mirror inbound acl 2000 rule 2 ?
    to    Mirror to

[Huawei]traffic-mirror inbound acl 2000 rule 2 to ?
```

```
    observe-port    Observe port

[Huawei]traffic-mirror inbound acl 2000 rule 2 to observe-port ?
    INTEGER<1-2>    The index of observe port

[Huawei]traffic-mirror inbound acl 2000 rule 2 to observe-port 1 ?
    <cr>
```

6.2、在接口上配置流镜像配置基于 ACL 的流镜像

命令与在全局或 VLAN 上配置基于 ACL 的流镜像类似，不同之处在于需在接口视图下配置。