H3C SR8800-F 核心路由器

ACL 和 QoS 命令参考

杭州华三通信技术有限公司
http://www.h3c.com.cn

资料版本：6W710-20141119
产品版本：SR8800-CMW710-R7143

前 言

H3C SR8800-F 核心路由器命令参考共分为十四本手册，介绍了 SR8800-F 核心路由器各软件特性的配置命令行，包括每条命令对应的视图、参数、缺省用户角色、使用指导、举例等。《ACL 和 QoS 命令参考》主要介绍 ACL（Access Control List，访问控制列表）和 QoS（Quality of Service，服务质量）的配置命令，包括 IPv4 ACL、IPv6 ACL、QoS 策略、优先级映射、拥塞管理等。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 端口编号示例约定

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

产品配套资料

H3C SR8800-F 核心路由器的配套资料包括如下部分：

大类	资料名称	内容介绍
产品知识介绍	产品彩页	帮助您了解SR8800-F的主要规格参数及亮点
	单板datasheet	帮助您了解SR8800-F的单板属性、特点、支持的标准等
硬件描述与安装	安全兼容性手册	列出SR8800-F的兼容性声明，并对兼容性和安全的细节进行说明
	安装指导	帮助您详细了解SR8800-F的硬件规格和安装方法，指导您对SR8800-F进行安装
	H3C光模块手册	帮助您详细了解SR8800-F设备支持的光模块的类型、外观与规格等内容
业务配置	配置指导	帮助您掌握SR8800-F软件功能的配置方法及配置步骤
	命令参考	详细介绍SR8800-F的命令，相当于命令字典，方便您查阅各个命令的功能
	典型配置举例	帮助您了解产品的典型应用和推荐配置，从组网需求、组网图、配置步骤几方面进行介绍
运行维护	故障处理	帮助您了解在使用SR8800-F过程中碰到困难或者问题的处理方法
	用户FAQ	以问答的形式，帮助您了解SR8800-F的一些软硬件特性及规格等问题
	日志手册	对SR8800-F的系统日志（System Log）消息进行介绍，主要用于指导您理解相关信息的含义，并做出正确的操作
	告警手册	对SR8800-F的告警（Trap）消息进行介绍，主要用于指导您理解相关信息的含义，并做出正确的操作
	MIB Companion	与软件版本配套的MIB Companion
	版本说明书	帮助您了解SR8800-F产品版本的相关信息（包括：版本配套说明、兼容性说明、特性变更说明、技术支持信息）及软件升级方法

资料获取方式

您可以通过H3C网站（www.h3c.com.cn）获取最新的产品资料：

H3C 网站与产品资料相关的主要栏目介绍如下：

- [服务支持/文档中心]：可以获取硬件安装类、软件升级类、配置类或维护类等产品资料。
- [产品技术]：可以获取产品介绍和技术介绍的文档，包括产品相关介绍、技术介绍、技术白皮书等。
- [解决方案]：可以获取解决方案类资料。
- [服务支持/软件下载]：可以获取与软件版本配套的资料。

技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

网址：http://www.h3c.com.cn

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 ACL

说明

本文中的“CSPC 单板”指的是单板丝印以“CSPC”开头（如 CSPC-GP48LB）的单板。

1.1 ACL配置命令

1.1.1 acl

acl 命令用来创建一个 ACL，并进入相应的 ACL 视图。

undo acl 命令用来删除指定或全部 ACL。

【命令】

acl [**ipv6**] **number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

undo acl [**ipv6**] { **all** | **name** *acl-name* | **number** *acl-number* }

【缺省情况】

不存在任何 ACL。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

number *acl-number*：指定 ACL 的编号。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

name *acl-name*：指定 ACL 的名称。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。

match-order { **auto** | **config** }：指定规则的匹配顺序，**auto** 表示按照自动排序（即“深度优先”原则）的顺序进行规则匹配，**config** 表示按照配置顺序即 ACL 的编号顺序进行规则匹配。缺省情况下，规则的匹配顺序为配置顺序。

all：指定全部 ACL。若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL。

【使用指导】

- 使用 **acl** 命令时，如果指定编号的 ACL 不存在，则创建该 ACL 并进入其视图，否则直接进入其视图。
- ACL 的名称只能在创建时设置。ACL 一旦创建，便不允许再修改或删除其原有名称。
- 当 ACL 内不存在任何规则时，用户可以使用本命令对该 ACL 的规则匹配顺序进行修改，否则不允许进行修改。

【举例】

创建一个编号为 2000 的 IPv4 基本 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

创建一个编号为 2001 的 IPv4 基本 ACL，指定其名称为 flow，并进入其视图。

```
<Sysname> system-view
[Sysname] acl number 2001 name flow
[Sysname-acl-basic-2001-flow]
```

【相关命令】

- **display acl**

1.1.2 acl copy

acl copy 命令用来复制并生成一个新的 ACL。

【命令】

acl [**ipv6**] **copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

source-acl-number：指定源 ACL 的编号，该 ACL 必须存在。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

name *source-acl-name*：指定源 ACL 的名称，该 ACL 必须存在。*source-acl-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

dest-acl-number：指定目的 ACL 的编号，该 ACL 必须不存在。若未指定本参数，系统将为目的 ACL 自动分配一个与源 ACL 类型相同且可用的最小编号。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

name *dest-acl-name*：指定目的 ACL 的名称，该 ACL 必须不存在。*dest-acl-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，ACL 的名称不允许使用英文单词 all。若未指定本参数，系统将不会为目的 ACL 设置名称。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

【使用指导】

- 目的 ACL 的类型要与源 ACL 的类型相同。
- 目的 ACL 的名称只能在复制时设置。目的 ACL 一旦生成，便不允许再修改或删除其原有名称。
- 除了 ACL 的编号和名称不同外，新生成的 ACL（即目的 ACL）的匹配顺序、规则匹配统计功能的使能情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 ACL 的相同。

【举例】

通过复制已存在的 IPv4 基本 ACL 2001，来生成一个新的编号为 2002 的同类型 ACL。

```
<Sysname> system-view
[Sysname] acl copy 2001 to 2002
```

1.1.3 acl logging interval

acl logging interval 命令用来配置报文过滤日志的生成与发送周期，设备将周期性地生成并发送报文过滤的日志信息，包括该周期内被匹配的报文数量以及所使用的 ACL 规则。

undo acl logging interval 命令用来恢复缺省情况。

【命令】

acl [**ipv6**] **logging interval** *interval*

undo acl [**ipv6**] **logging interval**

【缺省情况】

报文过滤日志的生成与发送周期为 0 分钟，即不记录报文过滤的日志。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

interval：若未指定 **ipv6** 关键字，表示 IPv4 报文过滤日志的生成与发送周期，否则表示 IPv6 报文过滤日志的生成与发送周期。取值范围为 0～1440，且必须为 5 的整数倍，0 表示不进行记录，单位为分钟。

【使用指导】

系统只支持对应用 IPv4 基本 ACL、IPv4 高级 ACL、IPv6 基本 ACL 或 IPv6 高级 ACL 进行报文过滤的日志进行记录，且在上述 ACL 中配置规则时必须指定 **logging** 参数。

【举例】

配置 IPv4 报文过滤日志的生成与发送周期为 10 分钟。

```
<Sysname> system-view
[Sysname] acl logging interval 10
```

【相关命令】

- **rule** (IPv4 advanced ACL view)
- **rule** (IPv4 basic ACL view)
- **rule** (IPv6 advanced ACL view)
- **rule** (IPv6 basic ACL view)

1.1.4 acl name

acl name 命令用来进入指定名称的 ACL 视图。

【命令】

acl [**ipv6**] **name** *acl-name*

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

acl-name：指定 ACL 的名称，该 ACL 必须存在。*acl-name* 为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

【举例】

进入已存在的、名称为 flow 的 IPv4 基本 ACL 的视图。

```
<Sysname> system-view
[Sysname] acl name flow
[Sysname-acl-basic-2001-flow]
```

进入已存在的、名称为 flow 的 IPv6 基本 ACL 的视图。

```
<Sysname> system-view
[Sysname] acl ipv6 name flow
```

```
[Sysname-acl6-basic-2001-flow]
```

【相关命令】

- **acl**

1.1.5 description

description 命令用来配置 ACL 的描述信息。

undo description 命令用来删除 ACL 的描述信息。

【命令】

description *text*

undo description

【缺省情况】

ACL 没有任何描述信息。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图/IPv6 基本 ACL 视图/IPv6 高级 ACL 视图/二层 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

text：表示 ACL 的描述信息，为 1～127 个字符的字符串，区分大小写。

【举例】

为 IPv4 基本 ACL 2000 配置描述信息。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] description This is an IPv4 basic ACL.
```

【相关命令】

- **display acl**

1.1.6 display acl

display acl 命令用来显示 ACL 的配置和运行情况。

【命令】

display acl [**ipv6**] { *acl-number* | **all** | **name** *acl-name* }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

acl-number：显示指定编号的 ACL 的配置和运行情况。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

all：显示全部 ACL 的配置和运行情况。若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL。

name *acl-name*：显示指定名称的 ACL 的配置和运行情况。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

【使用指导】

本命令将按照实际匹配顺序来排列 ACL 内的规则，即：当 ACL 的规则匹配顺序为配置顺序时，各规则将按照编号由小到大排列；当 ACL 的规则匹配顺序为自动排序时，各规则将按照“深度优先”原则由深到浅排列。

【举例】

显示 IPv4 基本 ACL 2001 的配置和运行情况。

```
<Sysname> display acl 2001
Basic ACL  2001, named flow, 1 rule, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5
 rule 5 permit source 1.1.1.1 0
 rule 5 comment This rule is used on GigabitEthernet 3/0/1
```

表1-1 display acl 命令显示信息描述表

字段	描述
Basic ACL 2001	该ACL的类型和编号，ACL的类型包括： • Basic ACL：表示 IPv4 基本 ACL • Advanced ACL：表示 IPv4 高级 ACL • Basic IPv6 ACL：表示 IPv6 基本 ACL • Advanced IPv6 ACL：表示 IPv6 高级 ACL • Ethernet frame ACL：表示二层 ACL
named flow	该ACL的名称为flow，-none-表示没有名称
1 rule	该ACL内包含的规则数量
match-order is auto	该ACL的规则匹配顺序为自动排序（匹配顺序为配置顺序时不显示本字段）
This is an IPv4 basic ACL.	该ACL的描述信息

字段	描述
ACL's step is 5	该ACL的规则编号的步长值为5
rule 5 permit source 1.1.1.1 0	规则5的具体内容，源地址为具体地址
rule 5 comment This rule is used on GigabitEthernet 3/0/1.	规则5的描述信息

1.1.7 display packet-filter

display packet-filter 命令用来显示 ACL 在报文过滤中的应用情况。

【命令】

display packet-filter { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | { **global** | **interface vlan-interface** *vlan-interface-number* } [**inbound** | **outbound**] [**slot** *slot-number*] }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

global：显示 ACL 在报文过滤中的全局（即所有物理接口）应用情况。

interface [*interface-type interface-number*]：显示指定接口上 ACL 在报文过滤中的应用情况。*interface-type interface-number* 表示接口类型和接口编号，这里的接口类型不包括 VLAN 接口。若未指定接口类型和接口编号，将显示除 VLAN 接口以外的所有接口上 ACL 在报文过滤中的应用情况。

interface vlan-interface *vlan-interface-number*：显示指定 VLAN 接口上 ACL 在报文过滤中的应用情况。*vlan-interface-number* 表示 VLAN 接口的编号。

inbound：显示入方向上 ACL 在报文过滤中的应用情况。

outbound：显示出方向上 ACL 在报文过滤中的应用情况。

slot *slot-number*：显示指定单板上 ACL 在报文过滤中的应用情况，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示主用主控板上 ACL 在报文过滤中的应用情况。

【使用指导】

若未指定 **inbound** 和 **outbound** 参数，将同时显示出、入方向上 ACL 在报文过滤中的应用情况。

【举例】

显示接口 GigabitEthernet3/0/1 入方向上 ACL 在报文过滤中的应用情况。

```
<Sysname> display packet-filter interface gigabitethernet 3/0/1 inbound
Interface: GigabitEthernet3/0/1
```

```
In-bound policy:
  ACL 2003, Hardware-count
  Default action: Deny
```

表1-2 display packet-filter 命令显示信息描述表

字段	描述
Interface	ACL在指定接口上的应用情况
In-bound policy	ACL在入方向上的应用情况
Out-bound policy	ACL在出方向上的应用情况
ACL 2003	IPv4基本ACL 2003应用成功
Hardware-count	规则匹配统计功能应用成功
Default action	报文过滤缺省动作，即对未匹配ACL的报文所采取的动作，Deny表示拒绝通过。如缺省过滤动作为允许通过，则不显示该字段。

1.1.8 display packet-filter statistics

display packet-filter statistics 命令用来显示 ACL 在报文过滤中应用的统计信息以及报文过滤缺省动作的统计信息。

【命令】

display packet-filter statistics { **global** | **interface** *interface-type interface-number* } { **inbound** | **outbound** } [[**ipv6**] { *acl-number* | **name** *acl-name* }] [**brief**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

global：显示全局（即所有物理接口）统计信息。

interface *interface-type interface-number*：显示指定接口上的统计信息。*interface-type interface-number* 表示接口类型和接口编号。

inbound：显示入方向上的统计信息。

outbound：显示出方向上的统计信息。

default：显示报文过滤缺省动作的统计信息。

acl-number：显示指定编号 ACL 在报文过滤中应用的统计信息。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。

- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

name *acl-name*：显示指定名称 ACL 在报文过滤中应用的统计信息。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

brief：显示简要统计信息。

【使用指导】

若未指定 **default**、*acl-number* 和 **name** *acl-name* 参数，将显示全部 ACL（若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL）在报文过滤中应用的统计信息以及报文过滤缺省动作的统计信息。

【举例】

显示接口 GigabitEthernet3/0/1 入方向上全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL）在报文过滤中应用的统计信息。

```
<Sysname> display packet-filter statistics interface gigabitethernet 3/0/1 inbound
Interface: GigabitEthernet3/0/1
In-bound policy:
  ACL 2001, Hardware-count
   From 2012-11-16 09:07:29 to 2012-11-16 09:14:03
   rule 0 permit
   Totally 0 packets, 0% permitted
   Totally 0 packets, 0% denied

  Default action: Deny
```

表1-3 display packet-filter statistics 命令显示信息描述表

字段	描述
Interface	在指定接口上应用的统计信息
In-bound policy	在入方向上应用的统计信息
Out-bound policy	在出方向上应用的统计信息
ACL 2001	IPv4基本ACL 2001应用成功
Hardware-count	规则匹配统计功能应用成功
From 2012-11-16 09:07:29 to 2012-11-16 09:14:03	该统计的起始和终止时间
Totally 0 packets, 0% permitted	该ACL允许符合条件报文的个数和通过率
Totally 0 packets, 0% denied	该ACL拒绝符合条件报文的个数和丢弃率
Default action	报文过滤缺省动作，即对未匹配ACL的报文所采取的动作，Deny表示拒绝通过。如缺省过滤动作为允许通过，则不显示该字段

【相关命令】

- **reset packet-filter statistics**

1.1.9 display packet-filter statistics sum

display packet-filter statistics sum 命令用来显示 ACL 在报文过滤中应用的累加统计信息。

【命令】

display packet-filter statistics sum { **inbound** | **outbound** } [**ipv6**] { *acl-number* | **name** *acl-name* } [**brief**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

inbound：显示入方向上 ACL 在报文过滤中应用的累加统计信息。

outbound：显示出方向上 ACL 在报文过滤中应用的累加统计信息。

acl-number：显示指定编号 ACL 在报文过滤中应用的累加统计信息。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

name *acl-name*：显示指定名称 ACL 在报文过滤中应用的累加统计信息。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

brief：显示 ACL 在报文过滤中应用的简要累加统计信息。

【举例】

显示入方向上 IPv4 基本 ACL 2001 在报文过滤中应用的累加统计信息。

```
<Sysname> display packet-filter statistics sum inbound 2001
Sum:
 In-bound policy:
  ACL 2001
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

表1-4 display packet-filter statistics sum 命令显示信息描述表

字段	描述
Sum	ACL在报文过滤中应用的累加统计信息
In-bound policy	ACL在入方向上应用的累加统计信息
Out-bound policy	ACL在出方向上应用的累加统计信息
ACL 2001	IPv4基本ACL 2001应用的累加统计信息
2 packets	该规则匹配了2个包（当匹配的包个数为0时不显示本字段）
Totally 2 packets, 100% permitted	该ACL允许符合条件报文的个数和通过率
Totally 0 packets, 0% denied	该ACL拒绝符合条件报文的个数和丢弃率

【相关命令】

- **reset packet-filter statistics**

1.1.10 display packet-filter verbose

display packet-filter verbose 命令用来显示 ACL 在报文过滤中的详细应用情况。

【命令】

display packet-filter verbose { **global** | **interface** *interface-type interface-number* } { **inbound** | **outbound** } [[**ipv6**] { *acl-number* | **name** *acl-name* }] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

global：显示 ACL 在报文过滤中的全局（即所有物理接口）详细应用情况。

interface *interface-type interface-number*：显示指定接口上 ACL 在报文过滤中的详细应用情况。*interface-type interface-number* 表示接口类型和接口编号。

inbound：显示入方向上 ACL 在报文过滤中的详细应用情况。

outbound：显示出方向上 ACL 在报文过滤中的详细应用情况。

acl-number：显示指定编号 ACL 在报文过滤中的详细应用情况。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

name *acl-name*：显示指定名称 ACL 在报文过滤中的详细应用情况。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

slot *slot-number*：显示指定单板上 ACL 在报文过滤中的详细应用情况，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示主用主控板上 ACL 在报文过滤中的详细应用情况。

【使用指导】

若未指定 *acl-number* 和 **name** *acl-name* 参数，将显示全部 ACL（若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL）在报文过滤中的详细应用情况。

【举例】

显示接口 GigabitEthernet3/0/1 入方向上全部 ACL（包括 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL）在报文过滤中的详细应用情况。

```
<Sysname> display packet-filter verbose interface gigabitethernet 3/0/1 inbound
Interface: GigabitEthernet3/0/1
In-bound policy:
  ACL 2001, Hardware-count
   rule 0 permit source 2.2.2.2 0
   rule 5 permit source 1.1.1.1 0

  Default action: Deny
```

表1-5 display packet-filter verbose 命令显示信息描述表

字段	描述
Interface	ACL在指定接口上的详细应用情况
In-bound policy	ACL在入方向上的详细应用情况
Out-bound policy	ACL在出方向上的详细应用情况
ACL 2001	IPv4基本ACL 2001应用成功
Hardware-count	规则匹配统计功能应用成功
Default action	报文过滤缺省动作，即对未匹配ACL的报文所采取的动作，Deny表示拒绝通过。如缺省过滤动作为允许通过，则不显示该字段

1.1.11 display qos-acl resource

display qos-acl resource 命令用来显示 QoS 和 ACL 资源的使用情况。

【命令】

display qos-acl resource [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

slot *slot-number*：显示指定单板上 QoS 和 ACL 资源的使用情况，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示所有单板上 QoS 和 ACL 资源的使用情况。

【举例】

显示 QoS 和 ACL 资源的使用情况。

```
<Sysname> display qos-acl resource
Interfaces: GE2/0/1 to GE2/0/24, XGE2/0/25 to XGE2/0/26
-------------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
 IPv4Acl          65536      0          0          65536      0%
 IPv6Acl          16384      0          0          16384      0%
 Car&Cnt          32768      0          0          32768      0%
 InBRASCar        65536      0          5138       60398      7%
 OutBRASCar       65536      0          5142       60394      7%
 TCPCar           16384      0          5151       11233      31%
 CarProf          220        0          4          216        1%
 Sampler          32768      0          0          32768      0%
```

表1-6 display qos-acl resource 命令显示信息描述表

字段	描述
Interfaces	资源对应的接口范围
Type	资源类型
Total	资源总数
Reserved	预留的资源数
Configured	已经配置的资源数
Remaining	剩余可用的资源数
Usage	已使用资源的百分比

1.1.12 packet-filter

packet-filter 命令用来在接口上应用 ACL 进行报文过滤。

undo packet-filter 命令用来取消在接口上应用 ACL 进行报文过滤。

【命令】

packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [**hardware-count**]

undo packet-filter [**ipv6**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

【缺省情况】

接口不对报文进行过滤。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

acl-number：指定 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

name *acl-name*：指定 ACL 的名称。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

inbound：对收到的报文进行过滤。

outbound：对发出的报文进行过滤。

hardware-count：表示使能规则匹配统计功能，缺省为关闭。本参数用于使能指定 ACL 内所有规则的匹配统计功能，而 **rule** 命令中的 **counting** 参数则用于使能当前规则的匹配统计功能。

【举例】

应用 IPv4 基本 ACL 2001 对接口 GigabitEthernet3/0/1 收到的报文进行过滤，并对过滤的报文进行统计。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] packet-filter 2001 inbound hardware-count
```

【相关命令】

- **display packet-filter**
- **display packet-filter statistics**
- **display packet-filter verbose**

1.1.13 packet-filter default deny

packet-filter default deny 命令用来配置报文过滤的缺省动作为 Deny，即禁止未匹配上 ACL 规则的报文通过。

undo packet-filter default deny 命令用来恢复缺省情况。

【命令】

packet-filter default deny

undo packet-filter default deny

【缺省情况】

报文过滤的缺省动作为 Permit，即允许未匹配上 ACL 规则的报文通过。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

配置报文过滤的缺省动作会在所有的应用对象下添加一个缺省动作应用，该应用也会像其它应用的 ACL 一样显示。

【举例】

配置报文过滤的缺省动作为 Deny。

```
<Sysname> system-view
[Sysname] packet-filter default deny
```

【相关命令】

- **display packet-filter**
- **display packet-filter statistics**
- **display packet-filter verbose**

1.1.14 packet-filter default hardware-count

packet-filter default hardware-count 命令用来在接口上使能报文过滤缺省动作统计功能。

undo packet-filter default hardware-count 命令用来在接口上关闭报文过滤缺省动作统计功能。

【命令】

packet-filter default { **inbound** | **outbound** } **hardware-count**

undo packet-filter default { **inbound** | **outbound** } **hardware-count**

【缺省情况】

报文过滤缺省动作统计功能处于关闭状态。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

inbound：表示收到的报文。

outbound：表示发出的报文。

【使用指导】

在接口上只有应用了 ACL 进行报文过滤，才允许使能报文过滤缺省动作统计功能。

【举例】

配置报文过滤的缺省动作为 Deny，在接口 GigabitEthernet3/0/1 上对收到的报文应用 IPv4 基本 ACL 2001 进行过滤，并使能报文过滤缺省动作统计功能。

```
<Sysname> system-view
[Sysname] packet-filter default deny
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] packet-filter 2001 inbound
[Sysname-GigabitEthernet3/0/1] packet-filter default inbound hardware-count
```

【相关命令】

- **packet-filter**
- **packet-filter default deny**
- **display packet-filter**
- **display packet-filter statistics**

1.1.15 reset acl counter

reset acl counter 命令用来清除 ACL 的统计信息。

【命令】

reset acl [**ipv6**] **counter** { *acl-number* | **all** | **name** *acl-name* }

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

acl-number：清除指定编号 ACL 的统计信息。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

all：清除全部 ACL 的统计信息。若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL。

name *acl-name*：清除指定名称 ACL 的统计信息。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

【举例】

清除 IPv4 基本 ACL 2001 的统计信息。

```
<Sysname> reset acl counter 2001
```

【相关命令】

- **display acl**

1.1.16 reset packet-filter statistics

reset packet-filter statistics 命令用来清除 ACL 在报文过滤中应用的统计信息（包括累加统计信息）。

【命令】

reset packet-filter statistics { **global** | **interface** [*interface-type interface-number*] } { **inbound** | **outbound** } [**ipv6**] { *acl-number* | **name** *acl-name* }] }

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

global：清除全局（即所有物理接口）统计信息。

interface [*interface-type interface-number*]：清除指定接口上的统计信息。*interface-type interface-number* 表示接口类型和接口编号。若未指定接口类型和接口编号，将清除所有接口上的统计信息。

inbound：清除入方向上的统计信息。

outbound：清除出方向上的统计信息。

acl-number：清除指定编号 ACL 在报文过滤中应用的统计信息。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL；否则表示 IPv6 基本 ACL。
- 3000～3999：若未指定 **ipv6** 关键字，表示 IPv4 高级 ACL；否则表示 IPv6 高级 ACL。
- 4000～4999：表示二层 ACL（指定 **ipv6** 关键字后不会显示本项）。

name *acl-name*：清除指定名称 ACL 在报文过滤中应用的统计信息。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，若未指定 **ipv6** 关键字，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称，否则表示 IPv6 基本 ACL 或 IPv6 高级 ACL 的名称。

【使用指导】

若未指定 **default**、*acl-number* 和 **name** *acl-name* 参数，将清除全部 ACL（若未指定 **ipv6** 关键字，表示全部 IPv4 基本 ACL、IPv4 高级 ACL 和二层 ACL；否则，表示全部 IPv6 基本 ACL 和 IPv6 高级 ACL）和缺省动作在报文过滤中应用的统计信息。

【举例】

清除接口 Ten-GigabitEthernet1/0/1 入方向上 IPv4 基本 ACL 2001 在报文过滤中应用的统计信息。

```
<Sysname> reset packet-filter statistics interface Ten-GigabitEthernet 3/0/1 inbound 2001
```

【相关命令】

- **display packet-filter statistics**
- **display packet-filter statistics sum**

1.1.17 rule (Ethernet frame header ACL view)

rule 命令用来为二层 ACL 创建一条规则。

undo rule 命令用来为二层 ACL 删除一条规则或删除规则中的部分内容。

【命令】

rule [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

undo rule *rule-id* [**counting** | **time-range**] *

【缺省情况】

二层 ACL 内不存在任何规则。

【视图】

二层 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

rule-id：指定二层 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

cos *vlan-pri*：指定 802.1p 优先级。*vlan-pri* 表示 802.1p 优先级，可输入的形式如下：

- 数字：取值范围为 0～7；
- 名称：**best-effort**、**background**、**spare**、**excellent-effort**、**controlled-load**、**video**、**voice** 和 **network-management**，依次对应于数字 0～7。

counting：表示使能规则匹配统计功能，缺省为关闭。本参数用于使能本规则的匹配统计功能，而 **packet-filter** 命令中的 **hardware-count** 参数则用于使能指定 ACL 内所有规则的匹配统计功能。

dest-mac *dest-address dest-mask*：指定目的 MAC 地址范围。*dest-address* 表示目的 MAC 地址，格式为 H-H-H。*dest-mask* 表示目的 MAC 地址的掩码，格式为 H-H-H。

lsap *lsap-type lsap-type-mask*：指定 LLC 封装中的 DSAP 字段和 SSAP 字段。*lsap-type* 表示数据帧的封装格式，为 16 比特的十六进制数。*lsap-type-mask* 表示 LSAP 的类型掩码，为 16 比特的十六进制数，用于指定屏蔽位。

type *protocol-type protocol-type-mask*：指定链路层协议类型。*protocol-type* 表示 16 比特的十六进制数表征的数据帧类型，对应 Ethernet_II 类型和 Ethernet_SNAP 类型帧中的 type 域。*protocol-type-mask* 表示类型掩码，为 16 比特的十六进制数，用于指定屏蔽位。

source-mac *source-address source-mask*：指定源 MAC 地址范围。*source-address* 表示源 MAC 地址，格式为 H-H-H。*source-mask* 表示源 MAC 地址的掩码，格式为 H-H-H。

time-range *time-range-name*：指定本规则生效的时间段。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL 和 QoS 配置指导”中的“时间段”。

【使用指导】

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

【举例】

为二层 ACL 4000 创建规则如下：允许 ARP 报文通过，但拒绝 RARP 报文通过。

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule permit type 0806 ffff
[Sysname-acl-ethernetframe-4000] rule deny type 8035 ffff
```

【相关命令】

- **acl**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.18 rule (IPv4 advanced ACL view)

rule 命令用来为 IPv4 高级 ACL 创建一条规则。

undo rule 命令用来为 IPv4 高级 ACL 删除一条规则或删除规则中的部分内容。

【命令】

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | { **dscp** | { **precedence** | **tos** } * } | **fragment** | **icmp-type** | **logging** | **source** | **source-port** | **time-range** | **vpn-instance**] *

【缺省情况】

IPv4 高级 ACL 内不存在任何规则。

【视图】

IPv4 高级 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

rule-id：指定 IPv4 高级 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv4 承载的协议类型，可输入的形式如下：

- 数字：取值范围为 0～255；
- 名称（括号内为对应的数字）：可选取 **gre**（47）、**icmp**（1）、**igmp**（2）、**ip**、**ipinip**（4）、**ospf**（89）、**tcp**（6）或 **udp**（17）。

*protocol*之后可配置如 表 1-7 所示的规则信息参数。

表1-7 规则信息参数

参数	类别	作用	说明
source { *source-address source-wildcard* | **any** }	源地址信息	指定ACL规则的源地址信息	*source-address*：源IP地址 *source-wildcard*：源IP地址的通配符掩码（为0表示主机地址） **any**：任意源IP地址
destination { *dest-address dest-wildcard* | **any** }	目的地址信息	指定ACL规则的目的地址信息	*dest-address*：目的IP地址 *dest-wildcard*：目的IP地址的通配符掩码（为0表示主机地址） **any**：任意目的IP地址

参数	类别	作用	说明
counting	统计	使能规则匹配统计功能，缺省为关闭	本参数用于使能本规则的匹配统计功能，而**packet-filter**命令中的**hardware-count**参数则用于使能指定ACL内所有规则的匹配统计功能
precedence *precedence*	报文优先级	IP优先级	*precedence*用数字表示时，取值范围为0～7；用文字表示时，分别对应**routine**、**priority**、**immediate**、**flash**、**flash-override**、**critical**、**internet**、**network**
tos *tos*	报文优先级	ToS优先级	*tos*用数字表示时，取值范围为0～15；用文字表示时，可以选取**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）、**min-monetary-cost**（1）、**normal**（0）
dscp *dscp*	报文优先级	DSCP优先级	*dscp*用数字表示时，取值范围为0～63；用文字表示时，可以选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）、**ef**（46）
fragment	分片信息	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定该参数，则表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效 CSPC单板和丝印为CMPE-1104的单板不支持该参数
logging	日志操作	对符合条件的报文可记录日志信息	该功能需要使用该ACL的模块支持日志记录功能，例如报文过滤
time-range *time-range-name*	时间段	指定本规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL和QoS配置指导”中的“时间段”
vpn-instance *vpn-instance-name*	VPN实例	对指定VPN实例中的报文有效	*vpn-instance-name*：MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写 若未指定本参数，表示该规则仅对非VPN报文有效 CSPC单板和丝印为CMPE-1104的单板不支持该参数

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-8 所示的规则信息参数。

表1-8 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	定义TCP/UDP报文的源端口信息	*operator*为操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有操作符**range**需要两个端口号做操作数，其它的只需要一个端口号做操作数
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	*port1*、*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用文字表示时，TCP端口号可以选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）、**www**（80）；UDP端口号可以选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）、**xdmcp**（177）
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 如果在一条规则中设置了多个TCP标志位的匹配值，则这些匹配条件之间的关系为“与”。譬如：当配置为**ack** 0 **psh** 1时，有些产品将匹配不携带ACK标志位且携带PSH标志位的TCP报文
established	TCP连接建立标识	定义对TCP连接报文的处理规则	TCP协议特有的参数，用于定义TCP报文中ACK或RST标志位为1的报文

当*protocol*为**icmp**（1）时，用户还可配置如 表 1-9 所示的规则信息参数。

表1-9 ICMP 特有的规则信息参数

参数	类别	作用	说明
icmp-type { *icmp-type* *icmp-code* | *icmp-message* }	ICMP报文的消息类型和消息码信息	指定本规则中ICMP报文的消息类型和消息码信息	*icmp-type*：ICMP消息类型，取值范围为0～255 *icmp-code*：ICMP消息码，取值范围为0～255 *icmp-message*：ICMP消息名称。可以输入的ICMP消息名称，及其与消息类型和消息码的对应关系如表1-10所示

表1-10 ICMP 消息名称与消息类型和消息码的对应关系

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

【使用指导】

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。
- CSPC 单板和丝印为 CMPE-1104 的单板不支持配置操作符 *operator* 取值为 **neq**。

【举例】

为 IPv4 高级 ACL 3000 创建规则如下：允许 129.9.0.0/16 网段内的主机与 202.38.160.0/24 网段内主机的 WWW 端口（端口号为 80）建立连接。

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255 destination-port eq 80
```

为 IPv4 高级 ACL 3001 创建规则如下：允许 IP 报文通过，但拒绝发往 192.168.1.0/24 网段的 ICMP 报文通过。

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-adv-3001] rule permit ip
```

为 IPv4 高级 ACL 3002 创建规则如下：在出、入双方向上都允许建立 FTP 连接并传输 FTP 数据。

```
<Sysname> system-view
[Sysname] acl number 3002
[Sysname-acl-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-adv-3002] rule permit tcp destination-port eq ftp-data
```

为 IPv4 高级 ACL 3003 创建规则如下：在出、入双方向上都允许 SNMP 报文和 SNMP Trap 报文通过。

```
<Sysname> system-view
[Sysname] acl number 3003
[Sysname-acl-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-adv-3003] rule permit udp destination-port eq snmptrap
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.19 rule (IPv4 basic ACL view)

rule 命令用来为 IPv4 基本 ACL 创建一条规则。

undo rule 命令用来为 IPv4 基本 ACL 删除一条规则或删除规则中的部分内容。

【命令】

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **source** | **time-range** | **vpn-instance**] *

【缺省情况】

IPv4 基本 ACL 内不存在任何规则。

【视图】

IPv4 基本 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

rule-id：指定 IPv4 基本 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

counting：表示使能规则匹配统计功能，缺省为关闭。本参数用于使能本规则的匹配统计功能，而 **packet-filter** 命令中的 **hardware-count** 参数则用于使能指定 ACL 内所有规则的匹配统计功能。

fragment：表示仅对非首片分片报文有效，而对非分片报文和首片分片报文无效。若未指定本参数，表示该规则对非分片报文和分片报文均有效。CSPC 单板和丝印为 CMPE-1104 的单板不支持该参数。

logging：表示对符合条件的报文可记录日志信息。该功能需要使用该 ACL 的模块支持日志记录功能，例如报文过滤。

source { *source-address source-wildcard* | **any** }：指定规则的源 IP 地址信息。*source-address* 表示报文的源 IP 地址，*source-wildcard* 表示源 IP 地址的通配符掩码（为 0 表示主机地址），**any** 表示任意源 IP 地址。

time-range *time-range-name*：指定本规则生效的时间段。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL 和 QoS 配置指导”中的“时间段”。

vpn-instance *vpn-instance-name*：表示对指定 VPN 实例中的报文有效。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定本参数，表示该规则仅对非 VPN 报文有效。SPC 单板和丝印为 MPE-1104 的单板不支持该参数。

【使用指导】

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

【举例】

为 IPv4 基本 ACL 2000 创建规则如下：仅允许来自 10.0.0.0/8、172.17.0.0/16 和 192.168.1.0/24 网段的报文通过，而拒绝来自所有其它网段的报文通过。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-basic-2000] rule deny source any
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.20 rule (IPv6 advanced ACL view)

rule 命令用来为 IPv6 高级 ACL 创建一条规则。

undo rule 命令用来为 IPv6 高级 ACL 删除一条规则或删除规则中的部分内容。

【命令】

rule [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **counting** | **destination** { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [{ { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **established** } | **counting** | **destination** | **destination-port** | **dscp** | **flow-label** | **fragment** | **icmp6-type** | **logging** | **routing** | **hop-by-hop** | **source** | **source-port** | **time-range** | **vpn-instance**] *

【缺省情况】

IPv6 高级 ACL 内不存在任何规则。

【视图】

IPv6 高级 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

rule-id：指定 IPv6 高级 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv6 承载的协议类型，可输入的形式如下：

- 数字：取值范围为 0～255；
- 名称（括号内为对应的数字）：可选取 **gre**（47）、**icmpv6**（58）、**ipv6**、**ipv6-ah**（51）、**ipv6-esp**（50）、**ospf**（89）、**tcp**（6）或 **udp**（17）。

*protocol*之后可配置如 表 1-11 所示的规则信息参数。

表1-11 规则信息参数

参数	类别	作用	说明
source { *source-address source-prefix* | *source-address/source-prefix* | **any** }	源IPv6地址	指定ACL规则的源IPv6地址信息	*source-address*：源IPv6地址 *source-prefix*：源IPv6地址的前缀长度，取值范围1～128 **any**：任意源IPv6地址
destination { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** }	目的IPv6地址	指定ACL规则的目的IPv6地址信息	*dest-address*：目的IPv6地址 *dest-prefix*：目的IPv6地址的前缀长度，取值范围1～128 **any**：任意目的IPv6地址
counting	统计	使能规则匹配统计功能，缺省为关闭	本参数用于使能本规则的匹配统计功能，而**packet-filter ipv6**命令中的**hardware-count**参数则用于使能指定ACL内所有规则的匹配统计功能
dscp *dscp*	报文优先级	DSCP优先级	*dscp*：用数字表示时，取值范围为0～63；用名称表示时，可选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）或**ef**（46）
flow-label *flow-label-value*	流标签字段	指定IPv6基本报文头中流标签字段的值	*flow-label-value*：流标签字段的值，取值范围为0～1048575

参数	类别	作用	说明
fragment	报文分片	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定本参数，表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效 CSPC单板和丝印为CMPE-1104的单板不支持该参数
logging	日志操作	对符合条件的报文可记录日志信息	该功能需要使用该ACL的模块支持日志记录功能，例如报文过滤
routing [**type** *routing-type*]	路由头	指定路由头的类型	*routing-type*：路由头类型的值，取值范围为0～255 若指定了**type** *routing-type*参数，表示仅对指定类型的路由头有效；否则，表示对IPv6所有类型的路由头都有效
hop-by-hop [**type** *hop-type*]	逐跳头	指定逐跳头的类型	*hop-type*：逐跳头类型的值，取值范围为0～255 若指定了**type** *hop-type*参数，表示仅对指定类型的逐跳头有效；否则，表示对IPv6所有类型的逐跳头都有效
time-range *time-range-name*	时间段	指定本规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL和QoS配置指导”中的“时间段”
vpn-instance *vpn-instance-name*	VPN实例	对指定VPN实例中的报文有效	*vpn-instance-name*：MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写 若未指定本参数，表示该规则仅对非VPN报文有效 CSPC单板和丝印为CMPE-1104的单板不支持该参数

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-12 所示的规则信息参数。

表1-12 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	定义TCP/UDP报文的源端口信息	*operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数 *port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）或**www**（80）；UDP端口号可选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）或**xdmcp**（177）
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 如果在一条规则中设置了多个TCP标志位的匹配值，则这些匹配条件之间的关系为“与”。譬如：当配置为**ack** 0 **psh** 1时，有些产品将匹配不携带ACK标志位且携带PSH标志位的TCP报文
established	TCP连接建立标识	定义对TCP连接报文的处理规则	TCP协议特有的参数，用于定义TCP报文中ACK或RST标志位为1的报文

当*protocol*为**icmpv6**（58）时，用户还可配置如 表 1-13 所示的规则信息参数。

表1-13 ICMPv6 特有的规则信息参数

参数	类别	作用	说明
icmp6-type { *icmp6-type* *icmp6-code* | *icmp6-message* }	ICMPv6报文的消息类型和消息码	指定本规则中ICMPv6报文的消息类型和消息码信息	*icmp6-type*：ICMPv6消息类型，取值范围为0～255 *icmp6-code*：ICMPv6消息码，取值范围为0～255 *icmp6-message*：ICMPv6消息名称。可以输入的ICMPv6消息名称，及其与消息类型和消息码的对应关系如表1-14所示

表1-14 ICMPv6 消息名称与消息类型和消息码的对应关系

ICMPv6 消息名称	ICMPv6 消息类型	ICMPv6 消息码
echo-reply	129	0
echo-request	128	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

【使用指导】

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。
- 新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl ipv6 all** 命令来查看所有已存在的规则。
- 如果 ACL 匹配的是 IPv6 扩展报文头内层的报文内容，则对于扩展报文头超过两层，或包含 Encapsulating Security Payload Header 报文头的报文，ACL 将无法进行匹配。
- CSPC 单板和丝印为 CMPE-1104 的单板不支持配置操作符 *operator* 取值为 **neq**。
- 需要注意的是，当 IPv6 高级 ACL 用于 QoS 策略的流分类或用于报文过滤功能时：如果 QoS 策略或报文过滤功能应用于出方向，不支持配置 **routing** 参数和 **flow-label** 参数。

【举例】

为 IPv6 高级 ACL 3000 创建规则如下：允许 2030:5060::/64 网段内的主机与 FE80:5060::/96 网段内主机的 WWW 端口（端口号为 80）建立连接。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::/64 destination fe80:5060::/96
destination-port eq 80
```

为 IPv6 高级 ACL 3001 创建规则如下：允许 IPv6 报文通过，但拒绝发往 FE80:5060:1001::/48 网段的 ICMPv6 报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3001
[Sysname-acl6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
[Sysname-acl6-adv-3001] rule permit ipv6
```

为 IPv6 高级 ACL 3002 创建规则如下：在出、入双方向上都允许建立 FTP 连接并传输 FTP 数据。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3002
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl6-adv-3002] rule permit tcp destination-port eq ftp-data
```

为 IPv6 高级 ACL 3003 创建规则如下：在出、入双方向上都允许 SNMP 报文和 SNMP Trap 报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3003
[Sysname-acl6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl6-adv-3003] rule permit udp destination-port eq snmptrap
```

为 IPv6 高级 ACL 3004 创建规则如下：在含有逐跳头的报文中，只允许转发含有 MLD 选项（Type＝5）的报文，丢弃其他报文。

```
<Sysname> system-view
[Sysname] acl ipv6 number 3004
[Sysname-acl6-adv-3004] rule permit ipv6 hop-by-hop type 5
[Sysname-acl6-adv-3004] rule deny ipv6 hop-by-hop
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.21 rule (IPv6 basic ACL view)

rule 命令用来为 IPv6 基本 ACL 创建一条规则。

undo rule 命令用来为 IPv6 基本 ACL 删除一条规则或删除规则中的部分内容。

【命令】

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**counting** | **fragment** | **logging** | **routing** | **source** | **time-range** | **vpn-instance**] *

【缺省情况】

IPv6 基本 ACL 内不存在任何规则。

【视图】

IPv6 基本 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

rule-id：指定 IPv6 基本 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

counting：表示使能规则匹配统计功能，缺省为关闭。本参数用于使能本规则的匹配统计功能，而 **packet-filter ipv6** 命令中的 **hardware-count** 参数则用于使能指定 ACL 内所有规则的匹配统计功能。

fragment：表示仅对非首片分片报文有效，而对非分片报文和首片分片报文无效。若未指定本参数，表示该规则对非分片报文和分片报文均有效。CSPC 单板和丝印为 CMPE-1104 的单板不支持该参数。

logging：表示对符合条件的报文可记录日志信息。该功能需要使用该 ACL 的模块支持日志记录功能，例如报文过滤。

routing [**type** *routing-type*]：表示对所有或指定类型的路由头有效，*routing-type* 表示路由头类型的值，取值范围为 0～255。若指定了 **type** *routing-type* 参数，表示仅对指定类型的路由头有效；否则，表示对所有类型的路由头都有效。

source { *source-address source-prefix* | *source-address/source-prefix* | **any** }：指定规则的源 IPv6 地址信息。*source-address* 表示报文的源 IPv6 地址，*source-prefix* 表示源 IPv6 地址的前缀长度，取值范围为 1～128，**any** 表示任意源 IPv6 地址。

time-range *time-range-name*：指定本规则生效的时间段。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL 和 QoS 配置指导”中的“时间段”。

vpn-instance *vpn-instance-name*：表示对指定 VPN 实例中的报文有效。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定本参数，表示该规则仅对非 VPN 报文有效。CSPC 单板和丝印为 CMPE-1104 的单板不支持该参数。

【使用指导】

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl ipv6 all** 命令来查看所有已存在的规则。
- CSPC 单板和丝印为 CMPE-1104 的单板不支持 **fragment** 参数和 **vpn-instance** 参数。

【举例】

为 IPv6 基本 ACL 2000 创建规则如下：仅允许来自 1001::/16、3124:1123::/32 和 FE80:5060:1001::/48 网段的报文通过，而拒绝来自所有其它网段的报文通过。

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 1001:: 16
[Sysname-acl6-basic-2000] rule permit source 3124:1123:: 32
[Sysname-acl6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl6-basic-2000] rule deny source any
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.22 rule comment

rule comment 命令用来为指定规则配置描述信息。

undo rule comment 命令用来删除指定规则的描述信息。

【命令】

rule *rule-id* **comment** *text*

undo rule *rule-id* **comment**

【缺省情况】

规则没有任何描述信息。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图/IPv6 基本 ACL 视图/IPv6 高级 ACL 视图/二层 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

rule-id：指定规则的编号，该规则必须存在。取值范围为 0～65534。

text：表示规则的描述信息，为 1～127 个字符的字符串，区分大小写。

【使用指导】

使用 **rule comment** 命令时，如果指定的规则没有描述信息，则为其添加描述信息，否则修改其描述信息。

【举例】

为 IPv4 基本 ACL 2000 配置规则 0，并为该规则配置描述信息。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used on GigabitEthernet 3/0/1.
```

【相关命令】

- **display acl**

1.1.23 step

step 命令用来配置规则编号的步长。

undo step 命令用来恢复缺省情况。

【命令】

step *step-value*

undo step

【缺省情况】

规则编号的步长为 5。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图/IPv6 基本 ACL 视图/IPv6 高级 ACL 视图/二层 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

step-value：表示规则编号的步长值，取值范围为 1～20。

【举例】

将 IPv4 基本 ACL 2000 的规则编号的步长配置为 2。

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] step 2
```

【相关命令】

- **display acl**

目 录

1 QoS策略

说明

本文中的“CSPC 单板”指的是单板丝印以“CSPC”开头（如 CSPC-GP48LB）的单板。

1.1 定义类的命令

1.1.1 display traffic classifier

display traffic classifier 命令用来显示类的配置信息。

【命令】

display traffic classifier user-defined [*classifier-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

user-defined：用户定义类。

classifier-name：类名，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，将显示所有类的配置信息。

slot *slot-number*：显示指定单板的流分类的信息，*slot-number* 表示单板所在的槽位号。如果未指定本参数，将显示主用主控板的类的配置信息。

【举例】

显示用户定义类的配置信息。

```
<Sysname> display traffic classifier user-defined

  User-defined classifier information:

   Classifier: 1 (ID 100)
     Operator: AND
     Rule(s) :
      If-match acl 2000

   Classifier: 2 (ID 101)
```

```
    Operator: AND
    Rule(s) :
     If-match protocol ipv6

  Classifier: 3 (ID 102)
    Operator: AND
    Rule(s) :
     -none-
```

表1-1 display traffic classifier 命令显示信息描述表

字段	描述
User-defined classifier information	用户自定义类的信息
Classifier	类的名字及其内容，内容可以有多种类型
Operator	分类规则之间的逻辑关系
Rule(s)	分类规则

1.1.2 if-match

if-match 命令用来定义匹配数据包的规则。

undo if-match 命令用来删除配置的匹配数据包的规则。

【命令】

if-match *match-criteria*

undo if-match *match-criteria*

【缺省情况】

没有定义匹配数据包的规则。

【视图】

类视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

match-criteria：类的匹配规则，具体情况如 表 1-2 所示。

表1-2 类的匹配规则取值

取值	描述
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	定义匹配ACL的规则 *acl-number*是ACL的序号，IPv4 ACL序号的取值范围是2000～3999，IPv6 ACL序号的取值范围是2000～3999，二层ACL序号的取值范围是4000～4999 *acl-name*是ACL的名称，为1～63个字符的字符串，不区分大小写，必须以英文字母a～z或A～Z开头，为避免混淆，ACL的名称不可以使用英文单词all

取值	描述
any	定义匹配所有数据包的规则 CSPEX-1204单板不支持定义匹配所有数据包的规则
authenticated-user	定义匹配已认证用户的数据包，且认证方式必须为IPoE、Portal或PPPoE
control-plane protocol *protocol-name*&<1-8>	定义匹配控制平面协议的规则，*protocol-name*&<1-8>为系统预定义匹配协议报文类型名称的列表，&<1-8>表示前面的参数最多可以输入8次。
control-plane protocol-group *protocol-group-name*	定义匹配控制平面协议组的规则，*protocol-group-name*取值为critical、important、management、monitor、normal、redirect
customer-dot1p *dot1p-value*&<1-8>	定义匹配内层VLAN Tag的802.1p优先级规则，*dot1p-value*&<1-8>为802.1p优先级值的列表，802.1p优先级的取值范围为0～7，&<1-8>表示前面的参数最多可以输入8次 CSPEX-1204单板不支持定义匹配内层VLAN Tag的802.1p优先级规则
customer-vlan-id *vlan-id-list*	定义匹配内层VLAN Tag的VLAN ID规则，*vlan-id-list*：VLAN列表，表示方式为*vlan-id-list* = { *vlan-id* | *vlan-id1* **to** *vlan-id2* }&<1-10>，*vlan-id*、*vlan-id1*、*vlan-id2*取值范围为1～4093，且*vlan-id1*的值必须小于*vlan-id2*的值；&<1-10>表示前面的参数最多可以重复输入10次
destination-mac *mac-address*	定义匹配目的MAC地址的规则
dscp *dscp-value*&<1-8>	定义匹配DSCP的规则，*dscp-value*&<1-8>为DSCP取值的列表，DSCP的取值范围为0～63，&<1-8>表示前面的参数最多可以输入8次；也可以输入关键字，具体如表1-4所示
inbound-interface *interface-type interface-number*	定义匹配入接口的规则，*interface-type interface-number*为接口类型和接口编号 仅CSPEX-1204单板支持
ip-precedence *ip-precedence-value*&<1-8>	定义匹配IP优先级的规则，*ip-precedence-value*&<1-8>为IP优先级的列表，IP优先级的取值范围为0～7，&<1-8>表示前面的参数最多可以输入8次
mpls-exp *exp-value*&<1-8>	定义匹配第一层MPLS EXP优先级的规则，*exp-value*&<1-8>为EXP的列表，EXP优先级的取值范围为0～7，&<1-8>表示前面的参数最多可以输入8次 仅CSPEX-1204单板支持
protocol *protocol-name*	定义匹配协议的规则，*protocol-name*取值为arp、ip和ipv6
qos-local-id *local-id-value*	定义匹配QoS本地ID值的规则，*local-id-value*为QoS本地ID，取值范围为1～4095 引用本参数的QoS策略在出方向不支持
service-dot1p *dot1p-value*&<1-8>	定义匹配外层VLAN Tag的802.1p优先级规则，*dot1p-value*&<1-8>为802.1p优先级值的列表，802.1p优先级的取值范围为0～7，&<1-8>表示前面的参数最多可以输入8次
service-vlan-id *vlan-id-list*	定义匹配外层VLAN Tag的VLAN ID规则，*vlan-id-list*：VLAN列表，表示方式为*vlan-id-list* = { *vlan-id* | *vlan-id1* **to** *vlan-id2* }&<1-10>，*vlan-id*、*vlan-id1*、*vlan-id2*取值范围为1～4093，且*vlan-id1*的值必须小于*vlan-id2*的值；&<1-10>表示前面的参数最多可以重复输入10次
source-mac *mac-address*	定义匹配源MAC地址的规则

说明

当流分类中各规则之间的逻辑关系为 **and** 时，同一类匹配规则只能配置一次，用户虽然可以通过重复执行 **if-match** 命令来配置多条匹配不同取值的规则，或在一条规则中使用 *list* 形式输入多个匹配值，但在应用使用该类的 QoS 策略时，对应该类的流行为将会无法正常执行。如果用户需要创建匹配以上某一字段多个取值或多个 ACL 的规则，需要在创建流分类时指定各规则之间的逻辑关系为 **or**。

说明

如果流分类的匹配规则中包括 **control-plane protocol** 或 **control-plane protocol-group**，则使用该流分类的 QoS 策略只能应用在控制平面上。

【使用指导】

在定义各个规则的时候，注意事项如下：

(1) 定义匹配 ACL 的规则

- 如果类中引用的 ACL 不存在，则使用该类的 QoS 策略将不能正常应用。
- 对同一个类，允许通过 ACL 名称和序号的方式分别引用一次同一个 ACL。

(2) 定义匹配目的 MAC 地址规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 匹配目的 MAC 地址规则只对以太网接口有意义。

(3) 定义匹配源 MAC 地址规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 匹配源 MAC 地址规则只对以太网接口有意义。

(4) 定义匹配 DSCP 的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 删除某条匹配 DSCP 的规则时，指定的所有 DSCP 值必须与该规则中定义的完全相同才会删除，顺序可不一样。

(5) 定义匹配内层 VLAN Tag 和外层 VLAN Tag 的 802.1p 优先级的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 删除某条匹配 802.1p 优先级的规则时，指定的所有 802.1p 优先级值必须与该规则中定义的完全相同才会删除，顺序可不一样。
- 若只携带单层 VLAN Tag，可以用外层 VLAN Tag 的 802.1p 优先级规则来匹配。

(6) 定义匹配 IP 优先级的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 删除某条匹配 IP 优先级的规则时，指定的所有 IP 优先级值必须与该规则中定义的完全相同才会删除，顺序可不一样。

(7) 定义匹配 MPLS EXP 优先级的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 删除某条匹配 MPLS EXP 优先级的规则时，指定的所有 MPLS EXP 优先级值必须与该规则中定义的完全相同才会删除，顺序可不一样。
- MPLS EXP 为 MPLS 报文特有的参数，该匹配规则仅对 MPLS 报文生效。
- 对于软转发 QoS，MPLS 报文不支持匹配 IP 相关匹配规则。

(8) 定义匹配内层 VLAN Tag 和外层 VLAN Tag 的 VLAN ID 的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 删除某条匹配 VLAN ID 的规则时，指定的所有 VLAN ID 值必须与该规则中定义的完全相同才会删除，顺序可不一样。
- 若只携带单层 VLAN Tag，可以用外层 VLAN Tag 的 VLAN ID 规则来匹配。

(9) 定义匹配预定义的上送控制平面或者管理口控制平面报文类型的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 删除某条匹配 protocol 的规则时，指定的所有 protocol 必须与该规则中定义的完全相同才会删除，顺序可不一样。
- 系统预定义的报文类型信息可以通过 **display qos policy control-plane pre-defined** 命令查看。

【举例】

定义类 class1 的匹配规则为：匹配目的 MAC 地址为 0050-ba27-bed3 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

定义类 class2 的匹配规则为：匹配源 MAC 地址为 0050-ba27-bed2 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source-mac 0050-ba27-bed2
```

定义类 class1 的匹配规则为：匹配内层 VLAN Tag 的网络 802.1p 优先级为 3。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-dot1p 3
```

定义类 class1 的匹配规则为：匹配外层 VLAN Tag 的 802.1p 优先级为 5。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-dot1p 5
```

定义类匹配 ACL3101。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3101
```

定义类匹配 ACL flow。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl name flow
```

定义类匹配 IPv6 ACL3101。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 3101
```

定义类匹配 IPv6 ACL flow。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 name flow
```

定义匹配所有数据包的规则。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match any
```

定义类 class1 的匹配规则为：匹配已认证用户的数据包。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match authenticated-user
```

定义类 class1 的匹配规则为：匹配 DSCP 值为 1 或 6 或 9 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match dscp 1 6 9
```

定义类 class1 的匹配规则为：匹配 IP 优先级值为 1 或 6 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ip-precedence 1 6
```

定义类匹配 IP 协议的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match protocol ip
```

定义类 class1 的匹配规则为：匹配内层 VLAN Tag 的 VLAN ID 值为 1 或 6 或 9 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-vlan-id 1 6 9
```

定义类 class1 的匹配规则为：匹配外层 VLAN Tag 的 VLAN ID 值为 2 或 7 或 10 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-vlan-id 2 7 10
```

定义类 class1 匹配 qos-local-id 3。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match qos-local-id 3
```

在流分类 class1 中配置匹配上送控制平面的 ARP 协议报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match control-plane protocol arp
```

在流分类 class1 中配置匹配上送控制平面的 normal 协议组报文。

```
<Sysname> system-view
```

```
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match control-plane protocol-group normal
```

1.1.3 traffic classifier

traffic classifier 命令用来定义一个类，并进入类视图。

undo traffic classifier 命令用来删除一个类。

【命令】

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

【缺省情况】

没有定义类。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

classifier-name：类名，为 1～31 个字符的字符串，区分大小写。

operator：指定各规则之间的逻辑运算符。缺省情况为 **and**。

and：指定类下的规则之间是逻辑与的关系，即数据包必须匹配全部规则才属于该类。

or：指定类下的规则之间是逻辑或的关系，即数据包只要匹配其中任何一个规则就属于该类。

【举例】

定义一个名为 class1 的类。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

【相关命令】

- **display traffic classifier**

1.2 定义流行为的命令

1.2.1 accounting

accounting 命令用来配置流量统计动作。

undo accounting 命令用来取消流量统计动作配置。

【命令】

accounting { **byte** | **packet** }

undo accounting

【缺省情况】

没有配置流量统计动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

byte：表示报文基于字节进行统计。

packet：表示报文基于包进行统计。

【举例】

为流行为配置流量统计动作，基于字节进行统计。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting byte
```

1.2.2 car

car 命令用来配置流量监管动作。

undo car 命令用来取消流量监管动作配置。

【命令】

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**green** *action* | **red** *action* | **yellow** *action*] * [**hierarchy-car** *hierarchy-car-name* [**mode** { **and** | **or** }]]

undo car

【缺省情况】

没有配置流量监管动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

cir *committed-information-rate*：承诺信息速率。流量的平均速率，单位为 kbps。取值范围为 8～160000000，实际生效的承诺信息速率为 *committed-information-rate* / 8 的商值，四舍五入取整数后再乘以 8。

cbs *committee-burst-size*：承诺突发尺寸，单位为 byte。

- 如果不指定 **cbs** 参数，缺省取值为 62.5 × *committed-information-rate* 的乘积。

- 如果指定 **cbs** 参数，取值范围 512～256000000。

实际生效的承诺突发尺寸为 *committee-burst-size* / 512 的商值，四舍五入取整数后再乘以 512。

ebs *excess-burst-size*：超出突发尺寸，缺省值为 512，单位为 byte。取值范围为 0～256000000，实际生效的超出突发尺寸为 *excess-burst-size* / 512 的商值，四舍五入取整数后再乘以 512。

pir *peak-information-rate*：峰值速率，单位为 kbps。取值范围为 8～160000000，实际生效的峰值速率为 *peak-information-rate* / 8 的商值，四舍五入取整数后再乘以 8。

green *action*：数据包的流量符合承诺速率时对数据包采取的动作，缺省动作为 **pass**。

red *action*：数据包的流量既不符合承诺速率也不符合峰值速率时对数据包采取的动作，缺省动作为 **discard**。

yellow *action*：数据包的流量不符合承诺速率但是符合峰值速率时对数据包采取的动作，缺省动作为 **pass**。

action：对数据包采取的动作，有以下几种：

- **discard**：丢弃数据包。
- **pass**：允许数据包通过。
- **remark-dot1p-pass** *new-cos*：设置新的 802.1P 报文的优先级值，并允许数据包通过，取值范围为 0～7。
- **remark-dscp-pass** *new-dscp*：设置报文新的 DSCP 值，并允许数据包通过，取值范围为 0～63。
- **remark-lp-pass** *new-local-precedence*：设置新的本地优先级，并允许数据包通过，取值范围为 0～7。

hierarchy-car-name：分层 CAR 的名称，目前暂不支持该参数。

mode：分层 CAR 和 CAR 动作的合作模式，目前暂不支持该参数。

【使用指导】

- 接口上应用的策略中使用 **car** 时，可以应用到接口报文的接收或者发送方向。
- QoS 策略引用了带有 **remark-lp-pass** 参数的 **car** 时，在出方向不支持。
- 如果多次使用该命令在同一个流行为上配置，最后一次配置生效。

【举例】

为流行为配置流量监管。报文正常流速为 200kbps，承诺突发尺寸为 50000bytes，速率大于 200kbps 时，报文 DSCP 值改为 0 并发送。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 50000 ebs 0 green pass red remark-dscp-pass 0
```

1.2.3 display traffic behavior

display traffic behavior 命令用来显示流行为的配置信息。

【命令】

display traffic behavior user-defined [*behavior-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

user-defined：用户定义行为。

behavior-name：行为名，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则显示所有流行为的配置信息。

slot *slot-number*：显示指定单板的流行为的信息，*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示主用主控板的流行为的配置信息。

【举例】

显示用户定义行为的配置信息。

```
<Sysname> display traffic behavior user-defined

  User-defined behavior information:

    Behavior: 1 (ID 100)
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 7000 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard

    Behavior: 2 (ID 101)
      Accounting enable: Packet
      Filter enable: Permit
      Marking:
        Remark dot1p 1
      Free account enable

    Behavior: 3 (ID 102)
      -none-
```

表1-3 display traffic behavior 命令显示信息描述表

字段	描述
User-defined behavior information	用户自定义流行为的信息
Behavior	行为的名字及其内容，内容可以有多种类型
Marking	标记相关信息
Remark dscp	重新标记报文的DSCP优先级值

字段	描述
Committed Access Rate	流量限速的相关信息
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，也就是容纳突发流量的令牌桶深度，单位为byte
EBS	超出突发尺寸，在双令牌桶算法中超出突发流量超过承诺突发流量的部分，单位为byte
Green action	对绿色报文的动作
Red action	对红色报文的动作
Yellow action	对黄色报文的动作
Accounting enable	流量统计动作
Filter enable	流量过滤动作
Remark dot1p 1	重新标记报文的802.1p优先级
Free account enable	表示使能了流量放行功能
none	表示没有配置其他流行为

1.2.4 filter

filter 命令用来配置流量过滤动作。

undo filter 命令用来取消流量过滤动作配置。

【命令】

filter { **deny** | **permit** }

undo filter

【缺省情况】

没有配置流量过滤动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

deny：丢弃数据包。

permit：允许数据包通过。

【举例】

为流行为配置丢弃数据包的过滤动作。

```
<Sysname> system-view
[Sysname] traffic behavior database
```

```
[Sysname-behavior-database] filter deny
```

1.2.5 free account

free account 命令用来配置流量放行，对于匹配的流量不进行限速和计费。

undo free account 命令用来取消流量放行。

【命令】

free account

undo free account

【缺省情况】

没有配置流量放行的动作。

【视图】

流行为视图

【支持的缺省用户角色】

network-admin

mdc-admin

【参数】

无

【使用指导】

只有通过 IPoE、Portal 或 PPPoE 认证的用户流量支持配置流量放行。

【举例】

配置流量放行动作，对于匹配的流量不进行限速和计费。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] free account
```

1.2.6 nest top-most

nest top-most 命令用来配置添加 VLAN Tag 的动作。

undo nest top-most 命令用来取消添加 VLAN Tag 的动作。

【命令】

nest top-most vlan *vlan-id*

undo nest top-most

【缺省情况】

没有配置添加 VLAN Tag 的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

vlan *vlan-id*：添加的 VLAN ID，取值范围为 1～4093。

【使用指导】

- 引用了添加 VLAN Tag 动作的 QoS 策略只能应用到接口的入方向上。
- 在同一个流行为上多次配置本命令，新配置将覆盖旧配置。
- CSPEX-1204 单板不支持本命令。

【举例】

在流行为 b1 上配置如下动作：添加 VLAN ID 为 123 的 VLAN Tag。

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] nest top-most vlan 123
```

1.2.7 primap color-map-dp

primap color-map-dp 命令用来配置流行为中的动作为根据报文颜色标记报文的丢弃优先级。

undo primap color-map-dp 命令用来取消流行为中的根据报文颜色标记报文的丢弃优先级的动作。

【命令】

primap color-map-dp

undo primap color-map-dp

【缺省情况】

没有配置流优先级映射动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

本命令需要和 car 结合在一起使用。

映射关系为：红色对应丢弃优先级 2，黄色对应丢弃优先级 1，绿色对应丢弃优先级 0。此映射关系固定，不能修改。

【举例】

根据报文的颜色标记报文的丢弃优先级。

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] car cir 1600
[Sysname-behavior-behavior1] primap color-map-dp
```

【相关命令】

- **primap pre-defined**
- **primap pre-defined color**

1.2.8 primap pre-defined color

primap pre-defined color 命令用来配置流行为中的动作为使用预先定义的带颜色优先级映射表为报文获取其他的优先级参数。

undo primap pre-defined color 命令用来取消流行为中的使用预先定义的带颜色优先级映射表为报文映射优先级的动作。

【命令】

primap pre-defined color { **dot1p-dot1p** | **dot1p-dp** | **dot1p-dscp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **dscp-exp** | **dscp-lp** | **exp-dot1p** | **exp-dp** | **exp-dscp** | **exp-exp** | **exp-lp** }

undo primap pre-defined color { **dot1p-dot1p** | **dot1p-dp** | **dot1p-dscp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **dscp-exp** | **dscp-lp** | **exp-dot1p** | **exp-dp** | **exp-dscp** | **exp-exp** | **exp-lp** }

【缺省情况】

没有配置流优先级映射动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

dot1p-dot1p：802.1p 优先级到 802.1p 优先级映射表。

dot1p-dp：802.1p 优先级到丢弃优先级映射表。

dot1p-dscp：802.1p 优先级到 DSCP 映射表。

dot1p-exp：802.1p 优先级到 EXP 映射表。

dot1p-lp：802.1p 优先级到本地优先级映射表。

dscp-dot1p：DSCP 到 802.1p 优先级映射表。

dscp-dp：DSCP 到丢弃优先级映射表。

dscp-dscp：DSCP 到 DSCP 映射表。

dscp-exp：DSCP 到 EXP 映射表。

dscp-lp：DSCP 到本地优先级映射表。

exp-dot1p：EXP 到 802.1p 优先级映射表。

exp-dp：EXP 到丢弃优先级映射表。

exp-dscp：EXP 到 DSCP 映射表。

exp-exp：EXP 到 EXP 映射表。

exp-lp：EXP 到本地优先级映射表。

【使用指导】

本命令需要和 CAR 结合在一起使用。

【举例】

使用带颜色的 DSCP 到丢弃优先级映射表为报文获取丢弃优先级参数。

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] car cir 1600
[Sysname-behavior-behavior1] primap pre-defined color dscp-dp
```

【相关命令】

- **display qos map-table color**
- **primap color-map-dp**

1.2.9 redirect

redirect 命令用来为流行为配置流量重定向动作。

undo redirect 命令用来取消流量重定向动作配置。

【命令】

redirect { **cpu** | **interface** *interface-type interface-number* | **slot** *slot-number* | **vsi** *vsi-name* }

undo redirect { **cpu** | **interface** *interface-type interface-number* | **slot** *slot-number* | **vsi** *vsi-name* }

【缺省情况】

没有配置流量重定向动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

cpu：重定向到 CPU。

interface：重定向到指定的接口。

interface-type interface-number：指定接口类型和接口编号，仅支持重定向到 OAP 单板的内联接口。

slot *slot-number*：重定向到指定的单板，*slot-number* 表示单板所在的槽位号。如果未指定本参数，将显示主用主控板的类的配置信息。

vsi *vsi-name*：重定向到指定 VSI（Virtual Station Interface，虚拟服务器接口）。*vsi-name*：表示指定的 VSI 名称，为 1～31 个字符的字符串，区分大小写。

【使用指导】

在配置重定向动作时，同一个流行为中重定向类型只能为重定向到 CPU、重定向到接口、重定向到 VSI 中的一种，以最后一次配置为准。

需要注意的是：

- 从 CSPEX-1204 单板上 PIC 系列子卡的广域网接口收到的报文，不支持重定向到 OAP 单板的内联接口。
- 从 HDLC 捆绑口收到的报文，不支持重定向到 OAP 单板的内联接口。

【举例】

为流行为配置流量重定向动作，重定向到 3 号槽位的单板。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect slot 3
```

【相关命令】

- **classifier behavior**
- **qos policy**
- **traffic behavior**

1.2.10 remark account-level

remark account-level 命令用来重新标记流量计费的级别。

undo remark account-level 命令用来取消配置流量计费的级别。

【命令】

remark account-level *account-level*

undo remark account-level

【缺省情况】

没有重新标记流量计费的级别。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

account-level：流量计费的级别，取值范围为 1～8。

【举例】

重新标记流量计费级别的值为 3。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark account-level 3
```

1.2.11 remark dot1p

remark dot1p 命令用来重新标记报文的 802.1p 优先级或配置内外层标签优先级复制功能。

undo remark dot1p 命令用来取消标记报文的 802.1p 优先级或内外层标签优先级复制功能。

【命令】

remark [**green** | **red** | **yellow**] **dot1p** *dot1p-value*

undo remark [**green** | **red** | **yellow**] **dot1p**

remark dot1p customer-dot1p-trust

undo remark dot1p

【缺省情况】

没有配置重新标记报文的动作或没有配置内外层标签优先级复制功能。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

green：对绿色报文进行重标记。CSPEX-1204 单板不支持对绿色报文进行重标记。

red：对红色报文进行重标记。CSPEX-1204 单板不支持对红色报文进行重标记。

yellow：对黄色报文进行重标记。CSPEX-1204 单板不支持对黄色报文进行重标记。

dot1p-value：802.1p 优先级，取值范围为 0～7。

customer-dot1p-trust：QoS 策略应用到端口后，将内层 VLAN tag 的 802.1p 优先级复制为外层 VLAN tag 的 802.1p 优先级。

【使用指导】

- 命令 **remark dot1p** *dot1p-value* 和 **remark dot1p customer-dot1p-trust** 是覆盖关系。
- 如果报文只携带一层 VLAN tag，则配置 **remark dot1p customer-dot1p-trust** 不会生效。
- 引用了 **remark dot1p customer-dot1p-trust** 动作的 QoS 策略不支持应用在出方向。

【举例】

重新标记报文的 802.1p 优先级值为 2。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

配置内外层标签优先级复制功能。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p customer-dot1p-trust
```

1.2.12 remark drop-precedence

remark drop-precedence 命令用来重新标记报文的丢弃优先级。

undo remark drop-precedence 命令用来恢复缺省情况。

【命令】

remark drop-precedence *drop-precedence-value*

undo remark drop-precedence

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

drop-precedence-value：丢弃优先级，取值范围为 0～2。

【使用指导】

本命令仅应用在入方向。

【举例】

重新标记报文的丢弃优先级值为 2。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark drop-precedence 2
```

1.2.13 remark dscp

remark dscp 命令用来重新标记报文的 DSCP 值。

undo remark dscp 命令用来取消标记报文的 DSCP 值。

【命令】

remark [**green** | **red** | **yellow**] **dscp** *dscp-value*

undo remark [**green** | **red** | **yellow**] **dscp**

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

green：对绿色报文进行重标记。CSPEX-1204 单板不支持对绿色报文进行重标记。

red：对红色报文进行重标记。CSPEX-1204 单板不支持对红色报文进行重标记。

yellow：对黄色报文进行重标记。CSPEX-1204 单板不支持对黄色报文进行重标记。

dscp-value：DSCP值，取值范围为 0～63，也可以是关键字，如 表 1-4 所示。

表1-4 DSCP 关键字与值的对应表

关键字	DSCP 值（二进制）	DSCP 值（十进制）
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

【举例】

重新标记报文的 DSCP 值为 6。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

1.2.14 remark ip-precedence

remark ip-precedence 命令用来重新标记报文的 IP 优先级。

undo remark ip-precedence 命令用来取消标记报文的 IP 优先级。

【命令】

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

ip-precedence-value：IP 优先级，取值范围为 0～7。

【举例】

重新标记报文的 IP 优先级值为 6。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark ip-precedence 6
```

1.2.15 remark local-precedence

remark local-precedence 命令用来重新标记报文的本地优先级。

undo remark local-precedence 命令用来取消标记报文的本地优先级。

【命令】

remark [**green** | **red** | **yellow**] **local-precedence** *local-precedence-value*

undo remark [**green** | **red** | **yellow**] **local-precedence**

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

green：对绿色报文进行重标记。CSPEX-1204 单板不支持对绿色报文进行重标记。

red：对红色报文进行重标记。CSPEX-1204 单板不支持对红色报文进行重标记。

yellow：对黄色报文进行重标记。CSPEX-1204 单板不支持对黄色报文进行重标记。

local-precedence-value：本地优先级，取值范围为 0～7。

【使用指导】

本命令仅应用在入方向。

【举例】

重新标记报文的本地优先级值为 2。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark local-precedence 2
```

1.2.16 remark qos-local-id

remark qos-local-id 命令用来重新标记报文的 QoS 本地 ID 值。

undo remark qos-local-id 命令用来恢复缺省情况。

【命令】

remark qos-local-id *local-id-value*

undo remark qos-local-id

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

local-id-value：QoS 本地 ID 值，取值范围为 1～4095。

【使用指导】

- 重标记 QoS 本地 ID 功能可以将匹配不同分类条件的多种报文划分到一个新的类（使用 QoS 本地 ID 进行标识），用户在对各类报文配置了原有分类对应的流行为之后，还可以针对这个新的分类实施另外的流行为，该流行为将对所有新类中的报文生效，从而实现对某一类报文的两层控制动作。
- 重标记 QoS 本地 ID 的动作仅能应用在入方向。

【举例】

重新标记报文的 QoS 本地 ID 值为 2。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark qos-local-id 2
```

1.2.17 traffic behavior

traffic behavior 命令用来定义一个流行为，并进入流行为视图。

undo traffic behavior 命令用来删除一个流行为。

【命令】

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

【缺省情况】

没有定义流行为。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

behavior-name：流行为名，为 1～31 个字符的字符串，区分大小写。

【举例】

定义一个名为 behavior1 的流行为。

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

【相关命令】

- **display traffic behavior**

1.3 定义策略和应用策略的命令

1.3.1 classifier behavior

classifier behavior 命令用来为类指定流行为。

undo classifier 命令用来取消为类指定的流行为。

【命令】

classifier *classifier-name* **behavior** *behavior-name* [**mode dcbx**]

undo classifier *classifier-name*

【缺省情况】

没有为类指定流行为。

【视图】

策略视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

classifier-name：类名，为 1～31 个字符的字符串，区分大小写。

behavior-name：流行为名，为 1～31 个字符的字符串，区分大小写。

mode dcbx：表示该策略为 DCBX（Data Center Bridging Exchange Protocol，数据中心桥能力交换协议）模式。有关 DCBX 的介绍，请参见“二层技术-以太网交换配置指导”中的“LLDP”。目前暂不支持该参数。

【使用指导】

- 策略下每个类只能与一个流行为关联。
- 如果配置本命令时指定的类和流行为不存在，系统将创建一个空的类和空的流行为。

【举例】

在策略 user1 中为类 database 指定采用流行为 test。

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
```

【相关命令】

- **qos policy**

1.3.2 control-plane

control-plane 命令用来进入控制平面视图。

【命令】

control-plane slot *slot-number*

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

slot *slot-number*：指定单板。*slot-number* 表示单板所在的槽位号。

【举例】

进入 3 号板控制平面视图。

```
<Sysname> system-view
[Sysname] control-plane slot 3
[Sysname-cp-slot3]
```

1.3.3 display qos policy

display qos policy 命令用来显示 QoS 策略的配置信息。

【命令】

display qos policy user-defined [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

user-defined：用户定义策略。

policy-name：策略名，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则显示所有用户定义策略的配置信息。

classifier *classifier-name*：策略中的类名，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则显示策略中所有类相关的配置信息。

slot *slot-number*：显示指定单板的策略的信息，*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示主用主控板的 QoS 策略的配置信息。

【举例】

显示用户定义策略的配置信息。

```
<Sysname> display qos policy user-defined

  User-defined QoS policy information:

  Policy: 1 (ID 100)
   Classifier: 1 (ID 100)
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 7000 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
   Classifier: 2 (ID 101)
     Behavior: 2
      Accounting enable: Packet
      Filter enable: Permit
      Marking:
        Remark dot1p 1
   Classifier: 3 (ID 102)
     Behavior: 3
      -none-
```

表1-5 display qos policy 命令显示信息描述表

字段	描述
User-defined QoS policy information	用户自定义策略的信息
Policy	策略名

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.4 display qos policy control-plane

display qos policy control-plane 命令用来显示控制平面应用 QoS 策略的信息。

【命令】

display qos policy control-plane slot *slot-number*

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

slot *slot-number*：显示指定单板的控制平面应用 QoS 策略的信息，*slot-number* 表示单板所在的槽位号。

【举例】

显示应用到控制平面的 QoS 策略信息。

```
<Sysname> display qos policy control-plane slot 3

Control plane slot 3

  Direction: Inbound

  Policy: copp
   Classifier: 3000
     Operator: OR
     Rule(s) :
      If-match control-plane protocol arp
     Behavior: copp
      Committed Access Rate:
        CIR 100 (kbps), CBS 6250 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 14 (Packets)
        Red packets   : 0 (Packets)
```

表1-6 display qos policy control-plane 命令显示信息描述表

字段	描述
Direction	对进入控制平面（Inbound）的报文应用QoS策略
Green packets	绿色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-5。

1.3.5 display qos policy control-plane pre-defined

display qos policy control-plane pre-defined 命令用来显示系统预定义的控制平面应用 QoS 策略的信息。

【命令】

display qos policy control-plane pre-defined [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

slot *slot-number*：显示指定单板的系统预定义的控制平面策略信息，*slot-number* 表示单板所在的槽位号。

【使用指导】

如果不指定槽位号，则显示所有在位单板的系统预定义的控制平面应用 QoS 策略的信息。

【举例】

显示 3 号板系统预定义的控制平面应用 QoS 策略的信息。

```
<Sysname> display qos policy control-plane pre-defined slot 3
Pre-defined policy information slot 2
  Protocol          Priority   Bandwidth (kbps)   Group
  Default           N/A        7168               N/A
  IS-IS             29         8192               critical
  VRRP              36         512                important
  OSPF Multicast    30         5120               critical
  OSPF Unicast      30         5120               critical
  IGMP              18         512                important
  OSFPv3 Unicast    30         5120               critical
  OSPFv3 Multicast  30         5120               critical
  VRRPv6            36         512                important
```

```
ARP                12          1024              normal
DHCP Snooping      18          256               redirect
DHCP               18          256               normal
802.1x             12          128               important
STP                36          256               critical
LACP               36          64                critical
GVRP               18          256               critical
BGP                24          1024              critical
ICMP               9           512               monitor
TTL Expires        18          64                monitor
IPOPTION           18          64                normal
BGPv6              24          1024              critical
Hop Limit Expires  18          64                monitor
IPOPTIONv6         18          64                normal
LLDP               24          64                important
DLDP               24          64                critical
TELNET             8           512               management
SSH                8           512               management
TACACS             8           512               management
RADIUS             8           512               management
HTTP               12          64                management
HTTPS              12          64                management
SNMP               8           512               management
ARP Snooping       18          1024              redirect
ICMPv6             8           512               monitor
DHCPv6             18          256               normal
BFD                31          256               critical
```

表1-7 display qos policy control-plane pre-defined 命令显示信息描述表

字段	描述
Pre-defined control plane policy	预定义控制平面策略内容
Protocol	系统预定义协议报文类型
Priority	优先级
Bandwidth	带宽
Group	控制平面协议组

1.3.6 display qos policy global

display qos policy global 命令用来显示基于全局应用 QoS 策略的信息。

【命令】

display qos policy global [**slot** *slot-number*] [**inbound** | **outbound**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

inbound：显示对全局接收到的报文应用 QoS 策略的信息。

outbound：显示对全局发送的报文应用 QoS 策略的信息。

slot *slot-number*：显示指定单板的基于全局应用 QoS 策略的信息，*slot-number* 表示单板所在的槽位号。

【使用指导】

- 如果未指定显示方向，则同时显示出入两个方向基于全局应用 QoS 策略的信息。
- 如果未指定槽位号，则显示主控板上基于全局应用 QoS 策略的信息，不显示各单板的信息。

【举例】

显示基于全局应用 QoS 策略的信息。

```
<Sysname> display qos policy global inbound

  Direction: Inbound

  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 7000 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dot1p 1
```

表1-8 display qos policy global 命令显示信息描述表

字段	描述
Direction	对接收到（Inbound）/发送（Outbound）的报文应用QoS策略
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.7 display qos policy interface

display qos policy interface 命令用来显示接口上 QoS 策略的配置信息和运行情况。

【命令】

display qos policy interface [*interface-type interface-number*] [**inbound** | **outbound**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口上 QoS 策略的配置信息和运行情况。

inbound：显示对接口接收到的报文应用 QoS 策略的信息。

outbound：显示对接口发送的报文应用 QoS 策略的信息。

【使用指导】

如果未指定显示方向，则同时显示出入两个方向接口上应用 QoS 策略的配置信息和运行情况。

【举例】

显示对接口 GigabitEthernet3/0/1 接收到的报文应用 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy interface gigabitethernet 3/0/1 inbound

Interface: GigabitEthernet3/0/1

  Direction: Inbound

  Policy: 1
   Classifier: 1
     Operator: AND
```

```
    Rule(s) :
     If-match acl 2000
    Behavior: 1
     Marking:
       Remark dscp 3
     Committed Access Rate:
       CIR 112 (kbps), CBS 7000 (Bytes), EBS 512 (Bytes)
       Green action  : pass
       Yellow action : pass
       Red action    : discard
       Green packets : 0 (Packets)
  Classifier: 2
    Operator: AND
    Rule(s) :
     If-match protocol ipv6
    Behavior: 2
     Accounting enable:
       0 (Packets)
     Filter enable: Permit
     Marking:
       Remark dot1p 1
```

表1-9 display qos policy interface 命令显示信息描述表

字段	描述
Direction	Policy应用在接口的方向
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.8 display qos vlan-policy

display qos vlan-policy 命令用来显示基于 VLAN 应用 QoS 策略的信息。

【命令】

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

name *policy-name*：显示指定策略名称的基于 VLAN 应用 QoS 策略的信息。*policy-name* 表示策略名称，为 1～31 个字符的字符串，区分大小写。

vlan *vlan-id*：显示指定 VLAN 上应用 QoS 策略的信息。*vlan-id* 为指定 VLAN 的 ID 号，取值范围为 1～4093。

inbound：显示对 VLAN 接收到的报文应用的 QoS 策略信息。

outbound：显示对 VLAN 发送的报文应用的 QoS 策略信息。

slot *slot-number*：显示指定单板上基于 VLAN 应用 QoS 策略的信息，*slot-number* 表示单板所在的槽位号。

【使用指导】

- 如果未指定显示方向，则同时显示出入两个方向基于 VLAN 应用 QoS 策略的信息。
- 如果未指定槽位号，则显示设备上所有基于 VLAN 应用 QoS 策略的信息。

【举例】

显示 VLAN 2 的 QoS 策略信息。

```
<Sysname> display qos vlan-policy vlan 2

Vlan 2

  Direction: Outbound

  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 7000 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0(Packets)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
```

```
Remark dot1p 1
```

表1-10 display qos vlan-policy 命令显示信息描述表

字段	描述
Direction	对VLAN接收到（Inbound）/发送（Outbound）的报文应用QoS策略
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.9 qos apply policy (interface view, control plane view)

qos apply policy 命令用来在接口或控制平面上应用 QoS 策略。

undo qos apply policy 命令用来取消接口或控制平面上应用的 QoS 策略。

【命令】

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

【缺省情况】

没有在接口或控制平面上应用 QoS 策略。

【视图】

接口视图/控制平面视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

policy-name：策略名，为 1～31 个字符的字符串，区分大小写。

inbound：对接口或控制平面接收到的报文应用 QoS 策略。

outbound：对接口发送的报文应用 QoS 策略。

【使用指导】

需要注意的是，应用策略时 inbound 和 outbound 方向的支持情况和流行为中定义的动作有关，详细情况如下表所示。

表1-11 单板对 QoS 策略的支持情况

动作	单板入方向（inbound）	单板出方向（outbound）
流量统计	支持	支持
流量监管	支持	支持
流量过滤	支持	支持

动作	单板入方向（inbound）	单板出方向（outbound）
流镜像	支持	支持
封装外层VLAN标签	支持	不支持
重定向	支持	不支持
标记报文的802.1p优先级	支持	支持
标记报文的丢弃优先级	支持	不支持
标记报文的DSCP优先级	支持	支持
标记报文的IP优先级	支持	支持
标记报文的本地优先级	支持	不支持
标记报文的qos-local-id	支持	不支持

【举例】

将策略 USER1 应用到接口 GigabitEthernet3/0/1 的出方向上。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos apply policy USER1 outbound
```

对进入 3 号槽控制平面的报文应用策略 aaa。

```
<Sysname> system-view
[Sysname] control-plane slot 3
[Sysname-cp-slot3] qos apply policy aaa inbound
```

1.3.10 qos apply policy (user-profile view)

qos apply policy 命令用来在 User Profile 下应用策略。

undo qos apply policy 命令用来取消 User Profile 下应用的策略。

【命令】

qos apply policy *policy-name* { **inbound** | **outbound** }

undo qos apply policy *policy-name* { **inbound** | **outbound** }

【缺省情况】

没有在 User Profile 下应用 QoS 策略。

【视图】

User Profile 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

inbound：入方向，对设备接收的上线用户流量（即上线用户发送的流量）应用策略。

outbound：出方向，对设备发送的上线用户流量（即上线用户接收的流量）应用策略。

policy-name：策略名，为 1～31 个字符的字符串。

【使用指导】

User Profile 被删除将导致其下引用的 QoS 策略被删除。

【举例】

对设备发送的上线用户 user 的流量应用策略 test（该策略已经建立）。

```
<Sysname> system-view
[Sysname] user-profile user
[Sysname-user-profile-user] qos apply policy test outbound
```

1.3.11 qos apply policy global

qos apply policy global 命令用来全局应用 QoS 策略。

undo qos apply policy global 命令用来取消全局应用的 QoS 策略。

【命令】

qos apply policy *policy-name* **global** { **inbound** | **outbound** }

undo qos apply policy *policy-name* **global** { **inbound** | **outbound** }

【缺省情况】

没有在全局应用 QoS 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

policy-name：策略名，为 1～31 个字符的字符串，区分大小写。

inbound：对设备所有端口接收到的流量应用 QoS 策略。

outbound：对设备所有端口发送的流量应用 QoS 策略，当前设备暂不支持该参数。

【使用指导】

全局应用的 QoS 策略对全部流量生效。

【举例】

将名为 user1 的策略应用到全局的入方向上。

```
<Sysname> system-view
[Sysname] qos apply policy user1 global inbound
```

1.3.12 qos policy

qos policy 命令用来定义一个策略，并进入策略视图。

undo qos policy 命令用来删除一个策略。

【命令】

qos policy *policy-name*

undo qos policy *policy-name*

【缺省情况】

没有定义策略。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

policy-name：策略名，为 1～31 个字符的字符串，区分大小写。

【使用指导】

如果该策略已经被应用，则不允许删除该策略，需要先在应用的位置上取消对该策略的应用，然后再使用 **undo qos policy** 命令删除该策略。

【举例】

定义一个名为 user1 的策略。

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

【相关命令】

- **classifier behavior**
- **qos apply policy**
- **qos apply policy global**
- **qos vlan-policy**

1.3.13 qos vlan-policy

qos vlan-policy 命令用来在指定 VLAN 上应用 QoS 策略。

undo qos vlan-policy 命令用来取消指定 VLAN 上应用的 QoS 策略。

【命令】

qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

undo qos vlan-policy *policy-name* **vlan** *vlan-id-list* { **inbound** | **outbound** }

【缺省情况】

没有在指定 VLAN 上应用 QoS 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

policy-name：策略名称，为 1～31 个字符的字符串，区分大小写。

vlan-id-list：VLAN ID 列表，形式可以是 *vlan-id* **to** *vlan-id*，其中，*vlan-id* 为指定 VLAN 的 ID 号，取值范围为 1～4093。可以输入多个不连续的 VLAN ID，中间以空格隔开。设备最多允许用户同时指定 8 个 VLAN ID。

inbound：对 VLAN 接收到的报文应用 QoS 策略。

outbound：对 VLAN 发送的报文应用 QoS 策略。

【举例】

在 VLAN 200、300、400、500 的入方向上应用 VLAN 策略 test。

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 inbound
```

1.3.14 reset qos policy control-plane

reset qos policy control-plane 命令用来清除控制平面应用 QoS 策略的统计信息。

【命令】

reset qos policy control-plane slot *slot-number*

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

slot *slot-number*：清除指定单板的基于控制平面应用 QoS 策略的统计信息，*slot-number* 表示单板所在的槽位号。

【举例】

清除应用到 3 号板控制平面的 QoS 策略统计信息。

```
<Sysname> reset qos policy control-plane slot 3
```

1.3.15 reset qos policy global

reset qos policy global 命令用来清除全局应用的 QoS 策略的统计信息。

【命令】

reset qos policy global [**inbound** | **outbound**]

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

inbound：清除全局接收到的报文应用 QoS 策略的统计信息。

outbound：清除全局发送的报文应用 QoS 策略的统计信息。

【使用指导】

如果不指定方向，则同时清除出入两个方向全局应用的 QoS 策略的统计信息。

【举例】

清除全局入方向应用的 QoS 策略的统计信息。

```
<Sysname> reset qos policy global inbound
```

1.3.16 reset qos vlan-policy

reset qos vlan-policy 命令用来清除 VLAN 应用的 QoS 策略的统计信息。

【命令】

reset qos vlan-policy [**vlan** *vlan-id*] [**inbound** | **outbound**]

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

vlan *vlan-id*：指定 VLAN。*vlan-id* 为指定 VLAN 的 ID 号，取值范围为 1～4093。

inbound：清除 VLAN 接收到的报文应用 QoS 策略的统计信息。

outbound：清除对 VLAN 发送的报文应用 QoS 策略的统计信息。

【使用指导】

如果不指定方向，则同时清除出入两个方向 VLAN 应用的 QoS 策略的统计信息。

【举例】

清除 VLAN 2 应用的 QoS 策略的统计信息。

```
<Sysname> reset qos vlan-policy vlan 2
```

2 优先级映射

2.1 优先级映射表配置命令

2.1.1 display qos map-table

display qos map-table 命令用来显示指定优先级映射表配置情况。

【命令】

display qos map-table [**inbound** [**dot1p-dot1p** | **dot1p-dp** | **dot1p-dscp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **dscp-exp** | **dscp-lp** | **exp-dot1p** | **exp-dp** | **exp-dscp** | **exp-exp** | **exp-lp**]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

表2-1 优先级映射表

优先级映射	描述
dot1p-dot1p	802.1p优先级到802.1p优先级映射表
dot1p-dp	802.1p优先级到丢弃优先级映射表
dot1p-dscp	802.1p优先级到DSCP映射表
dot1p-exp	802.1p优先级到EXP映射表
dot1p-lp	802.1p优先级到本地优先级映射表
dscp-dot1p	DSCP到802.1p优先级映射表
dscp-dp	DSCP到丢弃优先级映射表
dscp-dscp	DSCP到DSCP映射表
dscp-exp	DSCP到EXP映射表
dscp-lp	DSCP到本地优先级映射表
exp-dot1p	EXP到802.1p优先级映射表
exp-dp	EXP到丢弃优先级映射表
exp-dscp	EXP到DSCP映射表

优先级映射	描述
exp-exp	EXP到EXP映射表
exp-lp	EXP到本地优先级映射表

【使用指导】

如果未指定表的类型，将显示所有映射表的配置情况。

【举例】

显示 802.1p 优先级到本地优先级映射表的配置信息。

```
<Sysname> display qos map-table dot1p-lp
MAP-TABLE NAME: dot1p-lp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

表2-2 display qos map-table 命令显示信息描述表

字段	描述
MAP-TABLE NAME	映射表的名字
TYPE	映射表的类型
IMPORT	映射表的输入值
EXPORT	映射表的输出值

2.1.2 display qos map-table color

display qos map-table color 命令用来显示指定带颜色优先级映射表配置情况。

【命令】

display qos map-table color [**green** | **yellow** | **red**] { **inbound** [**dot1p-dot1p** | **dot1p-dp** | **dot1p-dscp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **dscp-exp** | **dscp-lp** | **exp-dot1p** | **exp-dp** | **exp-dscp** | **exp-exp** | **exp-lp**] | **outbound** [**dot1p-dot1p** | **dot1p-dscp** | **dot1p-exp** | **dscp-dot1p** | **dscp-dscp** | **dscp-exp** | **exp-dot1p** | **exp-dscp** | **exp-exp**] }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

green：绿色报文。

yellow：黄色报文。

red：红色报文。

inbound：接收报文方向。

outbound：发送报文方向。

其它参数请参见 表 2-1。

【使用指导】

经过流量监管处理的报文被分成了三种颜色（绿色、黄色、红色），为了对不同颜色报文进行优先级映射，设备提供了多张带颜色优先级映射表，分别对应相应颜色的优先级映射关系。流量监管对报文处理的相关内容请参见流量监管章节内容。

- 如果未指定表的类型，将显示所有带颜色映射表的配置情况。
- 如果未指定颜色，将显示所有颜色的带颜色映射表的配置情况。
- 如果未指定方向，将显示所有方向带颜色映射表的配置情况。

【举例】

显示绿色报文的接收报文方向的 EXP 到本地优先级映射表的配置信息。

```
<Sysname> display qos map-table color green inbound exp-lp
MAP-TABLE NAME: exp-lp   TYPE: pre-define   COLOR: green   DIRECTION: inbound
IMPORT  :  EXPORT
   0    :    0
   1    :    1
   2    :    2
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

表2-3 display qos map-table color 命令显示信息描述表

字段	描述
MAP-TABLE NAME	映射表的名字
TYPE	映射表的类型
COLOR	映射表的颜色
DIRECTION	映射表的方向
IMPORT	映射表的输入值
EXPORT	映射表的输出值

2.1.3 import

import 命令用来配置指定优先级映射表的映射关系。

undo import 命令用来删除配置的优先级映射表的映射关系，恢复其为缺省的映射关系。

【命令】

import *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

【缺省情况】

优先级映射表的映射关系请参见配置指导中的附录 B。

【视图】

优先级映射表视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

import-value-list：输入值列表。

export-value：输出值。

all：删除配置地该映射表的所有映射关系，恢复其为缺省的映射关系。

【举例】

配置 802.1p 优先级到丢弃优先级映射表的映射关系，与 802.1p 优先级 4、5 相对应的丢弃优先级为 1。

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp] import 4 5 export 1
```

【相关命令】

- **display qos map-table**

2.1.4 qos map-table

qos map-table 命令用来进入指定的优先级映射表视图。

【命令】

qos map-table inbound { **dot1p-dot1p** | **dot1p-dp** | **dot1p-dscp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **dscp-exp** | **dscp-lp** | **exp-dot1p** | **exp-dp** | **exp-dscp** | **exp-exp** | **exp-lp** }

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

其它参数请参见 表 2-1。

【举例】

进入 802.1p 优先级到丢弃优先级映射表视图。

```
<Sysname> system-view
[Sysname] qos map-table dot1p-dp
[Sysname-maptbl-dot1p-dp]
```

【相关命令】

- **display qos map-table**
- **import**

2.1.5 qos map-table color

qos map-table color 命令用来进入指定的带颜色优先级映射表视图。

【命令】

qos map-table color { **green** | **yellow** | **red** } { **inbound** { **dot1p-dot1p** | **dot1p-dp** | **dot1p-dscp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **dscp-exp** | **dscp-lp** | **exp-dot1p** | **exp-dp** | **exp-dscp** | **exp-exp** | **exp-lp** } | **outbound** { **dot1p-dot1p** | **dot1p-dscp** | **dot1p-exp** | **dscp-dot1p** | **dscp-dscp** | **dscp-exp** | **exp-dot1p** | **exp-dscp** | **exp-exp** } }

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

green：绿色报文。

yellow：黄色报文。

red：红色报文。

inbound：接收报文方向。

outbound：发送报文方向。

其它参数请参见 表 2-1。

【使用指导】

经过流量监管处理的报文被分成了三种颜色（绿色、黄色、红色），为了对不同颜色报文进行优先级映射，设备提供了多张带颜色优先级映射表，分别对应相应颜色的优先级映射关系。流量监管对报文处理的相关内容请参见流量监管章节内容。

每个优先级映射（颜色也相同）存在无方向、接收报文方向、发送报文方向三张不同的映射表。如果不指定方向，则表示进入无方向的优先级映射表视图。

【举例】

进入绿色报文的 EXP 到本地优先级映射表视图。

```
<Sysname> system-view
[Sysname] qos map-table color green exp-lp
[Sysname-maptbl-green-exp-lp]
```

进入红色报文的接收报文方向的 DSCP 到本地优先级映射表视图。

```
<Sysname> system-view
[Sysname] qos map-table color red inbound dscp-lp
[Sysname-maptbl-red-in-dscp-lp]
```

【相关命令】

- **display qos map-table color**
- **import**

2.2 端口优先级配置命令

2.2.1 qos priority

qos priority 命令用来配置当前端口的端口优先级。

undo qos priority 命令用来恢复端口优先级为缺省值。

【命令】

qos priority [**dot1p** | **dscp** | **exp**] *priority-value*

undo qos priority

【缺省情况】

端口优先级的缺省值为 0。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

priority-value：端口优先级值。当不指定端口优先级类型时，取值范围为 0～7；当设备支持多种类型的端口优先级时，各优先级的取值范围如 表 2-4 所示。

表2-4 各种端口优先级取值范围

端口优先级类型	*priority-value* 取值范围	说明
dot1p（802.1p优先级）	0～7	仅CSPEX-1204支持该参数
dscp（DSCP优先级）	0～63	仅CSPEX-1204支持该参数
exp（EXP优先级）	0～7	仅CSPEX-1204支持该参数

【举例】

配置接口 GigabitEthernet3/0/1 的端口优先级为 2。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos priority 2
```

【相关命令】

- **display qos trust interface**

2.3 端口优先级信任模式配置命令

2.3.1 display qos trust interface

display qos trust interface 命令用来显示当前配置的端口优先级信任模式信息和端口优先级的信息。

【命令】

display qos trust interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

interface-type interface-number：指定的接口类型和接口编号。如果未指定本参数，将显示所有接口的端口优先级信任模式信息。

【举例】

显示当前配置的端口优先级信任模式信息。

```
<Sysname> display qos trust interface gigabitethernet 3/0/1
Interface: GigabitEthernet3/0/1
 Port priority trust information
  Port priority:4
  Port priority trust type: auto
```

表2-5 display qos trust interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号构成
Port priority trust information	端口优先级信任信息
Port priority	端口优先级

字段	描述
Port priority trust type	端口优先级信任类型，取值为： • auto：根据报文的类型，自动提取报文中的优先级字段

2.3.2 qos trust

qos trust 命令用来配置端口优先级信任模式。

undo qos trust 命令用来恢复缺省情况。

【命令】

qos trust auto

undo qos trust

【缺省情况】

缺省情况下，端口信任模式为 none，即不信任任何优先级。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

auto：表示根据报文的类型，自动提取报文中的优先级字段进行优先级映射。对于只有非 IP 报文，采用 802.1p 优先级；对于 IP 报文，采用 IP 优先级；对于 MPLS 报文，采用 EXP。

【举例】

在接口 GigabitEthernet3/0/1 上配置优先级信任模式为为 auto 模式。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos trust auto
```

【相关命令】

- **display qos trust interface**

3 流量整形和接口限速

3.1 流量监管配置命令

3.1.1 qos car (user-profile view)

qos car 命令用来在 User Profile 下应用 CAR 策略。

undo qos car 命令用来取消应用的 CAR 策略。

【命令】

qos car { **inbound** | **outbound** } **any cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*]

undo qos car { **inbound** | **outbound** }

【缺省情况】

没有配置流量监管。

【视图】

User Profile 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

inbound：对上线用户发送的报文进行限速。

outbound：对上线用户接收到的报文进行限速。

any：对所有的 IP 数据包进行限速。

cir *committed-information-rate*：承诺信息速率，单位为 kbps，取值范围为 8～160000000，实际生效的承诺信息速率为 *committed-information-rate* / 8 的商值，四舍五入取整数后再乘以 8。

cbs *committed-burst-size*：承诺突发尺寸，即实际平均速率在承诺速率以内时的突发流量，单位为 byte。

- 如果不指定 **cbs** 参数，缺省取值为 62.5 × *committed-information-rate* 的乘积。
- 如果指定 **cbs** 参数，取值范围 512～256000000。

实际生效的承诺突发尺寸为 *committee-burst-size* / 512 的商值，四舍五入取整数后再乘以 512。

ebs *excess-burst-size*：过度突发尺寸，单位为 byte，缺省值为 0 byte，取值范围为 0～256000000，实际生效的超出突发尺寸为 *excess-burst-size* / 512 的商值，四舍五入取整数后再乘以 512。

pir *peak-information-rate*：峰值速率，单位为 kbps，取值范围为 8～160000000，实际生效的峰值速率为 *peak-information-rate* / 8 的商值，四舍五入取整数后再乘以 8。

【使用指导】

数据流量符合承诺速率时，允许数据包通过；数据流量不符合承诺速率时，丢弃数据包。

如果多次重复使用该命令，则最后一次配置生效。

本命令仅 CSPEX-1204 单板支持。

【举例】

对上线用户 user 接收的报文进行流量监管。报文正常流速为 200kbps，允许 50000byte 的突发流量通过，速率小于等于 200kbps 时正常发送，大于 200kbps 时，报文被丢弃。

```
<Sysname> system-view
[Sysname] user-profile user
[Sysname-user-profile-user] qos car outbound any cir 200 cbs 50000
```

3.2 流量整形配置命令

3.2.1 display qos gts interface

display qos gts interface 命令用来显示接口的流量整形配置情况和统计信息。

【命令】

display qos gts interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口的流量整形配置情况和统计信息。

【举例】

显示所有接口的流量整形配置情况和统计信息。

```
<Sysname> display qos gts interface
Interface: GigabitEthernet3/0/1
Rule: If-match queue 1
  CIR 128 (kbps), CBS 8192 (Bytes)
 Rule: If-match queue 2
  CIR 256 (kbps), CBS 16384 (Bytes)
```

表3-1 display qos gts 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Rule	匹配规则
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，也就是容纳突发流量的令牌桶深度，单位为byte

3.2.2 qos gts

qos gts 命令用来在接口上配置流量整形。

undo qos gts 命令用来取消接口上流量整形的配置。

【命令】

qos gts queue *queue-id* **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos gts queue *queue-id*

【缺省情况】

接口上没有配置流量整形。

【视图】

以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue *id*：对队列 queue 上的数据包进行流量整形，*queue-id* 为匹配的队列号。

cir *committed-information-rate*：承诺信息速率，单位为 kbps。千兆端口的取值范围为 8～1000000，万兆端口的取值范围为 8～10000000，实际生效的承诺信息速率为 *committed-information-rate* / 8 的商值，四舍五入取整数后再乘以 8。

cbs *committed-burst-size*：承诺突发尺寸，单位为 byte。

- 如果不指定 **cbs** 参数，*committed-burst-size* 缺省取值为 62.5ms**committed-information-rate*。
- 如果指定 **cbs** 参数，取值范围为 512～16000000。

实际生效的承诺突发尺寸为 *committee-burst-size* / 512 的商值，四舍五入取整数后再乘以 512。

【使用指导】

需要注意的是，CSPEX-1204 单板上，同一接口不能同时应用配置了加权轮询调度的队列调度策略和流量整形。

【举例】

在接口 GigabitEthernet3/0/1 上对队列 1 中的报文进行流量整形。正常流速为 6400kbps，突发流量为 51200bytes。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos gts queue 1 cir 6400 cbs 51200
```

3.3 接口限速配置命令

3.3.1 display qos lr interface

display qos lr interface 命令用来显示接口的接口限速配置情况和统计信息。

【命令】

display qos lr interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口的接口限速配置情况和运行统计信息。

【举例】

显示所有接口的接口限速配置情况和统计信息。

```
<Sysname> display qos lr interface
Interface : Ten-GigabitEthernet3/0/1
 Direction: Outbound
  CIR 12800 (kbps), CBS 512000 (Bytes)

Interface : Ten-GigabitEthernet3/0/2
 Direction: Outbound
  CIR 25600 (kbps), CBS 512000 (Bytes)
```

表3-2 display qos lr 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Direction	方向，目前只支持Outbound
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，也就是容纳突发流量的令牌桶深度，单位为Byte

3.3.2 qos lr

qos lr 命令用来在接口上配置接口限速。

undo qos lr 命令用来取消接口上配置接口限速的配置。

【命令】

qos lr { **inbound** | **outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos lr { **inbound** | **outbound** }

【缺省情况】

接口上没有配置接口限速。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

inbound：对接口接收的数据流进行限速。目前不支持该参数。

outbound：对接口发送的数据流进行限速。

cir *committed-information-rate*：承诺信息速率，单位为 kbps。千兆端口的取值范围为 300～1000000，万兆端口的取值范围为 2500～10000000。

cbs *committed-burst-size*：承诺突发尺寸，单位为 bytes。

- 如果不指定 **cbs** 参数，*committed-burst-size* 缺省取值为 62.5ms**committed-information-rate*。
- 如果指定 **cbs** 参数，取值范围为 4096～133169152。

【举例】

在接口 GigabitEthernet3/0/1 上出方向的报文进行接口限速。正常流速为 25600kbps，突发流量为 512000bytes。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos lr outbound cir 25600 cbs 512000
```

4 硬件实现拥塞管理

4.1 严格优先级队列配置命令

4.1.1 display qos queue sp

display qos queue sp interface 命令用来显示接口的 SP（Strict Priority，严格优先级）队列配置情况。

【命令】

display qos queue sp interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口的 SP 队列配置情况。

【举例】

显示 GigabitEthernet3/0/1 的严格优先级队列配置情况。

```
<Sysname> display qos queue sp interface gigabitethernet 3/0/1
Interface: GigabitEthernet3/0/1
 Output queue: Strict Priority queuing
```

表4-1 display qos queue sp interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Output queue	当前出队列类型

4.1.2 qos sp

qos sp 命令用来在接口上配置严格优先队列。

undo qos sp 命令用来恢复接口上缺省的队列算法。

【命令】

qos sp

undo qos sp

【缺省情况】

端口采用 SP 调度算法。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【举例】

在接口 GigabitEthernet3/0/1 上应用 SP 模式的队列调度。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos sp
```

【相关命令】

- **display qos queue sp interface**

4.2 加权轮询队列配置命令

4.2.1 display qos queue wrr interface

display qos queue wrr interface 命令用来显示接口的 WRR（Weighted Round Robin，加权轮询）队列配置情况。

【命令】

display qos queue wrr interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口的 WRR 队列配置情况。

【举例】

显示接口 GigabitEthernet3/0/1 的 WRR 队列配置情况。

```
<Sysname> display qos queue wrr interface gigabitethernet 3/0/1
Interface: GigabitEthernet3/0/1
```

```
Output queue: Weighted Round Robin queuing
Queue ID        Group           Weight
----------------------------------------
be              1               1
af1             1               1
af2             1               3
af3             1               4
af4             1               5
ef              1               6
cs6             1               7
cs7             1               8
```

表4-2 display qos queue wrr interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Output queue	当前出队列类型
Queue ID	队列号
Group	分组号，说明队列属于哪一个分组，缺省情况下，队列所属的分组号为1
Weight	各个队列的调度权重，当前WRR队列调度权重的计算方式为Weight， N/A表示该队列采用SP调度算法

4.2.2 qos wrr

qos wrr 命令用于在接口上使能 WRR 队列。

undo qos wrr 命令用于在接口上取消 WRR 队列，恢复缺省的队列算法。

【命令】

qos wrr weight

undo qos wrr weight

【缺省情况】

接口上采用 SP 队列算法。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

weight：表示按照每次轮询可发送的报文个数进行计算。

【使用指导】

必须先使用 **qos wrr** 命令在接口上使能 WRR 队列，然后才能进行 WRR 配置。

【举例】

在接口 GigabitEthernet3/0/1 上使能 WRR 队列。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos wrr weight
```

【相关命令】

- **display qos queue wrr interface**

4.2.3 qos wrr weight

qos wrr weight 命令用来配置 WRR 队列或修改 WRR 队列的参数。

undo qos wrr 命令用来恢复缺省情况。

【命令】

qos wrr *queue-id* **group** { **1** | **2** | **3** | **4** } **weight** *schedule-value*

undo qos wrr *queue-id*

【缺省情况】

在使用 WFQ 队列时，所有队列都处于 WRR 调度组 1 中，调度权重从队列 0 到 7 分别为 1、2、3、4、5、6、7、8。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue-id：队列序号，取值范围为 0～7 或 表 4-3 中的关键字。

group { **1** | **2** | **3** | **4** }：表示该队列属于哪个 WRR 优先组，缺省为 group 1。其中 group 1 表示该队列属于 WRR 优先组 1，group 2 表示该队列属于 WRR 优先组 2，group 3 表示该队列属于 WRR 优先组 3，group 4 表示该队列属于 WRR 优先组 4。各组之间执行优先级调度，由组 1 至组 4 优先级依次降低。目前只支持配置 WRR 优先组 1。

weight：表示按照每次轮询可发送的报文个数进行计算。

schedule-value：配置队列的调度权重，取值范围为 1～15。

【使用指导】

必须先使用 **qos wrr** 命令在接口上使能 WRR 队列，然后才能进行本配置。

*queue-id*除了支持数字外，还支持直接输入关键字，具体情况请参见 表 4-3。

表4-3 *queue-id* 数字和关键字对应表

queue-id 数字	*queue-id* 关键字
0	be
1	af1

queue-id 数字	*queue-id* 关键字
2	af2
3	af3
4	af4
5	ef
6	cs6
7	cs7

【举例】

在接口 GigabitEthernet3/0/1 上应用 WRR 队列，配置队列 0 的调度权重为 100，分组为 1。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos wrr weight
[Sysname-GigabitEthernet3/0/1] qos wrr 0 group 1 weight 100
```

【相关命令】

- **display qos queue wrr interface**
- **qos wrr**

4.2.4 qos wrr group sp

qos wrr group sp 命令用来配置队列加入 SP 组，采用严格优先级调度算法。

undo qos wrr group sp 命令用来恢复缺省情况。

【命令】

qos wrr *queue-id* **group sp**

undo qos wrr *queue-id*

【缺省情况】

当使用 WRR 队列时，所有队列都处于 WRR 调度组中。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue-id：队列序号，取值范围为 0～7 或 表 4-3 中的关键字。

sp：队列加入 SP 组，采用严格优先级调度算法。

【使用指导】

此命令需要在端口队列为 WRR 调度模式下使用。

SP 组与普通 WRR 优先组不同，加入 SP 组的端口队列采用严格优先级调度算法，不再采用加权轮循调度算法。调度时先调度 SP 组，然后调度其他 WRR 优先组。

必须先使用 **qos wrr** 命令在接口上使能 WRR 队列，然后才能进行本配置。

【举例】

在接口 GigabitEthernet3/0/1 上应用 WRR 队列，并配置队列 0 加入 SP 组进行严格优先级调度。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos wrr weight
[Sysname-GigabitEthernet3/0/1] qos wrr 0 group sp
```

【相关命令】

- **display qos queue wrr interface**
- **qos wrr**

4.3 加权公平队列配置命令

4.3.1 display qos queue wfq interface

display qos queue wfq interface 命令用来显示接口的 WFQ 配置情况。

【命令】

display qos queue wfq interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口的 WFQ 配置情况。

【举例】

显示接口 GigabitEthernet3/0/1 的加权公平队列配置情况。

```
<Sysname> display qos queue wfq interface gigabitethernet 3/0/1
Interface: GigabitEthernet3/0/1
 Output queue: Hardware Weighted Fair Queuing
 Queue ID        Weight          Min-Bandwidth
 ----------------------------------------------------------------
 be              1               1               0
 af1             1               1               0
 af2             1               1               0
 af3             1               1               0
```

```
af4             1               1               0
ef              1               1               0
cs6             1               1               0
cs7             1               1               0
```

表4-4 display qos queue wfq interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Output queue	当前出队列类型
Queue ID	队列号
Weight	队列调度权重值
Min-Bandwidth	队列的最小保证带宽值

4.3.2 qos bandwidth queue

qos bandwidth queue 命令用来配置端口队列的最小带宽保证。

undo qos bandwidth queue 命令用来恢复缺省情况。

【命令】

qos bandwidth queue *queue-id* **min** *bandwidth-value*

undo qos bandwidth queue *queue-id*

【缺省情况】

在使用 WFQ 队列时，不提供最小带宽保证。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue-id：队列序号，取值范围为 0～7 或 表 4-3 中的关键字。

min *bandwidth-value*：最小保证带宽值，千兆端口的取值范围为 8～1000000，万兆端口的取值范围为 8～10000000，单位为 kbps，表示端口流量拥塞时能够保证的最小队列带宽。

【使用指导】

必须先使用 **qos wfq** 命令在接口上使能 WFQ 队列，然后才能进行本配置。

【举例】

在接口 GigabitEthernet3/0/1 上配置队列 0 的最小保证带宽值为 100kbps。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos wfq weight
```

```
[Sysname-GigabitEthernet3/0/1] qos bandwidth queue 0 min 100
```

【相关命令】

- **qos wfq**

4.3.3 qos wfq

qos wfq 命令用来在接口上使能 WFQ 队列。

undo qos wfq 命令用来在接口上取消 WFQ 队列，恢复缺省的队列算法。

【命令】

qos wfq weight

undo qos wfq weight

【缺省情况】

接口使用 SP 队列调度算法。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

weight：表示按照权重进行计算。对于 CSPC 单板和 CMPE-1104 单板，表示按照每次轮询可发送的报文个数进行计算；对于 CSPEX-1204 单板，表示按照每次轮询可发送的字节数进行计算。

【使用指导】

必须先使用 **qos wfq** 命令在接口上使能 WFQ 队列，然后才能进行 WFQ 配置。

【举例】

在接口 GigabitEthernet3/0/1 上使能 WFQ 队列。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos wfq weight
```

【相关命令】

- **display qos queue wfq interface**

4.3.4 qos wfq weight

qos wfq weight 命令用来配置 WFQ 队列或修改 WFQ 队列的参数。

undo qos wfq 命令用来恢复缺省情况。

【命令】

qos wfq *queue-id* **weight** *schedule-value*

undo qos wfq *queue-id*

【缺省情况】

在使用 WFQ 队列时，所有队列的调度权重均为 1。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue-id：队列序号，取值范围为 0～7 或 表 4-3 中的关键字。

weight：表示按照权重进行计算。对于 CSPC 单板和 CMPE-1104 单板，表示按照每次轮询可发送的报文个数进行计算；对于 CSPEX-1204 单板，表示按照每次轮询可发送的字节数进行计算。

schedule-value：配置队列的调度权重，取值范围为 1～31。CSPC 单板和 CMPE-1104 单板仅支持配置队列的调度权重取值范围为 1～15。

【使用指导】

必须先使用 **qos wfq** 命令在接口上使能 WFQ 队列，然后才能进行本配置。

【举例】

在接口 GigabitEthernet3/0/1 上应用 WFQ 队列，并按照每次轮询可发送的字节数进行计算，配置队列 0 的调度权重为 10。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos wfq weight
[Sysname-GigabitEthernet3/0/1] qos wfq 0 weight 10
```

【相关命令】

- **display qos queue wfq interface**
- **qos bandwidth queue**
- **qos wfq**

4.4 队列调度策略配置命令

4.4.1 display qos qmprofile configuration

display qos qmprofile configuration 命令用来显示队列调度策略的配置情况。

【命令】

display qos qmprofile configuration [*profile-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

profile-name：队列调度策略名称，为 1～31 个字符的字符串，区分大小写。如果未指定本参数，则显示所有队列调度策略的配置情况。

slot *slot-number*：指定单板。*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示主用主控板的队列调度策略的配置情况。

【使用指导】

本命令仅 CSPEX-1204 单板支持。

【举例】

显示队列调度策略 myprofile 的配置情况。

```
<Sysname> display qos qmprofile configuration myprofile
Queue management profile: myprofile (ID 1)
 Queue ID   Type   Group   Schedule-unit   Value  Min-bandwidth  Service-type
 ------------------------------------------------------------------------------
 be         SP     N/A     N/A             N/A    0              hsi
 af1        SP     N/A     N/A             N/A    0              hsi
 af2        SP     N/A     N/A             N/A    0              hsi
 af3        SP     N/A     N/A             N/A    0              hsi
 af4        SP     N/A     N/A             N/A    0              hsi
 ef         SP     N/A     N/A             N/A    0              hsi
 cs6        SP     N/A     N/A             N/A    0              hsi
 cs7        SP     N/A     N/A             N/A    0              hsi
```

显示所有四队列调度策略的配置情况。

表4-5 display qos qmprofile configuration 命令显示信息描述表

字段	描述
Queue management profile	队列调度策略名称
Queue ID	队列号
Type	队列调度类型，包括SP（严格优先级）、WRR（加权轮询调度）
Group	优先组，N/A表示无效
Schedule unit	队列调度单位，包括weight和byte-count，N/A表示无效
vlaue	• 队列调度单位为 weight 时，表示权重值 • 队列调度单位为 byte-count 时，表示字节个数 • N/A 表示无效
Min Bandwidth	最小保证带宽
Service type	服务类型，包括hsi、stb、voip

4.4.2 display qos qmprofile interface

display qos qmprofile interface 命令用来显示接口的队列调度策略的配置情况。

【命令】

display qos qmprofile interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口的队列调度策略的配置情况。

【使用指导】

本命令仅 CSPEX-1204 单板支持。

【举例】

显示指定接口的队列调度策略的配置情况。

```
<Sysname> display qos qmprofile interface gigabitethernet 3/1/1
Interface: GigabitEthernet3/1/1
 Queue management profile: myprofile
```

表4-6 display qos qmprofile interface 命令显示信息描述表

字段	描述
Interface	接口名称
Queue management profile	队列调度策略名称

4.4.3 qos apply qmprofile

qos apply qmprofile 命令用来在接口上应用队列调度策略。

undo qos apply qmprofile 命令用来恢复缺省情况。

【命令】

qos apply qmprofile *profile-name*

undo qos apply qmprofile

【缺省情况】

接口使用 SP 队列调度算法。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

profile-name：队列调度策略名称，为 1～31 个字符的字符串，区分大小写。

【使用指导】

每个接口只能应用一个队列调度策略。

本命令仅 CSPEX-1204 单板支持。需要注意的是，同一接口不能同时应用配置了加权轮询调度的队列调度策略和流量整形。

【举例】

在接口上应用队列调度策略 myprofile。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/1/1
[Sysname-GigabitEthernet3/1/1] qos apply qmprofile myprofile
```

【相关命令】

- **display qos qmprofile interface**

4.4.4 qos qmprofile

qos qmprofile 命令用来创建用户自定义的队列调度策略，并进入相应的队列调度策略视图。

undo qos qmprofile 命令用来删除用户自定义的队列调度策略。

【命令】

qos qmprofile [**four-queue**] *profile-name*

undo qos qmprofile [**four-queue**] *profile-name*

【缺省情况】

不存在用户自定义的队列调度策略。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

four-queue：指定队列调度策略为四队列模式。若不指定该参数，则队列调度策略为八队列模式。

profile-name：队列调度策略名称，为 1～31 个字符的字符串，区分大小写。

【使用指导】

不能删除已经应用到接口的队列调度策略，必须先在应用的接口上取消对该队列调度策略的应用，然后再删除该队列调度策略。

不能删除已经应用到 Session Group Profile 的队列调度策略，必须先在应用的 Session Group Profile 上取消对该队列调度策略的应用，然后再删除该队列调度策略。

本命令仅 CSPEX-1204 单板支持。

【举例】

创建自定义的八队列调度策略 myprofile，并进入八队列调度策略视图。

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile]
```

创建自定义的四队列调度策略 myprofile，并进入四队列调度策略视图。

```
<Sysname> system-view
[Sysname] qos qmprofile four-queue myprofile
[Sysname-qmprofile-four-queue-myprofile]
```

【相关命令】

- **display qos qmprofile interface**
- **queue**

4.4.5 queue

queue 命令用来配置队列调度参数。

undo queue 命令用来恢复缺省情况。

【命令】

queue *queue-id* { **sp** | **wrr group** *group-id* **weight** *schedule-value* } [**min bandwidth** *bandwidth-value* | **service-type** *service-type-value*] *

undo queue *queue-id*

【缺省情况】

各队列采用严格优先级调度。

【视图】

队列调度策略视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue-id：队列序号，取值范围 0～7。

sp：配置队列为严格优先级调度。

wrr：配置队列为加权轮询调度。

group *group-id*：优先组号，取值范围 1～4。

weight *schedule-value*：配置队列的调度权重，取值范围 1～15，本参数配置后不生效。

Min bandwidth *bandwidth-value*：最小保证带宽值，单位为 kbps。端口流量拥塞时能够保证的最小队列带宽，取值范围 40～1000000，本参数配置后不生效。

service-type *service-type-value*：服务类型。包括 HSI（High Speed Internet，高速上网）、STB（Set Top Box，机顶盒）、VoIP（Voice Over Internet Protocol，在 IP 网络上传送语音），本参数配置后不生效。

【使用指导】

*queue-id*除了支持数字外，还支持直接输入关键字，具体情况请参见 表 4-3。

本命令仅 CSPEX-1204 单板支持。

【举例】

创建自定义的队列调度策略 myprofile，并配置队列 0 为严格优先级调度。

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 0 sp
```

创建自定义的队列调度策略 myprofile，并配置队列 1 为加权轮询调度，权重为 10，分组为 1。

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 1 wrr group 1 weight 10
```

【相关命令】

- **display qos qmprofile interface**
- **qos qmprofile**

4.4.6 queue(four-queue qmprofile view)

queue 命令用来配置队列调度参数。

undo queue 命令用来恢复缺省情况。

【命令】

queue *queue-id* { **sp** | **wrr group** *group-id* **weight** *schedule-value* } [**min-bandwidth** *bandwidth-value* | **service-type** *service-type-value*] *

undo queue *queue-id*

【缺省情况】

各队列采用严格优先级调度。

【视图】

四队列调度策略视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue-id：队列序号，取值范围 0～3。

sp：配置队列为严格优先级调度。

wrr：配置队列为加权轮询调度。

group *group-id*：WRR 优先组号，取值范围 1～4。

Weight *schedule-value*：配置队列的调度权重，取值范围 1～15，本参数配置后不生效。

min bandwidth *bandwidth-value*：最小保证带宽值，单位为 kbps。端口流量拥塞时能够保证的最小队列带宽，取值范围 40～1000000，本参数配置后不生效。

service-type *service-type-value*：服务类型。包括 HSI（High Speed Internet，高速上网）、STB（SetTop Box，机顶盒）、VoIP（Voice Over Internet Protocol，在 IP 网络上传送语音），本参数配置后不生效。

【使用指导】

对同一个队列多次配置时，后一次配置会覆盖前面的配置，以最后一次配置为准。

*queue-id*除了支持数字外，还支持直接输入关键字，具体情况请参见 表 4-3。

本命令仅 CSPEX-1204 单板支持。

【举例】

创建自定义的四队列调度策略 myprofile，并配置队列 0 为严格优先级调度。

```
<Sysname> system-view
[Sysname] qos qmprofile four-queue myprofile
[Sysname-qmprofile-four-queue-myprofile] queue 0 sp
```

创建自定义的四队列调度策略 myprofile，并配置队列 1 为加权轮询调度，权重为 15，分组为 1。

```
<Sysname> system-view
[Sysname] qos qmprofile four-queue myprofile
[Sysname-qmprofile-four-queue-myprofile] queue 1 wrr group 1 weight 15
```

4.5 基于类的队列配置命令

4.5.1 queue af

queue af 命令用来配置类进行确保转发（Assured-forwarding），并配置类可确保的最小带宽。

undo queue af 命令用来取消配置。

【命令】

queue af bandwidth *bandwidth* [**pir** *peak-information-rate*]

undo queue af

【缺省情况】

没有配置类进行确保转发。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

bandwidth：可确保的最小带宽，取值范围为 64～10000000，单位是 kbps。

pir *peak-information-rate*：峰值速率，取值范围为 64～10000000，单位为 kbps，实际生效的峰值速率为 *peak-information-rate* / 8 的商值，四舍五入取整数后再乘以 8。CSPC 单板和 CMPE-1104 单板不支持配置 pir。

【使用指导】

- 当在策略下将类与 **queue af** 所属行为关联时，必须满足：同一个策略下为确保转发（**queue af**）和加速转发（**queue ef**）的类指定的带宽之和必须不大于该策略所应用接口的可用带宽。
- 该命令在流行为视图下不能与 **queue ef**、**queue wfq** 同时使用。

【举例】

为流行为 database 配置确保转发，并且确保最小带宽为 200kbps。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
```

【相关命令】

- **traffic behavior**

4.5.2 queue ef

queue ef 命令用来配置类进行加速转发（Expedited-forwarding），报文进入绝对优先级队列，并配置最大带宽。

undo queue ef 命令用来取消配置。

【命令】

queue ef bandwidth *bandwidth* [**cbs** *burst*] [**pir** *peak-information-rate*]

undo queue ef

【缺省情况】

没有配置类进行加速转发。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

bandwidth：用户定义的需要加速转发的流量最大带宽，取值范围为 64～10000000，单位是 kbps。

cbs *burst*：承诺突发尺寸，即实际平均速率在用户定义带宽以内时的突发流量，取值范围为 1600～1000000000，单位为 byte，缺省值为 bandwidth 的 25 倍。用户配置的承诺突发尺寸不允许小于 50ms 承诺信息速率的流量，以避免令牌桶突发速率太小，影响网络流量的突发特征。

pir *peak-information-rate*：峰值速率，取值范围为 64～10000000，单位为 kbps。CSPC 单板和 CMPE-1104 单板不支持配置 pir。

【使用指导】

queue ef 命令用来配置加速转发（Expedited-forwarding），报文进入绝对优先级队列，并配置最大带宽。**undo queue ef** 命令用来取消配置。

本命令的注意事项如下：

- 该命令在流行为视图下不能与 **queue af**、**queue wfq** 同时使用。
- 同一个策略下为确保转发（**queue af**）和加速转发（**queue ef**）的类指定的带宽之和必须不大于该策略所应用接口的可用带宽。
- 对于设置绝对值形式 **queue ef bandwidth** *bandwidth* [**cbs** *burst*]，CBS = *burst*，若不指定 *burst*，CBS = *bandwidth*×25。

【举例】

配置报文进入优先级队列，最大带宽为 200kbps，承诺突发尺寸为 5000bytes。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue ef bandwidth 200 cbs 5000
```

【相关命令】

- **traffic behavior**

4.5.3 queue wfq

queue wfq 命令用来为缺省类配置采用公平队列。

undo queue wfq 命令用来取消配置。

【命令】

queue wfq

undo queue wfq

【缺省情况】

没有为缺省类配置采用公平队列。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

该命令在流行为视图下不能与 **queue af**、**queue ef** 同时使用。

【举例】

为用户配置的进入 BE 队列的类配置 WFQ。

```
<Sysname> system-view
```

```
[Sysname] traffic behavior be_behav
[Sysname-behavior-be_behav] queue wfq
```

【相关命令】

- **traffic behavior**

4.5.4 weight

weight 命令用来配置 WFQ 的权重。

undo weight 命令用来恢复缺省情况

【命令】

weight *weight-value*

undo weight

【缺省情况】

对于 CSPC 单板和 CMPE-1104 单板，AF 超出保证带宽的流量和 BE 队列的流量，WFQ 的权重为 1；EF 超出保证带宽的流量，WFQ 的权重为 0。

对于 CSPEX-1204 单板上的 POS 主接口和以太网主接口，AF 超出保证带宽的流量和 EF 超出保证带宽的流量，WFQ 的权重为 1；BE 的流量，WFQ 的权重为 0；对于 CSPEX-1204 单板上的其他接口及子接口，各队列的流量按照严格优先级进行调度。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

weight-value：权重值，取值范围为 1～63

【使用指导】

- 该命令在流行为视图下不能单独使用，必须与 **queue af**、**queue wfq** 两者中的一条配合使用。
- 仅 CSPEX-1204 支持配置加速转发流量的 WFQ 权重。
- 对于 CSPC 单板和 CMPE-1104 单板，AF 超出保证带宽的流量和 BE 队列的流量，按照 WFQ 的权重进行调度，若有剩余带宽，再发送 EF 超出保证带宽的流量。
- 对于 CSPEX-1204 单板上的 POS 主接口和以太网主接口，AF 超出保证带宽的流量、EF 超出保证带宽的流量和 BE 队列的流量，按照 WFQ 的权重进行调度。BE 队列的缺省 WFQ 权重为 0，即有剩余带宽时，才发送 BE 队列的流量；对于 CSPEX-1204 单板上的其他接口及子接口，各队列流量的优先级关系为 EF 队列保证带宽的流量 > AF 队列保证带宽的流量 > AF 队列超带宽的流量 > BE 队列的流量 > EF 队列超带宽的流量。

【举例】

配置流行为 database1 采用 AF，最小可保证带宽为 200kbps，超出 200kbps 的流量采用 WFQ 调度，其权重为 62。

```
<Sysname> system-view
```

```
[Sysname] traffic behavior database1
[Sysname-behavior-database1] queue af bandwidth 200
[Sysname-behavior-database1] weight 62
```

【相关命令】

- **traffic behavior**

5 拥塞避免

5.1 WRED表配置命令

5.1.1 display qos wred interface

display qos wred interface 命令用来显示接口的 WRED 配置情况。

【命令】

display qos wred interface [*interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口的 WRED 配置情况。

【举例】

显示接口 GigabitEthernet3/0/1 的 WRED 配置情况。

```
<Sysname> display qos wred interface gigabitethernet 3/0/1
Interface: GigabitEthernet3/0/1
 Current WRED configuration:
 Applied WRED table name: queue-table1
```

表5-1 display qos wred interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Current WRED configuration	当前WRED的配置情况
Applied WRED table name	当前应用的WRED表的名称

5.1.2 display qos wred table

display qos wred table 命令用来显示 WRED 表的配置情况。

【命令】

display qos wred table [**name** *table-name*] [**slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

name *table-name*：要显示的 WRED 表的名字。如果未指定本参数，则显示所有 WRED 表配置情况。

slot *slot-number*：指定单板。*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示主用主控板的 WRED 表配置情况。

【使用指导】

- 如果不指定表名字，将显示所有 WRED 表配置情况。
- 如果不指定槽位号，则显示设备上所有 WRED 表配置情况。

【举例】

显示 WRED 表 1 的配置情况，表 1 是一个已经配置好的 WRED 参数表。

```
<Sysname> display qos wred table name 1
Table name: 1
Table type: Queue based WRED
QID   gmin  gmax  gprob  ymin  ymax  yprob  rmin  rmax  rprob  exponent  ECN
------------------------------------------------------------------------------
0     100   1000  10     100   1000  10     100   1000  10     9         N
1     100   1000  10     100   1000  10     100   1000  10     9         N
2     100   1000  10     100   1000  10     100   1000  10     9         N
3     100   1000  10     100   1000  10     100   1000  10     9         N
4     100   1000  10     100   1000  10     100   1000  10     9         N
5     100   1000  10     100   1000  10     100   1000  10     9         N
6     100   1000  10     100   1000  10     100   1000  10     9         N
7     100   1000  10     100   1000  10     100   1000  10     9         N
```

表5-2 display qos wred table 命令显示信息描述表

字段	描述
Table name	WRED表名
Table type	WRED表类型
QID	队列ID
gmin	绿色报文的队列下限
gmax	绿色报文的队列上限
gprob	绿色报文的丢弃概率
ymin	黄色报文的队列下限
ymax	黄色报文的队列上限
yprob	黄色报文的丢弃概率

字段	描述
rmin	红色报文的队列下限
rmax	红色报文的队列上限
rprob	红色报文的丢弃概率
exponent	计算平均队列长度指数
ECN	是否对该队列开启了拥塞通知功能，Y表示开启，N表示未开启

5.1.3 qos wred apply

qos wred apply 命令用来在接口上应用 WRED 全局表。

undo qos wred apply 命令用来恢复接口缺省的尾丢弃模式，它同时取消 WRED 表的应用。

【命令】

qos wred apply [*table-name*]

undo qos wred apply

【缺省情况】

接口没有应用 WRED 全局表，即接口采用尾丢弃。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

table-name：WRED 表的名称。

【使用指导】

如果不指定 WRED 表的名称，则在接口上应用缺省 WRED 表。

【举例】

在接口 GigabitEthernet3/0/1 上应用 WRED 表。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos wred apply table1
```

【相关命令】

- **display qos wred interface**
- **display qos wred table**
- **qos wred table**

5.1.4 qos wred queue table

qos wred queue table 命令用来创建全局 WRED 表，同时进入该 WRED 表视图。

undo qos wred queue table 命令用来删除全局 WRED 表。

【命令】

qos wred queue table *table-name*

undo qos wred queue table *table-name*

【缺省情况】

设备上不存在 WRED 表。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue：基于队列的表，拥塞时根据报文所在队列进行随机丢弃。

table *table-name*：指定表的名称。

【使用指导】

设备不允许删除正在使用的表。如果想删除正在使用的表，请先在接口上取消应用的 WRED 表。

【举例】

创建基于 queue 的 WRED 表 queue-table1。

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1]
```

【相关命令】

- **display qos wred table**

5.1.5 queue

queue 命令用来配置基于队列的 WRED 表的内容。

undo queue 命令用来恢复缺省情况。

【命令】

queue *queue-id* [**drop-level** *drop-level*] **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo queue { *queue-id* | **all** }

【缺省情况】

WRED 表在创建之后，有缺省的一套参数，*low-limit* 的取值为 100，*high-limit* 的取值为 1000，*discard-prob* 的取值为 10。

【视图】

WRED 表视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue-id：队列编号。

drop-level *drop-level*：丢弃级别，在进行报文丢弃时参考的参数，0 对应绿色报文、1 对应黄色报文、2 对应红色报文。如果未指定本参数，后续配置的参数对该队列所有丢弃级别的报文都生效。

low-limit *low-limit*：队列平均长度的下限，取值范围为 0～16383。

high-limit *high-limit*：队列平均长度的上限，取值范围为 0～16383 且必须大于丢弃下限。

discard-probability *discard-prob*：以百分数形式表示的丢弃概率，取值范围为 0～100。当报文队列平均长度在上限和下限之间时，设备采用这个概率来丢弃报文。SPEX-1204 单板不支持配置该参数。

【使用指导】

当队列平均长度小于下限时，不丢弃报文。当队列平均长度在上限和下限之间时，设备随机丢弃报文，队列越长，丢弃概率越高。当队列平均长度超过上限时，丢弃所有到来的报文。

【举例】

配置全局 WRED 表 queue-table1 中队列 1 丢弃参数：对黄色报文的丢弃下限为 10，丢弃上限为 20，丢弃概率为 30%。

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 10 high-limit 20
discard-probability 30
```

【相关命令】

- **display qos wred table**
- **qos wred table**

5.1.6 queue ecn

queue ecn 命令用来对指定队列开启拥塞通知功能。

undo queue ecn 命令用来恢复缺省情况。

【命令】

queue *queue-id* **ecn**

undo queue *queue-id* **ecn**

【缺省情况】

对任何队列都未开启拥塞通知功能。

【视图】

WRED 表视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue-id：队列编号，取值范围为 0～7。

【使用指导】

在报文的发送端和接收端都支持 ECN 功能时，设备可以通过对 ECN 域的识别和标记将拥塞状况告知终端，避免拥塞加剧。

需要注意的是，SPEX-1204 单板不支持开启拥塞通知功能。

【举例】

在 WRED 表 queue-table1 中，对队列 1 开启拥塞通知功能。

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 ecn
```

【相关命令】

- **display qos wred table**
- **qos wred table**

5.1.7 queue weighting-constant

queue weighting-constant 命令用来配置计算平均队列长度的指数。

undo queue weighting-constant 命令用来恢复缺省情况。

【命令】

queue *queue-id* **weighting-constant** *exponent*

undo queue *queue-id* **weighting-constant**

【缺省情况】

计算平均队列长度的指数为 9。

【视图】

WRED 表视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue-id：队列编号。

weighting-constant *exponent*：计算平均队列长度的指数，*exponent* 的取值范围为 0～15。

【使用指导】

平均队列长度的指数越大，计算平均队列长度时对队列的实时变化越不敏感。计算队列平均长度的公式为：平均队列长度=（以前的平均队列长度×（1-1/2^n））＋（当前队列长度×（1/2^n））。其中 n 表示指数。

【举例】

在 WRED 表 queue-table1 中，配置计算平均队列长度的指数为 12。

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 weighting-constant 12
```

【相关命令】

- **display qos wred table**
- **qos wred table**

6 全局CAR

6.1 全局CAR配置命令

6.1.1 car name

car name 命令用来配置全局 CAR 动作。

undo car 用来删除全局 CAR 动作。

【命令】

car name *car-name* [**hierarchy-car** *hierarchy-car-name* [**mode** { **and** | **or** }]]

undo car

【缺省情况】

没有配置全局 CAR 动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

car-name：聚合 CAR 的名称，首字符需要以字母开头，为 1～31 个字符的字符串，区分大小写。

hierarchy-car-name：分层 CAR 的名称，首字符需要以字母开头，为 1～31 个字符的字符串，区分大小写，目前暂不支持该参数。

mode：分层 CAR 和聚合 CAR 动作的合作模式，目前暂不支持该参数。

【举例】

配置流行为 be1 的聚合 CAR 动作为 aggcar-1。

```
<Sysname> system-view
[Sysname] traffic behavior be1
[Sysname-behavior-be1] car name aggcar-1
```

【相关命令】

- **display qos car name**
- **display traffic behavior user-defined**

6.1.2 display qos car name

display qos car name 命令用来显示全局 CAR 的配置和统计信息。

【命令】

display qos car name [*car-name*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

car-name：全局 CAR 的名称，首字符需要以字母开头，为 1～31 个字符的字符串，区分大小写。显示指定全局 CAR 的配置和统计信息。如果未指定本参数，将显示所有全局 CAR 的配置和统计信息。

【举例】

显示全局 CAR 的配置和统计信息。

```
<Sysname> display qos car name
 Name: a
  Mode: aggregative
   CIR 10000 (kbps), CBS 625152 (Bytes), EBS 512 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
```

表6-1 display qos car name 命令显示信息描述表

字段	描述
Name	全局CAR的名称
Mode	全局CAR的类型 • aggregative：聚合 CAR • hierarchy：分层 CAR，目前暂不支持该参数
CIR CBS EBS	流量监管流量的参数配置
Green action	对绿色报文的动作 • discard：丢弃报文 • pass：允许报文通过
Yellow action	对黄色报文的动作 • discard：丢弃报文 • pass：允许报文通过
Red action	对红色报文的动作 • discard：丢弃报文 • pass：允许报文通过

6.1.3 qos car

qos car 命令用来配置聚合 CAR。

undo qos car 命令用来取消聚合 CAR 的配置。

【命令】

qos car *car-name* { **aggregative** | **hierarchy** } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peek-information-rate*]

undo qos car *car-name*

【缺省情况】

没有配置聚合 CAR。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

car-name：全局 CAR 的名称，首字符需要以字母开头，为 1～31 个字符的字符串，区分大小写。

aggregative：该全局 CAR 为聚合模式。

hierarchy：该全局 CAR 为分层模式，目前暂不支持该参数。

cir *committed-information-rate*：承诺信息速率。流量的平均速率，单位为 kbps。取值范围为 8～160000000，实际生效的承诺信息速率为 *committed-information-rate* / 8 的商值，四舍五入取整数后再乘以 8。

cbs *committed-burst-size*：承诺突发尺寸，即实际平均速率在承诺速率以内时的突发流量，单位为 byte：

- 如果不指定 **cbs** 参数，缺省取值为 62.5 × *committed-information-rate* 的乘积。
- 如果指定 **cbs** 参数，取值范围 512～256000000。

实际生效的承诺突发尺寸为 *committee-burst-size* / 512 的商值，四舍五入取整数后再乘以 512。

ebs *excess-burst-size*：超出突发尺寸，缺省值为 512，单位为 byte。取值范围为 0～256000000，实际生效的超出突发尺寸为 *excess-burst-size* / 512 的商值，四舍五入取整数后再乘以 512。

pir *peak-information-rate*：峰值速率，单位为 kbps。取值范围为 8～160000000，实际生效的峰值速率为 *peak-information-rate* / 8 的商值，四舍五入取整数后再乘以 8。

【使用指导】

- 聚合 CAR 配置需要在接口上应用或在策略中引用后才能生效。
- 配置聚合 CAR 后，对于不符合承诺信息速率，也不符合峰值速率的数据包直接丢弃，其他数据包允许通过。
- 当全局 CAR 为聚合模式时，**ebs** 和 **pir** 参数配置不生效。

【举例】

配置聚合 CAR 采取的 CAR 参数取值，**cir** 取值为 200，**cbs** 取值为 2000。

```
<Sysname> system-view
[Sysname] qos car aggcar-1 aggregative cir 200 cbs 2000
```

【相关命令】

- **display qos car name**

6.1.4 reset qos car name

reset qos car name 命令用来清除全局 CAR 的统计信息。

【命令】

reset qos car name [*car-name*]

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

car-name：全局 CAR 的名称，首字符需要以字母开头，为 1～31 个字符的字符串，区分大小写。清除指定全局 CAR 的统计信息。如果未指定本参数，将清除所有全局 CAR 的统计信息。

【举例】

清除全局 CAR aggcar-1 的统计信息。

```
<Sysname> reset qos car name aggcar-1
```

7 端口队列统计

7.1 端口队列统计配置命令

7.1.1 display qos queue-statistics interface outbound

display qos queue-statistics interface outbound 命令用来显示端口队列出方向的统计信息。

【命令】

display qos queue-statistics interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] **outbound**

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

interface-type interface-number：指定接口类型和接口编号。如果未指定本参数，将显示所有接口的队列出方向统计信息。

pvc：显示指定 PVC 的队列出方向统计信息。

pvc-name：PVC 名，长度为 1～15 个字符的字符串，区分大小写，PVC 名中不允许使用“/”和“-”，如“1/20”、“a-b”就不允许作为 PVC 名。

vpi/vci：*vpi* 为 VPI 值，取值范围为 0～255；*vci* 为 VCI 值，取值范围与接口类型相关，请参见“二层技术-广域网接入命令参考”中的“ATM”。*vpi* 与 *vci* 不能同时为 0。通常，*vci* 取值 0 到 31 保留用于特定用途，建议用户不要使用。

【使用指导】

当指定接口类型为 ATM 接口时，可以显示指定 ATM 接口的指定 PVC 的队列出方向统计信息，若不指定 PVC，则显示指定 ATM 接口下所有 PVC 的队列出方向统计信息。

【举例】

显示接口 GigabitEthernet3/0/1 的队列出方向统计信息。

```
<Sysname> display qos queue-statistics interface gigabitethernet 3/0/1 outbound
Interface: GigabitEthernet3/0/1
 Direction: outbound
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Queue 0
  Forwarded: 0 packets, 0 bytes
```

```
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 1
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 2
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 3
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 4
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 5
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 6
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 7
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
```

表7-1 display qos queue-statistics interface outbound 命令显示信息描述表

字段	描述
Interface	端口队列统计的端口
Direction	端口队列统计的方向
Forwarded	转发的数据包数目和字节数
Dropped	丢弃的数据包数目和字节数
Queue 0、Queue 1、Queue 2、Queue 3、Queue 4、Queue 5、Queue 6、Queue 7	某端口队列统计信息
Current queue length	当前队列长度

【相关命令】

- **reset counters interface**（接口管理命令参考/以太网接口）

7.1.2 qos queue-statistics

qos queue-statistics { **inbound** | **outbound** }命令用来使能端口队列统计功能。

undo qos queue-statistics { **inbound** | **outbound** }命令用来关闭端口队列统计功能。

【命令】

qos queue-statistics { **inbound** | **outbound** }

undo qos queue-statistics { **inbound** | **outbound** }

【缺省情况】

端口队列统计功能处于使能状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

inbound：使能入方向端口队列统计功能。本参数配置后不生效。

outbound：使能出方向端口队列统计功能。

【使用指导】

本命令仅 CSPEX-1204 单板支持。

【举例】

使能出方向端口队列统计功能。

```
<Sysname> system-view
[Sysname] qos queue-statistics outbound
```

【相关命令】

- **display qos queue-statistics interface outbound**

目 录

1 MPLS QoS

1.1 MPLS QoS配置命令

1.1.1 if-match mpls-exp

if-match mpls-exp 命令用来定义匹配第一层 MPLS EXP 优先级的规则。

undo if-match mpls-exp 命令用来删除匹配第一层 MPLS EXP 优先级的规则。

【命令】

if-match mpls-exp *exp-value*&<1-8>

undo if-match mpls-exp *exp-value*&<1-8>

【缺省情况】

没有定义匹配第一层 MPLS EXP 优先级的规则。

【视图】

类视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

exp-value&<1-8>：EXP 值的列表，EXP 优先级的取值范围为 0～7，&<1-8>表示前面的参数最多可以输入 8 次。如果指定了多个相同的 EXP 值，系统默认为一个；多个不同的 EXP 值是或的关系，即只要有一个值匹配，就算匹配这条规则。

【举例】

定义匹配第一层 EXP 优先级为 3 或 4 的报文的规则。

```
<Sysname> system-view
[Sysname] traffic classifier database
[Sysname-classifier-database] if-match mpls-exp 3 4
```

1.1.2 remark mpls-exp

remark mpls-exp 命令用来配置标记 MPLS 报文的 EXP 值。

undo remark mpls-exp 命令用来取消标记 MPLS 报文的 EXP 值。

【命令】

remark mpls-exp *exp-value*

undo remark mpls-exp

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

exp-value：MPLS 报文的 EXP 值，取值范围为 0～7。

【使用指导】

如果是多层标签，则是对最外层标签进行标记。

【举例】

配置标记 MPLS 报文的 EXP 值为 0。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark mpls-exp 0
```

目 录

1 时间段

1.1 时间段配置命令

1.1.1 display time-range

display time-range 命令用来显示时间段的配置和状态信息。

【命令】

display time-range { *time-range-name* | **all** }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

time-range-name：显示指定名称时间段的配置和状态信息。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

all：显示所有时间段的配置和状态信息。

【举例】

显示时间段 t4 的配置和状态信息。

```
<Sysname> display time-range t4
Current time is 17:12:34 11/23/2010 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2011 to 00:00 1/1/2012
 from 00:00 6/1/2011 to 00:00 7/1/2011
```

表1-1 display time-range 命令显示信息描述表

字段	描述
Current time	系统当前的时间
Time-range	时间段的配置信息，包括： • 时间段的名称 • 时间段的状态，包括 Active（生效）和 Inactive（未生效）两种状态 • 时间段的时间范围

1.1.2 time-range

time-range 命令用来创建一个时间段，来描述一个特定的时间范围。

undo time-range 命令用来删除一个时间段。

【命令】

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

【缺省情况】

不存在任何时间段。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

time-range-name：指定时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，时间段的名称不允许使用英文单词 all。

start-time **to** *end-time*：指定周期时间段的时间范围。*start-time* 表示起始时间，格式为 hh:mm，取值范围为 00:00～23:59；*end-time* 表示结束时间，格式为 hh:mm，取值范围为 00:00～24:00，且结束时间必须大于起始时间。

days：指定周期时间段在每周的周几生效。本参数可输入多次，但后输入的值不能与此前输入的值完全重叠（譬如输入 **6** 后不允许再输入 **sat**，但允许再输入 **off-day**），系统将取各次输入值的并集作为最终值（譬如依次输入 **1**、**wed** 和 **working-day** 之后，最终生效的时间将为每周的工作日）。本参数可输入的形式如下：

- 数字：取值范围为 0～6，依次表示周日～周六；
- 周几的英文缩写（从周日到周六依次为 **sun**、**mon**、**tue**、**wed**、**thu**、**fri** 和 **sat**）；
- 工作日（**working-day**）：表示从周一到周五；
- 休息日（**off-day**）：表示周六和周日；
- 每日（**daily**）：表示一周七天。

from *time1 date1*：指定绝对时间段的起始时间。*time1* 的格式为 hh:mm，取值范围为 00:00～23:59。*date1* 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月，取值范围为 1～12；DD 表示日，取值范围取决于所输入的月份；YYYY 表示年，取值范围为 1970～2100。若未指定本参数，绝对时间段的起始时间将为系统可表示的最早时间，即 1970 年 1 月 1 日 0 点 0 分。

to *time2 date2*：指定绝对时间段的结束时间。*time2* 的格式为 hh:mm，取值范围为 00:00～24:00。*date2* 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月，取值范围为 1～12；DD 表示日，

取值范围取决于所输入的月份；YYYY 表示年，取值范围为 1970～2100。结束时间必须大于起始时间。若未指定本参数，绝对时间段的结束时间将为系统可表示的最晚时间，即 2100 年 12 月 31 日 24 点 0 分。

【使用指导】

- 使用 **time-range** 命令时，如果指定名称的时间段不存在，则创建一个新的时间段（最多 1024 个）；如果指定名称的时间段已存在，则对旧时间段进行修改，即在其原有内容的基础上叠加新的内容。
- 使用 *start-time* **to** *end-time days* 这组参数所创建的时间段为周期时间段，它将以一周为周期循环生效；使用 **from** *time1 date1* 和 **to** *time2 date2* 这组参数所创建的时间段为绝对时间段，它将在指定时间范围内生效；而同时使用了上述两组参数所创建的时间段，将取周期时间段和绝对时间段的交集作为生效的时间范围，譬如：创建一个时间段，既定义其在每周一的 8 点到 12 点生效，又定义其在 2011 年全年生效，那么其最终将在 2011 年全年内每周一的 8 点到 12 点生效。
- 一个时间段内可包含一或多个周期时间段（最多 32 个）和绝对时间段（最多 12 个），当包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。

【举例】

创建名为 t1 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
<Sysname> system-view
[Sysname] time-range t1 08:00 to 18:00 working-day
```

创建名为 t2 的时间段，其时间范围为 2011 年全年。

```
<Sysname> system-view
[Sysname] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011
```

创建名为 t3 的时间段，其时间范围为 2011 年全年内每周休息日的 8 点到 12 点。

```
<Sysname> system-view
[Sysname] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2011 to 24:00 12/31/2011
```

创建名为 t4 的时间段，其时间范围为 2011 年 1 月和 6 月内每周一的 10 点到 12 点以及每周三的 14 到 16 点。

```
<Sysname> system-view
[Sysname] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

【相关命令】

- **display time-range**