H3C S12500-S 系列交换机

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：6W100-20170331
产品版本：S12500S-CMW710-R7536P02

前 言

本命令参考主要介绍 H3C S12500-S 系列交换机配置 ACL 和 QoS 功能时涉及的各种命令，包括创建 ACL、配置 QoS 策略，以及配置流量监管、流量整形、拥塞管理、拥塞避免等常用 QoS 技术时所使用的命令。

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 S12500-S 系列交换机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	帮助您了解产品的主要规格参数及亮点
硬件描述与安装	安全兼容性手册	列出产品的兼容性声明，并对兼容性和安全的细节进行说明
	快速安装指南	指导您对设备进行初始安装、配置，通常针对最常用的情况，减少您的检索时间
	安装手册	帮助您详细了解设备硬件规格和安装方法，指导您对设备进行安装
业务配置	配置指导	帮助您掌握设备软件功能的配置方法及配置步骤
	命令参考	详细介绍设备的命令，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	帮助您了解在使用产品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，帮助您了解产品的一些软硬件特性及规格等问题
	版本说明书	帮助您了解产品的版本相关信息（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
	日志手册	对产品的系统日志（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

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

1.1 ACL配置命令

1.1.1 acl

acl 命令用来创建 ACL，并进入 ACL 视图。如果指定的 ACL 已存在，则直接进入 ACL 视图。

undo acl 命令用来删除指定或全部 ACL。

【命令】

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

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

acl user-defined { *acl-number* | **name** *acl-name* }

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

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

undo acl mac { **all** | *acl-number* | **name** *acl-name* }

undo acl user-defined { **all** | *acl-number* | **name** *acl-name* }

undo acl [**ipv6**] **number** *acl-number*

【缺省情况】

不存在 ACL。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。如果未指定本参数，则表示 IPv4 ACL。

basic：指定创建基本 ACL。

advanced：指定创建高级 ACL。

mac：指定创建二层 ACL。

user-defined：指定创建用户自定义 ACL。

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：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

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** 表示按照配置顺序进行规则匹配。缺省情况下，规则的匹配顺序为配置顺序。用户自定义 ACL 不支持本参数，其规则匹配顺序只能为配置顺序。

all：指定类型中全部 ACL。

【使用指导】

使用 ACL 编号指定 ACL 时，设备提供以下两种方法：

- 通过[**ipv6**] **number** *acl-number* 指定。
- 通过[**ipv6**] **basic** *acl-number*、[**ipv6**] **advanced** *acl-number*、**mac** *acl-number* 和 **user-defined** *acl-number* 指定。

两种方式均可用于创建 ACL、删除 ACL 和进入 ACL 视图，且可以混合使用，例如通过 **number** *acl-number* 创建的 IPv4 高级 ACL，既可以通过 **advanced** *acl-number* 进入 IPv4 高级 ACL 视图，也可以通过 **advanced** *acl-number* 删除指定编号的 IPv4 高级 ACL。

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。

如果 ACL 规则的匹配项中包含了除 IP 五元组（源 IP 地址、源端口号、目的 IP 地址、目的端口号、传输层协议）、ICMP 报文或 ICMPv6 报文的消息类型和消息码信息、VPN 实例、日志操作和时间段之外的其它匹配项，则设备转发 ACL 匹配的这类报文时会启用慢转发流程。慢转发时设备会将报文上送控制平面，计算报文相应的表项信息。执行慢转发流程时，设备的转发能力将会有所降低。

【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 basic 2000
[Sysname-acl-ipv4-basic-2000]
```

创建一个 IPv4 基本 ACL，指定其名称为 flow，并进入其视图。

```
<Sysname> system-view
[Sysname] acl basic name flow
[Sysname-acl-ipv4-basic-flow]
```

创建一个编号为 3000 的 IPv4 高级 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000]
```

创建一个编号为 2000 的 IPv6 基本 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl ipv6 basic 2000
[Sysname-acl-ipv6-basic-2000]
```

创建一个 IPv6 基本 ACL，其名称为 flow，并进入其视图。

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

创建一个 IPv6 高级 ACL，其名称为 abc，并进入其视图。

```
<Sysname> system-view
[Sysname] acl ipv6 advanced name abc
[Sysname-acl-ipv6-adv-abc]
```

创建一个编号为 4000 的二层 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl mac 4000
[Sysname-acl-mac-4000]
```

创建一个二层 ACL，其名称为 flow，并进入其视图。

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

创建一个编号为 5000 的用户自定义 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl user-defined 5000
[Sysname-acl-user-5000]
```

创建一个用户自定义 ACL，其名称为 flow，并进入其视图。

```
<Sysname> system-view
[Sysname] acl user-defined name flow
[Sysname-acl-user-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** | **mac** | **user-defined**] **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】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

user-defined：指定 ACL 类型为用户自定义 ACL。

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：表示基本 ACL。
- 3000～3999：表示高级 ACL。

- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

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。

dest-acl-number：指定目的 ACL 的编号，该 ACL 必须不存在。本参数的取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

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。

【使用指导】

目的 ACL 的类型要与源 ACL 的类型相同。

除了 ACL 的编号或名称不同外，新生成的 ACL（即目的 ACL）的匹配顺序、规则匹配统计功能的开启情况、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。

若未指定 **ipv6**、**mac** 或 **user-defined** 参数，则表示 IPv4 ACL。

【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
```

通过复制已存在的 IPv4 基本 ACL test，来生成名为 paste 的同类型 ACL。

```
<Sysname> system-view
[Sysname] acl copy name test to name paste
```

1.1.3 acl logging interval

acl logging interval 命令用来配置报文过滤日志信息的生成与发送周期。

undo acl logging interval 命令用来恢复缺省情况。

【命令】

acl logging interval *interval*

undo acl logging interval

【缺省情况】

报文过滤日志信息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：报文过滤日志信息的生成与发送周期，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 进行报文过滤的报文过滤日志信息进行记录，且在上述 ACL 中配置规则时必须指定 **logging** 参数。

设备周期性地生成报文过滤日志信息并发送到信息中心，包括该周期内被匹配的报文数量以及所使用的 ACL 规则。有关信息中心的详细介绍请参见“网络管理和监控配置指导”中的“信息中心”。

【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 trap interval

acl trap interval 命令用来配置报文过滤告警信息的生成与发送周期。

undo acl trap interval 命令用来恢复缺省情况。

【命令】

acl trap interval *interval*

undo acl trap interval

【缺省情况】

报文过滤日告警信息的生成与发送周期为 0 分钟，即不记录报文过滤的告警信息。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

interval：报文过滤告警信息的生成与发送周期，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 进行报文过滤的报文过滤告警信息进行记录，且在上述 ACL 中配置规则时必须指定 **logging** 参数。

设备周期性地生成告警信息并发送到 SNMP 模块，包括该周期内被匹配的报文数量以及所使用的 ACL 规则。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

【举例】

配置 IPv4 报文过滤告警信息的生成与发送周期为 10 分钟。

```
<Sysname> system-view
[Sysname] acl trap 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)

1.1.5 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

用户自定义 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 basic 2000
```

```
[Sysname-acl-ipv4-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** | **mac** | **user-defined**] { *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】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

user-defined：指定 ACL 类型为用户自定义 ACL。

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：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

all：显示指定类型中全部 ACL 的配置和运行情况。

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。

【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。

如果未指定 **ipv6**、**mac** 或 **user-defined** 参数，则表示 IPv4 ACL。

【举例】

显示 IPv4 基本 ACL 2001 的配置和运行情况。

```
<Sysname> display acl 2001
Basic IPv4 ACL 2001, 1 rule, match-order is auto,
This is an IPv4 basic ACL.
```

```
ACL's step is 5, start ID is 0
 rule 5 permit source 1.1.1.1 0
 rule 5 comment This rule is used on Ten-GigabitEthernet1/0/1.
```

表1-1 display acl 命令显示信息描述表

字段	描述
Basic IPv4 ACL 2001	该ACL的类型和编号
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
ACL's step is 5	该ACL的规则编号的步长值为5
start ID is 0	该ACL的规则编号的起始值为0
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 Ten-GigabitEthernet1/0/1.	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】

（独立运行模式）

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

（IRF 模式）

display packet-filter { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **interface vlan-interface** *vlan-interface-number* [**inbound** | **outbound**] [**chassis** *chassis-number* **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】

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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板上 ACL 在报文过滤中的应用情况，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。若未指定本参数，将显示全局主用主控板上 ACL 在报文过滤中的应用情况。（IRF 模式）

【使用指导】

如果未指定 **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 VLAN 2 中出、入方向上 ACL 在报文过滤中的应用情况。

```
<Sysname> display packet-filter vlan 2
VLAN: 2
Inbound policy:
  IPv4 ACL 2001
  IPv6 ACL 2001
  MAC ACL 4001
  IPv4 default action: Deny
  IPv6 default action: Deny
  MAC default action: Deny
Outbound policy:
  IPv6 ACL 2001
  IPv6 default action: Deny
```

显示接口 Ten-GigabitEthernet1/0/1 入方向上 ACL 在报文过滤中的应用情况。

```
<Sysname> display packet-filter interface ten-gigabitethernet 1/0/1 inbound
Interface: Ten-GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
  IPv6 ACL 2002
  MAC ACL 4003 (Failed), Hardware-count (Failed)
  IPv4 default action: Deny, Hardware-count
  IPv6 default action: Deny, Hardware-count
```

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
Inbound policy	ACL在入方向上的应用情况
Outbound policy	ACL在出方向上的应用情况

字段	描述
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv6 ACL 2002 (Failed)	IPv6基本ACL 2002应用失败
Hardware-count	规则匹配统计功能应用成功
Hardware-count (Failed)	规则匹配统计功能应用失败
IPv4 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit • Hardware-count：报文过滤缺省动作统计功能应用成功 • Hardware-count (Failed)：报文过滤缺省动作统计功能应用失败
IPv6 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit • Hardware-count：报文过滤缺省动作统计功能应用成功 • Hardware-count (Failed)：报文过滤缺省动作统计功能应用失败
MAC default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit • Hardware-count：报文过滤缺省动作统计功能应用成功 • Hardware-count (Failed)：报文过滤缺省动作统计功能应用失败

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。

【命令】

display packet-filter statistics interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac** | **user-defined**] { *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】

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。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

user-defined：指定 ACL 类型为用户自定义 ACL。

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：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

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。

brief：显示简要统计信息。

【使用指导】

如果未指定 **default**、*acl-number*、**name** *acl-name* 和 ACL 类型（**ipv6**、**mac**、**user-defined**）参数，将显示全部 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。

如果未指定 **ipv6**、**mac** 或 **user-defined** 参数，则表示 IPv4 ACL。

【举例】

显示接口 Ten-GigabitEthernet1/0/1 入方向上全部 ACL 在报文过滤中应用的统计信息。

```
<Sysname> display packet-filter statistics interface ten-gigabitethernet 1/0/1 inbound
Interface: Ten-GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001, Hardware-count
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0 (Failed)
   rule 10 permit vpn-instance test (No resource)
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied

  IPv4 ACL 2002 (Failed)

  IPv6 ACL 2000

  MAC ACL 4000
   From 2011-06-04 10:25:34 to 2011-06-04 10:35:57
   rule 0 permit
```

```
IPv4 default action: Deny, Hardware-count
 From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
 Totally 7 packets

IPv6 default action: Deny, Hardware-count
 From 2011-06-04 10:25:41 to 2011-06-04 10:35:57
 Totally 0 packets
MAC default action: Deny, Hardware-count
 From 2011-06-04 10:25:34 to 2011-06-04 10:35:57
 Totally 0 packets
```

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
Inbound policy	在入方向上应用的统计信息
Outbound policy	在出方向上应用的统计信息
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv4 ACL 2002 (Failed)	IPv4基本ACL 2002应用失败
Hardware-count	规则匹配统计功能应用成功
Hardware-count (Failed)	规则匹配统计功能应用失败
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	该统计的起始和终止时间
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）
No resource	该规则对应的统计资源不足。在显示统计信息时，若该规则的统计资源不足，便会显示本字段
rule 5 permit source 1.1.1.1 0 (Failed)	规则5应用失败
Totally 2 packets permitted, 0 packets denied	该ACL允许和拒绝符合条件报文的个数
Totally 100% permitted, 0% denied	该ACL允许符合条件报文的通过率和拒绝符合条件报文的丢弃率
IPv4 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit • Hardware-count：报文过滤缺省动作统计功能应用成功 • Hardware-count (Failed)：报文过滤缺省动作统计功能应用失败

字段	描述
IPv6 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit • Hardware-count：报文过滤缺省动作统计功能应用成功 • Hardware-count (Failed)：报文过滤缺省动作统计功能应用失败
MAC default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit • Hardware-count：报文过滤缺省动作统计功能应用成功 • Hardware-count (Failed)：报文过滤缺省动作统计功能应用失败
Totally 7 packets	报文过滤缺省动作的执行次数

【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** | **mac** | **user-defined**] { *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。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

user-defined：指定 ACL 类型为用户自定义 ACL。

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：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

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。

brief：显示 ACL 在报文过滤中应用的简要累加统计信息。

【使用指导】

如果未指定 **ipv6**、**mac** 或 **user-defined** 参数，则表示 IPv4 ACL。

【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:
 Inbound policy:
  IPv4 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
```

显示入方向上 IPv4 基本 ACL 2000 在报文过滤中应用的简要累加统计信息。

```
<Sysname> display packet-filter statistics sum inbound 2000 brief
Sum:
 Inbound policy:
  IPv4 ACL 2000
   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
Inbound policy	ACL在入方向上应用的累加统计信息
Outbound policy	ACL在出方向上应用的累加统计信息
IPv4 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 permitted, 0 packets denied	该ACL允许和拒绝符合条件报文的个数
Totally 100% permitted, 0% denied	该ACL允许符合条件报文的通过率和拒绝符合条件报文的丢弃率

【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】

（独立运行模式）

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

（IRF 模式）

display packet-filter verbose interface *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac** | **user-defined**] { *acl-number* | **name** *acl-name* }] [**chassis** *chassis-number* **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】

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。当接口类型为以太网接口时，不需要指定 **chassis** 和 **slot** 参数。

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。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

user-defined：指定 ACL 类型为用户自定义 ACL。

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：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

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。

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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板上 ACL 在报文过滤中的详细应用情况，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。若未指定本参数，将显示全局主用主控板上 ACL 在报文过滤中的详细应用情况。（IRF 模式）

【使用指导】

若未指定 *acl-number*、**name** *acl-name* 和 ACL 类型（**ipv6**、**mac**、**user-defined**）参数，将显示全部 IPv4 ACL 在报文过滤中的详细应用情况。

如果未指定 **ipv6**、**mac** 或 **user-defined** 参数，则表示 IPv4 ACL。

【举例】

显示接口 Ten-GigabitEthernet1/0/1 入方向上全部 ACL 在报文过滤中的详细应用情况。

```
<Sysname> display packet-filter verbose interface ten-gigabitethernet 1/0/1 inbound
Interface: Ten-GigabitEthernet1/0/1
 Inbound policy:
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0 (Failed)
   rule 10 permit vpn-instance test (Failed)

  IPv4 ACL 2002 (Failed)

  IPv6 ACL 2000
   rule 0 permit

  MAC ACL 4000


  IPv4 default action: Deny

  IPv6 default action: Deny, Hardware-count (Failed)

  MAC 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
Inbound policy	ACL在入方向上的详细应用情况
Outbound policy	ACL在出方向上的详细应用情况
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv4 ACL 2002 (Failed)	IPv4基本ACL 2002应用失败

字段	描述
Hardware-count	规则匹配统计功能应用成功
Hardware-count (Failed)	规则匹配统计功能应用失败
rule 5 permit source 1.1.1.10 (Failed)	规则5应用失败
IPv4 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit • Hardware-count：报文过滤缺省动作统计功能应用成功 • Hardware-count (Failed)：报文过滤缺省动作统计功能应用失败
IPv6 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit • Hardware-count：报文过滤缺省动作统计功能应用成功 • Hardware-count (Failed)：报文过滤缺省动作统计功能应用失败
MAC default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit • Hardware-count：报文过滤缺省动作统计功能应用成功 • Hardware-count (Failed)：报文过滤缺省动作统计功能应用失败

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】

（独立运行模式）

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

（IRF 模式）

display qos-acl resource [**chassis** *chassis-number* **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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板上 QoS 和 ACL 资源的使用情况，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 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。（IRF 模式）

【使用指导】

如果指定的单板不支持统计 QoS 和 ACL 资源，将不会显示该单板上 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: XGE1/0/1 to XGE1/0/16 (slot 1)
-------------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
 VFP ACL          512        16         0          496        3%
 IFP ACL          2048       516        0          1532       25%
 IFP Meter        2048       515        0          1533       25%
 IFP Counter      2048       515        0          1533       25%
 EFP ACL          512        0          0          512        0%
 EFP Meter        512        0          0          512        0%
 EFP Counter      512        0          0          512        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： • ACL 表示 ACL 规则资源 • Meter 表示流量监管资源 • Counter 表示流量统计资源 • VFP 表示二层转发前的，应用于重标记 QoS 本地 ID 值功能的资源 • IFP 表示入方向的资源 • EFP 表示出方向的资源
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	预留的资源数与已配置的资源数之和占资源总数的百分比，分子按实际计算结果的整数部分显示，例如实际计算结果为50.8%，此处显示为50%。

1.1.12 packet-filter (interface view)

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** | **mac** | **user-defined**] { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [**hardware-count**]

undo packet-filter [**ipv6** | **mac** | **user-defined**] { *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】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

user-defined：指定 ACL 类型为用户自定义 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

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。

inbound：对收到的报文进行过滤。

outbound：对发出的报文进行过滤。

hardware-count：表示开启规则匹配统计功能，缺省为关闭。

【使用指导】

若未指定 **ipv6**、**mac** 或 **user-defined** 关键字，则表示 IPv4 ACL。

三层聚合接口/子接口不支持应用 ACL 进行报文过滤；三层聚合接口存在子接口时，该聚合子接口的成员端口也不支持应用 ACL 进行报文过滤。

本命令中的 **hardware-count** 参数用于开启指定 ACL 内所有规则的匹配统计功能，而 **rule** 命令中的 **counting** 参数则用于开启当前规则的匹配统计功能。

一个接口在一个方向上最多可应用 3 个 ACL 进行报文过滤，包括一个 IPv4 ACL、一个 IPv6 ACL 以及一个二层 ACL。

VSI 虚接口不支持在出方向应用 ACL 进行报文过滤，并且仅以下接口板支持在 VSI 虚接口上应用 ACL 进行报文过滤：LSXM2QGS12SG3、LSUM2TGS48SG0 和 LSXM2TGS32QSSG3 单板。

【举例】

应用 IPv4 基本 ACL 2001 对接口 Ten-GigabitEthernet1/0/1 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 ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] 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 filter

packet-filter filter 命令用来配置报文过滤在 VLAN 接口的生效范围。

undo packet-filter filter 命令用来恢复默认情况。

【命令】

packet-filter filter [**route** | **all**]

undo packet-filter filter

【缺省情况】

报文过滤仅对通过 VLAN 接口进行三层转发的报文生效。

【视图】

VLAN 接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

route：表示报文过滤仅对通过 VLAN 接口进行三层转发的报文生效。

all：表示报文过滤对所有报文（包括通过 VLAN 接口进行三层转发的报文和通过 VLAN 接口对应的物理接口进行二层转发的报文）均生效。

【举例】

配置 VLAN 接口 2 上的报文过滤方式为 route，即报文过滤仅对通过 VLAN 接口 2 进行三层转发的报文生效。

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] packet-filter filter route
```

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** | **mac** | **user-defined**] **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】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

user-defined：指定 ACL 类型为用户自定义 ACL。

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：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

all：清除指定类型中全部 ACL 的统计信息。

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。

【使用指导】

如果未指定 **ipv6**、**mac** 或 **user-defined** 参数，则表示 IPv4 ACL。

【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、累加统计信息以及报文过滤缺省动作的统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

user-defined：指定 ACL 类型为用户自定义 ACL。

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：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

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。

【使用指导】

如果未指定 **default**、*acl-number*、**name** *acl-name* 和 ACL 类型（**ipv6**、**mac**、**user-defined**）参数，将清除全部 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。

如果未指定 **ipv6**、**mac** 或 **user-defined** 参数，则表示 IPv4 ACL。

【举例】

清除在 VLAN 2 中入方向上 IPv4 基本 ACL 2001 在报文过滤中应用的统计信息。

```
<Sysname> reset packet-filter statistics vlan 2 inbound 2001
```

清除在接口 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 1/0/1 inbound 2001
```

【相关命令】

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

1.1.17 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** | **qos-local-id** *local-id-value* | **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** | **qos-local-id** | **source** | **source-port** | **time-range** | **vpn-instance**] *

undo rule { **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** | **qos-local-id** | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **user-group** *group-name* | **vpn-instance** *vpn-instance-name*] *

【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，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。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）。**ip** 表示所有协议类型。

*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	开启规则匹配统计功能，缺省为关闭	本参数用于开启本规则的匹配统计功能，而**packet-filter**命令中的**hardware-count**参数则用于开启指定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
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”
qos-local-id *local-id-value*	QoS本地ID值	指定ACL规则的QoS本地ID值	*local-id-value*：QoS本地ID值，取值范围为1～4095，当前仅支持取值为1～3999，缺省情况下未配置QoS本地ID值。有关QoS本地ID值的详细介绍和具体配置过程，请参见“三层技术-IP路由配置指导”中的“路由策略”
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，表示该规则对非VPN报文和VPN报文均有效

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 *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）、**dns**（53）、**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）
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，表示匹配不携带ACK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。 表示匹配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

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
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。

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。

display acl all 命令可以查看所有已存在的 IPv4 高级 ACL 规则和 IPv4 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 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。
- **undo rule** { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

【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 advanced 3000
[Sysname-acl-ipv4-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 advanced 3001
[Sysname-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-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 advanced 3002
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv4-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 advanced 3003
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv4-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）

1.1.18 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**] *

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

【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，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。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：表示开启规则匹配统计功能，缺省为关闭。

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。

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，表示该规则对非 VPN 报文和 VPN 报文均有效。

【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。

display acl all 命令可以查看所有已存在的 IPv4 高级 ACL 规则和 IPv4 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 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。
- **undo rule** { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

counting 参数用于开启本规则的匹配统计功能，而 **packet-filter** 命令中的 **hardware-count** 参数则用于开启指定 ACL 内所有规则的匹配统计功能。

【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 basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-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）

1.1.19 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* | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **qos-local-id** *local-id-value* | **routing** | **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** | **icmp6-type** | **logging** | **qos-local-id** | **routing** | **hop-by-hop** | **source** | **source-port** | **time-range** | **vpn-instance**] *

undo rule { **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* | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **qos-local-id** | **routing** | **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* | **user-group** *group-name* | **vpn-instance** *vpn-instance-name*] *

【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，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。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）。**ipv6** 表示所有协议类型。

*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	开启规则匹配统计功能，缺省为关闭	本参数用于开启本规则的匹配统计功能，而**packet-filter ipv6**命令中的**hardware-count**参数则用于开启指定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）

参数	类别	作用	说明
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
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	路由头	指定路由头的类型	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”
qos-local-id *local-id-value*	QoS本地ID值	指定ACL规则的QoS本地ID值	*local-id-value*：QoS本地ID值，取值范围为1～4095，当前仅支持取值为1～3999，缺省情况下未配置QoS本地ID值。有关QoS本地ID值的详细介绍和具体配置过程，请参见“三层技术-IP路由配置指导”中的“路由策略”
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，表示该规则对非VPN报文和VPN报文均有效

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，

参数	类别	作用	说明
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	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）、**dns**（53）、**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）
{ **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，表示匹配不携带ACK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。 表示匹配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

ICMPv6 消息名称	ICMPv6 消息类型	ICMPv6 消息码
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】

如果 QoS 策略或报文过滤功能应用于出方向，则不支持配置 flow-label 参数。

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。

display acl ipv6 all 命令可以查看所有已存在的 IPv6 高级 ACL 规则和 IPv6 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 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。
- **undo rule** { **deny** | **permit** }命令无法删除规则中的部分内容，使用 undo rule { deny | permit } 命令时，必须输入已存在规则的完整形式。

【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 advanced 3000
[Sysname-acl-ipv6-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 advanced 3001
```

```
[Sysname-acl-ipv6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
[Sysname-acl-ipv6-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 advanced 3002
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv6-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv6-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv6-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 advanced 3003
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv6-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 advanced 3004
[Sysname-acl-ipv6-adv-3004] rule permit ipv6 hop-by-hop type 5
[Sysname-acl-ipv6-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）

1.1.20 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** | **logging** | **routing** | **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** | **logging** | **routing** | **source** | **time-range** | **vpn-instance**] *

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

【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，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。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：表示开启规则匹配统计功能，缺省为关闭。

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：表示对 IPv6 所有类型的路由头有效。

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，表示该规则对非 VPN 报文和 VPN 报文均有效。

【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。

display acl ipv6 all 命令可以查看所有已存在的 IPv6 高级 ACL 规则和 IPv6 基本 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 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。
- **undo rule** { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

counting 参数用于开启本规则的匹配统计功能，而 **packet-filter ipv6** 命令中的 **hardware-count** 参数则用于开启指定 ACL 内所有规则的匹配统计功能。

【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 basic 2000
[Sysname-acl-ipv6-basic-2000] rule permit source 1001:: 16
[Sysname-acl-ipv6-basic-2000] rule permit source 3124:1123:: 32
[Sysname-acl-ipv6-basic-2000] rule permit source fe80:5060:1001:: 48
[Sysname-acl-ipv6-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）

1.1.21 rule (Layer 2 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** *dot1p* | **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**] *

undo rule { **deny** | **permit** } [**cos** *dot1p* | **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*] *

【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，系统将从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。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 *dot1p*：指定 802.1p 优先级。*dot1p* 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：表示开启规则匹配统计功能，缺省为关闭。

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，取值范围为十六进制数 0～ffff。*lsap-type-mask* 表示 LSAP 的类型掩码，用于指定屏蔽位，取值范围为十六进制数 0～ffff。

type *protocol-type protocol-type-mask*：指定链路层协议类型。*protocol-type* 表示数据帧类型，对应 Ethernet_II 类型和 Ethernet_SNAP 类型帧中的 type 域，取值范围为十六进制数 0～ffff。*protocol-type-mask* 表示类型掩码，用于指定屏蔽位，取值范围为十六进制数 0～ffff。

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。

display acl mac all 命令可以查看所有已存在的二层 ACL 规则。

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 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。
- **undo rule** { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

counting 参数用于开启本规则的匹配统计功能，而 **packet-filter** 命令中的 **hardware-count** 参数则用于开启指定 ACL 内所有规则的匹配统计功能。

【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 mac 4000
[Sysname-acl-mac-4000] rule permit type 0806 ffff
[Sysname-acl-mac-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）

1.1.22 rule (user-defined ACL view)

rule 命令用来为用户自定义 ACL 创建一条规则。

undo rule 命令用来为用户自定义 ACL 删除一条规则。

【命令】

rule [*rule-id*] { **deny** | **permit** } [{ **l2***rule-string rule-mask offset* }&<1-8>] [**counting** | **time-range** *time-range-name*] *

undo rule *rule-id*

undo rule { **deny** | **permit** } [{ **l2** *rule-string rule-mask offset* }&<1-8>] [**counting** | **time-range** *time-range-name*] *

【缺省情况】

用户自定义 ACL 内不存在任何规则。

【视图】

用户自定义 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

rule-id：指定用户自定义 ACL 规则的编号，取值范围为 0～65534。若未指定本参数，系统将按照步长为 5 从 0 开始，自动分配一个大于现有最大编号的步长最小倍数。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。

l2：表示从 L2 帧头开始偏移。

rule-string：指定用户自定义的规则字符串，必须是 16 进制数组成，字符长度必须是偶数。

rule-mask：指定规则字符串的掩码，用于和报文作“与”操作，必须是 16 进制数组成，字符长度必须是偶数，且必须与 *rule-string* 的长度相同。

offset：指定偏移量，它以用户指定的报文头部为基准，指定从第几个字节开始进行比较。

&<1-8>：表示前面的参数最多可以输入 8 次。

counting：表示开启规则匹配统计功能，缺省为关闭。

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，并导致创建失败。

display acl user-defined all 命令可以查看所有已存在的用户自定义 ACL 规则。

undo rule { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令删除整条规则时，必须输入已存在规则的完整形式。

counting 参数用于开启本规则的匹配统计功能，而 **packet-filter** 命令中的 **hardware-count** 参数则用于开启指定 ACL 内所有规则的匹配统计功能。

【举例】

为用户自定义 ACL 5005 创建规则如下：允许从 L2 帧头开始算起第 13、14 两字节的内容为 0x0806 的报文（即 ARP 报文）通过。

```
<Sysname> system-view
[Sysname] acl user-defined 5005
[Sysname-acl-user-5005] rule permit l2 0806 ffff 12
```

【相关命令】

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

1.1.23 rule comment

rule comment 命令用来为规则配置描述信息。

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 basic 2000
[Sysname-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] rule 0 comment This rule is used on ten-gigabitethernet 1/0/1.
```

【相关命令】

- **display acl**

1.1.24 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* [**start** *start-value*]

undo step

【缺省情况】

规则编号的步长为 5，起始值为 0。

【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。

start-value：表示规则编号的起始值。取值范围为 0～20。

【使用指导】

系统为规则自动分配编号的方式如下：系统从规则编号的起始值开始，自动分配一个大于现有最大编号的步长最小倍数。譬如原有编号为 0、5、9、10 和 12 的五条规则，步长为 5，此时如果创建一条规则且不指定编号，那么系统将自动为其分配编号 15。

如果步长或规则编号的起始值发生了改变，ACL 内原有全部规则的编号都将自动从规则编号的起始值开始按步长重新排列。譬如，某 ACL 内原有编号为 0、5、9、10 和 15 的五条规则，当修改步长为 2 之后，这些规则的编号将依次变为 0、2、4、6 和 8。

【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 basic 2000
[Sysname-acl-ipv4-basic-2000] step 2
```

【相关命令】

- **display acl**

目 录

1 QoS策略

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】

（独立运行模式）

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

（IRF 模式）

display traffic classifier user-defined [*classifier-name*] [**chassis** *chassis-number* **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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板上流分类的信息，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。如果未指定本参数，将显示全局主用主控板上类的配置信息。（IRF 模式）

【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: 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	类的名称及其内容，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】

未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，用户自定义ACL序号的取值范围是5000～5999 *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
any	定义匹配所有数据包的规则

取值	描述
control-plane protocol *protocol-name*&<1-8>	定义匹配控制平面或者管理口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，具体如表1-3所示，&<1-8>表示前面的参数最多可以输入8次
control-plane protocol-group *protocol-group-name*	定义匹配控制平面或者管理口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*	定义匹配内层VLAN Tag 802.1p优先级的规则，802.1p优先级的取值范围为0～7
customer-vlan-id *vlan-id-list*	定义匹配内层VLAN Tag VLAN ID的规则，*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1～4094，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，仅对以太网接口生效
dscp *dscp-value*	定义匹配DSCP的规则，DSCP的取值范围为0～63；也可以输入关键字，具体如表1-5所示
forwarding-layer route	定义匹配三层转发的报文
ip-precedence *ip-precedence-value*	定义匹配IP优先级的规则，IP优先级的取值范围为0～7
protocol *protocol-name*	定义匹配协议的规则，*protocol-name*取值为ip、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，目前仅支持取值为1～3999
service-dot1p *dot1p-value*&<1-8>	定义匹配外层VLAN Tag 802.1p优先级的规则，802.1p优先级的取值范围为0～7
service-vlan-id *vlan-id-list*	定义匹配外层VLAN Tag VLAN ID的规则，*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1～4094，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 若只携带单层VLAN Tag，可以用外层VLAN Tag的VLAN ID规则来匹配
source-mac *mac-address*	定义匹配源MAC地址的规则，仅对以太网接口生效
vlan-tag { double | none | single }	定义匹配报文携带的VLAN Tag层次的规则： • **double**：匹配携带双层 VLAN Tag 的报文 • **none**：匹配不携带 VLAN Tag 的报文 • **single**：匹配携带单层 VLAN Tag 的报文

表1-3 系统预定义匹配协议报文类型名称的列表

报文类型	说明
arp	ARP协议
arp-snooping	ARP Snooping协议
bfd	BFD协议
bgp	BGP协议

报文类型	说明
bgp4+	IPv6 BGP
dhcp	DHCP协议
dhcp-snooping	DHCP Snooping协议
dhcpv6	IPv6 DHCP协议
dldp	DLDP协议
dot1x	802.1p 协议
icmp	ICMP协议
icmpv6	IPv6 ICMP协议
igmp	IGMP协议
ip-option	带选项字段的IPv4报文
ipv6-option	带选项字段的IPv6报文
isis	IS-IS协议
lacp	LACP协议
lldp	LLDP协议
mvrp	MVRP协议（包含GVRP协议）
ospf-multicast	OSPF组播
ospf-unicast	OSPF单播
ospf3-multicast	OSPFv3组播
ospf3-unicast	OSPFv3单播
pvst	PVST协议
ssh	SSH协议
stp	STP协议
telnet	TELNET协议
vrrp	VRRP协议
vrrp6	IPv6 VRRP协议

【使用指导】

一个类下可配置多条匹配命令，各个配置之间互相不覆盖。

在定义匹配规则（控制平面和 VLAN ID）时，请注意：

一条命令可以配置多个规则，如果指定了多个相同的规则，系统默认为一个；一条命令中多个不同的规则是或的关系，即只要有一个值匹配，就算匹配这条规则。

- 删除某条匹配的规则时，必须与该规则中定义的完全相同才会删除，顺序可以不同。

在定义匹配 ACL 的规则时，请注意：

- 如果类中引用的 ACL 不存在，则不能在硬件中下发。

当 **if-match** 中引用的 ACL 规则的动作为 **deny** 时，则忽略 ACL 规则的动作，以流行为中定义的动作为准，报文匹配只使用 ACL 中的分类域。

【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 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 DSCP 值为 1 的报文。

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

定义类 class1 的匹配规则为：匹配 IP 优先级值为 1 的报文。

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

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 operator or
[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 operator or
[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或管理口控制平面的 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或管理口控制平面的 normal 协议组报文。

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

在流分类 class1 中配置匹配组播类型的报文。

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

1.1.3 traffic classifier

traffic classifier 命令用来创建一个类，并进入类视图。如果指定的类已经存在，则直接进入类视图。

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】

不存在类。

【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 命令用来恢复缺省情况。

【命令】

accounting [**byte** | **packet**]

undo accounting

【缺省情况】

未配置流量统计动作。

【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。

【使用指导】

若配置流量统计动作但不指定 **byte** 和 **packet** 参数，则设备会基于包进行流量统计。

【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 命令用来恢复缺省情况。

【命令】

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

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

undo car

【缺省情况】

未配置流量监管动作。

【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 且必须为 8 的整数倍。

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

- 如果不指定 cbs 参数，缺省取值为与 62.5 × committed-information-rate 的乘积最接近且不小于该乘积值的 512 的整数倍，但是最大值不能超过 256000000。
- 如果指定 cbs 参数，取值范围 512～256000000 且必须为 512 的整数倍。

ebs *excess-burst-size*：超出突发尺寸，单位为 byte。取值范围为 0～256000000 且必须为 512 的整数倍。

pir *peak-information-rate*：峰值速率，单位为 kbps。取值范围为 8～160000000 且必须为 8 的整数倍。不配置峰值速率表示所配置的是单速桶流量监管，否则表示双速桶流量监管。

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。

mode：分层 CAR 和 CAR 动作的合作模式。有 **and** 和 **or** 两种模式，默认为 **and** 模式。

- **and**：在该模式下，对于多条数据流应用同一个分层 CAR，必须每条流满足各自的 CAR 配置，同时各流量之和又满足分层 CAR 的配置，流量才能正常通过。
- **or**：在该模式下，对于多条数据流应用同一个分层 CAR，只要每条流满足各自的 CAR 配置或者各流量之和满足分层 CAR 配置，流量即可正常通过。

【使用指导】

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

如果未配置峰值速率，则表示所配置的是单速率流量监管，否则表示双速率流量监管。

【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 51200bytes，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 51200 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】

（独立运行模式）

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

（IRF 模式）

display traffic behavior user-defined [*behavior-name*] [**chassis** *chassis-number* **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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板上流行为的信息，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。如果未指定本参数，则显示全局主用主控板上流行为的配置信息。（IRF 模式）

【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 200 (kbps), CBS 51200 (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

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

表1-4 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

字段	描述
Marking	标记相关信息
Remark dscp	重新标记报文的DSCP优先级值
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，单位为byte
EBS	超出突发尺寸，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
Filter enable	流量过滤动作
Remark dot1p	重新标记报文的802.1p优先级值
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 命令用来恢复缺省情况。

【命令】

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

undo filter

【缺省情况】

未配置流量过滤动作。

【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 nest top-most

nest top-most 命令用来添加报文的外层 VLAN Tag。

undo nest top-most 命令用来恢复缺省情况。

【命令】

nest top-most vlan *vlan-id*

undo nest top-most

【缺省情况】

未添加报文外层 VLAN Tag。

【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 1～4094。

【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。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

【举例】

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

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

1.2.6 redirect

redirect 命令用来为流行为配置流量重定向动作。

undo redirect 命令用来恢复缺省情况。

【命令】

redirect { **cpu** | **interface** *interface-type interface-number* [**track-oap**] | **next-hop** { *ipv4-add1* [**track** *track-entry-number*] [*ipv4-add2* [**track** *track-entry-number*]] | *ipv6-add1* [**track** *track-entry-number*] [*ipv6-add2* [**track** *track-entry-number*]] } }

undo redirect { **cpu** | **interface** *interface-type interface-number* | **next-hop** }

【缺省情况】

未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。

track-oap：重定向到接口的行为需要关心 OAP client 的状态。

next-hop：重定向到指定的下一跳。

ipv4-add1：优选的下一跳 IPv4 地址。如果重定向到优选的 IPv4 地址失败，则会重定向到备选 IPv4 地址。

ipv4-add2：备选的下一跳 IPv4 地址。

ipv6-add1：优选的下一跳 IPv6 地址。如果重定向到优选的 IPv6 地址失败，则会重定向到备选 IPv6 地址。

ipv6-add2：备选的下一跳 IPv6 地址。

track *track-entry-number*：指定下一跳关联的 Track 项，优选和备选的地址可以分别指定不同的 Track 项。*track-entry-number* 取值范围为 1～1024。通过指定 Track 项，可实现与监测特性（如 NQA、BFD）的联动，详情请参见“可靠性配置指导”中的“Track”。

【使用指导】

配置 **track-oap** 后，只有存在 OAP Client 且指定接口为内部业务接口或连接独立业务部件接口，才会执行重定向动作，否则，设备不执行该重定向动作。有关内部业务接口和连接独立业务部件接口的详细介绍，请参见“OAA 配置指导”中的“OAP 单板配置”或“OAP 配置”。

基于接口应用 QoS 策略时，本系列设备只支持在二层以太网接口下配置流量重定向动作。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

在配置重定向到下一跳的动作时，指定的下一跳地址必须路由可达，如果同时配置了优选和备选地址，则至少需要有一个地址路由可达，否则将导致重定向失败。在配置生效后，重定向功能会定期查询路由表，检查下一跳地址是否有效；如果配置了 Track 项，则通过 Track 检测结果来判断下一跳地址是否有效。如果检测到优选和备选地址均失效，则重定向到下一跳的动作将不再生效。在 IRF 环境中，当 IRF 成员设备之间通过多个 IRF 物理端口互联时，不支持跨成员设备配置重定向到接口。即流量的入接口和重定向接口需要是同一成员设备上的接口。有关 IRF 的相关介绍请参见“虚拟化技术配置指导”中的“IRF”。

【举例】

为流行为配置流量重定向动作，重定向到接口 Ten-GigabitEthernet1/0/1。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface ten-gigabitethernet 1/0/1
```

【相关命令】

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

1.2.7 remark customer-vlan-id

remark customer-vlan-id 命令用来重标记报文的 CVLAN。

undo remark customer-vlan-id 命令用来恢复缺省情况。

【命令】

remark customer-vlan-id *vlan-id*

undo remark customer-vlan-id

【缺省情况】

未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】

vlan-id：表示重标记报文内层 VLAN（CVLAN）的编号，取值范围为 1～4094。

【举例】

在流行为 b1 上配置重标记报文的 CVLAN 为 VLAN 111。

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark customer-vlan-id 111
```

1.2.8 remark dot1p

remark dot1p 命令用来配置重新标记报文的 802.1p 优先级或内外层标签 802.1p 优先级复制动作。

undo remark dot1p 命令用来恢复缺省情况。

【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】

未配置重新标记报文 802.1p 优先级以及内外层标签 802.1p 优先级复制动作。

【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。

red：对红色报文进行重标记。

yellow：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：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。

对于只携带一层 VLAN tag 的报文，配置的 **remark dot1p customer-dot1p-trust** 不会生效。

在同一个流行为中，如果多次对同一种颜色的报文重新标记 802.1p 优先级，则最后一次执行的命令生效。

【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
```

1.2.9 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】

未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】

应用该动作的流行为只能应用在入方向。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

【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
```

1.2.10 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】

未配置重新标记报文 DSCP 值的动作。

【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。

red：对红色报文进行重标记。

yellow：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 1-5 所示。

表1-5 DSCP 关键字与值的对应表

关键字	DSCP 值（二进制）	DSCP 值（十进制）
af11	001010	10
af12	001100	12

关键字	DSCP 值（二进制）	DSCP 值（十进制）
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
default	000000	0
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
```

1.2.11 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】

未配置重新标记报文 IP 优先级的动作。

【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
```

1.2.12 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】

未配置重新标记报文本地优先级的动作。

【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。

red：对红色报文进行重标记。

yellow：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。

【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
```

1.2.13 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】

未配置重新标记报文的 QoS 本地 ID 值的动作。

【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，目前仅支持取值为 1～3999。

【使用指导】

一般情况下，在 QoS 策略的入方向对报文的 QoS 本地 ID 值进行标记，在 QoS 策略的出方向根据标记的 QoS 本地 ID 值对报文进行分类以及指定相应的流行为，两者要结合使用。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

【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
```

1.2.14 remark service-vlan-id

remark service-vlan-id 命令用来重标记报文的 SVLAN。

undo remark service-vlan-id 命令用来恢复缺省情况。

【命令】

remark service-vlan-id *vlan-id*

undo remark service-vlan-id

【缺省情况】

未配置重新标记报文的 SVLAN 的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

vlan-id：表示重标记报文外层 VLAN（SVLAN）的编号，取值范围为 1～4094。

【举例】

在流行为 b1 上配置重标记报文的 SVLAN 为 VLAN 222。

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark service-vlan-id 222
```

1.2.15 traffic behavior

traffic behavior 命令用来创建一个流行为，并进入流行为视图。如果指定的流行为已经存在，则直接进入流行为视图。

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】

不存在流行为。

【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 定义和应用QoS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** | **insert-before** *before-classifier-name*]

undo classifier *classifier-name*

【缺省情况】

没有为类指定流行为。

【视图】

QoS 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：表示该流分类与流行为的关联模式为 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”。

insert-before *before-classifier-name*：表示将配置的类插入到 QoS 策略中已存在的指定类之前。*before-classifier-name* 表示 QoS 策略中已存在的类名，为 1～31 个字符的字符串，区分大小写。不指定该参数时，表示新配置的类与流行为配对将添加到 QoS 策略最后。

【使用指导】

QoS 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 QoS 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
```

在 QoS 策略 user1 中为类 database 指定流行为 test，并将该类插入到策略中已存在的类 class-a 前。

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

【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】

（独立运行模式）

control-plane slot *slot-number*

（IRF 模式）

control-plane chassis *chassis-number* **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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：指定单板。*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。（IRF 模式）

【举例】

进入指定 slot 上的控制平面视图。（独立运行模式）

```
<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】

（独立运行模式）

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

（IRF 模式）

display qos policy user-defined [*policy-name* [**classifier** *classifier-name*]] [**chassis** *chassis-number* **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 QoS 策略。

policy-name：QoS 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*：QoS 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 QoS 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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板的 QoS 策略的信息，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。如果未指定本参数，则显示全局主用主控板的 QoS 策略的信息。（IRF 模式）

【举例】

显示用户定义 QoS 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 51200 (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 4
   Classifier: 3 (ID 102)
     Behavior: 3
      -none-
```

表1-6 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QoS策略的信息

字段	描述
Policy	QoS策略名

其它显示信息解释请参见 表 1-1 和 表 1-4。

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】

（独立运行模式）

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

（IRF 模式）

display qos policy control-plane chassis *chassis-number* **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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板的控制平面应用 QoS 策略的信息，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。（IRF 模式）

【举例】

显示应用到指定 slot 上的控制平面的 QoS 策略信息。（独立运行模式）

```
<Sysname> display qos policy control-plane slot 2

Control plane slot 2

  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 51200 (Bytes), EBS 512 (Bytes)
      Green action  : pass
      Yellow action : pass
      Red action    : discard
      Green packets : 0 (Packets) 0 (Bytes)
      Yellow packets: 0 (Packets) 0 (Bytes)
      Red packets   : 0 (Packets) 0 (Bytes)
  Classifier: 2
    Operator: AND
    Rule(s) :
     If-match protocol ipv6
    Behavior: 2
     Accounting enable:
       0 (Packets)
     Filter enable: Permit
     Marking:
       Remark dscp 3
  Classifier: 3
    Operator: AND
    Rule(s) :
     -none-
    Behavior: 3
     -none-
```

表1-7 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
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 1-6。

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】

（独立运行模式）

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

（IRF 模式）

display qos policy control-plane pre-defined [**chassis** *chassis-number* **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。如果未指定本参数，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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板的系统预定义的控制平面策略信息，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。如果未指定本参数，则显示所有成员设备上在位单板以及所有 PEX 设备的系统预定义的控制平面应用 QoS 策略的信息。（IRF 模式）

【举例】

显示指定 slot 上的系统预定义的控制平面应用 QoS 策略的信息。（独立运行模式）

```
<Sysname> display qos policy control-plane pre-defined slot 1
Pre-defined policy information slot 1
  Protocol          Priority   Bandwidth          Group
  IS-IS             29         512 (kbps)         critical
  VRRP              36         512 (kbps)         important
  OSPF Multicast    30         1024 (kbps)        critical
  OSPF Unicast      30         1024 (kbps)        critical
  PIM Multicast     24         128 (kbps)         critical
  PIM Unicast       24         128 (kbps)         critical
  IGMP              18         512 (kbps)         important
  PIMv6 Multicast   24         64 (kbps)          critical
  PIMv6 Unicast     24         64 (kbps)          critical
  OSPFv3 Unicast    30         1024 (kbps)        critical
  OSPFv3 Multicast  30         1024 (kbps)        critical
  VRRPv6            36         512 (kbps)         important
  ARP               12         768 (kbps)         normal
  DHCP Snooping     18         256 (kbps)         redirect
  DHCP              18         768 (kbps)         normal
  802.1x            12         128 (kbps)         important
  STP               36         256 (kbps)         critical
  LACP              36         64 (kbps)          critical
  MVRP              18         256 (kbps)         critical
  BGP               24         256 (kbps)         critical
  ICMP              9          512 (kbps)         monitor
  IPOPTION          18         384 (kbps)         normal
```

```
BGPv6              24          256 (kbps)          critical
IPOPTIONv6         18          64 (kbps)           normal
LLDP               24          64 (kbps)           important
DLDP               24          64 (kbps)           critical
TELNET             8           512 (kbps)          management
SSH                8           512 (kbps)          management
HTTP               12          64 (kbps)           management
HTTPS              12          64 (kbps)           management
TACACS             12          64 (kbps)           management
RADIUS             12          64 (kbps)           management
ARP Snooping       18          256 (kbps)          redirect
ICMPv6             8           512 (kbps)          monitor
PVST               35          2560 (kbps)         critical
DHCPv6             18          256 (kbps)          normal
BFD                31          12800 (kbps)        critical
```

表1-8 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
Default	其他协议
Priority	优先级
Bandwidth	带宽
Group	协议所属的协议组

其它显示信息解释请参见 表 1-3。

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】

（独立运行模式）

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

（IRF 模式）

display qos policy global [**chassis** *chassis-number* **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。如果未指定本参数，则显示主用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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板的基于全局应用 QoS 策略的信息，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。如果未指定本参数，则显示全局主用主控板上基于全局应用 QoS 策略的信息，不显示各单板及 PEX 设备的信息。（IRF 模式）

【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。

【举例】

显示基于全局应用 QoS 策略的信息。

```
<Sysname> display qos policy global
  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 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dscp 3
```

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

表1-9 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 1-4。

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 Ten-GigabitEthernet1/0/1 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 ten-gigabitethernet 1/0/1 inbound
Interface: Ten-GigabitEthernet1/0/1
  Direction: Inbound
```

```
  Policy: 1
   Classifier: 1
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dscp 3
   Classifier: 3
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      -none-
     Behavior: 3
      -none-
```

显示所有接口上 QoS 策略的接口的配置信息和运行情况。

```
<Sysname> display qos policy interface
Interface: Ten-GigabitEthernet1/0/1
  Direction: Inbound
```

```
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: Ten-GigabitEthernet1/0/2
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)

Interface: Ten-GigabitEthernet1/0/3
  Direction: Inbound
  Policy: b
   Classifier: b
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: b
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0(Packets)
        Red packets   : 0 (Packets)

Interface: Ten-GigabitEthernet1/0/3
  Direction: Inbound
  Policy: a
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: Ten-GigabitEthernet1/0/4
      Committed Access Rate:
        CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
```

```
        Red packets    : 0 (Packets)
```

表1-10 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
Matched	符合分类规则的数据包数目
5-minute statistics	最近5分钟的流速统计信息
Forwarded	符合分类规则的成功转发报文在统计周期内的平均速率
Dropped	符合分类规则的丢弃报文在统计周期内的平均速率
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 1-4。

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】

（独立运行模式）

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

（IRF 模式）

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**chassis** *chassis-number* **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 1～4094。

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。如果未指定本参数，则显示主用主控板上基于 VLAN 应用 QoS 策略的信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板上基于 VLAN 应用 QoS 策略的信息，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。如果未指定本参数，则显示全局主用主控板上基于 VLAN 应用 QoS 策略的信息。（IRF 模式）

【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。

【举例】

显示 VLAN 2 的 QoS 策略信息。

```
<Sysname> display qos vlan-policy vlan 2
Vlan 2
  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 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0(Packets) 0(Bytes)
        Yellow packets: 0(Packets) 0(Bytes)
        Red packets   : 0(Packets) 0(Bytes)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dscp 3
   Classifier: 3
     Operator: AND
     Rule(s) :
      -none-
```

```
Behavior: 3
 -none-
```

表1-11 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 1-4。

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

qos apply policy 命令用来在以太网服务实例、接口或控制平面上应用 QoS 策略。

undo qos apply policy 命令用来取消以太网服务实例、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】

未应用 QoS 策略。

【视图】

控制平面视图

接口视图

【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】

三层聚合接口/子接口不支持应用 QoS 策略；三层聚合接口存在子接口时，该聚合接口的成员端口也不支持应用 QoS 策略。

【举例】

将策略 USER1 应用到接口 Ten-GigabitEthernet1/0/1 的出方向上。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
```

```
[Sysname-Ten-GigabitEthernet1/0/1] 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 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】

未在全局应用 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。

【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
```

1.3.11 qos policy

qos policy 命令用来创建一个策略，并进入策略视图。如果指定的策略已经存在，则直接进入策略视图。

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】

不存在策略。

【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**

1.3.12 qos vlan-policy

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

undo qos vlan-policy 命令用来取消 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】

未在 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 1～4094。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
```

1.3.13 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】

（独立运行模式）

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

（IRF 模式）

reset qos policy control-plane chassis *chassis-number* **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。（独立运行模式）

chassis *chassis-number*：清除指定单板的基于控制平面应用 QoS 策略的统计信息，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。（IRF 模式）

【举例】

清除应用到指定 slot 上的控制平面的 QoS 策略统计信息。（独立运行模式）

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

1.3.14 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
```

1.3.15 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 1～4094。

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 命令用来显示优先级映射表配置情况。

【命令】

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

【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-dp	802.1p优先级到丢弃优先级映射表
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-dp	DSCP到丢弃优先级映射表
dscp-dscp	DSCP到DSCP映射表
exp-dot1p	EXP到802.1p优先级映射表
exp-dscp	EXP到DSCP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	映射表的名称
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 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 优先级到本地优先级映射表的映射关系，与 802.1p 优先级 4、5 相对应的本地优先级为 1。

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

【相关命令】

- **display qos map-table**

2.1.3 map export

map export 命令用来将映射关系配置到指定 MPLS 标签的 EXP 域。

undo map export 命令用来恢复缺省情况。

【命令】

map export mpls-exp

undo map export

【缺省情况】

如果入方向的报文为不带 MPLS 标签的私网报文，则映射关系同时被配置到出方向添加得第一层和第二层 MPLS 标签的 EXP 域；如果入方向的报文为带两层 MPLS 标签的公网报文，则映射关系只被配置到出方向第一层 MPLS 标签的 EXP 域。

【视图】

优先级映射表视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

mpls-exp：表示映射关系仅配置到第一层 MPLS 标签的 EXP 域。

【使用指导】

该命令仅对输出值为 EXP 的优先级映射表生效。

如果入方向的报文为不带 MPLS 标签的私网报文，则本命令配置后映射关系只被配置到第一层 MPLS 标签的 EXP 域，同时第二层 MPLS 标签的 EXP 域会被设置为 0；如果入方向的报文为带两层 MPLS 标签的公网报文，则本命令配置后则映射关系不会被配置到 MPLS 标签的 EXP 域。

【举例】

配置 802.1p 优先级到 EXP 优先级映射表的映射关系，与 802.1p 优先级 4、5 相对应的 EXP 优先级为 1，并且仅将映射关系配置到第一层 MPLS 标签的 EXP 域。

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

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 { **dot1p-dp** | **dot1p-exp** | **dot1p-lp** | **dscp-dp** | **dscp-dscp** | **exp-dot1p** }

【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 优先级到本地优先级映射表视图。

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

进入 802.1p 优先级到本地优先级映射表视图。

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

【相关命令】

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

2.2 端口优先级信任模式配置命令

2.2.1 display qos trust interface

display qos trust interface 命令用来显示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】

显示端口优先级信任模式信息。

```
<Sysname> display qos trust interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
 Port priority trust information
  Port priority:4
  Port priority trust type: dscp
```

表2-3 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
Port priority trust type	端口优先级信任类型，取值为： • dot1p：802.1p 优先级 • dscp：DSCP 优先级

2.2.2 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 { **dot1p** | **dscp** }

undo qos trust

【缺省情况】

设备信任报文的 802.1p 优先级。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

dot1p：信任报文自带的 802.1p 优先级，以此优先级进行优先级映射。

dscp：信任 IP 报文自带的 DSCP，以此优先级进行优先级映射。

【使用指导】

VXLAN 网络的公网侧端口和 AC 侧端口都不支持配置优先级信任模式为 DSCP。关于 VXLAN 的配置，请参见“VXLAN 配置指导”中的“VXLAN”。

【举例】

在接口 Ten-GigabitEthernet1/0/1 上配置优先级信任模式为信任报文自带的 802.1p 优先级。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos trust dot1p
```

【相关命令】

display qos trust interface

2.3 端口优先级配置命令

2.3.1 qos priority

qos priority 命令用来配置端口的端口优先级。

undo qos priority 命令用来恢复端口优先级为缺省值。

【命令】

qos priority *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，取值范围为 0～7。

【举例】

配置接口 Ten-GigabitEthernet1/0/1 的端口优先级为 2。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos priority 2
```

【相关命令】

- **display qos trust interface**

3 流量整形和限速

3.1 流量整形配置命令

3.1.1 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: Ten-GigabitEthernet1/0/1
 Rule: If-match queue 1
  CIR 1000 (kbps), CBS 62976 (Bytes)
 Rule: If-match queue 4
  CIR 400 (kbps), CBS 25088 (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，当采用绝对值形式输入时，单位为kbps；当采用百分比形式时，单位为%
CBS	承诺突发尺寸，当采用绝对值形式输入时，单位为byte；当采用百分比形式时，单位为ms，实际的CBS值是*cbs-time* 乘以实际的承诺信息速率（**cir**值乘以接口带宽）

3.1.2 qos gts (interface view)

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】

接口上未配置流量整形。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue *queue-id*：对队列上的数据包进行流量整形。*queue-id* 为匹配的队列号，取值范围为 0～7。

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 8～10000000，40GE 端口的取值范围为 8～40000000，100GE 端口的取值范围为 8～100000000。用户配置的数值必须是 8 的倍数。

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 62.5**committed-information-rate*，且必须为 512 的整数倍，如果乘积不是 512 的整数倍，就取比乘积大的最近的 512 的整数倍，最大不能超过 16000000。
- 如果指定 cbs 参数，取值范围为 512～16000000，*committed-burst-size* 必须为 512 的整数倍。

【使用指导】

不配置峰值速率表示所配置的是单速率流量整形，否则表示双速率流量整形。

【举例】

在接口 Ten-GigabitEthernet1/0/1 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 ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos gts queue 1 cir 6400 cbs 51200
```

3.2 限速配置命令

3.2.1 display qos lr interface

display qos lr interface 命令用来显示接口上的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-GigabitEthernet1/0/1
 Direction: Inbound
  CIR 2000 (kbps), CBS 20000 (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，可以是Inbound、Outbound
CIR	承诺信息速率，当采用绝对值形式输入时，单位为kbps；当采用百分比形式时，单位为%
CBS	承诺突发尺寸，当采用绝对值形式输入时，单位为byte；当采用百分比形式时，单位为ms，实际的CBS值是*cbs-time* 乘以实际的承诺信息速率（**cir**值乘以接口带宽）

3.2.2 qos lr

qos lr 命令用来配置限速。

undo qos lr 命令用来取消配置的限速。

【命令】

qos lr outbound cir *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos lr outbound

【缺省情况】

未配置限速。

【视图】

接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

outbound：对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 8～1000000，万兆端口的取值范围为 8～10000000，40GE 端口的取值范围为 8～40000000，100GE 端口的取值范围为 8～100000000。用户配置的数值必须是 8 的倍数。

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*，且必须为 512 的整数倍，如果乘积不是 512 的整数倍，就取比乘积大的最近的 512 的整数倍，最大不能超过 128000000。
- 如果指定 cbs 参数，取值范围为 512～128000000，*committed-burst-size* 必须为 512 的整数倍。

【举例】

对接口 Ten-GigabitEthernet1/0/1 上出方向的报文进行限速。正常流速为 256kbps，突发流量为 51200bytes，以后速率小于等于 256kbps 时正常发送，速率大于 256kbps 时，将进行限速。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos lr outbound cir 256 cbs 51200
```

4 拥塞管理

4.1 拥塞管理公共配置命令

4.1.1 display qos queue interface

display qos queue interface 命令用来显示接口上队列配置情况和统计信息。

【命令】

display qos queue 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队列配置情况和运行统计信息。

【举例】

显示所有接口下的队列信息。

```
<Sysname> display qos queue interface
Interface: Ten-GigabitEthernet1/0/1
 Output queue: Strict Priority queuing
Interface: Ten-GigabitEthernet1/0/2
 Output queue: Strict Priority queuing
Interface: Ten-GigabitEthernet1/0/3
 Output queue: Strict Priority queuing
Interface: Ten-GigabitEthernet1/0/4
 Output queue: Strict Priority queuing
Interface: Ten-GigabitEthernet1/0/5
 Output queue: Strict Priority queuing
Interface: Ten-GigabitEthernet1/0/6
 Output queue: Strict Priority queuing
```

表4-1 display qos queue 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组成
Output queue	当前出队列的相关信息

字段	描述
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按照每次轮询可发送的报文个数进行计算，N/A表示该队列采用SP调度算法
Byte count	各个队列的调度权重，当前WRR队列调度权重的计算方式为按照每次轮询可发送的字节数进行计算

4.2 严格优先级队列配置命令

4.2.1 display qos queue sp interface

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 Ten-GigabitEthernet1/0/1 的严格优先级队列配置情况。

```
<Sysname> display qos queue sp interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
 Output queue: Strict Priority queuing
```

表4-2 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组成
Output queue	当前出队列类型

4.2.2 qos sp

qos sp 命令用来在接口上配置严格优先队列。

undo qos sp 命令用来恢复缺省情况。

【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 Ten-GigabitEthernet1/0/1 上应用 SP 模式的队列调度。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos sp
```

【相关命令】

- **display qos queue sp interface**

4.3 加权轮询队列配置命令

4.3.1 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 Ten-GigabitEthernet1/0/1 的 WRR 队列配置情况。

```
<Sysname> display qos queue wrr interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
 Output queue: Weighted Round Robin queuing
 Queue ID        Queue name      Group           Weight
 ------------------------------------------------------
 0               be              1               1
 1               af1             1               1
 2               af2             1               1
 3               af3             1               1
 4               af4             1               1
 5               ef              1               1
 6               cs6             1               1
 7               cs7             sp              N/A
```

表4-3 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组成
Output queue	当前出队列类型
Queue ID	队列号
Queue name	队列名称
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按照每次轮询可发送的报文个数进行计算，N/A表示该队列采用SP调度算法
Byte count	各个队列的调度权重，当前WRR队列调度权重的计算方式为按照每次轮询可发送的字节数进行计算，N/A表示该队列采用SP调度算法

4.3.2 qos wrr

qos wrr 命令用来在接口上开启 WRR 队列。

undo qos wrr 命令用来恢复缺省情况。

【命令】

qos wrr { **byte-count** | **weight** }

undo qos wrr { **byte-count** | **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】

byte-count：表示按照每次轮询可发送的字节数进行计算。

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** 命令在接口上开启 WRR 队列，然后才能进行 WRR 配置。

【举例】

在接口 Ten-GigabitEthernet1/0/1 上开启 WRR 队列，并按照每次轮询可发送的报文个数进行计算。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr weight
```

在接口 Ten-GigabitEthernet1/0/1 上开启 WRR 队列，并按照每次轮询可发送的字节数进行计算。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr byte-count
```

【相关命令】

- **display qos queue wrr interface**

4.3.3 qos wrr { byte-count | weight }

qos wrr { **byte-count** | **weight** }命令用来配置 WRR 队列或修改 WRR 队列的参数。

undo qos wrr 命令用来取消 WRR 队列调度参数的配置。

【命令】

qos wrr *queue-id* **group** { **1** | **2** } { **byte-count** | **weight** } *schedule-value*

undo qos wrr *queue-id*

【缺省情况】

在使用 WRR 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。

表4-4 *queue-id* 数字和关键字对应表

queue-id 数字	*queue-id* 关键字
0	be
1	af1
2	af2
3	af3
4	af4
5	ef
6	cs6
7	cs7

group { **1** | **2** }：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。各组之间执行优先级调度，由组 1 至组 2 优先级依次降低。仅 SF 系列接口板支持配置 WRR 调度组 2。

byte-count：表示按照每次轮询可发送的字节数进行计算。

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** 命令在接口上开启 WRR 队列，然后才能进行本配置。

【举例】

在接口 Ten-GigabitEthernet1/0/1 上应用 WRR 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，分组为 1。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr byte-count
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr 0 group 1 byte-count 10
```

【相关命令】

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

4.3.4 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 命令用来取消将队列加入 SP 组。

【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 1 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。

【使用指导】

本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。

【举例】

在接口 Ten-GigabitEthernet1/0/1 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 ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr weight
[Sysname-Ten-GigabitEthernet1/0/1] qos wrr 0 group sp
```

【相关命令】

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

4.4 加权公平队列配置命令

4.4.1 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 Ten-GigabitEthernet1/0/1 的加权公平队列配置情况。

```
<Sysname> display qos queue wfq interface ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
 Output queue: Hardware Weighted Fair Queuing
 Queue ID        Queue name      Group           Byte count      Min Bandwidth
 ------------------------------------------------------------------------------
 0               be              1               1               64
 1               af1             1               1               64
 2               af2             1               1               64
 3               af3             1               1               64
 4               af4             1               1               64
 5               ef              1               1               64
 6               cs6             1               1               64
 7               cs7             1               1               64
```

表4-5 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组成
Output queue	当前出队列类型
Queue ID	队列号
Queue name	队列名称
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
Byte-count	各个队列的调度权重，当前WRR队列调度权重的计算方式为按照每次轮询可发送的字节数进行计算
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按照每次轮询可发送的报文个数进行计算， N/A表示该队列采用SP调度算法
Min-Bandwidth	队列的最小保证带宽值

4.4.2 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，每个队列的最小带宽保证为 64kbps。

【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。

min *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。千兆端口的取值范围为 8～1000000，万兆端口的取值范围为 8～10000000，40GE 端口的取值范围为 8～40000000，100GE 端口的取值范围为 8～100000000，单位为 kbps。

【使用指导】

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

【举例】

在接口 Ten-GigabitEthernet1/0/1 上配置队列 0 的最小保证带宽值为 100kbps。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wfq weight
[Sysname-Ten-GigabitEthernet1/0/1] qos bandwidth queue 0 min 100
```

【相关命令】

- **qos wfq**

4.4.3 qos wfq

qos wfq 命令用来在接口上开启 WFQ 队列。

undo qos wfq 命令用来恢复缺省情况。

【命令】

qos wfq { **byte-count** | **weight** }

undo qos wfq { **byte-count** | **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】

byte-count：表示按照每次轮询可发送的字节数进行计算。

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 wfq** 命令在接口上开启 WFQ 队列，然后才能进行 WFQ 配置。

【举例】

在接口 Ten-GigabitEthernet1/0/1 上开启 WFQ 队列，并按照每次轮询可发送的报文个数进行计算。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wfq weight
```

在接口 Ten-GigabitEthernet1/0/1 上开启 WFQ 队列，并按照每次轮询可发送的字节数进行计算。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wfq byte-count
```

【相关命令】

- **display qos queue wfq interface**

4.4.4 qos wfq { byte-count | weight }

qos wfq { **byte-count** | **weight** }命令用来配置 WFQ 队列或修改 WFQ 队列的参数。

undo qos wfq 命令用来取消 WFQ 队列调度参数的配置。

【命令】

qos wfq *queue-id* **group** { **1** | **2** } { **byte-count** | **weight** } *schedule-value*

undo qos wfq *queue-id*

【缺省情况】

在使用 WFQ 队列时，所有队列都处于 WFQ 调度组 1 中，各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。

group { **1** | **2** }：表示该队列属于哪个 WFQ 优先组，缺省为 group 1。其中 group 1 表示该队列属于 WFQ 优先组 1，group 2 表示该队列属于 WFQ 优先组 2。各组之间执行优先级调度，由组 1 至组 2 优先级依次降低。仅 SF 系列接口板支持配置 WFQ 调度组 2。

byte-count：表示按照每次轮询可发送的字节数进行计算。

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 1～16。

【使用指导】

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

【举例】

在接口 Ten-GigabitEthernet1/0/1 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，分组为 1。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wfq byte-count
[Sysname-Ten-GigabitEthernet1/0/1] qos wfq 0 group 1 byte-count 10
```

【相关命令】

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

4.4.5 qos wfq group sp

qos wfq 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 wfq group sp 命令用来取消将队列加入 SP 组。

【命令】

qos wfq *queue-id* **group sp**

undo qos wfq *queue-id*

【缺省情况】

当使用 WFQ 队列时，所有队列都处于 WFQ 调度组 1 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。

【使用指导】

本命令需要在端口队列为 WFQ 调度模式下使用。

SP 组与普通 WFQ 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 WFQ 优先组。

【举例】

在接口 Ten-GigabitEthernet1/0/1 上应用 WFQ 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 ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wfq weight
[Sysname-Ten-GigabitEthernet1/0/1] qos wfq 0 group sp
```

【相关命令】

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

4.5 队列调度策略配置命令

4.5.1 bandwidth queue

bandwidth queue 命令用来配置队列调度策略下队列的最小带宽保证。

undo bandwidth queue 命令用来恢复缺省情况。

【命令】

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

undo bandwidth queue *queue-id*

【缺省情况】

在队列调度策略中配置某个队列为 WFQ 队列后，该队列的最小带宽保证为 64kbps。

【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。取值范围为 0～7。

min *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。取值范围为 8～100000000。

【使用指导】

必须先在队列调度策略中将某个队列配置为 WFQ 队列，才能为该队列配置最小带宽保证。

【举例】

在队列调度策略 myprofile 中，配置队列 0 使用 WFQ 队列算法，使用报文个数作为调度权重，权重值为 1，分组为 1，并为该队列配置最小保证带宽值为 100kbps。

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 0 wfq group 1 weight 1
[Sysname-qmprofile-myprofile] bandwidth queue 0 min 100
```

4.5.2 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】

（独立运行模式）

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

（IRF 模式）

display qos qmprofile configuration [*profile-name*] [**chassis** *chassis-number* **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*：显示指定单板的队列调度策略的配置情况。*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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板的队列调度策略的配置情况，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。如果未指定本参数，则显示全局主用主控板的队列调度策略的配置情况。（IRF 模式）

【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   Schedule  Min         Max
                         unit       value     bandwidth   bandwidth
 ------------------------------------------------------------------------
 be        SP    N/A     N/A        N/A       0           N/A
 af1       WFQ   1       weight     1         200         N/A
 af2       WFQ   1       weight     1         0           N/A
 af3       WFQ   1       weight     2         0           N/A
 af4       WFQ   1       weight     2         0           N/A
 ef        WFQ   1       weight     3         0           N/A
 cs6       WFQ   1       weight     4         0           N/A
 cs7       WFQ   1       weight     3         0           N/A
```

表4-6 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）、WFQ（加权公平队列）
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
Schedule vlaue	• 队列调度单位为 weight 时，表示报文个数 • 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，N/A表示无效
Max bandwidth	最大带宽值，N/A表示无效

4.5.3 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。

【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 ten-gigabitethernet 1/0/1
Interface: Ten-GigabitEthernet1/0/1
Direction: Outbound
 Queue management profile: myprofile
```

表4-7 display qos qmprofile interface 命令显示信息描述表

字段	描述
Interface	接口名称
Direction	应用方向
Queue management profile	队列调度策略名称

4.5.4 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】

接口上未应用队列调度策略。

【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。

inbound：表示在接口的入方向上应用队列调度策略。如果未指定该参数，则表示在接口的出方向应用队列调度策略。

【使用指导】

每个接口在同一方向上只能应用一个队列调度策略。

【举例】

在接口 Ten-GigabitEthernet1/0/1 上应用队列调度策略 myprofile。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos apply qmprofile myprofile
```

【相关命令】

- **display qos qmprofile interface**

4.5.5 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。如果指定的队列调度策略已经存在，则直接进入该队列调度策略视图。

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 *profile-name*

undo qos qmprofile *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】

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】

如果需要删除已经应用到接口的队列调度策略，必须先在应用的位置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。

【举例】

创建队列调度策略 myprofile，并进入队列调度策略视图。

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

【相关命令】

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

4.5.6 queue (queue scheduling profile view)

queue 命令用来配置队列调度参数。

undo queue 命令用来取消队列调度参数的配置。

【命令】

queue *queue-id* { **sp** | **wfq group** *group-id* { **weight | byte-count** } *schedule-value* | **wrr group** *group-id* { **weight | byte-count** } *schedule-value* }

undo queue *queue-id*

【缺省情况】

缺省情况下，队列调度策略的内容是所有队列均采用 SP 方式调度。

【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。取值范围为 0～7。

sp：配置队列为严格优先级调度。

wfq：配置队列为加权公平调度。

wrr：配置队列为加权轮询调度。

group *group-id*：优先组号。*group-id* 取值范围为 1～2。仅 SF 系列接口板支持 *group-id* 取值为 2。对于 WFQ 队列，如果不选则此参数，则表示将队列加入组 1。

byte-count：表示按照每次轮询可发送的字节数进行计算。

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。对于 WFQ 优先组取值范围为 1～16，对于 WRR 优先组取值范围为 1～15。

【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**

5 拥塞避免

5.1 WRED配置命令

5.1.1 display qos wred interface

display qos wred interface 命令用来显示 WRED 配置情况和统计信息。

【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

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 WRED 配置情况和统计信息。

【举例】

显示所有接口的 WRED 配置情况和统计信息。

```
<Sysname> display qos wred interface
Interface: Ten-GigabitEthernet1/0/3
 Current WRED configuration:
 Applied WRED table name: q1
```

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】

（独立运行模式）

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

（IRF 模式）

display qos wred table [**name** *table-name*] [**chassis** *chassis-number* **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*：WRED 表的名称，为 1～32 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 WRED 表配置情况。

slot *slot-number*：显示指定单板的 WRED 表配置情况。*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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定单板的 WRED 表配置情况，*chassis-number* 表示设备在 IRF 中的成员编号或者 PEX 对应的虚拟框号，*slot-number* 表示单板或 PEX 所在的槽位号。如果未指定本参数，则显示全局主用主控板的 WRED 表配置情况。（IRF 模式）

【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

字段	描述
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
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 表。

undo qos wred apply 命令用来恢复缺省情况。

【命令】

qos wred apply [*table-name*]

undo qos wred apply

【缺省情况】

接口没有应用 WRED 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，为 1～32 个字符的字符串，区分大小写。如果未指定本参数，则在接口上应用缺省 WRED 表。

【举例】

在接口 Ten-GigabitEthernet1/0/1 上应用 WRED 表。

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] qos wred apply table1
```

【相关命令】

- **display qos wred interface**

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

5.1.4 qos wred queue table

qos wred queue table 命令用来创建 WRED 表，同时进入该 WRED 表视图。如果指定的 WRED 表已经存在，则直接进入 WRED 表视图。

undo qos wred queue table 命令用来删除 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】

table *table-name*：指定 WRED 表的名称，为 1～32 个字符的字符串，区分大小写。

【使用指导】

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

缺省 WRED 表可以通过 **display qos wred table** 命令显示，不允许修改和删除。

【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，*low-limit* 的缺省取值为 100，*high-limit* 的缺省取值为 1000，*discard-prob* 的缺省取值为 10。

【视图】

WRED 表视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

all：表示所有队列。

queue-id：队列编号。取值范围为 0～7。

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*：丢弃概率，取值越大，计算出的丢弃概率越小。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。

【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】

配置基于队列的 WRED 表 queue-table1 中队列 1 的丢弃参数：丢弃级别为 1，队列平均长度的下限为 10，队列平均长度的上限为 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 queue 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。

拥塞通知功能仅对 TCP 连接中的已知单播生效。

【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 queue 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。取值范围为 0～7。

weighting-constant *exponent*：计算平均队列长度的指数。*exponent* 的取值范围为 1～15。

【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 queue table**

6 聚合CAR

6.1 聚合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 用来恢复缺省情况。

【命令】

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

undo car

【缺省情况】

未配置全局 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。

mode：分层 CAR 和聚合 CAR 动作的合作模式。有 **and** 和 **or** 两种模式，默认为 **and** 模式。

- **and**：在该模式下，对于多条数据流应用同一个分层 CAR，必须每条流满足各自的聚合 CAR 配置，同时各流量之和又满足分层 CAR 的配置，流量才能正常通过。
- **or**：在该模式下，对于多条数据流应用同一个分层 CAR，只要每条流满足各自的聚合 CAR 配置或者各流量之和满足分层 CAR 配置，流量即可正常通过。

【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
```

配置流行为 be1 的聚合 CAR 动作为 aggcar-1，分层 CAR 动作为 hcar，合作模式为 or。

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

【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，包含聚合 CAR 和分层 CAR。

【举例】

显示全局 CAR 的配置和统计信息。（独立运行模式）

```
<Sysname> display qos car name
 Name: a
  Mode: aggregative
   CIR 32 (kbps) CBS: 2048 (Bytes) PIR: 888 (kbps) EBS: 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
  Slot 0:
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Slot 1:
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
  Slot 2:
   Apply failed

Name: b
  Mode: hierarchy
```

```
CIR 64 (kbps) CBS: 2048 (Bytes)
```

表6-1 display qos car name 命令显示信息描述表

字段	描述
Name	聚合CAR的名称
Mode	聚合CAR的类型，取值为aggregative（聚合CAR）和hierarchy（分层CAR）
CIR CBS PIR 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
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

6.1.3 qos car (system view)

qos car 命令用来配置聚合 CAR 或分层 CAR。

undo qos car 命令用来取消聚合 CAR 或分层 CAR 的配置。

【命令】

qos car *car-name* { **aggregative** | **hierarchy** } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

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

undo qos car *car-name*

【缺省情况】

未配置聚合 CAR 或分层 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。

cir *committed-information-rate*：承诺信息速率，单位为 kbps。取值范围为 8～160000000 且必须为 8 的整数倍。

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，缺省取值为与 62.5 × *committed-information-rate* 的乘积最接近且不小于该乘积值的 512 的整数倍，但是最大值不能超过 256000000。
- 如果指定 cbs 参数，取值范围 512～256000000 且必须为 512 的整数倍。

ebs *excess-burst-size*：过度突发尺寸，单位为 byte。本参数仅全局 CAR 为聚合模式时支持。

配置 **pir** 参数后：

- 如果不指定 **ebs**，则 **ebs** 缺省取值为与 62.5 × *peak-information-rate* 的乘积最接近且不小于 512 的整数倍，但是最大值不能超过 256000000。
- 如果指定 **ebs**，取值范围 0～256000000 且必须为 512 的整数倍。

未配置 **pir** 参数时，**ebs** 的取值范围为 0～256000000 且必须为 512 的整数倍。

pir *peak-information-rate*：峰值速率，单位为 kbps。取值范围为 8～160000000 且必须为 8 的整数倍，本参数仅全局 CAR 为聚合模式时支持。

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**，本参数仅全局 CAR 为聚合模式时支持。

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**，本参数仅全局 CAR 为聚合模式时支持。

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**，本参数仅全局 CAR 为聚合模式时支持。

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；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。

【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。

分层 CAR 配置需要在策略中引用后才能生效。

不配置峰值速率表示所配置的是单速率流量监管，否则表示双速率流量监管。

【举例】

配置聚合 CAR 采取的 CAR 参数取值，**cir** 取值为 25600，**cbs** 取值为 512000，对于红色报文采取丢弃的动作。

```
<Sysname> system-view
[Sysname] qos car aggcar-1 aggregative cir 25600 cbs 512000 red discard
```

配置分层 CAR 采取的 CAR 参数取值，**cir** 取值为 120，**cbs** 取值为 51200。

```
<Sysname> system-view
[Sysname] qos car h-car hierarchy cir 120 cbs 51200
```

【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，包含聚合 CAR 和分层 CAR。

【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*] **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。

【举例】

显示接口 Ten-GigabitEthernet1/0/1 的队列出方向统计信息。

```
<Sysname> display qos queue-statistics interface ten-gigabitethernet 1/0/1 outbound
Interface: Ten-GigabitEthernet1/0/1
 Direction: outbound
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Queue 0
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 1
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 2
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 3
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
```

```
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 4
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 5
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 6
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 Dropped: 0 packets, 0 bytes
 Current queue length: 0 packets
Queue 7
 Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
 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）

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。如果指定的时间段已经创建，则本命令可以修改时间段的时间范围。

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】

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。

在一个时间段中，可以使用以下两种方式定义时间范围：

- 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。

如果一个时间段中同时包含以上两种时间范围，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。例如在一个时间段中定义周期时间段为每周一的 8 点到 12 点，定义绝对时间段为 2015 年全年，那么该时间段的生效时间范围为 2015 年全年内每周一的 8 点到 12 点。

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**