H3C S12500-X & S12500X-AF 系列以太网交换机

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：6W101-20151130
产品版本：Release 1135 及以上

前 言

H3C S12500-X & S12500X-AF 系列以太网交换机 命令参考（R113x）共分为十七本手册，对S12500-X & S12500X-AF 系列交换机 Release 1135 及以上软件版本支持的命令进行了介绍。《ACL和 QoS 命令参考》主要介绍了配置 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。

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 命令用来创建一个 ACL，并进入相应的 ACL 视图。

undo acl 命令用来删除指定或全部 ACL。

【命令】

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

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

【缺省情况】

不存在任何 ACL。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

- 2000～2999：表示 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 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。

all：指定全部 IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 和用户自定义 ACL。

【使用指导】

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

【举例】

创建一个编号为 2000 的 IPv4 基本 ACL，并进入其视图。

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

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

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

【相关命令】

- **display acl**

1.1.2 acl copy

acl copy 命令用来复制并生成一个新的 ACL。

【命令】

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

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

- 2000～2999：表示 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称。

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

- 2000～2999：表示 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 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。若未指定本参数，系统将不会为目的 ACL 设置名称。对于基本 ACL 或高级 ACL，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称。

【使用指导】

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

【举例】

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

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

1.1.3 acl name

acl name 命令用来进入指定名称的 ACL 视图。

【命令】

acl name *acl-name*

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

【举例】

进入已存在的、名称为 flow 的 IPv4 基本 ACL 的视图。

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

【相关命令】

- **acl**

1.1.4 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/二层 ACL 视图/用户自定义 ACL

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

【举例】

为 IPv4 基本 ACL 2000 配置描述信息。

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

【相关命令】

- **display acl**

1.1.5 display acl

display acl 命令用来显示 ACL 的配置和运行情况。

【命令】

display acl { *acl-number* | **all** | **name** *acl-name* }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

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

- 2000～2999：表示 IPv4 基本 ACL。

- 3000～3999：表示 IPv4 高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

all：显示全部 IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 和用户自定义 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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称。

【使用指导】

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

【举例】

显示 IPv4 基本 ACL 2001 的配置和运行情况。

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

表1-1 display acl 命令显示信息描述表

字段	描述
Basic ACL 2001	该ACL的类型和编号，ACL的类型包括： • Basic ACL：表示 IPv4 基本 ACL • Advanced ACL：表示 IPv4 高级 ACL • Ethernet frame ACL：表示二层 ACL • User defined ACL：表示用户自定义 ACL
named flow	该ACL的名称为flow，-none-表示没有名称
1 rule	该ACL内包含的规则数量
match-order is auto	该ACL的规则匹配顺序为自动排序（匹配顺序为配置顺序时不显示本字段）
This is an IPv4 basic ACL.	该ACL的描述信息
ACL's step is 5	该ACL的规则编号的步长值为5
rule 5 permit source 1.1.1.1 0	规则5的具体内容
rule 5 comment This rule is used on FortyGigE 1/0/1.	规则5的描述信息

1.1.6 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 { **global** [**inbound** | **outbound**] [**slot** *slot-number*] | **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **interface vlan-interface** *vlan-interface-number* [**inbound** | **outbound**] [**slot** *slot-number*] }

IRF 模式：

display packet-filter { **global** [**inbound** | **outbound**] [**chassis** *chassis-number* **slot** *slot-number*] | **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】

global：显示 ACL 在报文过滤中的全局（即所有物理接口）应用情况。仅 Release 1138P01 及以上版本支持本参数。

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*：显示指定成员设备指定单板上 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，*slot-number* 表示单板所在的槽位号。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】

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

【举例】

显示接口 FortyGigE1/0/1 入方向上 ACL 在报文过滤中的应用情况。

```
<Sysname> display packet-filter interface fortygige 1/0/1 inbound
Interface: FortyGigE1/0/1
```

```
In-bound policy:
 ACL 2001 , 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
In-bound policy	ACL在入方向上的应用情况
ACL 2001	IPv4基本ACL 2001应用成功
Hardware-count	规则匹配统计功能应用成功

1.1.7 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 { **global** | **interface** *interface-type interface-number* } { **inbound** | **outbound** } [*acl-number* | **name** *acl-name*] [**brief**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

global：显示全局（即所有物理接口）统计信息。仅 Release 1138P01 及以上版本支持本参数。

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。

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 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称。

brief：显示简要统计信息。

【使用指导】

若未指定 *acl-number* 和 **name** *acl-name* 参数，将显示全部 ACL 在报文过滤中应用的统计信息。

【举例】

显示接口 FortyGigE1/0/1 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 fortygige 1/0/1 inbound
Interface: FortyGigE1/0/1
 In-bound policy:
  ACL 2001, Hardware-count
   From 2013-06-09 13:31:00 to 2013-06-09 13:31:42
   rule 0 permit source 2.2.2.2 0
   rule 5 permit source 1.1.1.1 0
   Totally 0 packets permitted, 0 packets denied
   Totally 0% permitted, 0% denied
```

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

字段	描述
Interface	在指定接口上应用的统计信息
In-bound policy	在入方向上应用的统计信息
ACL 2001	IPv4基本ACL 2001应用成功
Hardware-count	规则匹配统计功能应用成功
From 2013-06-09 13:31:00 to 2013-06-09 13:31:42	该统计的起始和终止时间
Totally 0 packets permitted, 0 packets denied	该ACL允许和拒绝符合条件报文的个数
Totally 0% permitted, 0% denied	该ACL允许和拒绝符合条件报文的百分比

【相关命令】

- **reset packet-filter statistics**

1.1.8 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** } { *acl-number* | **name** *acl-name* } [**brief**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

inbound：显示入方向上 ACL 在报文过滤中应用的累加统计信息。

outbound：显示出方向上 ACL 在报文过滤中应用的累加统计信息。

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

- 2000～2999：表示 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称。

brief：显示 ACL 在报文过滤中应用的简要累加统计信息。

【举例】

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

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

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

字段	描述
Sum	ACL在报文过滤中应用的累加统计信息
In-bound policy	ACL在入方向上应用的累加统计信息
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 0 packets permitted, 0 packets denied	该ACL允许和拒绝符合条件报文的个数
Totally 0% permitted, 0% denied	该ACL允许和拒绝符合条件报文的百分比

【相关命令】

- **reset packet-filter statistics**

1.1.9 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 { **global** | **interface** *interface-type interface-number* } { **inbound** | **outbound** } [*acl-number* | **name** *acl-name*] [**slot** *slot-number*]

IRF 模式：

display packet-filter verbose { **global** | **interface** *interface-type interface-number* } { **inbound** | **outbound** } [*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】

global：显示 ACL 在报文过滤中的全局（即所有物理接口）详细应用情况。仅 Release 1138P01 及以上版本支持本参数。

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。

inbound：显示入方向上 ACL 在报文过滤中的详细应用情况。

outbound：显示出方向上 ACL 在报文过滤中的详细应用情况。

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

- 2000～2999：表示 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称。

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

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备指定单板上 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，*slot-number* 表示单板所在的槽位号。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* 和 **name** *acl-name* 参数，将显示全部 ACL 在报文过滤中的详细应用情况。

【举例】

显示接口 FortyGigE1/0/1 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 fortygige 1/0/1 inbound
Interface: FortyGigE1/0/1
 In-bound policy:
  ACL 2001, Hardware-count
   rule 0 permit source 2.2.2.2 0
   rule 5 permit source 1.1.1.1 0
```

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

字段	描述
Interface	ACL在指定接口上的详细应用情况
In-bound policy	ACL在入方向上的详细应用情况
ACL 2001	IPv4基本ACL 2001应用成功
Hardware-count	规则匹配统计功能应用成功

1.1.10 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*：显示指定成员设备指定单板上 QoS 和 ACL 资源的使用情况，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。若未指定本参数，将显示 IRF 中所有成员设备的所有单板上 QoS 和 ACL 资源的使用情况。（IRF 模式）

【使用指导】

如果指定的单板、主控板或者成员设备不支持统计 QoS 和 ACL 资源，将不会显示该单板、主控板或者成员设备上 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: FGE1/0/1 to FGE1/0/6
-------------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
 IFP ACL          23040      4608       0          18432      20%
 IFP Meter        30720      48         0          30672      0%
 IFP Counter      8191       49         0          8142       0%
 EFP ACL          9216       0          0          9216       0%

Interfaces: FGE1/0/7 to FGE1/0/12
-------------------------------------------------------------------------
 Type             Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
 IFP ACL          23040      4608       0          18432      20%
 IFP Meter        30720      48         0          30672      0%
 IFP Counter      8191       49         0          8142       0%
 EFP ACL          9216       0          0          9216       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 • IFP 表示入方向的资源数目 • EFP 表示出方向的资源数目
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%。

1.1.11 packet-filter

packet-filter 命令用来在接口上应用 ACL 进行报文过滤。

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

【命令】

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

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

【缺省情况】

接口不对报文进行过滤。

【视图】

二层以太网接口视图/三层以太网接口视图/三层以太网子接口视图/VLAN 接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

- 2000～2999：表示 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 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。对于基本 ACL 或高级 ACL，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称。

inbound：对收到的报文进行过滤。

outbound：对发出的报文进行过滤。

extension：表示使用 TCAM 中的资源来实现报文过滤。仅 Release 1138P01 及以上版本支持本参数。

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

【使用指导】

在使用 **extension** 参数前，请先将设备硬件资源的运行模式设置为 ACL 模式。关于设备硬件资源运行模式的介绍，请参见“基础配置指导”中的“设备管理”。

使用 IPv4 高级 ACL 对 ACK 或 RST 标志位为 1 的 TCP 报文进行分类后，如果 **packet-filter** 命令直接指定该 IPv4 高级 ACL，则仅支持过滤接口收到的这类报文。

对于 ACK 或 RST 标志位为 1 的 TCP 报文，如果使用 **packet-filter** 命令对接口发出的这类报文进行过滤：

(1) 建议先通过 QoS 策略的方式重标记这类报文的 QoS 本地 ID 值；

(2) 使用 IPv4 高级 ACL 匹配重标记的 QoS 本地 ID 值；

(3) 通过 **packet-filter** 命令应用匹配重标记 QoS 本地 ID 值的 IPv4 高级 ACL，实现对接口发出的这类报文进行过滤，即过滤接口发出的 ACK 或 RST 标志位为 1 的 TCP 报文。

关于过滤接口发出的 ACK 或 RST 标志位为 1 的 TCP 报文的举例，请查看“ACL 和 QoS 配置指导”中的“ACL 配置”。

【举例】

应用 IPv4 基本 ACL 2001 对接口 FortyGigE1/0/1 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 fortygige 1/0/1
[Sysname-FortyGigE1/0/1] packet-filter 2001 inbound hardware-count
```

【相关命令】

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

1.1.12 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**

1.1.13 packet-filter global

packet-filter global 命令用来全局应用 ACL 进行报文过滤。

undo packet-filter global 命令用来取消全局应用 ACL 进行报文过滤。

【命令】

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

undo packet-filter { *acl-number* | **name** *acl-name* } **global** { **inbound** | **outbound** }

【缺省情况】

全局不对报文进行过滤。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

- 2000～2999：表示 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 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。对于基本 ACL 或高级 ACL，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称。

inbound：对收到的报文进行过滤。

outbound：对发出的报文进行过滤。

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

【使用指导】

仅 Release 1138P01 及以上版本支持本命令。

【举例】

应用 IPv4 基本 ACL 2001 对收到的报文进行过滤，并对过滤的报文进行统计。

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

```
[Sysname] packet-filter 2001 global inbound hardware-count
```

【相关命令】

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

1.1.14 reset acl counter

reset acl counter 命令用来清除 ACL 的统计信息。

【命令】

reset acl counter { *acl-number* | **all** | **name** *acl-name* }

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

- 2000～2999：表示 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 高级 ACL。
- 4000～4999：表示二层 ACL。
- 5000～5999：表示用户自定义 ACL。

all：清除全部 IPv4 基本 ACL、IPv4 高级 ACL、二层 ACL 和用户自定义 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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称。

【举例】

清除 IPv4 基本 ACL 2001 的统计信息。

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

【相关命令】

- **display acl**

1.1.15 reset packet-filter statistics

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

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

global：清除全局（即所有物理接口）统计信息。仅 Release 1138P01 及以上版本支持本参数。

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。

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 IPv4 基本 ACL。
- 3000～3999：表示 IPv4 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，必须以英文字母 a～z 或 A～Z 开头。对于基本 ACL 或高级 ACL，表示 IPv4 基本 ACL 或 IPv4 高级 ACL 的名称。

【使用指导】

若未指定 *acl-number* 和 **name** *acl-name* 参数，将清除全部 ACL 在报文过滤中应用的统计信息。

【举例】

清除接口 FortyGigE1/0/1 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 fortygige 1/0/1 inbound 2001
```

【相关命令】

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

1.1.16 rule (Ethernet frame header ACL view)

rule 命令用来为二层 ACL 创建一条规则。

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

【命令】

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

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

【缺省情况】

二层 ACL 内不存在任何规则。

【视图】

二层 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

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

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

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

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

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

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

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

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

【使用指导】

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。
- 当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。
- 当二层 ACL 用于 QoS 策略的流分类或用于报文过滤功能时：
  - 如果使用 **lsap** 参数，则 *lsap-type* 必须为 AAAA，*lsap-type-mask* 必须为 FFFF，否则 ACL 将无法正常应用。
  - 如果 QoS 策略或报文过滤功能应用于出方向，则不支持配置 **lsap**、**type** 和 **counting** 参数。

【举例】

为二层 ACL 4000 创建规则如下：拒绝源 MAC 地址前缀为 000f-e2 的所有报文通过。

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule deny source-mac 000f-e200-0000 ffff-ff00-0000
```

【相关命令】

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

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

【缺省情况】

IPv4 高级 ACL 内不存在任何规则。

【视图】

IPv4 高级 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv4 承载的协议类型，可输入的形式如下：

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

*protocol*之后可配置如 表 1-7 所示的规则信息参数。

表1-7 规则信息参数

参数	类别	作用	说明
source { *source-address* *source-wildcard* | **any** }	源地址信息	指定ACL规则的源地址信息	*source-address*：源IP地址 *source-wildcard*：源IP地址的通配符掩码（为0表示主机地址） **any**：任意源IP地址
destination { *dest-address* *dest-wildcard* | **any** }	目的地址信息	指定ACL规则的目的地址信息	*dest-address*：目的IP地址 *dest-wildcard*：目的IP地址的通配符掩码（为0表示主机地址） **any**：任意目的IP地址
counting	统计	使能规则匹配统计功能，缺省为关闭	本参数用于使能本规则的匹配统计功能，而**packet-filter**命令中的**hardware-count**参数则用于使能指定ACL内所有规则的匹配统计功能
precedence *precedence*	报文优先级	IP优先级	*precedence*用数字表示时，取值范围为0～7；用文字表示时，分别对应**routine**、**priority**、**immediate**、**flash**、**flash-override**、**critical**、**internet**、**network**
tos *tos*	报文优先级	ToS优先级	*tos*用数字表示时，取值范围为0～15；用文字表示时，可以选取**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）、**min-monetary-cost**（1）、**normal**（0）
dscp *dscp*	报文优先级	DSCP优先级	*dscp*用数字表示时，取值范围为0～63；用文字表示时，可以选取**af11**（10）、**af12**（12）、

参数	类别	作用	说明
			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	对所有分片报文生效	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
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，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” 仅Release 1138P01及以上版本支持本参数
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
destination-port *operator port1* [*port2*]	目的端口	定义TCP/UDP报文的目的端口信息	*port1*、*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用文字表示时，TCP端口号可以选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**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**

参数	类别	作用	说明
			（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）、**xdmcp**（177） 如果使用**domain**关键字来指定TCP端口号，在配置文件中保存时关键字将显示为**dns**
{ **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，用于定义TCP报文中ACK或RST标志位为1的报文

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

表1-9 ICMP 特有的规则信息参数

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

表1-10 ICMP 消息名称与消息类型和消息码的对应关系

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
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。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。
- 当 IPv4 高级 ACL 用于 QoS 策略的流分类或用于报文过滤功能时：
  - 不支持配置 **vpn-instance** 参数。
  - 不支持配置操作符 *operator* 取值为 **neq**。
  - 如果 QoS 策略或报文过滤功能应用于出方向，则不支持配置操作符 *operator* 取值为 **gt**、**lt** 和 **range**，也不支持配置 **counting** 参数，并且只能匹配三层转发报文。

【举例】

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

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

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

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

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

```
<Sysname> system-view
[Sysname] acl number 3002
```

```
[Sysname-acl-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-adv-3002] rule permit tcp destination-port eq ftp-data
```

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

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

【相关命令】

- **acl**
- **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** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

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

【缺省情况】

IPv4 基本 ACL 内不存在任何规则。

【视图】

IPv4 基本 ACL 视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

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

fragment：表示对所有分片报文生效。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。

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。
- 使用 **undo rule** 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。
- 当 IPv4 基本 ACL 用于 QoS 策略的流分类或用于报文过滤功能时：
  - 不支持配置 **vpn-instance** 参数。
  - 如果 QoS 策略或报文过滤功能应用于出方向，也不支持配置 counting 参数，则只能匹配三层转发报文。

【举例】

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

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

【相关命令】

- **acl**
- **display acl**

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

1.1.19 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*

【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，系统将按照步长从 0 开始，自动分配一个大于现有最大编号的最小编号。譬如现有规则的最大编号为 28，步长为 5，那么自动分配的新编号将是 30。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

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

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，则直接对旧规则进行覆盖，原有该编号的旧规则被删除。

- 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。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的二层 ACL 规则、IPv4 高级 ACL 规则、IPv4 基本 ACL 规则以及用户自定义 ACL 规则。
- 需要注意的是，当自定义 ACL 用于 QoS 策略的流分类或是包过滤功能时，不能在出方向进行应用。

【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 number 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）

1.1.20 rule comment

rule comment 命令用来为指定规则配置描述信息。

undo rule comment 命令用来删除指定规则的描述信息。

【命令】

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

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

【缺省情况】

规则没有任何描述信息。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图/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】

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

text：表示规则的描述信息，为 1～127 个字符的字符串，区分大小写。

【使用指导】

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

【举例】

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

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used for telnet.
```

【相关命令】

- **display acl**

1.1.21 step

step 命令用来配置规则编号的步长。

undo step 命令用来恢复缺省情况。

【命令】

step *step-value*

undo step

【缺省情况】

规则编号的步长为 5。

【视图】

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

【缺省用户角色】

network-admin

mdc-admin

【参数】

step-value：表示规则编号的步长值，取值范围为 1～20。

【举例】

将 IPv4 基本 ACL 2000 的规则编号的步长配置为 2。

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

【相关命令】

- **display acl**

目 录

1 QoS策略

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，将显示所有在位单板的类的配置信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的流分类的信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。如果未指定本参数，将显示所有成员设备上在位单板的类的配置信息。（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: 2 (ID 101)
  Operator: AND
  Rule(s) :
   If-match protocol ip

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

1.1.2 if-match

if-match 命令用来定义匹配数据包的规则。

undo if-match 命令用来删除配置的匹配数据包的规则。

【命令】

if-match *match-criteria*

undo if-match *match-criteria*

【缺省情况】

没有定义匹配数据包的规则。

【视图】

类视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

match-criteria：类的匹配规则，具体情况如 表 1-1 所示。

表1-2 类的匹配规则取值

取值	描述
acl { *acl-number* | **name** *acl-name* } [**inner**]	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2000～3999，二层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 **inner**表示使用ACL对VXLAN隧道报文的内层内容进行匹配 仅Release 1138P01及以上版本支持**inner**关键字
any	定义匹配所有数据包的规则
destination-mac *mac-address*	定义匹配目的MAC地址的规则
dscp *dscp-value*&<1-8>	定义匹配DSCP的规则，*dscp-value*&<1-8>为DSCP取值的列表，DSCP的取值范围为0～63，&<1-8>表示前面的参数最多可以输入8次；也可以输入关键字，具体如表1-4所示
ip-precedence *ip-precedence-value*&<1-8>	定义匹配IP优先级的规则，*ip-precedence-value*&<1-8>为IP优先级的列表，IP优先级的取值范围为0～7，&<1-8>表示前面的参数最多可以输入8次
protocol *protocol-name*	定义匹配协议的规则，*protocol-name*取值为ip
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
service-dot1p *dot1p-value*&<1-8>	定义匹配VLAN Tag的802.1p优先级的规则，*dot1p-value*&<1-8>为802.1p优先级值的列表，802.1p优先级的取值范围为0～7，&<1-8>表示前面的参数最多可以输入8次
service-vlan-id *vlan-id-list*	定义匹配VLAN Tag的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
source-mac *mac-address*	定义匹配源MAC地址的规则
vxlan { **any** | *vxlan-id* }	定义匹配VXLAN编号的规则 仅Release 1138P01及以上版本支持本规则

说明

- 对于同一匹配条件，若需匹配多个值，请先将流分类中各规则之间的逻辑关系配置为 **or**。
- 除 **service-vlan-id** 外，对于其他匹配条件，只有通过重复执行多次匹配单一取值的 **if-match** 命令才能对同一匹配条件的多个值进行匹配。
- 当流分类中各规则之间的逻辑关系为 **and** 时，若在一个流分类下，匹配的一条 ACL 中包含多条规则，则多条匹配规则之间的逻辑关系为 **or**。

【使用指导】

在定义各个规则的时候，注意事项如下：

(1) 定义匹配 ACL 的规则

- 如果类中引用的 ACL 不存在，则使用该类的 QoS 策略将不能正常应用。
- 当一个类下配置多条这样的命令时，各个配置之间互相不覆盖。
- 对同一个类，允许通过 ACL 名称和序号的方式分别引用一次同一个 ACL。
- 在定义匹配 VXLAN 隧道报文内层内容的规则时，ACL 中只能包含匹配报文源 IP 地址、目的 IP 地址、源端口号，目的端口号以及传输层协议类型的规则，不能包含匹配其它字段的规则。
- 在定义匹配 VXLAN 隧道报文内层内容的规则之前，当前流分类中必须已经存在定义匹配报文 VXLAN 编号的规则。
- 当一个流分类中同时存在使用 ACL 匹配 VXLAN 隧道报文的内层内容和外层内容的两条规则时，所匹配的 ACL 中只能存在一条规则，且匹配报文外层内容的 ACL 中只能包含匹配源 IP 地址的规则。

(2) 定义匹配目的 MAC 地址规则

- 当一个类下配置多条这样的命令时，各个配置之间互相不覆盖。

(3) 定义匹配源 MAC 地址规则

- 当一个类下配置多条这样的命令时，各个配置之间互相不覆盖。

(4) 定义匹配 DSCP 的规则

- 当一个类下配置多条这样的命令时，各个配置之间互相不覆盖。
- 删除某条匹配 DSCP 的规则时，指定的所有 DSCP 值必须与该规则中定义的完全相同才会删除，顺序可不一样。

(5) 定义匹配 VLAN Tag 的 802.1p 优先级的规则

- 当一个类下配置多条这样的命令时，各个配置之间互相不覆盖。
- 一条命令可以配置多个 802.1p 优先级值，最多可指定 8 个；如果指定了多个相同的 802.1p 优先级值，系统默认为一个；多个不同的 802.1p 优先级值是或的关系，即只要有一个值匹配，就算匹配这条规则。
- 删除某条匹配 802.1p 优先级的规则时，指定的所有 802.1p 优先级值必须与该规则中定义的完全相同才会删除，顺序可不一样。

(6) 定义匹配 VLAN Tag 的 VLAN ID 的规则

- 当一个类下配置多条这样的命令时，各个配置之间互相不覆盖。
- 一条命令可以配置多个 VLAN ID 值，如果指定了多个相同的 VLAN ID 值，系统默认为一个；多个不同的 VLAN ID 值是或的关系，即只要有一个值匹配，就算匹配这条规则。
- 删除某条匹配 VLAN ID 的规则时，指定的所有 VLAN ID 值必须与该规则中定义的完全相同才会删除，顺序可不一样。

(7) 定义匹配 IP 优先级的规则

- 当一个类下配置多条这样的命令时，各个配置之间互相不覆盖。
- 删除某条匹配 IP 优先级的规则时，指定的所有 IP 优先级值必须与该规则中定义的完全相同才会删除，顺序可不一样。

(8) 定义匹配 VXLAN 编号的规则

- 当一个类下配置多条这样的命令时，各个配置之间互相不覆盖。

【举例】

定义类 class1 的匹配规则为：匹配内层报文特征符合 ACL 3000 的所有 VXLAN 报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match vxlan any
[Sysname-classifier-class1] if-match acl 3000 inner
```

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 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 或 6 或 9 的报文。

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

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

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

定义类匹配 IP 协议的报文。

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

```
[Sysname-classifier-class1] if-match protocol ip
```

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

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

定义类 class1 匹配 qos-local-id 3。

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

定义类 class1 的匹配规则为：匹配 VXLAN 编号为 10 的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match vxlan 10
```

1.1.3 traffic classifier

traffic classifier 命令用来定义一个类，并进入类视图。

undo traffic classifier 命令用来删除一个类。

【命令】

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

undo traffic classifier *classifier-name*

【缺省情况】

没有定义类。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

operator：指定各规则之间的逻辑运算符。缺省情况为 **and**。

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

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

【举例】

定义一个名为 class1 的类。

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

【相关命令】

- **display traffic classifier**

1.2 定义流行为的命令

1.2.1 accounting

accounting 命令用来配置流量统计动作。

undo accounting 命令用来取消流量统计动作配置。

【命令】

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

undo accounting

【缺省情况】

没有配置流量统计动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

byte：表示报文基于字节进行统计。

packet：表示报文基于包进行统计。

【举例】

为流行为配置流量统计动作，基于字节进行统计。

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

1.2.2 car

car 命令用来配置流量监管动作。

undo car 命令用来取消流量监管动作配置。

【命令】

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]

car cir *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*]

undo car

【缺省情况】

没有配置流量监管动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

cir *committed-information-rate*：承诺信息速率。流量的平均速率，单位为 kbps。取值范围为 8～160000000 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，缺省值为 512，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。*peak-information-rate* 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。

【使用指导】

- 接口上应用的策略中使用 **car** 时，可以应用到接口报文的接收方向。
- 如果多次使用该命令在同一个流行为上配置，最后一次配置生效。

【举例】

为流行为配置流量监管。报文正常流速为 256kbps，承诺突发尺寸为 51200bytes，丢弃超出规定速率的报文。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 256 cbs 51200 ebs 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，则显示所有在位单板的流行为的配置信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的流行为的信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示所有成员设备上在位单板的流行为的配置信息。（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 128 (kbps), CBS 8192 (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1-3 display traffic behavior 命令显示信息描述表

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

字段	描述
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，也就是容纳突发流量的令牌桶深度，单位为byte
EBS	超出突发尺寸，在双令牌桶算法中超出突发流量超过承诺突发流量的部分，单位为byte
Green action	对绿色报文的动作
Red action	对红色报文的动作
Yellow action	对黄色报文的动作
Accounting enable	流量统计动作
Filter enable	流量过滤动作
none	表示没有配置其他流行为

1.2.4 filter

filter 命令用来配置流量过滤动作。

undo filter 命令用来取消流量过滤动作配置。

【命令】

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

undo filter

【缺省情况】

没有配置流量过滤动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

deny：丢弃数据包。

permit：允许数据包通过。

【举例】

为流行为配置丢弃数据包的过滤动作。

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

1.2.5 redirect

redirect 命令用来为流行为配置流量重定向动作。

undo redirect 命令用来取消流量重定向动作配置。

【命令】

redirect { **cpu** | **interface** *interface-type interface-number* }

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

【缺省情况】

没有配置流量重定向动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

cpu：重定向到 CPU。

interface：重定向到指定的接口。

interface-type interface-number：指定接口类型和接口编号。

【使用指导】

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

【举例】

为流行为配置流量重定向动作，重定向到接口 FortyGigE1/0/1。

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

【相关命令】

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

1.2.6 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 dscp *dscp-value*

undo remark dscp

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

表1-4 DSCP 关键字与值的对应表

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

【使用指导】

重标记 DSCP 优先级的动作仅在入方向生效，且只对在本设备上进行三层转发的报文生效。

【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
```

1.2.7 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 local-precedence *local-precedence-value*

undo remark local-precedence

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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
```

1.2.8 remark qos-local-id

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

undo remark qos-local-id 命令用来恢复缺省情况。

【命令】

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

undo remark qos-local-id

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

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

【使用指导】

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

【举例】

重新标记报文的 QoS 本地 ID 值为 2。

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

1.2.9 traffic behavior

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

undo traffic behavior 命令用来删除一个流行为。

【命令】

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

【缺省情况】

没有定义流行为。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

【举例】

定义一个名为 behavior1 的流行为。

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

【相关命令】

- **display traffic behavior**

1.3 定义策略和应用策略的命令

1.3.1 classifier behavior

classifier behavior 命令用来为类指定流行为。

undo classifier 命令用来取消为类指定的流行为。

【命令】

classifier *classifier-name* **behavior** *behavior-name* [**mode dcbx** | **insert-before** *before-classifier-name*] *

undo classifier *classifier-name*

【缺省情况】

没有为类指定流行为。

【视图】

策略视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

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

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

insert-before *before-classifier-name*：表示将配置的类插入到策略中已存在的指定类之前。*before-classifier-name* 表示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策略最后。

【使用指导】

- 策略下每个类只能与一个流行为关联。
- 如果配置本命令时指定的类和流行为不存在，系统将创建一个空的类和空的流行为。
- 不能对策略中已配置的类指定插入位置。

【举例】

在策略 user1 中为类 database 指定采用流行为 test。

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

【相关命令】

- **qos policy**

1.3.2 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：用户定义策略。

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

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

slot *slot-number*：显示指定单板的策略的信息，*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示所有在位单板的 QoS 策略的配置信息。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的策略的信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示所有成员设备上在位单板的 QoS 策略的配置信息。（IRF 模式）

【举例】

显示用户定义策略的配置信息。

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

  User-defined QoS policy information:

  Policy: 1 (ID 100)
   Classifier: 1 (ID 0)
     Behavior: 1
      Marking:
```

```
      Remark dscp 3
    Committed Access Rate:
      CIR 112 (kbps), CBS 8192 (Bytes), EBS 512 (Bytes)
  Classifier: 2 (ID 101)
    Behavior: 2
     Accounting enable: Packet
     Filter enable: Permit
     Marking:
       Remark dot1p 1
  Classifier: 3 (ID 102)
    Behavior: 3
     -none-
```

表1-5 display qos policy 命令显示信息描述表

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

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.3 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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上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，*slot-number* 表示单板所在的槽位号。（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。
- 如果未指定槽位号，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）
- 如果未指定成员编号和槽位号，则显示全局主用主控板上基于全局应用 QoS 策略的信息，不显示各单板的信息。（IRF 模式）

【举例】

显示基于全局应用 QoS 策略的信息。

```
<Sysname> display qos policy global inbound

  Direction: Inbound

  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 128 (kbps), CBS 8192 (Bytes), EBS 512 (Bytes)
        Green packets: 0(Packets)
        Red packets: 0(Packets)
   Classifier: 2
     Operator: AND
     Rule(s) : If-match protocol ip
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dot1p 1
```

表1-6 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
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.4 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 FortyGigE1/0/1 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 fortygige 1/0/1 inbound

Interface: FortyGigE1/0/1

  Direction: Inbound

  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 128 (kbps), CBS 8192 (Bytes), EBS 512 (Bytes)
        Green packets: 0(Packets)
        Red packets: 0(Packets)
   Classifier: 2
     Operator: AND
     Rule(s) : If-match protocol ip
     Behavior: 2
```

```
Accounting enable:
  0 (Packets)
Filter enable: Permit
Marking:
  Remark dot1p 1
```

表1-7 display qos policy interface 命令显示信息描述表

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

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.5 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。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的基于 VLAN 应用 QoS 策略的信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。（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。
- 如果未指定槽位号，则显示主用主控板上所有基于 VLAN 应用 QoS 策略的信息。（独立运行模式）
- 如果未指定成员编号和槽位号，则显示全局主用主控板上所有基于 VLAN 应用 QoS 策略的信息。（IRF 模式）

【举例】

显示 VLAN 2 的 QoS 策略信息。

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

Vlan 2

  Direction: Outbound

  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 128 (kbps), CBS 8192 (Bytes), EBS 512 (Bytes)
        Green packets: 0(Packets)
        Red packets: 0(Packets)
   Classifier: 2
     Operator: AND
     Rule(s) : If-match protocol ip
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dot1p 1
   Classifier: 3
     Operator: AND
     Rule(s) : -none-
     Behavior: 3
      -none-
```

显示名称为 1 的 QoS 策略在 VLAN 上应用的状态。

```
<Sysname> display qos vlan-policy name 1
Policy 1
```

```
Vlan 2: outbound
```

表1-8 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
Red packets	红色报文的流量统计
Vlan 2: outbound	该策略应用在VLAN2的出方向

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.6 qos apply policy

qos apply policy 命令用来在接口上应用 QoS 策略。

undo qos apply policy 命令用来取消接口上应用的 QoS 策略。

【命令】

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

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

【缺省情况】

没有在接口上应用 QoS 策略。

【视图】

二层以太网接口视图/三层以太网接口视图/三层以太网子接口视图

【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】

设备不支持在三层以太网子接口的出方向应用 QoS 策略。

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

表1-9 设备对 QoS 策略的支持情况

方向 动作	入方向	出方向
流量统计	支持	不支持

方向 动作	入方向	出方向
流量监管	支持	不支持
流量过滤	支持	支持
流镜像	支持	支持
重定向到端口	支持	不支持
重定向到CPU	支持	支持
标记报文的DSCP优先级	支持	不支持
标记报文的本地优先级	支持	不支持

【举例】

将策略 USER1 应用到接口 FortyGigE1/0/1 的出方向上。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos apply policy USER1 outbound
```

1.3.7 qos apply policy global

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

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

【命令】

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

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

【缺省情况】

没有在全局应用 QoS 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

policy-name：策略名，为 1～31 个字符的字符串，区分大小写。

inbound：对设备所有端口接收到的流量应用 QoS 策略。

outbound：对设备所有端口发送的流量应用 QoS 策略。

【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
```

1.3.8 qos policy

qos policy 命令用来定义一个策略，并进入策略视图。

undo qos policy 命令用来删除一个策略。

【命令】

qos policy *policy-name*

undo qos policy *policy-name*

【缺省情况】

没有定义策略。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

policy-name：策略名，为 1～31 个字符的字符串，区分大小写。

【使用指导】

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

【举例】

定义一个名为 user1 的策略。

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

【相关命令】

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

1.3.9 qos vlan-policy

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

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

【命令】

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

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

【缺省情况】

没有在指定 VLAN 上应用 QoS 策略。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

vlan-id-list：VLAN ID 列表，形式可以是 *vlan-id* **to** *vlan-id*，其中，*vlan-id* 为指定 VLAN 的 ID 号，取值范围为 1～4094。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
```

1.3.10 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
```

1.3.11 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 命令用来显示指定优先级映射表配置情况。

【命令】

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

【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-lp	802.1p优先级到本地优先级映射表
dscp-dot1p	DSCP到802.1p优先级映射表
dscp-dp	DSCP到丢弃优先级映射表
dscp-dscp	DSCP到DSCP映射表（仅对需要本设备进行三层转发的报文生效）

【使用指导】

如果未指定表的类型，将显示所有映射表的配置情况。

【举例】

显示 802.1p 优先级到本地优先级映射表的配置信息。

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

```
4       :       4
5       :       5
6       :       6
7       :       7
```

表2-2 display qos map-table 命令显示信息描述表

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

2.1.2 import

import 命令用来配置指定优先级映射表的映射关系。

undo import 命令用来删除配置地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 A。

【视图】

优先级映射表视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

import-value-list：输入值列表。

export-value：输出值。

all：删除配置地该映射表的所有映射关系，恢复其为缺省的映射关系。

【举例】

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

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

【相关命令】

- **display qos map-table**

- **display qos map-table color**

2.1.3 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-lp** | **dscp-dot1p**| **dscp-dp** | **dscp-dscp** }

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

参数请参见 表 2-1。

【举例】

进入 802.1p 优先级到丢弃优先级映射表视图。

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

【相关命令】

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

2.2 端口优先级配置命令

2.2.1 qos priority

qos priority 命令用来配置当前端口的端口优先级。

undo qos priority 命令用来恢复端口优先级为缺省值。

【命令】

qos priority *priority-value*

undo qos priority

【缺省情况】

端口优先级的缺省值为 0。

【视图】

二层以太网接口视图/三层以太网接口视图

【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 FortyGigE1/0/1 的端口优先级为 2。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos priority 2
```

【相关命令】

- **display qos trust interface**

2.3 端口优先级信任模式配置命令

2.3.1 display qos trust interface

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

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

【举例】

#显示端口 FortyGigE1/0/1 的优先级信任模式信息。

```
<Sysname> display qos trust interface fortygige 1/0/1
Interface: FortyGigE1/0/1
 Port priority information
  Port priority: 0
  Port priority trust type: none
```

表2-3 display qos trust interface 命令显示信息描述表（支持一种类型端口优先级的设备）

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

字段	描述
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

2.3.2 qos trust

qos trust 命令用来配置端口优先级信任模式。

undo qos trust 命令用来恢复缺省情况。

【命令】

qos trust { **dot1p** | **dscp** }

undo qos trust

【缺省情况】

设备信任报文的 802.1p 优先级。

【视图】

二层以太网接口视图/三层以太网接口视图

【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。

【举例】

在接口 FortyGigE1/0/1 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 fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos trust dot1p
```

【相关命令】

- **display qos trust interface**

3 流量整形和接口限速

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 : FortyGigE1/0/1
 Rule(s): If-match queue 1
  CIR 128 (kbps), CBS 8192 (Bytes)
 Rule(s): If-match queue 2
  CIR 256 (kbps), CBS 16384 (Bytes)
```

表3-1 display qos gts 命令显示信息描述表

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

3.1.2 qos gts

qos gts 命令用来在接口上配置流量整形。

undo qos gts 命令用来取消接口上流量整形的配置。

【命令】

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

undo qos gts queue *queue-number*

【缺省情况】

接口上没有配置流量整形。

【视图】

二层以太网接口视图/三层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

queue *queue-number*：对队列 queue 上的数据包进行流量整形，*queue-number* 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。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 62.5ms**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 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。

【举例】

在接口 FortyGigE1/0/1 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 fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos gts queue 1 cir 6400 cbs 51200
```

3.2 接口限速配置命令

3.2.1 display qos lr interface

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

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

【举例】

显示所有接口的接口限速配置情况。

```
<Sysname> display qos lr interface
Interface : FortyGigE1/0/1
 Direction: Outbound
  CIR 12800 (kbps), CBS 800256 (Bytes)

Interface : FortyGigE1/0/2
 Direction: Outbound
  CIR 25600 (kbps), CBS 1600000 (Bytes)
```

表3-2 display qos lr 命令显示信息描述表

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

3.2.2 qos lr

qos lr 命令用来在接口上配置接口限速。

undo qos lr 命令用来取消接口上配置接口限速的配置。

【命令】

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

undo qos lr outbound

【缺省情况】

接口上没有配置接口限速。

【视图】

二层以太网接口视图/三层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

outbound：对接口发送的数据流进行限速。

cir *committed-information-rate*：承诺信息速率，单位为 kbps。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】

在接口 FortyGigE1/0/1 上出方向的报文进行接口限速。正常流速为 25600kbps，突发流量为 512000bytes。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos lr outbound cir 25600 cbs 512000
```

4 拥塞管理

4.1 严格优先级队列配置命令

4.1.1 display qos queue sp

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

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

【举例】

显示 FortyGigE1/0/1 的严格优先级队列配置情况。

```
<Sysname> display qos queue sp interface fortygige 1/0/1
Interface: FortyGigE1/0/1
 Output queue: Strict Priority queuing
```

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

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

4.1.2 qos sp

qos sp 命令用来在接口上配置严格优先队列。

undo qos sp 命令用来恢复接口上缺省的队列算法。

【命令】

qos sp

undo qos sp

【缺省情况】

端口采用 SP 调度算法。

【视图】

二层以太网接口视图/三层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【举例】

在接口 FortyGigE1/0/1 上应用 SP 模式的队列调度。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos sp
```

【相关命令】

- **display qos queue sp interface**

4.2 加权轮询队列配置命令

4.2.1 display qos queue wrr interface

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

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

【举例】

显示接口 FortyGigE1/0/1 的 WRR 队列配置情况。

```
<Sysname> display qos queue wrr interface fortygige 1/0/1
Interface: FortyGigE1/0/1
```

```
Output queue: Weighted Round Robin queuing
Queue ID        Group           Weight
----------------------------------------
be              sp              NA
af1             1               2
af2             1               3
af3             1               4
af4             1               5
ef              1               9
cs6             1               13
cs7             1               15
```

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

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

4.2.2 qos wrr

qos wrr 命令用于在接口上使能 WRR 队列，并指明当前 WRR 队列调度权重的计算方式。

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

【命令】

qos wrr { **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】

二层以太网接口视图/三层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

byte-count：表示以字节数为调度单位，即按照每次轮询发送的字节数来体现调度权重。

weight：表示以报文个数为调度单位，即按照每次轮询发送的报文个数来体现调度权重。

【使用指导】

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

【举例】

在接口 FortyGigE1/0/1 上使能 WRR 队列，并将报文个数作为调度单位。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos wrr weight
```

在接口 FortyGigE1/0/1 上使能 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 fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos wrr byte-count
```

【相关命令】

- **display qos queue wrr interface**

4.2.3 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 命令用来恢复缺省情况。

【命令】

qos wrr *queue-id* **group 1** { **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】

二层以太网接口视图/三层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

group 1：表示队列所属的 WRR 调度组，目前仅支持 1 个 WRR 调度组。

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 1～127。

【使用指导】

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

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

表4-3 *queue-id* 数字和关键字对应表

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

【举例】

在接口 FortyGigE1/0/1 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 和 1 的调度权重分别为 10 和 5。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos wrr byte-count
[Sysname-FortyGigE1/0/1] qos wrr 0 group 1 byte-count 10
[Sysname-FortyGigE1/0/1] qos wrr 1 group 1 byte-count 5
```

【相关命令】

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

4.2.4 qos wrr group sp

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

undo qos wrr group sp 命令用来恢复缺省情况。

【命令】

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

undo qos wrr *queue-id*

【缺省情况】

当使用 WRR 队列时，所有队列都处于 WRR 调度组 1 中。

【视图】

二层以太网接口视图/三层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

sp：队列加入 SP 组，采用严格优先级调度算法。

【使用指导】

此命令需要在端口队列为 WRR 调度模式下使用。

SP 组与 WRR 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，然后按用户配置的调度权重对 WRR 调度组中的队列进行调度。

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

【举例】

在接口 FortyGigE1/0/1 上应用 WRR 队列，并按照每次轮询可发送的报文个数进行计算，配置队列 0 加入 SP 组进行严格优先级调度。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos wrr weight
[Sysname-FortyGigE1/0/1] qos wrr 0 group sp
```

【相关命令】

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

4.3 加权公平队列配置命令

4.3.1 display qos queue wfq interface

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

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

【举例】

显示接口 FortyGigE1/0/1 的加权公平队列配置情况。

```
<Sysname> display qos queue wfq interface fortygige 1/0/1
```

```
Interface: FortyGigE1/0/1
 Output queue: Hardware Weighted Fair Queuing
 Queue ID        Group           Byte-count      Min-Bandwidth
 ----------------------------------------------------------------
 be              1               1               64
 af1             1               1               64
 af2             1               1               64
 af3             1               1               64
 af4             1               1               64
 ef              1               1               64
 cs6             1               1               64
 cs7             1               1               64
```

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

字段	描述
Interface	接口名，由接口类型和接口编号结合在一起组成
Output queue	当前出队列类型
Queue ID	队列号
Group	分组号，说明队列所属分组
Byte-count	队列调度权重值 当前WFQ队列调度权重的计算方式为Byte-count
Min-Bandwidth	队列的最小保证带宽值

4.3.2 qos bandwidth queue

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

undo qos bandwidth queue 命令用来恢复缺省情况。

【命令】

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

undo qos bandwidth queue *queue-id*

【缺省情况】

在使用 WFQ 队列时，每个队列的最小带宽保证为 64kbps。

【视图】

二层以太网接口视图/三层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

min *bandwidth-value*：最小保证带宽值，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，表示端口流量拥塞时能够保证的最小队列带宽。

【使用指导】

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

【举例】

在接口 FortyGigE1/0/1 上配置队列 0 的最小保证带宽值为 100kbps。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos wfq weight
[Sysname-FortyGigE1/0/1] qos bandwidth queue 0 min 100
```

【相关命令】

- **qos wfq**

4.3.3 qos wfq

qos wfq 命令用来在接口上使能 WFQ 队列，并指明当前 WFQ 队列调度权重的计算方式。

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

【命令】

qos wfq { **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】

二层以太网接口视图/三层以太网接口视图

【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** 命令在接口上使能 WFQ 队列，然后才能进行 WFQ 配置。

【举例】

在接口 FortyGigE1/0/1 上使能 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 fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos wfq weight
```

在接口 FortyGigE1/0/1 上使能 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 fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos wfq byte-count
```

【相关命令】

- **display qos queue wfq interface**

4.3.4 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 命令用来恢复缺省情况。

【命令】

qos wfq *queue-id* **group 1** { **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 调度组中，各队列的调度权重均为 1。

【视图】

二层以太网接口视图/三层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

group 1 ：表示队列所属的 WFQ 调度组，目前仅支持 1 个 WFQ 调度组。

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 1～127。

【使用指导】

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

【举例】

在接口 FortyGigE1/0/1 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 和 1 的调度权重分别为 10 和 5。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos wfq byte-count
[Sysname-FortyGigE1/0/1] qos wfq 0 group 1 byte-count 10
[Sysname-FortyGigE1/0/1] qos wfq 1 group 1 byte-count 5
```

【相关命令】

- **display qos queue wfq interface**

- **qos bandwidth queue**
- **qos wfq**

4.3.5 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 命令用来恢复缺省情况。

【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 调度组中。

【视图】

二层以太网接口视图/三层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

sp：队列加入 SP 组，采用严格优先级调度算法。

【使用指导】

在使用 SP+WFQ 队列时，首先调度 WFQ 组的队列中满足最小保证带宽的流量；然后按 SP 方式对 SP 组中的队列进行调度；最后再对 WFQ 组中各队列的数据按权重进行调度。

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

【举例】

在接口 FortyGigE1/0/1 上应用 WFQ 队列，并按照每次轮询可发送的报文个数进行计算，配置队列 0 加入 SP 组进行严格优先级调度。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos wfq weight
[Sysname-FortyGigE1/0/1] qos wfq 0 group sp
```

【相关命令】

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

4.4 队列调度策略配置命令

4.4.1 bandwidth

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

undo bandwidth 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 或 表 4-3 中的关键字。

min *bandwidth-value*：最小保证带宽值，取值范围为 8～100000000，单位为 kbps，表示端口流量拥塞时能够为该队列保证的最小带宽。

【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
```

【相关命令】

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

4.4.2 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。

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*：指定成员设备上指定单板。*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。（IRF 模式）

【使用指导】

- 如果不指定队列调度策略的名称，将显示所有队列调度策略的配置情况。
- 如果不指定槽位号，则显示设备上所有队列调度策略的配置情况。（独立运行模式）
- 如果不指定成员编号和槽位号，则显示设备上所有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-unit    Schedule-vlaue    Bnadwidth
 ------------------------------------------------------------------------
 be          WFQ     N/A      weight           1                 64
 af1         WFQ     1        weight           1                 64
 af2         WFQ     N/A      weight           1                 1000
 af3         WFQ     N/A      weight           1                 64
 af4         SP      N/A      N/A              N/A               N/A
 ef          WFQ     N/A      weight           1                 64
 cs6         WFQ     1        weight           56                64
 cs7         SP      N/A      N/A              N/A               N/A
```

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

字段	描述
Queue management profile	队列调度策略名称
Queue ID	队列号
Type	队列调度类型，包括SP（严格优先级）、WRR（加权轮询调度）、WFQ

字段	描述
	（加权公平队列）
Group	队列分组，对于SP队列始终显示为N/A，对于WFQ队列和WRR队列则始终显示为1
Schedule-unit	队列调度权重类型，对于SP队列始终显示为N/A，对于WRR和WFQ队列可以根据配置显示为weight或byte-count
Schedule-vlaue	队列调度权重值，对于SP队列始终显示为N/A
Bnadwidth	队列最小带宽保证，仅当队列为WFQ队列时才能够配置

4.4.3 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 fortygige 1/0/1
Interface: FortyGigE1/0/1
 Queue management profile: myprofile
```

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

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

4.4.4 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】

二层以太网接口视图/三层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

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

【使用指导】

每个接口只能应用一个队列调度策略。

【举例】

在接口 FortyGigE1/0/1 上应用队列调度策略 myprofile。

```
<Sysname> system-view
[Sysname] interface fortygige 1/0/1
[Sysname-FortyGigE1/0/1] qos apply qmprofile myprofile
```

【相关命令】

- **display qos qmprofile interface**

4.4.5 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】

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

【举例】

创建自定义的队列调度策略 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**

4.4.6 queue

queue 命令用来配置队列调度参数。

undo queue 命令用来恢复缺省情况。

【命令】

queue *queue-id* { **sp** | **wfq group 1** { **byte-count** | **weight** } *schedule-value* | **wrr group 1** { **byte-count** | **weight** } *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。

group 1：表示队列所属的调度组。

byte-count：表示按照每次轮询发送的字节数作为调度权重进行计算。

weight：表示按照每次轮询可发送的报文个数作为调度权重进行计算。

schedule-value：调度权重，取值范围为 1～127。

wrr：配置队列为加权轮询调度。

【使用指导】

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

【举例】

创建自定义的队列调度策略 myprofile，并配置队列 0 为 SP 队列。

```
<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 WRR 队列，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 聚合CAR

5.1 聚合CAR配置命令

5.1.1 car name

car name 命令用来配置聚合 CAR 动作。

undo car 用来删除聚合 CAR 动作。

【命令】

car name *car-name*

undo car

【缺省情况】

没有配置聚合 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。

【举例】

配置流行为 be1 的聚合 CAR 动作为 aggcar-1。

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

【相关命令】

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

5.1.2 display qos car name

display qos car name 命令用来显示聚合 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：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。显示指定聚合 CAR 的配置和统计信息。如果未指定本参数，将显示所有聚合 CAR 的配置和统计信息。

【举例】

显示聚合 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 12800 (kbps), CBS 800256 (Bytes), EBS 512 (Bytes), PIR 25600 (kbps)
   Slot 0:
    Green packets: 54641 (Packets)
    Red packets: 856 (Packets)
   Slot 1:
    Green packets: 12541 (Packets)
    Red packets: 1235 (Packets)
```

显示聚合 CAR 的配置和统计信息。（IRF 模式）

```
<Sysname> display qos car name
 Name: a
  Mode: aggregative
  CIR 12800 (kbps), CBS 800256 (Bytes), EBS 512 (Bytes), PIR 25600 (kbps)
   Chassis 1 Slot 0:
    Green packets: 54641 (Packets)
    Red packets: 856 (Packets)
   Chassis 2 Slot 1:
    Green packets: 12541 (Packets)
    Red packets: 1235 (Packets)
```

表5-1 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，即aggregative
CIR CBS EBS PIR	流量监管流量的参数配置
Green packets	绿色报文的流量统计
Red packets	红色报文的流量统计

5.1.3 qos car

qos car 命令用来配置聚合 CAR。

undo qos car 命令用来取消聚合 CAR 的配置。

【命令】

qos car *car-name* **aggregative cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]

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

undo qos car *car-name*

【缺省情况】

没有配置聚合 CAR。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

car-name：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。

aggregative：配置的 CAR 模式为聚合 CAR。

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，缺省值为 512，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。*peak-information-rate* 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。

【使用指导】

聚合 CAR 配置需要通过 MQC 方式应用在接口入方向上才能生效。

【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
```

【相关命令】

- **display qos car name**

5.1.4 reset qos car name

reset qos car name 命令用来清除聚合 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：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。清除指定聚合 CAR 的统计信息。如果未指定本参数，将清除所有聚合 CAR 的统计信息。

【举例】

清除聚合 CAR aggcar-1 的统计信息。

```
<Sysname> reset qos car name aggcar-1
```

6 端口队列统计

6.1 端口队列统计配置命令

6.1.1 display qos queue-statistics

display qos queue-statistics 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：指定端口类型和端口编号。如果未指定本参数，将显示所有端口的队列出方向统计信息。

outbound：显示端口队列出方向的统计信息。

【使用指导】

查看端口队列出方向的统计信息前，请先通过 **statistic mode queue** 命令配置设备的报文统计模式为 **queue** 模式。

【举例】

显示端口 FortyGigE1/0/1 出方向的队列统计信息。

```
<Sysname> display qos queue-statistics interface FortyGigE 1/0/1 outbound

Interface: FortyGigE1/0/1
 Direction: outbound
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Queue 0
  Forwarded: 0 packets, 0 bytes
  Dropped: 0 packets, 0 bytes
  Total queue length: 0 packets
  Current queue length: 0 packets, 0% use ratio
 Queue 1
  Forwarded: 0 packets, 0 bytes
  Dropped: 0 packets, 0 bytes
  Total queue length: 0 packets
```

```
 Current queue length: 0 packets, 0% use ratio
Queue 2
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Total queue length: 0 packets
 Current queue length: 0 packets, 0% use ratio
Queue 3
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Total queue length: 0 packets
 Current queue length: 0 packets, 0% use ratio
Queue 4
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Total queue length: 0 packets
 Current queue length: 0 packets, 0% use ratio
Queue 5
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Total queue length: 0 packets
 Current queue length: 0 packets, 0% use ratio
Queue 6
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Total queue length: 0 packets
 Current queue length: 0 packets, 0% use ratio
Queue 7
 Forwarded: 0 packets, 0 bytes
 Dropped: 0 packets, 0 bytes
 Total queue length: 0 packets
 Current queue length: 0 packets, 0% use ratio
```

表6-1 display qos queue-statistics 命令显示信息描述表

字段	描述
Queue	队列编号
Forwarded	当前队列已转发的报文数量，包括报文个数（packets）和字节数（bytes），本版本不支持对当前队列已转发的报文数量的统计功能
Dropped	当前队列已丢弃的报文数量，包括报文个数（packets）和字节数（bytes）
Total queue length	队列长度，以报文个数（packets）为统计单位
Current queue length	当前队列中缓存的报文个数以及所占队列长度的百分比

【相关命令】

- **reset qos queue-statistics**
- **statistics mode queue**

6.1.2 display statistic mode

display statistic mode 命令用来显示设备的报文统计模式。

【命令】

display statistic mode

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示设备的报文统计模式统计。

```
<Sysname> display statistic mode
The packet statistic mode is vsi.
```

【相关命令】

- **statistic mode queue**
- **statistic mode vsi**（VXLAN 命令参考）

6.1.3 reset qos queue-statistics

reset qos queue-statistics 命令用来清除端口队列出方向的统计信息。

【命令】

reset qos queue-statistics interface [*interface-type interface-number*] **outbound**

【视图】

用户视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

interface-type interface-number：指定端口类型和端口编号。如果未指定本参数，将清除所有端口的队列出方向统计信息。

outbound：清除端口队列出方向的统计信息。

【举例】

清除端口 FortyGigE1/0/1 出方向的队列统计信息。

```
<Sysname> reset qos queue-statistics interface FortyGigE 1/0/1 outbound
```

【相关命令】

- **display qos queue-statistics**
- **statistics mode queue**

6.1.4 statistic mode queue

statistic mode queue 命令用来配置报文统计模式为端口队列出方向报文统计模式。

undo statistic mode 命令用来恢复缺省情况。

【命令】

statistic mode queue

undo statistic mode

【缺省情况】

报文统计模式为 VSI 模式。

【视图】

系统视图

【缺省用户角色】

network-admin

【使用指导】

对于端口队列出方向报文，统计信息可通过 **display qos queue-statistics** 命令查看。

【举例】

配置设备的报文统计模式为 **queue** 模式。

```
<Sysname> system-view
[Sysname] statistic mode queue
Do you want to change the packet statistic mode? [Y/N]:y
```

【相关命令】

- **display qos queue-statistics**
- **display statistic mode**
- **statistics mode vsi**（VXLAN 命令参考）

目 录

1 时间段

1.1 时间段配置命令

1.1.1 display time-range

display time-range 命令用来显示时间段的配置和状态信息。

【命令】

display time-range { *time-range-name* | **all** }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

time-range-name：显示指定名称时间段的配置和状态信息。*time-range-name* 表示时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。

all：显示所有时间段的配置和状态信息。

【举例】

显示时间段 t4 的配置和状态信息。

```
<Sysname> display time-range t4
Current time is 17:12:34 11/23/2010 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2011 to 00:00 1/1/2012
 from 00:00 6/1/2011 to 00:00 7/1/2011
```

表1-1 display time-range 命令显示信息描述表

字段	描述
Current time	系统当前的时间
Time-range	时间段的配置信息，包括： • 时间段的名称 • 时间段的状态，包括 Active（生效）和 Inactive（未生效）两种状态 • 时间段的时间范围

1.1.2 time-range

time-range 命令用来创建一个时间段，来描述一个特定的时间范围。

undo time-range 命令用来删除一个时间段。

【命令】

time-range *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-range-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

【缺省情况】

不存在任何时间段。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

time-range-name：指定时间段的名称，为 1～32 个字符的字符串，不区分大小写，必须以英文字母 a～z 或 A～Z 开头。为避免混淆，时间段的名称不允许使用英文单词 all。

start-time **to** *end-time*：指定周期时间段的时间范围。*start-time* 表示起始时间，格式为 hh:mm，取值范围为 00:00～23:59；*end-time* 表示结束时间，格式为 hh:mm，取值范围为 00:00～24:00，且结束时间必须大于起始时间。

days：指定周期时间段在每周的周几生效。本参数可输入多次，但后输入的值不能与此前输入的值完全重叠（譬如输入 **6** 后不允许再输入 **sat**，但允许再输入 **off-day**），系统将取各次输入值的并集作为最终值（譬如依次输入 **1**、**wed** 和 **working-day** 之后，最终生效的时间将为每周的工作日）。本参数可输入的形式如下：

- 数字：取值范围为 0～6，依次表示周日～周六；
- 周几的英文缩写（从周日到周六依次为 **sun**、**mon**、**tue**、**wed**、**thu**、**fri** 和 **sat**）；
- 工作日（**working-day**）：表示从周一到周五；
- 休息日（**off-day**）：表示周六和周日；
- 每日（**daily**）：表示一周七天。

from *time1 date1*：指定绝对时间段的起始时间。*time1* 的格式为 hh:mm，取值范围为 00:00～23:59。*date1* 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月，取值范围为 1～12；DD 表示日，取值范围取决于所输入的月份；YYYY 表示年，取值范围为 1970～2100。若未指定本参数，绝对时间段的起始时间将为系统可表示的最早时间，即 1970 年 1 月 1 日 0 点 0 分。

to *time2 date2*：指定绝对时间段的结束时间。*time2* 的格式为 hh:mm，取值范围为 00:00～24:00。*date2* 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月，取值范围为 1～12；DD 表示日，

取值范围取决于所输入的月份；YYYY 表示年，取值范围为 1970～2100。结束时间必须大于起始时间。若未指定本参数，绝对时间段的结束时间将为系统可表示的最晚时间，即 2100 年 12 月 31 日 24 点 0 分。

【使用指导】

- 使用 **time-range** 命令时，如果指定名称的时间段不存在，则创建一个新的时间段（最多 1024 个）；如果指定名称的时间段已存在，则对旧时间段进行修改，即在其原有内容的基础上叠加新的内容。
- 使用 *start-time* **to** *end-time days* 这组参数所创建的时间段为周期时间段，它将以一周为周期循环生效；使用 **from** *time1 date1* 和 **to** *time2 date2* 这组参数所创建的时间段为绝对时间段，它将在指定时间范围内生效；而同时使用了上述两组参数所创建的时间段，将取周期时间段和绝对时间段的交集作为生效的时间范围，譬如：创建一个时间段，既定义其在每周一的 8 点到 12 点生效，又定义其在 2011 年全年生效，那么其最终将在 2011 年全年内每周一的 8 点到 12 点生效。
- 一个时间段内可包含一或多个周期时间段（最多 32 个）和绝对时间段（最多 12 个），当包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。

【举例】

创建名为 t1 的时间段，其时间范围为每周工作日的 8 点到 18 点。

```
<Sysname> system-view
[Sysname] time-range t1 08:00 to 18:00 working-day
```

创建名为 t2 的时间段，其时间范围为 2011 年全年。

```
<Sysname> system-view
[Sysname] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011
```

创建名为 t3 的时间段，其时间范围为 2011 年全年内每周休息日的 8 点到 12 点。

```
<Sysname> system-view
[Sysname] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2011 to 24:00 12/31/2011
```

创建名为 t4 的时间段，其时间范围为 2011 年 1 月和 6 月内每周一的 10 点到 12 点以及每周三的 14 到 16 点。

```
<Sysname> system-view
[Sysname] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

【相关命令】

- **display time-range**

目 录

1 数据缓冲区

1.1 数据缓冲区配置命令

1.1.1 burst-mode enable

burst-mode enable 命令用来开启 Burst 功能。

undo burst-mode enable 命令用来关闭 Burst 功能。

【命令】

burst-mode enable

undo burst-mode enable

【缺省情况】

Burst 功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

在下列情况下，Burst 功能可以提供更好的报文缓存功能和流量转发性能：

- 广播或者组播报文流量密集，瞬间突发大流量的网络环境中；
- 报文从高速链路进入设备，由低速链路转发出去；或者报文从相同速率的多个接口同时进入设备，由一个相同速率的接口转发出去。

用户可以通过开启 Burst 功能，降低设备在上述特定环境中的报文丢包率，提高对报文的处理能力。

【举例】

开启 Burst 功能。

```
<Sysname> system-view
[Sysname] burst-mode enable
```

1.1.2 buffer usage threshold

buffer usage threshold 命令用来配置接口的数据缓冲区使用门限值。

undo buffer usage threshold 命令用来恢复缺省情况。

【命令】

独立运行模式：

buffer usage threshold slot *slot-number* **ratio** *ratio*

undo buffer usage threshold slot *slot-number*

IRF 模式：

buffer usage threshold chassis *chassis-number* **slot** *slot-number* **ratio** *ratio*

undo buffer usage threshold chassis *chassis-number* **slot** *slot-number*

【缺省情况】

设备上接口的数据缓冲区使用门限值为 100。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

slot *slot-number*：指定单板所在的槽位号。*slot-number* 表示单板所在的槽位号。（独立运行模式）

chassis *chassis-number* **slot** *slot-number*：指定成员设备上的指定单板。*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。（IRF 模式）

ratio *ratio*：以百分比形式配置接口的数据缓冲区使用门限值，*ratio* 的取值为 1～100。

【使用指导】

- 仅 Release 1138P01 及以上版本支持此命令。
- 只有将设备的报文统计模式配置为队列模式后（执行 **statistic mode queue** 命令），本命令的配置才能生效。关于报文统计模式的介绍，请参见“ACL 和 QoS 命令参考”中的“QoS 命令”。
- 配置接口的数据缓冲区使用门限后，设备会自动记录接口对缓冲区的使用情况。当接口上某一队列中需要处理的报文增多，造成该接口对数据缓冲区的使用比率超过设定的门限值时，系统会为该队列增加一次超量使用缓冲区的计数。
- 通过 **display buffer usage interface** 命令，可以查看接口的数据缓冲区使用统计信息。

【举例】

配置 2 号槽位单板上所有接口的数据缓冲区使用门限值为 50%。（独立运行模式）

```
<Sysname> system-view
[Sysname] buffer usage threshold slot 2 ratio 50
```

配置 2 号成员设备的 2 号槽位单板上所有接口的数据缓冲区使用门限值为 50%。（IRF 模式）

```
<Sysname> system-view
[Sysname] buffer usage threshold chassis 2 slot 2 ratio 50
```

【相关命令】

- **display buffer usage interface**

1.1.3 display buffer usage interface

display buffer usage interface 命令用来显示接口的数据缓冲区使用统计信息。

【命令】

display buffer usage 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，*interface-type* 为接口类型，*interface-number* 为接口编号。未指定 *interface-type* 参数时，显示设备上所有以太网接口的数据缓冲区使用统计信息；已指定 *interface-type* 但未指定 *interface-number* 时，显示设备上所有指定类型的以太网接口的数据缓冲区使用统计信息。

【使用指导】

仅 Release 1138P01 及以上版本支持此命令。

【举例】

#显示接口 Ten-GigabitEthernet1/0/1 的数据缓冲区使用统计信息。

```
<Sysname>display buffer usage interface ten-gigabitethernet 2/0/1
Interface              QueueID Total       Used        Threshold(%) Violations
--------------------------------------------------------------------------------
XGE2/0/1               0       9418032     0           30           0
                       1       9418032     0           30           0
                       2       9418032     0           30           0
                       3       9418032     0           30           0
                       4       9418032     0           30           0
                       5       9418032     0           30           0
                       6       9418032     0           30           0
                       7       9418032     0           30           0
```

display buffer usage interface 命令显示信息描述表

字段	描述
Interface	接口名称
QueueID	队列编号
Total	队列可用的数据缓冲区大小，单位为Byte
Used	队列已使用的数据缓冲区大小，单位为Byte
Threshold(%)	队列的数据缓冲区使用门限值，该值与队列所在接口的缓冲区使用门限值保持一致
Violations	队列超量使用缓冲区的计数，表示队列使用缓冲区超过设定门限值的次数 该字段仅在设备重启时，才会清零后重新计数