H3C MSR 系列路由器

ACL 和 QoS 命令参考(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W204-20190110
产品版本：MSR-CMW710-R0615

前 言

本命令参考主要介绍配置 ACL 和 QoS 功能时涉及的各种命令。

前言部分包含如下内容：

- 读者对象
- 本书约定
- 资料意见反馈

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终结单元。
	该图标及其相关描述文字代表无线终结者。
	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. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

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

1.1 ACL配置命令 ····· 1-1

1.1.1 accelerate ····· 1-1

1.1.2 acl ····· 1-2

1.1.3 acl copy ····· 1-4

1.1.4 acl logging interval ····· 1-5

1.1.5 acl trap interval ····· 1-6

1.1.6 description ····· 1-7

1.1.7 display acl ····· 1-7

1.1.8 display acl accelerate ····· 1-9

1.1.9 display packet-filter ····· 1-10

1.1.10 display packet-filter statistics ····· 1-14

1.1.11 display packet-filter statistics sum ····· 1-18

1.1.12 display packet-filter verbose ····· 1-19

1.1.13 packet-filter (Interface view) ····· 1-23

1.1.14 packet-filter (Zone-pair security view) ····· 1-24

1.1.15 packet-filter default deny ····· 1-25

1.1.16 reset acl counter ····· 1-26

1.1.17 reset packet-filter statistics ····· 1-27

1.1.18 rule (MAC ACL view) ····· 1-29

1.1.19 rule (IPv4 advanced ACL view) ····· 1-31

1.1.20 rule (IPv4 basic ACL view) ····· 1-37

1.1.21 rule (IPv6 advanced ACL view) ····· 1-40

1.1.22 rule (IPv6 basic ACL view) ····· 1-46

1.1.23 rule comment ····· 1-49

1.1.24 step ····· 1-50

1 ACL

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

1.1 ACL配置命令

1.1.1 accelerate

accelerate 命令用来开启 ACL 加速功能。

undo accelerate 命令用来关闭 ACL 加速功能。

【命令】

accelerate

undo accelerate

【缺省情况】

ACL 加速功能处于关闭状态。

【视图】

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

【缺省用户角色】

network-admin

【使用指导】

资源不足会导致 ACL 加速失败，但是匹配依然生效。规则有变化或者重新加速，在资源足够的前提下加速会生效。

ACL 加速成功后，再去修改或添加新的规则，可能由于资源不足，会导致新的规则加速失败，规则匹配不生效，但是不影响之前加速成功的规则。

【举例】

开启 ACL 2000 的加速功能。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] accelerate
```

【相关命令】

- **display acl accelerate**

1.1.2 acl

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

undo acl 命令用来删除指定或全部 ACL。

【命令】

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

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

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

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

【缺省情况】

不存在 ACL。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。

basic：指定创建基本 ACL。

advanced：指定创建高级 ACL。

mac：指定创建二层 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

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：指定类型中全部 ACL。

【使用指导】

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。

若未指定 **ipv6** 或 **mac** 关键字，则表示 IPv4 ACL。

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

【举例】

创建一个编号为 2000 的 IPv4 基本 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000]
```

创建一个 IPv4 基本 ACL，指定其名称为 flow，并进入其视图。

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

创建一个编号为 3000 的 IPv4 高级 ACL，并进入其视图。

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

创建一个编号为 2000 的 IPv6 基本 ACL，并进入其视图。

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

创建一个 IPv6 基本 ACL，其名称为 flow，并进入其视图。

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

创建一个 IPv6 高级 ACL，其名称为 abc，并进入其视图。

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

创建一个编号为 4000 的二层 ACL，并进入其视图。

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

创建一个二层 ACL，其名称为 flow，并进入其视图。

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

【相关命令】

- **display acl**

1.1.3 acl copy

acl copy 命令用来复制并生成一个新的 ACL。

【命令】

acl [**ipv6** | **mac**] **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

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

name *source-acl-name*：指定源 ACL 的名称，该 ACL 必须存在。*source-acl-name* 为 1～63 个字符的字符串，不区分大小写。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

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

【使用指导】

目的 ACL 的类型要与源 ACL 的类型相同。

除了 ACL 的编号或名称不同外，新生成的 ACL（即目的 ACL）的匹配顺序、规则匹配统计功能的开启情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 ACL 的相同。

若未指定 **ipv6** 或 **mac** 关键字，则表示 IPv4 ACL。

【举例】

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

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

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

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

1.1.4 acl logging interval

acl logging interval 命令用来配置报文过滤日志信息的生成与发送周期，同时开启报文的首包上送功能。

undo acl logging interval 命令用来恢复缺省情况。

【命令】

acl logging interval *interval*

undo acl logging interval

【缺省情况】

报文过滤日志信息的生成与发送周期为 0 分钟，即不记录报文过滤的日志。报文首包上送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：报文过滤日志信息的生成与发送周期，取值范围为 0～1440，且必须为 5 的整数倍，0 表示不进行记录，单位为分钟。

【使用指导】

系统只支持对应用 IPv4 基本 ACL、IPv4 高级 ACL、IPv6 基本 ACL 或 IPv6 高级 ACL 进行报文过滤的报文过滤日志信息进行记录，且在上述 ACL 中配置规则时必须指定 **logging** 关键字。

报文过滤日志的生成与发送周期起始于报文过滤中 ACL 匹配数据流的第一个数据包，报文过滤日志包括周期内被匹配的报文数量以及所使用的 ACL 规则。在一个周期内：

- 对于规则匹配数据流的第一个数据包，设备会立即生成报文过滤日志并发送到信息中心；
- 对于规则匹配数据流的其他数据包，设备将在周期结束后生成报文过滤日志并发送到信息中心。

有关信息中心的详细介绍请参见“网络管理和监控配置指导”中的“信息中心”。

【举例】

配置 IPv4 报文过滤日志的生成与发送周期为 10 分钟。

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

【相关命令】

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

1.1.5 acl trap interval

acl trap interval 命令用来配置报文过滤告警信息的生成与发送周期，同时开启报文的首包上送功能。

undo acl trap interval 命令用来恢复缺省情况。

【命令】

acl trap interval *interval*

undo acl trap interval

【缺省情况】

报文过滤告警信息的生成与发送周期为 0 分钟，即不记录报文过滤的告警信息。报文首包上送功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

interval：报文过滤告警信息的生成与发送周期，取值范围为 0～1440，且必须为 5 的整数倍，0 表示不进行记录，单位为分钟。

【使用指导】

系统只支持对应用 IPv4 基本 ACL、IPv4 高级 ACL、IPv6 基本 ACL 或 IPv6 高级 ACL 进行报文过滤的报文过滤告警信息进行记录，且在上述 ACL 中配置规则时必须指定 **logging** 关键字。

报文过滤告警信息的生成与发送周期起始于报文过滤中 ACL 匹配数据流的第一个数据包，报文过滤告警信息包括周期内被匹配的报文数量以及所使用的 ACL 规则。在一个周期内：

- 对于规则匹配数据流的第一个数据包，设备会立即生成报文过滤告警信息并发送到 SNMP 模块；
- 对于规则匹配数据流的其他数据包，设备将在周期结束后生成报文过滤告警信息并发送 SNMP 模块。

有关 SNMP 的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

【举例】

配置 IPv4 报文过滤告警信息的生成与发送周期为 10 分钟。

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

【相关命令】

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

1.1.6 description

description 命令用来配置 ACL 的描述信息。

undo description 命令用来删除 ACL 的描述信息。

【命令】

description *text*

undo description

【缺省情况】

ACL 没有任何描述信息。

【视图】

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

【缺省用户角色】

network-admin

【参数】

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

【举例】

为 IPv4 基本 ACL 2000 配置描述信息。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.
```

【相关命令】

- **display acl**

1.1.7 display acl

display acl 命令用来显示 ACL 的配置和运行情况。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

all：显示指定类型中全部 ACL 的配置和运行情况。

name *acl-name*：显示指定名称的 ACL 的配置和运行情况。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

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

若未指定 **ipv6** 或 **mac** 关键字，则表示 IPv4 ACL。

【举例】

显示所有 IPv4 ACL 的配置和运行情况。

```
<Sysname> display acl all
Basic IPv4 ACL 2001, 2 rules, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5
ACL accelerated
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used on GigabitEthernet 1/0/1.
 rule 10 permit source object-group permit (5 times matched)
Advanced IPv4 ACL 3001, 1 rule,
ACL's step is 5
 rule 0 permit ip source 1.1.1.0 0.0.0.255 destination 3.3.3.0 0.0.0.255
```

表1-1 display acl 命令显示信息描述表

字段	描述
Basic IPv4 ACL 2001	该ACL的类型和编号，ACL的类型包括： • Basic IPv4 ACL：表示 IPv4 基本 ACL • Advanced IPv4 ACL：表示 IPv4 高级 ACL

字段	描述
	• Basic IPv6 ACL：表示 IPv6 基本 ACL • Advanced IPv6 ACL：表示 IPv6 高级 ACL • MAC ACL：表示二层 ACL
2 rules	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
ACL accelerated	该ACL开启了加速功能
rule 5 permit source 1.1.1.1 0	规则5的具体内容，源地址为具体地址
rule 10 permit source object-group permit	规则10的具体内容，源地址为对象组
5 times matched	该规则匹配的次数为5（仅统计软件ACL的匹配次数，当匹配次数为0时不显示本字段）
rule 5 comment This rule is used on GigabitEthernet 1/0/1.	规则5的描述信息

1.1.8 display acl accelerate

display acl accelerate 命令用来显示 ACL 的加速状态。

【命令】

集中式设备－独立运行模式：

display acl accelerate { **summary** [**ipv6** | **mac**] | **verbose** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } }

分布式设备－独立运行模式/集中式设备－IRF 模式：

display acl accelerate { **summary** [**ipv6** | **mac**] | **verbose** [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* } **slot** *slot-number* }

分布式设备－IRF 模式：

display acl accelerate { **summary** [**ipv6** | **mac**] | **verbose** [**ipv6** | **mac**] { *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

【参数】

summary：显示 ACL 加速的概要信息。

verbose：显示 ACL 加速的详细信息。

ipv6：显示 IPv6 ACL 的加速状态。

mac：显示二层 ACL 的加速状态。

acl-number：显示指定编号的 ACL 的加速状态。*acl-number* 表示 ACL 的编号，取值范围及其代表的 ACL 类型如下：

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

name *acl-name*：显示指定名称的 ACL 的加速状态。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

slot *slot-number*：显示指定单板的 ACL 加速信息，该单板必须为加速芯片所在单板，*slot-number* 表示单板所在的槽位号。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备的 ACL 加速信息，该设备必须为加速芯片所在成员设备，*slot-number* 表示设备在 IRF 中的成员编号。（集中式设备－IRF 模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的 ACL 加速信息，该单板必须为加速芯片所在单板，*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。（分布式设备－IRF 模式）

【使用指导】

若未指定 **ipv6** 或 **mac** 关键字，则表示 IPv4 ACL。

【举例】

显示加速概要信息。

```
<Sysname> display acl accelerate summary
Basic IPv4 ACL 2000
```

显示加速详细信息。

```
<Sysname> display acl accelerate verbose 2000
Basic IPv4 ACL 2000.
 rule 0 permit
 rule 1 deny
```

表1-2 display acl accelerate verbose 命令显示信息描述表

字段	描述
failed	表示此规则加速失败，匹配不生效

1.1.9 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】

集中式设备－独立运行模式：

display packet-filter { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] }

分布式设备－独立运行模式/集中式设备－IRF 模式：

display packet-filter { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] } [**slot** *slot-number*]

分布式设备－IRF 模式：

display packet-filter { **interface** [*interface-type interface-number*] [**inbound** | **outbound**] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] } [**chassis** *chassis-number* **slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface [*interface-type interface-number*]：显示指定接口上 ACL 在报文过滤中的应用情况。*interface-type interface-number* 表示接口类型和接口编号。若未指定接口类型和接口编号，将显示除 VA 接口外所有接口上 ACL 在报文过滤中的应用情况。有关 VA 接口的详细介绍，请参见“二层技术-广域网接入配置指导”中的“PPPoE”。

zone-pair security [**source** *source-zone-name* **destination** *destination-zone-name*]：显示指定安全域间实例上 ACL 在报文过滤中的应用情况。*source-zone-name*：表示安全域间实例源安全域的名称，为 1～31 个字符的字符串，不区分大小写。*destination-zone-name*：表示安全域间实例目的安全域的名称，为 1～31 个字符的字符串，不区分大小写。

设备各款型对于本参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK支持 MSR810-LMS/810-LUS不支持
MSR 2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持

型号	参数	描述
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

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。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备上 ACL 在报文过滤中的应用情况，*slot-number* 表示设备在 IRF 中的成员编号。若未指定本参数，将显示主用设备上 ACL 在报文过滤中的应用情况。（集中式设备－IRF 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。（分布式设备－IRF 模式）

【使用指导】

显示安全域间实例上的应用情况时不区分方向，其他情况，若未指定 **inbound** 和 **outbound** 关键字，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 GigabitEthernet1/0/1 入方向上 ACL 在报文过滤中的应用情况。

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

显示安全域间实例源域 office 到目的域 library 上 ACL 在报文过滤中的应用情况。

```
<Sysname> display packet-filter zone-pair security source office destination library
Zone-pair: source office destination library
  IPv4 ACL 2001
  IPv4 ACL 2002
```

表1-3 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
Zone-pair	ACL在指定安全域间实例上的应用情况
Inbound policy	ACL在入方向上的应用情况
Outbound policy	ACL在出方向上的应用情况
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv6 ACL 2002 (Failed)	IPv6基本ACL 2002应用失败
IPv4 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
IPv6 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
MAC default action	报文过滤的缺省动作，包括：

字段	描述
	• Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit

1.1.10 display packet-filter statistics

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

【命令】

display packet-filter statistics { **interface** *interface-type interface-number* { **inbound** | **outbound** } [**default** | [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } [**brief**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

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

zone-pair security source *source-zone-name* **destination** *destination-zone-name*：显示指定安全域间实例上的统计信息。*source-zone-name*：表示安全域间实例源安全域的名称，为 1～31 个字符的字符串，不区分大小写。*destination-zone-name*：表示安全域间实例目的安全域的名称，为 1～31 个字符的字符串，不区分大小写。

设备各款型对于本参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK支持 MSR810-LMS/810-LUS不支持
MSR 2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持

型号	参数	描述
MSR3600-28-SI/3600-51-SI		支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

inbound：显示入方向上的统计信息。

outbound：显示出方向上的统计信息。

default：显示报文过滤缺省动作的统计信息。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

name *acl-name*：显示指定名称 ACL 在报文过滤中应用的统计信息。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

brief：显示简要统计信息。

【使用指导】

如果未指定 **default**、*acl-number*、**name** *acl-name* 和 ACL 类型（**ipv6**、**mac**）参数，将显示全部 ACL 在报文过滤中应用的统计信息。

若未指定 **ipv6** 或 **mac** 参数，则表示 IPv4 ACL。

显示安全域间实例统计信息时不区分方向。

【举例】

显示接口 GigabitEthernet1/0/1 入方向上全部 ACL 在报文过滤中应用的统计信息以及报文过滤缺省动作的统计信息。

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

  IPv6 ACL 2000

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

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

  IPv6 default action: Deny
   From 2011-06-04 10:25:41 to 2011-06-04 10:35:57
   Totally 0 packets

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

显示安全域间实例源域 office 到目的域 library 上 IPv4 高级 ACL 3000 在报文过滤中应用的统计信息。

```
<Sysname> display packet-filter statistics zone-pair security source office destination
library 3001
Zone-pair: source office destination library
IPv4 ACL 3001
   rule 0 permit source 2.2.2.2 0
   rule 5 permit source 1.1.1.1 0 counting (2 packets)
   rule 10 permit vpn-instance test (Failed)
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

表1-4 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
Zone-pair	在指定安全域间实例上应用的统计信息
Inbound policy	在入方向上应用的统计信息
Outbound policy	在出方向上应用的统计信息
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv4 ACL 2002 (Failed)	IPv4基本ACL 2002应用失败
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	该统计的起始和终止时间
2 packets	该规则匹配了2个包（当匹配的包个数为0时不显示本字段）
No resource	该规则对应的统计资源不足
rule 5 permit source 1.1.1.1 0 (Failed)	规则5应用失败
Totally 2 packets permitted, 0 packets denied	该ACL允许和拒绝符合条件报文的个数
Totally 100% permitted, 0% denied	该ACL允许符合条件报文的通过率和拒绝符合条件报文的丢弃率
IPv4 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
IPv6 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
MAC default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit

字段	描述
	• Permit：报文过滤缺省动作为 Permit
Totally 7 packets	报文过滤缺省动作的执行次数

【相关命令】

- **reset packet-filter statistics**

1.1.11 display packet-filter statistics sum

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

inbound：显示入方向上 ACL 在报文过滤中应用的累加统计信息。

outbound：显示出方向上 ACL 在报文过滤中应用的累加统计信息。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

name *acl-name*：显示指定名称 ACL 在报文过滤中应用的累加统计信息。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

brief：显示 ACL 在报文过滤中应用的简要累加统计信息。

【使用指导】

若未指定 **ipv6** 或 **mac** 关键字，则表示 IPv4 ACL。

【举例】

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

```
<Sysname> display packet-filter statistics sum inbound 2001
Sum:
 Inbound policy:
```

```
  IPv4 ACL 2001
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

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

```
<Sysname> display packet-filter statistics sum inbound 2000 brief
Sum:
 Inbound policy:
  IPv4 ACL 2000
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

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

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

【相关命令】

- **reset packet-filter statistics**

1.1.12 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】

集中式设备－独立运行模式：

display packet-filter verbose { **interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] }

分布式设备－独立运行模式/集中式设备－IRF 模式：

display packet-filter verbose { **interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *acl-number* | **name** *acl-name* }] } [**slot** *slot-number*]

分布式设备－IRF 模式：

display packet-filter verbose { **interface** *interface-type interface-number* { **inbound** | **outbound** } [[**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security source** *source-zone-name* **destination** *destination-zone-name* [[**ipv6**] { *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

【参数】

interface *interface-type interface-number*：显示指定接口上 ACL 在报文过滤中的详细应用情况。*interface-type interface-number* 表示接口类型和接口编号。当接口类型为以太网接口时，不需要指定 **chassis** 和 **slot** 关键字。

zone-pair security source *source-zone-name* **destination** *destination-zone-name*：显示指定安全域间实例上 ACL 在报文过滤中的详细应用情况。*source-zone-name*：表示安全域间实例源安全域的名称，为 1～31 个字符的字符串，不区分大小写。*destination-zone-name*：表示安全域间实例目的安全域的名称，为 1～31 个字符的字符串，不区分大小写。

设备各款型对于本参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK支持 MSR810-LMS/810-LUS不支持
MSR 2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**zone-pair security** [**source**	支持

型号	命令	描述
MSR830-4LM-WiNet	*source-zone-name* **destination** *destination-zone-name*]	不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

inbound：显示入方向上 ACL 在报文过滤中的详细应用情况。

outbound：显示出方向上 ACL 在报文过滤中的详细应用情况。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

name *acl-name*：显示指定名称 ACL 在报文过滤中的详细应用情况。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

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

slot *slot-number*：显示指定成员设备上 ACL 在报文过滤中的详细应用情况，*slot-number* 表示设备在 IRF 中的成员编号。若未指定本参数，将显示主用设备上 ACL 在报文过滤中的详细应用情况。（集中式设备－IRF 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。（分布式设备－IRF 模式）

【使用指导】

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

若未指定 **ipv6** 或 **mac** 参数，则表示 IPv4 ACL。

显示安全域间实例详细应用情况时不区分方向。

【举例】

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

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

  IPv4 ACL 2002 (Failed)

  IPv6 ACL 2000
   rule 0 permit

  MAC ACL 4000


  IPv4 default action: Deny

  IPv6 default action: Deny

  MAC default action: Deny
```

#显示安全域间实例源域 office 到目的域 library 上全部 ACL 在报文过滤中的详细应用情况。

```
<Sysname> display packet-filter verbose zone-pair security source office destination library
Zone-pair: source office destination library
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0
   rule 10 permit vpn-instance test
```

表1-6 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
Zone-pair	ACL在指定安全域间实例上的详细应用情况
Inbound policy	ACL在入方向上的详细应用情况
Outbound policy	ACL在出方向上的详细应用情况
IPv4 ACL 2001	IPv4基本ACL 2001应用成功
IPv4 ACL 2002 (Failed)	IPv4基本ACL 2002应用失败
rule 5 permit source 1.1.1.10 (Failed)	规则5应用失败
IPv4 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
IPv6 default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit
MAC default action	报文过滤的缺省动作，包括： • Deny：报文过滤缺省动作为 Deny 应用成功 • Deny (Failed)：报文过滤缺省动作为 Deny 应用失败，实际动作仍为 Permit • Permit：报文过滤缺省动作为 Permit

1.1.13 packet-filter (Interface view)


说明

如果接口工作在二层模式，则不支持本命令。

packet-filter 命令用来在接口上应用 ACL 进行报文过滤。

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

【命令】

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

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

【缺省情况】

接口不对报文进行过滤。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

name *acl-name*：指定 ACL 的名称。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

inbound：对收到的报文进行过滤。

outbound：对发出的报文进行过滤。

【使用指导】

若未指定 **ipv6** 或 **mac** 关键字，则表示 IPv4 ACL。

此功能在聚合成员端口上不生效。

【举例】

应用 IPv4 基本 ACL 2001 对接口 GigabitEthernet1/0/1 收到的报文进行过滤

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter 2001 inbound
```

【相关命令】

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

1.1.14 packet-filter (Zone-pair security view)

packet-filter 命令用来在安全域间实例上应用 ACL 进行报文过滤。

undo packet-filter 命令用来取消在安全域间实例上应用 ACL 进行报文过滤。

【命令】

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

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

【缺省情况】

在安全域间实例上没有应用 ACL 进行报文过滤。

【视图】

安全域间实例视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。若未指定本关键字，则表示 IPv4 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。

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。

【举例】

应用 IPv4 基本 ACL 2002 对源安全域 office 到目的安全域 library 的安全域间实例收到的报文进行过滤。

```
<Sysname> system-view
[Sysname] zone-pair security source office destination library
[Sysname-zone-pair-security-office-library] packet-filter 2002
```

【相关命令】

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

1.1.15 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

【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**

1.1.16 reset acl counter

reset acl counter 命令用来清除 ACL 的统计信息。

【命令】

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。
- 4000～4999：表示二层 ACL。

all：清除指定类型中全部 ACL 的统计信息。

name *acl-name*：清除指定名称 ACL 的统计信息。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

若未指定 **ipv6** 或 **mac** 关键字，则表示 IPv4 ACL。

【举例】

清除 IPv4 基本 ACL 2001 的统计信息。

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

【相关命令】

- **display acl**

1.1.17 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。

【命令】

reset packet-filter statistics { **interface** [*interface-type interface-number*] { **inbound** | **outbound** } [**default** | [**ipv6** | **mac**] { *acl-number* | **name** *acl-name* }] | **zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*] [[**ipv6**] { *acl-number* | **name** *acl-name* }] }

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

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

zone-pair security [**source** *source-zone-name* **destination** *destination-zone-name*]：清除指定接口上的统计信息。*source-zone-name*：表示安全域间实例源安全域的名称，为 1～31 个字符的字符串，不区分大小写。*destination-zone-name*：表示安全域间实例目的安全域的名称，为 1～31 个字符的字符串，不区分大小写。

设备各款型对于本参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK支持 MSR810-LMS/810-LUS不支持
MSR 2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持

型号	参数	描述
MSR 3610/3620/3620-DP/3640/3660		支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**zone-pair security** [**source** *source-zone-name* **destination** *destination-zone-name*]	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

inbound：清除入方向上的统计信息。

outbound：清除出方向上的统计信息。

default：清除缺省动作在报文过滤中应用的统计信息。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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

- 2000～2999：表示基本 ACL。
- 3000～3999：表示高级 ACL。

- 4000～4999：表示二层 ACL。

name *acl-name*：清除指定名称 ACL 在报文过滤中应用的统计信息。*acl-name* 表示 ACL 的名称，为 1～63 个字符的字符串，不区分大小写。

【使用指导】

如果未指定 **default**、*acl-number*、**name** *acl-name* 和 ACL 类型（**ipv6**、**mac**）关键字，将清除全部 ACL 在报文过滤中应用的统计信息以及报文过滤缺省动作的统计信息。

如果未指定 **ipv6** 或 **mac** 参数，则表示 IPv4 ACL。

清除安全域间实例统计信息时不区分方向且不支持 **default**。

【举例】

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

```
<Sysname> reset packet-filter statistics interface gigabitethernet 1/0/1 inbound 2001
```

【相关命令】

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

1.1.18 rule (MAC ACL view)

rule 命令用来为二层 ACL 创建一条规则。

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

【命令】

rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

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

undo rule [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **counting** | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *

【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

【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 *dot1p*：指定 802.1p 优先级。*dot1p* 表示 802.1p 优先级，可输入的形式如下：

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

counting：表示开启规则匹配统计功能，缺省为关闭。

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

lsap *lsap-type lsap-type-mask*：指定 LLC 封装中的 DSAP 字段和 SSAP 字段。*lsap-type* 表示数据帧的封装格式，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。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。

counting 关键字用于开启本规则的匹配统计功能。

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

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule** [*rule-id*] { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

【举例】

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

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

【相关命令】

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

1.1.19 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** { **object-group** *address-group-name* | *dest-address dest-wildcard* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | { **dscp** *dscp1* [**to** *dscp2*] | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

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

undo 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** { **object-group** *address-group-name* | *dest-address dest-wildcard* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | { **dscp** *dscp1* [**to** *dscp2*] | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **source** { **object-group** *address-group-name* | *source-address source-wildcard* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

【缺省情况】

IPv4 高级 ACL 内不存在任何规则。

【视图】

IPv4 高级 ACL 视图

【缺省用户角色】

network-admin

【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 { **object-group** *address-group-name* | *source-address* *source-wildcard* | **any** }	源地址信息	指定ACL规则的源地址信息	*address-group-name*：源地址对象组的名称 *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 { **object-group** *address-group-name* | *dest-address* *dest-wildcard* | **any** }	目的地址信息	指定ACL规则的目的地址信息	*address-group-name*：目的地址对象组的名称 *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	开启规则匹配统计功能，缺省为关闭	本关键字用于开启本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；用字符表示时，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；用字符表示时，可以选取**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）、**min-monetary-cost**（1）、**normal**（0）
dscp *dscp1* [**to** *dscp2*]	报文优先级	DSCP优先级	*dscp*用数字表示时，取值范围为0～63，用字符表示时，可以选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）、**ef**（46）。**to**用来表示DSCP优先级的范围，dscp2的值要大于等于dscp1的值
fragment	分片信息	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定该关键字，则表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效
logging	日志操作	对符合条件的报文可记录日志信息	该功能需要使用该ACL的模块支持日志记录功能，例如报文过滤

参数	类别	作用	说明
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。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL和QoS配置指导”中的“时间段”
vpn-instance *vpn-instance-name*	VPN实例	对指定VPN实例中的报文有效	*vpn-instance-name*：MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写 若未指定本参数，表示该规则仅对非VPN报文有效

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 { **object-group** *port-group-name* | *operator port1* [*port2*] }	源端口	定义TCP/UDP报文的源端口信息	*port-group-name*：端口对象组的名称 *operator*为操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有操作符**range**需要两个端口号做操作数，其它的只需要一个端口号做操作数 *port1*、*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用文字表示时，TCP端口号可以选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**dns**（53）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）、**www**（80）；UDP端口号可以选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）、**xdmcp**（177）
destination-port { **object-group** *port-group-name* | *operator port1* [*port2*] }	目的端口	定义TCP/UDP报文的目的端口信息	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 对于一条规则中各标志位的配置组合为“或”的关系。譬如：当配置为ack 0 psh 1时，将匹配不携带ACK或携带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。对于路由器，表示匹配携带ACK或RST标志位的TCP连接报文

设备各款型对于本参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**object-group**	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK支持 MSR810-LMS/810-LUS不支持
MSR 2600-6-X1/2600-10-X1		• MSR2600-6-X1：不支持 • MSR2600-10-X1：支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**object-group**	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**object-group**	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持

型号	特性	描述
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		支持

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

表1-9 ICMP 特有的规则信息参数

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

表1-10 ICMP 消息名称与消息类型和消息码的对应关系

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

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

创建的规则若与动态规则的内容完全相同，则会覆盖已有动态规则。

创建或修改的规则不能与手工配置的规则的内容完全相同，否则将提示出错，并导致该操作失败。

新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

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

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule** [*rule-id*] { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

【举例】

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

```
<Sysname> system-view
[Sysname] acl advanced 3000
[Sysname-acl-ipv4-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq 80
```

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

```
<Sysname> system-view
[Sysname] acl advanced 3001
[Sysname-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] rule permit ip
```

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

```
<Sysname> system-view
[Sysname] acl advanced 3002
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp source-port eq ftp-data
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp
[Sysname-acl-ipv4-adv-3002] rule permit tcp destination-port eq ftp-data
```

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

```
<Sysname> system-view
[Sysname] acl advanced 3003
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv4-adv-3003] rule permit udp destination-port eq snmptrap
```

【相关命令】

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

1.1.20 rule (IPv4 basic ACL view)

rule 命令用来为 IPv4 基本 ACL 创建一条规则。

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

【命令】

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

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

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

【缺省情况】

IPv4 基本 ACL 内不存在任何规则。

【视图】

IPv4 基本 ACL 视图

【缺省用户角色】

network-admin

【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：表示开启规则匹配统计功能，缺省为关闭。

fragment：表示仅对非首片分片报文有效，而对非分片报文和首片分片报文无效。若未指定本关键字，表示该规则对非分片报文和分片报文均有效。

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

source { **object-group** *address-group-name* | *source-address source-wildcard* | **any** }：指定规则的源 IP 地址信息。*address-group-name* 表示源 IP 地址对象组的名称，*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。

设备各款型对于本参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**object-group**	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK支持 MSR810-LMS/810-LUS不支持
MSR 2600-6-X1/2600-10-X1		• MSR2600-6-X1：不支持 • MSR2600-10-X1：支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**object-group**	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**object-group**	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持

型号	特性	描述
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		支持

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。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL 和 QoS 配置指导”中的“时间段”。

vpn-instance *vpn-instance-name*：表示对指定 VPN 实例中的报文有效。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定本参数，表示该规则仅对非 VPN 报文有效。

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

Counting 关键字用于开启本规则的匹配统计功能。

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

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule** [*rule-id*] { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

【举例】

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

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule permit source 10.0.0.0 0.255.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 172.17.0.0 0.0.255.255
[Sysname-acl-ipv4-basic-2000] rule permit source 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2000] rule deny source any
```

【相关命令】

- **acl**
- **acl logging interval**
- **display acl**

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

1.1.21 rule (IPv6 advanced ACL view)

rule 命令用来为 IPv6 高级 ACL 创建一条规则。

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

【命令】

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

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

undo 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** { **object-group** *address-group-name* | *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** } | **destination-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **dscp** *dscp* | **flow-label** *flow-label-value* | **fragment** | **icmp6-type** { *icmp6-type icmp6-code* | *icmp6-message* } | **logging** | **routing** [**type** *routing-type*] | **hop-by-hop** [**type** *hop-type*] | **source** { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** } | **source-port** { **object-group** *port-group-name* | *operator port1* [*port2*] } | **time-range** *time-range-name* | **vpn-instance** *vpn-instance-name*] *

【缺省情况】

IPv6 高级 ACL 内不存在任何规则。

【视图】

IPv6 高级 ACL 视图

【缺省用户角色】

network-admin

【参数】

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

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

protocol：表示 IPv6 承载的协议类型，可输入的形式如下：

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

*protocol*之后可配置如 表 1-11 所示的规则信息参数。

表1-11 规则信息参数

参数	类别	作用	说明
source { **object-group** *address-group-name* | *source-address source-prefix* | *source-address/source-prefix* | **any** }	源IPv6地址	指定ACL规则的源IPv6地址信息	*address-group-name*：源地址对象组的名称 *source-address*：源IPv6地址 *source-prefix*：源IPv6地址的前缀长度，取值范围1～128 **any**：任意源IPv6地址
destination { **object-group** address-group-name | *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** }	目的IPv6地址	指定ACL规则的目的IPv6地址信息	*address-group-name*：目的地址对象组的名称 *dest-address*：目的IPv6地址 *dest-prefix*：目的IPv6地址的前缀长度，取值范围1～128 **any**：任意目的IPv6地址
counting	统计	开启规则匹配统计功能，缺省为关闭	本参数用于开启本规则的匹配统计功能
dscp *dscp*	报文优先级	DSCP优先级	*dscp*：用数字表示时，取值范围为0～63；用名称表示时，可选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）或**ef**（46）
flow-label *flow-label-value*	流标签字段	指定IPv6基本报文头中流标签字段的值	*flow-label-value*：流标签字段的值，取值范围为0～1048575
fragment	报文分片	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定本参数，表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效
logging	日志操作	对符合条件的报文可记录日志信息	该功能需要使用该ACL的模块支持日志记录功能，例如报文过滤
routing [**type** *routing-type*]	路由头	指定路由头的类型	*routing-type*：路由头类型的值，取值范围为0～255 若指定了**type** *routing-type*参数，表示仅对指定类型的路由头有效；否则，表示对IPv6所有类型的路由头都有效

参数	类别	作用	说明
hop-by-hop [**type** *hop-type*]	逐跳头	指定逐跳头的类型	*hop-type*：逐跳头类型的值，取值范围为0～255 若指定了**type** *hop-type*参数，表示仅对指定类型的逐跳头有效；否则，表示对IPv6所有类型的逐跳头都有效
time-range *time-range-name*	时间段	指定本规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写。若该时间段尚未配置，该规则仍会成功创建但系统将给出提示信息，并在该时间段的配置完成后此规则才会生效。有关时间段的详细介绍和具体配置过程，请参见“ACL和QoS配置指导”中的“时间段”
vpn-instance *vpn-instance-name*	VPN实例	对指定VPN实例中的报文有效	*vpn-instance-name*：MPLS L3VPN的VPN实例名称，为1～31个字符的字符串，区分大小写 若未指定本参数，表示该规则仅对非VPN报文有效

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

表1-12 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port { **object-group** *port-group-name* | *operator port1* [*port2*] }	源端口	定义TCP/UDP报文的源端口信息	*port-group-name*：端口对象组的名称 *operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数 *port1*/*port2*：TCP或UDP的端口号，用数字表示时，取值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**dns**（53）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）或**www**（80）；UDP端口号可选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）或**xdmcp**（177）
destination-port { **object-group** *port-group-name* | *operator port1* [*port2*] }	目的端口	定义TCP/UDP报文的目的端口信息	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn**	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）	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）

参数	类别	作用	说明
syn-value | **urg** *urg-value* } *		的TCP报文的处理规则	对于一条规则中各标志位的配置组合为“或”的关系。譬如：当配置为ack 0 psh 1时，将匹配不携带ACK或携带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。对于路由器，表示匹配携带ACK或RST标志位的TCP连接报文

设备各款型对于本参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**object-group**	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK支持 MSR810-LMS/810-LUS不支持
MSR 2600-6-X1/2600-10-X1		• MSR2600-6-X1：不支持 • MSR2600-10-X1：支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**object-group**	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**object-group**	支持

型号	特性	描述
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		支持

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

表1-13 ICMPv6 特有的规则信息参数

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

表1-14 ICMPv6 消息名称与消息类型和消息码的对应关系

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

ICMPv6 消息名称	ICMPv6 消息类型	ICMPv6 消息码
unknown-next-hdr	4	1

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

创建的规则若与动态规则的内容完全相同，则会覆盖已有动态规则。创建或修改的规则不能与手工配置的规则的内容完全相同，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。

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

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule** [*rule-id*] { **deny** | **permit** }命令无法删除规则中的部分内容，使用 undo rule { deny | permit }命令时，必须输入已存在规则的完整形式。

【举例】

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

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

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

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

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

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

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

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

```
[Sysname-acl-ipv6-adv-3003] rule permit udp source-port eq snmptrap
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmp
[Sysname-acl-ipv6-adv-3003] rule permit udp destination-port eq snmptrap
```

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

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

【相关命令】

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

1.1.22 rule (IPv6 basic ACL view)

rule 命令用来为 IPv6 基本 ACL 创建一条规则。

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

【命令】

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

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

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

【缺省情况】

IPv6 基本 ACL 内不存在任何规则。

【视图】

IPv6 基本 ACL 视图

【缺省用户角色】

network-admin

【参数】

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

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

counting：表示开启规则匹配统计功能，缺省为关闭。

fragment：表示仅对非首片分片报文有效，而对非分片报文和首片分片报文无效。若未指定本关键字，表示该规则对非分片报文和分片报文均有效。

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

routing [**type** *routing-type*]：表示对所有或指定类型的路由头有效，*routing-type* 表示路由头类型的值，取值范围为 0～255。若指定了 **type** *routing-type* 参数，表示仅对指定类型的路由头有效；否则，表示对 IPv6 所有类型的路由头都有效。

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

设备各款型对于本参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**object-group**	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK支持 MSR810-LMS/810-LUS不支持
MSR 2600-6-X1/2600-10-X1		• MSR2600-6-X1：不支持 • MSR2600-10-X1：支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**object-group**	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持

型号	命令	描述
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**object-group**	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		支持

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

vpn-instance *vpn-instance-name*：表示对指定 VPN 实例中的报文有效。*vpn-instance-name* 表示 MPLS L3VPN 的 VPN 实例名称，为 1～31 个字符的字符串，区分大小写。若未指定本参数，表示该规则仅对非 VPN 报文有效。

【使用指导】

使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。

新创建或修改的规则不能与已有规则的内容完全相同，否则将提示出错，并导致该操作失败。

新创建或修改的规则若指定对象组，则该对象组必须存在，否则将提示出错，并导致该操作失败。

当 ACL 的规则匹配顺序为配置顺序时，允许修改该 ACL 内的任意一条已有规则；当 ACL 的规则匹配顺序为自动排序时，不允许修改该 ACL 内的已有规则，否则将提示出错。

counting 关键字用于开启本规则的匹配统计功能。

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

删除规则时需要注意的是：

- 使用 **undo rule** *rule-id* 命令时，如果没有指定任何可选参数，则删除整条规则；如果指定了可选参数，则只删除该参数所对应的内容。
- **undo rule** [*rule-id*] { **deny** | **permit** }命令无法删除规则中的部分内容，使用 **undo rule** { **deny** | **permit** }命令时，必须输入已存在规则的完整形式。

【举例】

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

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

【相关命令】

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

1.1.23 rule comment

rule comment 命令用来为指定规则配置描述信息。

undo rule comment 命令用来删除指定规则的描述信息。

【命令】

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

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

【缺省情况】

规则没有任何描述信息。

【视图】

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

【缺省用户角色】

network-admin

【参数】

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

text：表示规则的描述信息，为 1～127 个字符的字符串，区分大小写。

【使用指导】

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

【举例】

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

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] rule 0 comment This rule is used on GigabitEthernet 1/0/1.
```

【相关命令】

- **display acl**

1.1.24 step

step 命令用来配置规则编号的步长。

undo step 命令用来恢复缺省情况。

【命令】

step *step-value*

undo step

【缺省情况】

规则编号的步长为 5，起始值为 0。

【视图】

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

【缺省用户角色】

network-admin

【参数】

step-value：表示规则编号的步长值，取值范围为 1～20。

【使用指导】

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

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

【举例】

将 IPv4 基本 ACL 2000 的规则编号的步长配置为 2。

```
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] step 2
```

【相关命令】

- **display acl**

目 录

1 QoS策略 ····· 1-1

1.1 定义类的命令 ····· 1-1

1.1.1 display traffic classifier ····· 1-1

1.1.2 if-match ····· 1-3

1.1.3 traffic classifier ····· 1-10

1.2 定义流行为的命令 ····· 1-11

1.2.1 car ····· 1-11

1.2.2 car percent ····· 1-12

1.2.3 display traffic behavior ····· 1-13

1.2.4 filter ····· 1-16

1.2.5 gts ····· 1-17

1.2.6 gts percent ····· 1-18

1.2.7 redirect ····· 1-19

1.2.8 remark dot1p ····· 1-20

1.2.9 remark dscp ····· 1-20

1.2.10 remark ip-precedence ····· 1-22

1.2.11 remark local-precedence ····· 1-22

1.2.12 remark qos-local-id ····· 1-23

1.2.13 remark tunnel-dscp ····· 1-23

1.2.14 traffic behavior ····· 1-26

1.2.15 traffic-policy ····· 1-27

1.3 定义和应用QoS策略的命令 ····· 1-28

1.3.1 classifier behavior ····· 1-28

1.3.2 control-plane ····· 1-29

1.3.3 control-plane management ····· 1-30

1.3.4 display qos policy ····· 1-31

1.3.5 display qos policy advpn ····· 1-33

1.3.6 display qos policy control-plane ····· 1-35

1.3.7 display qos policy control-plane management ····· 1-37

1.3.8 display qos policy control-plane management pre-defined ····· 1-39

1.3.9 display qos policy control-plane pre-defined ····· 1-41

1.3.10 display qos policy interface ····· 1-44

1.3.11 display qos policy l2vpn-pw ····· 1-48

1.3.12 display qos policy user-profile ····· 1-50
1.3.13 qos apply policy (interface view, PVC view, control plane view, control plane management view,PW view) ····· 1-56
1.3.14 qos apply policy (user-profile view) ····· 1-57
1.3.15 qos policy ····· 1-59
1.3.16 reset qos policy advpn ····· 1-60
1.3.17 reset qos policy control-plane ····· 1-60
1.3.18 reset qos policy control-plane management ····· 1-61
1.4 接口流速统计配置命令 ····· 1-63
1.4.1 qos flow-interval ····· 1-63
2 优先级映射 ····· 2-1
2.1 优先级映射表配置命令 ····· 2-1
2.1.1 display qos map-table ····· 2-1
2.1.2 import (priority map view) ····· 2-2
2.1.3 qos map-table ····· 2-3
2.2 端口优先级配置命令 ····· 2-3
2.2.1 qos priority ····· 2-4
2.3 端口优先级信任模式配置命令 ····· 2-4
2.3.1 display qos trust interface ····· 2-5
2.3.2 qos trust ····· 2-5
3 流量监管、流量整形和限速 ····· 3-1
3.1 流量监管配置命令 ····· 3-1
3.1.1 display qos car interface ····· 3-1
3.1.2 display qos carl ····· 3-3
3.1.3 qos car (interface view) ····· 3-4
3.1.4 qos car any(user-profile view) ····· 3-6
3.1.5 qos carl ····· 3-8
3.2 流量整形配置命令 ····· 3-9
3.2.1 display qos gts interface ····· 3-9
3.2.2 qos gts ····· 3-11
3.3 限速配置命令 ····· 3-12
3.3.1 display qos lr ····· 3-12
3.3.2 qos lr ····· 3-13
4 拥塞管理 ····· 4-1
4.1 拥塞管理公共配置命令 ····· 4-1
4.1.1 display qos queue interface ····· 4-1

4.1.2 display qos queue l2vpn-pw ····· 4-3
4.1.3 reset qos statistics l2vpn-pw ····· 4-4
4.2 FIFO队列配置命令 ····· 4-4
4.2.1 display qos queue fifo ····· 4-4
4.2.2 qos fifo queue-length ····· 4-5
4.3 优先级队列配置命令 ····· 4-6
4.3.1 display qos queue pq interface ····· 4-6
4.3.2 display qos pql ····· 4-7
4.3.3 qos pq ····· 4-8
4.3.4 qos pql default-queue ····· 4-9
4.3.5 qos pql inbound-interface ····· 4-10
4.3.6 qos pql local-precedence ····· 4-10
4.3.7 qos pql protocol ····· 4-11
4.3.8 qos pql protocol mpls exp ····· 4-12
4.3.9 qos pql queue ····· 4-13
4.4 定制队列配置命令 ····· 4-13
4.4.1 display qos queue cq interface ····· 4-13
4.4.2 display qos cql ····· 4-15
4.4.3 qos cq ····· 4-15
4.4.4 qos cql default-queue ····· 4-16
4.4.5 qos cql inbound-interface ····· 4-17
4.4.6 qos cql local-precedence ····· 4-17
4.4.7 qos cql protocol ····· 4-18
4.4.8 qos cql protocol mpls exp ····· 4-19
4.4.9 qos cql queue ····· 4-20
4.4.10 qos cql queue serving ····· 4-20
4.5 加权公平队列配置命令 ····· 4-21
4.5.1 display qos queue wfq ····· 4-21
4.5.2 qos wfq ····· 4-23
4.6 实时传输协议队列的配置命令 ····· 4-24
4.6.1 display qos queue rtpq interface ····· 4-24
4.6.2 qos rtpq ····· 4-25
4.7 基于类的队列配置命令 ····· 4-26
4.7.1 display qos queue cbq ····· 4-26
4.7.2 qos reserved-bandwidth ····· 4-27
4.7.3 queue af ····· 4-28

4.7.4 queue ef ····· 4-29
4.7.5 queue sp ····· 4-30
4.7.6 queue wfq ····· 4-31
4.7.7 queue-length ····· 4-31
4.7.8 wred ····· 4-32
4.7.9 wred dscp ····· 4-33
4.7.10 wred ip-precedence ····· 4-34
4.7.11 wred weighting-constant ····· 4-35
4.8 报文信息预提取命令 ····· 4-36
4.8.1 qos pre-classify ····· 4-36
4.9 QoS令牌配置命令 ····· 4-36
4.9.1 qos qmtoken ····· 4-36
5 拥塞避免 ····· 5-1
5.1 WRED配置命令 ····· 5-1
5.1.1 display qos wred interface ····· 5-1
5.1.2 qos wred enable ····· 5-2
5.1.3 qos wred dscp ····· 5-3
5.1.4 qos wred ip-precedence ····· 5-4
5.1.5 qos wred weighting-constant ····· 5-5
6 QPPB ····· 6-1
6.1 QPPB配置命令 ····· 6-1
6.1.1 bgp-policy ····· 6-1

1 QoS策略

说明

- 各款型对于 ATM 接口的支持情况，请参见设备的安装手册和接口模块手册。
- 仅 MSR810-LMS/810-LUS/830-4LM-WiNet/3600-28-SI/3600-51-SI 不支持 l2vpn-pw。

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

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】

集中式设备－独立运行模式：

display traffic classifier { **system-defined** | **user-defined** } [*classifier-name*]

分布式设备－独立运行模式/集中式设备－IRF 模式：

display traffic classifier { **system-defined** | **user-defined** } [*classifier-name*] [**slot** *slot-number*]

分布式设备－IRF 模式：

display traffic classifier { **system-defined** | **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

【参数】

system-defined：系统定义类。

user-defined：用户定义类。

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

slot *slot-number*：显示指定单板的流分类的信息，*slot-number* 表示单板所在的槽位号。如果未指定本参数，将显示主用主控板的类的配置信息。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备的流分类的信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示主用设备的类的配置信息。（集中式设备－IRF 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，将显示全局主用主控板的类的配置信息。（分布式设备－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 not protocol ipv6

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

显示系统定义类 default-class 的配置信息。

```
<Sysname> display traffic classifier system-defined default-class
```

```
System-defined classifier information:

 Classifier: default-class (ID 0)
   Operator: AND
   Rule(s) :
    If-match any
```

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	类的名称及其内容，内容可以有多种类型
Operator	分类规则之间的逻辑关系
Rule(s)	分类规则

1.1.2 if-match

if-match 命令用来定义匹配数据包的规则。

undo if-match 命令用来删除配置的匹配数据包的规则。

【命令】

if-match [**not**] *match-criteria*

undo if-match [**not**] *match-criteria*

【缺省情况】

未定义匹配数据包的规则。

【视图】

类视图

【缺省用户角色】

network-admin

【参数】

not：不匹配该规则。

match-criteria：类的匹配规则，具体情况如 表 1-2 所示。

表1-2 类的匹配规则取值

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

取值	描述
app-group *group-name*	定义匹配应用组的规则，*group-name*为系统预定义应用组的名称。
application *app-name*	定义匹配应用名的规则，*app-name*为系统预定义应用的名称。
any	定义匹配所有数据包的规则
classifier *classifier-name*	定义匹配QoS类的规则，*classifier-name*为类名
control-plane protocol *protocol-name*&<1-8>	定义匹配控制平面或者管理口控制平面协议的规则，*protocol-name*&<1-8>为系统预定义匹配协议报文类型名称的列表，具体如表1-3所示，&<1-8>表示前面的参数最多可以输入8次。
control-plane protocol-group *protocol-group-name*	定义匹配控制平面或者管理口控制平面协议组的规则，*protocol-group-name*取值为critical、exception、important、management、monitor、normal、redirect
customer-dot1p *dot1p-value*&<1-8>	定义匹配内层VLAN Tag 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
customer-vlan-id *vlan-id-list*	定义匹配内层VLAN Tag VLAN ID的规则，*vlan-id-list*：VLAN列表，表示方式为*vlan-id-list* = { *vlan-id* | *vlan-id1* **to** *vlan-id2* }&<1-10>，*vlan-id*、*vlan-id1*、*vlan-id2*取值范围为1～4094，且*vlan-id1*的值必须小于*vlan-id2*的值；&<1-10>表示前面的参数最多可以重复输入10次
destination-mac *mac-address*	定义匹配目的MAC地址的规则
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1-5所示
inbound-interface *interface-type interface-number*	定义匹配入接口的规则，*interface-type interface-number*为接口类型和接口编号
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
local-precedence *local-precedence-value*&<1-8>	定义匹配本地优先级的规则，*local-precedence-value*&<1-8>为本地优先级的列表，本地优先级的取值范围为0～7，&<1-8>表示前面的参数最多可以输入8次
mpls-exp *exp-value*&<1-8>	定义匹配第一层MPLS EXP优先级的规则，*exp-value*&<1-8>为EXP的列表，EXP优先级的取值范围为0～7，&<1-8>表示前面的参数最多可以输入8次
packet-length { **min** *min-value* | **max** *max-value* } *	定义匹配报文长度的规则，*min-value*为匹配报文最小长度的字节数，*max-value*为匹配报文最大长度的字节数
protocol *protocol-name*	定义匹配协议的规则，*protocol-name*取值为arp、ip、ipv6
qos-local-id *local-id-value*	定义匹配QoS本地ID值的规则，*local-id-value*为QoS本地ID，取值范围为1～4095
rtp payload-type { *type-value*&<0-16> | **audio** | **video** }*	定义匹配RTP负载类型的规则，*type-value*&<0-16>为RTP负载类型值的列表，RTP负载类型的取值范围为0～127，&<0-16>表示前面的参数最多可以输入16次。**audio**表示RTP负载类型为音频，对应RTP负载类型值包括，0～23和33，**video**表示RTP负载类型为视频，对应RTP负载类型值的范围为24～3。
rtp start-port *start-port-number* **end-port** *end-port-number*	定义匹配RTP协议端口的规则。*start-port-number*为起始RTP端口号，取值范围为2000～65535；*end-port-number*为结束RTP端口号，取值范围为2000～65535

取值	描述
source-mac *mac-address*	定义匹配源MAC地址的规则
tunnel-dscp *dscp-value***&<1-8>**	定义匹配VXLAN报文外层IP头DSCP的规则，*dscp-value*&<1-8>为DSCP取值的列表，VXLAN报文外层IP头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1-5所示

表1-3 系统预定义匹配协议报文类型名称的列表

报文类型	说明
default	其他协议
arp	ARP协议
arp-snooping	ARP Snooping协议
bgp	BGP协议
bgp4+	IPv6 BGP
http	HTTP协议
https	HTTPS协议
icmp	ICMP协议
icmpv6	IPv6 ICMP协议
igmp	IGMP协议
isis	IS-IS协议
ldp	LDP协议
ldp6	IPv6 LDP协议
msdp	MSDP协议
ntp	NTP协议
oam	OAM协议
ospf-multicast	OSPF组播
ospf-unicast	OSPF单播
ospf3-multicast	OSPFv3组播
ospf3-unicast	OSPFv3单播
pim-multicast	PIM组播
pim-unicast	PIM单播
pim6-multicast	IPv6 PIM组播
pim6-unicast	IPv6 PIM单播
radius	RADIUS协议
rip	RIP协议

报文类型	说明
ripng	RIPng协议
rsvp	RSVP协议
snmp	SNMP协议
tacacs	TACACS协议
vrrp	VRRP协议
vrrp6	IPv6 VRRP协议
ssh	SSH协议
telnet	TELNET协议
ftp	FTP协议
tftp	TFTP协议

【使用指导】

在定义匹配 ACL 的规则时，请注意：

- 类中引用的 ACL 必须已经存在。
- 一个类下可配置多条匹配命令，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。
- 当 **if-match** 中引用的 ACL 规则的动作为 **deny** 时，则跳出该 **if-match**，继续进行后续规则的查找。

在定义匹配用户组或应用名的规则时，一个类下可配置多条匹配命令，各个配置之间互相不覆盖。

在定义匹配所处网络环境属性时，请注意：

- 一个类下可配置多条匹配命令，各个配置之间互相不覆盖。

在定义匹配类的规则时，一个类下可配置多条匹配命令，各个配置之间互相不覆盖。如果匹配类的规则之间既有逻辑与，又有逻辑或的关系，请使用以下方式配置。

例如，需要定义 classA，满足以下关系：规则 1 & 规则 2 | 规则 3，可以这样定义：

- traffic classifier classB operator and
- if-match 规则 1
- if-match 规则 2
- traffic classifier classA operator or
- if-match 规则 3
- if-match classifier classB

在定义匹配目的 MAC 地址的规则时，请注意：

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

在定义匹配源 MAC 地址的规则时，请注意：

- 一个类下可配置多条匹配命令，各个配置之间互相不覆盖。

- 匹配源 MAC 地址规则只对以太网接口有意义。

在定义匹配 DSCP 的规则时，请注意：

- 一个类下可配置多条匹配命令，各个配置之间互相不覆盖。
- 一条命令可以配置多个 DSCP 值，最多可指定 8 个；如果指定了多个相同的 DSCP 值，系统默认为一个；多个不同的 DSCP 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 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。

在定义匹配内层 VLAN Tag 和外层 VLAN Tag 802.1p 优先级的规则时，请注意：

- 一个类下可配置多条匹配命令，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。

在定义匹配 IP 优先级的规则时，请注意：

- 一个类下可配置多条匹配命令，各个配置之间互相不覆盖。
- 一条命令可以配置多个 IP 优先级值，最多可指定 8 个；如果指定了多个相同的 IP 优先级值，系统默认为一个；多个不同的 IP 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 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。

在定义匹配本地优先级的规则时，请注意：

- 一个类下可配置多条匹配命令，各个配置之间互相不覆盖。每条命令在配置后，本地优先级的值将自动按照从小到大的顺序排序。
- 一条命令可以配置多个本地优先级值，最多可指定 8 个；如果指定了多个相同的本地优先级值，系统默认为一个；多个不同的本地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。
- 删除某条匹配本地优先级的规则时，指定的所有本地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。

在定义匹配 MPLS EXP 优先级的规则时，请注意：

- 一个类下可配置多条匹配命令，各个配置之间互相不覆盖。
- 一条命令可以配置多个 MPLS EXP 优先级值，最多可指定 8 个；如果指定了多个相同的 MPLS EXP 优先级值，系统默认为一个；多个不同的 MPLS EXP 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 MPLS EXP 优先级的规则时，指定的所有 MPLS EXP 优先级值必须与该规则中定义的完全相同才会删除，顺序可不一样。
- MPLS EXP 为 MPLS 报文特有的参数，该匹配规则仅对 MPLS 报文生效。
- 对于软转发 QoS，MPLS 报文不支持匹配 IP 相关匹配规则。

在定义匹配报文长度的规则时，请注意：

- 一个类下可配置多条匹配命令，各个配置之间互相不覆盖。

- 如果只配置 **min**，则表示匹配大于 *min-value* 长度的报文；如果只配置 **max**，表示匹配小于 *max-value* 长度的报文；同时配置 **min** 和 **max**，表示匹配长度在 *min-value*～*max-value* 之间的报文。其中 *max-value* 必须大于等于 *min-value*。

在定义匹配预定义的上送控制平面或者管理口控制平面报文类型的规则时，请注意：

- 一个类下可配置多条匹配命令，各个配置之间互相不覆盖。
- 一条命令可以配置多个 protocol，如果指定了多个相同的 protocol，系统默认为一个；多个不同的 protocol 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 protocol 的规则时，指定的所有 protocol 必须与该规则中定义的完全相同才会删除，顺序可不一样。

在定义匹配 RTP 协议端口的规则时，请注意：

- 该命令用于匹配落在指定 RTP 端口号范围内的 RTP 报文，即匹配所有在 *start-port-number* 与 *end-port-number* 之间的偶数 UDP 端口号的报文。
- 一个类下可配置多条匹配命令，各个配置之间互相不覆盖。

【举例】

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

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

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

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

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

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

定义类匹配 ACL3101。

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

定义类匹配 ACL flow。

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

定义类匹配 IPv6 ACL3101。

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

定义类匹配 IPv6 ACL flow。

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

定义匹配所有数据包的规则。

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

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

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

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

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

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

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

定义类匹配 IP 协议的报文。

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

定义类 class1 的匹配规则为：匹配 RTP 端口号在 16384 和 32767 之间的偶数 UDP 端口号的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match rtp start-port 16384 end-port 32767
```

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

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

定义类 class1 匹配 QoS 本地 ID 值为 3 的报文。

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

匹配 RTP 负载类型值为 1、8、音频或视频类型的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class
[Sysname-behavior-class] if-match rtp payload-type 1 8 audio video
```

定义类 class1 匹配应用组 multimedia。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match app-group multimedia
```

定义类 class1 匹配应用名 3link。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match application 3link
```

在流分类 class1 中配置匹配上送控制平面或管理口控制平面的 ARP 协议报文。

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

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

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

在流分类 class1 中配置匹配报文长度为 100～200 字节的报文。

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match packet-length min 100 max 200
```

在流分类 class1 中配置匹配外层 IP 头 DSCP 值为 10 的 VXLAN 报文。

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

1.1.3 traffic classifier

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

undo traffic classifier 命令用来删除一个类。

【命令】

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

undo traffic classifier *classifier-name*

【缺省情况】

未配置类。

【视图】

系统视图

【缺省用户角色】

network-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 car

car 命令用来配置流量监管动作。

undo car 命令用来恢复缺省情况。

【命令】

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

car cir *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo car

【缺省情况】

未配置流量监管动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【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 8～10000000。

cbs *committee-burst-size*：承诺突发尺寸，单位为 byte，取值范围为 1000～1000000000，缺省取值为 500 毫秒以 CIR 速率通过的流量。

ebs *excess-burst-size*：超出突发尺寸，单位为 byte，取值范围为 0～1000000000，缺省值为 0。

pir *peak-information-rate*：峰值速率，单位为 kbps，取值范围为 8～10000000。

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

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

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

action：对数据包采取的动作，有以下几种：

- **discard**：丢弃数据包。
- **pass**：允许数据包通过。
- **remark-dot1p-pass** *new-cos*：设置新的 802.1P 报文的优先级值，并允许数据包通过，取值范围为 0～7。

- **remark-dscp-pass** *new-dscp*：设置报文新的 DSCP 值，并允许数据包通过，取值范围为 0～63。
- **remark-mpls-exp-pass** *new-exp*：设置新的 MPLS 报文的 EXP 标志位的值，并允许数据包通过，取值范围为 0～7。
- **remark-prec-pass** *new-precedence*：设置新的 IP 优先级，并允许数据包通过，取值范围为 0～7。

【使用指导】

接口上应用的策略中使用 **car** 时，可以应用到接口报文的接收或者发送方向。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

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。

【举例】

为流行为配置流量监管。报文正常流速为 200kbps，承诺突发尺寸为 51200bytes，速率大于 200kbps 时，报文 DSCP 值改为 0 并发送。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 51200 ebs 0 green pass red remark-dscp-pass 0
```

1.2.2 car percent

car cir percent 命令用来采用百分比的方式在流行为内配置流量监管动作。

undo car 命令用来恢复缺省情况。

【命令】

car cir percent *cir-percent* [**cbs** *cbs-time* [**ebs** *ebs-time*]] [**green** *action* | **red** *action* | **yellow** *action*] *

car cir percent *cir-percent* [**cbs** *cbs-time*] **pir percent** *pir-percent* [**ebs** *ebs-time*] [**green** *action* | **red** *action* | **yellow** *action*] *

【缺省情况】

未配置百分比形式的流量监管动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

cir percent *cir-percent*：承诺信息速率百分比，取值范围为 1～100。CIR 的实际值是百分比值乘以接口带宽值。

cbs *cbs-time*：用指定的时间（单位为 ms）来设置 CBS，实际的 CBS 值是 cbs-time 乘以实际的 cir 值（cir 值乘以接口带宽），取值范围为 50～2000。

ebs *ebs-time*：用指定的时间（单位为 ms）来设置 EBS，实际的 EBS 值是 ebs-time 乘以实际的 cir 值（cir 值乘以接口带宽），取值范围为 0～2000。

pir percent *pir-percent*：以百分比的形式来指定峰值速率，取值范围为 1～100。峰值速率不能比承诺信息速率小。不配置峰值速率表示所配置的是单速桶流量监管，否则表示双速桶流量监管。

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

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

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

action：对数据包采取的动作，有以下几种：

- **discard**：丢弃数据包。
- **pass**：允许数据包通过。
- **remark-dot1p-pass** *new-cos*：设置新的 802.1P 报文的优先级值，并允许数据包通过，取值范围为 0～7。
- **remark-dscp-pass** *new-dscp*：设置报文新的 DSCP 值，并允许数据包通过，取值范围为 0～63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。
- **remark-mpls-exp-pass** *new-exp*：设置新的 MPLS 报文的 EXP 标志位的值，并允许数据包通过，取值范围为 0～7。
- **remark-prec-pass** *new-precedence*：设置新的 IP 优先级，并允许数据包通过，取值范围为 0～7。

【使用指导】

接口上应用的 QoS 策略中使用 **car** 时，可以应用到接口报文的接收或者发送方向。

按百分比配置 CAR 的 QoS 策略只能应用到接口上。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

承诺速率=CIR * bandwidth，峰值速率=PIR * bandwidth，最顶层策略的 bandwidth 取应用此策略的接口带宽，嵌套策略的 bandwidth 取所在流行为下的 GTS 速率值，如没有 GTS，则取更上一层策略所在流行为的 GTS 速率，如没有取到，最终使用应用策略的接口带宽。

【举例】

为流行为配置流量监管。报文正常流速为带宽的 20%，承诺突发尺寸为 100ms。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir percent 20 cbs 100
```

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】

集中式设备－独立运行模式：

display traffic behavior { **system-defined** | **user-defined** } [*behavior-name*]

分布式设备－独立运行模式/集中式设备－IRF 模式：

display traffic behavior { **system-defined** | **user-defined** } [*behavior-name*] [**slot** *slot-number*]

分布式设备－IRF 模式：

display traffic behavior { **system-defined** | **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

【参数】

system-defined：系统定义行为。

user-defined：用户定义行为。

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

slot *slot-number*：显示指定单板的流行为的信息，*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示主用主控板的流行为的配置信息。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备的流行为的信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主用设备的流行为的配置信息。（集中式设备－IRF 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，则显示全局主用主控板的流行为的配置信息。（分布式设备－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 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
      Primap pre-defined table: dscp-lp
      Assured Forwarding:
        Bandwidth 30 (kbps)
        Discard Method: Tail

    Behavior: 2 (ID 101)
      Accounting enable: Packet
      Filter enable: Permit
```

```
      Marking:
        Remark mpls-exp 4
      Redirecting:
      Mirroring:
        Mirror to the VLAN: VLAN 1000
      Expedited Forwarding:
        Bandwidth 50 (kbps) CBS 1250 (Bytes)

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

显示系统定义行为的配置信息。

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

  System-defined behavior information:

    Behavior: be (ID 0)
      -none-

    Behavior: af (ID 1)
      Assured Forwarding:
        Bandwidth 20 (%)
        Discard Method: Tail

    Behavior: ef (ID 2)
      Expedited Forwarding:
        Bandwidth 20 (%) Cbs-ratio 25

    Behavior: be-flow-based (ID 3)
      Flow based Weighted Fair Queue:
        Max number of hashed queues: 256
        Discard Method: IP Precedence based WRED
        Exponential Weight: 9
        Pre  Low   High  Dis-prob
        -------------------------
        0    10    30    10
        1    10    30    10
        2    10    30    10
        3    10    30    10
        4    10    30    10
        5    10    30    10
        6    10    30    10
        7    10    30    10
```

表1-4 display traffic behavior 命令显示信息描述表

字段	描述
User-defined behavior information	用户自定义流行为的信息
System-defined behavior information	系统定义流行为的信息

字段	描述
Behavior	行为的名称及其内容，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
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，单位为byte
EBS	超出突发尺寸，单位为byte
Green action	对绿色报文的动作
Red action	对红色报文的动作
Yellow action	对黄色报文的动作
Bandwidth	队列的带宽
Discard Method	丢弃方式
Accounting enable	流量统计动作
Filter enable	流量过滤动作
Remark mpls-exp	重新标记报文的EXP优先级值
Redirecting	流量重定向相关信息
Mirroring	流量镜像相关信息
Expedited Forwarding	加速转发（EF队列）相关信息
none	表示未配置其他流行为
Flow based Weighted Fair Queue	基于流的加权公平队列相关信息
Max number of hashed queues	加权公平队列的长度
Exponential Weight	计算平均队列长度的指数
Pre	报文的IP优先级
Low	队列下限
High	队列上限
Dis-prob	计算丢弃概率时的分母

1.2.4 filter

filter 命令用来配置流量过滤动作。

undo filter 命令用来恢复缺省情况。

【命令】

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

undo filter

【缺省情况】

未配置流量过滤动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【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 gts

gts 命令用来采用绝对值的方式为流行为配置流量整形动作。

undo gts 命令用来恢复缺省情况。

【命令】

gts cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**queue-length** *queue-length*]

undo gts

【缺省情况】

未配置流量整形动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

cir *committed-information-rate*：承诺信息速率，单位为 kbps，取值范围为 8～10000000。

cbs *committed-burst-size*：承诺突发尺寸，实际平均速率在承诺速率以内时的突发流量，单位为 byte，取值范围为 1000～1000000000。

ebs *excess-burst-size*：超出突发尺寸，单位为 byte，取值范围为 0～1000000000。

queue-length *queue-length*：队列的最大长度，缺省值为 50，取值范围为 1～1024。

【使用指导】

接口上应用的 QoS 策略中使用 **gts** 时，只能应用到接口的出方向。

接口上应用配置了 **gts** 的 QoS 策略将导致原有的 **qos gts** 命令失效。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

【举例】

为流行为配置 GTS，正常流速为 200kbps，承诺突发尺寸为 51200bytes，速率大于 200kbps 时，将进入队列缓存，缓存队列长度为 100。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] gts cir 200 cbs 51200 ebs 0 queue-length 100
```

【相关命令】

- **gts percent**

1.2.6 gts percent

gts percent 命令用来采用百分比的方式为流行为配置流量整形动作。

undo gts 命令用来恢复缺省情况。

【命令】

gts percent cir *cir-percent* [**cbs** *cbs-time* [**ebs** *ebs-time*]] [**queue-length** *queue-length*]

undo gts

【缺省情况】

未配置百分比形式的流量整形动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

cir *cir-percent*：承诺信息速率百分比，取值范围为 1～100。CIR 的实际值是百分比值乘以接口带宽值。

cbs *cbs-time*：某段时间内的承诺突发尺寸，单位为 ms，缺省值为 500ms。CBS 的实际值是 CBS 的配置时间值乘以实际的承诺信息速率（**cir** 值乘以接口带宽），取值范围为 50～2000。

ebs *ebs-time*：某段时间内的超出突发尺寸，单位为 ms，缺省值为 0ms。EBS 的实际值是 EBS 的配置时间值乘以实际的承诺信息速率（**cir** 值乘以接口带宽），取值范围为 0～2000。

queue-length *queue-length*：队列的最大长度，缺省值为 50，取值范围为 1～1024。

【使用指导】

接口上应用的 QoS 策略中使用 **gts** 时，只能应用到接口的出方向。

接口上应用配置了 **gts** 的 QoS 策略将导致原有的 **qos gts** 命令失效。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

【举例】

配置使用流量整形，正常流量为 50%的接口带宽，在第一时间可以有 200ms×50%接口带宽的突发流量通过，以后速率小于等于 50%的接口带宽时正常发送，速率大于 50%的接口带宽时，将进入队列缓存。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] gts percent cir 50 cbs 200
```

【相关命令】

- **gts**

1.2.7 redirect

redirect 命令用来为流行为配置流量重定向动作。

undo redirect 命令用来恢复缺省情况。

【命令】

redirect interface *interface-type interface-number* [**track-oap**]

undo redirect interface *interface-type interface-number*

【缺省情况】

未配置流量重定向动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

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（对于重定向到隧道来说，接口类型是 **tunnel**；对于重定向到二层聚合接口来说，接口类型是 **bridge-aggregation**；对于重定向到三层聚合接口来说，接口类型是 **route-aggregation**）。

track-oap：关联重定向到接口的动作与 OAP Client 的状态。如果不指定该参数，则设备不会检测是否存在 OAP Client，并且不执行关联动作。

【使用指导】

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

【举例】

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

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface gigabitethernet1/0/1
```

【相关命令】

- **classifier behavior**

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

1.2.8 remark dot1p

remark dot1p 命令用来配置重新标记报文的 802.1p 优先级。

undo remark dot1p 命令用来取消标记报文的 802.1p 优先级。

【命令】

remark dot1p *dot1p-value*

undo remark dot1p

【缺省情况】

未配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

dot1p-value：802.1p 优先级，取值范围为 0～7。

【举例】

重新标记报文的 802.1p 优先级值为 2。

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

1.2.9 remark dscp

remark dscp 命令用来重新标记报文的 DSCP 值。

undo remark dscp 命令用来恢复缺省情况。

【命令】

remark dscp *dscp-value*

undo remark dscp

【缺省情况】

未配置重新标记报文 DSCP 值的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

dscp-value：DSCP值，取值范围为0～63，也可以是关键字，如 表 1-5 所示。

表1-5 DSCP 关键字与值的对应表

关键字	DSCP 值（二进制）	DSCP 值（十进制）
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】

对于硬件转发的产品，在同一个流行为中，如果已配置 **remark tunnel-dscp** 命令，则不允许再配置 **remark dscp** 命令，反之亦然。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

【举例】

重新标记报文的 DSCP 值为 6。

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

1.2.10 remark ip-precedence

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

undo remark ip-precedence 命令用来恢复缺省情况。

【命令】

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

【缺省情况】

未配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

ip-precedence-value：IP 优先级，取值范围为 0～7。

【使用指导】

对于硬件转发的产品，在同一个流行为中，如果已配置 **remark tunnel-dscp** 命令，则不允许再配置 **remark ip-precedence** 命令，反之亦然。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

【举例】

重新标记报文的 IP 优先级值为 6。

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

1.2.11 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 命令用来恢复缺省情况。

【命令】

remark local-precedence *local-precedence-value*

undo remark local-precedence

【缺省情况】

未配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【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
```

1.2.12 remark qos-local-id

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

undo remark qos-local-id 命令用来恢复缺省情况。

【命令】

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

undo remark qos-local-id

【缺省情况】

未配置重新标记报文的 QoS 本地 ID 值的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

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

【使用指导】

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

【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
```

1.2.13 remark tunnel-dscp

remark tunnel-dscp 命令用来重新标记隧道封装后报文外层 IP 头的 DSCP 值。

undo remark tunnel-dscp 命令用来恢复缺省情况。

【命令】

remark tunnel-dscp *dscp-value*

undo remark tunnel-dscp

设备各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	参数	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**remark tunnel-dscp** *dscp-value*	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK支持 MSR810-LMS/810-LUS不支持
MSR 2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**remark tunnel-dscp** *dscp-value*	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**remark tunnel-dscp** *dscp-value*	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持

型号	特性	描述
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

【缺省情况】

未配置重新标记报文外层 IP 头的 DSCP 值的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

dscp-value：隧道封装后报文外层IP头的DSCP值，取值范围为 0～63，也可以是 表 1-6 中对应的关键字。

表1-6 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

关键字	DSCP 值（二进制）	DSCP 值（十进制）
cs7	111000	56
ef	101110	46

【使用指导】

本命令对 GRE、VXLAN、IPv4-IPv4、IPv6-IPv4、IPv6、MPLS-TE 隧道封装后的报文生效。

如果流行为视图下配置了本命令，则指定该流行为的 QoS 策略仅支持应用在接口上。

对于硬件转发的产品，在同一个流行为中，如果已配置 **remark dscp** 命令或 **remark ip-precedence** 命令，则不允许再配置 **remark tunnel-dscp** 命令，反之亦然。

在同一个流行为中多次执行本命令，最后一次执行的命令生效。

【举例】

重新标记隧道封装后报文外层 IP 头的 DSCP 值为 2。

```
<Sysname> system-view
[Sysname] traffic behavior data
[Sysname-behavior-data] remark tunnel-dscp 2
```

1.2.14 traffic behavior

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

undo traffic behavior 命令用来删除一个流行为。

【命令】

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

【缺省情况】

不存在流行为。

【视图】

系统视图

【缺省用户角色】

network-admin

【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**

1.2.15 traffic-policy

traffic-policy 命令用来在父策略流行为视图下应用一个子策略。

undo traffic-policy 命令用来删除关联的子策略。

【命令】

traffic-policy *policy-name*

undo traffic-policy

【缺省情况】

未配置应用子策略的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

policy-name：QoS 策略名，为 1～31 个字符的字符串，区分大小写。如果 QoS 策略不存在，则自动创建该 QoS 策略。

【使用指导】

通过在流行为视图下应用子策略，可以实现策略嵌套功能。即由 **traffic classifier** 命令定义的某一类流量，除了执行父策略中定义的行为外，还由子策略再次对该类流量进行分类，并执行子策略中定义的行为。

在配置策略嵌套功能时，请注意：

- 在父策略行为下应用子策略时，最多只能嵌套二层策略，并且不能嵌套自身。
- 一个流行为中至多只能嵌套一个子策略。

父策略和子策略中的内容需满足以下要求：

- 如果子策略中配置了 CBQ，那么父策略中必须配置 GTS，并且配置的父策略 GTS 带宽必须大于子策略 CBQ 带宽，否则配置失败。
- 如果父策略的 GTS 配置采用百分比形式，则子策略 CBQ 带宽配置不允许采用绝对值形式；如果父策略的 GTS 配置采用绝对值形式，则子策略 CBQ 带宽配置既可以采用百分比形式，也可以采用绝对值形式。
- 子策略中不允许配置 GTS。

嵌套策略支持对 IPv4、IPv6 报文的处理。

如果嵌套策略已经应用在接口上，则不允许删除嵌套的子策略，必须先解除子策略和父策略的嵌套关系。

【举例】

配置策略嵌套，在父策略下应用子策略 child。

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

【相关命令】

- **traffic classifier**
- **traffic behavior**

1.3 定义和应用QoS策略的命令

1.3.1 classifier behavior

classifier behavior 命令用来为类指定流行为。

undo classifier 命令用来取消为类指定的流行为。

【命令】

classifier *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]

undo classifier *classifier-name*

【缺省情况】

没有为类指定流行为。

【视图】

QoS 策略视图

【缺省用户角色】

network-admin

【参数】

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

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

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

【使用指导】

QoS 策略下每个类只能与一个流行为关联。

如果配置本命令时指定的类和流行为不存在，系统将创建一个空的类和空的流行为。

如果 **undo** 命令指定的类为系统预定义类 default-class，表示恢复 default-class 对应的流行为为系统预定义流行为 be，而不是取消对应的流行为。

【举例】

在 QoS 策略 user1 中为类 database 指定采用流行为 test。

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

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

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

【相关命令】

- **qos policy**

1.3.2 control-plane

control-plane 命令用来进入控制平面视图。

【命令】

集中式设备－独立运行模式：

control-plane

分布式设备－独立运行模式/集中式设备－IRF 模式：

control-plane slot *slot-number*

分布式设备－IRF 模式：

control-plane chassis *chassis-number* **slot** *slot-number*

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

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

slot *slot-number*：指定成员设备。*slot-number* 表示设备在 IRF 中的成员编号。（集中式设备－IRF 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。（分布式设备－IRF 模式）

【举例】

进入控制平面视图。（集中式设备－独立运行模式）

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

进入 3 号板控制平面视图。（分布式设备－独立运行模式）

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

进入 3 号成员设备控制平面视图。（集中式设备－IRF 模式）

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

```
[Sysname-cp-slot3]
```

进入 1 号成员设备 3 号板控制平面视图。（分布式设备－IRF 模式）

```
<Sysname> system-view
[Sysname] control-plane chassis 1 slot 3
[Sysname-cp-chassis1-slot3]
```

1.3.3 control-plane management

control-plane management 命令用来进入管理口控制平面视图。

【命令】

control-plane management

设备各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**control-plane management**	不支持
MSR 2600-6-X1/2600-10-X1		不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		不支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**control-plane management**	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		不支持

型号	特性	描述
MSR810-LM-GL	**control-plane management**	不支持

型号	特性	描述
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

【视图】

系统视图

【缺省用户角色】

network-admin

【举例】

进入管理口控制平面视图。

```
<Sysname> system-view
[Sysname] control-plane management
[Sysname-cp-management]
```

1.3.4 display qos policy

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

【命令】

集中式设备－独立运行模式：

display qos policy { **system-defined** | **user-defined** } [*policy-name* [**classifier** *classifier-name*]]

分布式设备－独立运行模式/集中式设备－IRF 模式：

display qos policy { **system-defined** | **user-defined** } [*policy-name* [**classifier** *classifier-name*]] [**slot** *slot-number*]

分布式设备－IRF 模式：

display qos policy { **system-defined** | **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

【参数】

system-defined：系统定义 QoS 策略。

user-defined：用户定义 QoS 策略。

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

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

slot *slot-number*：显示指定单板的 QoS 策略的信息，*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示主用主控板的 QoS 策略的配置信息。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备的 QoS 策略的信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主用设备的 QoS 策略的配置信息。（集中式设备－IRF 模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的 QoS 策略的信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示全局主用主控板的 QoS 策略的配置信息。（分布式设备－IRF 模式）

【举例】

显示用户定义 QoS 策略的配置信息。

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

  User-defined QoS policy information:

  Policy: 1 (ID 100)
   Classifier: default-class (ID 0)
     Behavior: be
      -none-
   Classifier: 1 (ID 100)
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
   Classifier: 2 (ID 101)
     Behavior: 2
      Accounting enable: Packet
      Filter enable: Permit
      Marking:
        Remark mpls-exp 4
   Classifier: 3 (ID 102)
     Behavior: 3
      -none-
```

显示系统定义 QoS 策略的配置信息。

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

```
System-defined QoS policy information:

Policy: default (ID 0)
 Classifier: default-class (ID 0)
   Behavior: be
    -none-
 Classifier: ef (ID 1)
   Behavior: ef
    Expedited Forwarding:
      Bandwidth 20 (%) Cbs-ratio 25
 Classifier: af1 (ID 2)
   Behavior: af
    Assured Forwarding:
      Bandwidth 20 (%)
      Discard Method: Tail
 Classifier: af2 (ID 3)
   Behavior: af
    Assured Forwarding:
      Bandwidth 20 (%)
      Discard Method: Tail
 Classifier: af3 (ID 4)
   Behavior: af
    Assured Forwarding:
      Bandwidth 20 (%)
      Discard Method: Tail
 Classifier: af4 (ID 5)
   Behavior: af
    Assured Forwarding:
      Bandwidth 20 (%)
      Discard Method: Tail
```

表1-7 display qos policy 命令显示信息描述表

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

其它显示信息解释请参见 表 1-1 和 表 1-4。

1.3.5 display qos policy advpn

display qos policy advpn 命令用来显示 Tunnel 接口 Hub-Spoke 隧道应用 QoS 策略的配置信息和运行情况。

【命令】

display qos policy advpn tunnel *number* [*ipv4-address* | *ipv6-address*] [**outbound**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

number：Tunnel 接口编号，取值范围为已创建的接口编号。

ipv4-address：隧道 Spoke 侧的 IPv4 私网地址。

ipv6-address：隧道 Spoke 侧的 IPv6 私网地址。

outbound：显示 Hub-Spoke 隧道出方向应用 QoS 策略的配置信息和运行情况。

【使用指导】

如果未指定隧道 Spoke 侧的私网地址，则显示 Tunnel 接口下所有 Hub-Spoke 隧道应用 QoS 策略的配置信息和运行情况。有关 Hub-Spoke 隧道的详细介绍，请参见“三层技术—IP 业务配置指导”中的“ADVPN 配置”。

如果未指定方向，则同时显示 Hub-Spoke 隧道接口出入两个方向应用 QoS 策略的配置信息和运行情况。有关隧道的配置命令，请参见“三层技术—IP 业务命令参考”中的“隧道命令”。

【举例】

显示 Tunnel 接口下 Hub-Spoke 隧道出方向应用 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy advpn tunnel 1 outbound
Session: Tunnel1 192.168.0.3
  Direction: Outbound
  Policy: finance
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: finance
     Matched : 123713988 (Packets) 13608538380 (Bytes)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: finance
      Committed Access Rate:
        CIR 1500 (kbps), CBS 93750 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 14980239 (Packets) 1647826290 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 108733781 (Packets) 11960715910 (Bytes)
```

```
Session: Tunnel1 192.168.0.4 (inactive)
  Direction: Outbound
  Policy: business
```

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

字段	描述
Session	Hub-Spoke隧道信息，通过Tunnel接口和Spoke侧私网IPv4/IPv6地址可唯一标识一条Hub-Spoke隧道。其中Session: Tunnel1 192.168.0.4 (inactive)中的inactive表示Hub-Spoke隧道应用QoS策略失败或者应用的QoS策略不存在
Direction	QoS策略应用在Hub-Spoke隧道的方向
Matched	符合分类规则的数据包数目

其它显示信息解释请参见 表 1-1 和 表 1-4。

1.3.6 display qos policy control-plane

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

【命令】

集中式设备－独立运行模式：

display qos policy control-plane

分布式设备－独立运行模式/集中式设备－IRF 模式：

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

分布式设备－IRF 模式：

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

slot *slot-number*：显示指定单板的控制平面应用 QoS 策略的信息，*slot-number* 表示单板所在的槽位号。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备的控制平面应用 QoS 策略的信息，*slot-number* 表示设备在 IRF 中的成员编号。（集中式设备－IRF 模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的控制平面应用 QoS 策略的信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。（分布式设备－IRF 模式）

【举例】

显示应用到控制平面的 QoS 策略信息。

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

Control plane

  Direction: Inbound

  Policy: 1
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match not protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark mpls-exp 4
   Classifier: 3
     Operator: AND
     Rule(s) :
      -none-
     Behavior: 3
      -none-
```

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

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

其它显示信息解释请参见 表 1-7。

1.3.7 display qos policy control-plane management

display qos policy control-plane management 命令用于显示管理口控制平面应用的 QoS 策略信息。

【命令】

display qos policy control-plane management

设备各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**display qos policy control-plane management**	不支持
MSR 2600-6-X1/2600-10-X1		不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		不支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**display qos policy control-plane management**	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持

型号	命令	描述
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		不支持

型号	特性	描述
MSR810-LM-GL	**display qos policy control-plane management**	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示对进入管理口控制平面的报文应用的 QoS 策略信息。

```
<Sysname> display qos policy control-plane management

Control plane management

  Direction: Inbound

  Policy: a
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: a
     Matched : 3 (Packets) 180 (Bytes)
```

```
Operator: OR
Rule(s) :
 If-match control-plane protocol arp
 If-match control-plane protocol rip
 If-match control-plane protocol-group critical
 If-match acl 3001
 If-match control-plane protocol bgp
 If-match control-plane protocol bgp4+
 If-match control-plane protocol ftp
 If-match control-plane protocol http https icmp icmp6 ripng snmp
Behavior: a
 Committed Access Rate:
   CIR 128 (kbps), CBS 5120 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 3 (Packets) 180 (Bytes)
   Yellow packets: 0 (Packets) 0 (Bytes)
   Red packets   : 0 (Packets) 0 (Bytes)
```

表1-10 display qos policy control-plane management 命令显示信息描述表

字段	描述
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-7。

1.3.8 display qos policy control-plane management pre-defined

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

【命令】

display qos policy control-plane management pre-defined

设备各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**display qos policy control-plane management pre-defined**	不支持
MSR2600-6-X1/2600-10-X1		不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持

型号	命令	描述
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		不支持
MSR 3610/3620/3620-DP/3640/3660		不支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**display qos policy control-plane management pre-defined**	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		不支持

型号	特性	描述
MSR810-LM-GL	**display qos policy control-plane management pre-defined**	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【举例】

显示系统预定义的管理口控制平面应用 QoS 策略的信息。

```
<Sysname> display qos policy control-plane management pre-defined
Pre-defined policy information
  Protocol          Priority   Bandwidth (kbps)   Group
  Default           N/A        100000             N/A
  ARP               N/A        128                normal
  BGP               N/A        256                critical
  BGPv6             N/A        256                critical
  HTTP              N/A        512                management
  HTTPS             N/A        512                management
  ICMP              N/A        128                monitor
  ICMPv6            N/A        128                monitor
  OSPF Multicast    N/A        256                critical
  OSPF Unicast      N/A        256                critical
  OSPFv3 Multicast  N/A        256                critical
  OSFPv3 Unicast    N/A        256                critical
  RIP               N/A        1024               critical
  RIPng             N/A        256                critical
  SNMP              N/A        512                management
  SSH               N/A        512                management
  TELNET            N/A        512                management
  FTP               N/A        512                management
  TFTP              N/A        512                management
```

表1-11 display qos policy control-plane management pre-defined 命令显示信息描述表

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

1.3.9 display qos policy control-plane pre-defined

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

【命令】

集中式设备—独立运行模式：

display qos policy control-plane pre-defined

分布式设备—独立运行模式/集中式设备—IRF 模式：

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

分布式设备－IRF 模式：

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

slot *slot-number*：显示指定单板的系统预定义的控制平面策略信息，*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示所有在位单板的系统预定义的控制平面应用 QoS 策略的信息。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备的系统预定义的控制平面策略信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示所有成员设备的系统预定义的控制平面应用 QoS 策略的信息。（集中式设备－IRF 模式）

chassis *chassis-numbe*r **slot** *slot-number*：显示指定成员设备上指定单板的系统预定义的控制平面策略信息，*chassis-number* 表示设备在 IRF 中的成员编号，*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系统预定义的控制平面应用 QoS 策略的信息。（分布式设备－IRF 模式）

【举例】

显示 3 号板系统预定义的控制平面应用 QoS 策略的信息。（分布式设备－独立运行模式）

```
<Sysname> display qos policy control-plane pre-defined slot 3
Pre-defined policy information slot 3
  Protocol          Priority   Bandwidth (kbps)   Group
  Default           N/A        100000             N/A
  ARP               N/A        128                normal
  BGP               N/A        256                critical
  BGPv6             N/A        256                critical
  HTTP              N/A        512                management
  HTTPS             N/A        512                management
  ICMP              N/A        128                monitor
  ICMPv6            N/A        128                monitor
  OSPF Multicast    N/A        256                critical
  OSPF Unicast      N/A        256                critical
  OSPFv3 Multicast  N/A        256                critical
  OSFPv3 Unicast    N/A        256                critical
  RIP               N/A        1024               critical
  RIPng             N/A        256                critical
  SNMP              N/A        512                management
  SSH               N/A        512                management
  TELNET            N/A        512                management
  FTP               N/A        512                management
  TFTP              N/A        512                management
```

显示 3 号成员设备系统预定义的控制平面应用 QoS 策略的信息。（集中式设备－IRF 模式）

```
<Sysname> display qos policy control-plane pre-defined slot 3
Pre-defined policy information slot 3
  Protocol          Priority   Bandwidth (kbps)   Group
  Default           N/A        100000             N/A
  ARP               N/A        128                normal
  BGP               N/A        256                critical
  BGPv6             N/A        256                critical
  HTTP              N/A        512                management
  HTTPS             N/A        512                management
  ICMP              N/A        128                monitor
  ICMPv6            N/A        128                monitor
  OSPF Multicast    N/A        256                critical
  OSPF Unicast      N/A        256                critical
  OSPFv3 Multicast  N/A        256                critical
  OSFPv3 Unicast    N/A        256                critical
  RIP               N/A        1024               critical
  RIPng             N/A        256                critical
  SNMP              N/A        512                management
  SSH               N/A        512                management
  TELNET            N/A        512                management
  FTP               N/A        512                management
  TFTP              N/A        512                management
```

显示 1 号成员设备 3 号单板系统预定义的控制平面应用 QoS 策略的信息。（分布式设备－IRF 模式）

```
<Sysname> display qos policy control-plane pre-defined chassis 1 slot 3
Pre-defined policy information chassis 1 slot 3
  Protocol          Priority   Bandwidth (kbps)   Group
  Default           N/A        100000             N/A
  ARP               N/A        128                normal
  BGP               N/A        256                critical
  BGPv6             N/A        256                critical
  HTTP              N/A        512                management
  HTTPS             N/A        512                management
  ICMP              N/A        128                monitor
  ICMPv6            N/A        128                monitor
  OSPF Multicast    N/A        256                critical
  OSPF Unicast      N/A        256                critical
  OSPFv3 Multicast  N/A        256                critical
  OSFPv3 Unicast    N/A        256                critical
  RIP               N/A        1024               critical
  RIPng             N/A        256                critical
  SNMP              N/A        512                management
  SSH               N/A        512                management
  TELNET            N/A        512                management
  FTP               N/A        512                management
  TFTP              N/A        512                management
```

表1-12 display qos policy control-plane pre-defined 命令显示信息描述表

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

1.3.10 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】

集中式设备－独立运行模式：

display qos policy interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] [**inbound** | **outbound**]

分布式设备－独立运行模式/集中式设备－IRF 模式：

display qos policy interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] [**slot** *slot-number*] [**inbound** | **outbound**]

分布式设备－IRF 模式：

display qos policy interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] [**chassis** *chassis-number* **slot** *slot-number*] [**inbound** | **outbound**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

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

pvc { *pvc-name* | *vpi/vci* }：显示指定 ATM 接口上的指定 PVC 的信息，只有当接口为 ATM 接口时才能指定本参数。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。如果未指定本参数，将显示指定 ATM 接口上所有 PVC 的 QoS 策略的配置信息和运行情况。输入本参数时，无法输入参数 **inbound** 或 **outbound**。

slot *slot-number*：显示指定单板上指定接口的 QoS 策略的配置信息和运行情况。*slot-number* 表示单板所在的槽位号。只有当接口为 VLAN 接口、聚合接口等类型时才支持此参数。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备指定接口的 QoS 策略的配置信息和运行情况。*slot-number* 表示设备在 IRF 中的成员编号。只有当接口为 VLAN 虚接口、聚合口等类型时才支持此参数。（集中式设备－IRF 模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的指定接口的 QoS 策略的配置信息和运行情况。*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。只有当接口为 VLAN 虚接口、聚合口等类型时才支持此参数。（分布式设备－IRF 模式）

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。

如果指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS 策略的信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

显示对接口 GigabitEthernet1/0/1 接收到的报文应用 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy interface gigabitethernet 1/0/1 inbound
Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: 1
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
```

```
      Yellow packets: 0 (Packets) 0 (Bytes)
      Red packets   : 0 (Packets) 0 (Bytes)
  Classifier: 2
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     If-match not protocol ipv6
    Behavior: 2
     Accounting enable:
       0 (Packets)
     Filter enable: Permit
     Marking:
       Remark mpls-exp 4
  Classifier: 3
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
     Forwarded: 0/0 (pps/bps)
     Dropped  : 0/0 (pps/bps)
    Operator: AND
    Rule(s) :
     -none-
    Behavior: 3
     -none-
```

显示所有接口上 QoS 策略的接口的配置信息和运行情况。

```
<Sysname>display qos policy interface
Interface: GigabitEthernet5/0/1
  Direction: Inbound
  Policy: a
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: a
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: a
      Mirroring:
        Mirror to the interface: GigabitEthernet5/0/10
```

```
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)

Interface: GigabitEthernet5/0/17
  Direction: Inbound
  Policy: b
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: b
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: b
      Committed Access Rate:
        CIR 200 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0(Packets)
        Red packets   : 0 (Packets)

Interface: GigabitEthernet5/0/17
  Direction: Inbound
  Policy: a
   Classifier: default-class
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match any
     Behavior: be
      -none-
   Classifier: a
```

```
Operator: AND
Rule(s) :
 If-match any
Behavior: a
 Mirroring:
   Mirror to the interface: GigabitEthernet5/0/10
 Committed Access Rate:
   CIR 112 (kbps), CBS 5120 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets)
   Red packets   : 0 (Packets)
```

表1-13 display qos policy interface 命令显示信息描述表

字段	描述
Direction	Policy应用在接口的方向
Matched	符合分类规则的数据包数目
5-minute statistics	最近5分钟的流速统计信息
Forwarded	符合分类规则的成功转发报文在统计周期内的平均速率
Dropped	符合分类规则的丢弃报文在统计周期内的平均速率
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-1 和 表 1-4。

1.3.11 display qos policy l2vpn-pw

display qos policy l2vpn-pw 命令用来显示 L2VPN PW 上 QoS 策略的配置信息和运行情况。

【命令】

display qos policy l2vpn-pw [**peer** *ip-address* **pw-id** *pw-id*] [**outbound**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

peer *ip-address* **pw-id** *pw-id*：显示指定 PW 上的 QoS 策略的配置信息和运行情况。*ip-address* 为 PW 远端 PE 的 LSR ID。*pw-id* 为 PW 的 PW ID，取值范围为 1～4294967295。若未指定本参数，则显示所有 PW 上的 QoS 策略的配置信息和运行情况。

outbound：显示对 PW 发送的报文应用的 QoS 策略的信息。

【使用指导】

如果未指定显示方向，则显示出方向 PW 上应用 QoS 策略的配置信息和运行情况。

【举例】

显示远端 PE 地址为 1.1.1.1、PW ID 为 1 的 PW 发送报文方向上应用的 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy l2vpn-pw peer 1.1.1.1 pw-id 1 outbound

L2VPN-PW: peer 1.1.1.1, pw-id 1

  Direction: Outbound

  Policy: 1
   Classifier: 1
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Yellow packets: 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Matched : 0 (Packets) 0 (Bytes)
     5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
     Operator: AND
     Rule(s) :
      If-match not protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark mpls-exp 4
```

```
Classifier: 3
  Matched : 0 (Packets) 0 (Bytes)
  5-minute statistics:
   Forwarded: 0/0 (pps/bps)
   Dropped  : 0/0 (pps/bps)
  Operator: AND
  Rule(s) :
   -none-
  Behavior: 3
   -none-
```

表1-14 display qos policy l2vpn-pw 命令显示信息描述表

字段	描述
L2VPN-PW	显示指定PW的信息，PW通过远端PE地址和PW ID唯一标识
Direction	Policy应用在PW的方向
Matched	符合分类规则的数据包数目
5-minute statistics	最近5分钟的流速统计信息
Forwarded	符合分类规则的成功转发报文在统计周期内的平均速率
Dropped	符合分类规则的丢弃报文在统计周期内的平均速率
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-1 和 表 1-4。

1.3.12 display qos policy user-profile

display qos policy user-profile 命令用来显示用户上线后 User Profile 下应用的 QoS 策略的信息和运行情况。

【命令】

集中式设备－独立运行模式：

display qos policy user-profile [**name** *profile-name*] [**user-id** *user-id*] [**inbound** | **outbound**]

分布式设备－独立运行模式/集中式设备－IRF 模式：

display qos policy user-profile [**name** *profile-name*] [**user-id** *user-id*] [**slot** *slot-number*] [**inbound** | **outbound**]

分布式设备－IRF 模式：

display qos policy user-profile [**name** *profile-name*] [**user-id** *user-id*] [**chassis** *chassis-number* **slot** *slot-number*] [**inbound** | **outbound**]

设备各款型对于本节所描述的命令支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**display qos policy user-profile**	仅MSR810-LMS/810-LUS不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**display qos policy user-profile**	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**display qos policy user-profile**	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

name *profile-name*：指定 User Profile 的名称，为 1～31 个字符的字符串，只能包含英文字母[a-z,A-Z]、数字、下划线，且必须以英文字母开始，区分大小写。User Profile 的名称必须全局唯一。如果未指定本参数，将显示所有 User Profile 下应用的 QoS 策略的信息和运行情况。

user-id *user-id*：表示在线用户的 ID，为系统所分配，为十六进制数。若未指定本参数，则显示所有用户在 User Profile 下应用的 QoS 策略的信息和运行情况。

slot *slot-number*：显示指定单板上指定用户在 User Profile 下应用的 QoS 策略的信息和运行情况，*slot-number* 表示单板所在的槽位号。如果未指定本参数，将显示所有单板上的在线用户的 QoS 策略的信息和运行情况。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备上指定用户在 User Profile 下应用的 QoS 策略的信息和运行情况，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示所有成员设备上的在线用户上指定用户在 User Profile 下应用的 QoS 策略的信息和运行情况。（集中式设备－IRF 模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备指定单板上指定用户在 User Profile 下应用的 QoS 策略的信息和运行情况，*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。如果未指定本参数，将显示所有成员设备所有单板上指定用户在 User Profile 下应用的 QoS 策略的信息和运行情况。（分布式设备－IRF 模式）

inbound：显示在线用户在入方向上应用 QoS 策略的信息。

outbound：显示在线用户在出方向上应用 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上应用 QoS 策略的配置信息和运行情况。

【举例】

显示指定全局用户（从聚合口等全局口上线的用户）在 User Profile 下应用 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy user-profile name abc user-id 30000000 inbound
User-Profile: abc
  User ID: 0x30000000(global)
    Direction: Inbound
    Policy: p1
     Classifier: default-class
       Matched : 0 (Packets) 0 (Bytes)
       Operator: AND
       Rule(s) :
        If-match any
       Behavior: be
        -none-
```

显示指定的非全局用户在 User Profile 下应用 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy user-profile name abc user-id 30000001 inbound
User-Profile: abc
  slot 2:
    User ID: 0x30000001(local)
      Direction: Inbound
      Policy: p1
       Classifier: default-class
         Matched : 0 (Packets) 0 (Bytes)
         Operator: AND
         Rule(s) :
          If-match any
         Behavior: be
           -none-
```

显示指定 User Profile 下所有用户的 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy user-profile name abc inbound
User-Profile: abc
  User ID: 0x30000000(global)
    Direction: Inbound
    Policy: p1
     Classifier: default-class
       Matched : 0 (Packets) 0 (Bytes)
       Operator: AND
       Rule(s) :
        If-match any
       Behavior: be
        -none-

  slot 2:
    User ID: 0x30000001(local)
      Direction: Inbound
      Policy: p1
       Classifier: default-class
         Matched : 0 (Packets) 0 (Bytes)
         Operator: AND
         Rule(s) :
          If-match any
         Behavior: be
           -none-

  slot 3:
    User ID: 0x30000002(local)
      Direction: Inbound
      Policy: p1
       Classifier: default-class
         Matched : 0 (Packets) 0 (Bytes)
         Operator: AND
         Rule(s) :
```

```
          If-match any
         Behavior: be
          -none-
```

显示指定单板上所有用户在 User Profile abc 下应用 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy user-profile name abc slot 2
User-Profile: abc
User ID: 0x30000000(global)
    Direction: Inbound
    Policy: p1
     Classifier: default-class
       Matched : 0 (Packets) 0 (Bytes)
       Operator: AND
       Rule(s) :
        If-match any
       Behavior: be
        -none-

  User ID: 0x30000001(local)
    Direction: Inbound
    Policy: p1
     Classifier: default-class
       Matched : 0 (Packets) 0 (Bytes)
       Operator: AND
       Rule(s) :
        If-match any
       Behavior: be
        -none-
```

#显示所有单板上指定用户在 User Profile abc 下应用 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy user-profile name abc user-id 30000001
User-Profile: abc
  slot 2:
    User ID: 0x30000001(local)
      Direction: Inbound
      Policy: p1
       Classifier: default-class
         Matched : 0 (Packets) 0 (Bytes)
         Operator: AND
         Rule(s) :
          If-match any
         Behavior: be
          -none-

  slot 3:
    User ID: 0x30000001(local)
      Direction: Inbound
      Policy: p1
       Classifier: default-class
         Matched : 0 (Packets) 0 (Bytes)
```

```
        Operator: AND
        Rule(s) :
         If-match any
        Behavior: be
         -none-
```

显示所有 User Profile 的在线用户的 QoS 策略的配置信息和运行情况。

```
<Sysname> display qos policy user-profile
User-Profile: abc
  slot 3:
    User ID: 0x30000000(local)
      Direction: Inbound
      Policy: p1
       Classifier: default-class
         Matched : 0 (Packets) 0 (Bytes)
         Operator: AND
         Rule(s) :
          If-match any
         Behavior: be
          -none-

User-Profile: a12
  slot 4:
    User ID: 0x30000001(local)
      Direction: Inbound
      Policy: p1
       Classifier: default-class
         Matched : 0 (Packets) 0 (Bytes)
         Operator: AND
         Rule(s) :
          If-match any
         Behavior: be
          -none-
       Classifier: a
        Operator: AND
        Rule(s) :
         If-match any
        Behavior: a
         Mirroring:
          Mirror to the interface: GigabitEthernet1/0/1
         Committed Access Rate:
           CIR 112 (kbps), CBS 5120 (Bytes), EBS 0 (Bytes)
           Green action  : pass
           Yellow action : pass
           Red action    : discard
           Green packets : 0 (Packets)
           Red packets   : 0 (Packets)
```

表1-15 display qos policy user-profile 命令显示信息描述表

字段	描述
User-Profile	User Profile名称
User ID	上线用户的ID
global	该用户从聚合口等全局口上线
local	该用户从物理口上线
Mirror to the interface	镜像到接口
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
PIR	峰值信息速率
Direction	Policy应用在User Profile的方向
Matched	符合分类规则的数据包数目
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-1 和 表 1-4。

1.3.13 qos apply policy (interface view, PVC view, control plane view, control plane management view,PW view)

qos apply policy 命令用来在接口、PVC、PW、控制平面或管理口控制平面上应用 QoS 策略。

undo qos apply policy 命令用来取消接口、PVC、PW、控制平面或管理口控制平面上应用的 QoS 策略。

【命令】

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

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

【缺省情况】

未应用 QoS 策略。

【视图】

接口视图/PVC 视图/控制平面视图/管理口控制平面视图/交叉连接 PW 视图/VSI LDP PW 视图/VSI 静态 PW 视图

【缺省用户角色】

network-admin

【参数】

policy-name：策略名，为 1～31 个字符的字符串，区分大小写。

inbound：对接口或控制平面或管理口控制平面接收到的报文应用 QoS 策略。

outbound：对接口发送的报文应用 QoS 策略。

【使用指导】

策略在接口、PVC 或 PW 上应用的规则如下：

- 在应用策略时，如果策略中为确保转发和加速转发的类指定的带宽之和超过接口、PVC 或 PW 允许的可用带宽，则在该接口、PVC 或 PW 不可应用。如果对接口、PVC 或 PW 修改了可用带宽，此时如果策略中为确保转发和加速转发的类指定的带宽之和超过接口、PVC 或 PW 允许的可用带宽，则将策略删除。
- 入方向的策略与类关联的行为不允许有 **queue af**、**queue ef** 与 **queue wfq** 配置，也不允许有 GTS 配置。

在控制平面和管理口控制平面上应用策略时，不支持配置了 CBQ 的策略。

在 PW 下应用策略时，只能应用在 PW 的出方向上。

【举例】

将策略 USER1 应用到接口 GigabitEthernet1/0/1 的入方向上。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/1] qos apply policy USER1 inbound
```

对进入 3 号槽控制平面的报文应用策略 aaa。

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

对进入管理口控制平面的报文应用策略 bbb。

```
<Sysname> system-view
[Sysname] control-plane management
[Sysname-cp-management] qos apply policy bbb inbound
```

在 PW 的出方向上应用策略。

```
<Sysname> system-view
[Sysname] xconnect-group a
[Sysname-xcg-a] connection a
[Sysname-xcg-a-a] peer 1.1.1.1 pw-id 1
[Sysname-xcg-a-a-1.1.1.1-1] qos apply policy 1 outbound
```

1.3.14 qos apply policy (user-profile view)

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

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

【命令】

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

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

设备各款型对于本节所描述的命令支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**qos apply policy**	仅MSR810-LMS/810-LUS不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**qos apply policy**	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**qos apply policy**	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

【缺省情况】

未在 User Profile 下应用 QoS 策略。

【视图】

User Profile 视图

【缺省用户角色】

network-admin

【参数】

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

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

policy-name：策略名，为 1～31 个字符的字符串。

【使用指导】

User Profile 被删除将导致其下引用的 QoS 策略被删除。

【举例】

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

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

1.3.15 qos policy

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

undo qos policy 命令用来删除一个策略。

【命令】

qos policy *policy-name*

undo qos policy *policy-name*

【缺省情况】

不存在策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【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**

1.3.16 reset qos policy advpn

reset qos policy advpn 命令用来清除 Tunnel 接口 Hub-Spoke 隧道应用 QoS 策略的统计信息。

【命令】

reset qos policy advpn tunnel *number* [*ipv4-address* | *ipv6-address*] [**outbound**]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

number：Tunnel 接口编号，取值范围为已创建的接口编号。

Ipv4-address：隧道 Spoke 侧的 IPv4 私网地址。

ipv6-address：隧道 Spoke 侧的 IPv6 私网地址。

outbound：清除 Hub-Spoke 隧道出方向应用 QoS 策略的统计信息。

【使用指导】

如果未指定隧道 Spoke 侧的私网地址，则清除 Tunnel 接口下所有 Hub-Spoke 隧道应用 QoS 策略的统计信息。有关 Hub-Spoke 隧道的详细介绍，请参见“三层技术—IP 业务配置指导”中的“ADVPN 配置”。

如果未指定方向，则同时清除 Hub-Spoke 隧道接口出入两个方向应用 QoS 策略的统计信息。

【举例】

清除 Tunnel 接口下指定 Hub-Spoke 隧道出方向应用 QoS 策略的统计信息。

```
<Sysname> reset qos policy advpn tunnel 1 192.168.0.3 outbound
```

1.3.17 reset qos policy control-plane

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

【命令】

集中式设备—独立运行模式：

reset qos policy control-plane

分布式设备—独立运行模式/集中式设备—IRF 模式：

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

分布式设备－IRF 模式：

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

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

slot *slot-number*：清除指定单板的基于控制平面应用 QoS 策略的统计信息，*slot-number* 表示单板所在的槽位号。（分布式设备－独立运行模式）

slot *slot-number*：清除指定成员设备的基于控制平面应用 QoS 策略的统计信息，*slot-number* 表示设备在 IRF 中的成员编号。（集中式设备－IRF 模式）

chassis *chassis-number* **slot** *slot-number*：清除指定成员设备上指定单板的基于控制平面应用 QoS 策略的统计信息，*chassis-number* 表示设备在 IRF 中的成员编号，*slot-number* 表示单板所在的槽位号。（分布式设备－IRF 模式）

【举例】

清除控制平面的 QoS 策略统计信息。（集中式设备－独立运行模式）

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

清除应用到 3 号板控制平面的 QoS 策略统计信息。（分布式设备－独立运行模式）

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

清除应用到 3 号成员设备控制平面的 QoS 策略统计信息。（集中式设备－IRF 模式）

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

清除应用到 1 号成员设备 3 号板控制平面的 QoS 策略统计信息。（分布式设备－IRF 模式）

```
<Sysname> reset qos policy control-plane chassis 1 slot 3
```

1.3.18 reset qos policy control-plane management

reset qos policy control-plane management 命令用来清除管理口控制平面 QoS 策略的统计信息。

【命令】

reset qos policy control-plane management

设备各款型对于本节所描述的命令及参数的支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**reset qos policy control-plane management**	不支持
MSR2600-6-X1/2600-10-X1		不支持
MSR 2630		不支持
MSR3600-28/3600-51		不支持
MSR3600-28-SI/3600-51-SI		不支持
MSR		不支持

型号	命令	描述
3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		
MSR 3610/3620/3620-DP/3640/3660		不支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**reset qos policy control-plane management**	不支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		不支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		不支持
MSR2600-10-X1-WiNet		不支持
MSR2630-WiNet		不支持
MSR3600-28-WiNet		不支持
MSR3610-X1-WiNet		不支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		不支持

型号	特性	描述
MSR810-LM-GL	**reset qos policy control-plane management**	不支持
MSR810-W-LM-GL		不支持
MSR830-6EI-GL		不支持
MSR830-10EI-GL		不支持
MSR830-6HI-GL		不支持
MSR830-10HI-GL		不支持
MSR2600-6-X1-GL		不支持
MSR3600-28-SI-GL		不支持

【视图】

用户视图

【缺省用户角色】

network-admin

【举例】

清除管理口控制平面 QoS 策略的统计信息。

```
<Sysname> reset qos policy control-plane management
```

1.4 接口流速统计配置命令

1.4.1 qos flow-interval

qos flow-interval 命令用来配置接口流速统计时间。

undo qos flow-interval 命令用来恢复缺省情况。

【命令】

qos flow-interval *interval*

undo qos flow-interval

【缺省情况】

接口流速统计时间为 5 分钟。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

interval：流速统计时间，取值范围为 1～10 单位为分钟。

【使用指导】

配置本命令后，设备将以设置的统计时间为周期，统计周期内经过 QoS 策略流分类后每类报文的发送和丢弃速率，并以 t/5 为刷新周期定期刷新统计速率。

子接口的流速统计时间采用主接口的统计时间。

【举例】

配置接口 GigabitEthernet1/0/1 的流速统计时间为 10 分钟。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos flow-interval 10
```

【相关命令】

- **display qos policy interface**

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-lp** | **dscp-lp** | **lp-dot1p** | **lp-dscp**]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

表2-1 优先级映射表

优先级映射	描述
dot1p-lp	802.1p优先级到本地优先级映射表
dscp-lp	DSCP到本地优先级映射表
lp-dot1p	本地优先级到802.1p优先级映射表
lp-dscp	本地优先级到DSCP映射表

【使用指导】

如果未指定表的类型，将显示所有映射表的配置情况。

如果未指定方向，将显示所有方向的映射表的配置情况。

如果未指定任何参数，即 **display qos map-table** 命令将显示所有映射表（以及带颜色映射表）的配置情况。

【举例】

显示 802.1p 优先级到本地优先级映射表的配置信息。

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

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

表2-2 display qos map-table 命令显示信息描述表

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

2.1.2 import (priority map view)

import 命令用来配置指定优先级映射表的映射关系。

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

【命令】

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

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

【缺省情况】

优先级映射表的映射关系请参见配置指导中的附录 B。

【视图】

优先级映射表视图

【缺省用户角色】

network-admin

【参数】

import-value-list：输入值列表。

export-value：输出值。

all：删除配置地该映射表的所有映射关系，恢复其为缺省的映射关系。

【举例】

配置 802.1p 优先级到本地优先级映射表的映射关系，与 802.1p 优先级 4、5 相对应的本地优先级为 1。

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

【相关命令】

- **display qos map-table**
- **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-lp** | **dscp-lp** | **lp-dot1p** | **lp-dscp** }

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

其它参数请参见 表 2-1。

【举例】

进入 802.1p 优先级到本地优先级映射表视图。

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

【相关命令】

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

2.2 端口优先级配置命令

本特性仅在安装了二层交换卡的款型和如下款型的固定二层接口上支持。

描述	款型
固定二层接口	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR810-W-WiNet/810-LM-WiNet • MSR830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet • MSR3600-28-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL

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

【缺省用户角色】

network-admin

【参数】

priority-value：端口优先级值，取值范围为 0～7。

【举例】

配置接口 GigabitEthernet1/0/1 的端口优先级为 2。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] 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

本特性仅在安装了二层交换卡的款型和如下款型的固定二层接口上支持。

描述	款型
固定二层接口	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR810-W-WiNet/810-LM-WiNet • MSR830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet • MSR3600-28-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL

描述	款型
	• MSR2600-6-X1-GL/3600-28-SI-GL

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

【参数】

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

【举例】

显示当前配置的端口优先级信任模式信息（支持一种类型端口优先级的设备）。

```
<Sysname> display qos trust interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Port priority trust information
  Port priority:4
  Port priority trust type: dot1p,
```

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
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】

没有配置端口优先级信任模式。

【视图】

二层以太网接口视图

【缺省用户角色】

network-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。该参数仅在安装了 SIC-4GSW、SIC-4GSWP、SIC-4GSWF、HMIM-8GSWF、HMIM-24GSW/24GSWP 和 HMIM-8GSW 交换卡的款型以及 MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS/2600-6-X1/2600-10-X1/2630/3600-28/3600-51/3600-28-SI/3600-51-SI/3610/3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC/3620/3620-DP/3640/3660/810-W-WiNet/810-LM-WiNet/830-4LM-WiNet/830-5BEI-WiNet/830-6EI-WiNet/830-6BHI-WiNet/830-10BHI-WiNet/830-10BEI-WiNet/2600-10-X1-WiNet/2630-WiNet/3600-28-WiNet/3610-X1-WiNet/3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet/810-LM-GL/810-W-LM-GL/830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL/2600-6-X1-GL/3600-28-SI-GL 的固定二层接口上支持

【举例】

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

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

【相关命令】

- **display qos trust interface**

3 流量监管、流量整形和限速

说明

仅 MSR810-LMS/810-LUS/830-4LM-WiNet/3600-28-SI/3600-51-SI 不支持 l2vpn-pw。

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

3.1 流量监管配置命令

3.1.1 display qos car interface

display qos car interface 命令用来显示接口的流量监管配置情况和统计信息。

【命令】

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

【视图】

任意视图

【缺省级别】

network-admin

network-operator

【参数】

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

【举例】

显示接口 GigabitEthernet1/0/1 的流量监管配置情况和统计信息。

```
<Sysname> display qos car interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
 Direction: inbound
  Rule: If-match any
   CIR 128 (kbps), CBS 5120 (Bytes), PIR 128 (kbps), EBS 512 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
```

显示接口 GigabitEthernet1/0/2 的流量监管配置情况和统计信息。

```
<Sysname> display qos car interface gigabitethernet 1/0/2
Interface: GigabitEthernet1/0/2
 Direction: inbound
  Rule: If-match any
   CIR 50 (%), CBS 600 (ms), EBS 0 (ms), PIR 50 (%)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets), 0 (Bytes)
   Yellow packets: 0 (Packets), 0 (Bytes)
   Red packets   : 0 (Packets), 0 (Bytes)
```

表3-1 display qos car 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
Direction	指定流量监管的方向
Rule	数据包的匹配规则
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，单位为byte，实际的CBS值是*cbs-time* 乘以实际的承诺信息速率（**cir**值乘以接口带宽）
EBS	超出突发尺寸，单位为byte，实际的EBS值是*ebs-time* 乘以实际的承诺信息速率（**cir**值乘以接口带宽）
PIR	峰值信息速率，单位为kbps
Green action	对绿色报文的动作
Yellow action	对黄色报文的动作

字段	描述
Red action	对红色报文的动作
Green packets	绿色报文的流量统计
Yellow packets	黄色报文的流量统计
Red packets	红色报文的流量统计

3.1.2 display qos carl

display qos carl 命令用来显示 CAR 列表。

【命令】

集中式设备－独立运行模式：

display qos carl [*carl-index*]

分布式设备－独立运行模式/集中式设备－IRF 模式：

display qos carl [*carl-index*] [**slot** *slot-number*]

分布式设备－IRF 模式：

display qos carl [*carl-index*] [**chassis** *chassis-number* **slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

carl-index：CAR 列表的号码，取值范围为 1～199。如果未指定本参数，将显示所有的 CAR 列表。

slot *slot-number*：显示指定单板的 CAR 列表信息，*slot-number* 表示单板所在的槽位号。如果未指定本参数，则显示主用主控板的 CAR 列表的配置信息。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备的 CAR 列表信息，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，则显示主用设备的 CAR 列表的配置信息。（集中式设备－IRF 模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的 CAR 列表信息，*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，则显全局主用主控板上的 CAR 列表的配置信息。（分布式设备－IRF 模式）

【举例】

显示所有的 CAR 列表。

```
<Sysname> display qos carl
List  Rules
1     destination-ip-address range 1.1.1.1 to 1.1.1.2 per-address shared-bandwidth
2     destination-ip-address subnet 1.1.1.1 22 per-address shared-bandwidth
4     dscp 1 2 3 4 5 6 7 cs1
5     mac 0000-0000-0000
```

```
6     mpls-exp 0 1 2
9     precedence 0 1 2 3 4 5 6 7
10    source-ip-address range 1.1.1.1 to 1.1.1.2
11    source-ip-address subnet 1.1.1.1 31
```

表3-2 display qos carl 命令显示信息描述表

字段	描述
List	CAR列表号码
Rules	数据包的匹配规则

3.1.3 qos car (interface view)

qos car 命令用来在接口上配置流量监管。

undo qos car 命令用来取消接口上流量监管的配置。

【命令】

qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* | **carl** *carl-index* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action* | **red** *action* | **yellow** *action*] *

qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* | **carl** *carl-index* } **cir** *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

undo qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* | **carl** *carl-index* }

【缺省情况】

未配置流量监管。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

inbound：对接口接收到的数据包进行流量监管。

outbound：对接口发送的数据包进行流量监管。

any：对所有的 IP 数据包进行流量监管。

acl [**ipv6**] *acl-number*：对匹配 ACL 的数据包进行流量监管。*acl-number* 为 ACL 编号，取值范围为 2000～3999。若未指定 **ipv6** 关键字，表示 IPv4 ACL；否则表示 IPv6 ACL。

carl *carl-index*：对匹配 CAR 列表的数据包进行限速。*carl-index* 为承诺访问速率列表编号，取值范围为 1～199。

cir *committed-information-rate*：承诺信息速率，单位为 kbps，取值范围为 8～10000000。

cbs *committed-burst-size*：承诺突发尺寸，即实际平均速率在承诺速率以内时的突发流量，单位为 byte，取值范围为 1000～1000000000。

ebs *excess-burst-size*：过度突发尺寸，单位为 byte，取值范围为 0～1000000000。

pir *peak-information-rate*：峰值速率，单位为 kbps，取值范围为 8～10000000。

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

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

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

action：对数据包采取的动作，有以下几种：

- **continue**：继续由下一个 CAR 策略处理。
- **discard**：丢弃数据包。
- **pass**：允许数据包通过。
- **remark-dot1p-continue** *new-cos*：设置新的 802.1P 报文的优先级值，并继续由下一个 CAR 策略处理，取值范围为 0～7。
- **remark-dot1p-pass** *new-cos*：设置新的 802.1P 报文的优先级值，并允许数据包通过，取值范围为 0～7。
- **remark-dscp-continue** *new-dscp*：设置报文新的 DSCP 值，并继续由下一个 CAR 策略处理，取值范围为 0～63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。
- **remark-dscp-pass** *new-dscp*：设置报文新的 DSCP 值，并允许数据包通过，取值范围为 0～63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。
- **remark-mpls-exp-continue** *new-exp*：设置新的 MPLS 报文的 EXP 标志位的值，并继续由下一个 CAR 策略处理，取值范围为 0～7。
- **remark-mpls-exp-pass** *new-exp*：设置新的 MPLS 报文的 EXP 标志位的值，并允许数据包通过，取值范围为 0～7。
- **remark-prec-continue** *new-precedence*：设置新的 IP 优先级，并继续由下一个 CAR 策略处理，取值范围为 0～7。
- **remark-prec-pass** *new-precedence*：设置新的 IP 优先级，并允许数据包通过，取值范围为 0～7。

【使用指导】

在同一个接口上重复执行本命令可以配置多个 CAR 策略，策略的执行顺序与配置的先后顺序一致。

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。

【举例】

在接口 GigabitEthernet1/0/1 的出方向上对满足 ANY 规则的报文进行流量监管。报文正常流速为 200kbps，在第一时间可以有大于正常流量的突发流量通过，以后速率小于等于 200kbps 时正常发送，大于 200kbps 时，报文优先级改为 0 并发送。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos car outbound any cir 200 cbs 5120 ebs 0 green pass red
remark-prec-pass 0
```

【相关命令】

- **display qos car interface**
- **qos carl**

3.1.4 qos car any(user-profile view)

qos car any 命令用来在 User Profile 下对所有 IP 数据包配置流量监管。

undo qos car 命令用来取消流量监管的配置。

【命令】

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

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

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

设备各款型对于本节所描述的命令支持情况有所不同，详细差异信息如下：

型号	命令	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	**qos car** { **inbound** | **outbound** } **any cir** *committed-information-rate*	仅MSR810-LMS/810-LUS不支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	**qos car** { **inbound** | **outbound** } **any cir** *committed-information-rate*	支持
MSR830-4LM-WiNet		不支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持

型号	命令	描述
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	**qos car** { **inbound** | **outbound** } **any cir** *committed-information-rate*	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

【缺省情况】

未配置流量监管。

【视图】

User Profile 视图

【缺省用户角色】

network-admin

【参数】

inbound：对上线用户发送的报文进行限速。

outbound：对上线用户接收到的报文进行限速。

cir *committed-information-rate*：承诺信息速率，单位为 kbps，取值范围为 8～10000000。

cbs *committed-burst-size*：承诺突发尺寸，即实际平均速率在承诺速率以内时的突发流量，单位为 byte，取值范围为 1000～1000000000。

ebs *excess-burst-size*：过度突发尺寸，单位为 byte，缺省值为 0 byte，取值范围为 0～1000000000。

pir *peak-information-rate*：峰值速率，单位为 kbps，取值范围为 8～10000000。

【使用指导】

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

多次执行本命令，最后一次执行的命令生效。

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。

【举例】

对上线用户 user 接收的报文进行流量监管。报文正常流速为 200kbps，允许 51200byte 的突发流量通过，速率小于等于 200kbps 时正常发送，大于 200kbps 时，报文被丢弃。

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

```
[Sysname] user-profile user
[Sysname-user-profile-user] qos car outbound any cir 200 cbs 51200
```

3.1.5 qos carl

qos carl 命令用来创建或修改 CAR 列表。

undo qos carl 命令用来删除 CAR 列表。

【命令】

qos carl *carl-index* { **dscp** *dscp-list* | **mac** *mac-address* | **mpls-exp** *mpls-exp-value* | **precedence** *precedence-value* | { **destination-ip-address** | **source-ip-address** } { **range** *start-ip-address* **to** *end-ip-address* | **subnet** *ip-address mask-length* } [**per-address** [**shared-bandwidth**]] }

undo qos carl *carl-index*

【缺省情况】

未配置 CAR 列表。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

carl-index：CAR 列表号码，取值范围为 1～199。

dscp *dscp-list*：DSCP 取值列表。DSCP 为区分服务编码点，用数字表示时，取值范围为 0～63；用文字表示时，可以选取 **af11**、**af12**、**af13**、**af21**、**af22**、**af23**、**af31**、**af32**、**af33**、**af41**、**af42**、**af43**、**cs1**、**cs2**、**cs3**、**cs4**、**cs5**、**cs6**、**cs7**、**default**、**ef**。可以配置多个 DSCP 值，最多可指定 8 个；如果指定了多个相同的 DSCP 值，系统默认为一个；多个不同的 DSCP 值是或的关系，即只要有一个值匹配，就算匹配这条规则。

mac *mac-address*：16 进制的 MAC 地址。

mpls-exp *mpls-exp-value*：MPLS EXP 优先级，取值范围为 0～7。可以配置多个 MPLS EXP 值，最多可指定 8 个；如果指定了多个相同的 MPLS EXP 值，系统默认为一个；多个不同的 MPLS EXP 值是或的关系，即只要有一个值匹配，就算匹配这条规则。

precedence *precedence-value*：优先级，取值范围为 0～7。可以配置多个 **precedence** 值，最多可指定 8 个；如果指定了多个相同的 **precedence** 值，系统默认为一个；多个不同的 **precedence** 值是或的关系，即只要有一个值匹配，就算匹配这条规则。

destination-ip-address：基于目的 IP 地址的 CAR 列表。

source-ip-address：基于源 IP 地址的 CAR 列表。

range *start-ip-address* **to** *end-ip-address*：IP 地址段起始地址和 IP 地址段终止地址。*end-ip-address* 必须大于 *start-ip-addres*。**range** 指定的 IP 地址数量上限为 1024。

subnet *ip-address mask-length*：IP 子网地址和 IP 子网地址掩码长度，取值范围为 22～31。

per-address：表示对网段内逐 IP 地址流量进行限速，cir 为各 IP 地址独享的限制带宽，不能被网段内其他 IP 流量共享。如果未指定本参数，将对整个网段的流量进行限速，cir 为该网段内所有 IP 地址带宽之和，各个 IP 地址带宽按照流量大小的比例进行分配。

shared-bandwidth：表示网段内存在流量的 IP 地址均分配置的共享带宽，cir 为该网段内所有 IP 地址共享带宽，根据当前存在流量的 IP 地址数量，动态平均分配各 IP 地址占用的带宽。

【使用指导】

可以选择基于优先级、基于 MAC 地址、基于 MPLS EXP 优先级、基于 DSCP 或基于 IP 网段建立 CAR 列表。

重复执行本命令时，如果 *carl-index* 取值不同，将创建多个 CAR 列表；如果 *carl-index* 取值相同，则表示修改指定 CAR 列表的参数。

指定单个 IP 地址限速请使用接口视图下 **qos car acl** 命令配置。

【举例】

在接口 GigabitEthernet1/0/1 的出方向上应用 CAR 列表 1。CAR 列表 1 是对源地址属于子网 1.1.1.0/24 内每台主机限速 100kbps，网段内各 IP 地址的流量不共享剩余带宽。

```
<Sysname> system-view
[Sysname] qos carl 1 source-ip-address subnet 1.1.1.0 24 per-address
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos car outbound carl 1 cir 100 cbs 6250 ebs 0 green pass red discard
```

在接口 GigabitEthernet1/0/1 的出方向上应用 CAR 列表 2。CAR 列表 2 是对源地址属于 IP 地址段 1.1.2.100～1.1.2.199 内所有主机限速 5Mbps，网段内各 IP 地址的流量共享剩余带宽。

```
<Sysname> system-view
[Sysname] qos carl 2 source-ip-address range 1.1.2.100 to 1.1.2.199 per-address shared-bandwidth
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos car outbound carl 2 cir 5000 cbs 3125 ebs 31250 green pass red discard
```

【相关命令】

- **display qos carl**
- **qos car**

3.2 流量整形配置命令

3.2.1 display qos gts interface

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【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: GigabitEthernet1/0/1
 Rule: If-match acl 2001
  CIR 200 (kbps), CBS 51200 (Bytes), PIR 51200 (kbps), EBS 0 (Bytes)
  Queue Length: 100 (Packets)
  Queue Size: 70 (Packets)
  Passed   : 0 (Packets) 0 (Bytes)
  Discarded: 0 (Packets) 0 (Bytes)
  Delayed  : 0 (Packets) 0 (Bytes)

Interface: GigabitEthernet1/0/2
 Rule: If-match acl 2001
  CIR 50 (%), CBS 600 (ms), EBS 0 (ms)
  Queue Length: 100 (Packets)
  Queue Size: 70 (Packets)
  Passed   : 0 (Packets) 0 (Bytes)
  Discarded: 0 (Packets) 0 (Bytes)
  Delayed  : 0 (Packets) 0 (Bytes)
```

表3-3 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，单位为byte，实际的CBS值是*cbs-time* 乘以实际的承诺信息速率（**cir** 值乘以接口带宽）
EBS	超出突发尺寸，单位为byte，实际的EBS值是*ebs-time* 乘以实际的承诺信息速率（**cir** 值乘以接口带宽）
PIR	峰值速率，单位为kbps
Queue Length	缓冲队列能够容纳的数据包的个数
Queue Size	当前缓冲区中数据包的数目
Passed	已经通过的数据包数目和字节数
Discarded	被丢弃的数据包数目和字节数
Delayed	被延迟发送的数据包数目和字节数

3.2.2 qos gts

qos gts 命令用来在接口上配置流量整形。

undo qos gts 命令用来取消接口上流量整形的配置。

【命令】

qos gts { **any** | **acl** [**ipv6**] *acl-number* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**queue-length** *queue-length*]

qos gts { **any** | **acl** [**ipv6**] *acl-number* } **cir** *committed-information-rate* [**cbs** *committed-burst-size*] **pir** *peak-information-rate* [**ebs** *excess-burst-size*] [**queue-length** *queue-length*]

undo qos gts { **any** | **acl** [**ipv6**] *acl-number* }

【缺省情况】

未配置流量整形。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

any：对所有的数据包进行流量整形。

acl [**ipv6**] *acl-number*：对匹配 ACL 的数据包进行流量整形。*acl-number* 为 ACL 编号，取值范围为 2000～3999。若未指定 **ipv6** 关键字，表示 IPv4 ACL；否则表示 IPv6 ACL。

cir *committed-information-rate*：承诺信息速率，单位为 kbps，取值范围为 8～10000000。

cbs *committed-burst-size*：承诺突发尺寸，单位为 byte，取值范围为 1000～1000000000。

ebs *excess-burst-size*：超出突发尺寸，在双令牌桶算法中超出承诺突发流量的部分，单位为 byte，取值范围为 0～1000000000。

pir *peak-information-rate*：峰值速率，单位为 kbps。PIR 必须大于等于 CIR，取值范围为 8～10000000。

queue-length *queue-length*：缓存队列的最大长度。

【使用指导】

不配置峰值速率表示所配置的是单速桶流量整形，否则表示双速桶流量整形。

【举例】

在接口 GigabitEthernet1/0/1 上对满足 ACL 规则 2001 的报文进行流量整形。正常流速为 200kbps，突发流量为 51200bytes，以后速率小于等于 200kbps 时正常发送，速率大于 200kbps 时，将进入缓存队列，缓存队列长度为 100。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos gts acl 2001 cir 200 cbs 51200 ebs 0 queue-length 100
```

3.3 限速配置命令

3.3.1 display qos lr

display qos lr 命令用来显示接口或 PW 上的限速配置情况和统计信息。

【命令】

display qos lr { **interface** [*interface-type interface-number*] | **l2vpn-pw** [**peer** *ip-address* **pw-id** *pw-id*] }

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

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

peer *ip-address* **pw-id** *pw-id*：显示指定 PW 上的限速配置情况和运行统计信息。*ip-address* 为 PW 远端 PE 的 LSR ID。*pw-id* 为 PW 的 PW ID，取值范围为 1～4294967295。如果未指定本参数，将显示所有 PW 上的限速配置情况和运行统计信息。

【举例】

显示所有接口的接口限速配置情况和统计信息。

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
 Direction: Inbound
  CIR 2000 (kbps), CBS 20480 (Bytes), EBS 0 (Bytes)
  Passed   : 1000 (Packets) 1000 (Bytes)
  Discarded: 1000 (Packets) 1000 (Bytes)
  Delayed  : 1000 (Packets) 1000 (Bytes)
  Active shaping: No
Interface: GigabitEthernet1/0/2
 Direction: Outbound
  CIR 50 (%), CBS 600 (ms), EBS 0 (ms)
  Passed   : 1000 (Packets) 1000 (Bytes)
  Discarded: 1000 (Packets) 1000 (Bytes)
  Delayed  : 1000 (Packets) 1000 (Bytes)
  Active shaping: No
```

显示所有 PW 上的限速配置情况和统计信息。

```
<Sysname> display qos lr l2vpn-pw
L2VPN-PW: peer 1.2.3.4, pw-id 1
  Direction: Outbound
   CIR 1024 (kbps), CBS 64000 (Bytes), EBS 0 (Bytes)
   Passed   : 0 (Packets) 0 (Bytes)
   Delayed  : 0 (Packets) 0 (Bytes)
```

```
Active shaping: No
```

表3-4 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
L2VPN-PW	显示指定PW的信息，PW通过远端PE地址和PW ID唯一标识
Direction	方向，可以是Inbound、Outbound
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，单位为byte，实际的CBS值是*cbs-time* 乘以实际的承诺信息速率（**cir** 值乘以接口带宽）
EBS	超出突发尺寸，单位为byte，实际的EBS值是*ebs-time* 乘以实际的承诺信息速率（**cir** 值乘以接口带宽）
Passed	已经通过的数据包数目和字节数
Discarded	被丢弃的数据包数目和字节数
Delayed	被延迟发送的数据包数目和字节数
Active shaping	当前限速配置是否被激活，Yes表示激活，No表示未激活

3.3.2 qos lr

qos lr 命令用来配置限速。

undo qos lr 命令用来取消接口或 PW 配置的限速。

【命令】

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

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

【缺省情况】

未配置限速。

【视图】

接口视图/交叉连接 PW 视图/VSI LDP PW 视图/VSI 静态 PW 视图

【缺省用户角色】

network-admin

【参数】

outbound：对发送的数据流进行限速。

cir *committed-information-rate*：承诺信息速率，单位为 kbps，取值范围为 8～10000000

cbs *committed-burst-size*：承诺突发尺寸，单位为 bytes，取值范围为 500～1000000000。

ebs *excess-burst-size*：超出突发尺寸，在双令牌桶算法中超出承诺突发流量的部分，单位为 bytes，取值范围为 0～1000000000。

【举例】

对接口 GigabitEthernet1/0/1 上出方向的报文进行限速。正常流速为 200kbps，突发流量为 51200bytes，以后速率小于等于 200kbps 时正常发送，速率大于 200kbps 时，将进行限速。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 200 cbs 50000
```

4 拥塞管理

说明

- 各款型对于 ATM 接口的支持情况，请参见设备的安装手册和接口模块手册。
- 仅 MSR810-LMS/810-LUS/830-4LM-WiNet/3600-28-SI/3600-51-SI 不支持 l2vpn-pw。

设备各款型使用的命令行形式有所不同，详细差异信息如下：

命令行形式	款型
集中式	• MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK • MSR810-LMS/810-LUS • MSR2600-6-X1/2600-10-X1/2630 • MSR3600-28/3600-51/3600-28-SI/3600-51-SI • MSR3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC • MSR 3610/3620/3620-DP/3640/3660 • MSR810-W-WiNet/810-LM-WiNet/830-4LM-WiNet • MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet • MSR830-6BHI-WiNet/830-10BHI-WiNet • MSR2600-10-X1-WiNet/2630-WiNet • MSR3600-28-WiNet/3610-X1-WiNet • MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet • MSR810-LM-GL/810-W-LM-GL • MSR830-6EI-GL/830-10EI-GL/830-6HI-GL/830-10HI-GL • MSR2600-6-X1-GL/3600-28-SI-GL
分布式	MSR5620/5660/5680

4.1 拥塞管理公共配置命令

4.1.1 display qos queue interface

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

【命令】

display qos queue interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

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

pvc { *pvc-name* | *vpi/vci* }：显示指定 ATM 接口上的指定 PVC 的信息，只有当接口为 ATM 接口时才能指定本参数。*pvc-name* 表示 PVC 名，*vpi/vci* 表示 VPI/VCI 值。如果未指定本参数，将显示指定 ATM 接口上所有 PVC 的先进先出队列配置情况和统计信息。

【举例】

显示所有接口下的队列信息。

```
<Sysname> display qos queue interface
Interface: GigabitEthernet1/0/1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Weighted Fair queuing: Size/Length/Discards 0/64/0
  Weight: IP Precedence
  Queues: Active/Max active/Total 0/0/128

Interface: GigabitEthernet1/0/2
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
```

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

字段	描述
Interface	接口名，由接口类型和接口编号组成
Output queue	当前出队列的相关信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
FIFO queuing	先进先出队列
Size	激活的队列中数据包的总大小
Length	每个队列的队列长度
Discards	丢弃的数据包数目
Weighted Fair queuing	加权公平队列
Weight	权重类型，分为两类：IP Precedence和DSCP
Queues	WFQ队列的信息
Active	激活的WFQ队列数目
Max active	最大激活过的WFQ队列数目
Total	当前配置的WFQ队列总数

4.1.2 display qos queue l2vpn-pw

display qos queue l2vpn-pw 命令用来显示 PW 上队列配置情况和统计信息。

【命令】

display qos queue l2vpn-pw [**peer** *ip-address* **pw-id** *pw-id*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

peer *ip-address* **pw-id** *pw-id*：显示指定 PW 上的队列配置情况和统计信息。*ip-address* 为 PW 远端 PE 的 LSR ID。*pw-id* 为 PW 的 PW ID，取值范围为 1～4294967295。如果未指定本参数，将显示所有 PW 上的队列配置情况和统计信息。

【举例】

显示 PW 下的所有队列。

```
<Sysname> display qos queue l2vpn-pw
L2VPN-PW: peer 1.1.1.1, pw-id 1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
L2VPN-PW: peer 2.2.2.2 pw-id 2
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Weighted Fair queuing: Size/Length/Discards 0/64/0
  Weight: IP Precedence
  Queues: Active/Max active/Total 0/0/128
```

表4-2 display qos queue l2vpn-pw 命令显示信息描述表

字段	描述
L2VPN-PW	显示指定PW的信息，PW通过远端PE地址和PW ID唯一标识
Output queue	当前出队列的相关信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
Weighted Fair queuing	加权公平队列
Protocol queuing	协议队列
Size	激活的队列中数据包的总大小
Length	每个队列的队列长度
Discards	丢弃的数据包数目

字段	描述
Weight	权重类型，分为两类：IP Precedence和DSCP
Queues	WFQ队列的信息
Active	激活的WFQ队列数目
Max active	最大激活过的WFQ队列数目
Total	当前配置的WFQ队列总数

4.1.3 reset qos statistics l2vpn-pw

reset qos statistics l2vpn-pw 命令用来清除 PW 下 QoS 的统计信息。

【命令】

reset qos statistics l2vpn-pw [**peer** *ip-address* **pw-id** *pw-id*]

【视图】

用户视图

【缺省用户角色】

network-admin

【参数】

peer *ip-address* **pw-id** *pw-id*：清除指定 PW 上的 QoS 的统计信息。*ip-address* 为 PW 远端 PE 的 LSR ID。*pw-id* 为 PW 的 PW ID，取值范围为 1～4294967295。如果未指定本参数，将清除所有 PW 上的 QoS 的统计信息。

【举例】

清除 QoS 统计计数。

```
<Sysname> reset qos statistics l2vpn-pw peer 1.1.1.1 pw-id 1
```

4.2 FIFO队列配置命令

4.2.1 display qos queue fifo

display qos queue fifo 命令用来显示指定接口、指定 PVC、指定 PW 或所有接口及 PVC、所有 PW 上的先进先出队列配置情况和统计信息。

【命令】

display qos queue fifo interface { [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] | **l2vpn-pw** [**peer** *ip-address* **pw-id** *pw-id*] }

【视图】

任意视图

【缺省用户角色】

network-admin

network-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，将显示所有接口的先进先出队列配置情况和统计信息。

pvc { *pvc-name* | *vpi/vci* }：显示指定 ATM 接口上的指定 PVC 的信息，只有当接口为 ATM 接口时才能指定本参数。*pvc-name* 表示 PVC 名，*vpi/vci* 表示 VPI/VCI 值。如果未指定本参数，将显示指定 ATM 接口上所有 PVC 的先进先出队列配置情况和统计信息。

peer *ip-address* **pw-id** *pw-id*：显示指定 PW 上的先进先出队列配置情况和统计信息。*ip-address* 为 PW 远端 PE 的 LSR ID。*pw-id* 为 PW 的 PW ID，取值范围为 1～4294967295。如果未指定本参数，将显示所有 PW 上的先进先出队列配置情况和统计信息。

【举例】

显示所有接口的先进先出队列配置情况和统计信息。

```
<Sysname> display qos queue fifo interface
Interface: GigabitEthernet1/0/2
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
```

显示所有 PW 下的先进先出队列配置情况和统计信息。

```
<Sysname> display qos queue fifo l2vpn-pw
L2VPN-PW: peer 1.1.1.1, pw-id 1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - FIFO queuing: Size/Length/Discards 0/75/0
```

表4-3 display qos queue fifo 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号组成
L2VPN-PW	显示指定PW的信息，PW通过远端PE地址和PW ID唯一标识
Output queue	当前出队列的相关信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
FIFO queuing	先进先出队列
Size	激活的队列中数据包的总大小
Length	每个队列的队列长度
Discards	丢弃的数据包数目

4.2.2 qos fifo queue-length

qos fifo queue-length 命令用来配置先进先出队列的长度。

undo qos fifo queue-length 命令用来恢复缺省情况。

【命令】

qos fifo queue-length *queue-length*

undo qos fifo queue-length

【缺省情况】

先进先出队列的长度为 75。

【视图】

接口视图/PVC 视图/交叉连接 PW 视图/VSI LDP PW 视图/VSI 静态 PW 视图

【缺省用户角色】

network-admin

【参数】

queue-length：队列的长度，取值范围为 1～1024。

【使用指导】

在子接口上配置 FIFO 队列时，需要开启接口限速功能以保证队列生效。

【举例】

配置 FIFO 队列的长度为 100。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos fifo queue-length 100
```

【相关命令】

- **display qos queue fifo interface**

4.3 优先级队列配置命令

4.3.1 display qos queue pq interface

display qos queue pq interface 命令用来显示指定接口、指定 PVC 或所有接口及 PVC 上的优先级队列配置情况和统计信息。

【命令】

display qos queue pq interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-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，将显示所有接口上优先级队列配置情况和统计信息。

pvc { *pvc-name* | *vpi/vci* }：显示指定 ATM 接口上的指定 PVC 的信息，只有当接口为 ATM 接口时才能指定本参数。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。如果未指定本参数，将显示指定 ATM 接口上所有 PVC 的优先级队列配置情况和统计信息。

【使用指导】

若指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS PQ 的信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

显示接口 GigabitEthernet1/0/1 的优先级队列配置情况和统计信息。

```
<Sysname> display qos queue pq interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Priority queuing: PQL 1 Size/Length/Discards
Top:  0/20/0    Middle:  0/40/0    Normal:  0/60/0    Bottom:  0/80/0
```

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

字段	描述
Interface	接口名，由接口类型和接口编号组成
Output queue	出队列信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
Priority queuing	优先级队列，指明使用的优先级队列列表
Size	激活的队列中数据包的总大小
Length	每个队列的队列长度
Discards	丢弃的数据包数目
Top	高优先级队列
Middle	中优先级队列
Normal	普通优先级队列
Bottom	低优先级队列

4.3.2 display qos pql

display qos pql 命令用来显示指定或者所有优先级队列列表的内容。

【命令】

集中式设备－独立运行模式：

display qos pql [*pql-index*]

分布式设备－独立运行模式/集中式设备－IRF 模式：

display qos pql [*pql-index*] [**slot** *slot-number*]

分布式设备－IRF 模式：

display qos pql [*pql-index*] [**chassis** *chassis-number* **slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

slot *slot-number*：显示指定单板的优先级队列列表的内容，*slot-number* 表示单板所在的槽位号。如果未指定本参数，将显示主用主控板的优先级队列列表的内容。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备的优先级队列列表的内容，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示主用设备的优先级队列列表的内容。（集中式设备－IRF 模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的优先级队列列表的内容，*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，将显示全局主用主控板的优先级队列列表的内容。（分布式设备－IRF 模式）

【举例】

显示优先列表。

```
<Sysname> display qos pql
Current PQL configuration:
List  Queue   Parameters
-------------------------------------------------------
1     Top     Protocol ip less-than 1000
2     Normal  Length 80
2     Bottom  Length 40
3     Middle  Inbound-interface GigabitEthernet1/0/1
4     Top     Local-precedence  7
```

4.3.3 qos pq

qos pq 命令用来在接口或 PVC 上应用优先级队列调度机制。

undo qos pq 命令用来恢复缺省情况。

【命令】

qos pq pql *pql-index*

undo qos pq

【缺省情况】

接口及 PVC 的拥塞管理策略为 FIFO。

【视图】

接口视图/PVC 视图

【缺省用户角色】

network-admin

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

【使用指导】

若是 Tunnel 接口、子接口、三层聚合接口、HDLC 捆绑接口、RPR 逻辑接口，或是封装了 PPPoE、PPPoA、PPPoEoA、PPPoFR、MPoFR 协议的 VT、Dialer 接口，则接口需要开启接口限速功能以保证优先级队列功能生效。

在同一个接口或 PVC 视图下多次执行本命令，最后一次执行的命令生效。

可以为优先列表的组配置多条分类规则，在进行流分类时，数据流按照顺序进行匹配，如果匹配上某规则，则进入相应的队列，匹配结束；如果数据包不与任何规则匹配，则进入缺省队列。

【举例】

将第 12 组的优先列表应用到 GigabitEthernet1/0/1 上。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos pq pql 12
```

4.3.4 qos pql default-queue

qos pql default-queue 命令用来为未匹配任何规则的数据包指定一个缺省队列。

undo qos pql default-queue 命令用来恢复缺省情况。

【命令】

qos pql *pql-index* **default-queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **default-queue**

【缺省情况】

为未匹配任何规则的数据包指定的缺省队列为 **normal**。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。

【使用指导】

进行流分类的时候，如果数据包不与任何规则匹配，则进入缺省队列。

对于同一个 *pql-index*，多次执行本命令，最后一次执行的命令生效。

【举例】

将优先列表中第 12 组中无对应规则的包的缺省队列设定为 bottom。

```
<Sysname> system-view
[Sysname] qos pql 12 default-queue bottom
```

4.3.5 qos pql inbound-interface

qos pql inbound-interface 命令用来配置基于接口的分类规则。

undo qos pql inbound-interface 命令用来删除相应的分类规则。

【命令】

qos pql *pql-index* **inbound-interface** *interface-type interface-number* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **inbound-interface** *interface-type interface-number*

【缺省情况】

未配置任何分类规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列,优先级依次降低。

【使用指导】

对于同一个 *pql-index*，该命令可以重复使用，为来自不同接口的报文，建立不同的分类规则。

【举例】

配置组号为 12 的优先列表的分类规则，使得来自 GigabitEthernet1/0/1 的报文进入 **middle** 队列。

```
<Sysname> system-view
[Sysname] qos pql 12 inbound-interface gigabitethernet 1/0/1 queue middle
```

4.3.6 qos pql local-precedence

qos pql local-precedence 命令用来配置基于本地优先级的分类规则。

undo qos pql local-precedence 命令用来删除相应的规则。

【命令】

qos pql *pql-index* **local-pecedence** *local-precedence-list* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **local-precedence** *local-precedence-list*

【缺省情况】

未配置任何分类规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

local-precedence-list：要匹配的本地优先级的列表，最多可以输入 8 个 *local-precedence*，取值范围为 0～7。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。

【使用指导】

对于同一个 *pql-index*，该命令可以重复使用，为不同本地优先级的报文，建立不同的分类规则。

【举例】

配置组号为 12 的优先列表的分类规则，使得本地优先级等于 3 的报文进入 **middle** 队列。

```
<Sysname> system-view
[Sysname] qos pql 12 local-precedence 3 queue middle
```

4.3.7 qos pql protocol

qos pql protocol 命令用来配置基于协议的分类规则。

undo qos pql protocol 命令用来删除相应的分类规则。

【命令】

qos pql *pql-index* **protocol** { **ip** | **ipv6** } [*queue-key key-value*] **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **protocol** { **ip** | **ipv6** } [*queue-key key-value*]

【缺省情况】

未配置任何分类规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。

queue-key key-value：将 IP 或者 IPv6 报文分类进入队列。*queue-key* 和 *key-value* 的取值见下表。当不输入 *queue-key* 和 *key-value* 时，表示所有 IP 或者 IPv6 报文进入队列。

表4-5 queue-key 和 key-value 的取值

queue-key	*key-value*	说明
acl	access-list-number（2000～3999）	符合某访问控制列表定义的IP或者IPv6报文进入队列
fragments	-	分片的IP或者IPv6报文进入队列

queue-key	*key-value*	说明
greater-than	长度值（0～65535）	长度大于某个计数值的IP或者IPv6报文进入队列
less-than	长度值（0～65535）	长度小于某个计数值的IP或者IPv6报文进入队列
tcp	端口号（0～65535）	源或目的TCP端口号为指定的端口号的IP或者IPv6报文进入队列
udp	端口号（0～65535）	源或目的UDP端口号为指定的端口号的IP或者IPv6报文进入队列

【使用指导】

设备是以规则被配置的顺序来匹配数据包，如果发现数据包与某个规则匹配，便结束整个查找。

对于同一个 *pql-index*，该命令可以重复使用，为 IP 数据包建立多种分类规则。

当 *queue-key* 指定为 **tcp** 或 **udp** 时，*key-value* 的值既可以直接使用端口名称，也可以使用相关端口号。

【举例】

配置组号为 5 的优先列表的分类规则，使满足 ACL 为 3100 规则定义的 IP 报文进入 top 队列。

```
<Sysname> system-view
[Sysname] qos pql 5 protocol ip acl 3100 queue top
```

4.3.8 qos pql protocol mpls exp

qos pql protocol mpls exp 命令用来配置基于 MPLS EXP 优先级的分类规则。

undo qos pql protocol mpls exp 命令用来删除相应的分类规则。

【命令】

qos pql *pql-index* **protocol mpls exp** *exp-list* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **protocol mpls** exp *exp-list*

【缺省情况】

未配置任何分类规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

exp-list：要匹配的 MPLS EXP 优先级的报文列表，最多可以输入 8 个 *exp*，*exp* 取值范围为 0～7。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。

【使用指导】

对于同一个 *pql-index*，该命令可以重复使用，为不同 MPLS EXP 优先级的报文建立不同的分类规则

【举例】

配置组号为 12 的优先列表的分类规则，将 MPLS EXP 优先级为 2、4 的报文进入 top 队列。

```
<Sysname> system-view
[Sysname] qos pql 5 protocol mpls exp 2 4 queue top
```

4.3.9 qos pql queue

qos pql queue 命令用来设置各队列的长度。

undo qos pql queue 命令用来恢复队列长度的缺省值。

【命令】

qos pql *pql-index* **queue** { **bottom** | **middle** | **normal** | **top** } **queue-length** *queue-length*

undo qos pql *cql-index* **queue** { **bottom** | **middle** | **normal** | **top** } **queue-length**

【缺省情况】

高优先队列的缺省长度值为 20，中优先队列的缺省长度值为 40，正常优先队列的缺省长度值为 60，低优先队列的缺省长度值为 80。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

pql-index：优先列表的组号，取值范围为 1～16。

top、**middle**、**normal**、**bottom**：对应 PQ 的四个队列，优先级依次降低。

queue-length *queue-length*：队列的最大长度，即队列中所能容纳的数据包个数，取值范围为 1～1024。

【使用指导】

如果队列的长度达到最大值时，后面收到的属于该队列的数据包将被丢弃。

【举例】

配置优先列表第 5 组 top 队列的长度为 10。

```
<Sysname> system-view
[Sysname] qos pql 5 queue top queue-length 10
```

4.4 定制队列配置命令

4.4.1 display qos queue cq interface

display qos queue cq interface 命令用来显示指定接口、指定 PVC 或所有接口及 PVC 上的定制队列配置情况和统计信息。

【命令】

display qos queue cq interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-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，将显示所有接口上定制队列配置情况和统计信息。

pvc { *pvc-name* | *vpi/vci* }：显示指定 ATM 接口上的指定 PVC 的信息，只有当接口为 ATM 接口时才能指定本参数。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。如果未指定本参数，将显示指定 ATM 接口上所有 PVC 的定制队列配置情况和统计信息。

【使用指导】

若指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS CQ 的信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

#显示接口 GigabitEthernet1/0/1 的定制队列配置情况和统计信息。

```
<Sysname>display qos queue cq interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Custom queuing: CQL 1 Size/Length/Discards
 1:   0/  20/0          2:   0/  20/0          3:   0/  20/0
 4:   0/  20/0          5:   0/  20/0          6:   0/  20/0
 7:   0/  20/0          8:   0/  20/0          9:   0/  20/0
10:   0/  20/0         11:   0/  20/0         12:   0/  20/0
13:   0/  20/0         14:   0/  20/0         15:   0/  20/0
16:   0/  20/0
```

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

字段	描述
Interface	接口名，由接口类型和接口编号组成
Output queue	出队列信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
Custom queuing	定制队列，指明使用的定制队列列表
Size	激活的队列中数据包的总大小
Length	每个队列的队列长度
Discards	丢弃的数据包数目

4.4.2 display qos cql

display qos cql 命令用来显示指定或所有定制队列列表的内容。

【命令】

集中式设备－独立运行模式：

display qos cql [*cql-index*]

分布式设备－独立运行模式/集中式设备－IRF 模式：

display qos cql [*cql-index*] [**slot** *slot-number*]

分布式设备－IRF 模式：

display qos cql [*cql-index*] [**chassis** *chassis-number* **slot** *slot-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

cql-index：优先列表的组号，取值范围为 1～16。如果未指定本参数，则显示所有列表的内容。

slot *slot-number*：显示指定单板的定制列表的内容，*slot-number* 表示单板所在的槽位号。如果未指定本参数，将显示主用主控板的定制列表的内容。（分布式设备－独立运行模式）

slot *slot-number*：显示指定成员设备的定制列表的内容，*slot-number* 表示设备在 IRF 中的成员编号。如果未指定本参数，将显示主用设备的类的定制列表的内容。（集中式设备－IRF 模式）

chassis *chassis-number* **slot** *slot-number*：显示指定成员设备上指定单板的定制列表的内容，*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，将显示全局主用主控板的定制列表的内容。（分布式设备－IRF 模式）

【举例】

显示所有定制列表的内容。

```
<Sysname> display qos cql
Current CQL configuration:
List  Queue  Parameters
------------------------------------------------------
2     3      Protocol ip fragments
3     6      Length 100
3     1      Inbound-interface GigabitEthernet1/0/1
4     5      Local-precedence 7
```

4.4.3 qos cq

qos cq 命令用来在接口或 PVC 上应用定制队列。

undo qos cq 命令用来恢复缺省情况。

【命令】

qos cq cql *cql-index*

undo qos cq

【缺省情况】

接口或 PVC 的拥塞管理策略为 FIFO。

【视图】

接口视图/PVC 视图

【缺省用户角色】

network-admin

【参数】

cql-index：定制列表的组号，取值范围为 1~16。

【使用指导】

对于同一个接口或 PVC，多次执行本命令，最后一次执行的命令生效。

可以为定制列表的组配置多条分类规则，在进行流分类时，数据流按照顺序进行匹配，如果匹配上某规则，则进入相应的队列，匹配结束；如果数据包不与任何规则匹配，则进入缺省队列。

若是 Tunnel 接口、子接口、三层聚合接口、HDLC 捆绑接口，或是封装了 PPPoE、PPPoA、PPPoEoA、PPPoFR、MPoFR 协议的 VT、Dialer 接口，则接口需要开启接口限速功能以保证定制队列生效。

【举例】

将第 5 组的定制列表应用到 GigabitEthernet1/0/1 上。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos cq cql 5
```

4.4.4 qos cql default-queue

qos cql default-queue 命令用来为未匹配任何规则的数据包指定一个缺省队列。

undo qos cql default-queue 命令用来恢复缺省情况。

【命令】

qos cql *cql-index* **default-queue** *queue-id*

undo qos cql *cql-index* **default-queue**

【缺省情况】

队列号为 1。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue-id：队列号，取值范围为 1～16。

【使用指导】

在进行流分类的时候，如果数据包不与任何规则匹配，则进入缺省队列。

【举例】

指定定制列表第 5 组的缺省队列为 2。

```
<Sysname> system-view
[Sysname] qos cql 5 default-queue 2
```

4.4.5 qos cql inbound-interface

qos cql inbound-interface 命令用来建立基于接口的分类规则。

undo qos cql inbound-interface 命令用来删除相应的分类规则。

【命令】

qos cql *cql-index* **inbound-interface** *interface-type interface-number* **queue** *queue-id*

undo qos cql *cql-index* **inbound-interface** *interface-type interface-number*

【缺省情况】

未配置任何分类规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

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

queue-id：队列号，取值范围为 1～16。

【使用指导】

对于同一个 *cql-index*，该命令可以重复使用，为来自不同接口的报文，建立不同的分类规则。

【举例】

配置组号为 5 的定制列表的分类规则，将来自 GigabitEthernet1/0/1 的报文进入队列 3。

```
<Sysname> system-view
[Sysname] qos cql 5 inbound-interface gigabitethernet 1/0/1 queue 3
```

4.4.6 qos cql local-precedence

qos cql local-precedence 命令用来建立基于本地优先级的分类规则。

undo qos cql local-precedence 命令用来删除相应的规则。

【命令】

qos cql *cql-index* **local-precedence** *local-precedence-list* **queue** *queue-id*

undo qos cql *cql-index* **local-precedence** *local-precedence-list*

【缺省情况】

未配置任何分类规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

local-precedence-list：要匹配的本地优先级的列表，最多可以输入 8 个 *local-precedence*，取值范围为 0～7。

queue-id：定制队列的队列号，取值范围为 1~16。

【使用指导】

对于同一个 *cql-index*，该命令可以重复使用，为不同本地优先级的报文建立不同的分类规则。

【举例】

配置组号为 5 的定制列表的分类规则，将本地优先级等于 4 的报文进入队列 3。

```
<Sysname> system-view
[Sysname] qos cql 5 local-precedence 4 queue 3
```

4.4.7 qos cql protocol

qos cql protocol 命令用来配置基于协议的分类规则。

undo qos cql protocol 命令用来删除相应的分类规则。

【命令】

qos cql *cql-index* **protocol** { **ip** | **ipv6** } [*queue-key key-value*] **queue** *queue-id*

undo qos cql *cql-index* **protocol** { **ip** | **ipv6** } [*queue-key key-value*]

【缺省情况】

未配置任何分类规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue-id：队列号，取值范围为 1～16。

queue-key key-value：将IP或者IPv6 报文分类进入队列。*queue-key*和*key-value*的取值见 表 4-7。当不输入*queue-key*和*key-value*时，表示所有IP或者IPv6 报文进入队列。

表4-7 queue-key 和 key-value 的取值

queue-key	*key-value*	说明
acl	access-list-number（2000~3999）	符合某访问控制列表定义的IP或者IPv6报文就进入队列
fragments	-	只要是分片的IP或者IPv6报文就进入队列
greater-than	长度值（0~65535）	长度大于指定长度值的IP或者IPv6报文进入队列
less-than	长度值（0~65535）	长度小于指定长度值的IP或者IPv6报文进入队列
tcp	端口号（0~65535）	源或目的TCP端口号为指定的端口号的IP或者IPv6报文进入队列
udp	端口号（0~65535）	源或目的UDP端口号为指定的端口号的IP或者IPv6报文进入队列

【使用指导】

系统是以规则被配置的顺序来匹配数据包，如果发现数据包与某个规则匹配，便结束整个查找。

对于同一个 *cql-index*，该命令可以重复使用，为 IP 数据包建立多种分类规则。

当 *queue-key* 指定为 tcp 或 udp 时，*key-value* 的值既可以直接使用端口名称，也可以使用相关端口号。

【举例】

配置组号为 5 的定制列表的分类规则，将匹配访问控制列表 3100 的 IP 报文进入队列 3。

```
<Sysname> system-view
[Sysname] qos cql 5 protocol ip acl 3100 queue 3
```

4.4.8 qos cql protocol mpls exp

qos cql protocol mpls exp 命令用来配置基于 MPLS EXP 优先级的分类规则。

undo qos cql protocol mpls exp 命令用来删除相应的分类规则。

【命令】

qos cql *cql-index* **protocol mpls exp** *exp-list* **queue** *queue-id*

undo qos cql *cql-index* **protocol mpls exp** *exp-list*

【缺省情况】

未配置任何分类规则。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

exp-list：要匹配的 MPLS EXP 优先级的报文列表，最多可以输入 8 个 *exp*，*exp* 取值范围为 0～7。

queue-id：队列号，取值范围为 1～16。

【使用指导】

对于同一个 *cql-index*，该命令可以重复使用，为不同 MPLS EXP 优先级的报文建立不同的分类规则

【举例】

配置组号为 5 的定制列表的分类规则，将 MPLS EXP 优先级为 2、4 的报文进入队列 3。

```
<Sysname> system-view
[Sysname] qos cql 5 protocol mpls exp 2 4 queue 3
```

4.4.9 qos cql queue

qos cql queue 命令用来设置各队列的长度（所容纳的数据包个数）。

undo qos cql queue 命令用来恢复队列长度的缺省值。

【命令】

qos cql *cql-index* **queue** *queue-id* **queue-length** *queue-length*

undo qos cql *cql-index* **queue** *queue-id* **queue-length**

【缺省情况】

队列长度值是 20。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue-id：队列号，取值范围为 1～16。

queue-length：队列的最大长度，取值范围为 1～1024。

【使用指导】

如果队列的长度达到最大值时，后面收到的属于该队列的数据包将被丢弃。

【举例】

指定定制列表第 5 组队列 4 的长度为 40。

```
<Sysname> system-view
[Sysname] qos cql 5 queue 4 queue-length 40
```

4.4.10 qos cql queue serving

qos cql queue serving 命令用来设置各队列每次轮询所发送数据包的字节数。

undo qos cql queue serving 命令用来恢复发送数据包数的缺省值。

【命令】

qos cql *cql-index* **queue** *queue-id* **serving** *byte-count*

undo qos cql *cql-index* **queue** *queue-id* **serving**

【缺省情况】

发送数据包的字节数为 1500。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

cql-index：定制列表的组号，取值范围为 1～16。

queue-id：队列号，取值范围为 1～16。

byte-count：队列每次轮询所发送的数据包的字节数，取值范围为 1～16777215。

【举例】

指定定制列表第 5 组队列 2 每次轮询所发送数据包的字节数为 1400。

```
<Sysname> system-view
[Sysname] qos cql 5 queue 2 serving 1400
```

4.5 加权公平队列配置命令

4.5.1 display qos queue wfq

display qos queue wfq 命令用来显示指定接口、指定 PVC、指定 PW 或所有接口及 PVC、所有 PW 上的加权公平队列配置情况和统计信息。

【命令】

display qos queue wfq interface { [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] | **l2vpn-pw** [**peer** *ip-address* **pw-id** *pw-id*] }

【视图】

任意视图

【缺省用户角色】

network-admin

network-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，将显示所有接口的加权公平队列配置情况和统计信息。

pvc { *pvc-name* | *vpi/vci* }：显示指定 ATM 接口上的指定 PVC 的信息，只有当接口为 ATM 接口时才能指定本参数。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。如果未指定本参数，将显示指定 ATM 接口上所有 PVC 的加权公平队列配置情况和统计信息。

peer *ip-address* **pw-id** *pw-id*：显示指定 PW 上的加权公平队列配置情况和统计信息。*ip-address* 为 PW 远端 PE 的 LSR ID。*pw-id* 为 PW 的 PW ID，取值范围为 1～4294967295。如果未指定本参数，将显示所有 PW 上的加权公平队列配置情况和统计信息。

【举例】

显示接口 GigabitEthernet1/0/1 的加权公平队列配置情况和统计信息。

```
<Sysname> display qos queue wfq interface gigabitethernet 1/0/1
Interface: GigabitEthernet1/0/1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Weighted Fair queuing: Size/Length/Discards 0/64/0
  Weight: IP Precedence
  Queues: Active/Max active/Total 0/0/128
```

显示所有 PW 下的加权公平队列配置情况和统计信息。

```
<Sysname> display qos queue wfq l2vpn-pw
L2VPN-PW: peer 1.1.1.1, pw-id 1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Weighted Fair queuing: Size/Length/Discards 0/64/0
  Weight: IP Precedence
  Queues: Active/Max active/Total 0/0/128
```

表4-8 表 4-4 display qos queue wfq 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号组成
L2VPN-PW	显示指定PW的信息，PW通过远端PE地址和PW ID唯一标识
Output queue	当前出队列的相关信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
Weighted Fair queuing	加权公平队列
Size	激活的队列中数据包的总大小
Length	每个队列的队列长度
Discards	丢弃的数据包数目
Weight	权重类型，分为两类：IP Precedence和DSCP
Queues	WFQ队列的信息
Active	激活的WFQ队列数目
Max active	最大激活过的WFQ队列数目
Total	当前配置的WFQ队列总数

4.5.2 qos wfq

qos wfq 命令用来在接口、PVC 或 PW 上应用加权公平队列或修改加权公平队列的参数。

undo qos wfq 命令用来恢复缺省情况。

【命令】

qos wfq [**dscp** | **precedence**] [**queue-number** *total-queue-number* | **queue-length** *max-queue-length*] *

undo qos wfq

【缺省情况】

接口/PVC 使用的队列为 FIFO。

【视图】

接口视图/PVC 视图/交叉连接 PW 视图/VSI LDP PW 视图/VSI 静态 PW 视图

【缺省用户角色】

network-admin

【参数】

dscp：区分服务编码点权重类型。

precedence：IP 优先级权重类型。

queue-length *max-queue-length*：队列的最大长度，即每个队列中可容纳的数据包的最大个数，超出后数据包将被丢弃，取值范围为 1～1024，缺省值为 64。

queue-number *total-queue-number*：队列的总数目，可取的值为：16、32、64、128、256、512、1024、2048、4096，缺省值为 256。

【描述】

如果未指定权重类型，系统默认权重类型为 **precedence**。

对于 Tunnel 接口、子接口、三层聚合接口、HDLC 捆绑接口、RPR 逻辑接口，或是封装了 PPPoE、PPPoA、PPPoEoA、PPPoFR、MPoFR、PPPoFR、MPoFR 协议的 VT、Dialer 接口，则接口需要开启接口限速功能以保证加权公平队列功能生效。

【举例】

在接口 GigabitEthernet1/0/1 上应用 WFQ，并设置队列长度为 100，总队列个数设置为 512 个。

```
<Sysname> system-view
[Sysname] interface gigabitethernet1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq queue-length 100 queue-number 512
```

【相关命令】

- **display qos queue wfq interface**

4.6 实时传输协议队列的配置命令

4.6.1 display qos queue rtpq interface

display qos queue rtpq interface 命令用来显示指定接口、指定 PVC 或所有接口及 PVC 上 IP RTP Priority 的队列信息。

【命令】

display qos queue rtpq interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-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，将显示所有接口上当前 IP RTP Priority 的队列信息，包括当前的 RTP 长度和 RTP 报文的丢包数。

pvc { *pvc-name* | *vpi/vci* }：显示指定 ATM 接口上的指定 PVC 的信息，只有当接口为 ATM 接口时才能指定本参数。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。如果未指定本参数，将显示指定 ATM 接口上所有 PVC 的当前 IP RTP Priority 的队列信息，包括当前的 RTP 长度和 RTP 报文的丢包数。

【使用指导】

如指定接口为 Virtual-Template 接口，将显示继承该 Virtual-Template 接口的所有 Virtual-Access 接口下的 QoS RTP 队列的信息，Virtual-Template 本身无 QoS 信息显示。

【举例】

显示当前 IP RTP Priority 的队列信息。

```
<Sysname> display qos queue rtpq interface
Interface: GigabitEthernet1/0/1
Output queue - RTP queuing: Size/Max/Outputs/Discards 0/0/0/0
```

表4-9 display qos queue rtpq interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号组成
Output queue	当前的输出队列
Size	队列中数据包数目
Max	队列中数据包的历史最大数目
Outputs	发送出去的数据包数目
Discards	丢弃的数据包数目

4.6.2 qos rtpq

qos rtpq 命令用来开启接口或 PVC 下 RTP 队列，为某个 UDP 目的端口范围的 RTP 报文保留一个实时业务。

undo qos rtpq 命令用来恢复缺省情况。

【命令】

qos rtpq start-port *first-rtp-port-number* **end-port** *last-rtp-port-number* **bandwidth** *bandwidth* [**cbs** *committee-burst-size*]

undo qos rtpq

【缺省情况】

接口或 PVC 上没有启动 RTP 队列。

【视图】

接口视图/PVC 视图

【缺省用户角色】

network-admin

【参数】

start-port *first-rtp-port-number*：指定发起 RTP 报文的第一个 UDP 目的端口号，取值范围为 2000～65535。

end-port *last-rtp-port-number*：指定发起 RTP 报文的最后一个 UDP 目的端口号，取值范围为 2000～65535。

bandwidth *bandwidth*：RTP 队列所占用的带宽，取值范围为 8～1000000，单位为 kbps。

cbs *committee-burst-size*：指定承诺突发尺寸，取值范围为 1500～2000000 字节，单位为字节。

【使用指导】

若是 Tunnel 接口、子接口、三层聚合接口、HDLC 捆绑接口、RPR 逻辑接口，或是封装了 PPPoE、PPPoA、PPPoEoA、PPPoFR、MPoFR 协议的 VT、Dialer 接口，则接口需要开启接口限速功能以保证 RTP 队列功能生效。

该命令主要应用于对时延敏感的应用，如实时语音传输。**qos rtpq** 命令为语音业务提供最优先服务。

在配置 **bandwidth** 参数时，配置值通常应大于此实时业务所需的带宽总量，以预防突发流量的冲击。

【举例】

在接口 GigabitEthernet1/0/1 上启动 RTP 队列，发起 RTP 报文的第一个 UDP 目的端口号为 16384，发起 RTP 报文的最后一个 UDP 目的端口号为 32767，RTP 报文占用 64kbps 的带宽，如果输出接口拥塞，进入 RTP 队列。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos rtpq start-port 16384 end-port 32767 bandwidth 64
```

4.7 基于类的队列配置命令

4.7.1 display qos queue cbq

display qos queue cbq 命令用来显示指定接口、指定 PVC、指定 PW 或所有接口与 PVC、所有 PW 上基于类的队列配置信息和运行情况。

【命令】

display qos queue cbq interface { [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]] | **l2vpn-pw** [**peer** *ip-address* **pw-id** *pw-id*] }

【视图】

任意视图

【缺省用户角色】

network-admin

network-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，将显示所有接口的基于类的队列配置信息和运行情况。

pvc { *pvc-name* | *vpi/vci* }：显示指定 ATM 接口上的指定 PVC 的信息，只有当接口为 ATM 接口时才能指定本参数。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。如果未指定本参数，将显示指定 ATM 接口上所有 PVC 的基于类的队列配置信息和运行情况。

peer *ip-address* **pw-id** *pw-id*：显示指定 PW 上的加权公平队列配置情况和统计信息。*ip-address* 为 PW 远端 PE 的 LSR ID。*pw-id* 为 PW 的 PW ID，取值范围为 1～4294967295。如果未指定本参数，将显示所有 PW 上的基于类的队列配置情况和统计信息。

【举例】

显示所有接口的基于类的队列配置信息和运行情况。

```
<Sysname> display qos queue cbq interface
Interface: GigabitEthernet1/0/1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Class Based Queuing: Size/Discards 0/0
Queue Size: EF/AF/BE 0/0/0
  BE Queues: Active/Max active/Total 0/0/256
  AF Queues: Allocated 1
  Bandwidth(kbps): Available/Max reserve 74992/75000
```

显示所有 PW 下的基于类的队列配置情况和统计信息。

```
<Sysname> display qos queue cbq l2vpn-pw
L2VPN-PW: peer 1.1.1.1, pw-id 1
Output queue - Urgent queuing: Size/Length/Discards 0/100/0
Output queue - Protocol queuing: Size/Length/Discards 0/500/0
Output queue - Class Based Queuing: Size/Discards 0/0
Queue Size: EF/AF/BE 0/0/0
  BE Queues: Active/Max active/Total 0/0/256
```

```
AF Queues: Allocated 1
Bandwidth(kbps): Available/Max reserve 74992/75000
```

表4-10 display qos queue cbq 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号组成
L2VPN-PW	显示指定PW的信息，PW通过远端PE地址和PW ID唯一标识
Output queue	当前出队列的相关信息
Urgent queuing	紧急队列
Protocol queuing	协议队列
Class Based Queuing	基于类的队列
Size	激活的队列中数据包的总大小
Length	每个队列的队列长度
Discards	丢弃的数据包数目
EF	加速转发队列
AF	保证转发队列
BE	尽力转发队列
Active	BE队列当前处于激活状态的队列数
Max active	BE队列最大处于激活状态队列数
Total	BE队列总数
Bandwidth(kbps)	带宽
Available	CBQ当前可用带宽
Max reserve	CBQ最大预留带宽

4.7.2 qos reserved-bandwidth

qos reserved-bandwidth 命令用来设置最大预留带宽占可用带宽的百分比。

undo qos reserved-bandwidth 命令用来恢复缺省情况。

【命令】

qos reserved-bandwidth pct *percent*

undo qos reserved-bandwidth

【缺省情况】

最大预留带宽占可用带宽的百分比为 80。

【视图】

接口视图/PVC 视图

【缺省用户角色】

network-admin

【参数】

percent：预留带宽占可用带宽的百分比，取值范围为 1～100。

【使用指导】

为队列分配带宽时，考虑到部分带宽用于控制协议报文、二层帧头等，通常配置的最大预留带宽不大于可用带宽的 80%。

建议慎重使用该命令修改最大预留带宽。如果配置的最大预留带宽过大，发送的报文加上链路层的帧头有可能大于接口最大可用带宽，导致接口无法满足需求，建议使用缺省最大预留带宽。

接口最大可用带宽通过命令 **bandwidth** 进行配置，具体情况请参见接口分册命令参考中的介绍。

【举例】

配置 GigabitEthernet1/0/1 接口的最大预留带宽占可用带宽的百分比为 70。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos reserved-bandwidth pct 70
```

4.7.3 queue af

queue af 命令用来配置类采用 AF 队列，并配置类可确保的最小带宽。

undo queue af 命令用来恢复缺省情况。

【命令】

queue af bandwidth { *bandwidth* | **pct** *percentage* | **remaining-pct** *remaining-percentage* }

undo queue af

【缺省情况】

未配置类采用 AF 队列。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

bandwidth：带宽，单位 kbps,取值范围为 8～10000000。

pct *percentage*：可用带宽的百分比，取值范围为 1～100。

remaining-pct *remaining-percentage*：剩余带宽的百分比，取值范围为 1～100。

【使用指导】

在将类与 **queue af** 所属行为关联时，必须满足以下条件：

- 同一个策略下为 AF 队列和 EF 队列指定的带宽之和必须不大于该策略所应用接口的可用带宽；
- 同一个策略下为 AF 队列和 EF 队列指定的带宽百分比之和必须不大于 100；

- 同一个策略下 AF 队列和 EF 队列的带宽的配置必须都采用相同的值的类型，比如都采用绝对值形式，或者都采用百分比形式。

【举例】

为行为 database 配置采用 AF 队列，并且确保最小带宽为 200kbps。

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

【相关命令】

- **display qos queue cbq interface**
- **traffic behavior**

4.7.4 queue ef

queue ef 命令用来配置类采用 EF 队列，并配置最大带宽。

undo queue ef 命令用来恢复缺省情况。

【命令】

queue ef bandwidth { *bandwidth* [**cbs** *burst*] | **pct** *percentage* [**cbs-ratio** *ratio*] }

undo queue ef

【缺省情况】

未配置类采用 EF 队列。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

bandwidth：带宽，单位 kbps, 取值范围为 8～10000000。

cbs *burst*：指定承诺突发尺寸，单位为字节，取值范围为 32～1000000000，缺省值为 *bandwidth* ×25。

pct *percentage*：可用带宽的百分比，取值范围为 1～100。

cbs-ratio *ratio*：允许的突发因子，取值范围为 25～500，缺省值是 25。

【使用指导】

该命令在同一个流行为视图下不能与 **queue af**，**queue-length** 同时使用。

在策略下，缺省类 default-class 不能与 **queue ef** 所属 behavior 关联。

当将类与 **queue ef** 所属行为关联时，必须满足以下条件：

- 同一个策略下为 AF 队列和 EF 队列指定的带宽之和必须不大于该策略所应用接口的可用带宽。
- 同一个策略下为 AF 队列和 EF 队列指定的带宽百分比之和必须不大于 100。
- 同一个策略下 AF 队列和 EF 队列的带宽的配置必须都采用相同的值的类型，比如都采用绝对值形式，或者都采用百分比形式。

- 对于设置百分比形式 **queue ef bandwidth pct** *percentage* [**cbs-ratio** *ratio*]，CBS = 接口可用带宽×*percentage*×*ratio*÷100。
- 对于设置绝对值形式 **queue ef bandwidth** *bandwidth* [**cbs** *burst*]，CBS = *burst*，若不指定 *burst*，则 CBS = *bandwidth*×25。

【举例】

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

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

【相关命令】

- **display qos queue cbq interface**
- **traffic behavior**

4.7.5 queue sp

queue sp 命令用来配置类采用 SP 队列。

undo queue sp 用来恢复缺省情况。

【命令】

queue sp

undo queue sp

【缺省情况】

未配置类采用 SP 队列。

【视图】

流行为视图

【缺省用户角色】

network-admin

【使用指导】

配置了该命令的行为不能与缺省类关联使用。

在同一流行为视图下 **queue sp** 不能与 **queue ef** 命令同时使用。

在同一流行为视图下 **queue sp** 不能与 **queue af** 和 **queue-length** 命令同时使用。

【举例】

配置报文进入 SP 队列。

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

【相关命令】

- **display qos queue cbq interface**
- **traffic behavior**

4.7.6 queue wfq

queue wfq 命令用来为缺省类配置采用公平队列。

undo queue wfq 命令用来恢复缺省情况。

【命令】

queue wfq [**queue-number** *total-queue-number*]

undo queue wfq

【缺省情况】

没有为缺省类配置采用公平队列。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

queue-number *total-queue-number*：公平队列的数目，可取的值为 16、32、64、128、256、512、1024、2048、4096，即 2 的幂数，缺省值为 256。

【使用指导】

配置了该命令的行为仅可以与缺省类关联使用。

该命令可以搭配 **queue-length** 命令或 **wred** 命令使用。

【举例】

为缺省类配置使用 WFQ，队列数为 16。

```
<Sysname> system-view
[Sysname] traffic behavior test
[Sysname-behavior-test] queue wfq queue-number 16
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier default-class behavior test
```

【相关命令】

- **display qos queue cbq interface**
- **traffic behavior**

4.7.7 queue-length

queue-length 命令用来配置最大队列长度，丢弃方式为尾部丢弃。

undo queue-length 命令用来恢复缺省情况。

【命令】

queue-length *queue-length*

undo queue-length

【缺省情况】

丢弃方式为尾部丢弃方式，队列长度为 64。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

queue-length：队列最大阈值，取值范围为 1～1024。

【使用指导】

本命令必须在配置了 **queue af** 或 **queue wfq** 后使用。

配置 **queue-length** 后，若执行 **undo queue af** 和 **undo queue wfq** 命令，则 **queue-length** 也同时被取消。

【举例】

配置尾部丢弃，队列长度最大为 16。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
[Sysname-behavior-database] queue-length 16
```

【相关命令】

- **queue af**
- **queue wfq**

4.7.8 wred

wred 命令用来配置丢弃方式为加权随机早期检测。

undo wred 命令用来恢复缺省情况。

【命令】

wred [**dscp** | **ip-precedence**]

undo wred

【缺省情况】

未配置 WRED 动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

dscp：表明在为一个包计算丢弃概率时使用的是 DSCP 值。

ip-precedence：表明在为一个包计算丢弃概率时使用的是 IP 优先级值。缺省情况下使用的是 **ip-precedence**。

【使用指导】

本命令必须在配置了 **queue af** 或 **queue wfq** 后使用。

如果流行为中同时配置了 **wred** 和 **queue-length** 命令，则先配置的命令生效。

执行 **undo wred** 命令时将删除 WRED 相关的其他配置。

【举例】

配置采用加权早期检测方式，丢弃概率以 IP 优先级计算。

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

【相关命令】

- **queue af**
- **queue wfq**

4.7.9 wred dscp

wred dscp 命令用来设置 WRED 各 DSCP 的下限、上限和丢弃概率的分母。

undo wred dscp 命令用来取消 WRED 中某个 DSCP 的丢弃参数配置。

【命令】

wred dscp *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred dscp *dscp-value*

【缺省情况】

WRED 中所有 DSCP 的下限缺省值为 10，上限缺省值为 30。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

dscp-value：DSCP值，取值范围为 0～63，也可以是关键字，如 表 1-5 所示。

low-limit *low-limit*：WRED 下限，单位为报文个数，取值范围为 1～1024。

high-limit *high-limit*：WRED 上限，单位为报文个数，取值范围为 1～1024。

discard-probability *discard-prob*：丢弃概率的分母，取值范围为 1～255，缺省值为 10。

【使用指导】

进行本命令配置以前，必须已用 **wred dscp** 命令开启了基于 DSCP 的 WRED 丢弃方式。

执行 **undo wred** 命令将会同时取消 **wred dscp** 命令的配置。

取消 **queue af** 或 **queue wfq** 配置，WRED 丢弃参数的配置同时被取消。

【举例】

设置 DSCP 为 3 的报文的队列下限为 20，上限为 40，丢弃概率的分母为 15。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred dscp
[Sysname-behavior-database] wred dscp 3 low-limit 20 high-limit 40 discard-probability 15
```

【相关命令】

- **queue af**
- **queue wfq**
- **wred**

4.7.10 wred ip-precedence

wred ip-precedence 命令用来设置 WRED 各 IP 优先级的下限、上限和丢弃概率的分母。

undo wred ip-precedence 命令用来取消 WRED 中某个 IP 优先级的丢弃参数配置。

【命令】

wred ip-precedence *precedence* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred ip-precedence *precedence*

【缺省情况】

WRED 中所有 IP 优先级的下限缺省值为 10，上限缺省值为 30。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

precedence：IP 优先级，取值范围为 0～7。

low-limit *low-limit*：WRED 下限，单位为报文个数，取值范围为 1～1024。

high-limit *high-limit*：WRED 上限，单位为报文个数，取值范围为 1～1024。

discard-probability *discard-prob*：丢弃概率的分母，取值范围为 1～255，缺省值为 10。

【使用指导】

进行本命令配置以前，必须已用 **wred** 命令开启了基于 IP 优先级的 WRED 丢弃方式。

执行 **undo wred** 命令将会同时取消 **wred ip-precedence** 命令的配置。

取消 **queue af** 或 **queue wfq** 配置，WRED 丢弃参数的配置同时被取消。

【举例】

设置优先级为 3 的报文的队列下限为 20，上限为 40，丢弃概率的分母为 15。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behaviro-database] wred ip-precedence
[Sysname-behavior-database] wred ip-precedence 3 low-limit 20 high-limit 40
discard-probability 15
```

【相关命令】

- **queue af**
- **queue wfq**
- **wred**

4.7.11 wred weighting-constant

wred weighting-constant 命令用来设置 WRED 计算平均队列长度的指数。

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

【命令】

wred weighting-constant *exponent*

undo wred weighting-constant

【缺省情况】

WRED 计算平均队列长度的指数为 9。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

exponent：指数，取值范围为 1～16。

【使用指导】

进行本命令配置之前，需先配置 **queue af** 或 **queue wfq** 命令，并已使用 **wred** 命令开启了 WRED 丢弃方式。

执行 **undo wred** 命令将会同时取消 **wred weighting-constant** 命令的配置。

【举例】

配置计算平均队列长度的指数为 6。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
[Sysname-behavior-database] wred ip-precedence
[Sysname-behavior-database] wred weighting-constant 6
```

【相关命令】

- **queue af**
- **queue wfq**

- **wred**

4.8 报文信息预提取命令

4.8.1 qos pre-classify

qos pre-classify 命令用来开启报文信息预提取功能。

undo qos pre-classify 命令用来关闭报文信息预提取功能。

【命令】

qos pre-classify

undo qos pre-classify

【缺省情况】

报文信息预提取功能处于关闭状态。

【视图】

Tunnel 接口视图

【缺省用户角色】

network-admin

【举例】

在 Tunnel 接口上开启报文信息预提取功能。

```
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] qos pre-classify
```

4.9 QoS令牌配置命令

4.9.1 qos qmtoken

qos qmtoken 命令用来配置 QoS 的发送令牌功能。

undo qos qmtoken 命令用来取消 QoS 的发送令牌功能。

【命令】

qos qmtoken *token-number*

undo qos qmtoken

【缺省情况】

没有配置 QoS 的发送令牌功能。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

token-number：发送令牌数量，取值范围为 1～256。

【使用指导】

QoS 的发送令牌功能提供了一种底层队列的流量控制机制，它可以根据配置的令牌的数量控制向底层接口队列发送的报文数量。适用场景如下：

- 在使用 CBQ 队列时，由于底层队列的缓存，接口拥塞时 EF 队列的时延可能无法满足要求，使用该功能可降低接口拥塞时 EF 队列的时延。
- 进行 FTP 传输等工作时，由于上层 TCP 协议提供了流控功能，QoS 的队列可能失效，使用该功能可以改善队列失效的情况。

可以根据实际情况对该功能的参数 *token-number* 进行调整，以达到更好的效果。

如果上层协议（如 UDP）没有流控功能，建议不要使用 QoS 令牌功能，以提高数据传输的效率。

配置此功能时，需要注意的是：

- 配置此命令后需要用 **shutdown/undo shutdown** 命令重启接口来使能 QoS 的发送令牌功能。
- 目前只有串口和三层以太网接口支持该命令。

【举例】

设置 QoS 的发送令牌数量为 1。

```
<Sysname> system-view
[Sysname] interface serial 2/2/1
[Sysname-Serial2/2/1] qos qmtoken 1
[Sysname-Serial2/2/1] shutdown
[Sysname-Serial2/2/1] undo shutdown
```

5 拥塞避免

说明

各款型对于 ATM 接口的支持情况，请参见设备的安装手册和接口模块手册。

5.1 WRED配置命令

5.1.1 display qos wred interface

display qos wred interface 命令用来显示指定接口、指定 PVC 或所有接口及 PVC 上 WRED 配置情况和统计信息。

【命令】

display qos wred interface [*interface-type interface-number* [**pvc** { *pvc-name* | *vpi/vci* }]]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

interface-type interface-number：指定的接口类型和接口编号。如果未指定本参数，将显示所有接口的 WRED 配置情况和统计信息。

pvc { *pvc-name* | *vpi/vci* }：显示指定 ATM 接口上的指定 PVC 的信息，只有当接口为 ATM 接口时才能指定本参数。*pvc-name* 表示 PVC 名。*vpi/vci* 表示 VPI/VCI 值。如果未指定本参数，将显示指定 ATM 接口上所有 PVC 的 WRED 配置情况和统计信息。

【举例】

显示所有接口的 WRED 配置情况和统计信息。

```
<Sysname> display qos wred interface
Interface: GigabitEthernet1/0/4
 Current WRED configuration:
 Exponent: 9 (1/512)
 Pre  Low   High  Dis-prob Random-discard  Tail-discard
-----------------------------------------------------
0    10    30    10       0              0
1    10    30    10       0              0
2    10    30    10       0              0
3    10    30    10       0              0
4    10    30    10       0              0
```

```
5     10    30    10       0              0
6     10    30    10       0              0
7     10    30    10       0              0

Interface: GigabitEthernet1/0/3
 Current WRED configuration:
 Applied WRED table name: q1
```

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

字段	描述
Interface	接口名，由接口类型和接口编号组成
Exponent	计算平均队列长度的指数
Pre	报文的IP优先级
Low	队列下限
High	队列上限
Dis-prob	计算丢弃概率时的分母
Random-discard	随机丢弃的报文的数目
Tail-discard	尾丢弃报文的数目
Current WRED configuration	当前WRED的配置情况
Applied WRED table name	当前应用的WRED表的名称

5.1.2 qos wred enable

qos wred enable 命令用来在接口或 PVC 上开启 WRED。

undo qos wred enable 命令用来恢复缺省情况。

【命令】

qos wred [**dscp** | **ip-precedence**] **enable**

undo qos wred [**dscp** | **ip-precedence**] **enable**

【缺省情况】

队列丢弃方法为尾丢弃。

【视图】

接口视图/PVC 视图

【缺省用户角色】

network-admin

【参数】

dscp：表明计算丢弃概率时使用的是 DSCP 值。

ip-precedence：表明计算丢弃概率时使用的是 IP 优先级值。缺省情况下使用的是 **ip-precedence**。

【使用指导】

必须先在接口上配置 **qos wfq** 命令，才能配置本命令。

【举例】

在 GigabitEthernet1/0/1 接口上开启 WRED，丢弃概率以 IP 优先级计算。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq queue-length 100 queue-number 512
[Sysname-GigabitEthernet1/0/1] qos wred ip-precedence enable
```

【相关命令】

- **display qos wred interface**
- **qos wred enable**

5.1.3 qos wred dscp

qos wred dscp 命令用来设置各 DSCP 优先级的下限、上限和丢弃概率的分母。

undo qos wred dscp 命令用来恢复缺省情况。

【命令】

qos wred dscp *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo qos wred dscp *dscp-value*

【缺省情况】

下限缺省值为 10，上限缺省值为 30，丢弃概率缺的分母省值为 10。

【视图】

接口视图/PVC 视图

【缺省用户角色】

network-admin

【参数】

dscp-value：DSCP值，取值范围为 0～63，也可以是关键字，如 表 1-5 所示。

low-limit *low-limit*：WRED 下限，单位为报文个数，取值范围为 1～1024。

high-limit *high-limit*：WRED 上限，单位为报文个数，取值范围为 1～1024。

discard-probability *discard-prob*：丢弃概率的分母，取值范围为 1～255。

【使用指导】

必须先使用 **qos wred dscp enable** 在接口或 PVC 上应用基于 DSCP 的 WRED 后，才可以进行本配置。

阈值限制的是平均队列长度。

【举例】

在接口上设置 DSCP 优先级为 63 的报文的队列下限为 20，上限为 40，丢弃概率的分母为 15。

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

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq queue-length 100 queue-number 512
[Sysname-GigabitEthernet1/0/1] qos wred dscp enable
[Sysname-GigabitEthernet1/0/1] qos wred dscp 63 low-limit 20 high-limit 40
discard-probability 15
```

【相关命令】

- **display qos wred interface**
- **qos wred enable**

5.1.4 qos wred ip-precedence

qos wred ip-precedence 命令用来设置 IP 优先级的下限、上限和丢弃概率的分母。

undo qos wred ip-precedence 命令用来恢复缺省情况。

【命令】

qos wred ip-precedence *ip-precedence* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo qos wred ip-precedence *ip-precedence*

【缺省情况】

下限缺省值为 10，上限缺省值为 30，丢弃概率的分母缺省值为 10。

【视图】

接口视图/PVC 视图

【缺省用户角色】

network-admin

【参数】

ip-precedence *ip-precedence*：IP 优先级，取值范围为 0～7。

low-limit *low-limit*：WRED 下限，单位为报文个数，取值范围为 1～1024。

high-limit *high-limit*：WRED 上限，单位为报文个数，取值范围为 1～1024。

discard-probability *discard-prob*：丢弃概率的分母，取值范围为 1～255。

【使用指导】

必须先使用 **qos wred enable** 在接口或 PVC 上应用基于 IP 优先级的 WRED 后，才可以进行本配置。

阈值限制的是平均队列长度。

【举例】

在接口上设置 IP 优先级为 3 的报文的队列下限为 20，上限为 40，丢弃概率的分母为 15。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq queue-length 100 queue-number 512
[Sysname-GigabitEthernet1/0/1] qos wred ip-precedence enable
[Sysname-GigabitEthernet1/0/1] qos wred ip-precedence 3 low-limit 20 high-limit 40
discard-probability 15
```

【相关命令】

- **display qos wred interface**
- **qos wred enable**

5.1.5 qos wred weighting-constant

qos wred weighting-constant 命令用来设置 WRED 计算平均队列长度的指数。

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

【命令】

qos wred weighting-constant *exponent*

undo qos wred weighting-constant

【缺省情况】

WRED 计算平均队列长度的指数为 9。

【视图】

接口视图/PVC 视图

【缺省用户角色】

network-admin

【参数】

weighting-constant *exponent*：计算平均队列长度的指数，取值范围为 1～16。

【使用指导】

必须先使用 **qos wred enable** 在接口或 PVC 上应用 WRED 后，才可以配置 WRED 的参数。

【举例】

在 GigabitEthernet1/0/1 接口上配置计算平均队列长度的指数为 6。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq queue-length 100 queue-number 512
[Sysname-GigabitEthernet1/0/1] qos wred enable
[Sysname-GigabitEthernet1/0/1] qos wred weighting-constant 6
```

【相关命令】

- **display qos wred interface**
- **qos wred enable**

6 QPPB

6.1 QPPB配置命令

6.1.1 bgp-policy

bgp-policy 命令用来配置 QPPB 功能，即通过 BGP 传播路由策略中设置的 **apply ip-precedence** 和 **apply qos-local-id** 信息。

undo bgp-policy 命令用来恢复缺省情况。

【命令】

bgp-policy { **destination** | **source** } { **ip-prec-map** | **ip-qos-map** } *

undo bgp-policy { **destination** | **source** } [**ip-prec-map** | **ip-qos-map**] *

【缺省情况】

未配置 QPPB 功能。

【视图】

接口视图

【缺省用户角色】

network-admin

【参数】

destination：使用目的 IP 查找路由。

source：使用源 IP 查找路由。如果指定本参数，则以源 IP 为目的进行反向查找。

ip-prec-map：设置 IP 优先级。

ip-qos-map：设置 QoS 本地 ID。

【使用指导】

本配置只对接口接收的报文生效。

在 MPLS L3VPN 网络中，PE 公网接口入方向 QoS 业务在本配置之前进行；其他网络环境中 QoS 业务在本配置之后进行。

如果存在两条 **bgp-policy** 命令，分别指定 **source** 和 **destination**，后者的设置操作会覆盖前者。

【举例】

在接口 GigabitEthernet1/0/1 上根据源 IP 查找路由获得 IP 优先级和 QoS 本地 ID。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] bgp-policy source ip-prec-map ip-qos-map
```

【相关命令】

- **apply ip-precedence**（三层技术-IP 路由命令参考/路由策略）
- **apply qos-local-id**（三层技术-IP 路由命令参考/路由策略）

- **route-policy**（三层技术-IP 路由命令参考/路由策略）

目 录

1 MPLS QoS ····· 1-1
1.1 MPLS QoS配置命令 ····· 1-1
1.1.1 if-match mpls-exp ····· 1-1
1.1.2 remark mpls-exp ····· 1-1
1.1.3 remark second-mpls-exp ····· 1-2

1 MPLS QoS

1.1 MPLS QoS配置命令

1.1.1 if-match mpls-exp

if-match mpls-exp 命令用来定义匹配第一层 MPLS EXP 优先级的规则。

undo if-match mpls-exp 命令用来删除匹配第一层 MPLS EXP 优先级的规则。

【命令】

if-match [**not**] **mpls-exp** *exp-value*&<1-8>

undo if-match [**not**] **mpls-exp** *exp-value*&<1-8>

【缺省情况】

未定义匹配第一层 MPLS EXP 优先级的规则。

【视图】

类视图

【缺省用户角色】

network-admin

【参数】

not：不匹配该规则。

exp-value&<1-8>：EXP 值的列表，EXP 优先级的取值范围为 0～7，&<1-8>表示前面的参数最多可以输入 8 次。如果指定了多个相同的 EXP 值，系统默认为一个；多个不同的 EXP 值是或的关系，即只要有一个值匹配，就算匹配这条规则。

【举例】

定义匹配第一层 EXP 优先级为 3 或 4 的报文的规则。

```
<Sysname> system-view
[Sysname] traffic classifier database
[Sysname-classifier-database] if-match mpls-exp 3 4
```

1.1.2 remark mpls-exp

remark mpls-exp 命令用来配置标记 MPLS 报文的 EXP 值。

undo remark mpls-exp 命令用来取消标记 MPLS 报文的 EXP 值。

【命令】

remark mpls-exp *exp-value*

undo remark mpls-exp

【缺省情况】

未配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

exp-value：MPLS 报文的 EXP 值，取值范围为 0～7。

【举例】

配置标记 MPLS 报文的 EXP 值为 0。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark mpls-exp 0
```

1.1.3 remark second-mpls-exp

remark second-mpls-exp 命令用来配置标记第二层 MPLS 报文的 EXP 值。

undo remark second-mpls-exp 命令用来取消标记第二层 MPLS 报文的 EXP 值。

【命令】

remark second-mpls-exp *exp-value*

undo remark second-mpls-exp

【缺省情况】

未配置重新标记第二层 MPLS 报文 EXP 优先级的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

exp-value：第二层 MPLS 报文的 EXP 值，取值范围为 0～7。

【举例】

配置标记第二层 MPLS 报文的 EXP 值为 0。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark second-mpls-exp 0
```

目 录

1 帧中继QoS ····· 1-1

1.1 帧中继QoS配置命令 ····· 1-2

1.1.1 cbs ····· 1-2

1.1.2 cir ····· 1-3

1.1.3 cir allow ····· 1-3

1.1.4 display fr class-map ····· 1-4

1.1.5 ebs ····· 1-5

1.1.6 fifo queue-length ····· 1-6

1.1.7 fragment enable ····· 1-7

1.1.8 fragment size ····· 1-7

1.1.9 fr class ····· 1-8

1.1.10 fr de del ····· 1-8

1.1.11 fr del inbound-interface ····· 1-9

1.1.12 fr del protocol ····· 1-10

1.1.13 fr traffic-policing ····· 1-11

1.1.14 fr traffic-shaping ····· 1-12

1.1.15 fr-class ····· 1-13

1.1.16 traffic-shaping adaptation ····· 1-13

1.1.17 traffic-shaping adaptation percentage ····· 1-14

1 帧中继QoS

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

型号	特性	描述
MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK/810-LMS/810-LUS	帧中继 QoS	MSR810/810-W/810-W-DB/810-LM/810-W-LM/810-10-PoE/810-LM-HK/810-W-LM-HK不支持 810-LMS/810-LUS支持
MSR2600-6-X1/2600-10-X1		支持
MSR 2630		支持
MSR3600-28/3600-51		支持
MSR3600-28-SI/3600-51-SI		支持
MSR 3610-X1/3610-X1-DP/3610-X1-DC/3610-X1-DP-DC		支持
MSR 3610/3620/3620-DP/3640/3660		支持
MSR 5620/5660/5680		支持

型号	命令	描述
MSR810-W-WiNet/810-LM-WiNet	帧中继 QoS	不支持
MSR830-4LM-WiNet		支持
MSR830-5BEI-WiNet/830-6EI-WiNet/830-10BEI-WiNet		支持
MSR830-6BHI-WiNet/830-10BHI-WiNet		支持
MSR2600-10-X1-WiNet		支持
MSR2630-WiNet		支持
MSR3600-28-WiNet		支持
MSR3610-X1-WiNet		支持
MSR3610-WiNet/3620-10-WiNet/3620-DP-WiNet/3620-WiNet/3660-WiNet		支持

型号	特性	描述
MSR810-LM-GL	帧中继 QoS	支持
MSR810-W-LM-GL		支持
MSR830-6EI-GL		支持
MSR830-10EI-GL		支持

型号	特性	描述
MSR830-6HI-GL		支持
MSR830-10HI-GL		支持
MSR2600-6-X1-GL		支持
MSR3600-28-SI-GL		支持

1.1 帧中继QoS配置命令

1.1.1 cbs

cbs 命令用来配置帧中继虚电路的 CBS（Committed Burst Size，承诺突发尺寸）。

undo cbs 命令用来取消帧中继虚电路 CBS 的配置。

【命令】

cbs [**inbound** | **outbound**] *committed-burst-size*

undo cbs [**inbound** | **outbound**]

【缺省情况】

承诺突发尺寸为 56000bits。

【视图】

帧中继类视图

【缺省用户角色】

network-admin

【参数】

inbound：报文入方向的承诺突发尺寸，本参数仅当接口开启帧中继流量监管时有效。

outbound：报文出方向的承诺突发尺寸，本参数仅当接口开启帧中继流量整形时有效。

committed-burst-size：承诺突发尺寸，取值范围为 300～16000000，单位为 bit。

【使用指导】

如果配置时不指定报文方向，则表示同时配置在入方向和出方向上。

【举例】

配置名为 test1 的帧中继类在入方向和出方向上的 CBS 为 64000bits。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cbs 64000
```

【相关命令】

- **cir**
- **cir allow**
- **ebs**

1.1.2 cir

cir 命令用来配置帧中继虚电路的 CIR（Committed Information Rate，承诺信息速率）。

undo cir 命令用来恢复缺省情况。

【命令】

cir *committed-information-rate*

undo cir

【缺省情况】

承诺信息速率为 56000bps。

【视图】

帧中继类视图

【缺省用户角色】

network-admin

【参数】

committed-information-rate：承诺信息速率，取值范围为 1000～45000000，单位为 bps。

【使用指导】

承诺信息速率不能大于出方向允许的承诺信息速率。

【举例】

配置名为 test1 的帧中继类的 CIR 为 32000bps。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir 32000
```

【相关命令】

- **cbs**
- **cir allow**
- **ebs**

1.1.3 cir allow

cir allow 命令用来配置帧中继虚电路的 CIR ALLOW（Committed Information Rate ALLOW，允许的承诺信息速率）。

undo cir allow 命令用来取消帧中继虚电路的 CIR ALLOW 的配置。

【命令】

cir allow [**inbound** | **outbound**] *committed-information-rate*

undo cir allow [**inbound** | **outbound**]

【缺省情况】

允许的承诺信息速率为 56000bps。

【视图】

帧中继类视图

【缺省用户角色】

network-admin

【参数】

inbound：报文入方向所允许的承诺信息速率，本参数仅当接口开启帧中继流量监管时有效。

outbound：报文出方向所允许的承诺信息速率，本参数仅当接口开启帧中继流量整形时有效。

committed-information-rate：允许的承诺信息速率，取值范围为 1000～45000000，单位为 bps。

【使用指导】

执行本命令时，出方向允许的承诺信息速率不能小于承诺信息速率。

如果不指定报文方向，则表示同时配置在入方向和出方向上。

【举例】

配置名为 test1 的帧中继类的 CIR ALLOW 为 64000bps。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir allow 64000
```

1.1.4 display fr class-map

display fr class-map 命令用来显示帧中继类与接口以及虚电路的映射关系。

【命令】

display fr class-map [**fr-class** *class-name* | **interface** *interface-type interface-number*]

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

fr-class *class-name*：显示指定帧中继类与接口以及虚电路的映射关系。*class-name* 表示帧中继类名称，为 1～30 个字符的字符串，区分大小写。

interface *interface-type interface-number*：指定接口的类型和编号，可以指定主接口，也可以指定子接口。指定主接口时，显示帧中继类与该主接口及其子接口以及其下的虚电路的映射关系。指定子接口时，显示帧中继类与该子接口及其下的虚电路的映射关系。

【使用指导】

不指定接口和帧中继类名称时，显示所有帧中继类与接口以及虚电路的映射关系。

【举例】

显示接口 Serial2/1/1 与帧中继类的映射关系。

```
<Sysname> display fr class-map interface serial 2/1/1
```

```
Serial2/1/1
  fr-class ts1
  fr dlci 100
    fr-class ts
Serial2/1/1.1
  fr-class ts2
  fr dlci 222
    fr-class ts
```

显示帧中继类 ts 与接口的映射关系。

```
<Sysname> display fr class-map fr-class ts
Serial2/1/1
  fr dlci 100
    fr-class ts
Serial2/1/1.1
  fr dlci 222
    fr-class ts
```

表1-1 display fr class-map 命令显示信息描述表

字段	描述
Serial2/1/1 fr-class ts1	帧中继接口及关联的帧中继类
fr dlci 100 fr-class ts	帧中继接口下的虚电路及关联的帧中继类
Serial2/1/1.1 fr-class ts2	帧中继子接口及关联的帧中继类
fr dlci 222 fr-class ts	帧中继子接口下的虚电路及关联的帧中继类

1.1.5 ebs

ebs 命令用来配置帧中继虚电路的 EBS（Excess Burst Size，超出突发尺寸）。

undo ebs 命令用来取消帧中继虚电路的 EBS 的配置。

【命令】

ebs [**inbound** | **outbound**] *excess-burst-size*

undo ebs [**inbound** | **outbound**]

【缺省情况】

超出突发尺寸为 0bit。

【视图】

帧中继类视图

【缺省用户角色】

network-admin

【参数】

inbound：报文入方向的超出突发尺寸，本参数仅当接口开启帧中继流量监管时有效。

outbound：报文出方向的超出突发尺寸，本参数仅当接口开启帧中继流量整形时有效。

excess-burst-size：超出突发尺寸，取值范围为 0～16000000，单位为 bit。

【使用指导】

如果不指定报文方向，则表示配置的 EBS 值将同时在入方向和出方向生效。

【举例】

配置名为 test1 的帧中继类的超出突发尺寸为 32000bits。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] ebs 32000
```

【相关命令】

- **cbs**
- **cir**
- **cir allow**

1.1.6 fifo queue-length

fifo queue-length 命令用来配置帧中继虚电路的先进先出队列的长度。

undo fifo queue-length 命令用来恢复缺省配置。

【命令】

fifo queue-length *queue-length*

undo fifo queue-length

【缺省情况】

先进先出队列的长度为 75。

【视图】

帧中继类视图

【缺省用户角色】

network-admin

【参数】

queue-length：队列的长度，取值范围为 1～1024。

【举例】

配置名为 test1 的帧中继类的 FIFO 队列长度为 80。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-calss-test1] fifo queue-length 80
```

1.1.7 fragment enable

fragment enable 命令用来开启帧中继虚电路的 FRF.12 分片功能。

undo fragment enable 命令用来关闭帧中继虚电路的 FRF.12 分片功能。

【命令】

fragment enable

undo fragment enable

【缺省情况】

帧中继虚电路的 FRF.12 分片功能处于关闭状态。

【视图】

帧中继类视图

【缺省用户角色】

network-admin

【使用指导】

帧中继类开启了分片功能，则关联了该帧中继类的所有虚电路都开启了分片功能。

虚电路下的分片只支持 end-to-end 类型的分片。

【举例】

在名为 test1 的帧中继类下开启帧中继虚电路的 FRR.12 分片功能。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fragment enable
```

【相关命令】

- **fr class**

1.1.8 fragment size

fragment size 命令用来配置帧中继虚电路允许的报文分片长度。

undo fragment size 命令用来恢复缺省情况。

【命令】

fragment size *size*

undo fragment size

【缺省情况】

帧中继虚电路允许的报文分片长度为 45 字节。

【视图】

帧中继类视图

【缺省用户角色】

network-admin

【参数】

size：帧中继分片长度，取值范围为 16～1600，单位为字节。

【举例】

在名为 test1 的帧中继类下配置分片大小为 128 字节。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fragment size 128
```

1.1.9 fr class

fr class 命令用来创建帧中继类，并进入帧中继类视图。如果指定的帧中继类已经存在，则直接进入帧中继类视图。

undo fr class 命令用来删除指定的帧中继类。

【命令】

fr class *class-name*

undo fr class *class-name*

【缺省情况】

不存在帧中继类。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

class-name：帧中继类名称，为 1～30 个字符的字符串，区分大小写。

【使用指导】

只有将帧中继类同帧中继接口或虚电路相关联，并且开启相应接口的帧中继 QoS 功能，配置的帧中继类参数才会起作用。

删除帧中继类时，将释放所有帧中继接口和虚电路与该帧中继类的关联。

【举例】

创建名为 test1 的帧中继类。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1]
```

【相关命令】

- **fr-class**

1.1.10 fr de del

fr de del 命令用来将 DE（Discard Eligibility，合格丢弃）规则列表应用到指定的帧中继虚电路上。

undo fr de del 命令用来从虚电路上删除指定的 DE 规则列表。

【命令】

fr de del *list-number* **dlci** *dlci-number*

undo fr de del *list-number* **dlci** *dlci-number*

【缺省情况】

帧中继虚电路上没有应用 DE 规则列表。

【视图】

帧中继接口视图/MFR 接口视图

【缺省用户角色】

network-admin

【参数】

list-number：DE 规则列表编号，取值范围为 1～10。

dlci-number：帧中继虚电路编号，取值范围为 16～1007。

【使用指导】

在接口视图下配置本命令时，可以将 DE 规则列表应用到主接口及其子接口的帧中继虚电路上。

帧中继虚电路应用了 DE 规则列表后，如果有匹配 DE 规则列表的报文要发送，它会将报文的 DE 标志位置 1。

【举例】

将 DE 规则列表 3 应用到接口 Serial2/1/1 的 DLCI 100 上。

```
<Sysname> system-view
[Sysname] interface Serial 2/1/1
[Sysname-Serial2/1/1] fr dlci 100
[Sysname-Serial2/1/1-fr-dlci-100] quit
[Sysname-Serial2/1/1] fr de del 3 dlci 100
```

【相关命令】

- **fr del inbound-interface**
- **fr del protocol**

1.1.11 fr del inbound-interface

fr del inbound-interface 命令用来配置基于接口的 DE 规则列表。

undo fr del inbound-interface 命令用来从 DE 规则列表内删除指定的 DE 规则。

【命令】

fr del *list-number* **inbound-interface** *interface-type interface-number*

undo fr del *list-number* **inbound-interface** *interface-type interface-number*

【缺省情况】

不存在 DE 规则列表。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

list-number：DE 规则列表的编号，取值范围为 1～10。

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

【使用指导】

对于从指定接口接收的报文，在转发前将它的 DE 标志位置 1。

重复使用本命令可以为 DE 规则列表添加新的规则，每个 DE 规则列表最多可以配置 100 条规则。

删除 DE 规则列表中的最后一条规则时，该 DE 规则列表将被同时删除。

【举例】

在 DE 规则列表 1 内添加一条规则，对于从接口 Serial2/1/1 接收的报文，如果需要封装帧中继协议转发，转发前将报文的 DE 标志位置为 1。

```
<Sysname> system-view
[Sysname] fr del 1 inbound-interface serial 2/1/1
```

【相关命令】

- **fr de del**
- **fr del protocol**

1.1.12 fr del protocol

fr del protocol ip 命令用来配置基于 IP 协议的 DE 规则列表。

undo fr del protocol ip 命令用来从 DE 规则列表内删除指定的 DE 规则。

【命令】

fr del *list-number* **protocol ip** [**acl** *acl-number* | **fragments** | **greater-than** *min-number* | **less-than** *max-number* | **tcp-port** *tcpport-number* | **udp-port** *udpport-number*]

undo fr del *list-number* **protocol ip** [**acl** *acl-number* | **fragments** | **greater-than** *min-number* | **less-than** *max-number* | **tcp-port** *tcpport-number* | **udp-port** *udpport-number*]

【缺省情况】

不存在 DE 规则列表。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

list-number：DE 规则列表编号，取值范围为 1～10。

acl *acl-number*：符合 ACL 匹配条件的 IP 报文。*acl-number* 的取值范围为 2000～3999。

fragments：所有分片的 IP 报文。

greater-than *min-number*：报文长度大于 *min-number* 的 IP 报文。*min-number* 的取值范围为 0～65535，单位为字节。

less-than *max-number*：长度小于 *max-number* 的 IP 报文。*max-number* 的取值范围为 0～65535，单位为字节。

tcp-port *tcpport-number*：源或目的 TCP 端口号为 *tcpport-number* 的 IP 报文。*tcpport-number* 的值既可以直接使用上层应用名称，也可以使用端口号。

- 端口号：取值范围为 0～65535。
- 上层应用名称（括号内为对应的端口号）：可选取 bgp（179）、chargen（19）、cmd（514）、daytime（13）、discard（9）、domain（53）、echo（7）、exec（512）、finger（79）、ftp（21）、frp-data（20）、gopher（70）、hostname（101）、ident（113）、irc（194）、klogin（543）、kshell（544）、login（513）、lpd（515）、nntp（119）、pop2（109）、pop3（110）、smtp（25）、sunrpc（111）、tacacs（49）、talk（517）、telnet（23）、time（37）、uucp（540）、whois（43）或 www（80）。

udp-port *udpport-number*：源或目的 UDP 端口号为 *udpport-number* 的 IP 报文。*udpport-number* 的值既可以直接使用上层应用名称，也可以使用相关端口号。

- 端口号：取值范围为 0～65535。
- 上层应用名称（括号内为对应的端口号）：可选取 biff（512）、bootpc（68）、bootps（67）、discard（9）、dnsix（195）、domain（53）、echo（7）、mobile-ip（434）、nameserver（42）、netbios-dgm（138）、netbios-ns（137）、ntp（123）、rip（520）、snmp（161）、snmptrap（162）、sunrpc（111）、syslog（514）、tacacs（49）、talk（517）、tftp（69）、time（37）、who（513）或 xdmcp（177）。

【使用指导】

如果不指定任何参数，则为所有 IP 报文配置 DE 规则列表。

重复使用本命令可以为 DE 规则列表添加新的规则，每个 DE 规则列表最多可以配置 100 条规则。同一个 DE 规则列表中可以同时存在 **inbound-interface** 和 **protocol ip** 两种规则。

如果要删除一个 DE 规则列表，则必须先删除列表中的所有 DE 规则。

【举例】

在 DE 规则列表 1 内添加一条规则，对所有封装 IP 报文的帧中继报文，将其 DE 标志位置为 1。

```
<Sysname> system-view
[Sysname] fr del 1 protocol ip
```

【相关命令】

- **fr de del**
- **fr del inbound-interface**

1.1.13 fr traffic-policing

fr traffic-policing 命令用来开启帧中继流量监管功能。

undo fr traffic-policing 命令用来关闭帧中继流量监管功能。

【命令】

fr traffic-policing

undo fr traffic-policing

【缺省情况】

帧中继流量监管功能处于关闭状态。

【视图】

帧中继接口视图/MFR 接口视图

【缺省用户角色】

network-admin

【使用指导】

帧中继流量监管功能只能应用在帧中继网络的 DCE 端接口的入方向。

【举例】

开启接口 Serial2/1/1 的流量监管功能。

```
<Sysname> system-view
[Sysname] interface Serial 2/1/1
[Sysname-Serial2/1/1] fr traffic-policing
```

【相关命令】

- **fr class**

1.1.14 fr traffic-shaping

fr traffic-shaping 命令用来开启帧中继流量整形功能。

undo fr traffic-shaping 命令用来关闭帧中继流量整形功能。

【命令】

fr traffic-shaping

undo fr traffic-shaping

【缺省情况】

帧中继流量整形功能处于关闭状态。

【视图】

帧中继接口视图

【缺省用户角色】

network-admin

【使用指导】

帧中继流量整形功能应用于设备的出接口上，通常应用于帧中继网络的 DTE 端。

接口开启分片功能的情况下不能开启流量整形功能。

【举例】

在串口 Serial2/1/1 上开启帧中继流量整形功能。

```
<Sysname> system-view
[Sysname] interface serial 2/1/1
[Sysname-Serial2/1/1] fr traffic-shaping
```

1.1.15 fr-class

fr-class 命令用来将帧中继类与当前帧中继接口或虚电路关联起来。

undo fr-class 命令用来取消帧中继类与当前帧中继接口或虚电路的关联。

【命令】

fr-class *class-name*

undo fr-class *class-name*

【缺省情况】

帧中继类未与帧中继接口或虚电路相关联。

【视图】

帧中继接口视图（包括主接口和子接口）/帧中继 DLCI 视图

【缺省用户角色】

network-admin

【参数】

class-name：帧中继类的名称，为 1～30 个字符的字符串，区分大小写。该帧中继类必须已经存在。

【使用指导】

将一个帧中继类和接口关联起来之后，此接口上的所有虚电路都会继承此帧中继类的帧中继 QoS 参数。

【举例】

将名为 test1 的帧中继类与 DLCI 为 200 的帧中继虚电路关联起来。

```
<Sysname> system-view
[Sysname] interface serial 2/1/1
[Sysname-Serial2/1/1] fr dlci 200
[Sysname-Serial2/1/1-fr-dlci-200] fr-class test1
```

【相关命令】

- **fr class**

1.1.16 traffic-shaping adaptation

traffic-shaping adaptation 命令用来开启帧中继流量整形的自适应流量调节功能。

undo traffic-shaping adaptation 命令用来关闭帧中继流量整形的自适应流量调节功能。

【命令】

traffic-shaping adaptation { **becn** | **interface-congestion** *number* }

undo traffic-shaping adaptation { **becn** | **interface-congestion** }

【缺省情况】

帧中继流量整形的自适应流量调节功能处于关闭状态。

【视图】

帧中继类视图

【缺省用户角色】

network-admin

【参数】

becn：对带 BECN 标志的帧中继报文进行流量调节。

interface-congestion *number*：根据接口出队列中的报文数进行流量调节。*number* 表示接口出队列中的报文个数，取值范围为 1～40。

【使用指导】

如果配置调节方式为基于 BECN 调节，当路由器发送接口接收到帧中继网络发送过来的报文带有 BECN 标志时，所有开启了 FRTS 的 PVC 将开始下降发送速率，当路由器在 16 次自适应调节定时器超时时间之内没有收到带 BECN 标志的报文的时候则开始上升速率。

如果配置调节方式为基于 interface-congestion 调节，当发送接口的出队列的报文数到达设定值的时候，所有开启了 FRTS 的 PVC 将开始下降发送速率，当队列报文数小于设定值的时候则上升发送速率。

【举例】

开启对带 BECN 标志的帧中继报文的自适应流量调节功能。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] traffic-shaping adaptation becn
```

【相关命令】

- **fr traffic-shaping**

1.1.17 traffic-shaping adaptation percentage

traffic-shaping adaptation percentage 命令用来配置帧中继流量整形自适应流量调节的比例。

undo traffic-shaping adaptation percentage 命令用来恢复缺省情况。

【命令】

traffic-shaping adaptation percentage *number*

undo traffic-shaping adaptation percentage

【缺省情况】

帧中继流量整形自适应流量调节的比例为 25。

【视图】

帧中继类视图

【缺省用户角色】

network-admin

【参数】

number：帧中继流量整形自适应流量调节的比例（百分比），取值范围为 1～30。

【使用指导】

开启了帧中继流量整形的自适应流量调节功能后，当满足自适应调节的条件时，报文发送速率会以一定的百分比上升或下降，每次上升或下降的幅度为当前速率与百分比的乘积，调整后的速率最高上升到 CIR ALLOW、最低下降到 CIR。例如，当前的速率为 3000bps，调节比例为 20，CIR 的值为 2500bps，调整下降后的速率为 2400bps（3000-3000*20%），此时 2400 < 2500，因此下降后的速率应为 2500bps。

【举例】

配置帧中继流量整形自适应流量调节的比例为 20。

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] traffic-shaping adaptation 20
```

【相关命令】

- **fr traffic-shaping**

目 录

1 时间段 ····· 1-1
1.1 时间段配置命令 ····· 1-1
1.1.1 display time-range ····· 1-1
1.1.2 time-range ····· 1-2

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

【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。

all：显示所有时间段的配置和状态信息。

【举例】

显示时间段 t4 的配置和状态信息。

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

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

表1-1 display time-range 命令显示信息描述表

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

1.1.2 time-range

time-range 命令用来创建一个时间段，来描述一个特定的时间范围。如果指定的时间段已经创建，则本命令可以修改时间段的时间范围。

undo time-range 命令用来删除一个时间段。

【命令】

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

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

【缺省情况】

不存在时间段。

【视图】

系统视图

【缺省用户角色】

network-admin

【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。为避免混淆，时间段的名称不允许使用英文单词 all。

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

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

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

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

to *time2 date2*：指定绝对时间段的结束时间。*time2* 的格式为 hh:mm，取值范围为 00:00～24:00。*date2* 的格式为 MM/DD/YYYY 或 YYYY/MM/DD。MM 表示月，取值范围为 1～12；DD 表示日，取值范围取决于所输入的月份；YYYY 表示年，取值范围为 1970～2100。结束时间必须大于起始

时间。若未指定本参数，绝对时间段的结束时间将为系统可表示的最晚时间，即 2100 年 12 月 31 日 24 点 0 分。

【使用指导】

如果指定名称的时间段不存在，则创建一个新的时间段（最多 1024 个）；如果指定名称的时间段已存在，则对旧时间段进行修改，即在其原有内容的基础上叠加新的内容。

在一个时间段中，可以使用以下两种方式定义时间范围：

- 使用 *start-time* **to** *end-time days* 这组参数所创建的时间段为周期时间段，它将以一周为周期循环生效。
- 使用 **from** *time1 date1* 和 **to** *time2 date2* 这组参数所创建的时间段为绝对时间段，它将在指定时间范围内生效。

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

一个时间段内可包含一或多个周期时间段（最多 32 个）和绝对时间段（最多 12 个），当包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。

【举例】

创建名为 t1 的时间段，其时间范围为每周工作日的 8 点到 18 点。

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

创建名为 t2 的时间段，其时间范围为 2011 年全年。

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

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

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

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

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

【相关命令】

- **display time-range**