H3C 无线控制器产品

ACL 和 QoS 命令参考

新华三技术有限公司
http://www.h3c.com

资料版本：6W106-20190325

H3C、H3C、H3CS、H3CIE、H3CNE、Aolynk、Aolynk、H^{3}Care、H3care、IRF、NetPilot、Netflow、SecEngine、SecPath、SecCenter、SecBlade、Comware、ITCMM、HUASAN、华三均为新华三技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

H3C 无线控制器产品命令参考介绍了各个系列无线控制器和无线控制器业务板全部命令行，包括命令行功能，支持的关键字和参数，以及缺省取值和配置相关注意事项等，本手册主要介绍了 ACL 和 QoS 配置命令。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

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

本书约定

1. 命令行格式约定

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

2. 图形界面格式约定

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

格　式	意　义
	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一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 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

说明

WX1800H 系列、WX2500H 系列和 WX3000H 系列不支持 slot 参数。

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：

系列	型号	产品代码	特性	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	ACL	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		支持
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		WX3010H支持 WX3010H-X支持 WX3010H-L不支持 WX3024H支持 WX3024H-L不支持 WX3024H-F支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

1.1 ACL配置命令

1.1.1 acl

acl 命令用来创建一个 ACL，并进入相应的 ACL 视图。

undo acl 命令用来删除指定或全部 ACL。

【命令】

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

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

acl wlan client { *acl-number* | **name** *acl-name* }

acl wlan ap { *acl-number* | **name** *acl-name* }

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

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

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

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

【缺省情况】

不存在任何 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。

wlan client：指定创建无线客户端 ACL。

wlan ap：指定创建无线接入点 ACL。

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

- 100～199：表示无线客户端 ACL。
- 200～299：表示无线接入点 ACL。
- 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。无线客户端 ACL、无线接入点 ACL 不支持本参数，其规则匹配顺序只能为配置顺序。

all：指定类型中全部 ACL。

【使用指导】

- 使用 **acl** 命令时，如果指定编号或名称的 ACL 不存在，则创建该 ACL 并进入其视图，否则直接进入其视图。
- 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** 参数，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、日志操作和时间段之外的其它匹配项，则设备转发 ACL 匹配的这类报文时会启用慢转发流程。慢转发时设备会将报文上送控制平面，计算报文相应的表项信息。执行慢转发流程时，设备的转发能力将会有所降低。

【举例】

创建一个编号为 2000 的 IPv4 基本 ACL，并进入其视图。

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

创建一个 IPv4 基本 ACL，指定其名称为 flow，并进入其视图。

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

创建一个编号为 3000 的 IPv4 高级 ACL，并进入其视图。

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

创建一个编号为 2000 的 IPv6 基本 ACL，并进入其视图。

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

创建一个 IPv6 基本 ACL，其名称为 flow，并进入其视图。

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

创建一个 IPv6 高级 ACL，其名称为 abc，并进入其视图。

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

创建一个编号为 4000 的二层 ACL，并进入其视图。

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

创建一个二层 ACL，其名称为 flow，并进入其视图。

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

创建一个编号为 100 的无线客户端 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl wlan client 100
[Sysname-acl-client-100]
```

创建一个无线客户端 ACL，指定其名称为 flow，并进入其视图。

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

创建一个编号为 200 的无线接入点 ACL，并进入其视图。

```
<Sysname> system-view
[Sysname] acl wlan ap 200
[Sysname-acl-ap-200]
```

创建一个无线接入点 ACL，指定其名称为 flow，并进入其视图。

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

【相关命令】

- **display acl**

1.1.2 acl copy

acl copy 命令用来复制并生成一个新的 ACL。

【命令】

acl [**ipv6** | **mac**] **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：

- 100～199：表示无线客户端 ACL。
- 200～299：表示无线接入点 ACL。
- 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：

- 100～199：表示无线客户端 ACL。
- 200～299：表示无线接入点 ACL。
- 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使能情况、规则编号的步长、所包含的规则、规则的描述信息以及 ACL 的描述信息等都与源 ACL 的相同。
- 若未指定 **ipv6** 或 **mac** 参数，则表示 IPv4、无线客户端或者无线接入点 ACL。

【举例】

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

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

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

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

1.1.3 acl 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。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

trap：指定周期性地生成告警信息并发送到 SNMP 模块。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

interval *interval*：报文过滤日志信息或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 和 IPv6 高级 ACL 进行报文过滤的报文过滤告警信息进行记录。

【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)

1.1.4 description

description 命令用来配置 ACL 的描述信息。

undo description 命令用来删除 ACL 的描述信息。

【命令】

description *text*

undo description

【缺省情况】

ACL 没有任何描述信息。

【视图】

IPv4 基本 ACL 视图/IPv4 高级 ACL 视图/IPv6 基本 ACL 视图/IPv6 高级 ACL 视图/二层 ACL 视图/无线客户端 ACL 视图/无线接入点 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**

1.1.5 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** | **wlan**] { *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。

wlan：指定 ACL 类型为无线 ACL，包括无线客户端 ACL 和无线接入点 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：

- 100～199：表示无线客户端 ACL。
- 200～299：表示无线接入点 ACL。
- 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**、**mac** 或 **wlan** 参数，则表示 IPv4 ACL。

【举例】

显示 IPv4 基本 ACL 2001 的配置和运行情况。

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

表1-1 display acl 命令显示信息描述表

字段	描述
Basic IPv4 ACL 2001	该ACL的类型和编号，ACL的类型包括： • Basic IPv4 ACL：表示 IPv4 基本 ACL • Advanced IPv4 ACL：表示 IPv4 高级 ACL • Basic IPv6 ACL：表示 IPv6 基本 ACL • Advanced IPv6 ACL：表示 IPv6 高级 ACL • MAC ACL：表示二层 ACL • WLAN CLIENT ACL：表示无线客户端 ACL • WLAN AP ACL：表示无线接入点 ACL
1 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
rule 5 permit source 1.1.1.1 0	规则5的具体内容，源地址为具体地址
rule 5 comment This rule is used on GigabitEthernet 1/0/1.	规则5的描述信息

1.1.6 display packet-filter

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

【命令】

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

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：

系列	型号	产品代码	命令	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	**display packet-filter interface**	支持
WX2500H系列	WX2510H WX2510H-F	EWP-WX2510H-PWR EWP-WX2510H-F-PWR		支持

系列	型号	产品代码	命令	描述
	WX2540H WX2540H-F WX2560H	EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		不支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

【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，这里的接口类型不包括 VLAN 接口。若未指定接口类型和接口编号，将显示除 VLAN 接口以外的所有接口上 ACL 在报文过滤中的应用情况。

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，将显示所有成员设备上 ACL 在报文过滤中的应用情况。

【使用指导】

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

【举例】

显示接口 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
 In-bound policy:
  IPv4 ACL 2001
  IPv6 ACL 2002 (Failed)
  MAC ACL 4003 (Failed)
  IPv4 ACL 2004
  IPv4 default action: Deny
```

表1-2 display packet-filter 命令显示信息描述表

字段	描述
Interface	ACL在指定接口上的应用情况
In-bound policy	ACL在入方向上的应用情况
Out-bound policy	ACL在出方向上的应用情况
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： • 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

1.1.7 display packet-filter verbose

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

【命令】

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

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：

系列	型号	产品代码	命令	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	**display packet-filter verbose interface**	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		支持
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		不支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

【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 **slot** 参数。

inbound：显示入方向上 ACL 在报文过滤中的详细应用情况。

outbound：显示出方向上 ACL 在报文过滤中的详细应用情况。

ipv6：指定 ACL 类型为 IPv6 ACL。

mac：指定 ACL 类型为二层 ACL。

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，将显示所有成员设备上 ACL 在报文过滤中的详细应用情况。

【使用指导】

- 若未指定 *acl-number*、**name** *acl-name* 和 ACL 类型（**ipv6**、**mac**）参数，将显示全部 IPv4 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。

【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
 In-bound policy:
  IPv4 ACL 2001
   rule 0 permit
   rule 5 permit source 1.1.1.1 0 (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
```

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

字段	描述
Interface	ACL在指定接口上的详细应用情况
In-bound policy	ACL在入方向上的详细应用情况
Out-bound policy	ACL在出方向上的详细应用情况
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

1.1.8 packet-filter

packet-filter 命令用来在接口上应用 ACL 进行报文过滤。

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

【命令】

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

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

系列	型号	产品代码	命令	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	**packet-filter**	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F		支持

系列	型号	产品代码	命令	描述
	WX2560H	EWP-WX2560H		
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		不支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

【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 verbose**

1.1.9 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

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：

系列	型号	产品代码	命令	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	**packet-filter default deny**	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		支持
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		不支持
WX3500H系列	WX3508H WX3510H	EWP-WX3508H EWP-WX3510H		支持

系列	型号	产品代码	命令	描述
	WX3520H WX3520H-F WX3540H	EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

【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 verbose**

1.1.10 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** *vlan-pri* | **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* [**time-range**]

【缺省情况】

二层 ACL 内不存在任何规则。

【视图】

二层 ACL 视图

【缺省用户角色】

network-admin

【参数】

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

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

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

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

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

【举例】

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

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

1.1.11 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** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *

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

【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 1-4 所示的规则信息参数。

表1-4 规则信息参数

参数	类别	作用	说明
source { *source-address* *source-wildcard* | **any** }	源地址信息	指定ACL规则的源地址信息	*source-address*：源IP地址 *source-wildcard*：源IP地址的通配符掩码（为0表示主机地址） **any**：任意源IP地址
destination { *dest-address* *dest-wildcard* | **any** }	目的地址信息	指定ACL规则的目的地址信息	*dest-address*：目的IP地址 *dest-wildcard*：目的IP地址的通配符掩码（为0表示主机地址） **any**：任意目的IP地址
precedence *precedence*	报文优先级	IP优先级	*precedence*用数字表示时，取值范围为0～7；用文字表示时，分别对应**routine**、**priority**、**immediate**、**flash**、**flash-override**、**critical**、**internet**、**network**
tos *tos*	报文优先级	ToS优先级	*tos*用数字表示时，取值范围为0～15；用文字表示时，可以选取**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）、**min-monetary-cost**（1）、**normal**（0）
dscp *dscp*	报文优先级	DSCP优先级	*dscp*用数字表示时，取值范围为0～63；用文字表示时，可以选取**af11**（10）、**af12**（12）、**af13**（14）、**af21**（18）、**af22**（20）、**af23**（22）、**af31**（26）、**af32**（28）、**af33**（30）、**af41**（34）、**af42**（36）、**af43**（38）、**cs1**（8）、**cs2**（16）、**cs3**（24）、**cs4**（32）、**cs5**（40）、**cs6**（48）、**cs7**（56）、**default**（0）、**ef**（46）
fragment	分片信息	仅对分片报文的非首个分片有效，而对非分片报文和分片报文的首个分片无效	若未指定该参数，则表示该规则对所有报文（包括非分片报文和分片报文的每个分片）均有效
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

参数	类别	作用	说明
			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”

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-5 所示的规则信息参数。

表1-5 TCP/UDP 特有的规则信息参数

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

设备各款型对于本命令的参数支持情况有所不同，详细差异信息如下：

系列	型号	产品代码	参数	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	**neq**	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F		支持

系列	型号	产品代码	参数	描述
	WX2560H	EWP-WX2560H		
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		WX3010H不支持 WX3010H-X支持 WX3010H-L不支持 WX3024H不支持 WX3024H-L不支持 WX3024H-F不支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

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

表1-6 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1-7所示

表1-7 ICMP 消息名称与消息类型和消息码的对应关系

ICMP 消息名称	ICMP 消息类型	ICMP 消息码
echo	8	0

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

【使用指导】

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

【举例】

为 IPv4 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**
- **display acl**
- **step**
- **time-range**（ACL 和 QoS 命令参考/时间段）

1.1.12 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** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *

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

【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。

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

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

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

【使用指导】

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

【举例】

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

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

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

【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 1-8 所示的规则信息参数。

表1-8 规则信息参数

参数	类别	作用	说明
source { *source-address source-prefix* | *source-address/source-prefix* | **any** }	源IPv6地址	指定ACL规则的源IPv6地址信息	*source-address*：源IPv6地址 *source-prefix*：源IPv6地址的前缀长度，取值范围1～128 **any**：任意源IPv6地址

参数	类别	作用	说明
destination { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** }	目的IPv6地址	指定ACL规则的目的IPv6地址信息	*dest-address*：目的IPv6地址 *dest-prefix*：目的IPv6地址的前缀长度，取值范围1～128 **any**：任意目的IPv6地址
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
routing [**type** *routing-type*]	路由头	指定路由头的类型	*routing-type*：路由头类型的值，取值范围为0～255 若指定了**type** *routing-type*参数，表示仅对指定类型的路由头有效；否则，表示对IPv6所有类型的路由头都有效
hop-by-hop [**type** *hop-type*]	逐跳头	指定逐跳头的类型	*hop-type*：逐跳头类型的值，取值范围为0～255 若指定了**type** *hop-type*参数，表示仅对指定类型的逐跳头有效；否则，表示对IPv6所有类型的逐跳头都有效
time-range *time-range-name*	时间段	指定本规则生效的时间段	*time-range-name*：时间段的名称，为1～32个字符的字符串，不区分大小写。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”

当*protocol*为**tcp**（6）或**udp**（17）时，用户还可配置如 表 1-9 所示的规则信息参数。

表1-9 TCP/UDP 特有的规则信息参数

参数	类别	作用	说明
source-port *operator port1* [*port2*]	源端口	定义TCP/UDP报文的源端口信息	*operator*：操作符，取值可以为**lt**（小于）、**gt**（大于）、**eq**（等于）、**neq**（不等于）或者**range**（在范围内，包括边界值）。只有**range**操作符需要两个端口号做操作数，其它操作符只需要一个端口号做操作数 *port1*/*port2*：TCP或UDP的端口号，用数字表示时，取
destination-port *operator port1*	目的端口	定义TCP/UDP报文的目的端口信息	

参数	类别	作用	说明
[*port2*]			值范围为0～65535；用名称表示时，TCP端口号可选取**chargen**（19）、**bgp**（179）、**cmd**（514）、**daytime**（13）、**discard**（9）、**dns**（53）、**domain**（53）、**echo**（7）、**exec**（512）、**finger**（79）、**ftp**（21）、**ftp-data**（20）、**gopher**（70）、**hostname**（101）、**irc**（194）、**klogin**（543）、**kshell**（544）、**login**（513）、**lpd**（515）、**nntp**（119）、**pop2**（109）、**pop3**（110）、**smtp**（25）、**sunrpc**（111）、**tacacs**（49）、**talk**（517）、**telnet**（23）、**time**（37）、**uucp**（540）、**whois**（43）或**www**（80）；UDP端口号可选取**biff**（512）、**bootpc**（68）、**bootps**（67）、**discard**（9）、**dns**（53）、**dnsix**（90）、**echo**（7）、**mobilip-ag**（434）、**mobilip-mn**（435）、**nameserver**（42）、**netbios-dgm**（138）、**netbios-ns**（137）、**netbios-ssn**（139）、**ntp**（123）、**rip**（520）、**snmp**（161）、**snmptrap**（162）、**sunrpc**（111）、**syslog**（514）、**tacacs-ds**（65）、**talk**（517）、**tftp**（69）、**time**（37）、**who**（513）或**xdmcp**（177）
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	TCP报文标识	定义对携带不同标志位（包括ACK、FIN、PSH、RST、SYN和URG六种）的TCP报文的处理规则	TCP协议特有的参数。表示匹配携带不同标志位的TCP报文，各*value*的取值可为0或1（0表示不携带此标志位，1表示携带此标志位） 对于一条规则中各标志位的配置组合，按照“或”的规则进行匹配。譬如：当配置为**ack** 0 **psh** 1时，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。表示匹配携带ACK或RST标志位的TCP连接报文

设备各款型对于本命令的参数支持情况有所不同，详细差异信息如下：

系列	型号	产品代码	参数	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	**neq**	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		支持
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		WX3010H不支持 WX3010H-X支持 WX3010H-L不支持 WX3024H不支持 WX3024H-L不支持 WX3024H-F不支持
WX3500H系列	WX3508H WX3510H WX3520H	EWP-WX3508H EWP-WX3510H EWP-WX3520H		支持

系列	型号	产品代码	参数	描述
	WX3520H-F WX3540H	EWP-WX3520H-F EWP-WX3540H		
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

当*protocol*为**icmpv6**（58）时，用户还可配置如 表 1-10 所示的规则信息参数。

表1-10 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1-11所示

表1-11 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

ICMPv6 消息名称	ICMPv6 消息类型	ICMPv6 消息码
port-unreachable	1	4
redirect	137	0
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

【使用指导】

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

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

1.1.14 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** } [**fragment** | **routing** [**type** *routing-type*] | **source** { *source-address source-prefix* | *source-address/source-prefix* | **any** } | **time-range** *time-range-name*] *

undo rule *rule-id* [**fragment** | **routing** | **source** | **time-range**] *

【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。

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

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

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

【使用指导】

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

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

1.1.15 rule (WLAN-client ACL view)

rule 命令用来为无线客户端 ACL 创建一条规则。

undo rule 命令用来为无线客户端 ACL 删除一条规则。

【命令】

rule [*rule-id*] { **deny** | **permit** } [**ssid** *ssid-name*]

undo rule *rule-id*

【缺省情况】

无线客户端 ACL 内不存在任何规则。

【视图】

无线客户端 ACL 视图

【缺省用户角色】

network-admin

【参数】

rule-id：指定客户端 ACL 规则的编号，取值范围为 0～65534。如果未指定本参数，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。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 33。

deny：表示拒绝符合条件的报文。

permit：表示允许符合条件的报文。

ssid *ssid-name*：指定 WLAN（Wireless Local Area Network，无线局域网）的 SSID（Service Set Identifier，服务集标识符）名称，*ssid-name* 为 1～32 个字符的字符串，包括字母和数字，区分大小写，允许包含空格。如果未指定本参数，表示该规则对所有 SSID 均有效。

【使用指导】

- 使用 **rule** 命令时，如果指定编号的规则不存在，则创建一条新的规则；如果指定编号的规则已存在，则对旧规则进行修改，即在其原有内容的基础上叠加新的内容。
- 新创建或修改的规则不能与已有规则的内容完全相同，否则将提示错误，并导致该操作失败。
- 使用 **undo rule** 命令时，删除整条规则。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

【举例】

创建无线客户端 ACL 111，规则如下：允许 SSID 为 ME 的报文通过，但拒绝 SSID 为 HIM 的报文通过。

```
<Sysname> system-view
[Sysname] acl wlan client 111
[Sysname-acl-client-111] rule permit ssid ME
[Sysname-acl-client-111] rule deny ssid HIM
```

【相关命令】

- **acl wlan client**
- **display acl**
- **step**

1.1.16 rule (WLAN-AP ACL view)

rule 命令用来为无线接入点 ACL 创建一条规则。

undo rule 命令用来为无线接入点 ACL 删除一条规则。

【命令】

rule [*rule-id*] { **deny** | **permit** } [**mac** *mac-address mac-mask*] [**serial-id** *serial-id*]

undo rule *rule-id*

【缺省情况】

无线接入点 ACL 内不存在任何规则。

【视图】

无线接入点 ACL 视图

【缺省用户角色】

network-admin

【参数】

rule-id：指定无线接入点 ACL 规则的编号，取值范围为 0～65534。如果未指定本参数，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。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 33。

deny：表示拒绝符合条件的无线接入点。

permit：表示允许符合条件的无线接入点。

mac *mac-address mac-mask*：指定无线接入点的 MAC 地址范围。*mac-address* 表示 MAC 地址，格式为 H-H-H；*mac-mask* 表示 MAC 地址的掩码，格式为 H-H-H。如果未指定本参数，则对所有 MAC 生效。

serial-id *serial-id*：指定无线接入点的序列号。*serial-id* 为 1～32 个字符的字符串，不区分大小写。如果未指定本参数，则对所有序列号生效。

【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，否则将提示错误，并导致该操作失败。
- 使用 **undo rule** 命令时删除整条规则。
- 使用 **undo rule** 命令时必须指定一个已存在规则的编号，可以使用 **display acl all** 命令来查看所有已存在的规则。

【举例】

创建无线接入点 ACL 222，规则如下：允许序列号为 210235A42QB095000766 的无线接入点上线，拒绝序列号为 210235A42QB095000777 的无线接入点上线。

```
<Sysname> system-view
[Sysname] acl wlan ap 222
[Sysname-acl-ap-222] rule permit serial-id 210235A42QB095000766
[Sysname-acl-ap-222] rule deny serial-id 210235A42QB095000777
```

【相关命令】

- **acl wlan ap**
- **display acl**
- **step**

1.1.17 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/无线客户端 ACL 视图/无线接入点 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**

1.1.18 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/无线客户端 ACL 视图/无线接入点 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

说明

WX1800H 系列、WX2500H 系列和 WX3000H 系列不支持 slot 参数。

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：

系列	型号	产品代码	特性	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	QoS策略	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		支持
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		WX3010H支持 WX3010H-X支持 WX3010H-L不支持 WX3024H支持 WX3024H-L不支持 WX3024H-F支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

1.1 定义类的命令

1.1.1 display traffic classifier

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

【命令】

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

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

1.1.2 if-match

if-match 命令用来定义匹配数据包的规则。

undo if-match 命令用来删除配置的匹配数据包的规则。

【命令】

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

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

【缺省情况】

没有定义匹配数据包的规则。

【视图】

类视图

【缺省用户角色】

network-admin

【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

取值	描述
	文字母a～z或A～Z开头，为避免混淆，ACL的名称不可以使用英文单词all
any	定义匹配所有数据包的规则
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1-4所示
ip-precedence *ip-precedence-value*&<1-8>	定义匹配IP优先级的规则，*ip-precedence-value*&<1-8>为IP优先级的列表，IP优先级的取值范围为0～7，&<1-8>表示前面的参数最多可以输入8次
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
protocol *protocol-name*	定义匹配协议的规则，*protocol-name*取值为arp、bittorrent、ip、ipv6
source-mac *mac-address*	定义匹配源MAC地址的规则

【使用指导】

在定义各个规则的时候，注意事项如下：

(1) 定义匹配 ACL 的规则

- 如果类中引用的 ACL 不存在，则不能在硬件中下发。
- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 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**。
  - 如果分类 operator 是 or，则继续后面的 if-match 匹配。
  - 如果分类 operator 是 and，则跳出该分类。

(2) 定义匹配目的 MAC 地址规则

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

(3) 定义匹配源 MAC 地址规则

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

(4) 定义匹配 DSCP 的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。

- 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。

(5) 定义匹配内层 VLAN Tag 802.1p 优先级的规则

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

(6) 定义匹配 IP 优先级的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。
- 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。

(7) 定义匹配本地优先级的规则

- 一个类下可配置多条这样的命令，各个配置之间互相不覆盖。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。

(8) 定义匹配内层 VLAN Tag 的规则

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

【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
[Sysname-classifier-class1] if-match dscp 1 6 9
```

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

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

定义类 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
[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：匹配内层 VLAN Tag 的 VLAN ID 值为 1 或 6 或 9 的报文。

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

1.1.3 traffic classifier

traffic classifier 命令用来定义一个类，并进入类视图。

undo traffic classifier 命令用来删除一个类。

【命令】

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

undo traffic classifier *classifier-name*

【缺省情况】

没有定义类。

【视图】

系统视图

【缺省用户角色】

network-admin

【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 命令用来取消流量监管动作配置。

【命令】

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

undo car

【缺省情况】

没有配置流量监管动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【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。

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*：数据包的流量不符合承诺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**。（暂不支持）

action：对数据包采取的动作，有以下几种：

- **discard**：丢弃数据包。
- **pass**：允许数据包通过。

【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。
- 如果多次使用该命令在同一个流行为上配置，最后一次配置生效。

【举例】

为流行为配置流量监管。报文正常流速为 200kbps，承诺突发尺寸为 51200bytes。

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 51200 green pass
```

1.2.2 display traffic behavior

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

【命令】

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

【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)
      Filter enable: Permit
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
```

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)
      -none-

    Behavior: ef (ID 2)
      -none-

    Behavior: be-flow-based (ID 3)
      -none-
```

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

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

字段	描述
CIR	承诺信息速率，单位为kbps
CBS	承诺突发尺寸，单位为byte
EBS	超出突发尺寸，单位为byte（暂不支持）
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（暂不支持）
Filter enable	流量过滤动作
none	表示没有配置其他流行为

1.2.3 filter

filter 命令用来配置流量过滤动作。

undo filter 命令用来取消流量过滤动作配置。

【命令】

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

undo filter

【缺省情况】

没有配置流量过滤动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【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
```

1.2.4 remark dscp

remark dscp 命令用来重新标记报文的 DSCP 值。

undo remark dscp 命令用来取消标记报文的 DSCP 值。

【命令】

remark dscp *dscp-value*

undo remark dscp

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【参数】

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

表1-4 DSCP 关键字与值的对应表

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

【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
```

1.2.5 remark local-precedence

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

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

【命令】

remark local-precedence *local-precedence-value*

undo remark local-precedence

【缺省情况】

没有配置重新标记报文的动作。

【视图】

流行为视图

【缺省用户角色】

network-admin

【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
```

1.2.6 traffic behavior

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

undo traffic behavior 命令用来删除一个流行为。

【命令】

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

【缺省情况】

没有定义流行为。

【视图】

系统视图

【缺省用户角色】

network-admin

【参数】

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

【举例】

定义一个名为 behavior1 的流行为。

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

【相关命令】

- **display traffic behavior**

1.3 定义策略和应用策略的命令

1.3.1 classifier behavior

classifier behavior 命令用来为类指定流行为。

undo classifier 命令用来取消为类指定的流行为。

【命令】

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

undo classifier *classifier-name*

【缺省情况】

没有为类指定流行为。

【视图】

策略视图

【缺省用户角色】

network-admin

【参数】

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

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

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

【使用指导】

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

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

system-defined：系统定义策略。

user-defined：用户定义策略。

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

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

slot *slot-number*：显示指定成员设备的策略的信息，*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。

【举例】

显示用户定义策略的配置信息。

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

  User-defined QoS policy information:

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

```
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 112 (kbps), CBS 5120 (Bytes), EBS 0 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
   Classifier: 3 (ID 102)
     Behavior: 3
      -none-
```

显示系统定义策略的配置信息。

```
<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
      -none-
   Classifier: af1 (ID 2)
     Behavior: af
      -none-
   Classifier: af2 (ID 3)
     Behavior: af
      -none-
   Classifier: af3 (ID 4)
     Behavior: af
      -none-
   Classifier: af4 (ID 5)
     Behavior: af
      -none-
```

表1-5 display qos policy 命令显示信息描述表

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

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.3 display qos policy interface

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

【参数】

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

inbound：显示对接口接收到的报文应用 QoS 策略的信息。

outbound：显示对接口发送的报文应用 QoS 策略的信息。

【使用指导】

- 如果未指定显示方向，则同时显示出入两个方向接口上应用 QoS 策略的配置信息和运行情况。
- 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: 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 0 (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
     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1-6 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（不支持）
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.4 display qos policy 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】

display qos policy user-profile [**name** *profile-name*] [**user-id** *user-id*] [**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：

系列	型号	产品代码	命令	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	**display qos policy user-profile**	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		支持
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		不支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

【缺省情况】

无

【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。

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 1:
    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 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-
       Classifier: a
        Operator: AND
        Rule(s) :
```

```
 If-match any
Behavior: a
 Committed Access Rate:
   CIR 100 (kbps), CBS 6250 (Bytes), EBS 0 (Bytes)
   Green action  : pass
   Yellow action : pass
   Red action    : discard
   Green packets : 0 (Packets)
   Red packets   : 0 (Packets)
```

表1-7 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
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（不支持）
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（不支持）
Red packets	红色报文的流量统计

其它显示信息解释请参见 表 1-1 和 表 1-3。

1.3.5 qos apply policy (interface view)

qos apply policy 命令用来在接口上应用 QoS 策略。

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

【命令】

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

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

【缺省情况】

没有在接口上应用 QoS 策略。

【视图】

接口视图

【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】

策略在接口上应用的规则为在应用策略时，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允许的可用带宽，则在该接口不可应用。如果对接口修改了可用带宽，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允许的可用带宽，则将策略删除。

【举例】

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

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

1.3.6 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：

系列	型号	产品代码	命令	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	**qos apply policy**	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		支持
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		不支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E	EWP-WX5510E		支持

系列	型号	产品代码	命令	描述
	WX5540E	EWP-WX5540E		
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

【缺省情况】

没有在 User Profile 下应用 QoS 策略。

【视图】

User Profile 视图

【缺省用户角色】

network-admin

【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
```

1.3.7 qos policy

qos policy 命令用来定义一个策略，并进入策略视图。

undo qos policy 命令用来删除一个策略。

【命令】

qos policy *policy-name*

undo qos policy *policy-name*

【缺省情况】

没有定义策略。

【视图】

系统视图

【缺省用户角色】

network-admin

【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**

2 优先级映射

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：

系列	型号	产品代码	特性	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	优先级映射	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		支持
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		WX3010H支持 WX3010H-X支持 WX3010H-L不支持 WX3024H支持 WX3024H-L不支持 WX3024H-F支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

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 [**dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **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
dot11e-lp	802.11e优先级到本地优先级映射表
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-dot11e	本地优先级到802.11e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。
- 如果未指定任何参数，即 **display qos map-table** 命令将显示所有映射表的配置情况。

【举例】

显示 802.1p 优先级到本地优先级映射表的配置信息。

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

表2-2 display qos map-table 命令显示信息描述表

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

2.1.2 import

import 命令用来配置指定优先级映射表的映射关系。

undo import 命令用来删除配置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 优先级到丢弃优先级映射表的映射关系，与 802.1p 优先级 4、5 相对应的丢弃优先级为 1。

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

【相关命令】

- **display qos map-table**

2.1.3 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 { **dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp** }

【视图】

系统视图

【缺省用户角色】

network-admin

【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-dot1p-lp]
```

【相关命令】

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

2.2 端口优先级配置命令

2.2.1 qos priority

qos priority 命令用来配置当前端口的端口优先级。

undo qos priority 命令用来恢复端口优先级为缺省值。

【命令】

qos priority *priority-value*

undo qos priority

【缺省情况】

端口优先级为 0。

【视图】

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

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。

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

表2-3 display qos trust interface 命令显示信息描述表

字段	描述
Interface	接口名，由接口类型和接口编号构成
Port priority information	端口优先级信任信息
Port priority	端口优先级
Port dot1p priority	端口802.1p优先级
Port dscp priority	端口DSCP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】

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。

【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

3.1 流量监管配置命令

3.1.1 qos car

qos car 命令用来在 User Profile 下配置流量监管。

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*]

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：

系列	型号	产品代码	命令	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	**qos car { inbound | outbound } any cir**	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		支持
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		不支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40		支持

系列	型号	产品代码	命令	描述
	LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		

【缺省情况】

没有配置流量监管。

【视图】

User Profile 视图

【缺省用户角色】

network-admin

【参数】

inbound：对上线用户发送的报文进行限速。

outbound：对上线用户接收到的报文进行限速。

any：对所有的 IP 数据包进行限速。

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

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。

【使用指导】

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

如果多次重复使用该命令，则最后一次配置生效。

【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
```

目 录

1 时间段

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：

系列	型号	产品代码	特性	描述
WX1800H系列	WX1804H	EWP-WX1804H-PWR-CN	时间段	支持
WX2500H系列	WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H		支持
WX3000H系列	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F		WX3010H支持 WX3010H-X支持 WX3010H-L不支持 WX3024H支持 WX3024H-L不支持 WX3024H-F支持
WX3500H系列	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H		支持
WX5500E系列	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E		支持
WX5500H系列	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H		支持
AC插卡系列	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F		支持

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 09:40:55 5/26/2015 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2014 to 00:00 1/1/2015
 from 00:00 6/1/2015 to 00:00 7/1/2015
```

表1-1 display time-range 命令显示信息描述表

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

1.1.2 time-range

time-range 命令用来创建一个时间段，来描述一个特定的时间范围。

undo time-range 命令用来删除一个时间段。

【命令】

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

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

【缺省情况】

不存在任何时间段。

【视图】

系统视图

【缺省用户角色】

network-admin

【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】

- 使用 **time-range** 命令时，如果指定名称的时间段不存在，则创建一个新的时间段（最多 1024 个）；如果指定名称的时间段已存在，则对旧时间段进行修改，即在其原有内容的基础上叠加新的内容。

- 使用 *start-time* **to** *end-time days* 这组参数所创建的时间段为周期时间段，它将以一周为周期循环生效；使用 **from** *time1 date1* 和 **to** *time2 date2* 这组参数所创建的时间段为绝对时间段，它将在指定时间范围内生效；而同时使用了上述两组参数所创建的时间段，将取周期时间段和绝对时间段的交集作为生效的时间范围，譬如：创建一个时间段，既定义其在每周一的 8 点到 12 点生效，又定义其在 2011 年全年生效，那么其最终将在 2011 年全年内每周一的 8 点到 12 点生效。
- 一个时间段内可包含一或多个周期时间段（最多 32 个）和绝对时间段（最多 12 个），当包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。

【举例】

创建名为 t1 的时间段，其时间范围为每周工作日的 8 点到 18 点。

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

创建名为 t2 的时间段，其时间范围为 2015 年全年。

```
<Sysname> system-view
[Sysname] time-range t2 from 00:00 1/1/2015 to 24:00 12/31/2015
```

创建名为 t3 的时间段，其时间范围为 2015 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 1/1/2015 to 24:00 12/31/2015
```

创建名为 t4 的时间段，其时间范围为 2015 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 1/1/2015 to 24:00 1/31/2015
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2015 to 24:00 6/30/2015
```

【相关命令】

- **display time-range**