



# H3C MSR Router Series

## Comware 5 ACL and QoS Command Reference

New H3C Technologies Co., Ltd.  
<http://www.h3c.com>



Software version: MSR-CMW520-R2516  
Document version: 20180820-C-1.13

Copyright © 2006-2018, New H3C Technologies Co., Ltd. and its licensors

### All rights reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of New H3C Technologies Co., Ltd.

### Trademarks

H3C, **H3C**, H3CS, H3CIE, H3CNE, Aolynk,  , H<sup>3</sup>Care,  , IRF, NetPilot, Netflow, SecEngine, SecPath, SecCenter, SecBlade, Comware, ITCMM and HUASAN are trademarks of New H3C Technologies Co., Ltd.

All other trademarks that may be mentioned in this manual are the property of their respective owners.

### Notice

The information in this document is subject to change without notice. All contents in this document, including statements, information, and recommendations, are believed to be accurate, but they are presented without warranty of any kind, express or implied. H3C shall not be liable for technical or editorial errors or omissions contained herein.

# Preface

This command reference describes the ACL and QoS configuration commands.

This preface includes the following topics about the documentation:

- [Audience.](#)
- [Conventions.](#)
- [Documentation feedback.](#)

## Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators working with the routers.

## Conventions

The following information describes the conventions used in the documentation.





### Command conventions

Convention	Description
<b>Boldface</b>	<b>Bold</b> text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x   y   ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[ x   y   ... ]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x   y   ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select a minimum of one.
[ x   y   ... ] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.













### GUI conventions

Convention	Description
<b>Boldface</b>	Window names, button names, field names, and menu items are in Boldface. For example, the <b>New User</b> window opens; click <b>OK</b> .
>	Multi-level menus are separated by angle brackets. For example, <b>File &gt; Create &gt; Folder</b> .

## Symbols

Convention	Description
 <b>WARNING!</b>	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 <b>CAUTION:</b>	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 <b>IMPORTANT:</b>	An alert that calls attention to essential information.
<b>NOTE:</b>	An alert that contains additional or supplementary information.
 <b>TIP:</b>	An alert that provides helpful information.

## Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

## Examples provided in this document

Examples in this document might use devices that differ from your device in hardware model, configuration, or software version. It is normal that the port numbers, sample output, screenshots, and other information in the examples differ from what you have on your device.

# Documentation feedback

You can e-mail your comments about product documentation to [info@h3c.com](mailto:info@h3c.com).

We appreciate your comments.

# Contents

ACL configuration commands .....	1
acl .....	1
acl copy .....	2
acl ipv6 .....	3
acl ipv6 copy .....	4
acl ipv6 name .....	5
acl name .....	6
description .....	6
display acl .....	7
display acl ipv6 .....	9
display time-range .....	10
reset acl counter .....	11
reset acl ipv6 counter .....	12
rule (Ethernet frame header ACL view) .....	13
rule (IPv4 advanced ACL view) .....	14
rule (IPv4 basic ACL view) .....	18
rule (IPv6 advanced ACL view) .....	20
rule (IPv6 basic ACL view) .....	23
rule (simple ACL view) .....	25
rule (user-defined ACL view) .....	28
rule (WLAN ACL view) .....	29
rule comment .....	30
rule remark .....	31
step .....	33
time-range .....	34
QoS policy commands .....	37
Class commands .....	37
display traffic classifier .....	37
if-match .....	38
traffic classifier .....	43
Traffic behavior commands .....	44
car .....	44
display traffic behavior .....	46
filter .....	48
gts .....	48
gts percent .....	49
redirect .....	50
remark dot1p .....	51
remark dscp .....	52
remark ip-precedence .....	53
remark qos-local-id .....	53
traffic behavior .....	54
traffic-policy .....	55
QoS policy configuration and application commands .....	56
classifier behavior .....	56
display qos policy .....	56
display qos policy interface .....	58
qos apply policy (interface view, port group view, PVC view) .....	62
qos apply policy (user-profile view) .....	63
qos policy .....	64
Policy-based traffic rate statistics collecting interval commands .....	65
qos flow-interval .....	65
Priority mapping commands .....	66
Priority mapping table commands .....	66
display qos map-table .....	66

import .....	68
qos map-table .....	68
Port priority commands .....	70
qos priority .....	70
Per-port priority trust mode commands .....	70
display qos trust interface .....	70
qos trust .....	71
<b>Traffic policing, GTS and line rate commands .....</b>	<b>73</b>
Traffic policing commands .....	73
display qos car interface .....	73
display qos carl .....	74
qos car (interface view, port group view) .....	75
qos carl .....	76
GTS commands .....	78
display qos gts interface .....	78
qos gts .....	79
Line rate commands .....	80
display qos lr interface .....	80
qos lr .....	81
<b>Congestion management commands .....</b>	<b>83</b>
FIFO queuing commands .....	83
qos fifo queue-length .....	83
PQ commands .....	83
display qos pq interface .....	83
display qos pql .....	85
qos pq .....	85
qos pql default-queue .....	86
qos pql inbound-interface .....	87
qos pql protocol .....	88
qos pql queue .....	89
CQ commands .....	90
display qos cq interface .....	90
display qos cql .....	91
qos cq .....	92
qos cql default-queue .....	93
qos cql inbound-interface .....	93
qos cql protocol .....	94
qos cql queue .....	95
qos cql queue serving .....	96
WFQ commands .....	97
display qos wfq interface .....	97
qos wfq .....	98
CBQ commands .....	99
display qos cbq interface .....	99
qos max-bandwidth .....	100
qos reserved-bandwidth .....	101
queue af .....	102
queue ef .....	103
queue wfq .....	104
queue-length .....	104
wred .....	105
wred dscp .....	106
wred ip-precedence .....	107
wred weighting-constant .....	108
RTP queuing commands .....	109
display qos rtpq interface .....	109
qos rtpq .....	110
QoS token commands .....	111
qos qmtoken .....	111
Packet information pre-extraction commands .....	111

qos pre-classify .....	111
Local fragment pre-drop commands .....	112
qos fragment pre-drop .....	112
<b>Congestion avoidance commands .....</b>	<b>113</b>
WRED commands .....	113
display qos wred interface .....	113
qos wred enable .....	114
qos wred dscp .....	115
qos wred ip-precedence .....	115
qos wred weighting-constant .....	116
WRED table commands .....	117
display qos wred table .....	117
qos wred table .....	118
queue .....	119
qos wred apply .....	120
<b>DAR commands .....</b>	<b>122</b>
dar enable .....	122
dar max-session-count .....	122
dar p2p signature-file .....	123
dar protocol .....	123
dar protocol-group .....	126
dar protocol-rename .....	126
dar protocol-statistic .....	127
display dar information .....	128
display dar protocol .....	128
display dar protocol-rename .....	131
display dar protocol-statistic .....	132
if-match protocol .....	134
if-match protocol http .....	134
if-match protocol rtp .....	135
protocol .....	136
reset dar protocol-statistic .....	137
reset dar session .....	137
<b>FR QoS configuration commands .....</b>	<b>139</b>
apply policy outbound .....	139
cbs .....	139
cir .....	140
cir allow .....	141
congestion-threshold .....	142
cq .....	143
display fr class-map .....	143
display fr fragment-info .....	145
display fr switch-table .....	146
display qos policy interface .....	147
display qos pvc-pq interface .....	149
ebs .....	150
fifo queue-length .....	151
fr class .....	152
fr congestion-threshold .....	152
fr de del .....	153
fr del inbound-interface .....	154
fr del protocol .....	155
fr pvc-pq .....	156
fr traffic-policing .....	157
fr traffic-shaping .....	157
fragment .....	158
fr-class .....	158
pq .....	159
pvc-pq .....	160



rtpq .....	161
traffic-shaping adaptation .....	161
wfq .....	162
<b>MPLS QoS commands .....</b>	<b>164</b>
if-match mpls-exp .....	164
qos cql protocol mpls exp .....	164
qos pql protocol mpls exp .....	165
remark mpls-exp .....	165
<b>Index .....</b>	<b>167</b>

# ACL configuration commands

## acl

Use **acl** to create a WLAN, IPv4 basic, IPv4 advanced, Ethernet frame header, or user-defined ACL, and enter its view. If the ACL has been created, you directly enter its view.

Use **undo acl** to delete the specified ACLs.

### Syntax

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

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

### Default

No ACL exists.

### Views

System view

### Default command level

2: System level

### Parameters

**number** *acl-number*: Specifies the number of an access control list (ACL):

- 100 to 199 for WLAN ACLs
- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

The following matrix shows the ACL number ranges and hardware compatibility:

Hardware	Number ranges for <i>acl-number</i>
MSR800	All ranges except WLAN ACLs.
MSR 900	All ranges.
MSR900-E	All ranges except WLAN ACLs.
MSR 930	All ranges except WLAN ACLs.
MSR 20-1X	All ranges.
MSR 20	All ranges.
MSR 30	All ranges.
MSR 50	All ranges except that MPU-G2 does not support WLAN ACLs.
MSR 2600	All ranges.
MSR3600-51F	All ranges.

**name** *acl-name*: Assigns a name to the ACL for easy identification. The *acl-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**. The **name** option is not available for WLAN ACLs.

**match-order:** Sets the order in which ACL rules are compared against packets:

- **auto**—Compares ACL rules in depth-first order. The depth-first order differs with ACL categories. For more information, see *ACL and QoS Configuration Guide*.
- **config**—Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has higher priority. If no match order is specified, the config order applies by default.

The **match-order** keyword is not available for user-defined or WLAN ACLs. They always use the config order.

**all:** Deletes all WLAN, IPv4 basic, IPv4 advanced, Ethernet frame header, or user-defined ACLs.

## Usage guidelines

You can assign a name to an ACL only when you create it. After an ACL is created with a name, you cannot rename it or remove its name.

You can change match order only for ACLs that do not contain any rules.

To display any ACLs you have created, use the **display acl** command.

## Examples

# Create IPv4 basic ACL 2000, and enter its view.

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

# Create IPv4 basic ACL 2001 with the name **flow**, and enter its view.

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

## acl copy

Use **acl copy** to create a WLAN, IPv4 basic, IPv4 advanced, Ethernet frame header, or user-defined ACL by copying an ACL that already exists. The new ACL has the same properties and content as the source ACL, but not the same ACL number and name.

## Syntax

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

## Views

System view

## Default command level

2: System level

## Parameters

*source-acl-number*: Specifies an existing source ACL by its number:

- 100 to 199 for WLAN ACLs
- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

**name** *source-acl-name*: Specifies an existing source ACL by its name. The *source-acl-name* argument takes a case-insensitive string of 1 to 63 characters. The **name** option is not available for WLAN ACLs.

*dest-acl-number*: Assigns a unique number to the ACL you are creating. This number must be from the same ACL category as the source ACL. Available value ranges include:

- 100 to 199 for WLAN ACLs
- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

The following matrix shows the ACL number ranges and hardware compatibility:

Hardware	Number ranges for <i>acl-number</i>
MSR800	All ranges except WLAN ACLs.
MSR 900	All ranges.
MSR900-E	All ranges except WLAN ACLs.
MSR 930	All ranges except WLAN ACLs.
MSR 20-1X	All ranges.
MSR 20	All ranges.
MSR 30	All ranges.
MSR 50	All ranges except that MPU-G2 does not support WLAN ACLs.
MSR 2600	All ranges.
MSR3600-51F	All ranges.

**name** *dest-acl-name*: Assigns a unique name to the ACL you are creating. The *dest-acl-name* takes a case-insensitive string of 1 to 63 characters. It must start with an English letter, and to avoid confusion, it cannot be **all**. For this ACL, the system automatically picks the smallest number from all available numbers in the same ACL category as the source ACL. The **name** option is not available for WLAN ACLs.

## Usage guidelines

You can assign a name to an ACL only when you create it. After an ACL is created with a name, you cannot rename it or remove its name.

## Examples

# Create IPv4 basic ACL 2002 by copying IPv4 basic ACL 2001.

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

```
[Sysname] acl copy 2001 to 2002
```

## acl ipv6

Use **acl ipv6** to create an IPv6 basic, IPv6 advanced, or simple ACL, and enter its ACL view. If the ACL has been created, you directly enter its view.

Use **undo acl ipv6** to delete the specified ACLs.

## Syntax

**acl ipv6 number** *acl6-number* [ **name** *acl6-name* ] [ **match-order** { **auto** | **config** } ]

**undo acl ipv6** { **all** | **name** *acl6-name* | **number** *acl6-number* }

## Default

No ACL exists.

## Views

System view

## Default command level

2: System level

## Parameters

**number** *acl6-number*: Specifies the number of an ACL:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs
- 10000 to 42767 for simple ACLs

**name** *acl6-name*: Assigns a name to the ACL for easy identification. The *acl6-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**. The **name** option is not available for simple ACLs.

**match-order**: Sets the order in which ACL rules are compared against packets:

- **auto**—Compares ACL rules in depth-first order. The depth-first order differs with ACL categories. For more information, see *ACL and QoS Configuration Guide*.
- **config**—Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has higher priority. If no match order is specified, the config order applies by default.

The **match-order** keyword is not available for simple ACLs because a simple ACL contains only one rule.

**all**: Delete all IPv6 basic, IPv6 advanced, and simple ACLs.

## Usage guidelines

You can assign a name to an ACL only when you create it. After an ACL is created, you cannot rename it or remove its name.

You can change match order only for ACLs that do not contain any rules.

To display any ACLs you have created, use the **display acl ipv6** command.

## Examples

# Create IPv6 basic ACL 2000 and enter its view.

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

```
[Sysname] acl ipv6 number 2000
```

```
[Sysname-acl6-basic-2000]
```

# Create IPv6 basic ACL 2001 with the name **flow**, and enter its view.

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

```
[Sysname] acl ipv6 number 2001 name flow
```

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

## acl ipv6 copy

Use **acl ipv6 copy** to create an IPv6 basic or IPv6 advanced ACL by copying an ACL that already exists. The new ACL has the same properties and content as the source ACL, but not the same ACL number and name.

## Syntax

```
acl ipv6 copy { source-acl6-number | name source-acl6-name } to { dest-acl6-number | name dest-acl6-name }
```

## Views

System view

## Default command level

2: System level

## Parameters

*source-acl6-number*: Specifies an existing source ACL by its number:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

**name** *source-acl6-name*: Specifies an existing source ACL by its name. The *source-acl6-name* argument takes a case-insensitive string of 1 to 63 characters.

*dest-acl6-number*: Assigns a unique number to the ACL you are creating. This number must be from the same ACL category as the source ACL. Available value ranges include:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

**name** *dest-acl6-name*: Assigns a unique name to the ACL you are creating. The *dest-acl6-name* takes a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**. For this ACL, the system automatically picks the smallest number from all available numbers in the same ACL category as the source ACL.

## Usage guidelines

You can assign a name to an ACL only when you create it. After an ACL is created with a name, you cannot rename it or remove its name.

## Examples

```
# Create IPv6 basic ACL 2002 by copying IPv6 basic ACL 2001.
```

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

```
[Sysname] acl ipv6 copy 2001 to 2002
```

# acl ipv6 name

Use **acl ipv6 name** to enter the view of an IPv6 basic or IPv6 advanced ACL that has a name.

## Syntax

```
acl ipv6 name acl6-name
```

## Views

System view

## Default command level

2: System level

## Parameters

*acl6-name*: Specifies an IPv6 basic or IPv6 advanced ACL name, a case-insensitive string of 1 to 63 characters. It must start with an English letter. The ACL must already exist.

## Examples

```
# Enter the view of IPv6 basic ACL flow.
```

```
<Sysname> system-view
[Sysname] acl ipv6 name flow
[Sysname-acl6-basic-2001-flow]
```

## Related commands

**acl ipv6**

## acl name

Use **acl name** to enter the view of an IPv4 basic, IPv4 advanced, Ethernet frame header, or user-defined ACL that has a name.

## Syntax

**acl name** *acl-name*

## Views

System view

## Default command level

2: System level

## Parameters

*acl-name*: Specifies an IPv4 basic, IPv4 advanced, Ethernet frame header, or user-defined ACL name, a case-insensitive string of 1 to 63 characters. It must start with an English letter. The ACL must already exist.

## Examples

# Enter the view of IPv4 basic ACL **flow**.

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

## Related commands

**acl**

## description

Use **description** to configure a description for an ACL.

Use **undo description** to remove the ACL description.

## Syntax

**description** *text*

**undo description**

## Default

An ACL has no ACL description.

## Views

WLAN ACL view, IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, simple ACL view, Ethernet frame header ACL view, user-defined ACL view

## Default command level

2: System level

## Parameters

*text*: ACL description, a case-sensitive string of 1 to 127 characters.

## Usage guidelines

The MPU-G2 of an MSR 50 router and the MSR800, MSR900-E, and MSR 930 routers do not support WLAN ACL view.

## Examples

# Configure a description for IPv4 basic ACL 2000.

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

```
[Sysname] acl number 2000
```

```
[Sysname-acl-basic-2000] description This is an IPv4 basic ACL.
```

# Configure a description for IPv6 basic ACL 2000.

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

```
[Sysname] acl ipv6 number 2000
```

```
[Sysname-acl6-basic-2000] description This is an IPv6 basic ACL.
```

## Related commands

- **display acl**
- **display acl ipv6**

# display acl

Use **display acl** to display configuration and match statistics for WLAN, IPv4 basic, IPv4 advanced, Ethernet frame header, and user-defined ACLs.

## Syntax

```
display acl { acl-number | all | name acl-name } [ | { begin | exclude | include } regular-expression ]
```

## Views

Any view

## Default command level

1: Monitor level

## Parameters

*acl-number*: Specifies an ACL by its number:

- 100 to 199 for WLAN ACLs
- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

The following matrix shows the ACL number ranges and hardware compatibility:

Hardware	Number ranges for <i>acl-number</i>
MSR800	All ranges except WLAN ACLs.
MSR 900	All ranges.
MSR900-E	All ranges except WLAN ACLs.
MSR 930	All ranges except WLAN ACLs.



Hardware	Number ranges for <i>acl-number</i>
MSR 20-1X	All ranges.
MSR 20	All ranges.
MSR 30	All ranges.
MSR 50	All ranges except that MPU-G2 does not support WLAN ACLs.
MSR 2600	All ranges.
MSR3600-51F	All ranges.

**all:** Displays information for all WLAN, IPv4 basic, IPv4 advanced, Ethernet frame header, and user-defined ACLs.

**name *acl-name*:** Specifies an ACL by its name. The *acl-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter.

**|:** Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin:** Displays the first line that matches the specified regular expression and all lines that follow.

**exclude:** Displays all lines that do not match the specified regular expression.

**include:** Displays all lines that match the specified regular expression.

*regular-expression:* Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

This command displays ACL rules in config or depth-first order, whichever is configured.

## Examples

# Display configuration and match statistics for all WLAN, IPv4 basic, IPv4 advanced, Ethernet frame header, and user-defined ACLs.

```
<Sysname> display acl all
Basic ACL 2000, named flow, 3 rules,
This is an IPv4 basic ACL.
Statistics is enabled
ACL's step is 5
rule 0 permit
rule 5 permit source 1.1.1.1 0 (2 times matched)
rule 10 permit vpn-instance mk

Basic ACL 2001, named -none-, 3 rules, match-order is auto,
ACL's step is 5
rule 10 permit vpn-instance rd
rule 10 comment This rule is used in VPN rd.
rule 5 permit source 2.2.2.2 0
rule 0 permit
```

**Table 1 Command output**

Field	Description
Basic ACL 2000	Category and number of the ACL. The following field information is about IPv4 basic ACL 2000.
named flow	The name of the ACL is flow. "-none-" means the ACL is not named.

Field	Description
	This field is not present for a WLAN ACL.
3 rules	The ACL contains three rules.
match-order is auto	The match order for the ACL is auto, which sorts ACL rules in depth-first order. This field is not present when the match order is config.
This is an IPv4 basic ACL.	Description of the ACL.
ACL's step is 5	The rule numbering step is 5.
rule 0 permit	Content of rule 0.
2 times matched	There have been two matches for the rule. The statistic counts only ACL matches performed in software. .This field is not displayed when no packets have matched the rule.
Uncompleted	Applying the rule to hardware failed because no sufficient resources were available or the hardware does not support the rule. This event might occur when you modify a rule in an ACL that has been applied.
rule 10 comment This rule is used in VPN rd.	Comment about ACL rule 10.

## display acl ipv6

Use **display acl ipv6** to display configuration and match statistics for IPv6 basic, IPv6 advanced, and simple ACLs.

### Syntax

```
display acl ipv6 { acl6-number | all | name acl6-name } [ | { begin | exclude | include } regular-expression ]
```

### Views

Any view

### Default command level

1: Monitor level

### Parameters

*acl6-number*: Specifies an ACL by its number:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs
- 10000 to 42767 for simple ACLs

**all**: Displays information for all IPv6 basic and IPv6 advanced ACLs.

**name** *acl6-name*: Specifies an ACL by its name. The *acl6-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter.

**|**: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

This command displays ACL rules in config or depth-first order, whichever is configured.

## Examples

# Display configuration and match statistics for all IPv6 basic, IPv6 advanced, and simple ACLs.

```
<Sysname> display acl ipv6 all
Basic IPv6 ACL 2000, named flow, 3 rules,
This is an IPv6 basic ACL.
Statistics is enabled
ACL's step is 5
rule 0 permit
rule 5 permit source 1::/64 (2 times matched)
rule 10 permit vpn-instance mk

Basic IPv6 ACL 2001, named -none-, 3 rules, match-order is auto,
ACL's step is 5
rule 10 permit vpn-instance mk
rule 10 comment This rule is used in VPN rd
rule 5 permit source 1::/64
rule 0 permit
```

**Table 2 Command output**

Field	Description
Basic IPv6 ACL 2000	Category and number of the ACL. The following field information is about this IPv6 basic ACL 2000.
named flow	The name of the ACL is flow. "-none-" means the ACL is not named. This field is not available for a simple ACL.
3 rules	The ACL contains three rules.
match-order is auto	The match order for the ACL is auto, which sorts ACL rules in depth-first order. This field is not present when the match order is config.
This is an IPv6 basic ACL.	Description of the ACL.
ACL's step is 5	The rule numbering step is 5.
rule 0 permit	Content of rule 0.
2 times matched	There have been two matches for the rule. The statistic counts only ACL matches performed by software. This field is not displayed when no packets have matched the rule.
Uncompleted	Applying the rule to hardware failed because no sufficient resources were available or the hardware does not support the rule. This event might occur when you modify a rule in an ACL that has been applied.
rule 10 comment This rule is used in VPN rd	Comment about ACL rule 10.

## display time-range

Use **display time-range** to display the configuration and status of the specified time range or all time ranges.

## Syntax

**display time-range** { *time-range-name* | **all** } [ | { **begin** | **exclude** | **include** } *regular-expression* ]

## Views

Any view

## Default command level

1: Monitor level

## Parameters

**time-range-name**: Specifies a time range name, a case-insensitive string of 1 to 32 characters. It must start with an English letter.

**all**: Displays the configuration and status of all existing time ranges.

**|**: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

**regular-expression**: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Examples

# Display the configuration and status of time range **t4**.

```
<Sysname> display time-range t4
```

```
Current time is 17:12:34 4/13/2010 Tuesday
```

```
Time-range : t4 ( Inactive )
```

```
10:00 to 12:00 Mon
```

```
14:00 to 16:00 Wed
```

```
from 00:00 1/1/2010 to 00:00 2/1/2010
```

```
from 00:00 6/1/2010 to 00:00 7/1/2010
```

**Table 3 Command output**

Field	Description
Current time	Current system time.
Time-range	Configuration and status of the time range, including its name, status (active or inactive), and start time and end time.

## reset acl counter

Use **reset acl counter** to clear statistics for one or all WLAN, IPv4 basic, IPv4 advanced, Ethernet frame header, and user-defined ACLs.

## Syntax

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

## Views

User view

## Default command level

2: System level

## Parameters

*acl-number*: Specifies an ACL by its number:

- 100 to 199 for WLAN ACLs
- 2000 to 2999 for IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

The following matrix shows the ACL number ranges and hardware compatibility:

Hardware	Number ranges for <i>acl-number</i>
MSR800	All ranges except WLAN ACLs.
MSR 900	All ranges.
MSR900-E	All ranges except WLAN ACLs.
MSR 930	All ranges except WLAN ACLs.
MSR 20-1X	All ranges.
MSR 20	All ranges.
MSR 30	All ranges.
MSR 50	All ranges except that MPU-G2 does not support WLAN ACLs.
MSR 2600	All ranges.
MSR3600-51F	All ranges.

**all**: Clears statistics for all WLAN, IPv4 basic, IPv4 advanced, Ethernet frame header, and user-defined ACLs.

**name** *acl-name*: Specifies an ACL by its name. The *acl-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter.

## Examples

# Clear statistics for IPv4 basic ACL 2001.

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

## Related commands

**display acl**

# reset acl ipv6 counter

Use **reset acl ipv6 counter** to clear statistics for one or all IPv6 basic and IPv6 advanced ACLs.

## Syntax

```
reset acl ipv6 counter { acl6-number | all | name acl6-name }
```

## Views

User view

## Default command level

2: System level

## Parameters

*acl6-number*: Specifies an ACL by its number:

- 2000 to 2999 for IPv6 basic ACLs
- 3000 to 3999 for IPv6 advanced ACLs

**all**: Clears statistics for all IPv6 basic and advanced ACLs.

**name** *acl6-name*: Specifies an ACL by its name. The *acl6-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter.

## Examples

```
# Clear statistics for IPv6 basic ACL 2001.  
<Sysname> reset acl ipv6 counter 2001
```

## Related commands

**display acl ipv6**

# rule (Ethernet frame header ACL view)

Use **rule** to create or edit an Ethernet frame header ACL rule. You can edit ACL rules only when the match order is config.

Use **undo rule** to delete an Ethernet frame header ACL rule or some attributes in the rule. If no optional keywords are provided, this command deletes the entire rule. If optional keywords or arguments are provided, this command deletes the specified attributes.

## Syntax

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

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

## Default

An Ethernet frame header ACL does not contain any rule.

## Views

Ethernet frame header ACL view

## Default command level

2: System level

## Parameters

*rule-id*: Specifies a rule ID, which ranges from 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

**deny**: Denies matching packets.

**permit**: Allows matching packets to pass.

**cos** *vlan-pri*: Matches an 802.1p priority. The *vlan-pri* argument can be a number in the range 0 to 7, or in words, **best-effort** (0), **background** (1), **spare** (2), **excellent-effort** (3), **controlled-load** (4), **video** (5), **voice** (6), or **network-management** (7).

**counting**: Counts the number of times the ACL rule has been matched.

**dest-mac** *dest-address dest-mask*: Matches a destination MAC address range. The *dest-address* and *dest-mask* arguments represent a destination MAC address and mask in H-H-H format.

**logging:** Logs matching packets. This function is available only when the application module (such as the firewall) that uses the ACL supports the logging function.

**Isap** *Isap-type Isap-type-mask:* Matches the DSAP and SSAP fields in LLC encapsulation. The *Isap-type* argument is a 16-bit hexadecimal number that represents the encapsulation format. The *Isap-type-mask* argument is a 16-bit hexadecimal number that represents the LSAP mask.

**type** *protocol-type protocol-type-mask:* Matches one or more protocols in the Ethernet frame header. The *protocol-type* argument is a 16-bit hexadecimal number that represents a protocol type in Ethernet\_II and Ethernet\_SNAP frames. The *protocol-type-mask* argument is a 16-bit hexadecimal number that represents a protocol type mask.

**source-mac** *sour-address source-mask:* Matches a source MAC address range. The *sour-address* argument represents a source MAC address, and the *sour-mask* argument represents a mask in H-H-H format.

**time-range** *time-range-name:* Specifies a time range for the rule. The *time-range-name* argument is a case insensitive string of 1 to 32 characters. It must start with an English letter.

## Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt fails.

To view rules in an ACL and their rule IDs, use the **display acl all** command.

## Examples

# Create a rule in ACL 4000 to permit ARP packets and deny RARP packets.

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

## Related commands

- **acl**
- **display acl**
- **step**
- **time-range**

## rule (IPv4 advanced ACL view)

Use **rule** to create or edit an IPv4 advanced ACL rule. You can edit ACL rules only when the match order is config.

Use **undo rule** to delete an entire IPv4 advanced ACL rule or some attributes in the rule. If no optional keywords are provided, this command deletes the entire rule. If optional keywords or arguments are provided, this command deletes the specified attributes.

## Syntax

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

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

## Default

An IPv4 advanced ACL does not contain any rule.

## Views

IPv4 advanced ACL view

## Default command level

2: System level

## Parameters

**rule-id**: Specifies a rule ID in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

**deny**: Denies matching packets.

**permit**: Allows matching packets to pass.

**protocol**: Protocol carried by IPv4. It can be a number in the range of 0 to 255, or in words, **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), or **udp** (17). [Table 4](#) describes the parameters that you can specify regardless of the value that the *protocol* argument takes.

**Table 4 Match criteria and other rule information for IPv4 advanced ACL rules**

Parameters	Function	Description
<b>source</b> { <i>source-address</i> <i>source-wildcard</i>   <b>any</b> }	Specifies a source address	The <i>source-address source-wildcard</i> arguments represent a source IP address and wildcard mask in dotted decimal notation. An all-zero wildcard specifies a host address.  The <b>any</b> keyword specifies any source IP address.
<b>destination</b> { <i>dest-address</i> <i>dest-wildcard</i>   <b>any</b> }	Specifies a destination address	The <i>dest-address dest-wildcard</i> arguments represent a destination IP address and wildcard mask in dotted decimal notation. An all-zero wildcard specifies a host address.  The <b>any</b> keyword represents any destination IP address.
<b>counting</b>	Counts the number of times the ACL rule has been matched. This option is disabled by default.	N/A
<b>precedence</b> <i>precedence</i>	Specifies an IP precedence value	The <i>precedence</i> argument can be a number in the range of 0 to 7, or in words, <b>routine</b> (0), <b>priority</b> (1), <b>immediate</b> (2), <b>flash</b> (3), <b>flash-override</b> (4), <b>critical</b> (5), <b>internet</b> (6), or <b>network</b> (7).
<b>tos</b> <i>tos</i>	Specifies a ToS preference	The <i>tos</i> argument can be a number in the range of 0 to 15, or in words, <b>max-reliability</b> (2), <b>max-throughput</b> (4), <b>min-delay</b> (8), <b>min-monetary-cost</b> (1), or <b>normal</b> (0).
<b>dscp</b> <i>dscp</i>	Specifies a DSCP priority	The <i>dscp</i> argument can be a number in the range of 0 to 63, or in words, <b>af11</b> (10), <b>af12</b> (12), <b>af13</b> (14), <b>af21</b> (18), <b>af22</b> (20), <b>af23</b> (22), <b>af31</b> (26), <b>af32</b> (28), <b>af33</b> (30), <b>af41</b> (34), <b>af42</b> (36), <b>af43</b> (38), <b>cs1</b> (8), <b>cs2</b> (16), <b>cs3</b> (24), <b>cs4</b> (32), <b>cs5</b> (40), <b>cs6</b> (48), <b>cs7</b> (56), <b>default</b> (0), or <b>ef</b> (46).
<b>logging</b>	Logs matching packets	This function requires that the module that uses the ACL supports logging.



Parameters	Function	Description
<b>vpn-instance</b> <i>vpn-instance-name</i>	Applies the rule to packets in a VPN instance	The <i>vpn-instance-name</i> argument takes a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the rule applies only to non-VPN packets.
<b>fragment</b>	Applies the rule to only non-first fragments	Without this keyword, the rule applies to all fragments and non-fragments.
<b>time-range</b> <i>time-range-name</i>	Specifies a time range for the rule	The <i>time-range-name</i> argument takes a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the timer range.

**NOTE:**

If you provide the **precedence** or **tos** keyword in addition to the **dscp** keyword, only the **dscp** keyword takes effect.

If the *protocol* argument takes **tcp** (6) or **udp** (7), set the parameters shown in [Table 5](#).

**Table 5 TCP/UDP-specific parameters for IPv4 advanced ACL rules**

Parameters	Function	Description
<b>source-port</b> <i>operator port1</i> [ <i>port2</i> ]	Specifies one or more UDP or TCP source ports.	The <i>operator</i> argument can be <b>lt</b> (lower than), <b>gt</b> (greater than), <b>eq</b> (equal to), <b>neq</b> (not equal to), or <b>range</b> (inclusive range). The <i>port1</i> and <i>port2</i> arguments are TCP or UDP port numbers in the range of 0 to 65535. <i>port2</i> is needed only when the <i>operator</i> argument is <b>range</b> .
<b>destination-port</b> <i>operator port1</i> [ <i>port2</i> ]	Specifies one or more UDP or TCP destination ports.	TCP port numbers can be represented as: <b>chargen</b> (19), <b>bgp</b> (179), <b>cmd</b> (514), <b>daytime</b> (13), <b>discard</b> (9), <b>domain</b> (53), <b>echo</b> (7), <b>exec</b> (512), <b>finger</b> (79), <b>ftp</b> (21), <b>ftp-data</b> (20), <b>gopher</b> (70), <b>hostname</b> (101), <b>irc</b> (194), <b>klogin</b> (543), <b>kshell</b> (544), <b>login</b> (513), <b>lpd</b> (515), <b>nnntp</b> (119), <b>pop2</b> (109), <b>pop3</b> (110), <b>smtp</b> (25), <b>sunrpc</b> (111), <b>tacacs</b> (49), <b>talk</b> (517), <b>telnet</b> (23), <b>time</b> (37), <b>uucp</b> (540), <b>whois</b> (43), and <b>www</b> (80). UDP port numbers can be represented as: <b>biff</b> (512), <b>bootpc</b> (68), <b>bootps</b> (67), <b>discard</b> (9), <b>dns</b> (53), <b>dnsix</b> (90), <b>echo</b> (7), <b>mobilitp-ag</b> (434), <b>mobilitp-mn</b> (435), <b>nameserver</b> (42), <b>netbios-dgm</b> (138), <b>netbios-ns</b> (137), <b>netbios-ssn</b> (139), <b>ntp</b> (123), <b>rip</b> (520), <b>snmp</b> (161), <b>snmptrap</b> (162), <b>sunrpc</b> (111), <b>syslog</b> (514), <b>tacacs-ds</b> (65), <b>talk</b> (517), <b>tftp</b> (69), <b>time</b> (37), <b>who</b> (513), and <b>xdmcp</b> (177).
{ <b>ack</b> <i>ack-value</i>   <b>fin</b> <i>fin-value</i>   <b>psb</b> <i>psb-value</i>   <b>rst</b> <i>rst-value</i>   <b>syn</b> <i>syn-value</i>   <b>urg</b> <i>urg-value</i> } *	Specifies one or more TCP flags including ACK, FIN, PSB, RST, SYN, and URG.	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in a rule are ORed. For example, a rule configured with <b>ack 0 psb 1</b> matches packets with the ACK flag not bit set or packets with the PSB flag bit set.
<b>established</b>	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument takes **icmp** (1), set the parameters shown in [Table 6](#).

**Table 6 ICMP-specific parameters for IPv4 advanced ACL rules**

Parameters	Function	Description
<b>icmp-type</b> { <i>icmp-type</i> [ <i>icmp-code</i> ]   <i>icmp-message</i> }	Specifies the ICMP message type and code.	The <i>icmp-type</i> argument is in the range of 0 to 255. The <i>icmp-code</i> argument is in the range of 0 to 255. The <i>icmp-message</i> argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in <a href="#">Table 7</a> .

**Table 7 ICMP message names supported in IPv4 advanced ACL rules**

ICMP message name	ICMP message type	ICMP message code
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

## Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt fails.

To view rules in an ACL and their rule IDs, use the **display acl all** command.

## Examples

# Create an IPv4 advanced ACL rule to permit TCP packets with the destination port 80 from 129.9.0.0/16 to 202.38.160.0/24, and enable logging matching packets.

```
<Sysname> system-view
[Sysname] acl number 3000
```

```
[Sysname-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination
202.38.160.0 0.0.0.255 destination-port eq 80 logging
```

# Create IPv4 advanced ACL rules to permit all IP packets but the ICMP packets destined for 192.168.1.0/24.

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

# Create IPv4 advanced ACL rules to permit inbound and outbound FTP packets.

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

# Create IPv4 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

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

## Related commands

- **acl**
- **display acl**
- **step**
- **time-range**

## rule (IPv4 basic ACL view)

Use **rule** to create or edit an IPv4 basic ACL rule. You can edit ACL rules only when the match order is config.

Use **undo rule** to delete an entire IPv4 basic ACL rule or some attributes in the rule. If no optional keywords are provided, this command deletes the entire rule. If optional keywords or arguments are provided, this command deletes the specified attributes.

## Syntax

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

## Default

An IPv4 basic ACL does not contain any rule.

## Views

IPv4 basic ACL view

## Default command level

2: System level

## Parameters

**rule-id:** Specifies a rule ID in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

**deny:** Denies matching packets.

**permit:** Allows matching packets to pass.

**counting:** Counts the number of times the ACL rule has been matched. This option is disabled by default.

**fragment:** Applies the rule only to non-first fragments. A rule without this keyword applies to both fragments and non-fragments.

**logging:** Logs matching packets. This function is available only when the application module that uses the ACL supports the logging function.

**source { source-address source-wildcard | any }:** Matches a source address. The *source-address* *source-wildcard* arguments represent a source IP address and wildcard mask in dotted decimal notation. A wildcard mask of zeros specifies a host address. The **any** keyword represents any source IP address.

**time-range time-range-name:** Specifies a time range for the rule. The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the timer range.

**vpn-instance vpn-instance-name:** Applies the rule to packets in a VPN instance. The *vpn-instance-name* argument takes a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the rule applies only to non-VPN packets.

## Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt fails.

To view rules in an ACL and their rule IDs, use the **display acl all** command.

## Examples

# Create a rule in IPv4 basic ACL 2000 to deny the packets from any source IP segment but 10.0.0.0/8, 172.17.0.0/16, or 192.168.1.0/24.

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

## Related commands

- **acl**
- **display acl**
- **step**
- **time-range**

## rule (IPv6 advanced ACL view)

Use **rule** to create or edit an IPv6 advanced ACL rule. You can edit ACL rules only when the match order is config.

Use **undo rule** to delete an entire IPv6 advanced ACL rule or some attributes in the rule. If no optional keywords are provided, this command deletes the entire rule. If optional keywords or arguments are provided, this command deletes the specified attributes.

### Syntax

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

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

### Default

An IPv6 advanced ACL does not contain any rule.

### Views

IPv6 advanced ACL view

### Default command level

2: System level

### Parameters

**rule-id**: Specifies a rule ID in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

**deny**: Denies matching packets.

**permit**: Allows matching packets to pass.

**protocol**: Matches protocol carried over IPv6. It can be a number in the range of 0 to 255, or in words, **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), or **udp** (17). [Table 8](#) describes the parameters that you can specify regardless of the value that the *protocol* argument takes.

**Table 8 Match criteria and other rule information for IPv6 advanced ACL rules**

Parameters	Function	Description
<b>source</b> { <i>source-address</i> <i>source-prefix</i>   <i>source-address/s</i> <i>ource-prefix</i>   <b>any</b> }	Specifies a source IPv6 address.	The <i>source-address</i> and <i>source-prefix</i> arguments represent an IP source address, and prefix length in the range of 1 to 128. The <b>any</b> keyword represents any IPv6 source address.
<b>destination</b> { <i>dest-address</i> <i>dest-prefix</i>   <i>dest-address/dest</i> <i>-prefix</i>   <b>any</b> }	Specifies a destination IPv6 address.	The <i>dest-address</i> and <i>dest-prefix</i> arguments represent a destination IP address, and prefix length in the range of 1 to 128. The <b>any</b> keyword specifies any IPv6 destination address.

Parameters	Function	Description
<b>counting</b>	Counts the number of times the ACL rule has been matched. This option is disabled by default.	N/A
<b>dscp</b> <i>dscp</i>	Specifies a DSCP preference.	The <i>dscp</i> argument can be a number in the range of 0 to 63, or in words, <b>af11</b> (10), <b>af12</b> (12), <b>af13</b> (14), <b>af21</b> (18), <b>af22</b> (20), <b>af23</b> (22), <b>af31</b> (26), <b>af32</b> (28), <b>af33</b> (30), <b>af41</b> (34), <b>af42</b> (36), <b>af43</b> (38), <b>cs1</b> (8), <b>cs2</b> (16), <b>cs3</b> (24), <b>cs4</b> (32), <b>cs5</b> (40), <b>cs6</b> (48), <b>cs7</b> (56), <b>default</b> (0), or <b>ef</b> (46).
<b>flow-label</b> <i>flow-label-value</i>	Specifies a flow label value in an IPv6 packet header.	The <i>flow-label-value</i> argument is in the range of 0 to 1048575.
<b>logging</b>	Logs matching packets.	This function requires that the module that uses the ACL supports logging.
<b>routing</b> [ <b>type</b> <i>routing-type</i> ]	Specifies the type of routing header.	The <i>routing-type</i> argument takes a value in the range of 0 to 255. If no routing type header is specified, the rule applies to the IPv6 packets with any type of routing header.
<b>fragment</b>	Applies the rule to only non-first fragments.	Without this keyword, the rule applies to all fragments and non-fragments.
<b>time-range</b> <i>time-range-name</i>	Specifies a time range for the rule.	The <i>time-range-name</i> argument takes a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the timer range.
<b>vpn-instance</b> <i>vpn-instance-name</i>	Applies the rule to packets in a VPN instance.	The <i>vpn-instance-name</i> argument takes a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the rule applies to non-VPN packets.

If the *protocol* argument takes **tcp** (6) or **udp** (17), set the parameters shown in [Table 9](#).

**Table 9 TCP/UDP-specific parameters for IPv6 advanced ACL rules**

Parameters	Function	Description
<b>source-port</b> <i>operator port1</i> [ <i>port2</i> ]	Specifies one or more UDP or TCP source ports.	The <i>operator</i> argument can be <b>lt</b> (lower than), <b>gt</b> (greater than), <b>eq</b> (equal to), <b>neq</b> (not equal to), or <b>range</b> (inclusive range). The <i>port1</i> and <i>port2</i> arguments are TCP or UDP port numbers in the range of 0 to 65535. <i>port2</i> is needed only when the <i>operator</i> argument is <b>range</b> .
<b>destination-port</b> <i>operator port1</i> [ <i>port2</i> ]	Specifies one or more UDP or TCP destination ports.	TCP port numbers can be represented as: <b>chargen</b> (19), <b>bgp</b> (179), <b>cmd</b> (514), <b>daytime</b> (13), <b>discard</b> (9), <b>domain</b> (53), <b>echo</b> (7), <b>exec</b> (512), <b>finger</b> (79), <b>ftp</b> (21), <b>ftp-data</b> (20), <b>gopher</b> (70), <b>hostname</b> (101), <b>irc</b> (194), <b>klogin</b> (543), <b>kshell</b> (544), <b>login</b> (513), <b>lpd</b> (515), <b>nntp</b> (119), <b>pop2</b> (109), <b>pop3</b> (110), <b>smtp</b> (25), <b>sunrpc</b> (111), <b>tacacs</b> (49), <b>talk</b> (517), <b>telnet</b> (23), <b>time</b> (37), <b>uucp</b> (540), <b>whois</b> (43), and <b>www</b> (80). UDP port numbers can be represented as: <b>biff</b> (512), <b>bootpc</b> (68), <b>bootps</b> (67), <b>discard</b> (9), <b>dns</b> (53), <b>dnsix</b> (90), <b>echo</b> (7), <b>mobility-ag</b> (434), <b>mobility-mn</b> (435), <b>nameserver</b> (42), <b>netbios-dgm</b> (138), <b>netbios-ns</b> (137), <b>netbios-ssn</b> (139), <b>nntp</b> (119), <b>rip</b> (520), <b>snmp</b> (161), <b>snmptrap</b> (162), <b>sunrpc</b> (111), <b>syslog</b> (514), <b>tacacs-ds</b> (65), <b>talk</b> (517), <b>tftp</b> (69), <b>time</b> (37), <b>who</b> (513), and <b>xdmcp</b> (177).
{ <b>ack</b> <i>ack-value</i>	Specifies one or	Parameters specific to TCP.

Parameters	Function	Description
<b>fin</b> <i>fin-value</i>   <b>psh</b> <i>psh-value</i>   <b>rst</b> <i>rst-value</i>   <b>syn</b> <i>syn-value</i>   <b>urg</b> <i>urg-value</i> }	more TCP flags, including ACK, FIN, PSH, RST, SYN, and URG.	The value for each argument can be 0 (flag bit not set) or 1 (flag bit set).  The TCP flags in a rule are ORed. For example, a rule configured with <b>ack 0 psh 1</b> matches packets with the ACK flag bit not set or packets with the PSH flag bit set.
<b>established</b>	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP.  The rule matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument takes **icmpv6** (58), set the parameters shown in [Table 10](#).

**Table 10 ICMPv6-specific parameters for IPv6 advanced ACL rules**

Parameters	Function	Description
<b>icmp6-type</b> { <i>icmp6-type</i> <i>icmp6-code</i>   <i>icmp6-message</i> }	Specifies the ICMPv6 message type and code.	The <i>icmp6-type</i> argument is in the range of 0 to 255. The <i>icmp6-code</i> argument is in the range of 0 to 255. The <i>icmp6-message</i> argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in <a href="#">Table 11</a> .

**Table 11 ICMPv6 message names supported in IPv6 advanced ACL rules**

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

## Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt fails.

To view rules in an ACL and their rule IDs, use the **display acl ipv6 all** command.

## Examples

# Create an IPv6 advanced ACL rule to permit TCP packets with the destination port 80 from 2030:5060::/64 to FE80:5060::/96, and enable logging matching packets.

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

# Create IPv6 advanced ACL rules to permit all IPv6 packets but the ICMPv6 packets destined for FE80:5060:1001::/48.

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

# Create IPv6 advanced ACL rules to permit inbound and outbound FTP packets.

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

# Create IPv6 advanced ACL rules to permit inbound and outbound SNMP and SNMP trap packets.

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

## Related commands

- **acl ipv6**
- **display ipv6 acl**
- **step**
- **time-range**

## rule (IPv6 basic ACL view)

Use **rule** to create or edit an IPv6 basic ACL rule. You can edit ACL rules only when the match order is config.

Use **undo rule** to delete an entire IPv6 basic ACL rule or some attributes in the rule. If no optional keywords are provided, this command deletes the entire rule. If optional keywords or arguments are provided, this command deletes the specified attributes.



## Syntax

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

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

## Default

An IPv6 basic ACL does not contain any rule.

## Views

IPv6 basic ACL view

## Default command level

2: System level

## Parameters

**rule-id**: Specifies a rule ID in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

**deny**: Denies matching packets.

**permit**: Allows matching packets to pass.

**counting**: Counts the number of times the ACL rule has been matched. This option is disabled by default.

**fragment**: Applies the rule only to non-first fragments. A rule without this keyword applies to both fragments and non-fragments.

**logging**: Logs matching packets. This function requires that the module that uses the ACL supports logging.

**routing [ type routing-type ]**: Matches a specific type of routing header or any type of routing header. The *routing-type* argument takes a value in the range of 0 to 255. If no routing header type is specified, the rule matches any type of routing header.

**source { source-address source-prefix | source-address/source-prefix | any }**: Matches a source IP address. The *source-address* and *source-prefix* arguments represent a source IPv6 address and address prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.

**time-range time-range-name**: Specifies a time range for the rule. The *time-range-name* argument takes a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the timer range.

**vpn-instance vpn-instance-name**: Applies the rule to packets in a VPN. The *vpn-instance-name* argument takes a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the rule applies to non-VPN packets.

## Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt fails.

To view rules in an ACL and their rule IDs, use the **display acl ipv6 all** command.

## Examples

```
# Create an IPv6 basic ACL rule to deny the packets from any source IP segment but 1001::/16,  
3124:1123::/32, or FE80:5060:1001::/48.
```

```

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

```

## Related commands

- **acl ipv6**
- **display ipv6 acl**
- **step**
- **time-range**

## rule (simple ACL view)

Use **rule** to create or edit a simple ACL rule.

Use **undo rule** to delete an entire simple ACL rule or some attributes in the rule. If no optional keywords are provided, this command deletes the entire rule. If optional keywords or arguments are provided, this command deletes the specified attributes.

## Syntax

```

rule protocol [ addr-flag addr-flag | destination { dest-address dest-prefix | dest-address/dest-prefix
| any } | destination-port operator port1 [ port2 ] | dscp dscp | frag-type { fragment |
fragment-subseq | non-fragment | non-subseq } | icmp6-type { icmp6-type icmp6-code |
icmp6-message } | source { source-address source-prefix | source-address/source-prefix | any } |
source-port operator port1 [ port2 ] | tcp-type { tcpurg | tcpack | tcppsh | tcprst | tcpsyn | tcpfin } ]
*
```

```

undo rule [ addr-flag | destination | destination-port | dscp | frag-type | icmp6-type | source |
source-port | tcp-type ] *
```

## Default

A simple ACL does not contain any rule.

## Views

Simple ACL view

## Default command level

2: System level

## Parameters

*protocol*: Matches protocol carried over IPv6. It can be a number in the range of 0 to 255, or in words, **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), **udp** (17). If you specify a number, add keyword **protocol** before the number. [Table 12](#) describes the parameters that you can specify regardless of the value that the *protocol* argument takes.

**Table 12 Match criteria and other rule information for simple ACL rules**

Parameters	Function	Description
<b>addr-flag</b> <i>addr-flag</i>	Specifies an IPv6 source-destination address combination mode.	<p>The <i>addr-flag</i> argument is in the range of 1 to 6, where:</p> <ul style="list-style-type: none"> <li>• <b>1</b>—64-bit source address prefix + 64-bit destination address prefix</li> <li>• <b>2</b>—64-bit source address prefix + 64-bit destination address suffix</li> </ul>

Parameters	Function	Description
		<ul style="list-style-type: none"> <li><b>3</b>—64-bit source address suffix + 64-bit destination address prefix</li> <li><b>4</b>—64-bit source address suffix + 64-bit destination address suffix</li> <li><b>5</b>—128-bit source address</li> <li><b>6</b>—128-bit destination address</li> </ul>
<b>source</b> { <i>source-address</i> <i>source-prefix</i>   <i>source-address/source-prefix</i>   <b>any</b> }	Specifies a source IPv6 address.	The <i>source-address</i> and <i>source-prefix</i> arguments specify an IPv6 source address and its prefix length in the range of 1 to 128. The <b>any</b> keyword specifies any IPv6 source address.
<b>destination</b> { <i>dest-address</i> <i>dest-prefix</i>   <i>dest-address/dest-prefix</i>   <b>any</b> }	Specifies a destination IPv6 address.	The <i>dest-address</i> and <i>dest-prefix</i> arguments specify an IPv6 destination address and its prefix length in the range of 1 to 128. The <b>any</b> keyword specifies any IPv6 destination address.
<b>frag-type</b> { <b>fragment</b>   <b>fragment-subseq</b>   <b>non-fragment</b>   <b>non-subseq</b> }	Specifies to which type of packets the rule applies.	The <b>fragment</b> keyword applies the rule to only first fragments. The <b>fragment-subseq</b> keyword applies the rule to only non-first fragments. The <b>non-fragment</b> keyword applies the rule to only non-fragments. The <b>non-subseq</b> keyword applies the rule to only last fragments.
<b>dscp</b> <i>dscp</i>	Specifies the DSCP preference.	The <i>dscp</i> argument is in the range of 0 to 63.

If the *protocol* argument takes **tcp** (6) or **udp** (17), you can set the parameters shown in [Table 13](#).

**Table 13 TCP/UDP-specific parameters for simple ACL rules**

Parameters	Function	Description
<b>source-port</b> <i>operator</i> <i>port1</i> [ <i>port2</i> ]	Specifies one or more UDP or TCP source ports.	The <i>operator</i> argument can be <b>lt</b> (lower than), <b>gt</b> (greater than), <b>eq</b> (equal to), or <b>range</b> (inclusive range). The <i>port1</i> and <i>port2</i> arguments are TCP or UDP port numbers in the range of 0 to 65535. <i>port2</i> is needed only when the <i>operator</i> argument is <b>range</b> .
<b>destination-port</b> <i>operator port1</i> [ <i>port2</i> ]	Specifies one or more UDP or TCP destination ports.	TCP port numbers can be represented as: <b>chargen</b> (19), <b>bgp</b> (179), <b>cmd</b> (514), <b>daytime</b> (13), <b>discard</b> (9), <b>domain</b> (53), <b>echo</b> (7), <b>exec</b> (512), <b>finger</b> (79), <b>ftp</b> (21), <b>ftp-data</b> (20), <b>gopher</b> (70), <b>hostname</b> (101), <b>irc</b> (194), <b>klogin</b> (543), <b>kshell</b> (544), <b>login</b> (513), <b>lpd</b> (515), <b>nntp</b> (119), <b>pop2</b> (109), <b>pop3</b> (110), <b>smtp</b> (25), <b>sunrpc</b> (111), <b>tacacs</b> (49), <b>talk</b> (517), <b>telnet</b> (23), <b>time</b> (37), <b>uucp</b> (540), <b>whois</b> (43), and <b>www</b> (80). UDP port numbers can be represented as: <b>biff</b> (512), <b>bootpc</b> (68), <b>bootps</b> (67), <b>discard</b> (9), <b>dns</b> (53), <b>dnsix</b> (90), <b>echo</b> (7), <b>mobility-ag</b> (434), <b>mobility-mn</b> (435), <b>nameserver</b> (42), <b>netbios-dgm</b> (138), <b>netbios-ns</b> (137), <b>netbios-ssn</b> (139), <b>nntp</b> (123), <b>rip</b> (520), <b>snmp</b> (161), <b>snmptrap</b> (162), <b>sunrpc</b> (111), <b>syslog</b> (514), <b>tacacs-ds</b> (65), <b>talk</b> (517), <b>tftp</b> (69), <b>time</b> (37), <b>who</b> (513), and <b>xdmcp</b> (177).
<b>tcp-type</b> { <b>tcpurg</b>   <b>tcpack</b>   <b>tcpsh</b>   <b>tcprst</b>   <b>tcpsyn</b>   <b>tcpfin</b> }	Specifies a TCP flag.	Parameters specific to TCP.

If the *protocol* argument takes **icmpv6** (58), you can set the parameters shown in [Table 14](#).

**Table 14 ICMPv6-specific parameters for simple ACL rules**

Parameters	Function	Description
<b>icmp6-type</b> { <i>icmp6-type</i> <i>icmp6-code</i>   <i>icmp6-message</i> }	Specifies the ICMPv6 message type and code.	The <i>icmp6-type</i> argument is in the range of 0 to 255. The <i>icmp6-code</i> argument is in the range of 0 to 255. The <i>icmp6-message</i> argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in <a href="#">Table 15</a> .

**Table 15 ICMPv6 message names supported in simple ACL rules**

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

## Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt fails.

## Examples

# Create a rule for simple ACL 10000 to match TCP packets with the RST flag and the source address of 2200:100::/64.

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

```
[Sysname] acl ipv6 number 10000
```

```
[Sysname-acl6-simple-10000] rule tcp addr-flag 4 source 2200:100::/64 tcp-type tcprst
```

## Related commands

**acl ipv6**

# rule (user-defined ACL view)

Use **rule** to create or edit a user-defined ACL rule.

Use **undo rule** to delete an entire user-defined ACL rule.

## Syntax

**rule** [ *rule-id* ] { **deny** | **permit** } [ **I2** *rule-string rule-mask offset* ]&<1-8> [ **counting** | **time-range** *time-range-name* ] \*

**undo rule** *rule-id*

## Default

A user-defined ACL does not contain any rule.

## Views

User-defined ACL view

## Default command level

2: System level

## Parameters

**rule-id**: Specifies a rule ID in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

**deny**: Denies matching packets.

**permit**: Allows matching packets to pass.

**I2**: Specifies that the offset is relative to the beginning of the Layer 2 frame header.

**start**: Specifies that the offset is relative to the beginning of the outmost header. The start byte varies with device models.

**rule-string**: Defines a match pattern in hexadecimal format. Its length must be a multiple of two.

**rule-mask**: Defines a match pattern mask in hexadecimal format. Its length must be the same as that of the match pattern. A match pattern mask is used for ANDing the selected string of a packet.

**offset**: Offset in bytes after which the match operation begins.

**&<1-8>**: Specifies that up to eight match patterns can be defined in the ACL rule.

**counting**: Counts the number of times the ACL rule has been matched. This option is disabled by default.

**time-range** *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument takes a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the timer range.

## Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt fails.

To view rules in an ACL and their rule IDs, use the **display acl all** command.

## Examples

# Create a rule for user-defined ACL 5005 to permit packets in which the 13th and 14th bytes starting from the Layer 2 header are 0x0806 (that is, ARP packets).

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

## Related commands

- **acl**
- **display acl**
- **step**
- **time-range**

## rule (WLAN ACL view)

Use **rule** to create or edit a WLAN ACL rule.

Use **undo rule** to delete an entire WLAN ACL rule.

## Syntax

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

## Default

A WLAN ACL does not contain any rule.

## Views

WLAN ACL view

## Default command level

2: system level

## Parameters

**rule-id**: Specifies a rule ID in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

**deny**: Denies matching packets.

**permit**: Allows matching packets to pass.

**ssid** *ssid-name*: Specifies a WLAN's SSID name, a case-sensitive string of 1 to 32 alphanumeric characters. Spaces are allowed. If the **ssid** option is not specified, the rule applies to packets with any SSID.

## Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the ACL rule you are creating or editing has the same deny or permit statement as another rule in the ACL, your creation or editing attempt fails.

To view rules in an ACL and their rule IDs, use the **display acl all** command.

The following matrix shows the command and hardware compatibility:

Hardware	Rule (WLAN ACL view)
MSR800	No
MSR 900	Yes
MSR900-E	No

Hardware	Rule (WLAN ACL view)
MSR 930	No
MSR 20-1X	Yes
MSR 20	Yes
MSR 30	Yes
MSR 50	Yes (except MPU-G2)
MSR 2600	Yes
MSR3600-51F	Yes

## Examples

# Create a rule for WLAN ACL 100 to permit packets with the SSID name of **user1** and apply this ACL to user interface VTY 0 to restrict user access.

```
<Sysname> system-view
[Sysname] acl number 100
[Sysname-acl-wlan-100] rule permit ssid user1
[Sysname-acl-wlan-100] quit
[Sysname] user-interface vty 0
[Sysname-ui-vty0] acl 100 inbound
```

## Related commands

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

## rule comment

Use **rule comment** to add a comment about an existing ACL rule or edit its comment to make the rule easy to understand.

Use **undo rule comment** to delete the ACL rule comment.

## Syntax

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

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

## Default

An ACL rule has no rule comment.

## Views

WLAN ACL view, IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view, user-defined ACL view

The following matrix shows the WLAN ACL view and hardware compatibility:

Hardware	WLAN ACL view
MSR800	No
MSR 900	Yes
MSR900-E	No

Hardware	WLAN ACL view
MSR 930	No
MSR 20-1X	Yes
MSR 20	Yes
MSR 30	Yes
MSR 50	Yes (except MPU-G2)
MSR 2600	Yes
MSR3600-51F	Yes

## Default command level

2: System level

## Parameters

*rule-id*: Specifies an ACL rule ID in the range of 0 to 65534. The ACL rule must already exist.

*text*: Specifies a comment about the ACL rule, a case-sensitive string of 1 to 127 characters.

## Examples

# Create a rule in IPv4 basic ACL 2000 and add a comment about the rule.

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

# Create a rule in IPv6 basic ACL 2000 and add a comment about the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 1001::1 128
[Sysname-acl6-basic-2000] rule 0 comment This rule is used on Ethernet 1/1.
```

## Related commands

- **display acl**
- **display acl ipv6**

## rule remark

Use **rule remark** to add a start or end remark for a range of rules that are created for the same purpose.

Use **undo rule remark** to delete the specified or all rule range remarks.

## Syntax

**rule** [ *rule-id* ] **remark** *text*

**undo rule** [ *rule-id* ] **remark** [ *text* ]

## Default

No rule range remarks are configured.

## Views

WLAN ACL view, IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view, user-defined ACL view



## Default command level

2: System level

## Parameters

*rule-id*: Specifies a rule number in the range of 0 to 65534. The specified rule can be one that has been created or not. If you specify no rule ID when adding a remark, the system automatically picks the rule ID that is the nearest higher multiple of the numbering step to the current highest rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the system picks rule 30.

*text*: Specifies a remark, a case-sensitive string of 1 to 63 characters.

## Usage guidelines

A rule range remark always appears immediately above the specified rule. If the specified rule has not been created yet, the position of the comment in the ACL is as follows:

- If the match order is config, the remark is inserted into the ACL in descending order of rule ID.
- If the match order is auto, the remark is placed at the end of the ACL. After you create the rule, the remark appears above the rule.

To display rule range remarks in an ACL, use the **display this** or **display current-configuration**.

When you delete rule range remarks, follow these guidelines:

- If neither *rule-id* nor *text* is specified, all rule range remarks are removed.
- Use the **undo rule remark text** command to remove all remarks that are the same as the *text* argument.
- Use the **undo rule rule-id remark** command to delete a specific rule range remark. If you also specify the *text* argument, you must type in the remark the same as was specified to successfully remove the remark.

When adding an end remark for a rule range, you can specify the end rule number plus 1 for the *rule-id* argument so all rules in this range appears between the two remarks. You can also specify the end rule number for the *rule-id* argument. When you use this method, the end rule appears below the end remark. Whichever approach you use, be consistent.

## Examples

# Display the running configuration of IPv4 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] display this
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
 rule 5 permit source 10.1.1.1 0 time-range work-time
 rule 10 permit source 192.168.0.0 0.0.0.255
 rule 15 permit source 1.1.1.1 0
 rule 20 permit source 10.1.1.1 0
 rule 25 permit counting
#
return
```

# Add a start comment "Rules for VIP\_start" and an end comment "Rules for VIP\_end" for the rule range 10 to 25.

```
[Sysname-acl-basic-2000] rule 10 remark Rules for VIP_start
[Sysname-acl-basic-2000] rule 26 remark Rules for VIP_end
```

# Verify the configuration.

```
[Sysname-acl-basic-2000] display this
#
acl number 2000
 rule 0 permit source 14.1.1.0 0.0.0.255
 rule 5 permit source 10.1.1.1 0 time-range work-time
 rule 10 remark Rules for VIP_start
 rule 10 permit source 192.168.0.0 0.0.0.255
 rule 15 permit source 1.1.1.1 0
 rule 20 permit source 10.1.1.1 0
 rule 25 permit counting
 rule 26 remark Rules for VIP_end
#
return
```

## Related commands

- **display this**
- **display current-configuration** (*Fundamentals Command Reference*)

## step

Use **step** to set a rule numbering step for an ACL. The rule numbering step sets the increment by which the system numbers rules automatically. For example, the default ACL rule numbering step is 5. If you do not assign IDs to rules you are creating, they are numbered 0, 5, 10, 15, and so on. The wider the numbering step, the more rules you can insert between two rules. Whenever the step changes, the rules are renumbered, starting from 0. For example, if there are five rules numbered 5, 10, 13, 15, and 20, changing the step from 5 to 2 causes the rules to be renumbered 0, 2, 4, 6, and 8.

Use **undo step** to restore the default.

## Syntax

**step** *step-value*

**undo step**

## Default

The rule numbering step is 5.

## Views

WLAN ACL view, IPv4 basic/advanced ACL view, IPv6 basic/advanced ACL view, Ethernet frame header ACL view

The following matrix shows the view and router compatibility:

Hardware	WLAN ACL view
MSR800	No
MSR 900	Yes
MSR900-E	No
MSR 930	No
MSR 20-1X	Yes
MSR 20	Yes
MSR 30	Yes

Hardware	WLAN ACL view
MSR 50	Yes (except MPU-G2)
MSR 2600	Yes
MSR3600-51F	Yes

## Default command level

2: System level

## Parameters

*step-value*: ACL rule numbering step in the range of 1 to 20.

## Usage guidelines

After you restore the default numbering step by using the **undo step** command, the rules are renumbered in steps of 5.

## Examples

# Set the rule numbering step to 2 for IPv4 basic ACL 2000.

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

# Set the rule numbering step to 2 for IPv6 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] step 2
```

## Related commands

- **display acl**
- **display acl ipv6**

# time-range

Use **time-range** to configure a time range. If you provide an existing time range name, the command adds a statement to the time range.

Use **undo time-range** to delete a time range or a statement in the time range.

## Syntax

**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* ]

## Default

No time range exists.

## Views

System view

## Default command level

2: System level

## Parameters

*time-range-name*: Specifies a time range name. The name is a case-insensitive string of 1 to 32 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

*start-time to end-time*: Specifies a periodic statement. Both *start-time* and *end-time* are in hh:mm format (24-hour clock). The value is in the range of 00:00 to 23:59 for the start time, and 00:00 to 24:00 for the end time. The end time must be greater than the start time.

*days*: Specifies the day or days of the week (in words or digits) on which the periodic statement is valid. If you specify multiple values, separate each value with a space, and make sure that they do not overlap. These values can take one of the following forms:

- A digit in the range of 0 to 6, respectively, for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- A day of a week in abbreviated words: **sun**, **mon**, **tue**, **wed**, **thu**, **fri**, and **sat**.
- **working-day** for Monday through Friday.
- **off-day** for Saturday and Sunday.
- **daily** for the whole week.

*from time1 date1*: Specifies the start time and date of an absolute statement. The *time1* argument specifies the time of the day in hh:mm format (24-hour clock). Its value is in the range of 00:00 to 23:59. The *date1* argument specifies a date in MM/DD/YYYY or YYYY/MM/DD format, where MM is the month of the year in the range of 1 to 12, DD is the day of the month with the range depending on MM, and YYYY is the year in the calendar in the range of 1970 to 2100. If not specified, the start time is 01/01/1970 00:00 AM, the earliest time available in the system.

*to time2 date2*: Specifies the end time and date of the absolute time statement. The *time2* argument has the same format as the *time1* argument, but its value is in the range of 00:00 to 24:00. The *date2* argument has the same format and value range as the *date1* argument. The end time must be greater than the start time. If not specified, the end time is 12/31/2100 24:00 PM, the maximum time available in the system.

## Usage guidelines

You can create multiple statements in a time range. Each time statement can take one of the following forms:

- Periodic statement in the *start-time to end-time days* format. A periodic statement recurs periodically on a day or days of the week.
- Absolute statement in the *from time1 date1 to time2 date2* format. An absolute statement does not recur.
- Compound statement in the *start-time to end-time days from time1 date1 to time2 date2* format. A compound statement recurs on a day or days of the week only within the specified period. For example, to create a time range that is active from 08:00 to 12:00 on Monday between January 1, 2010 00:00 and December 31, 2010 23:59, use the **time-range test 08:00 to 12:00 mon from 00:00 01/01/2010 to 23:59 12/31/2010** command.

You can create a maximum of 256 time ranges, each with a maximum of 32 periodic statements and 12 absolute statements. The active period of a time range is calculated as follows:

1. Combining all periodic statements
2. Combining all absolute statements
3. Taking the intersection of the two statement sets as the active period of the time range

## Examples

# Create a periodic time range **t1**, setting it to be active between 8:00 to 18:00 during working days.

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

```
[Sysname] time-range t1 8:0 to 18:0 working-day
```

# Create an absolute time range **t2**, setting it to be active in the whole year of 2010.

```
<Sysname> system-view
[Sysname] time-range t2 from 0:0 1/1/2010 to 24:0 12/31/2010

# Create a compound time range t3, setting it to be active from 08:00 to 12:00 on Saturdays and
Sundays of the year 2010.

<Sysname> system-view
[Sysname] time-range t3 8:0 to 12:0 off-day from 0:0 1/1/2010 to 24:0 12/31/2010

# Create a compound time range t4, setting it to be active from 10:00 to 12:00 on Mondays and from
14:00 to 16:00 on Wednesdays in the period of January through June of the year 2010.

<Sysname> system-view
[Sysname] time-range t4 10:0 to 12:0 1 from 0:0 1/1/2010 to 24:0 1/31/2010
[Sysname] time-range t4 14:0 to 16:0 3 from 0:0 6/1/2010 to 24:0 6/30/2010
```

## **Related commands**

**display time-range**

# QoS policy commands

## Class commands

### display traffic classifier

Use **display traffic classifier** to display class information.

#### Syntax

```
display traffic classifier { system-defined | user-defined } [ classifier-name ] [ | { begin | exclude | include } regular-expression ]
```

#### Views

Any view

#### Default command level

1: Monitor level

#### Parameters

**system-defined**: Displays system-defined classes.

**user-defined**: Displays user-defined classes.

*classifier-name*: Class name, a string of 1 to 31 characters.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

#### Usage guidelines

If no class name is specified, the command displays information about all system-defined or user-defined classes.

#### Examples

# Display information about all user-defined classes.

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

```
User Defined Classifier Information:
```

```
Classifier: USER1
```

```
Operator: AND
```

```
Rule(s) : If-match ip-precedence 5
```

```
Classifier: database
```

```
Operator: AND
```

```
Rule(s) : If-match acl 3131
```

```
          If-match inbound-interface Ethernet1/1
```

**Table 16 Command output**

Field	Description
Classifier	Class name and its match criteria.
Operator	Match operator you set for the class. If the operator is AND, the class matches the packets that match all its match criteria. If the operator is OR, the class matches the packets that match any of its match criteria.
Rule(s)	Match criteria.

## if-match

Use **if-match** to define a match criterion.

Use **undo if-match** to delete a match criterion.

Use **if-match not** to define a criterion for matching traffic not conforming to the specified criterion.

Use **undo if-match not** to delete a criterion for matching traffic not conforming to the specified criterion.

### Syntax

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

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

**undo if-match** [ **not** ] **acl** [ **ipv6** ] { *acl-number* | **name** *acl-name* } [ **update acl** [ **ipv6** ] { *acl-number* | **name** *acl-name* } ]

### Views

Class view

### Default command level

2: System level

### Parameters

**not**: Matches packets that do not conform to the specified criterion.

*match-criteria*: Specifies a match criterion. [Table 17](#) shows the available criteria.

**acl** [ **ipv6** ] { *acl-number* | **name** *acl-name* }: Specifies an ACL already referenced in the class by the ACL name or ACL number.

**update acl** [ **ipv6** ] { *acl-number* | **name** *acl-name* }: Specifies a new ACL by its number or name to replace the ACL already referenced by the class.

**Table 17 The value range for the *match-criteria* argument**

Keyword and argument combination	Description
<b>acl</b> [ <b>ipv6</b> ] { <i>acl-number</i>   <b>name</b> <i>acl-name</i> }	Matches an ACL. The value range for the <i>acl-number</i> argument is 2000 to 5999 for an IPv4 ACL and 2000 to 3999 for an IPv6 ACL. The <i>acl-name</i> argument is a case-insensitive string of 1 to 63 characters, which must start with an English letter from a to z or A to Z, and to avoid confusion, cannot be <b>all</b> .
<b>any</b>	Matches all packets.
<b>classifier</b> <i>classifier-name</i>	Matches a QoS class.

Keyword and argument combination	Description
	The <i>classifier-name</i> argument is the name of the class.
<b>customer-dot1p</b> <i>8021p-list</i>	Matches the 802.1p priority of the customer network. The <i>8021p-list</i> argument is a list of up to eight 802.1p priority values. An 802.1p priority is in the range of 0 to 7.
<b>customer-vlan-id</b> { <i>vlan-id-list</i>   <i>vlan-id1 to vlan-id2</i> }	Matches the VLAN IDs of customer networks. The <i>vlan-id-list</i> argument is a list of up to eight VLAN IDs. The <i>vlan-id1 to vlan-id2</i> option specifies a VLAN ID range, where the <i>vlan-id1</i> must be smaller than the <i>vlan-id2</i> . A VLAN ID is in the range of 1 to 4094.
<b>destination-mac</b> <i>mac-address</i>	Matches a destination MAC address.
<b>dscp</b> <i>dscp-list</i>	Matches DSCP values. The <i>dscp-list</i> argument is a list of up to eight DSCP values. A DSCP value is in the range of 0 to 63.
<b>fr-de</b>	Matches DE flags of FR packets.
<b>inbound-interface</b> <i>interface-type interface-number</i>	Matches an incoming interface.
<b>ip-precedence</b> <i>ip-precedence-list</i>	Matches IP precedence. The <i>ip-precedence-list</i> argument is a list of up to eight IP precedence values. An IP precedence is in the range of 0 to 7.
<b>mpls-exp</b> <i>exp-list</i>	Matches MPLS EXP values. The <i>exp-list</i> argument is a list of up to eight EXP values. An EXP value is in the range of 0 to 7.
<b>protocol</b> <i>protocol-name</i>	Matches a protocol.
<b>protocol-group</b> <i>protocol-group-id</i>	Matches a protocol group ID. The <i>protocol-group-id</i> argument specifies a protocol group and is in the range of 1 to 64.
<b>qos-local-id</b> <i>local-id-value</i>	Matches a local QoS ID, which is in the range of 1 to 4095.
<b>rtp start-port</b> <i>start-port-number end-port end-port-number</i>	Matches RTP protocol ports. The value ranges for the <i>start-port-number</i> and <i>end-port-number</i> arguments are both 2000 to 65535.
<b>source-mac</b> <i>mac-address</i>	Matches a source MAC address.

## Usage guidelines

### Defining an ACL-based match criterion

If the ACL referenced in the **if-match** command does not exist, the class cannot be applied to hardware.

For a class, you can reference an ACL twice by its name and number with the **if-match** command, respectively.

### Defining a criterion to match a destination MAC address

You can configure multiple destination MAC address match criteria for a class.

A destination MAC address match criterion is significant only to Ethernet interfaces.

### Defining a criterion to match a source MAC address

You can configure multiple source MAC address match criteria for a class.



A criterion to match a source MAC address is significant only to Ethernet interfaces.

## Defining the relationships between match criteria

This subsection describes how to use both AND and OR operators to define the match relationships between the criteria for a class.

For example, define class **classA** with three match criteria. The relationship between them is criterion 1 AND criterion 2 OR criterion 3. Use the following commands:

**traffic class classB operator and**

**if-match criterion 1**

**if-match criterion 2**

**traffic class classA operator or**

**if-match criterion 3**

**if-match class classB**

You can configure multiple **if-match** clauses for a class.

## Defining a criterion to match DSCP values

- You can configure multiple DSCP match criteria for a class. All defined DSCP values are automatically sorted in ascending order.
- You can configure up to eight DSCP values in one command line. If multiple identical DSCP values are specified, the system considers them as one. If a packet matches one of the defined DSCP values, it matches the **if-match** clause.
- To delete a criterion that matches DSCP values, the specified DSCP values must be identical with those defined in the criterion (the sequence can be different).

## Defining a criterion to match 802.1p priority in customer VLAN tags

- You can configure multiple 802.1p priority match criteria for a class. All the defined 802.1p values are automatically arranged in ascending order.
- You can configure up to eight 802.1p priority values in one command line. If the same 802.1p priority value is specified multiple times, the system considers them as one. If a packet matches one of the defined 802.1p priority values, it matches the **if-match** clause.
- To delete a criterion that matches 802.1p priority values, the specified 802.1p priority values in the command must be identical with those defined in the criterion (the sequence can be different).

## Defining a criterion to match DE flags of FR packets

Only one DE flag match criterion can be configured for a class.

## Defining a criterion to match an incoming interface

- You can configure multiple incoming interface match criteria for a class.
- The specified incoming interface must exist. If the specified interface is a dynamic one, removing the interface deletes the match criterion.
- The following interface types are supported: ATM, Ethernet, serial, tunnel, and VT.

## Defining a criterion to match IP precedence values

- You can configure multiple IP precedence match criteria for a class. The defined IP precedence values are automatically arranged in ascending order.
- You can configure up to eight IP precedence values in one command line. If the same IP precedence is specified multiple times, the system considers them as one. If a packet matches one of the defined IP precedence values, it matches the **if-match** clause.

- To delete a criterion that matches IP precedence values, the specified IP precedence values in the command must be identical with those defined in the criterion (the sequence can be different).

### Defining a criterion to match local precedence values

- You can configure multiple local precedence match criteria for a class. The defined local precedence values are automatically arranged in ascending order.
- You can configure up to eight local precedence values in one command line. If the same local precedence value is specified multiple times, the system considers them as one. If a packet matches one of the defined local precedence values, it matches the **if-match** clause.
- To delete a criterion that matches local precedence values, the specified local precedence values must be identical with those defined in the match criterion (the sequence can be different).

### Defining a criterion to match MPLS EXP values

- You can configure multiple MPLS EXP match criteria for a class. The defined MPLS EXP values are automatically arranged in ascending order.
- You can configure up to eight MPLS EXP values in one command line. If the same MPLS EXP value is specified multiple times, the system considers them as one. If a packet matches one of the defined MPLS EXP values, it matches the **if-match** clause.
- To delete a criterion that matches MPLS EXP values, the specified MPLS EXP values in the command must be identical with those defined in the criterion (the sequence can be different). The MPLS EXP field exists only in MPLS packets, so this match criterion takes effect for only the MPLS packets.
- As for software forwarding QoS, MPLS packets do not support IP-related matching rules.

### Defining a criterion to match RTP protocol ports

- This command matches RTP packets with an even UDP destination port number in the specified RTP port number range.
- The RTP protocol port match criterion you configured overwrites the previous one, if any.

### Defining a criterion to match customer network VLAN IDs

- You can configure multiple VLAN ID match criteria for a class. The defined VLAN IDs are automatically arranged in ascending order.
- You can configure multiple VLAN IDs in one command line. If the same VLAN ID is specified multiple times, the system considers them as one. If a packet matches one of the defined VLAN IDs, it matches the **if-match** clause.
- To delete a criterion that matches VLAN IDs, the specified VLAN IDs in the command must be identical with those defined in the criterion (the sequence can be different).

### Examples

# Define a criterion to match any packets other than IP packets.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match not protocol ip
```

# Define a match criterion for class **class1** to match the packets with their destination MAC addresses being 0050-ba27-bed3.

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

# Define a match criterion for class **class2** to match the packets with their source MAC addresses being 0050-ba27-bed2.

```

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

# Define a match criterion for class class1 to match the packets with their customer network 802.1p
priority values being 3.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-dot1p 3

# Define a match criterion for class class1 to match the advanced ACL 3101.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3101

# Define a match criterion for class class1 to match the ACL named flow.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl name flow

# Define a match criterion for class class1 to match the advanced IPv6 ACL 3101.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 3101

# Define a match criterion for class class1 to match the IPv6 ACL named flow.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl ipv6 name flow

# Define a match criterion for class class1 to match all packets.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match any

# Define a match criterion for class class1 to match the packets with IP precedence 5. Configure
class class2 to match packets that both match class class1 and have destination MAC addresses
0050-BA27-BED3.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ip-precedence 5
[Sysname-classifier-class1] quit
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match classifier class1
[Sysname-classifier-class2] if-match destination-mac 0050-BA27-BED3

# Define a match criterion for class class1 to match the packets with their DSCP values being 1, 6 or
9.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match dscp 1 6 9

# Define a match criterion for class class1 to match the FR packets with DE flags.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match fr-de

```

# Define a match criterion for class **class1** to match the packets received on interface Ethernet 1/1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match inbound-interface ethernet 1/1
```

# Define a match criterion for class **class1** to match the packets with their IP precedence values being 1 or 6.

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

# Define a match criterion for class **class1** to match IP packets.

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

# Define a match criterion for class **class1** to match the RTP packets with an even UDP destination port number in the range of 16384 and 32767.

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

# Define a match criterion for class **class1** to match the packets of customer network VLAN 1, 6, or 9.

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

# Define a match criterion for class **class1** to match packets with their local QoS IDs being 3.

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

# Change the match criterion of class **class1** from ACL 2008 to ACL 2009.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 2008
[Sysname-classifier-class1] undo if-match acl 2008 update acl 2009
```

# Define a match criterion for class **class1** to match packets with their protocol group IDs being 2.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match protocol-group 2
```

## Related commands

**traffic classifier**

## traffic classifier

Use **traffic classifier** to create a class and enter class view.

Use **undo traffic classifier** to delete a class.

## Syntax

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

**undo traffic classifier** *classifier-name*

## Views

System view

## Default command level

2: System level

## Parameters

*classifier-name*: Specifies a class name, a string of 1 to 31 characters.

**operator**: Sets the operator to logic AND or OR for the class.

**and**: Specifies the logic AND operator. The class matches the packets that match all its criteria.

**or**: Specifies the logic OR operator. The class matches the packets that match any of its criteria.

## Usage guidelines

If no match operator is specified, the default AND operator applies.

The *classifier-name* argument cannot take the name of any system-defined class:

**default-class**, **ef**, **af1**, **af2**, **af3**, **af4**, **ip-prec0**, **ip-prec1**, **ip-prec2**, **ip-prec3**, **ip-prec4**, **ip-prec5**, **ip-prec6**, **ip-prec7**, **mpls-exp0**, **mpls-exp1**, **mpls-exp2**, **mpls-exp3**, **mpls-exp4**, **mpls-exp5**, **mpls-exp6**, **mpls-exp7**.

## Examples

```
# Create a class class1.  
<Sysname> system-view  
[Sysname] traffic classifier class1  
[Sysname-classifier-class1]
```

## Related commands

- **qos policy**
- **qos apply policy**
- **classifier behavior**

# Traffic behavior commands

## car

Use **car** to configure a CAR action in a traffic behavior.

Use **undo car** to delete the CAR action in a traffic behavior.

## Syntax

```
car cir { committed-information-rate [ cbs committed-burst-size [ ebs excess-burst-size ] ] [ pir peak-information-rate ] | percent percentage [ cbs committed-burst-size-ms [ ebs excess-burst-size-ms ] ] } [ green action ] [ red action ]
```

```
undo car
```

## Default

CBS is the amount of traffic transmitted at the rate of CIR over 500 ms.

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

**cir** *committed-information-rate*: Specifies the committed information rate (CIR) in kbps, which specifies an average traffic rate.

**cbs** *committed-burst-size*: Specifies the committed burst size (CBS) in bytes.

**ebs** *excess-burst-size*: Specifies the excess burst size (EBS) in bytes. The default is 0.

**percent** *percentage*: Specifies the CIR in percentage in the range of 0 to 100.

**cbs** *committed-burst-size-ms*: Specifies the CBS in milliseconds (ms) when the CIR is configured in percentage. The value range for the *committed-burst-size-ms* argument is 50 to 2000, and the default is 500.

**ebs** *excess-burst-size-ms*: Specifies the EBS in ms when the CIR is configured in percentage. The value range for the *excess-burst-size-ms* argument is 0 to 2000, and the default is 0.

**green** *action*: Action to take on packets that conform to CIR. The default is **pass**.

**red** *action*: Specifies the action to take on the packet that conforms to neither CIR nor PIR. The default is **discard**.

*action*: Sets the action to take on the packet:

- **discard**—Drops the packet.
- **pass**—Permits the packet to pass through.
- **remark-dscp-pass** *new-dscp*—Sets the DSCP value of the packet to *new-dscp* and permits the packet to pass through. The value range for the *new-dscp* argument is 0 to 63.
- **remark-prec-pass** *new-precedence*—Sets the IP precedence of the packet to *new-precedence* and permits the packet to pass through. The value range for the *new-precedence* argument is 0 to 7.

## Usage guidelines

A QoS policy that has a CAR action can be applied to inbound or outbound direction of an interface or PVC.

If a QoS policy that has a CAR action and the **qos car** command are both configured on the interface or PVC, only the CAR action in the policy takes effect.

A traffic behavior can contain only one CAR action. If you configure the **car** command multiple times in the same traffic behavior, the last configuration takes effect.

## Examples

# Configure a CAR action in traffic behavior **database** (set the CIR to 200 kbps, CBS to 50000 bytes, and EBS to 0, and permit the conforming packets to pass, and mark the excess packets with IP precedence 0 and forward them.)

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

# Configure a QoS policy (CIR as 50% of the interface bandwidth in the CAR action) and apply the QoS policy to interface GigabitEthernet 0/1.

```
<Sysname> system-view
[Sysname] traffic classifier c1
[Sysname-classifier-c1] if-match any
[Sysname-classifier-c1] quit
[Sysname] traffic behavior b1
```

```
[Sysname-behavior-b1] car cir percent 50
[Sysname-behavior-b1] quit
[Sysname] qos policy p1
[Sysname-qospolicy-p1] classifier c1 behavior b1
[Sysname-qospolicy-p1] quit
[Sysname] interface GigabitEthernet 0/1
[Sysname-GigabitEthernet0/1] qos apply policy p1 outbound
```

## Related commands

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

# display traffic behavior

Use **display traffic behavior** to display traffic behavior information.

## Syntax

```
display traffic behavior { system-defined | user-defined } [ behavior-name ] [ | { begin | exclude
| include } regular-expression ]
```

## Views

Any view

## Default command level

1: Monitor level

## Parameters

**system-defined**: Displays system-defined traffic behaviors.

**user-defined**: Displays user-defined traffic behaviors.

*behavior-name*: Behavior name, a string of 1 to 31 characters. If no traffic behavior is specified, this command displays information about all the system-defined or user-defined behaviors.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Examples

# Display user-defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined
User Defined Behavior Information:
  Behavior: test
    Assured Forwarding:
      Bandwidth 30 (Kbps)
      Discard Method: Tail
    General Traffic Shape:
      CIR 300 (kbps), CBS 15000 (byte), EBS 0 (byte)
      Queue length 50 (Packets)
```

```

Marking:
    Remark MPLS EXP 3
Filter enable: permit
Behavior: USER1
Marking:
    Remark IP Precedence 3
Committed Access Rate:
    CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte), PIR 16000 (kbps)
    Green Action: pass
    Red Action: discard
Expedited Forwarding:
    Bandwidth 50 (Kbps) CBS 1500 (Bytes)
Nesting:
    Nest Top-Most Vlan-ID 1000
Behavior: USER2
Mirror enable:
    Mirror type: interface
    Mirror destination: Ethernet0/5
Redirect enable:
    Redirect type: cpu
    Redirect destination: cpu
Nest Policy:
    Traffic-policy test
Behavior: USER3
Flow based Weighted Fair Queue:
    Max number of hashed queues: 1000
    Discard Method: Tail
Filter enable : deny

```

**Table 18 Command output**

Field	Description
User Defined Behavior Information	User-defined behavior information.
Behavior	Name of a behavior.
Assured Forwarding	Information about an assured forwarding (AF) queue.
Bandwidth	Bandwidth of a queue.
Discard Method	Drop mode used when traffic exceeds the queue bandwidth: tail drop, IP precedence-based WRED, or DSCP-based WRED.
General Traffic Shape	GTS configuration information.
Queue length	Length of a queue.
Marking	Information about traffic marking.
Remark	Type of precedence marked for traffic: DSCP, IP precedence, MPLS EXP, FR DE, dot1p (CoS), ATM CLP, or qos local ID.
Filter enable	Traffic filtering option: permit or deny.
Committed Access Rate	Information about the CAR action.
Green Action	Action to be taken on green packets. For more information, see <a href="#">car</a> .



Field	Description
Red Action	Action to be taken on red packets. For more information, see <a href="#">car</a> .
Expedited Forwarding	Information about expedited forwarding.
Nesting	Information about tagging packets with a VLAN tag.
Mirror enable	Traffic mirroring configuration information.
Mirror type	Traffic mirroring type, which can only be interface.
Mirror destination	Mirroring destination: interface name.
Redirect enable	Traffic redirecting configuration information.
Redirect type	Traffic redirecting type: interface or cpu.
Redirect destination	Destination for traffic redirecting: an interface name or cpu.
Nest Policy	Policy nesting configuration information.
Traffic-policy	Name of the policy nested.
Flow based Weighted Fair Queue	Flow-based WFQ configuration information.
Max number of hashed queues	Length of the weighted fair queue.
Filter enable	NetStream configuration information. The NetStream filtering option can be <b>permit</b> or <b>deny</b> .

## filter

Use **filter** to configure a traffic filtering action in a traffic behavior.

Use **undo filter** to delete the traffic filtering action.

### Syntax

**filter { deny | permit }**

**undo filter**

### Views

Traffic behavior view

### Default command level

2: System level

### Parameters

**deny**: Drops packets.

**permit**: Permits packet to pass through.

### Examples

# Configure the traffic filtering action as **deny** in traffic behavior **database**.

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

```
[Sysname] traffic behavior database
```

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

## gts

Use **gts** to configure a GTS action in absolute value in a traffic behavior.

Use **undo gts** to delete a GTS action.

## Syntax

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

```
undo gts
```

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

**cir** *committed-information-rate*: CIR in kbps, which specifies the average traffic rate.

**cbs** *committed-burst-size*: CBS in bytes, which specifies the size of bursty traffic when the actual average rate is not greater than CIR.

**ebs** *excess-burst-size*: EBS in bytes. The default is 0.

**queue-length** *queue-length*: Maximum queue length. The default is 50.

## Usage guidelines

A QoS policy that references the GTS-configured behavior can be applied in only the outbound direction of an interface or PVC.

A policy referencing a GTS-configured behavior overwrites the **qos gts** command on the interface or PVC, if both are configured.

If this command is configured for the same traffic behavior for multiple times, the last configuration takes effect.

## Examples

# Configure a GTS action in absolute value in traffic behavior **database**. The GTS parameters are as follows: CIR is 200 kbps, CBS is 50000 bytes, EBS is 0, and the maximum buffer queue length is 100.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] gts cir 200 cbs 50000 ebs 0 queue-length 100
```

## Related commands

- **gts percent**
- **qos policy**
- **traffic behavior**
- **classifier behavior**

## gts percent

Use **gts percent** to configure a GTS action in percentage in the traffic behavior.

## Syntax

```
gts percent cir cir-percent [ cbs cbs-time [ ebs ebs-time ] ]
```

```
undo gts
```

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

**cir** *cir-percent*: CIR in percentage in the range of 0 to 100. The actual CIR value is *cir-percent* × interface bandwidth.

**cbs** *cbs-time*: CBS in the specified time (in ms). The default *cbs-time* is 500 ms. The actual CBS value is *cbs-time* × the actual CIR value.

**ebs** *ebs-time*: EBS in the specified time (in ms). The default *ebs-time* is 0 ms. The actual EBS value is *ebs-time* × the actual CIR value.

## Usage guidelines

A QoS policy that references the GTS-configured behavior can be applied in only the outbound direction of an interface or PVC.

A policy referencing a GTS-configured behavior overwrites the **qos gts** command on the interface or PVC, if both configured.

If this command is configured for the same traffic behavior for multiple times, the last configuration takes effect.

## Examples

# Configure a GTS action in percentage in traffic behavior **database**. The GTS parameters are as follows: CIR is 50 and CBS is 2000.

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

## Related commands

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

# redirect

Use **redirect** to configure a traffic redirecting action in the traffic behavior.

Use **undo redirect** to delete the traffic redirecting action.

## Syntax

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

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

**cpu**: Redirects traffic to the CPU.

**interface**: Redirects traffic to an interface.

*interface-type interface-number*: Specifies an interface by its type and number.

## Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Command compatibility
MSR800	No
MSR 900	No
MSR900-E	No
MSR 930	No
MSR 20-1X	No
MSR 20	Yes (only the <b>cpu</b> keyword is supported)
MSR 30	Supported only on MIM Layer 2 Ethernet switching modules, MSR 30-11E, and MSR 30-11F
MSR 50	Supported only on FIC Layer 2 Ethernet switching modules
MSR 2600	Yes
MSR3600-51F	Yes

## Examples

# Configure redirecting traffic to Ethernet 1/1 in traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface ethernet1/1
```

## remark dot1p

Use **remark dot1p** to configure an 802.1p priority marking action.

Use **undo remark dot1p** to delete the action.

### Syntax

```
remark dot1p 8021p
undo remark dot1p
```

### Views

Traffic behavior view

### Default command level

2: System level

### Parameters

*8021p*: 802.1p priority to be marked for packets, in the range of 0 to 7.

## Examples

# Configure traffic behavior **database** to mark matching traffic with 802.1p 2.

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

## Related commands

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

## remark dscp

Use **remark dscp** to configure a DSCP marking action.

Use **undo remark dscp** to delete the action.

### Syntax

**remark dscp** *dscp-value*

**undo remark dscp**

### Views

Traffic behavior view

### Default command level

2: System level

### Parameters

*dscp-value*: DSCP value, which can be a number from 0 to 63 or any keyword in [Table 19](#).

**Table 19 DSCP keywords and values**

Keyword	DSCP value (binary)	DSCP value (decimal)
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

Keyword	DSCP value (binary)	DSCP value (decimal)
cs7	111000	56
ef	101110	46

## Examples

# Configure traffic behavior **database** to mark matching traffic with DSCP 6.

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

## Related commands

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

## remark ip-precedence

Use **remark ip-precedence** to configure an IP precedence marking action.

Use **undo remark ip-precedence** to delete the action.

## Syntax

```
remark ip-precedence ip-precedence-value
undo remark ip-precedence
```

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

*ip-precedence-value*: IP precedence value to be marked for packets, in the range of 0 to 7.

## Examples

# Set the IP precedence to 6 for packets.

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

## Related commands

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

## remark qos-local-id

Use **remark qos-local-id** to configure the action of setting the specified QoS-local ID for packets.

Use **undo remark qos-local-id** to delete the action.

## Syntax

```
remark qos-local-id local-id-value  
undo remark qos-local-id
```

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

*local-id-value*: QoS-local ID to be marked for packets, in the range of 1 to 4095.

## Examples

```
# Configure the action of marking packet with QoS-local ID 2.  
<Sysname> system-view  
[Sysname] traffic behavior database  
[Sysname-behavior-database] remark qos-local-id 2
```

# traffic behavior

Use **traffic behavior** to create a traffic behavior and enter traffic behavior view.

Use **undo traffic behavior** to delete a traffic behavior.

## Syntax

```
traffic behavior behavior-name  
undo traffic behavior behavior-name
```

## Views

System view

## Default command level

2: System level

## Parameters

*behavior-name*: Sets a behavior name, a string of 1 to 31 characters. The specified *behavior-name* must not be a system-defined traffic behavior name like **ef**, **af**, **be**, or **be-flow-based**.

## Usage guidelines

A traffic behavior is a set of actions, such as priority marking, dropping, rate limiting, and accounting. You provide QoS for a class of traffic by associating a traffic behavior with the class of traffic.

## Examples

```
# Create a traffic behavior named behavior1.  
<Sysname> system-view  
[Sysname] traffic behavior behavior1  
[Sysname-behavior-behavior1]
```

## Related commands

- **qos policy**
- **qos apply policy**
- **classifier behavior**

# traffic-policy

Use **traffic-policy** to reference a policy in a traffic behavior. By associating the traffic behavior with a class in another policy, you perform policy nesting. The referenced policy is the child policy and the referencing policy is the parent policy.

Use **undo traffic-policy** to remove the child policy from the behavior.

## Syntax

**traffic-policy** *policy-name*

**undo traffic-policy**

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

*policy-name*: Policy name, a string of 1 to 31 characters. The policy must already exist.

## Usage guidelines

You can reference a QoS policy in a traffic behavior to re-classify the traffic class associated with the behavior and take action on the re-classified traffic as defined in the policy.

With policy nesting, you can perform the associated behavior defined in the parent policy for a class of traffic, and in addition, use the child policy to further classify the class of traffic and perform the behaviors defined in the child policy.

Follow these guidelines when you nest QoS policies:

- A parent policy can nest only one child policy. This child policy cannot be the parent policy itself or the parent of any other policy.
- You can reference only one child policy in a behavior.
- If the parent policy and the child policy contain the same behavior, the system performs the behavior in the parent policy first and then that in the child policy.
- To configure CBQ in the child policy successfully, configure GTS in the parent policy, and make sure that the configured GTS bandwidth is no smaller than CBQ bandwidth configured in the child policy.
- If GTS bandwidth in the parent policy is set in percentage, also set CBQ bandwidth in percentage in the child policy.
- A child policy cannot contain GTS actions.
- Policy nesting is available for IPv4, IPv6, and MPLS packets.
- To delete the child policy after you apply the parent policy to an interface or PVC, first remove the child policy from the parent policy.

## Examples

# Nest the child policy **child** in traffic behavior **database** of the parent policy.

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

## Related commands

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



# QoS policy configuration and application commands

## classifier behavior

Use **classifier behavior** to associate a behavior with a class in a QoS policy.

Use **undo classifier** to remove a class from the policy.

### Syntax

**classifier** *classifier-name* **behavior** *behavior-name*

**undo classifier** *classifier-name*

### Views

Policy view

### Default command level

2: System level

### Parameters

*classifier-name*: Class name, a string of 1 to 31 characters.

*behavior-name*: Behavior name, a string of 1 to 31 characters.

### Usage guidelines

You cannot remove a default class.

You can perform a set of QoS actions on a traffic class by associating a traffic behavior with the traffic class.

You can configure multiple class-behavior associations in a QoS policy, and each class can associate with only one traffic behavior.

If the specified class or traffic behavior does not exist, the system creates a null class or traffic behavior.

### Examples

# Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**.

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

```
[Sysname] qos policy user1
```

```
[Sysname-qospolicy-user1] classifier database behavior test
```

```
[Sysname-qospolicy-user1]
```

### Related commands

- **qos policy**
- **route-policy** (*Layer 3—IP Routing Command Reference*)

## display qos policy

Use **display qos policy** to display system-defined or user-defined QoS policy configuration information.

### Syntax

**display qos policy** { **system-defined** | **user-defined** } [ *policy-name* [ **classifier** *classifier-name* ] ]  
[ [ { **begin** | **exclude** | **include** } *regular-expression* ]

## Views

Any view

## Default command level

1: Monitor level

## Parameters

**system-defined:** Displays system-defined QoS policies.

**user-defined:** Displays user-defined QoS policies.

*policy-name:* QoS policy name, a string of 1 to 31 characters. If no policy is specified, this command displays configuration information of all the policies.

*classifier-name:* Class name, a string of 1 to 31 characters.

**|:** Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin:** Displays the first line that matches the specified regular expression and all lines that follow.

**exclude:** Displays all lines that do not match the specified regular expression.

**include:** Displays all lines that match the specified regular expression.

*regular-expression:* Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Examples

# Display the configuration information of user-defined QoS policies.

```
<Sysname> display qos policy user-defined
User Defined QoS Policy Information:
Policy: test
Classifier: default-class
  Behavior: be
    -none-
Classifier: USER1
  Behavior: USER1
  Marking:
    Remark IP Precedence 3
  Committed Access Rate:
    CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte)
  Green Action: pass
  Red Action: discard
  Expedited Forwarding:
    Bandwidth 50 (Kbps) CBS 1500 (Bytes)
Classifier: database
  Behavior: database
  Assured Forwarding:
    Bandwidth 30 (Kbps)
    Discard Method: Tail
    Queue Length : 64 (Packets)
  General Traffic Shape:
    CIR 300 (kbps), CBS 15000 (byte), EBS 0 (byte)
    Queue length 50 (Packets)
  Marking:
    Remark MPLS EXP 3
```

**Table 20 Command output**

Field	Description
Policy	Policy name.
Classifier	Class name. A policy can contain multiple classes, and each class is associated with a traffic behavior. A class can be configured with multiple match criteria. For more information, see the <b>traffic classifier</b> command in " <a href="#">Class commands</a> ."
Behavior	Behavior associated with the class. A behavior is associated with a class. It can be configured with multiple actions. For more information, see the <b>traffic behavior</b> command in " <a href="#">Traffic behavior commands</a> ."

## display qos policy interface

Use **display qos policy interface** to display information about the QoS policy or policies applied to an interface/PVC or all interfaces/PVCs.

### Syntax

```
display qos policy interface [ interface-type interface-number [ pvc { pvc-name [ vpi/vci ] | vpi/vci } ] ] [ inbound | outbound ] [ [ { begin | exclude | include } regular-expression ]
```

### Views

Any view

### Default command level

1: Monitor level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number to display information about the QoS policy or policies applied to it.

**inbound**: Displays information about the QoS policy applied in the inbound direction of the specified interface.

**outbound**: Displays information about the QoS policy applied in the outbound direction of the specified interface.

**pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* }: Displays information about the QoS policy applied to a PVC on an ATM interface. *pvc-name* specifies the PVC by its name. *vpi/vci* specifies the PVC by its VPI/VCI pair. This option is only available for ATM interfaces. When you specify this option, the **inbound** and **outbound** keywords are not available.

[ ]: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

### Usage guidelines

If a VT interface is specified, this command displays information about the QoS policy or policies applied to each VA interface inheriting the VT interface, but does not display QoS information about the VT interface.

## Examples

# Display information about the QoS policy or policies applied to Ethernet1/1.

<Sysname> display qos policy interface ethernet 1/1

Interface: Ethernet1/1

Direction: Outbound

Policy: test

Classifier: default-class

Matched : 0(Packets) 0(Bytes)

5-minute statistics:

Forwarded: 0/0 (pps/bps)

Dropped : 0/0 (pps/bps)

Rule(s) : If-match any

Behavior: be

Default Queue:

Flow Based Weighted Fair Queuing

Max number of hashed queues: 256

Matched : 0/0 (Packets/Bytes)

Enqueued : 0/0 (Packets/Bytes)

Discarded: 0/0 (Packets/Bytes)

Discard Method: Tail

Classifier: USER1

Matched : 0(Packets) 0(Bytes)

5-minute statistics:

Forwarded: 0/0 (pps/bps)

Dropped : 0/0 (pps/bps)

Operator: AND

Rule(s) : If-match ip-precedence 5

Behavior: USER1

Marking: 0(Packets)

Remark IP Precedence 3

Committed Access Rate:

CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte)

Green Action: pass

Red Action: discard

Green : 0(Packets) 0(Bytes)

Red : 0(Packets) 0(Bytes)

Expedited Forwarding:

Bandwidth 50 (Kbps), CBS 1500 (Bytes)

Matched : 0/0 (Packets/Bytes)

Enqueued : 0/0 (Packets/Bytes)

Discarded: 0/0 (Packets/Bytes)

Classifier: database

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 3131
          If-match inbound interface Ethernet1/1
Behavior: database
General Traffic Shape:
  CIR 300 (kbps), CBS 15000 (byte), EBS 0 (byte)
  Queue Length: 50 (Packets)
  Queue size   : 0 (Packets)
  Passed      : 0(Packets) 0(Bytes)
  Discarded: 0(Packets) 0(Bytes)
  Delayed    : 0(Packets) 0(Bytes)
  Discard Method: Tail
Marking: 0(Packets)
  Remark MPLS EXP 3
Assured Forwarding:
  Bandwidth 30 (Kbps)
  Matched   : 0/0 (Packets/Bytes)
  Enqueued  : 0/0 (Packets/Bytes)
  Discarded: 0/0 (Packets/Bytes)
  Discard Method: Tail
Nest Policy:
Traffic policy son1
Classifier: default-class
  Matched : 0/0 (Packets/Bytes)
  5-minute statistics:
    Forwarded: 0/0 (pps/bps)
    Dropped   : 0/0 (pps/bps)
  Rule(s) : If-match any
  Behavior: be
  Default Queue:
    Flow Based Weighted Fair Queuing
    Max number of hashed queues: 256
    Matched   : 0/0 (Packets/Bytes)
    Enqueued  : 0/0 (Packets/Bytes)
    Discarded: 0/0 (Packets/Bytes)
    Discard Method: Tail
Classifier: son1
  Matched : 0/0 (Packets/Bytes)
  5-minute statistics:
    Forwarded: 0/0 (pps/bps)
    Dropped   : 0/0 (pps/bps)
  Operator: AND
  Rule(s) : If-match acl 3000
  Behavior: son1
  Marking: 0(Packets)
    Remark MPLS EXP 3
  Committed Access Rate:
    CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte)

```

```

Green Action: pass
Red Action: discard
Green: 0/0 (Packets/Bytes)
Red : 0/0 (Packets/Bytes)
Expedited Forwarding:
Bandwidth 1000 (Kbps), CBS 25000 (Bytes)
Matched : 0/0 (Packets/Bytes)
Enqueued : 0/0 (Packets/Bytes)
Discarded: 0/0 (Packets/Bytes)

```

**Table 21 Command output**

Field	Description
Interface	Interface type and interface number.
Direction	Direction in which the policy is applied to the interface.
Policy	Name of the policy applied to the interface.
Classifier	Class name and configuration information.
Matched	Number of packets meeting the match criteria.
5-minute statistics	Traffic rate statistics collected in the last 5 minutes. If the number of QoS policies for which traffic rate statistics are collected exceeds 1000, or the number of classes for which traffic rate statistics are collected exceeds 10000, <b>none</b> is displayed.
Forwarded	Average rate of successfully forwarded criteria-matching packets during the statistics collecting interval.
Dropped	Average rate of dropped criteria-matching packets during the statistics collecting interval.
Operator	Logical relationship between match criteria in the class.
Rule(s)	Match criteria in the class.
Behavior	Behavior name and configuration information.
Default queue	Default queuing mechanism.
Matched	Number of packets/bytes meeting the match criteria in the queue.
Enqueued	Number of packets/bytes enqueued.
Discarded	Number of packets/bytes dropped.
Discard Method	Drop mode.
Marking	Marking-related information.
Remark IP precedence	Set IP precedence for packets.
Remark MPLS EXP	Set EXP for MPLS packets.
Green Action	Action to take on green packets.
Red Action	Action to take on red packets.
Green	Traffic statistics for green packets.
Red	Traffic statistics for red packets.
Expedited Forwarding	EF queue information.
Assured Forwarding	AF queue information.

Field	Description
Bandwidth	Minimum guaranteed bandwidth.
General Traffic Shape	GTS information.
Queue Length	Number of packets that the buffer queue can hold.
Queue Size	Number of packets in the buffer.
Passed	Number of packets/bytes permitted to pass through.
Discarded	Number of packets/bytes dropped.
Delayed	Number of packets/bytes delayed.
Nest Policy	Child policy of the policy applied to the interface.
Traffic policy son1	The name of the child policy is <b>son1</b> .

## qos apply policy (interface view, port group view, PVC view)

Use **qos apply policy** to apply a QoS policy.

Use **undo qos apply policy** to remove the QoS policy.

### Syntax

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

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

### Views

Interface view, port group view, PVC view

### Default command level

2: System level

### Parameters

**inbound**: Inbound direction.

**outbound**: Outbound direction.

*policy-name*: Specifies a policy name, a string of 1 to 31 characters.

### Usage guidelines

All physical interfaces, except interfaces with X.25 or LAPB encapsulation enabled, can have QoS policies applied.

To successfully apply a policy to an interface/PVC, make sure that the total bandwidth assigned to AF and EF in the policy is smaller than the available bandwidth of the interface/PVC. If the available bandwidth of the interface/PVC is modified to a value smaller than the total bandwidth for AF and EF, the applied policy is removed. For a policy to be applied in the inbound direction, the referenced traffic behaviors must not be configured with commands **queue af**, **queue ef**, **queue wfq**, and **gts**.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group. Settings in PVC view take effect on the current PVC.

Using this command on a VT interface makes the configuration effective on all the VA interfaces of the VT interface.

Using this command on a WLAN-ESS interface makes the configuration effective on all the WLAN-DBSS interfaces of the WLAN-ESS interface.

A policy must be applied to an interface/PVC following these rules:

- You can apply a QoS policy configured with various QoS actions (such as remark, car, gts, queue af, queue ef, queue wfq, and wred) to common physical interfaces, PVCs, and VT interfaces used by Multilink PPP (MP).
- An inbound QoS policy cannot contain a GTS action or any of these queuing actions: **queue ef**, **queue af**, or **queue wfq**.

On a primary channel interface (for example, VT, dialer, BRI, and PRI interfaces) configured with the **qos max-bandwidth** command, AF and EF queues perform bandwidth check and calculation based on the bandwidth specified in the **qos max-bandwidth** command, so do the AF and EF queues synchronized to the sub-channel interfaces (for example, VA interfaces and B channels). In this case, the sub-channel interface bandwidth is ignored. Because the primary channel interfaces and the sub-channel interfaces are the same in QoS configurations, prompts are displayed for only the primary interface. If the **qos max-bandwidth** command is not configured on a primary channel interface, AF and EF queues on the primary channel interface performs bandwidth check and calculation based on bandwidth of 1 Gbps, and AF and EF queues synchronized to sub-channel interfaces (for example, VA interfaces and B channels) perform bandwidth check and calculation based on the actual bandwidth. If queuing on a sub-channel interface fails due to bandwidth changes, the prompts are output for the sub-channel interface.

You must enable the line rate function for the queuing function to take effect on these interfaces: tunnel interfaces, subinterfaces, HDLC link bundle interfaces, and VT/dialer interfaces configured with PPPoE, PPPoA, PPPoEoA, PPPoFR, or MPoFR (frame relay traffic shaping is not enabled on the frame relay interface). At the same time, you must configure the **qos max-bandwidth** command to provide base bandwidth for CBQ bandwidth calculation.

## Examples

# Apply policy **USER1** in the outbound direction of Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos apply policy USER1 outbound
```

## qos apply policy (user-profile view)

Use **qos apply policy** to apply a QoS policy to a user profile.

Use **undo qos apply policy** to remove the QoS policy.

## Syntax

```
qos apply policy policy-name { inbound | outbound }
undo qos apply policy [ policy-name ] { inbound | outbound }
```

## Views

User profile view

## Default command level

2: System level

## Parameters

**inbound**: Applies the QoS policy to the traffic sent by the online users.

**outbound**: Applies the QoS policy to the traffic received by the online users.

*policy-name*: Policy name, a string of 1 to 31 characters.

## Usage guidelines

You can only edit or remove the configurations in a disabled user profile. Disabling a user profile logs out the users that are using the user profile.



The QoS policy applied to a user profile takes effect when the user-profile is activated and the users are online.

Only the **remark**, **car**, and **filter** actions are supported in the QoS policies applied in user profile view.

A null policy cannot be applied in user profile view.

## Examples

# Apply policy **test** to the traffic received by the users online. (Assume that the QoS policy has been configured.)

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

## qos policy

Use **qos policy** to create a policy and enter policy view.

Use **undo qos policy** to delete a policy.

## Syntax

```
qos policy policy-name
undo qos policy policy-name
```

## Views

System view

## Default command level

2: System level

## Parameters

*policy-name*: Policy name, a string of 1 to 31 characters. The specified *policy-name* cannot be the name of the system-defined policy **default**.

## Usage guidelines

To use the **undo qos policy** command to delete a policy that has been applied to a certain object, you must first remove it from the object.

## Examples

```
# Define QoS policy user1.
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

## Related commands

- **classifier behavior**
- **qos apply policy**

# Policy-based traffic rate statistics collecting interval commands

## qos flow-interval

Use **qos flow-interval** to configure the QoS policy-based traffic rate statistics collecting interval for an interface.

Use **undo qos flow-interval** to restore the default.

### Syntax

**qos flow-interval** *interval*

**undo qos flow-interval**

### Default

QoS policy-based traffic rate statistics collecting interval is 5 minutes on an interface.

### Views

Interface view

### Default command level

2: System level

### Parameters

*interval*: QoS policy-based traffic rate statistics collecting interval (in minutes).

### Usage guidelines

The traffic rate statistics collecting interval of an ATM PVC is the same as that of the ATM interface.

The traffic rate statistics collecting interval of an FR DLCI is the same as that of the FR interface.

The traffic rate statistics collecting interval of a subinterface is the same as that of the main interface.

You can use the **display qos policy interface** command to view the QoS policy-based traffic rate statistics collecting interval setting and the collected statistics.

### Examples

# Set the QoS policy-based traffic rate statistics collecting interval to 10 minutes on Ethernet 1/1.

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

```
[Sysname] interface ethernet 1/1
```

```
[Sysname-Ethernet1/1] qos flow-interval 10
```

# Priority mapping commands

## Priority mapping table commands

### display qos map-table

Use **display qos map-table** to display the configuration of a priority mapping table.

#### Syntax

```
display qos map-table [ dot11e-lp | dot1p-lp | dscp-lp | lp-dot11e | lp-dot1p ] [ [ { begin | exclude | include } regular-expression ]
```

#### Views

Any view

#### Default command level

1: Monitor level

#### Parameters

**dot11e-lp**: 802.11e-to-local mapping table.

The following matrix shows the keyword and hardware compatibility (This matrix also applies to the **lp-dot11e** and **lp-dot1p** keywords):

Hardware	Keyword compatibility
MSR800	Yes
MSR 900	Yes
MSR900-E	Yes
MSR 930	Yes
MSR 20-1X	Supported only on WLAN-capable models and WLAN modules
MSR 20	Supported only on WLAN modules
MSR 30	Supported only on WLAN modules
MSR 50	Supported only on WLAN modules Not supported on routers installed with MPU-G2
MSR 2600	Yes
MSR3600-51F	Supported only on WLAN modules

**dot1p-lp**: 802.1p-to-local mapping table.

**dscp-lp**: DSCP-to-local mapping table.

The following matrix shows the keyword and hardware compatibility:

Hardware	Keyword compatibility
MSR800	Yes
MSR 900	No

Hardware	Keyword compatibility
MSR900-E	Yes
MSR 930	Yes
MSR 20-1X	No
MSR 20	No
MSR 30	Supported only on MSR 30-11E and MSR 30-11F
MSR 50	No
MSR 2600	Yes
MSR3600-51F	Yes

**lp-dot11e:** Local-to-802.11e mapping table.

**lp-dot1p:** Local-to-802.1p mapping table.

**|:** Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin:** Displays the first line that matches the specified regular expression and all lines that follow.

**exclude:** Displays all lines that do not match the specified regular expression.

**include:** Displays all lines that match the specified regular expression.

*regular-expression:* Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

If no priority mapping table is specified, this command displays the configuration information of all priority mapping tables. If no direction is specified, this command displays the priority mapping tables in any direction.

## Examples

# Display the configuration of the 802.1p-to-local mapping table.

```
<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
```

**Table 22 Command output**

Field	Description
MAP-TABLE NAME	Name of the priority mapping table.
TYPE	Type of the priority mapping table.
IMPORT	Input values of the priority mapping table.
EXPORT	Output values of the priority mapping table.

## Related commands

**qos map-table**

# import

Use **import** to configure a mapping from one or multiple input values to an output value.

Use **undo import** to restore the specified or all mappings to the default mappings.

## Syntax

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

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

## Views

Priority mapping table view

## Default command level

2: System level

## Parameters

*import-value-list*: List of input values.

*export-value*: Output value.

**all**: Deletes all the mappings in the priority mapping table.

## Examples

# Configure the 802.1p-to-local mapping table to map 802.1p priority values 4 and 5 to local precedence 1.

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

```
[Sysname] qos map-table dot1p-lp
```

```
[Sysname-maptbl-dot1p-lp] import 4 5 export 1
```

## Related commands

**display qos map-table**

# qos map-table

Use **qos map-table** to enter the specified priority mapping table view.

## Syntax

**qos map-table** { **dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** }

## Views

System view

## Default command level

2: System level

## Parameters

**dot11e-lp**: 802.11e-to-local mapping table.

The following matrix shows the keyword and hardware compatibility (This matrix also applies to the **lp-dot11e** and **lp-dot1p** keywords):

Hardware	Keyword compatibility
MSR800	Yes
MSR 900	Yes
MSR900-E	Yes
MSR 930	Yes
MSR 20-1X	Supported only on WLAN-capable models and WLAN modules
MSR 20	Supported only on WLAN modules
MSR 30	Supported only on WLAN modules
MSR 50	Supported only on WLAN modules Not supported on routers installed with MPU-G2
MSR 2600	Yes
MSR3600-51F	Supported only on WLAN modules

**dot1p-lp**: 802.1p-to-local mapping table.

**dscp-lp**: DSCP-to-local mapping table.

The following matrix shows the keyword and hardware compatibility:

Hardware	Keyword compatibility
MSR800	Yes
MSR 900	No
MSR900-E	Yes
MSR 930	Yes
MSR 20-1X	No
MSR 20	No
MSR 30	Supported only on MSR 30-11E and MSR 30-11F
MSR 50	No
MSR 2600	Yes
MSR3600-51F	Yes

**ip-dot11e**: Local-to-802.11e mapping table.

**ip-dot1p**: Local-to-802.1p mapping table.

## Usage guidelines

The priority mapping table takes effect on both incoming and outgoing packets.

## Examples

```
# Enter the 802.1p-to-local mapping table view.
<Sysname> system-view
[Sysname] qos map-table dot1p-lp
[Sysname-maptbl-dot1p-lp]
```

## Related commands

**display qos map-table**

# Port priority commands

## qos priority

Use **qos priority** to change the port priority of an interface.

Use **undo qos priority** to restore the default.

### Syntax

**qos priority** *priority-value*

**undo qos priority**

### Default

The default port priority of an interface is 0.

### Views

Interface view, port group view

### Default command level

2: System level

### Parameters

*priority-value*: Port priority value. The value range is 0 to 7, and the default is 0.

### Examples

# Set the port priority of interface Ethernet 1/1 to 2.

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

```
[Sysname] interface ethernet 1/1
```

```
[Sysname-Ethernet1/1] qos priority 2
```

# Per-port priority trust mode commands

## display qos trust interface

Use **display qos trust interface** to display priority trust mode and port priority information on an interface.

### Syntax

**display qos trust interface** [ *interface-type interface-number* ] [ | { **begin** | **exclude** | **include** } *regular-expression* ]

### Views

Any view

### Default command level

1: Monitor level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude:** Displays all lines that do not match the specified regular expression.

**include:** Displays all lines that match the specified regular expression.

*regular-expression:* Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

If no interface is specified, the command displays priority trust mode and port priority information for all interfaces.

## Examples

# Display the priority trust mode and port priority settings of Ethernet 1/1.

```
<Sysname> display qos trust interface ethernet 1/1
```

```
Interface: Ethernet1/1
```

```
Port priority trust information
```

```
Port priority:4
```

```
Port priority trust type: dot1p
```

**Table 23 Command output**

Field	Description
Interface	Interface type and interface number.
Port priority	Port priority set for the interface.
Port priority trust type	Priority trust mode on the interface, which can only be <b>dot1p</b> .

## qos trust

Use **qos trust** to configure an interface to use a particular priority field carried in packets for priority mapping.

Use **undo qos trust** to restore the default priority trust mode.

## Syntax

**qos trust { dot1p | dscp }**

**undo qos trust**

## Default

The function is disabled.

## Views

Layer 2 Ethernet interface view, port group view

## Default command level

2: System level

## Parameters

**dot1p:** Uses the 802.1p priority in incoming packets for priority mapping.

**dscp:** Uses the DSCP value in incoming packets for priority mapping.

The following matrix shows the keyword and hardware compatibility:

Hardware	Keyword compatibility
MSR800	Yes
MSR 900	No



Hardware	Keyword compatibility
MSR900-E	Yes
MSR 930	Yes
MSR 20-1X	No
MSR 20	No
MSR 30	Supported only on MSR 30-11E and MSR 30-11F
MSR 50	No
MSR 2600	Yes
MSR3600-51F	Yes

## Examples

# Set the trusted packet priority type to 802.1p priority on Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos trust dot1p
```

# Traffic policing, GTS and line rate commands

## Traffic policing commands

### display qos car interface

Use **display qos car interface** to display the CAR settings and operational statistics on a specified interface.

#### Syntax

**display qos car interface** [ *interface-type interface-number* ] [ | { **begin** | **exclude** | **include** } *regular-expression* ]

#### Views

Any view

#### Default command level

1: Monitor level

#### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

#### Usage guidelines

If no interface is specified, this command displays the CAR settings and operational statistics on all the interfaces.

If a VT interface is specified, this command displays QoS CAR information of all VA interfaces inheriting the VT interface, but does not display QoS information about the VT interface.

#### Examples

# Display the CAR settings and operational statistics on Ethernet 1/1.

```
<Sysname> display qos car interface ethernet1/1
Interface: Ethernet1/1
Direction: Inbound
  Rule(s): If-match Any
    CIR 10 (kbps),  CBS 2000 (byte),  EBS 0 (byte)
    Green Action: pass
    Red Action : discard
    Green : 0(Packets) 0(Bytes)
    Red   : 0(Packets) 0(Bytes)
Direction: Outbound
```

```

Rule(s): If-match ACL 2002
CIR 10 (kbps), CBS 1875 (byte), EBS 0 (byte)
Green Action: pass
Red Action : discard
Green : 0(Packets) 0(Bytes)
Red   : 0(Packets) 0(Bytes)

```

**Table 24 Command output**

Field	Description
Interface	Interface name, including interface type and interface number.
Direction	Direction in which traffic policing is applied.
Rule(s)	Match criteria.
CIR	CIR in kbps.
CBS	CBS in bytes, which specifies the depth of the token bucket for holding bursty traffic.
EBS	EBS in bytes, which specifies the traffic exceeding CBS when two token buckets are used.
Green Action	Action conducted to packets with the traffic rate lower than CIR.
Red Action	Action conducted to packets with the traffic rate exceeding CIR.
Green	Number and bytes of packets with the traffic rate lower than CIR.
Red	Number and bytes of packets with the traffic rate exceeding CIR.

## display qos carl

Use **display qos carl** to display information about a CAR list or all lists.

### Syntax

```
display qos carl [ carl-index ] [ | { begin | exclude | include } regular-expression ]
```

### Views

Any view

### Default command level

1: Monitor level

### Parameters

*carl-index*: CAR list number in the range of 1 to 199.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

### Usage guidelines

If no *carl-index* is specified, this command displays information about all the CAR lists.

## Examples

# Display the rule indexed 1 in the CARL.

```
<Sysname> display qos carl 1
```

Current CARL Configuration:

List Params

-----

1       MAC Address 0001-0001-0001

**Table 25 Command output**

Field	Description
List	CAR list number.
Params	Match object.

## qos car (interface view, port group view)

Use **qos car** to configure a CAR policy on an interface or port group.

Use **undo qos car** to delete a CAR policy on an interface or port group.

### Syntax

```
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 ]
```

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

### Views

Interface view, port group view

### Default command level

2: System Level

### Parameters

**inbound**: Limit the rate of incoming packets on the interface.

**outbound**: Limits the rate of outgoing packets on the interface.

**any**: Limits the rate all the IP data packets in the specified direction.

**acl** *acl-number*: Limits the rate of packets matching the IPv4 ACL.

**acl ipv6** *acl-number*: Limits the rate of packets matching the IPv6 ACL.

**carl** *carl-index*: Limits the rate of packets matching a CAR list. The *carl-index* argument is the index of a CAR list and is in the range of 1 to 199.

**cir** *committed-information-rate*: CIR in kbps.

**cbs** *committed-burst-size*: CBS in bytes, which specifies the size of bursty traffic when the actual average rate is not greater than CIR.

**ebs** *excess-burst-size*: EBS in bytes. The default is 0.

**pir** *peak-information-rate*: PIR in kbps. The default is 0.

**green**: Action conducted to packets when the traffic rate conforms to CIR. The default is **pass**.

**red**: Action conducted to packets when the traffic rate exceeds CIR. The default is **discard**.

*action*: Action conducted to packets:

- **continue**—Continues to process the packet using the next CAR policy.
- **discard**—Drops the packet.
- **pass**—Permits the packet to pass through.
- **remark-dscp-continue** *new-dscp*—Remarks the packet with a new DSCP value and hands it over to the next CAR policy. The value range is 0 to 63. Alternatively, you can specify the *new-dscp* argument with **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.
- **remark-dscp-pass** *new-dscp*—Remarks the packet with a new DSCP value and permits the packet to pass through. The value range is 0 to 63. Alternatively, you can specify the *new-dscp* argument with **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.
- **remark-prec-continue** *new-precedence*—Remarks the packet with a new IP precedence and hands it over to the next CAR policy. The value range is 0 to 7.
- **remark-prec-pass** *new-precedence*—Remarks the packet with a new IP precedence and permits the packet to pass through. The value range is 0 to 7.

## Usage guidelines

You can configure multiple CAR policies on an interface. The policies are applied in the order they are configured.

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

## Examples

# Perform CAR for packets matching CAR list 1 in the outbound direction of Ethernet 1/1. The CAR parameters are as follows: CIR is 200 kbps, CBS is 50000 bytes and EBS is 0. Conforming packets are transmitted, and excess packets are set with an IP precedence of 0 and transmitted.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos car outbound carl 1 cir 200 cbs 50000 ebs 0 green pass red
remark-prec-pass 0
```

## qos carl

Use **qos carl** to create or modify a CAR list.

Use **undo qos carl** to delete a CAR list.

## Syntax

```
qos carl carl-index { precedence precedence-value | mac mac-address | dscp dscp-list |
{ destination-ip-address | source-ip-address } { subnet ip-address mask-length | range
start-ip-address to end-ip-address } [ per-address [ shared-bandwidth ] ] }
```

```
undo qos carl carl-index
```

## Views

System view

## Default command level

2: System level

## Parameters

*carl-index*: CAR list number in the range of 1 to 199.

**precedence** *precedence*: Specifies a precedence value in the range of 0 to 7.

**mac** *mac-address*: Specifies a MAC address in hexadecimal format.

**dscp** *dscp-list*: Specifies a list of DSCP values. A DSCP value is in the range of 0 to 63 or any of the following keywords **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.

**destination-ip-address**: Configures a destination IP address-based CAR list.

**source-ip-address**: Configures a source IP address-based CAR list.

**subnet** *ip-address mask-length*: Specifies a subnet by the IP subnet address and IP subnet address mask length.

**range** *start-ip-address to end-ip-address*: Specifies an IP address range by the start address and end address. *end-ip-address* must be greater than *start-ip-address*.

**per-address**: Performs per-IP address rate limiting within the network segment. If this keyword is not specified, rate limiting is performed for the entire network segment.

**shared-bandwidth**: Specifies that traffic of all IP addresses within the network segment shares the remaining bandwidth.

## Usage guidelines

You can create a CAR list based on IP precedence, MAC address, DSCP, or IP network segment.

You can create multiple CAR lists with different CAR list indexes or modify the parameters for one CAR list.

You can configure up to eight precedence values for a CAR list. If the same precedence value is specified multiple times, the system considers them as one value by default. If a packet matches a precedence value on the CAR list, it matches the CAR list.

You can configure up to eight DSCP values for a CAR list. If a DSCP value is specified multiple times, the system counts them as one value by default. If a packet matches a DSCP value on the CAR list, it matches the CAR list.

To perform rate limiting for a single IP address, use the **qos car acl** command in interface view.

When you apply an IP network segment-based CAR list to an interface with the **qos car** command, the CIR you defined takes different meanings depending on the configuration of the **per-address** keyword and the **shared-bandwidth** keyword for the CAR list.

- If the **per-address** keyword is not specified, the CIR specifies the total bandwidth for the network segment and will be allocated to each IP address based on its traffic size.
- If the **per-address** keyword is specified but the **shared-bandwidth** keyword is not specified, the CIR specifies the bandwidth of each IP address, and the bandwidth cannot be shared by the other IP addresses within the network segment.
- If both the **per-address** keyword and the **shared-bandwidth** keyword are specified, the CIR specifies the total shared bandwidth for the network segment, and will be dynamically and evenly allocated to the traffic by IP address.

For example, apply a CAR list to an interface with 10 Mbps of total bandwidth to perform per-address rate limiting for the network segment 192.168.0.1 to 192.168.0.100. If the **shared-bandwidth** keyword is specified for the CAR list, you can set the CIR to 10 Mbps at maximum. If the **shared-bandwidth** keyword is specified for the CAR list, you can set the CIR to 100 kbps at maximum.

## Examples

# Configure precedence 7 for CAR list 1.

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

```
[Sysname] qos car 1 precedence 7
```

# Apply CAR list 1 to the outbound direction of Ethernet 1/1. CAR list 1 limits the rate of each PC on the subnet 1.1.1.0/24 to 100 kbps, and traffic of IP addresses in the subnet does not share the remaining bandwidth.

```

<Sysname> system-view
[Sysname] qos carl 1 source-ip-address subnet 1.1.1.0 24 per-address
[Sysname] interface ethernet1/1
[Sysname-Ethernet1/1] qos car outbound carl 1 cir 100 cbs 6250 ebs 0 green pass red discard

# Apply CAR list 1 to the outbound direction of Ethernet 2/1. CAR list 2 limits the rate of each PC on
the network segment 1.1.2.100 through 1.1.2.199 to 5 Mbps, and traffic of IP addresses in the subnet
share the remaining bandwidth.

<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 ethernet1/1
[Sysname-Ethernet1/1] qos car outbound carl 2 cir 5000 cbs 3125 ebs 31250 green pass red
discard

```

# GTS commands

## display qos gts interface

Use **display qos gts interface** to view generic traffic shaping (GTS) configuration information and operational statistics on a specified interface or all the interfaces.

### Syntax

**display qos gts interface** [ *interface-type interface-number* ] [ | { **begin** | **exclude** | **include** } *regular-expression* ]

### Views

Any view

### Default command level

1: Monitor level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

### Usage guidelines

If no interface is specified, this command displays the GTS configuration information and operational statistics on all the interfaces.

If a VT interface is specified, this command displays QoS GTS information of all VA interfaces inheriting the VT interface, but does not display QoS information about the VT interface.

### Examples

# Display the GTS configuration information and operational statistics on all the interfaces.

```

<Sysname> display qos gts interface
Interface: Ethernet1/1

```

```

Rule(s): If-match ACL 2001
CIR 200 (kbps), CBS 50000 (byte), EBS 0 (byte)
Queue Length: 100 (Packets)
Queue Size: 70 (Packets)
Passed : 0(Packets) 0(Bytes)
Discarded: 0(Packets) 0(Bytes)
Delayed : 0(Packets) 0(Bytes)

```

**Table 26 Command output**

Field	Description
Interface	Interface type and interface number.
Rule(s)	Match criteria.
CIR	CIR in kbps.
CBS	Committed burst size in bytes, which specifies the depth of the token bucket for holding bursty traffic.
EBS	Excess burst size in bytes, which specifies the traffic exceeding CBS when two token buckets are used.
Queue Length	Number of packets that the buffer can hold.
Queue Size	Number of packets in the buffer.
Passed	Number and bytes of the packets that have passed.
Discarded	Number and bytes of dropped packets.
Delayed	Number and bytes of delayed packets.

## qos gts

Use **qos gts** to set GTS parameters for a specific class of traffic or all the traffic on the interface or port group.

Use **qos gts acl** to set GTS parameters for the traffic matching the specific ACL. You can set GTS parameters for different traffic flows by using different ACLs.

Use **qos gts any** to set GTS parameters for all the traffic on the interface or port group.

Use **undo qos gts** to remove GTS parameters for a specific class of traffic or all the traffic on the interface or port group.

### Syntax

```
qos gts { any | acl acl-number } cir committed-information-rate [ cbs committed-burst-size [ ebs excess-burst-size ] [ queue-length queue-length ] ]
```

```
undo qos gts { any | acl acl-number }
```

### Default

No GTS parameters are configured on an interface.

### Views

Interface view, port group view

### Default command level

2: System level



## Parameters

**any**: Shapes all packets.

**acl** *acl-number*: Shapes packets that match the specified ACL.

**cir** *committed-information-rate*: CIR in kbps.

**cbs** *committed-burst-size*: CBS in bytes.

**ebs** *excess-burst-size*: Excessive burst size (EBS) in bytes, which specifies the traffic exceeding CBS when two token buckets are used. By default, the EBS is 0 and only one token bucket is used.

**queue-length** *queue-length*: Maximum queue length in the buffer. The maximum buffer queue length is 50 by default.

## Usage guidelines

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

When you configure GTS parameters on an interface or port group, ACLs for IPv6 are not supported. To use ACLs for IPv6 for GTS, configure GTS by using the MQC approach.

## Examples

# Shape the packets matching ACL 2001 on Ethernet 1/1. The GTS parameters are as follows: CIR is 200 kbps, CBS is 50000 bytes, EBS is 0, and the maximum buffer queue length is 100.

```
<Sysname> system-view
[Sysname] interface ethernet1/1
[Sysname-Ethernet1/1] qos gts acl 2001 cir 200 cbs 50000 ebs 0 queue-length 100
```

## Related commands

**acl**

# Line rate commands

## display qos lr interface

Use **display qos lr interface** to view the line rate configuration information and operational statistics on a specified interface or all the interfaces.

## Syntax

**display qos lr interface** [ *interface-type interface-number* ] [ | { **begin** | **exclude** | **include** } *regular-expression* ]

## Views

Any view

## Default command level

1: Monitor level

## Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

If no interface is specified, this command displays the line rate configuration information and operational statistics on all the interfaces.

If a VT interface is specified, this command displays QoS line rate information of all VA interfaces inheriting the VT interface, but does not display QoS information about the VT interface.

## Examples

# Display the line rate configuration information and operational statistics on all the interfaces.

```
<Sysname> display qos lr interface
Interface: Ethernet1/1
Direction: Outbound
    CIR 10 (kbps),  CBS 1875 (byte),  EBS 0 (byte)
Passed : 0(Packets) 0(Bytes)
Delayed: 0(Packets) 0(Bytes)
Active Shaping: NO
Direction: Inbound
    CIR 10 (kbps),  CBS 1875 (byte),  EBS 0 (byte)
Passed : 0(Packets) 0(Bytes)
Delayed: 0(Packets) 0(Bytes)
Active Shaping: NO
```

**Table 27 Command output**

Field	Description
Interface	Interface type and interface number.
Direction	Direction in which the line rate configuration is applied: inbound or outbound.
CIR	CIR in kbps.
CBS	CBS in bytes, which specifies the depth of the token bucket for holding bursty traffic.
EBS	Excessive burst size (EBS) in bytes, which specifies the traffic exceeding CBS when two token buckets are used.
Passed	Number and bytes of packets that have passed.
Delayed	Number and bytes of delayed packets.
Active Shaping	Whether the line rate configuration is activated.

## qos lr

Use **qos lr** to limit the rate of incoming packets or outgoing packets on the interface.

Use **undo qos lr** to remove the rate limit.

## Syntax

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

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

## Views

Interface view, port group view

## Default command level

2: System level

## Parameters

**inbound:** Limits the rate of incoming packets on the interface.

The following matrix shows the keyword and hardware compatibility:

Hardware	Keyword compatibility
MSR800	No
MSR 900	No
MSR900-E	No
MSR 930	No
MSR 20-1X	No
MSR 20	No
MSR 30	Supported only on the following interfaces and modules: <ul style="list-style-type: none"><li>Fixed Layer 2 Ethernet interfaces on MSR 30-11E and MSR 30-11F</li><li>MIM-16FSW and DMIM-24FSW Layer 2 Ethernet switching modules</li></ul>
MSR 50	Supported only on FIC-16FSW and DFIC-24FSW Layer 2 Ethernet switching modules
MSR 2600	No
MSR3600-51F	Supported only on fixed Layer 2 Ethernet interfaces

**outbound:** Limits the rate of outgoing packets on the interface.

**cir** *committed-information-rate*: Committed information rate (CIR) in kbps.

**cbs** *committed-burst-size*: Committed burst size (CBS) in bytes. The default CBS value is the traffic transmitted at the rate of CIR in 500 ms.

**ebs** *excess-burst-size*: Excessive burst size (EBS) in bytes, which specifies the traffic exceeding CBS when two token buckets are used. By default, the EBS is 0 and only one token bucket is used.

## Usage guidelines

Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

## Examples

# Limit the rate of outgoing packets on Ethernet 1/1, with CIR 20 kbps, CBS 2000 bytes, and EBS 0.

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

```
[Sysname] interface ethernet 1/1
```

```
[Sysname-Ethernet1/1] qos lr outbound cir 20 cbs 2000 ebs 0
```

# Congestion management commands

## FIFO queuing commands

### qos fifo queue-length

Use **qos fifo queue-length** to set the FIFO queue length.

Use **undo qos fifo queue-length** to restore the default.

#### Syntax

**qos fifo queue-length** *queue-length*

**undo qos fifo queue-length**

#### Views

Interface view, PVC view

#### Default command level

2: System level

#### Parameters

*queue-length*: Queue length threshold. The value range for this argument varies by device model.

#### Usage guidelines

You must enable the line rate function for the queuing function to take effect on these interfaces: tunnel interfaces, subinterfaces, HDLC link bundle interfaces, and VT/dialer interfaces configured with PPPoE, PPPoA, PPPoEoA, PPPoFR, or MPoFR (frame relay traffic shaping is not enabled on the frame relay interface).

#### Examples

```
# Set the FIFO queue length to 100.
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos fifo queue-length 100
```

## PQ commands

### display qos pq interface

Use **display qos pq interface** to display the Priority Queuing (PQ) configuration and statistics of an interface/PVC or all the interfaces/PVCs.

#### Syntax

**display qos pq interface** [ *interface-type interface-number* [ **pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* } ] ] [ **{ begin | exclude | include }** *regular-expression* ]

#### Views

Any view

#### Default command level

1: Monitor level

## Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

**pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* }: Specifies a PVC on an ATM interface. *pvc-name* specifies the PVC by its name. *vpi/vci* specifies the PVC by its VPI/VCI pair. This option is only available for ATM interfaces.

**|**: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

If no interface/PVC is specified, this command displays the PQ configuration and statistics of all interfaces/PVCs.

If a VT interface is specified, this command displays QoS PQ information of all VA interfaces inheriting the VT interface, but does not display QoS information about the VT interface.

## Examples

# Display the PQ configuration and statistics of Ethernet 1/1.

```
<Sysname> display qos pq interface ethernet 1/1
```

```
Interface: Ethernet1/1
```

```
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
```

**Table 28 Command output**

Field	Description
Interface	Interface type and interface number.
Output queue	Output queue information.
Priority queuing	Priority queuing. The PQ list in use is displayed.
Size	Number of packets in a queue.
Length	Queue length, which specifies the maximum number of packets a queue can hold.
Discards	Number of dropped packets.
Top	Top priority queue.
Middle	Middle priority queue.
Normal	Normal priority queue.
Bottom	Bottom priority queue.

## Related commands

**qos pq**

# display qos pql

Use **display qos pql** to display the configuration information of a PQ list or all the PQ lists.

## Syntax

**display qos pql** [ *pql-number* ] [ [ { **begin** | **exclude** | **include** } *regular-expression* ]

## Views

Any view

## Default command level

1: Monitor level

## Parameters

*pql-number*: Priority queue list number.

**|**: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

Default items are not displayed.

## Examples

# Display PQ lists.

```
<Sysname> display qos pql
```

Current PQL Configuration:

List	Queue	Params
------	-------	--------

-----		
1	Top	Protocol ip less-than 1000
2	Normal	Length 60
2	Bottom	Length 40
3	Middle	Inbound-interface Ethernet1/1
4	Top	Local-precedence 7

## Related commands

- **qos pq pql**
- **qos pq**

# qos pq

Use **qos pq** to apply a PQ list to an interface.

Use **undo qos pq** to restore the default.

## Syntax

**qos pq pql** *pql-index*

**undo qos pq**

## Default

The congestion management policy of an interface is FIFO.

## Views

Interface view, PVC view

## Default command level

2: System level

## Parameters

**pql**: Specifies a PQ list.

*pql-index*: PQ list index in the range of 1 to 16.

## Usage guidelines

All physical interfaces, except interfaces with X.25 or LAPB encapsulation enabled, can use PQ.

An interface can use only one PQ list.

Multiple match criteria can be configured for a PQ list. During traffic classification, the system matches packets with the rules in the PQ list. If a packet matches a certain rule, it is assigned to the priority queue, and the matching process is over. If a packet does not match any rule, it is allocated to the default priority queue.

You must enable the line rate function for the queuing function to take effect on these interfaces: tunnel interfaces, subinterfaces, HDLC link bundle interfaces, and VT/dialer interfaces configured with PPPoE, PPPoA, PPPoEoA, PPPoFR, or MPoFR (frame relay traffic shaping is not enabled on the frame relay interface).

## Examples

# Apply PQ list 12 to Ethernet 1/1.

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

```
[Sysname] interface ethernet 1/1
```

```
[Sysname-Ethernet1/1] qos pq pql 12
```

## Related commands

- **qos pql**
- **display qos pq interface**
- **display qos pql**
- **display interface**

## qos pql default-queue

Use **qos pql default-queue** to specify the default queue for packets matching no match criterion.

Use **undo qos pql default-queue** to restore the default.

## Syntax

**qos pql *pql-index* default-queue { bottom | middle | normal | top }**

**undo qos pql *pql-index* default-queue**

## Views

System view

## Default command level

2: System level

## Parameters

*pql-index*: PQ list index in the range of 1 to 16.

**top**, **middle**, **normal**, **bottom**: Corresponds to the four queues in PQ in descending priority order. The default queue is the **normal** queue.

## Usage guidelines

If this command is executed multiple times with the same *pql-index* argument, the new configuration overrides the previous one.

## Examples

# Assign packets matching no traffic match criterion in PQL 12 to the bottom queue.

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

```
[Sysname] qos pql 12 default-queue bottom
```

## Related commands

- **qos pql inbound-interface**
- **qos pql protocol**
- **qos pql queue**
- **qos pq**

# qos pql inbound-interface

Use **qos pql inbound-interface** to configure a match criterion for a PQ list to assign packets received from a specified interface to a specified queue.

Use **undo qos pql inbound-interface** to delete the match criterion.

## Syntax

**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*

## Default

No match criterion is configured.

## Views

System view

## Default command level

2: System level

## Parameters

*pql-index*: PQ list index in the range of 1 to 16.

*interface-type interface-number*: Specifies an interface by its type and number.

**top**, **middle**, **normal**, **bottom**: Corresponds to the four queues in PQ in descending priority order.

## Usage guidelines

You can execute this command multiple times with the same *pql-index* argument to create different match criteria for packets received from different interfaces.

## Examples

# Create a match criterion in PQ list 12 to assign packets received from Serial 2/0 to the middle queue.



```
<Sysname> system-view
[Sysname] qos pql 12 inbound-interface serial 2/0 queue middle
```

## Related commands

- **qos pql default-queue**
- **qos pql protocol**
- **qos pql queue**
- **qos pq**

## qos pql protocol

Use **qos pql protocol** to specify a queue for the IP packets that match a certain match criterion.

Use **undo qos pql protocol** to delete the match criterion.

## Syntax

```
qos pql pql-index protocol ip [ queue-key key-value ] queue { bottom | middle | normal | top }
undo qos pql pql-index protocol ip [ queue-key key-value ]
```

## Default

No match criterion is configured.

## Views

System view

## Default command level

2: System level

## Parameters

*pql-index*: PQ list index in the range of 1 to 16.

**top, middle, normal, bottom**: Corresponds to the four queues in PQ in descending priority order.

**ip** [ *queue-key key-value* ]: Classifies and enqueues IP packets. If neither the *queue-key* argument nor the *key-value* argument is specified, all IP packets are enqueued.

**Table 29 Values of the *queue-key* argument and the *key-value* argument**

queue-key	key-value	Description
acl	ACL number from 2000 to 3999	IP packets matching the specified ACL are enqueued.
fragments	—	Fragmented IP packets are enqueued.
greater-than	Length from 0 to 65535	IP packets larger than a specified value are enqueued.
less-than	Length (0 to 65535)	IP packets smaller than a specified value are enqueued.
tcp	Port number (0 to 65535)	IP packets with a specified source or destination TCP port number are enqueued.
udp	Port number (0 to 65535)	IP packets with a specified source or destination UDP port number are enqueued.

When the *queue-key* is **tcp** or **udp**, the *key-value* can be either a port name or port number.

## Usage guidelines

The system matches a packet with match criteria in the order configured. When the packet matches a certain criterion, the matching process is over.

You can execute this command multiple times with the same *pql-index* argument to create multiple match criteria for IP packets.

## Examples

# Create a rule in PQL 1 to assign IP packets matching ACL 3100 to the top queue.

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

```
[Sysname] qos pql 1 protocol ip acl 3100 queue top
```

## Related commands

- **qos pql default-queue**
- **qos pql inbound-interface**
- **qos pql queue**
- **qos pq**

## qos pql queue

Use **qos pql queue** to specify the length of a specified priority queue (the maximum number of packets that the priority queue can hold).

Use **undo qos pql queue** to restore the default for a priority queue.

## Syntax

**qos pql *pql-index* queue { bottom | middle | normal | top } queue-length *queue-length***

**undo qos pql *pql-index* queue { bottom | middle | normal | top } queue-length**

## Default

The queue length values for the four priority queues are as follows:

## Views

System view

## Default command level

2: System level

## Parameters

*pql-index*: PQL index in the range of 1 to 16.

*queue-length*: Queue length for the specified queue, in the range of 1 to 1024.

- 20 for the top queue
- 40 for the middle queue
- 60 for the normal queue
- 80 for the bottom queue

## Usage guidelines

If a queue is full, all subsequent packets to this queue are dropped.

## Examples

# Set the length of the top queue in PQL 10 to 10.

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

```
[Sysname] qos pql 10 queue top queue-length 10
```

## Related commands

- **qos pql default-queue**

- **qos pql inbound-interface**
- **qos pql protocol**
- **qos pq**

## CQ commands

### display qos cq interface

Use **display qos cq interface** to view the custom queuing (CQ) configuration and statistics of an interface/PVC or all the interfaces/PVCs.

#### Syntax

**display qos cq interface** [ *interface-type interface-number* [ **pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* } ] ] [ { **begin** | **exclude** | **include** } *regular-expression* ]

#### Views

Any view

#### Default command level

1: Monitor level

#### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

**pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* }: Specifies a PVC on an ATM interface. *pvc-name* specifies the PVC by its name. *vpi/vci* specifies the PVC by its VPI/VCI pair. This option is only available for ATM interfaces.

[ ]: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

#### Usage guidelines

If no interface/PVC is specified, this command displays the CQ configuration and statistics of all the interfaces/PVCs.

If a VT interface is specified, this command displays QoS CQ information of all VA interfaces inheriting the VT interface, but does not display QoS information about the VT interface.

#### Examples

# Display the CQ configuration and statistics of Ethernet 1/1.

```
<Sysname> display qos cq interface ethernet 1/1
Interface: Ethernet1/1
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

**Table 30 Command output**

Field	Description
Interface	Interface type and interface number.
Output queue	Output queue information.
Custom queuing	Custom queuing. The CQ list in use is displayed.
Size	Number of packets in a queue.
Length	Queue length, which specifies the maximum number of packets a queue can hold.
Discards	Number of dropped packets.

## Related commands

**qos cq**

## display qos cql

Use **display qos cql** to display the configuration of the specified or all custom queue lists.

## Syntax

**display qos cql** [ *cql-index* ] [ | { **begin** | **exclude** | **include** } *regular-expression* ]

## Views

Any view

## Default command level

1: Monitor level

## Parameters

*cql-index*: CQ list index in the range of 1 to 16.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

This command displays no default items. If no CQ list index is specified, this command displays the configuration of all CQ lists.

## Examples

# Display information about all CQ lists.

```
<Sysname> display qos cql
```

Current CQL Configuration:

List Queue Params

```
-----  
2      3      Protocol ip fragments  
3      6      Length 100
```

```

3      1      Inbound-interface Ethernet1/1
4      5      Local-precedence 7

```

## Related commands

- **qos cq**
- **qos cql**

## qos cq

Use **qos cq** to apply a CQ list to an interface.

Use **undo qos cq** to restore the default.

## Syntax

```

qos cq cql cql-index
undo qos cq

```

## Default

The congestion management policy on an interface is FIFO.

## Views

Interface view, PVC view

## Default command level

2: System level

## Parameters

*cql-index*: CQ list index in the range of 1 to 16.

## Usage guidelines

Except interfaces with X.25 or LAPB encapsulation enabled, all physical interfaces can use CQ.

An interface can use only one CQ list.

You can configure multiple match criteria for a CQ list. During traffic classification, the system matches packets with the rules in the CQ list. If a packet matches a certain rule, the packet is assigned to the queue, and the matching process is over. If the packet matches no rule in the CQ list, it is allocated to the default queue.

You must enable the line rate function for the queuing function to take effect on these interfaces: tunnel interfaces, subinterfaces, HDLC link bundle interfaces, and VT/dialer interfaces configured with PPPoE, PPPoA, PPPoEoA, PPPoFR, or MPoFR (frame relay traffic shaping is not enabled on the frame relay interface).

## Examples

```

# Apply CQ list 5 to Ethernet 1/1.
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos cq cql 5

```

## Related commands

- **qos cql default-queue**
- **qos cql inbound-interface**
- **qos cql protocol**
- **qos cql queue serving**
- **qos cql queue**

## qos cql default-queue

Use **qos cql default-queue** to specify the default queue for packets matching no match criterion in the CQ list.

Use **undo qos cql default-queue** to restore the default.

### Syntax

```
qos cql cql-index default-queue queue-number  
undo qos cql cql-index default-queue
```

### Default

The queue number is 1.

### Views

System view

### Default command level

2: System level

### Parameters

*cql-index*: CQ list index in the range of 1 to 16.

*queue-number*: Queue number in the range of 1 to 16.

### Usage guidelines

Packets that match no match criterion are allocated to the default queue.

### Examples

```
# Specify queue 2 as the default queue for CQ list 5.  
<Sysname> system-view  
[Sysname] qos cql 5 default-queue 2
```

### Related commands

- **qos cql inbound-interface**
- **qos cql protocol**
- **qos cql queue serving**
- **qos cql queue**
- **qos cq**

## qos cql inbound-interface

Use **qos cql inbound-interface** to configure a match criterion in a CQ list to allocate packets received on a specified interface to a specified queue.

Use **undo qos cql inbound-interface** to delete the match criterion.

### Syntax

```
qos cql cql-index inbound-interface interface-type interface-number queue queue-number  
undo qos cql cql-index inbound-interface interface-type interface-number
```

### Default

No match criterion is configured.

## Views

System view

## Default command level

2: System level

## Parameters

*cql-index*: CQ list index in the range of 1 to 16.

*interface-type interface-number*: Specifies an interface by its type and number.

*queue-number*: Queue number in the range of 1 to 16.

## Usage guidelines

You can execute this command multiple times with the same *cql-index* argument to create different match criteria for packets received from different interfaces.

## Examples

# Configure a match criterion in CQ list 5 to assign packets received from Ethernet 1/1 to queue 3.

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

```
[Sysname] qos cql 5 inbound-interface ethernet 1/1 queue 3
```

## Related commands

- **qos cql default-queue**
- **qos cql protocol**
- **qos cql queue serving**
- **qos cql queue**

# qos cql protocol

Use **qos cql protocol** to assign a custom queue for IP packets that match a certain criterion.

Use **undo qos cql protocol** to delete the match criterion.

## Syntax

**qos cql** *cql-index* **protocol ip** [ *queue-key key-value* ] **queue** *queue-number*

**undo qos cql** *cql-index* **protocol ip** [ *queue-key key-value* ]

## Default

No match criterion is configured.

## Views

System view

## Default command level

2: System level

## Parameters

*cql-index*: CQ list index in the range of 1 to 16.

**queue** *queue-number*: Specifies an custom queue by its number in the range of 1 to 16.

**ip** [ *queue-key key-value* ]: Classifies and enqueues IP packets. The values for the *queue-key* argument and the *key-value* argument are displayed in [Table 31](#). If neither the *queue-key* argument nor the *key-value* argument is specified, all IP packets are enqueued.

**Table 31 Values for the *queue-key* argument and the *key-value* argument**

queue-key	key-value	Description
acl	ACL number (2000 to 3999)	All IP packets matching the specified ACL are enqueued.
fragments	N/A	All fragmented IP packets are enqueued.
greater-than	Length (0 to 65535)	IP packets larger than a specified value are enqueued.
less-than	Length (0 to 65535)	IP packets smaller than a specified value are enqueued.
tcp	Port number (0 to 65535)	IP packets with a specified TCP source or destination port number are enqueued.
udp	Port number (0 to 65535)	IP packets with a specified UDP source or destination port number are enqueued.

When the *queue-key* argument is **tcp** or **udp**, the *key-value* argument can take either a port name or a port number.

### Usage guidelines

The system matches a packet with match criteria of a CQ list in the order configured. When the packet matches a certain criterion, it is allocated to the queue and the matching process is over.

You can execute this command multiple times with the same *cql-index* argument to create multiple match criteria for IP packets.

### Examples

# Configure a rule in CQ list 5 to assign packets matching ACL 3100 to queue 3.

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

```
[Sysname] qos cql 5 protocol ip acl 3100 queue 3
```

### Related commands

- **qos cql default-queue**
- **qos cql inbound-interface**
- **qos cql queue**
- **qos cql cql**

## qos cql queue

Use **qos cql queue** to specify the length of a custom queue, the maximum number of packets a custom queue can hold.

Use **undo qos cql queue** to restore the default.

### Syntax

```
qos cql cql-index queue queue-number queue-length queue-length
```

```
undo qos cql cql-index queue queue-number queue-length
```

### Views

System view

### Default command level

2: System level

### Parameters

*cql-index*: CQ list index in the range of 1 to 16.



*queue-number*: Queue number in the range of 1 to 16.

**queue-length** *queue-length*: Specifies the maximum queue length in the range of 1 to 1024. This argument is 20 by default.

## Usage guidelines

If the queue is full, subsequent packets are dropped.

## Examples

```
# Set the length of queue 4 in CQ list 5 to 40.
```

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

```
[Sysname] qos cql 5 queue 4 queue-length 40
```

## Related commands

- **qos cql default-queue**
- **qos cql inbound-interface**
- **qos cql protocol**
- **qos cql queue serving**
- **qos cql**

# qos cql queue serving

Use **qos cql queue serving** to set the byte count for a custom queue on a CQ list.

Use **undo qos cql queue serving** to restore the default.

## Syntax

**qos cql** *cql-index* **queue** *queue-number* **serving** *byte-count*

**undo qos cql** *cql-index* **queue** *queue-number* **serving**

## Views

System view

## Default command level

2: System level

## Parameters

*cql-index*: CQ list index in the range of 1 to 16.

*queue-number*: Queue number in the range of 1 to 16.

*byte-count*: Number of bytes of packets that the specified queue sends in each cycle of queue scheduling. The value range is 1 to 16777215, and the default is 1500.

## Examples

```
# Set the byte count of packets to 1400 for queue 2 on CQ list 5.
```

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

```
[Sysname] qos cql 5 queue 2 serving 1400
```

## Related commands

- **qos cql default-queue**
- **qos cql inbound-interface**
- **qos cql protocol**
- **qos cql queue**

- qos cq

# WFQ commands

## display qos wfq interface

Use **display qos wfq interface** to display weighted fair queuing (WFQ) configuration and statistics of an interface/PVC or all interfaces/PVCs.

### Syntax

**display qos wfq interface** [ *interface-type interface-number* [ **pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* } ] ]  
[ | { **begin** | **exclude** | **include** } *regular-expression* ]

### Views

Any view

### Default command level

1: Monitor level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

**pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* }: Specifies a PVC on an ATM interface. *pvc-name* specifies the PVC by its name. The *vpi/vci* argument specifies the PVC by its VPI/VCI pair. This option is only available for ATM interfaces.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

### Usage guidelines

If no interface is specified, this command displays the WFQ configuration and statistics of all the interfaces.

If a VT interface is specified, this command displays QoS WFQ information of all VA interfaces inheriting the VT interface, but does not display QoS information about the VT interface.

### Examples

# Display the WFQ configuration and statistics of Ethernet 1/1.

```
<Sysname> display qos wfq interface ethernet 1/1
Interface: Ethernet1/1
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
Hashed by IP Precedence
Hashed queues: 0/0/128 (Active/Max active/Total)
```

**Table 32 Command output**

Field	Description
Interface	Interface type and interface number.

Field	Description
Output queue	Information about the current output queue.
Size	Number of packets in the queue.
Length	Queue length.
Discards	Number of dropped packets.
Hashed by	Weight type: IP precedence or DSCP.
Hashed queues	Information about hashed queues.
Active	Number of active hashed queues.
Max active	Maximum number of active hashed queues.
Total	Total number of hashed queues.

## Related commands

**qos wfq**

## qos wfq

Use **qos wfq** to apply WFQ to an interface or modify WFQ parameters on an interface/PVC.

Use **undo qos wfq** to restore the default congestion management mechanism FIFO on the interface/PVC.

## Syntax

**qos wfq** [ **dscp** | **precedence** ] [ **queue-length** *max-queue-length* [ **queue-number** *total-queue-number* ] ]

**undo qos wfq**

## Default

The weight is based on IP precedence.

## Views

Interface view, PVC view

## Default command level

2: System level

## Parameters

**dscp**: DSCP weight.

**precedence**: IP precedence weight.

**queue-length** *max-queue-length*: Specifies the maximum number of packets a queue can hold. The value range for *max-queue-length* is 1 to 1024, and the default is 64.

**queue-number** *total-queue-number*: Specifies the total number of queues, which can be 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096. The default is 256.

## Usage guidelines

All physical interfaces except interfaces with X.25 or LAPB encapsulation enabled can use WFQ.

You must enable the line rate function for the queuing function to take effect on these interfaces: tunnel interfaces, subinterfaces, HDLC link bundle interfaces, and VT/dialer interfaces configured with PPPoE, PPPoA, PPPoEoA, PPPoFR, or MPoFR (frame relay traffic shaping is not enabled on the frame relay interface).

## Examples

# Apply WFQ to Ethernet 1/1, set the maximum queue length to 100, and the total number of queues to 512.

```
<Sysname> system-view
[Sysname] interface ethernet1/1
[Sysname-Ethernet1/1] qos wfq queue-length 100 queue-number 512
```

## Related commands

- **display interface**
- **display qos wfq interface**

# CBQ commands

## display qos cbq interface

Use **display qos cbq interface** to display the class-based queue (CBQ) configuration and operational information of an interface/PVC or all interfaces/PVCs.

## Syntax

**display qos cbq interface** [ *interface-type interface-number* [ **pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* } ] ]  
[ [ { **begin** | **exclude** | **include** } *regular-expression* ]

## Views

Any view

## Default command level

1: Monitor level

## Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

**pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* }: Specifies a PVC on an ATM interface. *pvc-name* specifies the PVC by its name. *vpi/vci* specifies the PVC by its VPI/VCI pair. This option is only available for ATM interfaces.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

If no interface is specified, this command displays the CBQ configuration and operational information of all interfaces.

If a VT interface is specified, this command displays QoS CBQ information of all VA interfaces inheriting the VT interface, but does not display QoS information about the VT interface.

## Examples

# Display the CBQ configuration and operational information of all interfaces.

```
<Sysname> display qos cbq interface
Interface: Ethernet1/1
```

```

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:  0/0/0 (EF/AF/BE)
BE Queues:   0/0/256 (Active/Max active/Total)
AF Queues:   1 (Allocated)
Bandwidth(Kbps): 74992/75000 (Available/Max reserve)

```

**Table 33 Command output**

Field	Description
Interface	Interface type and interface number.
Output queue	Information about the current output queue.
Size	Number of packets in the queue.
Length	Queue length.
Discards	Number of dropped packets.
EF	EF queue.
AF	AF queue.
BE	BE queue.
Active	Number of active BE queues.
Max active	Maximum number of active BE queues allowed.
Total	Total number of BE queues.
Available	Available bandwidth for CBQ.
Max reserve	Maximum reserved bandwidth for CBQ.

## qos max-bandwidth

Use **qos max-bandwidth** to configure the maximum available bandwidth of the interface.

Use **undo qos max-bandwidth** to restore the default.

### Syntax

**qos max-bandwidth** *bandwidth*

**undo qos max-bandwidth**

### Views

Interface view

### Default command level

2: System level

### Parameters

*bandwidth*: Maximum available bandwidth of the interface, in the range of 1 to 1000000 kbps.

### Usage guidelines

H3C recommends that you configure the maximum available bandwidth to be smaller than the actual available bandwidth of a physical interface or logical link.

If the maximum available bandwidth is not configured, the base QoS bandwidth used for CBQ calculation is as follows:

- Actual baudrate or rate of a physical interface.
- 1000000 kbps for VLAN interfaces.
- Total bandwidth of a logical serial interface formed by binding, such as T1/E1 interfaces, MFR interfaces, and MP interfaces.
- 1000000 kbps for template interfaces such as VT, dialer, BRI, and PRI interfaces.
- 384 kbps for cellular interfaces.
- 0 kbps for the other virtual interfaces such as tunnel interfaces and HDLC link bundle interfaces.

On a primary channel interface (such as VT, dialer, BRI, or PRI) configured with the **qos max-bandwidth** command, AF and EF perform queue bandwidth check and calculation based on the bandwidth specified with the **qos max-bandwidth** command. The same is true of AF and EF synchronized to the sub-channel interfaces (such as VA interfaces or B channels). In this case, the sub-channel interface bandwidth is ignored. Because the QoS configurations of the primary channel interface and the sub-channel interfaces are the same in this case, prompts are output only for the primary channel interface. If the **qos max-bandwidth** command is not configured, AF and EF on the primary channel interface calculate queue bandwidth based on 1 Gbps of bandwidth, and AF and EF synchronized to the sub-channel interfaces calculate queue bandwidth based on actual sub-channel interface bandwidth. In this case, if queuing on a sub-channel interface fails due to bandwidth change, the prompt will be output for the sub-channel interface.

On an MP-group interface or MFR interface configured with the **qos max-bandwidth** command, AF and EF perform queue bandwidth check and calculation based on the bandwidth specified with the **qos max-bandwidth** command. On an MP-group interface or MFR interface without the **qos max-bandwidth** command configured, if the sum of sub-channel bandwidth equals to or exceeds the sum of AF bandwidth and EF bandwidth, AF and EF calculate bandwidth based on the actual interface bandwidth. Otherwise, AF and EF calculate bandwidth based on 1 Gbps of bandwidth, and the message indicating insufficient bandwidth is displayed. In the latter case, the queuing function might fail to take effect. You can use the **qos reserved-bandwidth** command to set the maximum percentage of the reserved bandwidth to the available bandwidth.

On tunnel interfaces, subinterfaces, HDLC link bundle interfaces, or VT/dialer interfaces configured with PPPoE, PPPoA, PPPoEoA, PPPoFR, or MPoFR (frame relay traffic shaping is not enabled on the frame relay interface), you must configure the **qos max-bandwidth** command to provide the base bandwidth for CBQ calculation.

## Examples

```
# Set the maximum available bandwidth of Ethernet 1/1 to 16 kbps.
```

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos max-bandwidth 16
```

## qos reserved-bandwidth

Use **qos reserved-bandwidth** to set the maximum reserved bandwidth as a percentage of available bandwidth of the interface.

Use **undo qos reserved-bandwidth** to restore the default.

## Syntax

**qos reserved-bandwidth** *pct percent*

**undo qos reserved-bandwidth**

## Views

Interface view, PVC view

## Default command level

2: System level

## Parameters

**pct percent**: Specifies the percentage of available bandwidth to be reserved. The value range for *percent* is 1 to 100, and the default is 80.

## Usage guidelines

The maximum reserved bandwidth is set on a per-interface basis. It decides the maximum bandwidth assignable for the QoS queues on an interface. It is typically set no greater than 80% of available bandwidth, considering the bandwidth for control traffic and Layer 2 frame headers.

Use the default maximum reserved bandwidth setting in normal cases. When tuning the setting, make sure that the Layer 2 frame header plus the data traffic is under the maximum available bandwidth of the interface.

## Examples

```
# Set the maximum reserved bandwidth to 70% of available bandwidth on interface Serial 1/0.
```

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

```
[Sysname] interface Serial1/0
```

```
[Sysname-Serial1/0] qos reserved-bandwidth pct 70
```

# queue af

Use **queue af** to enable assured-forwarding (AF) and set the minimum guaranteed bandwidth for it.

Use **undo queue af** to delete the configuration.

## Syntax

**queue af bandwidth** { *bandwidth* | **pct percentage** }

**undo queue af**

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

**bandwidth**: Bandwidth in the range of 8 to 1000000 kbps.

**pct percentage**: Percentage of the available bandwidth.

## Usage guidelines

To associate the traffic behavior configured with the **queue af** command with a class in a policy, the following requirements must be met:

- The total bandwidth assigned for AF and EF in a policy must be no more than the maximum available bandwidth of the interface where the policy is applied.
- The total percentage of the maximum available bandwidth assigned for AF and EF in a policy must be no more than 100.
- The bandwidth assigned to AF and EF in a policy must use the same form, either as an absolute bandwidth value or as a percentage.

## Examples

```
# Configure AF in traffic behavior database and assign the minimum guaranteed bandwidth 200 kbps for it.
```

```

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

```

## Related commands

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

## queue ef

Use **queue ef** to configure expedited forwarding (EF) and assign the maximum bandwidth for it.

Use **undo queue ef** to delete the configuration.

## Syntax

```

queue ef bandwidth { bandwidth [ cbs burst ] | pct percentage [ cbs-ratio ratio ] }
undo queue ef

```

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

**bandwidth**: Bandwidth in the range of 8 to 1000000 kbps.

**cbs burst**: CBS in the range of 32 to 2000000 bytes. The default is *bandwidth*×25.

**pct percentage**: Percentage of the maximum available bandwidth, in the range of 1 to 100.

**cbs-ratio ratio**: Allowed burst ratio in the range of 25 to 500. This default is 25.

## Usage guidelines

The command cannot be used in conjunction with the **queue af** command, the **queue-length** command, or the **wred** command in traffic behavior view.

In a policy, the default class cannot be associated with the traffic behavior that has the **queue ef** command.

The total bandwidth assigned for AF and EF in a policy must be no more than the maximum available bandwidth of the interface where the policy is applied.

The total percentage of the maximum available bandwidth assigned for AF and EF in a policy must be no more than 100.

The bandwidths assigned for AF and EF in a policy must have the same type, bandwidth or percentage.

After the **queue ef bandwidth pct percentage [ cbs-ratio ratio ]** command is used, CBS equals (Interface available bandwidth × *percentage* × *ratio*)/100/1000.

After the **queue ef bandwidth bandwidth [ cbs burst ]** command is used, CBS equals *burst*. If the *burst* argument is not specified, CBS equals *bandwidth*×25.

## Examples

# Configure EF in traffic behavior **database**, with the maximum bandwidth as 200 kbps and CBS as 5000 bytes.

```

<Sysname> system-view

```



```
[Sysname] traffic behavior database
[Sysname-behavior-database] queue ef bandwidth 200 cbs 5000
```

## Related commands

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

## queue wfq

Use **queue wfq** to configure WFQ in the traffic behavior.

Use **undo queue wfq** to delete the configuration.

## Syntax

```
queue wfq [ queue-number total-queue-number ]
undo queue wfq
```

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

**queue-number** *total-queue-number*: Specifies the number of fair queues, which can be 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096. The default is 256.

## Usage guidelines

The traffic behavior configured with this command can only be associated with the default class. This command can be used in conjunction with the **queue-length** command or the **wred** command.

## Examples

```
# Configure the default class to use WFQ with 16 queues.
<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
```

## Related commands

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

## queue-length

Use **queue-length** to configure the maximum queue length and use tail drop.

Use **undo queue-length** to delete the configuration.

## Syntax

```
queue-length queue-length
```

**undo queue-length** *queue-length*

## Default

Tail drop is used, and the queue length is 64.

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

*queue-length*: Maximum queue length in the range of 1 to 512.

## Usage guidelines

Before configuring this command, make sure that the **queue af** command or the **queue wfq** command has been configured.

The queue length configured with the **queue-length** command is deleted when the **undo queue af** command or the **undo queue wfq** command is executed, and vice versa.

The queue length configured with the **queue-length** command is deleted when random drop is used using the **wred** command, and vice versa.

## Examples

# Configure a maximum queue length of 16 and specify tail drop for AF.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
[Sysname-behavior-database] queue-length 16
```

## Related commands

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

## wred

Use **wred** to use WRED drop.

Use **undo wred** to delete the configuration.

## Syntax

```
wred [ dscp | ip-precedence ]
undo wred
```

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

**dscp**: Uses the DSCP value for calculating drop probability for a packet.

**ip-precedence**: Uses the IP precedence value for calculating drop probability of a packet. This keyword is the default.

## Usage guidelines

You can configure this command only after you have configured the **queue af** command or the **queue wfq** command. Applying a QoS policy with WRED configured to an interface overwrites the previous interface-level WRED configuration.

## Examples

```
# Configure WRED in traffic behavior database and calculate drop probability based on IP precedence.
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred
```

## Related commands

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

## wred dscp

Use **wred dscp** to configure the lower limit, upper limit, and drop probability for packets with a specified DSCP value.

Use **undo wred dscp** to delete the configuration.

## Syntax

```
wred dscp dscp-value low-limit low-limit high-limit high-limit [discard-probability discard-prob ]
undo wred dscp dscp-value
```

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

**dscp-value**: DSCP value in the range of 0 to 63. This argument can also be represented using one of the keywords listed in [Table 19](#).

**low limit** *low-limit*: Specifies the lower WRED limit value in the range of 1 to 1024.

**high-limit** *high-limit*: Specifies the upper WRED limit value in the range of 1 to 1024.

**discard-probability** *discard-prob*: Specifies the drop probability denominator in the range of 1 to 255.

## Usage guidelines

Before configuring this command, make sure the DSCP-based WRED drop is enabled using the **wred** command.

Removing the **wred** command configuration removes the **wred dscp** command configuration as well.

The drop-related parameters are removed if the configuration set with the **queue af** command or the **queue wfq** command is removed.

## Examples

# Set the following parameters for packets with DSCP value 3: lower limit 20, upper limit 40, and drop probability 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
```

## Related commands

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

## wred ip-precedence

Use **wred ip-precedence** to configure the lower limit, upper limit, and drop probability for packets with a specified IP precedence.

Use **undo wred ip-precedence** to delete the configuration.

## Syntax

**wred ip-precedence** *precedence* **low-limit** *low-limit* **high-limit** *high-limit* [ **discard-probability** *discard-prob* ]

**undo wred ip-precedence** *precedence*

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

*precedence*: IP precedence value in the range of 0 to 7.

**low limit** *low-limit*: Specifies the lower WRED limit value in the range of 1 to 1024.

**high-limit** *high-limit*: Specifies the upper WRED limit value in the range of 1 to 1024.

**discard-probability** *discard-prob*: Specifies the drop probability denominator in the range of 1 to 255.

## Usage guidelines

Before configuring this command, make sure the IP precedence-based WRED drop is enabled using the **wred** command.

The **wred ip-precedence** command configuration is removed when the **wred** command configuration is removed.

The drop-related parameters are removed if the **queue af** command configuration or the **queue wfq** command configuration is removed.

## Examples

# Configure the following parameters for packets with IP precedence 3: lower limit 20, upper limit 40, and drop probability 15.

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

```
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred ip-precedence
[Sysname-behavior-database] wred ip-precedence 3 low-limit 20 high-limit 40
discard-probability 15
```

## Related commands

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

## wred weighting-constant

Use **wred weighting-constant** to configure the WRED exponent for calculating the average queue length.

Use **undo wred weighting-constant** to delete the configuration.

## Syntax

**wred weighting-constant** *exponent*

**undo wred weighting-constant**

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

*exponent*: Exponent in the range of 1 to 16. This argument is 9 by default.

## Usage guidelines

Before configuring this command, make sure that the **queue af** command or the **queue wfq** command is configured and WRED drop is enabled using the **wred** command.

The **wred weighting-constant** command configuration is removed if the **wred** command configuration is removed.

## Examples

# Set the exponent for calculating the average queue length to 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
```

## Related commands

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

# RTP queuing commands

## display qos rtpq interface

Use **display qos rtpq interface** to display the information of the current IP RTP priority queue, including the queue length and the number of dropped packets on an interface/PVC or all interfaces/PVCs.

### Syntax

```
display qos rtpq interface [ interface-type interface-number [ pvc { pvc-name [ vpi/vci ] | vpi/vci } ] ]  
[ | { begin | exclude | include } regular-expression ]
```

### Views

Any view

### Default command level

1: Monitor level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

**pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* }: Specifies a PVC on an ATM interface. The *pvc-name* argument specifies the PVC by its name. *vpi/vci* specifies the PVC by its VPI/VCI pair. This option is only available for ATM interfaces.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

### Usage guidelines

If no interface/PVC is specified, this command displays the RTP priority queuing configuration and statistics of all the interfaces/PVCs.

If a VT interface is specified, this command displays QoS RTP priority queuing information of all VA interfaces inheriting the VT interface, but does not display QoS information about the VT interface.

### Examples

# Display the information of the current IP RTP priority queue.

```
<Sysname> display qos rtpq interface
```

```
Interface: Ethernet1/1
```

```
Output queue : (RTP queuing : Size/Max/Outputs/Discards) 0/0/0/0
```

**Table 34 Command output**

Field	Description
Interface	Interface type and interface number.
Output queue	Current output queue.
Size	Number of packets in the queue.
Max	Historical maximum number of packets in the queue.

Field	Description
Outputs	Number of sent packets.
Discards	Number of dropped packets.

## qos rtpq

Use **qos rtpq** to enable RTP queuing for RTP packets with even UDP destination port numbers in the specified range on the interface/PVC.

Use **undo qos rtpq** to disable RTP queuing on the interface/PVC.

### Syntax

**qos rtpq start-port** *first-rtp-port-number* **end-port** *last-rtp-port-number* **bandwidth** *bandwidth* [**cbs** *burst*]

**undo qos rtpq**

### Default

RTP queuing is disabled on an interface/PVC.

### Views

Interface view, PVC view

### Default command level

2: System level

### Parameters

**start-port** *first-rtp-port-number*: First UDP port number in the range of 2000 to 65535.

**end-port** *last-rtp-port-number*: Last UDP port number in the range of 2000 to 65535.

**bandwidth** *bandwidth*: Bandwidth for the RTP priority queue, in the range of 8 to 1000000 in kbps.

**cbs** *burst*: CBS in bytes, in the range of 1500 to 2000000.

### Usage guidelines

This command provides preferential services for delay-sensitive applications, such as real-time voice transmission.

Set the *bandwidth* argument to a value greater than the total bandwidth that the real-time application requires to allow bursty traffic.

You must enable the line rate function for the queuing function to take effect on these interfaces: tunnel interfaces, subinterfaces, HDLC link bundle interfaces, and VT/dialer interfaces configured with PPPoE, PPPoA, PPPoEoA, PPPoFR, or MPoFR (frame relay traffic shaping is not enabled on the frame relay interface).

### Examples

# Configure RTP queuing on interface Serial 2/0: the RTP packets with even UDP destination port numbers in the range 16384 to 32767 are assigned to the RTP queue when congestion occurs on the outgoing interface, and the bandwidth for RTP packets is 64 kbps.

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

```
[Sysname] interface serial 2/0
```

```
[Sysname-Serial2/0] qos rtpq start-port 16384 end-port 32767 bandwidth 64
```

# QoS token commands

## qos qmtoken

Use **qos qmtoken** to set the number of QoS tokens.

Use **undo qos qmtoken** to disable the QoS token feature.

### Syntax

**qos qmtoken** *token-number*

**undo qos qmtoken**

### Default

The feature is disabled.

### Views

Interface view

### Default command level

2: System level

### Parameters

*token-number*: Number of tokens, in the range 1 to 50.

### Usage guidelines

This command is supported only on serial interfaces and BRI interfaces. After you configure this command on an interface, you must execute the **shutdown** command and then the **undo shutdown** command on the interface to have the feature take effect.

During FTP transmission, flow control provided by the upper layer protocol might invalidate the QoS queuing configuration. The QoS token feature provides a flow control mechanism for underlying-layer queues. This feature can control the number of packets sent to such queues based on the number of tokens.

H3C recommends that you set the *token-number* to 1 on an interface for FTP transmission.

### Examples

# Set the number of QoS tokens to 1.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] qos qmtoken 1
[Sysname-Serial2/0] shutdown
[Sysname-Serial2/0] undo shutdown
```

# Packet information pre-extraction commands

## qos pre-classify

Use **qos pre-classify** to enable packet information pre-extraction on the tunnel interface.

Use **undo qos pre-classify** to disable packet information pre-extraction on the tunnel interface.

### Syntax

**qos pre-classify**



**undo qos pre-classify**

### Default

Packet information pre-extraction is disabled on a tunnel interface.

### Views

Tunnel interface view

### Default command level

2: System level

### Examples

```
# Enable packet information pre-extraction on tunnel interface Tunnel 1.
<Sysname> system-view
[Sysname] interface tunnel 1
[Sysname-Tunnel1] qos pre-classify
```

## Local fragment pre-drop commands

### qos fragment pre-drop

Use **qos fragment pre-drop** to enable local fragment pre-drop on the interface.

Use **undo qos fragment pre-drop** to disable local fragment pre-drop on the interface.

### Syntax

```
qos fragment pre-drop
undo qos fragment pre-drop
```

### Default

Local fragment pre-drop is disabled on interfaces.

### Views

Interface view

### Default command level

2: System level

### Usage guidelines

If the first fragment of local fragments is dropped, all subsequent fragments are dropped.

Local fragment pre-drop applies to IPv4 and IPv6 local fragments.

### Examples

```
# Enable local fragment pre-drop on interface Ethernet 1/1.
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos fragment pre-drop
```

# Congestion avoidance commands

## WRED commands

### display qos wred interface

Use **display qos wred interface** to display the WRED configuration and statistics of an interface/PVC.

#### Syntax

**display qos wred interface** [ *interface-type interface-number* [ **pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* } ] ]  
[ | { **begin** | **exclude** | **include** } *regular-expression* ]

#### Views

Any view

#### Default command level

1: Monitor level

#### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

**pvc** { *pvc-name* [ *vpi/vci* ] | *vpi/vci* }: Specifies a PVC on an ATM interface. *pvc-name* specifies the PVC by its name. *vpi/vci* specifies the PVC by its VPI/VCI pair. This option is only available for ATM interfaces.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

#### Usage guidelines

If no interface/PVC is specified, this command displays the WRED configuration and statistics of all the interfaces/PVCs.

#### Examples

# Display the WRED configuration and statistics of Ethernet 1/1.

```
<Sysname> display qos wred interface ethernet 1/1
```

```
Interface: Ethernet1/1
```

```
Current WRED configuration:
```

```
Exponent: 9 (1/512)
```

	Precedence	Low	High	Discard	Random	Tail
		Limit	Limit	Probability	Discard	Discard
0		10	30	10	0	0
1		100	1000	1	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

**Table 35 Command output**

Field	Description
Interface	Interface type and interface number.
Exponent	WRED exponent for average queue length calculation.
Precedence	IP precedence.
Random discard	Number of packets randomly dropped.
Tail discard	Number of packets dropped using tail drop.
Low limit	Lower limit for a queue.
High limit	Upper limit for a queue.
Discard probability	Drop probability.

## qos wred enable

Use **qos wred enable** to enable WRED on an interface/PVC.

Use **undo qos wred enable** to restore the default.

### Syntax

**qos wred [ dscp | ip-precedence ] enable**

**undo qos wred enable**

### Default

Tail drop is used.

### Views

Interface view, PVC view

### Default command level

2: System level

### Parameters

**dscp**: Uses the DSCP values for calculating drop probability.

**ip-precedence**: Uses the IP precedence for calculating drop probability. This keyword is specified by default.

### Usage guidelines

The **qos wred enable** command can be configured on a hardware interface directly. However, to configure this command on a software interface, enable WFQ on the software interface first.

### Examples

# Enable WRED on Ethernet 1/1, and use the IP precedence for drop probability calculation.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos wfq queue-length 100 queue-number 512
[Sysname-Ethernet1/1] qos wred ip-precedence enable
```

## Related commands

- **qos wfq**
- **display qos wred interface**

## qos wred dscp

Use **qos wred dscp** to configure the lower limit, upper limit, and drop probability for a DSCP value.

Use **undo qos wred dscp** to restore the default.

## Syntax

**qos wred dscp** *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

**undo qos wred dscp** *dscp-value*

## Views

Interface view, PVC view

## Default command level

2: System level

## Parameters

*dscp-value*: DSCP value in the range of 0 to 63. This argument can also be represented using one of the keywords listed in [Table 19](#):

**low limit** *low-limit*: Specifies the lower WRED limit value in the range of 1 to 1024.

**high-limit** *high-limit*: Specifies the upper WRED limit value in the range of 1 to 1024.

**discard-probability** *discard-prob*: Specifies the drop probability denominator in the range of 1 to 255.

## Usage guidelines

Before this configuration, enable DSCP-based WRED on the interface/PVC with the **qos wred dscp enable** command first. The upper and lower limits restrict the average queue length.

## Examples

# Configure the following parameters for packets with DSCP value 63 on Ethernet 1/1: lower limit 20, upper limit 40, and drop probability 15.

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

```
[Sysname] interface ethernet 1/1
```

```
[Sysname-Ethernet1/1] qos wfq queue-length 100 queue-number 512
```

```
[Sysname-Ethernet1/1] qos wred dscp enable
```

```
[Sysname-Ethernet1/1] qos wred dscp 63 low-limit 20 high-limit 40 discard-probability 15
```

## Related commands

- **qos wred enable**
- **display qos wred interface**

## qos wred ip-precedence

Use **qos wred ip-precedence** to configure the lower limit, upper limit, and drop probability for an IP precedence value.

Use **undo qos wred ip-precedence** to restore the default.

## Syntax

```
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
```

## Views

Interface view, PVC view

## Default command level

2: System level

## Parameters

**ip-precedence** *precedence*: IP precedence value in the range of 0 to 7.

**low limit** *low-limit*: Specifies the lower WRED limit value in the range of 1 to 1024.

**high-limit** *high-limit*: Specifies the upper WRED limit value in the range of 1 to 1024.

**discard-probability** *discard-prob*: Specifies the drop probability denominator in the range of 1 to 255.

## Usage guidelines

Before this configuration, enable IP precedence-based WRED on the interface/PVC with the **qos wred enable** command first. The upper and lower limits restrict the average queue length.

## Examples

# Configure the following parameters for packets with IP precedence 3 on Ethernet 1/1: lower limit 20, upper limit 40, and drop probability 15.

```
<Sysname> system-view  
[Sysname] interface ethernet 1/1  
[Sysname-Ethernet1/1] qos wfq queue-length 100 queue-number 512  
[Sysname-Ethernet1/1] qos wred ip-precedence enable  
[Sysname-Ethernet1/1] qos wred ip-precedence 3 low-limit 20 high-limit 40  
discard-probability 15
```

## Related commands

- **qos wred enable**
- **display qos wred interface**

## qos wred weighting-constant

Use **qos wred weighting-constant** to configure the exponent for calculating the average queue length.

Use **undo qos wred weighting-constant** to restore the default.

## Syntax

```
qos wred weighting-constant exponent  
undo qos wred weighting-constant
```

## Views

Interface view, PVC view

## Default command level

2: System level

## Parameters

*exponent*: Exponent for average queue length calculation, in the range of 1 to 16. This argument is 9 by default.

## Usage guidelines

Before this configuration, enable WRED on the interface/PVC with the **qos wred enable** command first.

## Examples

# Set the exponent for the average queue length calculation to 6 on Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] qos wfq queue-length 100 queue-number 512
[Sysname-Ethernet1/1] qos wred enable
[Sysname-Ethernet1/1] qos wred weighting-constant 6
```

## Related commands

- **qos wred enable**
- **display qos wred interface**

# WRED table commands

## display qos wred table

Use **display qos wred table** to display the WRED table configuration information.

## Syntax

**display qos wred table** [ *table-name* ] [ [ { **begin** | **exclude** | **include** } *regular-expression* ]

## Views

Any view

## Default command level

1: Monitor level

## Parameters

*table-name*: Name of the WRED table to be displayed.

[ ]: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

If no WRED table name is specified, this command displays the configuration of all the WRED tables.

## Examples

# Display the configuration of WRED table 1.

```
<Sysname> display qos wred table 1
```

Table Name: 1

Table Type: Queue based WRED

QID:	gmin	gmax	gprob	ymin	ymax	yprob	rmin	rmax	rprob	exponent
0	76	134	1	33	66	2	11	23	3	9
1	76	134	1	33	66	2	11	23	3	9
2	76	134	1	33	66	2	11	23	3	9
3	76	134	1	33	66	2	11	23	3	9
4	76	134	1	33	66	2	11	23	3	9
5	76	134	1	33	66	2	11	23	3	9
6	76	134	1	33	66	2	11	23	3	9
7	76	134	1	33	66	2	11	23	3	9

**Table 36 Command output**

Field	Description
Table name	Name of a WRED table.
Table type	Type of a WRED table.
QID	Queue ID.
gmin	Lower limit for green packets.
gmax	Upper limit for green packets.
gprob	Drop probability for green packets.
ymin	Lower limit for yellow packets.
ymax	Upper limit for yellow packets.
yprob	Drop probability for yellow packets.
rmin	Lower limit for red packets.
rmax	Upper limit for red packets.
rprob	Drop probability for red packets.
Exponent	Exponent for average queue length calculation.

## qos wred table

Use **qos wred table** to create a WRED table and enter WRED table view.

Use **undo qos wred table** to delete a WRED table.

### Syntax

**qos wred queue table** *table-name*

**undo qos wred table** *table-name*

### Default

No global WRED table is created.

### Views

System view

### Default command level

2: System level

## Parameters

**queue:** Creates a queue-based table. Packets are dropped based on the queue when congestion occurs.

**table** *table-name*: Specifies a name for the table.

## Usage guidelines

A WRED table in use cannot be removed.

A queue-based WRED table applies to only Layer 2 ports, and vice versa.

## Examples

# Create a queue-based WRED table named **queue-table1**.

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

## Related commands

- **qos wfq**
- **qos wred enable**
- **display qos wred interface**

# queue

Use **queue** to configure the drop-related parameters for a specified queue in the queue-based WRED table.

Use **undo queue** to restore the default.

## Syntax

**queue** *queue-value* **low-limit** *low-limit* [ **discard-probability** *discard-prob* ]

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

## Default

A global queue-based WRED table has a set of default available parameters.

## Views

WRED table view

## Default command level

2: System level

## Parameters

**queue-value**: Queue number. This argument is available on only Layer 2 ports.

**low limit** *low-limit*: Specifies the lower WRED limit value in the range of 1 to 128.

**discard-probability** *discard-prob*: Specifies the drop probability denominator in the range of 1 to 16.

## Examples

# Configure the drop probability of queue 1 for the global queue-based WRED table **queue-table1**.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1]
[Sysname-wred-table-queue-table1] queue 1 low-limit 10 discard-probability 15
[Sysname-wred-table-queue-table1]
```



## Related commands

**qos wred table**

## qos wred apply

Use **qos wred apply** to apply a global WRED table on a port/port group.

Use **undo qos wred apply** to restore the default.

### Syntax

**qos wred apply** *table-name*

**undo qos wred apply**

### Default

The tail drop mode is used on a port.

### Views

Interface view, port group view

### Default command level

2: System level

### Parameters

*table-name*: Name of a global WRED table.

### Usage guidelines

The following matrix shows the command and hardware compatibility:

Hardware	Keyword compatibility
MSR800	No
MSR 900	No
MSR900-E	No
MSR 930	No
MSR 20-1X	No
MSR 20	No
MSR 30	Supported only on MIM-16FSW and DMIM-24FSW Layer 2 Ethernet switching modules
MSR 50	Supported only on FIC-16FSW and DFIC-24FSW Layer 2 Ethernet switching modules
MSR 2600	No
MSR3600-51F	Supported only on MIM-16FSW Layer 2 Ethernet switching modules

A queue-based WRED table is available on only Layer 2 ports. Only queue-based WRED tables can be applied on Layer 2 ports.

In interface view, the setting takes effect on the current port only. In port group view, the setting takes effect on all the ports in the port group.

### Examples

# Apply the queue-based WRED table **queue-table1** to the Layer 2 port Ethernet 1/1.

```
<Sysname> system-view  
[Sysname] interface ethernet 1/1  
[Sysname-Ethernet1/1] qos wred apply queue-table1
```

#### **Related commands**

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

# DAR commands

## dar enable

Use **dar enable** to enable DAR for traffic recognition on the current interface.

Use **undo dar enable** to disable DAR on the current interface.

### Syntax

**dar enable**

**undo dar enable**

### Default

DAR is disabled on an interface.

### Views

Interface view

### Default command level

2: System level

### Examples

# Enable DAR for traffic recognition on Ethernet 1/1.

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

```
[Sysname] interface ethernet 1/1
```

```
[Sysname-Ethernet1/1] dar enable
```

## dar max-session-count

Use **dar max-session-count** to set the maximum number of sessions that DAR can recognize.

Use **undo dar max-session-count** to restore the default.

### Syntax

**dar max-session-count** *count*

**undo dar max-session-count**

### Views

System view

### Default command level

2: System level

### Parameters

*count*: Maximum number of sessions that deeper application recognition (DAR) can recognize.

### Usage guidelines

DAR tasks are resource intensive. To prevent DAR tasks from affecting other network services, you can limit the maximum number of sessions that DAR can recognize. The limitation applies to HTTP, FTP, RTP, and RTCP. After the limitation is reached, DAR marks all incoming packets of these applications as unrecognizable. For the packets of other TCP/UDP protocols, DAR continues to perform packet recognition.

## Examples

```
# Set the maximum number of sessions that DAR can recognize to 1000.
<Sysname> system-view
[Sysname] dar max-session-count 1000
```

## dar p2p signature-file

Use **dar p2p signature-file** to load the specified P2P signature file.

Use **undo dar p2p signature-file** to unload the specified P2P signature file.

### Syntax

```
dar p2p signature-file filename
undo dar p2p signature-file
```

### Default

No P2P signature file exists in the system.

### Views

System view

### Default command level

2: System level

### Parameters

*filename*: P2P signature file name, which must be suffixed with .mtd.

### Usage guidelines

Place the signature file in the root directory. The system can load a signature file only from the root directory.

## Examples

```
# Load the P2P signature file p2p.mtd.
<Sysname> system-view
[Sysname] dar p2p signature-file flash:/p2p.mtd
```

## dar protocol

Use **dar protocol** to specify port numbers for an application protocol in DAR.

Use **undo dar protocol** to restore the default for a protocol.

### Syntax

```
dar protocol protocol-name { tcp | udp } port { port-value&<1-16> | range port-min port-max } *
undo dar protocol protocol-name { tcp | udp } port
```

### Default

No port numbers are defined for the ten user-defined protocols, RTP, and RTCP. The default port numbers of other protocols are listed in [Table 37](#).

**Table 37 Default port numbers of protocols**

Protocol name	Protocol type	Default port numbers
BGP	TCP/UDP	179

Protocol name	Protocol type	Default port numbers
Cifs	TCP	445
Citrix	TCP	1494
Citrix	UDP	1604
CUSEeMe	TCP	7648, 7649
CUSEeMe	UDP	7648, 7649, 24032
DHCP	UDP	67, 68
DNS	TCP/UDP	53
Exchange	TCP	135
Fasttrack	TCP	1214
Finger	TCP	79
FTP	TCP	21
Gnutella	TCP	6346, 6347, 6348, 6349, 6355, 5634
Gopher	TCP/UDP	70
H323	TCP	1300, 1718, 1719, 1720, 11000 through 11999
H323	UDP	1300, 1718, 1719, 1720, 11720
HTTP	TCP	80
IMAP	TCP/UDP	143, 220
IRC	TCP/UDP	194
Kerberos	TCP/UDP	88, 749
L2TP	UDP	1701
LDAP	TCP/UDP	389
Mgcp	TCP	2427, 2428, 2727
Mgcp	UDP	2427, 2727
Napster	TCP	6699, 8875, 8888, 7777, 6700, 6666, 6677, 6688, 4444, 5555
NetBIOS	TCP	137, 138, 139
NetBIOS	UDP	137, 138, 139
Netshow	TCP	1755
NFS	TCP/UDP	2049
NNTP	TCP/UDP	119
Notes	TCP/UDP	1352
Novadign	TCP/UDP	3460, 3461, 3462, 3463, 3464, 3465
NTP	TCP/UDP	123
PCAnywhere	TCP	5631, 65301
PCAnywhere	UDP	22, 5632
POP3	TCP/UDP	110
PPTP	TCP	1723

Protocol name	Protocol type	Default port numbers
Printer	TCP/UDP	515
RCMD	TCP	512, 513, 514
RIP	UDP	520
RSVP	UDP	1698, 1699
RTSP	TCP	554
Secure-FTP	TCP	990
Secure-HTTP	TCP	443
Secure-IMAP	TCP/UDP	585, 993
Secure-IRC	TCP/UDP	994
Secure-LDAP	TCP/UDP	636
Secure-NNTP	TCP/UDP	563
Secure-POP3	TCP/UDP	995
Secure-TELNET	TCP	992
SIP	TCP/UDP	5060
Skinny	TCP	2000, 2001, 2002
SMTP	TCP	25
SNMP	TCP/UDP	161, 162
SOCKS	TCP	1080
Sqlnet	TCP	1521
Sqlserver	TCP	1433
SSH	TCP	22
Streamwork	UDP	1558
Sunrpc	TCP/UDP	111
Syslog	UDP	514
Telnet	TCP	23
Tftp	UDP	69
Vdolive	TCP	7000
Winmx	TCP	6699
XWindows	TCP	6000, 6001, 6002, 6003

## Views

System view

## Default command level

2: System level

## Parameters

*protocol*: Protocol type, which can be one of the protocols listed in [Table 37](#), RTP, RTCP, user-defined01, user-defined02, ..., or user-defined10. No port is specified for the ten user-defined protocols (user-defined01 through user-defined10) in the initial state. A user-defined protocol takes

effect after a port is specified for it. You can use the **dar protocol-rename** command to change the name of a user-defined protocol.

**tcp**: TCP-based protocol.

**udp**: UDP-based protocol.

*port-value*: Port number of the protocol, in the range of 1 to 65535. This argument cannot conflict with the port numbers set for other application protocols in the DAR feature. <1-16> means that you can specify up to 16 port numbers for a protocol.

**range port-min port-max**: Sets a port number range from the *port-min* to the *port-max*. The difference between the minimum port number and the maximum port number must be smaller than 1000. The port numbers set for other application protocols in the DAR feature cannot be contained in the port number range.

## Examples

```
# Set the port numbers of RTP to 36000, 36001, and 40000 through 40999.
```

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

```
[Sysname] dar protocol rtp udp port 36000 36001 range 40000 40999
```

## dar protocol-group

Use **dar protocol-group** to create a P2P protocol group and enter its view.

Use **undo dar protocol-group** to delete the specified protocol group.

### Syntax

```
dar protocol-group group-id
```

```
undo dar protocol-group group-id
```

### Default

No protocol group exists in the system.

### Views

System view

### Default command level

2: System level

### Parameters

*group-id*: Protocol group ID in the range of 1 to 64.

## Examples

```
# Create P2P protocol group 1.
```

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

```
[Sysname] dar protocol-group 1
```

```
[Sysname-protocol-group-1]
```

## dar protocol-rename

Use **dar protocol-rename** to change the name of a user-defined protocol.

Use **undo dar protocol-rename** to restore the default.

### Syntax

```
dar protocol-rename old-name user-defined-name
```

**undo dar protocol-rename** *user-defined-name*

### Default

The names of the user-defined protocols are **user-defined01**, **user-defined02**, ..., **user-defined10**.

### Views

System view

### Default command level

2: System level

### Parameters

*old-name*: Initial name of a user-defined protocol, which is one of the following names: **user-defined01**, **user-defined02**, ..., **user-defined10**.

*user-defined-name*: New name of a user-defined protocol, a string of 1 to 31 characters. The new name cannot conflict with the existing protocol names. Additionally, the new name cannot be one of the following names: all, total, tcp, udp, ip, user-defined01, user-defined02, ..., user-defined10.

### Examples

# Change the user-defined protocol name **user-defined01** to **hello**.

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

```
[Sysname] dar protocol-rename user-defined01 hello
```

# Restore the user-defined protocol name **hello** to the default.

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

```
[Sysname] undo dar protocol-rename hello
```

## dar protocol-statistic

Use **dar protocol-statistic** to enable the packet accounting function of DAR.

Use **undo dar protocol-statistic** to disable the packet accounting function of DAR.

### Syntax

**dar protocol-statistic** [ **flow-interval** *time* ]

**undo dar protocol-statistic**

### Default

The packet accounting function of DAR is disabled.

### Views

Interface view

### Default command level

2: System level

### Parameters

**flow-interval** *time*: Specifies the accounting interval in minutes. The value range for *time* is 1 to 30, and the default is 5.

### Usage guidelines

The packet accounting function of DAR collects the traffic statistics on a per-application basis on interfaces. It helps you identify aggressive applications.



## Examples

# Enable the packet accounting function of DAR for Ethernet 1/1, setting the accounting interval to 7 minutes.

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

```
[Sysname] interface ethernet 1/1
```

```
[Sysname-Ethernet1/1] dar protocol-statistic flow-interval 7
```

## display dar information

Use **display dar information** to display DAR information.

### Syntax

**display dar information** [ | { **begin** | **exclude** | **include** } *regular-expression* ]

### Views

Any view

### Default command level

1: Monitor level

### Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Examples

# Display DAR information.

```
<Sysname> display dar information
```

```
Max session count      : 65536
```

```
Watched session count  : 1000
```

**Table 38 Command output**

Field	Description
Max session count	Maximum number of sessions.
Watched session count	Number of monitored sessions.

## display dar protocol

Use **display dar protocol** to display information about a protocol or all protocols in DAR.

### Syntax

**display dar protocol** { *protocol-name* | **all** } [ | { **begin** | **exclude** | **include** } *regular-expression* ]

### Views

Any view

## Default command level

1: Monitor level

## Parameters

**protocol-name:** Displays information about a protocol. The range for this argument is the same as that in the **dar protocol** command.

**all:** Displays information about all the protocols.

**|:** Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin:** Displays the first line that matches the specified regular expression and all lines that follow.

**exclude:** Displays all lines that do not match the specified regular expression.

**include:** Displays all lines that match the specified regular expression.

**regular-expression:** Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

For static port protocols and common application layer protocols, this command displays the TCP/UDP port number information.

## Examples

# Display information about all the protocols.

```
<Sysname> display dar protocol all
```

Protocol	TCP/UDP	Port
bgp	tcp	179
	udp	179
cifs	tcp	445
citrix	tcp	1494
	udp	1604
cuseeme	tcp	7648 7649
	udp	7648 7649 24032
dhcp	udp	67 68
dns	tcp	53
	udp	53
exchange	tcp	135
fasttrack	tcp	1214
finger	tcp	79
ftp	tcp	21
gnutella	tcp	5634 6355 range 6346 6349
gopher	tcp	70
	udp	70
h323	tcp	1300 1718 1719 1720 range 11000 11999
	udp	1300 1718 1719 1720 11720
http	tcp	80
imap	tcp	143 220
	udp	143 220
irc	tcp	194
	udp	194
kerberos	tcp	88 749
	udp	88 749

l2tp	udp	1701
ldap	tcp	389
	udp	389
mgcp	tcp	2427 2428 2727
	udp	2427 2727
napster	tcp	6699 8875 8888 7777 6700 6666 6677 6688 4444 5555
netbios	tcp	137 138 139
	udp	137 138 139
netshow	tcp	1755
nfs	tcp	2049
	udp	2049
nntp	tcp	119
	udp	119
notes	tcp	1352
	udp	1352
novadign	tcp	3460 3461 3462 3463 3464 3465
	udp	3460 3461 3462 3463 3464 3465
ntp	tcp	123
	udp	123
pcanywhere	tcp	5631 65301
	udp	22 5632
pop3	tcp	110
	udp	110
pptp	tcp	1723
printer	tcp	515
	udp	515
rcmd	tcp	512 513 514
rip	udp	520
rsvp	udp	1698 1699
rtcp		
rtp		
rtsp	tcp	554
secure-ftp	tcp	990
secure-http	tcp	443
secure-imap	tcp	585 993
	udp	585 993
secure-irc	tcp	994
	udp	994
secure-ldap	tcp	636
	udp	636
secure-nntp	tcp	563
	udp	563
secure-pop3	tcp	995
	udp	995
secure-telnet	tcp	992
sip	tcp	5060
	udp	5060
skinny	tcp	2000 2001 2002

```

smtp          tcp      25
snmp          tcp      161 162
              udp      161 162
socks         tcp      1080
sqlnet        tcp      1521
sqlserver     tcp      1433
ssh           tcp      22
streamwork    udp      1558
sunrpc        tcp      111
              udp      111
syslog        udp      514
telnet        tcp      23
tftp          udp      69
user-defined01
user-defined02
user-defined03
user-defined04
user-defined05
user-defined06
user-defined07
user-defined08
user-defined09
user-defined10
vdolive       tcp      7000
winmx         tcp      6699
xwindows      tcp      range 6000 6003

```

**Table 39 Command output**

Field	Description
Protocol	Protocol name.
TCP/UDP	Protocol type: TCP-based or UDP-based.
Port	Port number.

## display dar protocol-rename

Use **display dar protocol-rename** to display information about renamed user-defined protocols.

### Syntax

```
display dar protocol-rename [ | { begin | exclude | include } regular-expression ]
```

### Views

Any view

### Default command level

1: Monitor level

### Parameters

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin:** Displays the first line that matches the specified regular expression and all lines that follow.

**exclude:** Displays all lines that do not match the specified regular expression.

**include:** Displays all lines that match the specified regular expression.

*regular-expression:* Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Examples

# Display information about renamed user-defined protocols.

```
<Sysname> display dar protocol-rename
```

Default Name	User Defined Name
--------------	-------------------

-----

user-defined01	merry
----------------	-------

user-defined02

user-defined03

user-defined04

user-defined05

user-defined06

user-defined07

user-defined08

user-defined09

user-defined10

**Table 40 Command output**

Field	Description
Default Name	Default name of a user-defined protocol.
User Defined Name	New name of the user-defined protocol.

## display dar protocol-statistic

Use **display dar protocol-statistic** to display the DAR packet statistics.

### Syntax

```
display dar protocol-statistic [ p2p | protocol protocol-name | top top-number | all ] [ interface interface-type interface-number ] [ direction { in | out } ] [ { begin | exclude | include } regular-expression ]
```

### Default

This command displays both inbound and outbound traffic.

### Views

Any view

### Default command level

1: Monitor level

### Parameters

**p2p:** Displays P2P traffic statistics.

**protocol** *protocol-name:* Displays the packet statistics of the protocol specified for the *protocol-name* argument. The range for the *protocol-name* argument is the same as that in the **if-match protocol** command.

**top** *top-number*: Displays statistics for protocols with the most traffic. The number of protocols is identified by the *top-number* argument, which is in the range of 1 to 16.

**all**: Displays the packet statistics of all the protocols.

*interface-type interface-number*: Specifies an interface by its type and number.

**direction**: Displays the packet statistics of a direction. **in**: Displays statistics about the inbound traffic.

**out**: Displays statistics about the outbound traffic.

**|**: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Examples

# Display the packet statistics of all the protocols on Ethernet 1/1.

```
<Sysname> display dar protocol-statistic interface ethernet 1/1
Interface: Ethernet1/1
```

Protocol	In/Out	Packet Count	Byte Count	Bit Rate in 5 min (bps)	Max Bit Rate in 5 min (bps)
nethbios	IN	5	692	0	0
tcp-handshake	IN	1	48	0	0
	OUT	2	88	0	0
unknown-tcp	IN	1	42	0	0
Total	IN	7	782	0	0
	OUT	5	214	0	0

# Display the P2P traffic statistics on Ethernet 1/1.

```
<Sysname> display dar protocol-statistic p2p interface ethernet 1/1
Interface: Ethernet1/1
```

Protocol	In/Out	Packet Count	Byte Count	Bit Rate in 5 min (bps)	Max Bit Rate in 5 min (bps)
MSN	IN	0	0	0	0
	OUT	0	0	0	0
Yahoo Message	IN	0	0	0	0
	OUT	0	0	0	0
Total	IN	0	0	0	0
	OUT	3	126	0	0

**Table 41 Command output**

Field	Description
Protocol	Protocol name.
In/Out	Direction of packets (inbound/outbound).
Packet Count	Number of packets.

Field	Description
Byte Count	Number of bytes.
Bit Rate in 5 min(bps)	Average bit rate in 5 minutes (in bps).
Max Bit Rate in 5 min(bps)	Maximum bit rate in 5 minutes (in bps).

## if-match protocol

Use **if-match protocol** to define a protocol-based match criterion.

Use **undo if-match protocol** to delete the match criterion.

### Syntax

**if-match** [ **not** ] **protocol** *protocol-name*

**undo if-match** [ **not** ] **protocol** *protocol-name*

### Default

No protocol-based match criterion is configured.

### Views

Class view

### Default command level

2: System level

### Parameters

**not**: Specifies to match packets not conforming to the specified criterion.

*protocol-name*: Protocol name to be matched, which can be one of the following names: **bgp**, **cifs**, **citrix**, **cuseeme**, **dhcp**, **dns**, **egp**, **eigrp**, **exchange**, **fasttrack**, **finger**, **ftp**, **gnutella**, **gopher**, **gre**, **h323**, **icmp**, **igmp**, **imap**, **ip**, **ipinip**, **ipsec**, **ipv6**, **irc**, **kerberos**, **l2tp**, **ldap**, **mgcp**, **napster**, **netbios**, **netshow**, **nfs**, **nntp**, **notes**, **novadign**, **ntp**, **pcanywhere**, **pop3**, **pptp**, **printer**, **rcmd**, **rip**, **rsvp**, **rtcp**, **rtsp**, **secure-ftp**, **secure-http**, **secure-imap**, **secure-irc**, **secure-ldap**, **secure-nntp**, **secure-pop3**, **secure-telnet**, **sip**, **skinny**, **smtp**, **snmp**, **socks**, **sqlnet**, **sqlserver**, **ssh**, **streamwork**, **sunrpc**, **syslog**, **telnet**, **tfpp**, **vdolive**, **winmx**, **xwindows**, **unknown-tcp**, **unknown-udp**, **unknown-others**, **user-defined01**, **user-defined02**...**user-defined10** (if the names of user-defined01 through user-defined10 are modified, the new names are used). Among these protocols names, **unknown-tcp** identifies unknown TCP protocol packets, **unknown-udp** identifies unknown UDP protocol packets, and **unknown-others** identifies other unknown IP protocol packets. **user-defined01**, **user-defined02**,..., **user-defined10** are user-defined protocol names. These protocols are not effective unless port numbers are assigned for them with the **dar protocol** command.

### Examples

# Define a criterion to match the SMTP protocol for class **smtp-class**.

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

```
[Sysname] traffic classifier smtp-class
```

```
[Sysname-classifier-smtp-class] if-match protocol smtp
```

## if-match protocol http

Use **if-match protocol http** to define a match criterion for the HTTP protocol.

Use **undo if-match protocol http** to delete a HTTP protocol match criterion.

## Syntax

```
if-match [ not ] protocol http [ url url-string | host hostname-string | mime mime-type ]  
undo if-match [ not ] protocol http [ url url-string | host hostname-string | mime mime-type ]
```

## Default

No HTTP protocol match criterion is configured.

## Views

Class view

## Default command level

2: System level

## Parameters

**not:** Specifies to match packets not conforming to the specified criterion.

**url** *url-string*: Matches a URL string of 1 to 32 characters. The URL string supports simple wildcards.

**host** *hostname-string*: Matches a host name, a string of 1 to 32 characters. The host name string supports simple wildcards.

**mime:** *mime-type*: Matches a MIME type, a string of 1 to 32 characters. The MIME type supports simple wildcards.

**Table 42 Simple wildcard match rules**

Wildcard	Description
*	Matches any number of characters, which can be numbers, upper/lower case letters, hyphens, and underscores.
#	Matches one character, which can be a number, an upper/lower case letter, a hyphen, or an underscore.
	Matches either the string on the right or the string on the left.
( )	Matches either the string on the right or the string on the left within the specified range. For example, "index.(htm jsp)" is to match both index htm and index jsp.
[ ]	Matches any character specified in the square brackets, or matches a special character, including *, #, [, (,  , and ). For example, "[0-9]" is to match any number, "[*]" is to match *, and "[[]]" is to match [.

## Examples

# Define a criterion to match HTTP packets with the host name **\*.abc.com** for class **http-class**.

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

```
[Sysname] traffic classifier http-class
```

```
[Sysname-classifier-http-class] if-match protocol http host *.abc.com
```

## if-match protocol rtp

Use **if-match protocol rtp** to define an RTP protocol match criterion.

Use **undo if-match protocol rtp** to delete an RTP protocol match criterion.

## Syntax

```
if-match [ not ] protocol rtp [ payload-type { audio | video | payload-string &<1-16> } * ]  
undo if-match [ not ] protocol rtp [ payload-type { audio | video | payload-string&<1-16> } * ]
```



## Default

No RTP protocol match criterion is configured.

## Views

Class view

## Default command level

2: System level

## Parameters

**not**: Specifies to match packets not conforming to the specified criterion.

**payload-type**: Matches a payload type.

**audio**: Matches the audio RTP payload type.

**video**: Matches the video RTP payload type.

*payload-string*: Matches a list of RTP payload types. The value range for this argument is 0 to 127. &<1-16> means that you can specify up to 16 payload types.

## Usage guidelines

If no payload type is specified, all the RTP packets are matched.

## Examples

# Match RTP video packets for the class **rtp-class1**.

```
<Sysname> system-view
[Sysname] traffic classifier rtp-class1
[Sysname-classifier-rtp-class1] if-match protocol rtp payload-type video
```

# Match RTP packets with the payload type as 0, 1, 4, 5, 6, 10, or 64 for class **rtp-class2**.

```
<Sysname> system-view
[Sysname] traffic classifier rtp-class2
[Sysname-classifier-rtp-class2] if-match protocol rtp payload-type 0 1 4 5 6 10 64
```

# protocol

Use **protocol** to add the specified protocol to the current protocol group.

Use **undo protocol** to delete the specified protocol from the protocol group.

## Syntax

**protocol** *protocol-name*

**undo protocol** *protocol-name*

## Default

No protocol exists in a protocol group.

## Views

Protocol group view

## Default command level

2: System level

## Parameters

*protocol-name*: Protocol name, a string of 1 to 31 characters.

## Usage guidelines

Only the protocols included in the signature file can be added to a protocol group. If an existing protocol in the protocol group is not included in the signature file to be loaded, the protocol is removed from the protocol group automatically when the new signature file is loaded.

## Examples

```
# Add protocol MSN to protocol group 1.
<Sysname> system-view
[Sysname] dar protocol-group 1
[Sysname-protocol-group-1] protocol msn
```

# reset dar protocol-statistic

Use **reset dar protocol-statistic** to clear the DAR protocol statistics.

## Syntax

```
reset dar protocol-statistic { { { p2p | protocol protocol-name } | interface interface-type interface-number } * | all }
```

## Views

User view

## Default command level

1: Monitor level

## Parameters

**p2p**: Clears P2P traffic statistics.

**protocol** *protocol-name*: Clears the statistics of a protocol. The range for the *protocol-name* argument is the same as that in the **if-match protocol** command.

*interface-type interface-number*: Specifies an interface by its type and number.

**all**: Clears the statistics of all protocols.

## Examples

```
# Clear the FTP statistics of Ethernet 1/1.
<Sysname> reset dar protocol-statistic protocol ftp interface ethernet 1/1

# Clear the statistics of all the protocols.
<Sysname> reset dar protocol-statistic all
```

# reset dar session

Use **reset dar session** to clear the information of all the sessions.

## Syntax

```
reset dar session
```

## Views

User view

## Default command level

2: System level

## Examples

```
# Clear the information of all the sessions.
```

<Sysname> reset dar session

# FR QoS configuration commands

FR QoS is not available on the following routers:

- MSR800.
- MSR 900.
- MSR900-E.
- MSR 930 except for MSR 930-SA.

## apply policy outbound

Use **apply policy outbound** to apply a QoS policy.

Use **undo apply policy outbound** to cancel the application.

### Syntax

**apply policy** *policy-name* **outbound**

**undo apply policy outbound**

### Views

FR class view

### Default command level

2: System level

### Parameters

*policy-name*: Name of the applied policy, a string of 1 to 31 characters.

### Examples

# Define a class **class1**.

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

# Define a traffic behavior **behavior1**.

```
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] queue af bandwidth 56
[Sysname-behavior-behavior1] quit
```

# Define a policy **policy1**, and associate **class1** with **behavior1** in **policy1**.

```
[Sysname] qos policy policy1
[Sysname-qospolicy-policy1] classifier class1 behavior behavior1
[Sysname-qospolicy-policy1] quit
```

# Apply **policy1** to the FR class **test1**.

```
[Sysname] fr class test1
[Sysname-fr-class-test1] apply policy policy1 outbound
```

## cbs

Use **cbs** to set the CBS for the FR PVCs.

Use **undo cbs** to restore the default.

## Syntax

**cbs** [ **inbound** | **outbound** ] *committed-burst-size*

**undo cbs** [ **inbound** | **outbound** ]

## Views

FR class view

## Default command level

2: System level

## Parameters

**inbound**: Sets the CBS for the incoming packets. This argument is available when FR traffic policing is enabled on interfaces.

**outbound**: Sets the CBS for the outgoing packets. This argument is available when FR traffic policing is enabled on interfaces.

*committed-burst-size*: CBS in the range of 300 to 16000000 bits. The default value of CBS is 56000 bits.

## Usage guidelines

If the packet direction is not specified, the CBS is effective for both incoming packets and outgoing packets.

CBS is the traffic that an FR network is committed to send in an interval of Tc. If no congestion occurs, the FR network guarantees the traffic of CBS is sent.

## Examples

# Set CBS to 64000 bits for both incoming packets and outgoing packets of the FR class **test1**.

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

```
[Sysname] fr class test1
```

```
[Sysname-fr-class-test1] cbs 64000
```

## Related commands

- **ebs**
- **cir allow**
- **cir**

## cir

Use **cir** to set the Committed Information Rate (CIR) for FR PVCs.

Use **undo cir** to restore the default.

## Syntax

**cir** *committed-information-rate*

**undo cir**

## Views

FR class view

## Default command level

2: System level

## Parameters

*committed-information-rate*: Minimum CIR in the range of 1000 to 45000000 bps. The CIR is 56000 bps by default.

## Usage guidelines

CIR is the minimum transmit rate that a PVC can provide. When congestion occurs to the network, the user can still send data at the rate of CIR.

When congestion occurs to the network, DCE sends packets with the BECN flag bit 1 to DTE. On receiving the packets, DTE gradually decreases the transmit rate of PVCs from CIR ALLOW to CIR. If DTE receives no packets with the BECN flag bit 1 within 125 ms, DTE restores the transmit rate of PVCs to CIR ALLOW.

CIR must be equal to or lower than CIR ALLOW.

## Examples

# Set the minimum CIR to 32000 bps for the FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir 32000
```

## Related commands

- **cbs**
- **ebs**
- **cir allow**

# cir allow

Use **cir allow** to set the CIR ALLOW for FR PVCs.

Use **undo cir allow** to restore the default.

## Syntax

**cir allow** [ **inbound** | **outbound** ] *committed-information-rate*

**undo cir allow** [ **inbound** | **outbound** ]

## Views

FR class view

## Default command level

2: System level

## Parameters

**inbound**: Sets the CIR ALLOW for the incoming packets. This argument is available when FR traffic policing is enabled on interfaces.

**outbound**: Sets the CIR ALLOW for the outgoing packets. This argument is available when FR traffic policing is enabled on interfaces.

*committed-information-rate*: CIR ALLOW in the range of 1000 to 45000000 bps. The CIR ALLOW is 56000 bps by default.

## Usage guidelines

CIR ALLOW is the transmit rate that an FR PVC can provide when no congestion occurs to the network.

If the packet direction is not specified, the CIR ALLOW is effective for both incoming packets and outgoing packets.

CIR ALLOW must be greater than CIR.

## Examples

```
# Set CIR ALLOW to 64000 bps for the FR class test1.
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir allow 64000
```

## Related commands

- **cbs**
- **ebs**
- **cir**

# congestion-threshold

Use **congestion-threshold** to enable congestion management for FR PVCs.

Use **undo congestion-threshold** to disable the congestion management function.

## Syntax

```
congestion-threshold { de | ecn } queue-percentage
undo congestion-threshold { de | ecn }
```

## Default

The congestion management function is disabled for FR PVCs.

## Views

FR class view

## Default command level

2: System level

## Parameters

**de**: Drops FR packets with the DE flag bit 1 when congestion occurs.

**ecn**: Sets the BECN flag bits and FECN flag bits of FR packets to 1 when congestion occurs.

*queue-percentage*: Threshold for network congestion, expressed in the usage percentage of PVC queues (the percentage of the current PVC queue length to the total queue length). The value range for this argument is 1 to 100, and the default is 7.

## Usage guidelines

When the percentage of the current PVC queue length to the total PVC queue length exceeds the set threshold for congestion, congestion occurs to the PVCs. The congestion management function is performed for packets of PVCs as follows: dropping the FR packets with the DE flag bit 1, and setting the BECN flag bits and FECN flag bits of FR packets to 1.

## Examples

```
# Create an FR class test1 and configure the FR network to drop FR packets with the DE flag bit 1
when the current PVC queue length uses more than 80% of the total PVC queue length.
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] congestion-threshold de 80
```

## Related commands

**fr congestion-threshold**

## cq

Use **cq** to apply CQ to the FR PVCs.

Use **undo cq** to restore the default queuing (FIFO queuing).

### Syntax

**cq** **cql** *cql-index*

**undo cq**

### Default

PVCs use FIFO queuing.

### Views

FR class view

### Default command level

2: System level

### Parameters

**cql** *cql-index*: CQL index in the range of 1 to 16.

### Usage guidelines

If this command is executed multiple times for an FR class, the new configuration overwrites the previous one.

### Examples

# Apply CQL 10 to the FR class **test1**.

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

```
[Sysname] fr class test1
```

```
[Sysname-fr-class-test1] cq cql 10
```

### Related commands

- **wfq**
- **pq**
- **fr pvc-pq**

## display fr class-map

Use **display fr class-map** to display the mapping relationship between FR classes and interfaces (including the DLCIs of an interface, subinterfaces of an interface, and the DLCIs of subinterfaces).

### Syntax

**display fr class-map** { **fr-class** *class-name* | **interface** *interface-type interface-number* } [ | { **begin** | **exclude** | **include** } *regular-expression* ]

### Views

Any view

### Default command level

1: Monitor level



## Parameters

**fr-class** *class-name*: Displays the mapping relationship between the specified FR class and interfaces. The *class-name* argument is the name of an FR class, and is a string of 1 to 30 characters.

**interface** *interface-type interface-number*: Displays the mapping relationship between FR classes and the specified interface. The *interface-type interface-number* argument specifies an interface by its type and number.

**|**: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Usage guidelines

For this command, you can specify an FR class name, or specify a primary interface. However, you cannot specify a subinterface.

## Examples

# Display the mapping relationship between Serial 2/0 and FR classes.

```
<Sysname> display fr class-map interface serial 2/0
Serial2/0
  fr-class ts1
Serial2/0.1
  fr-class ts2
  fr dlci 100   Serial2/0
    fr-class ts
  fr dlci 222   Serial2/0.1
    fr-class ts
```

**Table 43 Command output**

Field	Description
Serial2/0 fr-class ts1	FR interface and the FR class corresponding to the FR interface.
Serial2/0.1 fr-class ts2	FR subinterface and the FR class corresponding to the FR subinterface.
fr dlci 100   Serial2/0 fr-class ts	PVC on the FR interface and the FR class corresponding to the PVC.
fr dlci 222   Serial2/0.1 fr-class ts	PVC on the FR subinterface and the FR class corresponding to the PVC.

# Display the mapping relationship between FR class **ts** and interfaces.

```
<Sysname> display fr class-map fr-class ts
  fr dlci 100   Serial2/0
    fr-class ts
  fr dlci 222   Serial2/0.1
    fr-class ts
```

# display fr fragment-info

Use **display fr fragment-info** to display the FR fragmentation information.

## Syntax

```
display fr fragment-info [ interface interface-type interface-number ] [ dlci-number ] [ | { begin | exclude | include } regular-expression ]
```

## Views

Any view

## Default command level

1: Monitor level

## Parameters

**interface** *interface-type interface-number*: Displays the FR fragmentation information about an interface specified by its type and number.

*dlci-number*: Displays the FR fragmentation information about an DLCI specified by its number in the range of 16 to 1007. With this argument specified, this command displays the detailed fragmentation information.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include**: Displays all lines that match the specified regular expression.

*regular-expression*: Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Examples

# Display the FR fragmentation information about FR fragments on all interfaces.

```
<Sysname> display fr fragment-info
interface Serial2/0:1:
dlci    type                size      in/out/drop
200     FRF12(End to End)   80        0/0/0
```

**Table 44 Command output**

Field	Description
dlci	DLCI number.
type	Fragment type: <b>FRF.12</b> , <b>FRF.11 Annex C</b> , or <b>Motorola fragment</b> .
size	Fragment size in bytes.
in/out/drop	Number of incoming/outgoing/dropped packets.

# Display the information about FR fragments on Serial 2/0:1.

```
<Sysname> display fr fragment-info interface serial 2/0:1 200
Type : FRF12(End to End)
Size : 80
Data-level: 200    Voice-level: 0
Pre-fragment:
    out pkts : 0          out bytes :0
Fragmented:
```

```

    in pkts : 0          out pkts : 0
    in bytes: 0          out bytes: 0
Assembled:
    in pkts : 0          in bytes :0
Dropped   :
    in pkts : 0          out pkts :0
    in bytes: 0          out bytes: 0
Out-of-sequence pkts: 0

```

**Table 45 Command output**

Field	Description
Type	Fragment type: <b>FRF.12</b> , <b>FRF.11 Annex C</b> , or <b>Motorola fragment</b> .
Size	Fragment size in bytes.
Data-level	Fragment size when voice service is not enabled.
Voice-level	Fragment size when voice service is enabled.
Pre-fragment	Number of packets to be fragmented.
Fragmented	Number of fragmented packets.
Assembled	Number of assembled fragments.
Dropped	Number of dropped fragments.
Out-of-sequence pkts	Number of out-of-sequence fragments.
out pkts / out bytes	Number of outgoing packets and bytes of outgoing packets.
in pkts / in bytes	Number of incoming packets and bytes of incoming packets.

## Related commands

**fragment**

## display fr switch-table

Use **display fr switch-table** to display the status and configuration of the specified FR switching PVCs.

## Syntax

```
display fr switch-table { all | name switch-name | interface interface-type interface-number } [ |
{ begin | exclude | include } regular-expression ]
```

## Views

Any view

## Default command level

1: Monitor level

## Parameters

**all**: Displays the information about all the switching PVC.

**name** *switch-name*: Displays the information about the switching PVC specified by the *switch-name* argument, which is a string of 1 to 256 characters.

**interface** *interface-type interface-number*. Displays the information about switching PVCs on the interface specified by the *interface-type interface-number* argument.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin:** Displays the first line that matches the specified regular expression and all lines that follow.

**exclude:** Displays all lines that do not match the specified regular expression.

**include:** Displays all lines that match the specified regular expression.

*regular-expression:* Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Examples

# Display the information about all the FR switching PVCs.

```
<Sysname> display fr switch-table all
```

Switch-Name	Interface	DLCI	Interface	DLCI	State
test	MFR0	100	MFR1	101	UP

**Table 46 Command output**

Field	Description
Switch-Name	Name of a switching PVC.
Interface	The first interface represents a local interface, and the second interface represents a peer interface.
DLCI	The first DLCI represents a local DLCI, and the second DLCI represents a remote DLCI.
State	Connection state of the frame relay switching link.

## Related commands

**fr switch**

# display qos policy interface

Use **display qos policy interface** to display the information about CBQ applied to a specific interface.

## Syntax

```
display qos policy interface [ interface-type interface-number [ dlci dlci-number ] | inbound | outbound ] [ [ { begin | exclude | include } regular-expression ]
```

## Views

Any view

## Default command level

1: Monitor level

## Parameters

*interface-type interface-number:* Specifies an interface by its type and number.

**dlci** *dlci-number:* Displays information about CBQ applied to a DLCI specified by the *dlci-number* argument, which is in the range of 16 to 1007.

**inbound:** Displays the information about CBQ applied in the inbound direction.

**outbound:** Displays the information about CBQ applied in the outbound direction.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin:** Displays the first line that matches the specified regular expression and all lines that follow.

**exclude:** Displays all lines that do not match the specified regular expression.

**include:** Displays all lines that match the specified regular expression.

**regular-expression:** Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Examples

# Display the information about CBQ applied to DLCI 25 of MFR 1.

```
<Sysname> display qos policy interface mfr 1
```

Interface: MFR1

Direction: Outbound

Policy: policy1

Classifier: default-class

Matched : 0(Packets) 0(Bytes)

5-minute statistics:

Forwarded: 0/0 (pps/bps)

Dropped : 0/0 (pps/bps)

Rule(s) : If-match any

Behavior:

Default Queue:

Flow Based Weighted Fair Queueing

Max number of hashed queues: 256

Matched : 0/0 (Packets/Bytes)

Enqueued : 0/0 (Packets/Bytes)

Discarded: 0/0 (Packets/Bytes)

Discard Method: Tail

Classifier: classifier1

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 2001

Behavior:

Assured Forwarding:

Bandwidth 10 (Kbps)

Matched : 0/0 (Packets/Bytes)

Enqueued : 0/0 (Packets/Bytes)

Discarded: 0/0 (Packets/Bytes)

**Table 47 Command output**

Field	Description
Interface	Interface with CBQ applied.
Direction	Direction in which the policy is applied to the interface.
Policy	Name of the policy applied to the interface.
Classifier	Classification rules in the policy and the configuration information.

Field	Description
Matched	Number of packets matching the classification rules.
5-minute statistics	Traffic rate statistics collected in the last 5 minutes. If the number of QoS policies for which traffic rate statistics are collected exceeds 1000, or the number of classes for which traffic rate statistics are collected exceeds 10000, <b>none</b> is displayed.
Forwarded	Average rate of successfully forwarded criteria-matching packets during the statistics collecting interval.
Dropped	Average rate of dropped criteria-matching packets during the statistics collecting interval.
Operator	Logical relationship among multiple classification rules in a class.
Rule(s)	Match rules of a class.
Behavior	Name of the traffic behavior in the policy and the configuration information.
Default Queue	Default queuing mechanism.
Flow Based Weighted Fair Queueing	Flow-based WFQ.
Max number of hashed queues	Maximum number of hashed queues.
Matched	Number of matched packets and the bytes of these packets.
Enqueued	Number of enqueued packets and bytes of these packets.
Discarded	Number of discarded packets and bytes of these packets.
Discard Method	Drop method: tail drop, IP precedence-based WRED, or DSCP-based WRED.
Assured Forwarding	Information about AF queues.
Bandwidth	Minimum bandwidth guaranteed for AF queues.

## display qos pvc-pq interface

Use **display qos pvc-pq interface** to display information about PVC Priority Queuing (PQ) on a specific FR interface.

### Syntax

**display qos pvc-pq interface** [ *interface-type interface-number* ] [ | { **begin** | **exclude** | **include** } *regular-expression* ]

### Views

Any view

### Default command level

1: Monitor level

### Parameters

*interface-type interface-number*: Specifies an interface by its type and number.

|: Filters command output by specifying a regular expression. For more information about regular expressions, see *Fundamentals Configuration Guide*.

**begin**: Displays the first line that matches the specified regular expression and all lines that follow.

**exclude**: Displays all lines that do not match the specified regular expression.

**include:** Displays all lines that match the specified regular expression.

*regular-expression:* Specifies a regular expression, a case-sensitive string of 1 to 256 characters.

## Examples

# Display information about PVC PQ on Serial 2/0.

```
<Sysname> display qos pvc-pq interface serial 2/0
Interface: Serial2/0
Output queue : (Urgent queuing : Size/Length/Discards)  0/100/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (PVC-PQ queuing : Size/Length/Discards)
Top:  0/20/0      Middle:  0/40/0      Normal:  0/60/0      Bottom:  0/80/0
```

**Table 48 Command output**

Field	Description
Interface	FR interface.
Output queue : (Urgent queuing : Size/Length/Discards)	Information about an output queue of urgent queuing: <ul style="list-style-type: none"><li>• Number of packets in the queue.</li><li>• Length of the queue.</li><li>• Number of dropped packets in the queue.</li></ul>
Output queue : (PVC-PQ queuing: Size/Length/Discards)	Information about an output queue of PVC PQ queuing: <ul style="list-style-type: none"><li>• Number of packets in the queue.</li><li>• Length of the queue.</li><li>• Number of dropped packets in the queue.</li></ul>
Top	Information about the output queue of the top queue.
Middle	Information about the output queue of the middle queue.
Normal	Information about the output queue of the normal queue.
Bottom	Information about the output queue of the bottom queue.

## ebs

Use **ebs** to set the EBS for the FR PVCs.

Use **undo ebs** to restore the default.

## Syntax

**ebs** [ **inbound** | **outbound** ] *excess-burst-size*

**undo ebs** [ **inbound** | **outbound** ]

## Views

FR class view

## Default command level

2: System level

## Parameters

**inbound:** Sets the EBS for the incoming packets. This argument is available when FR traffic policing is enabled on interfaces.

**outbound:** Sets the EBS for the outgoing packets. This argument is available when FR traffic policing is enabled on interfaces.

*excess-burst-size*: EBS in the range of 0 to 16000000 bits. The default value of EBS is 0 bits.

## Usage guidelines

EBS is the maximum amount of traffic, except CBS, that can be transmitted in the interval of Tc. When congestion occurs to the network, the excess traffic is dropped preferentially.

If neither the **inbound** keyword nor the **outbound** keyword is specified for this command, the EBS is effective for both incoming packets and outgoing packets.

## Examples

```
# Set the EBS to 32000 bits for the FR class test1.
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] ebs 32000
```

## Related commands

- **cbs**
- **cir allow**
- **cir**

# fifo queue-length

Use **fifo queue-length** to set the FIFO queue length for FR PVCs.

Use **undo fifo queue-length** to restore the default.

## Syntax

```
fifo queue-length queue-length
undo fifo queue-length
```

## Views

FR class view

## Default command level

2: System level

## Parameters

*queue-length*: FIFO queue length, which specifies the maximum number of packets that a FIFO queue can hold. The value range for this argument is 1 to 1024, and the default is 40.

## Usage guidelines

Set the FIFO queue length for a DLCI if the device functions as the DCE and an FR class is applied to the DLCI.

## Examples

```
# Set the FIFO queue length to 80 for the FR class test1.
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fifo queue-length 80
```

## Related commands

**fr class**



## fr class

Use **fr class** to create an FR class and enter FR class view.

Use **undo fr class** to remove the specified FR class.

### Syntax

**fr class** *class-name*

**undo fr class** *class-name*

### Default

No FR class is created.

### Views

System view

### Default command level

2: System level

### Parameters

*class-name*: Name of an FR class, a string of 1 to 30 characters.

### Usage guidelines

The FR class parameters do not take effect until you associate the FR class with an interface or PVC and enable the FR QoS function on the interface.

With an FR class removed, all the associations associating this FR class with an interface or a DLCI are released.

### Examples

```
# Create an FR class test1.  
<Sysname> system-view  
[Sysname] fr class test1  
[Sysname-fr-class-test1]
```

### Related commands

**fr-class**

## fr congestion-threshold

Use **fr congestion-threshold** to enable congestion management for an FR interface.

Use **undo fr congestion-threshold** to disable the congestion management function.

### Syntax

**fr congestion-threshold** { **de** | **ecn** } *queue-percentage*

**undo fr congestion-threshold** { **de** | **ecn** }

### Default

The congestion management function is disabled for FR interfaces.

### Views

FR interface view, MFR interface view

### Default command level

2: System level

## Parameters

**de:** Drops FR packets with the DE flag bit 1 when congestion occurs.

**ecn:** Sets the BECN flag bits and FECN flag bits of FR packets to 1 when congestion occurs.

*queue-percentage:* Congestion threshold, expressed in the interface queue utilization rate, which means the percentage of the current interface queue length to the total queue length. The value range for this argument is 1 to 100, and the default is 100.

## Usage guidelines

This command is similar to the **congestion-threshold** command. The difference between the two commands lies in that: this command is applicable to FR interfaces and the **congestion-threshold** command is applicable to FR PVCs.

This command is applicable to only FR DCE interfaces and NNI interfaces.

## Examples

# Configure Serial 2/0 to drop FR packets with the DE flag bit 1 when the current interface queues uses more than 80% of the total queue length.

```
<Sysname> system-view
[Sysname]interface serial 2/0
[Sysname-Serial2/0] fr interface-type dce
[Sysname-Serial2/0] fr congestion-threshold de 80
```

## Related commands

**congestion-threshold**

## fr de del

Use **fr de del** to apply a specific DE rule list to the specified FR PVC.

Use **undo fr de del** to remove the DE rule list from the specified FR PVC.

## Syntax

**fr de del** *list-number* **dlci** *dlci-number*

**undo fr de del** *list-number* **dlci** *dlci-number*

## Default

No DE rule list is applied to FR PVCs.

## Views

FR interface (primary interface or subinterface) view, MFR interface view

## Default command level

2: System level

## Parameters

*list-number:* DE rule list number in the range of 1 to 10.

*dlci-number:* FR PVC number in the range of 16 to 1007.

## Usage guidelines

Configured in primary interface view, this command applies a specific DE rule list only to the FR PVC of the primary interface. Configured in subinterface view, this command applies a specific DE rule list only to the subinterface.

With a DE rule list applied to an FR PVC, the DE flag bits of packets matching the DE rule list are set to 1.

## Examples

```
# Apply DE rule list 3 to DLCI 100 of Serial 2/0.
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr dlci 100
[Sysname-Serial2/0] fr de del 3 dlci 100
```

## Related commands

- **fr del inbound-interface**
- **fr del protocol**

# fr del inbound-interface

Use **fr del inbound-interface** to configure an interface-based DE rule list. Before the incoming packets of the specific interfaces are to be forwarded as FR packets, the DE flag bits of these packets are set to 1.

Use **undo fr del inbound-interface** to remove the specific DE rule from the DE rule list.

## Syntax

```
fr del list-number inbound-interface interface-type interface-number
undo fr del list-number inbound-interface interface-type interface-number
```

## Default

No DE rule list is created.

## Views

System view

## Default command level

2: System level

## Parameters

*list-number*: DE rule list number in the range of 1 to 10.

*interface-type interface-number*: Specifies an interface by its type and number.

## Usage guidelines

Execute this command multiple times to add new rules to a DE rule list. Up to 100 rules can be configured for a DE rule list. Executed once, the **undo fr del inbound-interface** command removes only one DE rule. To remove a DE rule list, make sure that all the DE rules in the DE rule list are removed.

## Examples

# Add a rule to DE rule list 1. The rule defines that: before the incoming packets of Serial 2/0 are to be forwarded as FR packets, the DE flag bits of these packets are set to 1.

```
<Sysname> system-view
[Sysname] fr del 1 inbound-interface serial 2/0
```

## Related commands

- **fr de del**
- **fr del protocol**

# fr del protocol

Use **fr del protocol ip** to configure an IP protocol-based DE rule list. The DE flag bits of FR packets encapsulated with the IP packets matching the specific rule are set to 1.

Use **undo fr del protocol ip** to remove the specific DE rules from the DE rule list.

## Syntax

**fr del** *list-number* **protocol ip** [ **acl** *acl-number* | **fragments** | **greater-than** *bytes* | **less-than** *bytes* | **tcp ports** | **udp ports** ]

**undo fr del** *list-number* **protocol ip** [ **fragments** | **acl** *acl-number* | **less-than** *bytes* | **greater-than** *bytes* | **tcp ports** | **udp ports** ]

## Default

No DE rule list is created.

## Views

System view

## Default command level

2: System level

## Parameters

*list-number*: DE rule list number in the range of 1 to 10.

**protocol ip**: IP protocol.

**acl** *acl-number*: IP packets matching the ACL identified by the *acl-number* argument, which is in the range of 2000 to 3999.

**fragments**: All the fragmented IP packets.

**greater-than** *bytes*: IP packets with the length greater than the *bytes* argument. The value range for the *bytes* argument is 0 to 65535.

**less-than** *bytes*: IP packets with the length less than the *bytes* argument. The value range for the *bytes* argument is 0 to 65535.

**tcp ports**: IP packets with the source or destination TCP port number as the *ports* argument. The value range for the *ports* argument is 0 to 65535. The *ports* argument can be either a port name or the associated port number.

**udp ports**: IP packets with the source or destination UDP port number as the *ports* argument. The value range for the *ports* argument is 0 to 65535. The *ports* argument can be either a port name or the associated port number.

## Usage guidelines

Execute this command multiple times to add new rules to a DE rule list. Up to 100 rules can be configured for a DE rule list. Executed once, the **undo fr del protocol ip** command removes only one DE rule. To remove a DE rule list, make sure that all the DE rules in the DE rule list are removed.

If you execute this command with no optional parameters specified, the DE rule list is created for all the IP packets.

## Examples

# Add a rule that sets the DE flag bits of all the FR packets encapsulated with IP packets to 1 to DE rule list 1.

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

```
[Sysname] fr del 1 protocol ip
```

## Related commands

- **fr de del**
- **fr del inbound-interface**

## fr pvc-pq

Use **fr pvc-pq** to apply PVC PQ to the queues of an FR interface and set the length (which specifies the maximum number of packets that a queue can hold) for each queue.

Use **undo fr pvc-pq** to restore the default queuing (FIFO queuing) for the queues of an FR interface.

## Syntax

**fr pvc-pq** [ *top-limit middle-limit normal-limit bottom-limit* ]

**undo fr pvc-pq**

## Default

An FR interface adopts FIFO queuing.

## Views

FR interface view, MFR interface view

## Default command level

2: System level

## Parameters

*high-limit*: Top queue length in the number of packets, in the range of 1 to 1024. This argument is 20 by default.

*middle-limit*: Middle queue length in the number of packets, in the range of 1 to 1024. This argument is 40 by default.

*normal-limit*: Normal queue length in the number of packets, in the range of 1 to 1024. This argument is 60 by default.

*bottom-limit*: Bottom queue length in the number of packets, in the range of 1 to 1024. This argument is 80 by default.

## Usage guidelines

With FR traffic policing enabled on an interface, only FIFO queuing or PVC PQ is available.

PVC PQ is a new queuing mechanism for FR classes. Similar to PQ, PVC PQ includes four queue types: top, middle, normal, bottom, in the descending priority order. The queue to which a DLCI is assigned is configured in an FR class. When congestion occurs on an interface, packets from different DLCIs are assigned to different PVC PQ queues. When packets in the four queues are scheduled, packets are scheduled in the descending order of queue priority.

## Examples

# Apply PVC PQ to Serial 2/0.

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

```
[Sysname] interface serial 2/0
```

```
[Sysname-Serial2/0] fr pvc-pq
```

## Related commands

**pvc-pq**

## fr traffic-policing

Use **fr traffic-policing** to enable FR traffic policing.

Use **undo fr traffic-policing** to disable FR traffic policing.

### Syntax

**fr traffic-policing**

**undo fr traffic-policing**

### Views

FR interface view, MFR interface view

### Default command level

2: System level

### Usage guidelines

FR traffic policing is applicable only to the ingress interfaces on the DCE side of an FR network.

Before enabling traffic policing for the incoming interfaces, make sure that FR switching is enabled on the DCE by using the **fr switching** command. For more information about the **fr switching** command, see *Layer 2—WAN Command Reference*.

### Examples

```
# Enable traffic policing on Serial 2/0.  
<Sysname> system-view  
[Sysname] interface serial 2/0  
[Sysname-Serial2/0] fr traffic-policing
```

### Related commands

**fr class**

## fr traffic-shaping

Use **fr traffic-shaping** to enable FRTS.

Use **undo fr traffic-shaping** to disable FRTS.

### Syntax

**fr traffic-shaping**

**undo fr traffic-shaping**

### Default

FRTS is disabled.

### Views

FR interface view, MFR interface view

### Default command level

2: System level

### Usage guidelines

FRTS is applied to the outgoing interfaces and are usually applied to the DCE of an FR network.

### Examples

```
# Enable FRTS on Serial 2/0.
```

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr traffic-shaping
```

### Related commands

- **fr class**
- **fr-class**
- **fr dlci** (*Layer 2—WAN Command Reference*)

## fragment

Use **fragment** to enable the packet fragmentation function (conforming to frame relay forum's FRF.12) for FR PVCs.

Use **undo fragment** to disable the packet fragmentation function.

### Syntax

```
fragment [ fragment-size ] [ data-level | voice-level ]
undo fragment [ data-level | voice-level ]
```

### Default

The packet fragmentation function is disabled for FR PVCs.

### Views

FR class view

### Default command level

2: System level

### Parameters

**fragment-size**: Fragment size in the range of 16 to 1600 bytes. This argument is 45 bytes by default.

**data-level**: Specifies the fragment size for data packets.

**voice-level**: Specifies the fragment size for voice packets.

### Usage guidelines

If neither **data-level** nor **voice-level** is specified, the fragment size is specified for data packets.

### Examples

# Enable the packet fragmentation function with the fragment size of 128 bytes for the FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fragment 128
```

### Related commands

**fr class**

## fr-class

Use **fr-class** to associate an FR class with the current FR PVC or FR interface.

Use **undo fr-class** to cancel the association.

## Syntax

**fr-class** *class-name*

**undo fr-class** *class-name*

## Default

No FR class is associated with an FR PVC or an FR interface.

## Views

FR DLCI view, FR interface view

## Default command level

2: System level

## Parameters

*class-name*: Name of an FR class, a string of 1 to 30 characters.

## Usage guidelines

Instead of removing an FR class, the **undo fr-class** command just cancels the association between the FR class and the current FR PVC or interface.

If the specified FR class does not exist, the **fr-class** command creates an FR class and then associates the FR class with the current FR PVC or FR interface. If the specified FR class exists, the **fr-class** command just associates the FR class with the current FR PVC or FR interface, without creating a new FR class.

For an interface associated with an FR class, all the PVCs on the interface inherit the FR QoS parameters in the FR class.

## Examples

# Associate the FR class **test1** with an FR PVC with DLCI 200.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr dlci 200
[Sysname-fr-dlci-Serial2/0-200] fr-class test1
```

## Related commands

- **fr class**
- **fr dlci** (*Layer 2—WAN Command Reference*)

## pq

Use **pq** to apply PQ to the FR PVCs.

Use **undo pq** to restore the default queuing (FIFO queuing).

## Syntax

**pq** *pql pql-index*

**undo pq**

## Default

FR PVCs adopt FIFO queuing.

## Views

FR class view



## Default command level

2: System level

## Parameters

*pql-index*: PQL index in the range of 1 to 16.

## Examples

```
# Apply PQL 10 to the FR class test1.
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] pq pql 10
```

## Related commands

- **cq**
- **wfq**
- **fr pvc-pq**

## pvc-pq

Use **pvc-pq** to assign packets from the FR PVC to a specific queue of PVC PQ.

Use **undo pvc-pq** to assign the packets from the FR PVC to the default queue of PVC PQ.

## Syntax

```
pvc-pq { bottom | middle | normal | top }
undo pvc-pq
```

## Default

Packets from the FR PVC are assigned to the normal queue.

## Views

FR class view

## Default command level

2: System level

## Parameters

**bottom**: Specifies the bottom queue.  
**middle**: Specifies the middle queue.  
**normal**: Specifies the normal queue.  
**top**: Specifies the top queue.

## Usage guidelines

PVC PQ queues include the top queue, the middle queue, the normal queue, and the bottom queue, in descending priority order.

The packets of a given PVC can only be assigned to a specific queue.

## Examples

```
# Assign packets from the PVCs associated with the FR class test1 to the top queue of PVC PQ.
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] pvc-pq top
```

## Related commands

**fr pvc-pq**

## rtpq

Use **rtpq** to configure and apply RTPQ in a FR class.

Use **undo rtpq** to cancel the RTPQ configuration in a FR class.

## Syntax

**rtpq start-port min-dest-port end-port max-dest-port bandwidth bandwidth [ cbs committed-burst-size ]**

**undo rtpq**

## Views

FR class view

## Default command level

2: System level

## Parameters

**start-port min-dest-port**: Lower threshold for destination UDP port numbers, in the range of 2000 to 65535.

**end-port max-dest-port**: Upper threshold for destination UDP port numbers, in the range of 2000 to 65535. The value of the *max-dest-port* argument cannot be smaller than that of the *min-dest-port* argument.

**bandwidth**: Specifies the RTP priority queue bandwidth in the range of 8 to 1000000 kbps.

**cbs committed-burst-size**: CBS in the range of 1500 to 2000000 bytes. The default is 55550 bytes.

## Usage guidelines

With the FR class configured with RTPQ applied to a PVC, an SP queue is established on the PVC, and the packets destined to the UDP ports within the port range specified in RTPQ are assigned to the RTP priority queue. When congestion occurs to the PVC, packets in the RTP priority queue are transmitted preferentially within the configured bandwidth. When no congestion occurs to the PVC, packets destination to the UDP ports within the specified range can be transmitted using the available bandwidth of the PVC. The UDP port range for VoIP is generally configured as 16384 to 37267.

## Examples

# Apply RTPQ to the FR class **test1** and set the RTP priority queue length to 20 kbps.

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

```
[Sysname] fr class test1
```

```
[Sysname-fr-class-test1] rtpq start-port 16383 end-port 16384 bandwidth 20
```

## traffic-shaping adaptation

Use **traffic-shaping adaptation** to enable FRTS adaptation.

Use **undo traffic-shaping adaptation** to disable this function.

## Syntax

**traffic-shaping adaptation { becn percentage | interface-congestion number }**

**undo traffic-shaping adaptation { becn | interface-congestion }**

## Default

FRTS adaptation is enabled for traffic with the BECN flag, and 25% of the total traffic is regulated every time.

## Views

FR class view

## Default command level

2: System level

## Parameters

**becn**: Regulates the traffic of packets with the BECN flag.

*percentage*: Percentage of the regulated traffic to the total traffic, in the range of 1 to 30. This argument is 25 by default.

**interface-congestion**: Performs traffic regulation according to the number of packets in the output queues on the interface.

*number*: Number of packets in the output queue of the interface, in the range of 1 to 40.

## Examples

# Enable FRTS adaptation to regulate the traffic of the FR packets with the BECN flag bit 1 and regulate 20% of the total traffic every time.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] traffic-shaping adaptation becn 20
```

## Related commands

- **fr traffic-shaping**
- **cir allow**
- **cir**

## wfq

Use **wfq** to apply WFQ to the FR PVC.

Use **undo wfq** to restore the default queuing (FIFO queuing) on the PVC.

## Syntax

**wfq [ congestive-discard-threshold [ dynamic-queues ] ]**

**undo wfq**

## Default

PVCs use FIFO queuing.

## Views

FR class view

## Default command level

2: System level

## Parameters

*congestive-discard-threshold*: Maximum number of packets that a WFQ queue can hold. If the number of packets exceeds the threshold, the newly arriving packets are dropped. The value range for this argument is 1 to 1024, and the default is 64.

*dynamic-queues*: Total number of WFQ queues, which can be 16, 32, 64, 128, 256, 512, 1024, 2048, or 4096. The default value of this argument is 256.

## Examples

# Apply WFQ to the FR class **test1**. Configure WFQ to provide 512 queues, each of which can hold up to 128 packets.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] wfq 128 512
```

## Related commands

- **cq**
- **pq**
- **fr pvc-pq**

# MPLS QoS commands

## if-match mpls-exp

Use **if-match mpls-exp** to define an MPLS EXP-based match criterion.

Use **undo if-match mpls-exp** to remove the match criterion.

### Syntax

**if-match** [ **not** ] **mpls-exp** *exp-value-list*

**undo if-match** [ **not** ] **mpls-exp** *exp-value-list*

### Views

Traffic class view

### Default command level

2: System level

### Parameters

**not**: Matches packets not conforming to the specified criterion.

*exp-value-list*: List of EXP values. Up to eight EXP values can be input. An EXP value is in the range of 0 to 7. If the same EXP value is specified multiple times, the system considers them as one. If a packet matches one of the defined MPLS EXP values, it matches the **if-match** clause.

### Examples

# Define a criterion to match packets with the MPLS EXP value 3 or 4.

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

```
[Sysname] traffic classifier database
```

```
[Sysname-classifier-database] if-match mpls-exp 3 4
```

## qos cql protocol mpls exp

Use **qos cql protocol mpls exp** to create a classification rule for an MPLS-based CQ list to assign MPLS packets with a specified EXP value to a specified queue.

Use **undo qos cql protocol mpls exp** to remove the classification rule.

### Syntax

**qos cql** *cql-index* **protocol mpls exp** *exp-value-list* **queue** *queue-number*

**undo qos cql** *cql-index* **protocol mpls exp** *exp-value-list*

### Views

System view

### Default command level

2: System level

### Parameters

*cql-index*: CQ list index in the range of 1 to 16.

**queue** *queue*: Specifies a custom queue by its number in the range of 0 to 16.

*exp-value-list*: List of EXP values in the range of 0 to 7. You can enter up to eight EXP values for this argument.

## Usage guidelines

This command can be executed multiple times with the same *cql-index* argument to create multiple classification rules for the CQ list.

The classification rules of a CQ list are matched in the order configured.

## Examples

# Create a classification rule for MPLS-based CQ list 10 to assign packets with the EXP value 1 to queue 2.

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

```
[Sysname] qos cql 10 protocol mpls exp 1 queue 2
```

## qos pql protocol mpls exp

Use **qos pql protocol mpls exp** to create a classification rule for an MPLS-based PQ list to assign MPLS packets with a specified EXP value to a specified queue.

Use **undo qos pql protocol mpls exp** to remove the classification rule.

## Syntax

**qos pql** *pql-index* **protocol mpls exp** *exp-value-list* **queue** { **bottom** | **middle** | **normal** | **top** }

**undo qos pql** *pql-index* **protocol mpls exp** *exp-value-list*

## Views

System view

## Default command level

2: System level

## Parameters

*pql-index*: PQ list index in the range of 1 to 16.

**top**, **middle**, **normal**, **bottom**: Corresponds to the four queues in PQ in the descending priority order.

*exp-value-list*: List of EXP values in the range of 0 to 7. You can enter up to eight EXP values for this argument.

## Usage guidelines

This command can be executed multiple times with the same *pql-index* argument to create multiple classification rules for a PQ list.

The classification rules of a PQ list are matched in the order configured.

## Examples

# Create a classification rule for MPLS-based PQ list 10 to assign MPLS packets with the EXP value 5 to the **top** queue.

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

```
[Sysname] qos pql 10 protocol mpls exp 5 queue top
```

## Related commands

**qos pql protocol**

## remark mpls-exp

Use **remark mpls-exp** to configure an EXP value marking action in a traffic behavior.

Use **undo remark mpls-exp** to delete the action.

## Syntax

**remark mpls-exp** *exp-value*

**undo remark mpls-exp**

## Views

Traffic behavior view

## Default command level

2: System level

## Parameters

*exp-value*: EXP value in the range of 0 to 7.

## Examples

# Set the EXP value to 0 for MPLS packets.

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

```
[Sysname] traffic behavior database
```

```
[Sysname-behavior-database] remark mpls-exp 0
```

# Index

## [A](#) [C](#) [D](#) [E](#) [F](#) [G](#) [I](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [W](#)

### A

- acl, [1](#)
- acl copy, [2](#)
- acl ipv6, [3](#)
- acl ipv6 copy, [4](#)
- acl ipv6 name, [5](#)
- acl name, [6](#)
- apply policy outbound, [139](#)

### C

- car, [44](#)
- cbs, [139](#)
- cir, [140](#)
- cir allow, [141](#)
- classifier behavior, [56](#)
- congestion-threshold, [142](#)
- cq, [143](#)

### D

- dar enable, [122](#)
- dar max-session-count, [122](#)
- dar p2p signature-file, [123](#)
- dar protocol, [123](#)
- dar protocol-group, [126](#)
- dar protocol-rename, [126](#)
- dar protocol-statistic, [127](#)
- description, [6](#)
- display acl, [7](#)
- display acl ipv6, [9](#)
- display dar information, [128](#)
- display dar protocol, [128](#)
- display dar protocol-rename, [131](#)
- display dar protocol-statistic, [132](#)
- display fr class-map, [143](#)
- display fr fragment-info, [145](#)
- display fr switch-table, [146](#)
- display qos car interface, [73](#)
- display qos carl, [74](#)
- display qos cbq interface, [99](#)
- display qos cq interface, [90](#)
- display qos cql, [91](#)
- display qos gts interface, [78](#)
- display qos lr interface, [80](#)
- display qos map-table, [66](#)
- display qos policy, [56](#)

- display qos policy interface, [147](#)
- display qos policy interface, [58](#)
- display qos pq interface, [83](#)
- display qos pql, [85](#)
- display qos pvc-pq interface, [149](#)
- display qos rtpq interface, [109](#)
- display qos trust interface, [70](#)
- display qos wfq interface, [97](#)
- display qos wred interface, [113](#)
- display qos wred table, [117](#)
- display time-range, [10](#)
- display traffic behavior, [46](#)
- display traffic classifier, [37](#)

### E

- ebs, [150](#)

### F

- fifo queue-length, [151](#)
- filter, [48](#)
- fr class, [152](#)
- fr congestion-threshold, [152](#)
- fr de del, [153](#)
- fr del inbound-interface, [154](#)
- fr del protocol, [155](#)
- fr pvc-pq, [156](#)
- fr traffic-policing, [157](#)
- fr traffic-shaping, [157](#)
- fragment, [158](#)
- fr-class, [158](#)

### G

- gts, [48](#)
- gts percent, [49](#)

### I

- if-match, [38](#)
- if-match mpls-exp, [164](#)
- if-match protocol, [134](#)
- if-match protocol http, [134](#)
- if-match protocol rtp, [135](#)
- import, [68](#)

### P

- pq, [159](#)
- protocol, [136](#)
- pvc-pq, [160](#)



## Q

qos apply policy (interface view, port group view, PVC view),[62](#)  
qos apply policy (user-profile view),[63](#)  
qos car (interface view, port group view),[75](#)  
qos carl,[76](#)  
qos cq,[92](#)  
qos cql default-queue,[93](#)  
qos cql inbound-interface,[93](#)  
qos cql protocol,[94](#)  
qos cql protocol mpls exp,[164](#)  
qos cql queue,[95](#)  
qos cql queue serving,[96](#)  
qos fifo queue-length,[83](#)  
qos flow-interval,[65](#)  
qos fragment pre-drop,[112](#)  
qos gts,[79](#)  
qos lr,[81](#)  
qos map-table,[68](#)  
qos max-bandwidth,[100](#)  
qos policy,[64](#)  
qos pq,[85](#)  
qos pql default-queue,[86](#)  
qos pql inbound-interface,[87](#)  
qos pql protocol,[88](#)  
qos pql protocol mpls exp,[165](#)  
qos pql queue,[89](#)  
qos pre-classify,[111](#)  
qos priority,[70](#)  
qos qmtoken,[111](#)  
qos reserved-bandwidth,[101](#)  
qos rtpq,[110](#)  
qos trust,[71](#)  
qos wfq,[98](#)  
qos wred apply,[120](#)  
qos wred dscp,[115](#)  
qos wred enable,[114](#)  
qos wred ip-precedence,[115](#)  
qos wred table,[118](#)  
qos wred weighting-constant,[116](#)  
queue,[119](#)  
queue af,[102](#)

queue ef,[103](#)  
queue wfq,[104](#)  
queue-length,[104](#)

## R

redirect,[50](#)  
remark dot1p,[51](#)  
remark dscp,[52](#)  
remark ip-precedence,[53](#)  
remark mpls-exp,[165](#)  
remark qos-local-id,[53](#)  
reset acl counter,[11](#)  
reset acl ipv6 counter,[12](#)  
reset dar protocol-statistic,[137](#)  
reset dar session,[137](#)  
rtpq,[161](#)  
rule (Ethernet frame header ACL view),[13](#)  
rule (IPv4 advanced ACL view),[14](#)  
rule (IPv4 basic ACL view),[18](#)  
rule (IPv6 advanced ACL view),[20](#)  
rule (IPv6 basic ACL view),[23](#)  
rule (simple ACL view),[25](#)  
rule (user-defined ACL view),[28](#)  
rule (WLAN ACL view),[29](#)  
rule comment,[30](#)  
rule remark,[31](#)

## S

step,[33](#)

## T

time-range,[34](#)  
traffic behavior,[54](#)  
traffic classifier,[43](#)  
traffic-policy,[55](#)  
traffic-shaping adaptation,[161](#)

## W

wfq,[162](#)  
wred,[105](#)  
wred dscp,[106](#)  
wred ip-precedence,[107](#)  
wred weighting-constant,[108](#)