



Hewlett Packard
Enterprise

HPE FlexFabric 5950 Switch Series

ACL and QoS Command Reference

Part number: 5200-2200a
Software version: Release 6123 and later
Document version: 6W101-20170120

© Copyright 2017 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use, or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

Microsoft® and Windows® are trademarks of the Microsoft group of companies.

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java and Oracle are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Contents

ACL commands	1
acl.....	1
acl copy	2
acl logging interval	3
acl trap interval.....	4
description.....	5
display acl	6
display packet-filter	7
display packet-filter statistics.....	8
display packet-filter statistics sum.....	11
display packet-filter verbose.....	12
display qos-acl resource	15
packet-filter.....	17
packet-filter default deny.....	18
packet-filter default hardware-count.....	19
reset acl counter.....	19
reset packet-filter statistics.....	20
rule (IPv4 advanced ACL view).....	21
rule (IPv4 basic ACL view).....	25
rule (IPv6 advanced ACL view).....	27
rule (IPv6 basic ACL view).....	32
rule (Layer 2 ACL view).....	33
rule comment	35
step	36
QoS policy commands	38
Traffic class commands	38
display traffic classifier	38
if-match	39
traffic classifier	44
Traffic behavior commands.....	45
accounting.....	45
car	46
display traffic behavior	47
filter	48
nest top-most	49
redirect	49
remark customer-vlan-id	50
remark dot1p	51
remark drop-precedence.....	52
remark dscp	52
remark ip-precedence	54
remark local-precedence.....	54
remark qos-local-id.....	55
remark service-vlan-id.....	55
traffic behavior.....	56
QoS policy commands	57
classifier behavior	57
control-plane	58
display qos policy	58
display qos policy control-plane	59
display qos policy control-plane pre-defined.....	60
display qos policy global	62
display qos policy interface	63
display qos policy user-profile.....	66
display qos vlan-policy	68
qos apply policy (interface view, control plane view)	69

qos apply policy (user profile view)	70
qos apply policy global	71
qos policy	71
qos vlan-policy	72
reset qos policy control-plane	73
reset qos policy global	73
reset qos vlan-policy	74
Priority mapping commands	75
Priority map commands	75
display qos map-table	75
import	76
qos map-table	76
Priority trust mode commands	77
display qos trust interface	77
qos trust	78
Port priority commands	78
qos priority	78
GTS and rate limit commands	80
GTS commands	80
display qos gts interface	80
qos gts	81
Rate limit commands	82
display qos lr interface	82
qos lr	82
Congestion management commands	84
Common commands	84
display qos queue interface	84
SP commands	85
display qos queue sp interface	85
qos sp	85
WRR commands	86
display qos queue wrr interface	86
qos wrr	87
qos wrr { byte-count weight }	88
qos wrr group sp	89
WFQ commands	90
display qos queue wfq interface	90
qos bandwidth queue	91
qos wfq	91
qos wfq { byte-count weight }	92
qos wfq group sp	93
Queue-based accounting commands	94
display qos queue-statistics interface outbound	94
Congestion avoidance commands	96
WRED commands	96
display qos wred interface	96
display qos wred table	96
qos wred apply	97
qos wred queue table	98
queue	99
queue ecn	100
queue weighting-constant	101
Aggregate CAR commands	102
car name	102
display qos car name	102
qos car (system view)	103
reset qos car name	105

Data buffer commands	106
buffer apply	106
buffer queue guaranteed.....	106
buffer queue shared.....	107
buffer total-shared.....	108
buffer usage threshold	109
burst-mode enable	109
display buffer.....	110
display buffer usage.....	111
display buffer usage interface	112
Time range commands	114
display time-range.....	114
time-range.....	114
Document conventions and icons	117
Conventions	117
Network topology icons.....	118
Support and other resources	119
Accessing Hewlett Packard Enterprise Support	119
Accessing updates.....	119
Websites	119
Customer self repair.....	120
Remote support.....	120
Documentation feedback	120
Index	121

ACL commands

acl

Use **acl** to create an ACL and enter its view, or enter the view of an existing ACL.

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

Syntax

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

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

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

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

Default

No ACLs exist.

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type. To specify the IPv4 ACL type, do not use this keyword.

basic: Specifies the basic ACL type.

advanced: Specifies the advanced ACL type.

mac: Specifies the Layer 2 ACL type.

number *acl-number*: Assigns a number to the ACL.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

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

match-order: Specifies the order in which ACL rules are compared against packets.

- **auto**: Compares ACL rules in depth-first order.
- **config**: Compares ACL rules in ascending order of rule ID. The rule with a smaller ID has a higher priority. If you do not specify a match order, the **config** order applies by default.

all: Specifies all ACLs of the specified type.

Usage guidelines

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

Matching packets are forwarded through slow forwarding if an ACL rule contains match criteria or has functions enabled in addition to the following match criteria and functions:

- Source and destination IP addresses.
- Source and destination ports.
- Transport layer protocol.

- ICMP or ICMPv6 message type, message code, and message name.
- VPN instance.
- Logging.
- Time range.

Slow forwarding requires packets to be sent to the control plane for forwarding entry calculation, which affects the device forwarding performance.

Examples

Create IPv4 basic ACL 2000 and enter its view.

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

Create IPv4 basic ACL **flow** and enter its view.

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

Create IPv4 advanced ACL 3000 and enter its view.

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

Create IPv6 basic ACL 2000 and enter its view.

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

Create IPv6 basic ACL **flow** and enter its view.

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

Create IPv6 advanced ACL **abc** and enter its view.

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

Create Layer 2 ACL 4000 and enter its view.

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

Create Layer 2 ACL **flow** and enter its view.

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

Related commands

display acl

acl copy

Use **acl copy** to create an ACL by copying an ACL that already exists.

Syntax

```
acl [ ipv6 | mac ] copy { source-acl-number | name source-acl-name } to { dest-acl-number | name dest-acl-name }
```

Views

System view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

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

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

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

dest-acl-number: Assigns a unique number to the new ACL. Available value ranges include:

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name dest-acl-name: Assigns a unique name to the new ACL. The *dest-acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**.

Usage guidelines

The new ACL and the source ACL must be the same type.

The new ACL has the same properties and content as the source ACL, but uses a different number or name from the source ACL.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

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

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

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

```
# Create IPv4 basic ACL paste by copying IPv4 basic ACL test.
```

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

```
[Sysname] acl copy name test to name paste
```

acl logging interval

Use **acl logging interval** to enable logging for packet filtering and set the interval.

Use **undo acl logging interval** to restore the default.

Syntax

```
acl logging interval interval
```


undo acl logging interval

Default

The interval is 0. The device does not generate log entries for packet filtering.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval at which log entries are generated and output. It must be a multiple of 5, in the range of 0 to 1440 minutes. To disable the logging, set the value to 0.

Usage guidelines

The logging feature is available for IPv4 or IPv6 ACL rules that have the **logging** keyword.

You can configure the ACL module to generate log entries for packet filtering and output them to the information center at the output interval. The log entry records the number of matching packets and the matched ACL rules. If an ACL is matched for the first time, the device immediately outputs a log entry to record the matching packet. For more information about the information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Configure the device to generate and output packet filtering log entries every 10 minutes.

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

Related commands

rule (IPv4 advanced ACL view)

rule (IPv4 basic ACL view)

rule (IPv6 advanced ACL view)

rule (IPv6 basic ACL view)

acl trap interval

Use **acl trap interval** to enable SNMP notifications for packet filtering and set the interval.

Use **undo acl interval** to restore the default.

Syntax

acl trap interval *interval*

undo acl trap interval

Default

The interval is 0. The device does not generate SNMP notifications for packet filtering.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval at which SNMP notifications are generated and output. It must be a multiple of 5, in the range of 0 to 1440 minutes. To disable SNMP notifications, set the value to 0.

Usage guidelines

The SNMP notifications feature is available for IPv4 or IPv6 ACL rules that have the **logging** keyword.

You can configure the ACL module to generate SNMP notifications for packet filtering and output them to the SNMP module at the output interval. The notification records the number of matching packets and the matched ACL rules. If an ACL is matched for the first time, the device immediately outputs a notification to record the matching packet. For more information about SNMP, see *Network Management and Monitoring Configuration Guide*.

Examples

```
# Configure the device to generate and output packet filtering SNMP notifications every 10 minutes.
<Sysname> system-view
[Sysname] acl trap interval 10
```

Related commands

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

description

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

Use **undo description** to delete an ACL description.

Syntax

```
description text
undo description
```

Default

An ACL does not have a description.

Views

- IPv4 basic/advanced ACL view
- IPv6 basic/advanced ACL view
- Layer 2 ACL view

Predefined user roles

- network-admin

Parameters

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

Examples

```
# Configure a description for IPv4 basic ACL 2000.
<Sysname> system-view
[Sysname] acl basic 2000
```

[Sysname-acl-ipv4-basic-2000] description This is an IPv4 basic ACL.

Related commands

display acl

display acl

Use **display acl** to display ACL configuration and match statistics.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

all: Specifies all ACLs of the specified type.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

This command displays ACL rules in **config** or **auto** order, whichever is configured.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

```
# Display configuration and match statistics for IPv4 basic ACL 2001.
```

```
<Sysname> display acl 2001
Basic IPv4 ACL 2001, 1 rules, match-order is auto,
This is an IPv4 basic ACL.
ACL's step is 5, start ID is 0
  rule 5 permit source 1.1.1.1 0
  rule 5 comment This rule is used on HundredGigE1/0/1.
```

Table 1 Command output

Field	Description
Basic IPv4 ACL 2001	Type and number of the ACL. The following field information is about IPv4 basic ACL 2000.
1 rules	The ACL contains two 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 displayed when the match order is config .

Field	Description
This is an IPv4 basic ACL.	Description of the ACL.
ACL's step is 5	The rule numbering step is 5.
start ID is 0	The start rule ID is 0.
rule 5 permit source 1.1.1.1 0	Content of rule 5. The rule permits packets sourced from the IP address 1.1.1.1.
rule 5 comment This rule is used on HundredGigE1/0/1.	Comment of rule 5.

display packet-filter

Use **display packet-filter** to display ACL application information for packet filtering.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. VLAN interfaces are not supported. If you do not specify an interface, this command displays ACL application information for packet filtering on all interfaces except VLAN interfaces.

interface vlan-interface *vlan-interface-number*: Specifies a VLAN interface by its number.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ACL application information for packet filtering for the master device.

Usage guidelines

If neither the **inbound** keyword nor the **outbound** keyword is specified, this command displays ACL application information for packet filtering in both directions.

Examples

```
# Display ACL application information for inbound packet filtering on interface HundredGigE 1/0/1.
```

```
<Sysname> display packet-filter interface hundredgige 1/0/1 inbound
```

```
Interface: HundredGigE1/0/1
```

```
Inbound policy:
```

```
IPv4 ACL 2001
```

```
IPv6 ACL 2002 (Failed)
```

```
MAC ACL 4003 (Failed), Hardware-count (Failed)
```

```
IPv4 ACL 2004, Hardware-count (Failed)
```

```
IPv4 default action: Deny, Hardware-count
```

Table 2 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv6 ACL 2002 (Failed)	The device has failed to apply IPv6 basic ACL 2002.
Hardware-count	ACL rule match counting has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches.
IPv4 default action	<p>Packet filter default action for packets that do not match any IPv4 ACLs:</p> <ul style="list-style-type: none"> • Deny—The default action deny has been successfully applied for packet filtering. • Deny (Failed)—The device has failed to apply the default action deny for packet filtering. The action permit still functions. • Permit—The default action permit has been successfully applied for packet filtering. • Hardware-count—The hardware-count feature has been successfully applied for the default action for packet filtering. • Hardware-count (Failed)—The device has failed to apply the hardware-count feature for the packet filtering default action.
IPv6 default action	<p>Packet filter default action for packets that do not match any IPv6 ACLs:</p> <ul style="list-style-type: none"> • Deny—The default action deny has been successfully applied for packet filtering. • Deny (Failed)—The device has failed to apply the default action deny for packet filtering. The action permit still functions. • Permit—The default action permit has been successfully applied for packet filtering. • Hardware-count—The hardware-count feature has been successfully applied for the default action for packet filtering. • Hardware-count (Failed)—The device has failed to apply the hardware-count feature for the packet filtering default action.
MAC default action	<p>Packet filter default action for packets that do not match any Layer 2 ACLs:</p> <ul style="list-style-type: none"> • Deny—The default action deny has been successfully applied for packet filtering. • Deny (Failed)—The device has failed to apply the default action deny for packet filtering. The action permit still functions. • Permit—The default action permit has been successfully applied for packet filtering. • Hardware-count—The hardware-count feature has been successfully applied for the default action for packet filtering. • Hardware-count (Failed)—The device has failed to apply the hardware-count feature for the packet filtering default action.

display packet-filter statistics

Use **display packet-filter statistics** to display packet filtering statistics and default action statistics.

Syntax

```
display packet-filter statistics interface interface-type interface-number { inbound | outbound }  
[ default | [ ipv6 | mac ] { acl-number | name acl-name } ] [ brief ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

default: Displays the default action statistics for packet filtering.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

brief: Displays brief statistics.

Usage guidelines

If **default**, *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command displays packet filtering statistics for all ACLs and default action statistics.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

```
# Display packet filtering statistics for all ACLs and default action statistics on incoming packets of  
HundredGigE 1/0/1.
```

```
<Sysname> display packet-filter statistics interface hundredgige 1/0/1 inbound
```

```
Interface: HundredGigE1/0/1
```

```
Inbound policy:
```

```
IPv4 ACL 2001, Hardware-count
```

```
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
```

```
rule 0 permit source 2.2.2.2 0 (2 packets)
```

```
rule 5 permit source 1.1.1.1 0 (Failed)
```

```
rule 10 permit vpn-instance test (No resource)
```

```
Totally 2 packets permitted, 0 packets denied
```

```
Totally 100% permitted, 0% denied
```

```
IPv4 ACL 2002 (Failed)
```

```
MAC ACL 4000
```

```

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

```

```
IPv6 ACL 2000
```

```

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

```

```

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

```

```

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

```

Table 3 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.
Hardware-count	ACL rule match counting has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches.
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	Start time and end time of the statistics.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
No resource	Resources are not enough for counting matches for the rule. In packet filtering statistics, this field is displayed for a rule when resources are not sufficient for rule match counting.
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs: <ul style="list-style-type: none"> • Deny—The default action deny has been successfully applied for packet filtering. • Deny (Failed)—The device has failed to apply the default action deny for packet filtering. The action permit still functions. • Permit—The default action permit has been successfully applied for packet filtering. • Hardware-count—The hardware-count feature has been successfully applied for the default action for packet filtering. • Hardware-count (Failed)—The device has failed to apply the hardware-count feature for the packet filtering default action.

Field	Description
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs: <ul style="list-style-type: none"> • Deny—The default action deny has been successfully applied for packet filtering. • Deny (Failed)—The device has failed to apply the default action deny for packet filtering. The action permit still functions. • Permit—The default action permit has been successfully applied for packet filtering. • Hardware-count—The hardware-count feature has been successfully applied for the default action for packet filtering. • Hardware-count (Failed)—The device has failed to apply the hardware-count feature for the packet filtering default action.
MAC default action	Packet filter default action for packets that do not match any Layer 2 ACLs: <ul style="list-style-type: none"> • Deny—The default action deny has been successfully applied for packet filtering. • Deny (Failed)—The device has failed to apply the default action deny for packet filtering. The action permit still functions. • Permit—The default action permit has been successfully applied for packet filtering. • Hardware-count—The hardware-count feature has been successfully applied for the default action for packet filtering. • Hardware-count (Failed)—The device has failed to apply the hardware-count feature for the packet filtering default action.
Totally 7 packets	The default action has been executed on seven packets.

Related commands

`reset packet-filter statistics`

display packet-filter statistics sum

Use `display packet-filter statistics sum` to display accumulated packet filtering statistics for an ACL.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.

- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

brief: Displays brief statistics.

Usage guidelines

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

Display accumulated packet filtering statistics for IPv4 basic ACL 2001 on incoming packets.

```
<Sysname> display packet-filter statistics sum inbound 2001
```

Sum:

Inbound policy:

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

Display brief accumulated packet filtering statistics for IPv4 basic ACL 2000 on incoming packets.

```
<Sysname> display packet-filter statistics sum inbound 2000 brief
```

Sum:

Inbound policy:

```
IPv4 ACL 2000
  Totally 2 packets permitted, 0 packets denied
  Totally 100% permitted, 0% denied
```

Table 4 Command output

Field	Description
Sum	Accumulated packet filtering statistics.
Inbound policy	Accumulated packet filtering statistics in the inbound direction.
Outbound policy	Accumulated packet filtering statistics in the outbound direction.
IPv4 ACL 2001	Accumulated packet filtering statistics of IPv4 basic ACL 2001.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.

Related commands

reset packet-filter statistics

display packet-filter verbose

Use **display packet-filter verbose** to display ACL application details for packet filtering.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. The **slot slot-number** option is not available for an Ethernet interface.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays ACL application details for packet filtering for the master device.

Usage guidelines

If *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command displays application details of all ACLs for packet filtering.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

```
# Display application details of all ACLs for inbound packet filtering on HundredGigE 1/0/1.
```

```
<Sysname> display packet-filter verbose interface hundredgige 1/0/1 inbound
```

```
Interface: HundredGigE1/0/1
```

```
Inbound policy:
```

```
IPv4 ACL 2001
```

```
rule 0 permit
```

```
rule 5 permit source 1.1.1.1 0 (Failed)
```

```
rule 10 permit vpn-instance test (Failed)
```

```
IPv4 ACL 2002 (Failed)
```

```
IPv6 ACL 2000
```

```
rule 0 permit
```

```
MAC ACL 4000
```

IPv4 default action: Deny

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

MAC default action: Deny

Table 5 Command output

Field	Description
Interface	Interface to which the ACL applies.
Inbound policy	ACL used for filtering incoming traffic.
Outbound policy	ACL used for filtering outgoing traffic.
IPv4 ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
IPv4 ACL 2002 (Failed)	The device has failed to apply IPv4 basic ACL 2002.
Hardware-count	ACL rule match counting has been successfully enabled.
Hardware-count (Failed)	The device has failed to enable counting ACL rule matches.
rule 5 permit source 1.1.1.1 0 (Failed)	The device has failed to apply rule 5.
IPv4 default action	<p>Packet filter default action for packets that do not match any IPv4 ACLs:</p> <ul style="list-style-type: none">• Deny—The default action deny has been successfully applied for packet filtering.• Deny (Failed)—The device has failed to apply the default action deny for packet filtering. The action permit still functions.• Permit—The default action permit has been successfully applied for packet filtering.• Hardware-count—The hardware-count feature has been successfully applied for the default action for packet filtering.• Hardware-count (Failed)—The device has failed to apply the hardware-count feature for the packet filtering default action.
IPv6 default action	<p>Packet filter default action for packets that do not match any IPv6 ACLs:</p> <ul style="list-style-type: none">• Deny—The default action deny has been successfully applied for packet filtering.• Deny (Failed)—The device has failed to apply the default action deny for packet filtering. The action permit still functions.• Permit—The default action permit has been successfully applied for packet filtering.• Hardware-count—The hardware-count feature has been successfully applied for the default action for packet filtering.• Hardware-count (Failed)—The device has failed to apply the hardware-count feature for the packet filtering default action.

Field	Description
MAC default action	<p>Packet filter default action for packets that do not match any Layer 2 ACLs:</p> <ul style="list-style-type: none"> • Deny—The default action deny has been successfully applied for packet filtering. • Deny (Failed)—The device has failed to apply the default action deny for packet filtering. The action permit still functions. • Permit—The default action permit has been successfully applied for packet filtering. • Hardware-count—The hardware-count feature has been successfully applied for the default action for packet filtering. • Hardware-count (Failed)—The device has failed to apply the hardware-count feature for the packet filtering default action.

display qos-acl resource

Use **display qos-acl resource** to display QoS and ACL resource usage.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS and ACL resource usage for all member devices.

Examples

```
# Display QoS and ACL resource usage.
```

```
<Sysname> display qos-acl resource
```

```
Interfaces: HGE1/0/25 to HGE1/0/30, XGE1/0/31:1 to XGE1/0/31:4
            HGE1/0/32 (slot 1)
```

```
-----
```

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	1024	16	0	1008	1%
IFP ACL	6144	2560	0	3584	41%
IFP Meter	1024	43	0	981	4%
IFP Counter	6144	2560	0	3584	41%
EFP ACL	1024	0	0	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

```
-----
```

```
Interfaces: HGE1/0/1 to HGE1/0/8, XGE1/0/33 (slot 1)
```

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	1024	16	0	1008	1%
IFP ACL	6144	2560	0	3584	41%
IFP Meter	1024	43	0	981	4%
IFP Counter	6144	2560	0	3584	41%
EFP ACL	1024	0	0	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

Interfaces: HGE1/0/9 to HGE1/0/16, XGE1/0/34 (slot 1)

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	1024	16	0	1008	1%
IFP ACL	6144	2560	0	3584	41%
IFP Meter	1024	43	0	981	4%
IFP Counter	6144	2560	0	3584	41%
EFP ACL	1024	0	0	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

Interfaces: HGE1/0/17 to HGE1/0/24 (slot 1)

Type	Total	Reserved	Configured	Remaining	Usage
VFP ACL	1024	16	0	1008	1%
IFP ACL	6144	2560	0	3584	41%
IFP Meter	1024	43	0	981	4%
IFP Counter	6144	2560	0	3584	41%
EFP ACL	1024	0	0	1024	0%
EFP Meter	512	0	0	512	0%
EFP Counter	512	0	0	512	0%

Table 6 Command output

Field	Description
Interfaces	Interface range for the resources.
Type	Resource type: <ul style="list-style-type: none"> • ACL—ACL rule resources. • Meter—Traffic policing resources. • Counter—Traffic accounting resources. • VFP—Resources for marking local QoS ID before Layer 2 forwarding. • IFP—Inbound resources. • EFP—Outbound resources.
Total	Total number of resources.
Reserved	Number of reserved resources.
Configured	Number of resources that has been applied.
Remaining	Number of resources that you can apply.

Field	Description
Usage	Configured and reserved resources as a percentage of total resources. If the percentage is not an integer, this field displays the integer part. For example, if the actual usage is 50.8%, this field displays 50%.

packet-filter

Use **packet-filter** to apply an ACL to an interface to filter packets.

Use **undo packet-filter** to remove an ACL from an interface.

Syntax

```
packet-filter [ ipv6 | mac ] { acl-number | name acl-name } { inbound | outbound }
[ hardware-count ]
```

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

Default

No ACL is applied to an interface to filter packets.

Views

Layer 2 Ethernet interface view
 Layer 2 aggregate interface view
 Layer 3 Ethernet interface/subinterface view
 Layer 3 aggregate interface view
 S-channel interface/S-channel bundle interface view
 VLAN interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

inbound: Filters incoming packets.

outbound: Filters outgoing packets.

hardware-count: Enables counting ACL rule matches performed in hardware. If you do not specify this keyword, rule matches for the ACL are not counted.

Usage guidelines

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

The **hardware-count** keyword in this command enables match counting for all rules in an ACL, and the **counting** keyword in the **rule** command enables match counting specific to rules.

To the same direction of an interface, you can apply a maximum of three ACLs: one IPv4 ACL, one IPv6 ACL, and one Layer 2 ACL.

You cannot apply an ACL to the outbound direction of a Layer 2 or Layer 3 aggregate interface.

Examples

```
# Apply IPv4 basic ACL 2001 to filter incoming traffic on HundredGigE 1/0/1, and enable counting
ACL rule matches performed in hardware.
```

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] packet-filter 2001 inbound hardware-count
```

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

packet-filter default deny

Use **packet-filter default deny** to set the packet filtering default action to **deny**. The packet filter denies packets that do not match any ACL rule.

Use **undo packet-filter default deny** to restore the default.

Syntax

packet-filter default deny

undo packet-filter default deny

Default

The packet filtering default action is **permit**. The packet filter permits packets that do not match any ACL rule.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The packet filter applies the default action to all ACL applications for packet filtering. The default action appears in the **display** command output for packet filtering.

Examples

```
# Set the packet filter default action to deny.
```

```
<Sysname> system-view
[Sysname] packet-filter default deny
```

Related commands

display packet-filter

display packet-filter statistics

display packet-filter verbose

packet-filter default hardware-count

Use **packet-filter default hardware-count** to enable hardware-count for the packet filtering default action.

Use **undo packet-filter default hardware-count** to disable hardware-count for the packet filtering default action.

Syntax

```
packet-filter default { inbound | outbound } hardware-count  
undo packet-filter default { inbound | outbound } hardware-count
```

Default

Hardware-count is disabled for the packet filtering default action.

Views

Interface view

Predefined user roles

network-admin

Parameters

inbound: Specifies the incoming packets.

outbound: Specifies the outgoing packets.

Usage guidelines

To enable hardware-count for the packet filtering default action on an interface, make sure you have applied ACLs to the interface for packet filtering.

Examples

Set the packet filtering default action to **deny**. Apply IPv4 basic ACL 2001 to HundredGigE 1/0/1 for filtering incoming packets, and enable hardware-count for the packet filtering default action on HundredGigE 1/0/1.

```
<Sysname> system-view  
[Sysname] packet-filter default deny  
[Sysname] interface hundredgige 1/0/1  
[Sysname-HundredGigE1/0/1] packet-filter 2001 inbound  
[Sysname-HundredGigE1/0/1] packet-filter default inbound hardware-count
```

Related commands

```
packet-filter  
packet-filter default deny  
display packet-filter  
display packet-filter statistics
```

reset acl counter

Use **reset acl counter** to clear statistics for ACLs.

Syntax

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


Views

User view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

all: Clears statistics for all ACLs of the specified type.

name *acl-name*: Clears statistics of an ACL specified by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

```
# Clear statistics for IPv4 basic ACL 2001.  
<Sysname> reset acl counter 2001
```

Related commands

display acl

reset packet-filter statistics

Use **reset packet-filter statistics** to clear the packet filtering statistics and accumulated statistics for an ACL and the default action statistics.

Syntax

```
reset packet-filter statistics interface [ interface-type interface-number ] { inbound | outbound }  
[ default | [ ipv6 | mac ] { acl-number | name acl-name } ]
```

Views

User view

Predefined user roles

network-admin

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If you do not specify an interface, this command clears packet filtering statistics for all interfaces.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

default: Clears the default action statistics for packet filtering.

ipv6: Specifies the IPv6 ACL type.

mac: Specifies the Layer 2 ACL type.

acl-number: Specifies an ACL by its number.

- 2000 to 2999 for basic ACLs.
- 3000 to 3999 for advanced ACLs.
- 4000 to 4999 for Layer 2 ACLs.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters.

Usage guidelines

If **default**, *acl-number*, **name** *acl-name*, **ipv6**, or **mac** is not specified, this command clears the packet filtering statistics for all ACLs and the default action statistics.

To specify the IPv4 ACL type, do not specify the **ipv6** or **mac** keyword.

Examples

```
# Clear IPv4 basic ACL 2001 statistics for inbound packet filtering on HundredGigE 1/0/1.
```

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

Related commands

display packet-filter statistics

display packet-filter statistics sum

rule (IPv4 advanced ACL view)

Use **rule** to create or edit an IPv4 advanced ACL rule.

Use **undo rule** to delete an entire IPv4 advanced ACL rule or some attributes in the rule.

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 | { precedence precedence | tos tos } * } | fragment | icmp-type { icmp-type [ icmp-code ] | icmp-message } | logging | source { source-address source-wildcard | any } | source-port operator port1 [ port2 ] | time-range time-range-name | vpn-instance vpn-instance-name ] *
```

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

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

Default

No IPv4 advanced ACL rules exist.

Views

IPv4 advanced ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. 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: Specifies one of the following values:

- A protocol number in the range of 0 to 255.
- A protocol by its name: **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), or **udp** (17). The **ip** keyword specifies all protocols.

Table 7 describes the parameters that you can specify regardless of the value for the *protocol* argument.

Table 7 Match criteria and other rule information for IPv4 advanced ACL rules

Parameters	Function	Description
source { <i>source-address</i> <i>source-wildcard</i> any }	Specifies a source address.	The <i>source-address</i> <i>source-wildcard</i> arguments specify a source IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard represents a host address. The any keyword specifies any source IP address.
destination { <i>dest-address</i> <i>dest-wildcard</i> any }	Specifies a destination address.	The <i>dest-address</i> <i>dest-wildcard</i> arguments specify a destination IP address and a wildcard mask in dotted decimal notation. An all-zero wildcard mask represents a host address. The any keyword represents any destination IP address.
counting	Counts the times that the rule is matched.	The counting keyword enables match counting specific to rules, and the hardware-count keyword in the packet-filter command enables match counting for all rules in an ACL. If the counting keyword is not specified, matches for the rule are not counted.
precedence <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: routine (0), priority (1), immediate (2), flash (3), flash-override (4), critical (5), internet (6), or network (7).
tos <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: max-reliability (2), max-throughput (4), min-delay (8), min-monetary-cost (1), or normal (0).
dscp <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: af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), default (0), or ef (46).
fragment	Applies the rule only to non-first fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.

Parameters	Function	Description
time-range <i>time-range-name</i>	Specifies a time range for the rule.	The <i>time-range-name</i> 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 time range. For more information about time range, see <i>ACL and QoS Configuration Guide</i> .
vpn-instance <i>vpn-instance-name</i>	Applies the rule to an MPLS L3VPN instance.	The <i>vpn-instance-name</i> argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies to both non-VPN packets and VPN packets.

If the *protocol* argument is **tcp** (6) or **udp** (7), set the parameters shown in [Table 8](#).

Table 8 TCP/UDP-specific parameters for IPv4 advanced ACL rules

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

If the *protocol* argument is **icmp** (1), set the parameters shown in [Table 9](#).

Table 9 ICMP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
icmp-type { <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 Table 10 .

Table 10 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 rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

When an IPv4 advanced ACL is used for QoS traffic classification or packet filtering in a VXLAN network, the ACL matches packets as follows:

- If the ACL is applied to the outgoing VXLAN packets on a VTEP, the ACL matches outer IPv4 header information.
- If the ACL is applied to the incoming VXLAN packets on a VTEP, the ACL matches inner IPv4 header information.
- If the ACL is applied to the incoming VXLAN packets on an intermediate transport device, the ACL matches outer IPv4 header information.

To view the existing IPv4 basic and advanced ACL rules, use the **display acl all** command.

The rule ID is required in the **undo rule rule-id** command.

If you do not specify optional parameters, the **undo rule rule-id** command deletes the entire rule. If you specify optional parameters, the **undo rule rule-id** command deletes the specified attributes.

The **undo rule { deny | permit }** command can only be used to delete the entire rule. You must specify all the attributes of the rule for the 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.
```

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

```
# 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 advanced 3001
[Sysname-acl-ipv4-adv-3001] rule deny icmp destination 192.168.1.0 0.0.0.255
[Sysname-acl-ipv4-adv-3001] rule permit ip
```

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

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

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

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

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv4 basic ACL view)

Use **rule** to create or edit an IPv4 basic ACL rule.

Use **undo rule** to delete an entire IPv4 basic ACL rule or some attributes in the rule.

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

Default

No IPv4 basic ACL rules exist.

Views

IPv4 basic ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. 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 times that the rule is matched. If you do not specify this keyword, matches for the rule are not counted.

fragment: Applies the rule only to non-first fragments. If you do not specify this keyword, the rule applies to both fragments and non-fragments.

logging: Logs matching packets. This feature is available only when the application module (for example, packet filtering) that uses the ACL supports the logging feature.

source { source-address source-wildcard | any }: Matches a source address. The *source-address* and *source-wildcard* arguments specify a source IP address and a wildcard mask in dotted decimal notation. A wildcard mask of zeros represents 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 time range. For more information about time range, see *ACL and QoS Configuration Guide*.

vpn-instance vpn-instance-name: Applies the rule to an MPLS L3VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies to both non-VPN packets and VPN packets.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

When an IPv4 basic ACL is used for QoS traffic classification or packet filtering in a VXLAN network, the ACL matches packets as follows:

- If the ACL is applied to the outgoing VXLAN packets on a VTEP, the ACL matches outer IPv4 header information.

- If the ACL is applied to the incoming VXLAN packets on a VTEP, the ACL matches inner IPv4 header information.
- If the ACL is applied to the incoming VXLAN packets on an intermediate transport device, the ACL matches outer IPv4 header information.

To view the existing IPv4 basic and advanced ACL rules, use the **display acl all** command.

The rule ID is required in the **undo rule rule-id** command.

If you do not specify optional parameters, the **undo rule rule-id** command deletes the entire rule. If you specify optional parameters, the **undo rule rule-id** command deletes the specified attributes.

The **undo rule { deny | permit }** command can only be used to delete the entire rule. You must specify all the attributes of the rule for the command.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting for all rules in an ACL.

Examples

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

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

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv6 advanced ACL view)

Use **rule** to create or edit an IPv6 advanced ACL rule.

Use **undo rule** to delete an entire IPv6 advanced ACL rule or some attributes in the rule.

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 ] | hop-by-hop [ type hop-type ] | source { source-address source-prefix | source-address/source-prefix | any } | source-port operator port1 [ port2 ] | time-range time-range-name | vpn-instance vpn-instance-name ] *
```

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

```
undo rule { deny | permit } protocol [ { { ack ack-value | fin fin-value | psh psh-value | rst rst-value | syn syn-value | urg urg-value } * | established } | counting | destination { dest-address dest-prefix | dest-address/dest-prefix | any } | destination-port operator port1 [ port2 ] | dscp dscp | flow-label
```


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

Default

No IPv6 advanced ACL rules exist.

Views

IPv6 advanced ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. 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: Specifies one of the following values:

- A protocol number in the range of 0 to 255.
- A protocol name: **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), or **udp** (17). The **ipv6** keyword specifies all protocols.

Table 11 describes the parameters that you can specify regardless of the value for the *protocol* argument.

Table 11 Match criteria and other rule information for IPv6 advanced ACL rules

Parameters	Function	Description
source { <i>source-address</i> <i>source-prefix</i> <i>source-address/so</i> <i>urce-prefix</i> any }	Specifies a source IPv6 address.	The <i>source-address</i> argument specifies an IPv6 source address. The <i>source-prefix</i> argument specifies a prefix length in the range of 1 to 128. The any keyword represents any IPv6 source address.
destination { <i>dest-address</i> <i>dest-prefix</i> <i>dest-address/dest-</i> <i>prefix</i> any }	Specifies a destination IPv6 address.	The <i>dest-address</i> argument specifies a destination IPv6 address. The <i>dest-prefix</i> argument specifies a prefix length in the range of 1 to 128. The any keyword represents any IPv6 destination address.
counting	Counts the times that the rule is matched.	The counting keyword enables match counting specific to rules, and the hardware-count keyword in the packet-filter ipv6 command enables match counting for all rules in an ACL. If the counting keyword is not specified, matches for the rule are not counted.
dscp <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, af11 (10), af12 (12), af13 (14), af21 (18), af22 (20), af23 (22), af31 (26), af32 (28), af33 (30), af41 (34), af42 (36), af43 (38), cs1 (8), cs2 (16), cs3 (24), cs4 (32), cs5 (40), cs6 (48), cs7 (56), default (0), or ef (46).
flow-label <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.

Parameters	Function	Description
fragment	Applies the rule only to non-first fragments.	If you do not specify this keyword, the rule applies to all fragments and non-fragments.
logging	Logs matching packets.	This feature requires that the module (for example, packet filtering) that uses the ACL supports logging.
routing [type <i>routing-type</i>]	Specifies an IPv6 routing header type.	<i>routing-type</i> : Value of the IPv6 routing header type, in the range of 0 to 255. If you specify the type <i>routing-type</i> option, the rule applies to the specified type of IPv6 routing header. If you do not specify the type <i>routing-type</i> option, the rule applies to all types of IPv6 routing headers.
hop-by-hop [type <i>hop-type</i>]	Specifies an IPv6 Hop-by-Hop Options header type.	<i>hop-type</i> : Value of the IPv6 Hop-by-Hop Options header type, in the range of 0 to 255. If you specify the type <i>hop-type</i> option, the rule applies to the specified type of IPv6 Hop-by-Hop Options header. If you do not specify the type <i>hop-type</i> option, the rule applies to all types of IPv6 Hop-by-Hop Options header.
time-range <i>time-range-name</i>	Specifies a time range for the rule.	The <i>time-range-name</i> 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 time range. For more information about time range, see <i>ACL and QoS Configuration Guide</i> .
vpn-instance <i>vpn-instance-name</i>	Applies the rule to an MPLS L3VPN instance.	The <i>vpn-instance-name</i> argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies to both non-VPN packets and VPN packets.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in [Table 12](#).

Table 12 TCP/UDP-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
source-port <i>operator port1</i> [<i>port2</i>]	Specifies one or more UDP or TCP source ports.	The <i>operator</i> argument can be lt (lower than), gt (greater than), eq (equal to), neq (not equal to), or range (inclusive range) . The <i>port1</i> and <i>port2</i> arguments are TCP or UDP port numbers in the range of 0 to 65535. The <i>port2</i> argument is needed only when the <i>operator</i> argument is range .
destination-port <i>operator port1</i> [<i>port2</i>]	Specifies one or more UDP or TCP destination ports.	TCP port numbers can be represented as: chargen (19), bgp (179), cmd (514), daytime (13), discard (9), dns (53), domain (53), echo (7), exec (512), finger (79), ftp (21), ftp-data (20), gopher (70), hostname (101), irc (194), klogin (543), kshell (544), login (513), lpd (515), nntp (119), pop2 (109), pop3 (110), smtp (25), sunrpc (111), tacacs (49), talk (517), telnet (23), time (37), uucp (540), whois (43), and www (80). UDP port numbers can be represented as: biff (512), bootpc (68), bootps (67), discard (9), dns (53), dnsix (90), echo (7), moblip-ag (434), moblip-mn (435), nameserver (42), netbios-dgm (138), netbios-ns (137), netbios-ssn (139), ntp (123), rip (520), snmp (161), snmptrap (162), sunrpc (111), syslog (514), tacacs-ds (65), talk (517), tftp (69), time (37), who (513), and xmcp (177).

Parameters	Function	Description
{ ack <i>ack-value</i> fin <i>fin-value</i> psh <i>psh-value</i> rst <i>rst-value</i> syn <i>syn-value</i> urg <i>urg-value</i> } *	Specifies one or more TCP flags, including ACK, FIN, PSH, 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 ANDed. For example, a rule configured with ack 0 psh 1 matches packets that have the ACK flag bit not set and the PSH flag bit set.
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmpv6** (58), set the parameters shown in [Table 13](#).

Table 13 ICMPv6-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
icmp6-type { <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 Table 14 .

Table 14 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

If an IPv6 advanced ACL is used for outbound QoS traffic classification or packet filtering, do not specify the **flow-label** parameter.

If an IPv6 advanced ACL is used for packet filtering, do not specify the **fragment** keyword.

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing IPv6 basic and advanced ACL rules, use the **display acl ipv6 all** command.

The rule ID is required in the **undo rule rule-id** command.

If you do not specify optional parameters, the **undo rule rule-id** command deletes the entire rule. If you specify optional parameters, the **undo rule rule-id** command deletes the specified attributes.

The **undo rule { deny | permit }** command can only be used to delete the entire rule. You must specify all the attributes of the rule for the 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.

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

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

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

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

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

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

Create IPv6 advanced ACL 3004, and configure two rules: one permits packets with the Hop-by-Hop Options header type as 5, and the other one denies packets with other Hop-by-Hop Options header types.

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

Related commands

acl

acl logging interval

display acl

step

time-range

rule (IPv6 basic ACL view)

Use **rule** to create or edit an IPv6 basic ACL rule.

Use **undo rule** to delete an entire IPv6 basic ACL rule or some attributes in the rule.

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 ] *
```

```
undo rule { 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 ] *
```

Default

No IPv6 basic ACL rules exist.

Views

IPv6 basic ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. 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 times that the rule is matched. If you do not specify this keyword, matches for the rule are not counted.

fragment: Applies the rule only to non-first fragments. If you do not specify this keyword, the rule applies to both fragments and non-fragments.

logging: Logs matching packets. This feature is available only when the application module (for example, packet filtering) that uses the ACL supports the logging feature.

routing [**type** *routing-type*]: Applies the rule to the specified type of IPv6 routing header or all types of IPv6 routing headers. The *routing-type* argument specifies the value of the IPv6 routing header type, in the range of 0 to 255. If you do not specify the **type** *routing-type* option, the rule applies to all types of IPv6 routing headers.

source { *source-address source-prefix* | *source-address/source-prefix* | **any** }: Matches a source IPv6 address. The *source-address* argument specifies a source IPv6 address. The *source-prefix* argument specifies an 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 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 time range. For more information about time range, see *ACL and QoS Configuration Guide*.

vpn-instance *vpn-instance-name*: Applies the rule to an MPLS L3VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If you do not specify a VPN instance, the rule applies to both non-VPN packets and VPN packets.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing IPv6 basic and advanced ACL rules, use the **display acl ipv6 all** command.

The rule ID is required in the **undo rule rule-id** command.

If you do not specify optional parameters, the **undo rule rule-id** command deletes the entire rule. If you specify optional parameters, the **undo rule rule-id** command deletes the specified attributes.

The **undo rule { deny | permit }** command can only be used to delete the entire rule. You must specify all the attributes of the rule for the command.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter ipv6** command enables match counting for all rules in an ACL.

Examples

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

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

Related commands

acl

acl logging interval

display acl

step

time-range

rule (Layer 2 ACL view)

Use **rule** to create or edit a Layer 2 ACL rule.

Use **undo rule** to delete an entire Layer 2 ACL rule or some attributes in the rule.

Syntax

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

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

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

Default

No Layer 2 ACL rules exist.

Views

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

rule-id: Specifies a rule ID in the range of 0 to 65534. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. 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 *dot1p*: Matches an 802.1p priority. The 802.1p priority can be specified by one of the following values:

- A priority number in the range of 0 to 7.
- A priority name: **best-effort** (0), **background** (1), **spare** (2), **excellent-effort** (3), **controlled-load** (4), **video** (5), **voice** (6), or **network-management** (7).

counting: Counts the times that the rule is matched. If you do not specify this keyword, matches for the rule are not counted.

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 the H-H-H format.

lsap *lsap-type lsap-type-mask*: Matches the DSAP and SSAP fields in LLC encapsulation. The *lsap-type* argument is a hexadecimal number that represents the encapsulation format. The value range for the *lsap-type* argument is 0 to ffff. The *lsap-type-mask* argument is a hexadecimal number that represents the LSAP mask. The value range for the *lsap-type-mask* argument is 0 to ffff.

type *protocol-type protocol-type-mask*: Matches one or more protocols in the Layer 2. The *protocol-type* argument is a hexadecimal number that represents a protocol type in Ethernet_II and Ethernet_SNAP frames. The value range for the *protocol-type* argument is 0 to ffff. The *protocol-type-mask* argument is a hexadecimal number that represents a protocol type mask. The value range for the *protocol-type-mask* argument is 0 to ffff.

source-mac *source-address source-mask*: Matches a source MAC address range. The *source-address* argument represents a source MAC address, and the *source-mask* argument represents a mask in the 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. 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 time range. For more information about time range, see *ACL and QoS Configuration Guide*.

Usage guidelines

Within an ACL, the permit or deny statement of each rule must be unique. If the rule you are creating or editing has the same deny or permit statement as another rule in the ACL, the rule will not be created or changed.

You can edit ACL rules only when the match order is **config**.

To view the existing Layer 2 ACL rules, use the **display acl mac all** command.

The rule ID is required in the **undo rule *rule-id*** command.

If you do not specify optional parameters, the **undo rule *rule-id*** command deletes the entire rule. If you specify optional parameters, the **undo *rule-id* rule** command deletes the specified attributes.

The **undo rule { deny | permit }** command can only be used to delete the entire rule. You must specify all the attributes of the rule for the command.

The **counting** keyword in this command enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting for all rules in an ACL.

Examples

```
# Create a rule in Layer 2 ACL 4000 to permit ARP packets and deny RARP packets.
```

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

Related commands

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

rule comment

Use **rule comment** to configure a comment for an ACL rule.

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

Syntax

```
rule rule-id comment text  
undo rule rule-id comment
```

Default

A rule does not have a comment.

Views

- IPv4 basic/advanced ACL view
- IPv6 basic/advanced ACL view
- Layer 2 ACL view

Predefined user roles

- network-admin

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.

Usage guidelines

This command adds a comment to a rule if the rule does not have a comment. It modifies the comment for a rule if the rule already has a comment.

Examples

```
# Create a rule for IPv4 basic ACL 2000, and add a comment about the rule.
<Sysname> system-view
[Sysname] acl basic 2000
[Sysname-acl-ipv4-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-ipv4-basic-2000] rule 0 comment This rule is used on hundredgige 1/0/1.
```

Related commands

display acl

step

Use **step** to set a rule numbering step for an ACL.

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

Syntax

step *step-value* [**start** *start-value*]

undo step

Default

The rule numbering step is 5, and the start rule ID is 0.

Views

IPv4 basic/advanced ACL view

IPv6 basic/advanced ACL view

Layer 2 ACL view

Predefined user roles

network-admin

Parameters

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

start *start-value*: Specifies the start rule ID in the range of 0 to 20.

Usage guidelines

The rule numbering step sets the increment by which the system numbers rules automatically. If you do not specify a rule ID when creating an ACL rule, the system automatically assigns it a rule ID. This rule ID is the nearest higher multiple of the numbering step to the current highest rule ID, starting from the start rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 12, the rule is numbered 15.

The wider the numbering step, the more rules you can insert between two rules. Whenever the step or start rule ID changes, the rules are renumbered, starting from the start rule ID. For example, if there are five rules numbered 0, 5, 9, 10, and 15, changing the step from 5 to 2 causes the rules to be renumbered 0, 2, 4, 6, and 8.

Examples

```
# Set the rule numbering step to 2 for IPv4 basic ACL 2000.
<Sysname> system-view
```

```
[Sysname] acl basic 2000
```

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

Related commands

display acl

QoS policy commands

Traffic class commands

display traffic classifier

Use **display traffic classifier** to display traffic classes.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined traffic classes.

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic class, this command displays all traffic classes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the traffic classes for the master device.

Examples

Display all user-defined traffic classes.

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

```
User-defined classifier information:
```

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

```
Operator: AND
```

```
Rule(s) :
```

```
  If-match acl 2000
```

```
Classifier: 2 (ID 101)
```

```
Operator: AND
```

```
Rule(s) :
```

```
  If-match protocol ipv6
```

```
Classifier: 3 (ID 102)
```

```
Operator: AND
```

```
Rule(s) :
```

```
  -none-
```

Table 15 Command output

Field	Description
Classifier	Traffic class name and its match criteria.
Operator	Match operator you set for the traffic class. If the operator is AND, the traffic class matches the packets that match all its match criteria. If the operator is OR, the traffic 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.

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

Default

No match criterion is configured.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

match-criteria: Specifies a match criterion. [Table 16](#) shows the available match criteria.

Table 16 Available match criteria

Option	Description
acl [ipv6] { <i>acl-number</i> name <i>acl-name</i> }	Matches an ACL. The value range for the <i>acl-number</i> argument is as follows: <ul style="list-style-type: none"> • 2000 to 3999 for IPv4 ACLs. • 2000 to 3999 for IPv6 ACLs. • 4000 to 4999 for Layer 2 MAC ACLs. The <i>acl-name</i> argument is a case-insensitive string of 1 to 63 characters, which must start with an English letter. To avoid confusion, make sure the argument is not all .
any	Matches all packets.
control-plane protocol <i>protocol-name</i> <1-8>	Matches control plane protocols. The <i>protocol-name</i> <1-8> argument specifies a space-separated list of up to eight system-defined control plane protocols. For available system-defined control plane protocols, see Table 17 .
control-plane protocol-group <i>protocol-group-name</i>	Matches a control plane protocol group. The <i>protocol-group-name</i> argument can be critical , important , management , monitor , normal , or redirect .

Option	Description
customer-dot1p <i>dot1p-value&<1-8></i>	Matches 802.1p priority values in inner VLAN tags of double-tagged packets. The <i>dot1p-value&<1-8></i> argument specifies a space-separated list of up to eight 802.1p priority values. The value range for the <i>dot1p-value</i> argument is 0 to 7.
customer-vlan-id <i>vlan-id-list</i>	Matches VLAN IDs in inner VLAN tags of double-tagged packets. The <i>vlan-id-list</i> argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of <i>vlan-id1 to vlan-id2</i> . The value for <i>vlan-id2</i> must be greater than or equal to the value for <i>vlan-id1</i> . The value range for the <i>vlan-id</i> argument is 1 to 4094.
destination-mac <i>mac-address</i>	Matches a destination MAC address. This option takes effect only on Ethernet interfaces.
dscp <i>dscp-value&<1-8></i>	Matches DSCP values. The <i>dscp-value&<1-8></i> argument specifies a space-separated list of up to eight DSCP values. The value range for the <i>dscp-value</i> argument is 0 to 63 or keywords shown in Table 19 .
ip-precedence <i>ip-precedence-value&<1-8></i>	Matches IP precedence values. The <i>ip-precedence-value&<1-8></i> argument specifies a space-separated list of up to eight IP precedence values. The value range for the <i>ip-precedence-value</i> argument is 0 to 7.
protocol <i>protocol-name</i>	Matches a protocol. The <i>protocol-name</i> argument can be , ipv6 , or ip .
qos-local-id <i>local-id-value</i>	Matches a local QoS ID in the range of 1 to 4095. For a QoS policy applied to the outbound direction, the value range for the <i>local-id-value</i> argument is 1 to 511. In an IRF fabric, if you use a QoS policy to mark the local QoS ID of incoming packets on a member device, you cannot match the marked packets by using local QoS IDs in the outbound direction on another member device. In a VXLAN network, if you use a QoS policy to mark the local QoS ID of incoming packets on a VTEP or VXLAN IP gateway, you cannot match the marked packets by using local QoS IDs in the outbound direction on the remote VTEP or VXLAN IP gateway.
service-dot1p <i>dot1p-value&<1-8></i>	Matches 802.1p priority values in outer VLAN tags. The <i>dot1p-value&<1-8></i> argument specifies a space-separated list of up to eight 802.1p priority values. The value range for the <i>dot1p-value</i> argument is 0 to 7.
service-vlan-id <i>vlan-id-list</i>	Matches VLAN IDs in outer VLAN tags. The <i>vlan-id-list</i> argument specifies a space-separated list of up to 10 VLAN items. Each item specifies a VLAN or a range of VLANs in the form of <i>vlan-id1 to vlan-id2</i> . The value for <i>vlan-id2</i> must be greater than or equal to the value for <i>vlan-id1</i> . The value range for the <i>vlan-id</i> argument is 1 to 4094. You can use this option to match single-tagged packets.
source-mac <i>mac-address</i>	Matches a source MAC address. This option takes effect only on Ethernet interfaces.
tunnel-id <i>tunnel-id</i>	Matches a VXLAN tunnel ID. For the traffic class to take effect, the tunnel must be a VXLAN tunnel.
vxlan { any <i>vxlan-id</i> }	Matches a VXLAN ID. If the device acts as an intermediate device in a VXLAN network, it supports matching VXLAN IDs only in the inbound direction.

Table 17 Available system-defined control plane protocols

Protocol	Description
arp	ARP packets
arp-snooping	ARP snooping packets
bfd	BFDP packets
bgp	BGP packets
bgp4+	IPv6 BGP packets
dhcp	DHCP packets
dhcp-snooping	DHCP snooping packets
dhcpv6	IPv6 DHCP packets
dldp	DLDP packets
dot1x	802.1X packets
hoplimit-expires	Hop-limit expire packets
http	HTTP packets
https	HTTPS packets
icmp	ICMP packets
icmpv6	ICMPv6 packets
igmp	IGMP packets
ip-option	IPv4 packets with the Options field
ipv6-option	IPv6 packets with the Options field
isis	IS-IS packets
lACP	LACP packets
lldp	LLDP packets
mvrp	MVRP packets (including GVRP packets)
ospf-multicast	OSPF multicast packets
ospf-unicast	OSPF unicast packets
ospf3-multicast	OSPFv3 multicast packets
ospf3-unicast	OSPFv3 unicast packets
pim-multicast	PIM multicast packets
pim-unicast	PIM unicast packets
pim6-multicast	IPv6 PIM multicast packets
pim6-unicast	IPv6 PIM unicast packets
radius	RADIUS packets
snmp	SNMP packets
ssh	SSH packets
stp	STP packets
tacacs	TACACS packets
telnet	Telnet packets
tll-expires	TTL expire packets
vrrp	VRRP packets

Protocol	Description
vrrp6	IPv6 VRRP packets

Usage guidelines

In a traffic class with the logical OR operator, you can configure multiple **if match** commands for any of the available match criteria.

When you configure a match criterion that can have multiple values in one **if-match** command, follow these restrictions and guidelines:

- You can specify up to eight values for any of the following match criteria in one **if-match** command:
 - Control plane protocol.
 - 802.1p priority.
 - DSCP.
 - IP precedence.
 - VLAN ID.
- If a packet matches one of the specified values, it matches the **if-match** command.
- To delete a criterion that has multiple values, the specified values in the **undo if-match** command must be the same as those specified in the **if-match** command. The order of the values can be different.

When you configure ACL-based match criteria, follow these restrictions and guidelines:

- If the ACL used as a match criterion does not exist, the traffic class cannot be applied to hardware.
- In a traffic class, you can add two **if-match** statements that use the same ACL as the match criterion. In one statement, specify the ACL by its name. In the other statement, specify the ACL by its number.
- The ACL is used for classification only and the permit/deny actions in ACL rules are ignored. Actions taken on matching packets are defined in traffic behaviors.

You can use both AND and OR operators to define the match relationships between the criteria for a class. For example, you can define relationships among three match criteria in traffic class **classA** as follows:

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

Examples

Define a match criterion for traffic class **class1** to match the packets with a destination MAC address of 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 traffic class **class2** to match the packets with a source MAC address of 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 traffic class **class1** to match the double-tagged packets with 802.1p priority 3 in the inner VLAN tag.

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

Define a match criterion for traffic class **class1** to match the packets with 802.1p priority 5 in the outer VLAN tag.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-dot1p 5
```

Define a match criterion for traffic class **class1** to match advanced ACL 3101.

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

Define a match criterion for traffic 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 traffic class **class1** to match advanced IPv6 ACL 3101.

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

Define a match criterion for traffic 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 traffic class **class1** to match all packets.

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

Define a match criterion for traffic class **class1** to match the packets with a DSCP value of 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 traffic class **class1** to match the packets with an IP precedence value of 1 or 6.

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

Define a match criterion for traffic 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 traffic class **class1** to match double-tagged packets with VLAN ID 1, 6, or 9 in the inner VLAN tag.

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



```

[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match customer-vlan-id 1 6 9
# Define a match criterion for traffic class class1 to match the packets with VLAN ID 2, 7, or 10 in the
outer VLAN tag.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-vlan-id 2 7 10
# Define a match criterion for traffic class class1 to match the packets with a local QoS ID of 3.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match qos-local-id 3
# Define a match criterion for traffic class class1 to match ARP protocol packets.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match control-plane protocol arp
# Define a match criterion for traffic class class1 to match packets of the protocols in protocol group
normal.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match control-plane protocol-group normal
# Define a match criterion for traffic class class1 to match the VXLAN packets with tunnel ID 2.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match tunnel-id 2
# Define a match criterion for traffic class class1 to match the packets with VXLAN 10.
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match vxlan 10

```

traffic classifier

Use **traffic classifier** to create a traffic class and enter its view, or enter the view of an existing traffic class.

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

Syntax

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

```
undo traffic classifier classifier-name
```

Default

No traffic classes exist.

Views

System view

Predefined user roles

network-admin

Parameters

classifier-name: Specifies a name for the traffic class, a case-sensitive string of 1 to 31 characters.

operator: Sets the operator to logic AND (the default) or OR for the traffic class.

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

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

Examples

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

Related commands

display traffic classifier

Traffic behavior commands

accounting

Use **accounting** to configure a traffic accounting action in a traffic behavior.

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

Syntax

accounting { **byte** | **packet** }

undo accounting

Default

No traffic accounting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

byte: Counts traffic in bytes.

packet: Counts traffic in packets.

Usage guidelines

The accounting action in a QoS policy does not take effect if the QoS policy is applied globally.

Examples

```
# Configure a traffic accounting action in traffic behavior database to count traffic in bytes.
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting byte
```

car

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

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

Syntax

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

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

```
undo car
```

Default

No CAR action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cir *committed-information-rate*: Specifies the committed information rate (CIR) in kbps or pps, which is an average traffic rate. If you specify the **pps** keyword, the CIR is specified in pps. If you do not specify the **pps** keyword, the CIR is specified in kbps. The value range for *committed-information-rate* is 8 to 160000000, in increments of 8.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes. The value range for *committed-burst-size* is 512 to 256000000, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 256000000 is converted to 256000000.

ebs *excess-burst-size*: Specifies the excess burst size (EBS) in bytes. The value range for *excess-burst-size* is 0 to 256000000, in increments of 512. If the PIR is configured, the default EBS is the product of 62.5 and the PIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 256000000 is converted to 256000000.

pir *peak-information-rate*: Specifies the peak information rate (PIR) in kbps or pps. If you specify the **pps** keyword, the PIR is specified in pps. If you do not specify the **pps** keyword, the PIR is specified in kbps. The PIR must be specified in the same unit as the CIR. The value range for *peak-information-rate* is 8 to 160000000, in increments of 8.

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

red *action*: Specifies the action to take on packets that conform to neither CIR nor PIR. The default setting is **discard**.

yellow *action*: Specifies the action to take on packets that conform to the PIR but not to the CIR. The default setting is **pass**.

action: Sets the action to take on the packet:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument is in the range of 0 to 7.

- **remark-dscp-pass** *new-dscp*: Sets the DSCP value of the packet to *new-dscp* and permits the packet to pass through. The *new-dscp* argument is in the range of 0 to 63.
- **remark-ip-pass** *new-local-precedence*: Sets the local precedence value of the packet to *new-local-precedence* and permits the packet to pass through. The *new-local-precedence* argument is in the range of 0 to 7.

Usage guidelines

To use two rates for traffic policing, configure the **car** command with the **pir** *peak-information-rate* option. To use one rate for traffic policing, configure the **car** command without the **pir** *peak-information-rate* option.

A QoS policy that uses a traffic behavior configured with CAR can be applied in either the inbound direction or outbound direction of an interface.

If you execute the **car** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

Configure a CAR action in traffic behavior **database**:

- Set the CIR to 200 kbps, CBS to 51200 bytes, and EBS to 0.
- Transmit the conforming packets, and mark the excess packets with DSCP value 0 and transmit them.

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

display traffic behavior

Use **display traffic behavior** to display traffic behaviors.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

user-defined: Specifies user-defined traffic behaviors.

behavior-name: Specifies a behavior by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic behavior, this command displays all traffic behaviors.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the traffic behaviors for the master device.

Examples

Display all user-defined traffic behaviors.

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

```
User-defined behavior information:
```

```

Behavior: 1 (ID 100)
  Marking:
    Remark dscp 3
  Committed Access Rate:
    CIR 200 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
    Green action : pass
    Yellow action : pass
    Red action   : discard

```

```

Behavior: 2 (ID 101)
  Accounting enable: Packet
  Filter enable: Permit
  Marking:
    Remark dscp 4
  Redirecting:
    Redirect to the CPU

```

Table 18 Command output

Field	Description
Behavior	Name and contents of a traffic behavior.
Marking	Information about priority marking.
Remark dscp	Action of setting the DSCP value for packets.
Committed Access Rate	Information about the CAR action.
Green action	Action to take on green packets.
Yellow action	Action to take on yellow packets.
Red action	Action to take on red packets.
Accounting enable	Traffic accounting action.
Filter enable	Traffic filtering action.
Redirecting	Information about traffic redirecting.
Mirroring	Information about traffic mirroring.
Pre	IP precedence.

filter

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

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

Syntax

```
filter { deny | permit }
```

```
undo filter
```

Default

No traffic filtering action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

deny: Drops packets.

permit: Transmits packets.

Examples

```
# Configure a traffic filtering action as deny in traffic behavior database.
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

nest top-most

Use **nest top-most** to configure an outer VLAN tag adding action in a traffic behavior.

Use **undo nest top-most** to restore the default.

Syntax

nest top-most vlan *vlan-id*

undo nest top-most

Default

No outer VLAN tag adding action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id *vlan-id*: Specifies the VLAN ID to be added in the outer VLAN tag, in the range of 1 to 4094.

Usage guidelines

If a QoS policy contains an outer VLAN tag adding action, apply it only to the incoming traffic of an interface.

If you execute the **nest top-most** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

```
# Configure traffic behavior b1 to add an outer VLAN tag with VLAN ID 123.
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] nest top-most vlan 123
```

redirect

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

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

Syntax

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

Default

No traffic redirecting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cpu: Redirects traffic to the CPU.

interface *interface-type interface-number*: Redirects traffic to an interface specified by its type and number.

Usage guidelines

If you execute the **redirect** command multiple times in the same traffic behavior, the most recent configuration takes effect.

A traffic redirecting action takes effect only when the QoS policy is applied to the inbound direction.

For traffic redirecting to an access port, make sure the PVID of the interfaces to which the QoS policy is applied is the same as the PVID of the access port. Otherwise, the access port drops redirected packets.

For traffic redirecting to a trunk port, make sure the PVID of the interfaces to which the QoS policy is applied is in the allowed VLAN list of the trunk port. Otherwise, the trunk port drops redirected packets.

Examples

```
# Configure redirecting traffic to HundredGigE 1/0/1 in traffic behavior database.  
<Sysname> system-view  
[Sysname] traffic behavior database  
[Sysname-behavior-database] redirect interface hundredgige 1/0/1
```

Related commands

classifier behavior

qos policy

traffic behavior

remark customer-vlan-id

Use **remark customer-vlan-id** to configure a CVLAN marking action in a traffic behavior.

Use **undo remark customer-vlan-id** to restore the default.

Syntax

```
remark customer-vlan-id vlan-id  
undo remark customer-vlan-id
```

Default

No CVLAN marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a CVLAN ID in the range of 1 to 4094.

Examples

```
# Configure traffic behavior b1 to mark matching packets with CVLAN 111.
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark customer-vlan-id 111
```

remark dot1p

Use **remark dot1p** to configure an 802.1p priority marking action or an inner-to-outer tag priority copying action in a traffic behavior.

Use **undo remark dot1p** to restore the default.

Syntax

```
remark [ green | red | yellow ] dot1p dot1p-value
undo remark [ green | red | yellow ] dot1p
remark dot1p customer-dot1p-trust
undo remark dot1p
```

Default

No 802.1p priority marking action or inner-to-outer tag priority copying action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dot1p-value: Specifies the 802.1p priority to be marked for packets, in the range of 0 to 7.

customer-dot1p-trust: Copies the 802.1p priority value in the inner VLAN tag to the outer VLAN tag.

Usage guidelines

The **remark dot1p dot1p-value** and **remark dot1p customer-dot1p-trust** commands override each other in the same traffic behavior. The **remark dot1p customer-dot1p-trust** command does not take effect on single-tagged packets.

If you execute the **remark dot1p dot1p-value** command multiple times for the same color, the most recent configuration takes effect.

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

# Configure an inner-to-outer tag priority copying action in traffic behavior database.
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p customer-dot1p-trust
```

remark drop-precedence

Use **remark drop-precedence** to configure a drop priority marking action in a traffic behavior.

Use **undo remark drop-precedence** to restore the default.

Syntax

```
remark drop-precedence drop-precedence-value
undo remark drop-precedence
```

Default

No drop priority marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

drop-precedence-value: Specifies the drop priority to be marked for packets, in the range of 0 to 2.

Usage guidelines

A traffic behavior that includes a drop priority marking action can be applied only to the inbound direction.

If you execute the **remark drop-precedence** command multiple times in the same traffic behavior, the most recent configuration takes effect.

Examples

```
# Configure traffic behavior database to mark matching traffic with drop priority 2.
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark drop-precedence 2
```

remark dscp

Use **remark dscp** to configure a DSCP marking action in a traffic behavior.

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

Syntax

```
remark [ green | red | yellow ] dscp dscp-value
undo remark [ green | red | yellow ] dscp
```

Default

No DSCP marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

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

Table 19 DSCP keywords and values

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

remark ip-precedence

Use **remark ip-precedence** to configure an IP precedence marking action in a traffic behavior.

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

Syntax

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

Default

No IP precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

ip-precedence-value: Specifies the 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
```

remark local-precedence

Use **remark local-precedence** to configure a local precedence marking action in a traffic behavior.

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

Syntax

remark [green | red | yellow] local-precedence *local-precedence-value*

undo remark [green | red | yellow] local-precedence

Default

No local precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

local-precedence-value: Specifies the local precedence to be marked for packets, in the range of 0 to 7.

Examples

```
# Configure traffic behavior database to mark matching traffic with local precedence 2.
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark local-precedence 2
```

remark qos-local-id

Use **remark qos-local-id** to configure a local QoS ID marking action in a traffic behavior.

Use **undo remark qos-local-id** to restore the default.

Syntax

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

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

Default

No local QoS ID marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

You can use one QoS policy to mark the local QoS ID for packets in the inbound direction. Then, you can use another QoS policy to apply other QoS features in the outbound direction based on the marked local QoS ID.

If you execute the **remark qos-local-id** command multiple times in the same traffic behavior, the most recent configuration takes effect.

For a QoS policy applied to the outbound direction, the value range for the *local-id-value* argument is 1 to 511.

In an IRF fabric, if you use a QoS policy to mark the local QoS ID of incoming packets on a member device, you cannot match the marked packets by using local QoS IDs in the outbound direction on another member device.

In a VXLAN network, if you use a QoS policy to mark the local QoS ID of incoming packets on a VTEP or VXLAN IP gateway, you cannot match the marked packets by using local QoS IDs in the outbound direction on the remote VTEP or VXLAN IP gateway.

Examples

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

remark service-vlan-id

Use **remark service-vlan-id** to configure an SVLAN marking action in a traffic behavior.

Use **undo remark service-vlan-id** to restore the default.

Syntax

remark service-vlan-id *vlan-id*

undo remark service-vlan-id

Default

No SVLAN marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an SVLAN ID in the range of 1 to 4094.

Examples

Configure traffic behavior **b1** to mark matching packets with SVLAN 222.

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

```
[Sysname] traffic behavior b1
```

```
[Sysname-behavior-b1] remark service-vlan-id 222
```

traffic behavior

Use **traffic behavior** to create a traffic behavior and enter its view, or enter the view of an existing traffic behavior.

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

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

Default

No traffic behaviors exist.

Views

System view

Predefined user roles

network-admin

Parameters

behavior-name: Specifies a name for the traffic behavior, a case-sensitive string of 1 to 31 characters.

Examples

Create a traffic behavior named **behavior1**.

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

```
[Sysname] traffic behavior behavior1
```

```
[Sysname-behavior-behavior1]
```

Related commands

`display traffic behavior`

QoS policy commands

classifier behavior

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

Use **undo classifier** to delete a class-behavior association from a QoS policy.

Syntax

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

undo classifier *classifier-name*

Default

No traffic behavior is associated with a traffic class.

Views

QoS policy view

Predefined user roles

network-admin

Parameters

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters.

behavior-name: Specifies a traffic behavior by its name, a case-sensitive string of 1 to 31 characters.

insert-before *before-classifier-name*: Inserts the new traffic class before an existing traffic class in the QoS policy. The *before-classifier-name* argument specifies an existing traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify the **insert-before** *before-classifier-name* option, the new traffic class is placed at the end of the QoS policy.

Usage guidelines

A traffic class can be associated only with one traffic behavior in a QoS policy.

If the specified traffic class or traffic behavior does not exist, the system defines a null traffic 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
```

Associate traffic class **database** with traffic behavior **test** in QoS policy **user1**, and insert traffic class **database** before an existing traffic class named **class-a**.

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

Related commands

`qos policy`

control-plane

Use **control-plane** to enter control plane view.

Syntax

control-plane slot *slot-number*

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Usage guidelines

A QoS policy applied in control plane view takes effect on all packets to the control plane except the packets sent from the management interface.

Examples

```
# Enter the control plane view of slot 3.
<Sysname> system-view
[Sysname] control-plane slot 3
[Sysname-cp-slot3]
```

display qos policy

Use **display qos policy** to display QoS policies.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Specifies user-defined QoS policies.

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a QoS policy, this command displays all user-defined QoS policies.

classifier *classifier-name*: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If you do not specify a traffic class, this command displays all traffic classes.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the QoS policies for the master device.

Examples

```
# Display all user-defined QoS policies.
<Sysname> display qos policy user-defined
```

User-defined QoS policy information:

```
Policy: 1 (ID 100)
Classifier: 1 (ID 100)
  Behavior: 1
  Marking:
    Remark dscp 3
  Committed Access Rate:
    CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
    Green action : pass
    Yellow action : pass
    Red action   : discard
Classifier: 2 (ID 101)
  Behavior: 2
  Accounting enable: Packet
  Filter enable: Permit
  Marking:
    Remark dot1p 4
Classifier: 3 (ID 102)
  Behavior: 3
  -none-
```

For the output description, see [Table 15](#) and [Table 18](#).

display qos policy control-plane

Use **display qos policy control-plane** to display QoS policies applied to a control plane.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

slot *slot-number*. Specifies an IRF member device by its member ID.

Examples

```
# Display the QoS policy applied to the control plane of slot 2.
```

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

```
Control plane slot 2
```

```
Direction: Inbound
```

```
Policy: 1
```

```
Classifier: 1
```



```

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

```

Table 20 Command output

Field	Description
Direction	Inbound direction on the control plane.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see [Table 15](#) and [Table 18](#).

display qos policy control-plane pre-defined

Use **display qos policy control-plane pre-defined** to display predefined control plane QoS policies.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*. Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays predefined control plane QoS policies for all member devices.

Examples

Display the predefined control plane QoS policy of slot 1.

```
<Sysname> display qos policy control-plane pre-defined slot 1
Pre-defined policy information slot 1
  Protocol          Priority  Bandwidth      Group
  -----
  Default           N/A     1000 (pps)     N/A
  IS-IS             18      1000 (pps)     critical
  VRRP              19      1000 (pps)     important
  OSPF Multicast    18      1000 (pps)     critical
  OSPF Unicast      18      1000 (pps)     critical
  PIM Multicast     12      500 (pps)      critical
  PIM Unicast       12      500 (pps)      critical
  IGMP              11      500 (pps)      important
  PIMv6 Multicast  12      300 (pps)      critical
  PIMv6 Unicast     12      300 (pps)      critical
  OSPFv3 Unicast   18      1000 (pps)     critical
  OSPFv3 Multicast 18      1000 (pps)     critical
  VRRPv6           19      1000 (pps)     important
  ARP               2       1000 (pps)     normal
  DHCP Snooping    10      300 (pps)      redirect
  DHCP              10      300 (pps)      normal
  802.1x           3       500 (pps)      important
  STP              17      300 (pps)      critical
  LACP             22      300 (pps)      critical
  MVRP             15      300 (pps)      critical
  BGP              16      1000 (pps)     critical
  ICMP             3       500 (pps)      monitor
  TTL Expires      5       300 (pps)      monitor
  IPOPTION         5       300 (pps)      normal
  BGPv6            16      1000 (pps)     critical
  Hop Limit Expires 5       300 (pps)      monitor
  IPOPTIONv6      5       300 (pps)      normal
  LLDP             14      300 (pps)      important
  DLDP             16      300 (pps)      critical
  TELNET           1       800 (pps)      management
  SSH              1       800 (pps)      management
  TACACS           1       800 (pps)      management
  RADIUS           1       800 (pps)      management
  HTTP            3       500 (pps)      management
```

HTTPS	3	500 (pps)	management
SNMP	4	800 (pps)	management
ARP Snooping	2	1000 (pps)	redirect
ICMPv6	3	300 (pps)	monitor
DHCPv6	10	300 (pps)	normal
BFD	21	1000 (pps)	critical

Table 21 Command output

Field	Description
Pre-defined control plane policy	Contents of the predefined control plane QoS policy.
Default	Protocols other than those listed.
Group	Protocol group of the protocol.

For descriptions of other fields, see [Table 17](#).

display qos policy global

Use **display qos policy global** to display global QoS policies.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

inbound: Displays inbound global QoS policies. An inbound global QoS policy applies to the incoming traffic globally.

outbound: Displays outbound global QoS policies. An outbound global QoS policy applies to the outgoing traffic globally.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays global QoS policies for the master device.

Usage guidelines

If you do not specify a direction, this command displays both inbound and outbound global QoS policies.

Examples

Display QoS policies applied globally.

```
<Sysname> display qos policy global
  Direction: Inbound
  Policy: 1
  Classifier: 1
    Operator: AND
  Rule(s) :
    If-match acl 2000
  Behavior: 1
```

```

Marking:
  Remark dscp 3
Committed Access Rate:
  CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
  Green action : pass
  Yellow action : pass
  Red action   : discard
  Green packets : 0 (Packets) 0 (Bytes)
  Yellow packets: 0 (Packets) 0 (Bytes)
  Red packets   : 0 (Packets) 0 (Bytes)
Classifier: 2
  Operator: AND
  Rule(s) :
    If-match protocol ipv6
  Behavior: 2
  Accounting enable:
    0 (Packets)
  Filter enable: Permit
  Marking:
    Remark dscp 3
Classifier: 3
  Operator: AND
  Rule(s) :
    -none-
  Behavior: 3
    -none-

```

Table 22 Command output

Field	Description
Direction	Direction (inbound or outbound) in which the QoS policy is applied.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see [Table 15](#) and [Table 18](#).

display qos policy interface

Use **display qos policy interface** to display the QoS policies applied to interfaces.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

slot slot-number: Specifies an IRF member device by its member ID. If you do not specify an IRF member device, this command displays QoS policies on the master device. Only virtual interfaces such as VLAN interfaces and aggregate interfaces support this option.

inbound: Displays the QoS policy applied to the incoming traffic of the specified interface.

outbound: Displays the QoS policy applied to the outgoing traffic of the specified interface.

Usage guidelines

If you do not specify a direction, this command displays the QoS policy applied to incoming traffic and the QoS policy applied to outgoing traffic.

Examples

Display the QoS policy applied to the incoming traffic of HundredGigE 1/0/1.

```
<Sysname> display qos policy interface hundredgige 1/0/1 inbound
```

```
Interface: HundredGigE1/0/1
  Direction: Inbound
  Policy: 1
  Classifier: 1
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
    Operator: AND
  Rule(s) :
    If-match acl 2000
  Behavior: 1
  Marking:
    Remark dscp 3
  Committed Access Rate:
    CIR 112 (kbps), CBS 51200 (Bytes), EBS 512 (Bytes)
    Green action : pass
    Yellow action : pass
    Red action   : discard
    Green packets : 0 (Packets) 0 (Bytes)
    Yellow packets: 0 (Packets) 0 (Bytes)
    Red packets  : 0 (Packets) 0 (Bytes)
  Classifier: 2
    Matched : 0 (Packets) 0 (Bytes)
    5-minute statistics:
      Forwarded: 0/0 (pps/bps)
      Dropped  : 0/0 (pps/bps)
    Operator: AND
  Rule(s) :
    If-match protocol ipv6
  Behavior: 2
  Accounting enable:
    0 (Packets)
```

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

Display the QoS policies applied to all interfaces.

```
<Sysname> display qos policy interface
Interface: HundredGigE1/0/1
  Direction: Inbound
  Policy: a
  Classifier: a
  Operator: AND
  Rule(s) :
    If-match any
  Behavior: a
  Mirroring:
    Mirror to the interface: HundredGigE1/0/2
  Committed Access Rate:
    CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
    Green action : pass
    Yellow action : pass
    Red action   : discard
    Green packets : 0 (Packets)
    Red packets  : 0 (Packets)

Interface: HundredGigE1/0/3
  Direction: Inbound
  Policy: b
  Classifier: b
  Operator: AND
  Rule(s) :
    If-match any
  Behavior: b
  Committed Access Rate:
    CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
    Green action : pass
    Yellow action : pass
    Red action   : discard
    Green packets : 0 (Packets)
    Red packets  : 0 (Packets)
```

```

Interface: HundredGigE1/0/3
  Direction: Inbound
  Policy: a
  Classifier: a
    Operator: AND
    Rule(s) :
      If-match any
  Behavior: a
  Mirroring:
    Mirror to the interface: HundredGigE1/0/4
  Committed Access Rate:
    CIR 112 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
    Green action  : pass
    Yellow action : pass
    Red action    : discard
    Green packets : 0 (Packets)
    Red packets  : 0 (Packets)

```

Table 23 Command output

Field	Description
Direction	Direction in which the QoS policy is applied to the interface.
Matched	Number of matching packets.
Forwarded	Average rate of successfully forwarded matching packets in a statistics collection period.
Dropped	Average rate of dropped matching packets in a statistics collection period.
Green packets	Traffic statistics for green packets.
Yellow packets	Traffic statistics for yellow packets.
Red packets	Traffic statistics for red packets.

For the description of other fields, see [Table 15](#) and [Table 18](#).

display qos policy user-profile

Use **display qos policy user-profile** to display QoS policies applied to user profiles.

Syntax

```

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

```

Views

Any view

Predefined user roles

```

network-admin
network-operator

```

Parameters

name *profile-name*: Specifies a user profile by its name, a case-sensitive string of 1 to 31 characters. Valid characters include English letters, digits, and underscores (_). The name must start with an English letter and must be unique. If you do not specify a user profile, this command displays QoS policies applied to all user profiles.

user-id *user-id*: Specifies an online user by a system-assigned, hexadecimal ID in the range of 0 to fffffffe. If you do not specify an online user, this command displays QoS policies applied to user profiles for all online users.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS policies applied to user profiles for all member devices.

inbound: Specifies QoS policies applied to incoming traffic.

outbound: Specifies QoS policies applied to outgoing traffic.

Usage guidelines

If you do not specify a direction, this command displays QoS policies applied in the inbound direction and QoS policies applied in the outbound direction.

Examples

Display the QoS policy applied to user profile **abc** for a global user.

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

Display the QoS policy applied to user profile **abc** for a local user.

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


Table 24 Command output

Field	Description
global	Indicates a global user, who comes online from a global interface such as an aggregate interface.
local	Indicates a local user, who comes online from a physical interface.
Matched	Number of packets that meet match criteria.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see [Table 15](#) and [Table 18](#).

display qos vlan-policy

Use **display qos vlan-policy** to display QoS policies applied to VLANs.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

name *policy-name*: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

vlan *vlan-id*: Specifies a VLAN by its ID in the range of 1 to 4094.

inbound: Displays QoS policies applied to incoming traffic.

outbound: Displays QoS policies applied to outgoing traffic.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays QoS policies applied to VLANs for the master device.

Usage guidelines

If you do not specify a direction, this command displays QoS policies applied to VLANs in both the inbound and outbound directions.

Examples

```
# Display QoS policies applied to VLAN 2.  
<Sysname> display qos vlan-policy vlan 2  
Vlan 2  
  Direction: Outbound  
  Policy: 1  
  Classifier: 1  
    Operator: AND  
  Rule(s) :  
    If-match acl 2000
```

```

Behavior: 1
Marking:
  Remark dscp 3
Committed Access Rate:
  CIR 112 (kbps), CBS 5120 (Bytes), EBS 512 (Bytes)
  Green action : pass
  Yellow action : pass
  Red action   : discard
  Green packets : 0 (Packets) 0 (Bytes)
  Yellow packets: 0 (Packets) 0 (Bytes)
  Red packets  : 0 (Packets) 0 (Bytes)
Classifier: 2
Operator: AND
Rule(s) :
  If-match protocol ipv6
Behavior: 2
Accounting enable:
  0 (Packets)
Filter enable: Permit
Marking:
  Remark dscp 3
Classifier: 3
Operator: AND
Rule(s) :
  -none-
Behavior: 3
  -none-

```

Table 25 Command output

Field	Description
Direction	Direction in which the QoS policy is applied for the VLAN.
Green packets	Statistics about green packets.
Yellow packets	Statistics about yellow packets.
Red packets	Statistics about red packets.

For the description of other fields, see [Table 15](#) and [Table 18](#).

qos apply policy (interface view, control plane view)

Use **qos apply policy** to apply a QoS policy to an interface or control plane.

Use **undo qos apply policy** to remove an applied QoS policy.

Syntax

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

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

Default

No QoS policy is applied.

Views

Control plane view
Layer 2/Layer 3 Ethernet interface view
Layer 3 Ethernet subinterface view
Layer 2/Layer 3 aggregate interface view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to incoming traffic.

outbound: Applies the QoS policy to outgoing traffic. This keyword is not supported in control plane view.

Usage guidelines

If a class uses control plane protocols or control plane protocol groups as match criteria, the action in the associated traffic behavior can only be **car** or the combination of **car** and **accounting packet**. Only the **cir** keyword in the **car** action can be applied correctly.

You can apply a QoS policy to only the inbound direction of a Layer 2 or Layer 3 aggregate interface.

Examples

Apply QoS policy **USER1** to the outgoing traffic of HundredGigE 1/0/1.

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos apply policy USER1 outbound
```

Apply QoS policy **aaa** to the incoming traffic of the control plane of slot 3.

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

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 a QoS policy applied to a user profile.

Syntax

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

Default

No QoS policy is applied to a user profile.

Views

User profile view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to the incoming traffic of the device (traffic sent by online users).

outbound: Applies the QoS policy to the outgoing traffic of the device (traffic received by online users).

Usage guidelines

Deleting a user profile also removes the QoS policies applied to the user profile.

Examples

```
# Apply QoS policy test to incoming traffic of user profile user.
<Sysname> system-view
[Sysname] user-profile user
[Sysname-user-profile-user] qos apply policy test outbound
```

qos apply policy global

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

Use **undo qos apply policy global** to remove a globally applied QoS policy.

Syntax

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

Default

No QoS policy is applied globally.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

inbound: Applies the QoS policy to the incoming packets on all interfaces.

outbound: Applies the QoS policy to the outgoing packets on all interfaces.

Usage guidelines

A global QoS policy takes effect on all incoming or outgoing traffic depending on the direction in which the QoS policy is applied.

Examples

```
# Globally apply QoS policy user1 to the incoming traffic.
<Sysname> system-view
[Sysname] qos apply policy user1 global inbound
```

qos policy

Use **qos policy** to create a QoS policy and enter its view, or enter the view of an existing QoS policy.

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

Syntax

```
qos policy policy-name
```

undo qos policy *policy-name*

Default

No QoS policies exist.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a name for the QoS policy, a case-sensitive string of 1 to 31 characters.

Usage guidelines

To delete a QoS policy that has been applied to an object, you must first remove the QoS policy from the object.

Examples

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

Related commands

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

qos vlan-policy

Use **qos vlan-policy** to apply a QoS policy to the specified VLANs.

Use **undo qos vlan-policy** to remove a QoS policy from the specified VLANs.

Syntax

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

Default

No QoS policy is applied to a VLAN.

Views

System view

Predefined user roles

network-admin

Parameters

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters.

vlan *vlan-id-list*: Specifies a space-separated list of up to eight VLAN IDs or a VLAN ID range in the form of *vlan-id1* to *vlan-id2*. The value for *vlan-id2* must be greater than or equal to the value for *vlan-id1*. The value range for the *vlan-id* argument is 1 to 4094.

inbound: Applies the QoS policy to incoming packets.

outbound: Applies the QoS policy to outgoing packets.

Examples

```
# Apply QoS policy test to the incoming traffic of VLAN 200, VLAN 300, VLAN 400, and VLAN 500.
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 inbound
```

reset qos policy control-plane

Use **reset qos policy control-plane** to clear the statistics of the QoS policy applied to a control plane.

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

Examples

```
# Clear the statistics of the QoS policy applied to the control plane of slot 3.
<Sysname> reset qos policy control-plane slot 3
```

reset qos policy global

Use **reset qos policy global** to clear the statistics of a global QoS policy.

Syntax

```
reset qos policy global [ inbound | outbound ]
```

Views

User view

Predefined user roles

network-admin

Parameters

inbound: Clears the statistics of the global QoS policy applied to incoming traffic globally.

outbound: Clears the statistics of the global QoS policy applied to outgoing traffic globally.

Usage guidelines

If you do not specify a direction, this command clears the statistics of the global QoS policies in both directions.

Examples

```
# Clear the statistics of the global QoS policy applied to the incoming traffic globally.
<Sysname> reset qos policy global inbound
```

reset qos vlan-policy

Use **reset qos vlan-policy** to clear the statistics of the QoS policy applied in a certain direction of a VLAN.

Syntax

```
reset qos vlan-policy [ vlan vlan-id ] [ inbound | outbound ]
```

Views

User view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN ID in the range of 1 to 4094.

inbound: Clears the statistics of the QoS policy applied to the incoming traffic of the specified VLAN.

outbound: Clears the statistics of the QoS policy applied to the incoming traffic of the specified VLAN.

Usage guidelines

If you do not specify a direction, this command clears the statistics of the QoS policies in both directions of the VLAN.

Examples

```
# Clear the statistics of QoS policies applied to VLAN 2.
```

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

Priority mapping commands

Priority map commands

display qos map-table

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

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

The device provides the following types of priority map.

Table 26 Priority maps

Priority mapping	Description
dot1p-dp	802.1p-drop priority map.
dot1p-exp	802.1p-EXP priority map.
dot1p-lp	802.1p-local priority map.
dscp-dot1p	DSCP-802.1p priority map.
dscp-dp	DSCP-drop priority map.
dscp-dscp	DSCP-DSCP priority map.
exp-dot1p	EXP-802.1p priority map.
exp-dp	EXP-drop priority map.

Usage guidelines

If you do not specify a priority map, this command displays the configuration of all priority maps.

Examples

```
# Display the configuration of the 802.1p-local priority map.
```

```
<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 27 Command output

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

import

Use **import** to configure mappings for a priority map.

Use **undo import** to restore the specified or all mappings to the default for a priority map.

Syntax

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

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

Default

The default priority maps are used. For more information, see *ACL and QoS Configuration Guide*.

Views

Priority map view

Predefined user roles

network-admin

Parameters

import-value-list: Specifies a list of input values.

export-value: Specifies the output value.

all: Restores all mappings in the priority map to the default.

Examples

Configure the 802.1p-local priority map to map 802.1p priority values 4 and 5 to local priority 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 map view.

Syntax

qos map-table{ **dot1p-dp** | **dot1p-exp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **exp-dot1p** | **exp-dp** }

Views

System view

Predefined user roles

network-admin

Parameters

For the description of other keywords, see [Table 26](#).

Examples

```
# Enter 802.1p-local priority map view.
<Sysname> system-view
[Sysname] qos map-table dot1p-1p
[Sysname-maptbl-dot1p-1p]
```

Related commands

display qos map-table
import

Priority trust mode commands

display qos trust interface

Use **display qos trust interface** to display the priority trust mode and port priorities of an interface.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface-type interface-number. Specifies an interface by its type and number. If you do not specify an interface, this command displays the priority trust mode and port priorities of all interfaces.

Examples

```
# Display the priority trust mode and port priority of HundredGigE 1/0/1.
<Sysname> display qos trust interface hundredgige 1/0/1
Interface: HundredGigE1/0/1
  Port priority trust information
  Port priority:4
  Port dscp priority: -
  Port priority trust type: dscp
```

Table 28 Command output

Field	Description
Interface	Interface type and interface number.

Field	Description
Port priority	Port priority set for the interface.
Port dscp priority	DSCP value rewritten for packets. If you have not rewritten the DSCP value of packets, this field displays a hyphen (-).
Port priority trust type	Priority trust mode on the interface: dot1p , dscp , or none . If the trust mode is none , the port priority is used for priority mapping.

qos trust

Use **qos trust** to configure the priority trust mode for an interface.

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

Syntax

```
qos trust { dot1p | dscp }
```

```
undo qos trust
```

Default

An interface does not trust any packet priority and uses the port priority as the 802.1p priority for mapping.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

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

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

Examples

```
# Set the priority trust mode to 802.1p priority on HundredGigE 1/0/1.
```

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

```
[Sysname] interface hundredgige 1/0/1
```

```
[Sysname-HundredGigE1/0/1] qos trust dot1p
```

Related commands

```
display qos trust interface
```

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 [ dscp ] priority-value
```

```
undo qos priority [ dscp ]
```

Default

The port priority is 0, and the DSCP value of packets is not modified.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

priority-value: Specifies a priority value. If the **dscp** keyword is not specified, this argument specifies the port priority in the range of 0 to 7. If the **dscp** keyword is specified, this argument specifies the DSCP value to be set for packets, in the range of 0 to 63.

Usage guidelines

When no priority trust mode is configured for an interface, the interface uses the port priority as the 802.1p priority for priority mapping. If the **qos priority dscp *priority-value*** command is configured, the interface modifies the DSCP value of Layer 3 packets in addition to performing priority mapping.

This command is no longer in effect after a priority trust mode is configured.

Examples

Set the port priority of HundredGigE 1/0/1 to 2, and modify the DSCP value of Layer 3 packets to 20.

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos priority 2
[Sysname-HundredGigE1/0/1] qos priority dscp 20
```

Related commands

display qos trust interface

GTS and rate limit commands

GTS commands

display qos gts interface

Use **display qos gts interface** to display the GTS information for interfaces.

Syntax

```
display qos gts interface [ interface-type interface-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number. Specifies an interface by its type and number. If you do not specify an interface, this command displays the GTS information for all interfaces.

Examples

Display the GTS information for all interfaces.

```
<Sysname> display qos gts interface
Interface: HundredGigE1/0/1
Rule: If-match acl 2001
  CIR 512 (kbps), CBS 51200 (Bytes), PIR 5120 (kbps), EBS 0 (Bytes)
  Queue Length: 100 (Packets)
  Queue Size: 70 (Packets)
  Passed   : 0 (Packets) 0 (Bytes)
  Discarded: 0 (Packets) 0 (Bytes)
  Delayed  : 0 (Packets) 0 (Bytes)

Interface: HundredGigE1/0/2
Rule: If-match acl 2001
  CIR 64 (kbps), CBS 51200 (Bytes), EBS 0 (Bytes)
  Queue Length: 100 (Packets)
  Queue Size: 70 (Packets)
  Passed   : 0 (Packets) 0 (Bytes)
  Discarded: 0 (Packets) 0 (Bytes)
  Delayed  : 0 (Packets) 0 (Bytes)
```

Table 29 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Rule	Match criteria.
CIR	CIR in kbps.

Field	Description
CBS	CBS in bytes.
EBS	EBS in bytes.
PIR	PIR in kbps.
Queue Length	Number of packets that the buffer can hold.
Queue Size	Number of packets in the buffer.
Passed	Number and bytes of packets that have been forwarded.
Discarded	Number and bytes of dropped packets.
Delayed	Number and bytes of delayed packets.

qos gts

Use **qos gts** to set GTS parameters on an interface.

Use **undo qos gts** to delete the GTS configuration on an interface.

Syntax

```
qos gts queue queue-id cir committed-information-rate [ cbs committed-burst-size ]
undo qos gts queue queue-id
```

Default

No GTS parameters are configured on an interface.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue *queue-id*: Shapes the packets in a queue specified by its ID. The value range for *queue-id* is 0 to 7.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 8 to 10000000 for 10-GE interfaces, 8 to 25000000 for 25-GE interfaces, and 8 to 100000000 for 100-GE interfaces. The specified value must be an integral multiple of 8.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 16000000, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 16000000 is converted to 16000000.

Usage guidelines

The specified CIR does not take interframe gaps into account and is smaller than the actually shaped rate on an interface.

An interframe gap is a time interval of 12 bits between frames. This gap serves the following roles:

- Allows the device to differentiate one frame from another.
- Allows for time for the device to process the current frame and to be prepared to receive the next frame.

Examples

```
# Shape the packets of queue 1 on HundredGigE 1/0/9 (CIR 6400 kbps and CBS 51200 bytes).
<Sysname> system-view
[Sysname] interface hundredgige 1/0/9
[Sysname- HundredGigE1/0/9] qos gts queue 1 cir 6400 cbs 51200
```

Rate limit commands

display qos lr interface

Use **display qos lr interface** to display the rate limit information for interfaces.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface-type interface-number. Specifies an interface by its type and number. If you do not specify an interface, this command displays the rate limit information for all interfaces.

Examples

```
# Display the rate limit information for all interfaces.
<Sysname> display qos lr interface
Interface: HundredGigE1/0/1
Direction: Inbound
CIR 2000 (kbps), CBS 20480 (Bytes)
```

Table 30 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Direction	Direction to which the rate limit configuration is applied: inbound or outbound.
CIR	CIR in kbps.
CBS	CBS in bytes.
EBS	EBS in bytes.
Passed	Number and bytes of packets that have passed.
Discarded	Number and bytes of dropped packets.
Delayed	Number and bytes of delayed packets.

qos lr

Use **qos lr** to configure rate limiting on an interface.

Use **undo qos lr** to delete the rate limit configuration.

Syntax

```
qos lr { inbound | outbound } cir committed-information-rate [ cbs committed-burst-size ]  
undo qos lr { inbound | outbound }
```

Default

No rate limit is configured on an interface.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

inbound: Limits the rate of incoming packets.

outbound: Limits the rate of outgoing packets.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for *committed-information-rate* is 8 to 10000000 for 10-GE interfaces, 8 to 25000000 for 25-GE interfaces, and 8 to 100000000 for 100-GE interfaces. The specified value must be an integral multiple of 8.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 128000000, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 128000000 is converted to 128000000.

Examples

Limit the rate of outgoing packets on HundredGigE 1/0/1, with CIR 256 kbps and CBS 51200 bytes.

```
<Sysname> system-view  
[Sysname] interface hundredgige 1/0/1  
[Sysname-HundredGigE1/0/1] qos lr outbound cir 256 cbs 51200
```


Congestion management commands

Common commands

display qos queue interface

Use **display qos queue interface** to display the queuing information for interfaces.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number. Specifies an interface by its type and number. If you do not specify an interface, this command displays the queuing information for all interfaces.

Examples

Display the queuing information for all interfaces.

```
<Sysname> display qos queue interface
```

```
Interface: HundredGigE1/0/1
```

```
Output queue: Weighted Round Robin queuing
```

```
Queue ID      Queue name    Group      Byte count
```

```
-----  
0             be           1          1  
1             af1          1          2  
2             af2          1          3  
3             af3          1          4  
4             af4          1          5  
5             ef           1          9  
6             cs6          1         13  
7             cs7          1         15
```

```
Interface: HundredGigE1/0/2
```

```
Output queue: Weighted Round Robin queuing
```

```
Queue ID      Queue name    Group      Byte count
```

```
-----  
0             be           1          1  
1             af1          1          2  
2             af2          1          3  
3             af3          1          4  
4             af4          1          5  
5             ef           1          9  
6             cs6          1         13
```

Table 31 Command output

Field	Description
Interface	Interface name, including the interface type and interface number.
Output queue	Type of the current output queue.
Group	Number of the group that holds the queue. The group number can only be 1.
Weight	Packet-count scheduling weight of the queue.
Byte-count	Byte-count scheduling weight of the queue.

SP commands

display qos queue sp interface

Use **display qos queue sp interface** to display the SP queuing configuration of an interface.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number. Specifies an interface by its type and number. If you do not specify an interface, this command displays the SP queuing configuration of all interfaces.

Examples

```
# Display the SP queuing configuration of HundredGigE 1/0/1.
<Sysname> display qos queue sp interface hundredgige 1/0/1
Interface: HundredGigE1/0/1
Output queue: Strict Priority queuing
```

Table 32 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Type of the current output queue.

qos sp

Use **qos sp** to enable SP queuing on an interface.

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

Syntax

```
qos sp
undo qos sp
```

Default

WRR queuing is used on an interface, and queues 0 through 7 have a weight of 1, 2, 3, 4, 5, 9, 13, and 15, respectively.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Examples

```
# Enable SP queuing on HundredGigE 1/0/1.
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos sp
```

Related commands

display qos queue sp interface

WRR commands

display qos queue wrr interface

Use **display qos queue wrr interface** to display the WRR queuing configuration of an interface.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface-type interface-number. Specifies an interface by its type and number. If you do not specify an interface, this command displays the WRR queuing configuration of all interfaces.

Examples

```
# Display the WRR queuing configuration of HundredGigE 1/0/1.
<Sysname> display qos queue wrr interface hundredgige 1/0/1
Interface: HundredGigE1/0/1
Output queue: Weighted Round Robin queuing
Queue ID      Queue name    Group      Weight
-----
0             be           1          1
1             af1         1          1
```

2	af2	1	1
3	af3	1	1
4	af4	1	1
5	ef	1	1
6	cs6	1	1
7	cs7	sp	N/A

Table 33 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Type of the current output queue.
Group	Number of the group a queue is assigned to. By default, all queues belong to group 1.
Weight	Packet-based queue scheduling weight of a queue. N/A is displayed for a queue that uses the SP scheduling algorithm.
Byte count	Byte-based scheduling weight of a queue.

qos wrr

Use **qos wrr** to enable WRR queuing on an interface.

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

Syntax

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

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

Default

WRR queuing is used on an interface, and queues 0 through 7 have a weight of 1, 2, 3, 4, 5, 9, 13, and 15, respectively.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

byte-count: Allocates bandwidth to queues in terms of bytes.

weight: Allocates bandwidth to queues based on their weights.

Usage guidelines

You must use the **qos wrr** command to enable WRR queuing before you can configure WRR queuing parameters for a queue on an interface.

Examples

Enable weight-based WRR queuing on HundredGigE 1/0/1.

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos wrr weight
```

Enable byte-count WRR queuing on HundredGigE 1/0/1.

```

<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos wrr byte-count

```

Related commands

display qos queue wrr interface

qos wrr { byte-count | weight }

Use **qos wrr { byte-count | weight }** to configure the WRR queuing parameters for a queue on an interface.

Use **undo qos wrr** to delete the WRR queuing parameters of a queue on an interface.

Syntax

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

undo qos wrr *queue-id*

Default

All queues on a WRR-enabled interface are in WRR group 1, and queues 0 through 7 have a weight of 1, 2, 3, 4, 5, 9, 13, and 15, respectively.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in [Table 34](#).

Table 34 The number-keyword map for the *queue-id* argument

Number	Keyword
0	be
1	af1
2	af2
3	af3
4	af4
5	ef
6	cs6
7	cs7

group 1: Specifies WRR group 1. Only WRR group 1 is supported in the current software version.

byte-count: Allocates bandwidth to queues in terms of bytes.

weight: Allocates bandwidth to queues based on their weights.

schedule-value: Specifies a scheduling weight for the specified queue in WRR queuing. The value range for this argument is 1 to 15.

Usage guidelines

You must use the **qos wrr** command to enable WRR queuing before you can configure WRR queuing parameters for a queue on an interface.

Examples

```
# Enable packet-based WRR queuing on HundredGigE 1/0/1, assign queue 0 to WRR group 1, and specify scheduling weight 10 for queue 0.
```

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos wrr weight
[Sysname-HundredGigE1/0/1] qos wrr 0 group 1 weight 10
```

Related commands

display qos queue wrr interface
qos wrr

qos wrr group sp

Use **qos wrr group sp** to assign a queue to the SP group.

Use **undo qos wrr group sp** to remove a queue from the SP group.

Syntax

```
qos wrr queue-id group sp  
undo qos wrr queue-id
```

Default

All queues on a WRR-enabled interface are in WRR group 1.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in [Table 34](#).

Usage guidelines

This command is available only on a WRR-enabled interface. Queues in the SP group are scheduled with SP. The SP group has higher scheduling priority than the WRR groups.

You must use the **qos wrr** command to enable WRR queuing before you can configure this command on an interface.

Examples

```
# Enable WRR queuing on HundredGigE 1/0/1, and assign queue 0 to the SP group.
```

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos wrr weight
[Sysname-HundredGigE1/0/1] qos wrr 0 group sp
```

Related commands

display qos queue wrr interface

qos wrr

WFQ commands

display qos queue wfq interface

Use **display qos queue wfq interface** to display the WFQ configuration of an interface.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number. Specifies an interface by its type and number. If you do not specify an interface, this command displays the WFQ configuration of all interfaces.

Examples

Display the WFQ configuration of HundredGigE 1/0/1.

```
<Sysname> display qos wfq interface hundredgige 1/0/1
```

```
Interface: HundredGigE1/0/1
```

```
Output queue: Hardware Weighted Fair Queuing
```

Queue ID	Queue name	Group	Byte count	Min Bandwidth
0	be	1	1	64
1	af1	1	1	64
2	af2	1	1	64
3	af3	1	1	64
4	af4	1	1	64
5	ef	1	1	64
6	cs6	1	1	64
7	cs7	1	1	64

Table 35 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Type of the current output queue.
Group	Number of the group that holds the queue. By default, all queues are in group 1.
Byte-count	Byte-count scheduling weight of the queue.
Min Bandwidth	Minimum guaranteed bandwidth for the queue.

qos bandwidth queue

Use **qos bandwidth queue** to set the minimum guaranteed bandwidth for a queue on an interface.

Use **undo qos bandwidth queue** to restore the default.

Syntax

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

undo qos bandwidth queue *queue-id*

Default

The minimum guaranteed bandwidth for a queue is 64 kbps.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in [Table 34](#).

min *bandwidth-value*: Sets the minimum guaranteed bandwidth in kbps. The value range for the *bandwidth-value* argument is 8 to 10000000 for 10-GE interfaces and 8 to 100000000 for 100-GE interfaces.

Usage guidelines

The minimum guaranteed bandwidth is the amount of bandwidth guaranteed for a queue when the interface is congested.

You must use the **qos wfq** command to enable WFQ before you can configure this command on an interface.

Examples

```
# Set the minimum guaranteed bandwidth to 100 kbps for queue 0 on HundredGigE 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos wfq weight
[Sysname-HundredGigE1/0/1] qos bandwidth queue 0 min 100
```

Related commands

qos wfq

qos wfq

Use **qos wfq** to enable WFQ on an interface.

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

Syntax

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

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

Default

Byte-count WRR queuing is used on an interface, and queues 0 through 7 have a weight of 1, 2, 3, 4, 5, 9, 13, and 15, respectively.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

byte-count: Allocates bandwidth to queues in terms of bytes.

weight: Allocates bandwidth to queues based on their weights.

Usage guidelines

You must use the **qos wfq** command to enable WFQ before you can configure WFQ queuing parameters for a queue on an interface.

Examples

```
# Enable weight-based WFQ on HundredGigE 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos wfq weight
```

```
# Enable byte-count WFQ on HundredGigE 1/0/1.
```

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos wfq byte-count
```

Related commands

display qos queue wfq interface

qos wfq { byte-count | weight }

Use **qos wfq { byte-count | weight }** to assign a queue to a WFQ group with a certain scheduling weight.

Use **undo qos wfq** to delete the WFQ queuing parameters of a queue on an interface.

Syntax

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

undo qos wfq *queue-id*

Default

All queues on a WFQ-enabled interface are in WFQ group 1 and have a weight of 1.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in [Table 34](#).

group 1: Specifies WFQ group 1. Only WFQ group 1 is supported in the current software version.

byte-count: Allocates bandwidth to queues in terms of bytes.

weight: Allocates bandwidth to queues based on their weights.

schedule-value: Specifies a scheduling weight for the specified queue in WFQ queuing. The value range for this argument is 1 to 15.

Usage guidelines

You must use the **qos wfq** command to enable WFQ before you configure this command.

Examples

```
# Enable byte-count WFQ on HundredGigE 1/0/1, and specify scheduling weight 10 for queue 0.
```

```
<Sysname> system-view
[Sysname] interface hundredgige 1/0/1
[Sysname-HundredGigE1/0/1] qos wfq byte-count
[Sysname-HundredGigE1/0/1] qos wfq 0 group 1 byte-count 10
```

Related commands

display qos queue wfq interface

qos bandwidth queue

qos wfq

qos wfq group sp

Use **qos wfq group sp** to assign a queue to the SP group.

Use **undo qos wfq group sp** to remove a queue from the SP group.

Syntax

qos wfq *queue-id* group sp

undo qos wfq *queue-id*

Default

All queues on a WFQ-enabled interface are in WFQ group 1.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7 or keywords in [Table 34](#).

Usage guidelines

This command is available only on a WFQ-enabled interface. Queues in the SP group are scheduled with SP, instead of WFQ. The SP group has higher scheduling priority than the WFQ groups.

You must use the **qos wfq** command to enable WFQ before you configure this command.

Examples

```
# Enable WFQ on HundredGigE 1/0/1, and assign queue 0 to the SP group.
```

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

```
[Sysname-HundredGigE1/0/1] qos wfq weight
[Sysname-HundredGigE1/0/1] qos wfq 0 group sp
```

Related commands

display qos queue wfq interface

qos bandwidth queue

qos wfq

Queue-based accounting commands

display qos queue-statistics interface outbound

Use **display qos queue-statistics interface outbound** to display queue-based outgoing traffic statistics for interfaces.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number. Specifies an interface by its type and number. If you do not specify an interface, this command displays the queue-based outgoing traffic statistics for all interfaces.

Examples

```
# Display queue-based outgoing traffic statistics for HundredGigE 1/0/1.
<Sysname> display qos queue-statistics interface hundredgige 1/0/1 outbound
Interface: HundredGigE1/0/1
Direction: outbound
Forwarded: 0 packets, 0 bytes
Dropped: 0 packets, 0 bytes
Queue 0
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
Queue 1
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
Queue 2
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
Queue 3
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
```

```

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

```

Table 36 Command output

Field	Description
Interface	Interface for which queue-based traffic statistics are displayed.
Direction	Direction of traffic for which statistics are collected.
Forwarded	Counts forwarded traffic both in packets and in bytes.
Dropped	Counts dropped traffic both in packets and in bytes.
Current queue length	Current queue length.

Related commands

reset counters interface (*Interface Command Reference*)

Congestion avoidance commands

WRED commands

display qos wred interface

Use **display qos wred interface** to display the WRED information for interfaces.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

interface-type interface-number. Specifies an interface by its type and number. If you do not specify an interface, this command displays the WRED information for all interfaces.

Examples

Display the WRED information for all interfaces.

```
<Sysname> display qos wred interface
Interface: HundredGigE1/0/3
Current WRED configuration:
Applied WRED table name: q1
```

Table 37 Command output

Field	Description
Interface	Interface type and interface number.

display qos wred table

Use **display qos wred table** to display the WRED table configuration.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

name *table-name*: Specifies a WRED table by its name, a case-sensitive string of 1 to 32 characters. If you do not specify a WRED table, this command displays the configuration of all WRED tables.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays the WRED table configuration for the master device.

Examples

Display the configuration of WRED table 1.

```
<Sysname> display qos wred table name 1
```

```
Table name: 1
```

```
Table type: Queue based WRED
```

QID	gmin	gmax	gprob	ymin	ymax	yprob	rmin	rmax	rprob	exponent	ECN
0	100	1000	10	100	1000	10	100	1000	10	9	N
1	100	1000	10	100	1000	10	100	1000	10	9	N
2	100	1000	10	100	1000	10	100	1000	10	9	N
3	100	1000	10	100	1000	10	100	1000	10	9	N
4	100	1000	10	100	1000	10	100	1000	10	9	N
5	100	1000	10	100	1000	10	100	1000	10	9	N
6	100	1000	10	100	1000	10	100	1000	10	9	N
7	100	1000	10	100	1000	10	100	1000	10	9	N

Table 38 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.
ECN	Indicates whether ECN is enabled for the queue: <ul style="list-style-type: none">• Y—Enabled.• N—Disabled.

qos wred apply

Use **qos wred apply** to apply a WRED table to an interface.

Use **undo qos wred apply** to restore the default.

Syntax

```
qos wred apply [ table-name ]  
undo qos wred apply
```

Default

No WRED table is applied to an interface, and the tail drop mode is used on an interface.

Views

Layer 2/Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

table-name: Specifies a WRED table by its name, a case-sensitive string of 1 to 32 characters. If you do not specify a WRED table, this command applies the default WRED table to the interface.

Examples

```
# Apply WRED table table1 to HundredGigE 1/0/1.  
<Sysname> system-view  
[Sysname] interface hundredgige 1/0/1  
[Sysname-HundredGigE1/0/1] qos wred apply table1
```

Related commands

```
display qos wred interface  
display qos wred table  
qos wred queue table
```

qos wred queue table

Use **qos wred queue table** to create a WRED table and enter its view, or enter the view of an existing WRED table.

Use **undo qos wred queue table** to delete a WRED table.

Syntax

```
qos wred queue table table-name  
undo qos wred queue table table-name
```

Default

No WRED tables exist.

Views

System view

Predefined user roles

network-admin

Parameters

table *table-name*: Specifies a name for the WRED table, a case-sensitive string of 1 to 32 characters.

Usage guidelines

You cannot delete a WRED table in use. To delete it, first remove it from the specified interface.

You can use the **display qos wred table** command to display the default WRED table, which cannot be modified or deleted.

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

display qos wred table

queue

Use **queue** to configure the drop-related parameters for a queue in the queue-based WRED table.

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

Syntax

```
queue queue-id [ drop-level drop-level ] low-limit low-limit high-limit high-limit
[ discard-probability discard-prob ]
undo queue { queue-id | all }
```

Default

The lower limit is 100, the upper limit is 1000, and the drop probability is 10%.

Views

WRED table view

Predefined user roles

network-admin

Parameters

all: Specifies all queues.

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7.

drop-level *drop-level*: Specifies a drop level. This argument is a consideration for dropping packets. The value 0 corresponds to green packets, the value 1 corresponds to yellow packets, and the value 2 corresponds to red packets. If you do not specify a drop level, the subsequent configuration takes effect on the packets in the queue regardless of the drop level.

low limit *low-limit*: Specifies the lower limit for the average queue length. The default and the value range for *low-limit* is 0 to 38000.

high-limit *high-limit*: Specifies the upper limit for the average queue length. The upper limit must be greater than the lower limit. The value range for *high-limit* is 0 to 38000.

discard-probability *discard-prob*: Specifies the denominator for drop probability calculation. The greater the denominator, the smaller the calculated drop probability. The value range for *discard-prob* is 0 to 100.

Usage guidelines

When the average queue size is smaller than the lower threshold, no packet is dropped. When the average queue size is between the lower threshold and the upper threshold, the packets are dropped at random. The longer the queue is, the higher the drop probability is. When the average queue size exceeds the upper threshold, subsequent packets are dropped.

Examples

In queue-based WRED table **queue-table1**, configure the following drop-related parameters for packets in queue 1:

- The drop level is 1.
- The lower limit for the average queue length is 10.
- The upper limit for the average queue length is 20.
- The drop probability is 30%.

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

```
[Sysname] qos wred queue table queue-table1
```

```
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 10 high-limit 20  
discard-probability 30
```

Related commands

display qos wred table

qos wred queue table

queue ecn

Use **queue ecn** to enable ECN for a queue.

Use **undo queue ecn** to restore the default.

Syntax

queue *queue-id* **ecn**

undo queue *queue-id* **ecn**

Default

ECN is disabled for a queue.

Views

WRED table view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID in the range of 0 to 7.

Usage guidelines

When both the receiver and sender support ECN, the device can notify the peer end of the congestion status by identifying and setting the ECN flag. ECN avoids deteriorating congestion.

Examples

In WRED table **queue-table1**, enable ECN for queue 1.

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

```
[Sysname] qos wred queue table queue-table1
```

```
[Sysname-wred-table-queue-table1] queue 1 ecn
```

Related commands

display qos wred table

qos wred queue table

queue weighting-constant

Use **queue weighting-constant** to specify an exponent for average queue length calculation for a queue.

Use **undo queue weighting-constant** to restore the default.

Syntax

queue *queue-id* **weighting-constant** *exponent*

undo queue *queue-id* **weighting-constant**

Default

The exponent for average queue length calculation is 9.

Views

WRED table view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value range for this argument is 0 to 7.

weighting-constant *exponent*: Specifies the WRED exponent for average queue length calculation. The value range for *exponent* is 0 to 15.

Usage guidelines

The bigger the exponent is, the less sensitive the average queue size is to real-time queue size changes. The average queue size is calculated using the formula:

Average queue size = previous average queue size $\times (1-2^{-n})$ + current queue size $\times 2^{-n}$,

where n can be configured with the **qos wred weighting-constant** command.

Examples

In WRED table **queue-table1**, set the exponent for average queue length calculation to 12 for queue 1.

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

```
[Sysname] qos wred queue table queue-table1
```

```
[Sysname-wred-table-queue-table1] queue 1 weighting-constant 12
```

Related commands

display qos wred table

qos wred queue table

Aggregate CAR commands

car name

Use **car name** to use an aggregate CAR action in a traffic behavior.

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

Syntax

car name *car-name*

undo car

Default

No aggregate CAR action is configured in a traffic behavior.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

car-name: Specifies the name of an aggregate CAR action. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters.

Examples

```
# Use aggregate CAR action aggcar-1 in traffic behavior be1.
```

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

```
[Sysname] traffic behavior be1
```

```
[Sysname-behavior-be1] car name aggcar-1
```

Related commands

display qos car name

display traffic behavior user-defined

display qos car name

Use **display qos car name** to display information about aggregate CAR actions.

Syntax

display qos car name [*car-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

car-name: Specifies an aggregate CAR action by its name. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters. If you do not specify an aggregate CAR action, this command displays information about all aggregate CAR actions.

Examples

Display information about all aggregate CAR actions.

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

Table 39 Command output

Field	Description
Name	Name of the aggregate CAR action.
Mode	Type of the CAR action, which can only be aggregative .
CIR CBS PIR EBS	Parameters for the CAR action.
Green action	Action to take on green packets: <ul style="list-style-type: none">• discard—Drops the packets.• pass—Permits the packets to pass through.
Yellow action	Action to take on yellow packets: <ul style="list-style-type: none">• discard—Drops the packets.• pass—Permits the packets to pass through.
Red action	Action to take on red packets: <ul style="list-style-type: none">• discard—Drops the packets.• pass—Permits the packets to pass through.
Green packet	Statistics about green packets.
Yellow packet	Statistics about yellow packets.
Red packet	Statistics about red packets.

qos car (system view)

Use **qos car aggregative** to configure an aggregate CAR action.

Use **undo qos car** to delete an aggregate CAR action.

Syntax

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

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

undo qos car *car-name*

Default

No aggregate CAR action is configured.

Views

System view

Predefined user roles

network-admin

Parameters

car-name: Specifies the name of the aggregate CAR action. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters.

cir *committed-information-rate*: Specifies the CIR in kbps, which is an average traffic rate. The value range for *committed-information-rate* is 8 to 160000000, in increments of 8.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for *committed-burst-size* is 512 to 256000000, in increments of 512. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product. A default value greater than 256000000 is converted to 256000000.

ebs *excess-burst-size*: Specifies the EBS in bytes. The value range for *excess-burst-size* is 0 to 256000000, in increments of 512. If the PIR is configured, the default EBS is the product of 62.5 and the PIR and must be an integral multiple of 512. When the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512. A default value greater than 256000000 is converted to 256000000.

pir *peak-information-rate*: Specifies the PIR in kbps. The value range for *peak-information-rate* is 8 to 160000000, in increments of 8.

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

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

yellow *action*: Specifies the action to take on packets that conform to PIR but not to CIR. The default setting is **pass**.

action: Specifies the action to take on packets:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument is in the range of 0 to 7.
- **remark-dscp-pass** *new-dscp*: Remarks the packet with a new DSCP value and permits the packet to pass through. The *new-dscp* argument is in the range of 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**.

Usage guidelines

To use two rates for aggregate CAR, configure the **qos car** command with the **pir peak-information-rate** option. To use one rate for aggregate CAR, configure the **qos car** command without the **pir peak-information-rate** option.

An aggregate CAR action takes effect only after it is applied to an interface or used in a QoS policy.

Examples

Configure aggregate CAR action **aggcar-1**, where CIR is 25600, CBS is 512000, and red packets are dropped.

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

Related commands

display qos car name

reset qos car name

Use **reset qos car name** to clear the statistics about aggregate CAR actions.

Syntax

```
reset qos car name [ car-name ]
```

Views

User view

Predefined user roles

network-admin

Parameters

car-name: Specifies an aggregate CAR action by its name. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters. If you do not specify an aggregate CAR action, this command clears statistics for all aggregate CAR actions.

Examples

Clear the statistics about aggregate CAR action **aggcar-1**.

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

Data buffer commands

Inappropriate data buffer changes can cause system problems. Before manually changing data buffer settings, make sure you understand its impact on your device. As a best practice, use the **burst-mode enable** command if the system requires large buffer spaces. The **burst-mode enable** command and the **buffer apply** command are mutually exclusive. If you have configured the data buffer by using one command, you must execute the **undo** form of the command before using the other command.

buffer apply

Use **buffer apply** to apply manually configured data buffer settings.

Use **undo buffer apply** to restore the default.

Syntax

buffer apply

undo buffer apply

Views

System view

Predefined user roles

network-admin

Usage guidelines

For data buffer settings to take effect, you must execute this command after configuring data buffer settings.

After applying manually configured data buffer settings, you cannot directly modify the applied settings. To modify them, you must cancel the application, reconfigure data buffer settings, and reapply the new settings.

This command might cause the PFC function to be on longer in effect or to operate incorrectly. For information about PFC configuration commands, see *Layer 2—LAN Switching Command Reference*.

Examples

```
# Apply manually configured data buffer settings.
```

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

```
[Sysname] buffer apply
```

buffer queue guaranteed

Use **buffer queue guaranteed** to set the fixed-area ratio for a queue.

Use **undo buffer queue guaranteed** to delete the fixed-area ratio setting of a queue.

Syntax

buffer egress [slot slot-number] cell queue queue-id guaranteed ratio ratio

undo buffer egress [slot slot-number] cell queue queue-id guaranteed

Default

The fixed-area ratio for a queue is 13%.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command applies to all IRF member devices.

cell: Specifies cell resources.

queue-id: Specifies a queue by its ID in the range of 0 to 7.

ratio *ratio*: Specifies the fixed-area ratio, in percentage. The value range for *ratio* is 1 to 100.

Usage guidelines

By default, all queues have an equal share of the fixed area. You can set the fixed-area ratio for a queue. The other queues equally share the remaining part.

The fixed-area space for a queue cannot be used by other queues. Therefore, it is also called the minimum guaranteed buffer for the queue. The sum of fixed-area ratios configured for all queues cannot exceed the total fixed-area ratio. Otherwise, the configuration fails.

Inappropriate data buffer changes can cause system problems. Before manually changing data buffer settings, make sure you understand its impact on your device. As a best practice, use the **burst-mode enable** command if the system requires large buffer spaces.

Examples

Configure queue 0 to use 20% fixed-area space of cell resources in the egress buffer.

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

```
[Sysname] buffer egress cell queue 0 guaranteed ratio 20
```

buffer queue shared

Use **buffer queue shared** to set the maximum shared-area ratio for a queue.

Use **undo buffer queue shared** to delete the maximum shared-area ratio setting of a queue.

Syntax

buffer egress [**slot** *slot-number*] **cell queue** *queue-id* **shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] **cell queue** *queue-id* **shared**

Default

The maximum shared-area ratio for a queue is 20%.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command applies to all IRF member devices.

cell: Specifies cell resources.

queue-id: Specifies a queue by its ID in the range of 0 to 7.

ratio ratio: Specifies the maximum shared-area ratio, in percentage. The value range for *ratio* is 1 to 100.

Usage guidelines

By default, all queues have an equal share of the shared area. You can set the shared-area ratio for a queue. The unconfigured queues use the default setting. The shared-area space for each queue is finally determined by the chip based on your configuration and the number of packets to be received and sent.

Inappropriate data buffer changes can cause system problems. Before manually changing data buffer settings, make sure you understand its impact on your device. As a best practice, use the **burst-mode enable** command if the system requires large buffer spaces.

Examples

```
# Configure queue 0 to use up to 10% shared-area space of cell resources in the egress buffer.  
<Sysname> system-view  
[Sysname] buffer egress cell queue 0 shared ratio 10
```

buffer total-shared

Use **buffer total-shared** to set the total shared-area ratio.

Use **undo buffer total-shared** to delete the total shared-area ratio setting.

Syntax

buffer egress [slot *slot-number*] cell total-shared ratio *ratio*

undo buffer egress [slot *slot-number*] cell total-shared

Default

The total shared-area ratio is 100%.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command applies to all IRF member devices.

cell: Specifies cell resources.

ratio *ratio*: Specifies the ratio of the shared area, in percentage. The value range for *ratio* is 1 to 100.

Usage guidelines

After you set the shared-area ratio, the remaining buffer space is automatically assigned to the fixed area.

Inappropriate data buffer changes can cause system problems. Before manually changing data buffer settings, make sure you understand its impact on your device. As a best practice, use the **burst-mode enable** command if the system requires large buffer spaces.

Examples

```
# Configure the shared area to use 50% space of cell resources in the egress buffer.
<Sysname> system-view
[Sysname] buffer egress cell total-shared ratio 50
```

buffer usage threshold

Use **buffer usage threshold** to set a per-interface buffer usage threshold.

Use **undo buffer usage threshold** to restore the default.

Syntax

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

undo buffer usage threshold slot *slot-number*

Default

The per-interface buffer usage threshold is 70%.

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID.

ratio *ratio*: Specifies the buffer usage threshold in percentage, in the range of 1 to 100.

Usage guidelines

After you configure this command, the switch automatically records buffer usage for each interface. When a queue on an interface uses more buffer space than the set threshold, the system counts one threshold violation for the queue.

To display the buffer usage statistics for interfaces, use the **display buffer usage interface** command.

Examples

```
# Set the per-interface buffer usage threshold to 50% for IRF member device 1.
<Sysname> system-view
[Sysname] buffer usage threshold slot 1 ratio 50
```

Related commands

display buffer usage interface

burst-mode enable

Use **burst-mode enable** to enable the Burst feature.

Use **undo burst-mode enable** to disable the Burst feature.

Syntax

burst-mode enable

undo burst-mode enable

Default

The Burst feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The Burst feature is especially useful for reducing packet losses under the following circumstances:

- Broadcast or multicast traffic is intensive, resulting in bursts of traffic.
- Traffic enters a device from a high-speed interface and goes out of a low-speed interface.
- Traffic enters a device from multiple same-rate interfaces and goes out of an interface with the same rate.

Disabling the Burst feature might cause the PFC function to be on longer in effect or to operate incorrectly. For information about PFC configuration commands, see *Layer 2—LAN Switching Command Reference*.

Examples

```
# Enable the Burst feature.
<Sysname> system-view
[Sysname] burst-mode enable
```

display buffer

Use **display buffer** to display buffer size settings.

Syntax

```
display buffer [ slot slot-number ] [ queue [ queue-id ] ]
```

Views

Any view

Predefined user roles

network-admin
network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command displays buffer size settings for all IRF member devices.

queue *queue-id*: Specifies a queue by its number in the range of 0 to 7. If you specify a queue, this command displays the fixed-area ratio and shared-area ratio for the specified queue. If you specify the **queue** keyword without the *queue-id* argument, this command displays the fixed-area ratio and shared-area ratio for each queue. If you do not specify the **queue** keyword, this command displays the total shared-area ratio.

Examples

```
# Display buffer size settings.
<Sysname> display buffer
Slot  Type      Eg(Total-shared)
1     cell      100
```

Eg: Size of the sending buffer
 Total-shared: Size of the shared buffer for all ports
 Unit: Ratio

Display the fixed-area ratio and shared-area ratio for all queues.

```
<Sysname> display buffer queue
```

```
Slot Queue      Type      Eg(Guaranteed , Shared)
1      0-7         cell      13 , 88
```

Eg: Size of the sending buffer

Guaranteed: Size of the minimum guaranteed buffer per queue

Shared: Size of the maximum shared buffer per queue

Unit: Ratio

Table 40 Command output

Field	Description
Type	Resource type.
Queue	Queue ID in the range of 0 to 7.
Eg	Egress buffer.
(Total-shared)	Total-shared indicates the total shared-area ratio.
(Guaranteed , Shared)	<ul style="list-style-type: none"> Guaranteed indicates the fixed-area ratio of a queue. Shared indicates the shared-area ratio of a queue.

display buffer usage

Use **display buffer usage** to display buffer usage.

Syntax

```
display buffer usage [ slot slot-number ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot slot-number: Specifies an IRF member device by its member ID (slot number). If you do not specify an IRF member device, this command displays buffer usage for all IRF member devices.

Examples

Display buffer usage.

```
<Sysname> display buffer usage
```

```
Egress total-shared cell buffer usage on slot 1 :
```

```
XPE 0
```

```
Total:    4033 KB
```

```
Used:      0 KB
```

```
Free:     4033 KB
```

```
XPE 1
```

```

Total:    4033 KB
Used:     0 KB
Free:    4033 KB
XPE 2
Total:    4033 KB
Used:     0 KB
Free:    4033 KB
XPE 3
Total:    4033 KB
Used:     0 KB
Free:    4033 KB

                    5sec    1min    5min
-----
Ten-GigabitEthernet1/0/1    XPE 0    0%     0%     0%
                             XPE 1    0%     0%     0%
                             XPE 2    0%     0%     0%
                             XPE 3    0%     0%     0%
Ten-GigabitEthernet1/0/2    XPE 0    0%     0%     0%
                             XPE 1    0%     0%     0%
                             XPE 2    0%     0%     0%
                             XPE 3    0%     0%     0%
Ten-GigabitEthernet1/0/3    XPE 0    0%     0%     0%
                             XPE 1    0%     0%     0%
                             XPE 2    0%     0%     0%
                             XPE 3    0%     0%     0%

```

Table 41 Command output

Field	Description
Egress total-shared cell buffer usage on slot	Usage of cell resources in the shared area on an IRF member device.
XPE	Model of the data buffer.
Total	Total size of the data buffer.
Used	Size of used data buffer.
Free	Size of free data buffer.
5sec	Percentage of the buffer that the port uses for the last 5 seconds.
1min	Percentage of the buffer that the port uses for the last 1 minute.
5min	Percentage of the buffer that the port uses for the last 5 minutes.

display buffer usage interface

Use **display buffer usage interface** to display buffer usage statistics for interfaces.

Syntax

```
display buffer usage interface [ interface-type [ interface-number ] ]
```

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type [*interface-number*]: Specifies an interface by its type and number. If you do not specify the *interface-type* argument, this command displays buffer usage statistics for all Ethernet interfaces. If you specify the *interface-type* argument without the *interface-number* argument, this command displays buffer usage statistics for all Ethernet interfaces of the specified type.

Examples

Display buffer usage statistics for HundredGigE 1/0/1.

```
<Sysname> display buffer usage interface hundredgige 1/0/1
```

Interface	QueueID	Total	Used	Threshold(%)	Violations
HGE1/0/1	0	9418032	0	30	0
	1	9418032	0	30	0
	2	9418032	0	30	0
	3	9418032	0	30	0
	4	9418032	0	30	0
	5	9418032	0	30	0
	6	9418032	0	30	0
	7	9418032	0	30	0

Table 42 Command output

Field	Description
Total	Data buffer size in bytes allowed for a queue.
Used	Data buffer size in bytes that has been used by a queue.
Threshold(%)	Buffer usage threshold for a queue. The threshold value is the same as the per-interface threshold value.
Violations	Number of threshold violations for a queue. The value of this field is reset upon a switch reboot.

Time range commands

display time-range

Use **display time-range** to display time range configuration and status.

Syntax

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

Views

Any view

Predefined user roles

network-admin
network-operator

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.

Examples

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

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

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

Table 43 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.

time-range

Use **time-range** to create or edit a 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 ranges exist.

Views

System view

Predefined user roles

network-admin

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. 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 they do not overlap. These values can take one of the following forms:

- A digit in the range of 0 to 6, 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 varying by MM, and YYYY is the year in the calendar in the range of 1970 to 2100. If you do not specify this option, 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 you do not specify this option, the end time is 12/31/2100 24:00 PM, the maximum time available in the system.

Usage guidelines

If an existing time range name is provided, this command adds a statement to the time range.

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, 2015, 00:00 and December 31, 2015, 23:59, use the **time-range test 08:00 to 12:00 Mon from 00:00 01/01/2015 to 23:59 12/31/2015** command.

You can create a maximum of 1024 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 08:00 to 18:00 working-day
```

Create an absolute time range **t2**, setting it to be active in the whole year of 2011.

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

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

Create a compound time range **t3**, setting it to be active from 08:00 to 12:00 on Saturdays and Sundays of the year 2011.

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

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

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 January and June of the year 2011.

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

```
[Sysname] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
```

```
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

Related commands

display time-range

Document conventions and icons

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.





Command conventions

Convention	Description
Boldface	Bold 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 at least 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
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the New User window appears; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 WARNING!	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION:	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.
 IMPORTANT:	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
 TIP:	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 card, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG card.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
www.hpe.com/assistance
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
 - Hewlett Packard Enterprise Support Center **Get connected with updates** page:
www.hpe.com/support/e-updates
 - Software Depot website:
www.hpe.com/support/softwaredepot
- To view and update your entitlements, and to link your contracts, Care Packs, and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:
www.hpe.com/support/AccessToSupportMaterials

ⓘ **IMPORTANT:**

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HP Passport set up with relevant entitlements.

Websites

Website	Link
Networking websites	

Hewlett Packard Enterprise Information Library for Networking	www.hpe.com/networking/resourcefinder
Hewlett Packard Enterprise Networking website	www.hpe.com/info/networking
Hewlett Packard Enterprise My Networking website	www.hpe.com/networking/support
Hewlett Packard Enterprise My Networking Portal	www.hpe.com/networking/mynetworking
Hewlett Packard Enterprise Networking Warranty	www.hpe.com/networking/warranty
General websites	
Hewlett Packard Enterprise Information Library	www.hpe.com/info/enterprise/docs
Hewlett Packard Enterprise Support Center	www.hpe.com/support/hpesc
Hewlett Packard Enterprise Support Services Central	ssc.hpe.com/portal/site/ssc/
Contact Hewlett Packard Enterprise Worldwide	www.hpe.com/assistance
Subscription Service/Support Alerts	www.hpe.com/support/e-updates
Software Depot	www.hpe.com/support/softwaredepot
Customer Self Repair (not applicable to all devices)	www.hpe.com/support/selfrepair
Insight Remote Support (not applicable to all devices)	www.hpe.com/info/insightremotesupport/docs

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty, Care Pack Service, or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.

Index

[A](#) [B](#) [C](#) [D](#) [F](#) [I](#) [N](#) [P](#) [Q](#) [R](#) [S](#) [T](#)

A

accounting, [45](#)
acl, [1](#)
acl copy, [2](#)
acl logging interval, [3](#)
acl trap interval, [4](#)

B

buffer apply, [106](#)
buffer queue guaranteed, [106](#)
buffer queue shared, [107](#)
buffer total-shared, [108](#)
buffer usage threshold, [109](#)
burst-mode enable, [109](#)

C

car, [46](#)
car name, [102](#)
classifier behavior, [57](#)
control-plane, [58](#)

D

description, [5](#)
display acl, [6](#)
display buffer, [110](#)
display buffer usage, [111](#)
display buffer usage interface, [112](#)
display packet-filter, [7](#)
display packet-filter statistics, [8](#)
display packet-filter statistics sum, [11](#)
display packet-filter verbose, [12](#)
display qos car name, [102](#)
display qos gts interface, [80](#)
display qos lr interface, [82](#)
display qos map-table, [75](#)
display qos policy, [58](#)
display qos policy control-plane, [59](#)
display qos policy control-plane pre-defined, [60](#)
display qos policy global, [62](#)
display qos policy interface, [63](#)
display qos policy user-profile, [66](#)
display qos queue interface, [84](#)
display qos queue sp interface, [85](#)
display qos queue wfq interface, [90](#)
display qos queue wrr interface, [86](#)

display qos queue-statistics interface outbound, [94](#)
display qos trust interface, [77](#)
display qos vlan-policy, [68](#)
display qos wred interface, [96](#)
display qos wred table, [96](#)
display qos-acl resource, [15](#)
display time-range, [114](#)
display traffic behavior, [47](#)
display traffic classifier, [38](#)

F

filter, [48](#)

I

if-match, [39](#)
import, [76](#)

N

nest top-most, [49](#)

P

packet-filter, [17](#)
packet-filter default deny, [18](#)
packet-filter default hardware-count, [19](#)

Q

qos apply policy (interface view, control plane view), [69](#)
qos apply policy (user profile view), [70](#)
qos apply policy global, [71](#)
qos bandwidth queue, [91](#)
qos car (system view), [103](#)
qos gts, [81](#)
qos lr, [82](#)
qos map-table, [76](#)
qos policy, [71](#)
qos priority, [78](#)
qos sp, [85](#)
qos trust, [78](#)
qos vlan-policy, [72](#)
qos wfq, [91](#)
qos wfq { byte-count | weight }, [92](#)
qos wfq group sp, [93](#)
qos wred apply, [97](#)
qos wred queue table, [98](#)
qos wrr, [87](#)
qos wrr { byte-count | weight }, [88](#)

qos wrr group sp,89
queue,99
queue ecn,100
queue weighting-constant,101

R

redirect,49
remark customer-vlan-id,50
remark dot1p,51
remark drop-precedence,52
remark dscp,52
remark ip-precedence,54
remark local-precedence,54
remark qos-local-id,55
remark service-vlan-id,55
reset acl counter,19
reset packet-filter statistics,20
reset qos car name,105

reset qos policy control-plane,73
reset qos policy global,73
reset qos vlan-policy,74
rule (IPv4 advanced ACL view),21
rule (IPv4 basic ACL view),25
rule (IPv6 advanced ACL view),27
rule (IPv6 basic ACL view),32
rule (Layer 2 ACL view),33
rule comment,35

S

step,36

T

time-range,114
traffic behavior,56
traffic classifier,44