15 QoS Commands

About This Chapter

15.1 MQC Configuration Commands

15.1.1 Command Support

For details about command support, see the description of each command. If no command support information is provided, all switch models support the command by default.

15.1.2 classifier behavior

Function

The **classifier behavior** command binds a traffic behavior to a traffic classifier in a traffic policy.

The **undo classifier** command unbinds a traffic behavior from a traffic classifier in a traffic policy.

By default, no traffic classifier or traffic behavior is bound to a traffic policy.

Format

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

undo classifier *classifier-name*

Parameters

Parameter	Description	Value
classifier-name	Specifies the name of a traffic classifier.	The value must be the name of an existing traffic classifier.
behavior-name	Specifies the name of a traffic behavior.	The value must be the name of an existing traffic behavior.

Views

Traffic policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To take an action for packets of a certain type, use a traffic classifier to group the packets into one class and use a traffic behavior to define an action. Then associate the traffic classifier with the traffic behavior and bind them to a traffic policy.

Prerequisites

- A traffic classifier has been created using the **traffic classifier** command.
- A traffic behavior has been created using the **traffic behavior** command.
- A traffic policy has been created using the **traffic policy** command.

Precautions

You can dynamically add, modify, or delete the bound traffic classifiers, traffic behaviors, or binding of traffic classifiers and traffic behaviors in a traffic policy that has been applied to the system, a VLAN, or an interface.

NOTICE

Dynamically updating the traffic classifiers and traffic behaviors in a traffic policy makes the traffic policy ineffective for a short time. Confirm the operation before you use this command.

In a traffic policy, one traffic classifier can be bound to only one traffic behavior; each traffic policy supports a maximum of 256 pairs of traffic classifiers and traffic behaviors.

Example

# Bind the traffic classifier **c1** to the traffic behavior **b1** in the traffic policy **p1**, and apply the traffic policy to GE0/0/1 in the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match any
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark 8021p 2
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-policy p1 inbound
[HUAWEI-GigabitEthernet0/0/1] quit
```

# Bind the traffic classifier **c1** to the new traffic behavior **newb1** in the traffic policy **p1** that has been applied to GE0/0/1 in the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior newb1
[HUAWEI-trafficpolicy-p1] quit
```

Related Topics

15.1.4 display traffic behavior

15.1.5 display traffic classifier

15.1.6 display traffic policy

15.1.31 traffic behavior

15.1.32 traffic classifier

15.1.33 traffic policy

15.1.3 display acl division

Function

The **display acl division** command displays division rules based on the VLAN ID range in a delivered traffic classification rule or port number range in a delivered ACL rule.

Format

display acl division *start-id* **to** *end-id*

Parameters

Parameter	Description	Value
start-id	Specifies the start VLAN ID or port number.	The value is an integer that ranges from 0 to 65535.
to *end-id*	Specifies the end VLAN ID or port number.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*] command is used to configure a traffic classification rule defining a VLAN ID range, or the **rule (advanced ACL view)** or **rule (advanced ACL6 view)** command is used with the protocol as TCP or UDP and the port number range specified, run the **display acl resource** command to view occupied ACL resources. The system divides a rule into multiple rules. The **display acl division** command displays division rules based on the VLAN ID range or port number range.

Example

# Display division rules based on VLAN 10 to VLAN 20 or PORT10 to PORT20.

```
<HUAWEI> display acl division 10 to 20
 Range: 10 to 20;  Total rules: 4
 -----------------------------------------------------
  [ 1]:Value = 10      Mask = 0xfffe  Range[    10,    11]
  [ 2]:Value = 12      Mask = 0xfffc  Range[    12,    15]
  [ 3]:Value = 16     Mask = 0xfffc  Range[   16,   19]
  [ 4]:Value = 20     Mask = 0xffff  Range[   20,   20]
```

Table 15-1 Description of the **display acl division** command output

Item	Description
Range	Input VLAN ID range or port number range.
Total rules	Number of division rules based on the VLAN ID range or port number range.
[1]	ID of the division rule.
Value	Start VLAN ID of the division rule.
Mask	Mask of the VLAN ID in the division rule.
Range	Division rule range.

Related Topics

15.1.28 if-match vlan-id

14.1.5 acl (system view)

14.1.16 rule (advanced ACL view)

14.1.17 rule (advanced ACL6 view)

15.1.4 display traffic behavior

Function

The **display traffic behavior** command displays the traffic behavior configuration on the device.

Format

display traffic behavior user-defined [*behavior-name*]

Parameters

Parameter	Description	Value
user-defined [*behavior-name*]	Displays the configuration of a specified traffic behavior. If the name of a traffic behavior is not specified, the configuration of all traffic behaviors is displayed.	The value must be the name of an existing traffic behavior.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic behavior** command displays the configuration of a specified traffic behavior or all traffic behaviors. The command output helps you check the traffic behavior configuration and locate faults.

Precautions

If no traffic behavior is created, the system displays the following information after this command is executed:

```
Info: There is no behavior exists.
```

If the specified traffic behavior name is incorrect, the system displays the following information after this command is executed:

```
Info: The behavior does not exist.
```

Example

# Display the configuration of all traffic behaviors.

```
<HUAWEI> display traffic behavior user-defined
  User Defined Behavior Information:
    Behavior: tb1
      Committed Access Rate:
        CIR 1000 (Kbps), CBS 125000 (Byte)
        PIR 1000 (Kbps), PBS 125000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard
      Remark:
        Remark 8021p 1
Total behavior number is 1
```

Table 15-2 Description of the **display traffic behavior user-defined** command output

Item	Description
Behavior	Traffic behavior name. To create a traffic behavior, run the **traffic behavior** command.
Committed Access Rate	CAR. To configure an action taken for packets whose rate exceeds the CAR, run the **car (traffic behavior view)** command.
CIR	Committed information rate (CIR). To set the CIR, run the **car (traffic behavior view)** command.

Item	Description
PIR	Peak information rate (PIR). To set the PIR, run the **car (traffic behavior view)** command.
CBS	Committed burst size (CBS). To set the CBS, run the **car (traffic behavior view)** command.
PBS	Peak burst size (PBS). To set the PBS, run the **car (traffic behavior view)** command.
Green Action	Action taken for green packets. To configure an action taken for green packets, run the **car (traffic behavior view)** command.
Yellow Action	Action taken for yellow packets. To configure an action taken for yellow packets, run the **car (traffic behavior view)** command.
Red Action	Action taken for red packets. To configure an action taken for red packets, run the **car (traffic behavior view)** command.
Remark	Re-marking action. To configure re-marking, run the **remark** command.
Total behavior number is 1	Total number of created traffic behaviors.

Related Topics

15.3.2 car (traffic behavior view)

15.1.31 traffic behavior

15.7.2 statistic enable (traffic behavior view)

15.1.5 display traffic classifier

Function

The **display traffic classifier** command displays the traffic classifier configuration on the device.

Format

display traffic classifier user-defined [*classifier-name*]

Parameters

Parameter	Description	Value
user-defined [*classifier-name*]	Displays the configuration of a specified traffic classifier. If the name of a traffic classifier is not specified, the configuration of all traffic classifiers is displayed.	The value must be the name of an existing traffic classifier.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic classifier** command displays the configuration of a specified traffic classifier or all traffic classifiers. The command output helps you check the traffic classifier configuration and locate faults.

Precautions

If no traffic classifier is created, the system displays the following information after this command is executed:

```
Info: There is no classifier exists.
```

If the specified traffic classifier name is incorrect, the system displays the following information after this command is executed:

```
Info: The classifier does not exist.
```

Example

# Display the configuration of all traffic classifiers on the device.

```
<HUAWEI> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c1
    Operator: AND
    Rule(s) : if-match vlan-id 120

   Classifier: c2
    Operator: AND
    Rule(s) : if-match vlan-id 110

   Classifier: c3
    Operator: AND
    Rule(s) : if-match vlan-id 100

Total classifier number is 3
```

Table 15-3 Description of the **display traffic classifier user-defined** command output

Item	Description
Classifier	Traffic classifier name. To create a traffic classifier, run the **traffic classifier** command.
Operator	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Rule(s)	Rule in a traffic classifier.
Total classifier number is	Total number of created traffic classifiers.

Related Topics

15.1.32 traffic classifier

15.1.6 display traffic policy

Function

The **display traffic policy** command displays the traffic policy configuration on the device.

Format

display traffic policy { **interface** [*interface-type interface-number* [.*subinterface-number*]] | **vlan** [*vlan-id*] | **ssid-profile** [*ssid-profile-name*] | **global** } [**inbound** | **outbound**]

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support sub-interfaces.

Only the S5720HI supports **ssid-profile** [*ssid-profile-name*].

Parameters

Parameter	Description	Value
interface [*interface-type interface-number* [.*subinterface-number*]]	Displays the traffic policy configuration on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* [.*subinterface-number*] specifies the interface or sub-interface number.	-
vlan [*vlan-id*]	Displays the traffic policy configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
ssid-profile [*ssid-profile-name*]	Displays the traffic policy configuration in a specified SSID profile.	The value must be the name of an existing SSID profile.
global	Displays the traffic policy configuration in the system.	-
inbound	Displays the traffic policy configuration in the inbound direction.	-
outbound	Displays the traffic policy configuration in the outbound direction.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic policy** command displays the configuration of a specified traffic policy or all traffic policies. The command output helps you check the traffic policy configuration and locate faults.

Example

# Display the configuration of the traffic policy applied to GE0/0/1 .

```
<HUAWEI> display traffic policy interface gigabitethernet 0/0/1

 Interface: GigabitEthernet0/0/1

 Direction: Inbound

 Policy: p1
  Classifier: c1
   Operator: AND
   Rule(s) :
     if-match acl 5500
     if-match 8021p 6
     if-match acl 3001
  Behavior: b1
    Statistic enable

    Committed Access Rate:
      CIR 1000 (Kbps), CBS 125000 (Byte)
      PIR 1000 (Kbps), PBS 125000 (Byte)
      Green Action   : pass
      Yellow Action  : pass
      Red Action     : discard
```

Table 15-4 Description of the **display traffic policy** command output

Item	Description
Interface	Interface to which the traffic policy is applied.
Direction	Direction to which a traffic policy is applied. To apply a traffic policy, run the **traffic-policy (interface view)** command.
Policy	Traffic policy name. To create a traffic policy, run the **traffic policy** command.
Classifier	Traffic classifier in a traffic policy. To create a traffic classifier, run the **traffic classifier** command.
Operator	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Rule(s)	Rule in a traffic classifier.
Behavior	Traffic behavior bound to the traffic classifier. To create a traffic behavior, run the **traffic behavior** command.
Committed Access Rate	CAR. To configure CAR, run the **car (traffic behavior view)** command.

Item	Description
CIR 100 (Kbps), CBS 9000 (Byte) PIR 40000 (Kbps), PBS 200000 (Byte)	Parameters in the QoS CAR profile, including the CIR, PIR, CBS, and PBS. To configure CAR parameters, run the **car (traffic behavior view)** command.
Green Action	Action taken for green packets. To configure an action taken for green packets, run the **car (traffic behavior view)** command.
Yellow Action	Action taken for yellow packets. To configure an action taken for yellow packets, run the **car (traffic behavior view)** command.
Red Action	Action taken for red packets. To configure an action taken for red packets, run the **car (traffic behavior view)** command.

# Display the traffic policy in the SSID profile named test on the S5720HI.

```
<HUAWEI> display traffic policy ssid-profile test inbound
 Ssid-profile: test

 Direction: Inbound

 Policy: 1
   Classifier: 1
    Operator: AND
    Rule(s) :
       if-match vlan-id 100
   Behavior: 1
     Permit
```

Table 15-5 Description of the **display traffic policy** command output

Item	Description
Ssid-profile	SSID profile to which the traffic policy is applied.
Direction	Direction to which a traffic policy is applied. To apply a traffic policy, run the **traffic-policy (SSID profile view)** command.
Policy	Traffic policy name. To create a traffic policy, run the **traffic policy** command.
Classifier	Traffic classifier in a traffic policy. To create a traffic classifier, run the **traffic classifier** command.

Item	Description
Operator	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Rule(s)	Rule in a traffic classifier.
Behavior	Traffic behavior bound to the traffic classifier. To create a traffic behavior, run the **traffic behavior** command.
Permit	Allows packets matching the rule in the traffic classifier to pass. To allow or disallow packets matching the rule in the traffic classifier to pass, run the **deny | permit** command.

Related Topics

15.3.2 car (traffic behavior view)

15.5.2 deny | permit

15.1.30 reset traffic policy statistics

15.7.2 statistic enable (traffic behavior view)

15.1.31 traffic behavior

15.1.32 traffic classifier

15.1.33 traffic policy

15.1.36 traffic-policy (interface view)

15.1.37 traffic-policy (SSID profile view)

15.1.41 traffic-policy global

15.1.7 display traffic policy statistics

Function

The **display traffic policy statistics** command displays packet statistics in the specified object or each object to which a traffic policy has been applied.

Format

display traffic policy statistics { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* [*.subinterface-number*] | **vlan** *vlan-id* | **ssid-profile** *ssid-profile-name* } { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name*]]

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support sub-interfaces.

Only the S5720HI supports **ssid-profile** *ssid-profile-name*.

display traffic policy statistics policy-name *policy-name*

display traffic policy statistics all

Parameters

Parameter	Description	Value
global	Displays packet statistics in the system to which a traffic policy has been applied.	-
slot *slot-id*	Displays packet statistics on a specified device to which a traffic policy has been applied. *slot-id* specifies the slot ID of the device.	The value range depends on the device configuration.
interface *interface-type interface-number* [*.subinterface-number*]	Displays packet statistics on a specified interface to which a traffic policy has been applied. ● *interface-type* specifies the interface type. ● *interface-number* [*.subinterface-number*] specifies the interface or sub-interface number.	-
vlan *vlan-id*	Displays packet statistics in a specified VLAN to which a traffic policy has been applied. *vlan-id* specifies the ID of the VLAN.	The value is an integer that ranges from 1 to 4094.
ssid-profile *ssid-profile-name*	Displays packet statistics in a specified SSID profile to which a traffic policy has been applied. *ssid-profile-name* specifies the name of the SSID profile.	The value must be the name of an existing SSID profile.
inbound	Displays packet statistics in the inbound direction to which a traffic policy has been applied.	-

Parameter	Description	Value
outbound	Displays packet statistics in the outbound direction to which a traffic policy has been applied.	-
verbose	Displays detailed packet statistics.	-
classifier-base	Displays statistics on packets matching a specified traffic classifier. If this parameter is specified, statistics on packets matching all traffic classifiers in the traffic policy are displayed.	-
rule-base	Displays statistics on packets matching a rule. If this parameter is specified, statistics on packets matching all rules are displayed.	-
class *classifier-name*	Specifies the name of a traffic classifier. If this parameter is specified, statistics on packets matching the specified traffic classifier or rules in the specified traffic classifier are displayed. If this parameter is not specified, statistics on packets matching all traffic classifiers are displayed.	The value must be the name of an existing traffic classifier.
policy-name *policy-name*	Displays packet statistics in each object to which the specified traffic policy is applied.	The value must be the name of an existing traffic policy.

Parameter	Description	Value
all	Displays packet statistics in each object to which a traffic policy has been applied, including packet statistics in the inbound or outbound directions in the system, on each interface, in each VLAN, and in each SSID profile.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic policy statistics** command displays packet statistics in the specified object or each object to which a traffic policy has been applied. The command output helps you check statistics on forwarded and discarded packets and locate faults.

Precautions

If no traffic policy is applied, the system displays the following information after this command is executed:

```
Info: The Policy is not applied in this view.
```

If you do not run the **statistic enable (traffic behavior view)** command in the view of the traffic behavior in a traffic policy, the system displays the following information after this command is executed:

```
Info: Statistic has not been enabled.
```

Example

# Display packet statistics on GE0/0/1 in the inbound direction to which a traffic policy has been applied.

```
<HUAWEI> display traffic policy statistics interface gigabitethernet 0/0/1 inbound

 Interface: GigabitEthernet0/0/1
 Traffic policy inbound: p1
 Rule number: 1
 Current status: success
 Statistics interval: 300
---------------------------------------------------------------------
 Board : 0
---------------------------------------------------------------------
 Matched          |      Packets:                            0
```

```
                |     Bytes:                          0
                |     Rate(pps):                        0
                |     Rate(bps):                        0
---------------------------------------------------------------------
  Passed        |     Packets:                          0
                |     Bytes:                          0
                |     Rate(pps):                        0
                |     Rate(bps):                        0
---------------------------------------------------------------------
  Dropped       |     Packets:                          0
                |     Bytes:                          0
                |     Rate(pps):                        0
                |     Rate(bps):                        0
---------------------------------------------------------------------
    Filter      |     Packets:                          0
                |     Bytes:                          0
---------------------------------------------------------------------
    Car         |     Packets:                          0
                |     Bytes:                          0
---------------------------------------------------------------------
```

# Display statistics on incoming packets matching a rule after the traffic policy is applied to the system.

```
<HUAWEI> display traffic policy statistics global inbound verbose rule-base
 Global :
 Traffic policy inbound: p1
 Rule number: 1
 Current status: success
 Statistics interval: 300
---------------------------------------------------------------------
 Classifier: c1 operator and
 Behavior: b1
 if-match 8021p 5
 Board : 0
---------------------------------------------------------------------
 Passed         |     Packets:                          0
                |     Bytes:                          0
                |     Rate(pps):                        0
                |     Rate(bps):                        0
---------------------------------------------------------------------
 Dropped        |     Packets:                          0
                |     Bytes:                          0
                |     Rate(pps):                        0
                |     Rate(bps):                        0
---------------------------------------------------------------------
```

# Display statistics on incoming packets matching a traffic classifier in the traffic policy that has been applied to GE0/0/1.

```
<HUAWEI> display traffic policy statistics interface gigabitethernet 0/0/1 inbound verbose classifier-base class c1

 Interface: GigabitEthernet0/0/1
 Traffic policy inbound: p1
 Rule number: 1
 Current status: success
 Statistics interval: 300
---------------------------------------------------------------------
 Classifier: c1 operator and
 Behavior: b1
 Board : 0
---------------------------------------------------------------------
 Matched        |     Packets:                          0
                |     Bytes:                          0
                |     Rate(pps):                        0
                |     Rate(bps):                        0
---------------------------------------------------------------------
  Passed        |     Packets:                          0
                |     Bytes:                          0
                |     Rate(pps):                        0
```

```
              |      Rate(bps):                    0
---------------------------------------------------------------------
  Dropped       |      Packets:                    0
              |      Bytes:                      0
              |      Rate(pps):                    0
              |      Rate(bps):                    0
---------------------------------------------------------------------
    Filter      |      Packets:                    0
              |      Bytes:                      0
---------------------------------------------------------------------
    Car         |      Packets:                    0
              |      Bytes:                      0
---------------------------------------------------------------------
```

# Display statistics about incoming packets matching rules after the traffic policy is applied to GigabitEthernet 0/0/1.

```
<HUAWEI> display traffic policy statistics interface GigabitEthernet 0/0/1 inbound verbose rule-base
Interface: GigabitEthernet0/0/1
Traffic policy inbound: tp2
Rule number: 2
Current status: success
Statistics interval: 300
---------------------------------------------------------------------
Classifier: c2 operator and
Behavior: b1
Board : 0
rule 15 permit ip source 10.154.128.6 0 (match-counter 0)
---------------------------------------------------------------------
Passed          |      Packets:                    0
              |      Bytes:                      -
              |      Rate(pps):                    0
              |      Rate(bps):                    -
---------------------------------------------------------------------
Dropped         |      Packets:                    0
              |      Bytes:                      -
              |      Rate(pps):                    0
              |      Rate(bps):                    -
---------------------------------------------------------------------
rule 70 permit ip source 10.10.12.0 0.0.0.31 (match-counter 0)
---------------------------------------------------------------------
Passed          |      Packets:                13,528
              |      Bytes:                      -
              |      Rate(pps):                    0
              |      Rate(bps):                    -
---------------------------------------------------------------------
Dropped         |      Packets:                    0
              |      Bytes:                      -
              |      Rate(pps):                    0
              |      Rate(bps):                    -
---------------------------------------------------------------------
```

Table 15-6 Description of the **display traffic policy statistics** command output

Item	Description
Interface	Interface to which the traffic policy is applied.
Global	System to which the traffic policy is applied.
Traffic policy inbound	Applied traffic policy.
Rule number	Number of valid rules in the traffic classifier.
Current status	Traffic policy status.

Item	Description
Statistics interval	Interval for collecting traffic statistics. To set the interval for collecting traffic statistics, run the **traffic statistics interval** command.
Classifier	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Behavior	Traffic behavior name. To create a traffic behavior, run the **traffic behavior** command.
Board	ID of the switch to which the traffic policy is applied. When you query the statistics on an Eth-Trunk, the system displays only the statistics on the switch where member interfaces in the Eth-Trunk are located.
Matched	Numbers of packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Passed	Numbers of forwarded packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Dropped	Numbers of discarded packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time. The discarded packets include the filtered packets and packets dropped by CAR.
Filter	Numbers of filtered packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Car	Numbers of packets and bytes that match traffic classification rules and are discarded by CAR. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time. To configure CAR, run the **car (traffic behavior view)** command.

Item	Description
Packets	Number of packets. If the information is displayed as -, the statistics on this item cannot be collected.
Bytes	Number of bytes. If the information is displayed as -, the statistics on this item cannot be collected.
Rate(pps)	Rate, in pps. If the information is displayed as -, the statistics on this item cannot be collected.
Rate(bps)	Rate, in bit/s. If the information is displayed as -, the statistics on this item cannot be collected.
match-counter 0	Number of times packets match ACL rules. **NOTE** FTP, TFTP, Telnet, SNMP, HTTP, routing, and multicast packets match software ACL rules, and the number of times packets match software ACL rules can be checked using a command. Other packets match hardware ACL rules, and the number of times packets match hardware ACL rules can be checked using other methods. For example, to view the number of times packets match ACL rules after a traffic policy is applied, run the **statistic enable (traffic behavior view)** command to enable traffic statistics in the traffic behavior and run the **display traffic policy statistics** command to check statistics.

Related Topics

15.3.2 car (traffic behavior view)

15.1.30 reset traffic policy statistics

15.7.2 statistic enable (traffic behavior view)

15.1.31 traffic behavior

15.1.32 traffic classifier

15.1.8 display traffic policy user-defined

Function

The **display traffic policy user-defined** command displays the user-defined traffic policy configuration.

Format

display traffic policy user-defined [*policy-name* [**classifier** *classifier-name*]]

Parameters

Parameter	Description	Value
policy-name	Displays the configuration of a specified user-defined traffic policy. If this parameter is not specified, the configuration of all user-defined traffic policies is displayed.	The value must be the name of an existing traffic policy.
classifier *classifier-name*	Displays the configuration of a traffic behavior bound to a specified traffic classifier in a traffic policy. If this parameter is not specified, the traffic policy configuration is displayed.	The value must be the name of an existing traffic classifier.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic policy user-defined** command displays the configuration of a specified traffic policy or all traffic policies. The command output helps you check the traffic policy configuration and locate faults.

Precautions

If no traffic policy is created, the system displays an error message after the **display traffic policy user-defined** command is executed:

```
Info: There is no policy exists.
```

If the specified traffic policy name is incorrect, the system displays an error message after the **display traffic policy user-defined** command is executed:

```
Error: The policy does not exist.
```

Example

# Display the user-defined traffic policy configuration.

```
<HUAWEI> display traffic policy user-defined
  User Defined Traffic Policy Information:
  Policy: p1
   Classifier: c1
    Operator: AND
     Behavior: tb1
      Remark:
        Remark 8021p 0
      Committed Access Rate:
        CIR 10000 (Kbps), CBS 1250000 (Byte)
        PIR 10000 (Kbps), PBS 1250000 (Byte)
        Green Action   : pass
        Yellow Action  : pass
        Red Action     : discard

Total policy number is 1
```

Table 15-7 Description of the **display traffic policy user-defined** command output

Item	Description
User Defined Traffic Policy Information	User-defined traffic policy configuration.
Policy	Traffic policy name. To create a traffic policy, run the **traffic policy** command.
Classifier	Traffic classifier in a traffic policy. To create a traffic classifier, run the **traffic classifier** command.
Operator	Relationship between rules in the traffic classifier. To create a traffic classifier, run the **traffic classifier** command.
Behavior	Traffic behavior associated with the traffic classifier in the traffic policy. To create a traffic behavior, run the **traffic behavior** command.
Committed Access Rate	CAR. To configure the CAR, run the **car (traffic behavior view)** command.
Green Action	Action taken for green packets. To configure an action taken for green packets, run the **car (traffic behavior view)** command.
Yellow Action	Action taken for yellow packets. To configure an action taken for yellow packets, run the **car (traffic behavior view)** command.
Red Action	Action taken for red packets. To configure an action taken for red packets, run the **car (traffic behavior view)** command.

Item	Description
Remark	Re-marking action. To configure re-marking, run the **remark** command.
Total policy number is	Total number of created traffic policies.

Related Topics

15.3.2 car (traffic behavior view)

15.1.31 traffic behavior

15.1.32 traffic classifier

15.1.33 traffic policy

15.1.9 display traffic-applied

Function

The **display traffic-applied** command displays information about ACL-based simplified and MQC-based traffic policies applied to the system, a VLAN, an interface, an SSID profile, or a traffic profile.

Format

display traffic-applied [**interface** [*interface-type interface-number*] | **vlan** [*vlan-id*]] { **inbound** | **outbound** } [**verbose**]

display traffic-applied [**ssid-profile** [*ssid-profile-name*] | **traffic-profile** [*traffic-profile-name*]] { **inbound** | **outbound** } (only supported by the S5720HI)

display traffic-applied brief

display traffic-applied record

Parameters

Parameter	Description	Value
interface [*interface-type interface-number*]	Displays information about ACL-based simplified and MQC-based traffic policies applied to a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, information about ACL-based simplified and MQC-based traffic policies applied to the system or a VLAN is displayed.	-
vlan [*vlan-id*]	Displays information about ACL-based simplified and MQC-based traffic policies applied to a specified VLAN. If this parameter is not specified, information about ACL-based simplified and MQC-based traffic policies applied to the system or an interface is displayed.	The value is an integer that ranges from 1 to 4094.
ssid-profile [*ssid-profile-name*]	Displays information about ACL-based simplified and MQC-based traffic policies applied to a specified SSID profile.	The value must be the name of an existing SSID profile.
traffic-profile [*traffic-profile-name*]	Displays information about ACL-based simplified and MQC-based traffic policies applied to a specified traffic profile.	The value must be the name of an existing traffic profile.

Parameter	Description	Value
inbound	Displays information about ACL-based simplified and MQC-based traffic policies applied in the inbound direction.	-
outbound	Displays information about ACL-based simplified and MQC-based traffic policies applied in the outbound direction.	-
verbose	Displays detailed information about ACL-based simplified and MQC-based traffic policies applied to the system, a VLAN, or an interface.	-
brief	Displays brief information about ACL-based simplified and MQC-based traffic policies applied to the system, a VLAN, an interface, an SSID profile, or a traffic profile.	-
record	Displays information about all ACL-based simplified traffic policies applied to the device.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display traffic-applied** command displays information about ACL-based simplified and MQC-based traffic policies applied to the system, a VLAN, or an interface.

Example

# Display information about globally applied ACL-based simplified and MQC-based traffic policies in the inbound direction.

```
<HUAWEI> display traffic-applied inbound
---------------------------------------------------------
Policy applied inbound global
  Policy:    p1
---------------------------------------------------------
```

Table 15-8 Description of the **display traffic-applied inbound** command output

Item	Description
Policy	Traffic policy name. To create a traffic policy, run the **traffic policy** command.

# Display the configuration of all ACL-based simplified traffic policies on the device.

```
<HUAWEI> display traffic-applied record
-----------------------------------------------------------------------
*interface GigabitEthernet0/0/1
 traffic-filter inbound acl 3000
  slot 0: success

-----------------------------------------------------------------------
*system
 traffic-filter inbound acl 3001
  slot 0: success

 traffic-filter outbound acl 3002
  slot 0: success

-----------------------------------------------------------------------
```

Table 15-9 Description of the **display traffic-applied record** command output

Item	Description
interface GigabitEthernet0/0/1	Interface where the ACL-based simplified traffic policy has been applied.
traffic-filter inbound acl 3000	Configuration of the ACL-based simplified traffic policy that has been applied. For details, see **ACL-based Simplified Traffic Policy Commands**.
slot	Slot where the ACL-based simplified traffic policy has been applied. The value is 0 in a non-stack scenario. In a stack scenario, the value depends on the device configuration.

Item	Description
success	Status of the ACL-based simplified traffic policy that has been applied: ● success: The ACL-based simplified traffic policy has been applied successfully. ● fail: The ACL-based simplified traffic policy fails to be applied.
system	Configuration of the ACL-based simplified traffic policy that has been applied globally.

Related Topics

15.1.41 traffic-policy global

15.1.36 traffic-policy (interface view)

15.1.37 traffic-policy (SSID profile view)

15.1.38 traffic-policy (VLAN view)

15.1.39 traffic-policy (VLANIF interface view)

15.1.10 display traffic-policy applied-record

Function

The **display traffic-policy applied-record** command displays traffic policy records.

Format

display traffic-policy applied-record [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Displays the record of a specified traffic policy. If this parameter is not specified, records of all the applied traffic policies are displayed.	The value must be the name of an existing traffic policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic-policy applied-record** command displays a record of an applied traffic policy or records of all applied traffic policies, including the view, interface number, and direction that the traffic policy/policies is/are applied to, traffic policy status on an SSID profile, and number of times the traffic policy/ policies is/are applied. The command output helps you check traffic policy records and locate faults.

Precautions

If no traffic policy is created, the system does not display any information after this command is executed.

If the specified traffic policy name is incorrect, the system displays the following information after this command is executed:

```
Info: Traffic policy does not exist.
```

Example

# Display the record of the traffic policy **p1** in a non-stack scenario.

```
<HUAWEI> display traffic-policy applied-record p1
-------------------------------------------------
  Policy Name:   p1
  Policy Index:  0
     Classifier:c1     Behavior:b1
-------------------------------------------------
 *interface GigabitEthernet0/0/1
    traffic-policy p1 outbound
      slot 0    :  success
 *vlan 100
    traffic-policy p1 outbound
      slot 0    :  success
 *system
    traffic-policy p1 global outbound
      slot 0    :  success
 *ssid-profile test
    traffic-policy p1 inbound
      slot 0    :  success
-------------------------------------------------
  Policy total applied times: 4.
```

# Display the record of the traffic policy **p1** in a stack scenario.

```
<HUAWEI> display traffic-policy applied-record p1
-------------------------------------------------
  Policy Name:   p1
  Policy Index:  1
     Classifier:c1     Behavior:b1
-------------------------------------------------
 *system
    traffic-policy p1 global inbound
      slot 2  :  success
      slot 1  :  success
      slot 0  :  success
 *system
    traffic-policy p1 global outbound
```

```
   slot 2  :  success
   slot 1  :  success
   slot 0  :  success
------------------------------------------------
 Policy total applied times: 2.
```

Table 15-10 Description of the **display traffic-policy applied-record** command output

Item	Description
Policy Name	Traffic policy name. To configure a traffic policy, run the **traffic policy** command.
Policy Index	Traffic policy index.
Classifier	Traffic classifier name. To configure a traffic classifier, run the **traffic classifier** command.
Behavior	Traffic behavior name. To configure a traffic behavior, run the **traffic behavior** command.
interface GigabitEthernet0/0/1	Interface to which the traffic policy is applied. To apply a traffic policy to an interface, run the **traffic-policy (interface view)** command.
traffic-policy p1 inbound	Inbound direction to which the traffic policy **p1** is applied.
traffic-policy p1 outbound	Outbound direction to which the traffic policy **p1** is applied.
slot	Status of the traffic policy applied to the specified slot. ● success: The traffic policy is applied successfully. ● fail: The traffic policy fails to be applied.
vlan	VLAN to which the traffic policy is applied. To apply a traffic policy to a VLAN, run the **traffic-policy (VLAN view)** command.
system	System to which the traffic policy is applied. To apply a traffic policy to the system, run the **traffic-policy global** command.
ssid-profile	SSID profile to which the traffic policy is applied. To apply a traffic policy to an SSID profile, run the **traffic-policy (SSID profile view)** command. **NOTE** Only the S5720HI supports SSID profiles.
Policy total applied times	Number of times the traffic policy is applied.

Related Topics

15.1.32 traffic classifier

15.1.31 traffic behavior

15.1.33 traffic policy

15.1.41 traffic-policy global

15.1.36 traffic-policy (interface view)

15.1.37 traffic-policy (SSID profile view)

15.1.38 traffic-policy (VLAN view)

15.1.11 if-match 8021p

Function

The **if-match 8021p** command configures a matching rule based on the 802.1p priority of VLAN packets in a traffic classifier.

The **undo if-match 8021p** command deletes a matching rule based on the 802.1p priority of VLAN packets in a traffic classifier.

By default, a matching rule based on the 802.1p priority of VLAN packets is not configured in a traffic classifier.

Format

if-match 8021p *8021p-value* &<1-8>

undo if-match 8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority in VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority in VLAN packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match 8021p** command to classify traffic based on the 802.1p priority in VLAN packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

After the **remark 8021p**, **add-tag vlan-id**, **remark cvlan-id**, and **remark vlan-id** commands are used, the system modifies VLAN tags of packets according to the re-marking configuration. These actions are called VLAN-based actions.

Regardless of whether the relationship between traffic classification rules is AND or OR, if you enter multiple values of 802.1p priorities, the packet that matches one 802.1p priority matches a rule.

If you run the **if-match 8021p** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure a matching rule based on the 802.1p priority of 1 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match 8021p 1
```

Related Topics

5.8.2 add-tag vlan-id

15.2.17 remark 8021p

5.9.5 remark cvlan-id

5.9.6 remark vlan-id

15.1.32 traffic classifier

15.1.12 if-match acl

Function

The **if-match acl** command configures a matching rule based on an Access Control List (ACL) in a traffic classifier.

The **undo if-match acl** command deletes a matching rule based on an ACL.

By default, a matching rule based on an ACL is not configured in a traffic classifier.

Format

if-match [**ipv6**] **acl** { *acl-number* | *acl-name* }

undo if-match [**ipv6**] **acl** { *acl-number* | *acl-name* }

Parameters

Parameter	Description	Value
ipv6	Indicates that IPv6 ACLs are matched. If this parameter is not specified, IPv4 ACLs are matched.	-
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 5999, and the value of an ACL6 ranges from 2000 to 3999. ● ACLs numbered 2000 to 2999 are basic ACLs, which are used to classify all packets. ● ACLs numbered 3000 to 3999 are advanced ACLs, which are used to classify packets based on Layer 3 information. ● ACLs numbered 4000 to 4999 are Layer 2 ACLs, which are used to classify packets based on the source MAC address, destination MAC address, and packet type. ● ACLs numbered 5000 to 5999 are user-defined ACLs.
acl-name	Specifies the name of an ACL.	The value must be the name of an existing ACL.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To classify packets based on the interface that receives packets, source IP address, destination IP address, protocol over IP, source and destination TCP port numbers, ICMP type and code, and source and destination MAC addresses, ARP packets, reference an ACL in a traffic classifier. You must first define an ACL and configure rules in the ACL, and then run the **if-match acl** command to configure a matching rule based on the ACL so that the device processes packets matching the same rule in the same manner.

Prerequisites

The following operations must have been performed:

- Create an ACL and configure rules in the ACL.
- Create a traffic classifier using the **traffic classifier** command.

Precautions

Regardless of whether the relationship between rules in a traffic classifier is AND or OR, if an ACL contains multiple rules, the packet that matches one ACL rule matches the ACL.

Only the S5720EI, S6720EI, and S6720S-EI support traffic classifiers with advanced ACLs containing the ttl-expired field.

You can configure multiple ACL rules in a traffic classifier to match different types of packets.

MTU-exceeded UDP packets will be fragmented. Only the first fragmented packet contains UDP information, and the other fragmented packets cannot be matched against ACL rules based on UDP information. Therefore, a traffic policy that contains **if-match acl** for matching UDP information does not take effect on fragmented packets. For example, if traffic policing is configured for traffic that contains a large number of fragmented packets and these fragmented packets do not match the UDP port number in an ACL rule, traffic policing is not performed on the fragmented packets. As a result, the actual rate is higher than the rate limit.

For S5720HI, ACL6 rules can define only the protocol number, source port number, destination port number, source IPv6 address, and destination IPv6 address. Additionally, ACL6-based traffic policies that contain these ACL6 rules cannot be applied to sub-interfaces and VLANIF interfaces.

Example

# Configure a matching rule based on ACL 2046 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] acl 2046
[HUAWEI-acl-basic-2046] rule permit source any
[HUAWEI-acl-basic-2046] quit
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match acl 2046
```

Related Topics

14.1.4 acl name

14.1.5 acl (system view)

15.1.23 if-match l2-protocol

15.1.32 traffic classifier

15.1.13 if-match any

Function

The **if-match any** command configures a matching rule based on all data packets in a traffic classifier.

The **undo if-match any** command deletes a matching rule based on all data packets in a traffic classifier.

By default, a matching rule based on all data packets is not configured in a traffic classifier.

Format

if-match any

undo if-match any

Parameters

None

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To process all the data packets in the same manner, run the **if-match any** command.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

After the **if-match any** command is run, only the matching rule configured using this command takes effect, and the other matching rules in the same traffic classifier will become ineffective.

Example

# Configure a matching rule based on all data packets in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match any
```

Related Topics

15.1.32 traffic classifier

15.1.14 if-match cvlan-8021p

Function

The **if-match cvlan-8021p** command configures a matching rule based on the 802.1p priority in the inner tag of QinQ packets in a traffic classifier.

The **undo if-match cvlan-8021p** command deletes a matching rule based on the 802.1p priority in the inner tag of QinQ packets in a traffic classifier.

By default, a matching rule based on the 802.1p priority in the inner tag of QinQ packets is not configured in a traffic classifier.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

if-match cvlan-8021p *8021p-value* &<1-8>

undo if-match cvlan-8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority in the inner tag of QinQ packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority of QinQ packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match cvlan-8021p** command to classify packets based on the 802.1p priority in the inner tag of QinQ packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

The **if-match cvlan-8021p** command is valid for only the double-tagged packets.

If you enter multiple 802.1p priorities in the inner tag of packets in the command, a packet matches a rule as long as it matches one of the 802.1p priorities in the inner tag of packets, regardless of whether the relationship between traffic classification rules is AND or OR.

If you run the **if-match cvlan-8021p** command multiple times in the same traffic classifier view, only the latest configuration takes effect.

Example

# Configure a matching rule based on the inner 802.1p priority of 1 in QinQ packets in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match cvlan-8021p 1
```

Related Topics

15.1.32 traffic classifier

15.1.15 if-match cvlan-id

Function

The **if-match cvlan-id** command configures a matching rule based on VLAN IDs in the inner and outer tags of QinQ packets in a traffic classifier. You can specify the VLAN ID range in the inner tag.

The **undo if-match cvlan-id** command deletes a matching rule based on VLAN IDs in the inner and outer tags of QinQ packets in a traffic classifier.

By default, a matching rule based on the VLAN ID in the inner and outer tags of QinQ packets is not configured in a traffic classifier.

NOTE

Only the S1720X, S1720X-E, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

if-match cvlan-id *start-cvlan-id* [**to** *end-cvlan-id*] [**vlan-id** *vlan-id*]

undo if-match cvlan-id *start-cvlan-id* [**to** *end-cvlan-id*] [**vlan-id** *vlan-id*]

Parameters

Parameter	Description	Value
start-cvlan-id [**to** *end-cvlan-id*]	Specifies the VLAN ID in the inner tag of a QinQ packet.	● *start-cvlan-id* specifies the start VLAN ID in the inner tag. The value is an integer that ranges from 1 to 4094. ● *end-cvlan-id* specifies the end VLAN ID in the inner tag. The value is an integer that ranges from 1 to 4094. The value of *end-cvlan-id* must be larger than the value of *start-cvlan-id*. If **to** *end-cvlan-id* is not specified, only the VLAN ID specified by *start-cvlan-id* is matched.
vlan-id *vlan-id*	Specifies the VLAN ID in the outer tag of a QinQ packet. If this parameter is not specified, only the VLAN ID in the inner tag of a QinQ packet is matched.	The value is an integer that ranges from 1 to 4094.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match cvlan-id** command to classify packets based on the VLAN ID in the inner tag of QinQ packets or VLAN IDs in inner and outer tags of QinQ packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

The **if-match cvlan-id** command is valid for only the double-tagged packets.

On the S6720EI, if a traffic policy contains the traffic classifier defining the **if-match cvlan-id** *start-cvlan-id* [**to** *end-cvlan-id*] **vlan-id** *vlan-id* matching rule, IPv6 ACL resources are occupied. To display information about IPv6 ACL resources, run the **display acl resource** command.

Example

# Configure a matching rule based on the VLAN ID of 100 in the inner tag of QinQ packets in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match cvlan-id 100
```

# Configure a matching rule based on the inner VLAN ID in the range of 100 to 200 and outer VLAN ID 300 of QinQ packets in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match cvlan-id 100 to 200 vlan-id 300
```

Related Topics

15.1.32 traffic classifier

15.1.16 if-match destination-mac

Function

The **if-match destination-mac** command configures a matching rule based on the destination MAC address in a traffic classifier.

The **undo if-match destination-mac** command deletes a matching rule based on the destination MAC address in a traffic classifier.

By default, a matching rule based on the destination MAC address is not configured in a traffic classifier.

Format

if-match destination-mac *mac-address* [*mac-address-mask*]

undo if-match destination-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
mac-address-mask	Specifies the mask of the destination MAC address. Similar to the mask of the IP address, the value F indicates that the destination MAC address is matched and the value 0 indicates that the destination MAC address is not matched. The mask of the MAC address determines a group of MAC addresses. The device can accurately match certain bits in the destination MAC address using the mask of the MAC address. In practice, you can set these bits to F in the mask of the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be 0-0-0.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match destination-mac** command to configure a matching rule based on the destination MAC address in a traffic classifier so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you run the **if-match destination-mac** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure a matching rule based on the destination MAC address of 0050-ba27-bed3 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match destination-mac 0050-ba27-bed3
```

# Configure a matching rule based on the destination MAC address of XX50-bXX7-bed3 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match destination-mac 0050-b007-bed3 00ff-f00f-ffff
```

Related Topics

15.1.26 if-match source-mac

15.1.32 traffic classifier

15.1.17 if-match discard

Function

The **if-match discard** command configures a matching rule based on drop packets in a traffic classifier.

The **undo if-match discard** command deletes a matching rule based on drop packets in a traffic classifier.

By default, a matching rule based on drop packets is not configured in a traffic classifier.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

if-match discard

undo if-match discard

Parameters

None

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After packets reach the device, invalid packets are discarded. You can run the **if-match discard** command to configure the device to match discarded packets, take action for the discarded packets such as traffic statistics and mirroring, and analyze them.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Example

# Configure a matching rule based on discarded packets in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match discard
```

Related Topics

15.1.32 traffic classifier

15.1.18 if-match double-tag

Function

The **if-match double-tag** command configures a matching rule based on double tags of packets in a traffic classifier.

The **undo if-match double-tag** command deletes a matching rule based on double tags of packets in a traffic classifier.

By default, a matching rule based on double tags of packets is not configured in a traffic classifier.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

if-match double-tag

undo if-match double-tag

Parameters

None

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match double-tag** command to classify traffic based on double tags so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Example

# Configure a matching rule based on double tags of packets in the traffic classifier **class1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier class1
[HUAWEI-classifier-class1] if-match double-tag
```

Related Topics

15.1.32 traffic classifier

15.1.19 if-match dscp

Function

The **if-match dscp** command configures a matching rule based on the Differentiated Services Code Point (DSCP) priority of packets in a traffic classifier.

The **undo if-match dscp** command deletes a matching rule based on the DSCP priority of packets in a traffic classifier.

By default, a matching rule based on the DSCP priority of packets is not configured in a traffic classifier.

Format

if-match dscp *dscp-value* &<1-8>

undo if-match dscp

Parameters

Parameter	Description	Value
dscp *dscp-value*	Specifies the DSCP priority.	The value can be a DiffServ code, an integer ranging from 0 to 63, or the name of the DSCP service type such as af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1-cs7, default, and ef. The values corresponding to service types are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match dscp** command to classify packets based on the DSCP priority of packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

if-match dscp can match both IPv4 and IPv6 packets.

If you enter multiple DSCP priorities in the command, a packet matches a rule as longs as it matches one of the DSCP priorities, regardless of whether the relationship between traffic classification rules is AND or OR.

If the relationship between rules in a traffic classifier is AND, the **if-match dscp** and **if-match ip-precedence** commands cannot be used in the traffic classifier simultaneously.

In a version earlier than V200R009C00, if **if-match dscp** *dscp-value* is configured in the traffic classifier on the switch, the traffic classifier can only match IPv4 packets. After the switch is upgraded to V200R009C00 and later versions, the traffic classifier can match IPv4 and IPv6 packets.

If you run the **if-match dscp** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure a matching rule based on the DSCP priority of 1 in the traffic classifier **class1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier class1
[HUAWEI-classifier-class1] if-match dscp 1
```

Related Topics

15.1.22 if-match ip-precedence

15.1.32 traffic classifier

15.1.20 if-match flow-id

Function

The **if-match flow-id** command configures a matching rule based on the flow ID in a traffic classifier.

The **undo if-match flow-id** command deletes a matching rule based on the flow ID in a traffic classifier.

By default, no matching rule based on the flow ID is configured in a traffic classifier.

NOTE

Only the S5720EI, S6720EI, and S6720S-EI support this command.

Format

if-match flow-id *flow-id*

undo if-match flow-id

Parameters

Parameter	Description	Value
flow-id	Specifies a flow ID.	The value is an integer that ranges from 1 to 8.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a traffic policy is applied to different interfaces or VLANs, to save ACL resources, you can run the **if-match flow-id** command to classify packets based on the flow ID so that the device processes packets matching the same flow ID in the same manner.

Assume that *M* ACLs are configured on the device to distinguish services, and each ACL contains *N* ACL rules. Traffic classifiers classify packets based on ACL rules, and the traffic policy containing the ACL rules are applied to *X* interfaces. If the action of re-marking flow IDs and matching rules based on the flow IDs are not configured, applying the traffic policy occupies *M***N***X* ACL resources. If the action of re-marking flow IDs and matching rules based on flow IDs are configured, applying the traffic policy occupies only *M**(*N*+*X*) ACL resources.

Prerequisites

The following operations must have been performed before this command is used:

- Run the **remark flow-id** command in the traffic behavior view to configure an action of re-marking the flow ID.
- Run the **traffic classifier** command in the system view to create a traffic classifier.

Precautions

It is recommended that the traffic classifier containing **if-match flow-id** and the traffic behavior containing **remark flow-id** be bound to different traffic policies.

The traffic policy containing **if-match flow-id** can be only applied to an interface, a VLAN, or the system in the inbound direction.

If you run the **if-match flow-id** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure a matching rule based on the flow ID of 1 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match flow-id 1
```

Related Topics

15.1.29 remark flow-id

15.1.32 traffic classifier

15.1.21 if-match inbound-interface

Function

The **if-match inbound-interface** command configures a matching rule based on an inbound interface in a traffic classifier.

The **undo if-match inbound-interface** command deletes a matching rule based on an inbound interface in a traffic classifier.

By default, a matching rule based on an inbound interface is not configured in a traffic classifier.

Format

if-match inbound-interface *interface-type interface-number*

undo if-match inbound-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an inbound interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match inbound-interface** command to classify traffic based on an inbound interface so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

A traffic policy containing **if-match inbound-interface** cannot be applied to an interface.

For the S5720HI, the inbound interface in this command cannot be an Eth-Trunk member interface.

A traffic policy containing the **if-match inbound-interface** rule can only be applied to the inbound direction.

If you run the **if-match inbound-interface** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure a matching rule based on the inbound interface of GE0/0/1 in the traffic classifier **class1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier class1
[HUAWEI-classifier-class1] if-match inbound-interface gigabitethernet 0/0/1
```

Related Topics

15.1.32 traffic classifier

15.1.22 if-match ip-precedence

Function

The **if-match ip-precedence** command configures a matching rule based on the IP precedence of packets in a traffic classifier.

The **undo if-match ip-precedence** command deletes a matching rule based on the IP precedence of packets in a traffic classifier.

By default, a matching rule based on the IP precedence of packets is not configured in a traffic classifier.

Format

if-match ip-precedence *ip-precedence-value* &<1-8>

undo if-match ip-precedence

Parameters

Parameter	Description	Value
ip-precedence-value	Specifies the IP precedence.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority of packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match ip-precedence** command to classify packets based on the IP precedence so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

After the **if-match ip-precedence** command is run, IP precedences are listed in ascending order.

If you enter multiple IP precedences in the **if-match ip-precedence** command, a packet matches a rule as long as it matches one of the IP precedence, regardless of whether the relationship between traffic classification rules is AND or OR.

In a traffic classifier where the relationship between rules is AND, the **if-match dscp** and **if-match ip-precedence** commands cannot be used simultaneously.

If you run the **if-match ip-precedence** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure a matching rule based on the IP precedence of 1 in the traffic classifier **class1**.

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

Related Topics

15.1.19 if-match dscp

15.1.22 if-match ip-precedence

15.1.32 traffic classifier

15.1.23 if-match l2-protocol

Function

The **if-match l2-protocol** command configures a matching rule based on the Layer 2 protocol type in a traffic classifier.

The **undo if-match l2-protocol** command deletes a matching rule based on the Layer 2 protocol type in a traffic classifier.

By default, a matching rule based on the Layer 2 protocol type is not configured in a traffic classifier.

Format

if-match l2-protocol { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }

undo if-match l2-protocol

Parameters

Parameter	Description	Value
arp	Indicates that ARP packets are classified.	The value of **arp** corresponds to 0x0806.
ip	Indicates that IP packets are classified.	The value of **ip** corresponds to 0x0800.
mpls	Indicates that MPLS packets are classified.	The value of **mpls** corresponds to 0x8847.
rarp	Indicates that RARP packets are classified.	The value of **rarp** corresponds to 0x8035.

Parameter	Description	Value
protocol-value	Specifies the value of a protocol type.	The value ranges from 0x0000 to 0xFFFF in hexadecimal notation and must start with 0x. If the value of *protocol-value* is smaller than 0x0600, the Destination Service Access Point (DSAP) and Source Service Access Point (SSAP) fields in the Logical Line Control (LLC) protocol packets are matched.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match l2-protocol** command to classify packets based on the Layer 2 protocol type so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

The device supports Layer 2 protocols including ARP, IP, MPLS, and RARP.

If you run the **if-match l2-protocol** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

If the relationship between rules in a traffic classifier is AND, and both the **if-match l2-protocol arp** and **if-match protocol** { **ip** | **ipv6** } commands are configured in this traffic classifier, of the two, only the **if-match l2-protocol arp** command takes effect.

Example

# Define a matching rule based on the protocol type of ARP in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match l2-protocol arp
```

Related Topics

15.1.32 traffic classifier

15.1.24 if-match outbound-interface

Function

The **if-match outbound-interface** command configures a matching rule based on an outbound interface in a traffic classifier.

The **undo if-match outbound-interface** command deletes a matching rule based on an outbound interface in a traffic classifier.

By default, a matching rule based on an outbound interface is not configured in a traffic classifier.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

if-match outbound-interface *interface-type interface-number*

undo if-match outbound-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an outbound interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match outbound-interface** command to classify packets based on an outbound interface so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

A traffic policy containing **if-match outbound-interface** cannot be applied to an interface.

For the S5720HI, the outbound interface in this command cannot be an Eth-Trunk member interface.

A traffic policy containing the **if-match outbound-interface** rule can only be applied to the outbound direction on the S5720HI.

If you run the **if-match outbound-interface** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure a matching rule based on the outbound interface of GE0/0/1 in the traffic classifier **class1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier class1
[HUAWEI-classifier-class1] if-match outbound-interface gigabitethernet 0/0/1
```

Related Topics

15.1.32 traffic classifier

15.1.25 if-match protocol

Function

The **if-match protocol** command configures a matching rule based on a protocol in a traffic classifier.

The **undo if-match protocol** command deletes a matching rule based on a protocol in a traffic classifier.

By default, a matching rule based on a protocol is not configured in a traffic classifier.

Format

if-match protocol { **ip** | **ipv6** }

undo if-match protocol

Parameters

Parameter	Description	Value
ip	Specifies an IP protocol.	-
ipv6	Specifies an IPv6 protocol.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match protocol** command to classify packets based on a protocol so that the device processes packets of the same protocol in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

Currently, the device supports IPv4 and IPv6.

If you run the **if-match protocol** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

If the relationship between rules in a traffic classifier is AND, and both the **if-match protocol** and **if-match l2-protocol arp** commands are configured in this traffic classifier, of the two, only the **if-match l2-protocol arp** command takes effect.

Example

# Configure a matching rule based on the IP protocol in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match protocol ip
```

Related Topics

15.1.32 traffic classifier

15.1.26 if-match source-mac

Function

The **if-match source-mac** command configures a matching rule based on the source MAC address in a traffic classifier.

The **undo if-match source-mac** command deletes a matching rule based on the source MAC address in a traffic classifier.

By default, a matching rule based on the source MAC address is not configured in a traffic classifier.

Format

if-match source-mac *mac-address* [*mac-address-mask*]

undo if-match source-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the source MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
mac-address-mask	Specifies the mask of the source MAC address. Similar to the mask of the IP address, the mask of the MAC address determines a group of MAC addresses. The device can accurately match certain bits in the source MAC address using the mask of the MAC address. In practice, you can set these bits to F in the mask of the source MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be 0-0-0.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match source-mac** command to classify packets based on the source MAC address so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you run the **if-match source-mac** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure a matching rule based on the source MAC address of 0050-ba27-bed2 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match source-mac 0050-ba27-bed2
```

# Configure a matching rule based on the source MAC address of XX50-bXX7-bed3 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match source-mac 0050-ba27-bed3 00ff-f00f-ffff
```

Related Topics

15.1.16 if-match destination-mac

15.1.32 traffic classifier

15.1.27 if-match tcp

Function

The **if-match tcp** command configures a matching rule based on the SYN Flag in the TCP packet header in a traffic classifier.

The **undo if-match tcp** command deletes a matching rule based on the SYN Flag in the TCP packet header in a traffic classifier.

By default, a matching rule based on the SYN Flag in the TCP packet header is not configured in a traffic classifier.

Format

if-match tcp syn-flag { *syn-flag-value* | **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }

undo if-match tcp syn-flag

Parameters

Parameter	Description	Value
syn-flag	Specifies the SYN Flag in the TCP packet header.	-
syn-flag-value	Specifies the SYN Flag in the TCP packet header.	The value is an integer that ranges from 0 to 63.
ack	Indicates that the SYN Flag type in the TCP packet header is ACK.	-
fin	Indicates that the SYN Flag type in the TCP packet header is FIN.	-
psh	Indicates that the SYN Flag type in the TCP packet header is PSH.	-
rst	Indicates that the SYN Flag type in the TCP packet header is RST.	-
syn	Indicates that the SYN Flag type in the TCP packet header is SYN.	-
urg	Indicates that the SYN Flag type in the TCP packet header is URG.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match tcp** command to classify packets based on the SYN Flag in the TCP packet header so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you run the **if-match tcp** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

# Configure a matching rule based on the SYN Flag of psh in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match tcp syn-flag psh
```

Related Topics

15.1.32 traffic classifier

15.1.28 if-match vlan-id

Function

The **if-match vlan-id** command configures a matching rule based on the VLAN ID of packets in a traffic classifier.

The **undo if-match vlan-id** command deletes a matching rule based on the VLAN ID of packets in a traffic classifier.

By default, a matching rule based on the VLAN ID of packets is not configured in a traffic classifier.

Format

if-match vlan-id *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]

undo if-match vlan-id *start-vlan-id* [**to** *end-vlan-id*] [**cvlan-id** *cvlan-id*]

NOTE

Only the S1720X, S1720X-E, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support the **cvlan-id** *cvlan-id* parameter.

Parameters

Parameter	Description	Value
start-vlan-id [**to** *end-vlan-id*]	Specifies the outer VLAN ID.	- *start-vlan-id* specifies the start outer VLAN ID. The value of *start-vlan-id* is an integer that ranges from 1 to 4094. - *end-vlan-id* specifies the end outer VLAN ID. The value of *end-vlan-id* is an integer that ranges from 1 to 4094. *end-vlan-id* must be larger than *start-vlan-id*. If **to** *end-vlan-id* is not specified, only the VLAN ID specified by *start-vlan-id* is matched.
cvlan-id *cvlan-id*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match vlan-id** command to classify packets based on the VLAN ID so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

On the S6720EI, if a traffic policy contains the traffic classifier defining the **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*] **cvlan-id** *cvlan-id* matching rule, IPv6 ACL resources are occupied. To display information about IPv6 ACL resources, run the **display acl resource** command.

Example

# Configure a matching rule based on VLAN 2 in the traffic classifier **c1**.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1] if-match vlan-id 2
```

Related Topics

15.1.32 traffic classifier

15.1.29 remark flow-id

Function

The **remark flow-id** command configures an action of re-marking the flow ID in a traffic behavior.

The **undo remark flow-id** command deletes the configuration.

By default, an action of re-marking the flow ID is not configured in a traffic behavior.

NOTE

Only the S5720EI, S6720EI, and S6720S-EI support this command.

Format

remark flow-id *flow-id*

undo remark flow-id

Parameters

Parameter	Description	Value
flow-id	Specifies the value of a flow ID.	The value is an integer that ranges from 1 to 8.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

When a traffic policy is applied to different interfaces or VLANs, to save ACL resources, you can run the **if-match flow-id** command to classify packets based on the flow ID so that the device processes packets matching the same flow ID in the same manner. Before the device classifies packets based on the flow ID, use the **remark flow-id** command to configure an action of re-marking the flow ID in a traffic behavior.

Assume that M ACLs are configured on the device to distinguish services, and each ACL contains N ACL rules. Traffic classifiers classify packets based on ACL rules, and the traffic policy containing the ACL rules are applied to X interfaces. If the action of re-marking flow IDs and matching rules based on the flow IDs are not configured, applying the traffic policy occupies $M*N*X$ ACL resources. If the action of re-marking flow IDs and matching rules based on flow IDs are configured, applying the traffic policy occupies only $M*(N+X)$ ACL resources.

Follow-up Procedure

Run the **traffic classifier** command to configure a traffic classifier and run the **if-match flow-id** command in the traffic classifier view to create a matching rule based on the flow ID.

Precautions

It is recommended that the traffic classifier containing **if-match flow-id** and the traffic behavior containing **remark flow-id** be bound to different traffic policies.

The traffic policy containing **remark flow-id** can be only applied to an interface, a VLAN, or the system in the inbound direction.

remark flow-id, **statistic enable**, and **car** cannot be configured in the same traffic behavior.

If you run the **remark flow-id** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

# Configure the device to re-mark the flow ID with 4 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark flow-id 4
```

Related Topics

15.1.20 if-match flow-id

15.1.31 traffic behavior

15.1.30 reset traffic policy statistics

Function

The **reset traffic policy statistics** command clears statistics on packets matching a traffic policy that has been applied to the specified object or each object.

Format

reset traffic policy statistics { **global** [**slot** *slot-id*] | **interface** *interface-type interface-number* [*.subinterface-number*] | **vlan** *vlan-id* | **ssid-profile** *ssid-profile-name* } { **inbound** | **outbound** }

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support sub-interfaces.

Only the S5720HI supports **ssid-profile** *ssid-profile-name*.

reset traffic policy statistics policy-name *policy-name*

reset traffic policy statistics all

Parameters

Parameter	Description	Value
global	Clears statistics on packets matching a traffic policy in the system.	-
slot *slot-id*	Clears statistics on packets matching a traffic policy on a specified device. *slot-id* specifies the slot ID of the device.	The value range depends on the device configuration.
interface *interface-type interface-number* [*.subinterface-number*]	Clears statistics on packets matching a traffic policy on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* [*.subinterface-number*] specifies the interface or sub-interface number.	-
vlan *vlan-id*	Clears statistics on packets matching a traffic policy in a specified VLAN. *vlan-id* specifies the ID of the VLAN.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
ssid-profile *ssid-profile-name*	Clears statistics on packets matching a traffic policy in a specified SSID profile. *ssid-profile-name* specifies the name of the SSID profile.	The value must the name of an existing SSID profile.
inbound	Clears traffic statistics in the inbound direction.	-
outbound	Clears traffic statistics in the outbound direction.	-
policy-name *policy-name*	Clears statistics on packets matching the specified traffic policy in each object.	The value must be the name of an existing traffic policy.
all	Clears statistics on packets matching a traffic policy in each object, including statistics on packets in the inbound and outbound directions in the system, on each interface, in each VLAN, and in each SSID profile.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before recollecting statistics on packets matching a traffic policy in the specified object or each object, run the **reset traffic policy statistics** command to clear existing packet statistics. Then run the **display traffic policy statistics** command to view packet statistics.

Precautions

The traffic policies that can be deleted from the device every second are limited. If many traffic policies are applied to the device, it may take a long time to delete the traffic policies.

The cleared traffic statistics cannot be restored. Exercise caution when you use the command.

If no traffic policy is applied, the system displays an error message after the **reset traffic policy statistics** command is executed:

```
Error: The Policy is not applied in this view.
```

If you do not run the **statistic enable (traffic behavior view)** command in the view of the traffic behavior in a traffic policy, the system displays an error message after the **reset traffic policy statistics** command is executed:

```
Info: Statistic has not been enabled.
```

Example

# Clear traffic statistics on GE0/0/1 in the inbound direction to which a traffic policy has been applied.

```
<HUAWEI> reset traffic policy statistics interface gigabitethernet 0/0/1 inbound
```

Related Topics

15.1.7 display traffic policy statistics

15.7.2 statistic enable (traffic behavior view)

15.1.33 traffic policy

15.1.31 traffic behavior

Function

The **traffic behavior** command creates a traffic behavior and displays the traffic behavior view, or directly displays the view of an existing traffic behavior.

The **undo traffic behavior** command deletes a traffic behavior.

By default, no traffic behavior is created in the system.

Format

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

Parameters

Parameter	Description	Value
behavior-name	Specifies the name of a traffic behavior.	The value is a string of 1 to 64 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A traffic classifier is used to differentiate services and must be associated with a flow control or resource allocation action such as packet filtering, traffic policing, and re-marking. The actions constitute a traffic behavior. The **traffic behavior** command creates a traffic behavior.

Follow-up Procedure

Configure an action in the traffic behavior view. For example, run the **car (traffic behavior view)** command to configure the traffic policing action.

Precautions

To delete a traffic behavior, unbind the traffic policy containing the traffic behavior from the system, an interface, or a VLAN where the traffic policy is applied and unbind the traffic behavior from the traffic classifier. To modify only actions in a traffic behavior, you do not need to unbind the traffic policy containing the traffic behavior from the system, an interface, or a VLAN.

On the device, a maximum of 256 traffic behaviors can be created and multiple traffic actions can be configured in a traffic behavior.

Example

# Create the traffic behavior **b1** and enter the traffic behavior view.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1]
```

Related Topics

15.1.2 classifier behavior

15.1.4 display traffic behavior

15.1.32 traffic classifier

15.1.33 traffic policy

15.1.32 traffic classifier

Function

The **traffic classifier** command creates a traffic classifier and displays the traffic classifier view, or directly displays the view of an existing traffic classifier.

The **undo traffic classifier** command deletes a traffic classifier.

By default, no traffic classifier is created in the system.

Format

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

undo traffic classifier *classifier-name*

Parameters

Parameter	Description	Value
classifier-name	Specifies the name of a user-defined traffic classifier.	The value is a string of 1 to 64 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
operator	Specifies the relationship between rules in a traffic classifier. If this parameter is not specified, the relationship between rules is OR by default.	-
and	Indicates that the relationship between rules is AND. After this parameter is specified, the following situations occur: ● If a traffic classifier contains ACL rules, packets match the traffic classifier only when the packets match one ACL rule and all the non-ACL rules. ● If a traffic classifier does not contain ACL rules, packets match the traffic classifier only when the packets match all the non-ACL rules.	-

Parameter	Description	Value
or	Indicates that the relationship between rules is OR. After this parameter is specified, packets match a traffic classifier if the packets match one or more rules.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A traffic classifier classifies traffic of a certain type using matching rules. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior (see **traffic behavior**) to a traffic policy and apply the traffic policy.

A traffic classifier can be created based on Layer 2 information such as the 802.1p priority in the VLAN ID, 802.1p priority in the C-VLAN ID, VLAN ID, C-VLAN ID, or Layer 2 protocol type, and Layer 3 information such as the DSCP priority or IP priority, or ACLs.

Follow-up Procedure

Define rules in the traffic classifier. For example, run the **if-match 8021p** command to define rules based on the 802.1p priority in the VLAN tag.

Precautions

To delete a traffic classifier, unbind the traffic policy containing the traffic classifier from the system, an interface, or a VLAN where the traffic policy is applied and unbind the traffic classifier from the traffic behavior.

A maximum of 512 traffic classifiers can be created on the device.

After the relationship between rules in a traffic classifier is changed, the system checks whether rules conflict. When the relationship between rules is changed from OR to AND and multiple rules are configured, for example, matching rules based on the 802.1p priority in the inner VLAN tag, DSCP priority, IP precedence, and VLAN ID, the rules may conflict and the traffic policy cannot take effect. If the relationship between rules is changed from AND to OR, the traffic policy still takes effect but services may be affected because more packets are matched. Exercise caution when you change the relationship between rules.

Example

# Create a traffic classifier **c1** and enter the traffic classifier view.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1 operator and
[HUAWEI-classifier-c1]
```

Related Topics

15.1.2 classifier behavior

15.1.5 display traffic classifier

15.1.31 traffic behavior

15.1.33 traffic policy

15.1.33 traffic policy

Function

The **traffic policy** command creates a traffic policy and specifies the matching order of traffic classifiers in the traffic policy.

The **undo traffic policy** command deletes a traffic policy.

By default, no traffic policy is created in the system.

Format

traffic policy *policy-name* [**match-order** { **auto** | **config** }] [**atomic**]

undo traffic policy *policy-name*

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support **match-order** { **auto** | **config** }.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value is a string of 1 to 64 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
match-order	Specifies the matching order of traffic classifiers in the traffic policy. By default, the matching order of traffic classifiers in a traffic policy is **config**.	-
auto	Indicates that the matching order depends on priorities of traffic classifier types. Traffic classifiers based on the following information are in descending order of priority: ● Layer 2 and IPv4 Layer 3 information ● Advanced ACL6 information ● Basic ACL6 information ● Layer 2 information ● IPv4 Layer 3 information ● User-defined ACL information If this parameter is specified, ACL resources are saved.	-
config	Indicates that the matching order depends on the sequence in which traffic classifiers were bound to traffic behaviors. If this parameter is specified, more ACL resources are consumed.	-

Parameter	Description	Value
atomic	Indicates the atomic attribute of a traffic policy. After this parameter is specified, if a traffic policy references an ACL and the ACL is applied to a specified object, dynamically updating the ACL does not interrupt services.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are obtained based on Layer 2 information, Layer 3 information, or ACLs. To implement differentiated services for service flows of packets, bind a traffic classifier and a traffic behavior to the created traffic policy and apply the traffic policy. You can use the **traffic policy** command to create a traffic policy. A maximum of 256 traffic policies can be created on the device.

Pre-configuration Tasks

A traffic classifier and a traffic behavior have been created.

Follow-up Procedure

- Run the **classifier behavior** command in the traffic policy view to associate the traffic policy with a traffic classifier and a traffic behavior.
- Run the **traffic-policy global**, **traffic-policy (interface view)**, **traffic-policy (VLAN view)** or **traffic-policy (VLANIF interface view)** command to apply the traffic policy to the system, an interface, or a VLAN to make the created traffic policy take effect.

Precautions

For the S5720HI, no matter whether the traffic policy defines the **auto** or **config** matching order, traffic classifiers bound to the traffic policy always take effect in the **config** order.

For the S5720EI, S6720EI, and S6720S-EI, when the traffic policy that defines the **config** matching order is applied to the inbound direction, traffic classifiers bound to the traffic policy take effect based on the **config** matching order. When the traffic policy is applied to the outbound direction, even if the matching order is

config, traffic classifiers bound to the traffic policy still take effect based on the **auto** matching order.

For the S5720EI, S6720EI, and S6720S-EI, when any of the following actions is defined in a traffic action of a traffic policy, even if the matching order is **config**, traffic classifiers bound to the traffic policy still take effect in the **auto** order:

- **mac-address learning disable**
- **remark 8021p**
- **remark cvlan-id**
- **remark flow-id**

You cannot directly modify the atomic attribute of a created traffic policy. To modify the atomic attribute, delete the traffic policy, and then recreate the traffic policy with the atomic attribute being specified or deleted.

The atomic attribute is valid for the traffic policy only containing the **permit** or **deny** action. If the traffic policy in which the atomic attribute is specified contains other actions in addition to **permit** or **deny**, applying the traffic policy will cause a failure to deliver the configuration.

For the traffic policy with specified atomic attribute, when the ACL configuration is being updated dynamically, ensure that the device has sufficient ACL resources. Otherwise, the updated ACL configuration will fail to be delivered.

If the atomic attribute is specified for a traffic policy and the device is downgraded from the current version to a version earlier than V200R011C10, the traffic policy configuration cannot be restored during device restart.

If the traffic policy that you want to delete has been applied to the system, an interface, or a VLAN, run the **undo traffic-policy** command to unbind the traffic policy in the corresponding view. Then run the **undo traffic policy** command in the system view to delete the traffic policy. The traffic policy that is not applied can be deleted directly.

When **rule** is configured in the traffic policy and **permit ip** is specified, many ARP Miss packets may be sent to the CPU. As a result, the device is disconnected.

Example

# Create a traffic policy **p1**, and associate the traffic classifier **c1** with the traffic behavior **b1** in the traffic policy.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match any
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark 8021p 2
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
```

# Delete the traffic policy **p1** that has been applied to the inbound indirection on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo traffic-policy p1 inbound
```

```
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] undo traffic policy p1
```

Related Topics

15.1.2 classifier behavior

15.1.6 display traffic policy

15.1.31 traffic behavior

15.1.32 traffic classifier

15.1.41 traffic-policy global

15.1.36 traffic-policy (interface view)

15.1.37 traffic-policy (SSID profile view)

15.1.38 traffic-policy (VLAN view)

15.1.39 traffic-policy (VLANIF interface view)

15.1.34 traffic statistics interval

Function

The **traffic statistics interval** command sets the interval at which the system measures the rates of forwarded and discarded packets in a queue.

The **undo traffic statistics interval** command restores the default interval.

By default, the system measures the rates of forwarded and discarded packets in a queue at intervals of 300s.

Format

traffic statistics interval *time-value*

undo traffic statistics interval [*time-value*]

Parameters

Parameter	Description	Value
time-value	Specifies the interval at which the system measures the rates of forwarded and discarded packets in a queue.	The value is an integer that ranges from 30 to 600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device is managed by a network management system (NMS), the MIB module checks the rates of forwarded and discarded packets in each queue at intervals and sends the rates to the NMS. You can view the rates of forwarded and discarded packets in each queue to analyze network performance or locate faults. The MIB module calculates the average rates forwarded and discarded packets during an interval configured by this command.

Example

# Set the interval at which the system measures the rates of forwarded and discarded packets in a queue to 100s.

```
<HUAWEI> system-view
[HUAWEI] traffic statistics interval 100
```

15.1.35 traffic statistics mode by-bytes

Function

The **traffic statistics mode by-bytes** command enables byte-based traffic statistics in a traffic policy.

The **undo traffic statistics mode by-bytes** command disables byte-based traffic statistics in a traffic policy.

By default, the byte-based traffic statistics function is not enabled in a traffic policy.

NOTE

The S5720EI, S5720HI, S6720EI, and S6720S-EI do not support this command.

Format

traffic statistics mode by-bytes

undo traffic statistics mode by-bytes

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the traffic statistics function is defined in a traffic policy, the switch collects traffic statistics by packet by default. To collect traffic statistics by byte, run the **traffic statistics mode by-bytes** command. Then the **display traffic policy statistics** command displays the packet rate by byte.

Example

# Enable byte-based traffic statistics in a traffic policy.

```
<HUAWEI> system-view
[HUAWEI] traffic statistics mode by-bytes
```

Related Topics

15.1.7 display traffic policy statistics

15.1.30 reset traffic policy statistics

15.1.36 traffic-policy (interface view)

Function

The **traffic-policy** command applies a traffic policy to an interface.

The **undo traffic-policy** command deletes a traffic policy from an interface.

By default, no traffic policy is applied to an interface.

Format

traffic-policy *policy-name* { **inbound** | **outbound** }

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

NOTE

Traffic policies can be applied to only the inbound direction of sub-interfaces on the S5720EI, S5720HI, S6720EI, and S6720S-EI.

NOTE

- Only the S6720EI, S6720S-EI, S5720HI, and S5720EI support Ethernet sub-interfaces.
- Only hybrid and trunk interfaces on the preceding switches support Ethernet sub-interface configuration.
- After you run the **undo portswitch** command to switch Layer 2 interfaces on the preceding series of switches into Layer 3 interfaces, you can configure Ethernet sub-interfaces on the interfaces.
- After an interface is added to an Eth-Trunk, sub-interfaces cannot be configured on the interface.
- VLAN termination sub-interfaces cannot be created on a VCMP client.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value must be the name of an existing traffic policy.
inbound	Applies a traffic policy to the inbound direction.	-
outbound	Applies a traffic policy to the outbound direction.	-

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, GE sub-interface view, XGE sub-interface view, 40GE sub-interface view, Eth-Trunk sub-interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy. You can use the **traffic-policy** command to apply a created traffic policy to an interface.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

Only one traffic policy can be applied to each direction on an interface, but a traffic policy can be applied to different directions on different interfaces.

After a traffic policy is applied to an interface, you cannot directly delete the traffic policy, the traffic classifier and traffic behavior bound to the traffic policy. In addition, you cannot modify the matching order of the rules in the traffic policy. However, you can modify the relationship between matching rules in the traffic classifier, matching rules in the traffic classifier, traffic action in the traffic behavior, and binding between the traffic classifier and the traffic behavior.

If the traffic policy that you want to delete has been applied to an interface, run the **undo traffic-policy** command to unbind the traffic policy from the interface. Then run the **undo traffic policy** command in the system view to delete the traffic policy.

Run the **undo traffic-policy** { **inbound** | **outbound** } command without *policy-name* specified to delete the traffic policy that has been applied to an interface and has the following names: i, in, inb, inbo, inbou, inboun, inbound, o, ou, out, outb, outbo, outbou, outboun, and outbound.

Example

# Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-policy p1 inbound
```

Related Topics

15.1.2 classifier behavior

15.1.6 display traffic policy

15.1.9 display traffic-applied

15.1.10 display traffic-policy applied-record

15.1.31 traffic behavior

15.1.32 traffic classifier

15.1.33 traffic policy

15.1.41 traffic-policy global

15.1.37 traffic-policy (SSID profile view)

15.1.38 traffic-policy (VLAN view)

15.1.39 traffic-policy (VLANIF interface view)

15.1.37 traffic-policy (SSID profile view)

Function

traffic-policy command applies a traffic policy to an SSID profile.

undo traffic-policy command deletes a traffic policy from an SSID profile.

By default, no traffic policy is applied to an SSID profile.

Format

traffic-policy *policy-name* { **inbound** | **outbound** }

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

NOTE

Only the S5720HI supports this command.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value must be the name of an existing traffic policy.
inbound	Applies a traffic policy to the inbound direction of an SSID profile.	-
outbound	Applies a traffic policy to the outbound direction of an SSID profile.	-

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy. You can use the **traffic-policy** command to apply a traffic policy to an SSID profile.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

Only one traffic policy can be applied to each direction in an SSID profile, but a traffic policy can be applied to different directions in different SSID profiles.

NOTE

After a traffic policy is applied to an SSID profile, you cannot directly delete the traffic policy, the traffic classifier and traffic behavior bound to the traffic policy. In addition, you cannot modify the matching order of the rules in the traffic policy. However, you can modify the relationship between matching rules in the traffic classifier, matching rules in the traffic classifier, priority of the traffic classifier, traffic action in the traffic behavior, and binding between the traffic classifier and the traffic behavior.

If the traffic policy that you want to delete has been applied to an SSID profile, run the **undo traffic-policy** command to unbind the traffic policy from the SSID profile. Then run the **undo traffic policy** command in the system view to delete the traffic policy.

Run the **undo traffic-policy** { **inbound** | **outbound** } command without *policy-name* specified to delete the traffic policy that has been applied to an SSID profile and has the following names: i, in, inb, inbo, inbou, inboun, inbound, o, ou, out, outb, outbo, outbou, outboun, and outbound.

Example

# Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction in the SSID profile named test.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] wlan
[HUAWEI-wlan-view] ssid-profile name test
[HUAWEI-wlan-ssid-prof-test] traffic-policy p1 inbound
```

Related Topics

15.1.2 classifier behavior

15.1.10 display traffic-policy applied-record

15.1.31 traffic behavior

15.1.32 traffic classifier

15.1.33 traffic policy

15.1.41 traffic-policy global

15.1.38 traffic-policy (VLAN view)

15.1.36 traffic-policy (interface view)

15.1.38 traffic-policy (VLAN view)

Function

The **traffic-policy** command applies a traffic policy to a VLAN.

The **undo traffic-policy** command deletes a traffic policy from a VLAN.

By default, no traffic policy is applied to a VLAN.

Format

traffic-policy *policy-name* { **inbound** | **outbound** }

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

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy.	The value must be the name of an existing traffic policy.

Parameter	Description	Value
inbound	Applies a traffic policy to the inbound direction of a VLAN.	-
outbound	Applies a traffic policy to the outbound direction of a VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy. You can use the **traffic-policy** command to apply a traffic policy to a VLAN.

Prerequisites

A traffic policy has been created using the **traffic policy** command.

Precautions

After a traffic policy is applied to a VLAN, the traffic policy takes effect for packets received and sent in the VLAN.

If a traffic policy has been applied to a VLAN, you are not allowed to delete the traffic policy or its traffic classifier and traffic behavior.

After a traffic policy is applied to a VLAN, you cannot directly delete the traffic policy, the traffic classifier and traffic behavior bound to the traffic policy. In addition, you cannot modify the matching order of the rules in the traffic policy. However, you can modify the relationship between matching rules in the traffic classifier, matching rules in the traffic classifier, traffic action in the traffic behavior, and binding between the traffic classifier and the traffic behavior.

To delete the traffic policy that has been applied, run the **undo traffic-policy** command in the corresponding view to unbind the traffic policy and then run the **undo traffic policy** command in the system view to delete the traffic policy.

Example

# Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] vlan 100
[HUAWEI-vlan100] traffic-policy p1 inbound
```

Related Topics

15.1.2 classifier behavior

15.1.6 display traffic policy

15.1.9 display traffic-applied

15.1.10 display traffic-policy applied-record

15.1.31 traffic behavior

15.1.32 traffic classifier

15.1.33 traffic policy

15.1.41 traffic-policy global

15.1.37 traffic-policy (SSID profile view)

15.1.39 traffic-policy (VLANIF interface view)

15.1.36 traffic-policy (interface view)

15.1.39 traffic-policy (VLANIF interface view)

Function

The **traffic-policy** command applies a traffic policy to a VLANIF interface.

The **undo traffic-policy** command deletes a traffic policy from a VLANIF interface.

By default, no traffic policy is applied to a VLANIF interface.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

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

undo traffic-policy [*policy-name*] **inbound**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value must be the name of an existing traffic policy.
inbound	Applies a traffic policy to the inbound direction.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy. You can use the **traffic-policy** command to apply a created traffic policy to a VLANIF interface.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

Only one traffic policy can be applied to the inbound direction on a VLANIF interface. A single traffic policy can be applied to the inbound direction on one or more VLANIF interfaces.

A traffic policy cannot be applied to a VLANIF interface corresponding to the super-VLAN or MUX VLAN.

On the S5720EI, S6720EI, and S6720S-EI, a traffic policy that is applied to a VLANIF interface is only valid for unicast packets and Layer 3 multicast packets on the VLANIF interface.

On the S5720HI:

- A traffic policy that is applied to a VLANIF interface is only valid for unicast packets on the VLANIF interface.
- A traffic policy that is applied to a VLANIF interface cannot contain a traffic classifier defining user-defined ACLs.

A traffic policy cannot be applied to a VLANIF interface when the bound traffic behavior of the traffic policy defines the following actions:

- **remark vlan-id**
- **remark cvlan-id**
- **remark 8021p**
- **remark flow-id**
- **mac-address learning disable**

After a traffic policy is applied to a VLANIF interface, you cannot directly delete the traffic policy, the traffic classifier and traffic behavior bound to the traffic policy. In addition, you cannot modify the matching order of the rules in the traffic policy. However, you can modify the relationship between matching rules in the traffic classifier, matching rules in the traffic classifier, traffic action in the traffic behavior, and binding between the traffic classifier and the traffic behavior.

If the traffic policy that you want to delete has been applied to a VLANIF interface, run the **undo traffic-policy** command to unbind the traffic policy from the VLANIF interface. Then run the **undo traffic policy** command in the system view to delete the traffic policy.

Run the **undo traffic-policy inbound** command without *policy-name* specified to delete the traffic policy that has been applied to a VLANIF interface and has the following names: i, in, inb, inbo, inbou, inboun, and inbound.

Example

# Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] traffic-policy p1 inbound
[HUAWEI-Vlanif100] quit
```

Related Topics

15.1.2 classifier behavior

15.1.6 display traffic policy

15.1.9 display traffic-applied

15.1.10 display traffic-policy applied-record

15.1.31 traffic behavior

15.1.32 traffic classifier

15.1.33 traffic policy

15.1.41 traffic-policy global

15.1.37 traffic-policy (SSID profile view)

15.1.36 traffic-policy (interface view)

15.1.38 traffic-policy (VLAN view)

15.1.40 traffic-policy fast-mode enable

Function

The **traffic-policy fast-mode enable** command enables fast delivery of ACL rules.

The **undo traffic-policy fast-mode enable** command disables fast delivery of ACL rules.

By default, fast delivery of ACL rules is disabled.

Format

traffic-policy fast-mode enable

undo traffic-policy fast-mode enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many ACL rules are applied in the system view, and then some of them are applied in the interface view, it takes a long time to deliver ACL rules. As a result, the ACL rules are slow to take effect, and the CPU usage is high. To speed up ACL delivery, run the **traffic-policy fast-mode enable** command.

Precautions

After the **traffic-policy fast-mode enable** command is run:

- ACL rules in effect may be invalid temporarily.
- The statistics on traffic policies are cleared.
- The device performance deteriorates.

Example

# Enable fast delivery of ACL rules.

```
<HUAWEI> system-view
[HUAWEI] traffic-policy fast-mode enable
```

15.1.41 traffic-policy global

Function

The **traffic-policy global** command applies a traffic policy to the system.

The **undo traffic-policy global** command deletes a traffic policy that is applied to the system.

By default, no traffic policy is applied to the system.

Format

traffic-policy *policy-name* **global** { **inbound** | **outbound** } [**slot** *slot-id*]

undo traffic-policy [*policy-name*] **global** { **inbound** | **outbound** } [**slot** *slot-id*]

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy.	The value must be the name of an existing traffic policy.
inbound	Applies a traffic policy to the inbound direction.	-
outbound	Applies a traffic policy to the outbound direction.	-
slot *slot-id*	On a stacked device, if *slot-id* is not specified, the traffic policy can be applied to all devices in the stack.	The value is fixed on a non-stacked device, and specifies the stack ID on a stacked device. **NOTE** If the value of *slot-id* is specified in the **undo traffic-policy** command, it must be the same with the ID of the specified slot to which the traffic policy is applied.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy.

You can use the **traffic policy global** command to apply a traffic policy to the system.

Prerequisites

A traffic policy has been created using the **traffic policy** command.

Precautions

If a traffic policy has been applied, you cannot directly change the traffic policy or its traffic classifier and traffic behavior.

After a traffic policy is applied, you cannot directly delete the traffic policy or the traffic classifier and traffic behavior bound to the traffic policy. In addition, you cannot modify the matching order of the rules in the traffic policy. However, you can modify the relationship between matching rules in the traffic classifier, matching rules in the traffic classifier, traffic action in the traffic behavior, and binding between the traffic classifier and the traffic behavior.

Run the **undo traffic-policy global** { **inbound** | **outbound** } command without *policy-name* specified to delete the traffic policy that has been applied to an interface and has the following names: g, gl, glo, glob, globa, and global.

The traffic policy that has the following names cannot be applied to the system: f, fa, fas, fast, fast-, fast-m, fast-mo, fast-mod, and fast-mode.

Example

# Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction.

```
<HUAWEI> system-view
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] traffic-policy p1 global inbound
```

Related Topics

15.1.2 classifier behavior

15.1.6 display traffic policy

15.1.9 display traffic-applied

15.1.10 display traffic-policy applied-record

15.1.31 traffic behavior

15.1.32 traffic classifier

15.1.33 traffic policy

15.1.37 traffic-policy (SSID profile view)

15.1.38 traffic-policy (VLAN view)

15.1.39 traffic-policy (VLANIF interface view)

15.1.36 traffic-policy (interface view)

15.1.42 traffic rate statistics enable

Function

The **traffic rate statistics enable** command enables traffic rate statistics collection in a traffic policy.

The **undo traffic rate statistics enable** command disables traffic rate statistics collection in a traffic policy.

By default, traffic rate statistics collection is enabled in a traffic policy.

Format

traffic rate statistics enable

undo traffic rate statistics enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the traffic statistics function is configured in a traffic policy and more than 60K traffic classification rules are configured, memory resources may be insufficient. To release memory resources, run the **undo traffic rate statistics enable** command to disable traffic rate statistics collection in the traffic policy.

Precautions

After traffic rate statistics collection is disabled in a traffic policy, the **display traffic policy statistics** command can still display the number of packets and bytes, but traffic rates are all displayed as -.

This command is valid for traffic policies configured after traffic rate statistics collection is enabled or disabled, and traffic rate statistics collection is not disabled in traffic policies that have been configured before this command is executed.

Before you disable traffic rate statistics collection in a traffic policy, traffic statistics are displayed as follows:

```
<HUAWEI> display traffic policy statistics global slot 0 inbound
 Global :
 Traffic policy inbound: test
 Rule number: 1
 Current status: success
 Statistics interval: 300
---------------------------------------------------------------------
 Board : 0
---------------------------------------------------------------------
 Matched          |      Packets:                          0
                  |      Bytes:                      0
                  |      Rate(pps):                    0
                  |      Rate(bps):                    0
---------------------------------------------------------------------
   Passed         |      Packets:                          0
                  |      Bytes:                      0
                  |      Rate(pps):                    0
                  |      Rate(bps):                    0
---------------------------------------------------------------------
   Dropped        |      Packets:                          0
                  |      Bytes:                      0
                  |      Rate(pps):                    0
                  |      Rate(bps):                    0
---------------------------------------------------------------------
     Filter       |      Packets:                        0
                  |      Bytes:                      0
```

```
--------------------------------------------------------------------
   Car        |     Packets:                         0
              |     Bytes:                           0
--------------------------------------------------------------------
```

After you disable traffic rate statistics collection in a traffic policy, traffic statistics are displayed as follows:

```
<HUAWEI> display traffic policy statistics global slot 0 inbound
 Global :
 Traffic policy inbound: testp
 Rule number: 1
 Current status: success
 Statistics interval: 300
--------------------------------------------------------------------
 Board : 0
--------------------------------------------------------------------
 Matched        |     Packets:                       0
              |     Bytes:                           0
              |     Rate(pps):                        -
              |     Rate(bps):                        -
--------------------------------------------------------------------
   Passed       |     Packets:                       0
              |     Bytes:                           0
              |     Rate(pps):                        -
              |     Rate(bps):                        -
--------------------------------------------------------------------
   Dropped      |     Packets:                       0
              |     Bytes:                           0
              |     Rate(pps):                        -
              |     Rate(bps):                        -
--------------------------------------------------------------------
   Filter       |     Packets:                       0
              |     Bytes:                           0
--------------------------------------------------------------------
   Car        |     Packets:                         0
              |     Bytes:                           0
--------------------------------------------------------------------
```

Example

# Disable traffic rate statistics collection in a traffic policy.

```
<HUAWEI> system-view
[HUAWEI] undo traffic rate statistics enable
```

Related Topics

15.7.2 statistic enable (traffic behavior view)

15.1.7 display traffic policy statistics

15.2 Priority Mapping Commands

15.2.1 Command Support

For details about command support, see the description of each command. If no command support information is provided, all switch models support the command by default.

15.2.2 8021p-inbound

Function

The **8021p-inbound** command maps the 802.1p priority of incoming VLAN packets in a DiffServ domain to the PHB and colors the packets.

The **undo 8021p-inbound** command restores the default mapping.

Table 15-11 lists the default mappings from the 802.1p priorities to PHBs and colors of incoming VLAN packets in a DiffServ domain.

Table 15-11 Mappings from 802.1p priorities to PHBs and colors of incoming packets in the DiffServ domain

802.1p Priority	PHB	Color
0	BE	green
1	AF1	green
2	AF2	green
3	AF3	green
4	AF4	green
5	EF	green
6	CS6	green
7	CS7	green

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

8021p-inbound *8021p-value* **phb** *service-class* [**green** | **yellow** | **red**]

undo 8021p-inbound [*8021p-value*]

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority of VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
phb *service-class*	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7, each of which corresponds to queues 0 to 7 respectively.
green	Indicates that packets are colored green.	-
yellow	Indicates that packets are colored yellow.	-
red	Indicates that packets are colored red.	-

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

Scenario

To implement QoS scheduling on incoming VLAN packets, you can use the **8021p-inbound** command to map the 802.1p priorities of the packets to the PHBs and colors. After a DiffServ domain is bound to the inbound interface of packets, the device forwards the packets to queues based on PHBs of the packets. Congestion management is implemented. Packets are scheduled according to their colors after a discard template is configured, avoiding congestion.

Precautions

- The color is used to determine whether packets are discarded during flow control, and is independent of the mapping from internal priorities to queues.
- The CoS values of packets are mapped to the corresponding internal priorities and the packets are colored accordingly. If no mapping from 802.1p priorities to CoS values is specified, the device uses the default mappings of the system.
- If you do not specify the parameter *8021p-value* when running the **undo 8021p-inbound** command, all the mapping between 802.1p priorities and CoS values is restored.

Example

# In DiffServ domain **ds1**, map the 802.1p priority 2 of the incoming VLAN packets to PHB AF1 and mark the packets yellow.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] 8021p-inbound 2 phb af1 yellow
```

Related Topics

15.2.3 8021p-outbound

15.2.3 8021p-outbound

Function

The **8021p-outbound** command maps the PHB and color of outgoing VLAN packets in a DiffServ domain to the 802.1p priority.

The **undo 8021p-outbound** command restores the default mapping.

Table 15-12 lists the default mappings from the PHBs and colors to 802.1p priorities of outgoing VLAN packets in a DiffServ domain.

Table 15-12 Mappings from PHBs and colors to 802.1p priorities of outgoing VLAN packets in the DiffServ domain

PHB	Color	802.1p Priority
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	1
AF1	yellow	1
AF1	red	1
AF2	green	2
AF2	yellow	2
AF2	red	2
AF3	green	3
AF3	yellow	3
AF3	red	3
AF4	green	4
AF4	yellow	4
AF4	red	4
EF	green	5
EF	yellow	5
EF	red	5
CS6	green	6
CS6	yellow	6
CS6	red	6
CS7	green	7
CS7	yellow	7
CS7	red	7

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

8021p-outbound *service-class* { **green** | **yellow** | **red** } **map** *8021p-value*

undo 8021p-outbound [*service-class* { **green** | **yellow** | **red** }]

Parameters

Parameter	Description	Value
service-class	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7, each of which corresponds to queues 0 to 7 respectively.
green	Indicates that packets are colored green.	-
yellow	Indicates that packets are colored yellow.	-
red	Indicates that packets are colored red.	-
map *8021p-value*	Specifies the 802.1p priority of VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

Scenario

After QoS scheduling is performed on VLAN packets, you can use the **8021p-outbound** command to map the PHB and color of the packets in a DiffServ domain to the 802.1p priority. After the DiffServ domain is bound to the outbound interface of the VLAN packets, the downstream device implements QoS scheduling according to the 802.1p priority.

Precautions

If you do not specify the parameters *service-class* and *color* when running the **undo 8021p-outbound** command, the default mappings from CoS values and colors to 802.1p priorities are restored.

Example

# In DiffServ domain **ds1**, map PHB AF1 of the outbound yellow VLAN packets to 802.1p priority 2.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] 8021p-outbound af1 yellow map 2
```

Related Topics

15.2.2 8021p-inbound

15.2.4 dei enable

Function

The **dei enable** command maps the drop eligible indicator (DEI) field in a VLAN tag to the drop priority.

The **undo dei enable** command cancels the configuration of the DEI field in a VLAN tag as the drop priority.

By default, the DEI field in a VLAN tag is not used as the drop priority.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

dei enable

undo dei enable

Parameters

None

Views

GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

The DEI is also called the Canonical Format Indicator (CFI) field in a VLAN tag and its value is 0 or 1. The DEI field in a VLAN tag is used as the drop priority of packets in certain situations. When the rate of packets on certain devices exceeds the CIR value, the DEI field is set to 1. In this case, the drop priority of the packets is high. When congestion occurs, subsequent devices first discard the packets whose DEI field is 1.

Precautions

After the **dei enable** command is run, the DEI field in the VLAN tag is mapped to the drop priority:

- The DEI field in the VLAN tag is mapped to the drop priority (packet color) on the inbound interface as follows:
  - When the DEI field is 0, packets are colored green.
  - When the DEI field is 1, packets are colored yellow.
- The drop priority is mapped to the DEI field on the outbound interface as follows:
  - Green and yellow packets correspond to DEI 0.
  - Red packets correspond to DEI 1.

To configure the DEI field in a VLAN tag as the drop priority on multiple interfaces, perform the configuration on a port group to reduce the workload.

Example

# Configure the DEI field in the VLAN tag as the drop priority on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dei enable
```

15.2.5 diffserv domain

Function

The **diffserv domain** command creates a DiffServ domain and displays the DiffServ domain view, or displays an existing DiffServ domain view.

The **undo diffserv domain** command deletes a specified DiffServ domain.

By default, the system defines a DiffServ mode named **default**.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

diffserv domain { **default** | *ds-domain-name* }

undo diffserv domain *ds-domain-name*

Parameters

Parameter	Description	Value
default	Indicates the default DiffServ domain preset in the system.	-
ds-domain-name	Specifies the name of a DiffServ domain.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The value cannot be n, no, non, or none. **NOTE** The value cannot be --.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

A DiffServ domain defines the mapping between the packet priority and PHB/ colors packets for managing and avoiding congestion. You can run the **display diffserv domain** command to view the mappings and packet colors defined in the DiffServ domain.

A DiffServ domain defines the mapping between the PHBs/colors and packet priorities (802.1p and DSCP). When binding a DiffServ domain to an interface, you can run the **trust** command to configure 802.1p or DSCP priority mapping on the interface.

Precautions

The DiffServ domain **default** exists by default. In addition to this domain, the device allows a maximum of 7 DiffServ domains. You can only change the mapping for the DiffServ domain **default**, but cannot delete the domain.

Example

# Create DiffServ domain **d1** and display the corresponding DiffServ domain view.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain d1
[HUAWEI-dsdomain-d1]
```

Related Topics

15.2.6 display diffserv domain

15.2.23 trust

15.2.6 display diffserv domain

Function

The **display diffserv domain** command displays the DiffServ domain configuration.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

display diffserv domain [**all** | **name** *ds-domain-name*]

Parameters

Parameter	Description	Value
all	Displays configurations of all DiffServ domains.	-
name *ds-domain-name*	Displays the detailed configuration of a specified DiffServ domain.	The value must the name of an existing DiffServ domain.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Scenario

After creating a DiffServ domain and configuring the mappings in the DiffServ domain, you can use the **display diffserv domain** command to view the configuration of the DiffServ domain.

If no optional parameter is specified, this command displays configurations of all DiffServ domains on the device.

Example

# Display the configuration of DiffServ domain **d1**(S5720HI).

```
<HUAWEI> display diffserv domain name d1
diffserv domain name:d1
 8021p-inbound 0 phb be green
 8021p-inbound 1 phb af1 green
 8021p-inbound 2 phb af2 green
 8021p-inbound 3 phb af3 green
 8021p-inbound 4 phb af4 green
 8021p-inbound 5 phb ef green
 8021p-inbound 6 phb cs6 green
 8021p-inbound 7 phb cs7 green
 8021p-outbound be green map 0
 8021p-outbound be yellow map 0
 8021p-outbound be red map 0
 8021p-outbound af1 green map 1
 8021p-outbound af1 yellow map 1
 8021p-outbound af1 red map 1
 8021p-outbound af2 green map 2
 8021p-outbound af2 yellow map 2
 8021p-outbound af2 red map 2
 8021p-outbound af3 green map 3
 8021p-outbound af3 yellow map 3
 8021p-outbound af3 red map 3
 8021p-outbound af4 green map 4
 8021p-outbound af4 yellow map 4
 8021p-outbound af4 red map 4
 8021p-outbound ef green map 5
 8021p-outbound ef yellow map 5
 8021p-outbound ef red map 5
 8021p-outbound cs6 green map 6
 8021p-outbound cs6 yellow map 6
 8021p-outbound cs6 red map 6
 8021p-outbound cs7 green map 7
 8021p-outbound cs7 yellow map 7
 8021p-outbound cs7 red map 7
 ip-dscp-inbound 0 phb be green
 ip-dscp-inbound 1 phb be green
 ip-dscp-inbound 2 phb be green
 ip-dscp-inbound 3 phb be green
 ip-dscp-inbound 4 phb be green
 ip-dscp-inbound 5 phb be green
 ip-dscp-inbound 6 phb be green
 ip-dscp-inbound 7 phb be green
 ip-dscp-inbound 8 phb af1 green
 ip-dscp-inbound 9 phb be green
 ip-dscp-inbound 10 phb af1 green
 ip-dscp-inbound 11 phb be green
 ip-dscp-inbound 12 phb af1 yellow
 ip-dscp-inbound 13 phb be green
 ip-dscp-inbound 14 phb af1 red
 ip-dscp-inbound 15 phb be green
 ip-dscp-inbound 16 phb af2 green
 ip-dscp-inbound 17 phb be green
 ip-dscp-inbound 18 phb af2 green
 ip-dscp-inbound 19 phb be green
 ip-dscp-inbound 20 phb af2 yellow
 ip-dscp-inbound 21 phb be green
 ip-dscp-inbound 22 phb af2 red
 ip-dscp-inbound 23 phb be green
 ip-dscp-inbound 24 phb af3 green
 ip-dscp-inbound 25 phb be green
 ip-dscp-inbound 26 phb af3 green
```

```
ip-dscp-inbound 27 phb be green
ip-dscp-inbound 28 phb af3 yellow
ip-dscp-inbound 29 phb be green
ip-dscp-inbound 30 phb af3 red
ip-dscp-inbound 31 phb be green
ip-dscp-inbound 32 phb af4 green
ip-dscp-inbound 33 phb be green
ip-dscp-inbound 34 phb af4 green
ip-dscp-inbound 35 phb be green
ip-dscp-inbound 36 phb af4 yellow
ip-dscp-inbound 37 phb be green
ip-dscp-inbound 38 phb af4 red
ip-dscp-inbound 39 phb be green
ip-dscp-inbound 40 phb ef green
ip-dscp-inbound 41 phb be green
ip-dscp-inbound 42 phb be green
ip-dscp-inbound 43 phb be green
ip-dscp-inbound 44 phb be green
ip-dscp-inbound 45 phb be green
ip-dscp-inbound 46 phb ef green
ip-dscp-inbound 47 phb be green
ip-dscp-inbound 48 phb cs6 green
ip-dscp-inbound 49 phb be green
ip-dscp-inbound 50 phb be green
ip-dscp-inbound 51 phb be green
ip-dscp-inbound 52 phb be green
ip-dscp-inbound 53 phb be green
ip-dscp-inbound 54 phb be green
ip-dscp-inbound 55 phb be green
ip-dscp-inbound 56 phb cs7 green
ip-dscp-inbound 57 phb be green
ip-dscp-inbound 58 phb be green
ip-dscp-inbound 59 phb be green
ip-dscp-inbound 60 phb be green
ip-dscp-inbound 61 phb be green
ip-dscp-inbound 62 phb be green
ip-dscp-inbound 63 phb be green
ip-dscp-outbound be green map 0
ip-dscp-outbound be yellow map 0
ip-dscp-outbound be red map 0
ip-dscp-outbound af1 green map 10
ip-dscp-outbound af1 yellow map 12
ip-dscp-outbound af1 red map 14
ip-dscp-outbound af2 green map 18
ip-dscp-outbound af2 yellow map 20
ip-dscp-outbound af2 red map 22
ip-dscp-outbound af3 green map 26
ip-dscp-outbound af3 yellow map 28
ip-dscp-outbound af3 red map 30
ip-dscp-outbound af4 green map 34
ip-dscp-outbound af4 yellow map 36
ip-dscp-outbound af4 red map 38
ip-dscp-outbound ef green map 46
ip-dscp-outbound ef yellow map 46
ip-dscp-outbound ef red map 46
ip-dscp-outbound cs6 green map 48
ip-dscp-outbound cs6 yellow map 48
ip-dscp-outbound cs6 red map 48
ip-dscp-outbound cs7 green map 56
ip-dscp-outbound cs7 yellow map 56
ip-dscp-outbound cs7 red map 56
mpls-exp-inbound 0 phb be green
mpls-exp-inbound 1 phb af1 green
mpls-exp-inbound 2 phb af2 green
mpls-exp-inbound 3 phb af3 green
mpls-exp-inbound 4 phb af4 green
mpls-exp-inbound 5 phb ef green
mpls-exp-inbound 6 phb cs6 green
mpls-exp-inbound 7 phb cs7 green
```

```
mpls-exp-outbound be green map 0
mpls-exp-outbound be yellow map 0
mpls-exp-outbound be red map 0
mpls-exp-outbound af1 green map 1
mpls-exp-outbound af1 yellow map 1
mpls-exp-outbound af1 red map 1
mpls-exp-outbound af2 green map 2
mpls-exp-outbound af2 yellow map 2
mpls-exp-outbound af2 red map 2
mpls-exp-outbound af3 green map 3
mpls-exp-outbound af3 yellow map 3
mpls-exp-outbound af3 red map 3
mpls-exp-outbound af4 green map 4
mpls-exp-outbound af4 yellow map 4
mpls-exp-outbound af4 red map 4
mpls-exp-outbound ef green map 5
mpls-exp-outbound ef yellow map 5
mpls-exp-outbound ef red map 5
mpls-exp-outbound cs6 green map 6
mpls-exp-outbound cs6 yellow map 6
mpls-exp-outbound cs6 red map 6
mpls-exp-outbound cs7 green map 7
mpls-exp-outbound cs7 yellow map 7
mpls-exp-outbound cs7 red map 7
```

Table 15-13 Description of the **display diffserv domain name d1** command output

Item	Description
diffserv domain name	Name of the DiffServ domain. To create a DiffServ domain, run the **diffserv domain** command.
8021p-inbound	Mapping from the 802.1p priority of incoming VLAN packets in a DiffServ domain to the PHB and color. To configure the mapping, run the **8021p-inbound** command.
8021p-outbound	Mapping from the PHB and color of outgoing VLAN packets in a DiffServ domain to the 802.1p priority. To configure the mapping, run the **8021p-outbound** command.
ip-dscp-inbound	Mapping from the DSCP priority of incoming IP packets in a DiffServ domain to the PHB and color. To configure the mapping, run the **ip-dscp-inbound** command.
ip-dscp-outbound	Mapping from the PHB and color of outgoing IP packets in a DiffServ domain to the DSCP priority. To configure the mapping, run the **ip-dscp-outbound** command.
mpls-exp-inbound	Mapping from the EXP priority of incoming MPLS packets in a DiffServ domain to the PHB and color. To configure the mapping, run the **mpls-exp-inbound** command.
mpls-exp-outbound	Mapping from the PHB and color of outgoing MPLS packets in a DiffServ domain to the PHB and color. To configure the mapping, run the **mpls-exp-outbound** command.

# Display configurations of all DiffServ domains on the device.

```
<HUAWEI> display diffserv domain
  index      DS name
```

```
--------------------------------------
   0        default
   1        ds1
   2        ds2
--------------------------------------
Total 8, Used 3
```

Table 15-14 Description of the **display diffserv domain** command output

Item	Description
index	Index of the DiffServ domain.
DS name	Name of the DiffServ domain. To create a DiffServ domain, run the **diffserv domain** command.
Total	Total number of DiffServ domains supported by the device.
Used	Number of created DiffServ domains on the device.

Related Topics

15.2.5 diffserv domain

15.2.7 display qos local-precedence-queue-map

Function

The **display qos local-precedence-queue-map** command displays the mapping between local precedences and queues.

Format

display qos local-precedence-queue-map

NOTE

The S5720HI does not support this command.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **qos local-precedence-queue-map** command, you can configure the mapping between local precedence values and queues. Then you can run the **display qos local-precedence-queue-map** command to display the configuration.

Example

# Display the mapping between local precedences and queues.

```
<HUAWEI> system-view
[HUAWEI] qos local-precedence-queue-map af3 2
[HUAWEI] display qos local-precedence-queue-map
 Current configurations of mapping between local-precedence and queue:
  local-precedence value: be     queue index: 0
  local-precedence value: af1    queue index: 1
  local-precedence value: af2    queue index: 2
  local-precedence value: af3    queue index: 2
  local-precedence value: af4    queue index: 4
  local-precedence value: ef     queue index: 5
  local-precedence value: cs6    queue index: 6
  local-precedence value: cs7    queue index: 7
```

Table 15-15 Description of the **display qos local-precedence-queue-map** command output

Item	Description
local-precedence value	Local priority.
queue index	Queue index mapping the local priority. To configure the mapping between local priorities and queues, run the **qos local-precedence-queue-map** command.

Related Topics

15.2.14 qos local-precedence-queue-map

15.2.8 display qos map-table

Function

The **display qos map-table** command displays the mapping between priorities.

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this command.

Format

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

NOTE

Only the S1720GFR, S2750EI, S5700LI, and S5700S-LI support the **ip-pre-dot1p** and **ip-pre-ip-pre** parameters.

Parameters

Parameter	Description	Value
dscp-dot1p	Specifies the name of the mapping table. That is, the mapping from DSCP priorities to 802.1p priorities.	-
dscp-dp	Specifies the name of the mapping table. That is, the mapping between the DSCP priority and the drop precedence is displayed.	-
dscp-dscp	Specifies the name of the mapping table. That is, the mapping between DSCP priorities.	-
ip-pre-dot1p	Specifies the name of the mapping table. That is, the mapping between the IP precedence and the 802.1p priority is displayed.	-
ip-pre-ip-pre	Specifies the name of the mapping table. That is, the mapping between the IP precedence and the IP precedence is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before and after configuring the mapping between priorities, you can use the **display qos map-table** command to check whether the priority mapping is correct.

If DSCP priority mapping is configured, the command displays only the DSCP priority mapping. If IP priority mapping is configured, the command displays only the IP priority mapping. If DSCP and IP priority mappings are not configured, the command displays the default settings of DSCP and IP priority mappings.

Example

# Display the mapping between the current DSCP priorities and Dot1p priorities.

```
<HUAWEI> display qos map-table dscp-dot1p
Input DSCP       Dot1P
------------------------
0               0
1               0
2               0
3               0
4               0
5               0
6               0
7               0
......
```

# Display all the mappings between the current priorities.

```
<HUAWEI> display qos map-table
Input DSCP       Dot1P   DP     DSCP
----------------------------------------
0              0      0      0
1              0      0      1
2              0      0      2
3              0      0      3
4              0      0      4
5              0      0      5
6              0      0      6
7              0      0      7
......

Input IP precedence      Dot1P   IP precedence
------------------------------------------------
0                     0      0
1                     1      1
2                     2      2
3                     3      3
4                     4      4
5                     5      5
6                     6      6
7                     7      7
```

Table 15-16 Description of the **display qos map-table** command output

Item	Description
Input DSCP	Input DSCP priority. The value is an integer that ranges from 0 to 63. To set the input DSCP priority, run the **input (DSCP mapping table view)** command.

Item	Description
Dot1P	Output 802.1p priority. The value is an integer that ranges from 0 to 7. To set the output 802.1p priority, run the **input (DSCP mapping table view)** and **input (IP precedence mapping table view)** commands.
DP	Output drop priority that corresponds to a color. The value is 0, 1, or 2. ● 0: green ● 1: yellow ● 2: red To set the output drop priority, run the **input (DSCP mapping table view)** command.
DSCP	Output DSCP priority. The value is an integer that ranges from 0 to 63. To set the output DSCP priority, run the **input (DSCP mapping table view)** command.
Input IP precedence	Input IP precedence. The value is an integer that ranges from 0 to 7. To set the input IP precedence, run the **input (IP precedence mapping table view)** command.
IP precedence	Output IP precedence. The value is an integer that ranges from 0 to 7. To set the output IP precedence, run the **input (IP precedence mapping table view)** command.

NOTE

A larger value indicates a higher priority.

Related Topics

15.2.9 input (DSCP mapping table view)

15.2.10 input (IP precedence mapping table view)

15.2.15 qos map-table

15.2.9 input (DSCP mapping table view)

Function

The **input** command sets the mapping in a DSCP mapping table.

The **undo input** command restores the default mapping in a DSCP mapping table.

Table 15-17 lists the default mapping from DSCP priorities to 802.1p priorities and from DSCP priorities to drop priorities. The default mapping from DSCP priorities to DSCP priorities remains unchanged.

Table 15-17 Default mapping from DSCP priorities to 802.1p priorities and from DSCP priorities to drop priorities

Input DSCP	Output Dot1p	Output DP
0-7	0	0
8-15	1	0
16-23	2	0
24-31	3	0
32-39	4	0
40-47	5	0
48-55	6	0
56-63	7	0

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this command.

Format

input { *input-value1* [**to** *input-value2*] } &<1-10> **output** *output-value*

undo input { **all** | { *input-value1* [**to** *input-value2*] } &<1-10> }

Parameters

Parameter	Description	Value
input-value1	Specifies the start DSCP priority that is entered.	The value is an integer that ranges from 0 to 63. A greater value indicates a higher priority.
to *input-value2*	Specifies the end DSCP priority that is entered.	The value is an integer that ranges from 0 to 63. A greater value indicates a higher priority. The value of *input-value2* must be greater than the value of *input-value1* and the two values determine the DSCP range.

Parameter	Description	Value
output *output-value*	Specifies the output 802.1p priority, output drop precedence, or output DSCP value.	The current mapping table view determines the value of **output-value**. The value ranges are as follows: The value ranges from 0 to 7 in the dscp-dot1p view. The value ranges from 0 to 2 in the dscp-dp view. ● The drop priority 0 corresponds to green packets. ● The drop priority 1 corresponds to yellow packets. ● The drop priority 2 corresponds to red packets. The value ranges from 0 to 63 in the dscp-dscp view. A greater value indicates a higher priority.
all	Indicates all mappings in the DSCP mapping table.	-

Views

DSCP mapping table view

Default Level

2: Configuration level

Usage Guidelines

You must run the **qos map-table** command to enter the corresponding DSCP mapping table view before running the **input** command.

The **input** command modifies the mapping from DSCP priorities to Dot1p priorities, from DSCP priorities to drop priorities, and from DSCP priorities to DSCP priorities in the DSCP table.

After running the **input** command, you can run the **display qos map-table** command to view the current DSCP mapping.

Example

# Set the mapping in the DSCP mapping table: Level 0 to level 7 in the DSCP mapping table are mapped to level 0 of 802.1p priority.

```
<HUAWEI> system-view
[HUAWEI] qos map-table dscp-dot1p
[HUAWEI-dscp-dot1p] input 0 to 7 output 0
```

Related Topics

15.2.8 display qos map-table

15.2.15 qos map-table

15.2.10 input (IP precedence mapping table view)

Function

The **input** command sets the mapping in the IP precedence table.

The **undo input** command restores the default mapping in the IP precedence table.

Table 15-18 lists the default mapping from IP precedences to Dot1p priorities and from IP preferences to IP preferences.

Table 15-18 Default mapping from IP precedences to 802.1p priorities and from IP precedences to IP precedences

Input IP precedence	Dot1p	IP precedence
0	0	0
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

NOTE

Only the S1720GFR, S2750EI, S5700LI, and S5700S-LI support this command.

Format

input *input-value1* [**to** *input-value2*] **output** *output-value*

undo input { **all** | *input-value1* [**to** *input-value2*] }

Parameters

Parameter	Description	Value
input-value1	Specifies the start IP precedence that is entered.	The value is an integer that ranges from 0 to 7. A greater value indicates a higher priority.
to *input-value2*	Specifies the end IP precedence that is entered.	The value is an integer that ranges from 0 to 7. A greater value indicates a higher priority. The value of *input-value2* must be greater than the value of *input-value1* and the two values determine the IP precedence range.
output *output-value*	Specifies the output 802.1p priority or output IP precedence.	The value is an integer that ranges from 0 to 7. A greater value indicates a higher priority.
all	Indicates all mappings in the IP precedence table.	-

Views

IP precedence mapping table view

Default Level

2: Configuration level

Usage Guidelines

You must run the **qos map-table** command to enter the corresponding IP precedence mapping table view before running the **input** command.

The **input** command modifies the mapping from IP precedences to Dot1p priorities and from IP preferences to IP preferences in the IP precedence table.

After running the **input** command in the IP precedence mapping table view, you can run the **display qos map-table** command to view the current IP precedence mapping.

Example

# Set the mapping in the IP precedence table: Level 0 to level 7 in the IP precedence table are mapped to level 0 of 802.1p.

```
<HUAWEI> system-view
[HUAWEI] qos map-table ip-pre-dot1p
[HUAWEI-ip-pre-dot1p] input 0 to 7 output 0
```

Related Topics

15.2.8 display qos map-table

15.2.15 qos map-table

15.2.11 ip-dscp-inbound

Function

The **ip-dscp-inbound** command maps the DSCP priority of incoming IP packets in a DiffServ domain to the PHB and colors the packets.

The **undo ip-dscp-inbound** command restores the default mapping.

Table 15-19 lists the default mappings from the DSCP priorities to PHBs and colors of incoming IP packets in a DiffServ domain.

Table 15-19 Mappings from DSCP priorities to PHBs and colors of incoming IP packets in the DiffServ domain

DSCP	PHB	Color	DSCP	PHB	Color
0	BE	green	32	AF4	green
1	BE	green	33	BE	green
2	BE	green	34	AF4	green
3	BE	green	35	BE	green
4	BE	green	36	AF4	yellow
5	BE	green	37	BE	green
6	BE	green	38	AF4	red
7	BE	green	39	BE	green
8	AF1	green	40	EF	green
9	BE	green	41	BE	green
10	AF1	green	42	BE	green
11	BE	green	43	BE	green
12	AF1	yellow	44	BE	green
13	BE	green	45	BE	green
14	AF1	red	46	EF	green
15	BE	green	47	BE	green
16	AF2	green	48	CS6	green

DSCP	PHB	Color	DSCP	PHB	Color
17	BE	green	49	BE	green
18	AF2	green	50	BE	green
19	BE	green	51	BE	green
20	AF2	yellow	52	BE	green
21	BE	green	53	BE	green
22	AF2	red	54	BE	green
23	BE	green	55	BE	green
24	AF3	green	56	CS7	green
25	BE	green	57	BE	green
26	AF3	green	58	BE	green
27	BE	green	59	BE	green
28	AF3	yellow	60	BE	green
29	BE	green	61	BE	green
30	AF3	red	62	BE	green
31	BE	green	63	BE	green

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

ip-dscp-inbound *dscp-value* **phb** *service-class* [**green** | **yellow** | **red**]

undo ip-dscp-inbound [*dscp-value*]

Parameters

Parameter	Description	Value
dscp-value	Specifies the DSCP priority of IP packets.	The value is an integer that ranges from 0 to 63.
phb *service-class*	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7, each of which corresponds to queues 0 to 7 respectively.

Parameter	Description	Value
green	Indicates that packets are colored green.	-
yellow	Indicates that packets are colored yellow.	-
red	Indicates that packets are colored red.	-

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

Scenario

To implement QoS scheduling for incoming IP packets carrying DSCP priorities, use the **ip-dscp-inbound** command to configure mappings from DSCP priorities of packets to PHBs and color the packets. After a DiffServ domain is bound to the inbound interface of packets, the device forwards the packets to queues based on PHBs of the packets. Congestion management is implemented. Packets are scheduled according to their colors after a discard template is configured, avoiding congestion.

Precautions

- The color is used to determine whether packets are discarded during flow control, and is independent of the mapping from internal priorities to queues.
- The CoS values of packets are mapped to the corresponding internal priorities and the packets are colored accordingly. If no mapping from DSCP priorities to CoS values is specified, the device uses the default mappings of the system.
- If you do not specify the parameter *dscp-value* when running the **undo ip-dscp-inbound** command, all mappings from DSCP priorities to CoS values is restored.

Example

# In DiffServ domain **ds1**, map DSCP priority 8 of the incoming IP packets to PHB AF1 and mark the packets yellow.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] ip-dscp-inbound 8 phb af1 yellow
```

Related Topics

15.2.12 ip-dscp-outbound

15.2.12 ip-dscp-outbound

Function

The **ip-dscp-outbound** command maps the PHB and color of outgoing IP packets in a DiffServ domain to the DSCP priority.

The **undo ip-dscp-outbound** command restores the default mapping.

Table 15-20 lists the default mappings from the PHBs and colors to DSCP priorities of outgoing IP packets in a DiffServ domain.

Table 15-20 Mappings from PHBs and colors to DSCP priorities of outgoing IP packets in the DiffServ domain

PHB	Color	DSCP
BE	green	0
BE	yellow	0
BE	red	0
AF1	green	10
AF1	yellow	12
AF1	red	14
AF2	green	18
AF2	yellow	20
AF2	red	22
AF3	green	26
AF3	yellow	28
AF3	red	30
AF4	green	34
AF4	yellow	36
AF4	red	38
EF	green	46
EF	yellow	46
EF	red	46
CS6	green	48
CS6	yellow	48
CS6	red	48

PHB	Color	DSCP
CS7	green	56
CS7	yellow	56
CS7	red	56

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

ip-dscp-outbound *service-class* { **green** | **yellow** | **red** } **map** *dscp-value*

undo ip-dscp-outbound [*service-class* { **green** | **yellow** | **red** }]

Parameters

Parameter	Description	Value
service-class	Specifies a PHB.	The value can be BE, AF1 to AF4, EF, CS6, or CS7, each of which corresponds to queues 0 to 7 respectively.
green	Indicates that packets are colored green.	-
yellow	Indicates that packets are colored yellow.	-
red	Indicates that packets are colored red.	-
map *dscp-value*	Specifies the DSCP priority of IP packets.	The value is an integer that ranges from 0 to 63.

Views

DiffServ domain view

Default Level

2: Configuration level

Usage Guidelines

Scenario

After QoS scheduling is performed on the IP packets, you can use the **ip-dscp-outbound** command to map the PHB and color of IP packets in a DiffServ domain to the DSCP priority. After the DiffServ domain is bound to the outbound interface of the IP packets, the downstream device implements QoS scheduling according to the DSCP priority.

Precautions

If you do not specify the parameters *service-class* and colors when running the **undo ip-dscp-outbound** command, the default mappings from CoS values and colors to DSCP priorities are restored.

Example

# In DiffServ domain **ds1**, map PHB AF1 of the outbound yellow IP packets to DSCP priority 8.

```
<HUAWEI> system-view
[HUAWEI] diffserv domain ds1
[HUAWEI-dsdomain-ds1] ip-dscp-outbound af1 yellow map 8
```

Related Topics

15.2.11 ip-dscp-inbound

15.2.13 port priority

Function

The **port priority** command configures the priority for an interface.

The **undo port priority** command restores the default priority of an interface.

By default, the priority of an interface is 0.

Format

port priority *priority-value*

undo port priority

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of an interface.	The value is an integer that ranges from 0 to 7. The default value is 0. A larger value indicates a higher priority of an interface.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

The 802.1p priority is determined by the 3-bit priority 802.1p field contained in a VLAN tag. The 802.1p priority is used to ensure QoS in the DiffServ model.

If an interface receives untagged packets, the interface priority is added to packets during the internal forwarding.

If an interface is configured to trust the 802.1p priority using the **trust 8021p** command, the interface adds the 802.1p priority to the received untagged packets. The device then searches for the internal priority (represented by a PHB and color) mapping the 802.1p priority and marks packets with the internal priority.

Precautions

- The **port priority** command is invalid if the current interface is a member interface of an Eth-Trunk.
- By default, the S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI do not trust any packet priorities. If the priority trusted by the device is not changed using the **trust** command, incoming packets on the interface where the priority is configured enter queues based on the configured priority. The 802.1p priority of packets forwarded by the interface is also changed to the priority of the interface.
- If you run the **port priority** command multiple times in the same interface view, only the latest configuration takes effect.
- When an interface switches to Layer 3 mode through the **undo portswitch** command, you cannot configure a priority for the Ethernet interface. This Ethernet interface uses priority 0.

Example

# Set the priority of GE0/0/1 to 1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port priority 1
```

Related Topics

15.2.23 trust

15.2.24 trust upstream

15.2.14 qos local-precedence-queue-map

Function

The **qos local-precedence-queue-map** command configures default mappings from local precedences to queues.

The **undo qos local-precedence-queue-map** command restores the default mapping from local precedences to queues.

Table 15-21 lists the default mappings from local priorities to queues.

Table 15-21 Mapping between local priorities and queues

Local Priority	Queue Index
BE	0
AF1	1
AF2	2
AF3	3
AF4	4
EF	5
CS6	6
CS7	7

Format

qos local-precedence-queue-map *local-precedence queue-index*

undo qos local-precedence-queue-map [*local-precedence*]

NOTE

The S5720HI does not support the mapping configuration between local priorities and queues.

Parameters

Parameter	Description	Value
local-precedence	Specifies the name of the local precedence.	The value can be **af1**, **af2**, **af3**, **af4**, **be**, **cs6**, **cs7**, or **ef**.
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

The device sends packets to the specified queue according to the mapping from local precedences to queues.

To make traffic across the entire network achieve consistent QoS, ensure that all the stations keep consistent mapping from local precedences to queues.

Precautions

If you run the **qos local-precedence-queue-map** command multiple times in the system view, only the latest configuration takes effect.

Example

# Map packets with local precedence AF3 to queue 2.

```
<HUAWEI> system-view
[HUAWEI] qos local-precedence-queue-map af3 2
```

Related Topics

15.2.7 display qos local-precedence-queue-map

15.2.17 remark 8021p

15.2.22 remark local-precedence

15.2.15 qos map-table

Function

The **qos map-table** command displays the DSCP or IP priority mapping table view.

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this command.

Format

qos map-table { **dscp-dot1p** | **dscp-dp** | **dscp-dscp** | **ip-pre-dot1p** | **ip-pre-ip-pre** }

NOTE

Only the S1720GFR, S2750EI, S5700LI, and S5700S-LI support the **ip-pre-dot1p** and **ip-pre-ip-pre** parameters.

Parameters

Parameter	Description	Value
dscp-dot1p	Displays the dscp-dot1p view. The dscp-dot1p table contains the mapping between DSCP priorities and 802.1p priorities.	-
dscp-dp	Displays the dscp-dp view. The dscp-dp table contains the mapping between DSCP priorities and drop precedences.	-
dscp-dscp	Displays the dscp-dscp view. The dscp-dscp table contains the mapping between DSCP priorities and DSCP priorities.	-
ip-pre-dot1p	Displays the ip-pre-dot1p view. The ip-pre-dot1p table contains the mapping between IP precedences and 802.1p priorities.	-
ip-pre-ip-pre	Enters the ip-pre-ip-pre view. The ip-pre-ip-pre table contains the mapping between IP precedences and IP precedences.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before mapping received packets based on the DSCP priority or IP precedence, run the **qos map-table** command to enter the priority mapping table view.

Precautions

On the S1720GFR, S2750EI, S5700LI, and S5700S-LI, the DSCP priority mapping and IP priority mapping cannot be used together.

- When you configure DSCP priority mapping on the device where IP priority mapping has been configured, the system displays the message "Error: Configuration conflicts with IP precedence map-table."
- When you configure IP priority mapping on the device where DSCP priority mapping has been configured, the system displays the message "Error: Configuration conflicts with DSCP map-table."
- In a version earlier than V200R007C00, DSCP priority mapping and IP priority mapping can be configured simultaneously. When the system software is upgraded to V200R007C00 or a later version, both DSCP priority mapping and IP priority mapping can be restored, but only the DSCP priority mapping table takes effect. To modify the DSCP priority mapping table, run the **undo input** command in the IP priority mapping table view to delete the IP priority mapping table configuration first. To modify the IP priority mapping table, run the **undo input** command in the DSCP priority mapping table view to delete the DSCP priority mapping table configuration first.

Follow-up Procedure

Run the **input (DSCP priority mapping table view)** or **input (IP precedence mapping table view)** command to configure the mapping.

Example

# Enter the dscp-dot1p view.

```
<HUAWEI> system-view
[HUAWEI] qos map-table dscp-dot1p
[HUAWEI-dscp-dot1p]
```

Related Topics

15.2.8 display qos map-table

15.2.10 input (IP precedence mapping table view)

15.2.9 input (DSCP mapping table view)

15.2.23 trust

15.2.16 qos phb marking enable

Function

The **qos phb marking enable** command enables PHB mapping for outgoing packets on an interface.

The **undo qos phb marking enable** command disables PHB mapping for outgoing packets on an interface.

By default, PHB mapping is enabled for outgoing packets on an interface.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

qos phb marking enable

undo qos phb marking enable

Parameters

None

Views

GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

After the **undo qos phb marking enable** command is executed on the interface of the edge node in a DiffServ domain, PHB mapping is disabled on the interface connected to a device that does not belong to the DiffServ domain.

Precautions

- The **trust upstream none** command is executed to disable PHB mapping on an interface. After the **trust upstream none** command is executed, the system does not perform PHB mapping for incoming and outgoing packets on the interface. Unlike the **trust upstream none** command, after the **undo qos phb marking enable** command is executed, the system does not perform PHB mapping for outgoing packets on the interface but performs PHB mapping for incoming packets on the interface.
- The **undo qos phb marking enable** and **trust upstream none** commands cannot be executed simultaneously.

Example

# Disable PHB mapping for outgoing packets on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo qos phb marking enable
```

Related Topics

15.2.24 trust upstream

15.2.17 remark 8021p

Function

The **remark 8021p** command configures an action of re-marking the 802.1p priority in VLAN packets in a traffic behavior.

The **undo remark 8021p** command deletes the configuration.

By default, an action of re-marking the 802.1p priority in VLAN packets is not configured in a traffic behavior.

Format

remark 8021p [*8021p-value* | **inner-8021p**]

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support the **inner-8021p** parameter.

undo remark 8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority in VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority in VLAN packets. If the value is not specified, the default value 0 is used.
inner-8021p	Inherits the 802.1p priority in the inner tag.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide differentiated services based on the inner 802.1p priority in VLAN packets, run the **remark 8021p** command to configure the device to re-mark the inner 802.1p priority in VLAN packets in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing 802.1p priority re-marking.

Precautions

If a traffic policy containing **remark 8021p** is applied to the outbound direction on an interface, the device still processes outgoing packets based on the original priority but the downstream Layer 2 device processes the packets based on the re-marked priority.

A traffic policy containing the **remark 8021p inner-8021p** action can only be used in the inbound direction. For the S5720-EI, S6720-EI, or S6720S-EI, if a traffic policy contains **remark 8021p inner-8021p**, the PRI field (802.1p priority) in single-tagged packets is changed to 0. In this case, you can configure **if-match double-tag** in a traffic classifier to change the 802.1p priority only of double-tagged packets.

If a traffic policy containing **remark 8021p** is applied to the outbound direction on an interface, the VLAN of the interface must work in tag mode.

When a traffic classifier defines **if-match** **ipv6 acl** { *acl-number* | *acl-name* }, **remark 8021p** [*8021p-value* | **inner-8021p**] cannot be configured on the S5720HI.

After the **remark 8021p**, **add-tag vlan-id**, **remark cvlan-id** or **remark vlan-id** command is used, the system modifies the VLAN tag of packets according to its configuration. A behavior configured through one of these commands is called VLAN-based action.

You must configure the VLAN-based action and non-VLAN-based action in different traffic behaviors bound to the same traffic policy.

If both the **trust 8021p** command and the traffic policy containing **remark 8021p** are used in the outbound direction on the interface of packets, the 802.1p priority specified by the **trust 8021p** command is the re-marked value. This is because the **remark 8021p** command takes precedence over the **trust 8021p** command.

The S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI do not trust any packet priorities by default. After packets enter the device, the device changes 802.1p priorities in packets to 0. If the traffic policy containing **if-match 8021p** and **remark 8021p** is configured, original 802.1p priorities in packets are not matched. As a result, the traffic policy does not take effect. Therefore, you need to configure the device to trust priorities of packets.

The **remark 8021p** and **remark local-precedence** commands cannot be used in the same traffic behavior.

If you run the **remark 8021p** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

# Re-mark 802.1p priorities of VLAN packets with 4 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark 8021p 4
```

Related Topics

15.1.11 if-match 8021p

15.2.22 remark local-precedence

5.9.6 remark vlan-id

15.1.31 traffic behavior

15.2.23 trust

15.2.18 remark 8021p (QoS profile view)

Function

The **remark 8021p** command configures the device to re-mark 802.1p priorities in VLAN packets in a QoS profile.

The **undo remark 8021p** command cancels the configuration.

By default, the device does not re-mark 802.1p priorities in VLAN packets in a QoS profile.

NOTE

Only the S5720HI supports this command.

Format

remark 8021p *8021p-value*

undo remark 8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority in a VLAN packet.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device needs to provide differentiated services based on 802.1p priorities in VLAN packets, run the **remark 8021p** command to configure the device to re-mark 802.1p priorities in VLAN packets in a QoS profile.

Precautions

If you run the **remark 8021p** command in the same QoS profile view multiple times, only the latest configuration takes effect.

Example

# Configure the device to re-mark 802.1p priorities in VLAN packets with 4 in the QoS profile **huawei**.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name huawei
[HUAWEI-qos-huawei] remark 8021p 4
```

15.2.19 remark dscp

Function

The **remark dscp** command configures an action of re-marking the DSCP priority in IP packets in a traffic behavior.

The **undo remark dscp** command deletes the configuration.

By default, an action of re-marking the DSCP priority in IP packets is not configured in a traffic behavior.

Format

remark dscp { *dscp-name* | *dscp-value* }

undo remark dscp

Parameters

Parameter	Description	Value
dscp-name	Specifies the DSCP priority name in IP packets.	The value can be **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.

Parameter	Description	Value
dscp-value	Specifies the DSCP priority in IP packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide differentiated services based on the DSCP priority, run the **remark dscp** command to configure the device to re-mark the DSCP priority in IP packets in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing DSCP priority re-marking.

Precautions

If a traffic policy containing **remark dscp** is applied to the outbound direction on an interface, the device still processes outgoing packets based on the original priority but the downstream Layer 3 device or above processes the packets based on the re-marked priority.

If the traffic policy containing **remark dscp** and the **trust dscp** command are used in the outbound direction on the interface of packets, the **remark dscp** command changes DSCP priorities in packets because the **remark dscp** command takes precedence over the **trust dscp** command.

The **remark dscp** and **remark ip-precedence** commands cannot be used in the same traffic behavior.

If you run the **remark dscp** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

For the S5720EI, S5720HI, S6720EI, and S6720S-EI, applying a traffic policy containing **remark dscp** does not change the local priority of packets on the device where **remark dscp** is configured. To change the local priority of packets on the device, configure **remark local-precedence** in the traffic policy.

Example

# Re-mark the DSCP priority in IP packets with 56 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark dscp 56
```

Related Topics

15.2.21 remark ip-precedence

15.1.31 traffic behavior

15.2.23 trust

15.2.20 remark dscp (QoS profile view)

Function

The **remark dscp** command configures the device to re-mark DSCP priorities in IP packets in a QoS profile.

The **undo remark dscp** command cancels the configuration.

By default, the device does not re-mark DSCP priorities in IP packets in a QoS profile.

NOTE

Only the S5720HI supports this command.

Format

remark dscp *dscp-value* { **inbound** | **outbound** }

undo remark dscp { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
dscp-value	Specifies the DSCP priority in IP packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
inbound	Specifies the DSCP priority in incoming IP packets.	-
outbound	Specifies the DSCP priority in outgoing IP packets.	-

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device needs to provide differentiated services based on DSCP priorities in IP packets, run the **remark dscp** command to configure the device to re-mark DSCP priorities in IP packets in a QoS profile.

Precautions

When the device processes IPv6 packets, or when the device uses the direct forwarding mode to process IPv4 packets, the **remark dscp** command cannot be used to re-mark DSCP priorities in these packets.

When packets match both outbound DSCP priority re-marking and outbound priority mapping that are configured on the device, only outbound priority mapping takes effect.

On the device that uses an earlier version of V200R011C10, the DSCP priority re-marking direction cannot be specified. When the device that uses an earlier version of V200R011C10 is upgraded to V200R011C10, the device re-marks DSCP priorities of incoming packets by default.

If you run the **remark dscp** command in the same QoS profile view multiple times, only the latest configuration takes effect.

Example

# Configure the device to re-mark the DSCP priority in incoming IP packets with 56 in the QoS profile **huawei**.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name huawei
[HUAWEI-qos-huawei] remark dscp 56 inbound
```

Related Topics

15.3.12 qos-profile

15.2.21 remark ip-precedence

Function

The **remark ip-precedence** command configures an action of re-marking the IP precedence in IP packets in a traffic behavior.

The **undo remark ip-precedence** command deletes the configuration.

By default, an action of re-marking the IP precedence in IP packets is not configured in a traffic behavior.

Format

remark ip-precedence *ip-precedence*

undo remark ip-precedence

Parameters

Parameter	Description	Value
ip-precedence	Specifies the IP precedence.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the downstream device needs to provide differentiated services based on the IP precedence, run the **remark ip precedence** command to configure the device to re-mark the IP precedence in IP packets in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing IP precedence re-marking.

Precautions

After the re-marking action is configured, the device still processes outgoing packets based on the original priority but the downstream Layer 3 device or above processes the packets based on the re-marked priority.

A traffic policy containing the **remark ip-precedence** action can be only used in the inbound direction.

The **remark dscp** and **remark ip-precedence** commands cannot be used in the same traffic behavior.

If you run the **remark ip-precedence** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

# Re-mark the IP precedence in IP packets with 6 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark ip-precedence 6
```

Related Topics

15.2.19 remark dscp

15.1.31 traffic behavior

15.2.22 remark local-precedence

Function

The **remark local-precedence** command configures an action of re-marking the internal priority in packets in a traffic behavior.

The **undo remark local-precedence** command deletes the configuration.

By default, an action of re-marking the internal priority in packets is not configured in a traffic behavior.

Format

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

undo remark local-precedence

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support **green**, **yellow**, and **red**.

Parameters

Parameter	Description	Value
local-precedence-name	Specifies the internal priority name.	The value can be **af1**, **af2**, **af3**, **af4**, **be**, **cs6**, **cs7**, or **ef**.
local-precedence-value	Specifies the internal priority value.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
green	Indicates that the green color corresponds to an internal priority.	-
yellow	Indicates that the yellow color corresponds to an internal priority.	-
red	Indicates that the red color corresponds to an internal priority.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide differentiated services based on the internal priority of packets, run the **remark local-precedence** command to configure the device to re-mark the internal priority of packets so that the device can provide QoS based on the re-marked priority.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing internal priority re-marking.

Precautions

Re-marking the internal priority only affects QoS processing of packets on the device.

The **remark 8021p** and **remark local-precedence** commands cannot be used in the same traffic behavior.

A traffic policy containing the **remark local-precedence** action can be only used in the inbound direction.

If you run the **remark local-precedence** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

# Re-mark the internal priority of packets with 2 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] remark local-precedence 2
```

Related Topics

15.2.17 remark 8021p

15.1.31 traffic behavior

15.2.23 trust

Function

The **trust** command specifies the priority to be mapped for packets.

The **undo trust** command cancels the configuration.

By default:

- The S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI do not trust priorities of packets.
- The S1720X, S1720X-E, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI process packets based on the mapping of the 802.1p priority.
- The S5720EI, S5720HI, S6720EI, and S6720S-EI process packets based on the mapping of the outer 802.1p priority.

Format

trust { **8021p** | **dscp** | **ip-precedence** } (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

undo trust { **8021p** | **dscp** | **ip-precedence** } (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

trust { **8021p** { **inner** | **outer** } | **dscp** } (S5720EI, S5720HI, S6720EI, S6720S-EI)

undo trust (S5720EI, S5720HI, S6720EI, S6720S-EI)

NOTE

Only the S1720GFR, S2750EI, S5700LI, and S5700S-LI support the **ip-precedence** parameter.

Parameters

Parameter	Description	Value
8021p	Maps packets based on the 802.1p priority.	-
inner	Maps packets based on the inner 802.1p priority.	-
outer	Maps packets based on the outer 802.1p priority.	-
dscp	Maps packets based on the DSCP priority.	-
ip-precedence	Maps packets based on the IP priority.	-

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a device does not trust any packet priority, packets enter queue 0 and 8021.p priorities in the packets are set to 0. Differentiated services cannot be provided. After the **trust** command is used, the device searches for the mapping table based on the priority in packets, re-marks the inner priority in packets, and sends packets to queues.

To set the same priority to be trusted on multiple interfaces, you can perform the configuration on a port group to reduce the workload.

Precautions

The S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI do not trust any packet priorities by default, so the device adds the interface priority to the packets entering the device. If some services are forwarded based on packet priorities, the forwarding result may be incorrect. For example, when two-way frame delay measurement for a VLAN is configured, you need to run the **trust** command to set the priority to be trusted.

On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI:

- When the **trust dscp** and **trust 8021p** commands are configured on the same interface:
  - The interface trusts DSCP priorities if IPv4 packets are received.
  - The interface trusts 802.1p priorities if VLAN packets are received.
- The **trust dscp** and **trust ip-precedence** commands cannot be run on the same interface.
- The DSCP priority mapping and IP priority mapping cannot be used together, so the type of trusted packet priority configured on an interface must be consistent with the global priority mapping type.

If both a traffic policy containing **remark 8021p** or **remark dscp** and the **trust 8021p** or **trust dscp** command are configured in the outbound interface of packets, only the traffic policy containing **remark 8021p** or **remark dscp** takes effect, and the **trust 8021p** or **trust dscp** command does not take effect.

On the S5720EI, S5720HI, S6720EI, and S6720S-EI, if you run the **trust 8021p inner**, **trust 8021p outer**, and **trust dscp** commands multiple times on the same interface, only the latest configuration takes effect.

Example

# Configure GE0/0/1 to trust DSCP priorities.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trust dscp
```

Related Topics

15.2.5 diffserv domain

15.2.24 trust upstream

15.2.24 trust upstream

Function

The **trust upstream** { **default** | *ds-domain-name* } command applies a DiffServ domain to an interface.

The **trust upstream none** command disables the priority mapping on an interface.

The **undo trust upstream** command restores the default settings.

By default, no DiffServ domain is bound to an interface.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

trust upstream { **default** | *ds-domain-name* | **none** }

undo trust upstream

Parameters

Parameter	Description	Value
default	Indicates the default DiffServ domain preset in the system.	-
ds-domain-name	Specifies the name of a DiffServ domain applied to an interface.	The value must the name of an existing DiffServ domain.
none	Indicates that none DiffServ domain is applied to an interface, and the priorities in packets are not trusted.	-

Views

GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

To map priorities of the packets sent from the upstream device to PHBs according to the mappings defined in a DiffServ domain, run the **trust upstream** command to apply the DiffServ domain to the inbound interface of the packets. The system then maps priorities of packets to PHBs according to the mappings defined in the DiffServ domain.

To map PHBs of the packets sent to the downstream device to priorities according to the mappings defined in a DiffServ domain, run the **trust upstream** command to apply the DiffServ domain to the outbound interface of the packets. The system then maps PHBs of packets to the priorities according to the mappings defined in the DiffServ domain.

Prerequisites

A DiffServ domain has been created.

Precautions

- After the **trust upstream** command is executed on an interface, the system maps the priorities of packets on the interface to the following values according to the mappings defined in the DiffServ domain:
  - PHB
  - Packet color

  For default mappings from 802.1p priorities to PHBs and colors, from PHBs and colors to 802.1p priorities, from DSCP priorities to PHBs and colors, from PHBs and colors to DSCP priorities, from EXP priorities to PHBs and colors, and from PHBs and colors to EXP priorities see the **8021p-inbound**, **8021p-outbound**, **ip-dscp-inbound**, **ip-dscp-outbound**, **mpls-exp-inbound**, and **mpls-exp-outbound** commands.
- After the **trust upstream none** command is executed, the system performs no priority mapping on packets passing the interface.
- To change the DiffServ domain bound to an interface, run the **undo trust upstream** command to unbind the original DiffServ domain from the interface, and then run the **trust upstream** command to apply the new DiffServ domain to the interface.
- If you run the **trust upstream** command multiple times in the same interface view, only the latest configuration takes effect.
- To apply a DiffServ domain to multiple interfaces, you can perform the configuration on the port group to reduce the workload.

Example

# Apply DiffServ domain **ds1** to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] trust upstream ds1
```

Related Topics

15.2.5 diffserv domain

15.2.23 trust

15.2.2 8021p-inbound

15.2.3 8021p-outbound

15.2.11 ip-dscp-inbound

15.2.12 ip-dscp-outbound

9.2.3 mpls-exp-inbound

9.2.4 mpls-exp-outbound

15.3 Traffic Policing, Traffic Shaping, and Interface-based Rate Limiting Commands

15.3.1 Command Support

For details about command support, see the description of each command. If no command support information is provided, all switch models support the command by default.

15.3.2 car (traffic behavior view)

Function

The **car** command configures traffic policing in a traffic behavior.

The **undo car** command deletes traffic policing from a traffic behavior.

By default, traffic policing is not configured in a traffic behavior.

Format

car [**aggregation**] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**green pass**] [**yellow** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] [**red** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

NOTE

Only the S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support **aggregation** and **share**.

car cir *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**green** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] [**yellow** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }] [**red** { **discard** | **pass** [**remark-dscp** *dscp-value* | **remark-8021p** *8021p-value*] }](S5720EI, S6720EI, S6720S-EI)

car cir *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**green** { **discard** | **pass** }] [**yellow** { **discard** | **pass** }] [**red** { **discard** | **pass** }] (S5720HI)

undo car

Parameters

Parameter	Description	Value
aggregation	Indicates aggregated CAR. Aggregated CAR can be applied to multiple interfaces, and traffic on the interfaces is restricted by aggregated CAR.	-
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.

Parameter	Description	Value
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. The PIR must be higher than or equal to the CIR. The default PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. The default CBS is 125 times the CIR. **NOTE** If the default CBS is smaller than 4000 because the CIR is small, the device uses the CBS of 4000. If the default CBS is larger than 4294967295 because the CIR is large, the device uses the CBS of 4294967295.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default PBS is 125 times the CIR. If the PIR is set, the default PBS is 125 times the PIR. **NOTE** If the default PBS is smaller than 4000 because the CIR or PIR is small, the device uses the PBS of 4000. If the default PBS is larger than 4294967295 because the CIR or PIR is large, the device uses the PBS of 4294967295.

Parameter	Description	Value
share	Indicates level-1 aggregated CAR. If level-1 aggregated CAR is defined in a traffic behavior, and a traffic classifier defining multiple matching rules is bound to this traffic behavior, traffic matching the traffic classifier is restricted by the level-1 aggregated CAR.	-
green **yellow** **red**	Specifies the packet color. The packet color is determined by **cbs** *cbs-value* and **pbs** *pbs-value* of this command. By default, green packets and yellow packets are allowed to pass through, and red packets are discarded.	-
discard	Discards packets.	If the action specified for green packets is **discard**, the action specified for yellow and red packets must be **discard**. If the action specified for yellow packets is **discard**, the action specified for red packets must be **discard**.
pass	Allows packets to pass through.	-
remark-8021p *8021p-value*	Re-marks the 802.1p priorities of packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
remark-dscp *dscp-value*	Re-marks the DSCP priority of packets.	The value is an integer that ranges from 0 to 63.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flow-based traffic policing controls traffic that matches traffic classification rules and discards the excess traffic to limit traffic within a proper range and to protect network resources.

When data is sent from a high-speed link to a low-speed link, the bandwidth on the interface of the low-speed link is insufficient. As a result, a large number of packets are discarded. To solve this problem, configure traffic policing for outgoing traffic on the interface of the high-speed link. The interface then discards the packets whose rate exceeds the traffic policing rate so that the outgoing traffic rate is limited within a proper range. You can also configure traffic policing for incoming traffic on the interface of the low-speed link. The interface then discards the received packets whose rate exceeds the traffic policing rate.

Traffic policing based on traffic policies controls rates of packets of different types.

The packet color is determined by the CBS and PBS:

- When the size of a packet is smaller than the CBS, the packet is colored green.
- When the size of a packet is greater than or equal to the CBS but smaller than the PBS, the packet is colored yellow.
- When the size of a packet is greater than or equal to the PBS, the packet is colored red.

After traffic policing is configured, the device counts forwarded and discarded packets.

Prerequisites

A traffic behavior has been created using the **traffic behavior** command.

Precautions

When a traffic policy containing traffic policing actions is applied to an interface, you must use the **undo traffic-policy** command to unbind the traffic policy if you need to change traffic policing parameters.

For the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, if a traffic behavior defines the **car** command with **remark-8021p** *8021p-value* or **remark-dscp** *dscp-value* specified, a traffic policy containing this traffic behavior can only be applied in the inbound direction.

If aggregated CAR is configured by specifying the **aggregation** parameter on the S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, the traffic policies containing this traffic behavior can only be applied in the inbound direction.

If a traffic behavior defines the **car** command with **share** specified, a traffic policy containing this traffic behavior can only be applied in the inbound direction.

The **aggregation** and **share** parameters cannot be specified simultaneously in one traffic behavior.

For the S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, if a traffic policy defining aggregated CAR and traffic statistics is applied to multiple interfaces, the system collects traffic statistics on all these interfaces. Traffic statistics on any one of the interfaces are the sum traffic statistics of all these interfaces.

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

When you use a traffic policy for rate limiting and apply the traffic policy in the Eth-Trunk interface view, if the Eth-Trunk interface contains several member interfaces, these member interfaces share the bandwidth specified by the rate limit.

Example

# Configure traffic policing in the traffic behavior **b1** as follows: Set the CIR to 1000 kbit/s, permit green and yellow packets to pass through, re-mark the 802.1p priority of green packets with 7, re-mark the DSCP priority of yellow packets with 20, and discard red packets.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] car cir 1000 green pass remark-8021p 7 yellow pass remark-dscp 20 red discard
```

Related Topics

15.1.7 display traffic policy statistics

15.1.31 traffic behavior

15.1.33 traffic policy

15.3.3 car (QoS profile view)

Function

The **car** command configures traffic policing in a QoS profile.

The **undo car** command deletes the traffic policing configuration from the QoS profile.

By default, traffic policing is not configured in a QoS profile.

Format

car cir *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] { **inbound** | **outbound** }

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

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

The S5720EI does not support inbound traffic policing. When the device configured with inbound traffic policing is upgraded from an earlier version (earlier than V200R007), the inbound traffic policing configuration fails to be restored.

The S6720EI and S6720S-EI do not support inbound traffic policing.

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the guaranteed average transmission rate.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The PIR must be higher than or equal to the CIR. The default PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default CBS is 188 times the CIR. If the PIR is set, the default CBS is 125 times the CIR.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default PBS is 313 times the CIR. If the PIR is set, the default PBS is 125 times the PIR.
inbound	Indicates inbound traffic policing.	-
outbound	Indicates outbound traffic policing.	-

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic policing discards excess traffic to limit traffic within a proper range and to protect network resources.

The **car** command configures traffic policing in a QoS profile.

Follow-up Procedure

Apply the QoS profile in the AAA domain view.

Precautions

When the traffic policing rate is larger than the maximum bandwidth of an interface, traffic policing does not take effect on the interface. Set the CIR and PIR to be smaller than the rate of an interface.

When the CBS is smaller than the number of bytes in a packet, the device directly discards the packet.

Example

# Create a QoS profile named **huawei** in which the CIR is set to 10000 kbit/s, the CBS is set to 10240 bytes, and the PBS is set to 10240 bytes.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name huawei
[HUAWEI-qos-huawei] car cir 10000 cbs 10240 pbs 10240 inbound
```

Related Topics

15.3.12 qos-profile

15.3.4 car share

Function

The **car share** command configures aggregated CAR in a traffic behavior.

The **undo car share** command cancels aggregated CAR in a traffic behavior.

By default, aggregated CAR is not configured in a traffic behavior.

NOTE

Only the S5720EI and S5720HI support this command.

Format

car *car-name* **share**

undo car [*car-name*] **share**

Parameters

Parameter	Description	Value
car-name	Specifies the name of a CAR profile.	The value must the name of an existing CAR profile.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple traffic classifiers are defined in a traffic policy and traffic behaviors associated with the traffic classifiers define CAR (using the **car cir** command) and aggregated CAR, the system limits the rates of flows using the configured CAR, aggregates the flows, and limits the rate of the aggregated traffic using the aggregated CAR in sequence. This process is called hierarchical traffic policing.

Hierarchical traffic policing multiplexes traffic statistics and controls services in a fine-granular manner. For example, hierarchical traffic policing limits the service traffic of level-1 and level-2 users or traffic of level-1 and level-2 user groups.

Prerequisites

A QoS CAR profile has been configured using the **qos car** command.

Precautions

The traffic policy defining the aggregated CAR action can only be used in the inbound direction.

After aggregated CAR is configured, all the rules in the traffic classifiers bound to the same traffic behavior share the CAR index. The system aggregates all the flows matching these traffic classifiers and uses CAR to limit the rate of the flows. If the traffic classifiers define both Layer 2 and Layer 3 information, the aggregated CAR configuration is invalid.

A traffic policy limits the traffic rate using the aggregated CAR only in the current applied object. For example, when the traffic policy **p1** defining the aggregated CAR is applied to **interface1** and **interface2**, the aggregated CAR applies to traffic on **interface1** and **interface2** respectively, without affecting each other.

On the S5720EI, if the sum of CIR values of each aggregated flow is larger than the specified CIR value for aggregated CAR in configured traffic policing, the system first guarantees the sum of CIR values of each flow. As a result, traffic exceeds the CIR value for aggregated CAR. On the S5720HI, the system polices aggregated flows based on the CIR value for aggregated CAR. On the S5720EI, to ensure that traffic is policed based on the CIR value for aggregated CAR, the CIR value for aggregated CAR must be larger than the sum of CIR values of each aggregated flow.

Example

# Configure aggregated CAR in the traffic behavior **tb1**.

```
<HUAWEI> system-view
[HUAWEI] qos car qoscar1 cir 2000
[HUAWEI] traffic behavior tb1
[HUAWEI-behavior-tb1] car cir 1000 pir 123456
[HUAWEI-behavior-tb1] car qoscar1 share
```

Related Topics

15.3.10 qos car

15.3.2 car (traffic behavior view)

15.1.31 traffic behavior

15.3.5 display qos-profile

Function

The **display qos-profile** command displays the configured QoS profile information.

Format

display qos-profile [**name** *profile-name* | **all**]

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a QoS profile.	The value must the name of an existing QoS profile.
all	Indicates all QoS profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display qos-profile** command displays the configuration of a specified QoS profile or all QoS profiles. The command output helps you check the QoS profile configuration and locate QoS faults.

Example

# Display the configurations of all QoS profiles.

```
<HUAWEI> display qos-profile all
Qos-profile[0]: huawei
--------------------------------------------
IcarConfiged:        0
IcarCir     :        0
IcarPir     :        0
IcarCbs     :        0
IcarPbs     :        0
EcarConfiged:        0
EcarCir     :        0
EcarPir     :        0
EcarCbs     :        0
EcarPbs     :        0
StatisiticEn:        1
Remark8021p :        0
8021pValue  :        0
RemarkDscp  :        0
DscpValue   :        0
--------------------------------------------
```

NOTE

The **display qos-profile** command on the S5720EI, S6720EI, and S6720S-EI does not display **IcarConfiged**, **IcarCir**, **IcarPir**, **IcarCbs**, **IcarPbs**, **Remark8021p**, **8021pValue**, **RemarkDscp**, or **DscpValue**.

Table 15-22 Description of the **display qos-profile all** command output

Item	Description
Qos-profile[0]	Name of a QoS profile. The number in bracket is the index that the system assigns to the QoS profile. To create a QoS profile, run the **qos-profile** command.

Item	Description
IcarConfiged	Whether inbound traffic policing is configured: ● 0: Inbound traffic policing is not configured. ● 1: Inbound traffic policing is configured. To configure inbound traffic policing in a QoS profile, run the **car (QoS profile view)** command.
IcarCir	CIR in the inbound direction. To change the value, run the **car (QoS profile view)** command.
IcarPir	PIR in the inbound direction. To change the value, run the **car (QoS profile view)** command.
IcarCbs	CBS in the inbound direction. To change the value, run the **car (QoS profile view)** command.
IcarPbs	PBS in the inbound direction. To change the value, run the **car (QoS profile view)** command.
EcarConfiged	Whether outbound traffic policing is configured: ● 0: Outbound traffic policing is not configured. ● 1: Outbound traffic policing is configured. To configure outbound traffic policing in a QoS profile, run the **car (QoS profile view)** command.
EcarCir	CIR in the outbound direction. To change the value, run the **car (QoS profile view)** command.
EcarPir	PIR in the outbound direction. To change the value, run the **car (QoS profile view)** command.
EcarCbs	CBS in the outbound direction. To change the value, run the **car (QoS profile view)** command.
EcarPbs	PBS in the outbound direction. To change the value, run the **car (QoS profile view)** command.

Item	Description
StatisiticEn	Whether the traffic statistics function is configured: • 0: The traffic statistics function is not configured. • 1: The traffic statistics function is configured. To configure the traffic statistics function in a QoS profile, run the **statistic enable (QoS profile view)** command.
Remark8021p	Whether 802.1p priority re-marking is configured: • 0: 802.1p priority re-marking is not configured. • 1: 802.1p priority re-marking is configured. To configure 802.1p priority re-marking in a QoS profile, run the **remark 8021p (QoS profile view)** command.
8021pValue	Re-marked 802.1p priority. To change the value, run the **remark 8021p (QoS profile view)** command.
RemarkDscp	Whether DSCP priority re-marking is configured: • 0: DSCP priority re-marking is not configured. • 1: DSCP priority re-marking is configured. To configure DSCP priority re-marking in a QoS profile, run the **remark dscp (QoS profile view)** command.
DscpValue	Re-marked DSCP priority. To change the value, run the **remark dscp (QoS profile view)** command.

# Display the summary configurations of all QoS profiles.

```
<HUAWEI> display qos-profile
     index                qos-profile name
-------------------------------------------------------------
     0                   huawei
-------------------------------------------------------------
 Total   64     Used    1
```

Table 15-23 Description of the **display qos-profile** command output

Item	Description
index	Index that the system assigns to a QoS profile.
qos-profile name	Name of a QoS profile.
Total	Maximum number of QoS profiles that can be configured.
Used	Number of used QoS profiles.

Related Topics

15.3.12 qos-profile

15.3.3 car (QoS profile view)

15.2.18 remark 8021p (QoS profile view)

15.2.20 remark dscp (QoS profile view)

15.3.6 display qos car

Function

The **display qos car** command displays the QoS CAR profile configuration.

NOTE

Only the S5720EI and S5720HI support this command.

Format

display qos car { **all** | **name** *car-name* }

Parameters

Parameter	Description	Value
all	Displays the configurations of all QoS CAR profiles.	-
name *car-name*	Displays the configuration of a specified QoS CAR profile.	The value must the name of an existing QoS CAR profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display qos car** command displays the configurations of all QoS CAR profiles or a specified QoS CAR profile. The command output helps you check the QoS CAR profile configuration and locate QoS faults.

Precautions

If you do not use the **qos car** command to create a QoS CAR profile, no information is displayed after the **display qos car** command is executed.

Example

# Display the configurations of all QoS CAR profiles.

```
<HUAWEI> display qos car all
   ------------------------------------------------------------------
   CAR Name      : qoscar1
   CAR Index    : 0
    car cir 8000 (Kbps) pir 10000 (Kbps) cbs 1000000 (byte) pbs 1250000 (byte)
  ------------------------------------------------------------------
   CAR Name      : qoscar2
   CAR Index    : 1
    car cir 5000 (Kbps) pir 8000 (Kbps) cbs 625000 (byte) pbs 1000000 (byte)
  ------------------------------------------------------------------
   CAR Name      : car1
   CAR Index    : 2
    car cir 1000 (Kbps) cbs 188000 (byte)
```

# Display the configuration of the QoS CAR profile named **car1**.

```
<HUAWEI> display qos car name car1
  ------------------------------------------------------------------
   CAR Name      : car1
   CAR Index    : 2
    car cir 1000 (Kbps) cbs 188000 (byte)
```

Table 15-24 Description of the **display qos car** command output

Item	Description
CAR Name	QoS CAR profile name. To configure a QoS CAR profile, run the **qos car** command.
CAR Index	Index of the QoS CAR profile.
car cir 8000 (Kbps) pir 10000 (Kbps) cbs 1000000 (byte) pbs 1250000 (byte)	Parameters of the QoS CAR profile, including the CIR, PIR, CBS, and PBS. To set parameters in a QoS CAR profile, run the **qos car** command.

Related Topics

15.3.10 qos car

15.3.7 display qos configuration

Function

The **display qos configuration** command displays the QoS configuration on an interface.

Format

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

Parameters

Parameter	Description	Value
interface [*interface-type interface-number*]	Displays the QoS configuration on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, the QoS configurations on all the interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display qos configuration** command displays QoS configurations on a specified interface or all interfaces. The command output helps you check the QoS configuration and locate QoS faults.

Example

# Display the QoS configuration on GE0/0/1 of the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, or S6720S-SI.

```
<HUAWEI> display qos configuration interface gigabitethernet 0/0/1
 interface GigabitEthernet0/0/1
 ----------------------------------------------------------------------------
 Trust flag                 | --
 Port priority              | 0
 Schedule-profile           | --
 Tail-drop-profile          | --
 Port lr                    | outbound, cir = --, cbs = --
 Port lr                    | inbound, cir = --, cbs = --
 ----------------------------------------------------------------------------
 queue-index | configuration |
 ----------------------------------------------------------------------------
 0           | shaping       | cir = --, cbs = --
             |               | pir = --, pbs = --
 ----------------------------------------------------------------------------
 1           | shaping       | cir = --, cbs = --
             |               | pir = --, pbs = --
 ----------------------------------------------------------------------------
 2           | shaping       | cir = --, cbs = --
             |               | pir = --, pbs = --
 ----------------------------------------------------------------------------
 3           | shaping       | cir = --, cbs = --
             |               | pir = --, pbs = --
 ----------------------------------------------------------------------------
 4           | shaping       | cir = --, cbs = --
             |               | pir = --, pbs = --
 ----------------------------------------------------------------------------
 5           | shaping       | cir = --, cbs = --
             |               | pir = --, pbs = --
 ----------------------------------------------------------------------------
 6           | shaping       | cir = --, cbs = --
             |               | pir = --, pbs = --
 ----------------------------------------------------------------------------
 7           | shaping       | cir = --, cbs = --
             |               | pir = --, pbs = --
 ----------------------------------------------------------------------------
```

# Display the QoS configuration on GE0/0/1 of the S5720EI, S6720EI, or S6720S-EI.

```
<HUAWEI> display qos configuration interface gigabitethernet 0/0/1
 interface GigabitEthernet0/0/1
 ----------------------------------------------------------------------------
 Trust flag                 | outer 8021p
 DS name                    | --
 DEI enable                 | disable
 PHB marking                | enable
 Port priority              | 0
 Port wred                  | --
 Port lr                    | outbound, cir = --, cbs = --
 Port lr                    | inbound, cir = --, cbs = --
 ----------------------------------------------------------------------------
 queue-index | configuration |
 ----------------------------------------------------------------------------
 0           | shaping       | cir = --, cbs = --
             |               | pir = --, pbs = --
             | schedule      | wrr, weight = 1
             | wred          | --
             | length        | --
 ----------------------------------------------------------------------------
 1           | shaping       | cir = --, cbs = --
             |               | pir = --, pbs = --
             | schedule      | wrr, weight = 1
```

```
            | wred          | --
            | length        | --
-----------------------------------------------------------------------------
2           | shaping       | cir = --, cbs = --
            |               | pir = --, pbs = --
            | schedule      | wrr, weight = 1
            | wred          | --
            | length        | --
-----------------------------------------------------------------------------
3           | shaping       | cir = --, cbs = --
            |               | pir = --, pbs = --
            | schedule      | wrr, weight = 1
            | wred          | --
            | length        | --
-----------------------------------------------------------------------------
4           | shaping       | cir = --, cbs = --
            |               | pir = --, pbs = --
            | schedule      | wrr, weight = 1
            | wred          | --
            | length        | --
-----------------------------------------------------------------------------
5           | shaping       | cir = --, cbs = --
            |               | pir = --, pbs = --
            | schedule      | wrr, weight = 1
            | wred          | --
            | length        | --
-----------------------------------------------------------------------------
6           | shaping       | cir = --, cbs = --
            |               | pir = --, pbs = --
            | schedule      | wrr, weight = 1
            | wred          | --
            | length        | --
-----------------------------------------------------------------------------
7           | shaping       | cir = --, cbs = --
            |               | pir = --, pbs = --
            | schedule      | wrr, weight = 1
            | wred          | --
            | length        | --
-----------------------------------------------------------------------------
```

# Display the QoS configuration on GE0/0/1 of the S5720HI.

```
<HUAWEI> display qos configuration interface gigabitethernet 0/0/1
 interface GigabitEthernet0/0/1
-----------------------------------------------------------------------------
Trust flag                | outer 8021p
DS name                   | --
DEI enable                | disable
Port priority             | 0
PHB marking               | enable
Port wred                 | --
Port lr                   | outbound, cir = --, cbs = --
Port lr                   | inbound, cir = --, cbs = --
TM enable                 | disable
-----------------------------------------------------------------------------
queue-index | configuration |
-----------------------------------------------------------------------------
1           | shaping       | cir = --, cbs = --
            |               | pir = --, pbs = --
            | schedule      | pq
            | wred          | --
            | length        | --
-----------------------------------------------------------------------------
2           | shaping       | cir = --, cbs = --
            |               | pir = --, pbs = --
            | schedule      | pq
            | wred          | --
            | length        | --
-----------------------------------------------------------------------------
3           | shaping       | cir = --, cbs = --
            |               | pir = --, pbs = --
```

```
          | schedule      | pq
          | wred          | --
          | length        | --
-------------------------------------------------------------------------------
4         | shaping       | cir = --, cbs = --
          |               | pir = --, pbs = --
          | schedule      | pq
          | wred          | --
          | length        | --
-------------------------------------------------------------------------------
5         | shaping       | cir = --, cbs = --
          |               | pir = --, pbs = --
          | schedule      | pq
          | wred          | --
          | length        | --
-------------------------------------------------------------------------------
6         | shaping       | cir = --, cbs = --
          |               | pir = --, pbs = --
          | schedule      | pq
          | wred          | --
          | length        | --
-------------------------------------------------------------------------------
7         | shaping       | cir = --, cbs = --
          |               | pir = --, pbs = --
          | schedule      | pq
          | wred          | --
          | length        | --
-------------------------------------------------------------------------------
```

Table 15-25 Description of the **display qos configuration** command output

Item	Description
Trust flag	Type of the external priority (802.1p priority, DSCP priority, or IP precedence) mapped to the internal priority (DiffServ level and color). To change the value, run the **trust** command.
DS name	DiffServ domain name. To create a DiffServ domain, run the **diffserv domain** command.
DEI enable	Whether the function that DEI field in a VLAN tag is mapped to the drop priority is enabled. ● enable: The function is enabled. ● disable: The function is disabled. To set the function that DEI field in a VLAN tag is mapped to the drop priority, run the **dei enable** command.
PHB marking	Whether PHB mapping is enabled for outgoing packets on the interface. ● enable: PHB mapping is enabled for outgoing packets on the interface. ● disable: PHB mapping is disabled for outgoing packets on the interface. To set PHB mapping, run the **qos phb marking enable** command.

Item	Description
Port priority	Default 802.1p priority added to untagged packets by the interface. To change the value, run the **port priority** command.
Port wred	Name of the WRED drop profile applied to the interface. To apply a WRED drop profile to an interface, run the **qos wred** command.
Schedule-profile	Name of the scheduling profile applied to the interface. To apply a scheduling profile to an interface, run the **qos schedule-profile (interface view)** command.
Tail-drop-profile	Name of the tail drop profile applied to the interface. To apply a tail drop profile to an interface, run the **qos tail-drop-profile (interface view)** command.
Port lr	Traffic shaping rate on the interface. To configure traffic shaping rate on an interface, run the **qos lr outbound** or **qos lr inbound** command.
TM enable	Whether the traffic manager (TM) is enabled to buffer and schedule packets. ● enable: The TM is enabled to buffer and schedule packets. ● disable: The TM is disabled from buffering and scheduling packets. To set enable or disable the TM, run the **qos traffic-manage enable** command.
queue-index	Interface queue index.
configuration	Interface queue configuration.
shaping	Traffic shaping configuration of the interface queue. To configure traffic shaping on an interface, run the **qos queue shaping** command.
cir	Committed information rate (CIR). To change the value, run the **qos queue shaping** command.
cbs	Committed burst size (CBS). To change the value, run the **qos queue shaping** command.
pir	Peak information rate (PIR). To change the value, run the **qos queue shaping** command.
pbs	Peak burst size (PBS). To change the value, run the **qos queue shaping** command.
schedule	Scheduling mode of the interface queue. To set the scheduling mode of interface queues, run the **qos { pq | wrr | drr }** command.

Item	Description
wred	WRED drop profile bound to an interface queue. To bind a WRED drop profile to an interface queue, run the **qos queue wred** command.
weight	Scheduling weight of a queue. To set the scheduling weight of a queue, run the **qos queue drr** or **qos queue wrr** command.
length	Interface queue length. The switch does not support modifying the interface queue length, and this field is always displayed as --.

15.3.8 display qos lr

Function

The **display qos lr** command displays the rate limit configuration on an interface.

Format

display qos lr { **inbound** | **outbound** } **interface** *interface-type interface-number*

NOTE

The S2750EI, S5700-10P-LI-AC, and S5700-10P-PWR-LI-AC that are enabled with Layer 3 hardware forwarding for IPv4 packets do not support **inbound**.

Parameters

Parameter	Description	Value
inbound	Displays the rate limit configuration in the inbound direction on an interface.	-
outbound	Displays the rate limit configuration in the outbound direction on an interface.	-
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display qos lr** command displays the rate limit configuration on a specified interface. The command output helps you check the rate limit on an interface and locate faults.

Precautions

If you do not use the **qos lr inbound** or **qos lr outbound** command to configure the rate limit on an interface, no information is displayed after the **display qos lr** command is executed.

Example

# Set the CIR of data packets to be sent from the GE0/0/1 to 20000 kbit/s and the CBS to 375000 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos lr outbound cir 20000 cbs 375000
[HUAWEI-GigabitEthernet0/0/1] quit
```

# Display the rate limit configuration on the GE0/0/1.

```
<HUAWEI> display qos lr outbound interface gigabitethernet 0/0/1
GigabitEthernet0/0/1 lr outbound:
 cir: 20000 Kbps, cbs: 375000 Byte
```

Table 15-26 Description of the **display qos lr** command output

Item	Description
cir	Committed information rate (CIR). To set the CIR, run the **qos lr inbound** or **qos lr outbound** command.
cbs	Committed burst size (CBS). To set the CBS, run the **qos lr inbound** or **qos lr outbound** command.

Related Topics

15.3.14 qos lr inbound

15.3.15 qos lr outbound

15.3.9 display qos statistics

Function

The **display qos statistics** command displays traffic statistics on an interface where rate limiting is performed in the inbound direction.

Format

display qos statistics interface *interface-type interface-number* **inbound**

display qos statistics inbound all [**nonzero**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays traffic statistics on a specified interface where rate limiting is performed. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
inbound	Displays traffic statistics in the inbound direction.	-
all	Displays traffic statistics on all interfaces where rate limiting is performed.	-
nonzero	Displays traffic statistics on all interfaces where rate limiting is performed and the statistics are not 0.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display qos statistics** command to view statistics on forwarded and discarded packets and check whether rate limiting takes effect. The command output helps you locate faults.

Prerequisites

The **qos lr inbound** command has been executed to configure rate limiting in the inbound direction on an interface.

Precautions

If the **qos lr inbound** command is not used, the system displays the following message after the **display qos statistics interface** *interface-type interface-number* **inbound** command is executed:

```
Info: There is no rate limited configuration inbound in the interface.
```

Example

# Display traffic statistics on GE0/0/1 where rate limiting is performed in the inbound direction.

```
<HUAWEI> display qos statistics interface gigabitethernet 0/0/1 inbound
-------------------------------------------------------
 Item                                Value
-------------------------------------------------------
 Passed packets                          0
 Passed bytes                           0
 Dropped packets                          0
 Dropped bytes                           0
-------------------------------------------------------
```

Table 15-27 Description of the **display qos statistics** command output

Item	Description
Passed packets	Number of forwarded packets.
Passed bytes	Number of forwarded bytes.
Dropped packets	Number of discarded packets.
Dropped bytes	Number of discarded bytes.

Related Topics

15.3.14 qos lr inbound

15.3.18 reset qos statistics

15.3.10 qos car

Function

The **qos car** command creates a QoS CAR profile and sets parameters in the QoS CAR profile.

The **undo qos car** command deletes a QoS CAR profile.

By default, no QoS CAR profile is created.

NOTE

Only the S5720EI and S5720HI support this command.

Format

qos car *car-name* **cir** *cir-value* [**cbs** *cbs-value* [**pbs** *pbs-value*] | **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]

undo qos car *car-name*

Parameters

Parameter	Description	Value
car-name	Specifies the name of a QoS CAR profile.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The value cannot be c, ci, or cir.
cir *cir-value*	Specifies the committed information rate (CIR), which is the average rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 4294967295, in kbit/s. The PIR must be higher than or equal to the CIR. The default PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default CBS is 188 times the CIR. If the PIR is set, the default CBS is 125 times the CIR.

Parameter	Description	Value
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. By default, the PBS is 125 times the PIR.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic policing controls traffic by monitoring the rate of traffic, and discards excess traffic to limit traffic within a proper range and to protect network resources.

When data is sent from a high-speed link to a low-speed link, the bandwidth on the interface of the low-speed link is insufficient. As a result, a large number of packets are discarded. To solve this problem, configure traffic policing for outgoing traffic on the interface of the high-speed link. The interface then discards the packets whose rate exceeds the traffic policing rate so that the outgoing traffic rate is limited within a proper range. You can also configure traffic policing for incoming traffic on the interface of the low-speed link. The interface then discards the received packets whose rate exceeds the traffic policing rate.

The packet color is determined by **cbs** *cbs-value* and **pbs** *pbs-value* of this command:

- When the size of a packet is smaller than the CBS, the packet is colored green.
- When the size of a packet is greater than or equal to the CBS but smaller than the PBS, the packet is colored yellow.
- When the size of a packet is greater than or equal to the PBS, the packet is colored red.

Precautions

A maximum of 512 QoS CAR profiles can be created on the switch.

When the traffic shaping rate is greater than the maximum rate of an interface, traffic policing is not performed on the interface. You need to set the CIR or PIR to be smaller than the maximum rate of the interface.

When the CBS is smaller than the number of bytes in a packet, packets of this type are discarded.

To prevent a device failure to identify the packet color, you are advised to set the PBS to be larger than the CBS.

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

Example

# Create a QoS CAR profile named **qoscar1**, and set the CIR to 10000 kbit/s and the CBS to 10240 bytes.

```
<HUAWEI> system-view
[HUAWEI] qos car qoscar1 cir 10000 cbs 10240
```

Related Topics

15.3.4 car share

15.3.6 display qos car

15.3.11 qos-car exclude-interframe

Function

The **qos-car exclude-interframe** command configures the device not to count the inter-frame gap and preamble of packets when the device calculates the traffic policing rate or rate limit.

The **undo qos-car exclude-interframe** command configures the device to count the inter-frame gap and preamble of packets when the device calculates the traffic policing rate or rate limit.

By default, the device calculates the inter-frame gap and preamble of packets when the device calculates the traffic policing rate or rate limit.

Format

qos-car exclude-interframe

undo qos-car exclude-interframe

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When traffic policing or rate limiting is configured on an interface, the device calculates the inter-frame gap and preamble of packets for the traffic policing rate or rate limit. As a result, the rate is inaccurate. After the **qos-car exclude-interframe** command is used, the device does not count the inter-frame gap and preamble of packets for the traffic policing rate or rate limit.

The **qos-car exclude-interframe** command affects calculation of the traffic policing rate and inbound rate limit. When the **car (traffic behavior view)** and **qos lr inbound** commands are used to configure traffic policing and inbound rate limiting, the device does not count the inter-frame gap and preamble for the traffic policing rate or rate limit.

Precautions

Before this command is used, the following formula is used to calculate the traffic policing rate or rate limit:

Traffic policing rate/Rate limit = (Original packet length + Inter-frame gap + Preamble) x Number of packets forwarded per second

The inter-frame gap and preamble occupy 20 bytes.

After this command is used, the following formula is used to calculate the traffic policing rate or rate limit:

Traffic policing rate/Rate limit = Original packet length x Number of packets forwarded per second

Example

# Configure the device not to count the inter-frame gap and preamble of packets when the device calculates the traffic policing rate.

```
<HUAWEI> system-view
[HUAWEI] qos-car exclude-interframe
```

Related Topics

15.3.2 car (traffic behavior view)

15.3.14 qos lr inbound

15.3.12 qos-profile

Function

The **qos-profile** command creates a QoS profile and displays its view, or directly displays the view of an existing QoS profile.

The **undo qos-profile** command deletes a QoS profile.

By default, no QoS profile is configured on the device.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

qos-profile name *profile-name*

undo qos-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a QoS profile.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The value cannot be --.
all	Indicates all QoS profiles.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can define QoS configurations in a QoS profile to implement such functions as traffic policing, priority re-marking, and traffic statistics.

Follow-up Procedure

- Define parameters in the QoS profile, including parameters of traffic policing, priority re-marking, and traffic statistics.
- Apply the QoS profile in the specified view.

Precautions

The **undo qos-profile all** command only deletes the QoS profiles that are not applied.

The switch supports a maximum of 64 QoS profiles.

Example

# Create a QoS profile named **huawei** and enter the QoS profile view.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name huawei
[HUAWEI-qos-huawei]
```

Related Topics

15.3.3 car (QoS profile view)

15.3.13 qos-shaping exclude-interframe

Function

The **qos-shaping exclude-interframe** command configures the device not to count the inter-frame gap and preamble of packets when the device calculates the traffic shaping rate.

The **undo qos-shaping exclude-interframe** command configures the device to count the inter-frame gap and preamble of packets when the device calculates the traffic shaping rate.

By default, the device counts the inter-frame gap and preamble of packets when the device calculates the traffic shaping rate.

Format

qos-shaping exclude-interframe

undo qos-shaping exclude-interframe

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After traffic shaping is configured on an interface, the device counts the inter-frame gap and preamble of packets for the traffic shaping rate. As a result, the rate is inaccurate. After the **qos-shaping exclude-interframe** command is used, the device does not calculate the inter-frame gap and preamble of packets for the traffic shaping rate.

The **qos-shaping exclude-interframe** command affects calculation of the traffic shaping rate and outbound rate limit. When the **qos queue shaping** and **qos lr**

outbound commands are used to configure traffic shaping and outbound rate limiting, the device does not count the inter-frame gap and preamble for the traffic shaping rate.

Precautions

Before this command is used, the following formula is used to calculate the traffic shaping rate:

Traffic shaping rate = (Original packet length + Inter-frame gap + Preamble) x Number of packets forwarded per second

The inter-frame gap and preamble occupy 20 bytes.

After this command is used, the following formula is used to calculate the traffic shaping rate:

Traffic shaping rate = Original packet length x Number of packets forwarded per second

When the rate of the MultiGE interface on the S6720SI is 5 Gbit/s, the **qos-shaping exclude-interframe** command does not take effect.

Example

# Configure the device not to count the inter-frame gap and preamble of packets when the device calculates the traffic shaping rate.

```
<HUAWEI> system-view
[HUAWEI] qos-shaping exclude-interframe
```

Related Topics

15.3.17 qos queue shaping

15.3.15 qos lr outbound

15.3.14 qos lr inbound

Function

The **qos lr inbound** command configures traffic policing in the inbound direction on an interface.

The **undo qos lr inbound** command cancels traffic policing in the inbound direction on an interface.

By default, traffic policing is not configured in the inbound direction on an interface.

NOTE

The S2750EI, S5700-10P-LI-AC, and S5700-10P-PWR-LI-AC that are enabled with Layer 3 hardware forwarding for IPv4 packets do not support this command.

Format

qos lr inbound cir *cir-value* [**cbs** *cbs-value*]

undo qos lr inbound

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer, in kbit/s. The value range differs depending on the interface type: ● Ethernet: 64 to 100000 ● MultiGE: 64 to 2500000 ● GigabitEthernet: 64 to 1000000 ● XGigabitEthernet: 64 to 10000000 ● 40GigabitEthernet: 64 to 40000000 ● Port group: 64 to 10000000

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS).	The value is an integer that ranges from 4000 to 4294967295, in bytes. If this parameter is not specified, the default CBS is 125 times the CIR. On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, the maximum value of the CBS is 65535 granularities. Each granularity depends on the CIR: ● When the CIR is in the range of 64 kbit/s to 1023 kbit/s, each granularity is 1 byte. ● When the CIR is in the range of 1024 kbit/s to 10230 kbit/s, each granularity is 8 bytes. ● When the CIR is in the range of 10231 kbit/s to 102300 kbit/s, each granularity is 64 bytes. ● When the CIR is in the range of 102301 kbit/s to 1023000 kbit/s, each granularity is 512 bytes. ● When the CIR is in the range of 1023001 kbit/s to 10000000 kbit/s, each granularity is 4096 bytes.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When data is sent from a high-speed link to a low-speed link, the bandwidth on the interface of the low-speed link is insufficient. As a result, a large number of packets are discarded. In this case, the data traffic rate needs to be limited. After the traffic policing rate for incoming packets on an interface is set by using the **qos lr inbound** command, if the rate of packets received by the interface is larger than the traffic policing rate, the packets are discarded.

Precautions

When interface-based 802.1X authentication is configured and the RADIUS server delivers the rate limit, the interface does not support the rate limit.

If both the IPSG function and inbound interface-based rate limiting are configured on an interface of the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, both IPSG and interface-based rate-limiting configurations take effect as long as the configurations do not conflict. Otherwise, only the IPSG configuration takes effect.

The **traffic-limit (interface view)** command limits the rate of packets matching an ACL, whereas the **qos lr inbound** command limits the rate of all packets on an interface. If both of them are configured,

- On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, the **qos lr inbound** command takes effect.
- On the S5720EI, S6720EI, and S6720S-EI, rate limiting is inaccurate.
- On the S5720HI, the actual rate limit is the smaller CIR between CIR values configured by the two commands.

Configuring the **qos lr inbound** command occupies system resources. If system resources are insufficient, the configuration fails.

If you run the **qos lr inbound** command multiple times on the same interface, only the latest configuration takes effect.

If you need to set the same traffic policing rate on multiple interfaces, you can perform the configuration on a port group to reduce the workload.

Example

# Set the CIR of data packets received by the GE0/0/1 to 20000 kbit/s and the CBS to 375000 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos lr inbound cir 20000 cbs 375000
[HUAWEI-GigabitEthernet0/0/1] quit
```

Related Topics

15.3.17 qos queue shaping

15.3.8 display qos lr

15.3.15 qos lr outbound

Function

The **qos lr outbound** command configures traffic shaping in the outbound direction on an interface.

The **undo qos lr outbound** command cancels traffic shaping in the outbound direction on an interface.

By default, traffic shaping is not configured in the outbound direction on an interface.

Format

qos lr outbound cir *cir-value* [**cbs** *cbs-value*]

undo qos lr outbound

NOTE

The S5720HI does not support **cbs** *cbs-value*.

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer, in kbit/s. The value range differs depending on the interface type: ● Ethernet: 64 to 100000 ● MultiGE: 64 to 2500000 ● GigabitEthernet: 64 to 1000000 ● XGigabitEthernet: 64 to 10000000 ● 40GigabitEthernet: 64 to 40000000 ● Port group: 64 to 10000000
cbs *cbs-value*	Specifies the committed burst size (CBS).	The value is an integer that ranges from 4000 to 4294967295, in bytes. If this parameter is not specified, the default CBS is 125 times the CIR.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of data flows are sent from the upstream device to its downstream device, to prevent congestion or packet loss, run the **qos lr outbound** command to configure traffic shaping on the outbound interface of the device to limit the traffic and burst traffic transmitted over a connection so that packets are sent at an even rate.

Similar to traffic policing, traffic shaping limits the traffic rate. When traffic policing is used, the system directly discards the packets whose rate is larger than the traffic policing rate. Traffic shaping, however, buffers the packets whose rate is larger than the traffic shaping rate. When there are sufficient tokens in the token bucket, the device forwards buffered packets at an even rate. Traffic shaping increases the delay, whereas traffic policing does not.

Precautions

When interface-based 802.1X authentication is configured and the RADIUS server delivers the rate limit, the interface does not support the rate limit.

If you need to set the same traffic shaping rate on multiple interfaces, you can perform the configuration on a port group to reduce the workload.

If both traffic shaping and queue shaping (configured by using the **qos queue shaping** command) are configured on an interface, the CIR of traffic shaping cannot be lower than the sum of CIR values of all the queues on the interface; otherwise, the traffic shaping result may be incorrect. For example, the queue with a lower priority may occupy the bandwidth of the queue with a higher priority.

Traffic shaping increases the delay because it uses the buffer mechanism.

If you run the **qos lr outbound** command multiple times on the same interface, only the latest configuration takes effect.

After traffic shaping is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

On the S1720X, S1720X-E, S5730SI, S5730S-EI, S6720LI, S6720SI, S6720S-LI, and S6720S-SI, the **cbs** *cbs-value* parameter specified in the **qos lr outbound** command does not take effect and has a fixed value of 132000, in bytes.

On the S1720GFR, S1720GW-E, S1720GWR-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI, the maximum value of **cbs** *cbs-value* specified in the **qos lr outbound** command is 16380000, in bytes, even if the specified value is greater than 16380000.

Example

# Set the CIR of data packets sent by the GE0/0/1 to 20000 kbit/s and the CBS to 375000 bytes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos lr outbound cir 20000 cbs 375000
[HUAWEI-GigabitEthernet0/0/1] quit
```

Related Topics

15.3.17 qos queue shaping

15.3.8 display qos lr

15.3.16 qos lr pps

Function

The **qos lr pps** command sets the rate limit on the management interface.

The **undo qos lr pps** command restores the default rate limit on the management interface.

By default, the rate limit on the management interface is 1000 pps.

NOTE

Only the S1720X, S1720X-E, S5710-X-LI, S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

qos lr pps *packets*

undo qos lr

Parameters

Parameter	Description	Value
packets	Specifies the maximum number of packets that are allowed to pass per second.	The value is an integer that ranges from 1 to 2400, in pps.

Views

MEth interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If there is heavy traffic on the management interface caused by malicious attacks or network exceptions, the CPU is overloaded and services are interrupted. To prevent this problem, run the **qos lr pps** command to set the rate limit of packets on the management interface.

Configuration Impact

If a small rate limit is used, FTP and Telnet functions may be affected.

If you run the **qos lr pps** command multiple times on the same interface, only the latest configuration takes effect.

In a stack, only the management interface of the master switch can reach the value specified by the **qos lr pps** command.

Example

# Set the rate limit of MEth0/0/1 to 100 pps.

```
<HUAWEI> system-view
[HUAWEI] interface meth 0/0/1
[HUAWEI-MEth0/0/1] qos lr pps 100
```

15.3.17 qos queue shaping

Function

The **qos queue shaping** command enables traffic shaping for a queue on a specified interface and sets traffic shaping parameters.

The **undo qos queue shaping** command restores the default scheduling parameters of each queue on an interface.

The following table describes the default scheduling parameters on an interface.

Format

qos queue *queue-index* **shaping cir** *cir-value* **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]

undo qos queue *queue-index* **shaping**

NOTE

The S5720HI does not support **cir**, **cbs**, and **pbs**.

Parameters

Parameter	Description	Value
queue-index	Specifies the queue index.	The value is an integer that ranges from 0 to 7.

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR) of a queue.	The value is an integer, in kbit/s. The value range differs depending on the interface type: ● Ethernet: 0 to 100000 ● MultiGE: 0 to 2500000 ● GigabitEthernet: 0 to 1000000 ● 40GigabitEthernet: 0 to 40000000 ● XGigabitEthernet: 0 to 10000000 ● Port group: 0 to 10000000 The default value is the maximum bandwidth of an interface.
pir *pir-value*	Specifies the peak information rate (PIR) of a queue.	The value is an integer, in kbit/s. The value range differs depending on the interface type: ● Ethernet: 64 to 100000 ● MultiGE: 64 to 2500000 ● GigabitEthernet: 64 to 1000000 ● XGigabitEthernet: 64 to 10000000 ● 40GigabitEthernet: 64 to 40000000 ● Port group: 64 to 10000000 The default value is the maximum bandwidth of an interface. The PIR must be higher than or equal to the CIR. The default PIR is equal to the CIR.

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the traffic rate of an interface on a downstream device is lower than that of the connected interface on the upstream device, traffic congestion may occur on the interface of the downstream device. You can configure traffic shaping for queues on the outbound interface of the upstream device and adjust the transmit rate of the interface.

The **qos queue shaping** command configures traffic shaping on packets of a specific service on an interface.

Prerequisites

Priority mapping based on simple traffic classification has been configured to map packet priorities to PHBs and colors, or internal priority re-marking based on complex traffic classification has been configured so that packets of different services enter different queues.

Precautions

If traffic shaping is configured both on an interface queue and an interface (using the **qos lr outbound** command), the CIR of the interface cannot be lower than the sum of CIR values of all the queues on the interface; otherwise, traffic shaping result may be incorrect. For example, the queue with a lower priority may occupy the bandwidth of the queue with a higher priority.

It is recommended that the CBS be 120 times the CIR.

After traffic shaping is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

When interface queue shaping is configured on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, only *pir* and *pbs* take effect, and the maximum value of *pbs* is 16380000.

If you run the **qos queue shaping** command multiple times on the same interface, only the latest configuration takes effect.

Example

# Set the CIR of queue 4 on the GE0/0/1 to 10000 kbit/s and the PIR to 20000 kbit/s.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos queue 4 shaping cir 10000 pir 20000
[HUAWEI-GigabitEthernet0/0/1] quit
```

Related Topics

15.3.15 qos lr outbound

15.3.18 reset qos statistics

Function

The **reset qos statistics** command clears traffic statistics on an interface where rate limiting is performed in the inbound direction.

Format

reset qos statistics interface *interface-type interface-number* **inbound**

reset qos statistics inbound all

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears traffic statistics on a specified interface where rate limiting is performed. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Parameter	Description	Value
inbound	Clears traffic statistics in the inbound direction.	-
all	Clears traffic statistics on all interfaces where rate limiting is performed.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting traffic statistics on an interface where rate limiting is performed in the inbound direction, run the **reset qos statistics** command to clear existing traffic statistics. Then run the **display qos statistics** command to view the traffic statistics.

Prerequisites

The **qos lr inbound** command has been executed to configure rate limiting in the inbound direction on an interface.

Precautions

If the **qos lr inbound** command is not used, the system displays the following error message when you run the **reset qos statistics interface** *interface-type interface-number* **inbound** command:

```
Error: There is no rate limited configuration inbound in the interface.
```

The cleared statistics cannot be restored. Exercise caution when you use this command.

Example

# Clear traffic statistics on GE0/0/1 where rate limiting is performed in the inbound direction.

```
<HUAWEI> reset qos statistics interface gigabitethernet 0/0/1 inbound
```

Related Topics

15.3.14 qos lr inbound

15.3.9 display qos statistics

15.4 Congestion Avoidance and Congestion Management Commands

15.4.1 Command Support

For details about command support, see the description of each command. If no command support information is provided, all switch models support the command by default.

15.4.2 color

Function

The **color** command sets parameters of a WRED drop file, including the upper drop threshold, lower drop threshold, and maximum drop probability.

The **undo color** command restores the default settings of a WRED drop profile.

By default, the upper drop threshold, lower drop threshold, and maximum drop probability of a WRED drop profile are all 100.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

color { **green** | **non-tcp** | **red** | **yellow** } **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*

undo color { **green** | **non-tcp** | **red** | **yellow** }

NOTE

Only the S5720EI, S6720EI, and S6720S-EI support the **non-tcp** parameter.

Parameters

Parameter	Description	Value
green	Sets WRED parameters for green packets.	-
non-tcp	Sets WRED parameters for non-TCP packets.	-
red	Sets WRED parameters for red packets.	-
yellow	Sets WRED parameters for yellow packets.	-
low-limit *low-limit-percentage*	Specifies the lower drop threshold. When the percentage of the packet count in a queue to the queue length reaches this value, the switch starts to discard packets.	The value is an integer that ranges from 0 to 100, in percentage. The default value is 100.

Parameter	Description	Value
high-limit *high-limit-percentage*	Specifies the upper drop threshold. When the percentage of the packet count in a queue to the queue length reaches this value, the switch discards all subsequent packets.	The value is an integer that ranges from *low-limit-percentage* to 100, in percentage. The default value is 100.
discard-percentage *discard-percentage*	Specifies the maximum drop probability.	The value is an integer that ranges from 1 to 100, in percentage. The default value is 100.

Views

Drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets enter a switch, the switch colors packets based on the mappings defined in a DiffServ domain. The system processes the packets of different colors based on the WRED configuration:

- When the queue length reaches the lower drop threshold, the switch discards some packets.
- When the queue length reaches the upper drop threshold, the switch discards all subsequent packets in the queue.

When congestion occurs, the switch first discards packets with the highest drop probability.

Precautions

If you run the **color** command multiple times in the same drop profile view, only the latest configuration takes effect.

Example

# Configure WRED drop profile **wred1** in which the lower drop threshold, upper drop threshold, and maximum drop probability of green packets are set to 80, 100, and 10 for green packets, to 60, 80, and 20 for yellow packets, and to 40, 60, and 40 for red packets.

```
<HUAWEI> system-view
[HUAWEI] drop-profile wred1
```

```
[HUAWEI-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[HUAWEI-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[HUAWEI-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
```

Related Topics

15.4.5 drop-profile

15.4.3 display drop-profile

Function

The **display drop-profile** command displays the WRED drop profile configuration.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

display drop-profile [**all** | **name** *drop-profile-name*]

Parameters

Parameter	Description	Value
all	Displays detailed information about all WRED drop profiles.	-
name *drop-profile-name*	Displays detailed information about a WRED drop profile with the specified name.	The value must be the name of an existing WRED drop profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display drop-profile** command to view the number of configured WRED drop profiles and all configuration of a specified WRED drop profile.

Precautions

If the **all** and **name** *drop-profile-name* parameters are not specified, brief information about all WRED drop profiles is displayed.

Example

# Display brief information about all WRED drop profiles on the switch.

```
<HUAWEI> display drop-profile
        index                   drop-profile name
-------------------------------------------------------------------
        0                     default
        1                     dp1
-------------------------------------------------------------------
 Total   64     Used   2
```

# Display detailed information about the WRED drop profile named **dp1**.

```
<HUAWEI> display drop-profile name dp1
Drop-profile[1]: dp1
Queue depth    : default
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     60          90          20
Yellow    100         100         100
Red       100         100         100
Non-tcp   100         100         100
-------------------------------------------------------------------
```

# Display detailed information about all WRED drop profiles on the switch.

```
<HUAWEI> display drop-profile all
Drop-profile[0]: default
Queue depth    : default
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     100         100         100
Yellow    100         100         100
Red       100         100         100
Non-tcp   100         100         100
-------------------------------------------------------------------
Drop-profile[1]: dp1
Queue depth    : default
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     60          90          20
Yellow    100         100         100
Red       100         100         100
Non-tcp   100         100         100
-------------------------------------------------------------------
```

Table 15-28 Description of the **display drop-profile** command output

Item	Description
index	WRED drop profile index.
drop-profile name	WRED drop profile name. To configure a WRED drop profile, run the **drop-profile** command.
Queue depth	Length of a queue. To configure the length of a queue, run the **queue-depth (WRED drop profile view)** command. **NOTE** Only the S5720HI supports this field.

Item	Description
Total	Total number of WRED drop profiles that can be configured on the switch.
Used	Number of configured WRED drop profiles.
Drop-profile[1]	WRED drop profile name in which 1 indicates the drop profile index.
Color	Color of packets: ● Green ● Yellow ● Red ● Non-tcp To set the color of packets, run the **color** command.
Low-limit	Lower drop threshold, in percentage. To set the lower drop threshold, run the **color** command.
High-limit	Upper drop threshold, in percentage. To set the upper drop threshold, run the **color** command.
Discard-percentage	Maximum drop probability, in percentage. To set the maximum drop probability, run the **color** command.

Related Topics

15.4.5 drop-profile

15.4.2 color

15.4.4 display qos queue statistics

Function

The **display qos queue statistics** command displays queue-based traffic statistics on an interface.

Format

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

display qos queue statistics all

Parameters

Parameter	Description	Value
queue *queue-index*	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
interface *interface-type interface-number*	Displays queue-based traffic statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
all	Displays queue-based traffic statistics on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check whether packets in each queue on an interface are forwarded or discarded due to congestion, run this command to check statistics on each queue on the interface.

Example

# Display queue-based traffic statistics on the GE0/0/1 on the S5720EI, S5720HI, S6720EI, and S6720S-EI.

```
<HUAWEI> display qos queue statistics interface gigabitethernet 0/0/1
------------------------------------------------------------
 Queue ID          : 0
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
```

```
---------------------------------------------------------
 Queue ID          : 1
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
---------------------------------------------------------
 Queue ID          : 2
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
---------------------------------------------------------
 Queue ID          : 3
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
---------------------------------------------------------
 Queue ID          : 4
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
---------------------------------------------------------
 Queue ID          : 5
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Used Length(byte) : 239,104
 Passed Packets    : 47,655,381
 Passed Rate(pps)  : 128
 Passed Bytes      : 4,956,144,598
 Passed Rate(bps)  : 106,976
 Dropped Packets   : 47,655,381
 Dropped Rate(pps) : 128
 Dropped Bytes     : 4,956,144,598
 Dropped Rate(bps) : 106,976
---------------------------------------------------------
 Queue ID          : 6
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
```

```
  Used Length(byte) : 239,104
  Passed Packets    : 47,655,381
  Passed Rate(pps)  : 128
  Passed Bytes      : 4,956,144,598
  Passed Rate(bps)  : 106,976
  Dropped Packets   : 47,655,381
  Dropped Rate(pps) : 128
  Dropped Bytes     : 4,956,144,598
  Dropped Rate(bps) : 106,976
----------------------------------------------------------
  Queue ID          : 7
  CIR(kbps)         : 0
  PIR(kbps)         : 1,000,000
  Used Length(byte) : 239,104
  Passed Packets    : 47,655,381
  Passed Rate(pps)  : 128
  Passed Bytes      : 4,956,144,598
  Passed Rate(bps)  : 106,976
  Dropped Packets   : 47,655,381
  Dropped Rate(pps) : 128
  Dropped Bytes     : 4,956,144,598
  Dropped Rate(bps) : 106,976
----------------------------------------------------------
```

Table 15-29 Description of the **display qos queue statistics** command output (S5720EI, S5720HI, S6720EI, S6720S-EI)

Item	Description
Queue ID	Queue index.
CIR(kbps)	Committed information rate (CIR). By default, the CIR is displayed as 0. If the CIR is configured for queue shaping, the configured CIR is displayed. To set the CIR, run the **qos queue shaping** command.
PIR(kbps)	Peak information rate (PIR). By default, the PIR is displayed as 1000000. If the PIR is configured for queue shaping, the configured PIR is displayed. To set the PIR, run the **qos queue shaping** command.
Used Length(byte)	Maximum number of bytes to be cached in a queue on an interface.
Passed Packets	Number of forwarded packets.
Passed Rate(pps)	Rate of forwarded packets, in pps.
Passed Bytes	Number of forwarded bytes.
Passed Rate(bps)	Rate of forwarded bytes, in bit/s.
Dropped Packets	Number of discarded packets.

Item	Description
Dropped Rate(pps)	Rate of discarded packets, in pps.
Dropped Bytes	Number of discarded bytes.
Dropped Rate(bps)	Rate of discarded bytes, in bit/s.

# Display queue-based traffic statistics on GE0/0/1 on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI.

```
<HUAWEI> display qos queue statistics interface gigabitethernet 0/0/1
------------------------------------------------------------
 Queue ID          : 0
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
------------------------------------------------------------
 Queue ID          : 1
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
------------------------------------------------------------
 Queue ID          : 2
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
------------------------------------------------------------
 Queue ID          : 3
 CIR(kbps)         : 0
 PIR(kbps)         : 1,000,000
 Passed Packets    : 0
 Passed Rate(pps)  : 0
 Passed Bytes      : 0
 Passed Rate(bps)  : 0
 Dropped Packets   : 0
 Dropped Rate(pps) : 0
 Dropped Bytes     : 0
 Dropped Rate(bps) : 0
------------------------------------------------------------
 Queue ID          : 4
 CIR(kbps)         : 0
 PIR(kbps)          : 1,000,000
 Passed Packets     : 0
 Passed Rate(pps)   : 0
 Passed Bytes       : 0
 Passed Rate(bps)   : 0
 Dropped Packets    : 0
 Dropped Rate(pps)  : 0
 Dropped Bytes      : 0
 Dropped Rate(bps)  : 0
-----------------------------------------------------------------
 Queue ID           : 5
 CIR(kbps)          : 0
 PIR(kbps)          : 1,000,000
 Passed Packets     : 0
 Passed Rate(pps)   : 0
 Passed Bytes       : 0
 Passed Rate(bps)   : 0
 Dropped Packets    : 0
 Dropped Rate(pps)  : 0
 Dropped Bytes      : 0
 Dropped Rate(bps)  : 0
-----------------------------------------------------------------
 Queue ID           : 6
 CIR(kbps)          : 0
 PIR(kbps)          : 1,000,000
 Passed Packets     : 6
 Passed Rate(pps)   : 0
 Passed Bytes       : 3,042
 Passed Rate(bps)   : 0
 Dropped Packets    : 0
 Dropped Rate(pps)  : 0
 Dropped Bytes      : 0
 Dropped Rate(bps)  : 0
-----------------------------------------------------------------
 Queue ID           : 7
 CIR(kbps)          : 0
 PIR(kbps)          : 1,000,000
 Passed Packets     : 0
 Passed Rate(pps)   : 0
 Passed Bytes       : 0
 Passed Rate(bps)   : 0
 Dropped Packets    : 0
 Dropped Rate(pps)  : 0
 Dropped Bytes      : 0
 Dropped Rate(bps)  : 0
-----------------------------------------------------------------
```

Table 15-30 Description of the **display qos queue statistics** command output (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

Item	Description
Queue ID	Queue index.
CIR(kbps)	Committed information rate (CIR). By default, the CIR that is displayed as 0. If the CIR is configured for queue shaping, the configured CIR is displayed. To set the CIR, run the **qos queue shaping** command.

Item	Description
PIR(kbps)	Peak information rate (PIR). By default, the PIR that is displayed as 1000000. If the PIR is configured for queue shaping, the configured PIR is displayed. To set the PIR, run the **qos queue shaping** command.
Passed Packets	Number of forwarded packets.
Passed Rate(pps)	Rate of forwarded packets, in pps.
Passed Bytes	Number of forwarded bytes.
Passed Rate(bps)	Rate of forwarded bytes, in bit/s.
Dropped Packets	Number of discarded packets.
Dropped Rate(pps)	Rate of discarded packets, in pps.
Dropped Bytes	Number of discarded bytes.
Dropped Rate(bps)	Rate of discarded bytes, in bit/s.

Related Topics

15.4.23 reset qos queue statistics

15.3.17 qos queue shaping

15.4.5 drop-profile

Function

The **drop-profile** command creates a WRED drop profile and displays the WRED drop profile view, or displays the existing WRED drop profile view.

The **undo drop-profile** command deletes a WRED drop profile.

By default, the system provides a WRED drop profile named **default**.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

drop-profile *drop-profile-name*

undo drop-profile *drop-profile-name*

Parameters

Parameter	Description	Value
drop-profile-name	Specifies the name of a WRED drop profile.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A WRED drop profile defines WRED parameters for packets of different priorities. After the WRED drop profile is applied to an interface or queues on an interface, congestion avoidance is implemented. The **drop-profile** command creates a WRED drop profile or displays the WRED drop profile view.

Precautions

The S5720HI supports a maximum of 16 WRED drop profiles, and other switches support a maximum of 64 WRED drop profiles, including the default drop profile. The default drop profile can be modified but cannot be deleted.

Follow-up Procedure

1. Set parameters for the WRED drop profile.

   Run the **color** command in the WRED drop profile view to set WRED parameters for packets of different priorities.
2. Apply the WRED drop profile to an interface or queues on an interface.

Example

# Create a WRED drop profile named **drop1** and enter the WRED drop profile view.

```
<HUAWEI> system-view
[HUAWEI] drop-profile drop1
[HUAWEI-drop-drop1]
```

Related Topics

15.4.3 display drop-profile

15.4.6 qos burst-mode (interface view)

Function

The **qos burst-mode** command configures a burst traffic buffering mode on an interface.

The **undo qos burst-mode** command restores the default burst traffic buffering mode on an interface.

By default, an interface uses the standard mode.

NOTE

Only the S5720EI, S6720EI, and S6720S-EI support this command.

Format

qos burst-mode { **enhanced** | **extreme** }

undo qos burst-mode { **enhanced** | **extreme** }

Parameters

Parameter	Description	Value
enhanced	Indicates the enhanced burst traffic buffering mode.	-
extreme	Indicates the extreme burst traffic buffering mode.	-

Views

GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Scenario

By default, the buffer size on an interface is small. When the traffic rate on an interface reaches 50% to 60% of the interface bandwidth, packets are lost on the interface. The burst traffic buffering mode enables an interface to occupy more available buffer space in the system to process burst traffic, improving a switch's packet processing performance.

The device buffer is allocated in static and dynamic modes. By default, each interface is allocated some static buffer space for the basic buffer requirement. The remaining buffer space is used as the dynamic buffer for a switch.

In standard mode, an interface can occupy only some dynamic buffer space on the switch.

In enhanced mode, an interface can occupy only some dynamic buffer space on the switch, and more dynamic buffer space than that in standard mode.

In extreme mode, an interface occupies the dynamic buffer space as well as static buffer space on interfaces in non-extreme mode.

Precautions

The **qos burst-mode (interface view)** and **qos queue buffer shared-ratio** commands cannot be used on the same interface.

When the enhanced mode is used, the **qos burst-mode (interface view)** and **qos burst-mode (system view)** commands cannot be used together.

The **extreme** mode is not recommended because forwarding of other interfaces may be affected and QoS results such as scheduling and shaping results may be incorrect.

The **extreme** mode is used only when the switch uses one or two interfaces. This mode takes effect only when it is configured globally and on an interface. If the **extreme** mode is configured globally but is not configured on an interface, traffic forwarding may be abnormal and multicast packets may fail to be obtained. If the **extreme** mode is configured on an interface but is not configured globally, the **extreme** mode does not take effect.

When the **extreme** mode is configured globally, the interface where the **extreme** mode is not configured cannot be used as a service interface.

Example

# Configure the enhanced burst traffic buffering mode on the GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos burst-mode enhanced
```

Related Topics

15.4.7 qos burst-mode (system view)

15.4.7 qos burst-mode (system view)

Function

The **qos burst-mode** command configures a burst traffic buffer mode on a switch.

The **undo qos burst-mode** command restores the default burst traffic buffer mode on a switch.

By default, the switch uses the standard mode.

NOTE

Only the S5720EI, S6720EI, and S6720S-EI support this command.

Format

qos burst-mode { **enhanced** | **extreme** } **slot** *slot-id*

undo qos burst-mode { **enhanced** | **extreme** } **slot** *slot-id*

Parameters

Parameter	Description	Value
enhanced	Indicates the enhanced burst traffic buffer mode.	-
extreme	Indicates the extreme burst traffic buffer mode.	-
slot *slot-id*	The default value of *slot-id* is 0 on a non-stacked switch. *slot-id* specifies the stack ID.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

By default, the buffer size on an interface is small. When the traffic rate on an interface reaches 50% to 60% of the interface bandwidth, packets are lost on the interface. After the burst traffic buffer mode is configured on a switch, all interfaces on the switch can occupy more buffer space in the system to process burst traffic, improving a switch's packet processing performance.

The device buffer is allocated in static and dynamic modes. By default, each interface is allocated some static buffer space for the basic buffer requirement. The remaining buffer space is used as the dynamic buffer for a switch.

In standard mode, an interface can occupy only some dynamic buffer space on the switch.

In enhanced mode, an interface can occupy only some dynamic buffer space on the switch, and more dynamic buffer space than that in standard mode.

In extreme mode, an interface occupies the dynamic buffer space as well as static buffer space on interfaces in non-extreme mode.

Precautions

The **qos burst-mode (system view)** and **qos queue buffer shared-ratio** commands cannot be used on the switch simultaneously.

The **extreme** mode is not recommended because forwarding of other interfaces may be affected and QoS results such as scheduling and shaping results may be incorrect.

The **extreme** mode is used only when the switch uses one or two interfaces. This mode takes effect only when it is configured globally and on an interface. If the **extreme** mode is configured globally but is not configured on an interface, traffic forwarding may be abnormal and multicast packets may fail to be obtained. If the **extreme** mode is configured on an interface but is not configured globally, the **extreme** mode does not take effect.

When the **extreme** mode is configured globally, the interface where the **extreme** mode is not configured cannot be used as a service interface.

Example

# Configure the enhanced burst traffic buffer mode in slot 0.

```
<HUAWEI> system-view
[HUAWEI] qos burst-mode enhanced slot 0
```

Related Topics

15.4.6 qos burst-mode (interface view)

15.4.8 qos { pq | wrr | drr }

Function

The **qos** { **pq** | **wrr** | **drr** } command configures a scheduling mode for queues on an interface.

The **undo qos** { **pq** | **wrr** | **drr** } command restores the default scheduling mode of queues on an interface.

By default, the scheduling mode of queues on an interface of the S5720HI is WDRR, and the scheduling mode of queues on an interface of other models is WRR.

Format

qos { **pq** | **wrr** | **drr** }

undo qos { **pq** | **wrr** | **drr** }

NOTE

The S5720HI does not support **wrr**.

Parameters

Parameter	Description	Value
pq	Indicates the PQ scheduling mode.	-
wrr	Indicates the WRR scheduling mode.	-
drr	Indicates the WDRR scheduling mode.	-

Views

GE interface view, XGE interface view, 40GE interface view, port group view (S5720EI, S5720HI, S6720EI, S6720S-EI)

Scheduling profile view (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When congestion occurs on a network, configure a combination of queue scheduling modes to adjust the delay and jitter of various service packets as follows:

- Packets of delay-sensitive services, such as the voice and video services, are processed preferentially.
- Among the delay-insensitive services, such as the email service, the packets with the same priority are processed equally and the packets with different priorities are processed based on their weights.

The switch supports PQ+WRR and PQ+WDRR. When a combination of queue scheduling modes is used, the switch first schedules the packets in queues using PQ scheduling. When all packets in the queues using PQ scheduling are sent out, the switch schedules the packets in queues using WRR or WDRR scheduling. Packets from the queues using PQ scheduling are scheduled based on packet priorities.

Precautions

- Before configuring a queue scheduling mode, map packet priorities to PHBs and colors or re-mark local priorities of packets. The packets of different priorities enter different queues.

- To set the same queue scheduling mode on multiple interfaces, perform the configuration on a port group to reduce the workload.
- When the scheduling mode of queues on an interface is set to PQ+WRR or PQ+WDRR, a queue can use only one scheduling mode. If you set multiple scheduling modes for a queue, only the latest configuration takes effect.
- If the queue scheduling mode is set to WDRR or WRR on an interface on the S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI, other interfaces on the switch use the same queue scheduling mode as this interface.
- On the S5730SI, S5730S-EI, S6720SI, and S6720S-SI, the WRR scheduling changed from WDRR scheduling takes effect only after the switch runs for a period with traffic transmitted.

Example

# Set the scheduling mode of queues on GE0/0/1 of the S5720HI to PQ.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos pq
```

# Set the scheduling mode of queues on GE0/0/1 of the S5700LI to WDRR.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test] qos drr
[HUAWEI-qos-schedule-profile-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos schedule-profile test
```

Related Topics

15.4.10 qos queue drr

15.4.15 qos queue wrr

15.4.16 qos schedule-profile (interface view)

15.4.17 qos schedule-profile (system view)

15.4.9 qos queue buffer shared-ratio

Function

The **qos queue buffer shared-ratio** command sets the maximum ratio of the dynamic buffer occupied by a queue on an interface.

The **undo qos queue buffer shared-ratio** command restores the default maximum ratio of the dynamic buffer occupied by a queue on an interface.

By default, the maximum ratio of the dynamic buffer occupied by a queue on an interface of the S5720EI is 50%, and the maximum ratio of the dynamic buffer occupied by a queue on an interface of the S6720EI and S6720S-EI is 20%.

NOTE

Only the S5720EI, S6720EI, and S6720S-EI support this command.

Format

qos queue *queue-index* **buffer shared-ratio** *ratio-value*

undo qos queue *queue-index* **buffer shared-ratio**

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
ratio-value	Specifies the maximum ratio of the dynamic buffer occupied by a queue on an interface, in percentage.	The value is an integer that ranges from 1 to 90. ● The default value on the S5720EI is 50. ● The default value on the S6720EI and S6720S-EI is 20.

Views

GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the buffer of an interface is small. When the traffic rate on an interface reaches 50% to 60% of the interface bandwidth, packets are lost on the interface. The switch uses static and dynamic modes to allocate the buffer. The switch allocates specified static buffer to each interface, and the remaining buffer is used as the dynamic buffer. When there is heavy burst traffic in a queue on an interface, you can run the **qos queue buffer shared-ratio** command to increase the maximum ratio of the dynamic buffer occupied by the queue. The switch allocates larger dynamic buffer to the queue to reduce packet loss on the queue.

Precautions

The available dynamic buffer on each interface is limited. When a queue on an interface occupies more dynamic buffer, there is less dynamic buffer that can be occupied by other queues on the interface. As a result, the queues' capability to forward burst traffic is lowered.

The **qos queue buffer shared-ratio** and **qos burst-mode (system view)** commands cannot be configured on the switch simultaneously.

The **qos queue buffer shared-ratio** and **qos burst-mode (interface view)** commands cannot be configured on the same interface simultaneously.

Example

# Set the maximum ratio of the dynamic buffer occupied by queue 3 on the GE0/0/1 to 35%.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos queue 3 buffer shared-ratio 35
```

15.4.10 qos queue drr

Function

The **qos queue drr** command sets the WDRR weight of queues that participate in WDRR scheduling.

The **undo qos queue drr** command restores the default WDRR weight of queues that participate in WDRR scheduling.

By default, the WDRR weight of queues that participate in WDRR scheduling is 1.

Format

qos queue *queue-index* **drr weight** *weight*

undo qos queue *queue-index* **drr**

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
weight *weight*	Specifies a WDRR weight.	The value is an integer. The value range is as follows: ● S5720EI: 0 to 63 ● Other models: 0 to 127

Views

GE interface view, XGE interface view, 40GE interface view, port group view (S5720EI, S5720HI, S6720EI, S6720S-EI)

Scheduling profile view (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WDRR schedules packets based on the packet length used as the weight. If the packet length is too long, WDRR allows the negative weight value so that long packets can be scheduled. In the next round, the queue with the negative weight value is not scheduled until its weight value becomes positive.

WDRR offsets the disadvantages of PQ scheduling and WRR scheduling. In PQ scheduling, packets in queues with lower priorities cannot be scheduled for a long time if congestion occurs. In WRR scheduling, bandwidth is allocated improperly when the packet length of each queue is different or variable.

When WDRR scheduling is used, set the weight for each queue. The switch schedules queues in turn according to the weights.

Precautions

When WDRR scheduling is applied and the weight of a queue is set to 0, the queue uses PQ scheduling and the scheduling mode is PQ+WDRR.

For the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI:

- When configuring the PQ+WDRR scheduling mode, ensure that queues with weight 0 (queues using PQ scheduling) are consecutively configured, without being interrupted by the configuration of the queues using WDRR scheduling.
- If PQ+WDRR scheduling is used and the numbers of the queues using PQ scheduling are consecutive (for example, queue 0, queues 0 and 1, and queues 0 to 2), the device schedules packets in queues using PQ scheduling after scheduling for the packets in queues using WDRR scheduling is completed.

On the S5720EI, if the queue scheduling mode is changed or the weight is changed during queue scheduling, packet loss occurs within 250 ms.

On the S6720EI and S6720S-EI, if the queue scheduling mode is changed or the weight is changed during queue scheduling, packet loss occurs within 20 ms.

To set the same WDRR weight on multiple interfaces, perform the configuration on a port group to reduce the workload.

Example

# Set the WDRR weight of queue 4 on GE0/0/1 of the S5720HI to 9.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos drr
[HUAWEI-GigabitEthernet0/0/1] qos queue 4 drr weight 9
```

# Set the WDRR weight of queue 4 on GE0/0/1 of the S5700LI to 9.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test] qos drr
[HUAWEI-qos-schedule-profile-test] qos queue 4 drr weight 9
[HUAWEI-qos-schedule-profile-test] quit
```

```
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos schedule-profile test
```

Related Topics

15.4.8 qos { pq | wrr | drr }

15.4.16 qos schedule-profile (interface view)

15.4.17 qos schedule-profile (system view)

15.4.11 qos queue max-buffer

Function

The **qos queue max-buffer** command sets the maximum number of bytes in all packets to be cached in a queue.

The **undo qos queue max-buffer** command restores the default maximum number of bytes in all packets to be cached in a queue.

The **qos queue green max-buffer** command sets the maximum number of bytes in green packets to be cached in a queue.

The **undo qos queue green max-buffer** command restores the default maximum number of bytes in green packets to be cached in a queue.

By default, on the S2750EI and S5700-10P-LI, the maximum buffer size of green packets in a queue is 1920 and the maximum buffer size of other packets in a queue is 1920, in cells. The size of a cell is 128 bytes.

By default, on other models, the maximum buffer size of all packets in a queue is 24 and the maximum buffer size of green packets in a queue is 12, in cells. The size of a cell is 128 bytes.

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this command.

Format

qos queue *queue-index* **green max-buffer** *cell-number* **non-green max-buffer** *cell-number* (S2750EI, S5700-10P-LI)

undo qos queue *queue-index* **green max-buffer** [*cell-number*] **non-green max-buffer** [*cell-number*] (S2750EI, S5700-10P-LI)

qos queue *queue-index* **max-buffer** *cell-number* [**green max-buffer** *cell-number*] (other models except the S2750EI and S5700-10P-LI)

undo qos queue *queue-index* **max-buffer** [*cell-number* **green max-buffer** *cell-number* | **green max-buffer**] (other models except the S2750EI and S5700-10P-LI)

qos queue *queue-index* **green max-buffer** *cell-number* (other models except the S2750EI and S5700-10P-LI)

undo qos queue *queue-index* **green max-buffer** (other models except the S2750EI and S5700-10P-LI)

Parameters

Parameter	Description	Value
queue *queue-index*	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
max-buffer *cell-number*	Specifies the maximum number of bytes in all packets to be cached in a queue.	The value is an integer, in cells. The value range is as follows: ● S1720GFR, S1720GW-E, S1720GWR-E, S1720GW, S1720GWR, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI: from 1 to 5444. ● S1720X, S1720X-E, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI: from 1 to 10000. The size of a cell is 128 bytes.
green max-buffer *cell-number*	Specifies the maximum number of bytes in green packets to be cached in a queue.	The value is an integer, in cells. The value range is as follows: ● S2750EI and S5700-10P-LI: from 1920 to 3100. ● S1720X, S1720X-E, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI: from 1 to 10000. ● Other models except the S2750EI, S5700-10P-LI, S1720X, S1720X-E, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI: from 1 to 5444. The size of a cell is 128 bytes.

Parameter	Description	Value
non-green max-buffer *cell-number*	Specifies the maximum number of bytes in non-green packets to be cached in a queue.	The value is an integer that ranges from 1920 to 3100, in cells. The size of a cell is 128 bytes.

Views

Tail drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When congestion occurs, the switch uses the tail drop method. When the queue length reaches the upper limit, excess packets (buffered at the queue tail) are discarded until congestion is removed. You can run the **qos queue max-buffer** command to set the maximum number of bytes in all packets or green packets to be cached in a queue so that the queue has sufficient buffer, preventing packet loss.

Prerequisites

A tail drop profile has been created using the **qos tail-drop-profile (system view)** command.

Precautions

You can also use the **qos queue max-length** command to set the maximum number of packets to be cached in a queue. If the maximum number of bytes or packets is reached, the device considers that congestion occurs and will discard subsequent packets.

Example

# Create a global tail drop profile named **test**, and then set the maximum buffer size of all packets in a BE queue for the global tail drop profile to 100, in cells.

```
<HUAWEI> system-view
[HUAWEI] qos tail-drop-profile test
[HUAWEI-tail-drop-profile-test] qos queue 0 max-buffer 100
```

Related Topics

15.4.12 qos queue max-length

15.4.19 qos tail-drop-profile (system view)

15.4.12 qos queue max-length

Function

The **qos queue max-length** command sets the maximum number of packets allowed in a queue.

The **undo qos queue max-length** command restores the default maximum number of packets allowed in a queue.

The **qos queue green max-length** command sets the maximum number of green packets allowed in a queue.

The **undo qos queue green max-length** command restores the default maximum number of green packets allowed in a queue.

By default, on the S2750EI and S5700-10P-LI, the maximum buffer size of green packets in a queue is 1280 and the maximum buffer size of other packets in a queue is 1280, in packets.

By default, on other models, the maximum buffer size of all packets in a queue is 22 and the maximum buffer size of green packets in a queue is 11, in packets.

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this command.

Format

qos queue *queue-index* **green max-length** *packet-number* **non-green max-length** *packet-number* (S2750EI, S5700-10P-LI)

undo qos queue *queue-index* **green max-length** [*packet-number*] **non-green max-length** [*packet-number*] (S2750EI, S5700-10P-LI)

qos queue *queue-index* **max-length** *packet-number* [**green max-length** *packet-number*] (other models except the S2750EI and S5700-10P-LI)

undo qos queue *queue-index* **max-length** [*packet-number* **green max-length** *packet-number* | **green max-length**] (other models except the S2750EI and S5700-10P-LI)

qos queue *queue-index* **green max-length** *packet-number* (other models except the S2750EI and S5700-10P-LI)

undo qos queue *queue-index* **green max-length** (other models except the S2750EI and S5700-10P-LI)

Parameters

Parameter	Description	Value
queue *queue-index*	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.

Parameter	Description	Value
max-length *packet-number*	Specifies the maximum number of packets allowed in a queue.	The value is an integer, in packets. The value range is as follows: ● S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI: from 1 to 5134. ● S1720X, S1720X-E, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI: from 1 to 10000.
green max-length *packet-number*	Specifies the maximum number of green packets to be cached in a queue.	The value is an integer, in packets. The value range is as follows: ● S2750EI and S5700-10P-LI: from 1280 to 3000. ● S1720X, S1720X-E, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI: from 1 to 10000. ● Other models except the S2750EI, S5700-10P-LI, S1720X, S1720X-E, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI: from 1 to 5134.
non-green max-length *packet-number*	Specifies the maximum number of non-green packets to be cached in a queue.	The value is an integer that ranges from 1280 to 3000, in packets.

Views

Tail drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When congestion occurs, the switch uses the tail drop method. When the queue length reaches the upper limit, excess packets (buffered at the queue tail) are discarded until congestion is removed. You can run the **qos queue max-length** command to set the maximum number of packets to be cached in a specified queue on an interface so that the queue has sufficient buffer, preventing packet loss.

Prerequisites

A tail drop profile has been created using the **qos tail-drop-profile (system view)** command.

Precautions

You can also run the **qos queue max-buffer** command to set the maximum number of bytes in all packets to be cached in a queue. If the maximum number of bytes or packets is reached, the device considers that congestion occurs and will discard subsequent packets.

Example

# Create a global tail drop template named **test** and set the maximum number of packets to be cached in queue 0 for the global tail drop template to 200.

```
<HUAWEI> system-view
[HUAWEI] qos tail-drop-profile test
[HUAWEI-tail-drop-profile-test] qos queue 0 max-length 200
```

Related Topics

15.4.11 qos queue max-buffer

15.4.19 qos tail-drop-profile (system view)

15.4.13 qos queue statistics interval

Function

The **qos queue statistics interval** command sets the interval for checking the rate of discarded packets in a queue.

The **undo qos queue statistics interval** command restores the default interval.

By default, the rate of discarded packets in a queue is checked every 300 seconds.

Format

qos queue statistics interval *interval-value*

undo qos queue statistics interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval for checking the rate of discarded packets in a queue.	The value is an integer that ranges from 60 to 600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the switch is managed by a network management system (NMS), the MIB module checks the rate of discarded packets in each queue at intervals and sends the rate to the NMS. You can view the rate of discarded packets in each queue to analyze network performance or locate faults. The **qos queue statistics interval** command sets the interval. The MIB module calculates the average rate at which packets in a queue is discarded at an interval.

Example

# Set the interval for checking the rate of discarded packets in a queue to 100 seconds.

```
<HUAWEI> system-view
[HUAWEI] qos queue statistics interval 100
```

15.4.14 qos queue wred

Function

The **qos queue wred** command applies a Weighted Random Early Detection (WRED) drop profile to the system or an interface queue.

The **undo qos queue wred** command deletes a WRED drop profile from the system or an interface queue.

By default, no WRED drop profile is applied to the system or an interface queue.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

qos queue *queue-index* **wred** *drop-profile-name*

undo qos queue *queue-index* **wred**

Parameters

Parameter	Description	Value
queue *queue-index*	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
drop-profile-name	Specifies the name of a WRED drop profile.	The value must be the name of an existing WRED drop profile.

Views

System view, GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Tail drop technology processes all packets in the same manner without classifying the packets. When the queue length reaches its maximum value, the packets that were added last (at the tail of the queue) are discarded. This packet drop policy may cause global TCP synchronization. As a result, TCP connections cannot be set up.

Random Early Detection (RED) and WRED are used to avoid global TCP synchronization.

RED and WRED randomly discard packets to prevent global TCP synchronization. When packets of a TCP connection are discarded, packets of other TCP connections can still be sent at a high rate, ensuring bandwidth use efficiency.

Prerequisites

A WRED drop profile has been created using the **drop-profile** command.

Precautions

On the switch, you can apply a WRED drop profile to an interface, the system, or a queue on an interface.

If a WRED drop profile is applied to the system and an interface simultaneously, the WRED drop profile applied to the interface takes effect. After a WRED drop profile is applied to the system, it takes effect on all the interfaces.

If you apply a WRED drop profile to an interface and a queue on an interface simultaneously, the system matches the packets with the profiles applied to the queue and interface in sequence. Then the switch performs congestion avoidance on the packets that match the WRED drop profile.

To apply the same WRED drop profile to queues with the same index on multiple interfaces, perform the configuration on a port group to reduce the workload.

Example

# Create a WRED drop profile named **wred1** and apply it to queue 1 on the GE0/0/1.

```
<HUAWEI> system view
[HUAWEI] drop-profile wred1
[HUAWEI-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[HUAWEI-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[HUAWEI-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
[HUAWEI-drop-wred1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos queue 1 wred wred1
```

Related Topics

15.4.5 drop-profile

15.4.2 color

15.4.15 qos queue wrr

Function

The **qos queue wrr** command sets the WRR weight of queues that participate in WRR scheduling.

The **undo qos queue wrr** command restores the default WRR weight of queues that participate in WRR scheduling.

By default, the WRR weight of queues that participate in WRR scheduling is 1.

Format

qos queue *queue-index* **wrr weight** *weight*

undo qos queue *queue-index* **wrr**

NOTE

The S5720HI does not support this command.

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.

Parameter	Description	Value
weight *weight*	Specifies a WRR weight.	The value is an integer. The value range is as follows: ● S5720EI: 0 to 63 ● Other models: 0 to 127

Views

GE interface view, XGE interface view, 40GE interface view, port group view (S5720EI, S6720EI, S6720S-EI)

Scheduling profile view (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Weighted Round Robin (WRR) ensures that packets in all the queues are scheduled in turn.

When using WRR scheduling, set the weight for each queue. The switch schedules queues in turn according to the weights.

Precautions

When WRR scheduling is applied and the weight of a queue is set to 0, the queue uses PQ scheduling and the scheduling mode is PQ+WRR.

For the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI:

- When configuring the PQ+WRR scheduling mode, ensure that queues with weight 0 (queues using PQ scheduling) are consecutively configured, without being interrupted by the configuration of the queues using WRR scheduling.
- If PQ+WRR scheduling is used and the numbers of the queues using PQ scheduling are consecutive (for example, queue 0, queues 0 and 1, and queues 0 to 2), the device schedules packets in queues using PQ scheduling after scheduling for the packets in queues using WRR scheduling is completed.

On the S5720EI, if the queue scheduling mode is changed or the weight is changed during queue scheduling, packet loss occurs within 250 ms.

On the S6720EI and S6720S-EI, if the queue scheduling mode is changed or the weight is changed during queue scheduling, packet loss occurs within 20 ms.

To set the same WRR weight on multiple interfaces, perform the configuration on a port group to reduce the workload.

Example

# Set the WRR weight of queue 4 on GE0/0/1 of the S5700LI to 9.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test] qos wrr
[HUAWEI-qos-schedule-profile-test] qos queue 4 wrr weight 9
[HUAWEI-qos-schedule-profile-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos schedule-profile test
[HUAWEI-GigabitEthernet0/0/1] quit
```

Related Topics

15.4.8 qos { pq | wrr | drr }

15.4.16 qos schedule-profile (interface view)

15.4.17 qos schedule-profile (system view)

15.4.16 qos schedule-profile (interface view)

Function

The **qos schedule-profile** command applies a global scheduling profile to an interface.

The **undo qos schedule-profile** command deletes a global scheduling profile from an interface.

By default, no global scheduling profile is applied to an interface.

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this command.

Format

qos schedule-profile *profile-name*

undo qos schedule-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a scheduling profile.	The value must be the name of an existing scheduling profile.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After running the **qos schedule-profile (system view)** command to create a global scheduling profile, you can run the **qos schedule-profile** command in the interface view to apply the global scheduling profile to an interface to perform queue scheduling.

Example

# Create a global scheduling profile named **test**, set the queue scheduling mode to PQ, and then apply the global scheduling profile to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test] qos pq
[HUAWEI-qos-schedule-profile-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos schedule-profile test
```

Related Topics

15.4.17 qos schedule-profile (system view)

15.4.17 qos schedule-profile (system view)

Function

The **qos schedule-profile** command creates a global scheduling profile and displays the scheduling profile view.

The **undo qos schedule-profile** command deletes a created global scheduling profile.

By default, no global scheduling profile is created.

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this command.

Format

qos schedule-profile *profile-name*

undo qos schedule-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a scheduling profile.	The value is a string of 1 to 16 case-insensitive characters without spaces. **NOTE** A maximum of six scheduling profiles are allowed; otherwise, the system displays an error message.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **qos schedule-profile** command in the system view to create a global scheduling profile, you can run the **qos { pq | wrr | drr }** command in the scheduling profile view to configure a queue scheduling mode. You can apply a global scheduling profile to a physical interface to perform queue scheduling.

Example

# Create a global scheduling profile named **test**.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test]
```

Related Topics

15.4.8 qos { pq | wrr | drr }

15.4.16 qos schedule-profile (interface view)

15.4.18 qos tail-drop-profile (interface view)

Function

The **qos tail-drop-profile** command applies a tail drop profile to an interface.

The **undo qos tail-drop-profile** command deletes a tail drop profile from an interface.

By default, no tail drop profile is applied to an interface.

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this command.

Format

qos tail-drop-profile *profile-name*

undo qos tail-drop-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a tail drop profile.	The value must be the name of an existing tail drop profile.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After running the **qos tail-drop-profile (system view)** command to create a global tail drop profile, run the **qos tail-drop-profile** command in the interface view to apply the global tail drop profile to an interface to drop packets at the end of a queue.

Example

# Create a global tail drop profile named **test**, set the maximum length of green packets in queue 1 for the global tail drop profile to 10, and then apply the global tail drop profile to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] qos tail-drop-profile test
[HUAWEI-tail-drop-profile-test] qos queue 1 green max-length 10
[HUAWEI-tail-drop-profile-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos tail-drop-profile test
```

Related Topics

15.4.19 qos tail-drop-profile (system view)

15.4.19 qos tail-drop-profile (system view)

Function

The **qos tail-drop-profile** command creates a global tail drop profile and displays the tail drop profile view.

The **undo qos tail-drop-profile** command deletes a global tail drop profile.

By default, no global tail drop profile is created.

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this command.

Format

qos tail-drop-profile *profile-name*

undo qos tail-drop-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a tail drop profile.	The value is a string of 1 to 16 case-insensitive characters, without spaces. **NOTE** A maximum of six tail drop profiles are allowed; otherwise, the system displays an error message.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **qos tail-drop-profile** command in the system view to create a tail drop profile, you can run the **qos queue max-length** or **qos queue max-buffer** command in the tail drop profile view to configure a queue. You can apply a global tail drop profile to a physical interface to drop packets at the end of a queue.

Example

# Create a global tail drop profile named **test**.

```
<HUAWEI> system-view
[HUAWEI] qos tail-drop-profile test
[HUAWEI-tail-drop-profile-test]
```

Related Topics

15.4.11 qos queue max-buffer

15.4.12 qos queue max-length

15.4.18 qos tail-drop-profile (interface view)

15.4.20 qos traffic-manage enable

Function

The **qos traffic-manage enable** command enables the traffic manager (TM) to buffer and schedule packets.

The **undo qos traffic-manage enable** command disables the TM from buffering and scheduling packets.

By default, the TM is enabled to buffer and schedule packets.

NOTE

Only the S5720HI supports this command.

Format

qos traffic-manage enable

undo qos traffic-manage enable

Parameters

None

Views

GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the TM is enabled to buffer and schedule packets. When heavy traffic needs to be forwarded on all interfaces, the device cannot ensure lossless forwarding. You can run the **undo qos traffic-manage enable** command to disable the TM from buffering and scheduling packets.

Configuration Note

After the **undo qos traffic-manage enable** command is executed, the S5720HI does not support queue-based traffic shaping, WRED, queue statistics collection, and congestion management.

After the **undo qos traffic-manage enable** command is executed, the switch does not support HQoS.

After the **undo qos traffic-manage enable** command is executed, the buffer of the device is greatly reduced.

Example

# Configure the TM not to buffer and schedule packets on the GE0/0/1.

```
<HUAWEI> system view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo qos traffic-manage enable
```

15.4.21 qos wred

Function

The **qos wred** command applies a WRED drop profile to an interface.

The **undo qos wred** command deletes a WRED drop profile from an interface.

By default, no WRED drop profile is applied to an interface.

NOTE

Only the S5720EI, S6720EI, and S6720S-EI support this command.

Format

qos wred *drop-profile-name*

undo qos wred

Parameters

Parameter	Description	Value
drop-profile-name	Specifies the name of a WRED drop profile.	The value must be the name of an existing WRED drop profile.

Views

GE interface view, XGE interface view, 40GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a WRED drop profile is applied to an interface, congestion avoidance is implemented on the interface.

Prerequisites

Before applying a WRED drop profile, run the **drop-profile** command to create a WRED drop profile.

Precautions

A WRED drop profile can be applied to an interface or a queue.

If you apply WRED drop profiles to an interface and to a queue on the interface, the system first matches the packets with the profiles applied to the queue and interface in sequence. The system performs congestion avoidance for the packets that match the WRED drop profiles.

To configure the same WRED drop profile on multiple interfaces, perform the configuration on a port group to reduce the workload.

Example

# Create a WRED drop profile named **wred1** and apply it to the GE0/0/1.

```
<HUAWEI> system view
[HUAWEI] drop-profile wred1
[HUAWEI-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[HUAWEI-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[HUAWEI-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
[HUAWEI-drop-wred1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] qos wred wred1
[HUAWEI-GigabitEthernet0/0/1] quit
```

Related Topics

15.4.5 drop-profile

15.4.2 color

15.4.22 queue-depth (WRED drop profile view)

Function

The **queue-depth** command sets the length of a queue.

The **undo queue-depth** command restores the default length of a queue.

By default, the system uniformly manages the lengths of queues.

Format

queue-depth *queue-depth-value*

undo queue-depth

NOTE

Only the S5720HI supports this command.

Parameters

Parameter	Description	Value
queue-depth-value	Specifies the queue length.	The value is an integer that ranges from 1024 to 805306368, in bytes.

Views

Drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets entering interface queues are processed based on parameters in a WRED drop profile, the percentage of the packet length to the queue length needs to be calculated. When the percentage reaches the lower drop threshold, the switch discards packets based on the drop probability. When the percentage reaches the upper drop threshold, the switch discards all subsequent packets. You can adjust the queue length to optimize the congestion avoidance effect.

Prerequisites

A WRED drop profile has been created and the WRED drop profile view has been displayed.

Precautions

When a small queue length is used, the delay of packets passing a queue is shortened but the queue buffer capability is lowered. When a large queue length is used, the queue buffer capability is improved but the delay of packets passing a queue is extended. In addition, when congestion occurs in a queue, many buffer resources are occupied. In this case, packets in other queues may be discarded due to insufficient buffer resources.

Example

# Configure WRED drop profile **wred1** and set the queue length to 2000 bytes.

```
<HUAWEI> system-view
[HUAWEI] drop-profile wred1
[HUAWEI-drop-wred1] queue-depth 2000
```

Related Topics

15.4.5 drop-profile

15.4.23 reset qos queue statistics

Function

The **reset qos queue statistics** command clears queue-based traffic statistics on an interface.

Format

reset qos queue statistics interface *interface-type interface-number*

reset qos queue statistics all

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears queue-based traffic statistics on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
all	Clears queue-based traffic statistics on all interfaces.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect queue-based statistics within a certain period, first run the **reset qos queue statistics** command to clear the existing statistics.

Precautions

The cleared queue-based statistics cannot be restored. Therefore, exercise caution when you run the command.

Example

# Clear queue-based traffic statistics on the GE0/0/1.

```
<HUAWEI> reset qos queue statistics interface gigabitethernet 0/0/1
```

Related Topics

15.4.4 display qos queue statistics

15.4.24 stack-port qos { pq | wrr | drr }

Function

The **stack-port qos** { **pq** | **wrr** | **drr** } command configures a scheduling mode of queues on an interface of the stack.

The **undo stack-port qos** { **pq** | **wrr** | **drr** } command restores the default scheduling mode of queues on an interface of the stack.

By default, the queue scheduling mode of queues is priority queuing (PQ).

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

stack-port qos { **pq** | **wrr** | **drr** }

undo stack-port qos { **pq** | **wrr** | **drr** }

NOTE

The S5720HI does not support WRR scheduling mode.

Parameters

Parameter	Description	Value
pq	Indicates the PQ scheduling mode.	-

Parameter	Description	Value
wrr	Indicates the Weighted Round Robin (WRR) scheduling mode.	-
drr	Indicates the Weighted Deficit Round Robin (WDRR) scheduling mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the stack is configured, stack protocol packets and packets between chassis are exchanged on the stack interface. If a large number of packets are exchanged, congestion may occur on the stack interface. As a result, core services such as video and voice services cannot be processed in a timely manner. You can set the scheduling mode on the stack interface so that services with the same priority are processed in the same manner and services with different priorities are processed based on weights.

Precautions

Before setting the scheduling mode of queues, configure priority mapping based on simple traffic classification to map packet priorities to per-hop behaviors (PHBs) and colors or configure internal priority re-marking based on complex traffic classification so that packets of different services enter different queues.

Example

# Set the queue scheduling mode on the stack interface to WRR.

```
<HUAWEI> system view
[HUAWEI] stack-port qos wrr
```

Related Topics

15.4.25 stack-port qos queue

15.4.25 stack-port qos queue

Function

The **stack-port qos queue** command configures the WRR or WDRR weight for queues on an interface of the stack.

The **undo stack-port qos queue** command restores the default WRR or WDRR weight for queues on a stack interface.

By default, the WRR or WDRR weight for queues on an interface of the stack is 1.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

stack-port qos queue *queue-index* { **wrr** | **drr** } **weight** *weight*

undo stack-port qos queue *queue-index* { **wrr** | **drr** } [**weight** *weight*]

NOTE

The WRR weight of queues cannot be set on the stack interface of the S5720HI.

Parameters

Parameter	Description	Value
queue *queue-index*	Specifies the index of a queue.	The value is an integer that ranges from 0 to 7.
wrr	Indicates the WRR weight.	-
drr	Indicates the WDRR weight.	-
weight *weight*	Specifies the WRR or WDRR weight.	The value is an integer. The value range is as follows: ● S5720EI: 0 to 63 ● Other models: 0 to 127

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When using WRR or WDRR scheduling, you can set the weight for each queue. Then the switch schedules queues in turn based on the weights. If the weight of a queue is set to 0, the queue uses PQ scheduling. In this case, PQ+WRR or PQ +WDRR is used.

Prerequisites

The **stack-port qos { pq | wrr | drr }** command has been executed to configure the WRR or WDRR scheduling mode of queues on a stack interface.

Example

# Set the WRR weight for queue 1 on the stack interface to 30.

```
<HUAWEI> system view
[HUAWEI] stack-port qos queue 1 wrr weight 30
```

Related Topics

15.4.24 stack-port qos { pq | wrr | drr }

15.4.26 stack-port qos schedule-profile

Function

The **stack-port qos schedule-profile** command applies a scheduling profile to a stack interface.

The **undo stack-port qos schedule-profile** command deletes a scheduling profile from a stack interface.

NOTE

The following switches support this command:

- S2720EI and S2750EI
- Other S5700LI models excluding the S5700-10P-LI-AC, S5700-28P-LI-BAT, S5700-28P-LI-24S-BAT, and S5700-10P-PWR-LI-AC
- S5700S-28P-PWR-LI-AC, S5700S-28X-LI-AC, and S5700S-52X-LI-AC
- S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI
- S5730SI and S5730S-EI
- S6720LI, S6720S-LI, S6720SI, and S6720S-SI

Format

stack-port qos schedule-profile *profile-name*

undo stack-port qos schedule-profile [*profile-name*]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a scheduling profile.	The value must be the name of an existing scheduling profile.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **qos schedule-profile** *profile-name* command is used to create a scheduling profile globally, run this command to apply the scheduling profile. Then the switch schedules traffic on the stack interface based on the scheduling mode defined in the scheduling profile.

Example

# Create a scheduling profile named **test** globally, set the queue scheduling mode to PQ, and apply the scheduling profile to the system.

```
<HUAWEI> system-view
[HUAWEI] qos schedule-profile test
[HUAWEI-qos-schedule-profile-test] qos pq
[HUAWEI-qos-schedule-profile-test] quit
[HUAWEI] stack-port qos schedule-profile test
```

Related Topics

15.4.17 qos schedule-profile (system view)

15.5 Filtering Configuration Commands

15.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

15.5.2 deny | permit

Function

The **deny** | **permit** command configures access control for service packets based on traffic classifiers.

- The **deny** command prevents service flows that match a specified rule from passing through.
- The **permit** command forwards packets matching traffic classification rules according to the original policy.

By default, an AC does not control service packets based on traffic classifiers.

Format

deny | **permit**

undo { **deny** | **permit** }

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device implements access control using a traffic policy. That is, you can use a traffic policy containing **deny** | **permit** on the device so that the device provides the firewall function to filter out specified types of packets. The **deny** | **permit** command only filters data packets, but does not process control packets such as STP BPDUs sent to the CPU.

Precautions

When you specify a packet filtering action for packets matching an ACL, if the ACL rule defines **permit**, the device processes packets according to the action (**deny** or **permit**) in the traffic behavior. If the ACL rule defines **deny**, the device discards packets regardless of whether **deny** or **permit** is configured in the traffic behavior.

When you specify the packet filtering action for packets matching an ACL to **deny** or **permit**, if the ACL rule contains the **logging** field, logs are recorded when packets are discarded or forwarded.

If a traffic policy in which the **deny** behavior is defined is applied to the outbound direction on the S5720EI, S5720HI, S6720EI, and S6720S-EI, control packets of

ICMP, OSPF, BGP, RIP, SNMP, and Telnet sent by the CPU are discarded. This affects relevant protocol functions.

In the same traffic behavior, the deny action cannot be used with other traffic actions. Before adding other traffic actions such as re-marking to a traffic behavior, ensure that the traffic behavior does not contain the deny action. If the traffic behavior contains the deny action, configure the permit action before configuring other traffic actions.

Example

# Configure a traffic policy **p1** to prevent the packets from VLAN 2 to pass through GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match vlan-id 2
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] deny
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-policy p1 inbound
```

Related Topics

15.1.31 traffic behavior

15.6 Redirection Configuration Commands

15.6.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

15.6.2 redirect cpu

Function

The **redirect cpu** command configures an action of redirecting packets to the CPU in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, an action of redirecting packets to the CPU is not configured in a traffic behavior.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

redirect cpu

undo redirect

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to the CPU.

Precautions

The traffic policy that contains the redirection action can only be applied to the system, an interface, or a VLAN.

NOTICE

After the traffic policy containing **redirect cpu** is used, the traffic matching the traffic classification rule is redirected to the CPU, causing CPU performance to deteriorate. Exercise caution when you run the **redirect cpu** command.

Example

# Redirect packets to the CPU in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] redirect cpu
```

Related Topics

15.1.31 traffic behavior

15.6.3 redirect interface

Function

The **redirect interface** command configures an action of redirecting packets to an interface in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, no action of redirecting packets to an interface is configured in a traffic behavior.

Format

redirect interface *interface-type interface-number* [**forced**]

undo redirect

NOTE

Tunnel interfaces do not support **forced**.

Only the S5720HI supports the action of redirecting packets to a tunnel interface.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface to which packets are redirected. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
forced	Directly discards packets when the redirect-to-interface in Down state.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **redirect interface** command configures an action of redirecting packets to an interface in a traffic behavior. For example, packets can be redirected to a firewall for security check.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to an interface.

Precautions

The traffic policy that contains the redirection action can only be applied to the system, an interface, or a VLAN in the inbound direction.

For the S5720HI, packets can be redirected to physical interfaces and Eth-Trunk interfaces in Layer 2 or Layer 3 mode. For other models, packets can be redirected only to physical interfaces and Eth-Trunk interfaces in Layer 2 mode.

The packets that are redirected to an interface will be discarded if the VLAN of the packets on the interface is not allowed.

Example

# Redirect packets to GE0/0/1 in the traffic behavior **b1**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] redirect interface gigabitethernet 0/0/1
```

Related Topics

15.1.31 traffic behavior

15.7 Statistics Configuration Commands

15.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

15.7.2 statistic enable (traffic behavior view)

Function

The **statistic enable** command enables the traffic statistics function in a traffic behavior.

The **undo statistic enable** command disables the traffic statistics function in a traffic behavior.

By default, the traffic statistics function in a traffic behavior is disabled.

Format

statistic enable

undo statistic enable

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the statistics on a traffic policy, you can use the **statistic enable** command to enable the statistics function. After the statistics function is enabled, you can use the **display traffic policy statistics** command to view the statistics.

Precautions

If only **statistic enable** is configured in a traffic behavior, the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support packet-based traffic statistics but not byte-based traffic statistics. After **traffic statistics mode by-bytes** is configured in the system view and traffic statistics is configured in a traffic policy, the switches support byte-based traffic statistics.

For the S5720HI, if a traffic policy defining traffic statistics is applied to an Eth-Trunk in the outbound direction, traffic statistics does not take effect for the packets sent by the CPU. In this case, you can configure traffic statistics or port mirroring in the inbound direction on the interface connected to the Eth-Trunk.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing the traffic statistics collection function.

Example

# Enable the statistics function in a traffic behavior **test**.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior test
[HUAWEI-behavior-test] statistic enable
```

Related Topics

15.1.7 display traffic policy statistics

15.1.30 reset traffic policy statistics

15.1.31 traffic behavior

15.7.3 statistic enable (QoS profile view)

Function

The **statistic enable** command enables traffic statistics in a QoS profile.

The **undo statistic enable** command disables traffic statistics in a QoS profile.

By default, the traffic statistics function is disabled in a QoS profile.

Format

statistic enable

undo statistic enable

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Parameters

None

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **statistic enable** command collects traffic statistics of successfully authenticated online users.

Precautions

When users that connected to the device through an Eth-Trunk go online through Portal authentication, the S5720EI, S6720EI, and S6720S-EI cannot provide traffic statistics for the users.

Example

# Enable traffic statistics in the QoS profile **huawei**.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name huawei
[HUAWEI-qos-huawei] statistic enable
```

Related Topics

15.3.12 qos-profile

15.8 ACL-based Simplified Traffic Policy Commands

15.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

15.8.2 display traffic-statistics

Function

The **display traffic-statistics** command displays ACL-based traffic statistics.

Format

display traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] { **inbound** | **outbound** } [**acl** { *bas-acl* | *adv-acl* | *user-acl* } [**rule** *rule-id*]]

display traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] { **inbound** | **outbound** } [**acl** { *acl-name* | *l2-acl* } [**rule** *rule-id*] [**acl** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]]

display traffic-statistics interface { **inbound** | **outbound** }

display traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] { **inbound** | **outbound** } [**acl ipv6** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays ACL-based traffic statistics in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays ACL-based traffic statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If *interface-type interface-number* is not specified, ACL-based traffic statistics on all interfaces are displayed.	-
inbound	Displays ACL-based traffic statistics in the inbound direction.	-
outbound	Displays ACL-based traffic statistics in the outbound direction.	-

Parameter	Description	Value
acl { *bas-acl* | *adv-acl* | *user-acl* }	Displays statistics on packets matching a specified ACL. ● *bas-acl* specifies a basic ACL. ● *adv-acl* specifies an advanced ACL. ● *user-acl* specifies a user-defined ACL.	The value is an integer. The value ranges are as follows: ● The value of *bas-acl* ranges from 2000 to 2999. ● The value of *adv-acl* ranges from 3000 to 3999. ● The value of *user-acl* ranges from 5000 to 5999.
acl { *acl-name* | *l2-acl* }	Displays statistics on packets matching a specified ACL. ● *acl-name* specifies the name of an ACL. ● *l2-acl* specifies the number of a Layer 2 ACL.	● The value of *acl-name* must be the name of an existing ACL. ● The value of *l2-acl* is an integer that ranges from 4000 to 4999.
acl ipv6	Displays traffic statistics based on the IPv6 ACL.	-
rule *rule-id*	Displays statistics on packets matching a specified ACL rule.	The IPv4 ACL rule ID is an integer that ranges from 0 to 4294967294, and the IPv6 ACL rule ID is an integer that ranges from 0 to 2047.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic-statistics** command displays ACL-based traffic statistics on an interface or in a VLAN. The command output helps you learn about forwarded and discarded packets matching and ACL, and locate faults.

Prerequisites

The traffic statistics function has been enabled using the **traffic-statistic (interface view)** or **traffic-statistic (system view)** command.

Example

# Display statistics on packets matching ACL 3009 in the inbound direction on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl 3009
[HUAWEI-acl-adv-3009] rule 1 permit ip
[HUAWEI-acl-adv-3009] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-statistic inbound acl 3009
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] display traffic-statistics interface gigabitethernet 0/0/1 inbound acl 3009
---------------------------------------------------------------------------
Interface GigabitEthernet0/0/1
 ACL:3009 Rule:1
     matched:0 packets, passed:0 packets, dropped:0
packets
---------------------------------------------------------------------------
```

Table 15-31 Description of the **display traffic-statistics** command output

Item	Description
ACL	ACL number.
Rule	ACL rule ID.
matched	Number of packets matching the ACL.
passed	Number of forwarded packets.
dropped	Number of discarded packets.

Related Topics

14.1.5 acl (system view)

14.1.9 display acl

15.8.17 traffic-statistic (interface view)

15.8.18 traffic-statistic (system view)

15.8.7 traffic-limit (interface view)

15.8.8 traffic-limit (system view)

15.8.3 reset traffic-statistics

Function

The **reset traffic-statistics** command clears ACL-based traffic statistics.

Format

reset traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] { **inbound** | **outbound** } [**acl** { *bas-acl* | *adv-acl* | *user-acl* } [**rule** *rule-id*]]

reset traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] { **inbound** | **outbound** } [**acl** { *acl-name* | *l2-acl* } [**rule** *rule-id*] [**acl** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]]

reset traffic-statistics { **interface** | **vlan** } { **inbound** | **outbound** }

reset traffic-statistics [**vlan** *vlan-id* | **interface** *interface-type interface-number*] { **inbound** | **outbound** } [**acl ipv6** { *bas-acl* | *adv-acl* | *acl-name* } [**rule** *rule-id*]]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Clears ACL-based traffic statistics in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Clears ACL-based traffic statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If *interface-type interface-number* is not specified, ACL-based traffic statistics on all interfaces are cleared.	-
inbound	Clears ACL-based traffic statistics in the inbound direction.	-
outbound	Clears ACL-based traffic statistics in the outbound direction.	-

Parameter	Description	Value
acl { *bas-acl* | *adv-acl* | *user-acl* }	Clears statistics on packets matching a specified ACL. ● *bas-acl* specifies a basic ACL. ● *adv-acl* specifies an advanced ACL. ● *user-acl* specifies a user-defined ACL.	The value is an integer. The value ranges are as follows: ● The value of *bas-acl* ranges from 2000 to 2999. ● The value of *adv-acl* ranges from 3000 to 3999. ● The value of *user-acl* ranges from 5000 to 5999.
acl { *acl-name* | *l2-acl* }	Clears statistics on packets matching a specified ACL. ● *acl-name* specifies the name of an ACL. ● *l2-acl* specifies the number of a Layer 2 ACL.	● The value of *acl-name* must be the name of an existing ACL. ● The value of *l2-acl* is an integer that ranges from 4000 to 4999.
acl ipv6	Clears traffic statistics based on the IPv6 ACL.	-
rule *rule-id*	Clears statistics on packets matching a specified ACL rule.	The IPv4 ACL rule ID is an integer that ranges from 0 to 4294967294, and the IPv6 ACL rule ID is an integer that ranges from 0 to 2047.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before recollecting ACL-based traffic statistics, run the **reset traffic-statistics** command to clear existing statistics. Then run the **display traffic-statistics** command to view ACL-based traffic statistics.

Precautions

After the **reset traffic-statistics** command is executed, statistics are cleared and cannot be restored. Exercise caution when you use this command.

Example

# Clear statistics about incoming packets that match rule 5 in the ACL named **test** on GE0/0/1.

```
<HUAWEI> reset traffic-statistics interface gigabitethernet 0/0/1 inbound acl test rule 5
```

Related Topics

14.1.5 acl (system view)

14.1.9 display acl

14.1.3 acl ipv6 (system view)

14.1.10 display acl ipv6

15.8.4 traffic-delete fast-mode enable

Function

The **traffic-delete fast-mode enable** command enables the device to rapidly delete ACL-based simplified traffic policies.

The **undo traffic-delete fast-mode enable** command disables the device from rapidly deleting ACL-based simplified traffic policies.

By default, the device is disabled from rapidly deleting ACL-based simplified traffic policies.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

traffic-delete fast-mode enable

undo traffic-delete fast-mode enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple ACL-based simplified traffic policies are configured and the ACL contains a large number of rules, it takes a long time for the device to delete the traffic policies. To solve the problem, run the **traffic-delete fast-mode enable** command to enable the device to rapidly delete ACL-based simplified traffic policies.

Precautions

After the **traffic-delete fast-mode enable** command is executed, the traffic policy statistics are cleared.

After the **traffic-delete fast-mode enable** command is used, if you configure a new ACL-based simplified traffic policy, the original ACL-based simplified traffic policy becomes invalid temporarily and takes effect only when the new ACL-based simplified traffic policy is applied successfully.

Example

# Enable the device to rapidly delete ACL-based simplified traffic policies.

```
<HUAWEI> system-view
[HUAWEI] traffic-delete fast-mode enable
```

15.8.5 traffic-filter (interface view)

Function

The **traffic-filter** command applies an ACL to an interface to filter packets on the interface.

The **undo traffic-filter** command cancels the configuration.

By default, no ACL is applied to an interface to filter packets on the interface.

Format

Use the following command in the inbound direction on an interface:

traffic-filter inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

undo traffic-filter inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

Use the following command in the outbound direction on an interface:

traffic-filter outbound acl { [**ipv6**] {*bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

undo traffic-filter outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-filter { **inbound** | **outbound** } **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-filter { **inbound** | **outbound** } **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-filter { **inbound** | **outbound** } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-filter { **inbound** | **outbound** } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
inbound	Configures ACL-based packet filtering in the inbound direction on an interface.	-
outbound	Configures ACL-based packet filtering in the outbound direction on an interface.	-
acl	Filters packets based on the IPv4 ACL.	-
ipv6	Configures IPv6 ACL-based packet filtering.	-
bas-acl	Filters packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Filters packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Filters packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Filters packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Filters packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-filter** command is executed on an interface, the device filters packets matching ACL rules:

- If the action in an ACL rule is **deny**, the device discards packets matching the rule.
- If the action in an ACL rule is **permit**, the device forwards packets matching the rule.
- If no rule is matched, packets are allowed to pass through.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-filter(system view)** and **traffic-filter (interface view)** commands are used simultaneously, the **traffic-filter (interface view)** command takes effect.

When the deny action is defined in the ACL rule associated with the **traffic-filter** command, the ACL rule can only be associated with the **traffic-mirror (interface view)**, **traffic-mirror (system view)**, **traffic-statistic (interface view)**, or **traffic-statistic (system view)** command. If the ACL rule is associated with other simplified traffic policies, the simplified traffic policies may not take effect.

When the permit action is defined in the ACL rule associated with the **traffic-filter** command, the ACL rule can be associated with other simplified traffic policies.

When the ACL rule containing the **logging** field is associated with the **traffic-filter** command, logs are recorded when packets are discarded or forwarded.

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

Outbound ACL-based packet filtering on an interface does not take effect on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI if:

- Outbound ACL-based packet filtering is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based packet filtering.

If an ACL rule defines **deny** and **traffic-filter** based on the ACL is applied to the outbound direction on the S5720EI, S5720HI, S6720EI, and S6720S-EI, when packets match the ACL rule, control packets of ICMP, OSPF, BGP, RIP, SNMP, and Telnet sent by the CPU are discarded. This affects relevant protocol functions.

Example

# On the GE0/0/1, configure packet filtering based on the ACL that rejects packets with source IP address 192.168.0.2/32.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 deny ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-filter inbound acl 3000
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

15.8.6 traffic-filter (system view)

Function

The **traffic-filter** command configures ACL-based packet filtering globally or in a VLAN.

The **undo traffic-filter** command cancels ACL-based packet filtering globally or in a VLAN.

By default, ACL-based packet filtering is not configured globally or in a VLAN.

NOTE

When ACL-based packet filtering is implemented in the system or in a VLAN, the ACL number is in the range of 2000 to 5999. When ACL-based packet filtering is implemented for user access control on the NAC network, the ACL number is in the range of 6000 to 9999. See **traffic-filter acl**.

Format

To configure ACL-based packet filtering in the inbound direction on a switch, use the following command:

traffic-filter [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

undo traffic-filter [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

To configure ACL-based packet filtering in the outbound direction on a switch, use the following command:

traffic-filter [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] {*bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

undo traffic-filter [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-filter [**vlan** *vlan-id*] { **inbound** | **outbound** } **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-filter [**vlan** *vlan-id*] { **inbound** | **outbound** } **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-filter [**vlan** *vlan-id*] { **inbound** | **outbound** } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-filter [**vlan** *vlan-id*] { **inbound** | **outbound** } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Configures ACL-based packet filtering in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
inbound	Configures ACL-based packet filtering in the inbound direction.	-
outbound	Configures ACL-based packet filtering in the outbound direction. **NOTE** Packet filtering based on the user-defined ACL cannot be applied to the outbound direction.	-
acl	Filters packets based on the IPv4 ACL.	-

Parameter	Description	Value
ipv6	Filters packets based on the IPv6 ACL.	-
bas-acl	Filters packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Filters packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Filters packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Filters packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Specifies the name of an ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Filters packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-filter** command is executed on the device, the device filters packets matching an ACL rule:

- If the action in the ACL rule is **deny**, the device discards packets matching the rule.
- If the action in the ACL rule is **permit**, the device forwards packets matching the rule.
- If no rule is matched, packets are allowed to pass through.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-filter (system view)** and **traffic-filter (interface view)** commands are used simultaneously, the **traffic-filter (interface view)** command takes effect.

When the deny action is defined in the ACL rule associated with the **traffic-filter** command, the ACL rule can only be associated with the **traffic-mirror (interface view)**, **traffic-mirror (system view)**, **traffic-statistic (interface view)**, or **traffic-statistic (system view)** command. If the ACL rule is associated with other simplified traffic policies, the simplified traffic policies may not take effect.

When the permit action is defined in the ACL rule associated with the **traffic-filter** command, the ACL rule can be associated with other simplified traffic policies.

When the ACL rule containing the **logging** field is associated with the **traffic-filter** command, logs are recorded when packets are discarded or forwarded.

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

Outbound ACL-based packet filtering on an interface does not take effect on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI if:

- Outbound ACL-based packet filtering is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based packet filtering.

If an ACL rule defines **deny** and **traffic-filter** based on the ACL is applied to the outbound direction on the S5720EI, S5720HI, S6720EI, and S6720S-EI, when packets match the ACL rule, control packets of ICMP, OSPF, BGP, RIP, SNMP, and Telnet sent by the CPU are discarded. This affects relevant protocol functions.

Example

# Configure ACL-based packet filtering in VLAN 100. The ACL rejects packets with source IP address 192.168.0.2/32.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] acl name test 3000
[HUAWEI-acl-adv-test] rule 5 deny ip source 192.168.0.2 0
[HUAWEI-acl-adv-test] quit
[HUAWEI] traffic-filter vlan 100 inbound acl name test
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

14.1.21 rule (user-defined ACL view)

15.8.5 traffic-filter (interface view)

15.8.7 traffic-limit (interface view)

Function

The **traffic-limit** command configures ACL-based traffic policing on an interface.

The **undo traffic-limit** command cancels ACL-based traffic policing on an interface.

By default, ACL-based traffic policing is not configured on an interface.

Format

Use the following command in the inbound direction on a switch interface:

traffic-limit inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

undo traffic-limit inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

Use the following command in the outbound direction on a switch interface:

traffic-limit outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

undo traffic-limit outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and traffic policing is used in the inbound direction on a switch interface, use the following command:

traffic-limit inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit inbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit inbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

traffic-limit inbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-*

value **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

undo traffic-limit inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-limit inbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and traffic policing is used in the outbound direction on a switch interface, use the following command:

traffic-limit outbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit outbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit outbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

traffic-limit outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

undo traffic-limit outbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-limit outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
inbound	Performs traffic policing for packets in the inbound direction of an interface.	-
outbound	Performs traffic policing for packets in the outbound direction of an interface.	-
acl	Performs traffic policing for packets based on the IPv4 ACL.	-
ipv6	Performs traffic policing for packets based on the IPv6 ACL.	-
bas-acl	Performs traffic policing for packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Performs traffic policing for packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Performs traffic policing for packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Performs traffic policing for packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Performs traffic policing for packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Performs traffic policing for packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.
cir *cir-value*	Specifies the committed information rate (CIR), which is the guaranteed average transmission rate.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.

Parameter	Description	Value
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. The PIR must be larger than or equal to the CIR. The default PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. The default CBS is 125 times the CIR. If the CIR multiplied by 125 is smaller than 4000, the default CBS is 4000.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default PBS is 125 times the CIR. If the PIR is set, the default PBS is 125 times the PIR. If the CIR or PIR multiplied by 125 is smaller than 4000, the default PBS is 4000.
green	Performs traffic policing for green packets. By default, green packets are allowed to pass through.	-
yellow	Performs traffic policing for yellow packets. By default, yellow packets are allowed to pass through.	-
red	Performs traffic policing for red packets. By default, red packets are discarded.	-
remark-8021p *8021p-value*	Re-marks the 802.1p priority in packets.	The value is an integer that ranges from 0 to 7.
remark-dscp *dscp-value*	Re-marks the DSCP priority in packets.	The value is an integer that ranges from 0 to 63.

Parameter	Description	Value
drop	Indicates that packets are discarded.	-
pass	Indicates that packets are allowed to pass through.	-

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-limit** command is executed on an interface, the device limits the rate and remarks the 802.1p or DSCP priority of packets matching an ACL.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-limit (system view)** and **traffic-limit (interface view)** commands are used simultaneously, the **traffic-limit (interface view)** command takes effect.

When the **traffic-limit (interface view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, the traffic rate is limited.

If the **traffic-limit** command with the same ACL rule specified is executed two or more times in the interface view, the system displays the following information:

```
Error:Sacl does not support config the same acl or rule repeatedly.
```

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

Outbound ACL-based traffic policing on an interface does not take effect on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI if:

- Outbound ACL-based traffic policing is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based traffic policing.

Example

# Configure ACL-based traffic policing in the inbound direction on GE0/0/1, set the CIR to 10000 kbit/s for packets matching ACL 3000, configure GE0/0/1 to allow green packets, yellow packets, and red packets to pass through, and re-mark the DSCP priority of red packets with 5.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-limit inbound acl 3000 cir 10000 green pass yellow pass red
pass remark-dscp 5
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

15.8.8 traffic-limit (system view)

15.8.8 traffic-limit (system view)

Function

The **traffic-limit** command configures ACL-based traffic policing globally or in a VLAN.

The **undo traffic-limit** command cancels ACL-based traffic policing globally or in a VLAN.

By default, ACL-based traffic policing is not configured globally or in a VLAN.

Format

To configure ACL-based traffic policing in the inbound direction on a switch, use the following command:

traffic-limit [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-*

value **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

undo traffic-limit [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

To configure ACL-based traffic policing in the outbound direction on a switch, use the following command:

traffic-limit [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

undo traffic-limit [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and traffic policing is used in the inbound direction on a switch, use the following command:

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-*

value] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

traffic-limit [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

undo traffic-limit [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-limit [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and traffic policing is used in the outbound direction on a switch, use the following command:

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**yellow** { **drop** | **pass** [**remark-dscp** *dscp-value*] }] [**red** { **drop** | **pass** [**remark-dscp** *dscp-value*] }]] (S5720EI, S6720EI, S6720S-EI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [[**green** { **drop** | **pass** }] [**yellow** { **drop** | **pass** }] [**red** { **drop** | **pass** }]] (S5720HI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

traffic-limit [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green pass**] [**yellow pass**] [**red** { **drop** | **pass** }] (S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI)

undo traffic-limit [**vlan** *vlan-id*] **outbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-limit [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
inbound	Performs traffic policing for packets in the inbound direction.	-
outbound	Performs traffic policing for packets in the outbound direction.	-
acl	Performs traffic policing for packets based on the IPv4 ACL.	-
ipv6	Performs traffic policing for packets based on the IPv6 ACL.	-
bas-acl	Performs traffic policing for packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Performs traffic policing for packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.

Parameter	Description	Value
l2-acl	Performs traffic policing for packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Performs traffic policing for packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Performs traffic policing for packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Performs traffic policing for packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.
cir *cir-value*	Specifies the committed information rate (CIR), which is the guaranteed average transmission rate.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. The PIR must be larger than or equal to the CIR. The default PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. The default CBS is 125 times the CIR. If the CIR multiplied by 125 is smaller than 4000, the default CBS is 4000.

Parameter	Description	Value
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 4000 to 4294967295, in bytes. If the PIR is not set, the default PBS is 125 times the CIR. If the PIR is set, the default PBS is 125 times the PIR. If the CIR or PIR multiplied by 125 is smaller than 4000, the default PBS is 4000.
green	Performs traffic policing for green packets. By default, green packets are allowed to pass through.	-
yellow	Performs traffic policing for yellow packets. By default, yellow packets are allowed to pass through.	-
red	Performs traffic policing for red packets. By default, red packets are discarded.	-
remark-8021p *8021p-value*	Re-marks the 802.1p priority in packets.	The value is an integer that ranges from 0 to 7.
remark-dscp *dscp-value*	Re-marks the DSCP priority in packets.	The value is an integer that ranges from 0 to 63.
drop	Indicates that packets are discarded.	-
pass	Indicates that packets are allowed to pass through.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-limit** command is executed on the device, the device limits the rate and remarks the 802.1p or DSCP priority of packets matching an ACL.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-limit (interface view)** and **traffic-limit (system view)** commands are used simultaneously, the **traffic-limit (interface view)** command takes effect.

When the **traffic-limit (system view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, the traffic rate is limited.

After traffic policing is configured on an interface, the number of packets that can be forwarded on the interface every second is relevant to the packet length calculation method. By default, the device calculates the 20-byte inter-frame gap and preamble. That is, the device calculates the actual packet length plus 20-byte inter-frame gap and preamble.

Outbound ACL-based traffic policing on an interface does not take effect on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI if:

- Outbound ACL-based traffic policing is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based traffic policing.

Example

# In the inbound direction in VLAN 100, configure traffic policing based on ACL 3000, set the CIR to 10000 kbit/s, and configure the device to permit green and yellow packets to pass through and to discard red packets.

```
<HUAWEI> system-view
[HUAWEI] traffic-limit vlan 100 inbound acl 3000 cir 10000 green pass yellow pass red drop
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

15.8.7 traffic-limit (interface view)

15.8.9 traffic-mirror (interface view)

Function

The **traffic-mirror** command configures ACL-based flow mirroring on an interface.

The **undo traffic-mirror** command cancels ACL-based flow mirroring on an interface.

By default, ACL-based flow mirroring is not configured on an interface.

Format

To configure a single ACL, use the following command:

traffic-mirror inbound { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror inbound { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-mirror inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-mirror inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-mirror inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
inbound	Mirrors packets in the inbound direction on an interface.	-
acl	Mirrors packets based on the IPv4 ACL.	-

Parameter	Description	Value
ipv6	Mirrors packets based on the IPv6 ACL.	-
bas-acl	Mirrors packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Mirrors packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Mirrors packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Mirrors packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Mirrors packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Mirrors packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.
to observe-port *o-index*	Specifies the index of the observing port to which packets are mirrored.	The value is an integer and the vale range depends on the product model: ● S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI: 1 ● S5720EI, S5720HI, S6720EI, and S6720S-EI: 1 to 8

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **traffic-mirror** command is configured, the device can perform flow mirroring or remote flow mirroring, without affecting traffic forwarding.

Prerequisites

An observing interface has been created through the **observe-port (local mirroring)** or **observe-port (remote mirroring)** command.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-mirror (system view)** and **traffic-mirror (interface view)** commands are used simultaneously, the **traffic-mirror (interface view)** command takes effect.

Example

# Configure ACL-based flow mirroring in the inbound direction on GE0/0/1, and mirror the packets matching ACL 3000 to the observing port with the index of 1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-mirror inbound acl 3000 to observe-port 1
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

16.8.7 observe-port (local observing port)

16.8.8 observe-port (remote observing port)

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

14.1.21 rule (user-defined ACL view)

15.8.10 traffic-mirror (system view)

15.8.10 traffic-mirror (system view)

Function

The **traffic-mirror** command configures ACL-based flow mirroring globally or in a VLAN.

The **undo traffic-mirror** command cancels ACL-based flow mirroring globally or in a VLAN.

By default, no ACL-based flow mirroring is configured globally or in a VLAN.

Format

To configure a single ACL, use the following command:

traffic-mirror [**vlan** *vlan-id*] **inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror [**vlan** *vlan-id*] **inbound** { **acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-mirror [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-mirror [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-mirror [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **to observe-port** *o-index*

undo traffic-mirror [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
inbound	Mirrors packets in the inbound direction.	-
acl	Mirrors packets based on the IPv4 ACL.	-
ipv6	Mirrors packets based on the IPv6 ACL.	-
bas-acl	Mirrors packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Mirrors packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Mirrors packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Mirrors packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Mirrors packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Mirrors packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.

Parameter	Description	Value
to observe-port *o-index*	Specifies the index of the observing port to which packets are mirrored.	The value is an integer and the vale range depends on the product model: ● S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI: 1 ● S5720EI, S5720HI, S6720EI, and S6720S-EI: 1 to 8

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **traffic-mirror** command is configured, the device can perform flow mirroring or remote flow mirroring, without affecting traffic forwarding.

Prerequisites

An observing port has been created through the **observe-port (local mirroring)** or **observe-port (remote mirroring)** command.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-mirror (interface view)** and **traffic-mirror (system view)** commands are used simultaneously, the **traffic-mirror (interface view)** command takes effect.

Example

# Configure ACL-based flow mirroring in the inbound direction in VLAN 100, and mirror the packets matching ACL 3000 to the observing port with the index of 1.

```
<HUAWEI> system-view
[HUAWEI] observe-port 1 interface gigabitethernet 0/0/1
[HUAWEI] traffic-mirror vlan 100 inbound acl 3000 to observe-port 1
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

16.8.7 observe-port (local observing port)

16.8.8 observe-port (remote observing port)

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

14.1.21 rule (user-defined ACL view)

15.8.9 traffic-mirror (interface view)

15.8.11 traffic-redirect (interface view)

Function

The **traffic-redirect** command configures ACL-based redirection on an interface.

The **undo traffic-redirect** command cancels ACL-based redirection on an interface.

By default, ACL-based redirection is not configured on an interface.

Format

To configure a single ACL, use the following command:

traffic-redirect inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } (S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, S6720S-EI)

traffic-redirect inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* } (S1720GFR, S2750EI, S5700LI, S5700S-LI, S5710-X-LI)

undo traffic-redirect inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-redirect inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } (S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, S6720S-EI)

traffic-redirect inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* } (S1720GFR, S2750EI, S5700LI, S5700S-LI, S5710-X-LI)

undo traffic-redirect inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-redirect inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } (S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, S6720S-EI)

traffic-redirect inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* } (S1720GFR, S2750EI, S5700LI, S5700S-LI, S5710-X-LI)

undo traffic-redirect inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-redirect inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } (S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, S6720S-EI)

traffic-redirect inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* } (S1720GFR, S2750EI, S5700LI, S5700S-LI, S5710-X-LI)

undo traffic-redirect inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

NOTE

Only the S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support **vpn-instance** *vpn-instance-name*.

Parameters

Parameter	Description	Value
inbound	Redirects packets in the inbound direction on an interface.	-
acl	Redirects packets based on the IPv4 ACL.	-
ipv6	Redirects packets based on the IPv6 ACL.	-
bas-acl	Redirects packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Redirects packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Redirects packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Redirects packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Redirects packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Redirects packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.
cpu	Redirects packets to the CPU.	-
interface *interface-type interface-number*	Redirects packets to a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vpn-instance *vpn-instance-name*	Redirects packets to a VPN instance.	The value must be an existing VPN instance name.

Parameter	Description	Value
ip-nexthop *ip-nexthop*	Redirects packets to a next-hop IPv4 address.	The value is in dotted decimal notation.
ipv6-nexthop *ipv6-nexthop*	Redirects packets to a next-hop IPv6 address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-redirect** command is executed on an interface, the device redirects packets matching an ACL to the CPU, a specified interface, or a specified next hop address.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-redirect (system view)** and **traffic-redirect (interface view)** commands are used simultaneously, the **traffic-redirect (interface view)** command takes effect.

When the **traffic-redirect (interface view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, traffic is redirected.

On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, if traffic matching **traffic-redirect (interface view)** also matches **traffic-secure (interface view)** or **traffic-secure (system view)**, **traffic-redirect**

(interface view) takes effect. On the S5720EI, S5720HI, S6720EI, and S6720S-EI, if the ACL defines the permit action, **traffic-secure (interface view)** or **traffic-secure (system view)** and **traffic-redirect (interface view)** take effect.

Before redirecting packets to an IPv6 address using this command, run the **ipv6 neighbor** command to configure a static neighbor.

Redirection to a next hop only takes effect on L3 traffic for the S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI.

NOTICE

If packets are redirected to the CPU, a large number of packets will be sent to the CPU, affecting normal services. Exercise caution when you configure redirection to the CPU.

Example

# Configure ACL-based redirection in the inbound direction on GE0/0/1, and redirect packets matching ACL 3000 to GE0/0/2.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-redirect inbound acl 3000 interface gigabitethernet 0/0/2
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

14.1.21 rule (user-defined ACL view)

15.8.12 traffic-redirect (system view)

15.8.12 traffic-redirect (system view)

Function

The **traffic-redirect** command configures ACL-based redirection globally or in a VLAN.

The **undo traffic-redirect** command cancels ACL-based redirection globally or in a VLAN.

By default, ACL-based redirection is not configured globally or in a VLAN.

NOTE

When ACL-based redirection is implemented in the system or in a VLAN, the ACL number is in the range of 2000 to 5999. When ACL-based redirection is implemented on the NAC network, the ACL number is in the range of 6000 to 9999. See **traffic-redirect acl**.

Format

To configure a single ACL, use the following command:

traffic-redirect [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } (S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, S6720S-EI)

traffic-redirect [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* } (S1720GFR, S2750EI, S5700LI, S5700S-LI, S5710-X-LI)

undo traffic-redirect [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-redirect [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } (S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, S6720S-EI)

traffic-redirect [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* } (S1720GFR, S2750EI, S5700LI, S5700S-LI, S5710-X-LI)

undo traffic-redirect [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-redirect [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* | [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } (S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, S6720S-EI)

traffic-redirect [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* } (S1720GFR, S2750EI, S5700LI, S5700S-LI, S5710-X-LI)

undo traffic-redirect [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-redirect [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface**

interface-type interface-number | [**vpn-instance** *vpn-instance-name*] **ip-nexthop** *ip-nexthop* | **ipv6-nexthop** *ipv6-nexthop* } (S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, S6720S-EI)

traffic-redirect [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **cpu** | **interface** *interface-type interface-number* } (S1720GFR, S2750EI, S5700LI, S5700S-LI, S5710-X-LI)

undo traffic-redirect [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

NOTE

Only the S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support **vpn-instance** *vpn-instance-name*.

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
inbound	Redirects packets to the inbound direction.	-
acl	Redirects packets based on the IPv4 ACL.	-
ipv6	Redirects packets based on the IPv6 ACL.	-
bas-acl	Redirects packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Redirects packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Redirects packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Redirects packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Redirects packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.

Parameter	Description	Value
rule *rule-id*	Redirects packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.
cpu	Redirects packets to the CPU.	-
interface *interface-type interface-number*	Redirects packets to a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vpn-instance *vpn-instance-name*	Redirects packets to a VPN instance.	The value must be an existing VPN instance name.
ip-nexthop *ip-nexthop*	Redirects packets to a next-hop IPv4 address.	The value is in dotted decimal notation.
ipv6-nexthop *ipv6-nexthop*	Redirects packets to a next-hop IPv6 address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-redirect** command is executed on the device, the device redirects packets matching an ACL to the CPU, a specified interface, or a specified next hop address.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-redirect (interface view)** and **traffic-redirect (system view)** commands are used simultaneously, the **traffic-redirect (interface view)** command takes effect.

When the **traffic-redirect (system view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, traffic is redirected.

On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, if traffic matching **traffic-redirect (system view)** also matches **traffic-secure (interface view)** or **traffic-secure (system view)**, **traffic-redirect (system view)** takes effect. On the S5720EI, S5720HI, S6720EI, and S6720S-EI, if the ACL defines the permit action, **traffic-secure (interface view)** or **traffic-secure (system view)** and **traffic-redirect (system view)** take effect.

Before redirecting packets to an IPv6 address using this command, run the **ipv6 neighbor** command to configure a static neighbor.

Redirection to a next hop only takes effect on L3 traffic for the S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, and S5720S-SI.

NOTICE

If packets are redirected to the CPU, a large number of packets will be sent to the CPU, affecting normal services. Exercise caution when you configure redirection to the CPU.

Example

# Configure ACL-based redirection in the inbound direction in VLAN 100, and redirect packets matching ACL 3000 to GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] traffic-redirect vlan 100 inbound acl 3000 interface gigabitethernet 0/0/1
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

14.1.21 rule (user-defined ACL view)

15.8.11 traffic-redirect (interface view)

15.8.13 traffic-remark (interface view)

Function

The **traffic-remark** command configures ACL-based re-marking on an interface.

The **undo traffic-remark** command cancels ACL-based re-marking on an interface.

By default, ACL-based re-marking is not configured on an interface.

Format

To configure ACL-based re-marking in the inbound direction on a switch interface, use the following command:

traffic-remark inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

To configure ACL-based re-marking in the outbound direction on a switch interface, use the following command:

traffic-remark outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

If both Layer 2 and Layer 3 ACLs are configured and re-marking is used in the inbound direction on a switch interface, use the following command:

traffic-remark inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

traffic-remark inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* |

dscp { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

traffic-remark inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

If both Layer 2 and Layer 3 ACLs are configured and re-marking is used in the outbound direction on a switch interface, use the following command:

traffic-remark outbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark outbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

traffic-remark outbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark outbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

traffic-remark outbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark outbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

Parameters

Parameter	Description	Value
inbound	Re-marks packets in the inbound direction.	-
outbound	Re-marks packets in the outbound direction.	-
acl	Re-marks packets based on the IPv4 ACL.	-
ipv6	Re-marks packets based on the IPv6 ACL.	-

Parameter	Description	Value
bas-acl	Re-marks packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Re-marks packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Re-marks packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Re-marks packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Re-marks packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Re-marks packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.
8021p *8021p-value*	Re-marks the 802.1p priority in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
cvlan-id *cvlan-id*	Re-marks the inner VLAN tag in QinQ packets. **NOTE** The inner VLAN tag in QinQ packets cannot be re-marked on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, or S6720S-SI.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
destination-mac *mac-address*	Re-marks the destination MAC address in packets. **NOTE** The destination MAC address in packets cannot be re-marked on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, or S6720S-SI.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
dscp { *dscp-name* | *dscp-value* }	Re-marks the DSCP priority in packets.	The value can be an integer in the range of 0 to 63, or DSCP service name, for example, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values corresponding to DSCP service names are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46 By default, the *dscp-value* is 0.
local-precedence *local-precedence-value*	Re-marks the local IP precedence in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
ip-precedence *ip-precedence-value*	Re-marks the IP precedence in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
vlan-id *vlan-id*	Re-marks the VLAN ID in packets.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-remark** command is executed on an interface, the device re-marks packets matching an ACL, for example, 802.1p priority, inner VLAN tag in QinQ packets, destination MAC address, DSCP service type, local IP precedence, IP precedence, and VLAN ID.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-remark (system view)** and **traffic-remark (interface view)** commands are used simultaneously, the **traffic-remark (interface view)** command takes effect.

When the **traffic-remark (interface view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, traffic is re-marked.

Outbound ACL-based re-marking on an interface does not take effect on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI if:

- Outbound ACL-based re-marking is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based re-marking.

Example

# Configure ACL-based re-marking in the inbound direction on GE0/0/1, and re-mark the VLAN ID in packets from source MAC address 0-0-1 with 100.

```
<HUAWEI> system-view
[HUAWEI] acl 4001
[HUAWEI-acl-L2-4001] rule 5 permit source-mac 0-0-1
[HUAWEI-acl-L2-4001] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-remark inbound acl 4001 rule 5 vlan-id 100
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

14.1.21 rule (user-defined ACL view)

15.8.14 traffic-remark (system view)

15.8.14 traffic-remark (system view)

Function

The **traffic-remark** command configures ACL-based re-marking globally or in a VLAN.

The **undo traffic-remark** command cancels ACL-based re-marking globally or in a VLAN.

By default, ACL-based re-marking is not configured globally or in a VLAN.

Format

To configure ACL-based re-marking in the inbound direction on a switch, use the following command:

traffic-remark [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-**

mac *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

To configure ACL-based re-marking in the outbound direction on a switch, use the following command:

traffic-remark [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

If both Layer 2 and Layer 3 ACLs are configured and re-marking is used in the inbound direction on a switch, use the following command:

traffic-remark [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

traffic-remark [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

traffic-remark [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **destination-mac** *mac-address* | **dscp** { *dscp-name* | *dscp-value* } | **ip-precedence** *ip-precedence-value* | **local-precedence** *local-precedence-value* | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **destination-mac** | **dscp** | **ip-precedence** | **local-precedence** | **vlan-id** }

If both Layer 2 and Layer 3 ACLs are configured and re-marking is used in the outbound direction on a switch, use the following command:

traffic-remark [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

traffic-remark [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

traffic-remark [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** *8021p-value* | **cvlan-id** *cvlan-id* | **dscp** { *dscp-name* | *dscp-value* } | **vlan-id** *vlan-id* }

undo traffic-remark [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] { **8021p** | **cvlan-id** | **dscp** | **vlan-id** }

Parameters

Parameter	Description	Value
vlan *vlan-id*	Configures ACL-based re-marking in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
inbound	Re-marks packets in the inbound direction.	-
outbound	Re-marks packets in the outbound direction.	-
acl	Re-marks packets based on the IPv4 ACL.	-
ipv6	Re-marks packets based on the IPv6 ACL.	-
bas-acl	Re-marks packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Re-marks packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Re-marks packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Re-marks packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Re-marks packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.

Parameter	Description	Value
rule *rule-id*	Re-marks packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.
8021p *8021p-value*	Re-marks the 802.1p priority in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
cvlan-id *cvlan-id*	Re-marks the inner VLAN tag in QinQ packets. **NOTE** The inner VLAN tag in QinQ packets cannot be re-marked on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, or S6720S-SI.	The value is an integer that ranges from 1 to 4094.
destination-mac *mac-address*	Re-marks the destination MAC address in packets. **NOTE** The destination MAC address in packets cannot be re-marked on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5720HI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, or S6720S-SI.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Parameter	Description	Value
dscp { *dscp-name* | *dscp-value* }	Re-marks the DSCP priority in packets.	The value can be an integer in the range of 0 to 63, or DSCP service name, for example, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1 to cs7, default, or ef. The values corresponding to DSCP service names are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46 By default, the *dscp-value* is 0.
local-precedence *local-precedence-value*	Re-marks the local IP precedence in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Parameter	Description	Value
ip-precedence *ip-precedence-value*	Re-marks the IP precedence in packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
vlan-id *vlan-id*	Re-marks the VLAN ID in packets.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-remark** command is executed on the device, the device re-marks packets matching an ACL, for example, 802.1p priority, inner VLAN tag in QinQ packets, destination MAC address, DSCP service type, local IP precedence, IP precedence, and VLAN ID.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-remark (interface view)** and **traffic-remark (system view)** commands are used simultaneously, the **traffic-remark (interface view)** command takes effect.

When the **traffic-remark (system view)** command and the **traffic-filter (interface view)** command or the **traffic-filter (system view)** command are used simultaneously, and the two commands are associated with the same ACL rule:

- If the deny action is configured in the ACL rule, traffic is discarded.
- If the permit action is configured in the ACL rule, traffic is re-marked.

Outbound ACL-based re-marking on an interface does not take effect on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI if:

- Outbound ACL-based re-marking is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based re-marking.

Example

# Configure ACL-based re-marking in the inbound direction in VLAN 100, and re-mark the VLAN ID in packets from source MAC address 0-0-1 with 101.

```
<HUAWEI> system-view
[HUAWEI] acl 4001
[HUAWEI-acl-L2-4001] rule 5 permit source-mac 0-0-1
[HUAWEI-acl-L2-4001] quit
[HUAWEI] traffic-remark vlan 100 inbound acl 4001 rule 5 vlan-id 101
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

14.1.21 rule (user-defined ACL view)

15.8.13 traffic-remark (interface view)

15.8.15 traffic-secure (interface view)

Function

The **traffic-secure** command configures ACL-based packet filtering on an interface.

The **undo traffic-secure** command cancels ACL-based packet filtering on an interface.

By default, ACL-based packet filtering is not configured on an interface.

Format

To configure a single ACL, use the following command:

traffic-secure inbound acl { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-secure inbound acl { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-secure inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-secure inbound acl { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

NOTE

The S2750EI, S5700-10P-LI-AC, and S5700-10P-PWR-LI-AC that are enabled with Layer 3 hardware forwarding for IPv4 packets do not support this command.

Parameters

Parameter	Description	Value
inbound	Filters packets in the inbound direction.	-
acl	Filters packets based on the IPv4 ACL.	-
bas-acl	Filters packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Filters packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Filters packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Filters packets based on a specified ACL rule.	The IPv4 ACL value ranges from 0 to 4294967294.

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-secure** command is executed on an interface, the device filters packets matching ACL rules:

- If the action in an ACL rule is **deny**, the device discards packets matching the rule.
- If the action in an ACL rule is **permit**, the device forwards packets matching the rule.
- If no rule is matched, packets are allowed to pass through.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, if traffic matching **traffic-secure (interface view)** also matches **traffic-redirect (interface view)** or **traffic-redirect (system view)**, **traffic-redirect (interface view)** or **traffic-redirect (system view)** takes effect. On the S5720EI, S5720HI, S6720EI, and S6720S-EI, if the ACL defines the permit action, **traffic-redirect (interface view)** or **traffic-redirect (system view)** and **traffic-secure (interface view)** take effect.

On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, **traffic-secure** takes precedence over other ACL-based simplified traffic policy commands except **traffic-redirect (interface view)** and **traffic-redirect (system view)**.

On the S5720EI, S5720HI, S6720EI, and S6720S-EI takes precedence over other ACL-based simplified traffic policy commands.

If both **traffic-secure** and other ACL-based simplified traffic policy commands need to be configured on the S5720EI, S5720HI, S6720EI, and S6720S-EI, **traffic-secure (interface view)**, and the ACL is based on the inner 802.1p priority, inner VLAN ID, or port range, configure the **traffic-secure** command, and then configure other ACL-based simplified traffic policy commands.

Example

# Configure the traffic filtering action on GE0/0/1 to discard the packets with source address 192.168.0.2 and mirror the packets with destination address 192.168.1.3 to the observing interface with the index of 1.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 deny ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] acl name test 3001
[HUAWEI-acl-adv-test] rule 5 permit ip destination 192.168.1.3 0
```

```
[HUAWEI-acl-adv-test] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-secure inbound acl 3000
[HUAWEI-GigabitEthernet0/0/1] traffic-mirror inbound acl 3001 to observe-port 1
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

15.8.16 traffic-secure (system view)

15.8.16 traffic-secure (system view)

Function

The **traffic-secure** command configures ACL-based packet filtering globally or in a VLAN.

The **undo traffic-secure** command cancels ACL-based packet filtering globally or in a VLAN.

By default, ACL-based packet filtering is not configured globally or in a VLAN.

Format

To configure a single ACL, use the following command:

traffic-secure [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-secure [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 ACLs and Layer 3 ACLs are configured, use the following command:

traffic-secure [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-secure [**vlan** *vlan-id*] **inbound acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

NOTE

The S2750EI, S5700-10P-LI-AC, and S5700-10P-PWR-LI-AC that are enabled with Layer 3 hardware forwarding for IPv4 packets do not support this command.

Parameters

Parameter	Description	Value
vlan *vlan-id*	Configures ACL-based packet filtering in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
inbound	Filters packets in the inbound direction.	-
acl	Filters packets based on the IPv4 ACL.	-
bas-acl	Filters packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Filters packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Filters packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Filters packets based on a specified ACL rule.	The IPv4 ACL value ranges from 0 to 4294967294.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-secure** command is executed on the device, the device filters packets matching ACL rules:

- If the action in an ACL rule is **deny**, the device discards packets matching the rule.
- If the action in an ACL rule is **permit**, the device forwards packets matching the rule.

- If no rule is matched, packets are allowed to pass through.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, if traffic matching **traffic-secure (system view)** also matches **traffic-redirect (interface view)** or **traffic-redirect (system view)**, **traffic-redirect (interface view)** or **traffic-redirect (system view)** takes effect. On the S5720EI, S5720HI, S6720EI, and S6720S-EI, if the ACL defines the permit action, **traffic-redirect (interface view)** or **traffic-redirect (system view)** and **traffic-secure (system view)** take effect.

On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, **traffic-secure** takes precedence over other ACL-based simplified traffic policy commands except **traffic-redirect (interface view)** and **traffic-redirect (system view)**.

On the S5720EI, S5720HI, S6720EI, and S6720S-EI, **traffic-secure** takes precedence over other ACL-based simplified traffic policy commands.

If both **traffic-secure** and other ACL-based simplified traffic policy commands need to be configured on the S5720EI, S5720HI, S6720EI, and S6720S-EI, and the ACL is based on the inner 802.1p priority, inner VLAN ID, or port range, configure the **traffic-secure** command, and then configure other ACL-based simplified traffic policy commands.

Example

# Configure the traffic filtering action globally to discard the packets with source address 192.168.0.2 and mirror the packets with destination address 192.168.1.3 to the observing interface with the index of 1.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 deny ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] acl name test 3001
[HUAWEI-acl-adv-test] rule 5 permit ip destination 192.168.1.3 0
[HUAWEI-acl-adv-test] quit
[HUAWEI] traffic-secure inbound acl 3000
[HUAWEI] traffic-mirror inbound acl 3001 to observe-port 1
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

15.8.15 traffic-secure (interface view)

15.8.17 traffic-statistic (interface view)

Function

The **traffic-statistic** command configures ACL-based traffic statistics on an interface.

The **undo traffic-statistic** command cancels ACL-based traffic statistics on an interface.

By default, no ACL-based traffic statistics function is configured on an interface.

Format

Use the following commands in the inbound direction on a switch interface:

traffic-statistic inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic inbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

Use the following commands in the outbound direction on a switch interface:

traffic-statistic outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

undo traffic-statistic outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and the ACL-based traffic statistics function is used in the inbound direction on a switch interface, use the following commands:

traffic-statistic inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic inbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic inbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic inbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and the ACL-based traffic statistics function is used in the outbound direction on a switch interface, use the following commands:

traffic-statistic outbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic outbound acl *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic outbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic outbound acl { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic outbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic outbound acl name *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
inbound	Collects statistics on packets in the inbound direction.	-
outbound	Collects statistics on packets in the outbound direction.	-
acl	Collects statistics on packets based on the IPv4 ACL.	-
ipv6	Collects statistics on packets based on the IPv6 ACL.	-
bas-acl	Collects statistics on packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Collects statistics on packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.

Parameter	Description	Value
l2-acl	Collects statistics on packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Collects statistics on packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.
name *acl-name*	Collects statistics on packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Collects statistics on packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.
by-bytes	Indicates that traffic statistics are collected based on the number of bytes. **NOTE** By default, traffic statistics are collected based on the number of packets. After **by-bytes** is specified, traffic statistics are collected based on the number of bytes.	-

Views

Ethernet interface view, MultiGE interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-statistic** command is executed on an interface, the device collects statistics on packets matching an ACL.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-statistic (system view)** and **traffic-statistic (interface view)** commands are used simultaneously, the **traffic-statistic (interface view)** command takes effect.

When the action in an ACL rule is **permit** or **deny**, the ACL can be associated with the **traffic-statistic** command, but **deny** does not take effect. That is, only traffic statistics are collected.

Outbound ACL-based traffic statistics on an interface does not take effect on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI if:

- Outbound ACL-based traffic statistics is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based traffic statistics.

For the S5720HI, if **traffic-statistic** is applied to an Eth-Trunk in the outbound direction, traffic statistics does not take effect for the packets sent by the CPU. In this case, you can configure traffic statistics or port mirroring in the inbound direction on the interface connected to the Eth-Trunk.

Example

# Configure the ACL-based traffic statistics function in the inbound direction on GE0/0/1 to collect statistics on packets matching rule 1 in ACL 3000.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-statistic inbound acl 3000 rule 1
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

15.8.2 display traffic-statistics

15.8.18 traffic-statistic (system view)

15.8.18 traffic-statistic (system view)

Function

The **traffic-statistic** command configures ACL-based traffic statistics globally or in a VLAN.

The **undo traffic-statistic** command cancels ACL-based traffic statistics globally or in a VLAN

By default, the ACL-based traffic statistics function is not configured globally or in a VLAN.

Format

Use the following command in the inbound direction on a switch:

traffic-statistic [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic [**vlan** *vlan-id*] **inbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

Use the following command in the outbound direction on a switch:

traffic-statistic [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

undo traffic-statistic [**vlan** *vlan-id*] **outbound acl** { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } | *l2-acl* | *user-acl* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and the ACL-based traffic statistics function is used in the inbound direction on a switch, use the following command:

traffic-statistic [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic [**vlan** *vlan-id*] **inbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic [**vlan** *vlan-id*] **inbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*] [**by-bytes**]

undo traffic-statistic [**vlan** *vlan-id*] **inbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

If both Layer 2 and Layer 3 ACLs are configured and the ACL-based traffic statistics function is used in the outbound direction on a switch, use the following command:

traffic-statistic [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic [**vlan** *vlan-id*] **outbound acl** *l2-acl* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic [**vlan** *vlan-id*] **outbound acl** { *bas-acl* | *adv-acl* } [**rule** *rule-id*] **acl** { *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

traffic-statistic [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

undo traffic-statistic [**vlan** *vlan-id*] **outbound acl name** *acl-name* [**rule** *rule-id*] **acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* } [**rule** *rule-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Configures ACL-based packet statistics in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
inbound	Collects statistics on packets in the inbound direction.	-
outbound	Collects statistics on packets in the outbound direction.	-
acl	Collects statistics on packets based on the IPv4 ACL.	-
ipv6	Collects statistics on packets based on the IPv6 ACL.	-
bas-acl	Collects statistics on packets based on a specified basic ACL.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Collects statistics on packets based on a specified advanced ACL.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Collects statistics on packets based on a specified Layer 2 ACL.	The value is an integer that ranges from 4000 to 4999.
user-acl	Collects statistics on packets based on a specified user-defined ACL.	The value is an integer that ranges from 5000 to 5999.

Parameter	Description	Value
name *acl-name*	Collects statistics on packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
rule *rule-id*	Collects statistics on packets based on a specified ACL rule.	The IPv4 ACL rule ID ranges from 0 to 4294967294, and the IPv6 ACL rule ID ranges from 0 to 2047.
by-bytes	Indicates that traffic statistics are collected based on the number of bytes. **NOTE** By default, traffic statistics are collected based on the number of packets. After **by-bytes** is specified, traffic statistics are collected based on the number of bytes.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-statistic** command is executed on the device, the device collects statistics on packets matching an ACL.

Precautions

If **name** *acl-name* is specified in the command, you need to run the **acl name** or **acl ipv6 name** command to create the corresponding ACL. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If **rule** *rule-id* is specified in the command, you need to create an ACL and configure the corresponding rule. Otherwise, the ACL-based simplified traffic policy fails to be configured.

If the **traffic-statistic (interface view)** and **traffic-statistic (system view)** commands are used simultaneously, the **traffic-statistic (interface view)** command takes effect.

When the action in an ACL rule is **permit** or **deny**, the ACL can be associated with the **traffic-statistic** command, but **deny** does not take effect. That is, only traffic statistics are collected.

Outbound ACL-based traffic statistics on an interface does not take effect on the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI if:

- Outbound ACL-based traffic statistics is configured, and the ACL is based on VLAN IDs.
- VLAN mapping is also configured on the interface, and the mapped VLAN ID is the same as the VLAN ID in ACL-based traffic statistics.

Example

# Configure the ACL-based traffic statistics function in the inbound direction in VLAN 100 to collect statistics on packets matching rule 1 in ACL 3000.

```
<HUAWEI> system-view
[HUAWEI] traffic-statistic vlan 100 inbound acl 3000 rule 1
```

Related Topics

14.1.5 acl (system view)

14.1.3 acl ipv6 (system view)

14.1.4 acl name

14.1.2 acl ipv6 name

14.1.9 display acl

14.1.10 display acl ipv6

15.8.2 display traffic-statistics

15.8.17 traffic-statistic (interface view)

15.9 HQoS Commands

15.9.1 Command Support

Only the S5720HI supports HQoS configuration commands.

15.9.2 color (flow queue WRED drop profile view)

Function

The **color** command configures upper and lower drop thresholds and maximum drop probability in a flow queue WRED drop profile based on the packet color.

The **undo color** command restores default parameters in a flow queue WRED drop profile.

By default, the upper and lower drop thresholds and maximum drop probability for green, yellow, and red packets are 100.

Format

color { **green** | **yellow** | **red** } **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*

undo color { **green** | **yellow** | **red** }

Parameters

Parameter	Description	Value
green	Indicates WRED parameters for green packets.	-
yellow	Indicates WRED parameters for yellow packets.	-
red	Indicates WRED parameters for red packets.	-

Parameter	Description	Value
low-limit *low-limit-percentage*	Specifies the lower drop threshold, in percentage. When the percentage of the packet length to the queue length reaches this value, the device discards packets based on the drop probability.	The value is an integer that ranges from 0 to 100. The default value is 100.
high-limit *high-limit-percentage*	Specifies the upper drop threshold, in percentage. When the percentage of the packet length to the queue length reaches this value, the device starts to discard all subsequent packets.	The value is an integer that ranges from *low-limit-percentage* to 100. The default value is 100.
discard-percentage *discard-percentage*	Specifies the maximum drop probability.	The value is an integer that ranges from 1 to 100. The default value is 100.

Views

Flow queue WRED drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets enter queues, the device colors packets based on the mapping defined in a DiffServ domain. The device processes packets entering flow queues based on parameters in a flow queue WRED drop profile. When the percentage of the packet length to the queue length reaches the lower drop threshold, the device discards packets based on the drop probability. When the percentage of the packet length to the queue length reaches the upper drop threshold, the device discards all subsequent packets.

Prerequisites

A flow queue WRED drop profile has been created and the flow queue WRED drop profile view has been displayed.

Example

# Configure flow queue WRED drop profile **wred1**, set the lower drop threshold, upper drop threshold, and maximum drop probability for green packets to 80%,

100%, and 10%, set the lower drop threshold, upper drop threshold, and maximum drop probability for yellow packets to 60%, 80%, and 20%, and set the lower drop threshold, upper drop threshold, and maximum drop probability for red packets to 40%, 60%, and 40%.

```
<HUAWEI> system-view
[HUAWEI] flow-wred-profile wred1
[HUAWEI-flow-wred-wred1] color green low-limit 80 high-limit 100 discard-percentage 10
[HUAWEI-flow-wred-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20
[HUAWEI-flow-wred-wred1] color red low-limit 40 high-limit 60 discard-percentage 40
```

Related Topics

15.9.9 flow-wred-profile

15.9.5 display flow-wred-profile

15.9.3 display flow-mapping-profile

Function

The **display flow-mapping-profile** command displays the flow mapping profile configuration.

Format

display flow-mapping-profile [**name** *flow-mapping-profile-name* | **all**]

Parameters

Parameter	Description	Value
name *flow-mapping-profile-name*	Displays detailed information about a specified flow mapping profile.	The value must be the name of an existing flow mapping profile.
all	Displays detailed information about all flow mapping profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display flow-mapping-profile** command to view the number of configured flow mapping profiles and all the configuration of the specified flow mapping profile.

Precautions

If **all** and **name** *flow-mapping-profile-name* are not specified, brief information about all flow mapping profiles is displayed.

Example

# Display brief information about all flow mapping profiles.

```
<HUAWEI> display flow-mapping-profile
       index                 flow-mapping-profile name
-----------------------------------------------------------------
       0                     default
       1                     map1
-----------------------------------------------------------------
 Total   8     Used   2
```

# Display detailed information about flow mapping profile **map1**.

```
<HUAWEI> display flow-mapping-profile name map1
Flow-mapping-profile[1]: map1
Flow-queue  Port-queue
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0          0
1          1
2          3
3          3
4          4
5          5
6          6
7          7
-----------------------------------------------------------------
```

# Display detailed information about all flow mapping profiles.

```
<HUAWEI> display flow-mapping-profile all
Flow-mapping-profile[0]: default
Flow-queue  Port-queue
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0          0
1          1
2          2
3          3
4          4
5          5
6          6
7          7
-----------------------------------------------------------------
Flow-mapping-profile[1]: map1
Flow-queue  Port-queue
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0          0
1          1
2          3
3          3
4          4
5          5
6          6
7          7
-----------------------------------------------------------------
```

Table 15-32 Description of the **display flow-mapping-profile** command output

Item	Description
index	Index of the flow mapping profile.
flow-mapping-profile name	Name of the flow mapping profile. To create a flow mapping profile, run the **flow-mapping-profile** command.
Total	Total number of flow mapping profiles.
Used	Number of configured flow mapping profiles.
Flow-mapping-profile[1]	Name of the flow mapping profile. The value 1 is the index of the flow mapping profile.
Flow-queue	Index of the flow queue. To configure the mapping between flow queues and interface queues, run the **map flow-queue (flow mapping profile view)** command.
Port-queue	Index of the interface queue. To configure the mapping between flow queues and interface queues, run the **map flow-queue (flow mapping profile view)** command.

Related Topics

15.9.7 flow-mapping-profile

15.9.4 display flow-queue-profile

Function

The **display flow-queue-profile** command displays the flow queue profile configuration.

Format

display flow-queue-profile [**name** *flow-queue-profile-name* | **all**]

Parameters

Parameter	Description	Value
name *flow-queue-profile-name*	Displays detailed information about a specified flow queue profile.	The value must be the name of an existing flow queue profile.
all	Displays detailed information about all flow queue profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display flow-queue-profile** command to view the number of configured flow queue profiles and all the configuration of the specified flow queue profile.

Precautions

If **all** and **name** *flow-queue-profile* are not specified, brief information about all flow queue profiles is displayed.

Example

# Display brief information about all flow queue profiles.

```
<HUAWEI> display flow-queue-profile
       index                  flow-queue-profile name
---------------------------------------------------------------
       0                      default
       1                      flow1
---------------------------------------------------------------
 Total   128     Used   2
```

# Display detailed information about flow queue profile **flow1**.

```
<HUAWEI> display flow-queue-profile name flow1
Flow-queue-profile[1]: flow1
Queue Schedule(Weight) Shaping         flow-wred-profile
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0     WFQ(50)          50%             wred1
1     PQ               None            default
2     PQ               None            default
3     PQ               None            default
4     PQ               None            default
5     PQ               None            default
```

```
6    PQ          None        default
7    PQ          None        default
----------------------------------------------------------------------
```

# Display detailed information about all flow queue profiles.

```
<HUAWEI> display flow-queue-profile all
Flow-queue-profile[0]: default
Queue Schedule(Weight) Shaping        flow-wred-profile
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0    PQ          None        default
1    PQ          None        default
2    PQ          None        default
3    PQ          None        default
4    PQ          None        default
5    PQ          None        default
6    PQ          None        default
7    PQ          None        default
----------------------------------------------------------------------
Flow-queue-profile[1]: flow1
Queue Schedule(Weight) Shaping        flow-wred-profile
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
0    WFQ(50)        50%          wred1
1    PQ          None        default
2    PQ          None        default
3    PQ          None        default
4    PQ          None        default
5    PQ          None        default
6    PQ          None        default
7    PQ          None        default
----------------------------------------------------------------------
```

Table 15-33 Description of the **display flow-queue-profile** command output

Item	Description
index	Index of the flow queue profile.
flow-queue-profile name	Name of the flow queue profile. To create a flow queue profile, run the **flow-queue-profile** command.
Total	Total number of flow queue profiles.
Used	Number of configured flow queue profiles.
Flow-queue-profile[1]	Name of the flow queue profile. The value 1 is the index of the flow queue profile. To create a flow queue profile, run the **flow-queue-profile** command.
Queue	Index of the flow queue, which corresponds to the local priority of packets.
Schedule(Weight)	Scheduling mode or weight of the flow queue. To set the scheduling mode and weight of a flow queue, run the **qos queue (flow queue profile view)** command.

Item	Description
Shaping	Traffic shaping rate or percentage of the flow queue. To set the traffic shaping and percentage of a flow queue, run the **qos queue (flow queue profile view)** command.
flow-wred-profile	Name of the WRED drop profile bound to the flow queue. To bind a WRED drop profile to a flow queue, run the **qos queue (flow queue profile view)** command.

Related Topics

15.9.8 flow-queue-profile

15.9.5 display flow-wred-profile

Function

The **display flow-wred-profile** command displays the configuration of flow queue WRED drop profiles.

Format

display flow-wred-profile [**name** *flow-wred-profile-name* | **all**]

Parameters

Parameter	Description	Value
name *flow-wred-profile-name*	Displays detailed information about a specified flow queue WRED drop profile.	The value must be the name of an existing flow queue WRED drop profile.
all	Displays detailed information about all flow queue WRED drop profiles.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display flow-wred-profile** command to view the number of configured flow queue WRED drop profiles and all the configuration of the specified flow queue WRED drop profile.

Precautions

If **all** and **name** *flow-wred-profile-name* are not specified, brief information about all flow queue WRED drop profiles is displayed.

Example

# Display brief information about all flow queue WRED drop profiles.

```
<HUAWEI> display flow-wred-profile
       index                  flow-wred-profile name
------------------------------------------------------------------
       0                      default
       1                      wred1
------------------------------------------------------------------
 Total   128     Used   2
```

# Display detailed information about flow queue WRED drop profile **wred1**.

```
<HUAWEI> display flow-wred-profile name wred1
Flow-wred-profile[1]: wred1
Queue depth         : 1048576
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     80          100         10
Yellow    60          80          20
Red       40          60          40
------------------------------------------------------------------
```

# Display detailed information about all flow queue WRED drop profiles.

```
<HUAWEI> display flow-wred-profile all
Flow-wred-profile[0]: default
Queue depth         : 1048576
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     100         100         100
Yellow    100         100         100
Red       100         100         100
------------------------------------------------------------------
Flow-wred-profile[1]: wred1
Queue depth         : 1048576
Color     Low-limit   High-limit  Discard-percentage
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Green     80          100         10
Yellow    60          80          20
Red       40          60          40
------------------------------------------------------------------
```

Table 15-34 Description of the display flow-wred-profile command output

Item	Description
index	Index of the flow queue WRED drop profile.

Item	Description
flow-wred-profile name	Name of the flow queue WRED drop profile. To create a flow queue WRED drop profile, run the **flow-wred-profile** command.
Total	Total number of flow queue WRED drop profiles.
Used	Number of configured flow queue WRED drop profiles.
Flow-wred-profile[1]	Name of the flow queue WRED drop profile. The value 1 is the index of the flow queue WRED drop profile. To create a flow queue WRED drop profile, run the **flow-wred-profile** command.
Queue depth	Queue length. To set the queue length, run the **queue-depth (flow queue WRED drop profile view)** command.
Color	Packet color. To set the packet color, run the **color (flow queue WRED drop profile view)** command.
Low-limit	Lower drop threshold in the flow queue WRED drop profile, in percentage. To set the lower drop threshold in a flow queue WRED drop profile, run the **color (flow queue WRED drop profile view)** command.
High-limit	Upper drop threshold in the flow queue WRED drop profile, in percentage. To set the upper drop threshold in a flow queue WRED drop profile, run the **color (flow queue WRED drop profile view)** command.
Discard-percentage	Maximum drop probability in the flow queue WRED drop profile, in percentage. To set the maximum drop probability in a flow queue WRED drop profile, run the **color (flow queue WRED drop profile view)** command.

Related Topics

15.9.2 color (flow queue WRED drop profile view)

15.9.9 flow-wred-profile

15.9.6 display traffic-user-queue statistics

Function

The **display traffic-user-queue statistics** command displays traffic statistics on subscriber queues.

Format

display traffic-user-queue statistics interface *interface-type interface-number* **outbound acl** { *bas-acl* | *adv-acl* } [**acl** { *l2-acl* | **name** *acl-name* }]

display traffic-user-queue statistics interface *interface-type interface-number* **outbound acl** *l2-acl* [**acl** { *bas-acl* | *adv-acl* | **name** *acl-name* }]

display traffic-user-queue statistics interface *interface-type interface-number* **outbound acl name** *acl-name* [**acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* }]

display traffic-user-queue statistics interface *interface-type interface-number* **outbound acl ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays traffic statistics on subscriber queues on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
outbound	Displays traffic statistics on subscriber queues in the outbound direction on an interface.	-
acl	Displays traffic statistics on subscriber queues based on IPv4 ACLs.	-
ipv6	Displays traffic statistics on subscriber queues based on IPv6 ACLs.	-
bas-acl	Displays traffic statistics on subscriber queues based on basic ACLs.	The value is an integer that ranges from 2000 to 2999.

Parameter	Description	Value
adv-acl	Displays traffic statistics on subscriber queues based on advanced ACLs.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Displays traffic statistics on subscriber queues based on Layer 2 ACLs.	The value is an integer that ranges from 4000 to 4999.
name *acl-name*	Displays traffic statistics on subscriber queues based on named ACLs. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic-user-queue statistics** command displays traffic statistics on subscriber queues based on ACLs on an interface. The command output helps you learn about forwarded and discarded packets matching ACLs and locate faults.

Prerequisites

The **traffic-user-queue** command has been executed to create a subscriber queue based on ACLs to implement HQoS.

Example

# Display traffic statistics on subscriber queues based on ACL 3009 in the outbound direction on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl 3009
[HUAWEI-acl-adv-3009] rule 1 permit ip
[HUAWEI-acl-adv-3009] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-user-queue outbound acl 3009 pir 2000
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] display traffic-user-queue statistics interface gigabitethernet 0/0/1 outbound acl 3009
--------------------------------------------------------------------------------
 Interface: GigabitEthernet0/0/1
--------------------------------------------------------------------------------
    Queue ID      |                    Statistics information
--------------------------------------------------------------------------------
        0         |          packets: pass:                            0
                  |                   drop:                            0
```

```
             |          bytes:   pass:                       0
             |                   drop:                       0
-------------------------------------------------------------------------------
   Queue ID      |                    Statistics information
-------------------------------------------------------------------------------
      1          |          packets: pass:                   0
             |                   drop:                       0
             |          bytes:   pass:                       0
             |                   drop:                       0
-------------------------------------------------------------------------------
   Queue ID      |                    Statistics information
-------------------------------------------------------------------------------
      2          |          packets: pass:                   0
             |                   drop:                       0
             |          bytes:   pass:                       0
             |                   drop:                       0
-------------------------------------------------------------------------------
   Queue ID      |                    Statistics information
-------------------------------------------------------------------------------
      3          |          packets: pass:                   0
             |                   drop:                       0
             |          bytes:   pass:                       0
             |                   drop:                       0
-------------------------------------------------------------------------------
   Queue ID      |                    Statistics information
-------------------------------------------------------------------------------
      4          |          packets: pass:                   0
             |                   drop:                       0
             |          bytes:   pass:                       0
             |                   drop:                       0
-------------------------------------------------------------------------------
   Queue ID      |                    Statistics information
-------------------------------------------------------------------------------
      5          |          packets: pass:                   0
             |                   drop:                       0
             |          bytes:   pass:                       0
             |                   drop:                       0
-------------------------------------------------------------------------------
   Queue ID      |                    Statistics information
-------------------------------------------------------------------------------
      6          |          packets: pass:                   0
             |                   drop:                       0
             |          bytes:   pass:                       0
             |                   drop:                       0
-------------------------------------------------------------------------------
   Queue ID      |                    Statistics information
-------------------------------------------------------------------------------
      7          |          packets: pass:                   0
             |                   drop:                       0
             |          bytes:   pass:                       0
             |                   drop:                       0
-------------------------------------------------------------------------------
```

Table 15-35 Description of the **display traffic-user-queue statistics** command output

Item	Description
Queue ID	Index of the flow queue.
packets	Number of collected packets. pass indicates the number of forwarded packets, and drop indicates the number of discarded packets.

Item	Description
bytes	Number of collected bytes. pass indicates the number of forwarded bytes, and drop indicates the number of discarded bytes.

Related Topics

15.9.14 traffic-user-queue (interface view)

15.9.7 flow-mapping-profile

Function

The **flow-mapping-profile** command creates a flow mapping profile or displays the view of an existing flow mapping profile.

The **undo flow-mapping-profile** command deletes the created flow mapping profile.

By default, the system predefines a flow mapping profile **default**.

Format

flow-mapping-profile *flow-mapping-profile-name*

undo flow-mapping-profile *flow-mapping-profile-name*

Parameters

Parameter	Description	Value
flow-mapping-profile-name	Specifies the name of a flow mapping profile.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the mapping between flow queues and interface queues is configured, the device can send flows of a service in a subscriber queue to a high- or low-priority interface queue.

Precautions

The flow mapping profile **default** cannot be modified or deleted.

Follow-up Procedure

Configure the mapping between flow queues and interface queues in the flow mapping profile view.

Example

# Create flow mapping profile **map1**.

```
<HUAWEI> system-view
[HUAWEI] flow-mapping-profile map1
[HUAWEI-flow-mapping-map1]
```

Related Topics

15.9.10 map flow-queue (flow mapping profile view)

15.9.3 display flow-mapping-profile

15.9.8 flow-queue-profile

Function

The **flow-queue-profile** command creates a flow queue profile or displays the view of an existing flow queue profile.

The **undo flow-queue-profile** command deletes the created flow queue profile.

By default, the system predefines a flow queue profile **default**.

Format

flow-queue-profile *flow-queue-profile-name*

undo flow-queue-profile *flow-queue-profile-name*

Parameters

Parameter	Description	Value
flow-queue-profile-name	Specifies the name of a flow queue profile.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring congestion management and traffic shaping parameters of a flow queue, you can run the **flow-queue-profile** *flow-queue-profile-name* command to create a flow queue profile and define parameters in the profile. To set the same scheduling mode and weight for different flow queues, reference the same flow queue profile.

Precautions

The flow queue profile **default** cannot be modified or deleted.

Follow-up Procedure

Configure congestion management and traffic shaping parameters of a flow queue and reference the flow queue WRED drop profile in the flow queue profile view.

Example

# Create flow queue profile **test**.

```
<HUAWEI> system-view
[HUAWEI] flow-queue-profile test
[HUAWEI-flow-queue-test]
```

Related Topics

15.9.4 display flow-queue-profile

15.9.9 flow-wred-profile

Function

The **flow-wred-profile** command creates a flow queue WRED drop profile or displays the view of an existing flow queue WRED drop profile.

The **undo flow-wred-profile** command deletes the created flow queue WRED drop profile.

By default, the system predefines a flow queue WRED drop profile **default**.

Format

flow-wred-profile *flow-wred-profile-name*

undo flow-wred-profile *flow-wred-profile-name*

Parameters

Parameter	Description	Value
flow-wred-profile-name	Specifies the name of a flow queue WRED drop profile.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring WRED parameters of a flow queue, you can run the **flow-wred-profile** *flow-wred-profile-name* command to create a flow queue WRED drop profile and define parameters in the profile. To use the same upper and lower drop thresholds and maximum drop probability for different flow queues, reference the same flow queue WRED drop profile.

Precautions

The flow queue WRED drop profile **default** cannot be modified or deleted.

Follow-up Procedure

Configure WRED parameters of the flow queue and queue length in the flow queue WRED drop profile view.

Example

# Create flow queue WRED drop profile **test**.

```
<HUAWEI> system-view
[HUAWEI] flow-wred-profile test
[HUAWEI-flow-wred-test]
```

Related Topics

15.9.2 color (flow queue WRED drop profile view)

15.9.5 display flow-wred-profile

15.9.10 map flow-queue (flow mapping profile view)

Function

The **map flow-queue** command configures the mapping between flow queues and interface queues.

The **undo map flow-queue** command restores the default mapping between flow queues and interface queues.

By default, a flow queue maps to an interface queue.

Format

map flow-queue *flow-queue-index* **to port-queue** *port-queue-index*

undo map flow-queue *flow-queue-index*

Parameters

Parameter	Description	Value
flow-queue *flow-queue-index*	Specifies the index of a flow queue.	The value is an integer that ranges from 0 to 7.
port-queue *port-queue-index*	Specifies the index of an interface queue.	The value is an integer that ranges from 0 to 7.

Views

Flow mapping profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a flow queue maps to an interface queue, that is, flow queues 0 to 7 maps to interface queues 0 to 7 respectively. To change the default mapping, run this command so that specified services in a subscriber queue enter interface queues with different priorities for scheduling and other QoS processing according to service requirements.

Prerequisites

A flow mapping profile has been created and the flow mapping profile view has been displayed.

Example

# Configure flow mapping profile **map1** and map flow queue 1 to interface queue 2.

```
<HUAWEI> system-view
[HUAWEI] flow-mapping-profile map1
[HUAWEI-flow-mapping-map1] map flow-queue 1 to port-queue 2
```

Related Topics

15.9.7 flow-mapping-profile

15.9.3 display flow-mapping-profile

15.9.11 qos queue (flow queue profile view)

Function

The **qos queue** command sets the scheduling mode, traffic shaping rate, and referenced flow queue WRED drop profile.

The **undo qos queue** command restores the default scheduling mode, traffic shaping rate, and referenced flow queue WRED drop profile.

By default, a flow queue uses PQ scheduling, PIR of a subscriber queue as the traffic shaping rate, and flow queue WRED drop profile **default**.

Format

qos queue *queue-index* { { **pq** | **wfq weight** *weight-value* } | { **shaping** { *shaping-value* | **shaping-percentage** *shaping-percentage-value* } } | { **flow-wred-profile** *flow-wred-profile-name* } } *

undo qos queue *queue-index* { { **pq** | **wfq** } | **shaping** | **flow-wred-profile** } *

Parameters

Parameter	Description	Value
queue-index	Specifies the index of a flow queue.	The value is an integer that ranges from 0 to 7.
pq	Indicates PQ scheduling.	-
wfq	Indicates WFQ scheduling.	-
weight *weight-value*	Specifies the weight of WFQ scheduling.	The value is an integer that ranges from 1 to 100.
shaping *shaping-value*	Specifies the traffic shaping rate.	The value is an integer that ranges from 64 to 10000000, in kbit/s.
shaping-percentage *shaping-percentage-value*	Specifies the traffic shaping percentage, that is, percentage of the traffic shaping rate to the PIR of a subscriber queue.	The value is an integer that ranges from 1 to 100.
flow-wred-profile *flow-wred-profile-name*	Specifies the name of a flow queue WRED drop profile.	The value must be the name of an existing flow queue WRED drop profile.

Views

Flow queue profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To manage packets in a flow queue, run this command to set the scheduling mode, traffic shaping rate, and referenced flow queue WRED drop profile.

Prerequisites

A flow queue profile has been created and the flow queue profile view has been displayed.

Precautions

The scheduling mode, traffic shaping rate, and flow queue WRED drop profile can be configured in any sequence. You can configure the scheduling mode, traffic shaping rate, and flow queue WRED drop profile independently or a combination of them.

Example

# Configure flow queue profile **flow1** where the WFQ weight of flow queue 0 is 50%, the traffic shaping percentage is 50%, and referenced flow queue WRED drop profile is **wred1**.

```
<HUAWEI> system-view
[HUAWEI] flow-queue-profile flow1
[HUAWEI-flow-queue-flow1] qos queue 0 wfq weight 50 shaping shaping-percentage 50 flow-wred-profile wred1
```

Related Topics

15.9.8 flow-queue-profile

15.9.4 display flow-queue-profile

15.9.12 queue-depth (flow queue WRED drop profile view)

Function

The **queue-depth** command sets the length of a flow queue.

The **undo queue-depth** command restores the default length of a flow queue.

By default, the length of a flow queue is 1048576 bytes.

Format

queue-depth *queue-depth-value*

undo queue-depth

Parameters

Parameter	Description	Value
queue-depth-value	Specifies the length of a flow queue.	The value is an integer that ranges from 1024 to 67092480, in bytes. The default value is 1048576.

Views

Flow queue WRED drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets entering flow queues are processed based on parameters in a flow queue WRED drop profile, the percentage of the packet length to the flow queue length needs to be calculated. When the percentage reaches the lower drop threshold, the device discards packets based on the drop probability. When the percentage reaches the upper drop threshold, the device discards all subsequent packets. You can adjust the flow queue length to optimize the congestion avoidance effect.

Prerequisites

A flow queue WRED drop profile has been created and the flow queue WRED drop profile view has been displayed.

Precautions

When a small flow queue length is used, the delay of packets passing a queue is shortened but the queue buffer capability is lowered. When a large flow queue length is used, the queue buffer capability is improved but the delay of packets passing a queue is extended. In addition, when congestion occurs in a flow queue, many buffer resources are occupied. In this case, packets in other flow queues may be discarded due to insufficient buffer resources. Therefore, the default flow queue length is recommended.

Example

# Configure flow queue WRED drop profile **wred1** and set the flow queue length to 2000 bytes.

```
<HUAWEI> system-view
[HUAWEI] flow-wred-profile wred1
[HUAWEI-flow-wred-wred1] queue-depth 2000
```

Related Topics

15.9.9 flow-wred-profile

15.9.5 display flow-wred-profile

15.9.13 reset traffic-user-queue statistics

Function

The **reset traffic-user-queue statistics** command clears traffic statistics on subscriber queues.

Format

reset traffic-user-queue statistics interface *interface-type interface-number* **outbound acl** { *bas-acl* | *adv-acl* } [**acl** { *l2-acl* | **name** *acl-name* }]

reset traffic-user-queue statistics interface *interface-type interface-number* **outbound acl** *l2-acl* [**acl** { *bas-acl* | *adv-acl* | **name** *acl-name* }]

reset traffic-user-queue statistics interface *interface-type interface-number* **outbound acl name** *acl-name* [**acl** { *bas-acl* | *adv-acl* | *l2-acl* | **name** *acl-name* }]

reset traffic-user-queue statistics interface *interface-type interface-number* **outbound acl ipv6** { *bas-acl* | *adv-acl* | **name** *acl-name* }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears traffic statistics on subscriber queues on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
outbound	Clears traffic statistics on subscriber queues in the outbound direction on an interface.	-
acl	Clears traffic statistics on subscriber queues based on IPv4 ACLs.	-
ipv6	Clears traffic statistics on subscriber queues based on IPv6 ACLs.	-
bas-acl	Clears traffic statistics on subscriber queues based on basic ACLs.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Clears traffic statistics on subscriber queues based on advanced ACLs.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Clears traffic statistics on subscriber queues based on Layer 2 ACLs.	The value is an integer that ranges from 4000 to 4999.
name *acl-name*	Clears traffic statistics on subscriber queues based on named ACLs. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before recollecting traffic statistics on subscriber queues in a given period of time, run this command to clear existing traffic statistics on subscriber queues.

Precautions

The cleared traffic statistics on subscriber queues cannot be restored. Exercise caution when you run this command.

Example

# Clear traffic statistics on subscriber queues based on ACL 3009 in the outbound direction on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] acl 3009
[HUAWEI-acl-adv-3009] rule 1 permit ip
[HUAWEI-acl-adv-3009] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-user-queue outbound acl 3009 pir 2000
[HUAWEI-GigabitEthernet0/0/1] return
<HUAWEI> reset traffic-user-queue statistics interface gigabitethernet 0/0/1 outbound acl 3009
```

Related Topics

15.9.14 traffic-user-queue (interface view)

15.9.14 traffic-user-queue (interface view)

Function

The **traffic-user-queue** command creates a subscriber queue on an interface to implement HQoS.

The **undo traffic-user-queue** command deletes a subscriber queue on an interface.

By default, no subscriber queue is configured on an interface.

Format

If a single ACL is used, use the following command:

traffic-user-queue outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } } **pir** *pir-value* [**flow-queue-profile** *flow-queue-profile-name* | **flow-mapping-profile** *flow-mapping-profile-name*] *

undo traffic-user-queue outbound acl { [**ipv6**] { *bas-acl* | *adv-acl* | **name** *acl-name* } }

If both Layer 2 and Layer 3 ACLs are configured, use the following command:

traffic-user-queue outbound acl { *l2-acl* | **name** *acl-name* } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* } **pir** *pir-value* [**flow-queue-profile** *flow-queue-profile-name* | **flow-mapping-profile** *flow-mapping-profile-name*] *

undo traffic-user-queue outbound acl { *l2-acl* | **name** *acl-name* } **acl** { *bas-acl* | *adv-acl* | **name** *acl-name* }

traffic-user-queue outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } **acl** { *l2-acl* | **name** *acl-name* } **pir** *pir-value* [**flow-queue-profile** *flow-queue-profile-name* | **flow-mapping-profile** *flow-mapping-profile-name*] *

undo traffic-user-queue outbound acl { *bas-acl* | *adv-acl* | **name** *acl-name* } **acl** { *l2-acl* | **name** *acl-name* }

Parameters

Parameter	Description	Value
outbound	Creates a subscriber queue in the outbound direction on an interface to implement HQoS scheduling.	-
acl	Creates a subscriber queue based on IPv4 ACLs to implement HQoS scheduling.	-
ipv6	Creates a subscriber queue based on IPv6 ACLs to implement HQoS scheduling.	-
bas-acl	Creates a subscriber queue based on basic ACLs to implement HQoS scheduling.	The value is an integer that ranges from 2000 to 2999.
adv-acl	Creates a subscriber queue based on advanced ACLs to implement HQoS scheduling.	The value is an integer that ranges from 3000 to 3999.
l2-acl	Creates a subscriber queue based on Layer 2 ACLs to implement HQoS scheduling.	The value is an integer that ranges from 4000 to 4999.

Parameter	Description	Value
name *acl-name*	Creates a subscriber queue based on named ACLs to implement HQoS scheduling. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.
pir *pir-value*	Specifies the peak information rate (PIR) of a subscriber queue, which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 10000000, in kbit/s.
flow-queue-profile *flow-queue-profile-name*	Specifies the name of the referenced flow queue profile.	The value must be the name of an existing flow queue profile.
flow-mapping-profile *flow-mapping-profile-name*	Specifies the name of the referenced flow mapping profile.	The value must be the name of an existing flow mapping profile.

Views

GE interface view, XGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Multiple users can be differentiated based on ACL rules. When different scheduling and shaping parameters need to be set for different users and differentiated services need to be provided for different service traffic of the same user, run the **traffic-user-queue** command to configure multiple subscriber queues, set different scheduling modes and traffic shaping rates, and reference different flow queue profiles and flow mapping profiles to implement fine-granular scheduling.

Prerequisites

The **acl (system view)** or **acl name** command has been executed to create an ACL.

Example

# Create a subscriber queue based on ACLs on the GE0/0/1 to implement HQoS.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[HUAWEI-acl-adv-3000] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-user-queue outbound acl 3000 pir 1000 flow-queue-profile
flow1 flow-mapping-profile map1
```

Related Topics

14.1.5 acl (system view)

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

15.9.7 flow-mapping-profile

15.9.8 flow-queue-profile

15.9.15 user-queue (qos-profile view)

Function

The **user-queue** command creates a subscriber queue in a QoS profile to implement HQoS.

The **undo user-queue** command deletes a subscriber queue from a QoS profile.

By default, no subscriber queue is configured in a QoS profile.

Format

user-queue pir *pir-value* [**flow-queue-profile** *flow-queue-profile-name*] [**flow-mapping-profile** *flow-mapping-profile-name*]

undo user-queue

Parameters

Parameter	Description	Value
pir *pir-value*	Specifies the peak information rate (PIR) of a subscriber queue, which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Parameter	Description	Value
flow-queue-profile *flow-queue-profile-name*	Specifies the name of the referenced flow queue profile. If the name of the referenced flow queue profile is not specified, the flow queue profile **default** is used.	The value must be the name of an existing flow queue profile.
flow-mapping-profile *flow-mapping-profile-name*	Specifies the name of the referenced flow mapping profile. If the name of the referenced flow mapping profile is not specified, the flow mapping profile **default** is used.	The value must be the name of an existing flow mapping profile.

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure HQoS for authentication users to implement fine-granular scheduling, run the **user-queue** command to create subscriber queues, set different traffic shaping rates, and reference different flow queue profiles and flow mapping profiles.

Prerequisites

A QoS profile has been created using the **qos-profile** command.

The user-defined flow queue profile and flow mapping profile have been created using the **flow-queue-profile** and **flow-mapping-profile** commands respectively. If the user-defined flow queue profile and flow mapping profile are not required, use the default ones.

Example

# Configure a user queue in the QoS profile **huawei** to implement HQoS.

```
<HUAWEI> system-view
[HUAWEI] qos-profile name huawei
[HUAWEI-qos-huawei] user-queue pir 1000 flow-queue-profile flow1 flow-mapping-profile map1
```

Related Topics

15.3.12 qos-profile

15.9.7 flow-mapping-profile

15.9.8 flow-queue-profile