HP 6125XLG Blade Switch

ACL and QoS

Command Reference

Part number: 5998-5353a
Software version: Release 240x
Document version: 6W101-20150515

Legal and notice information

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Contents

ACL commands

acl

Use **acl** to create an ACL, and enter its view. If the ACL has been created, you directly enter its view.

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

Syntax

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

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

Default

No ACL exists.

Views

System view

Predefined user roles

network-admin

Parameters

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

- 2000 to 2999 for IPv4 basic ACLs if the **ipv6** keyword is not specified and for IPv6 basic ACLs if the **ipv6** keyword is specified.
- 3000 to 3999 for IPv4 advanced ACLs s if the **ipv6** keyword is not specified and for IPv6 advanced ACLs if the **ipv6** keyword is specified.
- 4000 to 4999 for Ethernet frame header ACLs. This entry is not displayed if the **ipv6** keyword is specified.

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

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

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

all: Specifies all ACLs.

- If the **ipv6** keyword is not specified, all ACLs refer to all IPv4 basic, IPv4 advanced, and Ethernet frame header ACLs.
- If the **ipv6** keyword is specified, all ACLs refer to all IPv6 basic and IPv6 advanced ACLs.

Usage guidelines

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

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

Examples

Create IPv4 basic ACL 2000, and enter its view.

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

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

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

Related commands

display acl

acl copy

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

Syntax

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

Views

System view

Predefined user roles

network-admin

Parameters

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

- 2000 to 2999 for IPv4 basic ACLs if the **ipv6** keyword is not specified and for IPv6 basic ACLs if the **ipv6** keyword is specified.
- 3000 to 3999 for IPv4 advanced ACLs s if the **ipv6** keyword is not specified and for IPv6 advanced ACLs if the **ipv6** keyword is specified.
- 4000 to 4999 for Ethernet frame header ACLs. This entry is not displayed if the **ipv6** keyword is specified.

name *source-acl-name*: Specifies an existing source ACL by its name. The *source-acl-name* argument is a case-insensitive string of 1 to 63 characters. For a basic ACL or advanced ACL, if you do not specify the **ipv6** keyword, this option specifies the name of an IPv4 basic ACL or advanced ACL; if you specify the **ipv6** keyword, this option specifies the name of an IPv6 basic ACL or advanced ACL.

dest-acl-number: Assigns a unique number to the ACL you are creating. This number must be from the same ACL category as the source ACL. If no ACL number is specified, the system automatically picks the smallest number from all available numbers in the same ACL category as the source ACL. Available value ranges include:

- 2000 to 2999 for IPv4 basic ACLs if the **ipv6** keyword is not specified and for IPv6 basic ACLs if the **ipv6** keyword is specified.
- 3000 to 3999 for IPv4 advanced ACLs s if the **ipv6** keyword is not specified and for IPv6 advanced ACLs if the **ipv6** keyword is specified.

- 4000 to 4999 for Ethernet frame header ACLs. This entry is not displayed if the **ipv6** keyword is specified.

name *dest-acl-name*: Assigns a unique name to the ACL you are creating. The *dest-acl-name* is a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion, it cannot be **all**. If no ACL name is specified, the system does not name the ACL. For a basic ACL or advanced ACL, if you do not specify the **ipv6** keyword, this option specifies the name of an IPv4 basic ACL or advanced ACL; if you specify the **ipv6** keyword, this option specifies the name of an IPv6 basic ACL or advanced ACL.

Usage guidelines

The new ACL has the same properties and content as the source ACL, but not the same ACL number and name.

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

Examples

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

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

acl logging interval

Use **acl logging interval** to set the interval for generating and outputting packet filtering logs. The log information includes the number of matching packets and the matched ACL rules.

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

Syntax

acl [**ipv6**] **logging interval** *interval*

undo acl [**ipv6**] **logging interval**

Default

The interval is 0. No packet filtering logs are generated.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval in minutes at which packet filtering logs are generated and output. It must be a multiple of 5 and in the range of 0 to 1440. To disable generating packet filtering logs, assign 0 to the argument.

Usage guidelines

The system collects packet filtering logs for only IPv4 basic, IPv4 advanced, IPv6 basic, and IPv6 advanced ACL rules that have the **logging** keyword.

When the **ipv6** keyword is not specified, this command sets the interval for generating and outputting IPv4 packet filtering logs.

When the **ipv6** keyword is specified, this command sets the interval for generating and outputting IPv6 packet filtering logs.

Examples

Enable the device to generate and output IPv4 packet filtering logs at 10-minute intervals.

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

Related commands

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

acl name

Use **acl name** to enter the view of an ACL that has a name.

Syntax

acl [**ipv6**] **name** *acl-name*

Views

System view

Predefined user roles

network-admin

Parameters

acl-name: Specifies the name of an ACL, a case-insensitive string of 1 to 63 characters. It must start with an English letter. The ACL must already exist. For a basic ACL or advanced ACL, if you do not specify the **ipv6** keyword, this option specifies the name of an IPv4 basic ACL or advanced ACL. If you specify the **ipv6** keyword, this option specifies the name of an IPv6 basic ACL or advanced ACL.

Examples

Enter the view of IPv4 basic ACL **flow**, which already exists.

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

Enter the view of IPv6 basic ACL **flow**, which already exists.

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

Related commands

acl

description

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

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

Syntax

description *text*

undo description

Default

An ACL has no description.

Views

IPv4/IPv6 basic ACL view

IPv4/IPv6 advanced ACL view

Ethernet frame header ACL view

Predefined user roles

network-admin

Parameters

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

Examples

Configure a description for IPv4 basic ACL 2000.

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

Related commands

display acl

display acl

Use **display acl** to display configuration and match statistics for ACLs.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

acl-number: Specifies an ACL by its number:

- 2000 to 2999 for IPv4 basic ACLs if the **ipv6** keyword is not specified and for IPv6 basic ACLs if the **ipv6** keyword is specified.
- 3000 to 3999 for IPv4 advanced ACLs s if the **ipv6** keyword is not specified and for IPv6 advanced ACLs if the **ipv6** keyword is specified.

- 4000 to 4999 for Ethernet frame header ACLs. This entry is not displayed if the **ipv6** keyword is specified.

all: Displays information about all IPv4 basic, IPv4 advanced, and Ethernet frame header ACLs if you do not specify the **ipv6** keyword, or displays information about all IPv6 basic and IPv6 advanced ACLs if you specify the **ipv6** keyword.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. For a basic ACL or advanced ACL, if you do not specify the **ipv6** keyword, this option specifies the name of an IPv4 basic ACL or advanced ACL. If you specify the **ipv6** keyword, this option specifies the name of an IPv6 basic ACL or advanced ACL.

Usage guidelines

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

Examples

Display configuration and match statistics for IPv4 basic ACL 2001.

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

Table 1 Command output

Field	Description
Basic ACL 2001	Category and number of the ACL. The following field information is about IPv4 basic ACL 2000.
named flow	The name of the ACL is flow. If the ACL is not named, this field displays **-none-**.
1 rule	The ACL contains one rule.
match-order is auto	The match order for the ACL is auto, which sorts ACL rules in depth-first order. This field is not present when the match order is **config**.
This is an IPv4 basic ACL.	Description of this ACL.
ACL's step is 5	The rule numbering step is 5.
rule 5 permit source 1.1.1.1 0	Content of rule 5.
5 times matched	There have been five matches for the rule. The statistic counts only ACL matches performed in software. This field is not displayed when no packets matched the rule.
rule 5 comment This rule is used on Ten-GigabitEthernet 1/1/5.	Comment of ACL rule 5.

display packet-filter

Use **display packet-filter** to display whether an ACL has been successfully applied to an interface for packet filtering.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. VLAN interfaces are not supported. If no interface is specified, the command displays ACL application information on all interfaces except VLAN interfaces for packet filtering.

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

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument represents the ID of the IRF member device. If no IRF member device is specified, the command displays ACL application information for packet filtering on the master.

Usage guidelines

If you specify neither the **inbound** keyword nor the **outbound** keyword, the command displays the ACL application information for both inbound and outbound packet filtering.

Examples

Display ACL application information for inbound packet filtering on interface Ten-GigabitEthernet 1/1/5.

```
<Sysname> display packet-filter interface ten-gigabitethernet 1/1/5 inbound
Interface: Ten-GigabitEthernet1/1/5
In-bound policy:
  ACL 2001, Hardware-count
  ACL6 2002
  IPv4 default action: Deny
  IPv6 default action: Deny
 Out-bound policy:
  ACL 2001
  IPv4 default action: Deny
```

Table 2 Command output

Field	Description
Interface	Interface to which the ACL applies.
In-bound policy	ACL used for filtering incoming traffic.
Out-bound policy	ACL used for filtering outgoing traffic.
ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
Hardware-count	Successfully enables counting ACL rule matches.

Field	Description
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs. This field is displayed only when the default action is **deny**.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs. This field is displayed only when the default action is **deny**.
MAC default action	Packet filter default action for packets that do not match any Ethernet frame header ACLs. This field is displayed only when the default action is **deny**.

display packet-filter statistics

Use **display packet-filter statistics** to display match statistics of ACLs for packet filtering.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Displays the statistics of an interface specified by its type and number.

inbound: Displays the statistics in the inbound direction.

outbound: Displays the statistics in the outbound direction.

acl-number: Specifies the number of an ACL:

- 2000 to 2999 for IPv4 basic ACLs if the **ipv6** keyword is not specified and for IPv6 basic ACLs if the **ipv6** keyword is specified.
- 3000 to 3999 for IPv4 advanced ACLs s if the **ipv6** keyword is not specified and for IPv6 advanced ACLs if the **ipv6** keyword is specified.
- 4000 to 4999 for Ethernet frame header ACLs. This entry is not displayed if the **ipv6** keyword is specified.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. For a basic ACL or advanced ACL, if you do not specify the **ipv6** keyword, this option specifies the name of an IPv4 basic ACL or advanced ACL. If you specify the **ipv6** keyword, this option specifies the name of an IPv6 basic ACL or advanced ACL.

brief: Displays brief statistics.

Usage guidelines

When neither *acl-number* nor **name** *acl-name* is specified, this command displays match statistics of all ACLs for packet filtering.

Examples

Display match statistics of all ACLs for inbound packet filtering on Ten-GigabitEthernet 1/1/5.

```
<Sysname> display packet-filter statistics interface ten-gigabitethernet 1/1/5 inbound
Interface: Ten-GigabitEthernet1/1/5
 In-bound policy:
  ACL 2001, Hardware-count
   From 2011-06-04 10:25:21 to 2011-06-04 10:35:57
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0

  IPv4 default action: Deny
```

Table 3 Command output

Field	Description
Interface	Interface to which the ACL applies.
In-bound policy	ACL used for filtering incoming traffic.
Out-bound policy	ACL used for filtering outgoing traffic.
ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
Hardware-count	Successfully enables counting ACL rule matches.
From 2011-06-04 10:25:21 to 2011-06-04 10:35:57	Start time and end time of the statistics.
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs. This field is displayed only when the default action is **deny**.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs. This field is displayed only when the default action is **deny**.
MAC default action	Packet filter default action for packets that do not match any Ethernet frame header ACLs. This field is displayed only when the default action is **deny**.

Related commands

reset packet-filter statistics

display packet-filter statistics sum

Use **display packet-filter statistics sum** to display accumulated packet filtering ACL statistics.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

inbound: Displays the statistics in the inbound direction.

outbound: Displays the statistics in the outbound direction.

acl-number: Specifies the number of an ACL:

- 2000 to 2999 for IPv4 basic ACLs if the **ipv6** keyword is not specified and for IPv6 basic ACLs if the **ipv6** keyword is specified.
- 3000 to 3999 for IPv4 advanced ACLs s if the **ipv6** keyword is not specified and for IPv6 advanced ACLs if the **ipv6** keyword is specified.
- 4000 to 4999 for Ethernet frame header ACLs. This entry is not displayed if the **ipv6** keyword is specified.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. For a basic ACL or advanced ACL, if you do not specify the **ipv6** keyword, this option specifies the name of an IPv4 basic ACL or advanced ACL; if you specify the **ipv6** keyword, this option specifies the name of an IPv6 basic ACL or advanced ACL.

brief: Displays brief accumulated packet filtering ACL statistics.

Examples

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

```
<Sysname> display packet-filter statistics sum inbound 2001
Sum:
 In-bound policy:
  ACL 2001
   rule 0 permit source 2.2.2.2 0 (2 packets)
   rule 5 permit source 1.1.1.1 0
   Totally 2 packets permitted, 0 packets denied
   Totally 100% permitted, 0% denied
```

Table 4 Command output

Field	Description
Sum	Accumulated packet filtering ACL statistics.
In-bound policy	Accumulated ACL statistics used for filtering incoming traffic.
Out-bound policy	Accumulated ACL statistics used for filtering outgoing traffic.
ACL 2001	Accumulated ACL statistics used for IPv4 basic ACL 2001.

Field	Description
2 packets	Two packets matched the rule. This field is not displayed when no packets matched the rule.
Totally 2 packets permitted, 0 packets denied	Number of packets permitted and denied by the ACL.
Totally 100% permitted, 0% denied	Ratios of permitted and denied packets to all packets.

Related commands

reset packet-filter statistics

display packet-filter verbose

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

acl-number: Specifies the number of an ACL:

- 2000 to 2999 for IPv4 basic ACLs if the **ipv6** keyword is not specified and for IPv6 basic ACLs if the **ipv6** keyword is specified.
- 3000 to 3999 for IPv4 advanced ACLs s if the **ipv6** keyword is not specified and for IPv6 advanced ACLs if the **ipv6** keyword is specified.
- 4000 to 4999 for Ethernet frame header ACLs. This entry is not displayed if the **ipv6** keyword is specified.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. For a basic ACL or advanced ACL, if you do not specify the **ipv6** keyword, this option specifies the name of an IPv4 basic ACL or advanced ACL. If you specify the **ipv6** keyword, this option specifies the name of an IPv6 basic ACL or advanced ACL.

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument represents the ID of the IRF member device. If no IRF member device is specified, the command displays ACL application details for packet filtering on the master.

Usage guidelines

When neither *acl-number* nor **name** *acl-name* is specified, this command displays application details of all ACLs for packet filtering.

Examples

Display application details of all ACLs for inbound packet filtering on Ten-GigabitEthernet 1/1/5.

```
<Sysname> display packet-filter verbose interface ten-gigabitethernet 1/1/5 inbound
Interface: Ten-GigabitEthernet1/1/5
 In-bound policy:
  ACL 2001, Hardware-count
   rule 0 permit
   rule 5 permit source 1.1.1.1 0

  ACL6 2000, Hardware-count
   rule 0 permit

  ACL 4000, Hardware-count

  IPv4 default action: Deny

  IPv6 default action: Deny

  MAC default action: Deny
```

Table 5 Command output

Field	Description
Interface	Interface to which the ACL applies.
In-bound policy	ACL used for filtering incoming traffic.
Out-bound policy	ACL used for filtering outgoing traffic.
ACL 2001	IPv4 basic ACL 2001 has been successfully applied.
Hardware-count	Successfully enables counting ACL rule matches.
IPv4 default action	Packet filter default action for packets that do not match any IPv4 ACLs. This field is displayed only when the default action is **deny**.
IPv6 default action	Packet filter default action for packets that do not match any IPv6 ACLs. This field is displayed only when the default action is **deny**.
MAC default action	Packet filter default action for packets that do not match any Ethernet frame header ACLs. This field is displayed only when the default action is **deny**.

display qos-acl resource

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument represents the ID of the IRF member device. If no IRF member device is specified, the command displays QoS and ACL resource usage on all member devices.

Usage guidelines

The command does not display any usage data if the specified IRF member device does not support counting QoS and ACL resources.

Examples

Display QoS and ACL resource usage.

```
<Sysname> display qos-acl resource
Interfaces: XGE1/0/1 to XGE1/0/20, FGE1/1/1 to FGE1/1/4
            XGE1/1/5 to XGE1/1/12
-------------------------------------------------------------------------
 Type              Total      Reserved   Configured Remaining  Usage
-------------------------------------------------------------------------
 VFP ACL           1024       512        0          512        50%
 IFP ACL           2048       1536       0          512        75%
 IFP Meter         1024       768        0          256        75%
 IFP Counter       1024       768        0          256        75%
 EFP ACL           1024       0          0          1024       0%
 EFP Meter         512        0          0          512        0%
 EFP Counter       512        0          0          512        0%
```

Table 6 Command output

Field	Description
Interfaces	Interface range for the resources.
Type	Resource type: • **VFP ACL**—ACL rules for local QoS ID remarking before Layer 2 forwarding. • **IFP ACL**—ACL rules applied to inbound traffic. • **IFP Meter**—Traffic policing rules for inbound traffic. • **IFP Counter**—Traffic counting rules for inbound traffic. • **EFP Meter**—Traffic policing rules for outbound traffic. • **EFP Counter**—Traffic counting rules for outbound traffic.
Total	Total number of resources.

Field	Description
Reserved	Number of reserved resources.
Configured	Number of resources that have been applied.
Remaining	Number of resources that you can apply.
Usage	Percent of the configured and reserved resources to the total resources. If the percent is a non-integer, this field displays the integer part. For example, if the actual usage is 50.8%, this field displays 50%.

packet-filter

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

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

Syntax

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

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

Default

An interface does not filter packets.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view, VLAN interface view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number:

- 2000 to 2999 for IPv4 basic ACLs if the **ipv6** keyword is not specified and for IPv6 basic ACLs if the **ipv6** keyword is specified.
- 3000 to 3999 for IPv4 advanced ACLs s if the **ipv6** keyword is not specified and for IPv6 advanced ACLs if the **ipv6** keyword is specified.
- 4000 to 4999 for Ethernet frame header ACLs. This entry is not displayed if the **ipv6** keyword is specified.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. For a basic ACL or advanced ACL, if you do not specify the **ipv6** keyword, this option specifies the name of an IPv4 basic ACL or advanced ACL. If you specify the **ipv6** keyword, this option specifies the name of an IPv6 basic ACL or advanced ACL.

inbound: Filters incoming packets.

outbound: Filters outgoing packets.

hardware-count: Enables counting ACL rule matches performed in hardware. This keyword enables match counting for all rules in an ACL, and the **counting** keyword in the **rule** command enables match counting specific to rules. If the **hardware-count** keyword is not specified, rule matches for the ACL are not counted.

Examples

Apply IPv4 basic ACL 2001 to filter incoming traffic on Ten-GigabitEthernet 1/1/5, and enable counting ACL rule matches performed in hardware.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] packet-filter 2001 inbound hardware-count
```

Related commands

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

packet-filter default deny

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

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

Syntax

packet-filter default deny

undo packet-filter default deny

Default

The packet filter permits packets that do not match any ACL rule.

Views

System view

Predefined user roles

network-admin

Usage guidelines

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

Examples

Set the packet filter default action to **deny**.

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

Related commands

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

reset acl counter

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

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

acl-number: Specifies an ACL by its number:

- 2000 to 2999 for IPv4 basic ACLs if the **ipv6** keyword is not specified and for IPv6 basic ACLs if the **ipv6** keyword is specified.
- 3000 to 3999 for IPv4 advanced ACLs s if the **ipv6** keyword is not specified and for IPv6 advanced ACLs if the **ipv6** keyword is specified.
- 4000 to 4999 for Ethernet frame header ACLs. This entry is not displayed if the **ipv6** keyword is specified.

all: Clears statistics for all IPv4 basic, IPv4 advanced, and Ethernet frame header ACLs if you do not specify the **ipv6** keyword, or clears statistics for all IPv6 basic and IPv6 advanced ACLs if you specify the **ipv6** keyword.

name *acl-name*: Clears statistics of an ACL specified by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. For a basic ACL or advanced ACL, if you do not specify the **ipv6** keyword, this option specifies the name of an IPv4 basic ACL or advanced ACL. If you specify the **ipv6** keyword, this option specifies the name of an IPv6 basic ACL or advanced ACL.

Examples

Clear statistics for IPv4 basic ACL 2001.

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

Related commands

display acl

reset packet-filter statistics

Use **reset packet-filter statistics** to clear the match statistics (including the accumulated statistics) of ACLs for packet filtering.

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

interface [*interface-type interface-number*]: Specifies an interface by its type and number. If no interface is specified, the command clears packet filtering ACL statistics on all interfaces.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

acl-number: Specifies an ACL by its number:

- 2000 to 2999 for IPv4 basic ACLs if the **ipv6** keyword is not specified and for IPv6 basic ACLs if the **ipv6** keyword is specified.
- 3000 to 3999 for IPv4 advanced ACLs s if the **ipv6** keyword is not specified and for IPv6 advanced ACLs if the **ipv6** keyword is specified.
- 4000 to 4999 for Ethernet frame header ACLs. This entry is not displayed if the **ipv6** keyword is specified.

name *acl-name*: Specifies an ACL by its name. The *acl-name* argument is a case-insensitive string of 1 to 63 characters. It must start with an English letter. For a basic ACL or advanced ACL, if you do not specify the **ipv6** keyword, this option specifies the name of an IPv4 basic ACL or advanced ACL. If you specify the **ipv6** keyword, this option specifies the name of an IPv6 basic ACL or advanced ACL.

Usage guidelines

When neither *acl-number* nor **name** *acl-name* is specified, this command clears the match statistics of all ACLs for packet filtering.

Examples

Clear IPv4 basic ACL 2001 statistics for inbound packet filtering of interface Ten-GigabitEthernet 1/1/5.

```
<Sysname> reset packet-filter statistics interface ten-gigabitethernet 1/1/5 inbound 2001
```

Related commands

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

rule (Ethernet frame header ACL view)

Use **rule** to create or edit an Ethernet frame header ACL rule.

Use **undo rule** to delete an Ethernet frame header ACL rule or some attributes in the rule.

Syntax

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

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

Default

An Ethernet frame header ACL does not contain any rule.

Views

Ethernet frame header ACL view

Predefined user roles

network-admin

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

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

counting: Counts the number of times the Ethernet frame header ACL rule has been matched. The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted.

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

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

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

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

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

Usage guidelines

When an Ethernet frame header ACL with the **lsap** keyword specified is used for QoS traffic classification or packet filtering, the *lsap-type* argument must be AAAA and the *lsap-type-mask* argument must be FFFF. Otherwise, the ACL cannot be applied successfully.

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

You can edit ACL rules only when the match order is **config**. If no optional keywords are provided for the **undo rule** command, you delete the entire rule. If optional keywords or arguments are provided, you delete the specified attributes.

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

Examples

Create a rule in Ethernet frame header ACL 4000 to permit ARP packets and deny RARP packets.

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

Related commands

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

rule (IPv4 advanced ACL view)

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

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

Syntax

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

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

Default

An IPv4 advanced ACL does not contain any rule.

Views

IPv4 advanced ACL view

Predefined user roles

network-admin

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

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

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

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

Parameters	Function	Description
source { *source-address source-wildcard* | **any** }	Specifies a source address.	The *source-address source-wildcard* arguments represent a source IP address and wildcard mask in dotted decimal notation. An all-zero wildcard specifies a host address. The **any** keyword specifies any source IP address.
destination { *dest-address dest-wildcard* | **any** }	Specifies a destination address.	The *dest-address dest-wildcard* arguments represent a destination IP address and wildcard mask in dotted decimal notation. An all-zero wildcard specifies a host address. The **any** keyword represents any destination IP address.
counting	Counts the number of times the IPv4 advanced ACL rule has been matched.	The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted.
precedence *precedence*	Specifies an IP precedence value.	The *precedence* argument can be a number in the range of 0 to 7, or in words, **routine** (0), **priority** (1), **immediate** (2), **flash** (3), **flash-override** (4), **critical** (5), **internet** (6), or **network** (7).
tos *tos*	Specifies a ToS preference.	The *tos* argument can be a number in the range of 0 to 15, or in words, **max-reliability** (2), **max-throughput** (4), **min-delay** (8), **min-monetary-cost** (1), or **normal** (0).
dscp *dscp*	Specifies a DSCP priority.	The *dscp* argument can be a number in the range of 0 to 63, or in words, **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
fragment	Applies the rule to only non-first fragments.	Without this keyword, the rule applies to all fragments and non-fragments.
logging	Logs matching packets.	This function requires that the module (for example, packet filtering) that uses the ACL supports logging.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the timer range. For more information about time range, see *ACL and QoS Configuration Guide*.
vpn-instance *vpn-instance-name*	Applies the rule to a VPN instance.	The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the rule applies only to non-VPN packets.

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

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

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

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

Table 9 ICMP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
icmp-type { *icmp-type* *icmp-code* | *icmp-message* }	Specifies the ICMP message type and code.	The *icmp-type* argument is in the range of 0 to 255. The *icmp-code* argument is in the range of 0 to 255. The *icmp-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 10.

Table 10 ICMP message names supported in IPv4 advanced ACL rules

ICMP message name	ICMP message type	ICMP message code
echo	8	0
echo-reply	0	0

ICMP message name	ICMP message type	ICMP message code
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

Usage guidelines

If an ACL is for QoS traffic classification or packet filtering:

- Do not specify the **vpn-instance** keyword if the ACL is for outbound QoS traffic classification or outbound packet filtering.
- Do not specify **neq** for the *operator* argument.

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

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

If no optional keywords are provided for the **undo rule** command, you delete the entire rule. If optional keywords or arguments are provided, you delete the specified attributes.

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

Examples

Create an IPv4 advanced ACL rule to permit TCP packets with the destination port 80 from 129.9.0.0/16 to 202.38.160.0/24.

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

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

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

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

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

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

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

Related commands

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**

rule (IPv4 basic ACL view)

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

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

Syntax

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

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

Default

An IPv4 basic ACL does not contain any rule.

Views

IPv4 basic ACL view

Predefined user roles

network-admin

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Counts the number of times the IPv4 basic ACL rule has been matched. The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter** command enables match counting for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted.

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

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

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

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

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

Usage guidelines

If an ACL is for outbound QoS traffic classification or outbound packet filtering, do not specify the **vpn-instance** keyword.

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

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

If no optional keywords are provided for the **undo rule** command, you delete the entire rule. If optional keywords or arguments are provided, you delete the specified attributes.

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

Examples

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

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

```
[Sysname-acl-basic-2000] rule deny source any
```

Related commands

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**

rule (IPv6 advanced ACL view)

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

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

Syntax

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

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

Default

An IPv6 advanced ACL does not contain any rule.

Views

IPv6 advanced ACL view

Predefined user roles

network-admin

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

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

You can set the *protocol* argument to one of the values in Table 11 to match packets with the corresponding IPv6 extended header.

Table 11 Protocol values of IPv6 extended headers

Value of the *protocol* argument	IPv6 extended header
0	Hop-by-Hop Options Header.
43	Routing Header.
44	Fragment Header.
50	Encapsulating Security Payload Header.
51	Authentication Header.
60	Destination Options Header.

Table 12 describes the parameters that you can specify regardless of the value for the *protocol* argument.

Table 12 Match criteria and other rule information for IPv6 advanced ACL rules

Parameters	Function	Description
source { *source-address source-prefix* | *source-address/source-prefix* | **any** }	Specifies a source IPv6 address.	The *source-address* and *source-prefix* arguments represent an IPv6 source address, and prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.
destination { *dest-address dest-prefix* | *dest-address/dest-prefix* | **any** }	Specifies a destination IPv6 address.	The *dest-address* and *dest-prefix* arguments represent a destination IPv6 address, and prefix length in the range of 1 to 128. The **any** keyword specifies any IPv6 destination address.
counting	Counts the number of times the IPv6 advanced ACL rule has been matched.	The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter ipv6** command enables match counting for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted.
dscp *dscp*	Specifies a DSCP preference.	The *dscp* argument can be a number in the range of 0 to 63, or in words, **af11** (10), **af12** (12), **af13** (14), **af21** (18), **af22** (20), **af23** (22), **af31** (26), **af32** (28), **af33** (30), **af41** (34), **af42** (36), **af43** (38), **cs1** (8), **cs2** (16), **cs3** (24), **cs4** (32), **cs5** (40), **cs6** (48), **cs7** (56), **default** (0), or **ef** (46).
flow-label *flow-label-value*	Specifies a flow label value in an IPv6 packet header.	The *flow-label-value* argument is in the range of 0 to 1048575.
fragment	Applies the rule to only non-first fragments.	Without this keyword, the rule applies to all fragments and non-fragments.
logging	Logs matching packets.	This function requires that the module (for example, packet filtering) that uses the ACL supports logging.
routing [**type** *routing-type*]	Specifies routing header types.	*routing-type*: Value of the routing header type, in the range of 0 to 255. If you specify the **type** *routing-type* option, the rule applies to the specified type of routing header. Otherwise, the rule applies to any type of routing header.

Parameters	Function	Description
hop-by-hop [**type** *hop-type*]	Specifies Hop-by-Hop Options header types.	*hop-type*: Value of the Hop-by-Hop Options header type, in the range of 0 to 255. If you specify the **type** *hop-type* option, the rule applies to the specified type of Hop-by-Hop Options header. Otherwise, the rule applies to any type of Hop-by-Hop Options header.
time-range *time-range-name*	Specifies a time range for the rule.	The *time-range-name* argument is a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the timer range. For more information about time range, see *ACL and QoS Configuration Guide*.
vpn-instance *vpn-instance-name*	Applies the rule to a VPN instance.	The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the rule applies only to non-VPN packets.

If the *protocol* argument is **tcp** (6) or **udp** (17), set the parameters shown in Table 13.

Table 13 TCP/UDP-specific parameters for IPv6 advanced ACL rules

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

Parameters	Function	Description
established	Specifies the flags for indicating the established status of a TCP connection.	Parameter specific to TCP. The rule matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument is **icmpv6** (58), set the parameters shown in Table 14.

Table 14 ICMPv6-specific parameters for IPv6 advanced ACL rules

Parameters	Function	Description
icmp6-type { *icmp6-type icmp6-code* | *icmp6-message* }	Specifies the ICMPv6 message type and code.	The *icmp6-type* argument is in the range of 0 to 255. The *icmp6-code* argument is in the range of 0 to 255. The *icmp6-message* argument specifies a message name. Supported ICMP message names and their corresponding type and code values are listed in Table 15.

Table 15 ICMPv6 message names supported in IPv6 advanced ACL rules

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

Usage guidelines

If an ACL is for QoS traffic classification or packet filtering:

- Do not specify the **vpn-instance** or **fragment** keyword.
- Do not specify **neq** for the *operator* argument.

- Do not specify the **routing**, **hop-by-hop**, or **flow-label** keyword if the ACL is for outbound QoS traffic classification or outbound packet filtering.
- Do not specify **ipv6-ah** or **ipv6-esp** for the *protocol* argument, nor set its value to 0, 43, 44, 51, or 60, if the ACL is for outbound QoS traffic classification or outbound packet filtering.

If an ACL is to match information in the IPv6 packet payload, it cannot match the packet with more than two extension headers or with the Encapsulating Security Payload Header.

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

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

If no optional keywords are provided in the **undo rule** command, you delete the entire rule. If optional keywords or arguments are provided, you delete the specified attributes.

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

Examples

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

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

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

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

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

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

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

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

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

```
<Sysname> system-view
[Sysname] acl ipv6 number 3004
[Sysname-acl6-adv-3004] rule permit ipv6 hop-by-hop type 5
```

```
[Sysname-acl6-adv-3004] rule deny ipv6 hop-by-hop
```

Related commands

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**

rule (IPv6 basic ACL view)

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

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

Syntax

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

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

Default

An IPv6 basic ACL does not contain any rule.

Views

IPv6 basic ACL view

Predefined user roles

network-admin

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Counts the number of times the IPv6 basic ACL rule has been matched. The **counting** keyword enables match counting specific to rules, and the **hardware-count** keyword in the **packet-filter ipv6** command enables match counting for all rules in an ACL. If the **counting** keyword is not specified, matches for the rule are not counted.

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

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

routing [**type** *routing-type*]: Applies the rule to the specified type of routing header or all types of routing header. The *routing-type* argument specifies the value of the routing header type, which is in the range

of 0 to 255. If you specify the **type** *routing-type* option, the rule applies to the specified type of routing header. Otherwise, the rule applies to any type of routing header.

source { *source-address source-prefix* | *source-address/source-prefix* | **any** }: Matches a source IP address. The *ipv6-address* and *prefix-length* arguments represent a source IPv6 address and address prefix length in the range of 1 to 128. The **any** keyword represents any IPv6 source address.

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

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

Usage guidelines

If an ACL is for QoS traffic classification or packet filtering:

- Do not specify the **vpn-instance** or **fragment** keyword.
- Do not specify the **routing** keyword if the ACL is for outbound QoS traffic classification or outbound packet filtering.

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

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

If no optional keywords are provided in the **undo rule** command, you delete the entire rule. If optional keywords or arguments are provided, you delete the specified attributes.

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

Examples

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

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

Related commands

- **acl**
- **acl logging interval**
- **display acl**
- **step**
- **time-range**

rule comment

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

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

Syntax

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

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

Default

An ACL has not rule comment.

Views

IPv4/IPv6 basic ACL view

IPv4/IPv6 advanced ACL view

Ethernet frame header ACL view

Predefined user roles

network-admin

Parameters

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

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

Examples

Create a rule for IPv4 basic ACL 2000, and add a comment about the rule.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used for telnet.
```

Related commands

display acl

step

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

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

Syntax

step *step-value*

undo step

Default

The rule numbering step is five.

Views

IPv4/IPv6 basic ACL view

IPv4/IPv6 advanced ACL view

Ethernet frame header ACL view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

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

Examples

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

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

Related commands

display acl

QoS policy commands

Traffic class commands

display traffic classifier

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Displays user-defined traffic classes.

classifier-name: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If no traffic class is specified, this command displays information about all traffic classes.

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument represents its IRF member ID. If no IRF member device is specified, this command displays the traffic classes on all member devices.

Examples

Display information about all user-defined traffic classes.

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

  User-defined classifier information:

   Classifier: 1 (ID 100)
     Operator: AND
     Rule(s) :
      If-match acl 2000

   Classifier: 2 (ID 101)
     Operator: AND
     Rule(s) :
      If-match protocol ipv6

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

Table 16 Command output

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

if-match

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

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

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

Default

No match criterion is configured.

Views

Traffic class view

Predefined user roles

network-admin

Parameters

match-criteria: Specifies a match criterion. Table 17 shows the available match criteria.

Table 17 Available match criteria

Option	Description
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	Matches an ACL. The *acl-number* argument is in the range of 2000 to 3999 for an IPv4 ACL, 2000 to 3999 for an IPv6 ACL, and 4000 to 4999 for an Ethernet frame header ACL. The *acl-name* argument is a case-insensitive string of 1 to 63 characters, which must start with an English letter, and to avoid confusion, it cannot be **all**.
any	Matches all packets.
control-plane protocol *protocol-name*&<1-8>	Matches the control plane protocols. The *protocol-name-list*&<1-8> argument is a list of system-defined control plane protocols. For available system-defined control plane protocols, see Table 18. &<1-8> indicates that you can enter up to eight system-defined control plane protocols.

Option	Description
control-plane protocol-group *protocol-group-name*	Matches the control plane protocol group. The *protocol-group-name* argument can be **critical**, **important**, **management**, **monitor**, **normal**, or **redirect**.
customer-dot1p *dot1p-value*&<1-8>	Matches the 802.1p priority of the customer network. The *dot1p-value*&<1-8> argument is a list of 802.1p priority values. An 802.1p priority ranges from 0 to 7. &<1-8> indicates that you can enter up to eight 802.1p priority values.
customer-vlan-id *vlan-id-list*	Matches the customer VLAN IDs (CVLANs). The *vlan-id-list* argument is in the format of *vlan-id-list* = { *vlan-id* | *vlan-id1* **to** *vlan-id2* }&<1-10>, where the *vlan-id, vlan-id1,* and *vlan-id2* arguments represent the VLAN IDs and each range from 1 to 4094, *vlan-id1* must be no greater than *vlan-id2*, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.
destination-mac *mac-address*	Matches a destination MAC address.
dscp *dscp-value*&<1-8>	Matches DSCP values. The *dscp-value*&<1-8> argument is a list of DSCP values. A DSCP value ranges from 0 to 63 or can be a keyword shown Table 20. &<1-8> indicates that you can enter up to eight DSCP values.
ip-precedence *ip-precedence-value*&<1-8>	Matches IP precedence. The *ip-precedence-value*&<1-8> argument is a list of IP precedence values. An IP precedence ranges from 0 to 7. &<1-8> indicates that you can enter up to eight IP precedence values.
protocol *protocol-name*	Matches a protocol. The *protocol-name* argument can be IP or IPv6.
qos-local-id *local-id-value*	Matches a local QoS ID, which ranges from 1 to 4095. The switch supports local QoS IDs in the range of 1 to 3999.
service-dot1p *dot1p-value*&<1-8>	Matches the 802.1p priority of the service provider network. The *dot1p-value*&<1-8> argument is a list of 802.1p priority values. An 802.1p priority ranges from 0 to 7. &<1-8> indicates that you can enter up to eight 802.1p priority values.
service-vlan-id *vlan-id-list*	Matches the service provider VLAN IDs (SVLANs). The *vlan-id-list* argument is in the format of *vlan-id-list* = { *vlan-id* | *vlan-id1* **to** *vlan-id2* }&<1-10>, where the *vlan-id, vlan-id1,* and *vlan-id2* arguments represent the VLAN IDs and each range from 1 to 4094, *vlan-id1* must be no greater than *vlan-id2*, and &<1-10> indicates that you can specify up to 10 VLAN IDs or VLAN ID ranges.
source-mac *mac-address*	Matches a source MAC address.

Table 18 Available system-defined control plane protocols

Protocol	Description
arp	ARP packets
arp-snooping	ARP snooping packets
bgp	BGP packets

Protocol	Description
bgp4+	IPv6 BGP packets
bpdu-tunnel	BPDU tunnel packets
dhcp	DHCP packets
dhcp-snooping	DHCP snooping packets
dhcpv6	IPv6 DHCP packets
dldp	DLDP packets
dot1x	802.1p packets
gvrp	GVRP packets
icmp	ICMP packets
icmpv6	ICMP snooping packets
igmp	IGMP packets
ip-option	IPv4 packets with the Options field
ipv6-option	IPv6 packets with the Options field
isis	IS-IS packets
lacp	LACP packets
lldp	LLDP packets
ospf-multicast	OSPF multicast packets
ospf-unicast	OSPF unicast packets
ospf3-multicast	OSPFv3 multicast packets
ospf3-unicast	OSPFv3 unicast packets
ssh	SSH packets
stp	STP packets
telnet	Telnet packets
vrrp	VRRP packets
vrrp6	IPv6 VRRP packets

Usage guidelines

When an ACL is referenced by a QoS policy for traffic classification, the action (permit or deny) in the ACL is ignored, and the actions in the associated traffic behavior are performed.

If a class that uses the AND operator has multiple **if-match acl**, **if-match acl ipv6**, **if-match customer-vlan-id** or **if-match service-vlan-id** clauses, a packet that matches any of the clauses matches the class.

To successfully execute the traffic behavior associated with a traffic class that uses the AND operator, define only one **if-match** clause for any of the following match criteria, and enter only one value for any of the following *list* arguments (for example, the *8021p-list* argument):

- **customer-dot1p** *8021p-list*
- **destination-mac** *mac-address*
- **dscp** *dscp-list*

- **ip-precedence** *ip-precedence-list*
- **service-dot1p** *8021p-list*
- **source-mac** *mac-address*
- **control-plane protocol** *protocol-name*

To create multiple **if-match** clauses for these match criteria or specify multiple values for the *list* arguments, specify the operator of the class as OR and use the **if-match** command multiple times.

If a match criterion includes the **if-match control-plane protocol** or **if-match control-plane protocol-group** clause, the QoS policy that references this match criterion can only be applied to the control plane.

Defining an ACL-based match criterion

- If the ACL referenced in the **if-match** command does not exist, the relevant QoS policy cannot be applied normally.
- You can configure multiple ACLs for a class.
- For a traffic class, you can reference an ACL twice by its name and number with the **if-match** command, respectively.

Defining a criterion to match a destination MAC address

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

Defining a criterion to match a source MAC address

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

Defining a criterion to match DSCP values

- You can configure multiple DSCP match criteria for a traffic class. All defined DSCP values are automatically sorted in ascending order.
- To delete a criterion that matches DSCP values, the specified DSCP values must be identical with those defined in the criterion (the sequence may be different).

Defining a criterion to match 802.1p priority in customer or service provider VLAN tags

- You can configure multiple 802.1p priority match criteria for a traffic class. All the defined 802.1p values are automatically arranged in ascending order.
- To delete a criterion that matches 802.1p priority values, the specified 802.1p priority values in the command must be identical with those defined in the criterion (the sequence may be different).

Defining a criterion to match IP precedence values

- You can configure multiple IP precedence match criteria for a traffic class. The defined IP precedence values are automatically arranged in ascending order.
- To delete a criterion that matches IP precedence values, the specified IP precedence values in the command must be identical with those defined in the criterion (the sequence may be different).

Defining a criterion to match CVLANs or SVLANs

- You can configure multiple VLAN ID match criteria for a traffic class. The defined VLAN IDs are automatically arranged in ascending order.
- You can configure multiple VLAN IDs in one command line. If the same VLAN ID is specified multiple times, the system considers the VLAN IDs as one. If a packet matches one of the defined VLAN IDs, it matches the **if-match** clause.

- To delete a criterion that matches VLAN IDs, the specified VLAN IDs in the command must be identical with those defined in the criterion (the sequence may be different).

Defining a criterion to match control plane protocols

- You can configure multiple control plane protocol match criteria for a traffic class.
- This criterion cannot coexist with other criteria in a traffic class. Otherwise, the relevant QoS policy cannot be applied normally.
- You can configure multiple control plane protocols in one command line. If the same control plane protocol is specified multiple times, the system considers them as one. If a packet matches one of the defined control plane protocols, it matches the **if-match** clause.
- To delete a criterion that matches control plane protocols, the specified control plane protocols in the command must be identical with those defined in the criterion (the sequence may be different).

Examples

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

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

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

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

Define a match criterion for traffic class **class1** to match the packets with their customer network 802.1p priority values being 3.

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

Define a match criterion for traffic class **class1** to match the packets with their service provider network 802.1p priority values being 5.

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

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

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

Define a match criterion for traffic class **class1** to match the ACL named **flow**.

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

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

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

Define a match criterion for traffic class **class1** to match the IPv6 ACL named **flow**.

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

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

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

Define a match criterion for traffic class **class1** to match the packets with their DSCP values being 1, 6, or 9.

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

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

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

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

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

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

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

Define a match criterion for traffic class **class1** to match the packets of service provider network VLAN 2, 7, or 10.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match service-vlan-id 2 7 10
```

Define a match criterion for traffic class **class1** to match the packets with a local QoS ID of 3.

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

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

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

Define a match criterion for traffic class **class1** to match packets of the protocols in protocol group **normal**.

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

traffic classifier

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

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

Syntax

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

undo traffic classifier *classifier-name*

Default

No traffic class exists.

Views

System view

Predefined user roles

network-admin

Parameters

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

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

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

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

Examples

Create a traffic class **class1**.

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

Related commands

display traffic classifier

Traffic behavior commands

accounting

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

Use **undo accounting** to delete the traffic accounting action from a traffic behavior.

Syntax

accounting [**byte** | **packet**] *

undo accounting

Default

No traffic accounting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

byte: Counts traffic in bytes.

packet: Counts traffic in packets.

Examples

Configure a traffic accounting action in traffic behavior **database** to count traffic in bytes.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting byte
```

car

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

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

Syntax

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

undo car

Default

No CAR action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cir *committed-information-rate*: Specifies the committed information rate (CIR) in kbps, which specifies an average traffic rate. The value range for the *committed-information-rate* argument is an integral multiple of 8 between 8 and 160000000.

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

ebs *excess-burst-size*: Specifies the excess burst size (EBS) in bytes. The value range for the *excess-burst-size* argument is an integral multiple of 512 between 0 and 256000000, and the default value is 512.

pir *peak-information-rate*: Specifies the peak information rate (PIR) in kbps. The value range for the *peak-information-rate* argument is an integral multiple of 8 between 8 and 160000000.

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

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

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

action: Sets the action to take on the packet:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument ranges from 0 to 7.
- **remark-dscp-pass** *new-dscp*: Sets the DSCP value of the packet to *new-dscp* and permits the packet to pass through. The *new-dscp* argument ranges from 0 to 63.
- **remark-lp-pass** *new-local-precedence*: Sets the local precedence value of the packet to *new-local-precedence* and permits the packet to pass through. The *new-local-precedence* argument ranges from 0 to 7.

Usage guidelines

A QoS policy that references the traffic behavior can be applied in either the inbound direction or outbound direction of an interface.

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

Examples

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

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

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

display traffic behavior

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Displays user-defined traffic behaviors.

behavior-name: Behavior name, a case-sensitive string of 1 to 31 characters. If no traffic behavior is specified, this command displays information about all traffic behaviors.

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument represents its IRF member ID. If no IRF member device is specified, this command displays the traffic behaviors on all member devices.

Examples

Display information about user-defined traffic behaviors.

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

  User-defined behavior information:

    Behavior: 1 (ID 100)
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 128 (kbps), CBS 8192 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard

    Behavior: 2 (ID 101)
      Accounting enable: Packet
      Filter enable: Permit
      Marking:
        Remark dot1p 4
      Redirecting:
        Redirect to the CPU

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

Table 19 Command output

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

Field	Description
None	No other traffic behavior is configured.

filter

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

Use **undo filter** to delete a traffic filtering action from a traffic behavior.

Syntax

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

undo filter

Default

No traffic filtering action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

deny: Drops packets.

permit: Transmits the packets.

Examples

Configure a traffic filtering action as **deny** in traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

nest top-most

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

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

Syntax

nest top-most vlan *vlan-id*

undo nest top-most

Default

No VLAN tag adding action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id *vlan-id*: Specifies the ID of the VLAN tag to be added. The *vlan-id* argument ranges from 1 to 4094.

Usage guidelines

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

If the traffic behavior already contains a VLAN tag adding action, the new one overwrites the old one.

Examples

Configure traffic behavior **b1** to add VLAN tag 123.

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] nest top-most vlan 123
```

redirect

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

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

Syntax

redirect { **cpu** | **interface** *interface-type interface-number* }

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

Default

No traffic redirecting action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

cpu: Redirects traffic to the CPU.

interface: Redirects traffic to an interface.

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

Usage guidelines

Redirecting traffic to CPU and redirecting traffic to an interface are mutually exclusive with each other in the same traffic behavior. The last redirecting action configured takes effect.

Examples

Configure redirecting traffic to Ten-GigabitEthernet 1/1/5 in traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface Ten-GigabitEthernet 1/1/5
```

Related commands

- **classifier behavior**

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

remark customer-vlan-id

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

Use **undo remark customer-vlan-id** to remove the action from the traffic behavior.

Syntax

remark customer-vlan-id *vlan-id*

undo remark customer-vlan-id

Default

No CVLAN marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies a CVLAN ID, ranging from 1 to 4094.

Examples

Configure traffic behavior **b1** to mark matching packets with CVLAN 111.

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark customer-vlan-id 111
```

remark dot1p

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

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

Syntax

remark [**green** | **red** | **yellow**] **dot1p** *dot1p-value*

undo remark [**green** | **red** | **yellow**] **dot1p**

remark dot1p customer-dot1p-trust

undo remark dot1p

Default

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

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dot1p-value: Specifies the 802.1p priority to be marked for packets, which ranges from 0 to 7.

customer-dot1p-trust: Copies the 802.1p priority value in the inner VLAN tag to the outer VLAN tag after the QoS policy is applied to an interface.

Usage guidelines

Using both the **remark dot1p** *dot1p-value* command and the **remark dot1p customer-dot1p-trust** command will cause them to override each other. The most recent configuration of them takes effect.

The **remark dot1p customer-dot1p-trust** command does not take effect on single-tagged packets.

Examples

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

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

Configure an inner-to-outer tag priority copying action in traffic behavior **database**.

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

remark drop-precedence

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

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

Syntax

remark drop-precedence *drop-precedence-value*

undo remark drop-precedence

Default

No drop priority marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

drop-precedence-value: Specifies the drop priority to be marked for packets. This argument ranges from 0 to 2.

Usage guidelines

The command applies to only incoming traffic.

Examples

Configure traffic behavior **database** to mark matching traffic with drop priority 2.

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

remark dscp

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

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

Syntax

remark [**green** | **red** | **yellow**] **dscp** *dscp-value*

undo [**green** | **red** | **yellow**] **remark dscp**

Default

No DSCP marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dscp-value: DSCP value, which can be a number from 0 to 63 or a keyword in Table 20.

Table 20 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30

Keyword	DSCP value (binary)	DSCP value (decimal)
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

Examples

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

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

remark ip-precedence

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

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

Syntax

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

Default

No IP precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

ip-precedence-value: Specifies the IP precedence value to be marked for packets, which ranges from 0 to 7.

Examples

Set the IP precedence to 6 for packets.

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

```
[Sysname-behavior-database] remark ip-precedence 6
```

remark local-precedence

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

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

Syntax

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

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

Default

No local precedence marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

local-precedence-value: Sets the local precedence to be marked for packets, which ranges from 0 to 7.

Examples

Configure traffic behavior **database** to mark matching traffic with local precedence 2.

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

remark qos-local-id

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

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

Syntax

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

undo remark qos-local-id

Default

No local QoS ID marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

local-id-value: Specifies the local QoS ID to be marked for packets. The value range for this argument is 1 to 4095. The switch supports local QoS IDs in the range of 1 to 3999.

Usage guidelines

Remarking local QoS IDs combines different traffic classes into one new class, which is indicated by a local QoS ID. You can configure a traffic behavior for this new class to implement two levels of actions on a traffic class.

Remarking local QoS IDs applies to only the incoming traffic.

Examples

Configure the action of marking packet with local QoS ID 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark qos-local-id 2
```

remark service-vlan-id

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

Use **undo remark service-vlan-id** to remove the action from the traffic behavior.

Syntax

remark service-vlan-id *vlan-id*

undo remark service-vlan-id

Default

No SVLAN marking action is configured.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

vlan-id: Specifies an SVLAN ID, ranging from 1 to 4094.

Examples

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

```
<Sysname> system-view
[Sysname] traffic behavior b1
[Sysname-behavior-b1] remark service-vlan-id 222
```

traffic behavior

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

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

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

Default

No traffic behavior exists.

Views

System view

Predefined user roles

network-admin

Parameters

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

Examples

Create a traffic behavior named **behavior1**.

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

Related commands

display traffic behavior

QoS policy commands

classifier behavior

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

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

Syntax

classifier *classifier-name* **behavior** *behavior-name* [**mode dcbx**]

undo classifier *classifier-name*

Default

No traffic behavior is associated with a traffic class.

Views

QoS policy view

Predefined user roles

network-admin

Parameters

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

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

mode dcbx: Specifies that the class-behavior association applies only to the Data Center Bridging Exchange Protocol (DCBX). For more information about DCBX, see *Layer 2—LAN Switching Configuration Guide*.

Usage guidelines

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

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

Examples

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

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

Related commands

qos policy

control-plane

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

Syntax

control-plane slot *slot-number*

Views

System view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument is the member device ID in the IRF fabric.

Examples

Enter the control plane view of IRF member device 1.

```
<Sysname> system-view
[Sysname] control-plane slot 1
[Sysname-cp-slot1]
```

display qos policy

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

user-defined: Displays user-defined QoS policies.

policy-name: Specifies a QoS policy by its name, a case-sensitive string of 1 to 31 characters. If no QoS policy name is specified, this command displays configuration information of all the user-defined QoS policies.

classifier *classifier-name*: Specifies a traffic class by its name, a case-sensitive string of 1 to 31 characters. If no traffic class is specified, this command displays information about all traffic classes.

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument represents its IRF member ID. If no IRF member device is specified, this command displays the QoS policies on all member devices.

Examples

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

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

  User-defined QoS policy information:

  Policy: 1 (ID 100)
   Classifier: 1 (ID 100)
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 128 (kbps), CBS 8192 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
   Classifier: 2 (ID 101)
     Behavior: 2
      Accounting enable: Packet
      Filter enable: Permit
      Marking:
        Remark dot1p 4
   Classifier: 3 (ID 102)
     Behavior: 3
      -none-
```

display qos policy control-plane

Use **display qos policy control-plane** to display information about the QoS policies applied to the specified control plane.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument is the member device ID in the IRF fabric.

Examples

Display information about the QoS policy applied to the control plane.

```
<Sysname> display qos policy control-plane slot 1

Control plane

  Direction: Inbound

  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 128 (kbps), CBS 8192 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets) 0 (Bytes)
        Red packets   : 0 (Packets) 0 (Bytes)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
```

Table 21 Command output

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

For the output description, see Table 16 and Table 19.

display qos policy control-plane pre-defined

Use **display qos policy control-plane pre-defined** to display information about the pre-defined QoS policy applied to the control plane.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument is the member device ID in the IRF fabric.

Usage guidelines

If no slot number is specified, this command displays information about the pre-defined QoS policy applied to the control plane of each IRF member device.

Examples

Display information about the pre-defined QoS policy applied to the control plane of member device 1.

```
<Sysname> display qos policy control-plane pre-defined slot 1
Pre-defined policy information slot 1
  Protocol          Priority   Bandwidth (kbps)   Group
  IS-IS             37         512                critical
  VRRP              40         768                important
  OSPF Multicast    35         256                critical
  OSPF Unicast      35         256                critical
  IGMP              19         256                important
  OSPFv3 Unicast    34         256                critical
  OSPFv3 Multicast  34         256                critical
  VRRPv6            40         768                important
  ARP               8          256                normal
  DHCP Snooping     17         256                redirect
  DHCP              15         256                normal
  802.1x            9          128                important
  STP               43         256                critical
  LACP              38         64                 critical
  GVRP              11         256                critical
  BGP               27         256                critical
  ICMP              9          640                monitor
  IPOPTION          20         64                 normal
```

```
BGPv6              26          256               critical
IPOPTIONv6         13          64                normal
LLDP               25          128               important
DLDP               24          64                critical
TELNET             10          512               management
SSH                10          512               management
HTTP               10          64                management
HTTPS              10          64                management
ARP Snooping       10          256               redirect
ICMPv6             1           512               monitor
DHCPv6             12          256               normal
```

Table 22 Command output

Field	Description
Pre-defined policy information	Contents of the pre-defined control plane QoS policy.
Protocol	System-defined control plane protocol.
Group	Control plane protocol group.

display qos policy global

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

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

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument is the member device ID in the IRF fabric.

Usage guidelines

If no direction is specified, this command displays information about both inbound and outbound global QoS policies.

If no IRF member device is specified, this command displays the global QoS policies on the IRF fabric.

Examples

Display information about the inbound global QoS policy.

```
<Sysname> display qos policy global inbound

  Direction: Inbound

  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) :
      If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 128 (kbps), CBS 8192 (Bytes), EBS 512 (Bytes)
        Green action  : pass
        Yellow action : pass
        Red action    : discard
        Green packets : 0 (Packets)
        Red packets   : 0 (Packets)
   Classifier: 2
     Operator: AND
     Rule(s) :
      If-match protocol ipv6
     Behavior: 2
      Accounting enable:
        0 (Packets)
      Filter enable: Permit
      Marking:
        Remark dot1p 4
```

Table 23 Command output

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

For the output description, see Table 16 and Table 19.

display qos policy interface

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

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

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

Usage guidelines

If no direction is specified, the command displays information about the QoS policy applied to the incoming traffic and the QoS policy applied to the outgoing traffic.

Examples

Display information about the QoS policy applied to the incoming traffic of Ten-GigabitEthernet 1/1/5.

```
<Sysname> display qos policy interface Ten-GigabitEthernet1/1/5 inbound

Interface: Ten-GigabitEthernet1/1/5

  Direction: Inbound

  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 1
      Marking:
        Remark dscp 3
      Committed Access Rate:
        CIR 128 (kbps), CBS 8192 (Bytes), EBS 512 (Bytes)
        Green action: pass
        Yellow action: pass
        Red action: discard
        Green packets: 0 (Packets)
        Red packets: 0 (Packets)
   Classifier: 2
     Operator: AND
     Rule(s) : If-match protocol ipv6
     Behavior: 2
      Accounting Enable:
        0 (Packets)
      Filter Enable: Permit
      Marking:
        Remark dot1p 1
```

Table 24 Command output

Field	Description
Direction	Direction in which the QoS policy is applied to the interface.
Green packets	Traffic statistics for green packets.
Red packets	Traffic statistics for red packets.

For the output description, see Table 16 and Table 19.

display qos vlan-policy

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *policy-name*: Displays information about a QoS policy applied to VLANs. The *policy-name* argument is a case-sensitive string of 1 to 31 characters.

vlan *vlan-id*: Displays information about the QoS policies applied to the VLAN specified by its ID.

inbound: Displays information about the QoS policy applied to the incoming traffic of the specified VLAN.

outbound: Displays information about the QoS policy applied to the outgoing traffic of the specified VLAN.

slot *slot-number*: Displays information about QoS policies applied to VLANs of the IRF member device specified by the slot number.

Usage guidelines

If no direction is specified, this command displays information about QoS policies applied to VLANs in both the inbound and outbound directions.

If no IRF member device is specified, this command displays information about all QoS policies applied to VLANs on the device.

Examples

Display information about QoS policies applied to VLAN 2.

```
<Sysname> display qos vlan-policy vlan 2
Vlan 2

  Direction: Outbound

  Policy: 1
```

```
Classifier: 1
  Operator: AND
  Rule(s) : If-match acl 2000
  Behavior: 1
   Marking:
     Remark dscp 3
   Committed Access Rate:
     CIR 128 (kbps), CBS 8192 (Bytes), EBS 512 (Bytes)
     Green action: pass
     Yellow action: pass
     Red action: discard
     Green packets: 0(Packets)
     Red packets: 0(Packets)
Classifier: 2
  Operator: AND
  Rule(s) : If-match protocol ipv6
  Behavior: 2
   Accounting enable:
     0 (Packets)
   Filter enable: Permit
   Marking:
     Remark dot1p 1
Classifier: 3
  Operator: AND
  Rule(s) : -none-
  Behavior: 3
   -none-
```

Table 25 Command output

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

For the output description, see Table 16 and Table 19.

qos apply policy (interface view, control plane view)

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

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

Syntax

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

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

Default

No QoS policy is applied to an interface or control plane.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view, control plane view

Predefined user roles

network-admin

Parameters

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

inbound: Applies the QoS policy to the incoming traffic of an interface or control plane.

outbound: Applies the QoS policy to the outgoing traffic of an interface.

Examples

Apply QoS policy **USER1** to the outgoing traffic of Ten-GigabitEthernet 1/1/5.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos apply policy USER1 outbound
```

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

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

qos apply policy global

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

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

Syntax

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

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

Default

No QoS policy is applied globally.

Views

System view

Predefined user roles

network-admin

Parameters

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

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

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

Usage guidelines

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

Examples

Apply the QoS policy **user1** to the incoming traffic globally.

```
<Sysname> system-view
[Sysname] qos apply policy user1 global inbound
```

qos policy

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

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

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

Default

No QoS policy is configured.

Views

System view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

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

Examples

Define QoS policy **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

Related commands

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

qos vlan-policy

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

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

Syntax

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

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

Default

No QoS policy is applied to a VLAN.

Views

System view

Predefined user roles

network-admin

Parameters

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

vlan-id-list: Specifies a list of up to eight VLAN IDs. A VLAN ID ranges from 1 to 4094. You can enter individual discontinuous VLAN IDs and VLAN ID ranges in the form of *start-vlan-id* **to** *end-vlan-id* where the start VLAN ID must be smaller than the end VLAN ID. Each item in the VLAN list is separated by a space. You can specify up to eight VLAN IDs.

inbound: Applies the QoS policy to the incoming packets in the specified VLANs.

outbound: Applies the QoS policy to the outgoing packets in the specified VLANs.

Examples

Apply the QoS policy **test** to the incoming traffic of VLAN 200, VLAN 300, VLAN 400, and VLAN 500.

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 inbound
```

reset qos policy control-plane

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

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Clears the statistics of the QoS policies applied to the control plane of the IRF member device specified by the slot number.

Examples

Clear the statistics of the QoS policy applied to the control plane of member device 3.

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

reset qos policy global

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

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

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

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

Usage guidelines

If no direction is specified, this command clears the statistics of the global QoS policies in both directions.

Examples

Clear the statistics of the global QoS policy applied to the incoming traffic globally.

```
<Sysname> reset qos policy global inbound
```

reset qos vlan-policy

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

Syntax

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

Views

User view

Predefined user roles

network-admin

Parameters

vlan *vlan-id*: Specifies a VLAN ID, which ranges from 1 to 4094.

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

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

Usage guidelines

If no direction is specified, this command clears the statistics of the QoS policies in both directions of the VLAN.

Examples

Clear the statistics of QoS policies applied to VLAN 2.

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

Priority mapping commands

Priority map commands

display qos map-table

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

The device provides the following types of priority map.

Table 26 Priority maps

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

Usage guidelines

If no priority map is specified, this command displays the configuration information of all priority maps.

Examples

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

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

```
3     :     3
4     :     4
5     :     5
6     :     6
7     :     7
```

Table 27 Command output

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

import

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

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

Syntax

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

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

Default

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

Views

Priority map view

Predefined user roles

network-admin

Parameters

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

export-value: Specifies the output value.

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

Examples

Configure the 802.1p-drop priority map to map 802.1p priority values 4 and 5 to drop priority 1.

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

Related commands

display qos map-table

qos map-table

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

Syntax

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

Views

System view

Predefined user roles

network-admin

Parameters

For the description of the keywords, see Table 26.

Examples

Enter the 802.1p-drop priority map view.

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

Related commands

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

Port priority commands

qos priority

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

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

Syntax

qos priority *priority-value*

undo qos priority

Default

The port priority is 0.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

priority-value: Specifies the port priority value. The port priority ranges from 0 to 7.

Examples

Set the port priority of Ten-GigabitEthernet 1/1/5 to 2.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/1/5
[Sysname-Ten-GigabitEthernet 1/1/5] qos priority 2
```

Related commands

display qos trust interface

Priority trust mode commands

display qos trust interface

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, this command displays priority trust mode and port priority information of all interfaces.

Examples

Display the priority trust mode and port priority information of Ten-GigabitEthernet 1/1/5.

```
<Sysname> display qos trust interface Ten-GigabitEthernet 1/1/5
Interface: Ten-GigabitEthernet1/1/5
 Port priority information
  Port priority: 0
  Port priority trust type: none
```

Table 28 Command output

Field	Description
Interface	Interface type and interface number.
Port priority	Port priority set for the interface.
Port priority trust type	Priority trust mode on the interface: **dot1p**, **dscp**, or **none**. If the trust mode is **none**, the port priority is used for priority mapping.

qos trust

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

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

Syntax

qos trust { **dot1p** | **dscp** }

undo qos trust

Default

A Layer 2 Ethernet interface does not trust any packet priority. A Layer 3 Ethernet interface trusts the 802.1p priority of received packets.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

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

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

Usage guidelines

The **undo qos trust** command does not take effect on Layer 3 Ethernet interfaces.

Examples

Set the trusted packet priority type to 802.1p priority on Ten-GigabitEthernet 1/1/5.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos trust dot1p
```

Related commands

display qos trust interface

GTS and rate limit commands

GTS commands

display qos gts interface

Use **display qos gts interface** to view generic traffic shaping (GTS) configuration and statistics on a specified interface or all the interfaces.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, this command displays the GTS configuration and statistics on all the interfaces.

Examples

Display the GTS configuration and statistics on all the interfaces.

```
<Sysname> display qos gts interface
Interface: Ten-GigabitEthernet1/1/5
 Rule: If-match queue 1
  CIR 128 (kbps), CBS 8192 (Bytes)
 Rule: If-match queue 2
  CIR 256 (kbps), CBS 16384 (Bytes)
```

Table 29 Command output

Field	Description
Interface	Interface type and interface number.
Rule	Match criteria.
CIR	CIR in kbps.
CBS	CBS in bytes, which specifies the depth of the token bucket for holding bursty traffic.

qos gts

Use **qos gts** to set GTS parameters for traffic of a specific traffic class or all the traffic on the interface.

Use **qos gts** to set GTS parameters for the packets in a specific queue.

Use **undo qos gts** to remove GTS parameters for traffic of a specific queue on the interface.

Syntax

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

undo qos gts queue *queue-id*

Default

No GTS parameters are configured on an interface.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue *queue-id*: Shapes the packets in the specified queue. The value range for the *queue-id* argument is 0 to 7.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for the *committed-information-rate* argument is 8 to 10485760 for 10-GE interfaces and 8 to 41943040 for 40-GE interfaces. The values must be integral multiples of 8.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for the *committed-burst-size* argument is an integral multiple of 512 between 512 and 16777216. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. If the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product.

Examples

Shape the packets in queue 1 on Ten-GigabitEthernet 1/1/5. The GTS parameters are as follows: CIR is 6400 kbps and CBS is 51200 bytes.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos gts queue 1 cir 6400 cbs 51200
```

Rate limit commands

display qos lr interface

Use **display qos lr interface** to view the rate limit configuration and statistics on a specified interface or all the interfaces.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, this command displays the rate limit configuration and statistics on all the interfaces.

Examples

Display the rate limit configuration and statistics on all the interfaces.

```
<Sysname> display qos lr interface
Interface: Ten-GigabitEthernet1/1/5
 Direction: Outbound
  CIR 12800 (kbps), CBS 800256 (Bytes)

Interface: Ten-GigabitEthernet1/1/6
 Direction: Outbound
  CIR 25600 (kbps), CBS 1600000 (Bytes)
```

Table 30 Command output

Field	Description
Interface	Interface type and interface number.
Direction	Direction to which the rate limit configuration is applied: inbound or outbound.
CIR	CIR in kbps.
CBS	CBS in bytes, which specifies the depth of the token bucket for holding bursty traffic.

qos lr

Use **qos lr** to limit the rate of packets on the interface.

Use **undo qos lr** to remove the rate limit.

Syntax

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

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

Default

Rate limit is not configured on an interface.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

inbound: Limits the rate of incoming packets on the interface.

outbound: Limits the rate of outgoing packets on the interface.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for the *committed-information-rate* argument is 8 to 10485760 for 10-GE interfaces and 8 to 41943040 for 40-GE interfaces. The values must be integral multiples of 8.

cbs *committed-burst-size*: Specifies the CBS in bytes. The value range for the *committed-burst-size* argument is an integral multiple of 512 between 512 and 134217728. The default value for this argument is the product of 62.5 and the CIR and must be an integral multiple of 512. If the product is not an integral multiple of 512, it is rounded up to the nearest integral multiple of 512 that is greater than the product.

Examples

Limit the rate of outgoing packets on Ten-GigabitEthernet 1/1/5, with CIR 25600 kbps and CBS 512000 bytes.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos lr outbound cir 25600 cbs 512000
```

Queue-based accounting commands

display qos queue-statistics interface outbound

Use **display qos queue-statistics interface outbound** to display outbound traffic statistics collected for an interface on a per-queue basis.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, the command displays the outbound traffic statistics for all interfaces.

Examples

Display queue-based outbound traffic statistics for Ten-GigabitEthernet 1/1/5.

```
<Sysname> display qos queue-statistics interface ten-gigabitethernet 1/1/5 outbound
Interface: Ten-GigabitEthernet1/1/5
 Direction: outbound
 Forwarded: 2334 packets, 321598 bytes
 Dropped: 0 packets, 0 bytes
 Queue 0
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 1
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 2
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 3
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 4
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
```

```
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
Queue 5
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
Queue 6
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
Queue 7
  Forwarded: 2334 packets, 321598 bytes, 2 pps, 1464 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
```

Table 31 Command output

Field	Description
Interface	Interface for which queue-based traffic statistics are displayed.
Direction	Direction of traffic for which statistics are collected.
Forwarded	Counts forwarded traffic on the interface both in packets and in bytes.
Dropped	Counts dropped traffic on the interface both in packets and in bytes.

Related commands

reset qos queue-statistics interface outbound

reset qos queue-statistics interface outbound

Use **reset qos queue-statistics interface outbound** to clear queue-based outbound traffic statistics for an interface.

Syntax

reset qos queue-statistics interface [*interface-type interface-number*] **outbound**

Views

User view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, the command clears the outbound traffic statistics for all interfaces.

Examples

Clear queue-based outbound traffic statistics for Ten-GigabitEthernet 1/1/5.

```
<Sysname> reset qos queue-statistics interface ten-gigabitEthernet 1/1/5 outbound
```

Related commands

display qos queue-statistics interface outbound

Congestion management commands

SP commands

display qos queue sp interface

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, this command displays the SP queuing configuration of all the interfaces.

Examples

Display the SP queuing configuration of Ten-GigabitEthernet 1/1/5.

```
<Sysname> display qos queue sp interface Ten-GigabitEthernet 1/1/5
Interface: Ten-GigabitEthernet1/1/5
 Output queue: Strict Priority queuing
```

Table 32 Command output

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

qos sp

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

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

Syntax

qos sp

undo qos sp

Default

An interface uses the WRR queuing algorithm.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Examples

Enable SP queuing on Ten-GigabitEthernet 1/1/5.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos sp
```

Related commands

display qos queue sp interface

WRR commands

display qos queue wrr interface

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, this command displays the WRR queuing configuration of all the interfaces.

Examples

Display the WRR queuing configuration of Ten-GigabitEthernet 1/1/5.

```
<Sysname> display qos queue wrr interface Ten-GigabitEthernet 1/1/5
Interface: Ten-GigabitEthernet1/1/5
 Output queue: Weighted Round Robin queuing
 Queue ID        Group           Byte-count
 ----------------------------------------
 be              1               1
 af1             1               2
 af2             1               3
 af3             1               4
 af4             1               5
```

```
ef              1               9
cs6             1               13
cs7             1               15
```

Table 33 Command output

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

qos wrr

Use **qos wrr** to enable WRR queuing and specify the weight type for an interface.

Use **undo qos wrr** to disable WRR queuing and restore the default queue scheduling algorithm for an interface.

Syntax

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

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

Default

An interface uses the byte-count WRR queuing algorithm, and queues 0 through 7 have weights of 1, 2, 3, 4, 5, 9, 13, and 15, respectively.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

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

weight: Allocates bandwidth to queues in terms of packets.

Usage guidelines

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

Examples

Enable weight-based WRR queuing on Ten-GigabitEthernet 1/1/5.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos wrr weight
```

Enable byte-count WRR queuing on Ten-GigabitEthernet 1/1/5.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos wrr byte-count
```

Related commands

display qos queue wrr interface

qos wrr { byte-count | weight }

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

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

Syntax

qos wrr *queue-id* **group** { **1** | **2** } { **byte-count** | **weight** } *schedule-value*

undo qos wrr *queue-id*

Default

An interface uses the byte-count WRR queuing algorithm, and queues 0 through 7 are in WRR group 1, with their weights of 1, 2, 3, 4, 5, 9, 13, and 15, respectively.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value is an integer in the range of 0 to 7 or a keyword listed in Table 34.

group { **1** | **2** }: Specifies WRR group 1 or 2. If no group is specified, group 1 applies.

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

weight: Allocates bandwidth to queues in terms of packets.

schedule-value: Specifies a scheduling weight for the specified queue in WRR queuing, in the range of 1 to 15.

Usage guidelines

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

The *queue-id* argument can be either a number or a keyword. Table 34 shows the number-keyword map.

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

Number	Keyword
0	be
1	af1
2	af2

Number	Keyword
3	af3
4	af4
5	ef
6	cs6
7	cs7

Examples

Enable byte-count WRR queuing on Ten-GigabitEthernet 1/1/5, assign queue 0, with the scheduling weight 10, to WRR group 1, and assign queue 1, with the scheduling weight 5, to WRR group 2.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos wrr byte-count
[Sysname-Ten-GigabitEthernet1/1/5] qos wrr 0 group 1 byte-count 10
[Sysname-Ten-GigabitEthernet1/1/5] qos wrr 1 group 2 byte-count 5
```

Related commands

- **display qos queue wrr interface**
- **qos wrr**

qos wrr group sp

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

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

Syntax

qos wrr *queue-id* **group sp**

undo qos wrr *queue-id*

Default

An interface uses the byte-count WRR queuing algorithm, and all the queues are in WRR group 1.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value is an integer in the range of 0 to 7 or a keyword listed in Table 34.

sp: Assigns a queue to the SP group, which uses the SP queue scheduling algorithm.

Usage guidelines

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

This command is available only on a WRR-enabled interface. Queues in the SP group are scheduled with SP. The SP group has higher scheduling priority than the WRR group. Queues in a WRR group are scheduled according to user-configured weights, and WRR groups are scheduled at a 1:1 ratio.

Examples

Enable packet-based WRR queuing on Ten-GigabitEthernet 1/1/5, and assign queue 0 to the SP group.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos wrr weight
[Sysname-Ten-GigabitEthernet1/1/5] qos wrr 0 group sp
```

Related commands

- **display qos queue wrr interface**
- **qos wrr**

WFQ commands

display qos queue wfq interface

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

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, this command displays the WFQ configuration of all the interfaces.

Examples

Display the WFQ configuration of Ten-GigabitEthernet 1/1/5.

```
<Sysname> display qos queue wfq interface Ten-GigabitEthernet 1/1/5
Interface: Ten-GigabitEthernet1/1/5
 Output queue: Hardware Weighted Fair Queuing
 Queue ID        Group           Byte-count      Min-Bandwidth
 ------------------------------------------------------------------
 be              1               1               64
 af1             1               1               64
 af2             1               1               64
 af3             1               1               64
 af4             1               1               64
 ef              1               1               64
```

```
cs6             1               1               64
cs7             1               1               64
```

Table 35 Command output

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

qos bandwidth queue

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

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

Syntax

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

undo qos bandwidth queue *queue-id*

Default

The minimum guaranteed bandwidth is 64 kbps.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Queue ID. The value is an integer in the range of 0 to 7 or a keyword listed in Table 34.

min *bandwidth-value*: Sets the minimum guaranteed bandwidth in kbps for a queue when the interface is congested. The value range for the *bandwidth-value* argument is 8 to 10000000 for 10-GE interfaces and 8 to 40000000 for 40-GE interfaces.

Usage guidelines

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

Examples

Set the minimum guaranteed bandwidth to 100 kbps for queue 0 on Ten-GigabitEthernet 1/1/5.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos wfq weight
```

```
[Sysname-Ten-GigabitEthernet1/1/5] qos bandwidth queue 0 min 100
```

Related commands

qos wfq

qos wfq

Use **qos wfq** to enable WFQ and specify the WFQ weight type on an interface.

Use **undo qos wfq** to disable WFQ and restore the default queuing algorithm on an interface.

Syntax

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

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

Default

An interface uses the byte-count WRR queuing algorithm, and all the queues are in the WRR group.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

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

weight: Allocates bandwidth to queues in terms of packets.

Usage guidelines

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

Examples

Enable weight-based WFQ on Ten-GigabitEthernet 1/1/5.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos wfq weight
```

Enable byte-count WFQ on Ten-GigabitEthernet 1/1/5.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos wfq byte-count
```

Related commands

display qos queue wfq interface

qos wfq { byte-count | weight }

Use **qos wfq** { **byte-count** | **weight** } to assign a queue to a WFQ group with a certain scheduling weight.

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

Syntax

qos wfq *queue-id* **group** { **1** | **2** } { **byte-count** | **weight** } *schedule-value*

undo qos wfq *queue-id*

Default

When WFQ queuing is used on an interface, all the queues are in WFQ group 1 and have a weight of 1.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value is an integer in the range of 0 to 7 or a keyword listed in Table 34.

group { **1** | **2** }: Specifies WFQ group 1 or 2. If no group is specified, group 1 applies.

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

weight: Allocates bandwidth to queues in terms of packets.

schedule-value: Specifies a scheduling weight for the specified queue in WFQ queuing, in the range of 1 to 15.

Usage guidelines

You must use the **qos wfq** command to enable WFQ first before you configure this command.

Examples

Enable byte-count WFQ on interface Ten-GigabitEthernet 1/1/5, assign queue 0, with the scheduling weight 10, to WFQ group 1, and assign queue 1, with the scheduling weight 5, to WFQ group 2.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos wfq byte-count
[Sysname-Ten-GigabitEthernet1/1/5] qos wfq 0 group 1 byte-count 10
[Sysname-Ten-GigabitEthernet1/1/5] qos wfq 1 group 2 byte-count 5
```

Related commands

- **display qos queue wfq interface**
- **qos bandwidth queue**
- **qos wfq**

qos wfq group sp

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

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

Syntax

qos wfq *queue-id* **group sp**

undo qos wfq *queue-id*

Default

When WFQ queuing is used on an interface, all the queues are in the WFQ group.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue by its ID. The value is an integer in the range of 0 to 7 or a keyword listed in Table 34.

sp: Assigns a queue to the SP group, which uses the SP queue scheduling algorithm.

Usage guidelines

You must use the **qos wfq** command to enable WFQ first before you configure this command.

With this SP+WFQ queuing method, the system schedules traffic as follows:

1. The system schedules the traffic conforming to the minimum guaranteed bandwidth in each WFQ group and schedules the traffic of the two WFQ groups in the ratio of 1:1 in a round robin manner.
2. The system uses SP to schedule queues in the SP group.
3. If there is remaining bandwidth, the system schedules the traffic of queues in each WFQ group based on their weights and schedules the traffic of the two WFQ groups in the ratio of 1:1 ratio in a round robin manner.

Examples

Enable weight-based WFQ on Ten-GigabitEthernet 1/1/5, and assign queue 0 to the SP group.

```
<Sysname> system-view
[Sysname] interface ten-gigabitethernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos wfq weight
[Sysname-Ten-GigabitEthernet1/1/5] qos wfq 0 group sp
```

Related commands

- **display qos queue wfq interface**
- **qos bandwidth queue**
- **qos wfq**

Per-port queue-based accounting commands

display qos queue-statistics interface outbound

Use **display qos queue-statistics interface outbound** to display outgoing traffic statistics collected for an interface on a per-queue basis.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, the command displays the outgoing traffic statistics for all interfaces.

Examples

Display queue-based outgoing traffic statistics of Ten-GigabitEthernet 1/1/5.

```
<Sysname> display qos queue-statistics interface ten-gigabitethernet 1/1/5 outbound
Interface: Ten-GigabitEthernet1/1/5
 Direction: outbound
 Forwarded: 2334 packets, 321598 bytes
 Dropped: 0 packets, 0 bytes
 Queue 0
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 1
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 2
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 3
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
 Queue 4
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
```

```
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
Queue 5
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
Queue 6
  Forwarded: 0 packets, 0 bytes, 0 pps, 0 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
Queue 7
  Forwarded: 2334 packets, 321598 bytes, 2 pps, 1464 bps
  Dropped: 0 packets, 0 bytes
  Current queue length: 0 packets
```

Table 36 Command output

Field	Description
Interface	Interface for which queue-based traffic statistics are displayed.
Direction	Direction of traffic for which statistics are collected.
Forwarded	Counts forwarded traffic both in packets and in bytes.
Dropped	Counts dropped traffic both in packets and in bytes.

Related commands

reset qos queue-statistics interface outbound

reset qos queue-statistics interface outbound

Use **reset qos queue-statistics interface outbound** to clear per-queue outgoing traffic statistics for an interface.

Syntax

reset qos queue-statistics interface [*interface-type interface-number*] **outbound**

Views

User view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, the command clears the outgoing traffic statistics for all interfaces.

Usage guidelines

This command is available in Release 2403 and earlier versions.

Examples

Clear queue-based outgoing traffic statistics of Ten-GigabitEthernet 1/1/5.

```
<Sysname> reset qos queue-statistics interface ten-gigabitEthernet 1/1/5 outbound
```

Related commands

display qos queue-statistics interface outbound

Congestion avoidance commands

WRED commands

display qos wred interface

Use **display qos wred interface** to display the WRED configuration for an interface.

Syntax

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

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, this command displays the WRED configuration and statistics for all the interfaces.

Examples

Display the WRED configuration for all interfaces.

```
<Sysname> display qos wred interface
Interface: Ten-GigabitEthernet1/1/5
 Current WRED configuration:
  Applied WRED table name: 1
```

Table 37 Command output

Field	Description
Interface	Interface type and interface number.

display qos wred table

Use **display qos wred table** to display the WRED table configuration information.

Syntax

display qos wred table [**name** *table-name*] [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

name *table-name*: Specifies the name of the WRED table to be displayed.

slot *slot-number*: Specifies an IRF member device. The *slot-number* argument is the member device ID in the IRF fabric.

Usage guidelines

If no WRED table name is specified, this command displays the configuration of all the WRED tables.

Examples

Display the configuration of WRED table 1.

```
<Sysname> display qos wred table name 1
Table name: 1
Table type: Queue based WRED
QID   gmin  gmax  gprob  ymin  ymax  yprob  rmin  rmax  rprob  exponent  ECN
------------------------------------------------------------------------------
0     100   1000  10     100   1000  10     100   1000  10     9         N
1     100   1000  10     100   1000  10     100   1000  10     9         N
2     100   1000  10     100   1000  10     100   1000  10     9         N
3     100   1000  10     100   1000  10     100   1000  10     9         N
4     100   1000  10     100   1000  10     100   1000  10     9         N
5     100   1000  10     100   1000  10     100   1000  10     9         N
6     100   1000  10     100   1000  10     100   1000  10     9         N
7     100   1000  10     100   1000  10     100   1000  10     9         N
```

Table 38 Command output

Field	Description
Table name	Name of a WRED table.
Table type	Type of a WRED table.
QID	Queue ID.
gmin	Lower limit for green packets.
gmax	Upper limit for green packets.
gprob	Drop probability for green packets.
ymin	Lower limit for yellow packets.
ymax	Upper limit for yellow packets.
yprob	Drop probability for yellow packets.
rmin	Lower limit for red packets.
rmax	Upper limit for red packets.
rprob	Drop probability for red packets.
exponent	Exponent for average queue length calculation.
ECN	Indicates whether ECN is enabled for the queue: • **Y**—Enabled. • **N**—Disabled.

qos wred apply

Use **qos wred apply** to apply a WRED table to an interface.

Use **undo qos wred apply** to restore the default.

Syntax

qos wred apply [*table-name*]

undo qos wred apply

Default

No WRED table is applied to an interface, and the tail drop mode is used on an interface.

Views

Layer 2 Ethernet interface view, Layer 3 Ethernet interface view

Predefined user roles

network-admin

Parameters

table-name: Specifies a WRED table by its name.

Usage guidelines

If no WRED table is specified, this command applies the default WRED table to the interface.

Examples

Apply the queue-based WRED table **table1** to interface Ten-GigabitEthernet 1/1/5.

```
<Sysname> system-view
[Sysname] interface Ten-GigabitEthernet 1/1/5
[Sysname-Ten-GigabitEthernet1/1/5] qos wred apply table1
```

Related commands

- **display qos wred interface**
- **display qos wred table**
- **qos wred table**

qos wred table

Use **qos wred table** to create a WRED table and enter WRED table view.

Use **undo qos wred table** to delete a WRED table.

Syntax

qos wred queue table *table-name*

undo qos wred queue table *table-name*

Default

No WRED table exists on the switch.

Views

System view

Predefined user roles

network-admin

Parameters

queue: Creates a queue-based WRED table, which drops packets based on the queue when congestion occurs.

table *table-name*: Specifies a name for the WRED table.

Usage guidelines

You cannot delete a WRED table in use. To delete it, first remove it from the specified interface.

Examples

Create a queue-based WRED table named **queue-table1**.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1]
```

Related commands

display qos wred table

queue

Use **queue** to configure the drop-related parameters for a specified queue in the queue-based WRED table.

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

Syntax

queue *queue-id* [**drop-level** *drop-level*] **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo queue { *queue-id* | **all** }

Default

After a WRED table is created, the *low-limit* argument is 100, the *high-limit* argument is 1000, and the *discard-prob* argument is 10.

Views

WRED table view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue number in the range of 0 to 7.

drop-level *drop-level*: Specifies a drop level. This argument is a consideration for dropping packets. The value 0 corresponds to green packets, the value 1 corresponds to yellow packets, and the value 2 corresponds to red packets. If this argument is not specified, the subsequent configuration takes effect on the packets in the queue regardless of the drop level.

low limit *low-limit*: Specifies the lower limit for the average queue length, in the range of 0 to 38000.

high-limit *high-limit*: Specifies the upper limit for the average queue length. The *high-limit* argument is in the range of 0 to 38000 and must be greater than the *low-limit* argument.

discard-probability *discard-prob*: Specifies the numerator for drop probability calculation in percentage, in the range of 0 to 100.

Usage guidelines

When the average queue size is smaller than the lower threshold, no packet is dropped. When the average queue size is between the lower threshold and the upper threshold, the packets are dropped based on the user-configured drop probability. When the average queue size exceeds the upper threshold, subsequent packets are dropped.

Examples

In queue-based WRED table **queue-table1**, configure the following drop-related parameters for packets in queue 1: the drop level is 1, the lower limit for the average queue length is 10, the upper limit for the average queue length is 20, and the denominator for drop probability calculation is 30%.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 10 high-limit 20
discard-probability 30
```

Related commands

- **display qos wred table**
- **qos wred table**

queue ecn

Use **queue ecn** to enable ECN for a specified queue.

Use **undo queue ecn** to restore the default.

Syntax

queue *queue-id* **ecn**

undo queue *queue-id* **ecn**

Default

ECN is not enabled on any queue.

Views

WRED table view

Predefined user roles

network-admin

Parameters

queue-id: Queue number, which ranges from 0 to 7.

Usage guidelines

When both the receiver and sender support ECN, the device can notify the peer end of the congestion status by identifying and setting the ECN flag. ECN avoids deteriorating congestion.

Examples

In WRED table **queue-table1**, enable ECN for queue 1.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 ecn
```

Related commands

- **display qos wred table**
- **qos wred table**

queue weighting-constant

Use **queue weighting-constant** to specify an exponent for average queue length calculation for a specified queue.

Use **undo queue weighting-constant** to restore the default.

Syntax

queue *queue-id* **weighting-constant** *exponent*

undo queue *queue-id* **weighting-constant**

Default

The exponent for average queue length calculation is 9.

Views

WRED table view

Predefined user roles

network-admin

Parameters

queue-id: Specifies a queue number.

weighting-constant *exponent*: Specifies the WRED exponent for average queue length calculation, in the range of 0 to 15.

Usage guidelines

The bigger the exponent is, the less sensitive the average queue size is to real-time queue size changes. The average queue size is calculated using the formula: average queue size = previous average queue size × $(1-2^{-n})$ + current queue size × 2^{-n}, where n can be configured with the **qos wred weighting-constant** command.

Examples

In WRED table **queue-table1**, set the exponent for average queue length calculation to 12 for queue 1.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 weighting-constant 12
```

Related commands

- **display qos wred table**
- **qos wred table**

Aggregate CAR commands

car name

Use **car name** to reference an aggregate CAR action in a traffic behavior.

Use **undo car** to remove an aggregate CAR action from a traffic behavior.

Syntax

car name *car-name*

undo car

Default

No aggregate CAR action is configured in a traffic behavior.

Views

Traffic behavior view

Predefined user roles

network-admin

Parameters

car-name: Specifies the name of an aggregate CAR action. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters.

Examples

Reference the aggregate CAR action **aggcar-1** in the traffic behavior **be1**.

```
<Sysname> system-view
[Sysname] traffic behavior be1
[Sysname-behavior-be1] car name aggcar-1
```

Related commands

- **display qos car name**
- **display traffic behavior user-defined**

display qos car name

Use **display qos car name** to display the configuration and statistics of a specified aggregate CAR action.

Syntax

display qos car name [*car-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

car-name: Specifies the name of an aggregate CAR action. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters. If no CAR action is specified, this command displays the configuration and statistics of all the aggregate CAR actions.

Examples

Display aggregate CAR configuration.

```
<Sysname> display qos car name
 Name: a
  Mode: aggregative
  CIR 12800 (kbps), CBS 800256 (Bytes), EBS 512 (Bytes)
  Green action: pass
  Yellow action: pass
  Red action: discard
   Slot 1:
    Green packets: 54641 (Packets)
    Red packets: 856 (Packets)
   Slot 2:
    Green packets: 12541 (Packets)
    Red packets: 1235 (Packets)
```

Table 39 Command output

Field	Description
Name	Name of the aggregate CAR action.
Mode	Type of the aggregate CAR action: **aggregative.**
CIR CBS EBS PIR	Parameters for the CAR action.
Green action	Action to take on green packets: • **discard**—Drops the packets. • **pass**—Permits the packets to pass through.
Yellow action	Action to take on yellow packets: • **discard**—Drops the packets. • **pass**—Permits the packets to pass through.
Red action	Action to take on red packets: • **discard**—Drops the packets. • **pass**—Permits the packets to pass through.
Green packet	Statistics about green packets.
Red packet	Statistics about red packets.

qos car

Use **qos car** to configure an aggregate CAR action.

Use **undo qos car** to remove an aggregate CAR action.

Syntax

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

undo qos car *car-name*

Default

No aggregate CAR action is configured.

Views

System view

Predefined user roles

network-admin

Parameters

car-name: Specifies the name of the aggregate CAR action. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters.

aggregative: Specifies the aggregate CAR action.

cir *committed-information-rate*: Specifies the CIR in kbps. The value range for the *committed-information-rate* argument is an integral multiple of 8 between 8 and 160000000.

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

ebs *excess-burst-size*: Specifies the EBS in bytes. The value range for the *excess-burst-size* argument is an integral multiple of 512 between 0 and 256000000, and the default value is 512.

pir *peak-information-rate*: Specifies the PIR in kbps. The value range for the *peak-information-rate* argument is an integral multiple of 8 between 8 and 160000000.

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

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

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

action: Specifies the action to take on packets:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.
- **remark-dot1p-pass** *new-cos*: Sets the 802.1p priority value of the 802.1p packet to *new-cos* and permits the packet to pass through. The *new-cos* argument ranges from 0 to 7.
- **remark-dscp-pass** *new-dscp*: Remarks the packet with a new DSCP value and permits the packet to pass through. The value range is 0 to 63. Alternatively, you can specify the *new-dscp* argument with **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.

Usage guidelines

An aggregate CAR action takes effect only after it is applied to an interface or referenced in a QoS policy.

Examples

Configure the aggregate CAR action **aggcar-1**, where CIR is 25600, CBS is 512000, and red packets are dropped.

```
<Sysname> system-view
[Sysname] qos car aggcar-1 aggregative cir 25600 cbs 512000 red discard
```

Related commands

display qos car name

reset qos car name

Use **reset qos car name** to clear the statistics about a specific aggregate CAR action.

Syntax

reset qos car name [*car-name*]

Views

User view

Predefined user roles

network-admin

Parameters

car-name: Specifies the name of an aggregate CAR action. This argument must start with a letter, and is a case-sensitive string of 1 to 31 characters. If no *car-name* is specified, the statistics about all the aggregate CAR actions is cleared.

Examples

Clear the statistics about the aggregate CAR action **aggcar-1**.

```
<Sysname> reset qos car name aggcar-1
```

Data buffer commands

Inappropriate data buffer changes can cause system problems. Before manually changing data buffer settings, make sure you understand its impact on your device. If the system requires large buffer spaces, HP recommends that you use the **burst-mode enable** command. This command cannot be configured together with any other command in this chapter.

buffer apply

Use **buffer apply** to apply manually configured data buffer settings.

Use **undo buffer apply** to cancel the application.

Syntax

buffer apply

undo buffer apply

Views

System view

Predefined user roles

network-admin

Usage guidelines

After applying manually configured data buffer settings, you cannot directly modify the applied settings. To modify them, you must cancel the application, re-configure data buffer settings, and re-apply the new settings.

Examples

Apply manually configured data buffer settings.

```
<Sysname> system-view
[Sysname] buffer apply
```

buffer queue guaranteed

Use **buffer queue guaranteed** to set the fixed-area ratio for a queue.

Use **undo buffer queue guaranteed** to restore the default.

Syntax

buffer egress [**slot** *slot-number*] **cell queue** *queue-id* **guaranteed ratio** *ratio-value*

undo buffer egress [**slot** *slot-number*] **cell queue** *queue-id* **guaranteed**

Default

The fixed-area ratio for a queue is 12.5%.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its ID. Without this option, the command applies to all IRF member devices.

cell: Specifies cell resources.

queue-id: Specifies a queue by its number in the range of 0 to 7.

ratio *ratio-value*: Specifies the fixed-area ratio in percentage.

Usage guidelines

By default, all queues have an equal share of the fixed area. You can set the fixed-area ratio for a queue. After you configure the fixed-area ratios for some queues, the other queues each are assigned an equal share of the remaining part of the fixed area. The **display buffer queue** command displays a rounded-off value for the assignment result. Therefore, the sum of the ratios for all queues might be less than or greater than 100%.

The fixed-area space for a queue cannot be used by other queues. Therefore, it is also called the minimum guaranteed buffer for the queue. The sum of fixed-area ratios configured for queues cannot be greater than or equal to 100%, and queues 5, 6, and 7 must have available fixed-area space.

Examples

Configure queue 0 to use 15% fixed-area space of cell resources in the egress buffer of IRF member device 2.

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell queue 0 guaranteed ratio 15
```

buffer queue shared

Use **buffer queue shared** to set the maximum shared-area ratio for a queue.

Use **undo buffer queue shared** to restore the default.

Syntax

buffer egress [**slot** *slot-number*] **cell queue** *queue-id* **shared ratio** *ratio-value*

undo buffer egress [**slot** *slot-number*] **cell queue** *queue-id* **shared**

Default

The maximum shared-area ratio for a queue is 33%.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its ID. Without this option, the command applies to all IRF member devices.

cell: Specifies cell resources.

queue-id: Specifies a queue by its number in the range of 0 to 7.

ratio *ratio-value*: Specifies the maximum shared-area ratio in percentage.

Usage guidelines

By default, all queues have an equal share of the shared area. You can set the shared-area ratio for a queue. The other queues use the default setting. The shared-area ratio for each queue is finally determined by the chip based on your configuration and the number of packets to be sent.

For the maximum shared-area ratio for a queue, the percentage values 0 to 100 are divided into 10 ranges. Table 40 shows the effective values that correspond to the configured values of *ratio-value*.

Table 40 Mapping between configured values of *ratio-value* and effective values

Configured value of ratio-value	Effective value
0 to 1	1
2 to 3	3
4 to 7	6
8 to 16	11
17 to 29	20
30 to 42	33
43 to 60	50
61 to 76	67
77 to 86	80
89 to 100	89

Examples

Configure queue 0 to use up to 5% shared-area ratio of cell resources in the egress buffer of IRF member device 2.

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell queue 0 shared ratio 5
```

buffer total-shared

Use **buffer total-shared** to set the shared area ratio.

Use **undo buffer total-shared** to restore the default.

Syntax

buffer egress [**slot** *slot-number*] **cell total-shared ratio** *ratio-value*

undo buffer egress [**slot** *slot-number*] **cell total-shared**

Default

The shared area ratio is 100%.

Views

System view

Predefined user roles

network-admin

Parameters

egress: Specifies the egress buffer.

slot *slot-number*: Specifies an IRF member device by its ID. Without this option, the command applies to all IRF member devices.

cell: Specifies cell resources.

ratio *ratio-value*: Specifies the ratio of the shared area in percentage.

Usage guidelines

After you configure the shared area ratio, the remaining buffer space is automatically assigned to the fixed area.

Examples

Configure the shared area to use 65% space of cell resources in the egress buffer of IRF member device 2.

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell total-shared ratio 65
```

burst-mode enable

Use **burst-mode enable** to enable the Burst function.

Use **undo burst-mode enable** to disable the Burst function.

Syntax

burst-mode enable

undo burst-mode enable

Default

The Burst function is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

The Burst function is especially useful for reducing packet losses under circumstances such as the following:

- Broadcast or multicast traffic is intensive, resulting in bursts of traffic.
- Traffic enters a device from a high-speed interface and goes out of a low-speed interface, or enters from multiple same-rate interfaces and goes out of an interface also with the same rate.

Examples

Enable the Burst function.

```
<Sysname> system-view
[Sysname] burst-mode enable
```

display buffer

Use **display buffer** to display buffer configuration.

Syntax

display buffer [**slot** *slot-number*] [**queue** [*queue-id*]]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. Without this option, the command applies to all IRF member devices.

queue *queue-id*: Specifies a queue by its number in the range of 0 to 7. If no queue is specified, the command displays configuration information for all queues.

Usage guidelines

Without the **queue** keyword, this command displays the total shared-area ratio.

With the **queue** keyword, this command displays the fixed-area ratio and shared-area ratio for a queue.

Examples

Display the total shared-area ratio.

```
<Sysname> display buffer
Slot  Type    Eg(Total-shared)
1     cell    25

          Eg: Size of the sending buffer
Total-shared: Size of the shared buffer for all ports
        Unit: Ratio
```

Display the fixed-area ratio and shared-area ratio for each queue.

```
<Sysname> display buffer queue
Slot  Queue        Type    Eg(Guaranteed , Shared)
2     0            cell    20 , 33
2     1            cell    13 , 35
2     2-7          cell    11 , 33

          Eg: Size of the sending buffer
  Guaranteed: Size of the minimum guaranteed buffer per queue
      Shared: Size of the maximum shared buffer per queue
```

```
Unit: Ratio
```

Table 41 Command output

Field	Description
Slot	ID of an IRF member device.
Type	Resource type. The device supports only cell resources.
Queue	Queue ID in the range of 0 to 7.
Eg	Egress buffer.
(Total-shared)	Total shared-area size.
(Guaranteed , Shared)	• **Guaranteed**—Fixed-area ratio for a queue. • **Shared**—Shared-area ratio for a queue.
Unit	Unit for configuring the data buffer. The device supports only ratio.

display buffer usage

Use **display buffer usage** to display data buffer usage.

Syntax

display buffer usage [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. Without this option, the command applies to all IRF member devices.

Examples

Display data buffer usage.

```
<Sysname> display buffer usage
Egress total-shared cell buffer usage on slot 1 :
Total:    9197 KB
Used:       0 KB
Free:     9197 KB
                                      5sec     1min     5min
-------------------------------------------------------------------
Block 1                                 0%       0%       0%
Ten-GigabitEthernet1/0/1                0%       0%       0%
Ten-GigabitEthernet1/0/2                0%       0%       0%
Ten-GigabitEthernet1/0/3                0%       0%       0%
Ten-GigabitEthernet1/0/4                0%       0%       0%
```

```
Ten-GigabitEthernet1/0/5                0%      0%      0%
Ten-GigabitEthernet1/0/6                0%      0%      0%
Ten-GigabitEthernet1/0/7                0%      0%      0%
Ten-GigabitEthernet1/0/8                0%      0%      0%
Ten-GigabitEthernet1/0/9                0%      0%      0%
Ten-GigabitEthernet1/0/10               0%      0%      0%
Ten-GigabitEthernet1/0/11               0%      0%      0%
Ten-GigabitEthernet1/0/12               0%      0%      0%
Ten-GigabitEthernet1/0/13               0%      0%      0%
Ten-GigabitEthernet1/0/14               0%      0%      0%
Ten-GigabitEthernet1/0/15               0%      0%      0%
Ten-GigabitEthernet1/0/16               0%      0%      0%
Ten-GigabitEthernet1/0/17               0%      0%      0%
Ten-GigabitEthernet1/0/18               0%      0%      0%
Ten-GigabitEthernet1/0/19               0%      0%      0%
Ten-GigabitEthernet1/0/20               0%      0%      0%
FortyGigE1/1/1                          0%      0%      0%
FortyGigE1/1/2                          0%      0%      0%
FortyGigE1/1/3                          0%      0%      0%
FortyGigE1/1/4                          0%      0%      0%
Ten-GigabitEthernet1/1/5                0%      0%      0%
Ten-GigabitEthernet1/1/6                0%      0%      0%
Ten-GigabitEthernet1/1/7                0%      0%      0%
Ten-GigabitEthernet1/1/8                0%      0%      0%
Ten-GigabitEthernet1/1/9                0%      0%      0%
Ten-GigabitEthernet1/1/10               0%      0%      0%
Ten-GigabitEthernet1/1/11               0%      0%      0%
Ten-GigabitEthernet1/1/12               0%      0%      0%
```

Table 42 Command output

Field	Description
Egress total-shared cell buffer usage on slot	Usage of the shared area of cell resources on an IRF member device.
Total	Total size of the data buffer.
Used	Size of used data buffer.
Free	Size of free data buffer.
Block1	Block where the port resides. The block where the ports on the front panel of the device reside is fixed to Block 1.
5sec	Percentage of the buffer that the port uses for the last 5 seconds.
1min	Percentage of the buffer that the port uses for the last 1 minute.
5min	Percentage of the buffer that the port uses for the last 5 minutes.

Time range commands

display time-range

Use **display time-range** to display time range configuration and status.

Syntax

display time-range { *time-range-name* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

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

Examples

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

```
<Sysname> display time-range t4
Current time is 17:12:34 11/23/2010 Tuesday

Time-range : t4 (Inactive)
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2011 to 00:00 1/1/2012
 from 00:00 6/1/2011 to 00:00 7/1/2011
```

Table 43 Command output

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

time-range

Use **time-range** to create or edit a time range.

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

Syntax

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

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

Default

No time range exists.

Views

System view

Predefined user roles

network-admin

Parameters

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

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

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

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

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

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

Usage guidelines

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

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

- Periodic statement in the *start-time* **to** *end-time days* format. A periodic statement recurs periodically on a day or days of the week.
- Absolute statement in the **from** *time1 date1* **to** *time2 date2* format. An absolute statement does not recur.
- Compound statement in the *start-time* **to** *end-time days* **from** *time1 date1* **to** *time2 date2* format. A compound statement recurs on a day or days of the week only within the specified period. For example, to create a time range that is active from 08:00 to 12:00 on Monday between January 1, 2011 00:00 and December 31, 2011 23:59, use the **time-range test 08:00 to 12:00 mon from 00:00 01/01/2011 to 23:59 12/31/2011** command.

You can create a maximum of 1024 time ranges, each with a maximum of 32 periodic statements and 12 absolute statements. The active period of a time range is calculated as follows:

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

Examples

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

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

Create an absolute time range **t2**, setting it to be active in the whole year of 2011.

```
<Sysname> system-view
[Sysname] time-range t2 from 00:00 1/1/2011 to 24:00 12/31/2011
```

Create a compound time range **t3**, setting it to be active from 08:00 to 12:00 on Saturdays and Sundays of the year 2011.

```
<Sysname> system-view
[Sysname] time-range t3 08:00 to 12:00 off-day from 00:00 1/1/2011 to 24:00 12/31/2011
```

Create a compound time range **t4**, setting it to be active from 10:00 to 12:00 on Mondays and from 14:00 to 16:00 on Wednesdays in the period of January through June of the year 2011.

```
<Sysname> system-view
[Sysname] time-range t4 10:00 to 12:00 1 from 00:00 1/1/2011 to 24:00 1/31/2011
[Sysname] time-range t4 14:00 to 16:00 3 from 00:00 6/1/2011 to 24:00 6/30/2011
```

Related commands

display time-range

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking
- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com
- HP Education http://www.hp.com/learn

Conventions

This section describes the conventions used in this documentation set.

Command conventions

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

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

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

Network topology icons

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

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index

R

S

T

W