HP A8800 Routers

ACL and QoS

Command Reference

Part number: 5998-1761
Software version: A8800-CMW520-R3627
Document version: 6W102-20130906

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 configuration commands

In this chapter, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L. SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.

acl

Syntax

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

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

View

System view

Default level

2: System level

Parameters

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

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

name *acl-name*: Assigns a name to the ACL for easy identification. The *acl-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter, and to avoid confusion, 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: Deletes all IPv4 basic, IPv4 advanced, Ethernet frame header, and user-defined ACLs.

Description

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

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

By default, no ACL exists.

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

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

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

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

Examples

Create ACL 2000, and enter its view.

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

Create ACL 2002 with the name **flow**, and enter its view.

```
<Sysname> system-view
[Sysname] acl number 2002 name flow
[Sysname-acl-basic-2002-flow]
```

Enter the view of an ACL by specifying its number.

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

Enter the view of an ACL by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2002
[Sysname-acl-basic-2002-flow]
```

Delete the ACL numbered 2000.

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

Delete the ACL named **flow**.

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

acl copy

Syntax

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

View

System view

Default level

2: System level

Parameters

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

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

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

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

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

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

Description

Use **acl copy** to create an ACL by copying an ACL that already exists. Except for the number and name (if any), the new ACL has the same configuration as the source ACL.

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

Examples

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

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

acl ipv6

Syntax

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

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

View

System view

Default level

2: System level

Parameters

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

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

name *acl6-name*: Assigns a name to the ACL for easy identification. The *acl6-name* argument takes a case-insensitive string of 1 to 63 characters. It must start with an English letter, and to avoid confusion, 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: Delete all IPv6 basic and IPv6 advanced ACLs.

Description

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

Use **undo acl ipv6** to delete the specified IPv6 ACL or all IPv6 basic and IPv6 advanced ACLs.

By default, no ACL exists.

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

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

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

Examples

Create IPv6 ACL 2000 and enter its view.

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

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

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

acl ipv6 copy

Syntax

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

View

System view

Default level

2: System level

Parameters

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

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

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

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

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

name *dest-acl6-name*: Assigns a unique name to the ACL you are creating. The *dest-acl6-name* takes a case-insensitive string of 1 to 63 characters. It must start with an English letter and to avoid confusion,

cannot be **all**. For this ACL, the system automatically picks the smallest number from all available numbers in the same ACL category as the source ACL.

Description

Use **acl ipv6 copy** to create an IPv6 basic or IPv6 advanced ACL by copying an IPv6 basic or IPv6 advanced ACL that already exists. Except for the number and name (if any), the new ACL has the same configuration as the source ACL.

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

Examples

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

```
<Sysname> system-view
[Sysname] acl ipv6 copy 2001 to 2002
```

acl ipv6 logging frequence

Syntax

acl ipv6 logging frequence *frequence*

undo acl ipv6 logging frequence

View

System view

Default level

2: System level

Parameters

frequence: Specifies the interval in minutes at which IPv6 packet filtering logs are generated and output. It must be a multiple of 5, in the range of 0 to 1440. To disable generating IPv6 logs, assign 0 to the argument.

Description

Use **acl ipv6 logging frequence** to set the interval for generating and outputting IPv6 packet filtering logs. The log information includes the number of matching IPv6 packets and the matching ACL rules. This command logs only for IPv6 basic ACL rules and IPv6 advanced ACL rules that have the **logging** keyword.

Use **undo acl ipv6 logging frequence** to restore the default.

By default, the interval is 0. No IPv6 packet filtering logs are generated.

Related commands: **rule (IPv6 advanced ACL view)** and **rule (IPv6 basic ACL view)**.

Examples

Enable the device to generate and output IPv6 packet filtering logs at 10-minute intervals.

```
<Sysname> system-view
[Sysname] acl ipv6 logging frequence 10
```

acl ipv6 name

Syntax

acl ipv6 name *acl6-name*

View

System view

Default level

2: System level

Parameters

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

Description

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

Related commands: **acl ipv6**.

Examples

Enter the view of IPv6 basic ACL **flow**.

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

acl logging frequence

Syntax

acl logging frequence *frequence*

undo acl logging frequence

View

System view

Default level

2: System level

Parameters

frequence: Specifies the interval in minutes at which IPv4 packet filtering logs are generated and output. It must be a multiple of 5, in the range of 0 to 1440. To disable generating IPv4 logs, assign 0 to the argument.

Description

Use **acl logging frequence** to set the interval for generating and outputting IPv4 packet filtering logs. The log information includes the number of matching IPv4 packets and the matching ACL rules. This command logs only for IPv4 basic ACL rules and IPv4 advanced ACL rules that have the **logging** keyword.

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

By default, the interval is 0. No IPv4 packet filtering logs are generated.

Related commands: **rule (IPv4 advanced ACL view)** and **rule (IPv4 basic ACL view)**.

Examples

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

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

acl mode

Syntax

acl mode { **1** | **2** | **3** | **4** }

View

System view

Default Level

2: System level

Parameters

1: 18 bytes for an SPE card and 40 bytes for an SPC card.

2: 36 bytes for an SPE card and 40 bytes for an SPC card.

3: 18 bytes for an SPE card and 80 bytes for an SPC card.

4: 36 bytes for an SPE card and 80 bytes for an SPC card.

Description

Use **acl mode** to set the ACL rule length limit mode. The length limit mode takes effect after you restart the router.

By default, the ACL rule length limit mode is 2.

Examples

Set the ACL rule length limit mode to 1 so that the length limit for an SPE card is set to 18 bytes and that for an SPC card is set to 40 bytes.

```
<Sysname> system-view
[Sysname] acl mode 1
  ACL has been set to mode 1, and will take effect after the next system reboot.
```

acl name

Syntax

acl name *acl-name*

View

System view

Default level

2: System level

Parameters

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

Description

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

Related commands: **acl**.

Examples

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

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

description

Syntax

description *text*

undo description

View

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

Default level

2: System level

Parameters

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

Description

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

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

By default, an ACL has no ACL description.

Related commands: **display acl** and **display acl ipv6**.

Examples

Configure a description for IPv4 basic ACL 2000.

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

Configure a description for IPv6 basic ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This is an IPv6 basic ACL.
```

display acl

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

acl-number: Specifies an ACL by its number:

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

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

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

slot *slot-number*: Displays the match statistics for ACLs on a card. The *slot-number* argument specifies a card by its slot number. If no slot is provided, the command displays the configurations of ACLs on the device.

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

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

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

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

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

Description

Use **display acl** to display configuration and match statistics for the specified ACL or all IPv4 basic, IPv4 advanced, Ethernet frame header, and user-defined ACLs.

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

Examples

Display the configuration and match statistics for ACL 2001.

```
<Sysname> display acl 2001
Basic ACL  2001, named flow, 1 rule,
ACL's step is 5
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used in GE3/1/1
Basic ACL  2002, named -none-, 1 rule,
```

```
ACL's step is 5
 rule 0 permit source 10.110.0.0 0.0.0.255
```

Table 1 Command output

Field	Description
Basic ACL 2001	Category and number of the ACL. The following field information is about ACL 2001.
named flow	The name of the ACL is flow. "-none-" means the ACL is not named.
1 rule	The ACL contains one rule.
ACL's step is 5	The rule numbering step is 5.
5 times matched	There have been five matches for the rule. The statistic counts only ACL matches performed by software. This field is not displayed when no packets have matched the rule.
Uncompleted	Applying the rule to hardware failed because no sufficient resources were available or the hardware does not support the rule. This event might occur when you modify a rule in an ACL that has been applied.
rule 5 comment This rule is used in GE3/1/1.	The description of ACL rule 10 is "This rule is used in GE3/1/1."

display acl ipv6

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

acl6-number: Specifies an ACL by its number:

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

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

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

slot *slot-number*: Displays the match statistics for ACLs on a card. The *slot-number* argument represents the slot number of the card. If no slot number is provided, the command displays configuration information about all ACLs on the device.

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

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

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

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

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

Description

Use **display acl ipv6** to display the configuration and match statistics for the specified IPv6 ACL or all IPv6 basic and IPv6 advanced ACLs.

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

Examples

Display the configuration and match statistics for ACL 2001.

```
<Sysname> display acl ipv6 2001
Basic IPv6 ACL  2001, named flow, 1 rule,
ACL's step is 5
rule 0 permit source 1::2/128 (5 times matched)
rule 0 comment This rule is used in GE3/1/1
Basic IPv6 ACL  2002, named -none-, 1 rule,
 ACL's step is 5
 rule 0 permit source FF1E::101:101/128
```

Table 2 Command output

Field	Description
Basic IPv6 ACL 2001	Category and number of the ACL. The following field information is about this IPv6 basic ACL 2001.
named flow	The name of the ACL is flow. "-none-" means the ACL is not named.
1 rule	The ACL contains one rule.
ACL's step is 5	The rule numbering step is 5.
5 times matched	There have been five matches for the rule. The statistic counts only IPv6 ACL matches performed by software. This field is not displayed when no packets have matched the rule.
Uncompleted	Applying the rule to hardware failed because no sufficient resources were available or the hardware does not support the rule. This event might occur when you modify a rule in an ACL that has been applied.
rule 0 comment This rule is used in GE3/1/1.	The description of ACL rule 10 is "This rule is used in GE3/1/1."

display acl mode

Syntax

display acl mode [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default Level

1: Monitor level

Parameters

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

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

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

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

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

Description

Use **display acl mode** to display the ACL rule length limit mode.

Examples

Display the ACL rule length limit mode.

```
<Sysname> display acl mode
Current ACL mode              : mode 3 (SPE ACL key short, SPC ACL key long)
Acl mode after system restart : mode 3 (SPE ACL key short, SPC ACL key long)
Notice: Changing ACL mode will take effect only after system restart.
```

Table 3 Command output

Field	Description
Current acl mode	ACL rule length limit mode that is currently effective.
Acl mode after system restart	ACL rule length limit mode that is to be effective after system restart.

display acl resource

Syntax

display acl resource [| { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the usage of ACL rules on a card. The *slot-number* argument specifies the slot number of the card. If no slot number is specified, the usage of ACL rules on the main board is displayed.

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

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

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

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

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

Description

Use **display acl resource** to display the usage of ACL rules.

If a card does not support counting ACL rules, the command displays only the slot number of the card.

Examples

Display the usage of ACL resources on all cards.

```
<Sysname> display acl resource
  Slot: 2
  Resource   Total   Reserved  Configured  Remaining  Start       End
  Type       Number  Number    Number      Number     Interface   Interface
  ---------------------------------------------------------------------------
  IPV4-ACL   16384   0         0           16384      GE2/1/1     GE2/1/8
  IPV6-ACL   1024    0         0           1024       GE2/1/1     GE2/1/8
```

Table 4 Command output

Field	Description
Slot	Slot number of a card.
Resource Type	Resource type.
Total Number	Total number of ACL rules supported.
Reserved Number	Number of reserved ACL rules.
Configured Number	Number of ACL rules that have been applied.
Remaining Number	Number of ACL rules that you can apply.
Start Interface	Name of the start interface on the card.
End Interface	Name of the end interface on the card.

display flow-template interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and number. If no interface is specified, information about all user-defined flow templates applied to interfaces is displayed.

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

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

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

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

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

Description

Use **display flow-template interface** to display information about user-defined flow templates applied to interfaces.

Examples

Display information about all user-defined flow templates applied to interfaces.

```
<Sysname> display flow-template interface
Interface: GigabitEthernet2/1/1
user-defined flow template: basic
 name:1, index:2, total reference counts:1
 fields: service-cos
```

Table 5 Command output

Field	Description
Interface	Interface where the user-defined flow template is referenced.
user-defined flow template	Type of the user-defined flow template.
name	Name of the user-defined flow template.
index	Index of the user-defined flow template.
total reference counts	Total number of times that the user-defined flow template has been referenced.
fields	Fields included in the user-defined flow template.

display flow-template user-defined

Syntax

display flow-template user-defined [*flow-template-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

flow-template-name: Name of a user-defined flow template, a case-insensitive string of 1 to 31 characters. If no user-defined flow template name is specified, information about all user-defined flow templates is displayed.

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

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

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

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

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

Description

Use **display flow-template user-defined** to display information about user-defined flow templates.

Examples

Display information about all user-defined flow templates.

```
<Sysname> display flow-template user-defined
user-defined flow template: basic
 name:f1, index:1, total reference counts:1
 fields: ip-protocol fragments ip-precedence
user-defined flow template: basic
 name:f3, index:3, total reference counts:1
 fields: tos
```

Table 6 Command output

Field	Description
user-defined flow template	Type of the user-defined flow template.
name	Name of the user-defined flow template.
index	Index of the user-defined flow template.
total reference counts	Total number of times that the user-defined flow template has been referenced by switching chips.
fields	Fields included in the user-defined flow template.

display time-range

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

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

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

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

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

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

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

Description

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

Examples

Display the configuration and status of time range **test**.

```
<Sysname> display time-range test
Current time is 15:45:29 2/8/2007 Thursday
Time-range : test ( Active )
 08:00 to 18:00 working-day
```

Table 7 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.

flow-template

Syntax

flow-template flow-template-name

undo flow-template

View

Interface view, port group view

Default level

2: System level

Parameters

flow-template-name: Specifies the name of an existing user-defined flow template, a case-insensitive string of 1 to 31 characters.

Description

Use **flow-template** to apply a user-defined flow template to an interface or port group.

Use **undo flow-template** to restore the default.

The user-defined flow template applied to a port group takes effect on all interfaces in the group.

This command is available only on SPE cards.

You can apply only one user-defined flow template on an interface.

Examples

Apply user-defined flow template **f1** to GigabitEthernet 3/1/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 3/1/1
[Sysname-GigabitEthernet3/1/1] flow-template f1
```

Apply user-defined flow template **f1** to port group 1.

```
<Sysname> system-view
[Sysname] port-group manual 1
[Sysname-port-group-manual-1] group-member GigabitEthernet 3/1/1 to GigabitEthernet
3/1/6
[Sysname-port-group-manual-1] flow-template f1
```

flow-template basic

Syntax

flow-template *flow-template-name* **basic** { **customer-vlan-id** | **dip** | **dmac** | **dport** | **dscp** | **ethernet-protocol** | **fragments** | **icmp-code** | **icmp-type** | **ip-precedence** | **ip-protocol** | **mpls-exp** | **service-cos** | **sip** | **smac** | **sport** | **tcp-flag** | **tos** } *

undo flow-template { **all** | **name** *flow-template-name* }

View

System view

Default level

2: System level

Parameters

flow-template-name: Assigns a name to a user-defined flow template, a case-insensitive string of 1 to 31 characters.

basic: Sets the type of the user-defined flow template to basic.

customer-vlan-id: Customer VLAN ID.

dip: Destination IP address.

dmac: Destination MAC address.

dport: Destination port.

dscp: Differentiated service code point (DSCP) field in the IP header.

ethernet-protocol: Protocol type field in the Ethernet frame header.

fragments: Fragments field in the IP header.

icmp-code: ICMP code field.

icmp-type: ICMP type field.

ip-precedence: Precedence field in the IP header.

ip-protocol: Protocol type field in the IP header.

mpls-exp: EXP field in the MPLS label.

service-cos: Service provider 802.1p COS field.

sip: Source IP address.

smac: Source MAC address.

sport: Source port.

tcp-flag: Flags field in the TCP header.

tos: ToS field in the IP header.

all: Deletes all user-defined flow templates.

Description

Use **flow-template basic** to create a basic user-defined flow template.

Use **undo flow-template** to delete one or all user-defined flow templates. To guarantee a successful removal, check that the template you are deleting has not applied to any interface.

Examples

Create a basic user-defined flow template.

```
<Sysname> system-view
[Sysname] flow-template f1 basic dip smac ip-protocol tcp-flag
```

hardware-count enable

Syntax

hardware-count enable

undo hardware-count enable

View

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

Default level

2: System level

Parameters

None

Description

Use **hardware-count enable** to enable counting ACL rule matches performed in hardware. The device automatically counts the rule match counting performed in software when the ACL is referenced by packet filtering.

Use **undo hardware-count enable** to disable counting ACL rule matches performed in hardware. This command also resets the hardware match counters for all rules in the ACL. For a rule configured with the **counting** keyword, this command only resets the rule's hardware match counter.

By default, ACL rule matches performed in hardware are not counted.

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

Related commands: **display acl**, **display acl ipv6**, **firewall packet-filter**, and **rule**.

Examples

Enable rule match counting for IPv4 ACL 2000.

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

Enable rule match counting for IPv6 ACL 2000.

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

```
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] hardware-count enable
```

reset acl counter

Syntax

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

View

User view

Default level

2: System level

Parameters

acl-number: Specifies an ACL by its number:

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

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

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

Description

Use **reset acl counter** to clear statistics for the specified ACL or all ACLs.

Related commands: **display acl**.

Examples

Clear statistics for IPv4 basic ACL 2001.

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

Clear statistics for ACL **flow**.

```
<Sysname> reset acl counter name flow
```

reset acl ipv6 counter

Syntax

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

View

User view

Default level

2: System level

Parameters

acl6-number: Specifies an ACL by its number:

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

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

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

Description

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

Related commands: **display acl ipv6**.

Examples

Clear statistics for IPv6 basic ACL 2001.

```
<Sysname> reset acl ipv6 counter 2001
```

Clear statistics for ACL **flow**.

```
<Sysname> reset acl ipv6 counter name flow
```

rule (Ethernet frame header ACL view)

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**] *

View

Ethernet frame header ACL view

Default level

2: System level

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

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 IPv4 ACL rule has been matched. This feature is disabled by default. This keyword is valid when the rule is applied to the packet filtering firewall. For more information, see *Security Configuration Guide*.

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

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 *source-mask* argument represents a mask in H-H-H format.

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

Description

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

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

By default, an Ethernet frame header ACL does not contain any rule.

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 will fail.

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

Related commands: **acl**, **display acl**, **step**, and **time-range**.

Examples

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

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

rule (IPv4 advanced ACL view)

Syntax

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

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

View

IPv4 advanced ACL view

Default level

2: System level

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

protocol: Protocol carried by IPv4. It can be a number in the range of 0 to 255, or in words, **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), or **udp** (17). Table 8 describes the parameters that you can specify regardless of the value that the *protocol* argument takes.

Table 8 Match criteria and other rule information for 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 ACL rule has been matched, and disabled by default	This keyword is valid when the rule is applied to the packet filtering firewall.
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).

Parameters	Function	Description
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).
logging	Logs matching packets	This function requires that the module using the ACL supports logging. If an ACL has been applied to both the packet filtering firewall and policy-based routing modules, do not add or modify a rule that has the **logging** keyword in the ACL. Doing so can cause rule application failure on both modules. For more information about packet filtering firewall, see *Security Configuration Guide*. For more information about policy-based routing, see *Layer 3—IP Routing Configuration Guide*. Use the **logging** keyword together with the rule match counting function. To enable this function, you can either execute the **hardware-count enable** command in the ACL or specify the **counting** keyword in the ACL rule with **logging** specified.
reflective	Specifies that the rule be reflective	A rule with the **reflective** keyword can be defined only for TCP, UDP, or ICMP packets and can only be a permit statement.
vpn-instance *vpn-instance-name*	Applies the rule to packets in a VPN instance	The *vpn-instance-name* argument takes a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the rule applies only to non-VPN packets.
fragment	Applies the rule to only fragments	Without this keyword, the rule applies to all fragments and non-fragments. When the ACL rule length limit is 80 bytes on an SPC card, the ACL rule does not take effect on the first fragment of fragments for each incoming packet. For more information about the ACL rule length limit mode, see "acl mode."
time-range *time-range-name*	Specifies a time range for the rule	The *time-range-name* argument takes a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the timer range.

NOTE:

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

If the *protocol* argument takes **tcp** (6) or **udp** (7), you can set the parameters shown in Table 9.

Table 9 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**.
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports	TCP port numbers can be represented in these words: **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 in these words: **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 relationship between the TCP flags in a rule is AND.
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 takes **icmp** (1), you can set the parameters shown in Table 10.

Table 10 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 11.

Table 11 ICMP message names supported in IPv4 advanced ACL rules

ICMP message name	ICMP message type	ICMP message code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

Description

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

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

By default, an IPv4 advanced ACL does not contain any rule.

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 will fail.

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

Related commands: **acl**, **display acl**, **step**, and **time-range**.

Examples

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

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

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

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

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule 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
```

rule (IPv4 basic ACL view)

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**] *

View

IPv4 basic ACL view

Default level

2: System level

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Counts the number of times the IPv4 ACL rule has been matched. This feature is disabled by default. This keyword is valid when the rule is applied to the packet filtering firewall. For information about packet filtering firewall, see *Security Configuration Guide*.

fragment: Applies the rule only to fragments. A rule without this keyword applies to both fragments and non-fragments. When the ACL rule length limit is 80 bytes on an SPC card, the ACL rule does not take effect on the first fragment of fragments for each incoming packet. For more information about the ACL rule length limit mode, see "acl mode."

logging: Logs matching packets. This function requires that the module (for example, a firewall) using the ACL supports logging.If an ACL has been applied to both the packet filtering firewall and policy-based routing modules, do not add or modify a rule that has the **logging** keyword in the ACL. Doing so can cause rule application failure on both modules. For more information about packet filtering firewall, see *Security Configuration Guide*. For more information about policy-based routing, see *Layer 3—IP Routing Configuration Guide*. Use the **logging** keyword together with the rule match counting function. To enable this function, you can either execute the **hardware-count enable** command in the ACL or specify the **counting** keyword in the ACL rule with **logging** specified.

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.

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

Description

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

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

By default, an IPv4 basic ACL does not contain any rule.

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 will fail.

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

Related commands: **acl**, **display acl**, **step**, and **time-range**.

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
```

rule (IPv6 advanced ACL view)

Syntax

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

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

View

IPv6 advanced ACL view

Default level

2: System level

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

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

Table 12 Match criteria and other rule information for 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 ACL rule has been matched, and disabled by default	This keyword is valid when the rule is applied to the packet filtering firewall.

Parameters	Function	Description
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.
logging	Logs matching packets	This function requires that the module using the ACL supports logging. If an ACL has been applied to both the packet filtering firewall and policy-based routing modules, do not add or modify a rule that has the **logging** keyword in the ACL. Doing so can cause rule application failure on both modules. For more information about packet filtering firewall, see *Security Configuration Guide*. For more information about policy-based routing, see *Layer 3—IP Routing Configuration Guide*. Use the **logging** keyword together with the rule match counting function. To enable this function, you can either execute the **hardware-count enable** command in the ACL or specify the **counting** keyword in the ACL rule with **logging** specified.
routing [**type** *routing-type*]	Specifies the type of routing header	The *routing-type* argument takes a value in the range of 0 to 255. If no routing type header is specified, the rule applies to the IPv6 packets that have any type of routing header. The parameter is not supported in the current software version. The parameter is reserved for future support.
fragment	Applies the rule to only fragments	Without this keyword, the rule applies to all fragments and non-fragments.
time-range *time-range-name*	Specifies a time range for the rule	The *time-range-name* argument takes a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the timer range.
vpn-instance *vpn-instance-name*	Applies the rule to packets in a VPN instance	The *vpn-instance-name* argument takes a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the rule applies to non-VPN packets.

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

Table 13 TCP/UDP-specific parameters for 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**. TCP port numbers can be represented in these words: **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 in these words: **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 relationship between the TCP flags in a rule is AND.
established	Specifies the flags for indicating the established status of a TCP connection	Parameter specific to TCP. A rule with this keyword matches TCP connection packets with the ACK or RST flag bit set.

If the *protocol* argument takes **icmpv6** (58), you can 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

Description

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

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

By default, an IPv6 advanced ACL does not contain any rule.

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 will fail.

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

Related commands: **acl ipv6**, **display ipv6 acl**, **step**, and **time-range**.

Examples

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

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

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

```
<Sysname> system-view
[Sysname] acl ipv6 number 3001
[Sysname-acl6-adv-3001] rule 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
```

rule (IPv6 basic ACL view)

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**] *

View

IPv6 basic ACL view

Default level

2: System level

Parameters

rule-id: Specifies a rule ID, in the range of 0 to 65534. If no rule ID is provided when you create an ACL rule, the system automatically assigns it a rule ID. This rule ID takes the nearest higher multiple of the

numbering step to the current highest rule ID, starting from 0. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the rule is numbered 30.

deny: Denies matching packets.

permit: Allows matching packets to pass.

counting: Counts the number of times the IPv6 ACL rule has been matched. This feature is disabled by default. This keyword is valid when the rule is applied to the packet filtering firewall. For information about packet filtering firewall, see *Security Configuration Guide*.

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

logging: Logs matching packets. This function requires that the module (for example, a firewall) using the ACL supports logging.If an ACL has been applied to both the packet filtering firewall and policy-based routing modules, do not add or modify a rule that has the **logging** keyword in the ACL. Doing so can cause rule application failure on both modules. For more information about packet filtering firewall, see *Security Configuration Guide*. For more information about policy-based routing, see *Layer 3—IP Routing Configuration Guide*. Use the **logging** keyword together with the rule match counting function. To enable this function, you can either execute the **hardware-count enable** command in the ACL or specify the **counting** keyword in the ACL rule with **logging** specified.

routing [**type** *routing-type*]: Matches a specific type of routing header or any type of routing header. The *routing-type* argument takes a value in the range of 0 to 255. If no routing header type is specified, the rule matches any type of routing header. The parameter is not supported in the current software version. The parameter is reserved for future support.

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

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

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

Description

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

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

By default, an IPv6 basic ACL does not contain any rule.

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 will fail.

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

Related commands: **acl ipv6**, **display ipv6 acl**, **step**, and **time-range**.

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
```

rule (user-defined ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [{ { **ipv4** | **ipv6** | **l2** | **l4** } *rule-string rule-mask offset* }&<1-8>] [**counting** | **time-range** *time-range-name*] *

undo rule *rule-id*

View

User-defined ACL view

Default level

2: System level

Parameters

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

deny: Denies matching packets.

permit: Allows matching packets to pass.

ipv4: Specifies that the offset starts 20 bytes after the beginning of the IPv4 header.

ipv6: Specifies that the offset starts 40 bytes after the beginning of the IPv6 header.

l2: Specifies that the offset starts two bytes before the Layer 3 header.

l4: Specifies that the offset starts 20 bytes after the Layer 4 header.

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

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

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

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

counting: Counts the number of times the IPv4 ACL rule has been matched. This feature is disabled by default.

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument takes a case-insensitive string of 1 to 32 characters. It must start with an English letter. If the time range is not

configured, the system creates the rule. However, the rule using the time range can take effect only after you configure the timer range.

Description

Use **rule** to create a user-defined ACL rule. You cannot edit a user-defined ACL rule. If you number the ACL rule the same as an existing rule in the ACL, the new rule contents are added to the existing rule.

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

By default, a user-defined ACL does not contain any rule.

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 will fail.

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

Related commands: **acl**, **display acl**, **step**, and **time-range**.

Examples

Create a rule for user-defined ACL 5005 to permit ARP packets.

```
<Sysname> system-view
[Sysname] acl number 5005
[Sysname-acl-user-5005] rule permit l2 0806 ffff 0
```

rule comment

Syntax

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

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

View

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

Default level

2: System level

Parameters

rule-id: Specifies the ID of an existing ACL rule. The ID is in the range of 0 to 65534.

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

Description

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

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

By default, an IPv4 ACL rule has no rule comment.

Related commands: **display acl** and **display acl ipv6**.

Examples

Create a rule in IPv4 basic ACL 2000 and configure a description for this rule.

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

```
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used on GE3/1/2.
```

Create a rule in IPv6 basic ACL 3000 and configure a description for this rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 0 permit tcp source 2030:5060::9050/64
[Sysname-acl6-adv-3000] rule 0 comment This rule is used in GE3/1/1
```

rule remark

Syntax

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

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

View

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

Default level

2: System level

Parameters

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

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

Description

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

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

By default, no rule range remarks are configured.

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

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

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

When you delete rule range remarks, follow these guidelines:

- If neither *rule-id* nor *text* is specified, all rule range remarks are removed.
- Use the **undo rule remark** *text* command to remove all remarks that are the same as the *text* argument.

- Use the **undo rule** *rule-id* **remark** command to delete a specific rule range remark. If you also specify the *text* argument, you must type in the remark the same as was specified to successfully remove the remark.

TIP:

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

Related commands: **display this** and **display current-configuration** (*Fundamentals Command Reference*).

Examples

Display the running configuration of IPv4 basic ACL 2000.

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

Add a start comment “Rules for VIP_start” and an end comment “Rules for VIP_end” for the rule range 10 to 25.

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

Verify the configuration.

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

step

Syntax

step *step-value*

undo step

View

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

Default level

2: System level

Parameters

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

Description

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

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

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

Related commands: **display acl** and **display acl ipv6**.

Examples

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

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

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

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

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*]

View

System view

Default level

2: System level

Parameters

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

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

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

- A digit in the range of 0 to 6, respectively for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- A day of a week in 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 1 to 12, DD is the day of the month with the range depending on MM, and YYYY is the year in the calendar in the range of 1970 to 2100. If not specified, the start time is 01/01/1970 00:00 AM, the earliest time available in the system.

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

Description

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

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

By default, no time range exists.

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

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

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

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

Related commands: **display time-range**.

Examples

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

```
<Sysname> system-view
[Sysname] time-range t1 8:0 to 18:0 working-day
```

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

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

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

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

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

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

QoS policy configuration commands

In this chapter, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L. SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.

Class configuration commands

display traffic classifier

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

user-defined: Displays user-defined classes.

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

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

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

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

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

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

Description

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

If no class name is specified, information about all user-defined classes is displayed.

Examples

Display information about all user-defined classes.

```
<Sysname> display traffic classifier user-defined
User Defined Classifier Information:
 Classifier: USER1
  Operator: AND
  Rule(s) : If-match ip-precedence 5

 Classifier: database
  Operator: AND
```

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

Table 16 Command output

Field	Description
User Defined Classifier Information	User-defined class information.
Classifier	Class name and its match criteria.
Operator	Logical relationship between match criteria.
Rule(s)	Match criteria.

if-match

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

View

Class view

Default level

2: System level

Parameters

match-criteria: Match criterion. Table 17 shows the available criteria.

Table 17 Available settings for the match-criteria argument

Value	Description
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	Matches an ACL. The *acl-number* argument ranges from 2000 to 4999 for an IPv4 ACL, and 2000 to 3999 for an IPv6 ACL. The *acl-name* argument is a case-insensitive string of 1 to 32 characters, which must start with an English letter from a to z or A to Z and cannot be **all** to avoid confusion. On an SPC card, you can use a user-defined ACL in a QoS policy to identify only inbound traffic. On an SPE card, you cannot use a user-defined ACL in a QoS policy to identify traffic.
customer-dot1p *8021p-list*	Matches the 802.1p priority of the customer network. The *8021p-list* argument is a list of up to eight 802.1p priority values. An 802.1p priority is in the range 0 to 7.
customer-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	Matches the VLAN IDs of customer networks. The *vlan-id-list* argument is a list of up to eight VLAN IDs. The *vlan-id1* **to** *vlan-id2* specifies a VLAN ID range, where the *vlan-id1* must be smaller than the *vlan-id2*. A VLAN ID ranges from 1 to 4093.

Value	Description
destination-mac *mac-address*	Matches a destination MAC address.
dscp *dscp-list*	Matches DSCP values. The *dscp-list* argument is a list of up to eight DSCP values. A DSCP value is in the range 0 to 63.
forwarding-layer { **bridge** | **route** }	Matches Layer 2 forwarded packets or Layer 3 forwarded packets. Specify the **bridge** keyword to match Layer 2 forwarded packets or the **route** keyword to match Layer 3 forwarded packets. This option is available on only SPC cards.
ip-precedence *ip-precedence-list*	Matches IP precedence. The *ip-precedence-list* argument is a list of up to eight IP precedence values. An IP precedence ranges from 0 to 7.
mpls-exp *exp-list*	Matches MPLS EXP values. The *exp-list* argument is a list of up to eight EXP values. An EXP value ranges from 0 to 7.
mpls-label { *label-value-list* | *label-value1* **to** *label-value2* }	Matches MPLS labels. The *label-value-list* argument specifies a list of up to eight MPLS label values. *label-value1* **to** *label-value2* specifies an MPLS label value range, where *label-value1* must be smaller than *label-value2*. An MPLS label value ranges from 1 to 1048575.
protocol *protocol-name*	Matches the specified protocol. The *protocol-name* argument can be IP or IPv6.
second-mpls-exp *exp-list*	Matches inner MPLS EXP values. The *exp-list* argument is a list of up to eight EXP values. An EXP value ranges from 0 to 7.
second-mpls-label { *label-value-list* | *label-value1* **to** *label-value2* }	Matches inner MPLS labels. The *label-value-list* argument specifies a list of up to eight MPLS label values. *label-value1* **to** *label-value2* specifies an MPLS label range, where *label-value1* must be smaller than *label-value2*. An MPLS label ranges from 1 to 1048575.
service-dot1p *8021p-list*	Matches the 802.1p priority of the service provider network. The *8021p-list* argument is a list of up to eight 802.1p priority values. An 802.1p priority is in the range 0 to 7.
service-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	Matches the VLAN IDs of SP networks. The *vlan-id-list* argument is a list of up to eight VLAN IDs. The *vlan-id1* **to** *vlan-id2* specifies a VLAN ID range, where the *vlan-id1* must be smaller than the *vlan-id2*. A VLAN ID ranges from 1 to 4093.
source-mac *mac-address*	Matches a source MAC address.

Description

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

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

When defining match criteria, follow the guidelines described in the subsections:

1. Defining an ACL-based match criterion
   - If the ACL referenced in the **if-match** command does not exist, the class cannot be applied to hardware.
   - For a class with the operator as OR, you can reference an ACL twice, respectively by its name and number. For a class with the operator as AND, you can reference an ACL only once by its name or number.
2. Defining a criterion to match a destination MAC address
   - If this command is executed multiple times for a class, the new configuration does not overwrite the previous one.
   - A criterion to match a destination MAC address is significant only to Ethernet interfaces.
3. Defining a criterion to match a source MAC address
   - If this command is executed multiple times for a class, the new configuration does not overwrite the previous one.
   - A criterion to match a source MAC address is significant only to Ethernet interfaces.
4. Defining a criterion to match DSCP precedence values
   - If this command is executed multiple times for a class, the new configuration does not overwrite the previous one. After such a command is configured, all the DSCP values are arranged in ascending order automatically.
   - You can configure up to eight DSCP values in one command line. If multiple identical DSCP values are specified, the system considers them as one. The relationship between different DSCP values is **OR**. If a packet matches one of the defined DSCP values, it is considered as matching the if-match clause.
   - To delete a rule matching DSCP values, the specified DSCP values must be identical with those defined in the rule (sequence may be different).
5. Defining a criterion to match Layer 2 or Layer 3 forwarded packets
   - The **if-match forwarding-layer bridge** and **if-match forwarding-layer route** commands are mutually exclusive in a class.
   - You must use a **forwarding-layer** match criterion together with other match criteria. The other match criteria in the class cannot conflict with the **forwarding-layer** match criterion, regardless of the operator of the class.
6. Defining a criterion to match 802.1p priority in customer VLAN tags
   - You can configure multiple 802.1p priority match criteria for a class. All the defined 802.1p values are automatically arranged in ascending order.
   - You can configure up to eight 802.1p priority values in one command line. If the same 802.1p priority value is specified multiple times, the system considers them as one. If a packet matches one of the defined 802.1p priority values, it matches the **if-match** clause.
   - To delete a criterion that matches 802.1p priority values, the specified 802.1p priority values in the command must be identical with those defined in the criterion (the sequence may be different).
7. Defining a criterion to match IP precedence values

- If this command is executed multiple times in a class, the new configuration does not overwrite the previous one. When such a command is configured, the IP precedence values are arranged automatically in ascending order.
- You can configure up to eight IP precedence values in one command line. If the same IP precedence is specified multiple times, the system considers them as one. The relationship between different IP precedence values is **OR**. If a packet matches one of the defined IP precedence values, it is considered as matching the if-match clause.
- To delete a criterion matching IP precedence values, the specified IP precedence values in the command must be identical with those defined in the criterion (sequence may be different).

8. Defining a criterion to match customer network VLAN IDs or service provider network VLAN IDs
   - If this command is executed multiple times in a class, the new configuration does not overwrite the previous one. After such a command is configured, all the VLAN IDs are arranged in ascending order automatically.
   - You can configure multiple VLAN IDs in one command line. If the same VLAN ID is specified multiple times, the system considers them as one. The relationship between different VLAN IDs is logical **OR**. If a packet matches one of the defined VLAN IDs, it is considered as matching the if-match clause.
   - To delete a criterion matching VLAN IDs, the specified VLAN IDs in the command must be identical with those defined in the criterion (sequence may be different).
9. Defining a criterion to match MPLS EXP values
   - You can configure multiple MPLS EXP match criteria for a class. The defined MPLS EXP values are automatically arranged in ascending order.
   - You can configure up to eight MPLS EXP values in one command line. If the same MPLS EXP value is specified multiple times, the system considers them as one. If a packet matches one of the defined MPLS EXP values, it matches the **if-match** clause.
   - To delete a criterion that matches MPLS EXP values, the specified MPLS EXP values in the command must be identical with those defined in the criterion (the sequence may be different).
   - The MPLS EXP field exists only in MPLS packets, so this match criterion takes effect for only the MPLS packets.
10. Defining a criterion to match MPLS labels
    - You can configure multiple MPLS label match criteria for a class. The defined MPLS labels are automatically arranged in ascending order.
    - You may configure multiple MPLS label values in one command. If the same MPLS label value is specified multiple times, the system considers them as one. If a packet matches one of the defined MPLS label values, it matches the **if-match** clause.
    - To delete a criterion that matches MPLS label values, the specified MPLS label values in the command must be identical with those defined in the criterion (the sequence may be different).

Related commands: **traffic classifier**.

Examples

Define a match criterion for class **class1** to match the packets with the destination MAC address 0050-BA27-BED3.

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

Define match criteria for class **class2** to match the packets that have the source MAC address 0050-ba27-bed2.

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

Define a match criterion for class **class1** to match the packets with a DSCP precedence of 1, 6 or 9.

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

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

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

traffic classifier

Syntax

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

undo traffic classifier *classifier-name*

View

System view

Default level

2: System level

Parameters

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

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

and: Specifies the relationship between the match criteria in the class as logic AND, which means that the packets that match all the criteria belong to this class.

or: Specifies the relationship between the criteria in the class as logic OR, which means that the packets that match any of the criteria belong to this class.

Description

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

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

By default, the relationship between match criteria in a class is **and**, and the relationship between match criteria is logical AND.

Related commands: **qos policy**, **qos apply policy**, and **classifier behavior**.

Examples

Define class **class1**.

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

```
[Sysname-classifier-class1]
```

Traffic behavior configuration commands

accounting

Syntax

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

undo accounting

View

Traffic behavior view

Default level

2: System level

Parameters

byte: Counts traffic in bytes.

packets: Counts traffic in packets. With this keyword specified, the CAR also counts traffic in packets.

Description

Use **accounting** to enable traffic accounting for the traffic behavior.

Use **undo accounting** to disable traffic accounting.

If you specify neither **byte** nor **packets**, traffic is counted in bytes.

View the related statistics with the **display qos policy interface** command. the **display qos vlan-policy** command, or the **display qos policy global** command.

1. On an SPE-1010, SPE-1020, SPE-1010-E, or SPE-1020-E card:

   For packets forwarded at Layer 3, such as IPv4/IPv6 unicast packets, multicast packets, tunnel packets, and L3VPN incoming tunnel packets, the **accounting** command only takes the IP header and payload into account. Take 128-byte Layer-3 packets for example. The traffic size is calculated following these formulae:

   - When the incoming port and the outgoing port are Ethernet interfaces and the packets are untagged:

     Traffic size = Number of packets × (128 bytes of packet length – 4 bytes of CRC – 14 bytes of Layer-2 header)

   - When the incoming port and the outgoing port are POS interfaces:

     Traffic size = Number of packets × (128 bytes of packet length– 4 bytes of CRC – 4 bytes of Layer-2 header)

2. On an SPC, SPE-1010-II, SPE-1020-II, SPE-1010-E-II, or SPE-1020-E-II card:

   The **accounting** command takes the total packet length into account.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

Enable traffic accounting for traffic behavior **database**.

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

```
[Sysname] traffic behavior database
[Sysname-behavior-database] accounting
```

car

Syntax

car cir *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peak-information-rate*] [**red** { **discard** | **pass** }]

undo car

View

Traffic behavior view

Default level

2: System level

Parameters

cir *committed-information-rate*: Committed information rate (CIR) in kbps, in the range of 64 to 10000000.

cbs *committed-burst-size*: Committed burst size (CBS) in bytes, in the range of 1875 to 1000000000. By default, CBS is the traffic size that can be transmitted at the rate of CIR over 500 ms.

ebs *excess-burst-size*: Excess burst size (EBS) in bytes, in the range of 0 to 1000000000. The default is 0.

pir *peak-information-rate*: Peak information rate (PIR) in kbps, in the range of 64 to 10000000.

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

- **discard**: Drops the packets.
- **pass**: Permits the packets to pass through.

Description

Use **car** to configure a CAR action for the traffic behavior.

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

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

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

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

1. On an SPE-1010, SPE-1020, SPE-1010-E, or SPE-1020-E card:

   For packets forwarded at Layer 3, such as IPv4/IPv6 unicast packets, multicast packets, tunnel packets, and L3VPN incoming tunnel packets, CAR only takes the IP header and payload into account. The port rate parameters configured in the **car** command are transformed into the theoretical output rate following these formulae (take 128-byte Layer-3 packets for example, and assume that the rate is set to 10000 kbps):

   - When the incoming port and the outgoing port are Ethernet interfaces and the packets are untagged, the theoretical outgoing interface rate is calculated following this formula:

10000 kbps × 128 bytes/(128 bytes of packet length – 4 bytes of CRC – 14 bytes of Layer-2 header)

- When the incoming port and the outgoing port are POS interfaces, the theoretical outgoing interface rate is calculated following this formula:

  10000 kbps × 128 bytes/(128 bytes of packet length – 4 bytes of CRC – 4 bytes of Layer-2 header)

2. On an SPC, SPE-1010-II, SPE-1020-II, SPE-1010-E-II, or SPE-1020-E-II card:

   The configured rate is the same as the theoretical output rate.

Examples

Configure a CAR action for traffic behavior **database**, setting CIR to 200 kbps and CBS to 50000 bytes, and dropping the packets not conforming to CIR.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 50000 red discard
```

display traffic behavior

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

user-defined: Displays user-defined traffic behaviors.

behavior-name: Behavior name, a string of 1 to 31 characters. If no traffic behavior is specified, the information of all the user-defined behaviors is displayed.

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

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

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

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

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

Description

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

Examples

Display user-defined traffic behaviors.

```
<Sysname> display traffic behavior user-defined
  User Defined Behavior Information:
    Behavior: ben
```

```
    Mirror enable:
      Mirror type: vlan
      Mirror destination: 23
  Behavior: 23
    Mirror enable:
      Mirror type: vlan
      Mirror destination: 25
```

Table 18 Command output

Field	Description
Mirror enable	Information about traffic mirroring.
Mirror type	Traffic mirroring type: • VLAN. • CPU. • Interface.
Mirror destination	Traffic mirroring destination: • VLAN ID. • Interface name.

filter

Syntax

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

undo filter

View

Traffic behavior view

Default level

2: System level

Parameters

deny: Drops packets.

permit: Permits packets to pass through.

Description

Use **filter** to configure a traffic filtering action for the traffic behavior.

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

Examples

Configure the traffic filtering action as deny for traffic behavior **database**.

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

primap color-map-dp

Syntax

primap color-map-dp

undo primap color-map-dp

View

Traffic behavior view

Default level

2: System level

Description

Use **primap color-map-dp** to configure the action of mapping the packet color to the drop precedence value in the traffic behavior.

Use **undo primap color-map-dp** to delete the action.

These two commands must be used in conjunction with the **car** command.

The packet color-to-drop precedence mappings are fixed as follows:

- red to drop precedence 2
- yellow to drop precedence 1
- green to drop precedence 0

Examples

Configure the action of mapping packet color to drop precedence in traffic behavior **behavior 1**.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] car cir 1600
[Sysname-behavior-behavior1] primap color-map-dp
```

primap pre-defined

Syntax

primap pre-defined dscp-dscp

undo primap pre-defined dscp-dscp

View

Traffic behavior view

Default level

2: System level

Parameters

pre-defined: Pre-defined priority mapping table.

dscp-dscp: DSCP-to-DSCP priority mapping table.

Description

Use **primap** to configure the action of mapping source precedence to target precedence through the specified priority mapping table for the traffic behavior.

Use **undo primap pre-defined** to remove the action.

Related commands: **display qos map-table**.

Examples

Specify a DSCP-to-DSCP priority mapping table for traffic behavior **behavior1**.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] primap pre-defined dscp-dscp
```

primap pre-defined color

Syntax

primap pre-defined color { **up-dot1p** | **up-dscp** | **up-exp** | **up-lp** }

undo primap pre-defined color { **up-dot1p** | **up-dscp** | **up-exp** | **up-lp** }

View

Traffic behavior view

Default level

2: System level

Parameters

pre-defined: Specifies the predefined priority mapping table.

color: Uses colored priority mapping tables for priority mapping.

up-dot1p: Specifies the user priority-to-802.1p mapping table.

up-dscp: Specifies the user priority-to-DSCP mapping table.

up-exp: Specifies the user priority-to-EXP mapping table.

up-lp: Specifies the user priority-to-local mapping table.

Description

Use **primap pre-defined color** to configure the action of mapping source precedence to target precedence through the specified colored priority mapping table for a traffic behavior.

Use **undo primap pre-defined color** to delete the action.

You must use the **primap pre-defined color** command together with the **car** command.

Related commands: **display qos map-table color**.

Examples

Configure the action of mapping user priority values to local precedence through the colored user priority-to-local mapping table in traffic behavior **behavior1**.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] car cir 1600
[Sysname-behavior-behavior1] primap pre-defined color up-lp
```

redirect

Syntax

redirect { **cpu** | **interface** *interface-type interface-number* | **next-hop** { *ipv4-add1* [**track** *track-entry-number*] [*ipv4-add2* [**track** *track-entry-number*]] | *ipv6-add1* [*interface-type interface-number*] [**track** *track-entry-number*] [*ipv6-add2* [*interface-type interface-number*] [**track** *track-entry-number*]] } [**fail-action** { **discard** | **forward** }] | **vpn-instance** *vpn-instance-name* }

undo redirect { **cpu** | **interface** *interface-type interface-number* | **next-hop** | **vpn-instance** }

View

Traffic behavior view

Default level

2: System level

Parameters

cpu: Redirects traffic to the CPU.

interface: Redirects traffic to an interface, which must be a NAT service interface.

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

next-hop: Redirects traffic to a next hop. The next hop must be a directly-connected address.

ipv4-add1/*ipv4-add2*: IPv4 address of the next hop. The *ipv4-add2* argument backs up *ipv4-add1*. If redirecting traffic to *ipv4-add1* fails, traffic will be redirected to *ipv4-add2*.

ipv6-add1/*ipv6-add2*: IPv6 address of the next hop. The *ipv6-add2* argument backs up *ipv6-add1*. If redirecting traffic to *ipv6-add1* fails, traffic will be redirected to *ipv6-add2*. Traffic cannot be redirected to a link-local address. If the IPv6 address is not a link-local address, you do not need to specify an interface for the IPv6 address of the next hop.

track *track-entry-number*: Specifies the track entry associated with the next hop. For different IP addresses, specify different track entries. The *track-entry-number* argument ranges from 1 to 1024. By specifying track entries, you can enable the traffic redirecting action to collaborate with the tracking modules, such as NQA and BFD. For more information about tracking modules, see *High Availability Configuration Guide*.

fail-action { **discard** | **forward** }: Specifies the action to take when the next hop address for a packet does not exist.

- **discard**: Drops the packet.
- **forward**: Forwards the packet. This action applies if no fail-action is specified.

vpn-instance *vpn-instance-name*: Redirects traffic to the VPN instance specified by the *vpn-instance-name* argument. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.

Description

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

Use **undo redirect** to remove the traffic redirect action.

The actions of redirecting traffic to CPU, redirecting traffic to an interface, redirecting traffic to the next hop, and redirecting traffic to a VPN instance are mutually exclusive with each other in the same traffic behavior.

CAUTION:

Do not bind the outgoing interface for the redirected traffic to a NAT service interface.

Examples

Configure the action of redirecting traffic to the CPU for traffic behavior **database**.

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

redirect-default

Syntax

redirect-default next-hop *ipv4-add1* [**track** *track-entry-number*] [*ipv4-add2* [**track** *track-entry-number*]]

undo redirect-default next-hop

View

Traffic behavior view

Default level

2: System level

Parameters

next-hop: Redirects traffic to a next hop.

ipv4-add1/*ipv4-add2*: IPv4 address of the next hop. The *ipv4-add2* argument specifies the backup of *ipv4-add1*. If redirect to *ipv4-add1* fails, traffic will be redirected to *ipv4-add2*.

track *track-entry-number*: Specifies the track entry associated with the next hop. For different IP addresses, specify different track entries. The *track-entry-number* argument ranges from 1 to 1024. By specifying track entries, you can enable the traffic redirecting action to collaborate with the tracking modules, such as NQA and BFD. For detailed information about tracking modules, see *High Availability Configuration Guide*.

Description

Use **redirect-default** to configure the default traffic redirecting action.

Use **undo redirect-default** to remove the default traffic redirecting action.

Examples

Configure the default traffic redirecting action as redirecting traffic to next hop 1.1.1.1.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect-default next-hop 1.1.1.1
```

remark dot1p

Syntax

remark dot1p *8021p*

undo remark dot1p

View

Traffic behavior view

Default level

2: System level

Parameters

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

Description

Use **remark dot1p** to configure the action of setting the specified 802.1p priority for packets.

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

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

Set the 802.1p priority to 2.

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

remark drop-precedence

Syntax

remark drop-precedence *drop-precedence-value*

undo remark drop-precedence

View

Traffic behavior view

Default level

2: System level

Parameters

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

Description

Use **remark drop-precedence** to configure the action of setting the specified drop precedence for packets.

Use **undo remark drop-precedence** to remove the action.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

Set the drop precedence to 2 for packets.

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

remark dscp

Syntax

remark dscp *dscp-value*

undo remark dscp

View

Traffic behavior view

Default level

2: System level

Parameters

dscp-value: DSCP value, in the range of 0 to 63 or a keyword, as shown in Table 19.

Table 19 DSCP keywords and values

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

Description

Use **remark dscp** to configure the action of setting the specified DSCP value for packets.

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

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

Set the DSCP value of packets to 6.

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

remark ip-precedence

Syntax

remark ip-precedence *ip-precedence-value*

undo remark ip-precedence

View

Traffic behavior view

Default level

2: System level

Parameters

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

Description

Use **remark ip-precedence** to configure the action of setting the specified IP precedence for packets.

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

With this command configured, the low-order three bits of the DSCP field of an IP packet will be set to 0.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

Set the IP precedence of packets to 6.

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

remark local-precedence

Syntax

remark local-precedence *local-precedence*

undo remark local-precedence

View

Traffic behavior view

Default level

2: System level

Parameters

local-precedence: Local precedence value to be marked for packets, which can be a number or keyword. The number-keyword mapping is shown in Table 20.

Table 20 Description on the local-precedence argument

Keyword	Local precedence value (decimal)
af1	1
af2	2
af3	3
af4	4
be	0
cs6	6
cs7	7
ef	5

Description

Use **remark local-precedence** to configure the action of setting the specified local precedence for packets.

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

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

Set the local precedence of packets to 2.

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

remark mpls-exp

Syntax

remark mpls-exp *exp-value*

undo remark mpls-exp

View

Traffic behavior view

Default level

2: System level

Parameters

exp-value: EXP value to be marked for MPLS packets, in the range of 0 to 7.

Description

Use **remark mpls-exp** to configure the action of setting the specified EXP value for MPLS packets.

Use **undo remark mpls-exp** to remove the action.

Related commands: **qos policy**, **traffic behavior**, and **classifier behavior**.

Examples

Set the EXP value of MPLS packets to 2.

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

traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

View

System view

Default level

2: System level

Parameters

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

Description

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

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

Related commands: **qos policy**, **qos apply policy**, and **classifier behavior**.

Examples

Create traffic behavior **behavior1**.

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

QoS policy configuration and application commands

classifier behavior

Syntax

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

undo classifier *classifier-name*

View

Policy view

Default level

2: System level

Parameters

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

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

Description

Use **classifier behavior** to specify a behavior for a class in the policy.

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

Each class in the policy can be associated with only one behavior.

If the class and traffic behavior specified for the command do not exist, the system creates a null class and a null traffic behavior.

Related commands: **qos policy**.

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
```

display qos policy

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

user-defined: Displays user-defined QoS policies.

policy-name: Displays information about the QoS policy. If no policy is specified, the configuration information of all the policies is displayed. The *policy-name* argument is a string of 1 to 31 characters.

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

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

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

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

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

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

Description

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

Examples

Display the configuration information of user-defined QoS policies.

```
<Sysname> display qos policy user-defined
  User Defined QoS Policy Information:

  Policy: user1
   Classifier: class1
     Behavior: test
      Accounting Enable
      Committed Access Rate:
        CIR 20000 (kbps), CBS 300000 (byte), EBS 100 (byte), PIR 25000 (kbps)
        Red Action: discard
      Filter enable : permit
      Marking:
        Remark dot1p COS 2
```

Table 21 Command output

Field	Description
Policy	Policy name.
Classifier	Class name. A policy can contain multiple classes, and each class is associated with a traffic behavior. A class can be configured with multiple match criteria. For more information, see the **traffic classifier** command.
Behavior	A behavior is associated with a class. It can be configured with multiple actions. For more information, see the **traffic behavior** command.
Accounting	Traffic accounting is configured in the traffic behavior.
Committed Access Rate	Information about rate limiting.
Red Action	Action to take on packets not conforming to CIR.
Filter enable	Traffic filtering is configured in the traffic behavior.
Marking	Information about priority marking.

display qos policy global

Syntax

display qos policy global [**slot** *slot-number*] [**inbound** | **outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

inbound: Displays information about the inbound global QoS policy. An inbound global QoS policy applies to the inbound direction of all ports.

outbound: Displays information about the outbound global QoS policy. An outbound global QoS policy applies to the outbound direction of all ports.

slot *slot-number*: Displays information about the global QoS policies on the card specified by the slot number.

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

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

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

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

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

Usage guidelines

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

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

If no slot number is specified, this command displays the global QoS policy or policies on the main processing unit.

The command is available on only SPC cards.

Examples

Display information about the inbound global QoS policy.

```
<Sysname> display qos policy global inbound

  Direction: Inbound

  Policy: 1
   Classifier: 2
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 2
       Accounting Enable
         20864 (Bytes)
       Committed Access Rate:
         CIR 128 (kbps), CBS 8000 (byte), EBS 0 (byte)
         Red Action: discard
         Green : 12928(Bytes)
         Yellow: 7936(Bytes)
         Red   : 43904(Bytes)
```

Table 22 Command output

Field	Description
Direction	Indicates that the QoS policy is applied in the inbound direction or outbound direction.
Policy	Policy name and its contents.
Classifier	Class name and its contents.
Mode	Mode that the association between the class and the traffic behavior supports.
Operator	Logical relationship between match criteria.
Rule(s)	Match criteria.
Behavior	Name of the traffic behavior, and the actions in the traffic behavior.
Accounting	Class-based accounting action and the collected statistics.
Committed Access Rate	Information about traffic rate limiting.
CIR	CIR in kbps.
CBS	Committed burst size in bytes, which specifies the depth of the token bucket for holding bursty traffic.
EBS	Excessive burst size (EBS) in bytes, which specifies the traffic exceeding CBS when two token buckets are used.
Red Action	Action to take on red packets.
Green	Statistics about green packets.
Yellow	Statistics about yellow packets.
Red	Statistics about red packets.

display qos policy interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

inbound: Displays the QoS policy configuration in the inbound direction.

outbound: Displays the QoS policy configuration in the outbound direction.

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

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

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

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

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

Description

Use **display qos policy interface** to display the QoS policy configuration and operational information of the specified interface or all interfaces.

Examples

Display the QoS policy configuration and operational information on GigabitEthernet 2/1/1.

```
<Sysname> display qos policy interface GigabitEthernet 2/1/1
Interface: GigabitEthernet2/1/1

  Direction: Outbound

  Policy: user1
   Classifier: class1
     Operator: AND
     Rule(s) : If-match acl 2001
               If-match ip-precedence 1
     Behavior: test
      Mirror enable:
        Mirror type: cpu
      Assured Forwarding:
        Bandwidth 3000 (Kbps)
        Matched  : 3905267/429580690 (Packets/Bytes)
        Enqueued : 13384/1471580 (Packets/Bytes)
        Discarded: 3891883/428109110 (Packets/Bytes)
      Filter Enable: permit
      Marking:
        Remark DSCP cs5
```

Table 23 Command output

Field	Description
Interface	Interface type and interface number.
Direction	The direction in which the policy is applied to the interface.
Policy	Name of the policy applied to the interface.
Classifier	Class name and configuration information.
Operator	Logical relationship between match criteria in the class.
Rule(s)	Match criteria in the class.
Behavior	Behavior name and configuration information.
Mirror enable	Information about traffic mirroring.

Field	Description
Mirror type	Traffic mirroring type: • **VLAN**—Mirrors traffic to a VLAN. • **CPU**—Mirrors traffic to a CPU. • **Interface**—Mirrors traffic to an interface.
Assured Forwarding	Information about AF queues.
Bandwidth	Bandwidth of the queue.
Matched	Number of packets matching the match criteria.
Enqueued	Number of packets and bytes enqueued.
Discarded	Number of packets and bytes dequeued.
Filter enable	Traffic filtering information: • **permit**—Forwards packets. • **deny**—Drops packets.
Marking	Information about priority marking.
Remark	Type of priority to be marked: • DSCP. • IP precedence. • MPLS EXP. For more information, see "Traffic behavior configuration commands."

display qos vlan-policy

Syntax

display qos vlan-policy { **name** *policy-name* | **vlan** [*vlan-id*] } [**slot** *slot-number*] [**inbound** | **outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

name *policy-name*: Displays the information of the VLAN QoS policy identified by its name. The *policy-name* argument is a string of 1 to 31 characters.

vlan *vlan-id*: Displays the QoS policy or policies applied to a VLAN identified by its VLAN ID, which ranges from 1 to 4093.

inbound: Displays the QoS policy applied to the inbound direction of the specified VLAN.

outbound: Displays the QoS policy applied to the outbound direction of the specified VLAN.

slot *slot-number*: Displays VLAN QoS policy information for the specified card. If no card is specified, the command displays VLAN QoS policy information for the main processing unit.

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

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

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

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

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

Description

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

If no direction is specified, this command displays VLAN QoS policy information for both inbound and outbound directions.

If no slot number is specified, this command displays all VLAN QoS policy information on the device.

Examples

Display information about the QoS policy **test** on the card in slot 6.

```
<Sysname> display qos vlan-policy name test slot 6
Policy user1
    Vlan 2: inbound
```

Table 24 Command output

Field	Description
Policy	Name of the QoS policy.
Vlan	ID of the VLAN where the VLAN policy is applied.
Inbound	The QoS policy is applied in the inbound direction of the VLAN.

Display the QoS policy applied to VLAN 2.

```
<Sysname> display qos vlan-policy vlan 2
Vlan 2
  Direction: Inbound
  Policy: user1
   Classifier: class1
     Operator: AND
     Rule(s) : If-match acl 2001
     Behavior: test
      Accounting Enable:
        0 (Packets)
        0 (Bytes)
      Committed Access Rate:
        CIR 2000 (kbps), CBS 30000 (byte), EBS 100 (byte), PIR 25000 (kbps)
        Red Action: discard
        Green : 0(Bytes)
        Yellow: 0(Bytes)
        Red   : 0(Bytes)
      Filter Enable: permit
      Marking:
        Remark dot1p COS 2
```

Table 25 Command output

Field	Description
Vlan	ID of the VLAN where the QoS policy is applied.
Direction	Direction of the VLAN in which the QoS policy is applied.
Classifier	Class name and its contents.
Operator	Logical relationship between match criteria.
Rule(s)	Match criteria.
Behavior	Name of the behavior, and its actions.
Accounting	Accounting is enabled.
Committed Access Rate	CAR information.
CIR	Committed information rate (CIR) in kbps.
CBS	Committed burst size (CBS) in bytes, which specifies the depth of the token bucket for holding burst traffic.
EBS	Excessive burst size (EBS) in bytes, which specifies the amount of traffic exceeding the CBS when two token buckets are adopted.
PIR	Peak information rate.
Red Action	Action on red packets.
Green	Statistics about green packets.
Yellow	Statistics about yellow packets.
Red	Statistics about red packets.

qos apply policy

Syntax

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

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

View

Interface view, port group view

Default level

2: System level

Parameters

inbound: Inbound direction.

outbound: Outbound direction.

policy *policy-name*: Specifies a policy by its name, which is a string of 1 to 31 characters.

Description

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

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

You can apply QoS policies to all physical interfaces but X.25-enabled or LAPB-enabled interfaces.

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

Examples

Apply policy **USER1** in the outbound direction of GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet2/1/1
[Sysname-GigabitEthernet2/1/1] qos apply policy USER1 outbound
```

qos apply policy global

Syntax

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

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

View

System view

Default level

2: System level

Parameters

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

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

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

Description

Use **qos apply policy global** to apply a QoS policy globally. A global QoS policy takes effect on all inbound or outbound traffic depending on the direction in which the policy is applied.

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

This command is available only on the SPC cards.

Examples

Apply the QoS policy **user1** in the inbound direction globally.

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

qos policy

Syntax

qos policy *policy-name*

undo qos policy *policy-name*

View

System view

Default level

2: System level

Parameters

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

Description

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

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

A policy applied to an interface cannot be deleted directly. You must cancel application of the policy on the interface before deleting the policy with the **undo qos policy** command.

The specified *policy-name* cannot be the name of the system-defined policy **default**.

Related commands: **classifier behavior** and **qos apply policy**.

Examples

Create a policy **user1**.

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

qos vlan-policy

Syntax

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

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

View

System view

Default level

2: System level

Parameters

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

vlan-id-list: A list of discrete VLAN IDs in the range 1 to 4093. You can input up to eight VLAN IDs in the list. Separate each VLAN ID with a space. You can also specify a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*, with *vlan-id2* be greater than *vlan-id1*. The value range for *vlan-id1* and *vlan-id2* are 1 to 4093.

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

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

Description

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

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

QoS policies applied to VLANs are called "VLAN QoS polices".

Examples

Apply the QoS policy **test** to the inbound direction of VLAN 200, VLAN 300, VLAN 400, VLAN 500, VLAN 600, VLAN 700, VLAN 800, and VLAN 900.

```
<Sysname> system-view
[Sysname] qos vlan-policy test vlan 200 300 400 500 600 700 800 900 inbound
```

reset qos policy global

Syntax

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

View

User view

Default level

1: Monitor level

Parameters

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

Usage guidelines

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

This command is available on only SPC cards.

Examples

Clear the statistics of the global QoS policy in the inbound direction.

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

reset qos vlan-policy

Syntax

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

View

User view

Default level

1: Monitor level

Parameters

vlan-id: VLAN ID, in the range of 1 to 4094.

inbound: Clears the statistics of the QoS policy applied in the inbound direction of the specified VLAN.

outbound: Clears the statistics of the QoS policy applied in the outbound direction of the specified VLAN.

Description

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

Examples

Clear the statistics of QoS policies applied to VLAN 2.

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

Priority mapping configuration commands

In this chapter, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L. SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.

Priority mapping table configuration commands

display qos map-table

Syntax

display qos map-table [**dscp-dscp** | **inbound** [**up-dp** | **up-lp** | **up-up**] | **outbound** [**up-dp** | **up-fc** | **up-lp** | **up-rpr**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

inbound: Specifies the priority mapping table for incoming packets.

outbound: Specifies the priority mapping table for outgoing packets.

dscp-dscp: DSCP-to-DSCP priority mapping table.

up-dp: User-to-drop priority mapping table.

up-up: User-to-user priority mapping table.

up-fc: User-to-forwarding-class priority mapping table.

up-lp: User-to-local priority mapping table.

up-rpr: User-to-RPR priority mapping table.

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

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

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

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

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

Description

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

If no priority mapping table is specified, the configuration information of all priority mapping tables is displayed.

Related commands: **qos map-table**.

Examples

Display the configuration of the user-to-local priority mapping table for incoming packets.

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

Table 26 Command output

Field	Description
MAP-TABLE NAME	Name of the priority mapping table.
TYPE	Type of the priority mapping table.
DIRECTION	Direction of the priority mapping table.
IMPORT	Import entries of the priority mapping table.
EXPORT	Export entries of the priority mapping table.

display qos map-table color

Syntax

display qos map-table color [**green** | **yellow** | **red**] [**up-dot1p** | **up-dscp** | **up-lp** | **up-exp**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

color: Specifies colored priority mapping tables.

green: Specifies green packets.

yellow: Specifies yellow packets.

red: Specifies red packets.

up-dot1p: Specifies the user priority-to-802.1p mapping table.

up-dscp: Specifies the user priority-to-DSCP mapping table.

up-exp: Specifies the user priority-to-EXP mapping table.

up-lp: Specifies the user priority-to-local mapping table.

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

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

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

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

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

Usage guidelines

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

If no priority table type is specified, this command displays the configuration of all the colored priority mapping tables.

If no color is specified, this command displays the configuration information of all the colored priority mapping tables.

Related commands: **qos map-table color**.

Examples

Display the configuration of the user-to-802.1p mapping table for green packets.

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

Table 27 Command output

Field	Description
MAP-TABLE NAME	Priority mapping table name.
TYPE	Priority mapping table type.
COLOR	Priority mapping table color.
IMPORT	Input values of the priority mapping table.
EXPORT	Output values of the priority mapping table.

import

Syntax

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

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

View

Priority mapping table view

Default level

2: System level

Parameters

import-value-list: List of input values.

export-value: Output value.

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

Description

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

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

Related commands: **display qos map-table**.

NOTE:

In a DSCP-to-DSCP priority mapping table, only entries with an odd number as the input can take effect. To configure a DSCP-to-DSCP mapping for an even source DSCP value, use the even source DSCP value plus one as the input value. For example, to create a mapping for source DSCP precedence 4, you need to use 5 as the input value for the mapping.

Examples

Configure the DSCP-to-DSCP priority mapping table to map DSCP values 5 to DSCP value 1.

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

qos map-table

Syntax

qos map-table { **dscp-dscp** | **inbound** { **up-dp** | **up-lp** | **up-up** } | **outbound** { **up-dp** | **up-fc** | **up-lp** | **up-rpr** } }

View

System view

Default level

2: System level

Parameters

inbound: Specifies the priority mapping table for incoming packets.

outbound: Specifies the priority mapping table for outgoing packets.

dscp-dscp: DSCP-to-DSCP priority mapping table.

up-dp: User-to-drop priority mapping table.

up-up: User-to-user priority mapping table.

up-fc: User-to-forwarding-class priority mapping table.

up-lp: User-to-local priority mapping table.

up-rpr: User-to-RPR priority mapping table.

Description

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

Related commands: **display qos map-table**.

Examples

Enter the DSCP-to-DSCP priority mapping table view.

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

qos map-table color

Syntax

qos map-table color { **green** | **red** | **yellow** } { **up-dot1p** | **up-dscp** | **up-lp** | **up-exp** }

View

System view

Default level

2: System level

Parameters

color: Specifies colored priority mapping tables.

green: Specifies green packets.

yellow: Specifies yellow packets.

red: Specifies red packets.

up-dot1p: Specifies the user priority-to-802.1p mapping table.

up-dscp: Specifies the user priority-to-DSCP mapping table.

up-exp: Specifies the user priority-to-EXP mapping table.

up-lp: Specifies the user priority-to-local mapping table.

Usage guidelines

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

Related commands: **display qos map-table color**.

Examples

Enter the green user-to-802.1p mapping table view.

```
<Sysname> system-view
[Sysname] qos map-table color green up-dot1p
[Sysname-maptbl-green-up-dot1p]
```

Port priority configuration commands

qos priority

Syntax

qos priority *priority-value*

undo qos priority

View

Interface view, port group view

Default level

2: System level

Parameters

priority-value: Port priority value, in the range of 0 to 7.

Description

Use **qos priority** to change the port priority of a port.

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

The default port priority is 0.

To view the port priority of a port, use the **display qos trust interface** command.

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

In respect to subinterfaces, only the subinterfaces on SPE cards support the **qos priority** command.

Examples

Set the priority of GigabitEthernet 2/1/1 to 2.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos priority 2
```

Priority trust mode configuration commands

display qos trust interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

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

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

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

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

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

Description

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

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

Examples

Display the priority trust mode and port priority settings of GigabitEthernet 2/1/1.

```
<Sysname> display qos trust interface GigabitEthernet 2/1/1
Interface: GigabitEthernet2/1/1
 Port priority information
  Port priority :0
  Port priority trust type : untrust
```

Table 28 Command output

Field	Description
Interface	Interface type and interface number.
Port priority	Port priority.
Port priority trust type	Priority trust mode on the interface. If the trust mode is untrust, the port priority is used for priority mapping. If not, a priority field in the incoming packet is used.

qos trust

Syntax

qos trust auto

undo qos trust

View

Interface view, port group view

Default level

2: System level

Parameters

auto: Uses a priority in incoming packets for priority mapping.

- An SPE card uses the 802.1p priority of Layer 2 packets, the IP precedence of Layer 3 packets, and the EXP of MPLS packets for priority mapping.
- An SPC card uses the IP precedence of IP packets, EXP of MPLS packets, and 802.1p priority of any other non-IP packet for priority mapping.

Description

Use **qos trust auto** to configure an interface to use a particular priority field in the incoming packet for priority mapping.

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

When a packet arrives on an interface, the router assigns a set of parameters (including 802.1p priority, DSCP precedence, local precedence, and drop precedence) to the packet as configured.

A local precedence is locally significant and corresponds to an output queue.

A drop precedence is used for packet drop. The value 2 corresponds to red packets, the value 1 corresponds to yellow packets, and the value 0 corresponds to green packets.

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

In respect to subinterfaces, only the subinterfaces on SPE cards support the **qos trust auto** command.

Examples

Specify auto priority trust mode for GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos trust auto
```

GTS and rate limit configuration commands

In this chapter, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L. SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.

GTS configuration commands

display qos gts interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

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

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

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

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

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

Description

Use **display qos gts interface** to view generic traffic shaping (GTS) configuration information on the specified interface or all the interfaces if no interface is specified.

With GTS enabled on an interface, this command can display the GTS configuration information of the interface regardless of the interface state (up or down).

Examples

Display the GTS configuration information on GigabitEthernet 2/1/5.

```
<Sysname> display qos gts interface GigabitEthernet2/1/5
Interface: GigabitEthernet2/1/5
 Rule(s): If-match any
 CIR 160 (kbps), CBS 10240 (byte)
```

Table 29 Command output

Field	Description
Interface	Interface type and interface number.
Rule(s)	Match criteria.
CIR	Committed information rate (CIR) in kbps.
CBS	Committed burst size in bytes, which specifies the depth of the token bucket for holding burst traffic.

qos gts any

Syntax

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

undo qos gts any

View

Interface view, port group view

Default level

2: System level

Parameters

any: Shapes all packets.

cir *committed-information-rate*: Specifies the committed information rate (CIR) in kbps. The value range for *committed-information-rate* varies by interface type as follows:

- 300 to 1000000 on a GE interface or the corresponding Layer 3 Ethernet subinterface.
- 2500 to 10000000 on a 10-GE interface or the corresponding Layer 3 Ethernet subinterface.
- 300 to 10000000 on a non-FR POS interface.
- 40 to 1000000 on an MP-group interface or non-FR serial port.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes, a multiple of 1024. A value that is not a multiple of 1024 is converted into a multiple of 1024. The value range and default for *committed-burst-size* vary by interface type as follows:

- For Ethernet interfaces and Layer 3 Ethernet subinterfaces, the CBS ranges from 4096 to 133169152 and the default CBS value is the traffic transmitted at the rate of CIR in 500 ms.
- For non-FR POS interfaces, the CBS ranges from 1024 to 133169152 and the default CBS value is the traffic transmitted at the rate of CIR in 500 ms.
- For MP-group interfaces and non-FR serial ports, the CBS ranges from 1024 to 15360 and the default CBS value is 1024.

Description

Use **qos gts any** to set GTS parameters for all traffic on an interface.

Use **undo qos gts any** to remove the GTS parameters for all traffic on an interface.

By default, no GTS parameters are configured on any interface.

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

The **qos gts any** command and the **qos lr outbound** command are mutually exclusive for an interface, subinterface, or port group.

In respect to subinterfaces, only the Layer 3 Ethernet subinterfaces on the SPE cards support the **qos gts any** command.

The **qos gts any** command does not take effect on MFR interfaces, FR POS interfaces, and FR serial ports.

Examples

Configure GTS for all traffic of interface GigabitEthernet 2/1/1, setting CIR to 640 kbps and CBS to 1024000 bytes.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos gts any cir 640 cbs 1024000
```

qos gts queue

Syntax

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

undo qos gts queue *queue*

View

Interface view, port group view

Default level

2: System level

Parameters

queue *queue-number*: Shapes the packets in the queue identified by the *queue-number* argument. The *queue-number* argument can be a number or keyword, and the number-keyword mapping is shown in Table 30.

Table 30 Description on the queue argument

Keyword	Queue number (decimal)
af1	1
af2	2
af3	3
af4	4
be	0
cs6	6
cs7	7
ef	5

cir committed-information-rate: Specifies the committed information rate (CIR) in kbps. The value range for *committed-information-rate* varies by interface type as follows:

- 300 to 1000000 on a GE interface.
- 2500 to 10000000 on a 10-GE interface.
- 300 to 10000000 on a non-FR POS interface.
- 40 to 1000000 on a serial port channelized from an E-CPOS interface.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes, a multiple of 1024. A value that is not a multiple of 1024 is converted into a multiple of 1024. The value range and default for *committed-burst-size* vary by interface type as follows:

- For Ethernet interfaces, the CBS ranges from 4096 to 133169152 and the default CBS value is the traffic transmitted at the rate of CIR in 500 ms.
- For non-FR POS interfaces, the CBS ranges from 1024 to 133169152 and the default CBS value is the traffic transmitted at the rate of CIR in 500 ms.
- For serial ports channelized from E-CPOS interfaces, the CBS ranges from 1024 to 15360 bytes, and the default CBS value is 1024.

Description

Use **qos gts queue** to set GTS parameters for the packets in a queue on an interface.

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

By default, no GTS parameters are configured on any interface.

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

The **qos gts queue** command is not available on subinterfaces.

The **qos gts queue** command does not take effect on FR POS interfaces.

Examples

Shape the traffic in queue af1 of interface GigabitEthernet 2/1/1, setting CIR to 640 kbps and CBS to 1024000 bytes.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos gts queue af1 cir 640 cbs 1024000
```

Rate limit configuration commands

display qos lr interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

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

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

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

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

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

Description

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

If no interface is specified, this command displays the rate limit configuration information on all the interfaces.

With rate limit enabled on an interface, this command can display the rate limit configuration information of the interface regardless of the interface state (up or down).

Examples

Display the rate limit configuration information on interface GigabitEthernet 2/1/5.

```
<Sysname> display qos lr interface GigabitEthernet2/1/5
Interface: GigabitEthernet2/1/5
 Direction: Outbound
 CIR 300 (kbps), CBS 18750 (byte)
```

Table 31 Command output

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

qos lr

Syntax

qos lr outbound cir *committed-information-rate* [**cbs** *committed-burst-size*]

undo qos lr outbound

View

Interface view, port group view

Default level

2: System level

Parameters

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

cir *committed-information-rate*: Specifies the committed information rate (CIR) in kbps. The value range for *committed-information-rate* varies by interface type as follows:

- 300 to 1000000 on a GE interface or the corresponding Layer 3 Ethernet subinterface.
- 2500 to 10000000 on a 10-GE interface or the corresponding Layer 3 Ethernet subinterface.
- 300 to 10000000 on a non-FR POS interface.
- 40 to 1000000 on an MP-group interface or non-FR serial port.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes, a multiple of 1024. A value that is not a multiple of 1024 is converted into a multiple of 1024. The value range and default for *committed-burst-size* vary by interface type as follows:

- For Ethernet interfaces and Layer 3 Ethernet subinterfaces, the CBS ranges from 4096 to 133169152 and the default CBS value is the traffic transmitted at the rate of CIR in 500 ms.
- For non-FR POS interfaces, the CBS ranges from 1024 to 133169152 and the default CBS value is the traffic transmitted at the rate of CIR in 500 ms.
- For MP-group interfaces and non-FR serial ports, the CBS ranges from 1024 to 15360 and the default CBS value is 1024.

Description

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

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

By default, no rate limit is configured on an interface.

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

The **qos gts any** command and the **qos lr** command are mutually exclusive for an interface, subinterface, or port group.

In respect to subinterfaces, only the Layer 3 Ethernet subinterfaces on the SPE cards support the **qos lr** command.

The **qos lr** command does not take effect on MFR interfaces, FR POS interfaces, and FR serial ports.

Examples

Limit the rate of outgoing packets on interface GigabitEthernet 2/1/1, with CIR 640 kbps and CBS 1024000 bytes.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos lr outbound cir 640 cbs 1024000
```

Hardware congestion management configuration commands

In this chapter, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L. SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.

Queue scheduling profile configuration commands

The commands in this chapter are available on only the SPC cards.

display qos qmprofile configuration

Syntax

display qos qmprofile configuration [*profile-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

profile-name: Queue scheduling profile name, a string of 1 to 31 case-sensitive characters.

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

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

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

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

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

Description

Use **display qos qmprofile configuration** to display queue scheduling profile configurations.

If a queue scheduling profile is specified, only the configuration of the profile is displayed. If no queue scheduling profile is specified, the configuration of all queue scheduling profiles is displayed.

Examples

Display the configuration of queue scheduling profile **myprofile**.

```
<Sysname> display qos qmprofile configuration myprofile
Queue management profile: myprofile
 Queue ID    Type    Group    Weight
 ----------------------------------
 0           SP      N/A      N/A
```

```
1              SP       N/A      N/A
2              SP       N/A      N/A
3              SP       N/A      N/A
4              SP       N/A      N/A
5              SP       N/A      N/A
6              WRR      1        200
7              SP       N/A      N/A
```

Table 32 Command output

Field	Description
Queue management profile	Queue scheduling profile name.
Queue ID	ID of a queue.
Type	Queue scheduling type: • SP. • WRR.
Group	For a WRR queue, this field displays the WRR priority group to which the queue belongs. For a queue using any other scheduling mechanism, this field is insignificant and N/A is displayed.
Weight	Scheduling weight. N/A indicates that the Weight field is insignificant for the queue.

display qos qmprofile interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

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

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

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

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

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

Description

Use **display qos qmprofile interface** to display the queue scheduling profile applied to the specified interface.

If no interface is specified, all applications of queue scheduling profiles to interfaces are displayed.

Examples

Display the queue scheduling profile applied to GigabitEthernet 3/0/1.

```
<Sysname> display qos qmprofile interface gigabitethernet 3/0/1
Interface: GigabitEthernet3/0/1
Queue management profile: myprofile
```

Table 33 Command output

Field	Description
Interface	Interface name.
Queue management profile	Name of the queue scheduling profile applied to the interface.

qos apply qmprofile

Syntax

qos apply qmprofile *profile-name*

undo qos apply qmprofile

View

Interface view, port group view

Default level

2: System level

Parameters

profile-name: Queue scheduling profile name, a string of 1 to 31 case-sensitive characters.

Description

Use **qos apply qmprofile** to apply a queue scheduling profile to the interface or port group.

Use **undo qos apply qmprofile** to restore the default.

By default, queues 1 through 4 use the WRR queuing and queues 0, 5, 6, and 7 use the SP queuing on interfaces of SPC cards.

Only one queue scheduling profile can be applied to an interface.

Subinterfaces do not support this command.

Examples

Apply queue scheduling profile **myprofile** to GigabitEthernet 3/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 3/0/1
[Sysname-GigabitEthernet3/0/1] qos apply qmprofile myprofile
```

qos qmprofile

Syntax

qos qmprofile *profile-name*

undo qos qmprofile *profile-name*

View

System view

Default level

2: System level

Parameters

profile-name: Queue scheduling profile name, a string of 1 to 31 case-sensitive characters.

Description

Use **qos qmprofile** to create a queue scheduling profile and enter queue scheduling profile view.

Use **undo qos qmprofile** to delete a queue scheduling profile.

To delete a queue scheduling profile already applied to an interface, remove it from the interface first and then delete it.

In a newly created queue scheduling profile, queues 1 through 4 use the WRR queuing and queues 0, 5, 6, and 7 use the SP queuing.

Examples

Create queue scheduling profile **myprofile** and enter queue scheduling profile view.

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile]
```

queue

Syntax

queue *queue-number* { **sp** | **wrr group** *group-id* **weight** *weight-value* }

undo queue *queue-number*

View

Queue scheduling profile view

Default level

2: System level

Parameters

queue-number: Queue number, which ranges from 0 to 7.

sp: Enables SP for the queue.

wrr: Enables WRR for the queue.

group-id: WRR priority group ID, which ranges from 1 to 2.

weight-value: Scheduling weight, which ranges from 1 to 63.

Description

Use **queue** to configure queue scheduling parameters for a queue.

Use **undo queue** to restore the default for a queue.

To guarantee that the queue scheduling is exact, make sure that the queues assigned to a WRR group are continuous.

Examples

Create queue scheduling profile **myprofile** and configure queue 1 to use SP.

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 1 sp
```

Create queue scheduling profile **myprofile**, configure queue 1 to use WRR, set the scheduling weight of queue 1 to 20, and assign queue 1 to WRR priority group 1.

```
<Sysname> system-view
[Sysname] qos qmprofile myprofile
[Sysname-qmprofile-myprofile] queue 1 wrr group 1 weight 20
```

WFQ queuing configuration commands

WFQ configuration commands are applicable to only SPE cards

display qos wfq interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

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

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

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

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

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

Description

Use **display qos wfq interface** to display the weighted fair queuing (WFQ) configuration on an interface.

If no interface is specified, the WFQ configuration of all the interfaces is displayed.

Related commands: **qos wfq**.

Examples

Display the WFQ configuration of GigabitEthernet 2/1/1.

```
<Sysname> display qos wfq interface GigabitEthernet 2/1/1
Interface: GigabitEthernet2/1/1
Output queue: Hardware weighted fair queue
Queue ID    Weight            Min-Bandwidth
-----------------------------------------
  be        1                 NA
  af1       1                 2000
  af2       1                 NA
  af3       1                 NA
  af4       1                 NA
  ef        1                 NA
  cs6       1                 NA
  cs7       1                 NA
```

Table 34 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Type of the current output queue.
Queue ID	ID of a queue.
Weight	Queue weight based on which queues are scheduled.
Min-Bandwidth	The minimum guaranteed bandwidth for the queue, in kbps. NA indicates that no configuration is available.

qos bandwidth queue

Syntax

qos bandwidth queue *queue-number* **min** *bandwidth-value*

undo qos bandwidth queue *queue-number* [**min** *bandwidth-value*]

View

Interface view, port group view

Default level

2: System level

Parameters

queue-number: Queue specified by the *queue-number* argument, which can be a number or keyword. The number-keyword mapping is shown in Table 35. The bandwidth configuration does not take effect on queue 0 (queue be).

Table 35 Description on the *queue-number* argument

Keyword	Queue number (decimal)
af1	1
af2	2
af3	3

Keyword	Queue number (decimal)
af4	4
be	0
cs6	6
cs7	7
ef	5

min *bandwidth-value*: Minimum guaranteed bandwidth (in kbps), which specifies the minimum bandwidth guaranteed for a queue when the port is congested.

Description

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

Use **undo qos bandwidth queue** to cancel the minimum guaranteed bandwidth configuration for a queue on a port.

By default, no minimum guaranteed bandwidth is configured for a port.

Settings in ATM interface view take effect on all PVCs of the ATM interface. Settings in interface view take effect on the current interface. Settings in port group view take effect on all ports in the port group.

An SPC card does not support this command.

Subinterfaces do not support this command.

Examples

Set the minimum guaranteed bandwidth to 100 kbps for queue 1 on GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 2/1/1
[Sysname-GigabitEthernet2/1/1] qos bandwidth queue 1 min 100
```

qos wfq weight

Syntax

qos wfq *queue-number* **weight** *schedule-value*

undo qos wfq *queue-number* **weight**

View

Interface view, port group view

Default level

2: System level

Parameters

queue-number: Queue specified by the *queue-number* argument, which can be a number or keyword. The number-keyword mapping is shown in Table 35.

weight *schedule-value*: Specifies the scheduling weight for the specified queue, in the range of 1 to 63.

Description

Use **qos wfq weight** to configure a scheduling weight for a WFQ queue on a port.

Use **undo qos wfq weight** to restore the default scheduling weight for a WFQ queue on a port.

By default, the scheduling weight of a WFQ queue is 1.

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

In respect to subinterfaces, only the Layer 3 Ethernet subinterfaces of the SPE cards support this command.

An SPC card does not support this command.

Related commands: **display qos wfq interface**.

Examples

Set the scheduling weight of queue 3 and queue 4 to 20 and 30 on GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet2/1/1
[Sysname-GigabitEthernet2/1/1] qos wfq 3 weight 20
[Sysname-GigabitEthernet2/1/1] qos wfq 4 weight 30
```

CBQ configuration commands

CBQ configuration commands are applicable to only SPE cards.

queue af

Syntax

queue af bandwidth *bandwidth*

undo queue af

View

Traffic behavior view

Default level

2: System level

Parameters

bandwidth: Guaranteed bandwidth for assured forwarding (AF), which ranges from 64 to 10000000 in kbps.

Description

Use **queue af** to enable assured-forwarding (AF) and set the guaranteed bandwidth for the AF traffic.

Use **undo queue af** to remove the configuration from the traffic behavior.

The total bandwidth assigned to AF and EF in a policy must be no more than the maximum available bandwidth of the interface where the policy is applied.

Related commands: **queue ef**.

Examples

Enable AF and set the guaranteed bandwidth to 5 Mbps for the AF traffic in behavior **af_behav**.

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

```
[Sysname] traffic behavior af_behav
[Sysname-behavior-af_behav] queue af bandwidth 5000
[Sysname-behavior-af_behav] quit
```

queue ef

Syntax

queue ef bandwidth *bandwidth* [**cbs** *burst*]

undo queue ef

View

Traffic behavior view

Default level

2: System level

Parameters

bandwidth: Guaranteed bandwidth for expedited forwarding (EF), which ranges from 64 to 10000000 in kbps.

cbs *burst*: Sets the committed burst size (CBS) in bytes, which specifies the maximum burst traffic size permitted when the average traffic rate conforms to the configured *bandwidth*. CBS ranges from 1600 to 1000000000 bytes, and defaults to *bandwidth*×25. The CBS should be greater than traffic transmitted within 50ms at the rate of *bandwidth*. Otherwise, the burst traffic rate is too low, and the burst traffic transmission is affected.

Description

Use **queue ef** to enable expedited forwarding (EF), and configure the guaranteed bandwidth for the EF traffic.

The total bandwidth assigned to AF and EF in a policy must be no more than the maximum available bandwidth of the interface where the policy is applied.

Related commands: **queue af**.

Examples

Enable EF and set the guaranteed bandwidth to 30 Mbps for the EF traffic in behavior **ef_behav**.

```
<Sysname> system-view
[Sysname] traffic behavior ef_behav
[Sysname-behavior-ef_behav] queue ef bandwidth 30000
[Sysname-behavior-ef_behav] quit
```

queue wfq

Syntax

queue wfq

undo queue wfq

View

Traffic behavior view

Default level

2: System level

Parameters

None

Description

Use **queue wfq** to configure WFQ for the behavior.

Use **undo queue wfq** to remove the configuration.

Examples

Configure WFQ for behavior **be_behav**.

```
[Sysname] traffic behavior be_behav
[Sysname-behavior-be_behav] queue wfq
```

wred

Syntax

wred [**dscp** | **ip-precedence**]

undo wred

View

Traffic behavior view

Default level

2: System level

Parameters

dscp: Uses DSCP for calculating drop probability for a packet.

ip-precedence: Uses IP precedence for calculating drop probability for a packet. This is the default.

Description

Use **wred** to enable WRED drop in a traffic behavior.

Use **undo wred** to remove the configuration from a traffic behavior.

To use this command, make sure that the **queue af** or **queue wfq** command has been configured.

Examples

Configure WRED for behavior **af_behav**.

```
<Sysname> system-view
[Sysname] traffic behavior af_behav
[Sysname-behavior-af_behav] queue af bandwidth 5000
[Sysname-behavior-af_behav] wred
```

Congestion avoidance configuration commands

In this chapter, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L. SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.

WRED configuration commands

WRED configuration commands are available to only SPE cards.

display qos wred interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

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

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

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

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

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

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

Description

Use **display qos wred interface** to display the WRED configuration and statistics of an interface.

If no interface is specified, the WRED configuration and statistics for all interfaces are displayed.

Examples

Display the WRED configuration and statistics of interface GigabitEthernet 2/1/1.

```
<Sysname> display qos wred interface GigabitEthernet 2/1/1
Interface: GigabitEthernet2/1/1
 Current WRED configuration:
 Applied WRED table name: 123
```

Table 36 Command output

Field	Description
Interface	Interface type and interface number.
Applied WRED table name	Name of the applied WRED table.

WRED table configuration commands

WRED table configuration commands are applicable to only SPE cards

display qos wred table

Syntax

display qos wred table [*table-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

table-name: Name of the WRED table to be displayed.

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

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

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

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

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

Description

Use **display qos wred table** to display the WRED table configuration.

If no WRED table name is specified, configurations of all WRED tables are displayed.

Examples

Display the configuration of WRED table 1.

```
<Sysname> display qos wred table 1
Table Name: 1
Table Type: Queue based WRED
QID:  gmin  gmax  gprob  ymin  ymax  yprob  rmin  rmax  rprob  exponent
------------------------------------------------------------------------
 0 10224  10240   100 10224  10240   100 10224  10240   100      8
 1 10224  10240   100 10224  10240   100 10224  10240   100      8
 2 10224  10240   100 10224  10240   100 10224  10240   100      8
 3 10224  10240   100 10224  10240   100 10224  10240   100      8
 4 10224  10240   100 10224  10240   100 10224  10240   100      8
```

```
5 10224  10240   100 10224  10240   100 10224  10240   100      8
6 10224  10240   100 10224  10240   100 10224  10240   100      8
7 10224  10240   100 10224  10240   100 10224  10240   100      8
```

Table 37 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	Maximum drop probability for green packets.
ymin	Lower limit for yellow packets.
ymax	Upper limit for yellow packets.
yprob	Maximum drop probability for yellow packets.
rmin	Lower limit for red packets.
rmax	Upper limit for red packets.
rprob	Maximum drop probability for red packets.
exponent	Exponent for average length calculation.

qos wred table

Syntax

qos wred queue table *table-name*

undo qos wred table *table-name*

View

System view

Default level

2: System level

Parameters

queue: Creates a queue-based table; packets are dropped based on the queue when congestion occurs.

table *table-name*: Specifies an name for the table. The *table-name* argument is a string of 1 to 32 characters.

Description

Use **qos wred queue table** to create a WRED table and enter WRED table view.

Use **undo qos wred table** to remove a global WRED table.

By default, no global WRED table is created.

A WRED table in use cannot be removed.

Related commands: **display qos wred table** and **display qos wred interface**.

Examples

Create WRED table **exp-table1**.

```
<Sysname> system-view
[Sysname] qos wred queue table exp-table1
[Sysname-wred-table-exp-table1]
```

queue

Syntax

queue *queue-number* [**drop-level** *drop-level*] **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo queue { *queue-number* | **all** }

View

WRED table view

Default level

2: System level

Parameters

queue-number: Queue number. This argument is available on only Layer 2 ports.

drop-level *drop-level*: Specifies a drop level. 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*: Lower limit, which is 10224 by default.

high-limit *high-limit*: Upper limit, which is 10240 by default.

discard-probability *discard-prob*: Denominator for drop probability. Each drop level corresponds to an independent denominator. The *discard-prob* argument is 100 by default.

Description

Use **queue** to configure the drop parameters for a specified queue in the queue-based WRED table.

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

By default, a global queue-based WRED table has a set of default available parameters.

Related commands: **qos wred table**.

Examples

Configure the drop parameters for packets with drop level 1 in queue 1 for the global queue-based WRED table **queue-table1**.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 10 high-limit 20
discard-probability 30
```

queue weighting-constant

Syntax

queue *queue-number* **weighting-constant** *exponent*

undo queue *queue-number* **weighting-constant**

View

WRED table view

Default level

2: System level

Parameters

queue-number: Queue number.

weighting-constant *exponent*: Specifies the exponent for average queue length calculation, in the range of 0 to 21. This argument is 8 by default.

Description

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.

Related commands: **qos wred table**.

Examples

Set the exponent for average queue length calculation to 12 for queue 1 in the queue-based WRED table **queue-table1**.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 weighting-constant 12
```

qos wred apply

Syntax

qos wred apply *table-name*

undo qos wred apply

View

Interface view, port group view

Default level

2: System level

Parameters

table-name: Name of a global WRED table.

Description

Use **qos wred apply** to apply a global WRED table on a port/port group.

Use **undo qos wred apply** to restore the default.

By default, the tail drop mode is adopted on a port.

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

An SPC card does not support this command.

In respect to subinterfaces, only the Layer 3 Ethernet subinterfaces of the SPE cards support this command.

Related commands: **display qos wred interface**, **display qos wred table**, and **qos wred table**.

Examples

Apply the queue-based WRED table **queue-table1** to the Layer 2 port GigabitEthernet 2/1/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet2/1/1
[Sysname-GigabitEthernet2/1/1] qos wred apply queue-table1
```

Aggregate CAR configuration commands

car name

Syntax

car name *car-name*

undo car

View

Traffic behavior view

Default level

2: System level

Parameters

car-name: Name of an aggregate CAR action.

Description

Use **car name** to reference an aggregate CAR action for the traffic behavior.

Use **undo car** to remove the aggregate CAR action from the traffic behavior.

Examples

Reference the aggregate CAR action **aggcar-1** for the traffic behavior **be1**.

```
<Sysname> system-view
[Sysname] traffic behavior be1
[Sysname-behavior-be1] car name aggcar-1
```

display qos car name

Syntax

display qos car name [*car-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

car-name: Name of an aggregate CAR action.

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

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

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

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

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

Description

Use **display qos car name** to display the configuration and statistics of a specified aggregate CAR action.

If no CAR action is specified, the configuration and statistics of all the aggregate CAR policies are displayed.

Examples

Display the configuration and statistics of the aggregate CAR action **aggcar-1**.

```
<Sysname> display qos car name aggcar-1
 Name: aggcar-1
  Mode: aggregative
 CIR 200(kbps)  CBS: 2000(byte)  EBS: 40000(byte)  PIR: 2000(kbps)
  Red Action: discard
  Green packet 2000(Bytes)
  Yellow packet 400(Bytes)
  Red packet 6000(Bytes)
```

Table 38 Command output

Field	Description
Name	Name of the CAR action.
Mode	Mode of the CAR action.
CIR CBS EBS PIR	Parameters for the aggregate CAR action.
Red Action	Action on red packets.
Green packet	Statistics about green packets.
Yellow packet	Statistics about yellow packets.
Red packet	Statistics about red packets.

qos car aggregative

Syntax

qos car *car-name* **aggregative cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**pir** *peek-information-rate*] [**red** { **discard** | **pass** }]

undo qos car *car-name*

View

System view

Default level

2: System level

Parameters

car-name: Name of an aggregate CAR action, a string of 1 to 31 characters.

aggregative: Indicates that the global CAR action is aggregative. Only aggregate CAR is supported.

cir *committed-information-rate*: Committed information rate (CIR) in kbps, in the range of 64 to 10000000.

cbs *committed-burst-size*: Specifies the committed burst size (CBS) in bytes, which specifies the size of burst traffic when the actual average rate is no bigger than CIR. CBS ranges from 1875 to 1000000000. By default, CBS is the traffic transmitted in 500 ms at the rate of CIR. The CBS to be configured must be no smaller than the traffic transmitted at the rate of CIR in 50 ms. Otherwise, the burst rate of the token bucket is too low, and affects burst traffic transmission.

ebs *excess-burst-size*: Excess burst size (EBS) in bytes, in the range of 0 to 1000000000.

pir *peak-information-rate*: Peak information rate (PIR) in kbps, in the range of 64 to 10000000. If PIR is not configured, only one token bucket is configured for TP. Otherwise, two token buckets are configured for TP.

red *action*: Specifies the action to be taken on red packets. Red packets are packets whose rate neither conforms to CIR nor conforms to PIR.

The *action* argument can be:

- **discard**: Drops the packet.
- **pass**: Permits the packet to pass through.

Description

Use **qos car aggregative** to configure an aggregate CAR action.

Use **undo qos car aggregative** to remove an aggregate CAR action.

An aggregate CAR action does not take effect until it is referenced in a policy.

- On an SPE-1010, SPE-1020, SPE-1010-E, or SPE-1020-E card:

For packets forwarded at Layer 3, such as IPv4/IPv6 unicast packets, multicast packets, tunnel packets, and L3VPN incoming tunnel packets, aggregate CAR only takes the IP header and payload into account. The port rate parameters configured in the **qos car aggregative** command are transformed into the theoretical output rate following these formulae (take 128-byte Layer-3 packets for example, and assume that the rate is set to 10000 kbps):

  - When the incoming port and the outgoing port are Ethernet interfaces and the packets are untagged, the theoretical outgoing interface rate is calculated following this formula:

    10000 kbps × 128 bytes/(128 bytes of packet length – 4 bytes of CRC – 14 bytes of Layer-2 header)

  - When the incoming port and the outgoing port are POS interfaces, the theoretical outgoing interface rate is calculated following this formula:

    10000 kbps × 128 bytes/(128 bytes of packet length – 4 bytes of CRC – 4 bytes of Layer-2 header)

- On an SPC, SPE-1010-II, SPE-1020-II, SPE-1010-E-II, or SPE-1020-E-II card:

  The configured rate is the same as the theoretical output rate.

Examples

Configure the aggregate CAR action **aggcar-1**, where CIR is 200, CBS is 2000, and red packets are dropped.

```
<Sysname> system-view
[Sysname] qos car aggcar-1 aggregative cir 200 cbs 2000 red discard
```

reset qos car name

Syntax

reset qos car name [*car-name*]

View

User view

Default level

2: System level

Parameters

car-name: Name of an aggregate CAR action.

Description

Use **reset qos car name** to clear the statistics about the specified aggregate CAR action.

If no *car-name* is specified, the statistics about all aggregate CAR policies is cleared.

Examples

Clear the statistics about the aggregate CAR action **aggcar-1**.

```
<Sysname> reset qos car name aggcar-1
```

QoS traffic accounting configuration commands

In this chapter, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L. SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.

The QoS traffic accounting configuration commands are applicable to only the ports operating in bridge mode on an SPC card

display qos traffic-counter

Syntax

display qos traffic-counter { **inbound** | **outbound** } { **counter0** | **counter1** } **slot** *slot-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

inbound: Inbound direction.

outbound: Outbound direction.

counter0: Counter 0.

counter1: Counter 1.

slot *slot-number*: Specifies a card by its slot number.

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

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

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

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

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

Description

Use **display qos traffic-counter** to display the traffic statistics collected by the specified counter and display the configuration of the counter.

Examples

Display the outbound traffic statistics of counter 0 on card 4.

```
<Sysname> display qos traffic-counter outbound counter0 slot 4
Slot 4 outbound counter0 mode:
 Interface: all
```

```
 VLAN: all
 Local precedence: all
 Drop priority: all

Traffic-counter summary:
 Unicast: 0 packets
 Multicast: 0 packets
 Broadcast: 0 packets
 Control packets: 2 packets
 Bridge egress filtered packets: 0 packets
 Tail drop packets: 0 packets
 Multicast Tail drop packets: 6 packets
 Forward restrictions packets: 0 packets
```

Table 39 Command output

Field	Description
Slot 4 outbound counter0 mode	Monitored objects of the counter in the outbound direction.
Interface	Interfaces monitored by the counter.
VLAN	VLANs monitored by the counter.
Local precedence	Local precedence values monitored by the counter.
Drop priority	Drop precedence values monitored by the counter.
Traffic-counter summary	Summary statistics collected by the counter.
Unicast	The number of unicast packets.
Multicast	The number of multicast packets.
Broadcast	The number of broadcast packets.
Control packets	The number of control packets.
Bridge egress filtered packets	The number of packets filtered in the egress direction of the bridge.
Tail drop packets	The number of unicast packets dropped by tail drop.
Multicast Tail drop packets	The number of multicast and broadcast packets dropped by tail drop.
Forward restrictions packets	The number of packets whose forwarding is restricted (this field is not supported).

Display the inbound traffic statistics of counter 0 on card 1.

```
<Sysname> display qos traffic-counter inbound counter0 slot 1
Slot 1 inbound counter0 mode:
 Interface: all
 VLAN: all

Traffic-counter summary:
 Bridge in frames: 5490000 packets
 Bridge local discarded: 0 packets
 Bridge vlan ingress filter discarded: 0 packets
```

```
Bridge security filter discarded: 0 packets
```

Table 40 Command output

Field	Description
Slot 1 inbound counter0 mode	Monitored objects of the counter in the inbound direction.
Interface	Interfaces monitored by the counter.
VLAN	VLANs monitored by the counter.
Traffic-counter summary	Summary statistics collected by the counter.
Bridge in frames	The number of packets received by the bridge.
Bridge local discarded	The number of packets dropped by the bridge (except the packets dropped due to other causes).
Bridge vlan ingress filter discarded	The number of incoming packets filtered based on the VLAN.
Bridge security filter discarded	The number of packets filtered by the security function of the bridge.

qos traffic-counter

Syntax

qos traffic-counter { **inbound** | **outbound** } { **counter0** | **counter1** } **slot** *slot-number* [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**local-precedence** *lp-value*] [**drop-priority** *dp-value*]

undo qos traffic-counter { **inbound** | **outbound** } { **counter0** | **counter1** } **slot** *slot-number*

View

System view

Default level

2: System level

Parameters

inbound: Inbound direction.

outbound: Outbound direction.

counter0: Counter 0.

counter1: Counter 1.

slot *slot-number*: Specifies a card by its slot number.

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

vlan-id: VLAN ID, in the range of 1 to 4093.

local-precedence: Local precedence value, in the range of 0 to 7.

drop-priority: Drop precedence, in the range of 0 to 2.

Description

Use **qos traffic-counter** to enable the traffic accounting function

Use **undo qos traffic-counter** to disable the traffic accounting function.

By default, the traffic accounting function is disabled.

A card provides two counters for traffic accounting. The monitored object can be a port, a VLAN, a local precedence value, or a drop precedence value.

- If no port is specified, the traffic of all the ports on the card is monitored.
- If no VLAN is specified, the traffic of all the VLANs is monitored.
- If no local precedence value is specified, the traffic with any local precedence value is monitored.
- If no drop precedence value is specified, the traffic with any drop precedence value is monitored.

NOTE:

When you redefine the monitored object on a card with the **qos traffic-counter** command, the counter resets automatically.

Examples

Enable counter 0 in slot 4 to collect statistics about the outbound traffic on GigabitEthernet 4/0/1.

```
<Sysname> system-view
[Sysname] qos traffic-counter outbound counter0 slot 4 interface gigabitethernet 4/0/1
```

reset qos traffic-counter

Syntax

reset qos traffic-counter { **inbound** | **outbound** } { **counter0** | **counter1** } **slot** *slot-number*

View

User view

Default level

2: System level

Parameters

inbound: Inbound direction.

outbound: Outbound direction.

counter0: Counter 0.

counter1: Counter 1.

slot *slot-number*: Specifies a card by its slot number.

Description

Use **reset qos traffic-counter** to clear the traffic statistics collected by a counter on a card.

Examples

Clear the outbound traffic statistics collected by counter 0 on card 4.

```
<Sysname> reset qos traffic-counter outbound counter0 slot 4
```

Per-port queue-based traffic statistics displaying commands

display qos queue-statistics interface

Syntax

display qos queue-statistics interface [*interface-type interface-number*] [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }] [**dlci** *dlci-number*] [**outbound**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

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

pvc: Displays the queue-based traffic statistics for a PVC on an ATM interface. This keyword is available only for ATM interfaces.

pvc-name: Specifies the PVC by its name.

vpi/vci: Specifies the PVC by its VPI/VCI pair.

dlci *dlci-number*: Specifies a virtual circuit by its data link connection identifier (DLCI) on a frame relay interface. The *dlci-number* argument ranges from 16 to 1007. The **dlci** *dlci-number* option is available only on interfaces enabled with frame relay encapsulation.

outbound: Displays queue-based outbound traffic statistics.

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

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

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

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

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

Description

Use **display qos queue-statistics interface** to display the port queue traffic statistics.

If no interface is specified, statistics for all interfaces are displayed.

For more information about the **reset counters interface** command, see *Interface Command Reference*.

The command does not take effect on an interface with HQoS configured.

Examples

Display port queue traffic statistics in the outbound direction of GigabitEthernet 2/1/3.

```
<Sysname>display qos queue-statistics interface GigabitEthernet 2/1/3
Interface: GigabitEthernet2/1/3
Direction: Outbound
    Pass: 0 packets, 0 bytes
    Drop: 0 packets, 0 bytes

  Data Flow:
    Queue 0:
      Pass: 0 packets, 0 bytes
      Drop: 0 packets, 0 bytes
      Total queue length  : 4096 packets
      Current queue length: 0 packets, 0% use ratio

    Queue 1:
      Pass: 0 packets, 0 bytes
      Drop: 0 packets, 0 bytes
      Total queue length  : 2048 packets
      Current queue length: 0 packets, 0% use ratio

    Queue 2:
      Pass: 0 packets, 0 bytes
      Drop: 0 packets, 0 bytes
      Total queue length  : 2048 packets
      Current queue length: 0 packets, 0% use ratio

    Queue 3:
      Pass: 0 packets, 0 bytes
      Drop: 0 packets, 0 bytes
      Total queue length  : 2048 packets
      Current queue length: 0 packets, 0% use ratio

    Queue 4:
      Pass: 0 packets, 0 bytes
      Drop: 0 packets, 0 bytes
      Total queue length  : 2048 packets
      Current queue length: 0 packets, 0% use ratio

    Queue 5:
      Pass: 0 packets, 0 bytes
      Drop: 0 packets, 0 bytes
      Total queue length  : 512 packets
      Current queue length: 0 packets, 0% use ratio

    Queue 6:
      Pass: 0 packets, 0 bytes
      Drop: 0 packets, 0 bytes
      Total queue length  : 512 packets
      Current queue length: 0 packets, 0% use ratio
```

```
Queue 7:
  Pass: 0 packets, 0 bytes
  Drop: 0 packets, 0 bytes
  Total queue length  : 8192 packets
  Current queue length: 0 packets, 0% use ratio
```

Table 41 Command output

Field	Description
Interface	Interface for which port queue traffic statistics are to be displayed.
Direction	Direction for which port queue traffic statistics are to be displayed.
Pass	The number of packets forwarded and the number of bytes forwarded.
Drop	The number of packets dropped and the bytes of packets dropped.
Data Flow	Traffic statistics per queue.
Queue	Queue ID.
Total queue length	The total queue length.
Current queue length	The current queue length.
use ratio	Usage of the queue.

QoS pipe mode configuration commands

In this chapter, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L. SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.

qos pipe-mode

Syntax

qos pipe-mode

undo qos pipe-mode

View

System view

Default level

2: System level

Parameters

None

Description

Use **qos pipe-mode** to configure the QoS pipe mode.

Use **undo qos pipe-mode** to cancel the QoS pipe mode.

By default, the QoS pipe mode is not configured.

With the QoS pipe mode configured, packets can pass through any of the following networks and keep their DSCP values unchanged.

- MPLS L2VPN network
- MPLS L3VPN network
- VPLS network

As a result, the forwarding and scheduling of the IP packets on the downstream devices are not affected. For more information, see *ACL and QoS Configuration Guide*.

This command is available only on SPC cards.

After the QoS pipe mode is configured, the **qos priority** and **qos trust** commands configured on an SPC card do not take effect.

Examples

Configure the QoS pipe mode.

```
<Sysname> system-view
[Sysname] qos pipe-mode
```

FR QoS configuration commands

cir allow

Syntax

cir allow [**inbound** | **outbound**] *committed-information-rate*

undo cir allow [**inbound** | **outbound**]

View

FR class view

Default level

2: System level

Parameters

inbound: Sets the CIR ALLOW for the incoming packets. This keyword is available when FR traffic policing is enabled on interfaces. The router does not support this keyword in the current software version. The keyword is reserved for future support.

outbound: Sets the CIR ALLOW for the outgoing packets. This keyword is available when FR traffic policing is enabled on interfaces.

committed-information-rate: CIR ALLOW in bps, in the range of 56000 to 2500000000. The CIR ALLOW is 56000 bps by default.

Description

Use **cir allow** to set the CIR ALLOW for FR PVCs.

Use **undo cir allow** to restore the default.

The CIR ALLOW is the transmit rate that an FR PVC can provide when no congestion occurs to the network.

If the packet direction is not specified, the CIR ALLOW is effective for both incoming packets and outgoing packets.

NOTE:

Do not configure the CIR ALLOW to be smaller than the CIR, which defaults to 56000 bps.

Examples

Set the CIR ALLOW to 64000 bps for FR class **test1**.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir allow 64000
```

display fr class-map

Syntax

display fr class-map { **fr-class** *class-name* | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

class-name: FR class name, which is a string of 1 to 30 characters.

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

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

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

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

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

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

Description

Use **display fr class-map** to display the mapping relationship between FR classes and interfaces (including the DLCIs of an interface, subinterfaces of an interface, and the DLCIs of subinterfaces).

For this command, you can specify an FR class name, or specify a primary interface. However, you cannot specify a subinterface.

Examples

Display the mapping relationship between Serial 2/1/6:0 and FR classes.

```
<Sysname> display fr class-map interface Serial 2/1/6:0
Serial2/1/6:0
  fr-class ts
```

Table 42 Command output

Field	Description
Serial2/1/6:0	FR interface.
fr-class	FR class.

fr class

Syntax

fr class *class-name*

undo fr class *class-name*

View

System view

Default level

2: System level

Parameters

class-name: FR class name, which is a string of 1 to 30 characters.

Description

Use **fr class** to create an FR class and enter FR class view.

Use **undo fr class** to remove the specified FR class.

By default, no FR class is created.

The FR class parameters do not take effect until you associate the FR class with an interface or PVC and enable the FR QoS function on the interface.

With an FR class removed, all the associations associating this FR class with an interface or a DLCI are released.

Related commands: **fr-class**.

Examples

Create FR class **test1**, and enter its view.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1]
```

fr-class

Syntax

fr-class *class-name*

undo fr-class *class-name*

View

FR interface/subinterface view, FR DLCI view

Default level

2: System level

Parameters

class-name: FR class name, which is a string of 1 to 30 characters.

Description

Use **fr-class** to associate an FR class with the current FR PVC.

Use **undo fr-class** to cancel the association.

By default, no FR class is associated with an FR interface/subinterface or FR PVC.

If the specified FR class exists, the **fr-class** command associates the FR class with the current FR PVC. If the specified FR class does not exist, the system prompts that the FR class does not exist.

Instead of removing an FR class, the **undo fr-class** command just cancels the association between the FR class and the current FR PVC. To remove an FR class, use the **undo fr class** command.

Related commands: **fr class**.

Examples

Associate FR class **test1** with an FR PVC with DLCI 200.

```
<Sysname> system-view
[Sysname] interface Serial 2/1/6:0
[Sysname-Serial2/1/6:0] fr dlci 200
[Sysname-fr-dlci-Serial12/1/6:0-200] fr-class test1
```

fr traffic-shaping

Syntax

fr traffic-shaping

undo fr traffic-shaping

View

FR interface view, MFR interface view

Default level

2: System level

Parameters

None

Description

Use **fr traffic-shaping** to enable FRTS.

Use **undo fr traffic-shaping** to disable FRTS.

By default, FRTS is disabled.

FRTS is applied to the outgoing interfaces and are usually applied to the DCE of an FR network.

Related commands: **fr class** and **fr-class**; **fr dlci** (*Layer 2—WAN Command Reference*).

Examples

Enable FRTS on Serial 2/1/6:0.

```
<Sysname> system-view
[Sysname] interface Serial 2/1/6:0
[Sysname-Serial 2/1/6:0] fr traffic-shaping
```

HQoS configuration commands

In this chapter, SPC cards refer to the cards prefixed with SPC, for example, SPC-GT48L. SPE cards refer to the cards prefixed with SPE, for example, SPE-1020-E-II.

Only SPE cards support HQoS. SPC cards do not support HQoS.

Forwarding class configuration commands

display qos forwarding-class

Syntax

display qos forwarding-class [*fc-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

fc-name: Forwarding class name, a case-sensitive string of 1 to 31 characters.

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

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

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

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

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

Description

Use **display qos forwarding-class** to display forwarding class information. If no forwarding class is specified, this command displays information about all forwarding classes.

Examples

Display information about all forwarding classes.

```
<Sysname> display qos forwarding-class
Forwarding class: BE, ID: 0

Forwarding class: AF, ID: 1

Forwarding class: EF, ID: 2

Forwarding class: NC, ID: 3
```

remark forwarding-class

Syntax

remark forwarding-class { **id** *fc-id* | **name** *fc-name* }

undo remark forwarding-class

View

Traffic behavior view

Default level

2: System level

Parameters

id *fc-id*: Specifies a forwarding class by its ID, range from 0 to 3. Only the ID of a pre-defined forwarding class can be specified.

name *fc-name*: Specifies a forwarding class by its name, a case-sensitive string of 1 to 31 characters. Only the name of a pre-defined forwarding class can be specified.

Description

Use **remark forwarding-class** to mark traffic with a forwarding class.

Use **undo remark forwarding-class** to delete the forwarding class marking action.

Your marking action configuration can overwrite the old forwarding class marking action (if any) in the traffic behavior.

Examples

Mark traffic with a forwarding class **BE**.

```
<Sysname> system-view
[Sysname] traffic behavior testtb
[Sysname-behavior-testtb] remark forwarding-class name BE
```

Forwarding group configuration commands

display qos forwarding-group

Syntax

display qos forwarding-group [*fg-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

fg-name: Forwarding group name, a case-sensitive string of 1 to 31 characters.

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

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

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

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

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

Description

Use **display qos forwarding-group** to display forwarding group information. If no forwarding group is specified, this command displays information about all forwarding groups.

Examples

Display information about forwarding group **testfg**.

```
<Sysname> display qos forwarding-group testfg
Forwarding group: testfg, ID: 10
  Forwarding group: subfg1, ID: 1, profile: fgprofile1
    Forwarding class: BE, ID: 0, profile: profile1
    Forwarding class: AF, ID: 1, profile: profile2
  Forwarding group: subfg2, ID: 2, profile: fgprofile2
    Forwarding class: EF, ID: 2, profile: profile3
Forwarding class: NC, ID: 3, profile: profile4
```

The profile field in the output indicates the forwarding profile associated with a forwarding class or forwarding group.

forwarding-class profile

Syntax

forwarding-class *fc-name* **profile** *fp-name*

undo forwarding-class *fc-name*

View

Forwarding group view

Default level

2: System level

Parameters

fc-name: Forwarding class name, a case-sensitive string of 1 to 31 characters.

fp-name: Forwarding profile name, a case-sensitive string of 1 to 31 characters.

Description

Use **forwarding-class** to nest a forwarding class in a forwarding group and specify a forwarding profile for this forwarding class.

Use **undo forwarding-class** to remove the specified forwarding class from the forwarding group.

The forwarding class to be nested in a forwarding group and the forwarding profile to be specified for the forwarding class must already exist.

You cannot nest a forwarding class in a forwarding group with child forwarding groups nested.

You cannot remove a forwarding class from a forwarding group that has been applied to an interface.

Examples

Nest forwarding class **BE** in forwarding group **testfg** and specify forwarding profile **testfp** for this forwarding class.

```
<Sysname> system-view
[Sysname] qos forwarding-group testfg
[Sysname-hqos-fg-testfg] forwarding-class BE profile testfp
```

forwarding-group profile (forwarding-group view)

Syntax

forwarding-group *sub-fg-name* **profile** *fp-name*

undo forwarding-group *sub-fg-name*

View

Forwarding group view

Default level

2: System level

Parameters

sub-fg-name: Child forwarding group name, a case-sensitive string of 1 to 31 characters.

fp-name: Forwarding profile name, a case-sensitive string of 1 to 31 characters.

Description

Use **forwarding-group profile** to nest a child forwarding group in a forwarding group and specify a forwarding profile for this child forwarding group.

Use **undo forwarding-group** to remove the specified child forwarding group from the forwarding group.

The child forwarding group to be nested in a forwarding group and the forwarding profile to be specified for the child forwarding group must already exist.

You cannot nest a child forwarding group in a forwarding group with nested forwarding classes.

A forwarding group with nested child forwarding groups cannot be nested in another forwarding group.

You cannot nest child forwarding groups in a forwarding group that has been applied to an interface or remove nested child forwarding groups from the forwarding group.

Examples

Nest child forwarding group **subfg** in forwarding group **testfg** and specify forwarding profile **testfp** for this child forwarding group.

```
<Sysname> system-view
[Sysname] qos forwarding-group testfg
[Sysname-hqos-fg-testfg] forwarding-group subfg profile testfp
```

qos copy forwarding-group

Syntax

qos copy forwarding-group *fg-source* **to** *fg-dest*&<1-8>

View

System view

Default level

2: System level

Parameters

fg-source: Source forwarding group name, a case-sensitive string of 1 to 31 characters. The forwarding group identified by this argument must already exist.

fg-dest: Destination forwarding group name, a case-sensitive string of 1 to 31 characters. Up to eight destination forwarding groups can be specified. These forwarding groups must not be ones that already exist.

Description

Use **qos copy forwarding-group** to create multiple forwarding groups from a source forwarding group. Any failure that occurs during a copy process does not affect the destination forwarding groups that have been created successfully.

Examples

Copy forwarding group **fg-source** to forwarding group **fg-des1** and forwarding group **fg-des2**.

```
<Sysname> system-view
[Sysname] qos copy forwarding-group fg-source to fg-des1 fs-des2
```

qos forwarding-group

Syntax

qos forwarding-group *fg-name* [**id** *fg-id*]

undo qos forwarding-group *fg-name*

View

System view

Default level

2: System level

Parameters

fg-name: User-defined forwarding group name, a case-sensitive string of 1 to 31 characters. This argument cannot take the name of the pre-defined forwarding group.

id *fg-id*: Specifies a user-defined forwarding group ID, in the range of 0 to 255. The *fg-id* argument cannot take the pre-defined forwarding group ID. If no ID is specified, the system assigns the lowest free ID to the forwarding group.

Description

Use **qos forwarding-group** to create a forwarding group and enter forwarding group view.

Use **undo qos forwarding-group** to delete the specified user-defined forwarding group.

To delete a forwarding group nested in another forwarding group or scheduler policy, remove the nesting relationship first.

You cannot modify or delete the pre-defined forwarding group (named **default** and numbered 0).

Examples

Create forwarding group **testfg**.

```
<Sysname> system-view
[Sysname] qos forwarding-group testfg
```

Drop profile configuration commands

display qos drop-profile

Syntax

display qos drop-profile [*dp-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

dp-name: Drop profile name, a case-sensitive string of 1 to 31 characters.

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

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

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

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

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

Description

Use **display qos drop-profile** to display drop profile information. If no drop profile is specified, this command displays information about all drop profiles.

Examples

Display information about drop profile named **testdp**.

```
<Sysname> display qos drop-profile testdp
Drop profile: testdp, ID: 10
  Green thresholds: 50/60/30(min/max/prob)
  Yellow thresholds: 50/60/30(min/max/prob)
  Red thresholds: 50/60/30(min/max/prob)
  Weighting constant: 2
```

Table 43 Command output

Field	Description
Drop profile	Drop profile name.
ID	Drop profile ID.
Green thresholds	Drop parameters for green packets.

Field	Description
Yellow thresholds	Drop parameters for yellow packets.
Red thresholds	Drop parameters for red packets.
min	Threshold at which packet drop begins.
max	Threshold at which all newly arriving packets are dropped.
prob	Drop probability.
Weighting constant	Exponent for average queue length calculation.

green

Syntax

green low-limit *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo green

View

Drop profile view

Default level

2: System level

Parameters

low-limit *low-limit*: Specifies the lower threshold in packets. When the average queue length reaches the threshold, newly arriving packets are randomly dropped. The *low-limit* argument ranges from 0 to 10240 and defaults to 10224.

high-limit *high-limit*: Specifies the upper threshold in packets. When the average queue length reaches the upper threshold, all newly arriving packets are dropped. The *high-limit* argument ranges from 0 to 10240 and defaults to 10240.

discard-probability *discard-prob*: Specifies the drop probability. The *discard-prob* argument ranges from 0 to 100 and defaults to 100.

Description

Use **green** to set drop parameters for green packets.

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

Examples

Set drop parameters for green packets as follows: set lower threshold to 500, upper threshold to 700, and drop probability to 40.

```
<Sysname> system-view
[Sysname] qos drop-profile testdp
[Sysname-hqos-dp-testdp] green low-limit 500 high-limit 700 discard-probability 40
```

qos drop-profile

Syntax

qos drop-profile *dp-name* [**id** *dp-id*]

undo qos drop-profile *dp-name*

View

System view

Default level

2: System level

Parameters

dp-name: User-defined drop profile name, a case-sensitive string of 1 to 31 characters. This argument cannot take the name of the pre-defined drop profile.

id *dp-id*: Specifies the user-defined drop profile ID, in the range of 0 to 31. The *dp-id* argument cannot take the ID of the pre-defined drop profile. If no ID is specified, the system assigns the lowest free ID to the drop profile.

Description

Use **qos drop-profile** to create a user-defined drop profile and enter drop profile view.

Use **undo qos drop-profile** to delete a user-defined drop profile.

You cannot delete a drop profiles that have been referenced.

You cannot modify or delete the pre-defined drop profile (named **default** and numbered 0).

Examples

Create drop profile **testdp**.

```
<Sysname> system-view
[Sysname] qos drop-profile testdp
```

red

Syntax

red low-limit *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo red

View

Drop profile view

Default level

2: System level

Parameters

low-limit *low-limit*: Specifies the lower threshold in packets. When the average queue length reaches the threshold, newly arriving packets are randomly dropped. The *low-limit* argument ranges from 0 to 10240 and defaults to 10224.

high-limit *high-limit*: Specifies the upper threshold in packets. When the average queue length reaches the upper threshold, all newly arriving packets are dropped. The *high-limit* argument ranges from 0 to 10240 and defaults to 10240.

discard-probability *discard-prob*: Specifies the drop probability. The *discard-prob* argument ranges from 0 to 100 and defaults to 100.

Description

Use **red** to set drop parameters for red packets.

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

Examples

Set drop parameters for red packets as follows: set lower threshold to 500, upper threshold to 700, and drop probability to 40.

```
<Sysname> system-view
[Sysname] qos drop-profile testdp
[Sysname-hqos-dp-testdp] red low-limit 500 high-limit 700 discard-probability 40
```

weighting-constant

Syntax

weighting-constant *exponent*

undo weighting-constant

View

Drop profile view

Default level

2: System level

Parameters

exponent: Exponent for average queue length calculation. The *exponent* argument ranges from 0 to 21 and defaults to 8.

Description

Use **weighting-constant** to set the exponent for average queue length calculation.

Use **undo weighting-constant** to restore the default.

Examples

Set the exponent for average queue length calculation to 2.

```
<Sysname> system-view
[Sysname] qos drop-profile testdp
[Sysname-hqos-dp-testdp] weighting-constant 2
```

yellow

Syntax

yellow low-limit *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo yellow

View

Drop profile view

Default level

2: System level

Parameters

low-limit *low-limit*: Specifies the lower threshold in packets. When the average queue length reaches the threshold, newly arriving packets are randomly dropped. The *low-limit* argument ranges from 0 to 10240 and defaults to 10224.

high-limit *high-limit*: Specifies the upper threshold in packets. When the average queue length reaches the upper threshold, all newly arriving packets are dropped. The *high-limit* argument ranges from 0 to 10240 and defaults to 10240.

discard-probability *discard-prob*: Specifies the drop probability. The *discard-prob* argument ranges from 0 to 100 and defaults to 100.

Description

Use **yellow** to set drop parameters for yellow packets.

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

Examples

Set drop parameters for yellow packets as follows: set lower threshold to 500, upper threshold to 700, and drop probability to 40.

```
<Sysname> system-view
[Sysname] qos drop-profile testdp
[Sysname-hqos-dp-testdp] yellow low-limit 500 high-limit 700 discard-probability 40
```

Forwarding profile configuration commands

bandwidth

Syntax

bandwidth *bandwidth-value*

undo bandwidth [*bandwidth-value*]

View

Forwarding profile view

Default level

2: System level

Parameters

bandwidth-value: Minimum guaranteed bandwidth (in kbps), in the range of 40 to 2500000.

Description

Use **bandwidth** to set the minimum guaranteed bandwidth for the hardware queue of the forwarding class associated with the forwarding profile.

Use **undo bandwidth** to cancel the configuration.

By default, no minimum guaranteed bandwidth is configured for a forwarding profile.

Examples

Set the minimum guaranteed bandwidth to 2000 kbps in the forwarding profile **testfp**.

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

```
[Sysname] qos forwarding-profile testfp
[Sysname-hqos-fp-testfp] bandwidth 2000
```

display qos forwarding-profile

Syntax

display qos forwarding-profile [*fp-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

fp-name: Forwarding profile name, a case-sensitive string of 1 to 31 characters.

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

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

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

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

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

Description

Use **display qos forwarding-profile** to display forwarding profile information. If no forwarding profile is specified, this command displays information about all forwarding profiles.

Examples

Display information about forwarding profile **testfp**.

```
<Sysname> display qos forwarding-profile testfp
Forwarding profile: testfp, ID: 1
  cir 320 (kbps), cbs 1024 (Bytes)
  wfq: weight 2
  drop profile: testdp
  bandwidth: 20000(kbps)
```

drop-profile

Syntax

drop-profile *dp-name*

undo drop-profile

View

Forwarding profile view

Default level

2: System level

Parameters

dp-name: Drop profile name, a case-sensitive string of 1 to 31 characters.

Description

Use **drop-profile** to bind a drop profile to a forwarding profile.

Use **undo drop-profile** to remove the drop profile from the forwarding profile.

By default, a forwarding profile does not reference any drop profile but adopts tail drop.

Examples

Bind drop profile **testdp** to forwarding profile **testfp**.

```
<Sysname> system-view
[Sysname] qos forwarding-profile testfp
[Sysname-hqos-fp-testfp] drop-profile testdp
```

gts cir

Syntax

gts cir *cir-value* [**cbs** *cbs-value*]

undo gts

View

Forwarding profile view

Default level

2: System level

Parameters

cir *cir-value*: Specifies the committed information rate (CIR) in kbps, which ranges from 40 to 10000000 in steps of 40.

cbs *cbs-value*: Specifies the committed burst size (CBS) in bytes, which ranges from 1024 to 133169152 in steps of 1024. The default CBS value (in bytes) is the traffic transmitted at the rate of CIR within 500 ms.

Description

Use **gts** to configure GTS parameters for a forwarding profile.

Use **undo gts** to delete the GTS configuration.

By default, no GTS parameters are configured for a forwarding profile, and the traffic rate is not limited.

Examples

Configure GTS parameters for forwarding profile **testfp** as follows: set the CIR to 320 kbps and CBS to 2048 bytes.

```
<Sysname> system-view
[Sysname] qos forwarding-profile testfp
[Sysname-hqos-fp-testfp] gts cir 320 cbs 2048
```

qos forwarding-profile

Syntax

qos forwarding-profile *fp-name* [**id** *fp-id*]

undo qos forwarding-profile *fp-name*

View

System view

Default level

2: System level

Parameters

fp-name: User-defined forwarding profile name, a case-sensitive string of 1 to 31 characters. This argument cannot be the name of a pre-defined forwarding profile.

id *fp-id*: Specifies the user-defined forwarding profile ID, in the range of 0 to 255. The *fp-id* argument cannot take any pre-defined forwarding profile ID. If no ID is specified, the system assigns the lowest free ID to the forwarding profile.

Description

Use **qos forwarding-profile** to create a user-defined forwarding profile and enter forwarding profile view.

Use **undo qos forwarding-profile** to delete the specified user-defined forwarding profile.

You cannot delete a forwarding profile that has been referenced.

Examples

Create a user-defined forwarding profile named **testfp**.

```
<Sysname> system-view
[Sysname] qos forwarding-profile testfp
```

wfq

Syntax

wfq [**weight** *weight-value*]

undo wfq

View

Forwarding profile view

Default level

2: System level

Parameters

weight *weight-value*: Specifies the scheduling weight, in the range of 1 to 63. The default scheduling weight is 1.

Description

Use **wfq** to configure the forwarding profile to adopt weighted fair queuing (WFQ) queue scheduling. Queues with the same priority are scheduled according to their weights. The weight of a queue determines the percentage of bandwidth assigned to the queue.

Use **undo wfq** to disable WFQ in the forwarding profile.

By default, a forwarding profile uses WFQ with the scheduling weight 1.

Examples

Configure forwarding profile **testfp** to use WFQ queue scheduling, and set the weight to 2.

```
<Sysname> system-view
[Sysname] qos forwarding-profile testfp
[Sysname-hqos-fp-testfp] wfq weight 2
```

Scheduler policy configuration commands

display qos scheduler-policy diagnosis interface

Syntax

display qos scheduler-policy diagnosis interface [*interface-type interface-number* [**outbound**]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

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

outbound: Displays the diagnosis information in the outbound direction of the specified interfaces.

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

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

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

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

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

Description

Use **display qos scheduler-policy diagnosis interface** to display the diagnosis information of a specific interface. If no interface is specified, this command displays the diagnosis information of all interfaces.

Examples

Display the diagnosis information in the outbound direction of GigabitEthernet 3/1/1.

```
<Sysname> display qos scheduler-policy diagnosis interface gigabitEthernet 3/1/1 outbound
SP -- scheduler policy    FG -- forwarding group    FC -- forwarding class
FP -- forwarding profile
------------------------------------------------------------------------
Interface: GigabitEthernet3/1/1
Direction: outbound
SP: sp20
```

```
FG: default    FP: default
Rule: group
FP status: Success

FG: default
Rule: group
  FC: BE    FP: default
FP status: Success

FG: fg10
Rule: group
  FG: fg11    FP: fp11
  Rule: match qos-local-id 11 to 20
  FP status: GTS Failed

FG: fg10
Rule: group
  FG: fg11
  Rule: match qos-local-id 11 to 20
    FC: BE    FP: default
  FP status: Success
```

Table 44 Command output

Field	Description
scheduler policy	Scheduler policy name.
forwarding group	Forwarding group name.
forwarding class	Forwarding class name.
forwarding profile	Forwarding profile name.
match	The match mode is adopted for instantiation.
qos-local-id	Match criteria for instantiation.

FP status	The issuing status of an forwarding profile:
	• **Success**—All contents have been issued successfully.
	• If a forwarding profile has failed to be issued completely, the reason is displayed:
	  ◦ **GTS Failed**—The GTS parameters have failed to be issued to a forwarding class/forwarding group.
	  ◦ **WRED Failed**—The WRED parameters have failed to be issued to a forwarding class/forwarding group.
	  ◦ **WFQ Failed**—The WFQ queue scheduling algorithm has failed to be issued to a forwarding class/forwarding group.
	  ◦ **Queue bind Failed**—The queue binding has failed to be issued to a forwarding class/forwarding group.
	  ◦ **Bandwidth Failed**—The minimum guaranteed bandwidth has failed to be applied to a forwarding class/forwarding group.

display qos scheduler-policy interface

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

interface-type interface-number: Specifies an interface by its type and interface number. If no interface is specified, this command displays the scheduler policy configurations and statistics for all ports.

outbound: Displays the scheduler policy settings and traffic statistics in the outbound direction of the specified interface. The A8800 routers support only the outbound direction. Even if the **outbound** keyword is not specified, this command displays only the settings and statistics for the outbound direction of the interface.

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

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

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

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

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

Description

Use **display qos scheduler-policy interface** to display the scheduler policy settings and scheduler policy statistics of an interface.

Examples

Display the scheduler policy settings and statistics in the outbound direction of GigabitEthernet 2/1/1 after enabling QoS traffic accounting in the outbound direction.

```
<Sysname> display qos scheduler-policy interface gigabitethernet 2/1/1 outbound
SP -- scheduler policy   FG -- forwarding group   FC -- forwarding class
FP -- forwarding profile
-------------------------------------------------------------------------------
Interface: GigabitEthernet2/1/1
Direction: Outbound
SP: p1
  FG: default    FP: default
  Rule: group
      Forwarded: 0 packets, 0 bytes
      Forwarded green: 0 packets, 0 bytes
      Forwarded yellow: 0 packets, 0 bytes
      Forwarded red: 0 packets, 0 bytes
      Dropped: 0 packets, 0 bytes
  FG: default
```

```
Rule: group
  FC: BE    FP: default
    Total queue length: 512 packets
    Current queue length: 0 packets, 0% use rate
    Forwarded: 0 packets, 0 bytes
    Forwarded green: 0 packets, 0 bytes
    Forwarded yellow: 0 packets, 0 bytes
    Forwarded red: 0 packets, 0 bytes
    Dropped: 0 packets, 0 bytes
FG: default
Rule: group
  FC: AF    FP: default
    Total queue length: 512 packets
    Current queue length: 0 packets, 0% use rate
    Forwarded: 0 packets, 0 bytes
    Forwarded green: 0 packets, 0 bytes
    Forwarded yellow: 0 packets, 0 bytes
    Forwarded red: 0 packets, 0 bytes
    Dropped: 0 packets, 0 bytes
FG: default
Rule: group
  FC: EF    FP: default
    Total queue length: 512 packets
    Current queue length: 0 packets, 0% use rate
    Forwarded: 0 packets, 0 bytes
    Forwarded green: 0 packets, 0 bytes
    Forwarded yellow: 0 packets, 0 bytes
    Forwarded red: 0 packets, 0 bytes
    Dropped: 0 packets, 0 bytes
FG: default
Rule: group
  FC: NC    FP: default
    Total queue length: 512 packets
    Current queue length: 0 packets, 0% use rate
    Forwarded: 0 packets, 0 bytes
    Forwarded green: 0 packets, 0 bytes
    Forwarded yellow: 0 packets, 0 bytes
    Forwarded red: 0 packets, 0 bytes
    Dropped: 0 packets, 0 bytes
```

Table 45 Command output

Field	Description
scheduler policy	Scheduler policy name.
forwarding group	Forwarding group name.
forwarding class	Forwarding class name.
forwarding profile	Forwarding profile name.
Interface	Interface to which the scheduler policy is applied.

Field	Description
Direction	Direction in which the scheduler policy is applied.
Rule	Match criteria for instantiation.
Total queue length	Total length of the queue.
Current queue length	Current length of the queue.
use rate	Current queue length/total queue length.
Forwarded packets/bytes	Number of forwarded packets/bytes.
Forwarded green packets/bytes	Number of forwarded green packets/bytes.
Forwarded yellow packets/bytes	Number of forwarded yellow packets/bytes.
Forwarded red packets/bytes	Number of forwarded red packets/bytes.
Dropped packets/bytes	Number of dropped packets/bytes.

display qos scheduler-policy name

Syntax

display qos scheduler-policy name [*sp-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

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

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

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

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

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

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

Description

Use **display qos scheduler-policy name** to display scheduler policy information. If no scheduler policy name is specified, this command displays information about all scheduler policies.

Examples

Display information about scheduler policy **test_sp**.

```
<Sysname> display qos scheduler-policy name test_sp
SP -- scheduler policy    FG -- forwarding group    FC -- forwarding class
FP -- forwarding profile    L -- layer
------------------------------------------------------------------------
SP: sp(1)
 |--FG(L1): default(0)
```

```
|   |      FP: default(0)
|   |      group
|   |
|   |--FC: BE(0)
|   |      FP: default(0)
|   |--FC: AF(1)
|   |      FP: default(0)
|   |--FC: EF(2)
|   |      FP: default(0)
|   |--FC: NC(3)
|          FP: default(0)
|
|--FG(L1): 2(1)
    |      FP: 2(2)
    |      group
    |
    |--FG(L2): 1(2)
        |      FP: 1(1)
        |      match: qos-local-id 2 to 10
        |
        |--FC: BE(0)
        |      FP: 3(3)
        |--FC: AF(1)
        |      FP: default(0)
        |--FC: EF(2)
        |      FP: default(0)
        |--FC: NC(3)
               FP: default(0)
```

Table 46 Command output

Field	Description
scheduler policy	Scheduler policy name.
forwarding group	Forwarding group name.
forwarding class	Forwarding class name.
forwarding profile	Forwarding profile name.
layer	Layer name.
match	The match mode is adopted for instantiation.
group	The group mode is adopted for instantiation.
qos-local-id	Match criteria for instantiation.
Number in the brackets	Index number of the field (forwarding class/forwarding group/forwarding profile/scheduler policy).

forwarding-group group

Syntax

forwarding-group *fg-name* **group**

undo forwarding-group *fg-name* **group**

View

Scheduler policy layer view

Default level

2: System level

Parameters

fg-name: Forwarding group name, a case-sensitive string of 1 to 31 characters.

Description

Use **forwarding-group group** to instantiate a forwarding group in the group mode.

Use **undo forwarding-group group** to delete the instance generated from the forwarding group in the group mode.

A forwarding group with nested forwarding classes cannot be instantiated in the group mode.

Examples

Instantiate forwarding group **testfg** of scheduler policy **testsp** in the group mode.

```
<Sysname> system-view
[Sysname] qos scheduler-policy testsp
[Sysname-hqos-sp-testsp] layer 1
[Sysname-hqos-sp-testsp-layer1] forwarding-group testfg group
```

forwarding-group match

Syntax

forwarding-group *fg-name* **match** [**extended**] **qos-local-id** { *local-id-list* | *local-id1* **to** *local-id2* }

undo forwarding-group *fg-name* **match** [**extended**] **qos-local-id** { *local-id-list* | *local-id1* **to** *local-id2* }

View

Scheduler policy layer view

Default level

2: System level

Parameters

fg-name: Forwarding group name, a case-sensitive string of 1 to 31 characters.

extended: Makes bulk configuration to create a forwarding group instance based on each classification rule.

qos-local-id { *local-id-list* | *local-id1* **to** *local-id2* }: Matches packets by QoS-local-ID marked for them. The local-id-list argument is the list of QoS-local-IDs, for which you can input up to eight QoS-local-IDs. The local-id1 to local-id2 argument specifies a QoS-local-ID range, where the *local-id1* argument must be smaller than the *local-id2* argument. A QoS-local-ID is in the range of 1 to 4095.

Description

Use **forwarding-group match** to instantiate a forwarding group in the match mode according to the specified match criterion.

Use **undo forwarding-group match** to delete the instance generated from the forwarding group according to the specified match criterion.

In the same scheduler policy, instantiate a parent forwarding group before instantiating its child forwarding groups.

In the same scheduler policy, make sure that the match criterion of a child forwarding group is covered in the match criterion of its parent forwarding group. This restriction is not true for the parent forwarding group instantiated in the group mode.

When applying a scheduler policy to an interface, make sure that the match criterion of each parent forwarding group equals the set of match criteria of its child forwarding groups. This restriction is not true for the parent forwarding group instantiated in the group mode.

In the same scheduler policy, the instantiation match criterion of a forwarding group cannot overlap the instantiation match criterion of any other forwarding group except its parent forwarding group or child forwarding groups.

For any forwarding group in a scheduler policy already applied to a port, you cannot instantiate the forwarding group or delete its instances.

Related commands: **forwarding-group group**.

Examples

Instantiate forwarding group **testfg** in scheduler policy **testfp** in the match mode.

```
<Sysname> system-view
[Sysname] qos scheduler-policy testsp
[Sysname-hqos-sp-testsp] layer 1
[Sysname-hqos-sp-testsp-layer1] forwarding-group testfg match extended qos-local-id 1 to
4
```

forwarding-group profile (scheduler-policy view)

Syntax

forwarding-group *fg-name* **profile** *fp-name*

undo forwarding-group *fg-name*

View

Scheduler policy view

Default level

2: System level

Parameters

fg-name: Forwarding group name, a case-sensitive string of 1 to 31 characters.

fp-name: Forwarding profile name, a case-sensitive string of 1 to 31 characters.

Description

Use **forwarding-group profile** to nest a forwarding group in a scheduler policy and specify a forwarding profile for this forwarding group.

Use **undo forwarding-group** to remove the specified forwarding group from the scheduler policy.

The forwarding group to be nested in a scheduler policy and the forwarding profile to be specified for the forwarding group must already exist.

You cannot remove any forwarding group from a scheduler policy that has been applied to a port.

You cannot remove the default forwarding group automatically nested in a scheduler policy.

Examples

Nest forwarding group **subfg** in scheduler policy **testsp** and specify forwarding profile **testfp** for this forwarding group.

```
<Sysname> system-view
[Sysname] qos scheduler-policy testsp
[Sysname-hqos-sp-testsp] forwarding-group testfg profile testfp
```

layer

Syntax

layer { **1** | **2** }

View

Scheduler policy view, scheduler policy layer view

Default level

2: System level

Parameters

1: Enters scheduler policy layer 1 view.

2: Enters scheduler policy layer 2 view.

Description

Use **layer** to enter scheduler policy layer view.

Examples

Enter scheduler policy layer 1 view.

```
<Sysname> system-view
[Sysname] qos scheduler-policy testsp
[Sysname-hqos-sp-testsp] layer 1
[Sysname-hqos-sp-testsp-layer1]
```

qos apply scheduler-policy

Syntax

qos apply scheduler-policy *sp-name* **outbound**

undo qos apply scheduler-policy outbound

View

Ethernet interface view, port group view, POS interface view, ATM interface view, serial interface view, MP-group interface view

Default level

2: System level

Parameters

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

Description

Use **qos apply scheduler-policy** to apply a scheduler policy in the inbound direction of an interface or port group.

Use **undo qos apply scheduler-policy** to remove the scheduler policy applied in the inbound direction of the interface or port group.

Configured in interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

The scheduler policy applied to an interface is mutually exclusive with the QoS policies (including queue-based GTS, port-based WRED, and hardware congestion management) applied to the interface.

Examples

Apply scheduler policy **testsp** to interface GigabitEthernet 3/1/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet3/1/1
[Sysname-GigabitEthernet3/1/1] qos apply scheduler-policy testsp outbound
```

Apply scheduler policy **testsp** to interface Serial 2/1/19:0.

```
<Sysname> system-view
[Sysname] interface Serial 2/1/19:0
[Sysname-Serial2/1/19:0]qos apply scheduler-policy testsp outbound
```

qos copy scheduler-policy

Syntax

qos copy scheduler-policy *sp-source* **to** *sp-dest*

View

System view

Default level

2: System level

Parameters

sp-source: Source scheduler policy name, a case-sensitive string of 1 to 31 characters. The source scheduler policy identified by this argument must already exist.

sp-dest: Destination scheduler policy name, a case-sensitive string of 1 to 31 characters. The specified destination scheduler policy must not be one that already exists.

Description

Use **qos copy scheduler-policy** to create a new scheduler policy of the same contents as the specified source scheduler policy.

Examples

Copy the contents of scheduler policy **sp-source** to create a new scheduler policy named **sp-dest**.

```
<Sysname> system-view
[Sysname] qos copy scheduler-policy sp-source to sp-dest
```

qos scheduler-policy

Syntax

qos scheduler-policy *sp-name* [**id** *sp-id*]

undo qos scheduler-policy *sp-name*

View

System view

Default level

2: System level

Parameters

sp-name: User-defined scheduler policy name, a case-sensitive string of 1 to 31 characters.

id *sp-id*: Specifies a user-defined scheduler policy ID, in the range of 0 to 15. If no ID is specified, the system assigns the lowest free ID to the scheduler policy.

Description

Use **qos scheduler-policy** to create a user-defined scheduler policy and enter scheduler policy view.

Use **undo qos scheduler-policy** to delete the user-defined scheduler policy.

On creation, a user-defined scheduler policy nests the default forwarding group and associates the default forwarding group with the default forwarding profile automatically.

You cannot delete the scheduler policy that has been applied to an interface.

Examples

Create a user-defined scheduler policy **testsp**.

```
<Sysname> system-view
[Sysname] qos scheduler-policy testsp
```

remark qos-local-id

Syntax

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

undo remark qos-local-id

View

Traffic behavior view

Default level

2: System level

Parameters

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

Description

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.

Examples

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

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

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.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index