HP 5500 EI & 5500 SI Switch Series

ACL and QoS

Command Reference

Part number: 5998-1704

Software version: Release 2220

Document version: 6W100-20130810

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

- The term "Layer 3 Ethernet interface" in this chapter refers to route-mode Ethernet ports. You can set an Ethernet port to operate in route mode by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).
- The HP 5500 SI Switch Series does not support Layer 3 Ethernet ports.

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

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 ACLs and Ethernet frame header ACLs.

Description

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

Use **undo acl** to delete the specified IPv4 or Ethernet frame header ACL, or all IPv4 and Ethernet frame header ACLs.

By default, no ACL exists.

You can assign a name to an IPv4 or Ethernet frame header ACL only when you create it. After an ACL is created with a name, you cannot rename it or remove its name.

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

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

Examples

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

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

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

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

acl copy

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

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

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 IPv4 or an Ethernet frame header ACL by copying an ACL that already exists. The new ACL has the same properties and content as the source ACL, but not the same ACL number and name.

You can assign a name for 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 IPv6 ACL:

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

name *acl6-name*: Assigns a name to the IPv6 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 ACLs.

Description

Use **acl ipv6** to create an IPv6 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 ACLs.

By default, no ACL exists.

You can assign a name to an IPv6 ACL only when you create it. After an IPv6 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 IPv6 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 IPv6 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 IPv6 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 IPv6 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 ACL by copying an IPv6 ACL that already exists. The new ACL has the same properties and content as the source ACL, but not the same ACL number and name.

You can assign a name to an IPv6 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 IPv6 ACL rules. This command logs only for IPv6 basic and 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: **packet-filter ipv6**, **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 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 ACL that has a name.

Related commands: **acl ipv6**.

Examples

# Enter the view of IPv6 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 IPv4 ACL rules. This command logs only for IPv4 basic and 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: **packet-filter**, **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 name

Syntax

acl name *acl-name*

View

System view

Default level

2: System level

Parameters

acl-name: Specifies the IPv4 ACL name, a case-insensitive string of 1 to 63 characters. It must start with an English letter. The IPv4 ACL must already exist.

Description

Use **acl name** to enter the view of an IPv4 ACL that has a name.

Related commands: **acl**.

Examples

# Enter the view of IPv4 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

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 IPv4 basic ACLs
- 3000 to 3999 for IPv4 advanced ACLs
- 4000 to 4999 for Ethernet frame header ACLs

all: Displays information for all IPv4 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 match statistics for ACLs on an IRF member switch. The *slot-number* argument represents the ID of the IRF member switch. Available values for the *slot-number* argument are member IDs already assigned in the IRF fabric. If no IRF member switch is specified, the command displays matches statistics for ACLs on all member switches.

|: 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 or all IPv4 ACLs.

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

Examples

# Display the configuration and match statistics for all IPv4 ACLs.

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

Basic ACL  2001, named -none-, 3 rules, match-order is auto,
ACL's step is 5
 rule 10 permit source 1.1.1.1 0
 rule 10 comment This rule is used in rd.
 rule 5 permit source 2.2.2.2 0
 rule 0 permit
```

Table 1 Command output

Field	Description
Basic ACL 2000	Category and number of the ACL. The following field information is about IPv4 basic ACL 2000.

Field	Description
named flow	The name of the ACL is flow. "-none-" means the ACL is not named.
3 rules	The ACL contains three rules.
match-order is auto	The match order for the ACL is auto, which sorts ACL rules in depth-first order. This field is not present when the match order is config.
Statistics is enabled	The rule match counting is enabled for this ACL.
ACL's step is 5	The rule numbering step is 5.
rule 0 permit	Content of rule 0.
5 times matched	There have been five matches for the rule. If the **counting** keyword is configured for the rule or the **hardw**are-count enable command is enabled for the ACL, the statistic counts both rule matches performed in both software and hardware. Otherwise, the statistics counts only rule matches performed in software.
rule 10 comment This rule is used in rd.	The description of ACL rule 10 is "This rule is used in rd."

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 IPv6 ACL by its number:

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

all: Displays information for all IPv6 ACLs.

name *acl6-name*: Specifies an IPv6 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 IPv6 ACLs on an IRF member switch. The *slot-number* argument represents the ID of the IRF member switch. Available values for the *slot-number* argument are member IDs already assigned in the IRF fabric. If no IRF member switch is specified, the command displays match statistics for IPv6 ACLs on all member switches.

|: 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 ACLs.

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

Examples

# Display the configuration and match statistics for all IPv6 ACLs.

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

 Basic IPv6 ACL  2001, named -none-, 3 rules, match-order is auto,
 ACL's step is 5
 rule 10 permit source1::/64
 rule 10 comment This rule is used in rd.
 rule 5 permit source 2::/64
 rule 0 permit
```

Table 2 Command output

Field	Description
Basic IPv6 ACL 2000	Category and number of the ACL. The following field information is about this IPv6 basic ACL 2000.
named flow	The name of the ACL is flow. "-none-" means the ACL is not named.
3 rules	The ACL contains three rules.
match-order is auto	The match order for the ACL is auto, which sorts ACL rules in depth-first order. This field is not present when the match order is config.
Statistics is enabled	The rule match counting is enabled for this ACL.
ACL's step is 5	The rule numbering step is 5.
rule 0 permit	Content of rule 0.
5 times matched	There have been five matches for the rule. If the **counting** keyword is configured for the rule or the **hardware-count enable** command is enabled for the ACL, the statistic counts both rule matches performed in both software and hardware. Otherwise, the statistics counts only rule matches performed in software.
rule 10 comment This rule is used in rd.	The description of ACL rule 10 is "This rule is used in rd."

display acl resource

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays the usage of ACL rules on an IRF member switch. The *slot-number* argument represents the ID of the IRF member switch. Available values for the *slot-number* argument are member IDs already assigned in the IRF fabric. If no IRF member switch is specified, the command displays the usage of ACL rules on all member switches.

|: 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.

Examples

# Display the usage of ACL rules on a device.

```
<Sysname> display acl resource
 Interface:
   GE2/0/1 to GE2/0/28, XGE2/2/1 to XGE2/2/2
---------------------------------------------------------------------
 Type          Total       Reserved    Configured  Remaining   Usage
---------------------------------------------------------------------
 VFP ACL       1024        0           0           1024        0%
 IFP ACL       4096        1536        0           2560        37%
 IFP Meter     2048        768         0           1280        37%
 IFP Counter   2048        768         0           1280        37%
 EFP ACL       512         0           0           512         0%
 EFP Meter     256         0           0           256         0%
 EFP Counter   512         0           0           512         0%
```

Table 3 Command output

Field	Description
Interface	Interface indicated by its type and number

Field	Description
Type	Rule type: - **VFP ACL**—ACL rules for QinQ before Layer 2 forwarding - **IFP ACL**—ACL rules for inbound traffic - **IFP Meter**—Traffic policing rules for inbound traffic - **IFP Counter**—Traffic counting rules for inbound traffic - **EFP ACL**—ACL rules for outbound traffic - **EFP Meter**—Traffic policing rules for outbound traffic - **EFP Counter**—Traffic counting rules for outbound traffic
Total	Total number of ACL rules supported
Reserved	Number of reserved ACL rules
Configured	Number of ACL rules that have been applied
Remaining	Number of ACL rules that you can apply
Usage	Usage of the ACL rules

display packet-filter

Syntax

display packet-filter { { **all** | **interface** *interface-type interface-number* } [**inbound** | **outbound**] | **interface vlan-interface** *vlan-interface-number* [**inbound** | **outbound**] [**slot** *slot-number*] } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

all: Specifies all interfaces.

interface *interface-type interface-number*: Specifies an interface by its type and number. VLAN interfaces are not supported.

inbound: Specifies the inbound direction.

outbound: Specifies the outbound direction.

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

slot *slot-number*: Specifies an IRF member switch. The *slot-number* argument is the ID of the IRF member switch. Available values for the *slot-number* argument are member IDs already assigned in the IRF fabric. If no IRF member switch is specified, the command displays application status of incoming and outgoing packet filtering ACLs for VLAN interfaces of the master.

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

- The ACL application status may be different on the master and on an IRF member switch because of ACL resource insufficiency. You can specify the slot number in the **display packet-filter** command to check the ACL application status on the member switch.
- If you specify neither the **inbound** keyword nor the **outbound** keyword, the command displays the application status of both incoming and outgoing packet filtering ACLs.

Examples

# Display the application status of incoming and outgoing packet filtering ACLs for interface GigabitEthernet 1/0/1.

```
<Sysname> display packet-filter interface gigabitethernet 1/0/1
  Interface: GigabitEthernet1/0/1
  In-bound Policy:
    acl 2001, Successful
  Out-bound Policy:
    acl6 2500, Fail
```

Table 4 Command output

Field	Description
Interface	Interface to which the ACL applies.
In-bound Policy	ACL used for filtering incoming traffic on the interface.
Out-bound Policy	ACL used for filtering outgoing traffic on the interface.
acl 2001, Successful	IPv4 ACL 2001 has been applied to the interface.
acl6 2500, Fail	The device has failed to apply IPv6 ACL 2500 to the interface.

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, 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 **t4**.

```
<Sysname> display time-range t4
Current time is 17:12:34 4/13/2010 Tuesday

Time-range : t4 ( Inactive )
 10:00 to 12:00 Mon
 14:00 to 16:00 Wed
 from 00:00 1/1/2010 to 23:59 1/31/2010
 from 00:00 6/1/2010 to 23:59 6/30/2010
```

Table 5 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

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

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.

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. For an individual rule, rule match counting works as long as either the **hardware-count enable** command or the **counting** keyword is configured.

When an ACL is referenced by a QoS policy, this command or the **counting** keyword does not take effect. No ACL rule matches are counted.

Related commands: **display acl**, **display acl ipv6**, 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
```

packet-filter

Syntax

packet-filter { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

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

View

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

Default level

2: System level

Parameters

acl-number: Specifies an IPv4 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

name *acl-name*: Specifies an IPv4 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.

inbound: Filters incoming packets.

outbound: Filters outgoing packets.

Description

Use **packet-filter** to apply an IPv4 basic, IPv4 advanced, or Ethernet frame header ACL to an interface to filter packets.

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

By default, an interface does not filter packets.

Related commands: **display packet-filter**.

Examples

# Apply IPv4 ACL 2001 to filter incoming traffic on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter 2001 inbound
```

packet-filter ipv6

Syntax

packet-filter ipv6 { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** }

undo packet-filter ipv6 { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** }

View

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

Default level

2: System level

Parameters

acl6-number: Specifies an IPv6 ACL by its number:

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

name *acl6-name*: Specifies an IPv6 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.

inbound: Filters incoming IPv6 packets.

outbound: Filters outgoing IPv6 packets.

Description

Use **packet-filter ipv6** to apply an IPv6 basic or IPv6 advanced ACL to an interface to filter IPv6 packets.

Use **undo packet-filter ipv6** to restore the default.

By default, an interface does not filter IPv6 packets.

Related commands: **display packet-filter**.

Examples

# Apply IPv6 ACL 2500 to filter incoming packets on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] packet-filter ipv6 2500 inbound
```

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

all: Clears statistics for all IPv4 and Ethernet frame header ACLs.

name *acl-name*: Specifies an IPv4 or Ethernet frame header 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 IPv4 or Ethernet frame header ACL, or all IPv4 and Ethernet frame header ACLs.

Related commands: **display acl**.

Examples

# Clear statistics for IPv4 basic ACL 2001.

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

# Clear statistics for IPv4 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 IPv6 ACL by its number:

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

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

name *acl6-name*: Specifies an IPv6 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 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 IPv6 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-addr dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *sour-addr 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 Ethernet frame header ACL rule has been matched in hardware.

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

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

NOTE:

If the Ethernet frame header ACL is for QoS traffic classification or packet filtering, to use the **lsap** keyword, the *lsap-type* argument must be AAAA, and the *lasp-type-mask* argument must be FFFF. Otherwise, the ACL cannot be function normally.

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-addr dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **logging** | **precedence** *precedence* | **source** { *sour-addr sour-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name* | **tos** *tos* | **vpn-instance** *vpn-instance-name*] *

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

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 6 describes the parameters that you can specify regardless of the value that the *protocol* argument takes.

Table 6 Match criteria and other rule information for IPv4 advanced ACL rules

Parameters	Function	Description
source { *sour-addr sour-wildcard* | **any** }	Specifies a source address	The *sour-addr sour-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-addr dest-wildcard* | **any** }	Specifies a destination address	The *dest-addr 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 in hardware.	—
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 (for example, packet filter) that uses the ACL supports logging.
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. Only HP 5500 EI Switch Series supports this option.
fragment	Applies the rule to only non-first 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.

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 7.

Table 7 TCP/UDP-specific parameters for IPv4 advanced ACL rules

Parameters	Function	Description
source-port *operator port1* [*port2*]	Specifies one or more UDP or TCP source ports	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), or **range** (inclusive range). The *port1* and *port2* arguments are TCP or UDP port numbers in the range of 0 to 65535. *port2* is needed only when the *operator* argument is **range**. TCP port numbers can be represented 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).
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	Specifies one or more TCP flags including ACK, FIN, PSH, RST, SYN, and URG	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in one rule are ANDed.
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 8.

Table 8 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 9.

Table 9 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.

If an IPv4 advanced ACL is for QoS traffic classification or packet filtering:

- Do not specify the **vpn-instance** keyword.
- Do not specify **neq** for the *operator* argument.
- The **logging** and **counting** keywords (even if specified) do not take effect for QoS traffic classification.

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

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

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

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

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

rule (IPv4 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **source** { *sour-addr sour-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 in hardware.

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

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

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

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

vpn-instance *vpn-instance-name*: Applies the rule to packets in a VPN instance. The *vpn-instance-name* argument takes a case-sensitive string of 1 to 31 characters. If no VPN instance is specified, the rule applies only to non-VPN packets. Only HP 5500 EI Switch Series support this option.

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**.

NOTE:

- If an IPv4 basic ACL is for QoS traffic classification, do not specify the **vpn-instance** keyword, and the **logging** and **counting** keywords (even if specified) do not take effect for QoS.
- If an IPv4 basic ACL is for packet filtering, do not specify the **vpn-instance** keyword.

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 dest-prefix* | *dest/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 source-prefix* | *source/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 10 describes the parameters that you can specify regardless of the value that the *protocol* argument takes.

Table 10 Match criteria and other rule information for IPv6 advanced ACL rules

Parameters	Function	Description
source { *source source-prefix* | *source/source-prefix* | **any** }	Specifies a source IPv6 address	The *source* 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 dest-prefix* | *dest/dest-prefix* | **any** }	Specifies a destination IPv6 address	The *dest* 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 in hardware	—
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 (for example, packet filter) that uses the ACL supports logging.
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.
fragment	Applies the rule to only non-first 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. Only HP 5500 EI Switch Series supports this option.

If the *protocol* argument takes **tcp** (6) or **udp** (17), you can set the parameters shown in Table 11.

Table 11 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). 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).
destination-port *operator port1* [*port2*]	Specifies one or more UDP or TCP destination ports	
{ **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } *	Specifies one or more TCP flags, including ACK, FIN, PSH, RST, SYN, and URG	Parameters specific to TCP. The value for each argument can be 0 (flag bit not set) or 1 (flag bit set). The TCP flags in one rule are ANDed.
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 **icmpv6** (58), you can set the parameters shown in Table 12.

Table 12 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 13.

Table 13 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.

If an IPv6 advanced ACL is for QoS traffic classification or packet filtering:

- Do not specify the **fragment**, **routing**, or **vpn-instance** keyword, or specify **neq** for the *operator* argument.
- Do not specify the **flow-label** keyword if the ACL is for outbound QoS traffic classification or outbound packet filtering.
- The **logging** and **counting** keywords (even if specified) do not take effect for QoS traffic classification.

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 permit ipv6
[Sysname-acl6-adv-3001] rule deny icmpv6 destination fe80:5060:1001:: 48
```

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

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

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

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

rule (IPv6 basic ACL view)

Syntax

rule [*rule-id*] { **deny** | **permit** } [**counting** | **fragment** | **logging** | **routing** [**type** *routing-type*] | **source** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* **|** **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 in hardware.

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

logging: Logs matching packets. This function requires that the module (for example, packet filter) that uses the ACL supports logging.

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

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

time-range *time-range-name*: Specifies a time range for the rule. The *time-range-name* argument 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**.

NOTE:

- If an IPv6 basic ACL is for QoS traffic classification, do not specify the **fragment**, **routing** or **vpn-instance** keyword. The keyword can cause ACL application failure. The **logging** and **counting** keywords (even if specified) do not take effect for QoS.
- If an IPv6 basic ACL is for packet filtering, do not specify the **fragment**, **routing** or **vpn-instance** keyword.

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 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

Default level

2: System level

Parameters

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

text: Adds a comment about 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 add a comment about the rule.

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

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

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

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

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

Use **undo rule remark** to delete a rule range remark.

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**, **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), and each value is in the range of 00:00 to 23:59. 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, for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday, respectively.
- 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 of 1 to 12, DD is the day of the month with the range depending on MM, and YYYY is the year in the calendar in the range of 1970 to 2100. If not specified, the start time is 01/01/1970 00:00 AM, the earliest time available in the system.

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

Description

Use **time-range** to configure a 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.

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

You can create a maximum of 256 time ranges, each with a maximum of 32 periodic statements and 12 absolute statements.

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 23:59 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 23:59 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 23:59 1/31/2010
[Sysname] time-range t4 14:0 to 16:0 3 from 0:0 6/1/2010 to 23:59 6/30/2010
```

QoS policy configuration commands

- Both bridge mode (Layer 2) and route mode (Layer 3) Ethernet ports support the QoS policy function. The term "interface" in this document collectively refers to these two types of ports. You can use the **port link-mode** command to set an Ethernet port to operate in bridge or route mode (see *Layer 2—LAN Switching Configuration Guide*.)
- Only the HP 5500 EI switch supports Layer 3 Ethernet ports.

Class configuration commands

display traffic classifier

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

user-defined: Displays user-defined classes.

tcl-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 traffic classifier** to display class information.

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

Examples

# Display information about all user-defined classes.

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

```
Classifier: database
 Operator: AND
 Rule(s) : if-match acl 3131
```

Table 14 Command output

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

if-match

Syntax

if-match *match-criteria*

undo if-match *match-criteria*

View

Class view

Default level

2: System level

Parameters

match-criteria: Specifies a match criterion. Table 15 shows the available criteria.

Table 15 The value range for the *match-criteria* argument

Keyword and argument combination	Description
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	Matches an ACL. The *acl-number* argument ranges from 2000 to 3999 for an IPv4 ACL, 2000 to 3999 for an IPv6 ACL, and 4000 to 4999 for an Ethernet frame header ACL. The *acl-name* argument is a case-insensitive string of 1 to 63 characters, which must start with an English letter from a to z or A to Z, and to avoid confusion, cannot be **all**.
any	Matches all packets.
dscp *dscp-list*	Matches DSCP values. The *dscp-list* argument is a list of up to eight DSCP values. A DSCP value can be a number from 0 to 63 or any keyword in Table 17.
destination-mac *mac-address*	Matches a destination MAC address.

Keyword and argument combination	Description
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 ranges from 0 to 7.
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 ranges from 0 to 7.
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.
protocol *protocol-name*	Matches a protocol. The *protocol-name* argument can be IP or IPv6.
source-mac *mac-address*	Matches a source MAC address.
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 4094.
service-vlan-id { *vlan-id-list* | *vlan-id1* **to** *vlan-id2* }	Matches the VLAN IDs of ISP networks. The *vlan-id-list* 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 4094.
system-index *index-value-list*	Matches a pre-defined match criterion (system-index) for packets sent to the control plane. The *index-value-list* argument specifies a list of up to eight system indexes. The system index ranges from 1 to 128.

NOTE:

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

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

- **customer-dot1p** *8021p-list*
- **destination-mac** *mac-address*
- **dscp** *dscp-list*
- **ip-precedence** *ip-precedence-list*
- **service-dot1p** *8021p-list*
- **source-mac** *mac-address*

- **system-index** *index-value-list*

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

Description

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

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

When defining match criteria, use the usage guidelines described in these subsections.

Defining an ACL-based match criterion

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

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

Defining a criterion to match a destination MAC address

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

Defining a criterion to match a source MAC address

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

Defining a criterion to match DSCP values

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

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

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

Defining a criterion to match IP precedence values

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

Defining a criterion to match customer network VLAN IDs or service provider network VLAN IDs

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

Referencing a pre-define match criterion for packets sent to the control plane

- You can configure multiple match criteria in a class for packets sent to the control plane.
- You can configure multiple system indexes in one command. If the same system index is specified multiple times, the system considers them as one. If a packet matches one of the defined system indexes, it matches the **if-match** clause.
- To delete a criterion that matches system indexes, the specified system indexes in the command must be identical with those defined in the criterion (the sequence may be different).
- You can use the **display qos policy control-plane pre-defined** command to display the pre-defined match criteria for packets sent to the control plane of the switch.

Related commands: **traffic classifier**.

Examples

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Define a match criterion for class **class1** to match the packets of SVLAN 2, 7, or 10.

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

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

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

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

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

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

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

# Define a match criterion for class **class1** to match packets matching the pre-defined system-index 1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match system-index 1
```

traffic classifier

Syntax

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

undo traffic classifier *tcl-name*

View

System view

Default level

2: System level

Parameters

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

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

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

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

Description

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

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

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

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

Examples

# Create a class **class1**.

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

Traffic behavior configuration commands

accounting

Syntax

accounting

undo accounting

View

Traffic behavior view

Default level

2: System level

Parameters

None

Description

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

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

You can use the accounting action to collect statistics for a traffic class, for example, the traffic sourced from a certain IP address.

You can use the **display qos policy interface** command and the **display qos vlan-policy** command to display class-based traffic statistics.

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

Examples

# Configure the accounting action in the 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*] [**green** *action*] [**yellow** *action*] [**red** *action*]

undo car

View

Traffic behavior view

Default level

2: System level

Parameters

cir *committed-information-rate*: Specifies the committed access rate (in kbps), which limits the average traffic rate. The CIR ranges from 64 to 10000000, and must be a multiple of 64.

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

- If you do not specify the **cbs** keyword, the CBS is 62.5 × *committed-information-rate* by default and cannot not exceed 16000000.
- If you specify the **cbs** keyword, the CBS ranges from 4000 to 16000000.

ebs *excess-burst-size*: Specifies the excess burst size (EBS) in bytes. The *excess-burst-size* argument ranges from 0 to 16000000, and defaults to 4000.

pir *peak-information-rate*: Specifies the peak information rate (PIR) in kbps. The *peak-information-rate* argument ranges from 64 to 10000000 and must be a multiple of 64.

green *action*: Specifies the action to take on a packet that conforms to CIR. The default is **pass**.

yellow *action*: Specifies the action to take on a packet that conforms to PIR but not to CIR. The default is **pass**.

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

action: Sets the action to take on the packet:

- **discard**—Drops the packet.
- **pass**—Permits the packet to pass through.
- **remark-dscp-pass** *new-dscp*—Sets the DSCP value of the packet to *new-dscp* and permits the packet to pass through. The *new-dscp* argument ranges from 0 to 63 or is a keyword in Table 17.

Description

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

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

You can use a CAR action to rate limit inbound or outbound traffic.

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

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

Examples

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

- Set the CIR to 128 kbps, CBS to 50000 bytes, and EBS to 0.
- Allow the conforming packets to pass, and mark the excess packets with DSCP precedence 0 and forward them.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 128 cbs 50000 ebs 0 green pass red remark-dscp-pass
0
```

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, this command displays information about all the user-defined behaviors.

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

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

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

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

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

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: 2
      Accounting enable:
```

```
    Committed Access Rate:
      CIR 12800 (kbps), CBS 40960 (byte), EBS 4000 (byte)
      Green Action: pass
      Red Action: discard
      Yellow Action: pass
    Redirect enable:
      Redirect type: cpu
      Redirect destination: cpu
    Marking:
      Remark dot1p COS 1
    Marking:
      Remark DSCP af12
```

Table 16 Command output

Field	Description
User Defined Behavior Information	User-defined behavior information.
Behavior	Traffic behavior name.
Marking	Information about traffic marking.
Remark	Type of precedence marked for traffic, which can be DSCP, IP precedence, dot1p (COS), local precedence, drop precedence, customer VLAN ID or service VLAN ID. For more information about these precedence types, see "Traffic behavior configuration commands."
Accounting enable	Class-based accounting mode.
Committed Access Rate	Information about the CAR action.
Green Action	Action to take on green packets, which can be **pass** or **discard**.
Red Action	Action to take on red packets, which can be **pass** or **discard.**
Redirect enable	Traffic redirecting configuration.
Redirect type	Traffic redirecting type, which can be redirecting traffic to the CPU, an interface, or the next hop.
Redirect destination	Destination for traffic redirecting, which can be an interface name, the next hop IP address, or the CPU.

filter

Syntax

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

undo filter

View

Traffic behavior view

Default level

2: System level

Parameters

deny: Drops packets.

permit: Permits packet to pass through.

Description

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

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

Examples

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

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

redirect

Syntax

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

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

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

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

View

Traffic behavior view

Default level

2: System level

Parameters

cpu: Redirects traffic to the CPU.

interface: Redirects traffic to an interface.

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

next-hop: Redirects traffic to a next hop.

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, the switch redirects the traffic 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, the switch redirects the traffic to *ipv6-add2*. If the specified next hop IPv6 address is a link-local address, you must also specify the outgoing interface. Otherwise, you do not need to specify the outgoing interface.

fail-action { **discard** | **forward** }: Specifies the action to take on a packet whose next hop address does not exist. If no **fail-action** is specified, the default action **forward** applies.

- **discard**: Drops the packet.
- **forward**: Forwards the packet.

Description

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

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

NOTE:

- The HP 5500 SI switch does not support the **next-hop** or **fail-action** keyword.
- Redirecting traffic to CPU, redirecting traffic to an interface and redirecting traffic to the next hop are mutually exclusive with one another in a traffic behavior.

Examples

# Configure redirecting traffic to GigabitEthernet 1/0/1 in the traffic behavior **database**.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface gigabitethernet1/0/1
```

remark dot1p

Syntax

remark dot1p { *8021p* | **customer-dot1p-trust** }

undo remark dot1p

View

Traffic behavior view

Default level

2: System level

Parameters

8021p: 802.1p priority to be marked for packets, which ranges from 0 to 7.

customer-dot1p-trust: Copies the 802.1p priority value in the inner VLAN tag to the outer VLAN tag after the QoS policy is applied to a port. This keyword does not take effect on single-tagged packets.

Description

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

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

The **remark dot1p** *8021p* command and the **remark dot1p customer-dot1p-trust** command override each other, whichever is configured the last.

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

Examples

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

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

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

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

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. The value range is 0 to 2. The switch preferentially drops packets with the highest drop precedence.

Description

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

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

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

Examples

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

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

remark dscp

Syntax

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

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

View

Traffic behavior view

Default level

2: System level

Parameters

green: Specifies green packets.

red: Specifies red packets.

yellow: Specifies yellow packets.

dscp-value: DSCP value, which can be a number from 0 to 63 or any keyword in Table 17.

Table 17 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 a DSCP marking action.

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

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

Examples

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

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

remark ip-precedence

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, which ranges from 0 to 7.

Description

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

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

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

Examples

# Set the IP precedence to 6 for packets.

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

remark local-precedence

Syntax

remark local-precedence *local-precedence*

undo remark local-precedence

View

Traffic behavior view

Default level

2: System level

Parameters

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

Description

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

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

If a traffic behavior has both **remark local-precedence** and **remark dot1p** actions, the re-marked local precedence and 802.1p priority must be the same for the class-behavior association to be successfully applied.

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

Examples

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

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

traffic behavior

Syntax

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

View

System view

Default level

2: System level

Parameters

behavior-name: Sets a 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 delete a traffic behavior.

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

Examples

# Create a traffic behavior named **behavior1**.

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

QoS policy configuration and application commands

classifier behavior

Syntax

classifier *tcl-name* **behavior** *behavior-name* [**mode dot1q-tag-manipulation**]

undo classifier *tcl-name*

View

Policy view

Default level

2: System level

Parameters

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

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

mode dot1q-tag-manipulation: Specifies that the class-behavior association is for VLAN mapping purposes. For more information about VLAN mapping, see *Layer 2—LAN Switching Configuration Guide*.

Description

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

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

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

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

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

NOTE:

In a QoS policy that has multiple class-behavior associations, do not configure the **nest**, **remark customer-vlan-id**, or **remark service-vlan-id** action together with any other action in the same traffic behavior, so the QoS policy can function as expected.

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
[Sysname-qospolicy-user1]
```

control-plane

Syntax

control-plane slot *slot-number*

View

System view

Default level

2: System level

Parameters

slot *slot-number*: Enter the control plane view of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the switches in the IRF fabric.

Description

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

Examples

# Enter the control plane view of IRF member 2.

```
<Sysname> system-view
[Sysname] control-plane 2
```

```
[Sysname-cp-slot2]
```

display qos policy

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

user-defined: Displays user-defined QoS policies.

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

tcl-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 information.

Examples

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

```
<Sysname> display qos policy user-defined
User Defined QoS Policy Information:
Policy: test
 Classifier: 1
   Behavior: be
-none-

 Classifier: USER1
   Behavior: USER1
    Committed Access Rate:
      CIR 256 (kbps), CBS 15000 (byte), EBS 0 (byte)
      Green Action: pass
      Red  Action: discard
    Marking:
      Remark IP Precedence 3
```

Table 18 Command output

Field	Description
Policy	Policy name.
Classifier	Class name. A policy can have multiple classes, and each class is associated with a traffic behavior. A class can have multiple match criteria. For more information, see the **traffic classifier** command in "Class configuration commands."
Behavior	Behavior associated with the class. A behavior specifies a set of actions to take on the traffic that matches the associated class. For more information, see the **traffic behavior** command in "Traffic behavior configuration commands."

display qos policy control-plane

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays information about the QoS policy or policies applied to the control plane of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF fabric.

inbound: Displays information about the QoS policy applied in the inbound direction of the control plane.

|: 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 control-plane** to display information about the QoS policy or policies applied to the specified control plane.

Examples

# Display information about the inbound QoS policy for the control plane of IRF member 3.

```
<Sysname> display qos policy control-plane slot 3 inbound
Control-plane slot 3
  Direction: Inbound
  Policy: 1
```

```
    Classifier: 2
      Operator: AND
      Rule(s) : If-match system-index 10
      Behavior: 2
        Committed Access Rate:
          CIR 128 (kbps), CBS 8000 (byte), EBS 0 (byte)
          Red Action: discard
          Green : 12928(Bytes)
          Red   : 43904(Bytes)
        Filter Enable: deny
```

Table 19 Command output

Field	Description
Control-plane	Control plane.
Direction	Direction (inbound or outbound) in which the policy is applied. Only the inbound direction is supported.
Policy	Policy name and its contents.
Classifier	Class name and its contents.
Operator	Logical relationship between match criteria.
Rule(s)	Match criteria.
Behavior	Name of the behavior, and the actions configured in the behavior.
Committed Access Rate	Information about CAR.
CIR	Committed information rate (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.
Red	Statistics about red packets.
Filter Enable	Information about packet filtering (deny indicates dropping packets, and permit indicates forwarding packets).
none	Indicates no other behavior is configured.

display qos policy control-plane pre-defined

Syntax

display qos policy control-plane pre-defined [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

Any view

Default level

1: Monitor level

Parameters

slot *slot-number*: Displays information about the pre-defined QoS policy applied to the control plane of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF fabric.

|: 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 control-plane pre-defined** to display information about the pre-defined QoS policy applied to the control plane.

If no IRF member ID is specified, this command displays information about the pre-defined QoS policy applied to the control plane of each member switch in the IRF fabric.

Examples

# Display information about the pre-defined QoS policy applied to the control plane of IRF member 2.

```
<Sysname> display qos policy control-plane pre-defined slot 2
===================================================================
 Pre-defined Control-plane Policy Slot 2
-------------------------------------------------------------------
  Index |   PacketType              |  Priority  |  BandWidth(Kbps)
-------------------------------------------------------------------
  1          ISIS                         4           256
  4          VRRP                         5           256
  7          IPV4_MC_RIP                  4           256
  8          IPV4_BC_RIP                  4           256
  9          MCAST_NTP                    3           64
  10         BCAST_NTP                    3           64
  11         IPV4_MC_OSPF_5               4           256
  12         IPV4_MC_OSPF_6               4           256
  13         IPV4_UC_OSPF                 4           256
  14         IPV4_MC_PIM                  3           128
  15         IPV4_UC_PIM                  3           128
  16         IPV4_IGMP                    3           64
  17         LDP                          3           128
  18         IPV6_MC_PIM                  3           128
  19         IPV6_UC_PIM                  3           128
  20         IPV6_MLD                     3           64
  21         IPV6_RIPNG                   3           256
  22         IPV6_UC_OSPFV3               3           256
  23         IPV6_MC_OSPFV3_5             3           256
```

24	IPV6_MC_OSPFV3_6	3	256
25	IPV6_LDP	3	64
26	IPV6_VRRP	3	256
27	RRPP	6	64
28	IPV4_AUTORP	3	64
29	ARP	1	64
30	ARP_REPLY	1	64
31	DHCP_CLIENT	3	256
32	DHCP_SERVER	3	256
33	DHCP_RELAY_CLIENT	3	256
34	DHCP_RELAY_SERVER	3	256
35	DOT1X	1	64
36	STP	6	128
37	LACP	5	64
38	GVRP	3	256
39	HGMP	5	128
40	BGP	3	256
41	ICMP	1	640
44	IPV6_BGP	3	256
45	IPV6_ND_PASS	1	128
46	IPV6_ND_DEST	1	128
47	IPV6_PING	1	128
50	IPV6_DHCP	3	64
53	LLDP	3	128
54	DLDP	3	64
61	TELNET/SSH	1	512
62	HTTP/HTTPS	1	128
63	SNMP	1	512
64	SMARTLINK	6	64
67	ARP_DAI	1	128
71	IPV4_UC_DHCP	3	256
72	IPV4_UCOSPF_TTL	4	256
73	IPV4_UC_PIM_TTL	3	64
74	BGP_TTL	3	256
76	IPV6_ICMP	1	640
77	IPV6_TELNET/SSH	1	512
80	HGMP_BC	6	64
82	PVST	3	768
88	HGMP_BRIDGEMAC	6	256
90	DHCPV6_UC_CLIENT	3	256
91	DHCPV6_UC_RELAY	3	256
92	DHCPV6_RSERVER	3	256
94	BFD_ARP_REPLY	2	256
98	BFD_ECHO	5	256
99	BFD_CTRL	5	256
100	BFD_MULTIHOP	5	256
102	IPV6_ND_DAI	3	128
103	IPV6_DHCP_CLIENT	3	256

```
  104         IPV6_DHCP_SERVER             3           256
  105         IRDP                         4           256
  106         IPV6_CPUDST_CAR              3           128
=================================================================
```

Table 20 Command output

Field	Description
Pre-defined Control-plane Policy	Contents of the pre-defined control plane QoS policy
Index	Pre-defined system index
PacketType	Match criterion

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. This keyword is not available on the HP 5500 SI switch.

slot *slot-number*: Displays the global QoS policy configuration of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF fabric.

|: 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 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 the *slot-number* argument is not specified, the global QoS policy configuration of all devices in the IRF fabric is displayed.

Examples

# Display information about the inbound global QoS policy.

```
<Sysname> display qos policy global

Direction: Inbound

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

Direction: Outbound

  Policy: 2
   Classifier: 2 (Failed)
     Operator: AND
     Rule(s) : If-match customer-dot1p 3
     Behavior: 1
      Marking:
        Remark local precedence 2
```

Table 21 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	The name and content of a class. If the switch has failed to apply the class-behavior association, the field displays "**(Failed)**" behind the class name. In an IRF fabric: • If the **display** command is executed without any member switch specified, "**(Failed)**" indicates that the class-behavior association has failed to apply to the IRF fabric globally. • If a member switch is specified, "**(Failed)**" indicates that the class-behavior association has failed to apply to the specified IRF member switch. The failure to apply one class-behavior association does not affect the application of other associations in the QoS policy.
Operator	Logical relationship between match criteria.

Field	Description
Rule(s)	Match criteria.
Behavior	Name of the traffic behavior, and the actions in the traffic behavior.

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 to display information about the QoS policy or policies applied to it.

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

outbound: Displays information about the QoS policy applied in the outbound direction of the specified interface. This keyword is not available on the HP 5500 SI switch.

|: 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 information about the QoS policy or policies applied to an interface or all interfaces.

Examples

# Display information about the QoS policy or policies applied to GigabitEthernet 1/0/1.

```
<Sysname> display qos policy interface gigabitethernet 1/0/1
  Interface: GigabitEthernet1/0/1
  Direction: Inbound
  Policy: 1
   Classifier: 1
     Operator: AND
     Rule(s) : If-match acl 2000
     Behavior: 1
      Accounting Enable:
```

```
Mirror enable:
  Mirror type: interface
  Mirror destination: GigabitEthernet1/0/2
Redirect enable:
  Redirect type: cpu
  Redirect destination: cpu
Marking:
  Remark Customer VLAN ID 100
Marking:
  Remark dot1p COS 2
Marking:
  Remark IP precedence 3
Marking:
  Remark qos local ID 3
```

Table 22 Command output

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

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 information about the VLAN QoS policy specified by its name, a string of 1 to 31 characters.

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

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

outbound: Displays information about the QoS policy applied to the outbound direction of the specified VLAN. This keyword is not available on the HP 5500 SI switch.

slot *slot-number*: Displays the VLAN QoS policy information of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF fabric.

|: 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 VLAN QoS policy information.

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

If no member switch is specified, this command displays VLAN QoS policy information for the IRF fabric.

Examples

# Display information about the VLAN QoS policy **test** on IRF member switch 6.

```
<Sysname> display qos vlan-policy name test slot 6
  Policy test
    Vlan 200: inbound
    Vlan 300: outbound
```

Table 23 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.
outbound	The QoS policy is applied in the outbound direction of the VLAN.

# Display information about the QoS policies applied to VLAN 2.

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

Direction: Inbound

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

Direction: Outbound

  Policy: 2
   Classifier: 3 (Failed)
     Operator: AND
     Rule(s) : If-match customer-dot1p 3
     Behavior: 3
      Marking:
        Remark local precedence 2
```

Table 24 Command output

Field	Description
Vlan	ID of the VLAN where the QoS policy is applied.
Direction	Direction in which the QoS policy is applied for the VLAN.
Classifier	The name and content of a class. If the switch has failed to apply the class-behavior association, the field displays "**(Failed)**" after the class name. In an IRF environment: • If you specify the **slot** keyword in the display command, "**(Failed)**" indicates that the class-behavior association has failed to be applied to the IRF fabric. • If the **slot** keyword is not specified, "**(Failed)**" indicates that the class-behavior association has failed to be applied to the specified IRF member switch. A QoS policy can comprise multiple class-behavior associations. The failure to apply one class-behavior association does not affect the others.
Operator	Logical relationship between match criteria.
Rule(s)	Match criteria.
Behavior	Name of the behavior, and its actions.

qos apply policy (interface view, port group view, control plane view)

Syntax

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

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

View

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

Default level

2: System level

Parameters

inbound: Inbound direction.

outbound: Outbound direction. This keyword is not supported in control plane view. This keyword is not available on the HP 5500 SI switch.

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

Description

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

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

Examples

# Apply policy **USER1** in the inbound direction of GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos apply policy USER1 inbound
```

# Apply policy **aaa** to the inbound direction of the switch numbered 3 in the IRF fabric.

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

qos apply policy (user-profile view)

Syntax

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

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

View

User profile view

Default level

2: System level

Parameters

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

outbound: Applies the QoS policy to the traffic received by the online users. This keyword is not available on the HP 5500 SI switch.

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

Description

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

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

If a user profile is activated, the QoS policy, including the ACLs referenced in the QoS policy, applied to it cannot be configured or removed.

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

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

A null policy cannot be applied in user profile view.

Examples

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

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

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. This keyword is not available on the HP 5500 SI switch.

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.

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-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 delete a policy.

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

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

Examples

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

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

outbound: Applies the QoS policy to the outgoing packets in the specified VLANs. This keyword is not available on the HP 5500 SI switch.

Description

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

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

Examples

# Apply the QoS policy **test** to the inbound direction of VLAN 200, VLAN 300, VLAN 400, and VLAN 500.

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

reset qos policy control-plane

Syntax

reset qos policy control-plane slot *slot-number* [**inbound**]

View

User view

Default level

1: Monitor level

Parameters

slot *slot-number*: Clears the statistics of the QoS policy or policies applied to the control plane of the specified device in the IRF fabric. The range for the *slot-number* argument depends on the number of devices and the numbering of the devices in the IRF fabric.

inbound: Clears the statistics of the QoS policy applied to the inbound direction of the control plane.

Description

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

Examples

# Clear statistics for the inbound QoS policy of the control plane on IRF member 3.

```
<Sysname> reset qos policy control-plane slot 3 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. This keyword is not available on the HP 5500 SI switch.

Description

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

If no direction is specified, the statistics of the global QoS policies in both directions are cleared.

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, which ranges from 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. This keyword is not available on the HP 5500 SI switch.

Description

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

If no direction is specified, the statistics of the QoS policies in both directions of the VLAN are cleared.

Examples

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

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

Priority mapping configuration commands

- Both bridge mode (Layer 2) and route mode (Layer 3) Ethernet ports support the priority mapping function. The term "interface" in this chapter collectively refers to these types of ports. You can use the **port link-mode** command to set an Ethernet port to operate in bridge or route mode (see *Layer 2—LAN Switching Configuration Guide*).
- Only the HP 5500 EI switch supports Layer 3 Ethernet ports.

Priority mapping table configuration commands

display qos map-table

Syntax

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

View

Any view

Default level

1: Monitor level

Parameters

dot1p-dp: 802.1p-to-drop mapping table.

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

dscp-dot1p: DSCP-to-802.1p mapping table.

dscp-dp: DSCP-to-drop mapping table.

dscp-dscp: DSCP-to-DSCP 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, this command displays the configuration information of all priority mapping tables.

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

Examples

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

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

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

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

Table 25 Command output

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

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**.

Examples

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

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

qos map-table

Syntax

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

View

System view

Default level

2: System level

Parameters

dot1p-dp: 802.1p-to-drop mapping table.

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

dscp-dot1p: DSCP-to-802.1p mapping table.

dscp-dp: DSCP-to-drop mapping table.

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

Description

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

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

Examples

# Enter the 802.1p-to-drop mapping table view.

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

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 an interface.

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

The default port priority is 0.

You can use the **display qos trust interface** command to view the port priority of an interface.

When a switch receives an untagged packet on an interface, the switch uses the port priority of the interface as the 802.1p priority of the received packet, and then looks up the 802.1p-to-local and 802.1p-to-drop priority mapping tables and mark the packet with the corresponding local precedence and drop precedence.

Examples

# Set the port priority of interface GigabitEthernet 1/0/1 to 2.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos priority 2
```

Port 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 priority trust mode and port priority information on an interface.

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

Examples

# Display the priority trust mode and port priority settings of GigabitEthernet 1/0/1.

```
<Sysname> display qos trust interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Port priority information
  Port priority :0
  Port priority trust type : dscp
```

Table 26 Command output

Field	Description
Interface	Interface type and interface number
Port priority	Port priority set for the interface
Port priority trust type	Priority trust mode on the interface: • **dscp**—Uses the DSCP precedence of incoming packets for priority mapping. • **dot1p**—Uses the 802.1p priority of incoming packets for priority mapping. • **untrust**—Uses the port priority for priority mapping.

qos trust

Syntax

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

undo qos trust

View

Interface view, port group view

Default level

2: System level

Parameters

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

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

Description

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

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

By default, the port priority of the incoming interface is used for priority mapping.

In interface view, the setting takes effect on the current interface only. In port group view, the setting takes effect on all ports in the port group.

Examples

# Set the trusted packet priority type to DSCP priority on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos trust dscp
```

GTS and rate limit configuration commands

- Both bridge mode (Layer 2) and route mode (Layer 3) Ethernet ports support the GTS and rate limit functions. The term "interface" in this chapter collectively refers to these two types of ports. You can use the **port link-mode** command to set an Ethernet port to operate in bridge or route mode (see *Layer 2—LAN Switching Configuration Guide*).
- Only the HP 5500 EI switch supports Layer 3 Ethernet ports.

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 and operational statistics on a specified interface or all the interfaces.

If no interface is specified, this command displays the GTS configuration information and operational statistics on all the interfaces.

Examples

# Display the GTS configuration information and operational statistics on all the interfaces.

```
<Sysname> display qos gts interface
Interface: GigabitEthernet1/0/1
Rule(s): If-match queue 2
 CIR 640 (kbps), CBS 40960 (byte)
```

Table 27 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 bursty traffic

qos gts

Syntax

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

undo qos gts queue *queue-number*

View

Interface view, port group view

Default level

2: System level

Parameters

queue *queue-number*: Shapes the packets in the specified queue. The *queue-number* argument ranges from 0 to 7.

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

- On a GE port, the argument ranges from 64 to 1000000, and must be a multiple of 64.
- On a 10-GE port, the argument ranges from 64 to 10000000, and must be a multiple of 64.

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

- If you do not specify the **cbs** keyword, the CBS is 62.5 × *committed-information-rate* by default and must be a multiple of 4096. If 62.5 × *committed-information-rate* is not a multiple of 4096, the closest higher multiple of 4096 applies. The CBS cannot exceed 16777216.
- If you specify the **cbs** keyword, the CBS ranges from 4096 to 16777216 and must be a multiple of 4096.

Description

Use **qos gts** to set GTS parameters for the traffic of the specified queue on the interface or port group.

Use **undo qos gts** to remove GTS parameters for the traffic of the specified queue on the interface or port group.

By default, no GTS parameters are configured 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.

Examples

# Configure GTS on interface GigabitEthernet 1/0/1 to limit the traffic rate to 640 kbps for queue 2.

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

```
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos gts queue 2 cir 640
```

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 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 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.

Examples

# Display the rate limit configuration information on all the interfaces.

```
<Sysname> display qos lr interface
Interface: GigabitEthernet1/0/1
Direction: Outbound
 CIR 64000 (kbps),  CBS 4000000 (byte)
```

Table 28 Command output

Field	Description
Interface	Interface type and interface number
Direction	Direction in which the rate limit configuration is applied
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:

- On a GE port, the argument ranges from 64 to 1000000, and must be a multiple of 64.
- On a 10-GE port, the argument ranges from 64 to 10000000, and must be a multiple of 64.

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

- If you do not specify the **cbs** keyword, the CBS is 62.5 × *committed-information-rate* by default and must be a multiple of 4000. If 62.5 × *committed-information-rate* is not a multiple of 4000, the closest higher multiple of 4000 applies. The CBS cannot exceed 16000000.
- If you specify the **cbs** keyword, the CBS ranges from 4000 to 16000000 and must be a multiple of 4000.

Description

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

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

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

Examples

# Limit the rate of outgoing packets on GigabitEthernet 1/0/1, with CIR 640 kbps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos lr outbound cir 640
```

Congestion management configuration commands

- Both bridge mode (Layer 2) and route mode (Layer 3) Ethernet ports support the congestion management functions. The term "interface" in this chapter collectively refers to these two types of ports. You can use the **port link-mode** command to set an Ethernet port to operate in bridge or route mode (see *Layer 2—LAN Switching Configuration Guide*).
- Only the HP 5500 EI switch supports Layer 3 Ethernet ports.

SP queuing configuration commands

display qos sp

Syntax

display qos sp 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 sp interface** to view the strict priority (SP) queuing configuration of an interface.

If no interface is specified, this command displays the SP queuing configuration of all the interfaces.

Related commands: **qos sp**.

Examples

# Display the SP queuing configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos sp interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Strict-priority queue
```

Table 29 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Pattern of the current output queue.
Strict-priority queue	SP queuing is used for queue scheduling.

qos sp

Syntax

qos sp

undo qos sp

View

Interface view, port group view

Default level

2: System level

Parameters

None

Description

Use **qos sp** to configure SP queuing on a port.

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

The default queuing algorithm on a port is WRR queuing.

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

Related commands: **display qos sp interface**.

Examples

# Enable SP queuing pattern 1 on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos sp
```

WRR queuing configuration commands

display qos wrr interface

Syntax

display qos wrr 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 wrr interface** to display the weighted round robin (WRR) queuing configuration on an interface.

If no interface is specified, this command displays the WRR queuing configuration of all the interfaces.

Related commands: **qos wrr**.

Examples

# Display the WRR queuing configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos wrr interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Output queue: Weighted round robin queue
Queue ID    Group    Weight
-------------------------------------
   0         1        1
   1         sp       N/A
   2         1        3
   3         1        4
   4         1        5
   5         1        6
   6         1        7
   7         1        8
```

Table 30 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Pattern of the current output queue.
Queue ID	ID of a queue.
Group	Number of the group a queue is assigned to: • **1**—WRR group • **sp**—SP group
Weight	Queue weight based on which queues are scheduled. **N/A** indicates that the queue uses the SP queue scheduling algorithm.

qos wrr

Syntax

qos wrr [**byte-count** | **weight**]

undo qos wrr

View

Interface view, port group view

Default level

2: System level

Parameters

byte-count: Enables byte-count WRR, which allocates bandwidth to queues in terms of bytes. If you specify neither **byte-count** nor **weight** for this command, this command enables byte-count WRR.

weight: Enables packet-based WRR, which allocates bandwidth to queues in terms of packets.

NOTE:

Only the HP 5500 EI switch supports the two keywords.

Description

Use **qos wrr** to enable WRR queuing.

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

The default queuing algorithm on a port is WRR queuing.

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

Examples

# Enable WRR queuing on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr
```

qos wrr byte-count

IMPORTANT:

Only the HP 5500 EI switch supports this command.

Syntax

qos wrr *queue-id* **group 1 byte-count** *schedule-value*

undo qos wrr *queue-id* **group 1 byte-count**

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Specifies a queue by its ID, which ranges from 0 to 7.

1: Specifies a group the queue belongs to group 1.

byte-count *schedule-value*: Specifies a scheduling weight for the specified queue in byte-count WRR queuing. The *schedule-value* argument ranges from 1 to 15.

Description

Use **qos wrr byte-count** to specify a scheduling weight for the specified queue in byte-count WRR queuing.

Use **undo qos wrr byte-count** to restore the default weight for the specified queue in byte-count WRR queuing.

By default, the weights of queues 0 through 7 are 1, 2, 3, 4, 5, 9, 13, and 15 in byte-count WRR queuing.

Before using this command to configure weights for queues, make sure that byte-count WRR queuing is enabled on the interface. Otherwise, the weight configuration does not take effect.

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

Related commands: **display qos wrr interface** and **qos wrr**.

Examples

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

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

qos wrr group sp

Syntax

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

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

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Specifies a queue by its ID, which ranges from 0 to 7.

sp: Specifies strict priority (SP) queuing.

Description

Use **qos wrr group sp** to assign a queue to the strict priority (SP) group on a WRR-enabled interface.

Use **undo qos wrr group sp** to remove a queue from the SP group on a WRR-enabled interface.

The Switch Series provides eight output queues per port. You can assign some queues on a port to the SP scheduling group and the others to the WRR scheduling group (group 1) to implement SP+WRR queuing. The switch schedules packets in the SP scheduling group preferentially, and when the SP scheduling group is empty, schedules the packets in the WRR scheduling group. Queues in the SP scheduling group are scheduled with the SP queue scheduling algorithm. Queues in the WRR scheduling group are scheduled with WRR.

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

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

Related commands: **display qos wrr interface** and **qos wrr**.

Examples

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

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

qos wrr weight

Syntax

qos wrr *queue-id* **group 1 weight** *schedule-value*

undo qos wrr *queue-id* **group 1 weight**

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Queue ID, which ranges from 0 to 7.

1: Assigns the queue to group 1, the WRR queuing group.

weight *schedule-value*: Specifies a scheduling weight for the specified queue in packet-based WRR queuing. The *schedule-value* argument ranges from 1 to 15.

Description

Use **qos wrr weight** to assign a queue to a WRR group, with a certain scheduling weight, on an interface that performs packet-based WRR queuing.

Use **undo qos wrr weight** to restore the default WRR queuing settings of a queue on an interface that performs packet-based WRR queuing.

By default, the weights of queues 0 through 7 are 1, 2, 3, 4, 5, 9, 13, and 15 on an interface that performs packet-based WRR queuing.

Before using this command to configure weights for queues, make sure that packet-based WRR queuing is enabled on the port. Otherwise, the weight configuration does not take effect.

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

Related commands: **display qos wrr interface** and **qos wrr**.

Examples

# Enable packet-based WRR queuing on GigabitEthernet 1/0/1, and assign queue 0, with the scheduling weight 10, to WRR group 1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wrr weight
[Sysname-GigabitEthernet1/0/1] qos wrr 0 group 1 weight 10
```

WFQ configuration commands

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, this command displays the WFQ configuration of all the interfaces.

Related commands: **qos wfq**.

Examples

# Display the WFQ configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos wfq interface gigabitethernet 1/0/-1
Interface: GigabitEthernet1/0/1
 Output queue: Hardware weighted fair queue
Queue ID        Group           Byte-count      Min-Bandwidth
----------------------------------------------------------------
```

```
0                 1                1                64
1                 1                1                64
2                 1                1                64
3                 1                1                64
4                 1                1                64
5                 1                1                64
6                 1                1                64
7                 1                1                64
```

Table 31 Command output

Field	Description
Interface	Interface type and interface number.
Output queue	Pattern of the current output queue.
Queue ID	ID of a queue.
Group	Number of the group a queue is assigned to: • **1**—WFQ group • **sp**—SP group
Byte-count	Scheduling weight of the queue in byte-count WFQ, which assigns bandwidth to queues in terms of bytes. If you enable packet-based WFQ on the interface, this field is replaced with **Weight**. For queues in the SP group, **NA** is displayed.
Min-Bandwidth	Minimum guaranteed bandwidth.

qos bandwidth queue

Syntax

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

undo qos bandwidth queue *queue-id* [**min** *bandwidth-value*]

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Queue ID, ranging from 0 to 7.

min *bandwidth-value*: Sets the minimum guaranteed bandwidth (in kbps) for a queue when the port is congested. This argument ranges from 64 to 1000000 for a GE port and 64 to 10000000 for a 10-GE port.

Description

Use **qos bandwidth queue** to set the minimum guaranteed bandwidth for a specified queue on the port/port group.

Use **undo qos bandwidth queue** to cancel the configuration.

By default, the minimum guaranteed bandwidth is 64 kbps for a queue.

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

Configure minimum guaranteed bandwidth only for queues of WFQ-enabled ports.

Examples

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

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq
[Sysname-GigabitEthernet1/0/1] qos bandwidth queue 0 min 100
```

qos wfq

Syntax

qos wfq [**byte-count** | **weight**]

undo qos wfq

View

Interface view, port group view

Default level

2: System level

Parameters

byte-count: Enables byte-count WFQ, which allocates bandwidth to queues in terms of bytes.

weight: Enables packet-based WFQ, which allocates bandwidth to queues in terms of packets.

Description

Use **qos wfq** to enable WFQ on a port.

Use **undo qos wfq** to restore the default queuing algorithm on a port.

The default queuing algorithm on a port is WRR queuing.

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

You must enable WFQ before you can configure WFQ queuing parameters for a queue on an interface.

Examples

# Enable byte-count WFQ on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq byte-count
```

qos wfq byte-count

Syntax

qos wfq *queue-id* **group 1 byte-count** *schedule-value*

undo qos wfq *queue-id* **group 1 byte-count**

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Specifies a queue by its ID, which ranges from 0 to 7.

group 1: Assigns a queue to the WFQ group.

byte-count *schedule-value*: Specifies a scheduling weight for the specified queue in byte-count WFQ queuing. The scheduling weight ranges from 1 to 15. The WRR queue scheduling process based on scheduling weights varies by switch model as follows:

- On an HP 5500 EI switch, the interface bandwidth is allocated to queues in proportion to their scheduling weights.
- On an HP 5500 SI switch, each scheduling weight corresponds to a scheduling unit, which specifies the number of bytes that can be scheduled from the queue in a cycle of queue scheduling. Table 32 shows the scheduling weight-to-scheduling unit map.

Table 32 The scheduling weight-to-scheduling unit map on an HP 5500 SI switch

Scheduling weight	Scheduling unit
1	10 KB
2	20 KB
3	40 KB
4	80 KB
5	160 KB
6	320 KB
7	640 KB
8	1280 KB
9	2560 KB
10	5120 KB
11	10 MB
12	20 MB
13	40 MB
14	80 MB
15	160 MB

Description

Use **qos wfq byte-count** to assign a queue to a WFQ group, with a certain scheduling weight, on an interface that performs byte-count WFQ queuing.

Use **undo qos wfq byte-count** to restore the default on an interface that performs byte-count WFQ queuing.

By default, the scheduling weights of queues 0 through 7 are all 1 on an interface that performs byte-count WFQ queuing.

Before using this command on an interface, make sure that the interface is enabled with byte-count WFQ queuing. Otherwise, the weight configuration does not take effect.

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

Related commands: **display qos wfq interface** and **qos wfq**.

Examples

# Enable byte-count WFQ on interface GigabitEthernet 1/0/1, and assign queue 0, with the scheduling weight 10.

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

qos wfq group sp

Syntax

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

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

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Specifies a queue by its ID, which ranges from 0 to 7.

sp: Specifies strict priority (SP) queuing.

Description

Use **qos wfq group sp** to assign a queue to the strict priority (SP) group on an interface that performs SP+WFQ queuing.

Use **undo qos wfq group sp** to remove a queue from the SP group on an interface that performs SP+WFQ queuing.

This command is available only on a WFQ-enabled interface. Queues in the SP group are scheduled with SP, instead of WFQ.

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

Related commands: **display qos wfq interface** and **qos wfq**.

Examples

# Enable WFQ on interface GigabitEthernet 1/0/1, and assign queue 0 to the SP group.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
```

```
[Sysname-GigabitEthernet1/0/1] qos wfq
[Sysname-GigabitEthernet1/0/1] qos wfq 0 group sp
```

qos wfq weight

Syntax

qos wfq *queue-id* **group 1 weight** *schedule-value*

undo qos wfq *queue-id* **group 1 weight**

View

Interface view, port group view

Default level

2: System level

Parameters

queue-id: Specifies a queue by its ID, which ranges from 0 to 7.

group 1: Assigns a queue to the WFQ group.

weight *schedule-value*: Specifies a scheduling weight for the specified queue. The scheduling weight ranges from 1 to 15.

Description

Use **qos wfq weight** to assign a queue to a WFQ group, with a certain scheduling weight, on an interface that performs packet-based WFQ queuing.

Use **undo qos wfq weight** to restore the default WFQ settings of a queue on an interface that performs packet-based WFQ queuing.

By default, the scheduling weights of queues 0 through 7 are all 1 on an interface that performs packet-based WFQ queuing.

Before configuring this command, make sure that the interface is enabled with packet-based WFQ queuing. Otherwise, the weight configuration does not take effect.

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

Related commands: **display qos wfq interface**, **qos bandwidth queue**, and **qos wfq**.

Examples

# Enable packet-based WFQ on GigabitEthernet 1/0/1, and assign queue 0, with the scheduling weight 10.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wfq weight
[Sysname-GigabitEthernet1/0/1] qos wfq 0 group 1 weight 10
```

Congestion avoidance configuration commands (available only on the HP 5500 EI)

Both bridge mode (Layer 2) and route mode (Layer 3) Ethernet ports support the congestion avoidance functions. The term "interface" in this chapter collectively refers to these two types of ports. You can use the **port link-mode** command to set an Ethernet port to operate in bridge or route mode (see *Layer 2—LAN Switching Configuration Guide*).

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 a port 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 of an interface.

If no interface is specified, this command displays the WRED configuration of all the interfaces.

Examples

# Display the WRED configuration of GigabitEthernet 1/0/1.

```
<Sysname> display qos wred interface GigabitEthernet 1/0/1
Interface: GigabitEthernet1/0/1
 Current WRED configuration:
 Applied WRED table name: queue-table1
```

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 information.

If no WRED table name is specified, this command displays the configuration of all the WRED tables.

Examples

# Display the configuration of WRED table 1.

```
<Sysname> display qos wred table 1
Table Name: 1
Table Type: Queue based WRED
QID:  gmin  gmax  gprob  ymin  ymax  yprob
------------------------------------------------
 0    10    NA    10     10    NA    10
 1    10    NA    10     10    NA    10
 2    10    NA    10     10    NA    10
 3    10    NA    10     10    NA    10
 4    10    NA    10     10    NA    10
 5    10    NA    10     10    NA    10
 6    10    NA    10     10    NA    10
 7    10    NA    10     10    NA    10
```

Table 33 Command output

Field	Description
Table name	Name of a WRED table
Table type	Type of a WRED table
QID	ID of the queue

Field	Description
gmin	Lower threshold configured for green packets, whose drop precedence is 0
gmax	Upper threshold configured for green packets, whose drop precedence is 0
gprob	Drop probability slope configured for green packets, whose drop precedence is 0
ymin	Lower threshold configured for yellow packets, whose drop precedence is 1
ymax	Upper threshold configured for yellow packets, whose drop precedence is 1
yprob	Drop probability slope configured for yellow packets, whose drop precedence is 1

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 used on a port.

In interface view, the setting takes effect on the current port only. In port group view, the setting takes effect on all the ports in the port group.

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 port GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] qos wred apply queue-table1
```

qos wred queue table

Syntax

qos wred queue table *table-name*

undo qos wred table *table-name*

View

System view

Default level

2: System level

Parameters

table *table-name*: Specifies a name for the table.

Description

Use **qos wred queue table** to create a WRED table and enter WRED table view.

Use **undo qos wred table** to delete a WRED table.

By default, no global WRED table is created.

A WRED table in use cannot be removed.

Related commands: **qos wfq**, **qos wred enable**, and **display qos wred interface**.

Examples

# Create an EXP-based WRED table named **exp-table1**.

```
<Sysname> system-view
[Sysname] qos wred exp table exp-table1
[Sysname-wred-table-exp-table1]
```

queue

Syntax

queue *queue-value* [**drop-level** *drop-level*] **low-limit** *low-limit* [**discard-probability** *discard-prob*]

undo queue { *queue-value* | **all** }

View

WRED table view

Default level

2: System level

Parameters

queue-value: Queue number, which ranges from 0 to 7.

drop-level *drop-level*: Drop level, which ranges from 0 to 1. 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 threshold of the queue buffer usage (in percentage). When the queue buffer usage exceeds the lower threshold, the switch starts to drop packets. This argument ranges from 1 to 100 and defaults to 50.

discard-probability *discard-prob*: Specifies the parameter for drop probability calculation. The *discard-prob* argument ranges from 0 to 128, and defaults to 10. You can set the parameter for each drop level. Table 34 shows the denominator and the drop probability dependencies.

Table 34 Denominator and the drop probability dependencies

discard-prob	Drop probability
0	100%
1 to 8	1/8
9 to 16	1/16
17 to 32	1/32
33 to 64	1/64
65 to 128	1/128

Description

Use **queue** to configure the queue-based WRED table.

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

By default, the lower threshold is 10 and the *discard-prob* argument is 10 for all drop levels in a WRED table.

Related commands: **qos wred queue table**.

Examples

# Configure drop-related parameters for queue-based WRED table **queue-table1** as follows: set the lower threshold to 10 and **discard-probability** to 30 for packets with drop level 1.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 drop-level 1 low-limit 10 discard-probability
30
```

Data buffer configuration commands

Automatic data buffer configuration commands

burst-mode enable

Syntax

burst-mode enable

undo burst-mode enable

View

System view

Default level

2: System level

Parameters

None

Description

Use **burst-mode enable** to enable the burst function.

Use **undo burst-mode enable** to disable the burst function.

By default, the burst function is disabled.

The burst function allows the switch to automatically determine the shared resource size, the minimum guaranteed resource size for each queue, the maximum shared resource size for each queue, and the maximum shared resource size per port. The function helps optimize the packet buffering scheme to ameliorate forwarding performance.

NOTE:

The **burst-mode enable** command is mutually exclusive with any manual data buffer configuration commands.

Examples

# Enable the burst function.

```
<Sysname> system-view
[Sysname] burst-mode enable
```

Manual data buffer configuration commands

△ CAUTION:

- Data buffer configuration is complicated and has significant impacts on the forwarding performance of a device. Do not modify the data buffer parameters unless you are sure that your device will benefit from the change. If a larger buffer is needed, enable the burst function to allocate buffer automatically.
- The commands in this section are mutually exclusive with the **burst-mode enable** command.

buffer apply

Syntax

buffer apply

undo buffer apply

View

System view

Default level

2: System level

Parameters

None

Description

Use **buffer apply** to apply the configured data buffer settings.

Use **undo buffer apply** to restore the default.

Table 35 shows the default data buffer allocation schemes of the HP 5500 SI/EI Switch Series.

Table 35 Default data buffer allocation schemes

Resource type	Shared resource size in percentage	Minimum guaranteed resource size per queue in percentage	Maximum shared resource size per queue in percentage
Cell resource	50%	12%	50%
Packet resource	N/A	51% for queue 2 and 7% for any other queue	N/A

Examples

# Apply the data buffer settings.

```
<Sysname> system-view
[Sysname] buffer apply
```

buffer egress queue guaranteed

Syntax

buffer egress [**slot** *slot-number*] { **cell** | **packet** } **queue** *queue-id* **guaranteed ratio** *ratio*

undo buffer egress [**slot** *slot-number*] { **cell** | **packet** } **queue** *queue-id* **guaranteed**

View

System view

Default level

2: System level

Parameters

slot *slot-number*: Specifies an IRF member switch number. For a standalone switch, the *slot-number* argument can only be 1. In an IRF fabric, if an IRF member switch is specified, this command applies only to the member switch; if no member switch is specified, this command applies to all member switches.

cell: Configures the minimum guaranteed resource size for a queue in the cell resource.

packet: Configures the minimum guaranteed resource size for a queue in the packet resource.

queue-id: Specifies a queue ID, in the range of 0 to 7.

ratio: Sets the minimum guaranteed resource size for the specified queue as a percentage of the dedicated buffer per port. The value range is 0 to 100.

Description

Use **buffer egress queue guaranteed** to configure the minimum guaranteed resource size for a queue in the cell resource or packet resource.

Use **undo buffer egress queue guaranteed** to restore the default.

By default, the minimum guaranteed resource size for a queue is 12% of the dedicated buffer of the port in the cell resource; the minimum guaranteed resource size is 51% for queue 2 and 7% for any other queue in the packet resource.

The minimum guaranteed resource settings apply to the queue with the same number on each port.

The dedicated resource of a port is shared by eight queues. After you change the minimum guaranteed resource size for a queue, the switch will automatically allocate the remaining dedicated resource among all queues that are not manually assigned a minimum guaranteed resource space. For example, if you set the minimum guaranteed resource size to 30% for a queue, the other seven queues will each share 10% of the remaining dedicated resource of the port.

Examples

# Set 20% of the dedicated buffer per port as the minimum guaranteed resource for queue 0 in the cell resource.

```
<Sysname> system-view
[Sysname] buffer egress cell queue 0 guaranteed ratio 20
```

# In an IRF, set 15% of the dedicated buffer per port as the minimum guaranteed resource for queue 0 in the cell resource on member switch 2.

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell queue 0 guaranteed ratio 15
```

buffer egress shared

Syntax

buffer egress [**slot** *slot-number*] **cell shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] **cell shared**

View

System view

Default level

2: System level

Parameters

slot *slot-number*: Specifies an IRF member switch number. For a standalone device, the *slot-number* argument can only be 1. In an IRF, with *slot-number* specified, this command configures the buffer resource of the member switch specified by *slot-number*; without *slot-number* specified, this command configures the buffer resource of all the member switches in the IRF fabric.

cell: Configures the maximum shared resource size per port in the cell resource.

ratio: Sets the maximum shared resource size per port as a percentage of the shared resource in the range of 0 to 100.

Description

Use **buffer egress shared** to configure the maximum shared resource size per port in the cell resource.

Use **undo buffer egress shared** to restore the default.

By default, the maximum shared resource size per port is 50% of the shared resource in the cell resource.

Examples

# Set the maximum shared resource size per port to 30% in the cell resource.

```
<Sysname> system-view
[Sysname] buffer egress cell shared ratio 30
```

# In an IRF, set the maximum shared resource size per port to 40% in the cell resource on member switch 2.

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell shared ratio 40
```

buffer egress total-shared

Syntax

buffer egress [**slot** *slot-number*] **cell total-shared ratio** *ratio*

undo buffer egress [**slot** *slot-number*] **cell total-shared**

View

System view

Default level

2: System level

Parameters

slot *slot-number*: Specifies an IRF member switch number. For a standalone device, the *slot-number* argument can only be 1. In an IRF, with *slot-number* specified, this command configures the buffer resource of the member switch specified by *slot-number*; without *slot-number* specified, this command configures the buffer resource of all the member switches in the IRF fabric.

cell: Configures the shared resource size in the cell buffer.

ratio: Sets the shared resource size as a percentage of the cell resource in the range of 0 to 100.

Description

Use **buffer egress total-shared** to configure the shared resource size in the cell resource or packet resource.

Use **undo buffer egress total-shared** to restore the default.

By default, on the Switch Series, 60% of the cell resource is the shared resource.

Examples

# Set 50% of the cell resource as the shared resource.

```
<Sysname> system-view
[Sysname] buffer egress cell total-shared ratio 50
```

# In an IRF, set 65% of the cell resource as the shared resource on member switch 2.

```
<Sysname> system-view
[Sysname] buffer egress slot 2 cell total-shared ratio 65
```

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking
- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com
- HP Education http://www.hp.com/learn

Conventions

This section describes the conventions used in this documentation set.

Command conventions

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

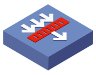
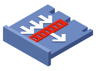
GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
⚠ WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
❗ IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
💡 TIP	An alert that provides helpful information.

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index